Chapitre 4
Identité et accès

1. Introduction

L'identité (ou plutôt les identités) et les accès représentent des points bien à part pour le Cloud Azure, car une partie du sujet identité est souvent traitée par des équipes qui ne sont pas les administrateurs Azure mais plutôt les administrateurs de l'annuaire d'entreprise, par exemple l'Active Directory Microsoft.

La seconde partie accès ou RBAC est plutôt traitée par les administrateurs Azure.

Il existe une séparation nette entre les deux équipes et il est très rare que l'ensemble des responsabilités soit porté par une seule et même équipe.

Le cas courant pour la gestion est donc une équipe Active Directory qui est déjà responsable de l'existant sur site (On-premises) et qui va continuer à assurer ce rôle pour l'Azure Active Directory (que l'on trouve régulièrement sous le terme AAD ou Azure AD).

Lors de la création d'un Cloud Azure, cette équipe va synchroniser l'AD existant sur le Cloud et ainsi créer un nouvel annuaire avec un type d'objets et d'attributs choisis. Il n'est pas nécessaire de faire une copie complète mais plutôt de conserver uniquement des objets et attributs utilisés sur Azure. Cette première synchronisation est suivie d'une planification régulière et fréquente (au fil de l'eau) pour avoir des données à jour. L'outil utilisé se nomme AD Connect.

Lors de la synchronisation, les mots de passe sont également transférés de manière très sécurisée puis sont de nouveau hachés avec une complexité importante. Le hachage est une fonction permettant de ne pas stocker en clair le mot de passe. Ce point est évoqué régulièrement : est ce qu'il existe un risque à stocker ses mots de passe dans Azure ? Pour stocker les mots de passe, l'annuaire Azure applique une sécurité bien supérieure à ce qu'il est possible de faire sur l'annuaire local. Il n'y a pas vraiment de question à se poser sur ce point de sécurité.

Remarque

Cette synchronisation de mot de passe n'est pas obligatoire. Il est aussi possible de ne pas synchroniser tous les mots de passe et de choisir une synchronisation sélective pour exclure certains profils.

Cette présentation sommaire de l'AAD est incomplète mais suffisante pour comprendre l'authentification Azure. Elle s'appuie sur un annuaire de ressources d'entreprise.

En matière d'identité, il faut bien faire la différence entre l'authentification et les accès, autrement dit l'autorisation aux ressources. Être authentifié, c'est avoir prouvé que l'on est bien en possession d'un compte et du mot de passe associé. Une fois cette vérification effectuée, l'utilisateur est authentifié.

Être autorisé, c'est avoir des droits sur une ressource. La gestion des droits d'accès est appelée RBAC (*Azure Role-Based Access Control* ou contrôle d'accès basé sur un rôle Azure).

Dans cette méthode d'accès basés sur les rôles, il existe trois composantes :

– L'objet de sécurité qui va être utilisé.
– Son attachement à une liste de rôles (quels rôles lui sont attribués).
– L'étendue couverte, c'est-à-dire la limite fixée pour l'application de ces accès. Par exemple, un groupe de ressources (attention, il y a un mécanisme d'héritage : si l'étendue est le groupe de ressources, l'utilisateur hérite de droits sur les ressources enfants de ce groupe).

Dans le schéma suivant, on observe un exemple simple d'accès en lecture à une machine virtuelle pour un objet de sécurité utilisateur. Les rôles ou listes de rôles sont expliqués un peu plus loin dans le chapitre :

Accès pour une étendue de machine virtuelle

En termes de rôles, il faut distinguer les rôles Azure AD et les rôles d'accès aux ressources Azure. Ce sont deux notions proches mais qui n'ont pas du tout la même fonction dans la gestion des accès. Ce sujet est traité de façon détaillée dans la section Rôles Azure AD et rôles d'accès aux ressources de ce chapitre.

Même s'il y a des spécificités liées à l'utilisation du Cloud, la gestion des accès aux ressources Azure n'est pas déroutante pour les administrateurs.

2. Rôles Azure AD et rôles d'accès aux ressources

Les accès Azure sont découpés en deux grandes familles : les rôles Azure AD et les rôles d'accès aux ressources.

Un rôle Azure AD autorise des actions sur des objets comme les utilisateurs, les groupes et les applications.

Rôles d'administration

Les rôles d'administration peuvent être utilisés pour accorder l'accès à Azure AD et à d'autres services Microsoft. En savoir plus

Rechercher par nom ou description | Ajouter des filtres

Rôle	Description	Type
Administrateur Azure DevOps	Peut gérer la stratégie et les paramètres d'organisation Azure DevOps.	Intégré
Administrateur Azure Information Protection	Peut gérer tous les aspects du produit Azure Information Protection.	Intégré
Administrateur Cloud App Security	Peut gérer tous les aspects du produit Cloud App Security.	Intégré
Administrateur d'application	Peut créer et gérer tous les aspects des inscriptions d'applications et des applications d'entreprise.	Intégré
Administrateur d'appareil cloud	Accès complet pour gérer des appareils dans Azure AD.	Intégré
Administrateur d'appareils Teams	Peut effectuer des tâches d'administration sur des appareils certifiés Teams.	Intégré
Administrateur d'application cloud	Peut créer et gérer tous les aspects des inscriptions d'applications et des applications d'entreprise, à l'exception du proxy d'appl...	Intégré
Administrateur d'applications Office	Peut gérer les services cloud des applications Office, notamment la gestion des stratégies et des paramètres, et gérer la possibil...	Intégré
Administrateur d'attribut de flux utilisateur ID externe	Peut créer et gérer le schéma d'attribut disponible pour tous les flux utilisateur.	Intégré
Administrateur d'authentification	A accès pour afficher, définir et réinitialiser les informations de méthode d'authentification pour tout utilisateur non administrat...	Intégré
Administrateur d'authentification privilégié	Autorisé à afficher, définir et réinitialiser les informations de méthode d'authentification pour tout utilisateur (administrateur ou...	Intégré
Administrateur d'identité hybride	Peut gérer la synchronisation cloud d'AD vers Azure AD et les paramètres de fédération.	Intégré

Liste des rôles prédéfinis Azure AD, vue partielle

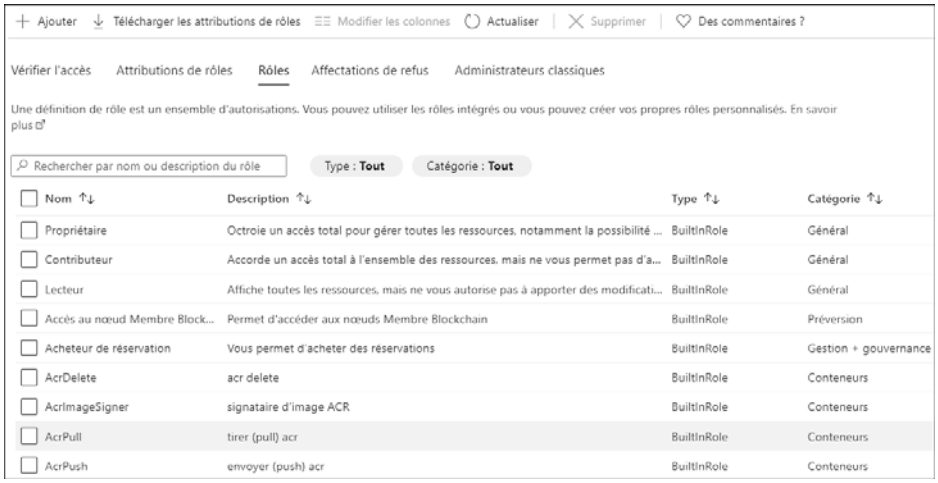
Les listes de rôles prédéfinis sont très fournies. Par exemple, le rôle Administrateur d'utilisateurs est décrit de la façon suivante (source éditeur Microsoft) :

Les utilisateurs dotés de ce rôle peuvent créer et gérer tous les aspects des utilisateurs et des groupes. De plus, ce rôle inclut la possibilité de gérer les tickets de support et de surveiller l'intégrité du service. Certaines restrictions s'appliquent. Par exemple, ce rôle n'autorise pas la suppression d'un administrateur général. Les administrateurs de comptes utilisateur peuvent modifier les mots de passe des utilisateurs, des administrateurs du support technique et des autres administrateurs de compte utilisateur uniquement.

Ce rôle est complet, avec des actions possibles sur les utilisateurs, sur les tickets de support mais aussi des limitations comme le fait de ne pas pouvoir supprimer un administrateur général.

Si ces listes prédéfinies ne sont pas suffisantes, elles peuvent être complétées par des rôles personnalisés selon le niveau de licence souscrit par l'entreprise.

Les rôles d'accès sur une ressource Azure sont différents. Ils sont organisés par catégories de ressources pour faciliter la gestion. Ainsi, les catégories Stockage, Réseau, IA + Machine Learning ou Bases de données sont plus faciles à mettre en place.



Rôles pour les ressources Azure et catégories, vue partielle

Puis on retrouve des niveaux d'actions (de responsabilité) sur ces rôles : **Lecteur**, **Contributeur**, **Propriétaire**, etc.

Le rôle **Lecteur** est décrit de la façon suivante (source éditeur Microsoft) :

Affiche toutes les ressources, mais ne vous autorise pas à apporter des modifications.

Un contributeur aura des droits plus élevés de gestion avec quelques restrictions, un propriétaire aura, lui, un accès total aux ressources. Ici donc, ce sont clairement des accès typés ressources avec des autorisations de gestion de services.

Attention, dans les deux types de rôles, des autorisations donnent l'impression de se recouper mais il n'en est rien.

Pour illustrer ce point, il nous faut comparer le rôle Azure AD **Administrateur d'utilisateurs** et le rôle d'accès **Administrateur de l'accès utilisateur**.

– **Administrateur d'utilisateurs** : administrer les utilisateurs, c'est créer et gérer tous les aspects de compte des utilisateurs et des groupes.
– **Administrateur de l'accès utilisateur** : administrer l'accès des utilisateurs, c'est la possibilité de gérer leurs accès à des ressources Azure.

Dans la section Exercices de ce chapitre, le fichier JSON des autorisations est présenté partiellement pour clarifier le fonctionnement et les différences entre ces deux familles d'accès.

3. Autorisation, concept de base

Obtenir des autorisations sur Azure se fait en plusieurs étapes. Il s'agit d'abord de créer un objet de sécurité ; il en existe quatre :

– Utilisateur
– Groupe(s)
– Principal de service
– Identité managée (système ou utilisateur)

Sur ces objets sont attachés des rôles, par exemple un rôle d'Administrateur de l'accès utilisateur. Il existe un grand nombre de rôles dits prédéfinis, prêts à l'utilisation. Si ces rôles prédéfinis ne sont pas suffisants, comme expliqué, il est tout à fait possible de créer des rôles particuliers.

Pour la dernière étape, il faut définir une étendue pour appliquer ces rôles. Il existe quatre étendues : les abonnements, les groupes de management, les ressources et les groupes de ressources.

Cette granularité permet de positionner des autorisations très fines puisqu'un objet utilisateur peut se voir attacher une ou plusieurs listes de rôles et que cet ensemble est ensuite affecté sur une ou plusieurs étendues spécifiques.

Pour en finir avec cette introduction, on applique sur Azure comme On-premises la règle du moindre privilège : donner les bons droits et les bonnes autorisations, mais pas plus que nécessaire.

Dans la suite du chapitre, ces points seront revus en détail.

3.1 L'objet de sécurité

Comme expliqué en introduction, le premier niveau de l'identité est un objet de sécurité. Quatre objets sont disponibles : **Utilisateur, Groupe(s)**, **Principal de service** ou **Identité managée (système ou utilisateur)**.

Si les objets utilisateurs et groupes sont très connus, voici quelques explications complémentaires sur le principal de service et l'identité managée.

Le principal de service est un objet applicatif. C'est une identité pour votre application. Sur cette identité sont définies les stratégies d'accès et les autorisations.

L'identité managée est plus récente et assez proche du principal de service. Dans la définition de l'identité managée, on trouve souvent le terme principal de service spécial. La principale différence est la possibilité d'activer une identité managée sur une ressource Azure. Par exemple, une machine virtuelle peut porter une identité managée.