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.

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.

3.1 Taille du disque et performance

La facturation des disques managés dépend de leur taille et de la performance choisie.

Un disque Premium (disque SSD) est plus cher mais aussi plus performant qu'un disque Standard.

Le tableau ci-dessous répertorie les différents disques managés Premium, la taille attribuée à chacun d'eux ainsi que les performances associées :

Type de disque Premium	P4	P6	P10	P20	P30	P40	P50
Taille du disque	32 Go	64 Go	128 Go	512 Go	1024 Go (1 To)	2 048 Go (2 To)	4 095 Go (4 To)
IOPS par disque	120	240	500	2 300	5 000	7500	7500
Débit par disque	25 Mo par seconde	50 Mo par seconde	100 Mo par seconde	150 Mo par seconde	200 Mo par seconde	250 Mo par seconde	250 Mo par seconde

Le nombre de disques, choisi par l'administrateur, dépend de la taille de disque souhaitée. Il est possible de réserver un seul disque P50 ou plusieurs disques P10 pour répondre aux besoins d'une application hébergée sur une machine virtuelle.

Le tableau ci-dessous répertorie les différents disques managés Standard et la taille attribuée à chacun d'eux :

Disques managés Standard	S4	S6	S10	S20	S30	S40	S50
Taille du disque	32 Gio	64 Gio	128 Go	512 Go	1 024 Gio (1 Tio)	2 048 Gio (2 Tio)	4 095 Gio (4 Tio)

Lors du calcul du coût estimé d'une machine virtuelle, outre la taille du disque, pensez à estimer la bande passante des données sortantes et le nombre de transactions pour les disques standards.

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 balises (décrites dans ce chapitre) pour identifier précisément une ressource ainsi que son propriétaire.

3. Disques managés

Afin de simplifier la gestion des disques virtuels des machines virtuelles Azure, Microsoft propose à ses clients d'utiliser Azure Managed Disks (ou disques managés). La taille et les performances (Premium SSD ou Standard HDD) sont gérés par Azure en arrière-plan. Auparavant, l'administrateur devait créer des comptes de stockage dédiés à la prise en charge des disques (fichiers de disques durs virtuels) et gérer manuellement les montées en puissance. Désormais, depuis un emplacement centralisé (un disque managé par région Azure), le disque sera utilisé pour créer l'ensemble de vos machines virtuelles (jusqu'à 10 000 disques par abonnement).

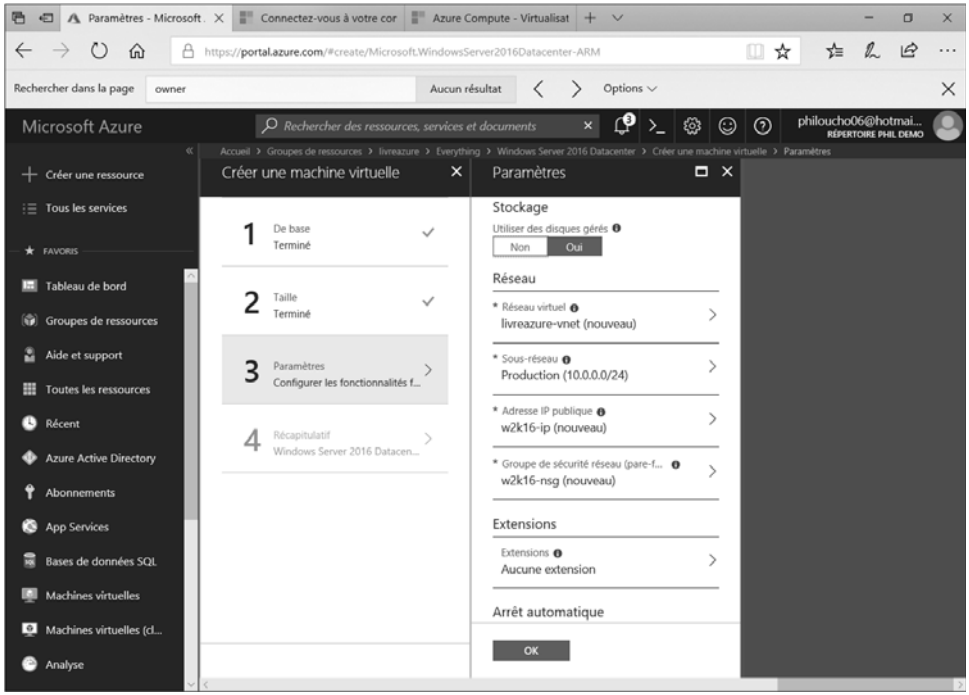
La disponibilité annoncée est de 99,999 % via trois réplicas des données dans une même région, offrant ainsi un taux de défaillance annuel de 0 %. Des services annexes tel qu'Azure Backup s'appuie sur les disques gérés pour assurer une sauvegarde et une restauration fiable des machines virtuelles Azure.

3.2 Sécurité

Un disque géré propose deux types de chiffrement :

1. SSE (*Storage Service Encryption*) assure le chiffrement au repos et est activé par défaut. L'activation peut néanmoins s'effectuer après la création du disque géré.
2. ADE (*Azure Disk Encryption*) chiffre les données via BitLocker pour les systèmes Windows ou DM-Crypt pour les systèmes Linux. Ce chiffrement n'est pas activé par défaut mais peut l'être sur les disques de système d'exploitation et de données des machines virtuelles Azure.

L'utilisation d'un disque géré est activée par défaut lors de la création d'une machine virtuelle, dans l'étape 4 - Paramètres :



4. Compte de stockage

Un grand nombre de ressources Azure nécessitent un compte de stockage (ou Azure Storage) pour fonctionner : une base de données, une machine virtuelle, des sauvegardes, des journaux d'événements… Un compte de stockage fournit un espace sécurisé pour stocker les données du client. Le temps de disponibilité minimal est de 99,9 %. Sa limite d'espace est de 5 Pétatoctets, ce qui permet d'envisager sereinement des scénarios de Big Data ou de diffusion de contenus multimédias. En fonction du type de compte de stockage retenu, le client ne paie que l'espace consommé et les opérations qu'il effectue sur les disques ou bien l'espace provisionné d'un disque entier. Évolutif, le compte de stockage alloue automatiquement les ressources appropriées en fonction de la montée en charge détectée.

Vous pouvez y accéder via différents scénarios, depuis :

– Un poste de travail muni d'un navigateur.
– Une application installée localement.
– Un appareil mobile.
– Un langage de programmation tel que .NET, C++.
– Des API REST.
– Des machines virtuelles.
– Des partages.
– Une base de données.
– Etc.

Une bonne pratique est de créer trois comptes de stockage dans un abonnement : l'un pour stocker les disques virtuels des machines virtuelles, l'autre pour les sauvegarder, le dernier pour héberger les journaux d'événements.

La création d'un compte de stockage s'effectue indifféremment depuis le nouveau portail :

- Dans votre navigateur Internet, saisissez l'adresse du nouveau portail : https://portal.azure.com. Utilisez l'identifiant et le mot de passe créés précédemment lors de la souscription à l'offre gratuite ou bien ceux que vous possédez déjà. Dans notre exemple, le nom d'utilisateur est philoucho06@hotmail.fr.

- Cliquez sur **Comptes de stockage** dans le menu de gauche, puis sur **Ajouter**.

Remarque

Un compte de stockage peut être aussi créé durant le processus de création d'autres ressources, telle une machine virtuelle.

Saisissez un nom unique tel que **stockagelivreazurex** (sans majuscules et où x est un numéro choisi par vos soins), en minuscule obligatoirement.

Remarque

Un nom de domaine portant l'extension .core.windows.net sera automatiquement créé, ce qui signifie qu'un compte de stockage doit posséder un nom unique dans Azure.

- Sélectionnez le modèle de déploiement (**Resource Manager**), le type de compte (**Storage (v1 à usage général)**), l'emplacement (**Europe du Nord**), la réplication attendue (Stockage géo-redondant avec accès en lecture (RA-GRS) (option par défaut sélectionnée), Stockage redondant dans une zone (ZRS), Stockage localement redondant (LRS), Stockage géo-redondant (GRS)) que nous détaillerons plus bas. Dans notre cas, ce sera **Stockage localement redondant (LRS)**. Puis, sélectionnez le niveau de performance attendue (**Standard** ou Premium). Si vous souhaitez garantir que les transferts seront sécurisés vers votre compte de stockage, cliquez sur **Activé**. Sélectionnez enfin l'abonnement et le groupe de ressources (**livreazure**) l'intégrant.

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.

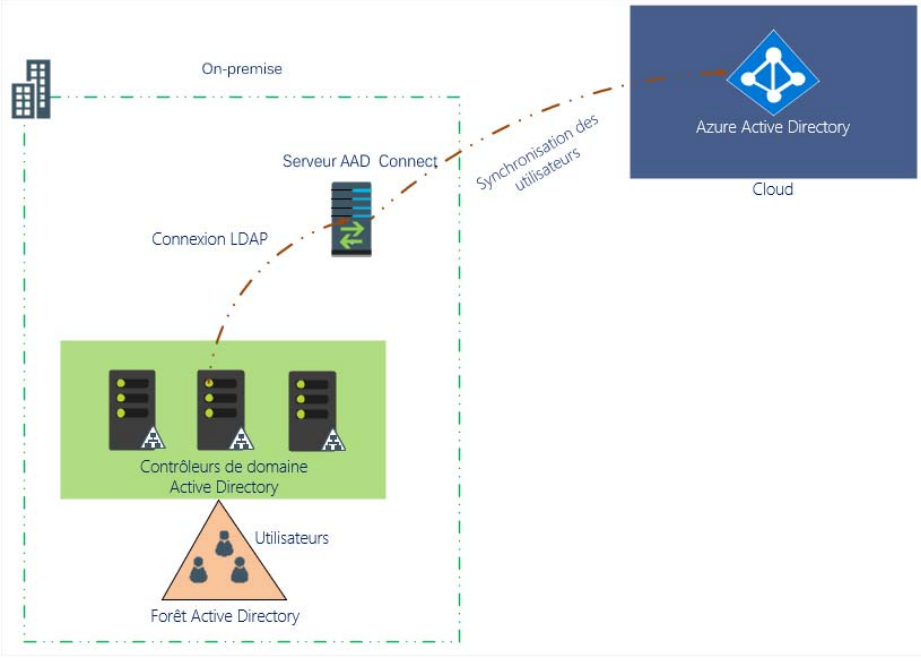
Dans ce cas, il faut étudier la mise en œuvre d'une solution hybride permettant à un utilisateur, dont l'identité est contenue dans l'annuaire Active Directory local, d'accéder aux ressources internes de l'entreprise et de disposer d'une identité dans le cloud (et plus précisément dans Azure Active Directory)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

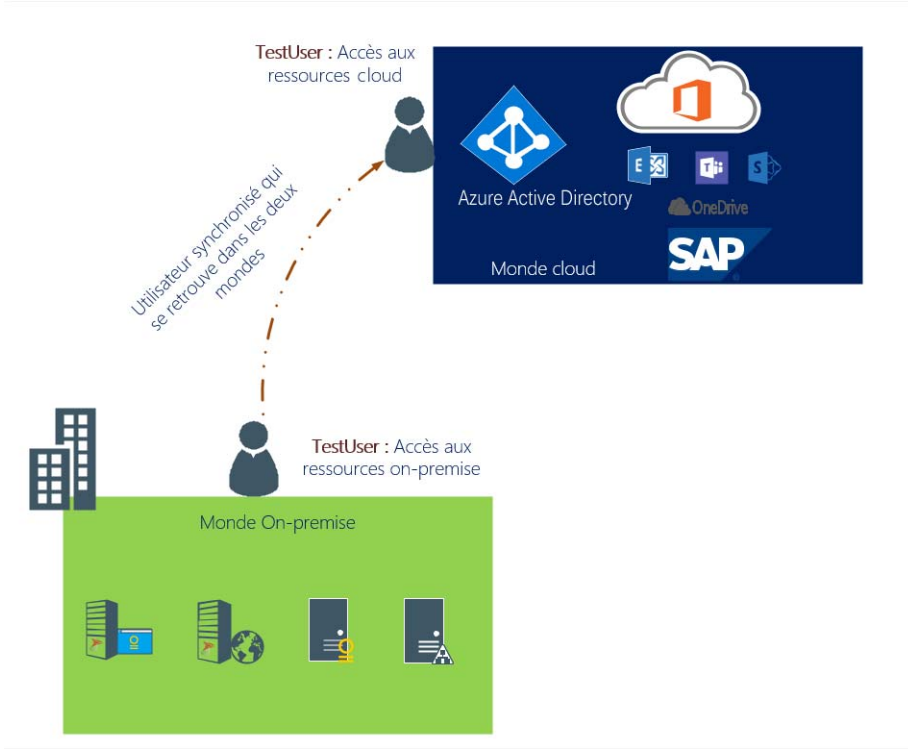
Sur l'illustration précédente, nous remarquons que le serveur Azure Active Directory Connect se connecte à la forêt Active Directory via l'un des contrôleurs de domaine et effectue une synchronisation avec Azure Active Directory en fonction des règles et filtrage d'OU imposés. Avec cette configuration 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

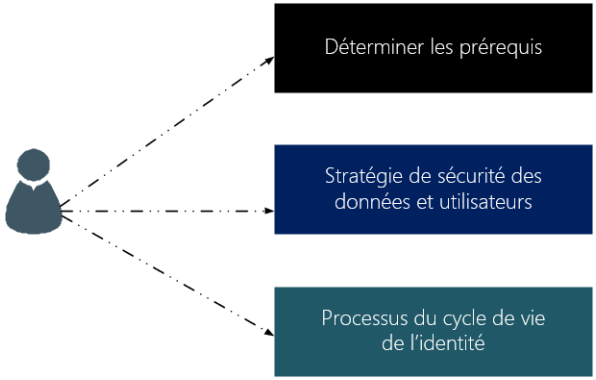
Ces attributs permettent l'authentification et le fonctionnement des utilisateurs. Aucune donnée personnelle des utilisateurs n’est stockée.

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.