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://docs.microsoft.com/fr-fr/azure/cloud-adoption-framework/ready/azure-best-practices/naming-and-tagging

3. Disque managé

Afin de simplifier la gestion des disques virtuels des machines virtuelles Azure, Microsoft offre à ses clients d'utiliser des Managed Disks (ou disques managés). La taille et les performances (Premium SSD, Standard SSD, Standard HDD ou Ultra Disk) sont gérées par Azure en arrière-plan. Les disques managés sont l'équivalent d'un disque physique sur un serveur, mais virtualisé comme un disque dur virtuel. L'administrateur spécifie la taille de disque ainsi que son type, et quelques secondes plus tard, le disque est disponible.

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. De plus, chaque compte de stockage possédait des URL pour accéder à ses différents services, tels que Blob, Table, File d'attente, etc. Vous l'aurez compris, posséder une machine virtuelle avec un disque dur virtuel vhd accessible potentiellement depuis Internet était une faille de sécurité potentielle.

Désormais, un disque non accessible depuis Internet sera utilisé pour créer votre machine virtuelle, et vous pourrez posséder jusqu'à 50 000 disques par abonnement, en fonction du type (SSD ou standard).

Les disques managés assurent une disponibilité de 99,999 % mais… sans SLA associé. Le SLA pris en compte par Microsoft est celui de la machine virtuelle. Chaque machine virtuelle a au moins un disque managé hébergeant le système d'exploitation, et vous pouvez ajouter, en fonction de la taille de la machine virtuelle, des disques managés hébergeant les données.

La capture instantanée d'un disque managé est une copie en lecture de ce dernier, stockée en tant que disque managé standard. Cela est comparable à une sauvegarde d'un disque virtuel. Les disques managés prennent également en charge la création d'une image d'un système d'exploitation à partir de votre disque dur virtuel (VHD) depuis un hyperviseur Hyper-V ou converti depuis un hyperviseur VMWare (disque virtuel vmdk vers vhd). L'utilisation de l'utilitaire Sysprep est également supporté afin de préparer un système à son clonage.

Notez enfin qu'un disque temporaire, présent sur chaque machine virtuelle, n'est pas un disque managé.

3.1 Taille du disque et performance

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

Un disque Premium (disque SSD) est par exemple plus cher mais aussi plus performant qu'un disque Standard. Ce type de disque est conçu pour gérer un volume important d'E/S, avec un débit élevé et une faible latence. Néanmoins, il ne permet pas la réplication interrégion.

Quatre types de disques managés sont disponibles :

– SSD Premium : conçu pour traiter un volume important d'E/S, avec un débit élevé et une faible latence.
– SSD Standard : SSD à faible coût, disponible pour héberger votre production. La latence associée est plus faible par rapport aux disques HDD Standard. Peut être mis à niveau vers un disque SSD Premium.
– HDD Standard : adaptés aux charges de travail de développement, donc ne recherchant pas la performance. Peut engendrer la perte du SLA d'une machine virtuelle seule, comme nous le verrons dans ce chapitre.
– Disque Ultra : recommandé pour obtenir des performances maximales, avec une recherche de latence la plus faible possible ainsi qu'un débit et des opérations d'E/S par seconde (IOPS) constamment élevés.

Le site ci-dessous répertorie les différents disques managés Premium, Standard, la taille attribuée à chacun d'eux ainsi que les performances associées : https://azure.microsoft.com/fr-fr/pricing/details/managed-disks/

Le nombre de disques, choisi par l'administrateur, dépend de la taille de la machine virtuelle créée. Il est possible de combiner différents disques managés, en utilisant par exemple un seul disque P50 (4 To) et plusieurs disques P10 (128 Go) pour répondre aux besoins d'une application hébergée sur une machine virtuelle.

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.

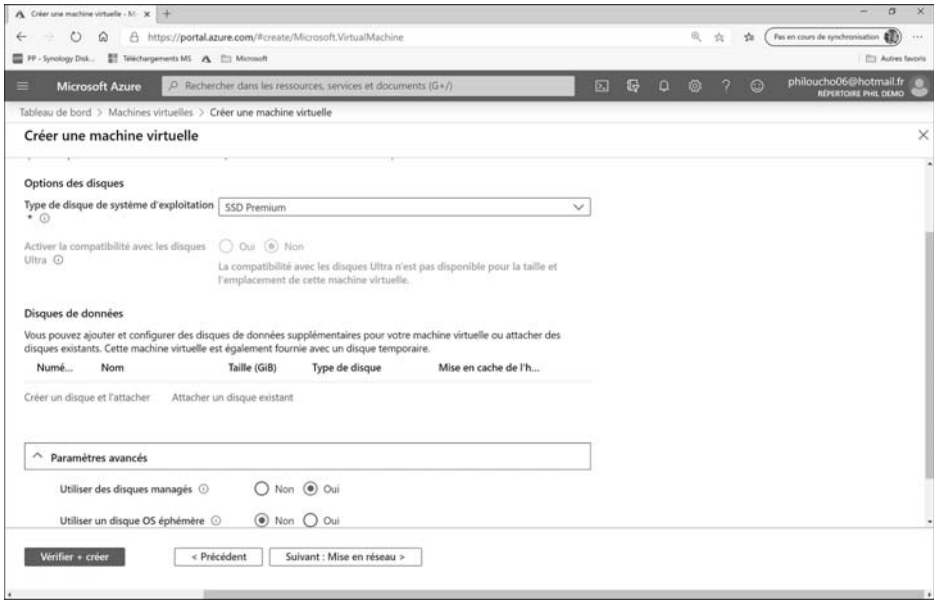
Il est important d'appréhender que la facturation se base sur l'espace du disque alloué, que vous consommiez un octet ou l'intégralité de l'espace, la facture sera identique.

3.2 Sécurité

Un disque managé (ou géré en Français) propose deux types de chiffrement au repos. Un chiffrement au repos est conçu pour garantir que les données sont chiffrées quand elles sont sur le disque. Si un attaquant télécharge un disque dur VHD d'une machine virtuelle Azure comprenant des données chiffrées, mais qu'il ne dispose pas des clés de chiffrement, il devra résoudre le chiffrement pour lire les données. Voici les deux protections proposées par Microsoft :

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 managé est activée par défaut lors de la création d'une machine virtuelle, dans **Disques**.



Notez qu'en cliquant sur **Paramètres avancés**, l'utilisateur a le choix de ne pas utiliser un disque managé pour héberger son disque dur virtuel, au profit d'un compte de stockage.

4. Compte de stockage

Un grand nombre de ressources Azure nécessitent un compte de stockage (ou Azure Storage) pour fonctionner : une base de données, 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 à l'aide d'un disque managé. 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 au moins deux comptes de stockage dans un abonnement : l'un pour stocker les sauvegardes, le second pour archiver les journaux d'activité.

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

- Dans votre navigateur Internet, saisissez l'adresse du 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 du portail, puis sur **Ajouter**.

Remarque

Un compte de stockage peut aussi être créé durant le processus de création d'autres ressources, telle qu'une machine virtuelle ou la sauvegarde de celle-ci.

Sélectionnez le groupe de ressources (livreazure) l'intégrant.

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.