Lecture Individuelle 2

Microsoft Azure, en pratique

[1]

[1] https://www.arpeje.fr/wp-content/uploads/2022/03/images-blog-ArpeJe-1.png

Table des matières

1. Introduction

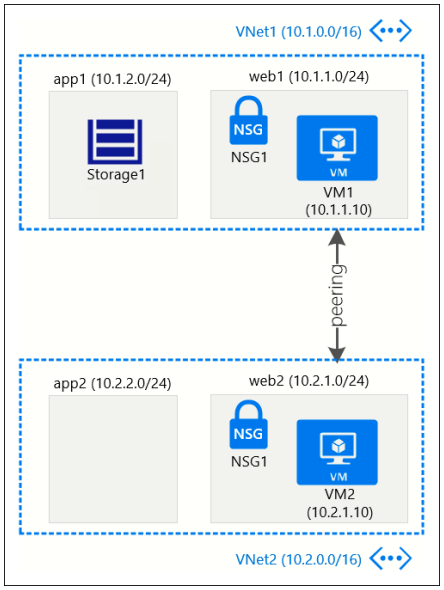
Dans cette lecture individuelle pratique, nous allons mettre en pratique les connaissances théoriques acquises lors de notre exploration des aspects théoriques de Microsoft Azure, réalisé dans le cadre de ma première lecture individuelle. Nous plongerons dans l'utilisation concrète de cette plateforme proposée par Microsoft.

Cette exploration pratique de Microsoft Azure servira de support à deux compétences importantes : la compétence B2, qui consiste à être capable de concevoir et d'exploiter des ressources, services et fonctionnalités d'une infrastructure virtuelle, que ce soit dans le cloud ou d'autres environnements, et la compétence B3 en matière de disaster recovery, où nous apprendrons à protéger nos données et nos applications contre les incidents et à assurer leur récupération en cas de sinistre, bien que de manière légère, sans entrer dans les détails les plus avancés.

2. Planification de la topologie de votre réseau virtuel

Voici comment est formé la topologie d'un réseau virtuel sur Azure :

- Le réseau virtuel est divisé en deux sous-réseaux afin de refléter les niveaux d'application standard.
- Chaque réseau virtuel est protégé par un seul groupe de sécurité réseau.
- Un point d'extrémité de service relie un réseau virtuel à un compte de stockage.
- Le peering permet de relier les deux sous-réseaux



2.1. Création d'un réseau virtuel

Voici les différentes étapes sur Azure afin de créer un réseau virtuel :

1. Créer un nouveau groupe de ressources ou ajoutez à un groupe de ressources existant.
2. Chercher dans le portail Azure « réseaux virtuels », puis appuyez sur ajouter.
3. Remplissez les différents champs et appuyez sur créer.

Pour la pratique, utilisez les valeurs suivantes :

- Nom : VNet1
- Espace d'adresses : 10.2.0.0/16
- Abonnement : votre abonnement
- Groupe de ressources : votre groupe de ressources sélectionné
- Emplacement : La région Azure la plus proche de chez vous.
- Nom du sous-réseau : Par défaut
- Plage d'adresses du sous-réseau : 10.2.1.0/24
- Protection DDoS : Basique
- Service Endpoints : Désactivé
- Pare-feu : Désactivé

Une fois qu'Azure a déployé le réseau virtuel, vous devez revoir ses paramètres de configuration pour définir un deuxième sous-réseau. Suivez les étapes suivantes pour atteindre cet objectif :

1. Dans la liste de paramètres du réseau virtuel, sélectionnez sous-réseaux
2. Remplissez tous les champs et appuyez sur créer pour terminer la configuration

Voici les valeurs par défaut :

1. Nom : app1
2. Plage d'adresses : 10.2.1.0/24
3. Groupe de sécurité réseau : Aucun
4. Table de routage : Aucune
5. Service Endpoints Services : 0 sélectionné
6. Déléguer le sous-réseau à un service : Aucun

Dans la liste de paramètres de votre réseau virtuel, si vous sélectionnez supervision → diagramme, vous pouvez accéder à un diagramme vectoriel qui représente votre réseau virtuel.

2.2. Configuration des réseaux virtuels

Avant de peupler votre réseau virtuel, vous devez procéder à quelques ajustements pour vous assurer qu'il se comporte comme vous le souhaitez.

2.2.1. Configuration des groupes de sécurité réseau (NSG)

Les NSG sont des filtres de trafic que vous pouvez associer aux cartes d'interface réseau virtuelles des VM ou aux sous-réseaux VNet. Il est recommandé d'associer les NSG à des sous-réseaux afin de réduire les problèmes futurs et d'appliquer les mêmes règles de trafic entrant et sortant à plusieurs machines virtuelles simultanément.

Un NSG se compose de plusieurs règles d’accès ayant les propriétés suivantes :

- Priorité
- Nom
- Port
- Protocole
- Source
- Destination
- Action

Un NSG fait passer chaque flux de trafic par sa liste de règles entrantes ou sortantes, en fonction de la direction du trafic. La première règle qui s'applique devient la règle effective. À moins de disposer d'une règle fourre-tout pour refuser tout le trafic non classifié, vous vous exposez à des types de connexion que vous ne souhaitez pas, ce qui pourrait compromettre la sécurité de votre VM.

Voici les règles entrantes par défaut :

Nom	Description
AllowVnetInBound	Autorise le trafic entrant en provenance de ce VNet et de tous les VNet peering associés
AllowAzureLoadBalancerInBound	Autorise le trafic de sonde de santé entrant en provenance de n'importe quelle adresse IP de l'équilibreur de charge Azure
DenyAllInBound	Règle générale assurant que tout le trafic entrant non intercepté par une règle précédente est refusé

Voici les règles de sortie par défaut :

Nom	Description
AllowVnetOutBound	Permet le trafic sortant de ce VNet vers tous les VNet peering associés
AllowInternetBound	Autorise les machines virtuelles à accéder à internet depuis le VNet
DenyAllOutBound	Règle générale assurant que tout le trafic sortant non intercepté par une règle précédente est refusé

2.3. Création d'un groupe de sécurité réseau (NSG)

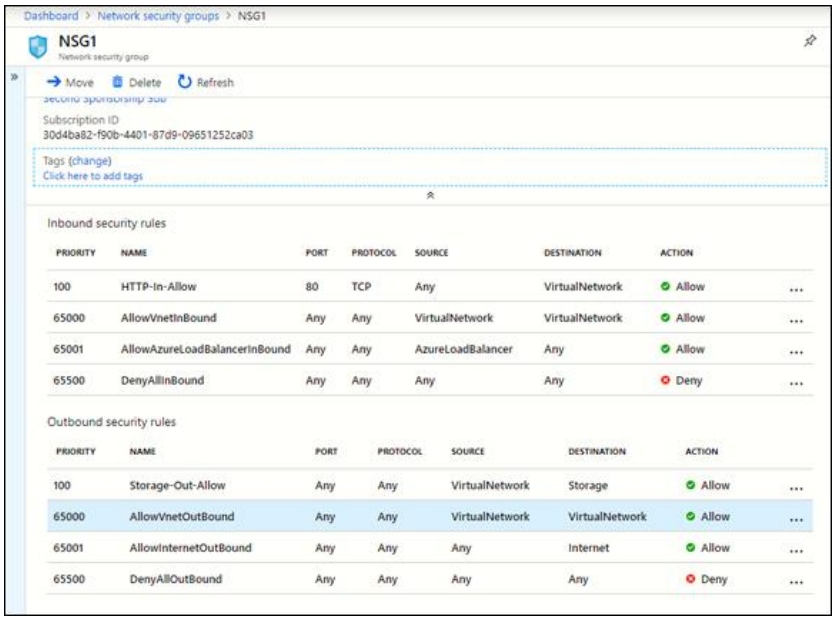
Pour créer un NSG qui autorise le trafic HTTP entrant (port TCP 80), suivez ces étapes :

1. Utilisez la recherche globale du portail Azure pour trouver l'onglet Groupes de sécurité réseau (NSG), puis cliquez sur Ajouter dans la barre d'outils.
2. Remplissez le formulaire de création du groupe de sécurité réseau et cliquez sur créer. Utilisez ces propriétés :
   Nom : NSG1
   Abonnement : [votre abonnement]
   Groupe de ressources : [votre groupe de ressources]
   Emplacement : [votre région]
3. Après le déploiement, sélectionnez votre NSG et parcourez le paramètre Règles de sécurité entrantes dans la liste Paramètres. Cliquez sur ajouter.
4. Remplissez le formulaire de création de la règle de sécurité entrante et cliquez sur Créer. Utilisez ces propriétés de configuration pour NSG1 :
   - Source : Service Tag, Internet
     Votre source peut être une liste d'adresses IP ou de plages d'adresses séparées par des virgules, une balise de service ou un groupe de sécurité d'application. Pour l'instant, il faut comprendre que cette règle s'applique au trafic entrant provenant de l'Internet public.
   - Plages de ports source : Toutes (indiquées par l'astérisque)
   - Destination : VirtualNetwork (balises de service à la rescousse)
   - Plage de ports de destination : 80
   - Protocole : TCP
   - Action : Autoriser

- Priorité : 100
- Name : HTTP-In-Allow
- Description : (ajoutez si vous le souhaitez)

5. Créez une nouvelle règle de sécurité sortante pour NSG1 :
   Cette règle autorise le trafic depuis le sous-réseau par défaut vers le compte de stockage que vous placerez sur le sous-réseau app1. Utilisez les propriétés suivantes :
   - Source : Réseau virtuel
   - Source Port Ranges : N'importe laquelle
   - Destination : Service tag, Storage
   - Port de destination : Toute plage de ports de destination
   - Protocole : Tous
   - Action : Autoriser
   - Priorité : 100
   - Name : Stockage-Sortie-Autoriser
   - Description : (à compléter si vous le souhaitez)

Faire exercice et mettre image et traduire !!!



2.3.1. Association du NSG aux sous-réseaux appropriés

Suivez ces étapes pour associer votre nouveau NSG au sous-réseau par défaut sur VNet1 et au sous-réseau web2 sur le sous-réseau VNet2 :

1. Sur la configuration de votre NSG1, sélectionnez Sous-réseaux.
2. Sur « sous-réseaux », cliquez sur associer.
3. Sur « associer un sous-réseau », choisissez le réseau virtuel et le sous-réseau appropriés.
4. Vous devez effectuer cette procédure deux fois : une fois pour VNet1/default et une fois pour VNet2/default2.

2.4. Comprendre les points de terminaison de service

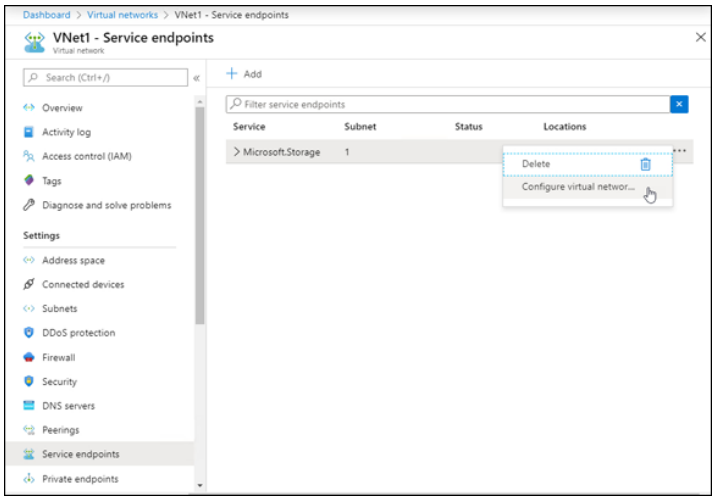
Les points de terminaison de service sécurisent certains services Azure en limitant leur connectivité à un réseau virtuel. Il se peut que vous disposiez d'un compte de stockage contenant des données sensibles auxquelles seules les machines virtuelles d'un réseau virtuel particulier doivent pouvoir accéder. Dans ce cas, la création d'un point de terminaison de service pour le compte de service sur le réseau virtuel approprié permet d'atteindre l'objectif fixé.

Pour créer un point de terminaison de service Microsoft.Storage sur le sous-réseau Vnet1 app1, procédez comme suit :

1. Naviguez jusqu'au réseau virtuel un et sélectionnez le paramètre « Service Endpoints ».
2. Cliquez sur ajouter, puis sélectionnez Microsoft.Storage comme service et app1 comme sous-réseau.
3. Cliquez sur ajouter pour terminer la configuration.

Il faut maintenant associer un compte de stockage au sous-réseau app1 :

1. Dans le portail Azure, naviguez jusqu'au réseau virtuel 1 et sélectionnez le paramètre Service Endpoints.
2. Dans le menu contextuel Microsoft.Storage, choisissez « Configurer les réseaux virtuels dans un compte de stockage ».
3. Sélectionnez votre compte de stockage et le paramètre pare-feu et réseaux virtuels dans la lame « mise en réseau ».
4. Dans la section « Autoriser l'accès à partir de », sélectionnez « Réseaux sélectionnés ».
5. Dans la section Réseaux virtuels, choisissez Ajouter un réseau virtuel existant.
6. Parcourez le réseau virtuel VNet1 et le sous-réseau app1, puis cliquez sur Ajouter.
7. Cliquez sur Enregistrer pour terminer la configuration.



La lame Pare-feu et réseaux virtuels du compte de stockage contient quelques options supplémentaires une fois que vous avez activé les points de terminaison de service :

- Ajouter l'adresse IP de votre client : Si vous ne sélectionnez pas cette option, vous ne pourrez pas accéder au compte de stockage à partir de votre poste de travail actuel.
- Autoriser les services Microsoft de confiance à accéder à ce compte de stockage : Activez cette option pour vous assurer que d'autres services Azure (tels que Key Vault, Azure AD, etc.) peuvent accéder au compte de stockage et vice versa.

2.5. Connecter des réseaux virtuels

Voici deux façons de lier logiquement deux réseaux virtuels pour prendre en charge les topologies qui le nécessitent :

1. Avec des réseaux virtuels de production/développement qui prennent en charge la communication inter-réseaux.
2. Avec des architectures de réseaux virtuels en étoile dans lesquelles le réseau virtuel en étoile est relié à l'environnement sur site.

Azure propose de connecter des réseaux virtuels grâce au « VNet peering ».

2.6. Configuration du VNet peering

Le peering VNet est un moyen de connecter deux réseaux virtuels Azure. Jusqu'à fin 2018, des passerelles de réseaux virtuels et un réseau privé virtuel (VPN) de réseau à réseau étaient nécessaires pour connecter des réseaux virtuels dans différentes régions. Aujourd'hui, les réseaux virtuels de différentes régions et même de différents abonnements Azure peuvent être mis en relation.

Le trafic réseau à travers un peering VNet est privé, se déroulant sur le réseau principal d'Azure et utilisant des adresses IP privées. Aucun coût ou surcharge lié au VPN n'est requis pour le peering, bien que vous puissiez déployer un VPN VNet-à-VNet si vos besoins en matière de sécurité l'exigent. Vous pouvez également configurer les deux côtés de l'échange de trafic à partir d'un seul réseau virtuel.

Suivez ces étapes pour configurer un peering de VNet entre vos réseaux virtuels VNet1 et VNet2 :

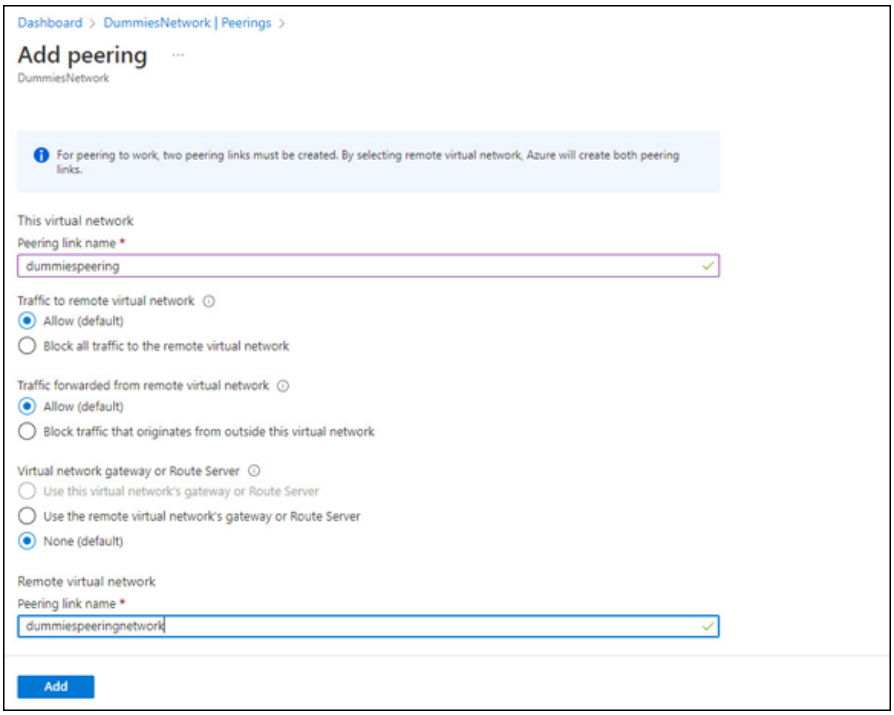
1. Dans le portail Azure, naviguez jusqu'à VNet1, sélectionnez le paramètre « Peerings » et cliquez sur ajouter.
2. Utilisez les propriétés de configuration suivantes :
    - Nom du peering du VNet1 vers le réseau virtuel distant : vnet1-to-vnet2-peering
    - Modèle de déploiement du réseau virtuel : Gestionnaire de ressources
    - Abonnement : [votre abonnement]
    - Réseau virtuel : VNet2
    - Nom du peering du réseau virtuel distant vers le VNet1 : vnet2-to-vnet1-peering
    - Autoriser l'accès au réseau virtuel (dans les deux sens) : Activé
    - Configurer les paramètres de trafic transféré (dans les deux directions) : Désactivé

- Autoriser le transit de la passerelle : non sélectionné

3. Cliquez sur OK pour soumettre votre configuration à ARM.

Finalement, les pages Peerings de VNet1 et VNet2 devraient afficher l'état du peering comme Connecté.

Vous disposez désormais d'un chemin de routage entre les deux VNets qui ne passe que par Azure - pas d'Internet public (ou de connexion VPN).



3. Déploiement et configuration des machines virtuelles Azure

Une machine virtuelle est une représentation logicielle d'un ordinateur. Chaque région Azure est composée de plusieurs centres de données ; chaque centre de données est constitué de milliers de serveurs lames. Les machines virtuelles s'exécutent au sein de cette gigantesque structure de calcul.

Chaque VM se voit attribuer des ressources matérielles virtuelles à partir de son hôte matériel parent :

- Calcul (CPU [unité centrale de traitement] et RAM [mémoire vive])
- Stockage
- Réseau

Les serveurs du centre de données de Microsoft exécutent une version spécialisée de Windows Server Core, et vos machines virtuelles résident sur des hôtes Microsoft Hyper-V.

Azure prend également en charge les distributions Linux 64 bits.

3.1. Démarrer le déploiement d'une machine virtuelle à partir d'Azure Marketplace

Le moyen le plus rapide de déployer une VM dans Azure est sans doute de le faire à partir d'Azure Marketplace. Azure Marketplace est un portail en ligne qui propose des milliers d'images de VM Microsoft et non Microsoft.

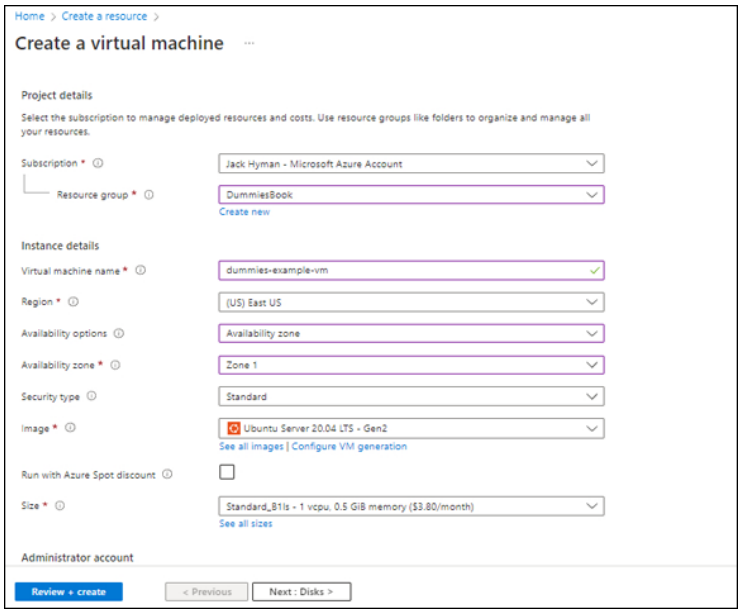
Vous pouvez accéder à Azure Marketplace à partir du portail Azure en saisissant marketplace dans la zone de recherche globale. Vous pouvez également vous connecter avec votre compte Azure et commencer à chercher la machine virtuelle de vos rêves sur www.azure.com/marketplace.

3.1.1. Déploiement d'une machine virtuelle Linux

Déploiement depuis le portail Azure :

1. Cherchez « Ubuntu Server 18.04 LTS » dans Azure Marketplace, puis sélectionnez créer.
2. Remplissez l'onglet « de base », voici quelques informations importantes :
    - Exécuter avec Azure Spot Discount : si vous n'avez pas besoin de votre image de machine virtuelle 24h/24 et 7j/7 et que vous souhaitez économiser de l'argent, pensez à cocher la case. Une instance Azure Spot permet aux clients d'acheter des machines virtuelles à partir d'un pool de capacité disponible inutilisée à un prix nettement inférieur. Vous pouvez économiser jusqu'à 90 % par rapport au tarif à l'utilisation.
    - Taille : Pour l'instant, acceptez la taille de machine virtuelle par défaut recommandée par Microsoft.
    - Type d'authentification : Les VM Linux sont différentes des VM Windows car vous pouvez utiliser une authentification basée sur une clé Secure Shell (SSH) ou une authentification basée sur un mot de passe. Pour cet exercice, choisissez un mot de passe.
    - Ports entrants publics : À des fins de test, associez une adresse IP publique à cette VM, et connectez-vous à l'instance via SSH.

3. Remplissez l'onglet « Disques ». Cet onglet vous permet de faire un choix initial concernant le système d'exploitation et les disques de données de la VM. Choisissez un disque dur standard pour économiser de l'argent.
4. Remplissez l'onglet « Réseau ». Voici les différents paramètres à choisir :
    - Réseau virtuel : par défaut
    - Sous-réseau : par défaut
    - IP publique : par défaut
    - Groupe de sécurité réseau : de base
    - Ports entrants publiques : autoriser les ports sélectionnés
    - Sélectionnez les ports entrants : sélectionnez SSH
    - Équilibrage de charge : sélectionnez Non.



5. Remplissez l'onglet «Gestion ». Assurez-vous que les diagnostics de démarrage sont activés et que toutes les autres options sont désactivées. Les diagnostics de démarrage sont requis pour utiliser la console série de la VM, c'est donc toujours une bonne idée de l'activer le plus tôt possible.
6. Cliquez sur l'onglet « vérifier + créer », puis sélectionnez « créer ».

3.1.2. Connexion à la machine virtuelle Linux

Utilisez Azure Cloud Shell afin d'établir une connexion SSH à votre machine virtuelle :

1. Allez dans le panneau de votre machine virtuelle et notez son adresse IP publique.
2. Ouvrez Cloud Shell et connectez-vous à votre machine virtuelle en spécifiant le nom de votre compte administrateur par défaut et l'adresse IP publique. « ssh compte@adresseip ».

3.2. Démarrer et arrêter une machine virtuelle avec PowerShell

Suivez ces étapes pour utiliser PowerShell sur votre poste de travail Windows afin d'arrêter et démarrer une machine virtuelle :

1. Ouvrez une console PowerShell en tant qu'administrateur et connectez-vous à Azure.

Pour ce faire, exécutez la commande « Connect-AzAccount » et authentifiez-vous auprès d'Azure.

2. Listez les machines virtuelles dans un groupe de ressources.
   Vous ne vous souvenez peut-être pas du nom de votre machine virtuelle, mais si vous vous souvenez du nom du groupe de ressources, exécutez cette commande « Get-AzVM -ResourceGroupeName 'VotreNom' »
3. Arrêtez la machine virtuelle cible avec cette commande : « Stop-AzVm -Name 'nom' -ResourceGroupeName 'nom' -Force
4. Démarrez une machine virtuelle avec la commande « Get-AzVM -Name 'nom' -ResourceGroupName 'nom' | Start-AzVM
   Le caractère pipe (|) passe les résultats du premier segment (obtenir une référence à la VM cible) au deuxième segment. Cette technique s'appelle le pipelining.

3.3. Redimensionner une machine virtuelle

Pour redimensionner une machine virtuelle sur Azure, suivez ces étapes :

1. Dans les paramètres de votre machine virtuelle, sélectionnez « taille ».
2. Modifiez les filtres pour filtrer les tailles de machine virtuelles disponibles.
   Vous pouvez filtrer la taille de la VM en utilisant n'importe quelle combinaison des propriétés suivantes :
   - Taille : Les choix sont Petit, Moyen et Grand.
   - Génération : Les choix sont Actuelle, Précédente et Ancienne.
   - Famille : Les choix sont Usage général, GPU, Calcul haute performance, Optimisé pour le calcul, Optimisé pour la mémoire et Optimisé pour le stockage.
   - Disque Premium : Les choix sont Pris en charge et Non pris en charge.
   - vCPUs : Les choix vont de 1 à 64 cœurs vCPU.
   - RAM : Les choix vont de 2 Go à 432 Go.
3. Sélectionnez la taille souhaitée et cliquez sur redimensionner.

Votre machine virtuelle redémarre avec les nouvelles ressources matérielles virtuelles.

4. Déploiement et gestion des services App Azure

4.1. Introduction aux services App Azure

Azure App Service est un service d'hébergement d'applications Web basé sur le protocole HTTP. L'idée c'est que si vous êtes prêt à céder le contrôle total à l'infrastructure sous-jacente de l'application, vous recevrez en échange :

- Réplication globale et disponibilité géographique
- Mise à l'échelle automatique
- Intégration native dans les pipelines d'intégration continue/déploiement continue

App Service utilise des machines virtuelles, mais vous ne devez pas vous en soucier de leur maintenance. Au lieu de cela, vous vous focalisez exclusivement sur votre application et son code source.

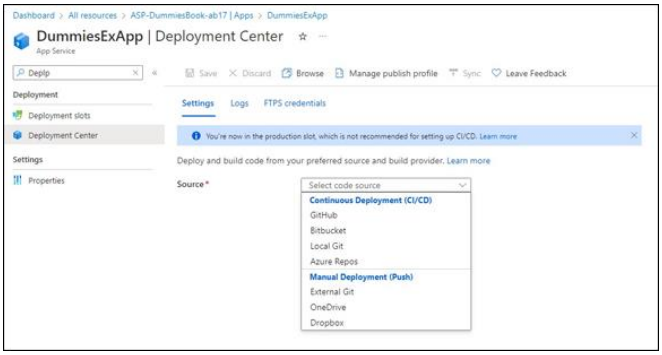
4.2. Déploiement d'une application web

Déploiement depuis le portail Azure :

1. Dans le menu du portail Azure, dans créer une nouvelle ressource, sélectionnez « Web App », puis cliquez sur créer.
2. Remplissez le formulaire Créer une application Web comme suit :
    - Nom de l'application : le nom de votre application doit être unique au monde, car Microsoft le place dans le domaine DNS azurewebsites.net. Mais vous pouvez et devez lier votre propre domaine DNS d'entreprise à votre site dès que possible après avoir créé l'application Web.
    - Plan/Emplacement App Service : créez un nouveau plan App Service dans votre emplacement d'origine. Choisissez S1 Standard, qui est la plus petite taille d'instance de VM permettant de débloquer des fonctionnalités de niveau production.
    - Application Insights : sélectionnez l'option Désactiver. (Je discute de la surveillance des applications Web plus loin dans ce chapitre dans « Surveillance d'une application Web ».)
3. Cliquez sur Créer pour soumettre le déploiement.
4. Ouvrez l'application Web.

4.2.1. Intégration de Git

Git s'intègre parfaitement à Azure App Service. En fait, les applications App Service peuvent héberger leur propre référentiel Git.



4.2.2. Connexion à une application web avec Visual Studio

Voici le workflow général

1. Créer un répertoire Git localement pour votre application sur Azure
2. Clonez le référentiel basé sur Azure sur votre poste de travail local.
3. Travaillez avec l'application localement et transférez périodiquement les modifications vers Azure.

Voici les différentes étapes afin de réaliser cela :

1. Dans les paramètres de votre Web App, dans le portail Azure, sélectionnez « Centre de déploiement ».
2. Choisissez « Local Git » comme fournisseur de code source.
3. Pour fournisseur de build, choisissez le service de build App service.
4. Dans le panneau du centre de déploiement, copiez l'URL de clonage dans le champ référentiel.
5. Ouvrez Azure Cloud Shell et créez des informations d'identification de déploiement Git.
   Ces informations seront utiles afin de s'authentifier auprès du référentiel Git sur Azure. Lorsque vous êtes sur la session Azure Cloud Shell, exécutez la commande suivante :

   ```
   az webapp deployment user set --password &lt;your password&gt; --user-name &lt;your username&gt;
   ```

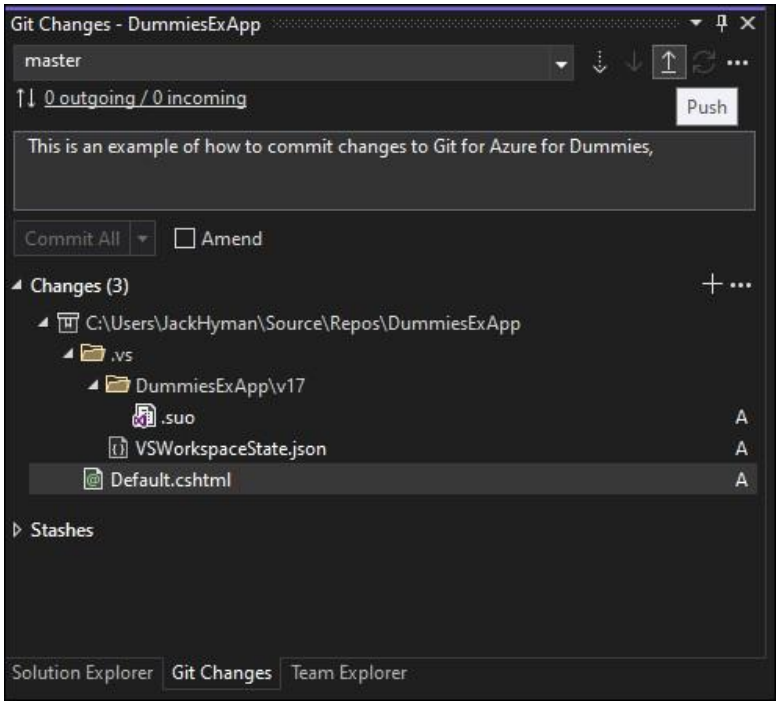
   Make a note of both the username and password, because you'll need them for the next step.
6. Accédez à la barre de menu et localisez Git. Sélectionnez Cloner dans la section Dépôts Git locaux
7. Collez l'URL de votre clone App Service (étape 4) et vérifiez le chemin du répertoire local et le nom du dossier. Cliquez sur Cloner.
8. Entrez vos informations d'identification de déploiement Git lorsque Visual Studio vous les demande.
9. Vous voyez le référentiel cloné dans le volet Explorateur de solutions. Dans la barre de menu, choisissez Fichier ⇒ Nouveau ⇒ Projet à partir du code existant.
10. La boîte de dialogue Créer un nouveau projet s'ouvre. Recherchez la correspondance la plus proche de votre application Web existante.
11. Vous avez déployé une application Web ASP.NET dans App Service. Le choix logique est donc Application Web ASP.NET (.NET Framework).
12. Donnez à la version locale un nom, tel que 1.0, et un emplacement de sauvegarde.
13. Sélectionnez le modèle vide.
14. Laissez tous les autres paramètres à leurs valeurs par défaut et cliquez sur OK.

4.2.3. Pousser une modification de code vers Azure

Après avoir fait une modification sur votre code, vous devez transmettre cette modification à Azure. Suivez ces étapes pour mettre à jour votre code sur Azure :

1. Dans l'explorateur de solutions, cliquez sur le bouton « changer de vue » pour passer à la vue Dossier.

2. Évaluez les fichiers qui ont été modifiés depuis votre dernier transfert vers Azure en accédant à Git Changes.
3. Entrez un message de validation significatif, puis choisissez Commit All et Push dans la barre de menu.



4.3. Configuration d'une application web

4.3.1. Configuration de la scalabilité automatique

Supposons que vous souhaitiez configurer votre application Web pour passer d'une à trois instances, en fonction de la charge CPU du plan App Service surveillée sur une période de 10 minutes. Tout aussi important, vous souhaitez réduire votre nombre minimum d'instances lorsque le pic d'utilisation s'installe. Voici les étapes afin de réaliser cela :

1. Dans les paramètres de votre application Web, sélectionnez « Scale Out » (plan App Service), puis cliquez sur « Custom Autoscale ».
2. Pour le mode Échelle, sélectionnez Échelle basée sur une métrique et configurez les limites d'instance. Il est important de comprendre la différence entre les trois options de limite d'instance :

   Minimum : le plus petit nombre d'instances que vous souhaitez exécuter. Notez que vous êtes facturé pour chaque instance.

   Maximum : le plus grand nombre d'instances simultanées dont vous envisagez d'avoir besoin.

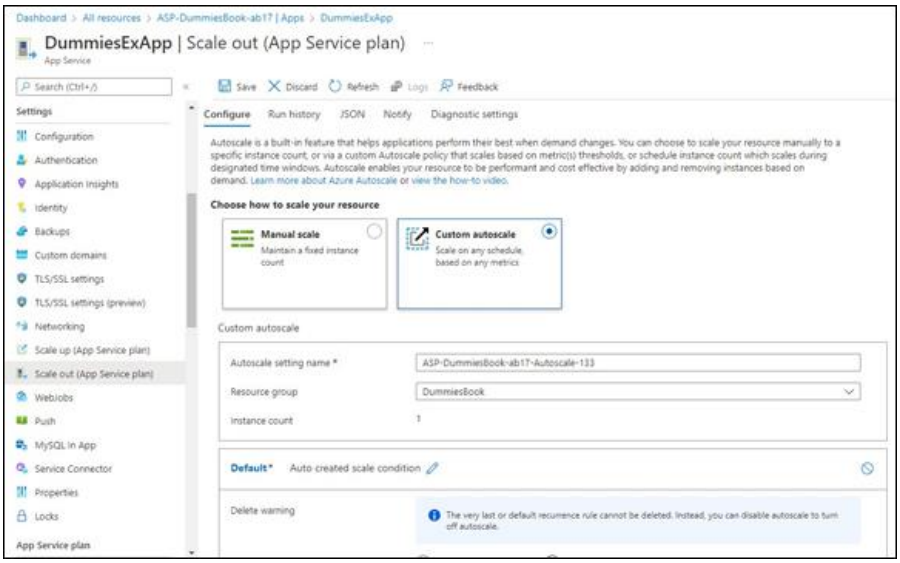
   Par défaut : valeur qu'Azure utilise comme solution de secours s'il ne parvient pas à calculer une métrique.
3. Sélectionnez Ajouter une règle pour définir une règle d'échelle.
   Utilisez les paramètres suivants comme référence, mais n'hésitez pas à expérimenter :

   Agrégation temporelle : moyenne

   Nom de la métrique : pourcentage de CPU

Nom de la dimension, opérateur, valeurs : Instance : = Toutes les valeurs
Statistique de grain temporel : moyenne
Opérateur et seuil : supérieur à 70
Durée : 10 minutes
Action : Augmentez le nombre d'une instance, avec un temps de recharge de 5 minutes.
La valeur de refroidissement spécifie la durée pendant laquelle Azure attend avant de procéder à une nouvelle mise à l'échelle.

4. Cliquez sur Ajouter.
   Vous avez créé une condition d'échelle pour étendre l'échelle de votre application Web, mais n'oubliez pas la de créer une condition pour diminuer l'échelle de cette-même.
5. Sélectionnez Ajouter une échelle pour créer une nouvelle règle de métrique qui réduit le cluster lorsque l'utilisation du processeur atteint 40 % ou moins.



4.4. Surveillance de votre application web

Grâce à Application Insights, il est possible de surveiller vos applications App Service. Il s'agit d'une plateforme de gestion des performances des applications hébergée sur Azure qui fournit une analyse approfondie et détaillée de presque n'importe quelle application, qu'elle soit hébergée sur Azure, sur site ou sur un autre cloud. Application Insights est une fonctionnalité intégrée à Azure Monitor.

Voici quelques-unes des informations qu'Application Insights peut fournir à vos développeurs :

- Temps de requête et de réponse et taux d'échec : Vous pouvez voir quelles pages de votre application Web sont les plus ou les moins populaires à différents moments de la journée, ainsi que d'où se connectent vos utilisateurs.
- Taux de dépendance : Vous pouvez visualiser graphiquement toutes les dépendances de votre application vis-à-vis des composants externes, ce qui peut garantir une

disponibilité continue lorsque vous devez effectuer des opérations de maintenance ou de migration.
- Compteurs de performances : Vous pouvez observer les statistiques de performance collectées à partir de l'infrastructure VM sous-jacente de votre application Web.
- Tableaux de bord : Vous pouvez représenter graphiquement vos données de télémétrie de manière facilement compréhensible.
- Profileur : Vous pouvez suivre les opérations de requêtes et de réponses de votre application Web, opération par opération.

4.4.1. Ajout de la ressource Application Insights :

Suivez ces étapes pour créer une nouvelle ressource Application Insights dans votre abonnement Azure :

1. Dans le portail Azure, accédez à l'onglet supervision, localisez l'onglet Application Insights, puis cliquez sur Créer.
2. Configurez les détails de la ressource.
   Le point principal auquel vous devez être attentif est qu'afin de garantir la latence la plus faible, localisez votre ressource Application Insights dans la même région Azure que l'application Web avec laquelle elle sera associée.
3. Soumettez le déploiement en cliquant sur Examinez + Créez, puis sur Créer.

Afin de visualiser les insights de votre application, ouvrez votre ressource Application Insights, puis cliquez sur tableau de bord de l'application dans l'onglet aperçu.

Il est possible d'intégrer Applications Insights directement dans votre éditeur de code en ajoutant le kit de développement logiciel (SDK) à votre projet. Cela vous permet de collecter des données de télémétrie depuis votre application et de les envoyer à votre ressource Application Insights pour analyse.

5. Protection et gestions des services App Azure

5.1. Protection des services App

L'un des avantages de la sauvegarde intégrée dans Azure App Service est qu'en plus de sauvegarder le code source de l'application, Azure sauvegarde également ses paramètres de configuration associés et les fichiers de support :

- Les artefacts du système de fichiers de l'application
- Les données de configuration de l'application
- La base de données connectée à l'application

5.2. Sauvegarde des services App

Pour sauvegarder les applications App Service, suivez ces étapes :

1. Sur la page Paramètres de votre application, cliquez sur Sauvegardes.
2. Dans la barre d'outils, cliquez sur Configurer.
3. Complétez la page Configuration de sauvegarde avec les informations suivantes :
   - Stockage de sauvegarde : Sélectionnez un compte de stockage dans la même région et créez ou désignez un conteneur existant pour stocker les sauvegardes de votre application.
   - Planification des sauvegardes : Planifiez des sauvegardes automatiques tous les n jours ou heures, et choisissez votre période de rétention en jours.
   - Sauvegarde de la base de données (facultatif) : Incluez une connexion de base de données dans la définition de la sauvegarde.
4. Cliquez sur Enregistrer pour valider votre configuration.
5. Cliquez sur Sauvegarder pour soumettre le déploiement.

5.3. Restauration des services App

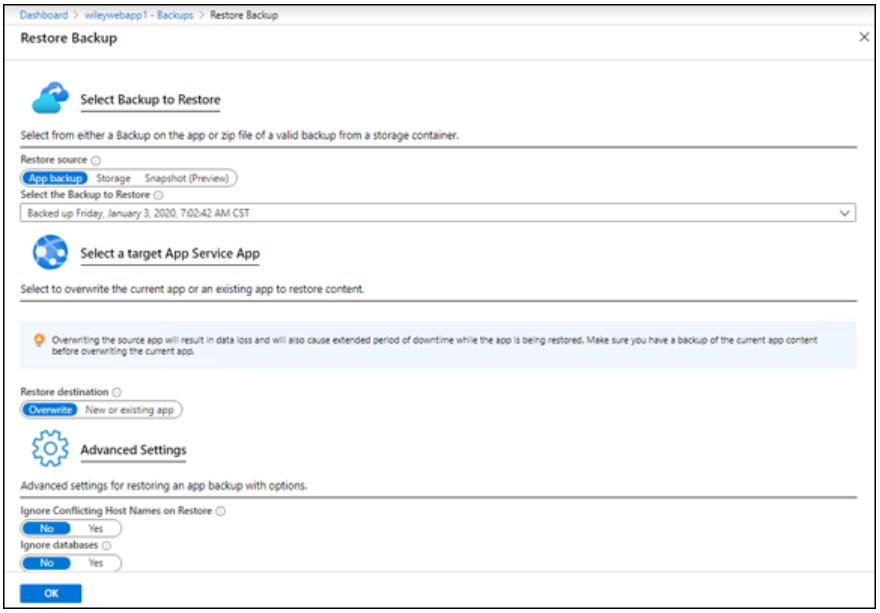
Cette section examine l'autre côté de la pièce proverbiale : la restauration des applications. Peut-être souhaitez-vous effectuer une restauration d'essai d'App Service pour vous assurer que la sauvegarde est cohérente.

Pour restaurer un App Service, suivez ces étapes :

1. Accédez à l'onglet Sauvegardes de votre application App Service.
2. Dans la section Sauvegarde, sélectionnez Restaurer.
3. Complétez la page Restaurer la sauvegarde.
   Source de restauration : Les choix sont Sauvegarde de l'application (choisissez celui-ci), Stockage ou Instantané.
   Sélectionnez la sauvegarde à restaurer : Cette liste répertorie les sauvegardes précédemment effectuées.
   Destination de restauration : Les choix sont Écraser ou Nouvelle application ou Application existante.
   Ignorer les noms d'hôte en conflit lors de la restauration : Les choix sont Non ou Oui. Laissez cette option sur Non pour empêcher Azure de restaurer une application App Service avec un nom en conflit dans votre environnement.

Ignorer les bases de données : Les choix sont Non ou Oui. Si votre application web a une chaîne de connexion de base de données, vous voudrez définir cette option sur Non.

4. Cliquez sur OK pour terminer le processus de restauration de l'App Service.



Bibliographie

Hyman, J. A. (2023). *Microsoft Azure for dummies*. John Wiley & Sons.