RÉSUME THÉORIQUE - FILIÈRE INFRASTRUCTURE DIGITALE

M212 – Administrer un environnement Cloud propriétaire en ligne public

53 heures

SOMMAIRE

MODALITÉS PÉDAGOGIQUES

1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques

2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life

3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life

4

DU CONTENU INTERACTIF

Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life

5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage

PARTIE 1

Provisionner une machine virtuelle

Dans ce module, vous allez :

- Établir les prérequis à la création d’une machine virtuelle
- Créer une machine virtuelle
- Configurer la disponibilité d’une machine virtuelle

18 heures

CHAPITRE 1

Établir les prérequis à la création d'une VM

Ce que vous allez apprendre dans ce chapitre :

- Initialiser la création d'une VM
- Contrôler le système d'exploitation d'une VM
- Gérer la configuration d'une VM
- Configurer la disponibilité de la VM

6 heures

CHAPITRE 1

Établir les prérequis à la création d'une VM

1. **Disponibilité selon les SLA**
2. Taille appropriée de la machine virtuelle
3. Limites des machines virtuelles en termes de quota
4. Image et disques de machine virtuelle

01- Établir les prérequis à la création d'une VM

Disponibilité selon les SLA

Qu'est ce qu'un Service Level Agreement (SLA) ?

- Le **Service Level Agreement** abrévié **SLA**. On peut le traduire par **Accord de niveaux de service**, est un document qui définit la qualité de service entre un fournisseur et un client pour définir le niveau de service proposé par le fournisseur et accepté par le client.
- Le **SLA** tend à devenir un outil essentiel aux clients souhaitant bénéficier d'une sécurité élevée sur certains de leurs niveaux de sécurité de stockage ainsi que sur la gestion de leurs données à caractère personnel. L'optimisation des performances des fournisseurs de services nécessite de définir, d'analyser et de contrôler de nombreuses métriques.

La disponibilité du SLA est mesurée en déterminant le pourcentage de temps pendant lequel un service sous contrat peut réellement être consulté sur une période de temps. Généralement, ce pourcentage est proche de 99 % ou 99,9 % pour divers fournisseurs. C'est plutôt le système de pénalités qui différencie vraiment les SLA. C'est un détail très important et qui n'est pas toujours fourni par les prestataires de services.

1 Définir les **points de satisfaction** du **client**

2 Définir des mesures de **contrôle** de la **qualité** de service

4 Définir et **suivre** la qualité de service par des **indicateurs clés**

3 **Prévenir** les **contentieux** relatifs aux services entre le fournisseur et le client

PARTIE 1

Objectif de SLA

Le **SLA** est intimement lié à l'univers du Cloud. Il veille à ce que les clients aient un certain niveau de sécurité lors du stockage et de la gestion de leurs données personnelles. Il est ensuite nécessaire de définir très précisément divers indicateurs de qualité qui peuvent être mesurés, analysés et surveillés régulièrement. Enfin, il y a lieu de prévoir des sanctions si le prestataire de services ne remplit pas les obligations mentionnées dans le SLA.

Distinction entre SLA et UC, OLA

Service Level Agreement (SLA)	il formalise les relations dans l'organisation entre le client métier», comme une direction opérationnelle, et la direction des systèmes d'information.
Underpinning contract (UC)	il régit les relations entre la direction des systèmes d'information et ses sous-traitants, prestataires de services ou fournisseurs..
Operational level agreement (OLA)	il établit les relations entre les différentes entités ou services de l'organisation des IT.

SLA contenu

- Le **type de service à fournir** : il doit spécifier les types de services ainsi que tous les détails de ces derniers. Dans le cas d'une connectivité réseau IP, les types de services doivent décrire les fonctions comme l'utilisation et la maintenance des équipements réseau, la largeur de bande de connexion à fournir, etc.
- Le **niveau de performance souhaité des services, en particulier sa fiabilité et sa réactivité** : un service fiable est celui qui souffre de perturbations minimes durant un espace de temps spécifique, mais également celui qui est disponible presque tout le temps. Un service avec une bonne réactivité réalisera les actions rapidement auprès des clients.
- Les **étapes à suivre pour signaler les problèmes du service** : cette étape a pour but de spécifier les coordonnées à signaler et l'ordre dans lequel les détails sur le problème doivent être communiqués. Le contrat doit également informer sur l'intervalle de temps au cours duquel le problème sera examiné.
- Le **temps de réponse et les solutions aux problèmes examinés** : le temps de réponse est la période de temps au cours duquel le fournisseur de service va lancer son enquête sur le problème. Le temps de résolution du problème est la période durant laquelle le problème actuel du service sera résolu et corrigé.
- Le **suivi des processus et les rapports de niveau de service** : ce composant décrit comment les niveaux de performance sont supervisés et surveillés. Ce processus implique la collecte de différents types de statistiques, la fréquence à laquelle ces statistiques seront collectées et la façon dont ces statistiques seront accessibles par les clients.
- Les **répercussions pour le fournisseur de services qui ne respecte pas son engagement** : si le fournisseur n'est pas en mesure de satisfaire aux exigences énoncées dans le SLA, ce dernier devra faire face aux conséquences pour cet échec. Ces conséquences peuvent inclure le droit du client de résilier le contrat ou de demander un remboursement pour les pertes subies par le client en raison de la défaillance du service.
- **Les conditions de paiement**: doivent être très précise afin que le client ait une limitation de temps et que le fournisseur ait au moins un engagement de la part de son client.

CHAPITRE 1

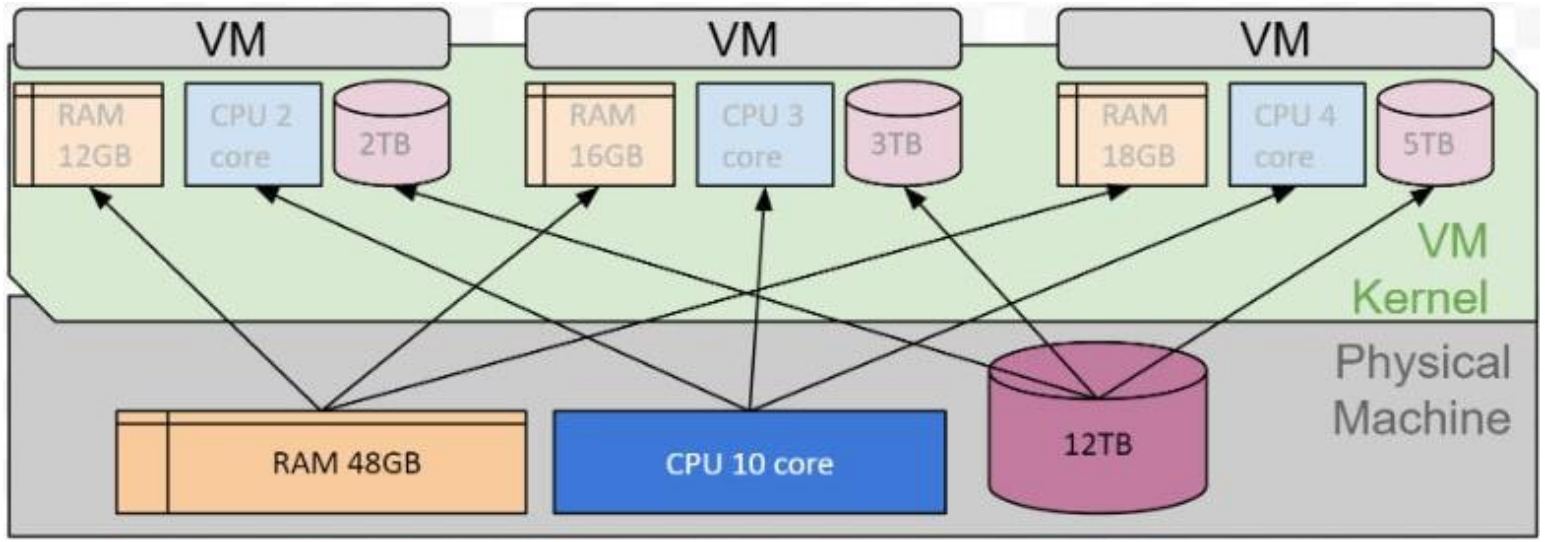
Établir les prérequis à la création d'une VM

1. Disponibilité selon les SLA
2. **Taille appropriée de la machine virtuelle**
3. Limites des machines virtuelles en termes de quota
4. Image et disques de machine virtuelle

PARTIE 1

Machine virtuelle (VM) : Définition

- Une **machine virtuelle** abrévié (en anglais : **VM)** est un environnement virtuel qui se comporte comme un système informatique virtuel avec son propre processeur, sa mémoire, ses interfaces réseau et son espace de stockage, mais construit au-dessus d'un système matériel physique (local ou externe).
- Les **machines virtuelles** vous permettent d'exécuter plusieurs systèmes d'exploitation simultanément sur un seul ordinateur. Par exemple, vous pouvez exécuter une distribution **Linux** sur votre ordinateur portable exécutant **MacOs**. Chaque système d'exploitation, comme tout autre système d'exploitation ou application, s'exécute sur du matériel hôte. Par conséquent, l'expérience de l'utilisateur final émulée dans une machine virtuelle est presque identique à celle d'un système d'exploitation s'exécutant en temps réel sur une machine physique.



Machine virtuelle d'Azure

Les machines virtuelles Azure constituent une ressource de Cloud computing à la demande et scalable. Elles sont semblables aux machines virtuelles hébergées dans Windows Hyper-V. Elles incluent un processeur, de la mémoire, du stockage et des ressources réseau. Vous pouvez démarrer et arrêter les machines virtuelles à volonté, comme avec Hyper-V, et les gérer à partir du portail Azure ou avec Azure CLI.

Vous pouvez également avoir recours à un client prenant en charge le protocole RDP (Remote Desktop Protocol) pour vous connecter directement à l'interface utilisateur du bureau de Windows et utiliser la machine virtuelle comme si vous étiez connecté à un ordinateur Windows local.

Fonctionnalité d'une machine virtuelle

- Le partage de différents environnements virtuels est géré par des hyperviseurs, généralement hébergés dans des Clouds publics, privés ou hybrides. Effectuez le partitionnement des ressources et attribuez des partitions à chaque machine virtuelle. Cela se fait à l'aide d'un logiciel installé sur une machine physique. Ces derniers disposent généralement de ce qu'on appelle un pool commun de ressources physiques. Avantage principal ? Autorisez les machines virtuelles qui ont besoin d'accéder à des ressources supplémentaires à gérer les demandes croissantes des utilisateurs.

Parmi les avantages d'une machine virtuelle

- Tester un nouveau système d'exploitation sans avoir besoin de partitionner son disque dur. Le test peut ainsi s'effectuer sans risques d'endommager le disque dur de votre machine.
- Développer un logiciel ou un programme pour un autre système d'exploitation.
- Se servir de logiciels qui ne peuvent pas tourner sur le système d'exploitation de votre machine physique. Vous pouvez ainsi disposer d'une machine virtuelle par système d'exploitation et même de plusieurs versions du même système d'exploitation.
- Réaliser des économies en installant plusieurs machines virtuelles sur un seul support physique plutôt que de multiplier les ordinateurs en service.

Familles de machine virtuelle

Pour choisir une taille appropriée d'une VM, il faut agir à la fois sur son CPU et sa mémoire.

Sur Azure, les tailles des machines virtuelles sont regroupées par famille :

Famille	Taille	Description
Usage général	B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC, DCv2, Dv4, Dsv4, Ddv4, Ddsv4, Dv5, Dsv5, Ddv5, Ddsv5, Dasv5, Dadsv5	Rapport CPU/mémoire équilibré. Idéal pour les tests et le développement, les bases de données petites à moyennes et les serveurs Web à trafic faible à moyen.
Calcul optimisé	F, Fs, Fsv2, FX	Rapport CPU/mémoire élevé. Convient aux serveurs Web à trafic moyen, aux appareils réseau, aux processus par lots et aux serveurs d'applications.
Mémoire optimisée	Esv3, Ev3, Easv4, Eav4, Ebdsv5, Ebsv5, Ev4, Esv4, Edv4, Edsv4, Ev5, Esv5, Edv5, Edsv5, Easv5, Eadsv5, Mv2, M, DSv2, Dv2	Rapport mémoire/processeur élevé. Idéal pour les serveurs de bases de données relationnelles, les caches moyens à grands et les analyses en mémoire.
Stockage optimisé	Lsv2, Lsv3, Lasv3	Haut débit de disque et IO idéal pour les bases de données Big Data, SQL, NoSQL, l'entreposage de données et les grandes bases de données transactionnelles.
GPU	NC, NCv2, NCv3, NCasT4_v3, ND, NDv2, NV, NVv3, NVv4, NDasrA100_v4, NDm_A100_v4	Machines virtuelles spécialisées ciblées pour le rendu graphique lourd et le montage vidéo, ainsi que la formation et l'inférence de modèles (ND) avec apprentissage en profondeur. Disponible avec un ou plusieurs GPU.
Calcul haute performance	HB, HBv2, HBv3, HC, H	Nos machines virtuelles CPU les plus rapides et les plus puissantes avec des interfaces réseau à haut débit (RDMA) en option.

CHAPITRE 1

Établir les prérequis à la création d'une VM

1. Disponibilité selon les SLA
2. Taille appropriée de la machine virtuelle
3. **Limites des machines virtuelles en termes de quota**
4. Image et disques de machine virtuelle

Pourquoi le quota ?

De nombreux services Azure ont des quotas, qui correspondent au nombre de ressources affecté à votre abonnement Azure. Chaque quota représente une ressource comptable spécifique, telle que le nombre de machines virtuelles que vous pouvez créer, le nombre de comptes de stockage que vous pouvez utiliser simultanément, le nombre de ressources réseau que vous pouvez consommer ou le nombre d'appels d'API à un service particulier que vous pouvez Fabriquer.

Le concept de quotas est conçu pour aider à protéger les clients contre des problèmes tels que les déploiements de ressources inexactes et la consommation erronée. Pour Azure, cela permet de minimiser les risques liés à une consommation trompeuse ou inappropriée et à une demande inattendue.

Afficher les détails des quotas

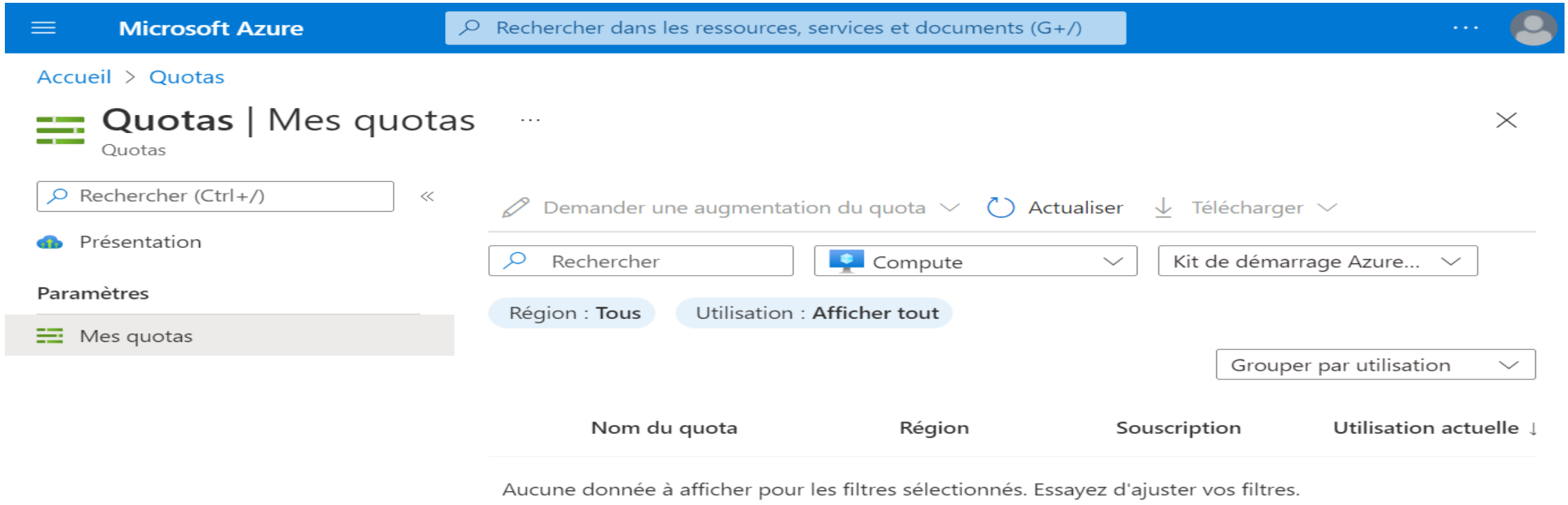
Pour afficher des informations détaillées sur vos quotas, sélectionnez Mes quotas dans le volet gauche de la page Quotas.

Sur la page Mes quotas , vous pouvez choisir les quotas et les données d'utilisation à afficher. Les options de filtrage en haut de la page vous permettent de filtrer par emplacement, fournisseur, abonnement et utilisation. Vous pouvez également utiliser la zone de recherche pour rechercher un quota spécifique. Selon le fournisseur que vous sélectionnez, vous pouvez constater des différences dans les filtres et les colonnes.

01- Établir les prérequis à la création d'une VM

Limites des machines virtuelles en termes de quota

Augmenter les quotas de vCPU de la famille de VM



Dans la liste des quotas, vous pouvez basculer la flèche affichée à côté de Quota pour développer et fermer des catégories. Vous pouvez faire la même chose à côté de chaque catégorie pour explorer et créer une vue des informations dont vous avez besoin.

PARTIE 1

Augmenter les quotas de vCPU de la famille de VM

Azure Resource Manager applique deux types de quotas vCPU pour les machines virtuelles :

- quotas vCPU standards
- quotas de vCPU ponctuels

Les quotas vCPU standard s'appliquent aux VM payantes et aux instances de VM réservées. Ils sont appliqués à deux niveaux, pour chaque abonnement, dans chaque région :

- Le premier niveau correspond au quota régional total de vCPU.
- Le deuxième niveau est le quota de vCPU de la famille de machines virtuelles, comme les vCPU de la série D.

Lors d'une demande d'augmentation de quota, les étapes diffèrent selon que le quota est ajustable ou non.

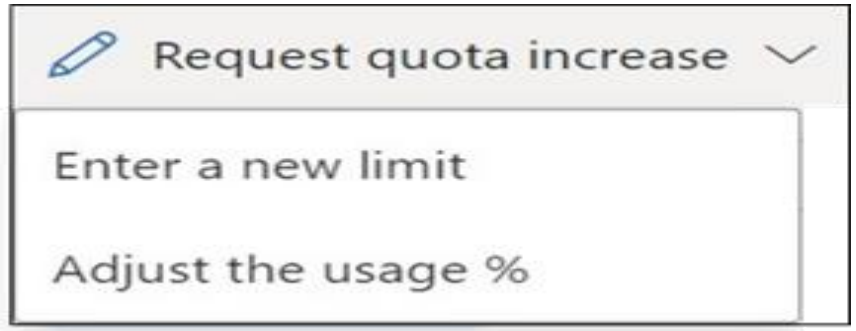
- Quotas ajustables : les quotas pour lesquels vous pouvez demander des augmentations de quota entrent dans cette catégorie. Chaque abonnement a une valeur de quota par défaut pour chaque quota. Vous pouvez demander une augmentation pour un quota ajustable à partir de la page Accueil Azure Mes quotas , en fournissant un montant ou un pourcentage d'utilisation et en le soumettant directement. C'est le moyen le plus rapide d'augmenter les quotas.
- Quotas non modifiables : ce sont des quotas qui ont une limite dure, généralement déterminée par le périmètre de l'abonnement. Pour apporter des modifications, vous devez soumettre une demande de support, et l'équipe de support Azure vous aidera à fournir des solutions.

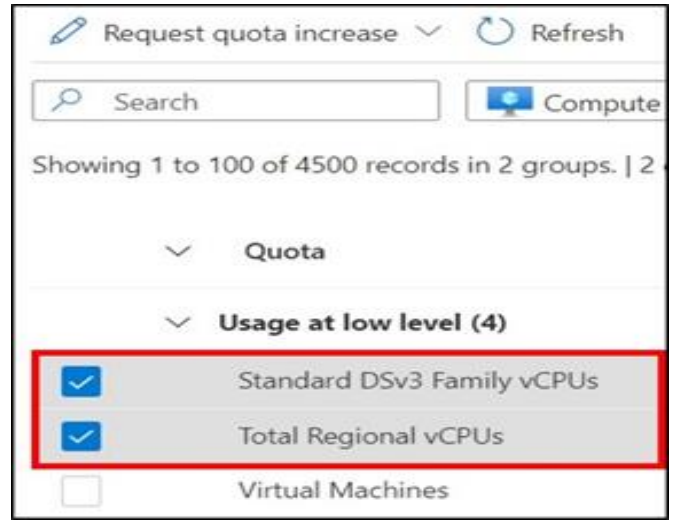
Demander une augmentation pour les quotas ajustables (1/4)

Vous pouvez soumettre une demande d'augmentation de quota de vCPU standard par famille de machines virtuelles à partir de Mes quotas , accessible rapidement à partir d' Azure Home .

1. Pour afficher la page Quotas , connectez-vous au portail Azure et saisissez quotas » dans la zone de recherche, puis sélectionnez Quotas .
2. Sur la page Présentation , sélectionnez Calculer .
3. Sur la page Mes quotas , sélectionnez le ou les quotas que vous souhaitez augmenter.
4. En haut de la page, sélectionnez Demander une augmentation de quota ,

   puis sélectionnez la manière dont vous souhaitez augmenter le ou les quotas.

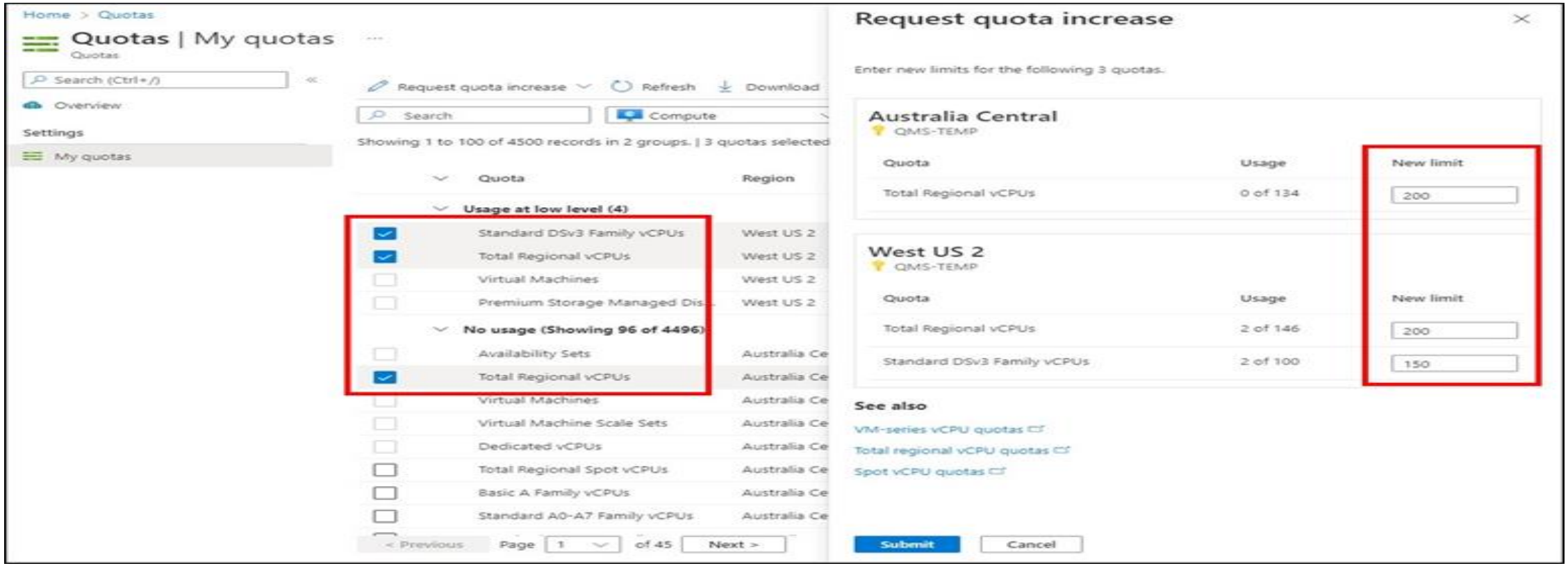




PARTIE 1

Demander une augmentation pour les quotas ajustables (2/4)

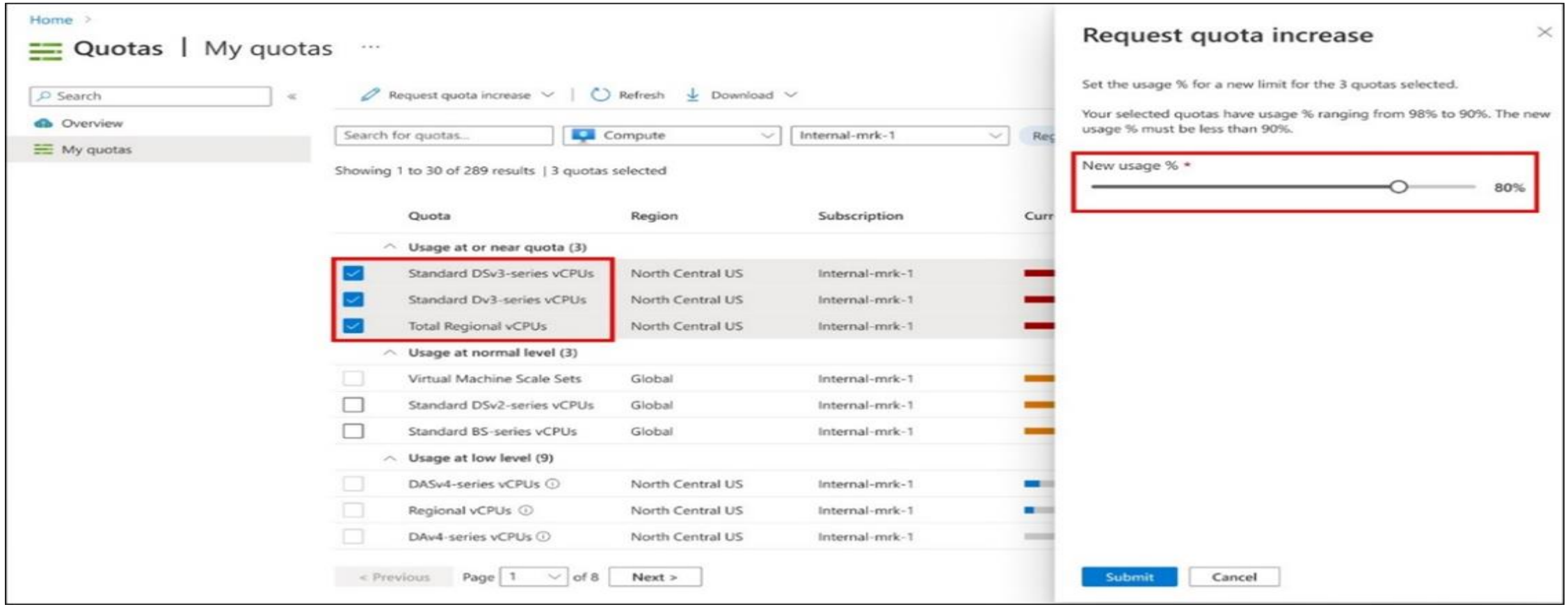
5. Si vous avez sélectionné Saisir une nouvelle limite, dans le volet Demander une augmentation de quota, saisissez une valeur numérique pour votre ou vos nouvelles limites de quota, puis sélectionnez Soumettre .



PARTIE 1

Demander une augmentation pour les quotas ajustables (3/4)

6. Si vous avez sélectionné Ajuster le % d'utilisation, dans le volet Demander une augmentation de quota , réglez le curseur sur un nouveau pourcentage d'utilisation. L'ajustement du pourcentage calcule automatiquement la nouvelle limite pour chaque quota à augmenter.



PARTIE 1

Demander une augmentation pour les quotas ajustables (4/4)

Votre demande sera examinée et vous serez informé si la demande peut être satisfaite. Cela se produit généralement en quelques minutes. Si votre demande n'est pas satisfaite, vous verrez un lien où vous pouvez ouvrir une demande d'assistance afin qu'un ingénieur de l'assistance puisse vous aider avec l'augmentation.

https://docs.microsoft.com/en-us/azure/azure-portal/supportability/how-to-create-azure-support-request

CHAPITRE 1

Établir les prérequis à la création d’une VM

1. Disponibilité selon les SLA
2. Taille appropriée de la machine virtuelle
3. Limites des machines virtuelles en termes de quota
4. **Image et disques de machine virtuelle**

Image de machine virtuelle

Une image de machine virtuelle est un fichier unique qui contient un disque virtuel sur lequel un système d'exploitation amorçable est installé.

Les images de machines virtuelles sont disponibles dans différents formats. Un format décrit la manière dont les bits composant un fichier sont disposés sur le support de stockage. La connaissance d'un format est nécessaire pour qu'un consommateur puisse interpréter correctement le contenu du fichier (plutôt que de simplement le voir comme un tas de bits).

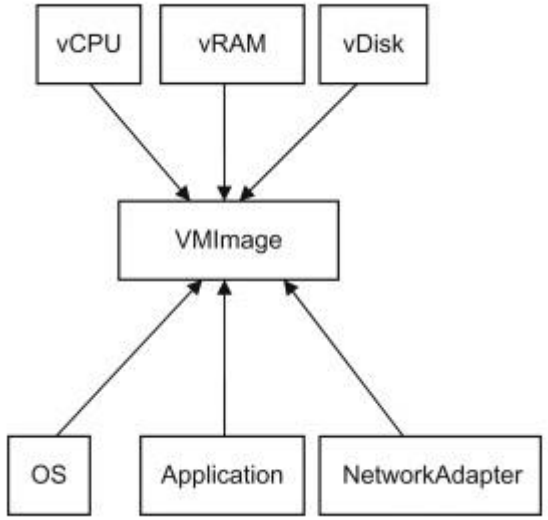
Lors de l'examen d'une image de machine virtuelle stockée, deux types de format peuvent entrer en jeu.

Format de conteneur

- Le fichier stocké peut être un conteneur qui contient le disque virtuel. Par exemple, le disque virtuel peut être contenu dans un tar fichier qui doit être ouvert avant que le disque puisse être récupéré. Il est toutefois possible que le disque virtuel ne soit pas contenu dans un fichier, mais soit simplement stocké tel quel par le service d'imagerie.

Formatage du disque

- Le disque virtuel lui-même a ses bits disposés dans un certain format. Un service consommateur doit connaître ce format avant de pouvoir utiliser efficacement le disque virtuel



PARTIE 1

Créer une image de la machine virtuelle

Utilisez le portail Azure pour effectuer les tâches suivantes. Veuillez vous connecter avec les informations d'identification qui vous ont été fournies pour cet atelier.

Convertir VM en image

1. Accédez à la page des services de machines virtuelles .
2. Ouvrez la machine virtuelle voulue.
3. Vérifiez que l'état s'affiche comme arrêté .
4. Utilisez le fichier RDP avec votre client RDP préféré.
5. Cliquez sur l' option Capturer dans le menu de commandes et utilisez les paramètres suivants :
    - **Nom**: VmImage
    - **Groupe de ressources** : laissez la valeur par défaut sélectionnée
    - **Supprimer automatiquement cette machine virtuelle** : non
    - **Saisissez le nom de la machine virtuelle** :vm
    - Cliquez sur Créer .

PARTIE 1

Créer une machine virtuelle à partir de l'image

1. Accédez à la page Services d' images .
2. Cliquez sur VmImage , que nous venons de créer.
3. Cliquez sur l' option + Créez une VM dans le menu de commandes et utilisez les paramètres suivants :

- **Bases**
    1. Abonnement : laisser tel quel
    2. Groupe de ressources : laisser tel quel
    3. Nom de la machine virtuelle : vm2
    4. Région : laisser tel quel
    5. Options de disponibilité : aucune
    6. Image : laisser tel quel
    7. Taille : B2s
    8. Compte administrateur : utilisez les identifiants de VM fournis
    9. Ports entrants publics : aucun
    10. Type de licence : serveur Windows
    11. Souhaitez-vous utiliser une licence Windows Server existante ? : Non

Créer une machine virtuelle à partir de l'image

1. Cliquez sur Suivant : Disques .
    - Disques
        1. Laissez tel quel
            - Cliquez sur Suivant : Mise en réseau
2. La mise en réseau
    - **Réseau virtuel** : vnet1
    - **Sous -réseau** : sous- réseau1
    - **IP publique** : laisser tel quel
    - **Groupe de sécurité réseau NIC** : Aucun
    - Cliquez sur Réviser + créer
    - Cliquez sur Créer

Disques de machine virtuelle (1/3)

Dans la virtualisation, les disques virtuels sont l'endroit où les systèmes d'exploitation invités sont installés, ce qui en fait l'équivalent des disques durs traditionnels. Une fois qu'une machine virtuelle a été installée avec un disque virtuel exécutant un système d'exploitation invité, elle est prête à être utilisée.

Les disques virtuels se présentent sous différents formats, selon le logiciel de virtualisation utilisé par le créateur pour les créer. Les formats de disque virtuel les plus populaires incluent Virtual Disk Image (VDI), Virtual Hard Disk (VHD) et Virtual Machine Disk (VMDK). VDI est le format de disque virtuel pour Oracle VirtualBox, VHD et VHDX sont conçus pour les produits de virtualisation de Microsoft, et VMDK est le propre format de disque virtuel de VMware.

Disque dur virtuel vs disque dur physique:

Un disque dur virtuel possède des fonctionnalités similaires à celles d'un disque dur physique . Par exemple, il contient souvent les mêmes secteurs de disque dur , comme un système de fichiers , des partitions de disque, etc. Il apparaît et fonctionne également comme un disque dur physiquement connecté au système. Comme un disque dur, le VHD peut effectuer les opérations suivantes :

- Créer des secteurs de disque, des fichiers et des dossiers
- Exécuter un système d'exploitation
- Exécuter des applications utilisateur

Disques de machine virtuelle (2/3)

Azure propose actuellement quatre types de disques managés, chaque type étant destiné à répondre à un scénario client spécifique :

- **Disques Ultra** : Charges de travail gourmandes en E/S, telles que les bases de données de niveau supérieur (par exemple, SQL et Oracle), et autres charges de travail très lourdes en transactions.
    1. **Taille maximale du disque :** 65 536 gibioctets (Gio)
    2. **Débit max :** 4 000 Mo/s
    3. **Nb max. d'E/S par seconde :** 160 000
- **Disques SSD Premium** : Charges de travail de production et sensibles aux performances.
    1. **Taille maximale du disque :** 32 767 Gio
    2. **Débit max :** 900 Mo/s
    3. **Nb max. d'E/S par seconde :** 20 000
- **SSD Standard :** Serveurs web, applications d'entreprise peu utilisées et Dev/Test
    1. **Taille maximale du disque :** 32 767 Gio
    2. **Débit max :** 750 Mo/s
    3. **Nb max. d'E/S par seconde :** 6000
- Disques durs Standard

Disques de machine virtuelle (3/3)

- **Disques durs HDD Standard** :
    1. **Taille maximale du disque :** 32 767 gibioctets (Gio)
    2. **Débit max :** 500 Mo/s
    3. **Nb max. d'E/S par seconde :** 2000

CHAPITRE 2

Créer une machine virtuelle

Ce que vous allez apprendre dans ce chapitre :

- Créer une VM via l'interface graphique du portail Azure
- Préparer un script de création d'une VM via Azure CLI

6 heures

CHAPITRE 2

Créer une machine virtuelle

1. **Provisionnement d’une VM via l’interface graphique**
2. Préparation d’un script de création d’une VM

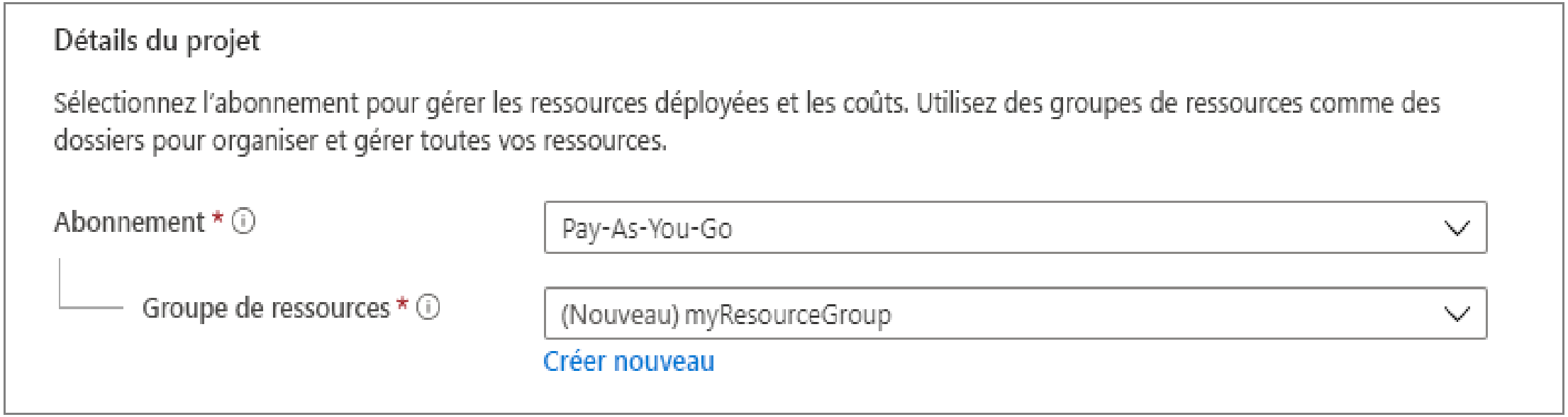
Provisionnement d'une VM sur Azure

Vous pouvez définir et déployer des machines virtuelles sur Azure de plusieurs façons :

- Portail Azure
- Script
  - Azure CLI
  - Azure PowerShell

Créer une machine virtuelle Windows via l'interface graphique du portail Azure

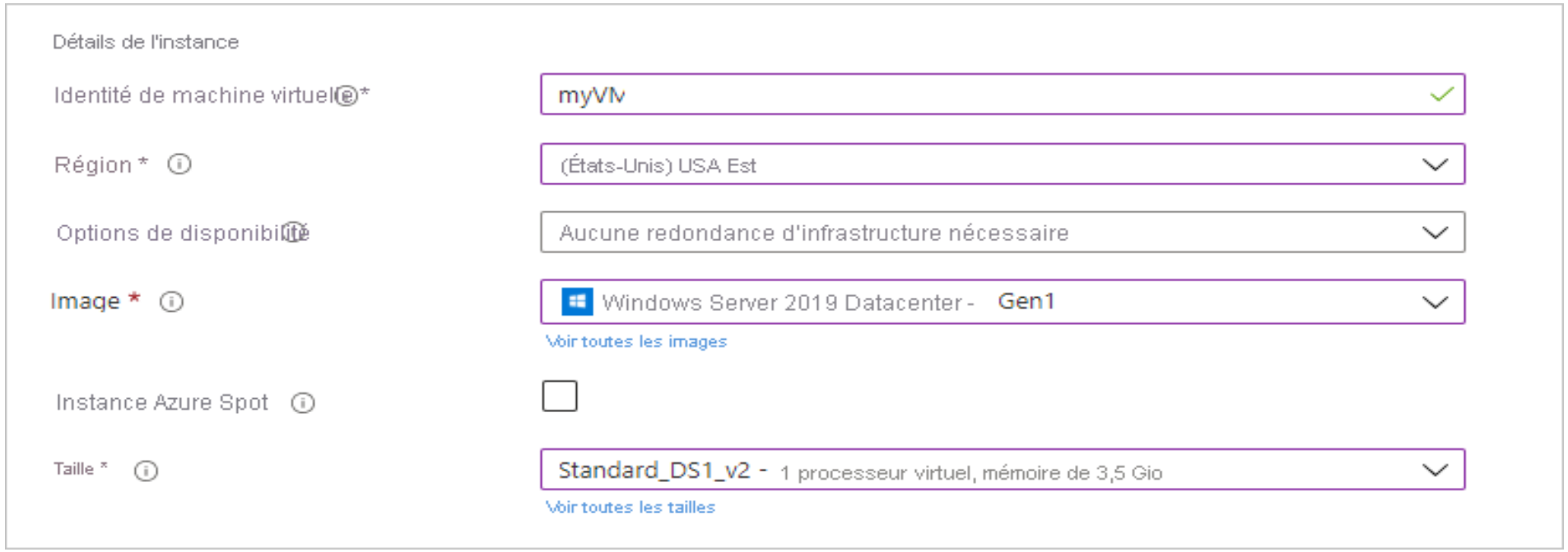
1. Entrez machines virtuelles dans la zone de recherche.
2. Sous Services, sélectionnez Machines virtuelles.
3. Dans la page Machines virtuelles, sélectionnez Créer, puis Machine virtuelle. La page Créer une machine virtuelle s'ouvre.
4. Sous l'onglet de base, sous Détails du projet, vérifiez que l'abonnement approprié est sélectionné, puis choisissez Créer pour créer un groupe de ressources. Entrez le nom myResourceGroup.



PARTIE 1

Créer une machine virtuelle Windows via l'interface graphique du portail Azure

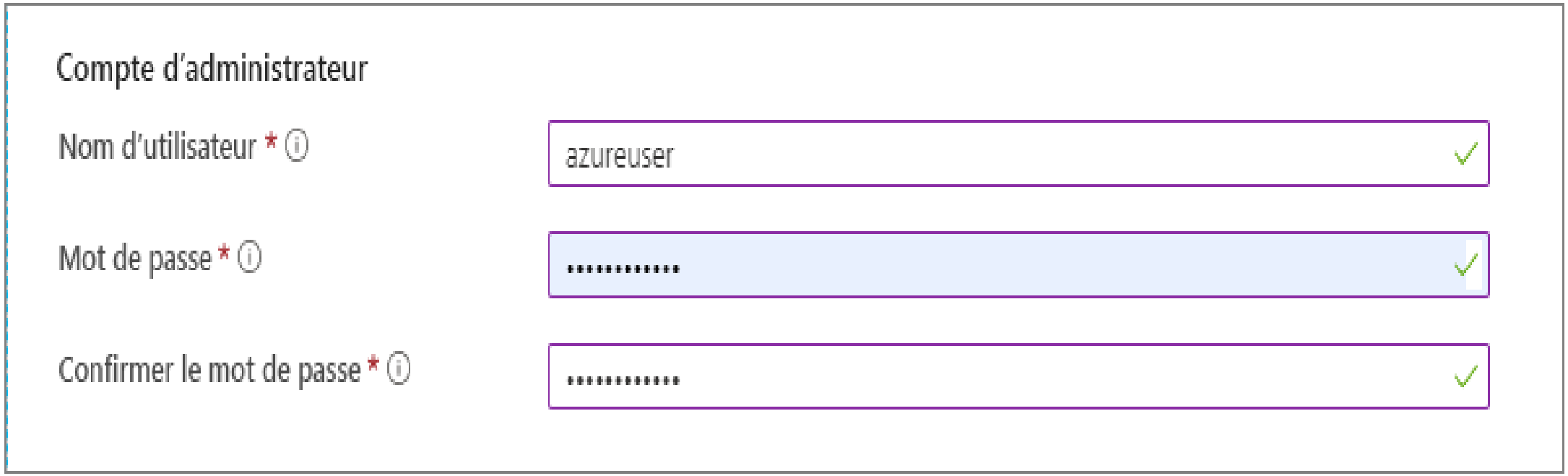
5. Sous **Détails de l'instance**, tapez *myVM* comme **Nom de la machine virtuelle**, puis choisissez *Windows Server 2019 Datacenter - Gen2* comme **Image**. Conservez les autres valeurs par défaut.



PARTIE 1

Créer une machine virtuelle Windows via l'interface graphique du portail Azure

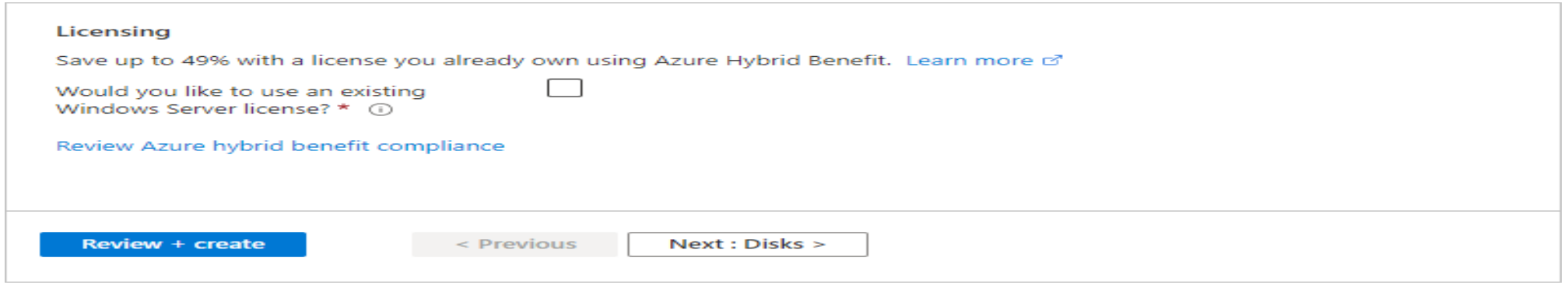
6. Sous Compte d'administrateur, indiquez un nom d'utilisateur (par exemple, azureuser) et un mot de passe. Le mot de passe doit contenir au moins 12 caractères et satisfaire aux exigences de complexité définies.



Créer une machine virtuelle Windows via l'interface graphique du portail Azure

7. Sous **Règles des ports d'entrée**, choisissez **Autoriser les ports sélectionnés**, puis sélectionnez **RDP (3389)** et **HTTP (80)** dans la liste déroulante.

8. Conservez les valeurs par défaut restantes, puis sélectionnez le bouton Vérifier + créer en bas de la page.



PARTIE 1

Créer une machine virtuelle Windows via l'interface graphique du portail Azure

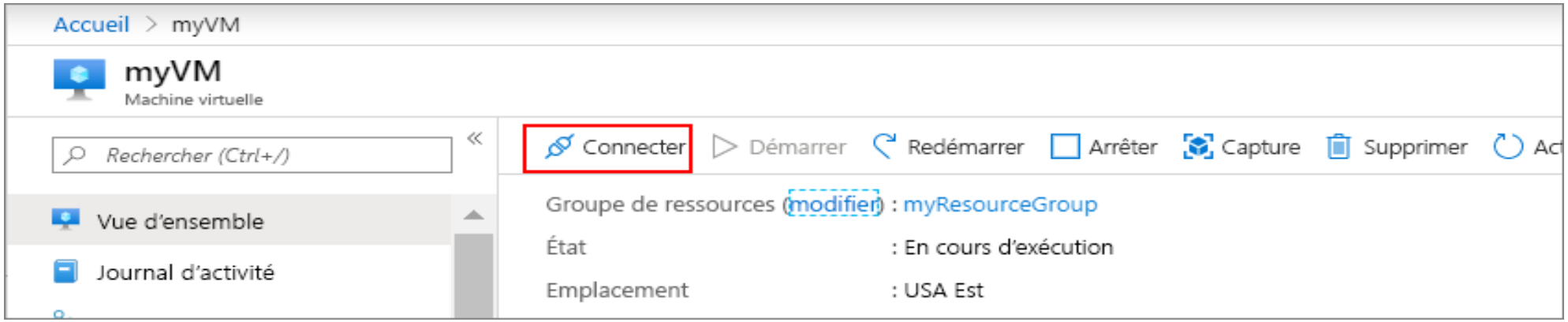
09. Une fois la validation exécutez, sélectionnez le bouton Créer en bas de la page.
10. Une fois le déploiement effectué, sélectionnez Accéder à la ressource.

PARTIE 1

Connexion à la machine virtuelle

Créez une connexion Bureau à distance à la machine virtuelle. Ces instructions expliquent comment se connecter à la machine virtuelle à partir d'un ordinateur Windows. Sur un Mac, vous avez besoin d'un client RDP similaire à ce Client Bureau à distance disponible sur le Mac App Store.

1. Sur la page Vue d'ensemble de votre machine virtuelle, sélectionnez le bouton Connecter puis sélectionner RDP.



1. Sur la page Se connecter avec RDP, conservez les options par défaut pour vous connecter par adresse IP sur le port 3389 et cliquez sur Télécharger le fichier RDP.
2. Ouvrez le fichier RDP téléchargé et, à l'invite, cliquez sur Se connecter.
3. Dans la fenêtre Sécurité Windows, sélectionnez Plus de choix, puis Utiliser un autre compte. Tapez le nom d'utilisateur sous la forme localhost\username, entrez le mot de passe créé pour la machine virtuelle, puis cliquez sur OK.
4. Un avertissement de certificat peut s'afficher pendant le processus de connexion. Cliquez sur Oui ou Continuer pour créer la connexion.

CHAPITRE 2

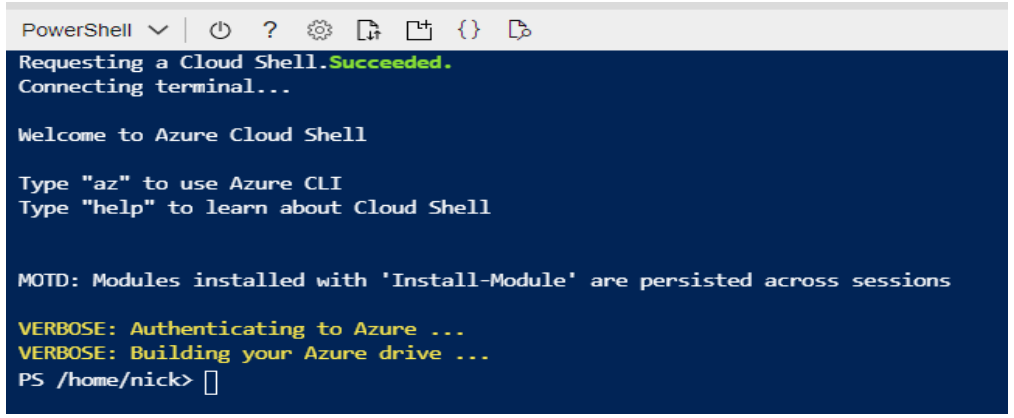
Créer une machine virtuelle

1. Provisionnement d’une VM via l’interface graphique
2. **Préparation d’un script de création d’une VM**

Préparation d'un script de création d'une VM

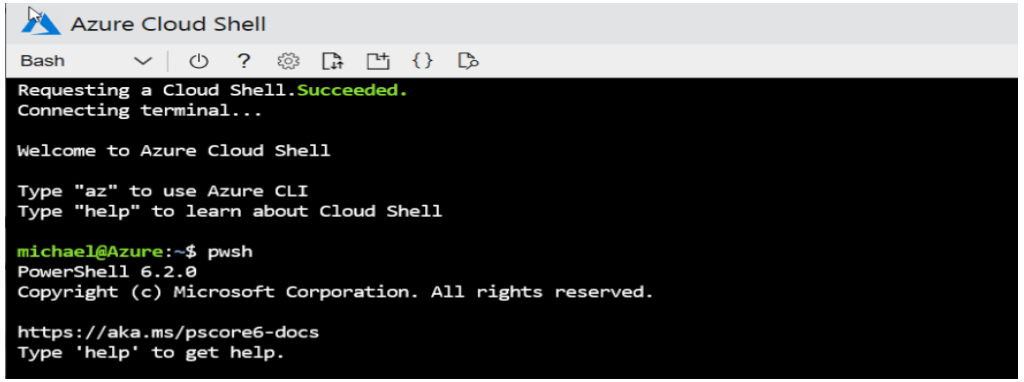
❖ Azure PowerShell

Azure PowerShell est un ensemble d'applets de commande permettant de gérer les ressources Azure directement à partir de PowerShell. Azure PowerShell est conçu pour faciliter l'apprentissage et la prise en main, mais fournit des fonctionnalités puissantes pour l'automatisation.



❖ Azure Cloud Shell

Azure Cloud Shell inclut un éditeur de fichier intégré, créé à partir de l'éditeur Monaco open source. L'éditeur Cloud Shell prend en charge des fonctionnalités telles que la mise en surbrillance du langage, la palette de commandes et un explorateur de fichiers.



PARTIE 1

Préparation d'un script de création d'une VM

Le module **Azure PowerShell** est utilisé pour créer et gérer des ressources Azure avec des lignes de commande ou des scripts PowerShell. Ce guide de démarrage rapide montre comment utiliser le module Azure PowerShell pour déployer une machine virtuelle (VM) exécutant Windows Server 2016 sur Azure. Nous effectuerons également une connexion RDP à la VM et installerons un serveur Web IIS pour démontrer la VM en action.

Azure Cloud Shell est un shell interactif gratuit que vous pouvez utiliser pour exécuter les étapes de cet article. Il dispose d'outils Azure communs préinstallés et configurés pour être utilisés avec votre compte.

Pour ouvrir Cloud Shell, sélectionnez simplement Essayer dans le coin supérieur droit d'un bloc de code. Vous pouvez également lancer Cloud Shell dans un onglet de navigateur distinct en accédant à https://shell.azure.com/powershell .

```
New-AzVm `
    -ResourceGroupName 'myResourceGroup' `
    -Name 'myVM' `
    -Location 'East US' `
    -VirtualNetworkName 'myVnet' `
    -SubnetName 'mySubnet' `
    -SecurityGroupName 'myNetworkSecurityGroup' `
    -PublicIpAddressName 'myPublicIpAddress' `
    -OpenPorts 80,3389
```

CHAPITRE 3

Configurer la disponibilité des VM

Ce que vous allez apprendre dans ce chapitre :

- Dimensionner automatiquement une VM
- Appréhender le choix des régions et des zones de disponibilité
- Assurer la haute disponibilité et l'équilibrage de charge d'une VM
- Sauvegarder et répliquer une VM

6 heures

CHAPITRE 3

Configurer la disponibilité des VM

1. **Mise à l'échelle automatiquement**
2. Choix des régions et des zones de disponibilité
3. Haute disponibilité et équilibrage de charge
4. Sauvegarde et Réplication

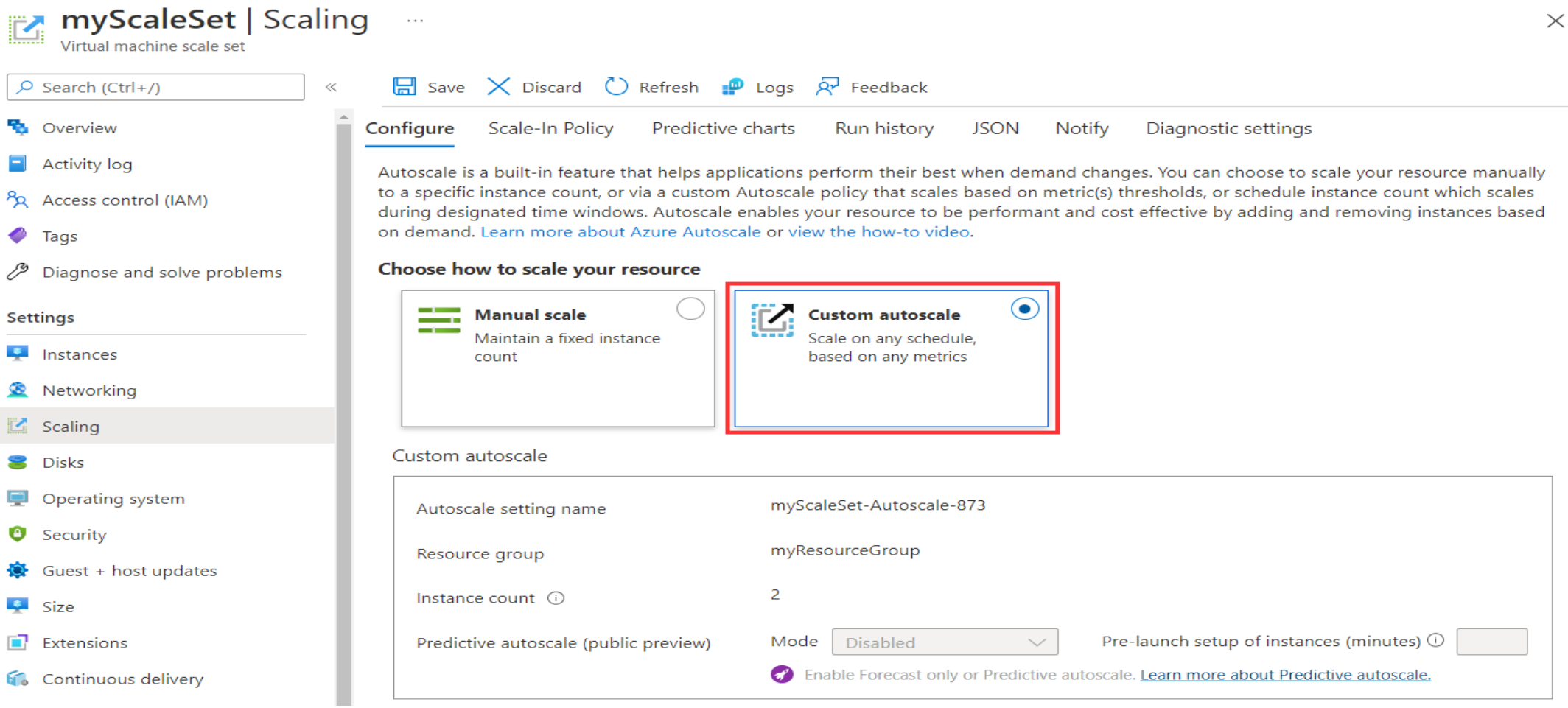
Configurer la disponibilité des VM

Si la demande de votre application augmente, la charge sur les instances de machine virtuelle dans votre groupe identique augmente. Si cette augmentation de la charge est cohérente, au lieu d'une brève demande, vous pouvez configurer des règles de mise à l'échelle automatique pour augmenter le nombre d'instances de machine virtuelle dans le groupe identique. Lorsque ces instances de machine virtuelle sont créées et que vos applications sont déployées, le groupe identique commence à distribuer le trafic vers les instances via l'équilibreur de charge. Vous contrôlez les métriques à surveiller, telles que l'usage du processeur ou du disque, la durée pendant laquelle la charge de l'application doit respecter un seuil donné, et le nombre d'instances de machine virtuelle à ajouter au groupe identique.

- Ouvrez le portail Azure et sélectionnez **Groupes de ressources** dans le menu à gauche du tableau de bord.
- Sélectionnez le groupe de ressources qui contient votre groupe identique, puis choisissez ce groupe dans la liste des ressources.
- Choisissez **Mise à l'échelle** dans le menu à gauche de la fenêtre des groupes identiques. Sélectionnez le bouton pour effectuer une **Mise à l'échelle automatique personnalisée** :

PARTIE 1

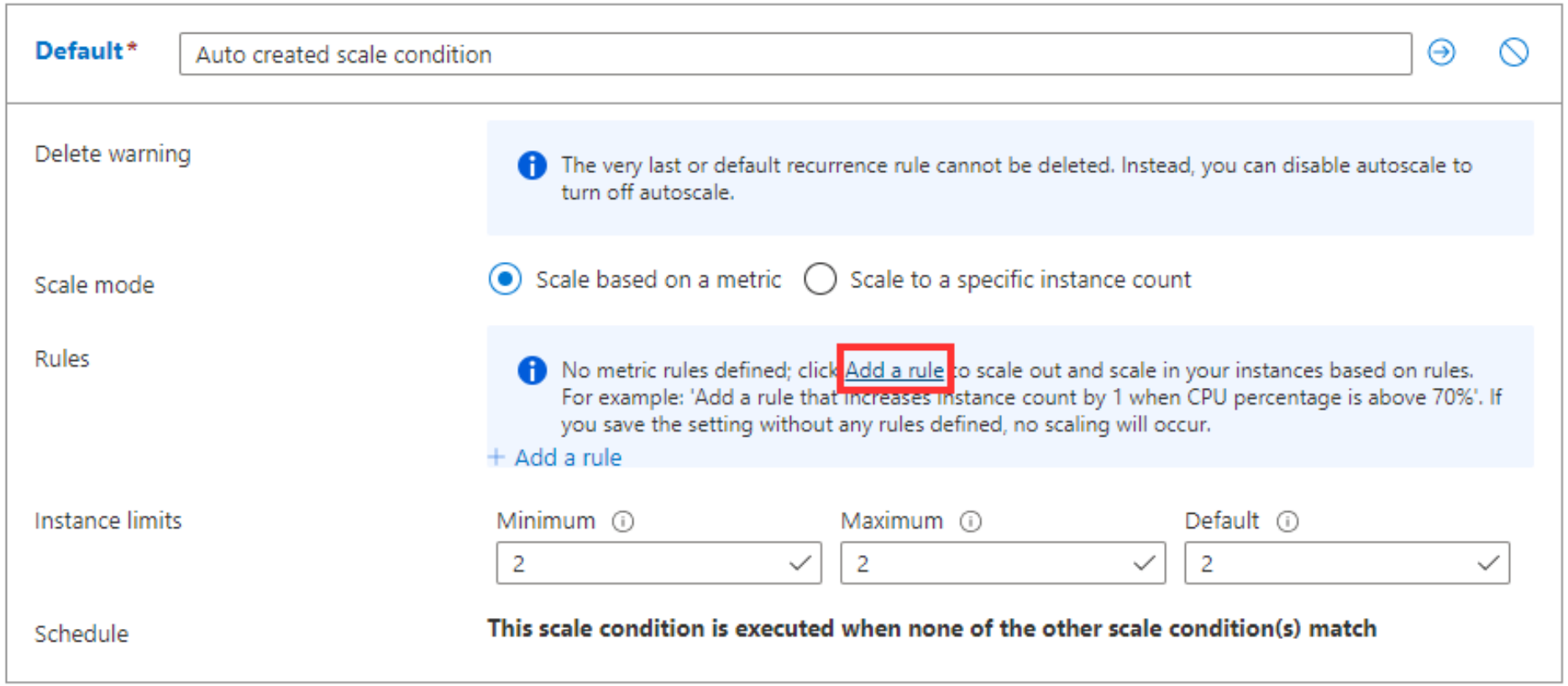
Configurer la disponibilité des VM



PARTIE 1

Configurer la disponibilité des VM

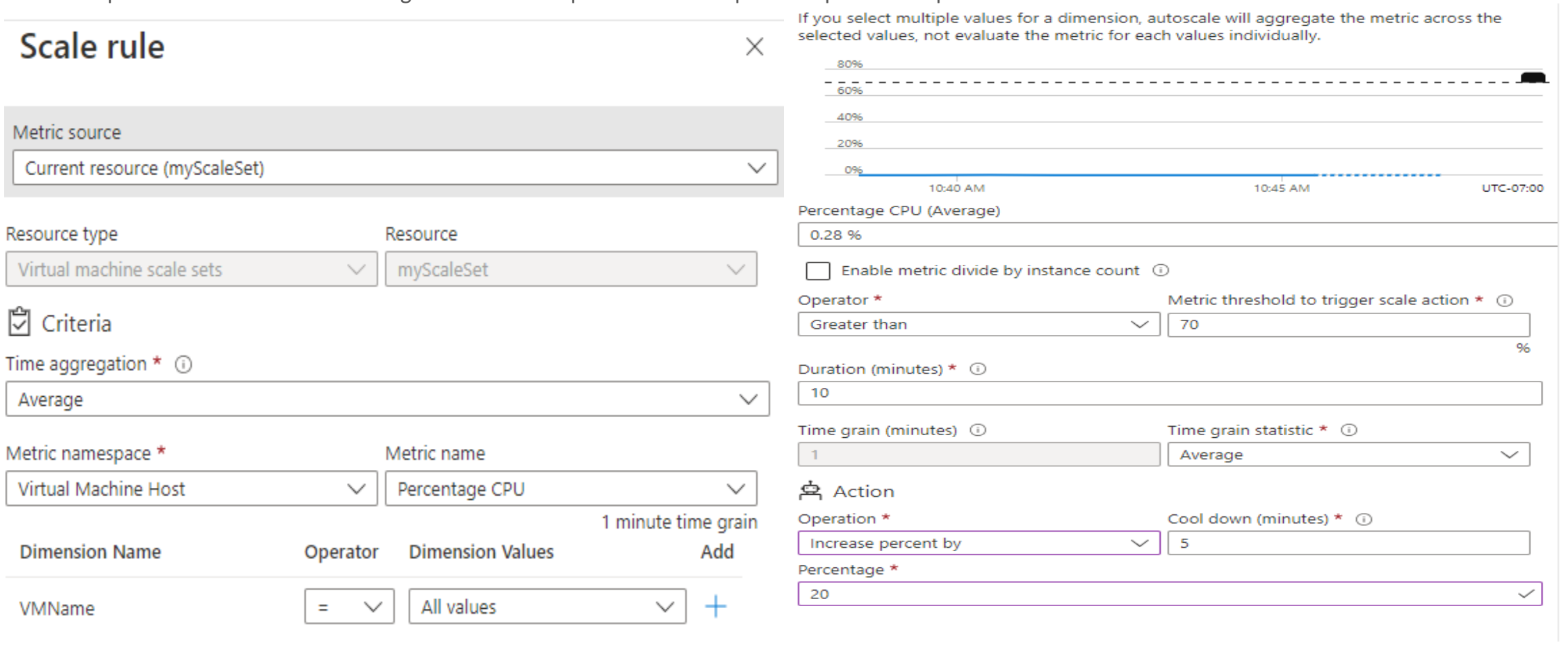
4. Sélectionnez l'option pour Ajouter une règle.



PARTIE 1

Configurer la disponibilité des VM

Les exemples suivants montrent une règle créée dans le portail Azure et qui correspond à ces paramètres :



CHAPITRE 3

Configurer la disponibilité des VM

1. Mise à l'échelle automatiquement
2. **Choix des régions et des zones de disponibilité**
3. Haute disponibilité et équilibrage de charge
4. Sauvegarde et Réplication

Trouver la zone géographique Azure qui répond à vos besoins

Obtenez toutes les informations dont vous avez besoin pour vous lancer sur Azure dans la zone géographique qui correspond le mieux à vos besoins, qu'il s'agisse de conformité ou de fonctionnalités de résilience. Sélectionnez une zone géographique Azure à l'aide du menu déroulant et comparez-la à d'autres zones géographiques.

Régions

Chaque région Azure comprend des centres de données déployés dans un périmètre défini par la latence. Ils sont connectés via un réseau régional dédié à faible latence. Cette conception garantit que les services Azure dans n'importe quelle région offrent les meilleures performances et sécurité possibles.

Zones de disponibilité

Les zones de disponibilité Azure sont des emplacements physiquement séparés au sein de chaque région Azure localement tolérante aux pannes. Les pannes vont des pannes logicielles et matérielles à des événements tels que des tremblements de terre, des inondations et des incendies. La tolérance aux pannes est obtenue grâce à la redondance et à l'isolation logique des services Azure. Pour garantir la résilience, toutes les régions avec des zones de disponibilité activées ont au moins trois zones de disponibilité distinctes.

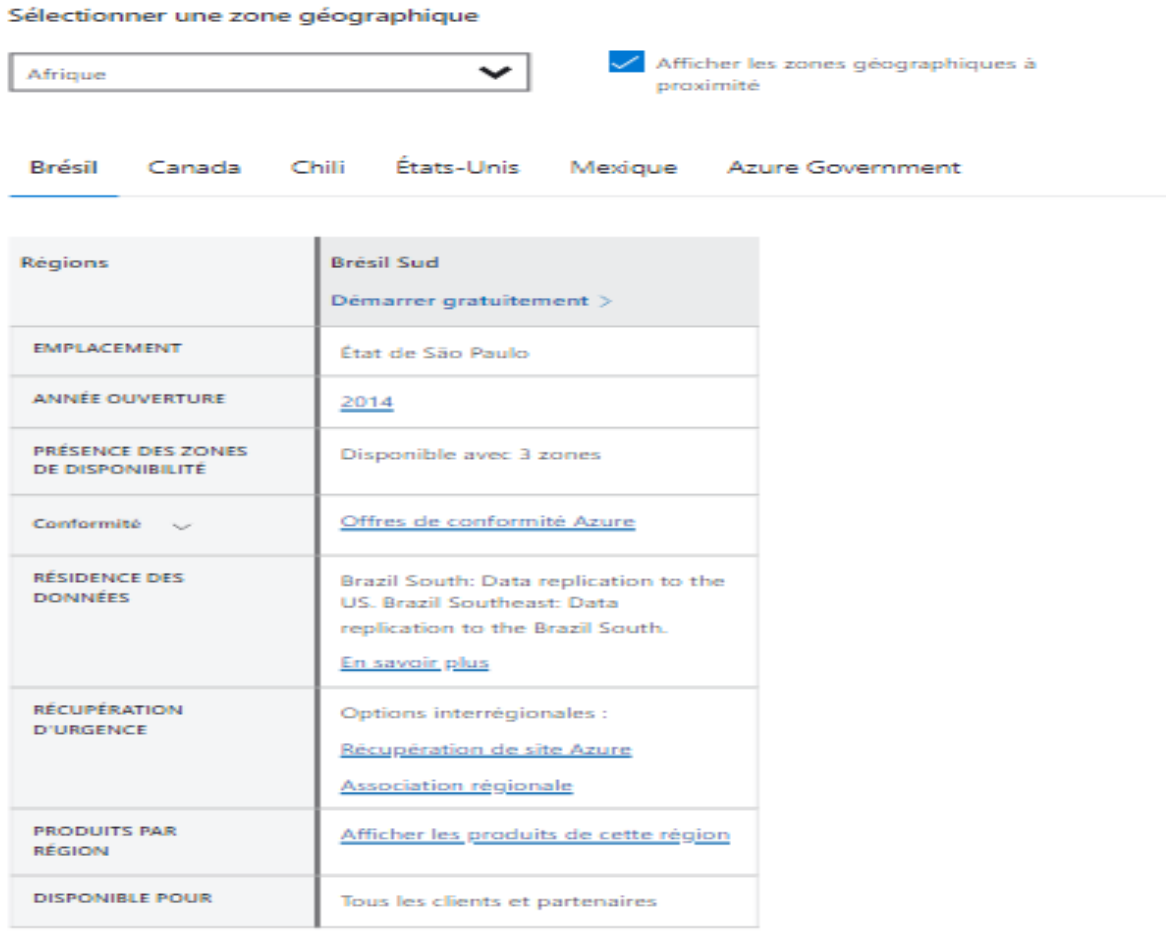
03- Configurer la disponibilité des VM
Choix des régions et des zones de disponibilité

Trouver la zone géographique Azure qui répond à vos besoins

Conformité et résidence des données
Obtenez de l'aide pour choisir la géographie adaptée à vos besoins en matière de résidence et de conformité.

Disponibilité du service
Vérifiez que les services Azure dont vous avez besoin sont disponibles dans la région du centre de données que vous envisagez.

Tarification
Tenez compte du coût dans votre processus de décision.



PARTIE 1

CHAPITRE 3

Configurer la disponibilité des VM

1. Mise à l'échelle automatiquement
2. Choix des régions et des zones de disponibilité
3. **Haute disponibilité et équilibrage de charge**
4. Sauvegarde et Réplication

Créer un groupe à haute disponibilité

Rappel

La haute disponibilité est une fonctionnalité qui permet le fonctionnement des ressources Cloud pendant de longues périodes sans aucune interruption

En utilisant Azure CLI ou PowerShell, exécuter les commandes suivantes :

1- Créez un groupe de ressources.

Azure PowerShell | Copier | Essayer

```
New-AzResourceGroup `
   -Name myResourceGroupAvailability `
   -Location EastUS
```

PARTIE 1

Créer un groupe à haute disponibilité

2- Créez un groupe à haute disponibilité

Azure PowerShell | Copier | Essayer

```
New-AzAvailabilitySet `
   -Location "EastUS" `
   -Name "myAvailabilitySet" `
   -ResourceGroupName "myResourceGroupAvailability" `
   -Sku aligned `
   -PlatformFaultDomainCount 2 `
   -PlatformUpdateDomainCount 2
```

Créer un groupe à haute disponibilité

3- Créer des machines virtuelles dans un groupe à haute disponibilité

Vous devez créer des machines virtuelles au sein du groupe à haute disponibilité pour vous assurer qu'elles sont correctement réparties dans le matériel. Vous ne pouvez pas ajouter une machine virtuelle existante à un groupe à haute disponibilité après sa création.

Quand vous créez une machine virtuelle à l'aide de New-AzVM, vous utilisez le paramètre -AvailabilitySetName pour spécifier le nom du groupe à haute disponibilité.

Tout d'abord, définissez un nom d'utilisateur administrateur et un mot de passe pour la machine virtuelle avec Get-Credential :

Azure PowerShell Copier Essayer

```
$cred = Get-Credential
```

PARTIE 1

Créer un groupe à haute disponibilité

4- Créez maintenant deux machines virtuelles avec New-AzVM dans le groupe à haute disponibilité.

Azure PowerShell | Copier | Essayer

```
for ($i=1; $i -le 2; $i++)
{
    New-AzVm `
        -ResourceGroupName "myResourceGroupAvailability" `
        -Name "myVM$i" `
        -Location "East US" `
        -VirtualNetworkName "myVnet" `
        -SubnetName "mySubnet" `
        -SecurityGroupName "myNetworkSecurityGroup" `
        -PublicIpAddressName "myPublicIpAddress$i" `
        -AvailabilitySetName "myAvailabilitySet" `
        -Credential $cred
}
```

Créer un groupe à haute disponibilité

5- Vérifier les tailles de machines virtuelles disponibles

Lorsque vous créez une machine virtuelle à l'intérieur d'un groupe à haute disponibilité, vous devez connaître les tailles de machine virtuelle qui sont disponibles sur le matériel. Utilisez la commande Get-AzVMSize afin d'obtenir toutes les tailles disponibles pour les machines virtuelles que vous pouvez déployer dans le groupe à haute disponibilité.

Azure PowerShell Copier Essayer

```
Get-AzVMSize `
   -ResourceGroupName "myResourceGroupAvailability" `
   -AvailabilitySetName "myAvailabilitySet"
```

PARTIE 1

Équilibrage de charge des VM

L'équilibrage de charge offre un niveau plus élevé de disponibilité en répartissant les demandes entrantes sur plusieurs machines virtuelles. Dans ce didacticiel, vous allez découvrir les différents composants de l'équilibreur de charge Azure qui répartissent le trafic et fournissent une haute disponibilité.

Un équilibreur de charge Azure est un équilibreur de charge de type Couche 4 (TCP, UDP) qui offre une haute disponibilité en répartissant le trafic entrant entre les machines virtuelles saines. Une sonde d'intégrité d'équilibreur de charge surveille un port donné sur chaque machine virtuelle et ne distribue le trafic que vers une machine virtuelle opérationnelle.

Vous définissez une configuration IP frontale qui contient une ou plusieurs adresses IP publiques. Cette configuration IP frontale permet d'accéder à votre équilibreur de charge et à vos applications via Internet.

Dans ce qui suit, on va aborder les actions suivantes :

1. Créer un équilibrage de charge Azure
2. Créer une sonde d'intégrité d'équilibreur de charge
3. Créer des règles de trafic pour l'équilibrage de charge
4. Utiliser l'extension de script personnalisé pour créer un site de base IIS
5. Créer des machines virtuelles et les attacher à un équilibrage de charge
6. Afficher un équilibrage de charge en action
7. Ajouter et supprimer des machines virtuelles d'un équilibreur de charge

1- Créer un groupe de ressources

Pour pouvoir créer votre équilibreur de charge, vous devez créer un groupe de ressources avec la commande az group create. L'exemple suivant crée un groupe de ressources nommé myResourceGroupLoadBalancer dans l'emplacement westus :

Azure CLI Copier Essayer

```
az group create --name myResourceGroupLoadBalancer --location eastus
```

2- Créer une adresse IP publique

Pour accéder à votre application sur Internet, vous avez besoin d'une adresse IP publique pour l'équilibreur de charge.

Créez une adresse IP publique avec la commande az network public-ip create. L'exemple suivant crée une adresse IP publique nommée myPublicIP dans le groupe de ressources myResourceGroupLoadBalancer :

Azure CLI | Copier | Essayer

```
az network public-ip create \
    --resource-group myResourceGroupLoadBalancer \
    --name myPublicIP
```

3- Créer un équilibrage de charge

L'exemple suivant crée un équilibreur de charge nommé myLoadBalancer et affecte l'adresse myPublicIP à la configuration IP frontale :

Azure CLI | Copier | Essayer

```
az network lb create \
    --resource-group myResourceGroupLoadBalancer \
    --name myLoadBalancer \
    --frontend-ip-name myFrontEndPool \
    --backend-pool-name myBackEndPool \
    --public-ip-address myPublicIP
```

4- Créer une sonde d'intégrité

Pour permettre à l'équilibrage de charge de surveiller l'état de votre application, vous utilisez une sonde d'intégrité. La sonde d'intégrité ajoute ou supprime dynamiquement des machines virtuelles de la rotation d'équilibrage de charge en fonction de leur réponse aux vérifications d'intégrité. Par défaut, une machine virtuelle est supprimée de la distribution d'équilibrage de charge après deux échecs consécutifs à des intervalles de 15 secondes. Vous créez une sonde d'intégrité selon un protocole ou une page de vérification d'intégrité spécifique pour votre application.

L'exemple suivant permet de créer une sonde TCP. Vous pouvez également créer des sondes HTTP personnalisées pour des contrôles d'intégrité plus affinés. Lorsque vous utilisez une sonde HTTP personnalisée, vous devez créer la page de contrôle d'intégrité, par exemple healthcheck.js. La sonde doit retourner une réponse HTTP 200 OK pour l'équilibreur de charge pour assurer la rotation de l'hôte.

Pour créer une sonde d'intégrité TCP, utilisez la commande az network lb probe create. L'exemple suivant permet de créer une sonde d'intégrité nommée myHealthProbe :

Azure CLI | Copier | Essayer

```
az network lb probe create \
    --resource-group myResourceGroupLoadBalancer \
    --lb-name myLoadBalancer \
    --name myHealthProbe \
    --protocol tcp \
    --port 80
```

PARTIE 1

5- Créer une règle d'équilibreur de charge

Une règle d'équilibrage de charge est utilisée pour définir la distribution du trafic vers les machines virtuelles. Vous définissez la configuration IP frontale pour le trafic entrant et le pool d'adresses IP principal pour recevoir le trafic, ainsi que le port source et le port de destination requis. Pour veiller à ce que seules les machines virtuelles saines reçoivent le trafic, vous devez également définir la sonde d'intégrité à utiliser.

Utilisez az network lb rule create pour créer une règle d'équilibrage de charge. L'exemple suivant crée une règle nommée myLoadBalancerRule, utilise la sonde d'intégrité myHealthProbe et équilibre le trafic sur le port 80 :

Azure CLI | Copier | Essayer

```
az network lb rule create \
    --resource-group myResourceGroupLoadBalancer \
    --lb-name myLoadBalancer \
    --name myLoadBalancerRule \
    --protocol tcp \
    --frontend-port 80 \
    --backend-port 80 \
    --frontend-ip-name myFrontEndPool \
    --backend-pool-name myBackEndPool \
    --probe-name myHealthProbe
```

CHAPITRE 3

Configurer la disponibilité des VM

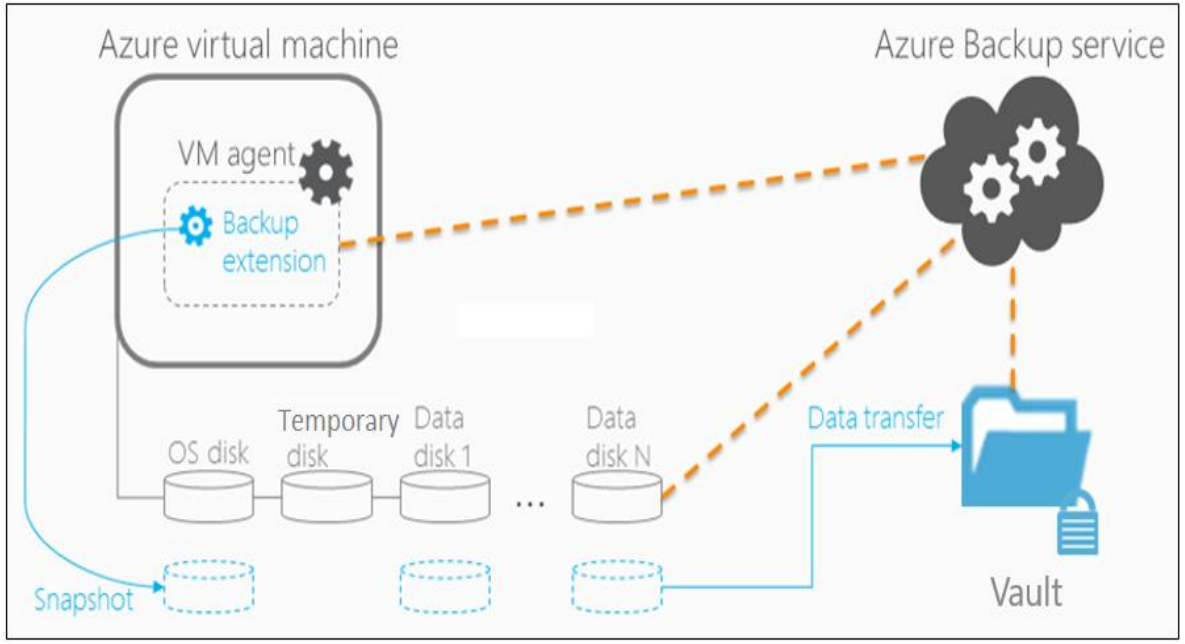
1. Mise à l'échelle automatiquement
2. Choix des régions et des zones de disponibilité
3. Haute disponibilité et équilibrage de charge
4. **Sauvegarde et Réplication**

Sauvegarder une machine virtuelle dans Azure

Azure fournit une solution de sauvegarde et de reprise après sinistre simple, sécurisée, évolutive et économique de bout en bout intégrée à des solutions de protection des données sur site. En cas d'interruption de service, de suppression accidentelle ou de corruption de données, restaurez les services professionnels de manière opportune et coordonnée. L'architecture native d'Azure, la haute disponibilité, les solutions de sauvegarde résilientes et de reprise après sinistre sont faciles à concevoir.

Sur Azure, vous pouvez protéger vos données en effectuant des sauvegardes à intervalles réguliers. La sauvegarde Azure crée des points de récupération pouvant être stockés dans des coffres de récupération géo-redondants.

Dans ce qui suit, on verra comment sauvegarder une machine virtuelle (VM) avec le portail Azure.



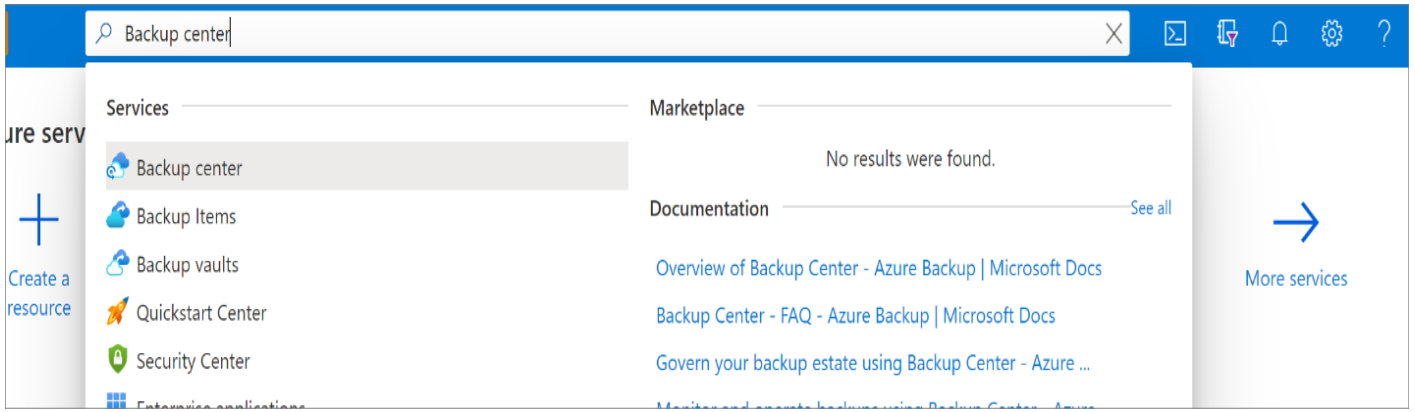
PARTIE 1

01- Créer un Coffre Recovery Services

Un Coffre Recovery Services est un conteneur logique qui stocke les données de sauvegarde de chaque ressource protégée, telles que des machines virtuelles Azure. Lorsque le travail de sauvegarde d'une ressource protégée s'exécute, il crée un point de récupération à l'intérieur du Coffre Recovery Services. Vous pouvez ensuite utiliser un de ces points de récupération pour restaurer des données à un moment donné dans le temps.

Pour créer un archivage de Recovery Services :

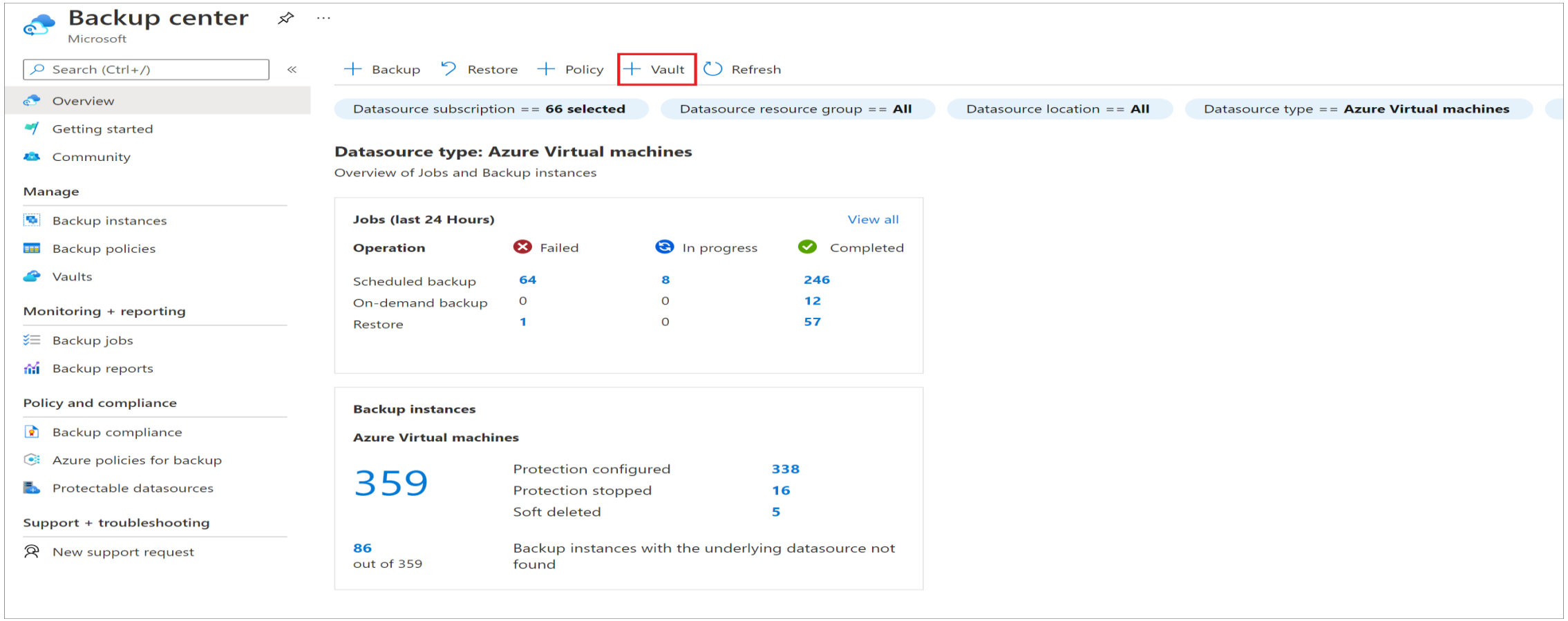
1. Connectez-vous à votre abonnement sur le portail Azure.
2. Recherchez Centre de sauvegarde dans le portail Azure, puis accédez au tableau de bord Centre de sauvegarde.



PARTIE 1

01- Créer un Coffre Recovery Services

3. Sélectionnez **+Coffre** sous l'onglet **Vue d'ensemble**.



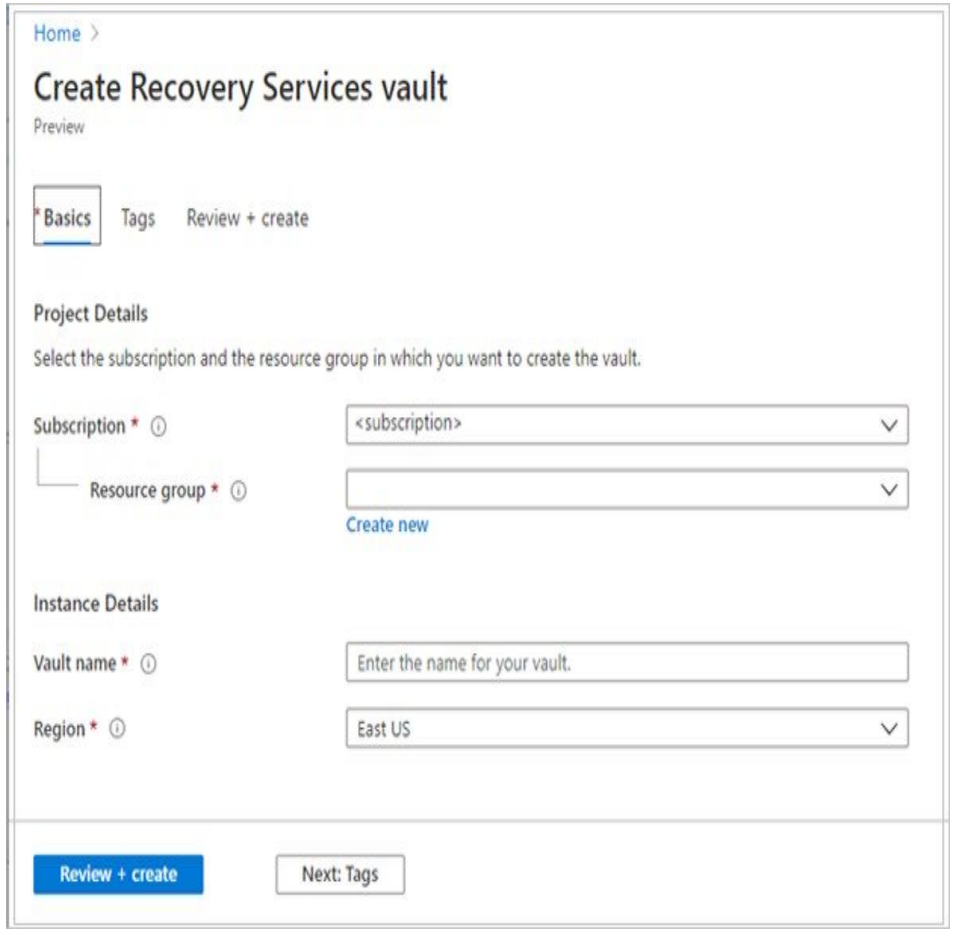
PARTIE 1

01- Créer un Coffre Recovery Services

4. Sélectionnez **Coffre Recovery Services**>**Continuer**.

5. La boîte de dialogue Coffre Recovery Services s'ouvre. Renseignez les valeurs suivantes :

   - **Abonnement** : Choisissez l'abonnement à utiliser. Si vous êtes membre d'un seul abonnement, son nom s'affiche. Si vous ne savez pas quel abonnement utiliser, utilisez l'abonnement par défaut (suggéré). Vous ne disposez de plusieurs choix que si votre compte professionnel ou scolaire est associé à plusieurs abonnements Azure.
   - **Groupe de ressources** : Utilisez un groupe de ressources existant ou créez-en un. Pour voir la liste des groupes de ressources disponibles dans votre abonnement, sélectionnez Utiliser existant, puis sélectionnez une ressource dans la liste déroulante. Pour créer un groupe de ressources, sélectionnez Créer et entrez le nom. Pour plus d'informations sur les groupes de ressources, consultez Vue d'ensemble d'Azure Resource Manager.
   - **Nom du coffre** : Entrez un nom convivial pour identifier le coffre. Le nom doit être unique pour l'abonnement Azure. Spécifiez un nom composé d'au moins deux caractères, mais sans dépasser 50 caractères. Il doit commencer par une lettre et ne peut être constitué que de lettres, chiffres et traits d'union.
   - **Région** : Sélectionnez la région géographique du coffre. Pour que vous puissiez créer un coffre pour aider à protéger une source de données, le coffre doit se trouver dans la même région que la source de données.



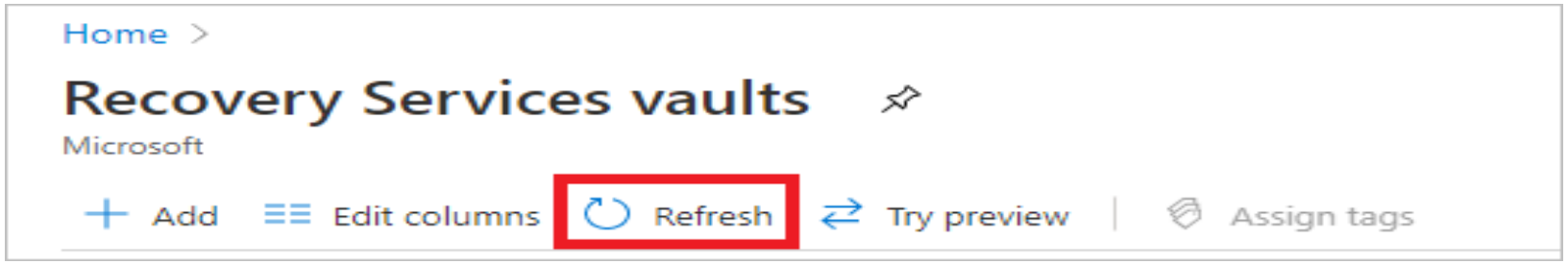
01- Créer un Coffre Recovery Services

6. Après avoir fourni les valeurs, sélectionnez Vérifier + créer.

7. Quand vous êtes prêt à créer le Coffre Recovery Services, sélectionnez **Créer**.

01- Créer un Coffre Recovery Services

8. La création du Coffre Recovery Services peut prendre un certain temps. Surveillez les notifications d'état dans la zone **Notifications** dans l'angle supérieur droit du portail. Une fois que le coffre est créé, il apparaît dans la liste des coffres Recovery Services. Si vous ne voyez pas votre coffre, sélectionnez **Actualiser**.

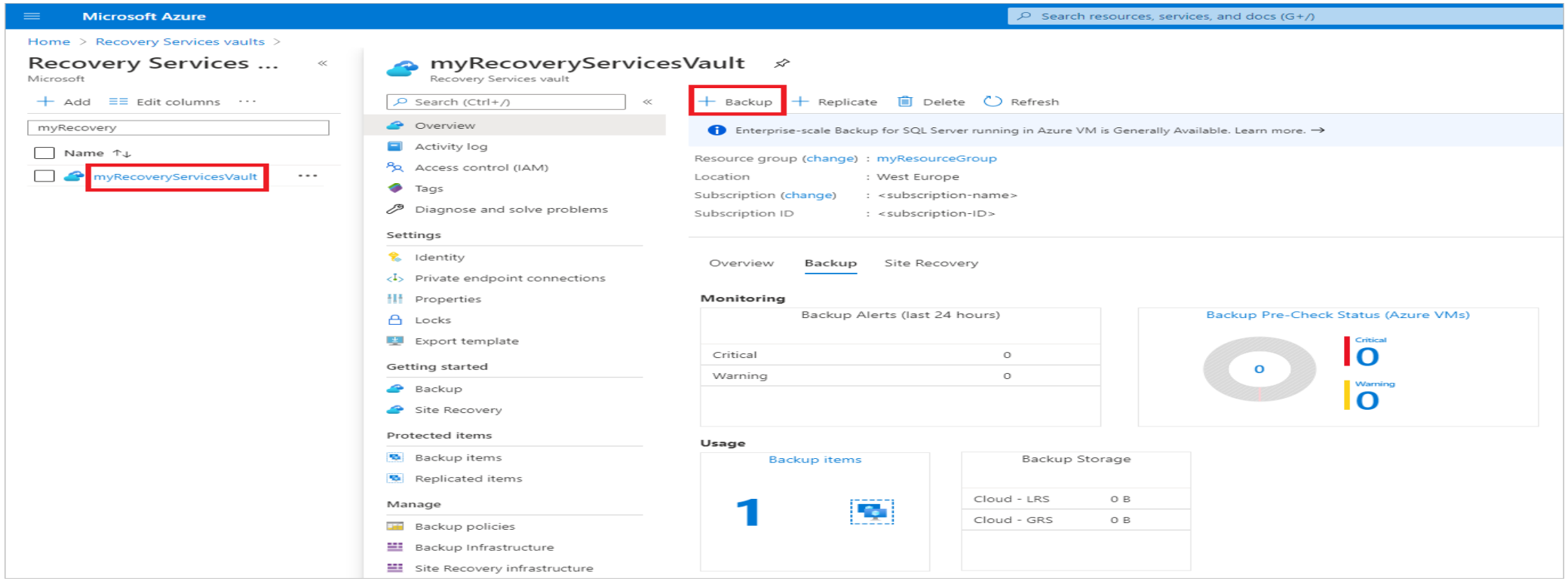


PARTIE 1

02- Appliquer une stratégie de sauvegarde

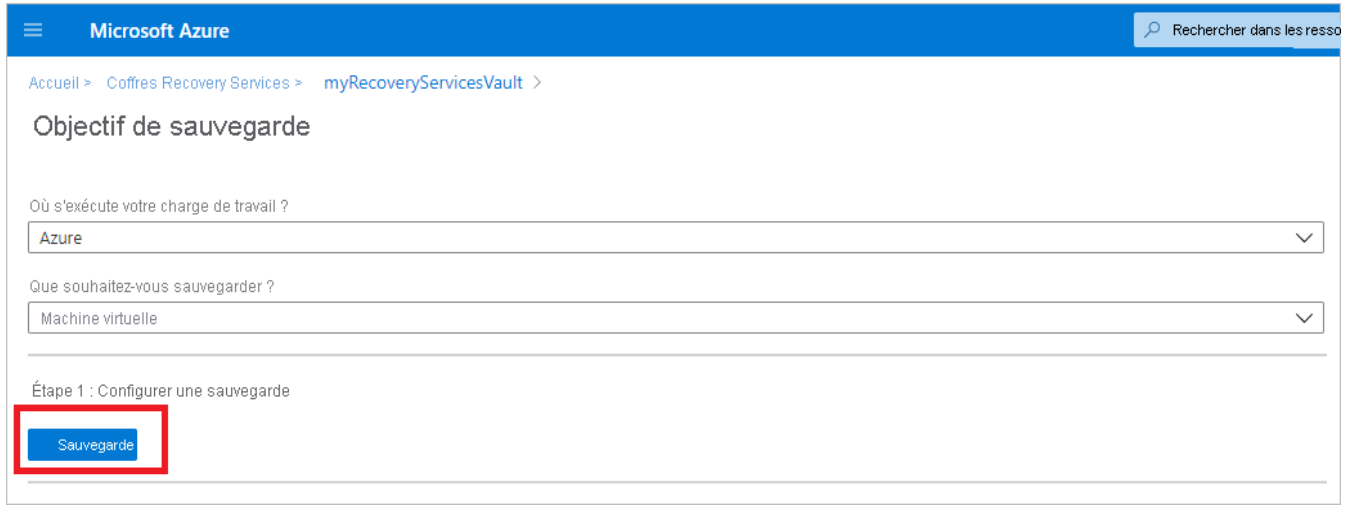
Pour appliquer une stratégie de sauvegarde à vos machines virtuelles Azure, procédez comme suit :

1. Accédez à Centre de sauvegarde puis, sous l'onglet Vue d'ensemble, cliquez sur +Sauvegarde.



02- Appliquer une stratégie de sauvegarde

2. Sélectionnez Machines virtuelles Azure comme Type de source de données, puis sélectionnez le coffre que vous avez créé. Puis, cliquez sur Continuer.



02- Appliquer une stratégie de sauvegarde

3. Assigner une stratégie de sauvegarde.

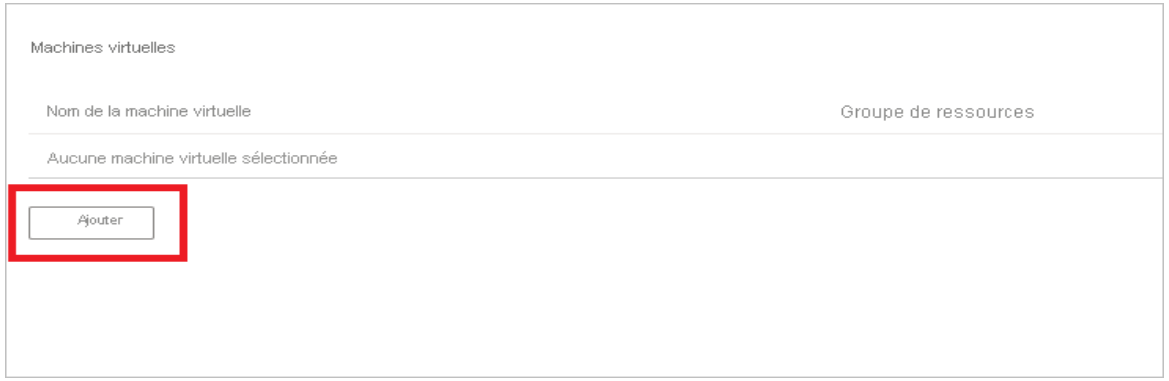
- La stratégie par défaut sauvegarde la machine virtuelle une fois par jour. Les sauvegardes quotidiennes sont conservées pendant 30 jours. Les instantanés de récupération instantanée sont conservés pendant deux jours.
- Si vous ne souhaitez pas utiliser la stratégie par défaut, sélectionnez **Créer** et créez une stratégie personnalisée.

PARTIE 1

03- Sélectionner une machine virtuelle à sauvegarder

Créez une simple sauvegarde quotidienne planifiée dans un Coffre Recovery Services.

1. Sous Machines virtuelles, sélectionnez Ajouter.



03- Sélectionner une machine virtuelle à sauvegarder

2. Le volet Sélectionner les machines virtuelles s'ouvre. Sélectionnez les machines virtuelles que vous souhaitez sauvegarder à l'aide de la stratégie. Sélectionnez ensuite OK.
    - Les machines virtuelles sélectionnées sont validées.
    - Vous pouvez uniquement sélectionner les machines virtuelles situées dans la même région que le coffre.
    - Vous pouvez sauvegarder des machines virtuelles uniquement dans un même coffre.

04- Activer la sauvegarde sur une machine virtuelle

Pour activer la sauvegarde de la machine virtuelle, dans Sauvegarde, sélectionnez Activer la sauvegarde. Cette action permet de déployer la stratégie dans le coffre et sur les machines virtuelles, puis d'installer l'extension de sauvegarde sur l'agent de machine virtuelle en cours d'exécution sur la machine virtuelle Azure.

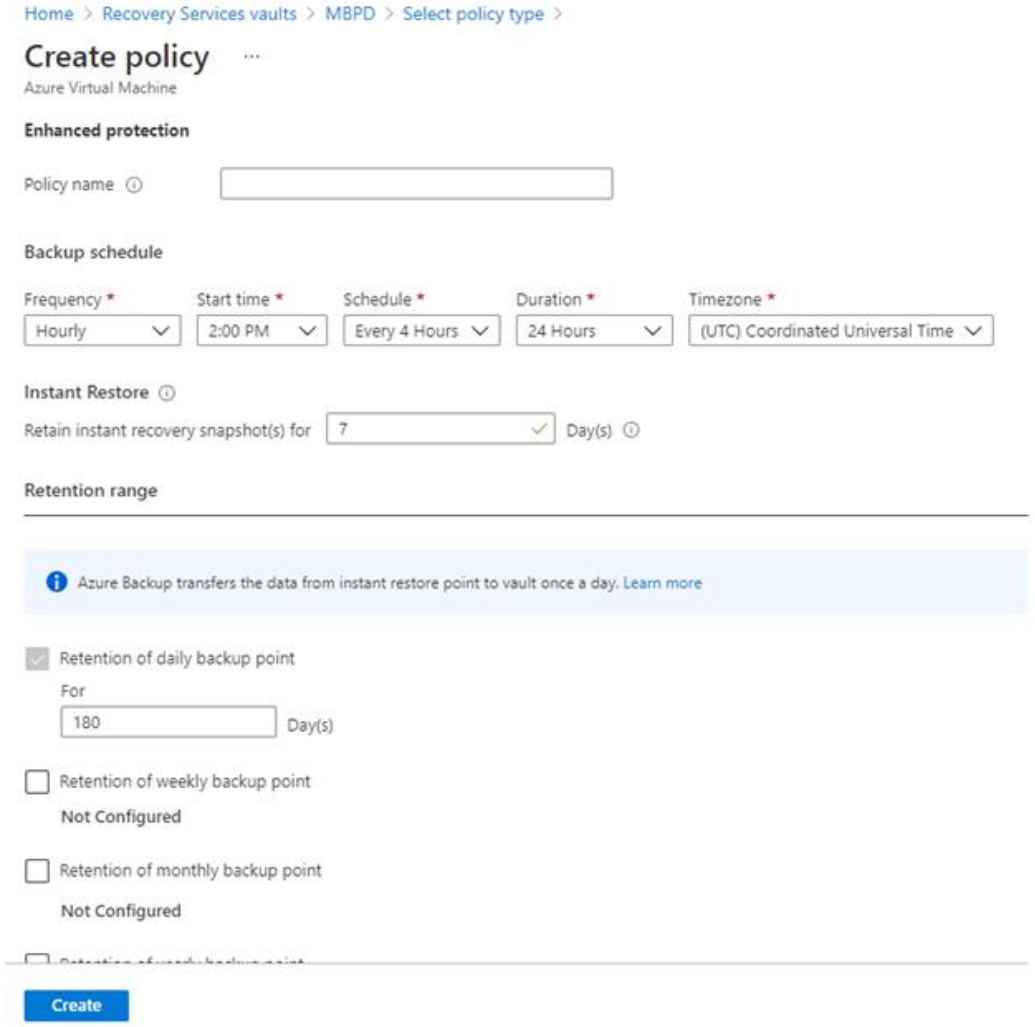
Après avoir activé la sauvegarde :

- Il installe l'extension de sauvegarde, que la machine virtuelle soit ou non en cours d'exécution.
- Une sauvegarde initiale s'exécute conformément à votre planification de sauvegarde.
- Lors de l'exécution des sauvegardes, notez que :
  - Une machine virtuelle en cours d'exécution a le plus de chances de capturer un point de récupération cohérent au niveau applicatif.
  - Cependant, même si la machine virtuelle est désactivée, elle est sauvegardée. Une machine virtuelle de ce type est appelée machine virtuelle en mode hors connexion. Dans ce cas, le point de récupération est cohérent en cas de plantage.
- Aucune connectivité sortante explicite n'est nécessaire pour permettre la sauvegarde de machines virtuelles Azure.

05- Créer une stratégie personnalisée

Si vous avez choisi de créer une stratégie de sauvegarde, renseignez les paramètres de stratégie.

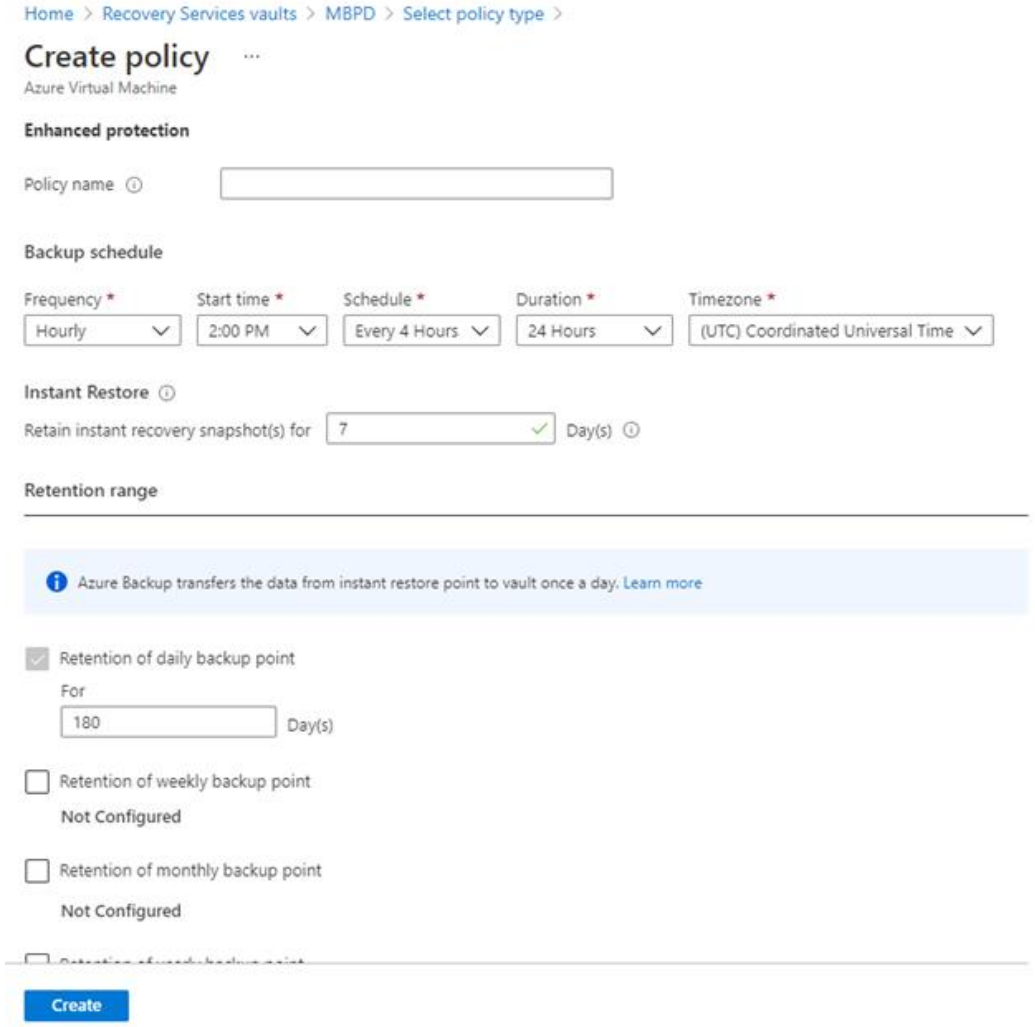
1. Dans Nom de la stratégie, spécifiez un nom explicite.
2. Dans Planification de sauvegarde, spécifiez quand les sauvegardes doivent être effectuées. Vous pouvez effectuer des sauvegardes quotidiennes ou hebdomadaires pour les machines virtuelles Azure.
3. Dans Restauration instantanée, spécifiez la durée pendant laquelle vous souhaitez conserver les instantanés localement en vue d'une restauration instantanée.
    - Quand vous effectuez une restauration, les disques de la machine virtuelle sauvegardée sont copiés depuis le stockage vers l'emplacement de stockage de récupération, via le réseau. Avec la restauration instantanée, vous pouvez tirer parti des instantanés stockés localement pendant un travail de sauvegarde, sans attendre que les données de sauvegarde soient transférées vers le coffre.
    - Vous pouvez conserver les instantanés en vue de la restauration instantanée entre un à cinq jours. La valeur par défaut est de 2 jours.



PARTIE 1

05- Créer une stratégie personnalisée

4. Dans Durée de rétention, spécifiez la durée pendant laquelle vous souhaitez conserver vos points de sauvegarde quotidiens ou hebdomadaires.
5. Dans Rétention du point de sauvegarde mensuel et Rétention du point de sauvegarde annuel, indiquez si vous souhaitez conserver une sauvegarde mensuelle ou annuelle de vos sauvegardes quotidiennes ou hebdomadaires.
6. Sélectionnez OK pour enregistrer la stratégie.
7. Dans Durée de rétention, spécifiez la durée pendant laquelle vous souhaitez conserver vos points de sauvegarde quotidiens ou hebdomadaires.
8. Dans Rétention du point de sauvegarde mensuel et Rétention du point de sauvegarde annuel, indiquez si vous souhaitez conserver une sauvegarde mensuelle ou annuelle de vos sauvegardes quotidiennes ou hebdomadaires.
9. Sélectionnez OK pour enregistrer la stratégie.



PARTIE 1

06- Démarrer un travail de sauvegarde

La sauvegarde initiale s'exécutera conformément à la planification, mais vous pouvez l'exécuter immédiatement comme suit :

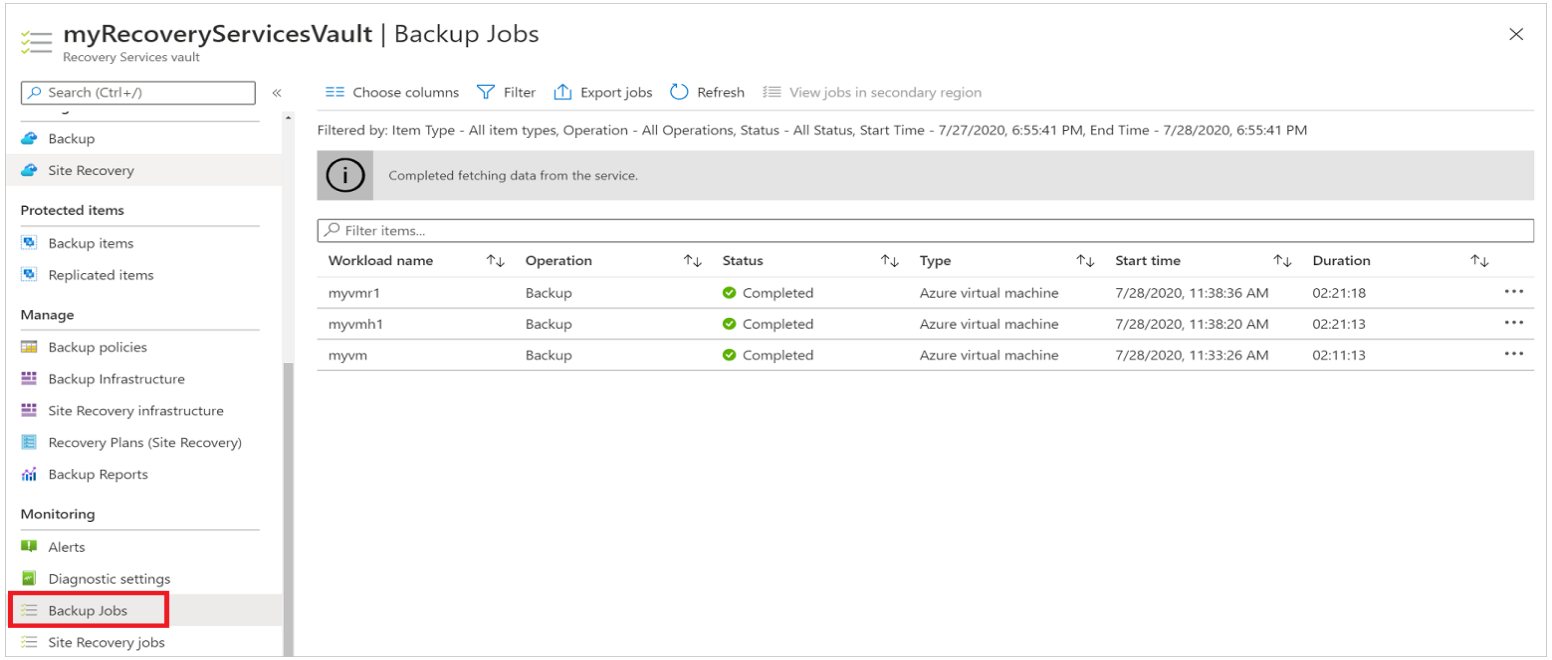
1. Accédez au Centre de sauvegarde, puis sélectionnez l'option de menu Instances de sauvegarde.
2. Sélectionnez Machines virtuelles Azure comme Type de source de données. Recherchez ensuite la machine virtuelle que vous avez configurée pour la sauvegarde.
3. Cliquez avec le bouton droit sur la ligne appropriée ou sélectionnez l'icône plus (...), puis cliquez sur Sauvegarder maintenant.
4. Dans Sauvegarder maintenant, utilisez le contrôle de calendrier pour sélectionner le dernier jour de rétention du point de récupération. Sélectionnez ensuite OK.
5. Surveiller les notifications du portail. Pour surveiller la progression du travail, accédez au Centre de sauvegarde>Travaux de sauvegarde, puis filtrez la liste des travaux en cours. Selon la taille de votre machine virtuelle, la création de la sauvegarde initiale peut prendre un certain temps.

PARTIE 1

07- Surveiller le travail de sauvegarde

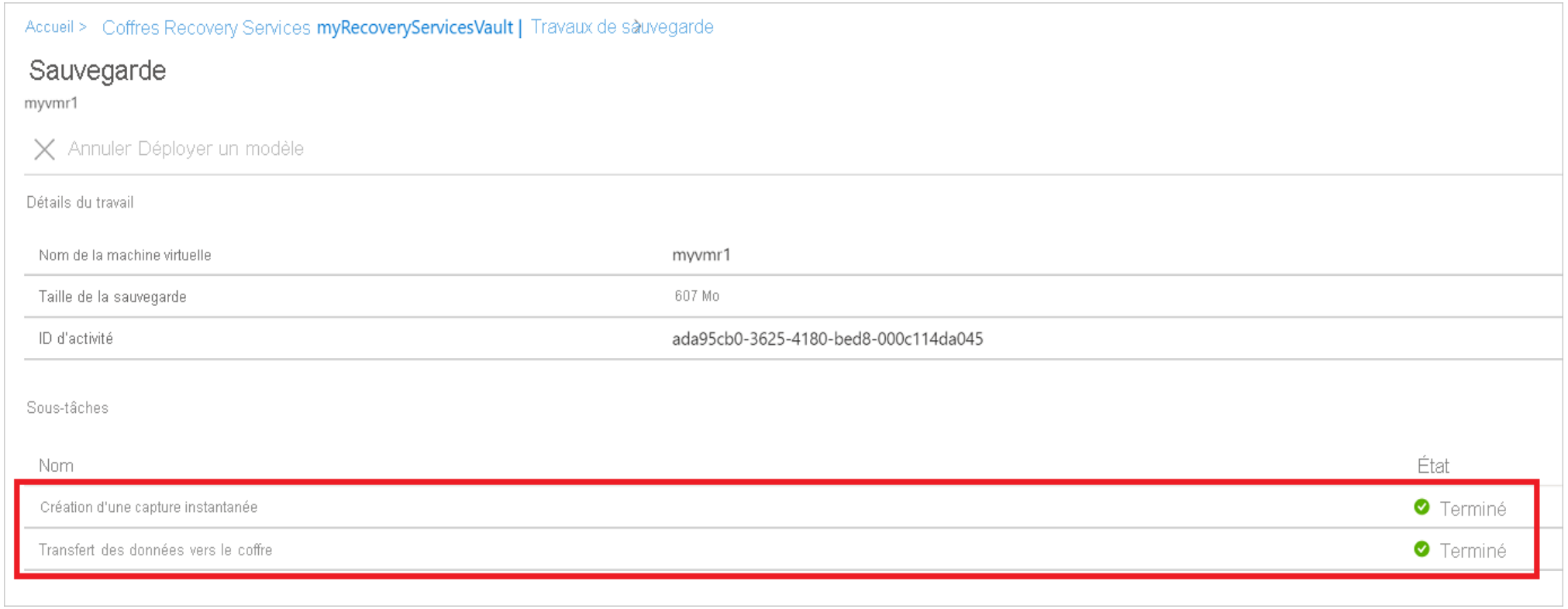
Les détails du travail de sauvegarde pour chaque sauvegarde de machine virtuelle se composent de deux phases : la phase Capture instantanée, suivie de la phase Transférer les données vers le coffre.

La phase de capture instantanée garantit la disponibilité d'un point de récupération stocké avec les disques pour les restaurations instantanées, et les captures instantanées sont disponibles pendant au maximum cinq jours en fonction de la conservation des captures instantanées configurée par l'utilisateur. Le transfert des données vers le coffre crée un point de récupération dans le coffre pour la conservation à long terme. Le transfert des données vers le coffre ne démarre qu'une fois la phase de prise d'instantané terminée.



07- Surveiller le travail de sauvegarde

Il existe deux sous-tâches en cours d'exécution sur le back-end, dont une pour le travail de sauvegarde front-end que vous pouvez consulter à partir du volet de résultats du travail de sauvegarde, comme indiqué ci-dessous :



PARTIE 1

07- Surveiller le travail de sauvegarde

La phase Transférer les données vers le coffre peut prendre plusieurs jours selon la taille des disques, l'activité par disque et plusieurs autres facteurs.

L'état du travail peut varier selon les scénarios suivants :

Désormais, avec cette fonctionnalité, pour la même machine virtuelle, deux sauvegardes peuvent s'exécuter en parallèle, mais dans chaque phase (prise d'instantané, transfert des données vers le coffre), une seule sous-tâche peut être en cours d'exécution.

Ainsi, les scénarios où un travail de sauvegarde en cours entraîne l'échec de la sauvegarde du jour suivant sont évités grâce à cette fonctionnalité de découplage. Les sauvegardes des jours suivants peuvent voir la réalisation de la phase de prise d'instantané, mais pas celle de la phase Transférer les données vers le coffre, si le travail de sauvegarde d'un jour précédent est dans l'état en cours. Le point de récupération incrémentielle créé dans le coffre capture toute l'évolution à partir du point de récupération de plus récent créé dans le coffre. Il n'y a aucun impact sur l'utilisateur en ce qui concerne les coûts.

Instantané	Transférer les données vers le coffre	État du travail
Complété	En cours	En cours
Complété	Ignoré	Complété
Complété	Complété	Complété
Complété	Échec	Terminé avec un avertissement
Échec	Échec	Échec

PARTIE 2

Déployer un réseau virtuel

Dans ce module, vous allez :

- Explorer les aspects de bases d’un réseau virtuel
- Explorer les aspects avancés d’un réseau virtuel

8 heures

CHAPITRE 1

Explorer les aspects de bases d’un réseau virtuel

Ce que vous allez apprendre dans ce chapitre :

- Appliquer les concepts de base d’un réseau virtuel
- Paramétrer les aspects d'un réseau virtuel

4 heures

CHAPITRE 1

Explorer les aspects de bases d’un réseau virtuel

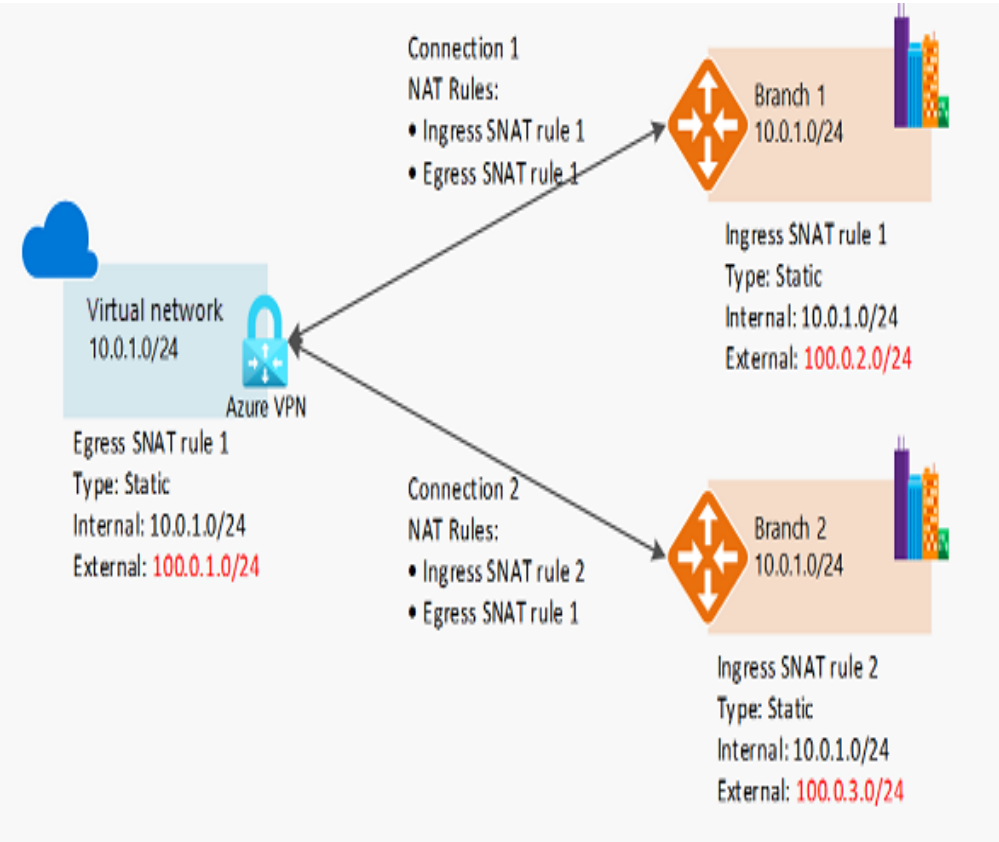
1. **Espace d’adressage et sous-réseaux**
2. IP publique et IP privée
3. Passerelle
4. Serveurs DNS

Espace d'adressage

Lors de la création d'un réseau virtuel, vous devez spécifier un espace d'adressage IP privé personnalisé à l'aide d'adresses (RFC 1918) publiques et privées. Azure attribue aux ressources d'un réseau virtuel une adresse IP privée à partir de l'espace d'adressage que vous attribuez. Par exemple, si vous déployez une machine virtuelle dans un réseau virtuel avec l'espace d'adressage 10.0.0.0/16, la machine virtuelle reçoit une adresse IP privée telle que 10.0.0.4.

Pendant la création d'un réseau virtuel, il faut prendre en charge les éléments suivants :

- Vous pouvez ajouter un espace d'adressage après avoir créé votre réseau virtuel. Ce processus n'a pas besoin d'une interruption si le réseau virtuel est déjà connecté à un autre réseau virtuel par le biais de l'appairage de réseaux virtuels. Au lieu de cela, chaque appairage distant a besoin qu'une opération de resynchronisation soit effectuée suite à la modification de l'espace réseau.
- Azure réserve cinq adresses IP dans chaque sous-réseau. Prenez en compte ces adresses lorsque vous dimensionnez des réseaux virtuels et les sous-réseaux qu'ils englobent.
- Certains services Azure nécessitent des sous-réseaux dédiés. Ces services sont le Pare-feu Azure et la passerelle VPN Azure.
- Vous pouvez déléguer des sous-réseaux à certains services pour créer des instances de ceux-ci à l'intérieur du sous-réseau.



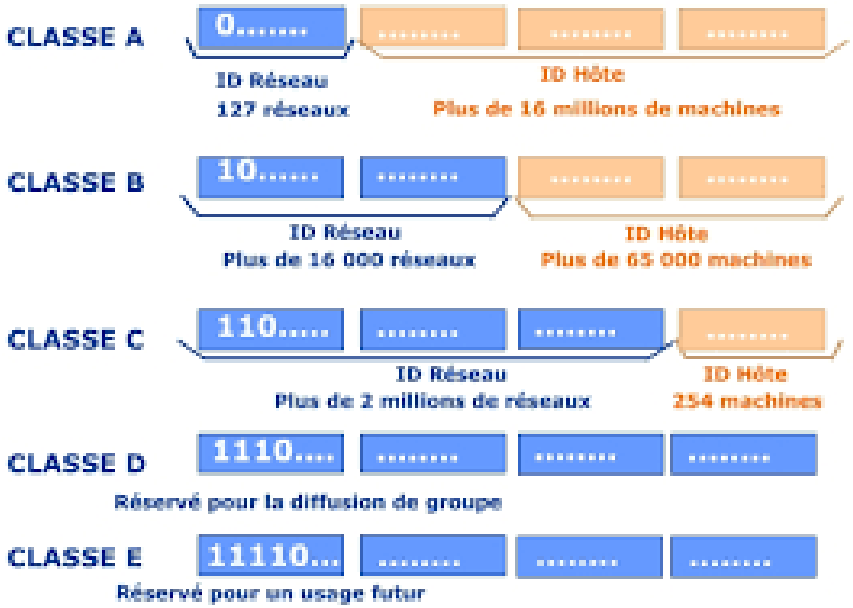
PARTIE 2

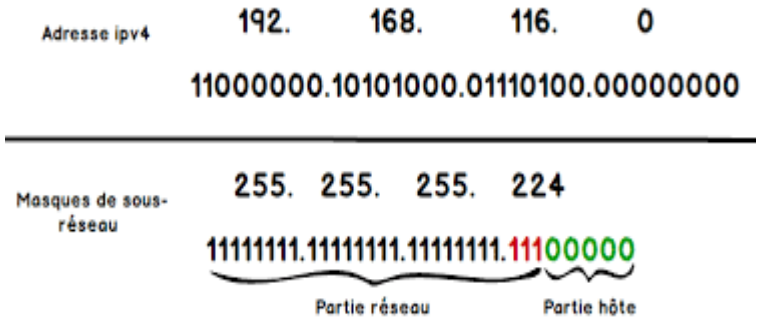
Espace d'adressage

- Planifiez à l'avance des espaces d'adressage IP qui ne se chevauchent pas dans les régions Azure et les emplacements locaux.
- Utilisez des adresses IP de l'allocation d'adresses pour l'Internet privé, appelées adresses RFC 1918.
- N'utilisez pas les plages d'adresses suivantes :
  - 224.0.0.0/4 (multidiffusion)
  - 255.255.255.255/32 (diffusion)
  - 127.0.0.0/8 (bouclage)
  - 169.254.0.0/16 (lien-local)
  - 168.63.129.16/32 (DNS interne)
- Pour les environnements au sein desquels la disponibilité des adresses IP privées est limitée, vous pouvez utiliser le protocole IPv6. Les réseaux virtuels peuvent être IPv4 seulement ou à double pile IPv4 + IPv6.
- Ne créez pas de grands réseaux virtuels tels que /16. Cela permet de s'assurer que l'espace d'adressage IP n'est pas gaspillé. Le plus petit sous-réseau IPv4 pris en charge est /29 et le plus grand est /2 lorsque des définitions de sous-réseaux CIDR (Classless Inter-Domain Routing). La taille des sous-réseaux IPv6 doit être exactement de /64.
- Ne créez pas de réseaux virtuels sans planifier à l'avance l'espace d'adressage requis.
- N'utilisez pas d'adresses IP publiques pour les réseaux virtuels, en particulier si les adresses IP publiques n'appartiennent pas à votre organisation.

Plage d'adresse de sous-réseaux

Les sous-réseaux vous permettent de segmenter le réseau virtuel en sous-réseaux, et d'allouer une partie de l'espace d'adressage du réseau virtuel à chaque sous-réseau. Vous pouvez ensuite déployer des ressources Azure dans un sous-réseau spécifique. Comme dans un réseau traditionnel, les sous-réseaux vous permettent de segmenter votre espace d'adressage de réseau virtuel en segments appropriées pour le réseau interne de l'organisation. Cela améliore également l'efficacité l'allocation d'adresse. Vous pouvez sécuriser des ressources au sein de sous-réseaux à l'aide de Groupes de sécurité réseau.





PARTIE 2

Création d'un réseau virtuel sur Azure

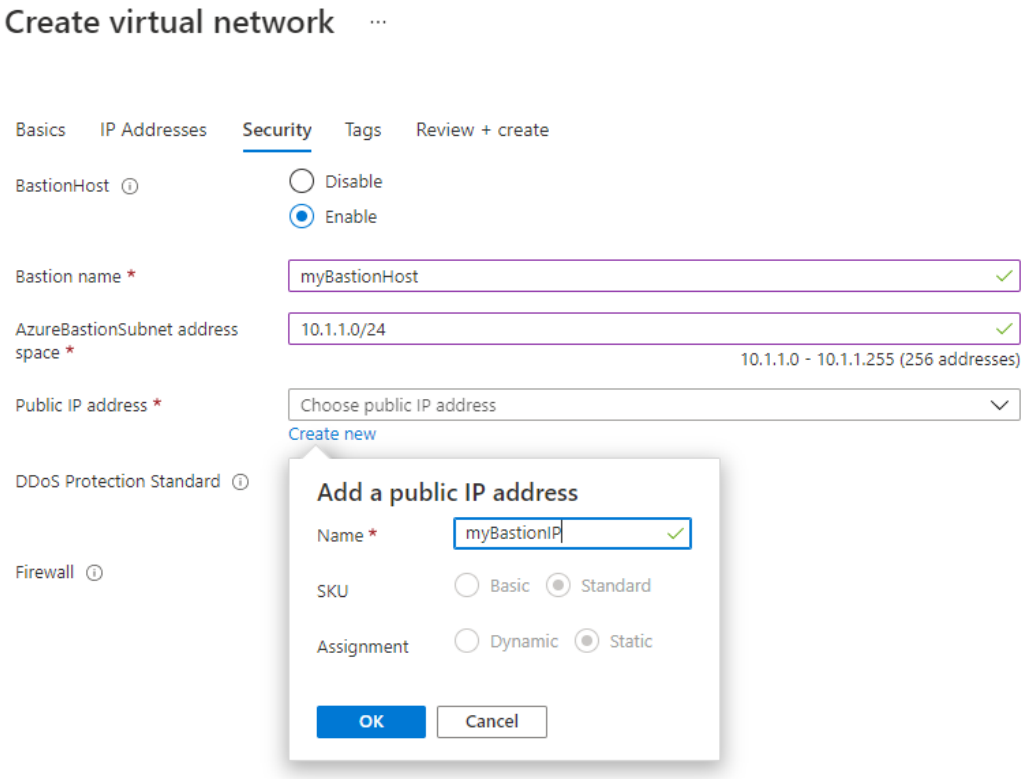
Pour ajouter un sous-réseau sur Azure :

1. Accédez au portail Azure pour afficher vos réseaux virtuels. Recherchez et sélectionnez Réseaux virtuels.
2. Sélectionnez le nom du réseau virtuel auquel vous souhaitez ajouter un sous-réseau.
3. Sous Paramètres, sélectionnez Sous-réseaux>Sous-réseau.
4. Dans la boîte de dialogue Ajouter un sous-réseau, entrez les valeurs des paramètres suivants :
    - **Nom :** Le nom doit être unique au sein du réseau virtuel. Pour une compatibilité maximale avec d'autres services Azure, nous recommandons d'utiliser une lettre comme premier caractère du nom. Par exemple, Azure Application Gateway ne se déploiera pas dans un sous-réseau portant un nom qui commence par un nombre.
    - **Plage d'adresses de sous-réseau :** La plage doit être unique dans l'espace d'adressage du réseau virtuel. La plage ne peut pas chevaucher d'autres plages d'adresses de sous-réseau au sein du réseau virtuel. L'espace d'adressage doit être spécifié en utilisant la notation de routage CIDR (Classless InterDomain Routing).
    - Par exemple, dans un réseau virtuel avec l'espace d'adressage 10.0.0.0/16, vous pouvez définir l'espace d'adressage de sous-réseau 10.0.0.0/22. La plus petite plage que vous puissiez spécifier est /29. Celle-ci fournit huit adresses IP pour le sous-réseau. Azure réserve la première et la dernière adresses dans chaque sous-réseau pour la conformité du protocole. Trois adresses supplémentaires sont réservées à l'usage du service Azure. Par conséquent, définir un sous-réseau avec une plage d'adresses /29 produit trois adresses IP utilisables dans le sous-réseau.

PARTIE 2

Création d'un réseau virtuel sur Azure

- **Ajouter un espace d'adressage IPv6 :** Vous pouvez créer un réseau virtuel à double pile (qui prend en charge IPv4 et IPv6) en ajoutant un espace d'adressage IPv6 existant. Vous pouvez également ajouter la prise en charge d'IPv6 ultérieurement, après avoir créé le réseau virtuel. Actuellement, IPv6 n'est pas entièrement pris en charge pour tous les services d'Azure.
- **Passerelle NAT :** Pour fournir une traduction d'adresses réseau (NAT) aux ressources d'un sous-réseau, vous pouvez associer une passerelle NAT existante à un sous-réseau. La passerelle NAT doit être associée au même abonnement et se trouver au même emplacement que le réseau virtuel.
- **Groupe de sécurité réseau :** Vous pouvez associer un groupe de sécurité réseau existant à un sous-réseau pour filtrer le trafic réseau entrant et sortant du sous-réseau. Le groupe de sécurité réseau doit exister dans le même abonnement et au même emplacement que le réseau virtuel.
- **Table de routage :** Vous pouvez éventuellement associer une table de route existante à un sous-réseau pour contrôler le routage du trafic réseau vers d'autres réseaux. La table de routage doit exister dans le même abonnement et au même emplacement que le réseau virtuel.



Création d'un réseau virtuel sur Azure

- **Points de terminaison de service :** Un sous-réseau peut éventuellement avoir un ou plusieurs points de terminaison de service activés. Pour activer un point de terminaison de service pour un service spécifique, sélectionnez le ou les services pour lesquels vous souhaitez activer des points de terminaison de service dans la liste **Services**. Azure configure automatiquement l'emplacement d'un point de terminaison. Par défaut, Azure configure les points de terminaison de service dans la région du réseau virtuel. Pour le Stockage Azure, Azure configure automatiquement les points de terminaison dans des régions appairées Azure pour permettre la prise en charge de scénarios de basculement régionaux.
- **Délégation de sous-réseau :** Un sous-réseau peut éventuellement avoir une ou plusieurs délégations activées. La délégation de sous-réseau donne des autorisations explicites au service pour créer des ressources propres au service dans le sous-réseau à l'aide d'un identificateur unique pendant le déploiement du service. Pour déléguer à un service, sélectionnez le service souhaité dans la liste **Services**.
- **Stratégie réseau pour les points de terminaison privés :** Pour contrôler le trafic à destination d'un point de terminaison privé, vous pouvez utiliser des groupes de sécurité réseau, des groupes de sécurité d'application ou des itinéraires définis par l'utilisateur. *Activez* la stratégie réseau de point de terminaison privé pour utiliser ces contrôles sur un sous-réseau. Une fois activée, la stratégie réseau s'applique à tous les points de terminaison privés du sous-réseau.

5. Pour ajouter le sous-réseau au réseau virtuel que vous avez sélectionné, cliquez sur **OK**.

Modifier les paramètres d'un sous-réseau

1. Accédez au portail Azure pour afficher vos réseaux virtuels. Recherchez et sélectionnez Réseaux virtuels.
2. Sélectionnez le nom du réseau virtuel contenant le sous-réseau que vous souhaitez modifier.
3. Dans Paramètres, sélectionnez Sous-réseaux.
4. Dans la liste des sous-réseaux, sélectionnez le sous-réseau dont vous souhaitez modifier les paramètres.
5. Dans la page du sous-réseau, modifiez l'un des éléments suivants :

Paramètre	Description
Plage d'adresses de sous-réseau	Si aucune ressource n'a été déployée dans le sous-réseau, vous pouvez changer la plage d'adresses. Si des ressources existent déjà dans le sous-réseau, vous devez soit déplacer les ressources vers un autre sous-réseau, soit les supprimer d'abord du sous-réseau. La procédure à suivre pour supprimer ou déplacer une ressource varie en fonction de celle-ci. Pour savoir comment supprimer ou déplacer des ressources dans des sous-réseaux, lisez la documentation relative à chaque type de ressource. Consultez les contraintes pour la plage d'adresses à l'étape d'ajout d'un sous-réseau.
Ajouter un espace d'adressage IPv6, Passerelle NAT, Groupe de sécurité réseau et Table de routage	Consultez l'étape d'ajout d'un sous-réseau

Modifier les paramètres d'un sous-réseau

Paramètre	Description
Points de terminaison de service	Consultez les points de terminaison de service à l'étape d'ajout ud'un sous-réseau. Quand vous activez un point de terminaison de service pour un sous-réseau existant, assurez-vous qu'aucune tâche critique n'est en cours d'exécution sur l'une des ressources du sous-réseau. Les points de terminaison de service changent d'itinéraire sur chaque interface réseau dans le sous-réseau. L'itinéraire par défaut avec l'adresse de préfixe 0.0.0.0/0 et le type de tronçon suivant Internet sont remplacés par un nouvel itinéraire avec les préfixes d'adresse du service et le type de tronçon suivant VirtualNetworkServiceEndpoint. Le changement de routage peut entraîner l'arrêt des connexions TCP ouvertes. Le point de terminaison de service est activé après que les flux de trafic vers le service sur toutes les interfaces réseau ont été mis à jour avec le nouvel itinéraire.
Délégation de sous-réseau	Vous pouvez modifier la délégation de sous-réseau pour qu'elle ait zéro ou plusieurs délégations activées. Si une ressource pour un service est déjà déployée dans le sous-réseau, la délégation de sous-réseau ne peut être ni ajoutée ni supprimée tant que toutes les ressources pour le service ne sont pas supprimées. Pour déléguer à un autre service, sélectionnez le service souhaité dans la liste Services.
Stratégie réseau pour les points de terminaison privés	Consultez la partie précédente.

6. Sélectionnez Enregistrer.

Supprimer un sous-réseau

Vous pouvez supprimer un sous-réseau uniquement si aucune ressource ne s'y trouve. Si le sous-réseau contient des ressources, vous devez les supprimer pour pouvoir supprimer le sous-réseau. La procédure à suivre pour supprimer une ressource varie en fonction de celle-ci. Pour savoir comment supprimer des ressources dans des sous-réseaux, lisez la documentation relative à chaque type de ressource.

1. Accédez au portail Azure pour afficher vos réseaux virtuels. Recherchez et sélectionnez Réseaux virtuels.
2. Sélectionnez le nom du réseau virtuel contenant le sous-réseau que vous souhaitez supprimer.
3. Dans Paramètres, sélectionnez Sous-réseaux.
4. Dans la liste des sous-réseaux, sélectionnez le sous-réseau que vous souhaitez supprimer.
5. Sélectionnez Supprimer, puis Oui dans la boîte de dialogue de confirmation.

CHAPITRE 1

Explorer les aspects de bases d’un réseau virtuel

1. Espace d’adressage et sous-réseaux
2. **IP publique et IP privée**
3. Passerelle
4. Serveurs DNS

IP publique : Définition

Les adresses IP publiques permettent aux ressources Internet de communiquer avec :

- Les ressources Azure (communication entrante).
- L'Internet et les services Azure publics.

Dans Azure, une adresse IP publique est une ressource ayant ses propres propriétés. Voici quelques-unes des ressources auxquelles vous pouvez associer une ressource d'adresse IP publique :

- Interfaces réseau de machine virtuelle
- Groupes identiques de machines virtuelles
- Équilibreurs de charge publics
- Passerelles de réseau virtuel (VPN/ER)
- Passerelles NAT
- Passerelles d'application
- Pare-feu Azure
- Hôte Bastion
- Serveur de routes

IP publique : Critères d'attribution

Le tableau ci-dessous présente la propriété avec laquelle une adresse IP publique peut être associée à une ressource, ainsi que les méthodes d'allocation. Notez que la prise en charge du protocole IPv6 public n'est actuellement pas disponible pour tous les types de ressources.

Ressources de niveau supérieur	Association d'adresse IP	IPv4 dynamique	IPv4 statique	IPv6 dynamique	IPv6 statique
Machine virtuelle	interface réseau	Oui	Oui	Oui	Oui
Équilibreur de charge public	Configuration frontale	Oui	Oui	Oui	Oui
Passerelle de réseau virtuel (VPN)	Configuration IP de la passerelle	Oui (non-AZ uniquement)	Oui	Non	Non
Passerelle de réseau virtuel (ER)	Configuration IP de la passerelle	Oui	Non	Oui (préversion)	No
Passerelle NAT	Configuration IP de la passerelle	Non	Oui	Non	Non
passerelle d'application	Configuration frontale	Oui (V1 uniquement)	Oui (V2 uniquement)	Non	Non
Pare-feu Azure	Configuration frontale	Non	Oui	Non	Non
Hôte Bastion	Configuration IP publique	Non	Oui	Non	Non
Serveur de routes	Configuration frontale	Non	Oui	Non	Non

IP publique : La taille (SKU)

Les adresses IP publiques sont créées avec l'une des références SKU suivantes :

Adresse IP publique	standard	De base
Méthode d'allocation	Statique	Pour IPv4 : dynamique ou statique ; pour IPv6 : dynamique.
Délai d'inactivité	Dotées d'un délai d'inactivité du flux entrant réglable de 4 à 30 minutes, avec une valeur par défaut de 4 minutes et d'un délai d'inactivité du flux sortant fixe de 4 minutes.	Dotées d'un délai d'inactivité du flux entrant réglable de 4 à 30 minutes, avec une valeur par défaut de 4 minutes et d'un délai d'inactivité du flux sortant fixe de 4 minutes.
Sécurité	Modèle sécurisé par défaut et proche du trafic entrant quand il est utilisé en tant que serveur frontal. Il est nécessaire d'autoriser le trafic avec le groupe de sécurité réseau (NSG) (par exemple, sur la carte réseau d'une machine virtuelle à laquelle est attachée une adresse IP publique de référence SKU standard).	Ouvertes par défaut. Il est recommandé d'utiliser des groupes de sécurité réseau, mais cela est facultatif pour restreindre le trafic entrant ou sortant.
Zones de disponibilité	Pris en charge. Les IP standard peuvent être non-zonales, zonales ou redondantes interzone. Les IP redondantes dans une zone peuvent être créées seulement dans des régions où 3 zones de disponibilité sont actives. Les IP créées avant que les zones soient actives ne sont pas redondantes dans une zone.	Non pris en charge.
Préférence de routage	Pris en charge pour permettre un contrôle plus précis de la façon dont le trafic est routé entre Azure et Internet.	Non pris en charge.
Niveau global	Pris en charge via des équilibreurs de charge inter-région.	Non pris en charge.

IP publique : Type d'affectation

Les adresses IP publiques ont deux types d'affectations :

- Statique : une adresse IP est attribuée à la ressource au moment de sa création. L'adresse IP est libérée lorsque la ressource est supprimée.
- Dynamique : si vous sélectionnez la méthode dynamique, l'adresse IP n'est pas attribuée à la ressource au moment de sa création. L'adresse IP est attribuée lorsque vous associez la ressource d'adresse IP publique à une ressource. L'adresse IP est libérée lorsque vous arrêtez ou supprimez la ressource.

Des adresses IP publiques statiques sont fréquemment utilisées dans les cas suivants :

- Lorsque vous devez mettre à jour les règles de pare-feu pour communiquer avec vos ressources Azure.
- La résolution de noms DNS est telle qu'une modification de l'adresse IP nécessiterait une mise à jour des enregistrements A.
- Vos ressources Azure communiquent avec d'autres applications ou services qui utilisent un modèle de sécurité basé sur une adresse IP.
- Vous utilisez des certificats TLS/SSL liés à une adresse IP.

Des adresses IP publiques de base sont couramment utilisées quand il n'existe pas de dépendance sur l'adresse IP. Par exemple, une ressource IP publique est libérée à partir d'une ressource nommée Ressource A. Ressource A reçoit une adresse IP différente au démarrage si la ressource IP publique est réaffectée. Une adresse IP associée est libérée si la méthode d'allocation passe de statique à dynamique. Une adresse IP associée est inchangée si la méthode d'allocation passe de dynamique à statique. Définissez la méthode d'allocation statique pour vous assurer que l'adresse IP ne change pas.

IP privée : Définition

Les adresses IP privées permettent à des ressources de communiquer dans Azure.

Les ressources peuvent être :

- Des services Azure tels que :
  - Interfaces réseau de machine virtuelle
  - Équilibreurs de charge interne (ILB)
  - Passerelles d'application
- Dans un réseau virtuel.
- Accessibles sur un réseau local via une passerelle VPN ou un circuit ExpressRoute.

Les adresses IP privées permettent la communication avec ces ressources sans utilisation d'adresse IP publique.

Méthode d'allocation

Azure attribue des adresses IP privées aux ressources à partir de la plage d'adresses du sous-réseau de réseau virtuel dans lequel se trouvent les ressources.

Azure réserve les quatre premières adresses dans chaque plage d'adresses de sous-réseau. Ces adresses ne peuvent pas être attribuées à des ressources. Par exemple, si la plage d'adresses du sous-réseau est 10.0.0.0/16, les adresses 10.0.0.0-10.0.0.3 et 10.0.255.255 ne sont pas disponibles. Les adresses IP de la plage d'adresses du sous-réseau peuvent uniquement être attribuées à une ressource à la fois.

IP privée : Méthodes d'attribution

Il existe deux méthodes d'attribution d'adresses IP :

- **Dynamique** : Azure attribue la première adresse IP non attribuée ou non réservée de la plage d'adresses du sous-réseau. Par exemple, Azure attribue l'adresse 10.0.0.10 à une nouvelle ressource si les adresses 10.0.0.4 à 10.0.0.9 sont déjà attribuées à d'autres ressources.

  La méthode d'allocation par défaut est dynamique. Une fois attribuées, les adresses IP dynamiques sont libérées si :

  - Une interface réseau est supprimée
  - Une interface réseau est réaffectée à un autre sous-réseau au sein du même réseau virtuel
  - La méthode d'allocation devient statique et une adresse IP différente est spécifiée

  Par défaut, Azure définit l'adresse statique sur l'adresse dynamique attribuée précédemment quand vous sélectionnez la méthode d'allocation statique à la place de la méthode dynamique.

- **Statique** : vous sélectionnez et attribuez n'importe quelle adresse IP non attribuée ou non réservée de la plage d'adresses du sous-réseau.

  Par exemple, la plage d'adresses d'un sous-réseau est 10.0.0.0/16 et les adresses 10.0.0.4 à 10.0.0.9 sont attribuées à d'autres ressources. Vous pouvez attribuer n'importe quelle adresse comprise entre 10.0.0.10 et 10.0.255.254. Les adresses statiques ne sont libérées que si l'interface réseau est supprimée.

  Azure attribue l'adresse IP statique en tant qu'adresse IP dynamique quand la méthode d'allocation est changée. La réaffectation se produit même si l'adresse n'est pas la suivante disponible dans le sous-réseau. L'adresse change quand l'interface réseau est attribuée à un autre sous-réseau.

  Pour attribuer l'interface réseau à un sous-réseau différent, vous devez remplacer la méthode d'allocation statique par la méthode d'allocation dynamique. Attribuez l'interface réseau à un sous-réseau différent, puis redéfinissez la méthode d'allocation sur statique. Attribuez une adresse IP à partir de la plage d'adresses du nouveau sous-réseau.

CHAPITRE 1

Explorer les aspects de bases d’un réseau virtuel

1. Espace d’adressage et sous-réseaux
2. IP publique et IP privée
3. **Passerelle**
4. Serveurs DNS

Définition

Une passerelle de réseau virtuel est composée de deux machines virtuelles ou plus qui sont automatiquement configurées et déployées sur un sous-réseau spécifique que vous créez, appelé sous-réseau de la passerelle. Les machines virtuelles de passerelle contiennent des tables de routage et exécutent des services de passerelle spécifiques. Vous ne pouvez pas configurer directement les machines virtuelles qui font partie de la passerelle de réseau virtuel, même si les paramètres que vous sélectionnez lors de la configuration de votre passerelle ont un impact sur les machines virtuelles de passerelle créées.

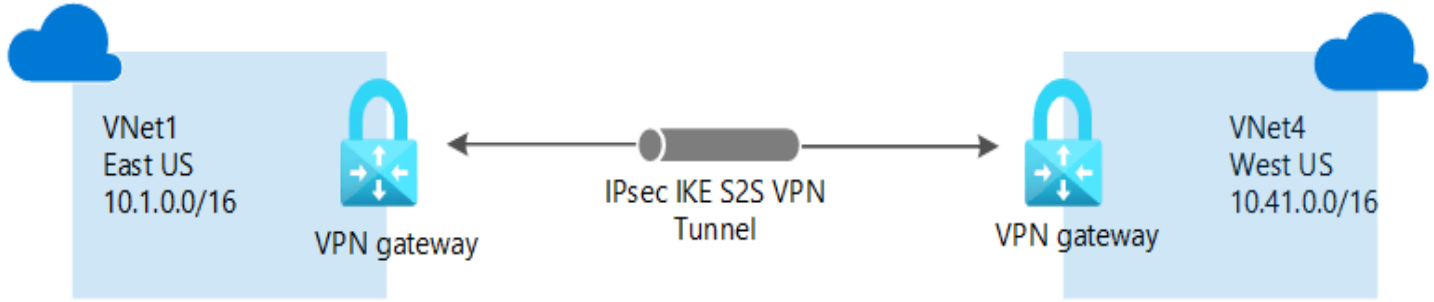
Qu'est-ce qu'une passerelle VPN ?

Quand vous configurez une passerelle de réseau virtuel, vous configurez un paramètre qui spécifie le type de passerelle. Le type de passerelle détermine la manière dont la passerelle de réseau virtuel est utilisée et les actions qu'elle exécute. Le type de passerelle Vpn » spécifie que le type de passerelle de réseau virtuel créé est une passerelle VPN ». Ceci la distingue d'une passerelle ExpressRoute, qui utilise un type de passerelle différent. Un réseau virtuel peut avoir deux passerelles de réseau virtuel : une passerelle VPN et une passerelle ExpressRoute.

Lors de la création d'une passerelle VPN, les machines virtuelles de passerelle sont déployées dans le sous-réseau de la passerelle et configurées avec les paramètres que vous avez spécifiés. Ce processus peut prendre 45 minutes ou plus, selon le niveau tarifaire de la passerelle que vous sélectionnez. Après avoir créé une passerelle VPN, vous pouvez créer une connexion de tunnel IPsec/IKE VPN entre cette passerelle VPN et une autre (de réseau virtuel à réseau virtuel), ou créer une connexion de tunnel IPsec/IKE VPN intersite entre la passerelle VPN et un périphérique VPN local (de site à site). Vous pouvez également créer une connexion VPN de point à site (VPN sur OpenVPN, IKEv2 ou SSTP), ce qui vous permet de vous connecter à votre réseau virtuel à partir d'un emplacement distant, par exemple une salle de conférence ou votre domicile.

Configurer une connexion de passerelle VPN

Une connexion par passerelle VPN s'appuie sur plusieurs ressources qui sont configurées avec des paramètres spécifiques. La plupart des ressources peuvent être configurées séparément, mais certaines d'entre elles doivent être configurées dans un certain ordre.



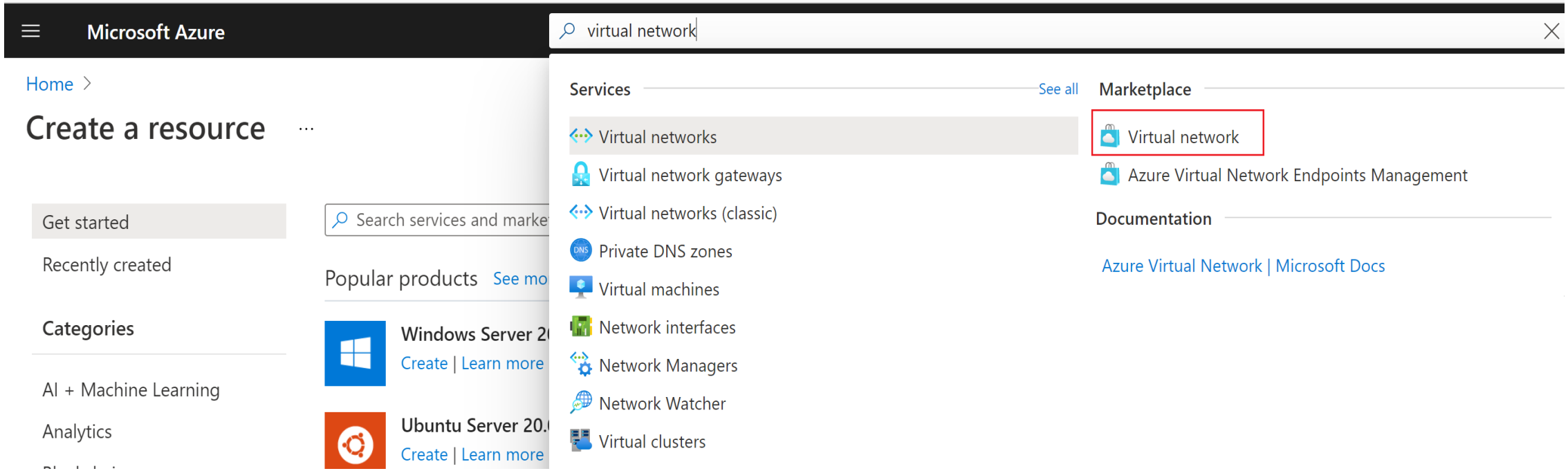
Pour créer une connexion de passerelle VPN, on va suivre les étapes suivantes :

1. Créer un réseau virtuel (VNET1)
2. Créer une passerelle de réseau virtuel
3. Créer un réseau virtuel (VNET4)
4. Configurer la connexion de passerelle VNet1

PARTIE 2

Les étapes de création : 1- Créer un réseau virtuel (VNET1)

1. Connectez-vous au portail Azure.
2. Dans **Rechercher dans les ressources, services et documents (G+/)**, saisissez ***réseau virtuel***. Sélectionnez **Réseau virtuel** dans les résultats de **Place de marché** pour ouvrir la page **Réseau virtuel**.

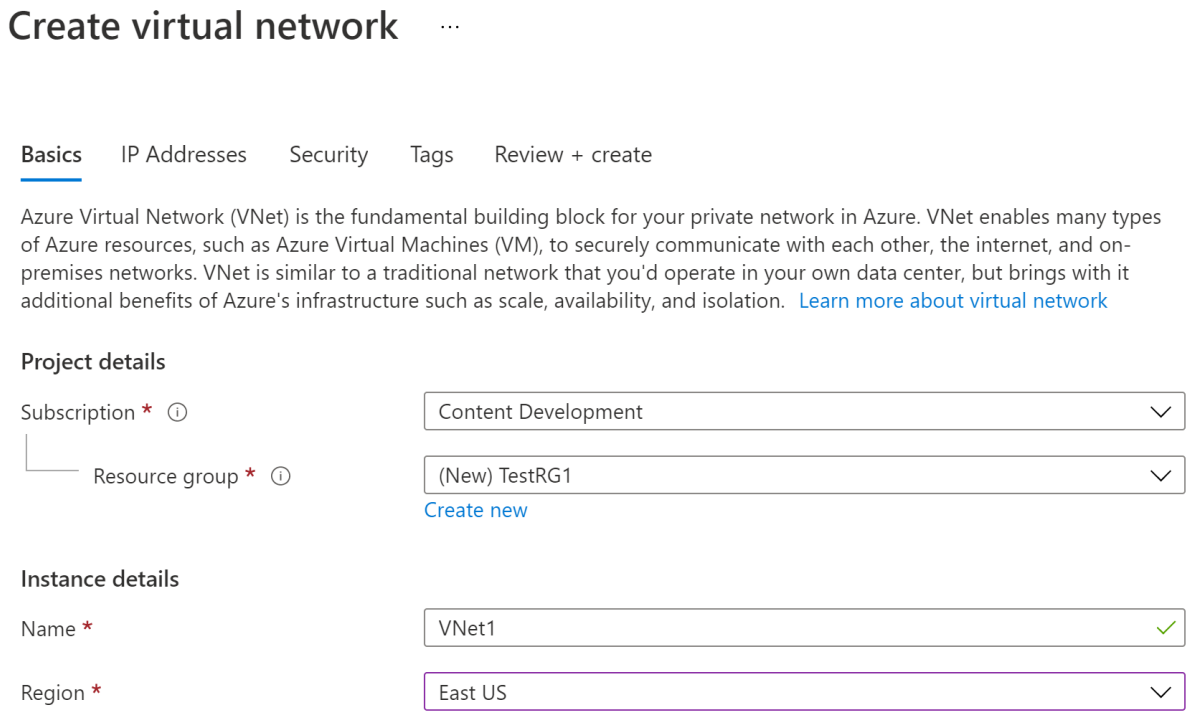


PARTIE 2

Les étapes de création : 1- Créer un réseau virtuel

3. Dans la page Réseau virtuel, sélectionnez Créer. La page Créer un réseau virtuel s'ouvre.
4. Sous l'onglet Informations de base, configurez les paramètres de réseau virtuel pour créer un réseau virtuel

- **Abonnement**: vérifiez que l'abonnement listé est approprié. Vous pouvez modifier des abonnements à l'aide de la liste déroulante.
- **Groupe de ressources** : sélectionnez un groupe de ressources existant ou sélectionnez **Créer nouveau** pour en créer un.
- **Name** : entrez le nom du réseau virtuel.
- **Région** : sélectionnez l'emplacement du réseau virtuel. L'emplacement détermine où se trouveront les ressources que vous déployez sur ce réseau virtuel.

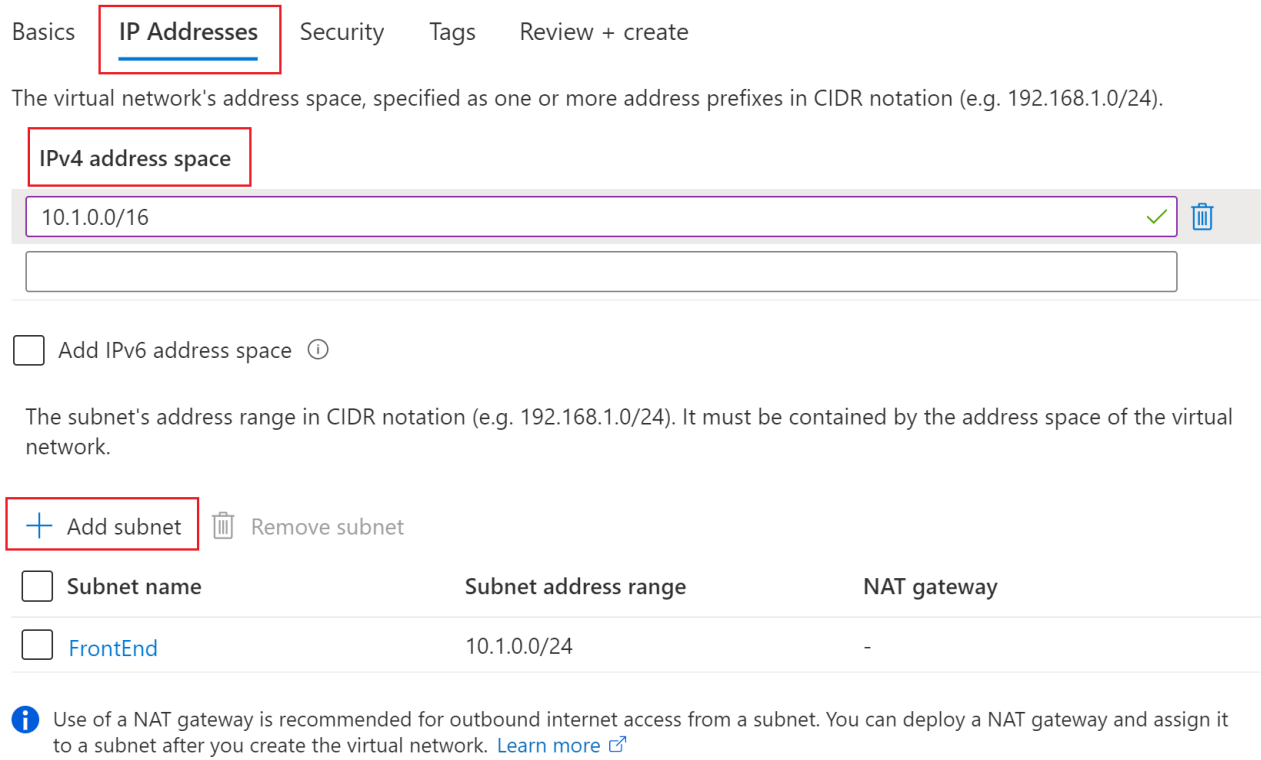


PARTIE 2

Les étapes de création : 1- Créer un réseau virtuel

5. Sélectionnez **Adresses IP** pour passer à l'onglet Adresses IP. Sous l'onglet Adresses IP, configurez les paramètres. Les valeurs affichées dans l'exemple peuvent être ajustées en fonction des paramètres dont vous avez besoin.

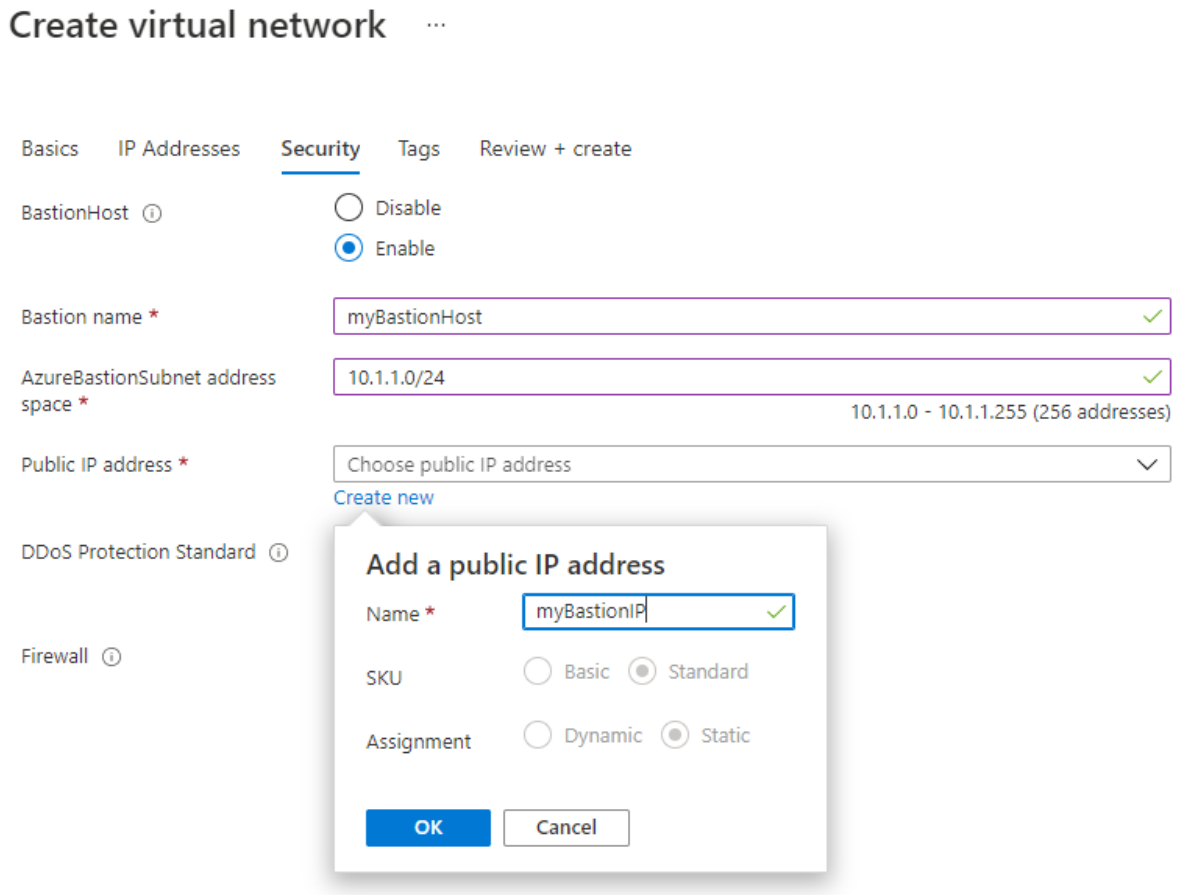
- **Espace d'adressage IPv4** : Un espace d'adressage est créé automatiquement par défaut. Vous pouvez sélectionner l'espace d'adressage et le définir selon vos propres valeurs.
- **+ Ajouter un sous-réseau** : Si vous utilisez l'espace d'adressage par défaut, un sous-réseau par défaut est créé automatiquement. Sélectionnez **+ Ajouter un sous-réseau** pour ouvrir la fenêtre **Ajouter un sous-réseau**. Configurez les paramètres suivants, puis sélectionnez **Ajouter** en bas de la page pour ajouter les valeurs.
  - **Nom du sous-réseau** : Exemple : "FrontEnd" .
  - **Plage d'adresses de sous-réseau** : plage d'adresses de ce sous-réseau.



PARTIE 2

Les étapes de création : 1- Créer un réseau virtuel

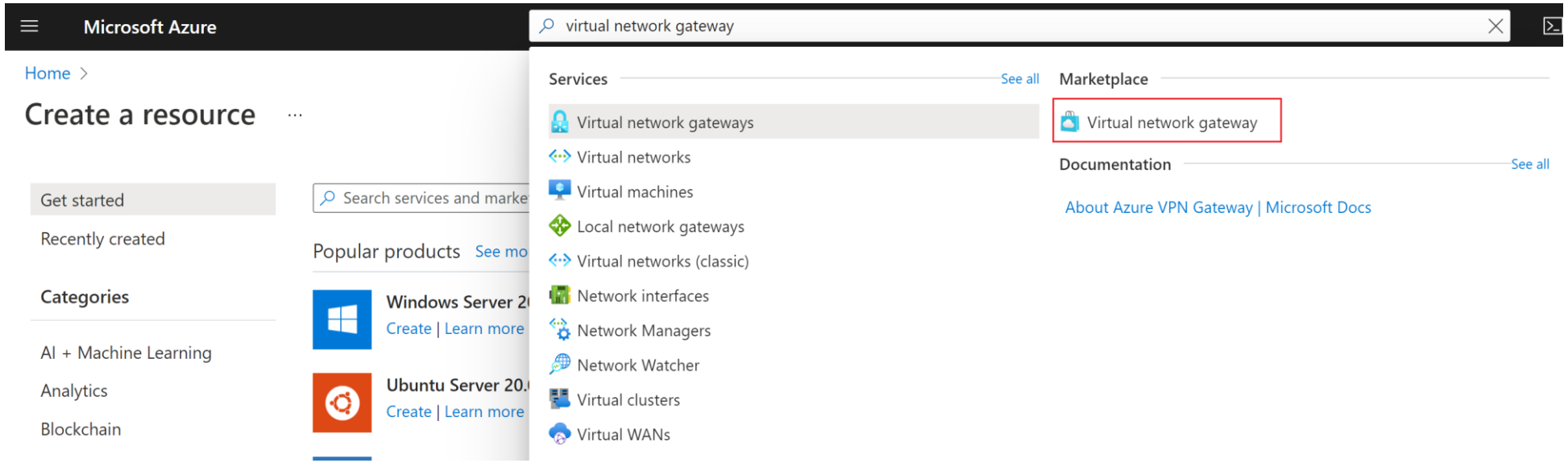
6. Sélectionnez **Sécurité** pour accéder à l'onglet Sécurité. Conservez les valeurs par défaut pour le moment.
   - **BastionHost** : Désactiver
   - **Protection DDoS Standard** : Désactiver
   - **Pare-feu** : Désactiver
7. Sélectionnez **Vérifier + créer** pour vérifier les paramètres de réseau virtuel.
8. Une fois les paramètres validés, sélectionnez **Créer** pour créer le réseau virtuel.



PARTIE 2

Les étapes de création : 2- Créer une passerelle de réseau virtuel

1. Dans **Rechercher dans les ressources, services et documents (G+/)**, tapez **passerelle de réseau virtuel**. Recherchez la **passerelle réseau virtuel** dans les résultats de la recherche de la Place de marché et sélectionnez-la pour ouvrir la page **Créer une passerelle réseau virtuel**.

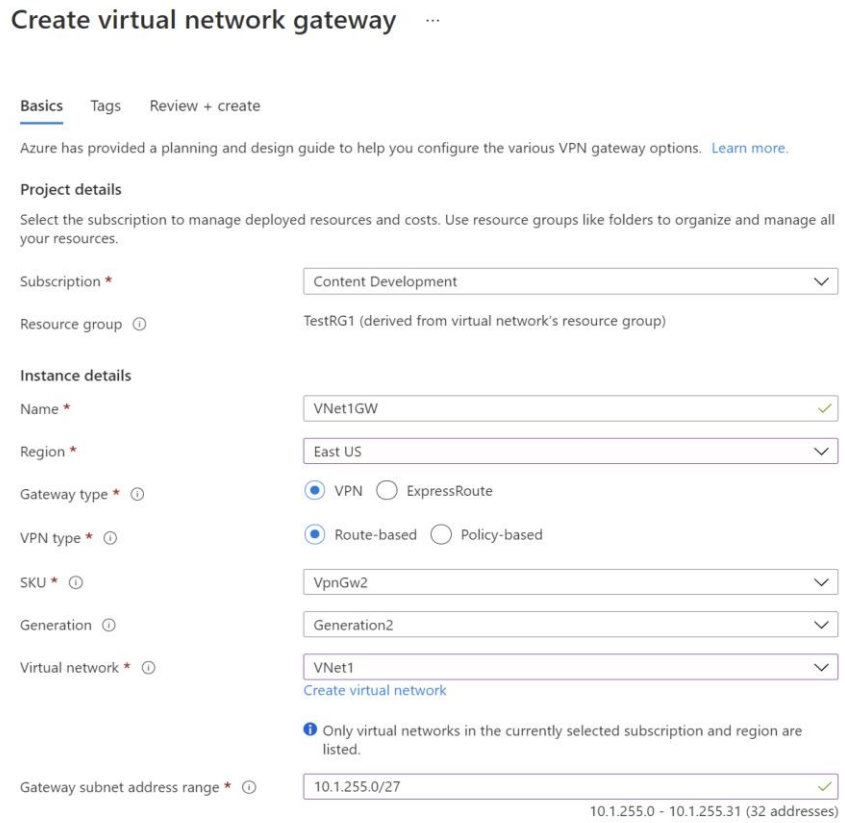


PARTIE 2

Les étapes de création : 2- Créer une passerelle de réseau virtuel

2. Sous l'onglet **Général**, renseignez les valeurs pour **Détails du projet** et **Détails de l'instance**.

- **Abonnement**: Sélectionnez l'abonnement à utiliser dans la liste déroulante.
- **Groupe de ressources** : Ce paramètre est renseigné automatiquement quand vous sélectionnez votre réseau virtuel sur cette page.
- **Name** : Nommez votre passerelle. Le nommage de votre passerelle n'est pas identique au nommage d'un sous-réseau de passerelle. Il s'agit du nom de l'objet passerelle que vous créez.
- **Région** : Sélectionnez la région où vous voulez créer cette ressource. La région de la passerelle doit être la même que celle du réseau virtuel.
- **Type de passerelle** : Sélectionnez **VPN**. Les passerelles VPN utilisent le type de passerelle de réseau virtuel **VPN**.

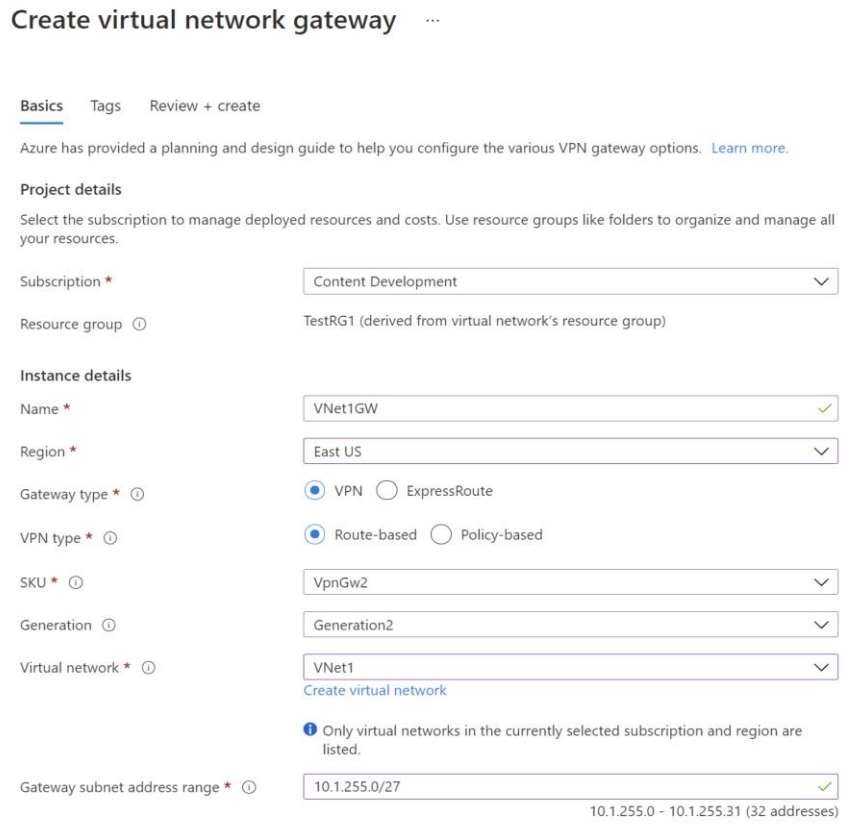


PARTIE 2

Les étapes de création : 2- Créer une passerelle de réseau virtuel

2. Sous l'onglet **Général**, renseignez les valeurs pour **Détails du projet** et **Détails de l'instance**.

- **Type de VPN** : sélectionnez le type de VPN spécifié pour votre configuration. La plupart des configurations requièrent un type de VPN basé sur un itinéraire.
- **Niveau tarifaire** : sélectionnez le niveau tarifaire (SKU) de la passerelle que vous voulez utiliser dans la liste déroulante. Les références répertoriées dans la liste déroulante dépendent du type de VPN que vous sélectionnez. Veillez à sélectionner une référence (SKU) qui prend en charge les fonctionnalités que vous voulez utiliser.
- **Génération** : sélectionnez la génération que vous voulez utiliser.
- **Réseau virtuel** : sélectionnez le réseau virtuel auquel vous souhaitez ajouter cette passerelle dans la liste déroulante. Si vous ne voyez pas le VNet pour lequel vous voulez créer une passerelle, assurez-vous que vous avez sélectionné l'abonnement et la région corrects dans les paramètres précédents.



PARTIE 2

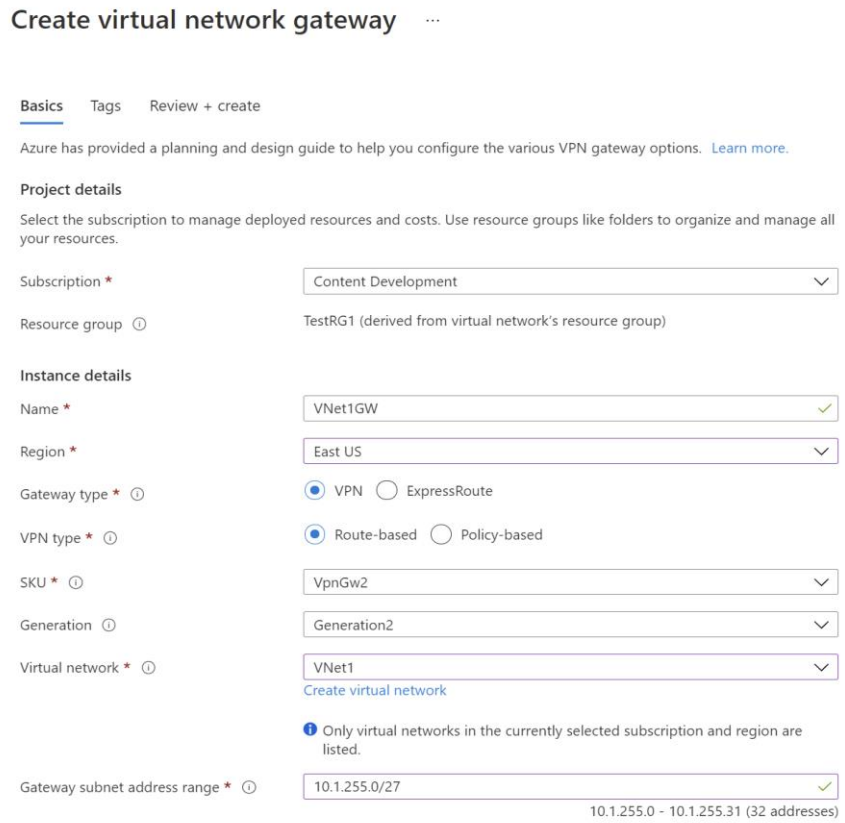
Les étapes de création : 2- Créer une passerelle de réseau virtuel

2. Sous l'onglet **Général**, renseignez les valeurs pour **Détails du projet** et **Détails de l'instance**.

- **Plage d'adresses de sous-réseau de la passerelle** : Ce champ apparaît uniquement si votre réseau virtuel n'a pas de sous-réseau de passerelle. Il est préférable de spécifier /27 ou plus grand (/26, /25, etc.). Ceci permet d'obtenir suffisamment d'adresses IP pour les modifications futures, comme l'ajout d'une passerelle ExpressRoute. Nous vous déconseillons de créer une plage inférieure à /28. Si vous disposez déjà d'un sous-réseau de passerelle, vous pouvez en voir les détails en accédant à votre réseau virtuel. Sélectionnez **Sous-réseaux** pour afficher la plage. Si vous souhaitez modifier la plage, vous pouvez supprimer et recréer le sous-réseau de passerelle.

- **Type d'adresse IP publique** : dans la plupart des cas, vous voulez utiliser le type d'adresse IP publique De base. Si ce champ n'est pas dans la page du portail, vous avez peut-être sélectionné une référence SKU de passerelle qui pré-sélectionne cette valeur pour vous.

- **Adresse IP publique** : Laissez l'option **Créer** sélectionnée.



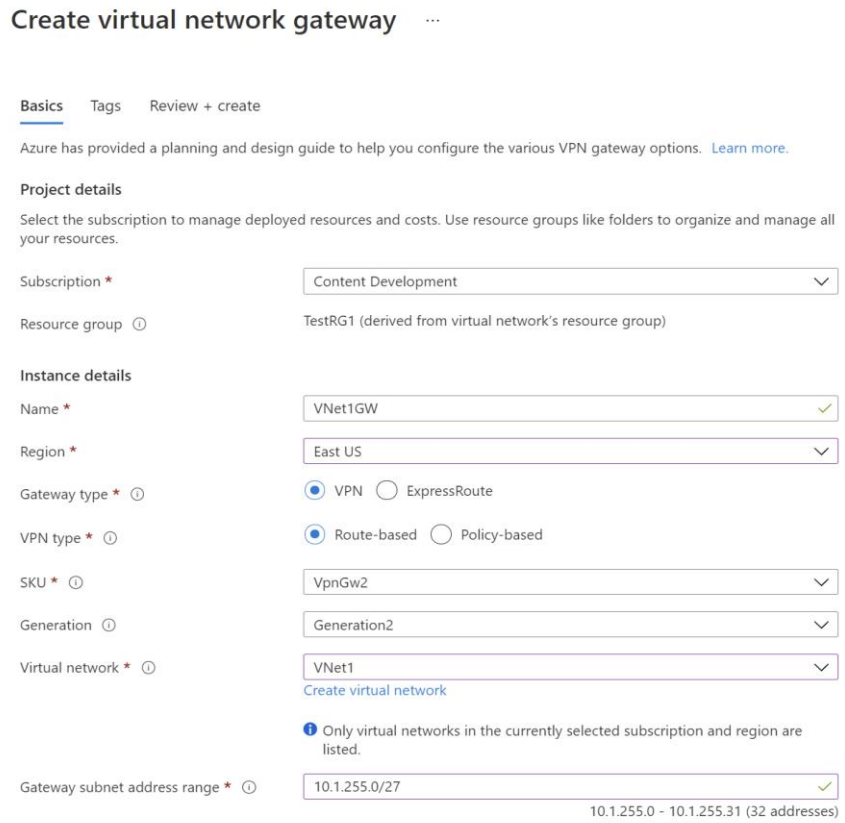
PARTIE 2

Les étapes de création : 2- Créer une passerelle de réseau virtuel

2. Sous l'onglet **Général**, renseignez les valeurs pour **Détails du projet** et **Détails de l'instance**.

- **Plage d'adresses de sous-réseau de la passerelle** : Ce champ apparaît uniquement si votre réseau virtuel n'a pas de sous-réseau de passerelle. Il est préférable de spécifier /27 ou plus grand (/26, /25, etc.). Ceci permet d'obtenir suffisamment d'adresses IP pour les modifications futures, comme l'ajout d'une passerelle ExpressRoute. Nous vous déconseillons de créer une plage inférieure à /28. Si vous disposez déjà d'un sous-réseau de passerelle, vous pouvez en voir les détails en accédant à votre réseau virtuel. Sélectionnez **Sous-réseaux** pour afficher la plage. Si vous souhaitez modifier la plage, vous pouvez supprimer et recréer le sous-réseau de passerelle.

- **Type d'adresse IP publique** : Dans la plupart des cas, vous voulez utiliser le type d'adresse IP publique De base. Si ce champ n'est pas dans la page du portail, vous avez peut-être sélectionné une référence SKU de passerelle qui pré-sélectionne cette valeur pour vous.

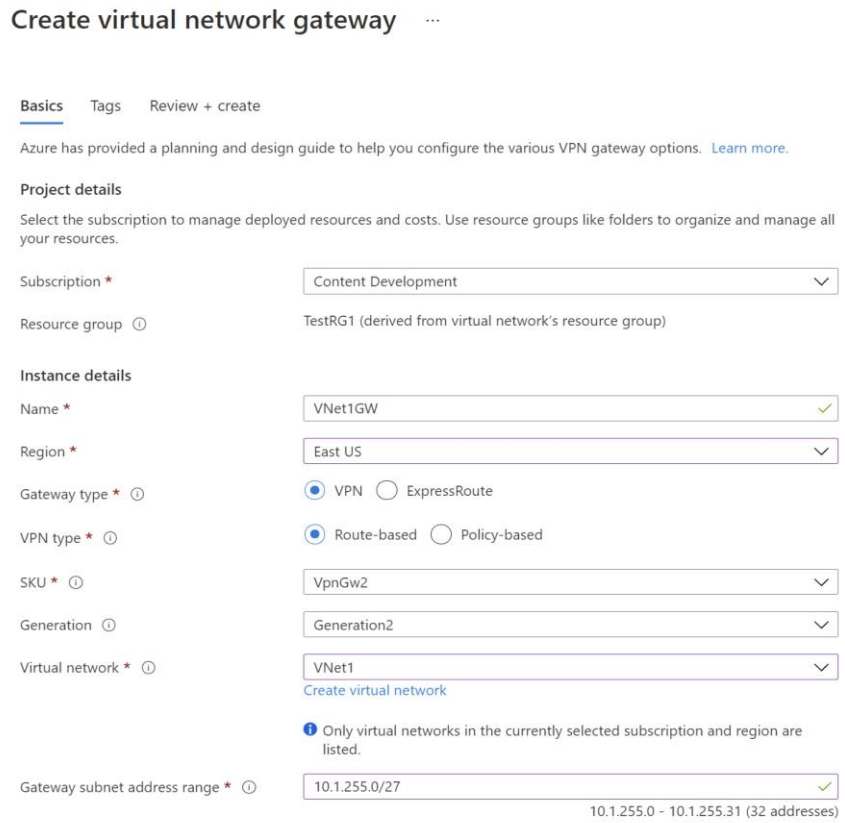


PARTIE 2

Les étapes de création : 2- Créer une passerelle de réseau virtuel

2. Sous l'onglet **Général**, renseignez les valeurs pour **Détails du projet** et **Détails de l'instance**.

- **Adresse IP publique** : Laissez l'option **Créer** sélectionnée.
  - **Nom de l'adresse IP publique** : Dans la zone de texte, tapez un nom pour votre instance d'adresse IP publique.
  - **Référence SKU d'adresse IP publique** : ce champ est contrôlé par le paramètre **Type d'adresse IP publique**.
  - **Attribution** : La passerelle VPN prend en charge seulement le mode dynamique.
  - **Activer le mode actif/actif** : Sélectionnez uniquement **Activer le mode actif/actif** si vous créez une configuration de passerelle active/active. Sinon, laissez ce paramètre **Désactivé**.
  - Laissez l'option **Configurer BGP** définie sur **Désactivé**, sauf si votre configuration exige spécifiquement ce paramètre. Si vous avez besoin de ce paramètre, la valeur par défaut ASN est 65515, même si vous pouvez la changer.

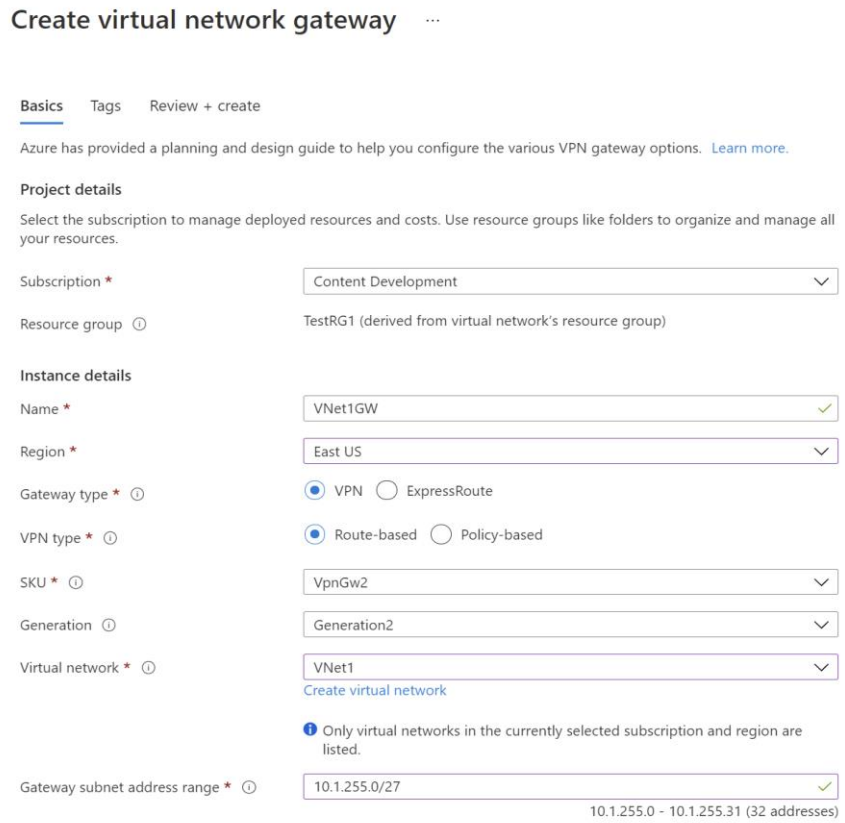


PARTIE 2

Les étapes de création : 2- Créer une passerelle de réseau virtuel

2. Sous l'onglet **Général**, renseignez les valeurs pour **Détails du projet** et **Détails de l'instance**.

- **Nom de l'adresse IP publique** : Dans la zone de texte, tapez un nom pour votre instance d'adresse IP publique.
- **Référence SKU d'adresse IP publique** : Ce champ est contrôlé par le paramètre **Type d'adresse IP publique**.
- **Attribution** : La passerelle VPN prend en charge seulement le mode dynamique.
- **Activer le mode actif/actif** : Sélectionnez uniquement **Activer le mode actif/actif** si vous créez une configuration de passerelle active/active. Sinon, laissez ce paramètre **Désactivé**.
- Laissez l'option **Configurer BGP** définie sur **Désactivé**, sauf si votre configuration exige spécifiquement ce paramètre. Si vous avez besoin de ce paramètre, la valeur par défaut ASN est 65515, même si vous pouvez la changer.

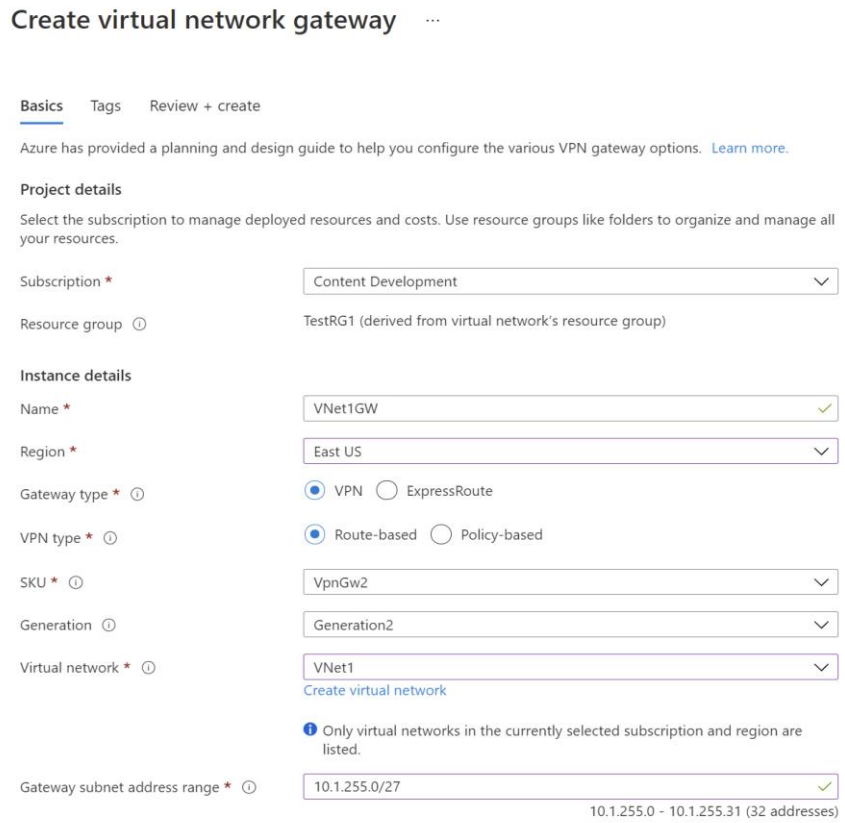


PARTIE 2

Les étapes de création : 2- Créer une passerelle de réseau virtuel

2. Sous l'onglet **Général**, renseignez les valeurs pour **Détails du projet** et **Détails de l'instance**.

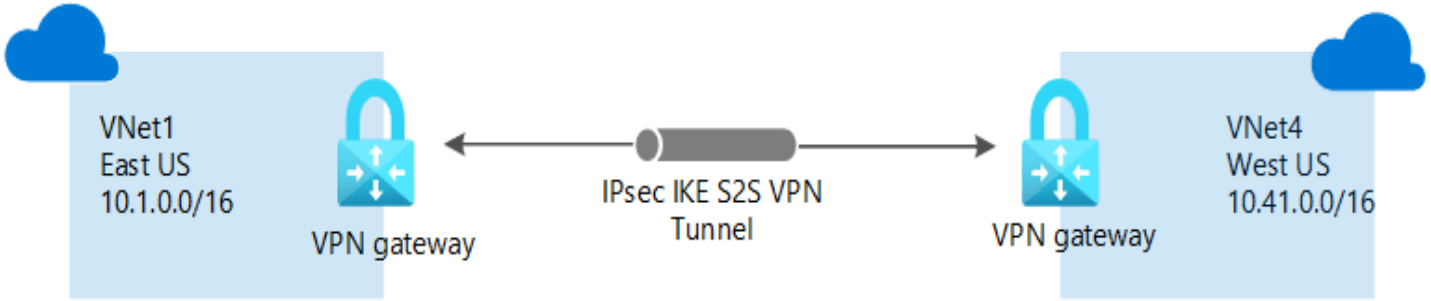
- Sélectionnez **Vérifier + créer** pour exécuter la validation.
- Une fois la validation réussie, sélectionnez **Créer** pour déployer la passerelle VPN.
- Vous pouvez voir l'état du déploiement dans la page Vue d'ensemble pour votre passerelle. La création et le déploiement complets d'une passerelle peuvent prendre 45 minutes ou plus. Une fois la passerelle créée, examinez le réseau virtuel dans le portail pour obtenir l'adresse IP affectée à la passerelle. Cette dernière apparaît sous la forme d'un appareil connecté.



PARTIE 2

Les étapes de création : 3- Créer un réseau virtuel (VNET4)

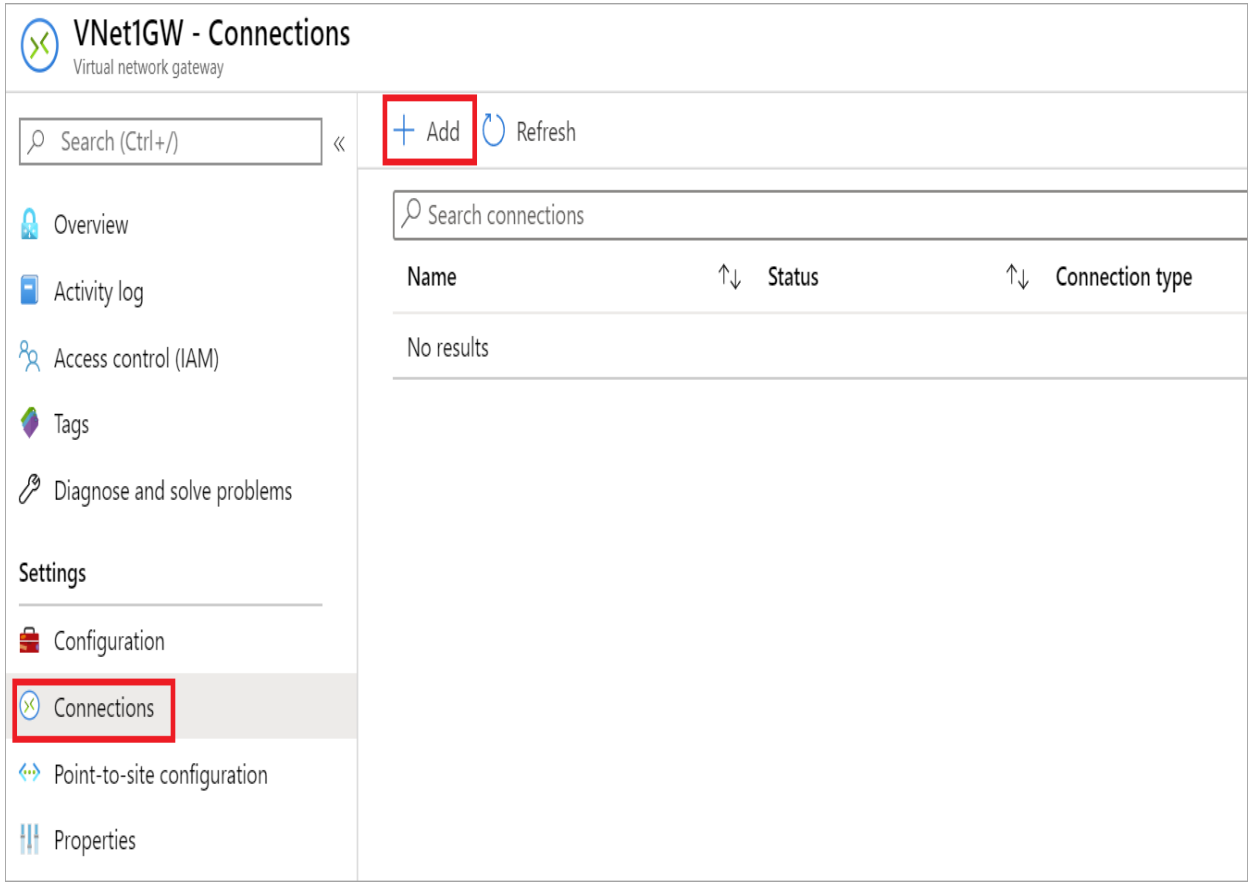
Après avoir configuré VNet1, créez VNet4 et la passerelle VNet4 en répétant les étapes précédentes et en remplaçant les valeurs par les valeurs de VNet4. Vous n'avez pas besoin d'attendre que la création de la passerelle de réseau virtuel pour VNet1 soit terminée pour configurer VNet4. Si vous utilisez vos propres valeurs, assurez-vous que les espaces d'adressage ne chevauchent pas les réseaux virtuels auxquels vous souhaitez vous connecter.



Les étapes de création : 4- Configurer la connexion de passerelle VNet1

Lorsque les passerelles de réseau virtuel pour VNet1 et VNet4 sont terminées, vous pouvez créer vos connexions de passerelle de réseau virtuel. Dans cette section, vous allez créer une connexion de VNet1 à VNet4. Ces étapes s'appliquent uniquement aux réseaux virtuels situés dans le même abonnement. Si vos réseaux virtuels figurent dans des abonnements différents, vous devrez utiliser PowerShell pour établir la connexion. Toutefois, si vos réseaux virtuels se trouvent dans des groupes de ressources différents au sein du même abonnement, vous pouvez les connecter à l'aide du portail.

1. Dans le portail Azure, sélectionnez **Toutes les ressources**, entrez *passerelle de réseau virtuel* dans la recherche de zone, puis accédez à la passerelle de votre réseau virtuel. Par exemple, **VNet1GW**. Sélectionnez la passerelle pour ouvrir la page **Passerelle de réseau virtuel**.
2. Sur la page Passerelle, accédez à **Paramètres - Connexions**. Sélectionnez ensuite **Ajouter**.

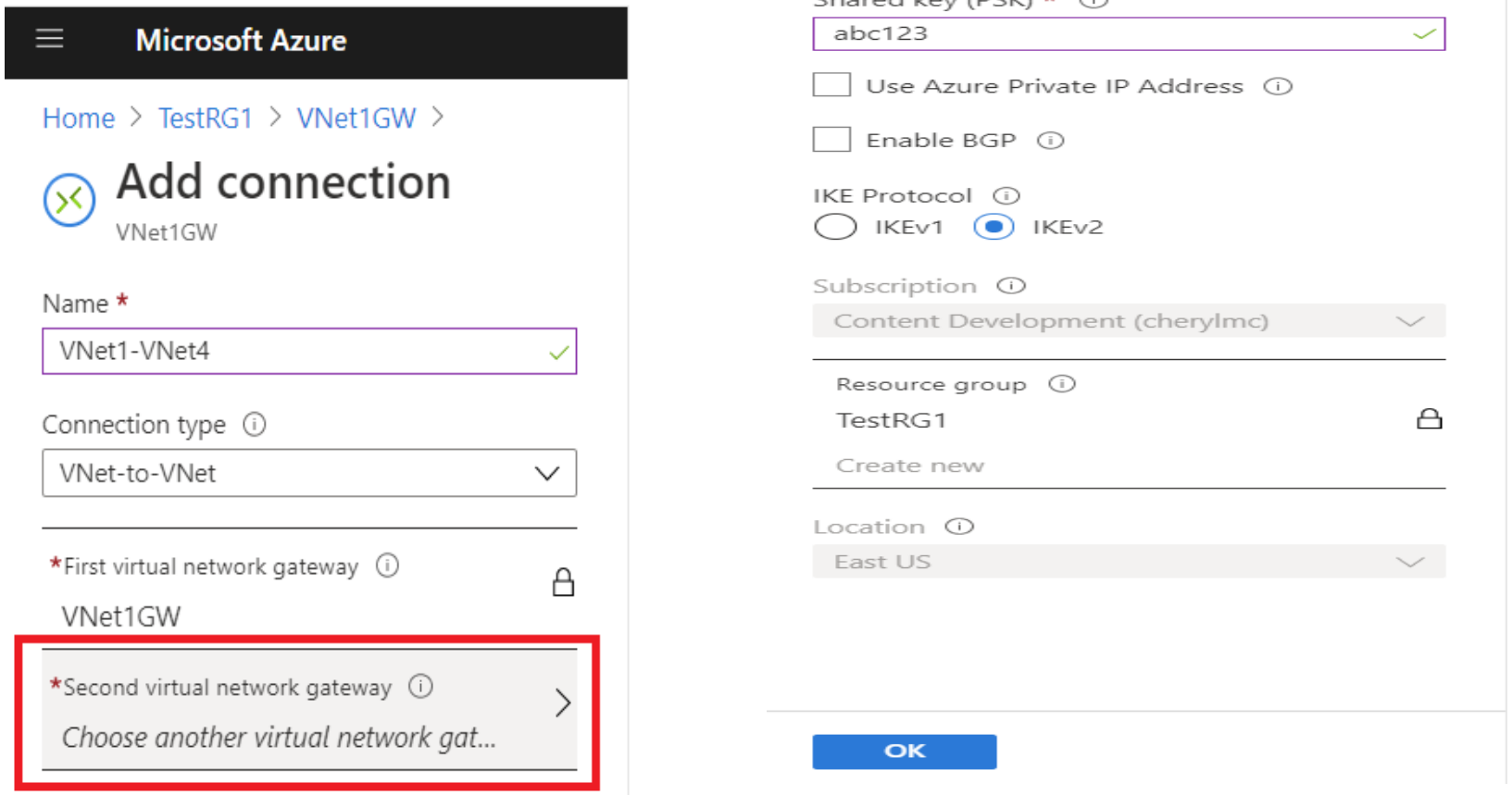


PARTIE 2

PARTIE 2

Les étapes de création : 4- Configurer la connexion de passerelle VNet1

3. La page **Ajouter une connexion** s'ouvre.



Les étapes de création : 4- Configurer la connexion de passerelle VNet1

Sur la page **Ajouter une connexion**, renseignez les valeurs correspondant à votre connexion :

- **Name** : Entrez un nom pour votre connexion. Par exemple, *VNet1toVNet4*.
- **Type de connexion** : Sélectionnez **Réseau virtuel à réseau virtuel** dans la liste déroulante.
- **Première passerelle de réseau virtuel** : La valeur de ce champ est automatiquement renseignée parce que vous créez cette connexion à partir de la passerelle de réseau virtuel spécifiée.
- **Deuxième passerelle de réseau virtuel** : Ce champ correspond à la passerelle de réseau virtuel sur laquelle vous souhaitez créer une connexion. Sélectionnez **Choisir une autre passerelle de réseau virtuel** pour ouvrir la page **Choisir la passerelle de réseau virtuel**.

PARTIE 2

Les étapes de création : 4- Configurer la connexion de passerelle VNet1

- Cette page répertorie les différentes passerelles de réseau virtuel disponibles. Notez que seules les passerelles de réseau virtuel incluses dans votre abonnement sont répertoriées. Si vous souhaitez vous connecter à une passerelle de réseau virtuel qui ne se trouve pas dans votre abonnement, utilisez PowerShell.
- Sélectionnez la passerelle de réseau virtuel à laquelle vous souhaitez vous connecter.
- **Clé partagée** : Dans ce champ, entrez une clé partagée pour votre connexion. Vous pouvez générer ou créer cette clé vous-même. Dans une connexion de site à site, la clé que vous utilisez est exactement la même pour votre appareil local et votre connexion de passerelle de réseau virtuel. Le concept est similaire, sauf qu'au lieu de se connecter à un périphérique VPN, vous vous connectez à une autre passerelle de réseau virtuel.

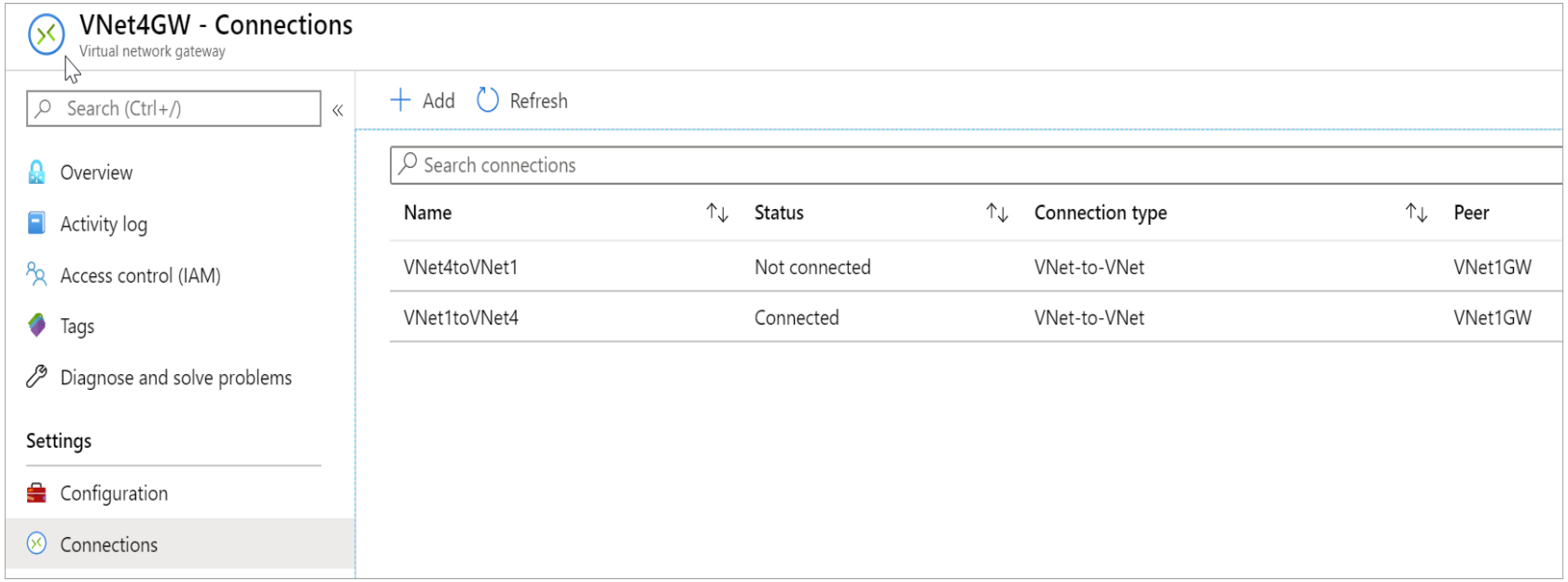
4. Sélectionnez OK pour enregistrer vos modifications.

Configurer la connexion de passerelle VNet4

Créez ensuite une connexion de VNet4 à VNet1. Dans le portail, recherchez la passerelle de réseau virtuel associée à VNet4. Suivez les étapes de la section précédente, en remplaçant les valeurs pour créer une connexion de VNet4 à VNet1. Vérifiez que vous utilisez la même clé partagée.

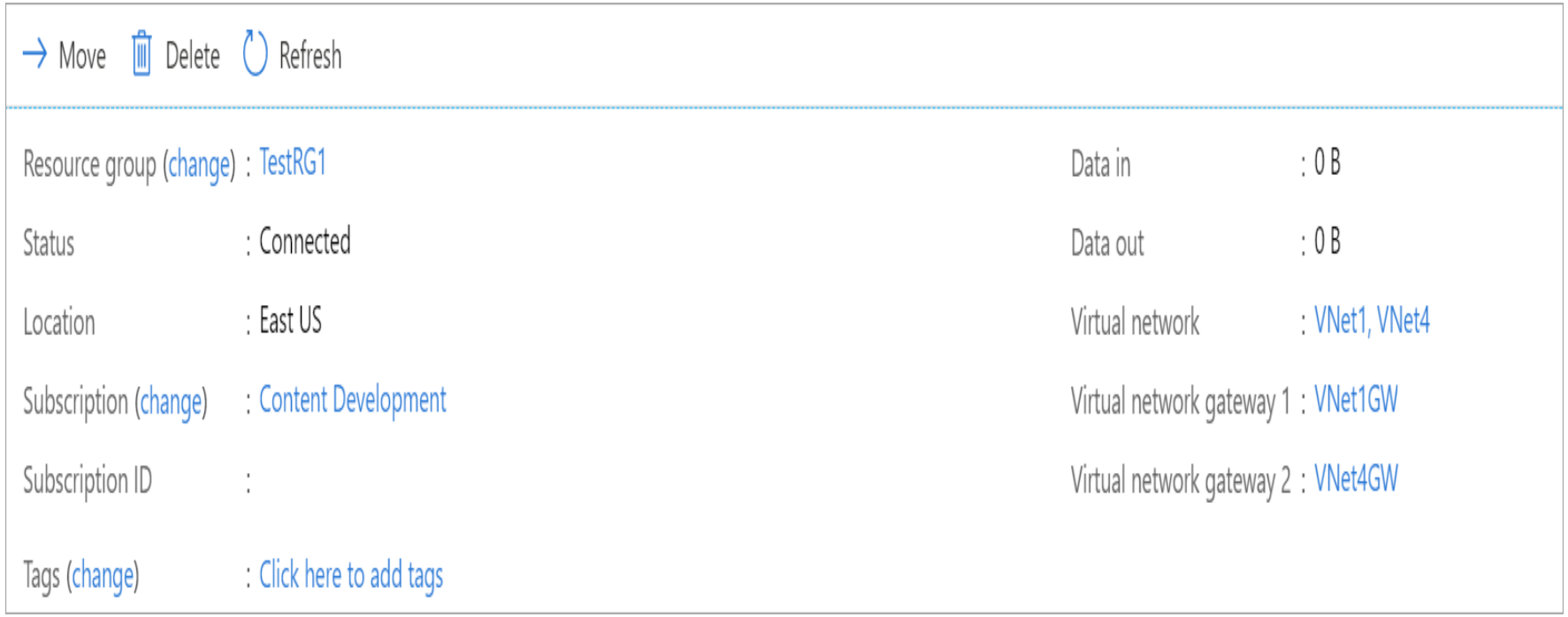
Les étapes de création : 4- Configurer la connexion de passerelle VNet1

1. Recherchez la passerelle de réseau virtuel dans le portail Azure.
2. Sur la page **Passerelle de réseau virtuel**, sélectionnez **Connexion** pour afficher la page **Connexion** de la passerelle de réseau virtuel. Une fois la connexion établie, la valeur d'**État** devient **Connecté**.



Les étapes de création : 4- Configurer la connexion de passerelle VNet1

3. Dans la colonne **Nom**, sélectionnez l'une des connexions pour afficher plus d'informations. Lorsque les données commencent à circuler, des valeurs apparaissent pour **Données entrantes** et **Données sortantes**.



CHAPITRE 1

Explorer les aspects de bases d’un réseau virtuel

1. Espace d’adressage et sous-réseaux
2. IP publique et IP privée
3. Passerelle
4. **Serveurs DNS**

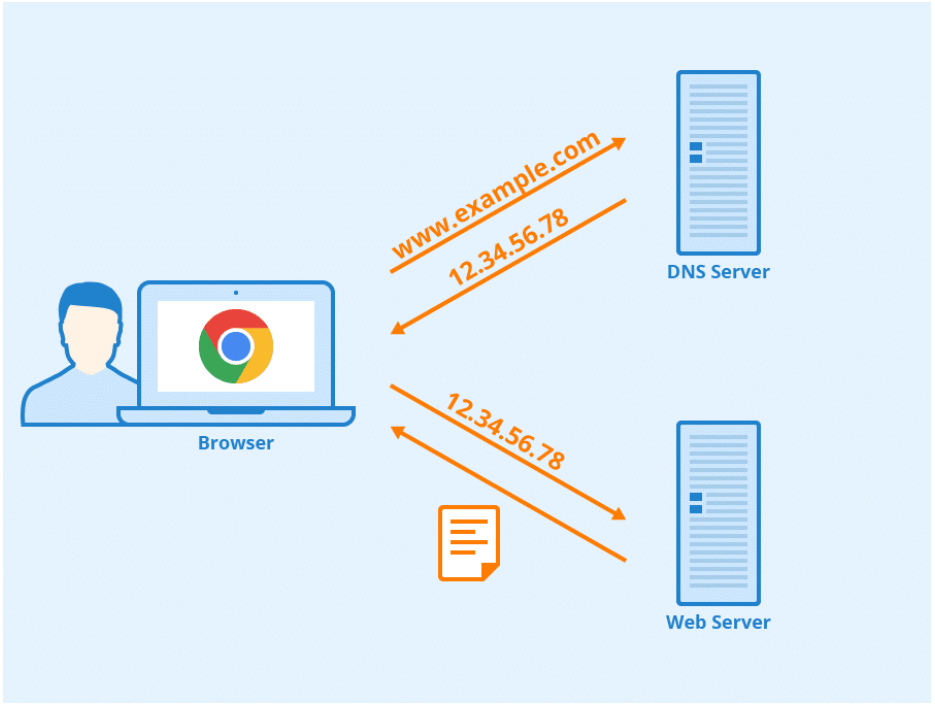
Définition du DNS

Selon la manière dont vous utilisez Azure pour héberger les solutions IaaS, PaaS et les solutions hybrides, vous pouvez être amené à configurer les machines virtuelles et d'autres ressources déployées sur un réseau virtuel pour qu'elles communiquent entre elles. Même si vous pouvez activer la communication par le biais d'adresses IP, il est bien plus simple d'utiliser des noms dont vous vous souviendrez facilement et qui ne seront pas modifiés.

Quand des ressources déployées sur des réseaux virtuels doivent résoudre des noms de domaine en adresses IP internes, elles peuvent utiliser l'une des trois méthodes suivantes :

- Azure DNS Private Zones
- Résolution de noms dans Azure
- Résolution de noms à l'aide de votre propre serveur DNS

  (qui peut rediriger les requêtes vers les serveurs DNS fournis par Azure)



PARTIE 2

Fonctionnalités du DNS

La résolution de noms fournie par Azure présente les avantages suivants :

- Simplicité d'utilisation. Aucune configuration n'est requise.
- Haute disponibilité : Vous n'avez pas besoin de créer et de gérer les clusters de vos propres serveurs DNS.
- Vous pouvez utiliser le service conjointement à vos propres serveurs DNS pour résoudre les noms d'hôte locaux et Azure.
- Vous pouvez utiliser la résolution de noms entre les machines virtuelles et les instances de rôle du même service Cloud, sans qu'un nom de domaine complet soit nécessaire.
- Vous pouvez utiliser la résolution de noms entre les machines virtuelles des réseaux virtuels qui utilisent le modèle de déploiement Azure Resource Manager, sans qu'un nom de domaine complet ne soit nécessaire. Les réseaux virtuels du modèle de déploiement classique nécessitent un nom de domaine complet lors de la résolution de noms dans des services Cloud différents.
- Vous pouvez utiliser des noms d'hôte qui décrivent vos déploiements de façon plus appropriée, au lieu de noms générés automatiquement.

Qu'est-ce qu'Azure DNS Private Resolver ?

Azure DNS Private Resolver est un nouveau service qui vous permet d'interroger des zones privées Azure DNS à partir d'un environnement local, et vice versa, sans déployer de serveurs DNS basés sur des machines virtuelles.

Comment cela fonctionne-t-il ?

Azure DNS Private Resolver nécessite un réseau virtuel Azure. Lorsque vous créez un Azure DNS Private Resolver à l'intérieur d'un réseau virtuel, un ou plusieurs points de terminaison entrants sont établis et peuvent être utilisés comme destination pour les requêtes DNS. Le point de terminaison sortant du résolveur traite les requêtes DNS en fonction d'un ensemble de règles de transfert DNS que vous configurez. Les requêtes DNS lancées dans les réseaux liés à un ensemble de règles peuvent être envoyées à d'autres serveurs DNS.

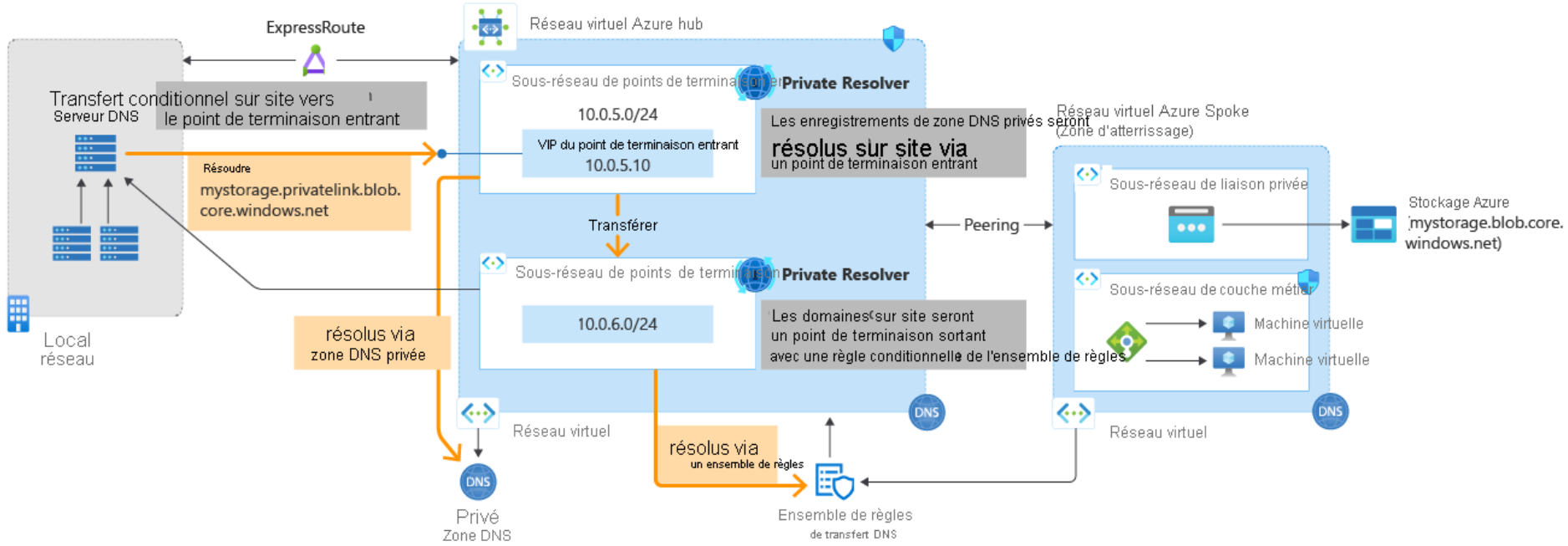
Vous n'avez pas besoin de changer les paramètres de client DNS sur vos machines virtuelles pour utiliser Azure DNS Private Resolver.

Le processus de requête DNS lors de l'utilisation d'Azure DNS Private Resolver est résumé ci-dessous :

- Le client d'un réseau virtuel émet une requête DNS.
- Si les serveurs DNS de ce réseau virtuel sont spécifiés comme personnalisés, la requête est alors transférée aux adresses IP spécifiées.
- Si les serveurs DNS par défaut (fournis par Azure) sont configurés dans le réseau virtuel et qu'il existe des zones DNS privées liées au même réseau virtuel, ces zones sont consultées.
- Si la requête ne correspond pas à une zone DNS privée liée au réseau virtuel, les liens de réseau virtuel pour les ensembles de règles de transfert DNS sont consultés.
- Si aucun lien d'ensemble de règles n'est présent, Azure DNS est utilisé pour résoudre la requête.
- Si des liens d'ensemble de règles sont présents, les règles de transfert DNS sont évaluées.
- Si une correspondance de suffixe est trouvée, la requête est transmise à l'adresse spécifiée.

Qu'est-ce qu'Azure DNS Private Resolver ?

L'architecture d'Azure DNS Private Resolver est résumée dans la figure suivante. La résolution DNS entre les réseaux virtuels Azure et les réseaux locaux nécessite Azure ExpressRoute ou un VPN.



PARTIE 2

CHAPITRE 2

Explorer les aspects avancés d’un réseau virtuel

Ce que vous allez apprendre dans ce chapitre :

- Implémenter l’isolement et la segmentation
- Appliquer les règles de routage et de filtrage du trafic
- Interconnecter des réseaux virtuels
- Assurer la communication avec des ressources locales

4 heures

CHAPITRE 2

Explorer les aspects avancés d’un réseau virtuel

1. **Isolement et segmentation**
2. Routage et filtrage du trafic
3. Interconnexion des réseaux virtuels
4. Communication avec des ressources locales

Les bonnes pratique de l'isolement et la segmentation

Les réseaux virtuels Azure sont similaires aux réseaux LAN de votre réseau local. Un réseau virtuel Azure repose sur un concept, celui de la création d'un réseau basé sur un espace d'adressage IP privé unique, au sein duquel vous pouvez placer toutes vos machines virtuelles Azure. Les espaces d'adressage IP privés disponibles se trouvent dans les plages des classes A (10.0.0.0/8), B (172.16.0.0/12) et C (192.168.0.0/16).

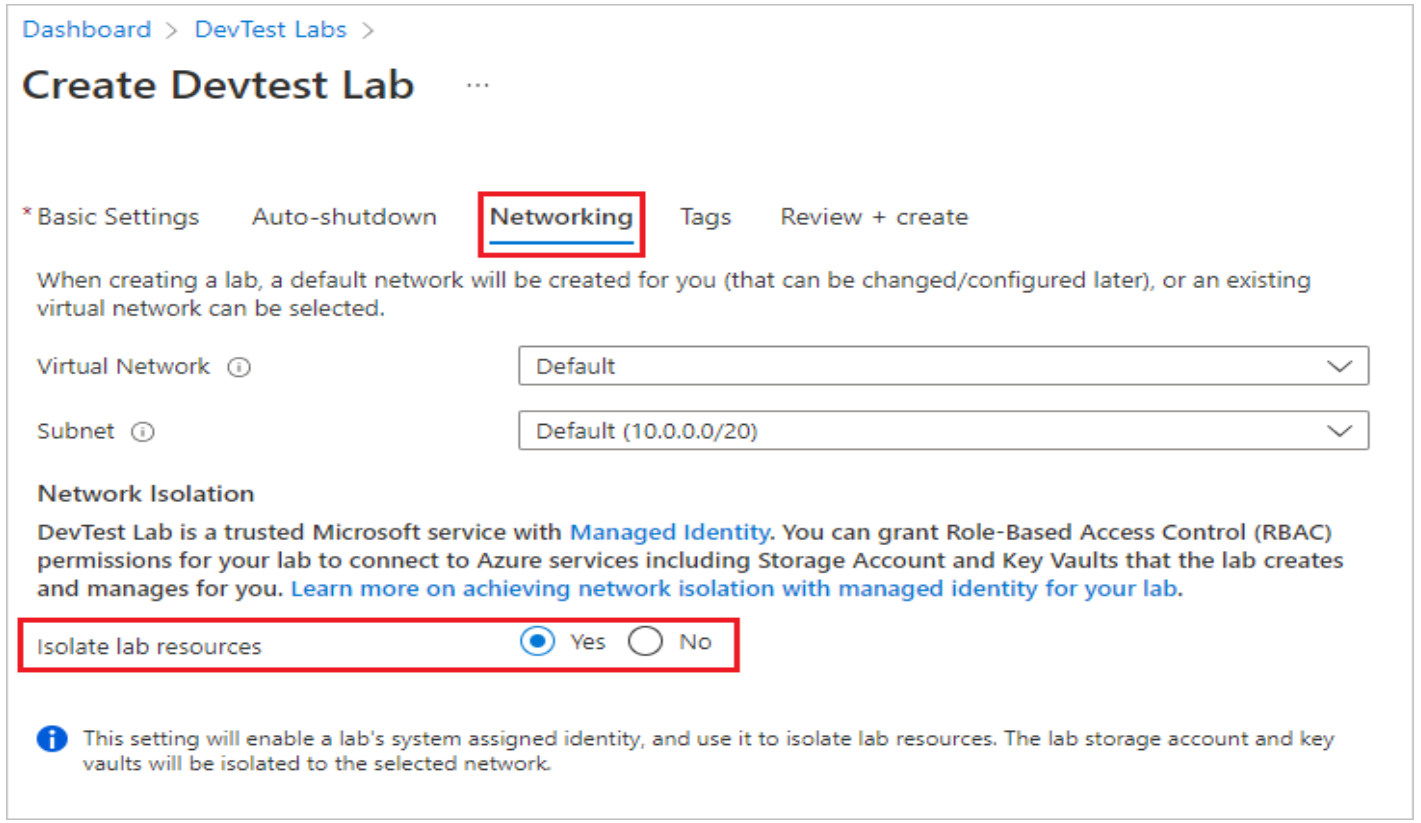
Meilleures pratiques pour segmenter logiquement les sous-réseaux :

- N'attribuez pas de règle d'autorisation avec de larges plages (autorisez, par exemple, de 0.0.0.0 à 255.255.255.255).
  Détail : Assurez-vous que les procédures de résolution des problèmes découragent ou interdisent la configuration de ces types de règles. Ces règles d'autorisation induisent un sentiment de sécurité erroné : elles sont fréquemment trouvées et exploitées par les équipes rouges.
- Segmentez l'espace d'adressage plus volumineux en sous-réseaux.
  Détail : Pour créer vos sous-réseaux, utilisez les principes de création de sous-réseau reposant sur CIDR .
- Créez des contrôles d'accès réseau entre les sous-réseaux. Le routage entre les sous-réseaux se fait automatiquement. Il est donc inutile de configurer manuellement des tables de routage. Par défaut, il n'y a aucun contrôle d'accès réseau entre les sous-réseaux que vous créez sur un réseau virtuel Azure.
  Détail : Utilisez un groupe de sécurité réseau pour vous protéger contre le trafic non sollicité dans les sous-réseaux Azure. Un groupe de sécurité réseau est un simple appareil d'inspection des paquets, avec état, qui applique la méthode basée sur les 5 tuples (adresse IP source, port source, adresse IP de destination, port de destination et protocole de couche 4) pour créer des règles visant à autoriser ou refuser le trafic réseau. Vous pouvez autoriser ou refuser le trafic vers et depuis une ou plusieurs adresses IP, ou entre des sous-réseaux entiers, dans les deux directions.
- Lorsque vous utilisez des groupes de sécurité réseau pour le contrôle d'accès réseau entre les sous-réseaux, vous pouvez placer des ressources appartenant au même rôle ou à la même zone de sécurité dans leurs propres sous-réseaux.

Exemple de service : DevTest Labs

Pour activer l'isolement réseau pour le réseau virtuel et le sous-réseau **par défaut** créés par DevTest Labs pour le labo :

1. Pendant la création du labo, sur l'écran **Créer un labo DevTest**, sélectionnez l'onglet **Mise en réseau**. **(https://docs.microsoft.com/fr-fr/azure/devtest-labs/devtest-lab-create-lab)**
2. En regard d'**isoler les ressources de labo**, sélectionnez **Oui**.
3. Finalisez la création du labo.



Une fois que vous avez créé le labo,

aucune action supplémentaire n'est nécessaire.

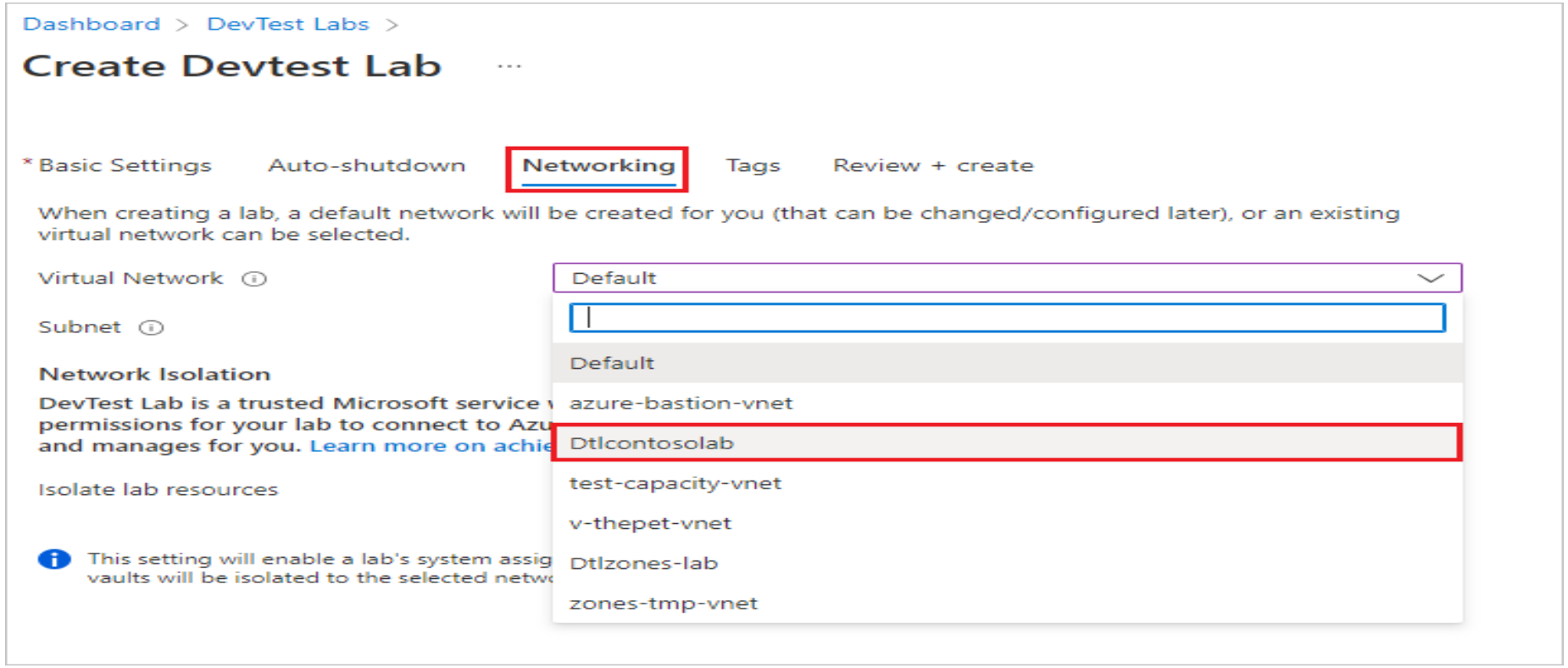
Le labo gère désormais l'isolement des ressources.

PARTIE 2

Exemple de service : DevTest Labs

Pour utiliser un autre réseau virtuel existant pour le labo et activer l'isolement réseau pour ce réseau :

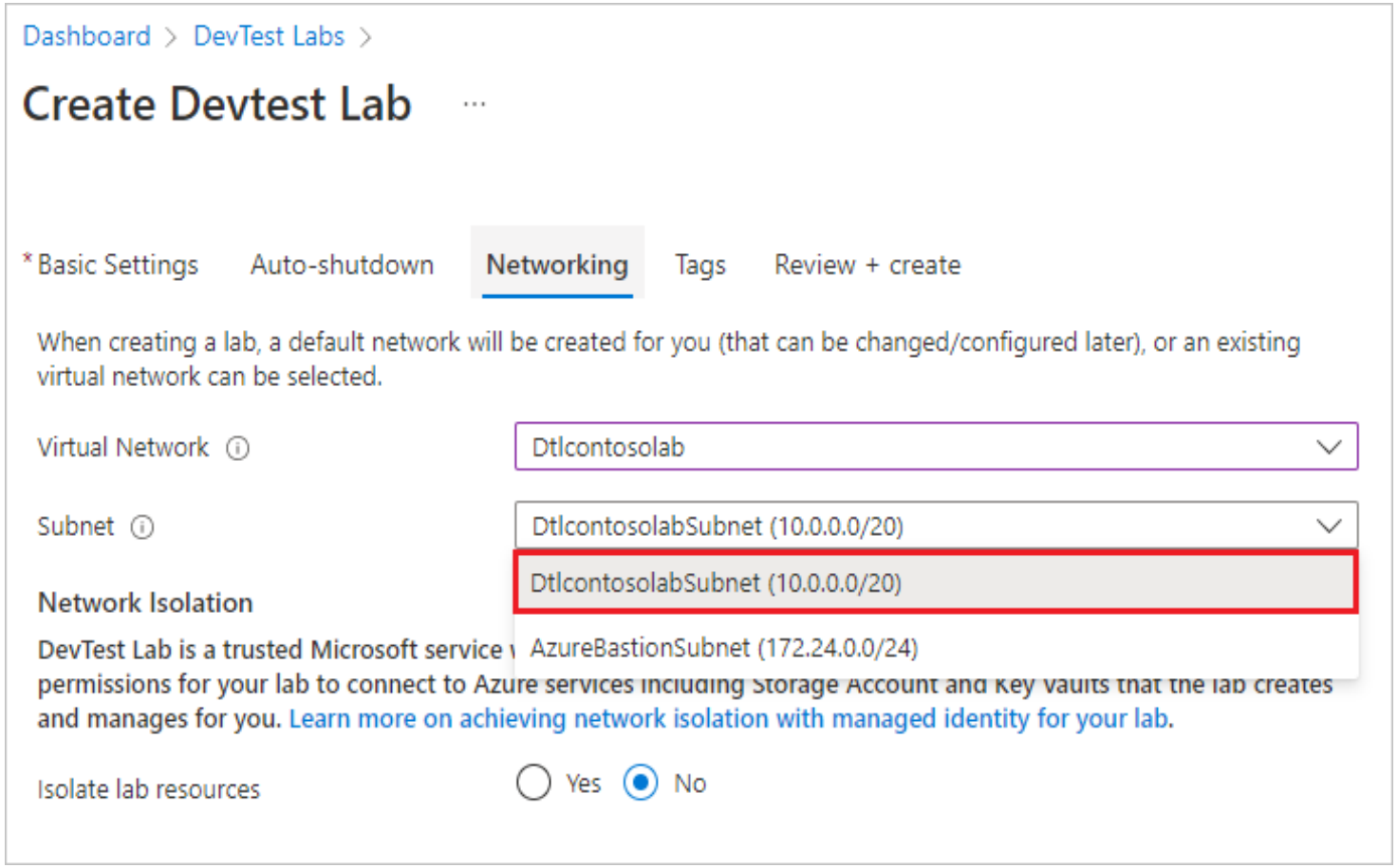
1. Pendant la Création du labo ,(https://docs.microsoft.com/fr-fr/azure/devtest-labs/devtest-lab-create-lab) sous l'onglet **Mise en réseau** de l'écran **Créer un labo DevTest**, sélectionnez un réseau dans la liste déroulante. La liste affiche uniquement les réseaux dans la même région et le même abonnement que le labo.



PARTIE 2

Exemple de service : DevTest Labs

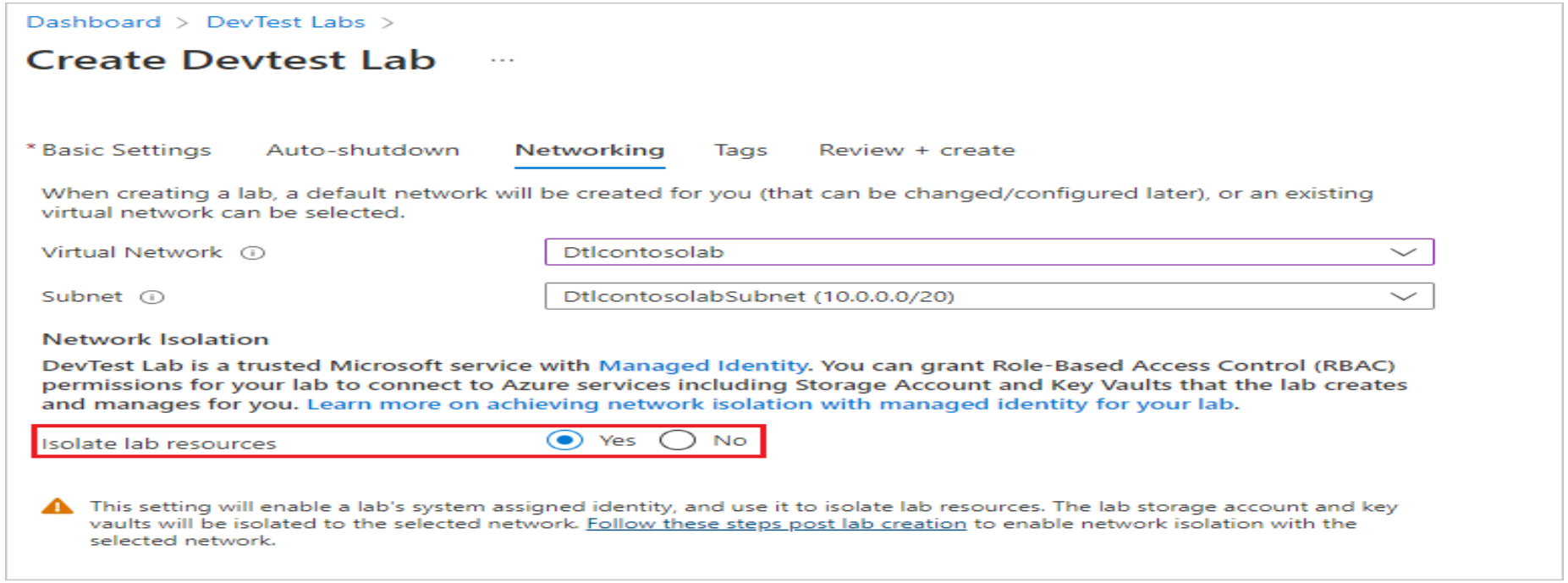
2. Sélectionner un sous-réseau.



PARTIE 2

Exemple de service : DevTest Labs

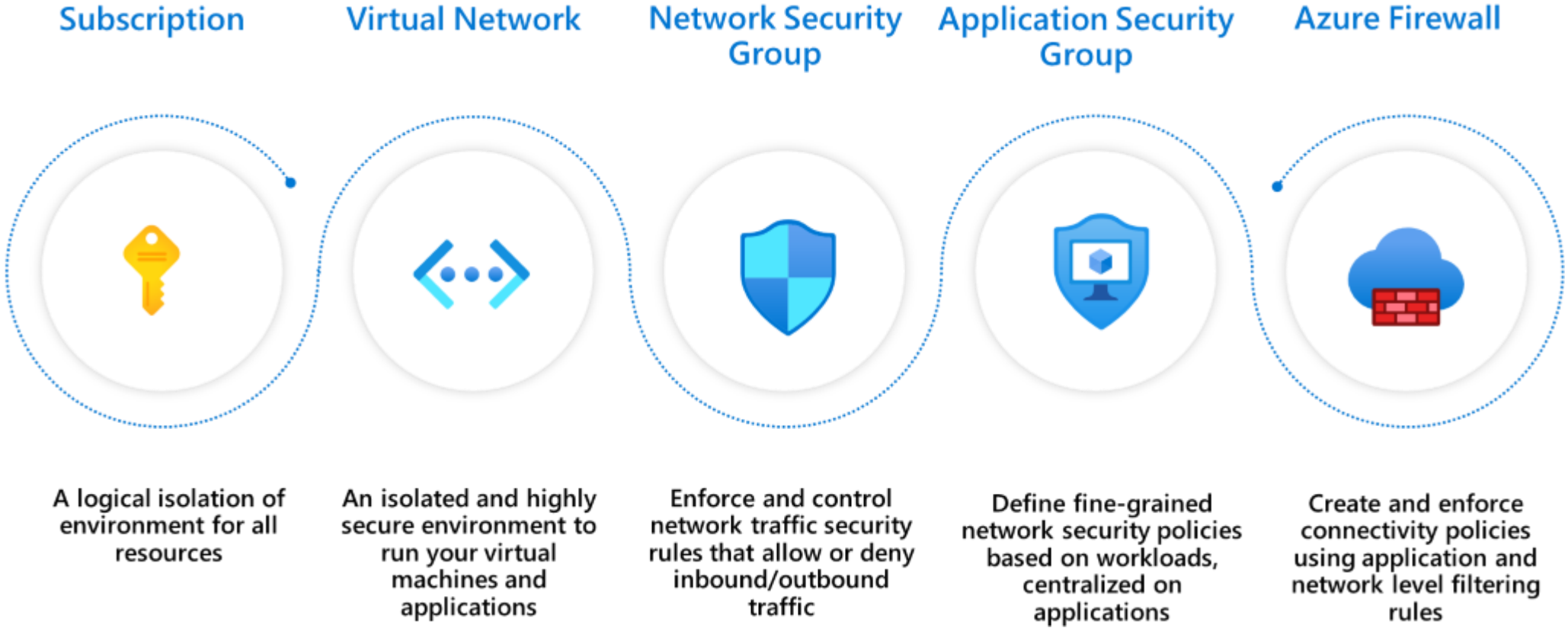
3. En regard d'**isoler les ressources de labo**, sélectionnez **Oui**.



4. Finalisez la création du labo.

PARTIE 2

Fonctionnalités de segmentation Azure



Fonctionnalités de segmentation Azure

1. Abonnement: construction de haut niveau qui fournit une séparation des entités reposant sur une plateforme. Celle-ci est destinée à définir les limites entre les grandes organisations d'une entreprise. En outre, la communication entre les ressources de différents abonnements doit être explicitement provisionnée.
2. Réseau virtuel : créé au sein d'un abonnement dans des espaces d'adressage privés.
   Il fournit aux ressources une autonomie au niveau du réseau. Par défaut, aucun trafic n'est autorisé entre deux réseaux virtuels. Comme les abonnements, toute communication entre les réseaux virtuels doit être approvisionnée de manière explicite.
3. Groupes de sécurité réseau (NSG) : mécanismes de contrôle d'accès permettant de contrôler le trafic entre les ressources au sein d'un réseau virtuel, et également avec les réseaux externes, comme Internet, d'autres réseaux virtuels, etc.
   Les groupes de sécurité réseau permettent une stratégie de segmentation précise, grâce à la création de périmètres pour un sous-réseau, une machine virtuelle ou un groupe de machines virtuelles. Pour plus d'informations sur les opérations qu'il est possible d'effectuer avec les sous-réseaux dans Azure, consultez Sous-réseaux (réseaux virtuels Azure).
4. Groupes de sécurité d'application (ASG) : similaires aux groupes de sécurité réseau, mais référencés avec un contexte d'application. Cela vous permet de regrouper un ensemble de machines virtuelles sous une balise d'application et de définir des règles de trafic qui sont ensuite appliquées à chacune des machines virtuelles sous-jacentes.
5. Pare-feu Azure : pare-feu natif Cloud avec état fourni en tant que service, qui peut être déployé dans un réseau virtuel ou dans des déploiements de hubs Azure Virtual WAN pour le filtrage du trafic entre les ressources Cloud, Internet et locales.
   Vous créez des règles ou des stratégies (à l'aide du Pare-feu Azure ou d'Azure Firewall Manager) en spécifiant l'autorisation/refus du trafic à l'aide des contrôles de couche 3 à 7. Vous pouvez également filtrer le trafic vers Internet en utilisant à la fois Pare-feu Azure et des tiers en dirigeant tout ou partie du trafic via des fournisseurs de sécurité tiers pour le filtrage avancé et la protection des utilisateurs.

CHAPITRE 2

Explorer les aspects avancés d’un réseau virtuel

1. Isolement et la segmentation
2. **Routage et filtrage du trafic**
3. Interconnexion des réseaux virtuels
4. Communication avec des ressources locales

PARTIE 2

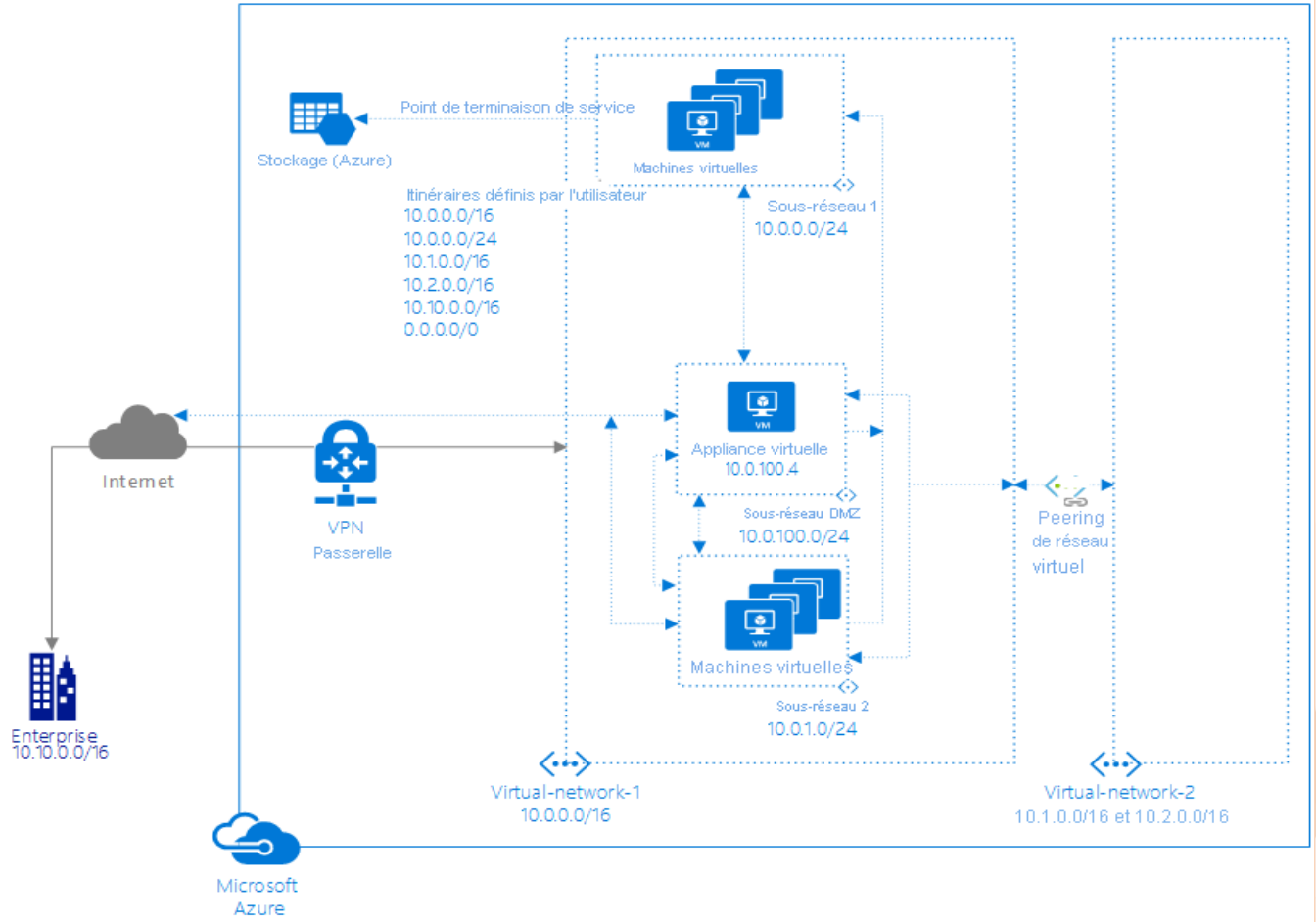
Routage du trafic de réseau virtuel

Azure crée automatiquement une table de routage pour chaque sous-réseau au sein d'un réseau virtuel Azure et y ajoute les itinéraires par défaut du système.

Vous pouvez remplacer certaines des routes système d'Azure par des routes personnalisée, et ajouter d'autres routes personnalisées aux tables de routage.

Azure achemine le trafic sortant à partir d'un sous-réseau selon les itinéraires disponibles dans la table de routage d'un sous-réseau.

L'illustration suivante montre une mise en œuvre du routage du trafic de réseau virtuel.



Source : Microsoft

Routage du trafic du sous-réseau virtuel "sous-réseau1"

La table de routage du *Sous-réseau1* dans l'illustration précédente contient les itinéraires suivants :

id	Source	State	Préfixes d'adresse	Type de tronçon suivant	Adresse IP de tronçon suivant	Nom d'itinéraire défini par l'utilisateur
1	Default	Non valide	10.0.0.0/16	Réseau virtuel		
2	Utilisateur	Actif	10.0.0.0/16	Appliance virtuelle	10.0.100.4	Au sein de VNet1
3	Utilisateur	Actif	10.0.0.0/24	Réseau virtuel		Dans le Sous-réseau1
4	Default	Non valide	10.1.0.0/16	Peering de réseaux virtuels		
5	Default	Non valide	10.2.0.0/16	Peering de réseaux virtuels		
6	Utilisateur	Actif	10.1.0.0/16	None		ToVNet2-1-Drop
7	Utilisateur	Actif	10.2.0.0/16	None		ToVNet2-2-Drop
8	Default	Non valide	10.10.0.0/16	Passerelle de réseau virtuel	[X.X.X.X]	
9	Utilisateur	Actif	10.10.0.0/16	Appliance virtuelle	10.0.100.4	To-On-Prem
10	Default	Actif	[X.X.X.X]	VirtualNetworkServiceEndpoint		
11	Default	Non valide	0.0.0.0/0	Internet		
12	Utilisateur	Actif	0.0.0.0/0	Appliance virtuelle	10.0.100.4	Default-NVA

Routage du trafic du sous-réseau virtuel "sous-réseau1"

Les identificateurs d'itinéraire sont décrits ci-dessous :

- **ID1** : Azure a automatiquement ajouté cette route pour tous les sous-réseaux de *Virtual-network-1*, car 10.0.0.0/16 est la seule plage d'adresses définie dans l'espace d'adressage du réseau virtuel. Si l'itinéraire défini par l'utilisateur dans l'itinéraire ID2 n'a pas été créé, le trafic envoyé vers n'importe quelle adresse entre 10.0.0.1 et 10.0.255.254 est acheminé dans le réseau virtuel, car le préfixe est plus long que 0.0.0.0/0 et ne fait pas partie des préfixes d'adresse de tous les autres itinéraires. Azure change automatiquement l'état de *Actif* à *Non valide*, lorsque ID2, un itinéraire défini par l'utilisateur, est ajouté, car il a le même préfixe que l'itinéraire par défaut, et les itinéraires définis par l'utilisateur substituent les itinéraires par défaut. L'état de cet itinéraire est toujours *Actif* pour le *Sous-réseau2*, car la table de routage à laquelle appartient l'itinéraire défini par l'utilisateur, ID2, n'est pas associée au *Sous-réseau2*.

id	Source	State	Préfixes d'adresse	Type de tronçon suivant	Adresse IP de tronçon suivant	Nom d'itinéraire défini par l'utilisateur
1	Default	Non valide	10.0.0.0/16	Réseau virtuel		

Routage du trafic du sous-réseau virtuel "sous-réseau1"

Les identificateurs d'itinéraire sont décrits ci-dessous :

- **ID2** : Azure a ajouté cette route quand une route définie par l'utilisateur pour le préfixe d'adresse 10.0.0.0/16 a été associée au sous réseau Subnet1 du réseau virtuel Virtual-network-1. L'itinéraire défini par l'utilisateur spécifie 10.0.100.4 comme l'adresse IP de l'appliance virtuelle, car cette adresse est l'adresse IP privée affectée à la machine virtuelle de l'appliance virtuelle. La table de routage à laquelle cette route appartient n'est pas associée à Subnet2 et n'apparaît donc pas dans la table de routage de Subnet2. Cet itinéraire remplace l'itinéraire par défaut pour le préfixe 10.0.0.0/16 (ID1), qui a automatiquement acheminé le trafic adressé à 10.0.0.1 et à 10.0.255.254 dans le réseau virtuel via le type de tronçon suivant de réseau virtuel. Cet itinéraire existe afin de forcer tout le trafic sortant à traverser une appliance virtuelle.

id	Source	State	Préfixes d'adresse	Type de tronçon suivant	Adresse IP de tronçon suivant	Nom d'itinéraire défini par l'utilisateur
2	Utilisateur	Actif	10.0.0.0/16	Appliance virtuelle	10.0.100.4	Au sein de VNet1

Routage du trafic du sous-réseau virtuel "sous-réseau1"

Les identificateurs d'itinéraire sont décrits ci-dessous :

- **ID3** : Azure a ajouté cette route quand une route définie par l'utilisateur pour le préfixe d'adresse 10.0.0.0/24 a été associée au sous-réseau *Subnet1*. Le trafic destiné aux adresses comprises entre 10.0.0.1 et 10.0.0.254 reste dans le sous-réseau, au lieu d'être acheminé vers l'appliance virtuelle spécifiée dans la règle précédente (ID2), car il a un préfixe plus long que l'itinéraire ID2. Cette route n'a pas été associée à *Subnet2* et n'apparaît donc pas dans la table de routage de *Subnet2*. Cet itinéraire substitue efficacement l'itinéraire ID2 pour le trafic au sein du *Sous-réseau1*.

id	Source	State	Préfixes d'adresse	Type de tronçon suivant	Adresse IP de tronçon suivant	Nom d'itinéraire défini par l'utilisateur
3	Utilisateur	Actif	10.0.0.0/24	Réseau virtuel		Dans le Sous-réseau1

Routage du trafic du sous-réseau virtuel "sous-réseau1"

Les identificateurs d'itinéraire sont décrits ci-dessous :

- **ID4** : Azure a ajouté automatiquement les routes dans les ID 4 et 5 de tous les sous-réseaux de *Virtual-network-1* quand le réseau virtuel a été appairé avec *Virtual-network-2*. *Virtual-network-2* possède deux plages d'adresses dans son espace d'adressage : 10.1.0.0/16 et 10.2.0.0/16 ; Azure a donc ajouté une route pour chaque plage. Si les itinéraires définis par l'utilisateur dans l'itinéraire ID 6 et 7 n'ont pas été créés, le trafic envoyé vers n'importe quelle adresse entre 10.1.0.1-10.1.255.254 et 10.2.0.1-10.2.255.254 serait acheminé vers le réseau virtuel homologué, car le préfixe est plus long que 0.0.0.0/0 et ne fait pas partie des préfixes d'adresse de tous les autres itinéraires. Azure a automatiquement changé l'état de *Actif* à *Non valide* lorsque les itinéraires dans ID 6 et 7 ont été ajoutés, car ils ont les mêmes préfixes que les itinéraires dans ID 4 et 5 et les itinéraires définis par l'utilisateur substituent les itinéraires par défaut. L'état des itinéraires dans ID 4 et 5 est toujours *Actif* pour le *Sous-réseau2*, car la table de routage à laquelle appartiennent les itinéraires définis par l'utilisateur dans ID 6 et 7 n'est pas associée au *Sous-réseau2*.

id	Source	State	Préfixes d'adresse	Type de tronçon suivant	Adresse IP de tronçon suivant	Nom d'itinéraire défini par l'utilisateur
4	Default	Non valide	10.1.0.0/16	Peering de réseaux virtuels		

PARTIE 2

Routage du trafic du sous-réseau virtuel "sous-réseau1"

Les identificateurs d'itinéraire sont décrits ci-dessous :

- **ID5** : Même explication que pour ID4.

id	Source	State	Préfixes d'adresse	Type de tronçon suivant	Adresse IP de tronçon suivant	Nom d'itinéraire défini par l'utilisateur
5	Default	Non valide	10.2.0.0/16	Peering de réseaux virtuels		

Routage du trafic du sous-réseau virtuel "sous-réseau1"

Les identificateurs d'itinéraire sont décrits ci-dessous :

- **ID6** : Azure a ajouté cette route et la route dans ID7, quand des routes définies par l'utilisateur pour les préfixes d'adresse 10.1.0.0/16 et 10.2.0.0/16 ont été associées au sous-réseau *Subnet1*. Le trafic destiné aux adresses comprises entre 10.1.0.1 et 10.1.255.254 et entre 10.2.0.1 et 10.2.255.254 est supprimé par Azure au lieu d'être acheminé vers le réseau virtuel homologué, car les itinéraires définis par l'utilisateur remplacent les itinéraires par défaut. Les routes ne sont pas associées à *Subnet2* et n'apparaissent donc pas dans la table de routage de *Subnet2*. Les itinéraires remplacent les itinéraires ID4 et ID5 pour le trafic sortant du *Sous-réseau1*. Les itinéraires ID6 et ID7 existent afin de supprimer le trafic destiné à l'autre réseau virtuel.

id	Source	State	Préfixes d'adresse	Type de tronçon suivant	Adresse IP de tronçon suivant	Nom d'itinéraire défini par l'utilisateur
6	Utilisateur	Actif	10.1.0.0/16	None		ToVNet2-1-Drop

Routage du trafic du sous-réseau virtuel "sous-réseau1"

Les identificateurs d'itinéraire sont décrits ci-dessous :

- **ID7** : Même explication que pour ID6.

id	Source	State	Préfixes d'adresse	Type de tronçon suivant	Adresse IP de tronçon suivant	Nom d'itinéraire défini par l'utilisateur
7	Utilisateur	Actif	10.2.0.0/16	None		ToVNet2-2-Drop

Routage du trafic du sous-réseau virtuel "sous-réseau1"

Les identificateurs d'itinéraire sont décrits ci-dessous :

- **ID8** : Azure a ajouté automatiquement cette route pour tous les sous-réseaux de *Virtual-network-1* lorsqu'une passerelle de réseau virtuel de type VPN a été créée au sein du réseau virtuel. Azure a ajouté l'adresse IP publique de la passerelle de réseau virtuel à la table de routage. Le trafic envoyé vers n'importe quelle adresse entre 10.10.0.1 et 10.10.255.254 est acheminé vers la passerelle de réseau virtuel. Le préfixe est plus long que 0.0.0.0/0 et ne fait pas partie des préfixes d'adresse des autres itinéraires.

id	Source	State	Préfixes d'adresse	Type de tronçon suivant	Adresse IP de tronçon suivant	Nom d'itinéraire défini par l'utilisateur
8	Default	Non valide	10.10.0.0/16	Passerelle de réseau virtuel	[X.X.X.X]	

Routage du trafic du sous-réseau virtuel "sous-réseau1"

Les identificateurs d'itinéraire sont décrits ci-dessous :

- **ID9** : Azure a ajouté cette route quand une route définie par l'utilisateur pour le préfixe d'adresse 10.10.0.0/16 a été ajoutée à la table de routage associée à *Subnet1*. Cet itinéraire remplace ID8. L'itinéraire envoie tout le trafic destiné au réseau local à une NVA pour inspection, plutôt que d'acheminer le trafic directement sur site.

id	Source	State	Préfixes d'adresse	Type de tronçon suivant	Adresse IP de tronçon suivant	Nom d'itinéraire défini par l'utilisateur
9	Utilisateur	Actif	10.10.0.0/16	Appliance virtuelle	10.0.100.4	To-On-Prem

Routage du trafic du sous-réseau virtuel "sous-réseau1"

Les identificateurs d'itinéraire sont décrits ci-dessous :

- **ID10** : Azure a ajouté automatiquement cette route au sous-réseau lorsqu'un point de terminaison de service pour un service Azure a été activé pour le sous-réseau. Azure achemine le trafic à partir du sous-réseau vers une adresse IP publique du service, sur le réseau d'infrastructure Azure. Le préfixe est plus long que 0.0.0.0/0 et ne fait pas partie des préfixes d'adresse des autres itinéraires. Un point de terminaison de service a été créé afin de permettre au trafic destiné au stockage Azure de circuler directement vers le stockage Azure.

id	Source	State	Préfixes d'adresse	Type de tronçon suivant	Adresse IP de tronçon suivant	Nom d'itinéraire défini par l'utilisateur
10	Default	Actif	[X.X.X.X]	VirtualNetworkServiceEndpoint		

Routage du trafic du sous-réseau virtuel "sous-réseau1"

Les identificateurs d'itinéraire sont décrits ci-dessous :

- **ID11:** : Azure a automatiquement ajouté cette route à la table de routage de tous les sous-réseaux de *Virtual-network-1* et de *Virtual-network-2*. Le préfixe d'adresse 0.0.0.0/0 est le préfixe le plus court. Tout le trafic envoyé à des adresses avec un plus long préfixe d'adresse est routé en fonction d'autres itinéraires. Par défaut, Azure achemine tout le trafic destiné aux adresses autres que les adresses spécifiées dans l'un des autres itinéraires vers Internet. Azure a automatiquement changé l'état de *Actif* à *Non valide* pour le *Sous-réseaut1* lorsqu'un itinéraire défini par l'utilisateur pour le préfixe d'adresse 0.0.0.0/0 (ID12) a été associé au sous-réseau. L'état de cet itinéraire est toujours *Actif* pour tous les autres sous-réseaux dans les deux réseaux virtuels, car l'itinéraire n'est associé à aucun autre sous-réseau au sein de tout autre réseau virtuel.

id	Source	State	Préfixes d'adresse	Type de tronçon suivant	Adresse IP de tronçon suivant	Nom d'itinéraire défini par l'utilisateur
11	Default	Non valide	0.0.0.0/0	Internet		

Routage du trafic du sous-réseau virtuel "sous-réseau1"

Les identificateurs d'itinéraire sont décrits ci-dessous :

- **ID12** :Azure a ajouté cette route quand une route définie par l'utilisateur pour le préfixe d'adresse 0.0.0.0/0 a été associée à *Subnet1*. L'itinéraire défini par l'utilisateur spécifie 10.0.100.4 comme l'adresse IP de l'appliance virtuelle. Cette route n'est pas associée à *Subnet2* et n'apparaît donc pas dans la table de routage de *Subnet2*. Tout le trafic destiné à toute adresse qui n'est pas incluse dans les préfixes d'adresse de tout autre itinéraire est envoyé à l'appliance virtu elle. L'ajout de cet itinéraire a changé l'état de l'itinéraire par défaut pour le préfixe d'adresse 0.0.0.0/0 (ID11) de *Actif* à *Non valide* pour le *Sous-réseau1*, car un itinéraire défini par l'utilisateur remplace un itinéraire par défaut.

id	Source	State	Préfixes d'adresse	Type de tronçon suivant	Adresse IP de tronçon suivant	Nom d'itinéraire défini par l'utilisateur
12	Utilisateur	Actif	0.0.0.0/0	Appliance virtuelle	10.0.100.4	Default-NVA

Routage du trafic du sous-réseau virtuel "sous-réseau1"

La table de routage du *Sous-réseau2* dans l'image contient les itinéraires suivants :

Source	State	Préfixes d'adresse	Type de tronçon suivant	Adresse IP de tronçon suivant
Default	Actif	10.0.0.0/16	Réseau virtuel	
Default	Actif	10.1.0.0/16	Peering de réseaux virtuels	
Default	Actif	10.2.0.0/16	Peering de réseaux virtuels	
Default	Actif	10.10.0.0/16	Passerelle de réseau virtuel	[X.X.X.X]
Default	Actif	0.0.0.0/0	Internet	
Default	Actif	10.0.0.0/8	None	
Default	Actif	100.64.0.0/10	None	
Default	Actif	192.168.0.0/16	None	

La table de routage du *Sous-réseau2* contient tous les itinéraires par défaut créés par Azure et les itinéraires facultatifs de peering de réseau virtuel et de passerelle de réseau virtuel. Azure a ajouté les itinéraires facultatifs à tous les sous-réseaux du réseau virtuel lorsque la passerelle et le peering ont été ajoutés au réseau virtuel. Azure a supprimé les itinéraires pour les préfixes d'adresse 10.0.0.0/8, 192.168.0.0/16 et 100.64.0.0/10 de la table de routage de *Subnet1* lorsque l'itinéraire défini par l'utilisateur pour le préfixe d'adresse 0.0.0.0/0 a été ajouté à *Subnet1*.

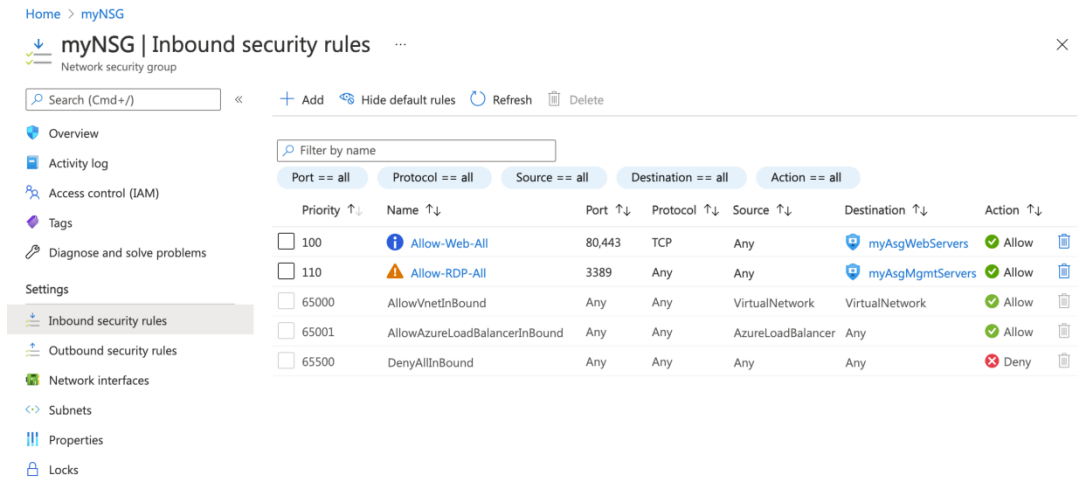
Routage du trafic du sous-réseau virtuel "sous-réseau1"

Vous pouvez filtrer le trafic réseau entrant dans un sous-réseau avec un groupe de sécurité reseau (NSG).

Les groupes de sécurité réseau contiennent des règles de sécurité qui filtrent le trafic réseau par adresse IP, port et protocole. Les règles de sécurité sont appliquées aux ressources déployées dans un sous-réseau.

Dans ce qui suit on va suivre les étapes suivantes:

1. Créer un groupe de sécurité réseau et les règles associées
2. Créer un réseau virtuel et associer un groupe de sécurité réseau à un sous-réseau
3. Déployer des machines virtuelles dans un sous-réseau
4. Tester les filtres de trafic



PARTIE 2

Filtrage du trafic

Sur Azure, on peut utiliser un groupe de sécurité réseau pour filtrer le trafic réseau sortant et entrant respectivement à destination et en provenance de ressources Azure dans un réseau virtuel Azure.

Les groupes de sécurité réseau contiennent des règles de sécurité qui filtrent le trafic réseau par adresse IP, port et protocole. Quand un groupe de sécurité réseau est associé à un sous-réseau, des règles de sécurité sont appliquées aux ressources déployées dans ce sous-réseau.

Dans ce qui suit, on va suivre les étapes suivantes pour le filtrage du trafic de réseau virtuel avec NSG :

1. Créer un groupe de sécurité réseau et les règles associées
2. Créer des groupes de sécurité d'application
3. Créer un réseau virtuel et associer un groupe de sécurité réseau à un sous-réseau
4. Déployer des machines virtuelles et associer leurs interfaces réseau aux groupes de sécurité d'application
5. Tester les filtres de trafic

Filtrage du trafic de réseau virtuel avec NSG : 1- Créer un NSG

L'exemple suivant crée un groupe de ressources dans l'emplacement *eastus* :

Azure PowerShell — Copier — Essayer

```
New-AzResourceGroup -ResourceGroupName myResourceGroup -Location EastUS
```

L'exemple suivant crée deux groupes de sécurité d'application :

Azure PowerShell

```
$webAsg = New-AzApplicationSecurityGroup `
  -ResourceGroupName myResourceGroup `
  -Name myAsgWebServers `
  -Location eastus

$mgmtAsg = New-AzApplicationSecurityGroup `
  -ResourceGroupName myResourceGroup `
  -Name myAsgMgmtServers `
  -Location eastus
```

Filtrage du trafic de réseau virtuel avec NSG : 1- Créer un NSG

Créer des règles de sécurité

L'exemple suivant crée une règle qui autorise le trafic entrant à partir d'Internet vers le groupe de sécurité d'application *myWebServers* par les ports 80 et 443 :

```
$webRule = New-AzNetworkSecurityRuleConfig `
  -Name "Allow-Web-All" `
  -Access Allow `
  -Protocol Tcp `
  -Direction Inbound `
  -Priority 100 `
  -SourceAddressPrefix Internet `
  -SourcePortRange * `
  -DestinationApplicationSecurityGroupId $webAsg.id `
  -DestinationPortRange 80,443
```

L'exemple suivant crée une règle qui autorise le trafic entrant depuis Internet vers le groupe de sécurité d'application *myMgmtServers* via le port 3389 :

```
$mgmtRule = New-AzNetworkSecurityRuleConfig `
  -Name "Allow-RDP-All" `
  -Access Allow `
  -Protocol Tcp `
  -Direction Inbound `
  -Priority 110 `
  -SourceAddressPrefix Internet `
  -SourcePortRange * `
  -DestinationApplicationSecurityGroupId $mgmtAsg.id `
  -DestinationPortRange 3389
```

Filtrage du trafic de réseau virtuel avec NSG : 2- Associer le NSG à un sous-réseau

L'exemple suivant crée un réseau virtuel nommé *myVirtualNetwork* :

Azure PowerShell

```
$virtualNetwork = New-AzVirtualNetwork `
  -ResourceGroupName myResourceGroup `
  -Location EastUS `
  -Name myVirtualNetwork `
  -AddressPrefix 10.0.0.0/16
```

L'exemple suivant ajoute un sous-réseau nommé *mySubnet* au réseau virtuel et l'associe au groupe de sécurité réseau *myNsg* :

Azure PowerShell

```
Add-AzVirtualNetworkSubnetConfig `
  -Name mySubnet `
  -VirtualNetwork $virtualNetwork `
  -AddressPrefix "10.0.2.0/24" `
  -NetworkSecurityGroup $nsg
$virtualNetwork | Set-AzVirtualNetwork
```

Filtrage du trafic de réseau virtuel avec NSG : 3- Déployer des machines virtuelles dans le sous-réseau

Avant de créer les machines virtuelles, récupérez l'objet de réseau virtuel avec le sous-réseau à l'aide de la commande

Get-AzVirtualNetwork :

PowerShell

```
$virtualNetwork = Get-AzVirtualNetwork `
 -Name myVirtualNetwork `
 -Resourcegroupname myResourceGroup
```

Créez une adresse IP publique pour chaque machine virtuelle avec (**https://docs.microsoft.com/fr-fr/powershell/module/az.network/new-azpublicipaddress?view=azps-8.2.0**) :

PowerShell

```
$publicIpWeb = New-AzPublicIpAddress `
  -AllocationMethod Dynamic `
  -ResourceGroupName myResourceGroup `
  -Location eastus `
  -Name myVmWeb

$publicIpMgmt = New-AzPublicIpAddress `
  -AllocationMethod Dynamic `
  -ResourceGroupName myResourceGroup `
  -Location eastus `
  -Name myVmMgmt
```

Filtrage du trafic de réseau virtuel avec NSG : 3- Déployer des machines virtuelles dans le sous-réseau

Créez deux interfaces réseau

L'exemple suivant crée une interface réseau, lui associe l'adresse IP publique *myVmWeb* et la rend membre du groupe de sécurité d'application *myAsgWebServers* :

PowerShell

```
$webNic = New-AzNetworkInterface `
  -Location eastus `
  -Name myVmWeb `
  -ResourceGroupName myResourceGroup `
  -SubnetId $virtualNetwork.Subnets[0].Id `
  -ApplicationSecurityGroupId $webAsg.Id `
  -PublicIpAddressId $publicIpWeb.Id
```

L'exemple suivant crée une interface réseau, lui associe l'adresse IP publique *myVmMgmt* et la rend membre du groupe de sécurité d'application *myAsgMgmtServers* :

PowerShell

```
$mgmtNic = New-AzNetworkInterface `
  -Location eastus `
  -Name myVmMgmt `
  -ResourceGroupName myResourceGroup `
  -SubnetId $virtualNetwork.Subnets[0].Id `
  -ApplicationSecurityGroupId $mgmtAsg.Id `
  -PublicIpAddressId $publicIpMgmt.Id
```

PARTIE 2

Filtrage du trafic de réseau virtuel avec NSG : 3- Déployer des machines virtuelles dans le sous-réseau

Créez deux machines virtuelles dans le réseau virtuel pour pouvoir valider le filtrage du trafic à une étape ultérieure.

Créez une configuration de machine virtuelle avec **New-AzVMConfig**, puis créez la machine virtuelle avec New-AzVM**.** L'exemple suivant crée une machine virtuelle qui servira de serveur web. L'option `-AsJob` crée la machine virtuelle en arrière-plan. Vous pouvez donc passer à l'étape suivante :

Azure PowerShell

```
# Create user object
$cred = Get-Credential -Message "Enter a username and password for the virtual machine."

$webVmConfig = New-AzVMConfig `
  -VMName myVmWeb `
  -VMSize Standard_DS1_V2 | `
Set-AzVMOperatingSystem -Windows `
  -ComputerName myVmWeb `
  -Credential $cred | `
Set-AzVMSourceImage `
  -PublisherName MicrosoftWindowsServer `
  -Offer WindowsServer `
  -Skus 2016-Datacenter `
  -Version latest | `
Add-AzVMNetworkInterface `
  -Id $webNic.Id
New-AzVM `
  -ResourceGroupName myResourceGroup `
  -Location eastus `
  -VM $webVmConfig `
  -AsJob
```

Filtrage du trafic de réseau virtuel avec NSG : 3- Déployer des machines virtuelles dans le sous-réseau

Créez une machine virtuelle comme un serveur d'administration :

Azure PowerShell

```
# Create user object
$cred = Get-Credential -Message "Enter a username and password for the virtual machine."

# Create the web server virtual machine configuration and virtual machine.
$mgmtVmConfig = New-AzVMConfig `
   -VMName myVmMgmt `
   -VMSize Standard_DS1_V2 | `
Set-AzVMOperatingSystem -Windows `
   -ComputerName myVmMgmt `
   -Credential $cred | `
Set-AzVMSourceImage `
   -PublisherName MicrosoftWindowsServer `
   -Offer WindowsServer `
   -Skus 2016-Datacenter `
   -Version latest | `
Add-AzVMNetworkInterface `
   -Id $mgmtNic.Id
New-AzVM `
   -ResourceGroupName myResourceGroup `
   -Location eastus `
   -VM $mgmtVmConfig
```

Filtrage du trafic de réseau virtuel avec NSG : 4- Tester les filtres de trafic

Utilisez **Get-AzPublicIpAddress** pour retourner l'adresse IP publique d'une machine virtuelle. L'exemple suivant retourne l'adresse IP publique de la machine virtuelle *myVmMgmt* :

Azure PowerShell

```
Get-AzPublicIpAddress `
  -Name myVmMgmt `
  -ResourceGroupName myResourceGroup `
  | Select IpAddress
```

Utilisez la commande suivante pour créer une session Bureau à distance avec la machine virtuelle *myVmMgmt* à partir de votre ordinateur local. Remplacez `<publicIpAddress>` par l'adresse IP retournée par la commande précédente.

```
mstsc /v:<publicIpAddress>
```

PARTIE 2

Filtrage du trafic de réseau virtuel avec NSG : 4- Tester les filtres de trafic

Ouvrez le fichier .rdp téléchargé. Si vous y êtes invité, sélectionnez **Connexion**.

Entrez le nom d'utilisateur et le mot de passe spécifiés lors de la création de la machine virtuelle (il se peut que vous deviez choisir **Plus de choix**, puis **Utiliser un compte différent** pour spécifier les informations d'identification que vous avez entrées lors de la création de la machine virtuelle), puis sélectionnez **OK**. Un avertissement de certificat peut s'afficher pendant le processus de connexion. Sélectionnez**Oui** pour poursuivre le processus de connexion.

La connexion réussit, car le port 3389 autorise le trafic entrant depuis Internet vers le groupe de sécurité d'application *myAsgMgmtServers* dans lequel se situe l'interface réseau attachée à la machine virtuelle *myVmMgmt*.

Utilisez la commande suivante pour créer une connexion Bureau à distance vers la machine virtuelle *myVmWeb* à partir de la machine virtuelle *myVmMgmt*, avec la commande suivante, à partir de PowerShell :

```
mstsc /v:myvmWeb
```

Filtrage du trafic de réseau virtuel avec NSG : 4- Tester les filtres de trafic

La connexion réussit car une règle de sécurité par défaut au sein de chaque groupe de sécurité réseau autorise le trafic par tous les ports entre toutes les adresses IP au sein d'un réseau virtuel. Vous ne pouvez pas créer une connexion Bureau à distance à la machine virtuelle *myVmWeb* depuis Internet, car la règle de sécurité pour le *myAsgWebServers* n'autorise pas les données entrantes venant d'Internet sur le port 3389.

Utilisez la commande suivante pour installer Microsoft IIS sur la machine virtuelle *myVmWeb* à partir de PowerShell :

PowerShell

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

Filtrage du trafic de réseau virtuel avec NSG : 4- Tester les filtres de trafic

Une fois l'installation d'IIS terminée, déconnectez-vous de la machine virtuelle *myVmWeb*, ce qui vous laisse dans la connexion Bureau à distance de la machine virtuelle *myVmMgmt*. P

Déconnectez-vous de la machine virtuelle *myVmMgmt*.

Sur votre ordinateur, entrez la commande suivante à partir de PowerShell pour récupérer l'adresse IP publique du serveur *myVmWeb* :

Azure PowerShell

```
Get-AzPublicIpAddress `
  -Name myVmWeb `
  -ResourceGroupName myResourceGroup `
  | Select IpAddress
```

A partir de votre ordinateur, accédez à http://<public-ip-address-from-previous-step>

La connexion sera réussie, car le port 80 autorise le trafic entrant depuis Internet vers le groupe de sécurité d'application *myAsgWebServers* dans lequel se situe l'interface réseau attachée à la machine virtuelle *myVmWeb*.

CHAPITRE 2

Explorer les aspects avancés d’un réseau virtuel

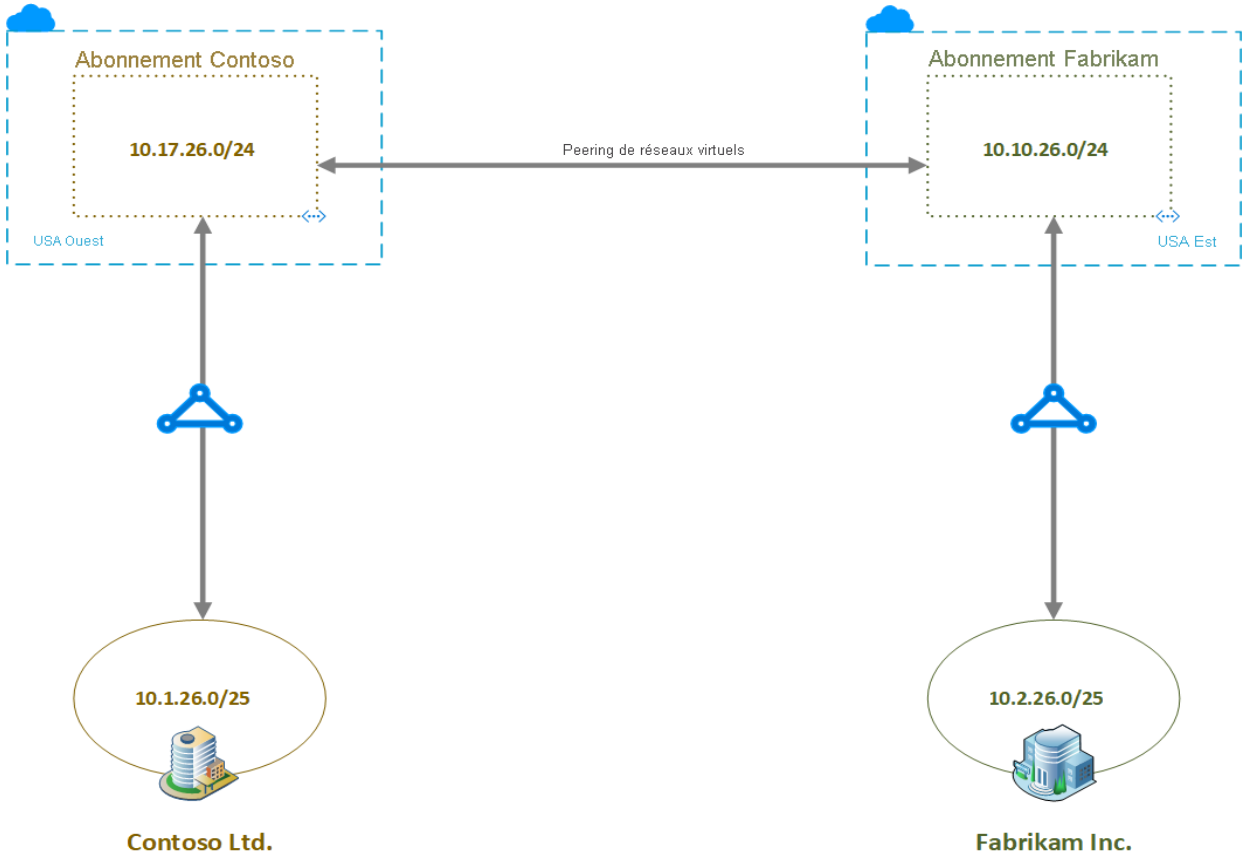
1. Isolement et la segmentation
2. Routage et filtrage du trafic
3. **Interconnexion des réseaux virtuels**
4. Communication avec des ressources locales

Principe de l'interconnexion des réseaux virtuels

L'interconnexion des réseaux virtuels (en anglais VNet Peering) est un moyen de connexion deux réseaux virtuels.

Le peering de réseaux virtuels prend en charge l'interconnexion de deux réseaux virtuels dans la même région Azure (communément appelé VNet Peering) ainsi que dans deux régions Azure différentes (communément appelé Global VNet Peering).

L'illustration suivante présente l'architecture réseau après la configuration du Global VNet Peering.



PARTIE 2

Interconnexion de réseaux virtuels de deux abonnements : Constoso et Fabrikam

Le tableau suivant présente les itinéraires connus pour accéder à la machine virtuelle de l'abonnement Contoso. Prêtez attention à la dernière entrée du tableau. Cette entrée est le résultat de l'interconnexion des réseaux virtuels.

Télécharger Actualiser

Les 200 premiers enregistrements sont affichés, cliquez sur Télécharger ci-dessus pour les voir tous.

Étendue Interface réseau (Contoso-VM01-nic)

Itinéraires effectifs

SOURCE	ÉTAT	PRÉFIXES D'ADRESSE	TYPE DE TRONÇON SUIVANT	ADRESSE IP DU TYPE DE TRONÇON SU
Par défaut	Actif	10.17.26.0/24	Réseau virtuel	-
Passerelle de réseau virtuel	Actif	10.1.26.0/25	Passerelle de réseau virtuel	10.3.129.53
Passerelle de réseau virtuel	Actif	10.1.26.0/25	Passerelle de réseau virtuel	10.3.129.52
Par défaut	Actif	0.0.0.0/0	Internet	-
Par défaut	Actif	10.0.0.0/8	Aucun	-
Par défaut	Actif	100.64.0.0/10	Aucun	-
Par défaut	Actif	192.168.0.0/16	Aucun	-
Par défaut	Actif	10.10.26.0/24	VNetGlobalPeering	-

PARTIE 2

Interconnexion de réseaux virtuels de deux abonnements : Constoso et Fabrikam

Le tableau suivant présente les itinéraires connus pour accéder à la machine virtuelle de l'abonnement Fabrikam. Prêtez attention à la dernière entrée du tableau. Cette entrée est le résultat de l'interconnexion des réseaux virtuels.

Download Refresh

Showing only top 200 records, click Download above to see all.

Scope Network interface (Fabrikam-VM01-nic)

Effective routes

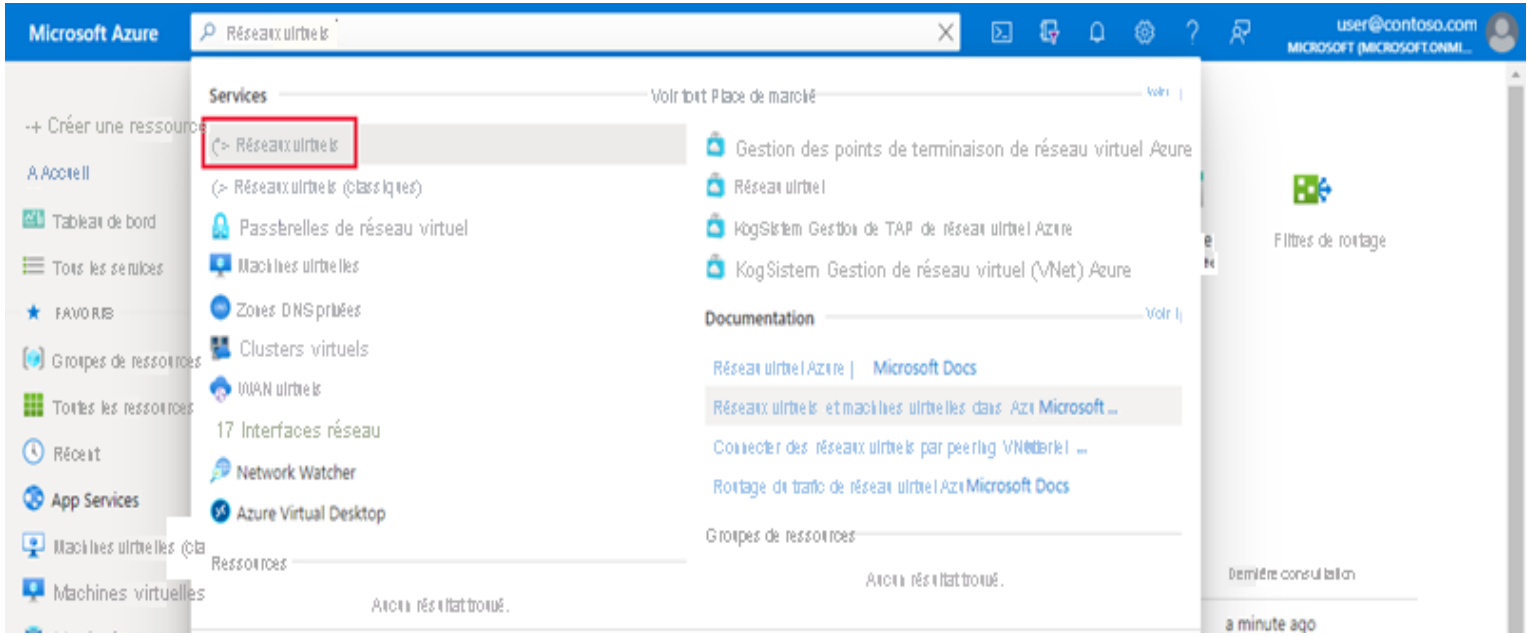
SOURCE	STATE	ADDRESS PREFIXES	NEXT HOP TYPE	NEXT HOP TYPE IP ADDRESS
Default	Active	10.10.26.0/24	Virtual network	-
Virtual network gateway	Active	10.2.26.0/25	Virtual network gateway	10.3.129.24
Virtual network gateway	Active	10.2.26.0/25	Virtual network gateway	10.3.129.25
Default	Active	0.0.0.0/0	Internet	-
Default	Active	10.0.0.0/8	None	-
Default	Active	100.64.0.0/10	None	-
Default	Active	192.168.0.0/16	None	-
Default	Active	10.17.26.0/24	VNetGlobalPeering	-

Le VNet Peering relie directement deux réseaux virtuels (absence de tronçon suivant pour l'entrée *VNetGlobalPeering* dans les deux tableaux ci-dessus)

Interconnexion de réseaux virtuels de deux abonnements : Créer un peering

Avant de créer un peering, familiarisez-vous avec les exigences et contraintes ainsi qu'avec les autorisations nécessaires.

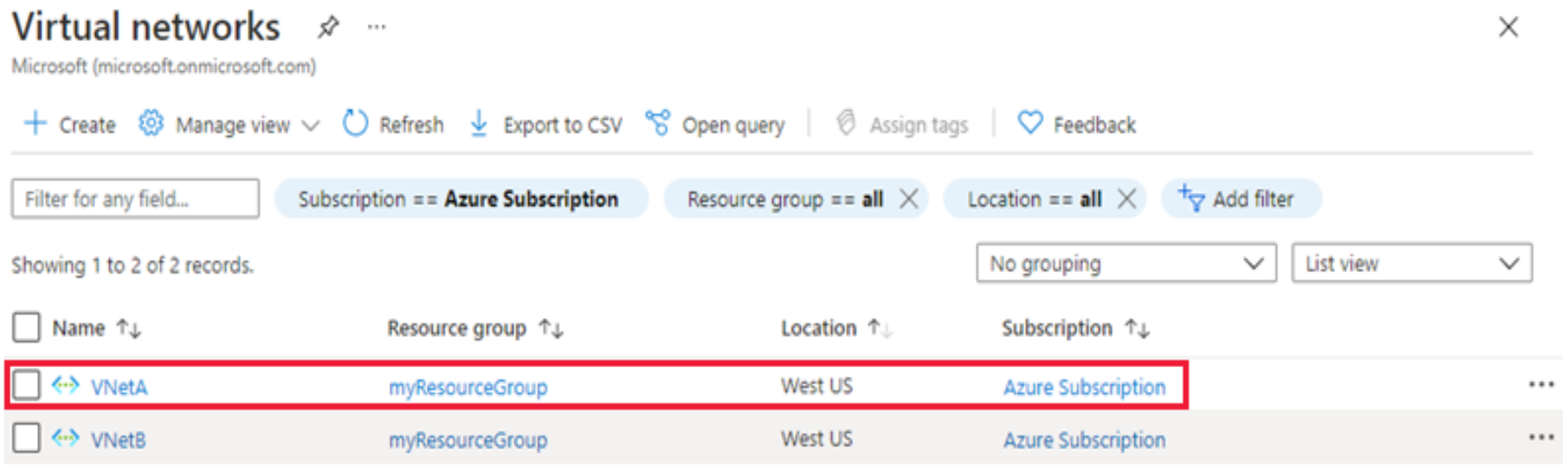
- Dans la zone de recherche située en haut du Portail Azure, entrez *Réseaux virtuels*. Quand la mention **Réseaux virtuels** apparaît dans les résultats de recherche, sélectionnez-la. Ne sélectionnez pas **Réseaux virtuels (classiques)** , car vous ne pouvez pas créer un peering à partir d'un réseau virtuel déployé via le modèle de déploiement classique.



PARTIE 2

Interconnexion de réseaux virtuels de deux abonnements : Créer un peering

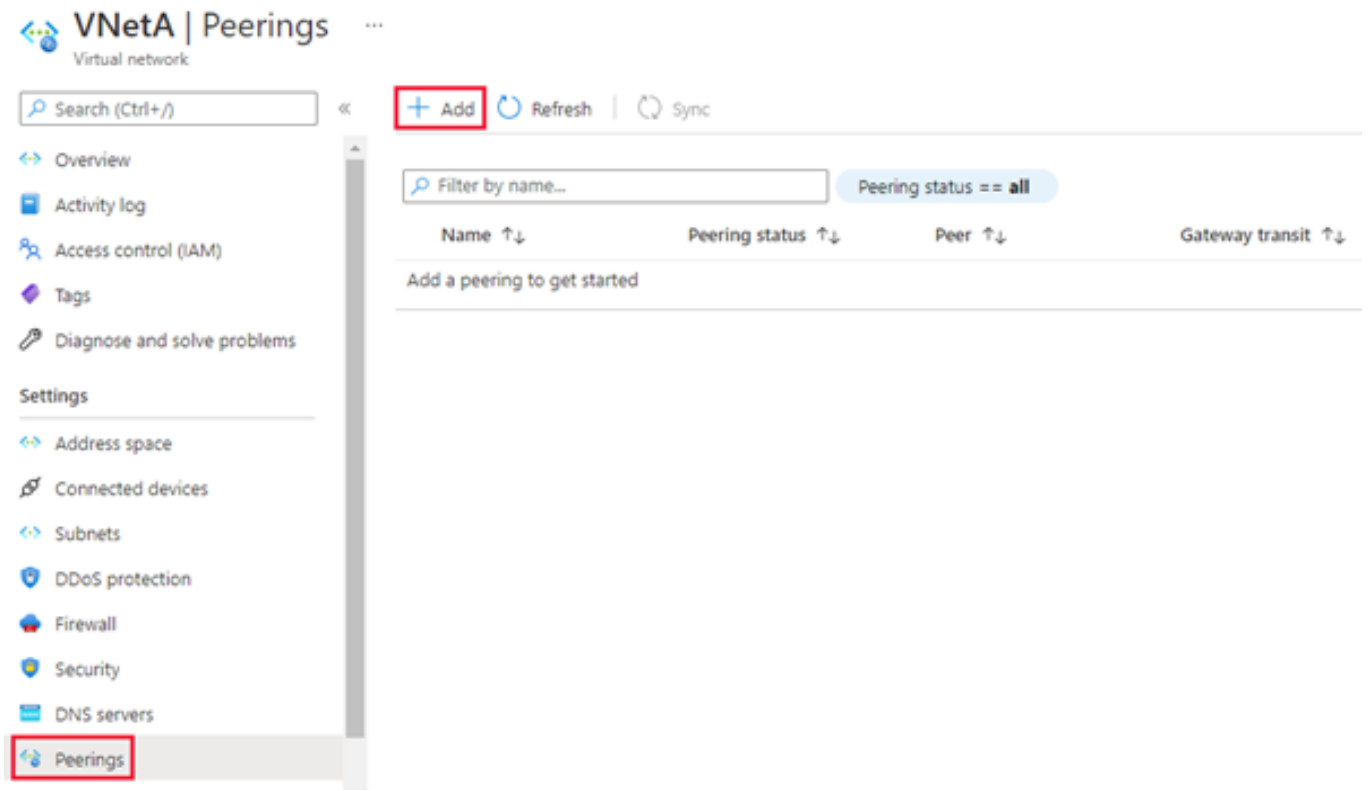
2. Sélectionnez dans la liste le réseau virtuel pour lequel vous souhaitez créer un peering.



PARTIE 2

Interconnexion de réseaux virtuels de deux abonnements : Créer un peering

3. Sélectionnez **Peerings** sous le menu *Paramètres*, puis sélectionnez **+ Ajouter**.



CHAPITRE 2

Explorer les aspects avancés d’un réseau virtuel

1. Isolement et la segmentation
2. Routage et filtrage du trafic
3. Interconnexion des réseaux virtuels
4. **Communication avec des ressources locales**

Les différents mécanismes pour une communication avec des ressources locales

Vous pouvez connecter vos ordinateurs et réseaux locaux à un réseau virtuel à l'aide de n'importe quelle option suivante :

- **Réseau privé virtuel (VPN) de point à site :** connexion établie entre un réseau virtuel et un ordinateur unique de votre réseau. Chaque ordinateur qui doit établir une connexion avec un réseau virtuel doit configurer ses connexions. Ce type de connexion est utile si vous n'êtes pas familiarisé avec Azure, ou pour les développeurs car elle nécessite peu voire pas de modifications de votre réseau existant. La communication entre votre ordinateur et un réseau virtuel passe par un tunnel chiffré via Internet.
- **VPN de site à site :** connexion établie entre votre appareil VPN local et une passerelle VPN Azure déployée dans un réseau virtuel. Ce type de connexion permet à n'importe quelle ressource locale de votre choix d'accéder à un réseau virtuel. La communication entre votre appareil VPN local et une passerelle VPN Azure passe par un tunnel chiffré via Internet.
- **Azure ExpressRoute :** connexion établie entre votre réseau et Azure via un partenaire ExpressRoute. Cette connexion est privée. Toutefois, le trafic ne passe pas par Internet.

Communication avec des ressources locales : Point à Site

Une connexion par passerelle VPN point à site (P2S) vous permet de créer une connexion sécurisée à votre réseau virtuel à partir d'un ordinateur de client individuel. Une connexion P2S est établie en étant démarrée à partir de l'ordinateur client. Cette solution est utile pour les télétravailleurs souhaitant se connecter à un réseau virtuel à partir d'un emplacement distant, comme depuis leur domicile ou pendant une conférence. De même, l'utilisation d'un VPN P2S est une solution utile qui constitue une alternative au VPN Site à Site (S2S) lorsqu'un nombre restreint de clients doit se connecter à un réseau virtuel.

Le protocole utilisé par le P2S ?

La connexion VPN point à site peut utiliser un des protocoles suivants :

- **Protocole OpenVPN®**, un protocole VPN basé sur SSL/TLS. Une solution VPN TLS peut pénétrer des pare-feu, puisque la plupart des pare-feu ouvrent le port de sortie TCP 443 utilisé par le protocole TLS. Vous pouvez utiliser OpenVPN pour vous connecter à partir d'appareils Android, iOS (11.0 et versions ultérieures), Windows, Linux et Mac (macOS 10.13 et versions ultérieures).
- **SSTP (Secure Socket Tunneling Protocol)** est un protocole VPN propriétaire basé sur le protocole TLS. Une solution VPN TLS peut pénétrer des pare-feu, puisque la plupart des pare-feu ouvrent le port de sortie TCP 443 utilisé par le protocole TLS. SSTP est pris en charge sur les appareils Windows uniquement. Azure prend en charge toutes les versions de Windows disposant de SSTP et prend en charge TLS 1.2 (Windows 8.1 et versions ultérieures).
- **VPN IKEv2**, une solution de VPN IPsec basée sur des normes. Un VPN IKEv2 peut être utilisé pour se connecter à partir d'appareils Mac (macOS 10.11 et versions ultérieures).

Communication avec des ressources locales : Points de terminaison de service de réseau virtuel

Le point de terminaison de service de réseau virtuel fournit une connexion sécurisée et directe aux services Azure sur un itinéraire optimisé du réseau principal Azure. Les points de terminaison permettent de sécuriser vos ressources critiques du service Azure pour vos réseaux virtuels uniquement. Les points de terminaison de service permettent aux adresses IP privées du réseau virtuel d'atteindre le point de terminaison d'un service Azure sans qu'une adresse IP publique soit nécessaire sur le réseau virtuel.

Mise à la disposition générale

- Stockage Azure (Microsoft.Storage) : mis à la disposition générale dans toutes les régions Azure.
- Azure SQL Database (Microsoft.Sql) : mis à la disposition générale dans toutes les régions Azure.
- Azure Synapse Analytics (Microsoft.Sql) : Mis à la disposition générale dans toutes les régions Azure pour les pools SQL dédiés (anciennement SQL DW).
- Serveur Azure Database pour PostgreSQL (Microsoft.Sql) : mis à la disposition générale dans les régions Azure où le service de base de données est disponible.
- Serveur Azure Database pour MySQL (Microsoft.Sql) : mis à la disposition générale dans les régions Azure où le service de base de données est disponible.
- Azure Database for MariaDB (Microsoft.Sql) : mis à la disposition générale dans les régions Azure où le service de base de données est disponible.
- Azure Cosmos DB (Microsoft.AzureCosmosDB) : mis à la disposition générale dans toutes les régions Azure.
- Azure Key Vault (Microsoft.KeyVault) : mis à la disposition générale dans toutes les régions Azure.
- Azure Service Bus (Microsoft.ServiceBus) : mis à la disposition générale dans toutes les régions Azure.
- Azure Event Hubs (Microsoft.EventHub) : mis à la disposition générale dans toutes les régions Azure.

Communication avec des ressources locales : Points de terminaison de service de réseau virtuel

Les points de terminaison de service fournissent les avantages suivants :

- **Sécurité améliorée de vos ressources de service Azure** : Les espaces d'adressage privé de réseau virtuel peuvent se chevaucher. Vous ne pouvez pas utiliser d'espaces qui se chevauchent pour identifier de manière unique le trafic provenant de votre réseau virtuel. Les points de terminaison de service permettent de sécuriser les ressources de service Azure sur votre réseau virtuel en étendant l'identité du réseau virtuel à ce service. Une fois que vous avez activé les points de terminaison de service dans votre réseau virtuel, vous pouvez ajouter une règle de réseau virtuel afin de sécuriser les ressources du service Azure pour votre réseau virtuel. L'ajout de règles améliore la sécurité en supprimant totalement l'accès Internet public aux ressources et en autorisant le trafic uniquement à partir de votre réseau virtuel.
- **Routage optimal pour le trafic de service Azure à partir de votre réseau virtuel** : Aujourd'hui, tous les itinéraires dans votre réseau virtuel qui forcent le trafic Internet vers vos appliances locales et/ou virtuelles forcent également le trafic de service Azure à prendre le même itinéraire que le trafic Internet. Les points de terminaison de service fournissent un routage optimal pour le trafic Azure.

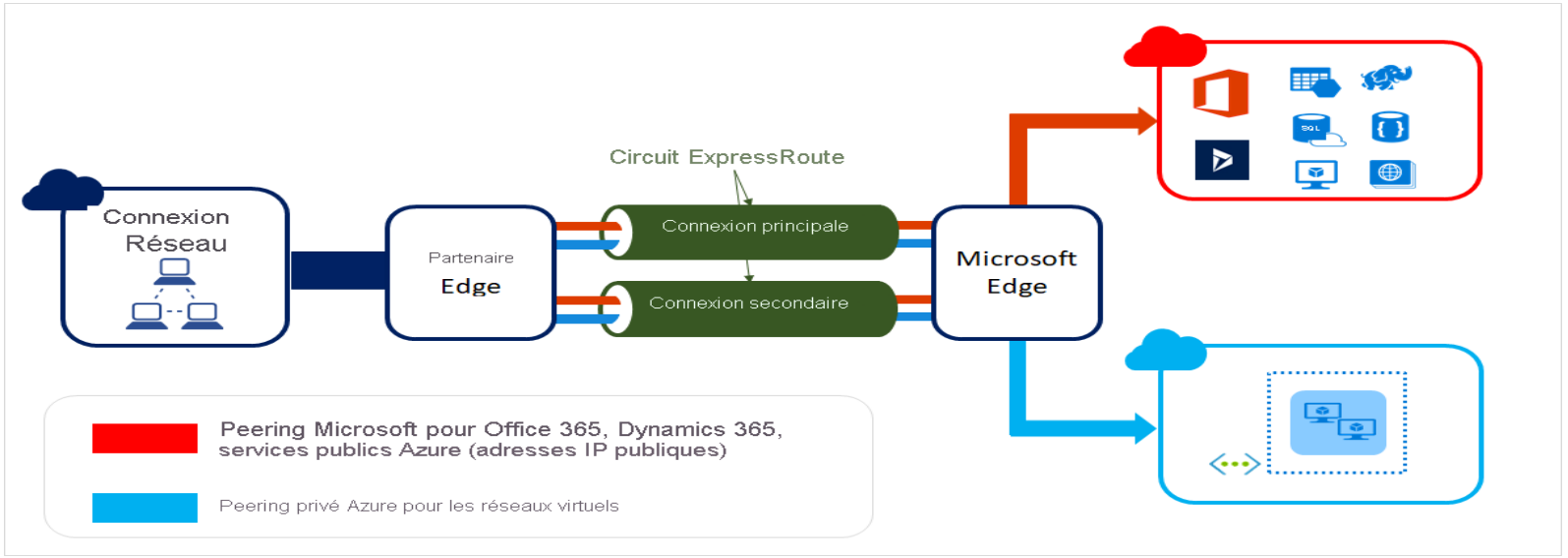
Les points de terminaison acheminent toujours le trafic de service directement à partir de votre réseau virtuel vers le service sur le réseau principal de Microsoft Azure. La conservation du trafic sur le réseau principal d'Azure vous permet de continuer l'audit et la surveillance du trafic Internet sortant à partir de vos réseaux virtuels, via le tunneling forcé, sans affecter le trafic de service.

- **Une configuration simple et un temps de gestion réduit** : Les adresses IP publiques réservées dans vos réseaux virtuels ne sont désormais plus nécessaires pour sécuriser les ressources Azure via le pare-feu IP. Aucune traduction d'adresses réseau (NAT) ni aucun appareil de passerelle n'est requis pour configurer les points de terminaison de service. Vous pouvez configurer des points de terminaison de service par un simple clic sur un sous-réseau. La conservation des points de terminaison ne requiert aucun temps système supplémentaire.

Communication avec des ressources locales : Express Route

ExpressRoute vous permet d'étendre vos réseaux locaux dans le Cloud Microsoft via une connexion privée avec l'aide d'un fournisseur de connectivité. Avec ExpressRoute, vous pouvez établir des connexions aux services de Cloud computing Microsoft, comme Microsoft Azure et Microsoft 365.

La connectivité peut provenir d'un réseau universel (IP VPN), d'un réseau Ethernet point à point ou d'une interconnexion virtuelle via un fournisseur de connectivité dans un centre de colocalisation. Les connexions ExpressRoute ne passent pas par l'Internet public. Elles offrent ainsi une meilleure fiabilité, des vitesses supérieures, des latences cohérentes et une plus grande sécurité que les connexions classiques sur Internet.



Communication avec des ressources locales : Express Route

Express Route fourni les avantages suivants :

- Connectivité de couche 3 entre votre réseau local et le Cloud de Microsoft via un fournisseur de connectivité. La connectivité peut provenir d'un réseau universel (IPVPN), d'une connexion Ethernet point à point, ou d'une interconnexion virtuelle via un échange Ethernet.
- Connectivité aux services de Cloud de Microsoft dans toutes les régions de la zone géopolitique.
- Connectivité globale aux services de Microsoft dans toutes les régions grâce au module complémentaire ExpressRoute premium.
- Routage dynamique entre votre réseau et Microsoft via le protocole de routage dynamique standard (BGP).
- Redondance intégrée dans chaque emplacement de peering pour une plus grande fiabilité.
- SLA de disponibilité de la connexion.
- Support de la qualité de service pour Skype Entreprise.

PARTIE 3

Gérer les données

Dans ce module, vous allez :

- Explorer les fonctionnalités de stockage
- Découvrir les types de stockage

8 heures

CHAPITRE 1

Explorer les fonctionnalités de stockage

Ce que vous allez apprendre dans ce chapitre :

- Appréhender les différentes fonctionnalités de stockage
- Différencier entre les types de stockage offert par le fournisseur Cloud (Azure)

4 heures

CHAPITRE 1

Explorer les fonctionnalités de stockage

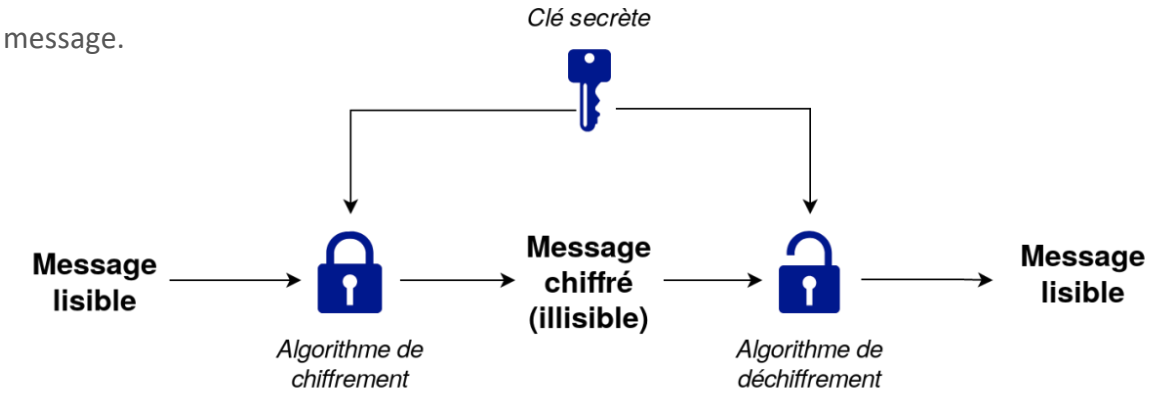
1. **Chiffrement**
2. Stockage régional
3. Redondance de zone

Définition et but du chiffrement

Le chiffrement est un procédé cryptographique qui consiste à protéger des données incompréhensibles pour ceux qui ne possèdent pas la clé de chiffrement. Le chiffrement des données dans l'informatique a pour but d'assurer la confidentialité des données stockées ou transmises à un système informatique (SI). Les données sont cryptées à l'aide d'un algorithme de cryptage et d'un jeu de clés.

Le principal objectif du chiffrement consiste à garantir la confidentialité des données numériques stockées sur des systèmes informatiques ou transmises via Internet ou d'autres réseaux. Les algorithmes de chiffrement modernes jouent un rôle crucial dans la sécurité des systèmes informatiques et des communications, car ils assurent non seulement la confidentialité, mais également les éléments de sécurité essentiels suivants :

- **Authentification** : permet de vérifier l'origine d'un message.
- **Intégrité** : apporte la preuve que le contenu d'un message n'a pas été modifié depuis son envoi.
- **Non-répudiation** : empêche l'expéditeur d'un message de nier avoir envoyé ce message.



PARTIE 3

Types de chiffrement : Chiffrement symétrique

Le chiffrement symétrique est un type de chiffrement dans lequel une seule clé symétrique secrète est utilisée pour chiffrer le texte en clair et déchiffrer le texte crypté.

Méthodes de chiffrement symétrique courantes

- **Data Encryption Standards (DES)** : DES est un algorithme de chiffrement par blocs de bas niveau qui convertit le texte brut en blocs de 64 bits et les convertit en texte chiffré à l'aide de clés de 48 bits.
- **Triple DES** : Triple DES exécute le chiffrement DES à trois reprises en chiffrant, en déchiffrant, puis en chiffrant à nouveau les données.
- **Norme de chiffrement avancée (AES)** : AES est souvent désigné comme la référence absolue en termes de cryptage des données et est utilisé dans le monde entier, notamment par le gouvernement américain.
- **Twofish** : Twofish est considéré comme l'un des algorithmes de chiffrement les plus rapides et son utilisation est gratuite.

Types de chiffrement : Chiffrement asymétrique

Le chiffrement asymétrique, également connu sous le nom de cryptographie à clé publique, chiffre et déchiffre les données à l'aide de deux clés cryptographiques asymétriques distinctes. Ces deux clés sont appelées clé publique » et clé privée ».

Méthodes courantes de chiffrement asymétrique

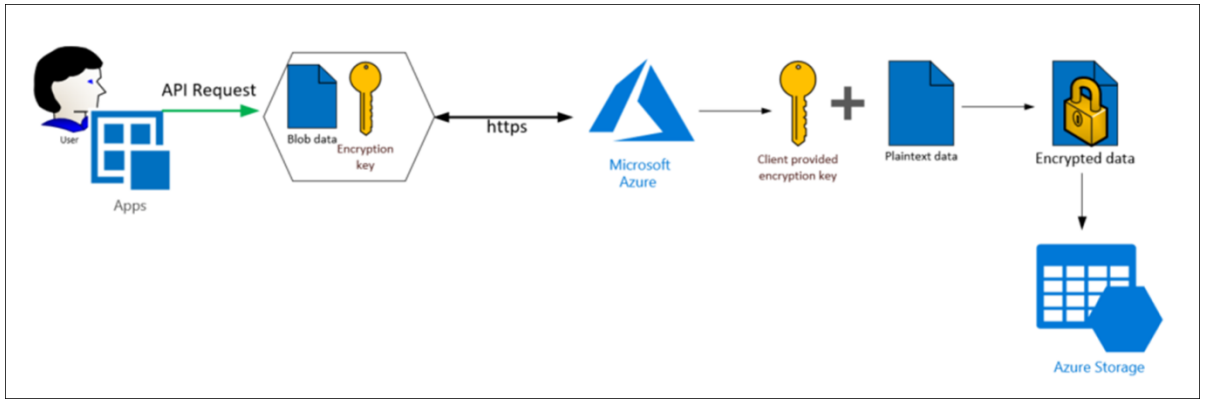
- **RSA** : RSA, du nom des informaticiens Ron Rivest, Adi Shamir et Leonard Adleman, est un algorithme couramment utilisé pour chiffrer les données à l'aide d'une clé publique et pour les déchiffrer avec une clé privée afin de les transmettre en toute sécurité.
- **Infrastructure à clé publique (PKI)** : PKI est un moyen de gérer les clés de chiffrement par l'émission et la gestion de certificats numériques.

Chiffrement des données dans Azure

Azure propose plusieurs options pour chiffrer les données au repo :

- CHIFFREMENT CÔTÉ CLIENT
- CHIFFREMENT CÔTÉ SERVEUR

Avec le CHIFFREMENT CÔTÉ CLIENT, vous pouvez chiffrer les données avant de les télécharger sur Azure Storage. Vous pouvez également choisir de faire en sorte qu'Azure gère les opérations de chiffrement avec le CHIFFREMENT CÔTÉ SERVEUR à l'aide de clés gérées par Microsoft ou à l'aide de clés gérées par le client dans le coffre de clés Azure.



Chiffrement des données dans Azure : CHIFFREMENT CÔTÉ CLIENT

Le chiffrement côté client est effectué en dehors d'Azure. Il inclut :

- Les données chiffrées par une application qui s'exécute dans le centre de données du client ou par une application de service.
- Les données sont déjà chiffrées lorsqu'elles sont reçues par Azure.

Avec le chiffrement côté client, les fournisseurs de services Cloud n'ont pas accès aux clés de chiffrement et ne peuvent pas déchiffrer ces données. Vous conservez un contrôle total des clés.

Chiffrement des données dans Azure : CHIFFREMENT CÔTÉ SERVEUR

Les trois modèles de chiffrement côté serveur offrent différentes caractéristiques de gestion de clés, que vous pouvez choisir en fonction de vos besoins :

- **Clés gérées par le service** : ce modèle fournit une combinaison de contrôle et de fonctionnalités avec une faible surcharge.
- **Clés gérées par le client** : ce modèle vous permet de contrôler les clés, avec notamment la prise en charge de BYOK (Bring Your Own Keys), ou d'en générer de nouvelles.
- **Clés gérées par le service sur le matériel contrôlé par le client** : ce modèle vous permet de gérer les clés dans votre référentiel propriétaire, en dehors du contrôle de Microsoft. Cette caractéristique est appelée HYOK (Host Your Own Key). Toutefois, la configuration est complexe et la plupart des services Azure ne prennent pas en charge ce modèle.

Les principales technologies de chiffrement de disque : Azure Storage Service Encryption (SSE)

SSE est un service de chiffrement intégré à Azure qui sert à protéger les données au repos. La plateforme de stockage Azure chiffre automatiquement les données avant qu'elles ne soient stockées sur plusieurs services de stockage dont Disques managés Azure. Le chiffrement est activé par défaut avec le chiffrement AES 256 bits et est géré par l'administrateur de compte de stockage.

SSE est activé pour tous les comptes de stockage nouveaux et existants, et il ne peut pas être désactivé. Vos données étant sécurisées par défaut, vous n'avez pas besoin de modifier votre code ou vos applications pour tirer parti de SSE.

SSE n'affecte pas les performances des services de stockage Azure.

Les principales technologies de chiffrement de disque : Azure Disk Encryption (ADE)

ADE est géré par le propriétaire de la machine virtuelle. Il contrôle le chiffrement de Windows et des disques contrôlés par machine virtuelle Linux à l'aide de BitLocker sur les machines virtuelles Windows et de DM-Crypt sur les machines virtuelles Linux. **BitLocker** Drive Encryption est une fonction de protection des données qui s'intègre au système d'exploitation et répond aux menaces de vol de données ou d'exposition des ordinateurs perdus, volés ou mis hors service de manière inappropriée. De même, **DM-Crypt** chiffre les données au repos pour Linux avant d'écrire dans le stockage.

ADE garantit que toutes les données sur les disques des machines virtuelles sont chiffrées au repos dans le stockage Azure, et ADE est nécessaire pour les machines virtuelles sauvegardées dans le Recovery Vault.

Avec ADE, les machines virtuelles démarrent sous des clés et des stratégies contrôlées par le client. ADE est intégré à Azure Key Vault pour gérer les secrets et les clés de chiffrement de disque.

CHAPITRE 1

Explorer les fonctionnalités de stockage

1. Chiffrement
2. **Stockage régional**
3. Redondance de zone

Stockage régional

Azure Storage stocke toujours plusieurs copies de vos données afin qu'elles soient protégées contre les événements planifiés et imprévus, y compris les pannes matérielles transitoires, les pannes de réseau ou de courant et les catastrophes naturelles massives. La redondance garantit que votre compte de stockage atteint ses objectifs de disponibilité et de durabilité, même en cas de panne.

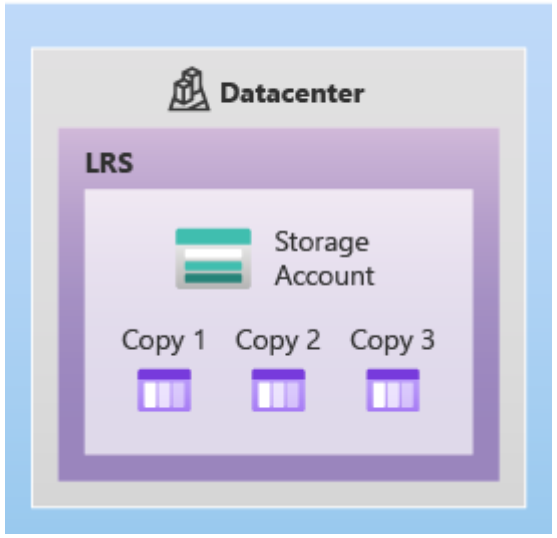
Lorsque vous décidez de l'option de redondance la mieux adaptée à votre scénario, tenez compte des compromis entre des coûts inférieurs et une disponibilité accrue. Les facteurs qui aident à déterminer l'option de redondance à choisir incluent :

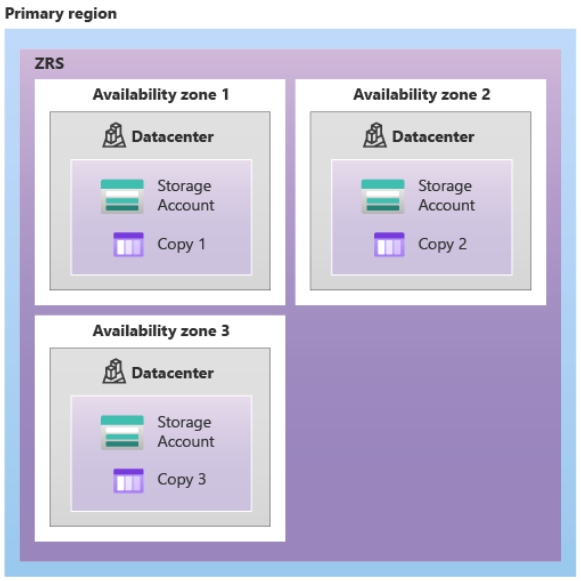
- Comment vos données sont répliquées dans la région primaire.
- Si vos données sont répliquées dans une deuxième région géographiquement éloignée de la région principale, pour se protéger contre les catastrophes régionales (géo-réplication).
- Si votre application nécessite un accès en lecture aux données répliquées dans la région secondaire si la région primaire devient indisponible pour une raison quelconque (géo-réplication avec accès en lecture).

Redondance dans la région primaire

Les données des comptes de stockage Azure sont toujours répliquées trois fois dans la région principale. Azure Storage propose deux options pour répliquer les données dans la région principale.

- **Le stockage localement redondant (LRS)** copie vos données de manière synchrone trois fois dans un emplacement physique unique dans la région primaire. LRS est l'option de réplication la moins chère, mais n'est pas recommandée pour les applications nécessitant une disponibilité ou une durabilité élevées.
- **Le stockage redondant entre zones (ZRS)** copie vos données de manière synchrone sur trois zones de disponibilité Azure dans la région principale. Pour les applications nécessitant une haute disponibilité, Microsoft recommande d'utiliser ZRS dans la région principale et également de répliquer dans une région secondaire.





CHAPITRE 1

Explorer les fonctionnalités de stockage

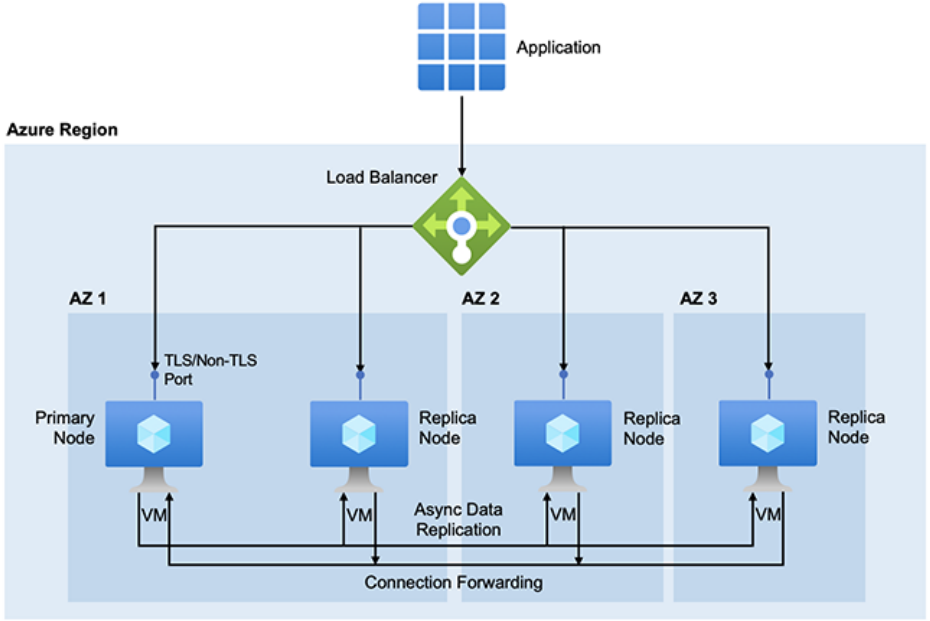
1. Chiffrement
2. Stockage régional
3. **Redondance de zone**

Redondance de zone

Stockage Azure stocke toujours plusieurs copies de vos données afin qu'elles soient protégées contre des événements planifiés ou non, notamment des défaillances matérielles temporaires, des pannes du réseau ou de l'alimentation électrique, et des catastrophes naturelles majeures. La redondance garantit que votre compte de stockage répond à ses objectifs de disponibilité et de durabilité, même en cas de défaillance.

Les facteurs déterminant le choix de l'option de redondance sont

- Mode de réplication de vos données dans la région primaire.
- Réplication éventuelle de vos données vers une deuxième région géographiquement éloignée de la région primaire, afin d'offrir une protection contre les catastrophes régionales (géoréplication).
- Nécessité ou non pour l'application d'avoir accès en lecture aux données répliquées dans la région secondaire si la région primaire n'est plus disponible pour une raison quelconque (géoréplication avec accès en lecture).



PARTIE 3

CHAPITRE 2

Découvrir les types de stockage

Ce que vous allez apprendre dans ce chapitre :

- Créer du stockage d’objets blob
- Créer du stockage de fichiers
- Créer du stockage de table

4 heures

CHAPITRE 2

Découvrir les types de stockage

1. **Stockage d’objets blob**
2. Stockage de fichiers
3. Stockage de table

Stockage d'objets blob

Le **stockage Blob Azure** est la solution de stockage d'objet de Microsoft pour le Cloud. Stockage Blob est optimisé pour le stockage d'immenses quantités de données non structurées. Les données non structurées sont des données qui n'obéissent pas à un modèle ou une définition de données en particulier, comme des données texte ou binaires.

À propos du stockage d'objets blob

- Mise à disposition d'images ou de documents directement dans un navigateur.
- Stockage de fichiers pour un accès distribué.
- Diffusion en continu de vidéo et d'audio.
- Écriture dans les fichiers journaux.
- Stockage de données pour la sauvegarde et la restauration, la récupération d'urgence et l'archivage.
- Stockage des données pour l'analyse par un service local ou hébergé par Azure.

CHAPITRE 2

Découvrir les types de stockage

1. Stockage d’objets blob
2. **Stockage de fichiers**
3. Stockage de table

Stockage de fichiers

La plate-forme Azure Storage est la solution de stockage Cloud de Microsoft pour les scénarios de stockage de données actuels. Azure Storage fournit un stockage hautement disponible, hautement évolutif, durable et sécurisé pour une grande variété d'objets de données Cloud.

Avantages de Stockage Azure :

- **Durable et hautement disponible.** La redondance garantit que vos données sont sécurisées en cas de défaillance matérielle temporaire. Vous pouvez également choisir de répliquer des données entre des centres de données ou des régions géographiques pour une protection supplémentaire contre les catastrophes locales ou les catastrophes naturelles. Les données ainsi répliquées restent hautement disponibles en cas de panne inattendue.
- **Sécurisé.** Toutes les données écrites dans un compte de stockage Azure sont chiffrées par le service. Le Stockage Azure vous permet de contrôler de manière plus précise qui a accès à vos données.
- **Évolutif.** Le Stockage Azure est conçu pour être hautement évolutif afin de répondre aux besoins de stockage de données et de performances des applications actuelles.
- **Géré.** Azure gère la maintenance du matériel, les mises à jour et les problèmes critiques pour vous.
- **Accessible.** Les données dans le Stockage Azure sont accessibles n'importe où dans le monde via HTTP ou HTTPS. Microsoft fournit des bibliothèques clientes pour le Stockage Azure dans une variété de langages, dont .NET, Java, Node.js, Python, PHP, Ruby, Go et autres encore, ainsi qu'une API REST avancée. Le stockage Azure prend en charge l'écriture de scripts Azure PowerShell ou l'interface de ligne de commande Azure. De plus, le portail Azure et l'Explorateur Stockage Azure offrent des solutions visuelles simples pour utiliser vos données.

CHAPITRE 2

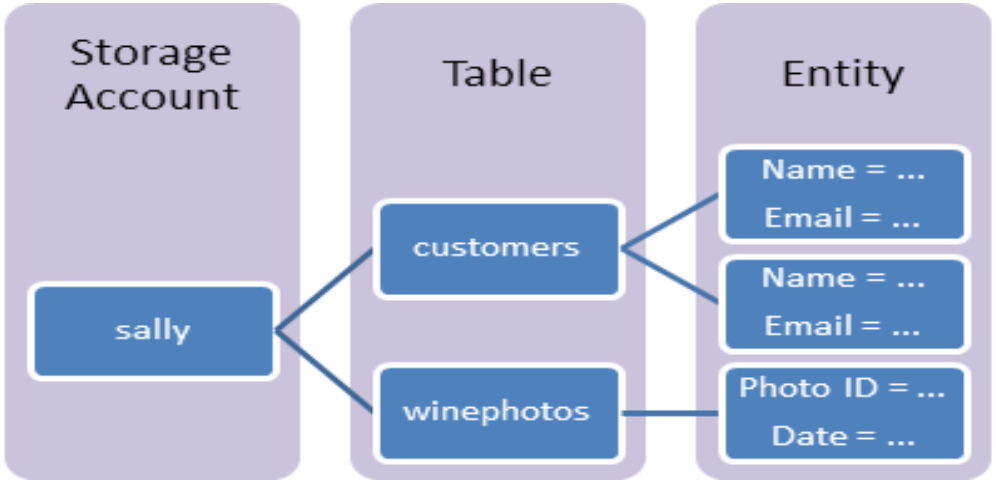
Découvrir les types de stockage

1. Stockage d’objets blob
2. Stockage de fichiers
3. **Stockage de table**

Stockage de table

Le **stockage de table Azure** est utilisé pour stocker de grandes quantités de données structurées. Il s'agit d'un magasin de données NoSQL qui accepte les appels authentifiés provenant de l'intérieur et de l'extérieur du Cloud Azure. Les tables Azure sont idéales pour stocker des données structurées non relationnelles. Voici quelques utilisations courantes du stockage de table :

- Stockage de To de données structurées capables de servir des applications à l'échelle du Web
- Stockage d'ensembles de données qui ne nécessitent pas de jointures complexes, de clés étrangères ou de procédures stockées et qui peuvent être dénormalisés pour un accès rapide
- Interroger rapidement des données à l'aide d'un index clusterisé
- Accès aux données à l'aide du protocole OData et des requêtes LINQ avec les bibliothèques WCF Data Service .NET



PARTIE 4

Administrer des applications web

Dans ce module, vous allez :

- Administrer un site web avec des machines virtuelles
- Administrer un site web avec un service géré (PaaS)

8 heures

CHAPITRE 1

Administrer un site web avec des machines virtuelles

Ce que vous allez apprendre dans ce chapitre :

- Préparer un environnement applicatif
- Déployer une application web dans une VM

4 heures

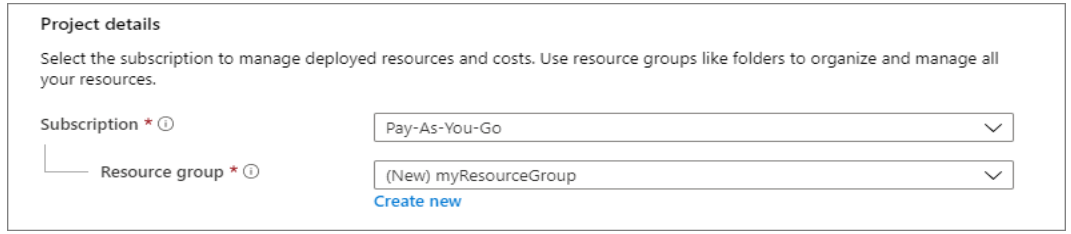
CHAPITRE 1

Administrer un site web avec des machines virtuelles

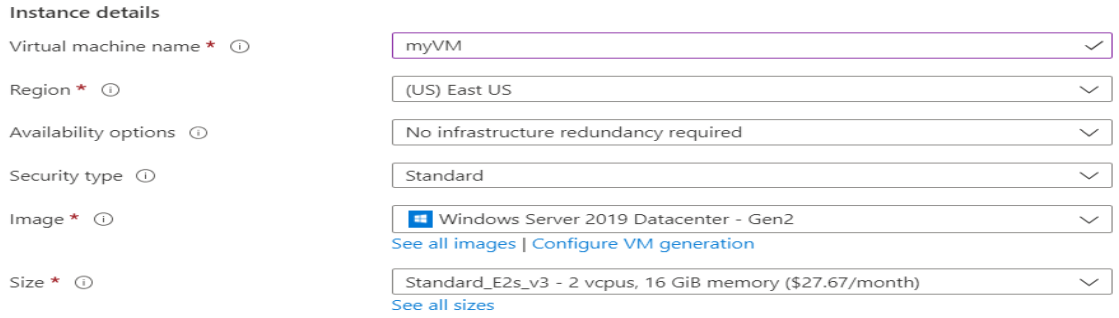
1. **Création de la VM**
2. Téléchargement et installation de l’environnement applicatif
3. Déploiement d’un site web

Création de la VM

1. Entrez *les machines virtuelles* dans la recherche.
2. Sous **Services**, sélectionnez **Machines virtuelles** .
3. Dans la page **Machines virtuelles** sélectionnez **Créer** puis **Machine virtuelle**. La page **Créer une machine virtuelle** s'ouvre.
4. Dans l' onglet Général, sous **Détails du projet**, assurez-vous que l'abonnement correct est sélectionné, puis choisissez **Créer un nouveau** groupe de ressources. Entrez *myResourceGroup* pour le nom.



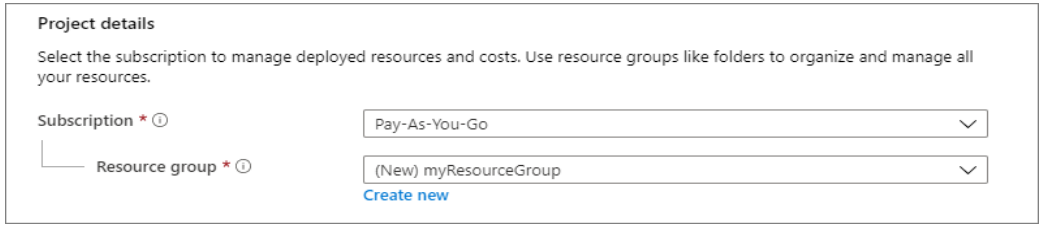
1. Sous **Détails de l'instance**, entrez myVM pour le **nom de la machine virtuelle** et choisissez *Windows Server 2019 Datacenter - Gen2* pour l' **image** . Laissez les autres valeurs par défaut.



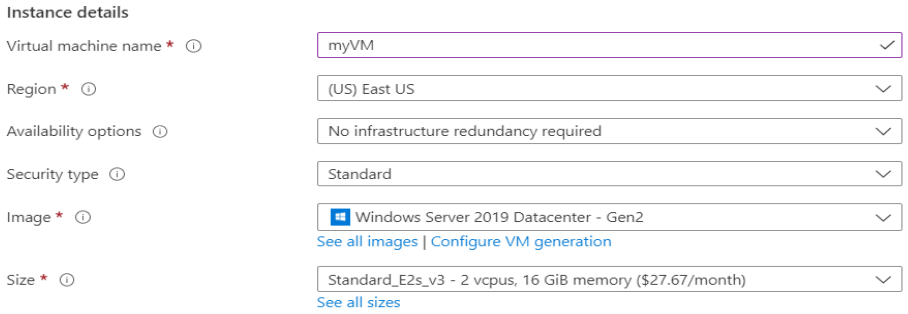
PARTIE 4

Création de la VM

6. Sous **Compte administrateur** , fournissez un nom d'utilisateur, tel que ***azureuser*** et un mot de passe. Le mot de passe doit comporter au moins 12 caractères et répondre aux exigences de complexité définies .

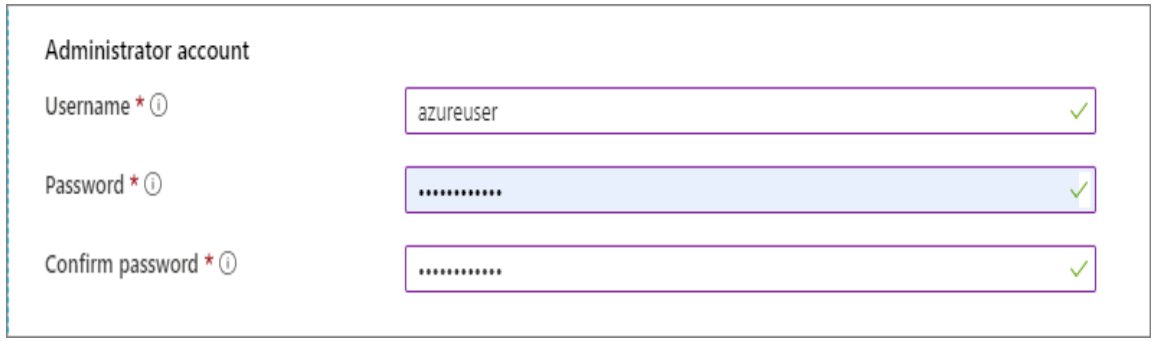


6. Sous **Règles de port entrant** , choisissez **Autoriser les ports sélectionnés** , puis sélectionnez **RDP (3389)** et **HTTP (80)** dans le menu déroulant.

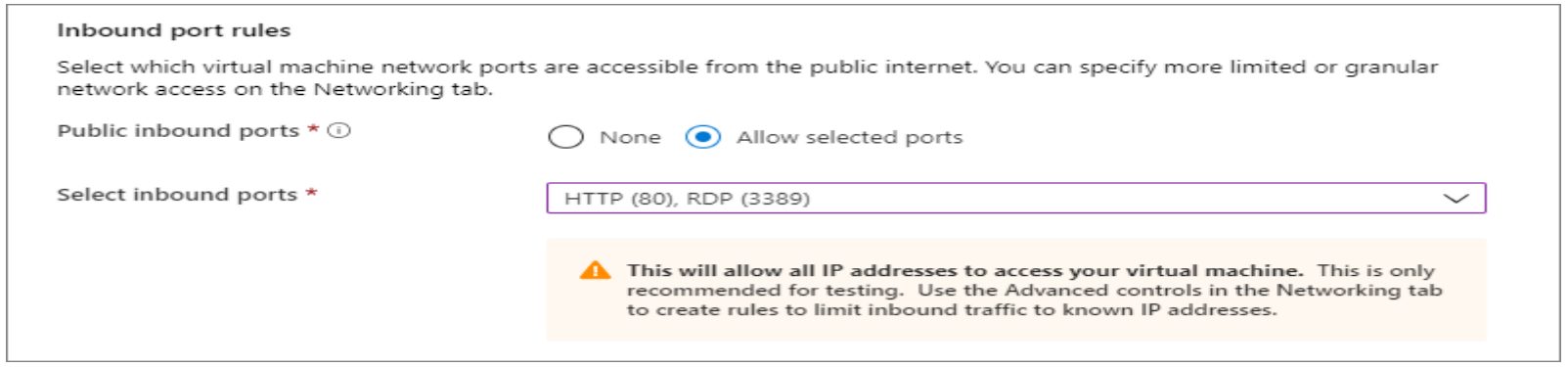


6. Laissez les valeurs par défaut restantes, puis sélectionnez le bouton **Réviser + créer** en bas de la page.

Création de la VM



9. Une fois la validation effectuée, sélectionnez le bouton **Créer** en bas de la page.
10. Une fois le déploiement terminé, sélectionnez **Accéder à la ressource** .



CHAPITRE 1

Administrer un site web avec des machines virtuelles

1. Création de la VM
2. **Téléchargement et installation de l'environnement applicatif**
3. Déploiement d'un site web

Téléchargement et installation de l'environnement applicatif (Application web Java)

Installer Java

1. Connectez-vous à votre machine virtuelle en utilisant votre client SSH.
2. À l'invite Bash sur votre machine virtuelle, exécutez la commande suivante :
3. sudo apt-get install default-jdk

3. Validez votre installation. Tout en restant connecté à votre machine virtuelle dans votre session SSH, exécutez la commande suivante :

java –version

Installer et configurer Tomcat

- Connectez-vous à votre machine virtuelle en utilisant votre client SSH.
- Créez un utilisateur Tomcat en effectuant les étapes suivantes :

a. Créez un groupe Tomcat à l'aide de la commande suivante :

sudo groupadd tomcat

b. Créez un utilisateur Tomcat. Ajoutez cet utilisateur au groupe Tomcat avec le répertoire de base */opt/tomcat*. Vous déployez Tomcat dans ce répertoire :

sudo useradd -s /bin/false -g tomcat -d /opt/tomcat tomcat

Téléchargement et installation de l'environnement applicatif (Application web Java)

- **Installez Tomcat en effectuant les étapes suivantes :**

a. Obtenez l'URL du fichier tar de la dernière version de Tomcat 8 sur la (https://tomcat.apache.org/download-80.cgi)

b. Utilisez cURL pour télécharger la dernière version en suivant le lien. Exécutez les commandes suivantes :

```
cd /tmp
    curl -O <URL for the tar for the latest version of Tomcat 8>
```

c. Installez Tomcat dans le répertoire */opt/tomcat*. Créez le dossier, puis ouvrez l'archive :

```
sudo mkdir /opt/tomcat
    sudo tar xzvf apache-tomcat-8*tar.gz -C /opt/tomcat --strip-components=1
    sudo chown -R tomcat webapps/ work/ temp/ logs/
```

4. Mettez à jour les autorisations pour Tomcat en exécutant les commandes suivantes :

```
sudo chgrp -R tomcat /opt/tomcat
sudo chmod -R g+r conf
sudo chmod g+x conf
```

Téléchargement et installation de l'environnement applicatif (Application web Java)

5. Créez un fichier de service *systemd* afin de pouvoir exécuter Tomcat en tant que service.

a. Tomcat a besoin de savoir où vous avez installé Java. Ce chemin d'accès est la plupart du temps nommé *JAVA_HOME*. Trouvez l'emplacement en question en exécutant :

```
sudo update-java-alternatives -l
```

Le résultat doit se présenter ainsi :

```
Output
    java-1.8.0-openjdk-amd64      1081      /usr/lib/jvm/java-1.8.0-openjdk-amd64
```

Vous pouvez construire la valeur de la variable *JAVA_HOME* en ajoutant */jre* au chemin de la sortie. Pour l'exemple précédent, la valeur serait */usr/lib/jvm/java-1.8.0-openjdk-amd64/jre*.

b. Utilisez la valeur obtenue de votre serveur pour créer le fichier de service systemd :

BashCopier

```
sudo nano /etc/systemd/system/tomcat.service
```

Téléchargement et installation de l'environnement applicatif (Application web Java)

c. Collez le contenu suivant dans votre fichier de service. Si nécessaire, remplacez la valeur de *JAVA_HOME* par la valeur trouvée sur votre système. Vous pouvez également avoir besoin de modifier les paramètres d'allocation de mémoire spécifiés dans CATALINA_OPTS :

Text Copier

```
[Unit]
Description=Apache Tomcat Web Application Container
After=network.target

[Service]
Type=forking

Environment=JAVA_HOME=/usr/lib/jvm/java-1.8.0-openjdk-amd64/jre
Environment=CATALINA_PID=/opt/tomcat/temp/tomcat.pid
Environment=CATALINA_HOME=/opt/tomcat
Environment=CATALINA_BASE=/opt/tomcat
Environment='CATALINA_OPTS=-Xms512M -Xmx1024M -server -XX:+UseParallelGC'
Environment='JAVA_OPTS=-Djava.awt.headless=true -Djava.security.egd=file:/dev/./urandom'

ExecStart=/opt/tomcat/bin/startup.sh
ExecStop=/opt/tomcat/bin/shutdown.sh

User=tomcat
Group=tomcat
UMask=0007
RestartSec=10
Restart=always

[Install]
WantedBy=multi-user.target
```

Téléchargement et installation de l'environnement applicatif (Application web Java)

d. Enregistrez et fermez le fichier.

e. Rechargez le démon systemd pour qu'il prenne connaissance de votre fichier de service :

```
sudo systemctl daemon-reload
```

f. Démarrez le service Tomcat :

```
sudo systemctl start tomcat
```

g. Vérifiez qu'il a démarré sans erreur, en entrant :

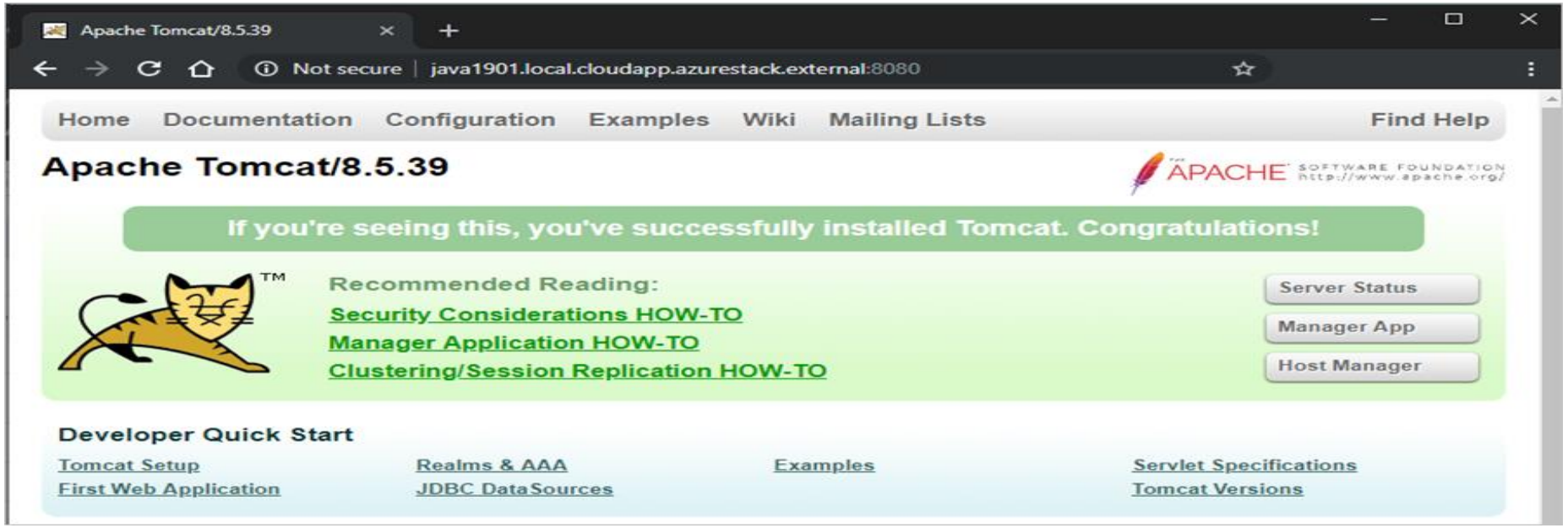
```
sudo systemctl status tomcat
```

Téléchargement et installation de l'environnement applicatif (Application web Java)

6. Vérifiez le serveur Tomcat. Tomcat utilise le port 8080 pour accepter les demandes classiques. Autorisez le trafic vers ce port en exécutant la commande suivante :

   sudo ufw allow 8080

7. Ouvrez un navigateur dans le même réseau que votre système Azure Stack Hub, puis ouvrez votre serveur, *yourmachine.local.Cloudapp.azurestack.external:8080*.



Téléchargement et installation de l'environnement applicatif (Application web Java)

- La page Apache Tomcat se charge sur votre serveur. Vous configurez maintenant le serveur de façon à pouvoir accéder à Server Status, à l'application Manager et à Host Manager.

8. Activez le fichier de service pour que Tomcat se lance automatiquement au redémarrage de votre serveur :

```
sudo systemctl enable tomcat
```

9. Pour avoir accès à l'interface de gestion web, configurez le serveur Tomcat.

a. Modifiez le fichier *tomcat-users.xml* et définissez un rôle et un utilisateur pour la connexion. Définissez l'utilisateur de sorte qu'il ait accès à manager-gui et à admin-gui.

```
sudo nano /opt/tomcat/conf/tomcat-users.xml
```

Téléchargement et installation de l'environnement applicatif (Application web Java)

b. Ajoutez les éléments suivants à la section <tomcat-users> :

```
<role rolename="tomcat"/>
      <user username="<username>" password="<password>" roles="tomcat,manager-gui,admin-gui"/>
```

Votre fichier final peut, par exemple, se présenter ainsi :

```
   <tomcat-users xmlns="http://tomcat.apache.org/xml"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
            version="1.0">
      <role rolename="tomcat"/>
      <user username="tomcatuser" password="changemepassword" roles="tomcat,manager-gui,admin-gui"/>
      </tomcat-users>
```

c. Enregistrez et fermez le fichier.

Téléchargement et installation de l'environnement applicatif (Application web Java)

d. De même, mettez à jour *context.xml* de l'application Host Manager :

```
sudo nano /opt/tomcat/webapps/host-manager/META-INF/context.xml
```

e. Enregistrez et fermez le fichier.

11. Pour mettre à jour le serveur avec les modifications, redémarrez le service Tomcat :

```
sudo systemctl restart tomcat
```

12. Ouvrez un navigateur dans le même réseau que votre système Azure Stack Hub, puis ouvrez votre serveur : *yourmachine.local.Cloudapp.azurestack.external:8080*.

a. Pour voir l'état du serveur Tomcat et vérifier que vous y avez accès, sélectionnez **Server Status**.

b. Connectez-vous avec vos informations d'identification Tomcat.

CHAPITRE 1

Administrer un site web avec des machines virtuelles

1. Création de la VM
2. Téléchargement et installation de l'environnement applicatif
3. **Déploiement d'un site web**

Déployer et exécuter l'application

1. Connectez-vous à votre machine virtuelle en utilisant votre client SSH. Pour obtenir des instructions
2. Pour mettre à jour le serveur avec votre package d'application, arrêtez le service Tomcat :

```
sudo systemctl stop tomcat
```

3. Pour pouvoir écrire dans le dossier webapps, ajoutez l'utilisateur FTP au groupe Tomcat. Cet utilisateur est celui que vous avez défini quand vous avez créé votre machine virtuelle dans Azure Stack Hub.

```
sudo usermod -a -G tomcat <VM-user>
```

4. Pour effacer le dossier webapps, puis charger votre fichier WAR créé ou mis à jour, connectez-vous à votre machine virtuelle avec FileZilla. Pour obtenir des instructions, consultez (https://docs.microsoft.com/fr-fr/azure-stack/user/azure-stack-dev-start-howto-ssh-public-key?view=azs-2206#connect-with-sftp-with-filezilla)
    a. Effacez le dossier *TOMCAT_HOME/webapps*.
    b. Ajoutez votre fichier WAR au dossier *TOMCAT_HOME/webapps* (par exemple, */opt/tomcat/webapps/*).
5. Tomcat développe et déploie automatiquement l'application. Vous pouvez la voir en utilisant le nom DNS que vous avez créé auparavant.

CHAPITRE 2

Administrer un site web avec un service géré (PaaS)

Ce que vous allez apprendre dans ce chapitre :

- Provisionner une plateforme applicative PaaS
- Mettre à l'échelle selon un événement
- Mettre à l'échelle selon une planification
- Appréhender la notion du la serverless

4 heures

CHAPITRE 2

Administrer un site web avec un service géré (PaaS)

1. **Provisionnement de la plateforme d'hébergement**
2. Mise à l'échelle basée sur un événement
3. Mise à l'échelle basée sur une planification
4. Abstraction des serveurs avec serverless

Provisionnement de la plateforme d'hébergement

Les services d'hébergement Cloud vous donnent accès à un hébergement hautes performances, évolutif et fiable fourni dans un modèle d'infrastructure en tant que service (IaaS) avec des serveurs à charge équilibrée.

Ceux-ci sont proposés par des fournisseurs de services d'hébergement Cloud et des fournisseurs de services gérés pour les entreprises de toutes tailles.

Les services d'hébergement Cloud sont couramment utilisés par les grandes entreprises, les établissements d'enseignement, les services de santé, les agences gouvernementales ou d'autres organisations. Les sociétés d'hébergement Cloud peuvent offrir une variété de services de paiement à l'utilisation.

méthode d'approvisionnement:

- Le service d'approvisionnement **Azure AD** gère l'approvisionnement et l'approvisionnement d'utilisateurs d'Azure AD vers votre application (approvisionnement sortant) et de votre application vers Azure AD (approvisionnement entrant). Le service se connecte aux points de terminaison de l'API de gestion des utilisateurs SCIM (System for Inter-Domain Identity Management) fournis par votre application.
- Lorsque vous utilisez Microsoft Graph, votre application gère l'approvisionnement entrant et sortant des utilisateurs et des groupes d'Azure AD vers votre application en interrogeant l'API Microsoft Graph.
- L'approvisionnement d'utilisateurs SAML JIT (Security Assertion Markup Language Just in Time) peut être activé si votre application utilise SAML pour la fédération. Les informations de revendication envoyées dans le jeton SAML sont utilisées pour approvisionner les utilisateurs.

Provisionnement de la plateforme d'hébergement

Azure App Service est le moyen le plus rapide et le plus simple d'héberger des applications web et des API dans Azure. Azure App Service fournit une solution d'hébergement de plateforme en tant que service entièrement gérée qui prend en charge les applications .NET, Java, JavaScript et Python. Les options d'hébergement sont disponibles sur Windows et Linux en fonction du runtime d'application.

Azure App Service correctifs et gère automatiquement les infrastructures de système d'exploitation et de langage pour vous. App Service prend également en charge la mise à l'échelle automatique, la haute disponibilité et les emplacements de déploiement afin de passer votre temps à créer de grandes applications plutôt que de vous soucier des problèmes d'infrastructure.

Azure App Service prend également en charge l'exécution d'applications web conteneurisées. Les conteneurs personnalisés offrent aux applications hébergées dans app service un accès complet au système d'exploitation sous-jacent et permettent d'héberger des applications web à l'aide de n'importe quelle pile d'applications tout en tirant parti des fonctionnalités telles que la mise à l'échelle automatique et la haute disponibilité fournies par Azure App Service.

Static Web Apps est un service qui génère et déploie automatiquement des applications web de pile complète sur Azure à partir d'un dépôt de code. Azure Static Web Apps interagit directement avec GitHub ou Azure DevOps pour surveiller, générer et déployer automatiquement des modifications à partir d'un référentiel de code chaque fois qu'une demande de validation ou de tirage se produit sur une branche spécifiée.

Les applications web statiques sont généralement créées à l'aide de bibliothèques et de frameworks tels que Angular, React, Svelte, Vue ou Blazor où le rendu côté serveur n'est pas requis. En outre, Azure Static Web Apps support Azure'utilisation d'une architecture d'API serverless par le biais d'une API Azure Functions intégrée ou d'une liaison à une application Azure Functions existante.

Provisionnement de la plateforme d'hébergement

Azure Spring Apps Pour les microservices Spring Boot, Azure Spring Apps fournit un service managé qui facilite l'exécution de ces services dans Azure. Aucune modification de code n'est requise pour exécuter ces services dans Azure. Le service gère l'infrastructure des applications Spring Cloud, ce qui permet aux développeurs de se concentrer sur leur code. Azure Spring Apps assure la gestion du cycle de vie en utilisant des outils complets, tels que la supervision et les diagnostics, la gestion des configurations, la découverte de services, l'intégration CI/CD, les déploiements bleus-verts, etc.

Azure Kubernetes Services est un service d'orchestration de conteneurs entièrement géré qui peut être utilisé pour déployer, mettre à l'échelle et gérer des conteneurs Docker et des applications basées sur des conteneurs dans un environnement de cluster. Azure Kubernetes Service simplifie le déploiement de clusters Kubernetes managés dans Azure en déchargeant la surcharge opérationnelle comme la surveillance et la maintenance de l'intégrité, de sorte que vous n'avez qu'à gérer et à gérer les nœuds de l'agent.

Azure Kubernetes Service vous permet de créer et d'exécuter des applications modernes, portables et basées sur des microservices à l'aide d'applications sans état et avec état à mesure que les équipes progressent dans l'adoption des applications basées sur des microservices.

Azure Container Instances est un service managé qui vous permet d'exécuter des conteneurs directement sur Azure, sans avoir à gérer des machines virtuelles et sans avoir à adopter un service de niveau supérieur. Azure Container Instances est une solution qui convient à tous les scénarios qui peuvent fonctionner dans des conteneurs isolés, notamment les applications simples, l'automatisation des tâches et les tâches de build. Azure Container Instances peut démarrer des conteneurs dans Azure en quelques secondes, sans avoir à configurer ni gérer des machines virtuelles.

CHAPITRE 2

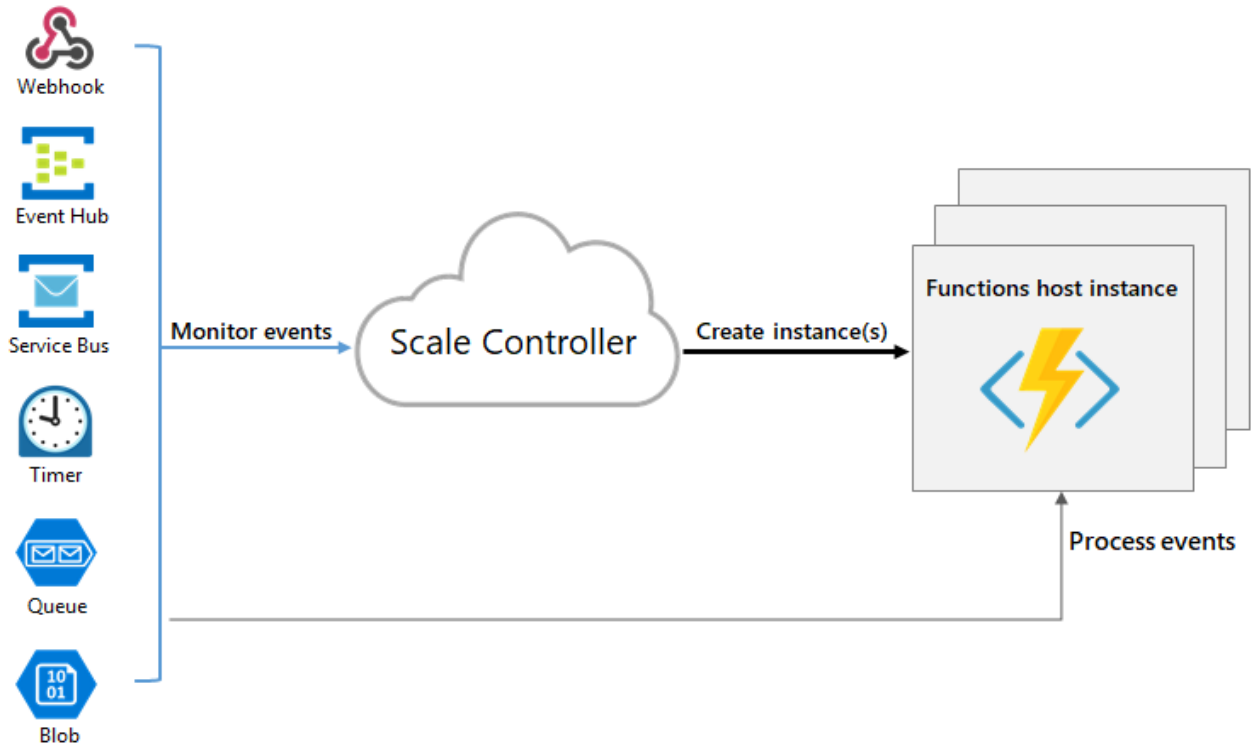
Administrer un site web avec un service géré (PaaS)

1. Provisionnement de la plateforme d'hébergement
2. **Mise à l'échelle basée sur un événement**
3. Mise à l'échelle basée sur une planification
4. Abstraction des serveurs avec serverless

Mise à l'échelle du runtime

Azure Functions utilise un composant appelé *contrôleur de mise à l'échelle* pour surveiller la fréquence des événements et déterminer s'il convient d'effectuer un scale-out ou un scale-in. Le contrôleur de mise à l'échelle utilise une méthode heuristique pour chaque type de déclencheur. Par exemple, si vous utilisez un déclencheur de stockage File d'attente Azure, il est mis à l'échelle en fonction de la longueur de la file d'attente et de l'âge du plus ancien message en file d'attente.

L'unité d'échelle pour Azure Functions est la Function App. Quand les instances de l'application de fonction font l'objet d'une augmentation de taille, des ressources supplémentaires sont allouées pour exécuter plusieurs instances de l'hôte Azure Functions. À l'inverse, quand la demande de calcul est réduite, le contrôleur de mise à l'échelle supprime des instances de l'hôte de fonction. Le nombre d'instances est finalement réduit à zéro si aucune fonction n'est exécutée dans une application de fonction.



PARTIE 4

Démarrage à froid

Une fois que votre application de fonction a été inactive pendant quelques minutes, la plateforme peut effectuer un scale-down à zéro du nombre d'instances sur lesquelles votre application s'exécute. La prochaine requête présente la latence supplémentaire de la mise à l'échelle de zéro à un. Cette latence est appelée *démarrage à froid*. Le nombre de dépendances requises par votre application de fonction peut avoir un impact sur le temps de démarrage à froid. Le démarrage à froid est plus problématique pour les opérations synchrones, telles que les déclencheurs HTTP, qui doivent retourner une réponse. Si les démarrages à froid ont un impact sur vos fonctions, envisagez l'exécution dans un plan Premium ou dans un plan Dedicated avec le paramètre **Always-on** activé.

Limiter le scale-out

Vous souhaiterez peut-être limiter le nombre maximal d'instances utilisées par une application pour effectuer un scale-out. C'est le cas le plus fréquent lorsqu'un composant en aval comme une base de données a un débit limité. Par défaut, les fonctions du plan Consommation effectuent un scale-out jusqu'à 200 instances, et les fonctions du plan Premium jusqu'à 100 instances. Vous pouvez spécifier une valeur maximale inférieure pour une application spécifique en modifiant la valeur `functionAppScaleLimit`. Le `functionAppScaleLimit` peut être défini sur `0` ou sur `null` pour une utilisation sans restriction, ou sur une valeur valide comprise entre 1 et le maximum de l'application.

Azure PowerShell

```
$resource = Get-AzResource -ResourceType Microsoft.Web/sites -ResourceGroupName <RESOURCE_GROUP> -Name <FUNCTION_APP-
   NAME>/config/web

$resource.Properties.functionAppScaleLimit = <SCALE_LIMIT>

$resource | Set-AzResource -Force
```

PARTIE 4

CHAPITRE 2

Administrer un site web avec un service géré (PaaS)

1. Provisionnement de la plateforme d'hébergement
2. Mise à l'échelle basée sur un événement
3. **Mise à l'échelle basée sur une planification**
4. Abstraction des serveurs avec serverless

Créer un plan de mise à l'échelle

Maintenant que vous avez attribué le rôle Contributeur de mise sous et hors tension de la virtualisation de Bureau au principal de service sur vos abonnements, vous pouvez créer un plan de mise à l'échelle. Pour créer un plan de mise à l'échelle :

1. Ouvrez le portail Azure.
2. Dans la barre de recherche, tapez *Azure Virtual Desktop* et sélectionnez l'entrée de service correspondante.
3. Sélectionnez **Plans de mise à l'échelle**, puis sélectionnez **Créer**.
4. Sous l'onglet **Principes de base**, regardez sous **Détails du projet**, puis sélectionnez le nom de l'abonnement auquel vous allez attribuer le plan de mise à l'échelle.
5. Si vous souhaitez créer un nouveau groupe de ressources, sélectionnez **Créer**. Si vous souhaitez utiliser un groupe de ressources existant, sélectionnez son nom dans le menu déroulant.
6. Entrez un nom pour le plan de mise à l'échelle dans le champ **Nom**.
7. Si vous le souhaitez, vous pouvez également ajouter un nom « convivial » qui sera affiché pour vos utilisateurs et une description pour votre plan.

Créer un plan de mise à l'échelle

5. Si vous le souhaitez, vous pouvez également ajouter un nom « convivial » qui sera affiché pour vos utilisateurs et une description pour votre plan.
6. Pour **Région**, sélectionnez une région pour votre plan de mise à l'échelle. Les métadonnées pour l'objet seront stockées dans la zone géographique associée à la région.
7. Pour **Fuseau horaire**, sélectionnez le fuseau horaire à utiliser avec votre plan.
8. Dans **Étiquettes d'exclusion**, entrez un nom d'étiquette pour les machines virtuelles que vous ne souhaitez pas inclure dans les opérations de mise à l'échelle. Par exemple, vous pouvez baliser les machines virtuelles configurées en mode maintenance afin que la mise à l'échelle automatique ne remplace pas le mode de maintenance pendant la maintenance à l'aide de l'étiquette d'exclusion « excludeFromScaling ». Si vous avez défini « excludeFromScaling » comme champ de nom d'étiquette sur l'une des machines virtuelles du pool d'hôtes, la mise à l'échelle automatique ne démarre pas, ne s'arrête pas ou ne modifie pas le mode de maintenance de ces machines virtuelles particulières.
9. Sélectionnez **Suivant** pour accéder à l'onglet **Planifications**.

Configurer une planification

Les planifications vous permettent de définir le moment où la mise à l'échelle automatique active les modes Augmentation et Diminution au cours de la journée. Dans chaque phase de la planification, la mise à l'échelle automatique ne désactive les machines virtuelles que lorsque la capacité du pool d'hôtes utilisée ne dépasse pas le seuil de capacité. Les valeurs par défaut que vous voyez quand vous essayez de créer une planification sont les valeurs suggérées pour les jours de la semaine, mais vous pouvez les modifier si nécessaire.

Pour créer ou modifier une planification :

1. Sous l'onglet **Planifications**, sélectionnez **Ajouter une planification**.
2. Entrez un nom pour votre planification dans le champ **Nom de la planification**.
3. Dans le champ **Répéter**, sélectionnez les jours où votre planification va se répéter.
4. Sous l'onglet **Augmentation**, renseignez les champs suivants :
    - Pour **Heure de début**, sélectionnez une heure dans le menu déroulant pour commencer à préparer les machines virtuelles pour les heures de pointe de l'activité.
    - Pour **Algorithme d'équilibrage de charge**, nous recommandons de sélectionner **Algorithme de parcours en largeur**. L'équilibrage de charge en largeur d'abord va distribuer les utilisateurs sur les machines virtuelles existantes pour conserver des temps d'accès rapides.
    - Pour **Pourcentage minimal d'hôtes**, entrez le pourcentage d'hôtes de session que vous souhaitez toujours conserver dans cette phase. Si le pourcentage que vous entrez n'est pas un nombre entier, il est arrondi au nombre entier supérieur le plus proche. Par exemple, dans un pool d'hôtes de sept hôtes de session, si vous définissez le pourcentage minimal d'hôtes pendant les heures d'accélération sur **10 %**, une machine virtuelle restera toujours active pendant les heures d'accélération et ne sera pas désactivée par la mise à l'échelle automatique.

Configurer une planification

- Pour **Seuil de capacité**, entrez le pourcentage de capacité du pool d'hôtes disponible qui doit déclencher une action de mise à l'échelle. Par exemple, si deux hôtes de session dans le pool d'hôtes présentant une limite de session maximale de 20 sont activés, la capacité du pool d'hôtes disponible est de 40. Si vous définissez le seuil de capacité sur **75 %** et que les hôtes de session possèdent plus de 30 sessions utilisateur, la mise à l'échelle automatique active un troisième hôte de session. Cela permet de modifier la capacité du pool d'hôtes disponible pour passer de 40 à 60.

5. Sous l'onglet **Heures de pointe**, renseignez les champs suivants :

- Pour le champ **Heures de début**, entrez une heure de début pour la période où le taux d'utilisation est le plus élevé au cours de la journée. Veillez à ce que l'heure soit dans le même fuseau horaire que celui que vous avez spécifié pour votre plan de mise à l'échelle. Cette heure correspond également à l'heure de fin de la phase d'augmentation.
- Pour **Équilibrage de charge**, vous pouvez sélectionner l'équilibrage de charge en largeur d'abord ou l'équilibrage de charge en profondeur d'abord. L'équilibrage de charge de largeur répartit les nouvelles sessions utilisateur entre tous les hôtes de session du pool. L'équilibrage de charge en profondeur d'abord répartit les nouvelles sessions utilisateur sur un hôte de session disponible qui a le plus grand nombre de connexions sans avoir encore atteint sa limite maximale de sessions.
- Pour **Diminution**, vous entrez des valeurs dans des champs similaires à **Augmentation**, mais cette fois-ci, c'est pour le moment où l'utilisation du pool d'hôtes diminue. Ceci comprend les champs suivants :
    - Heure de début
    - Algorithme d'équilibrage de charge
    - Pourcentage minimal d'hôtes (%)
    - Seuil de capacité (%)
    - Forcer la déconnexion des utilisateurs

CHAPITRE 2

Administrer un site web avec un service géré (PaaS)

1. Provisionnement de la plateforme d'hébergement
2. Mise à l'échelle basée sur un événement
3. Mise à l'échelle basée sur une planification
4. **Abstraction des serveurs avec serverless**

Conception d'architecture des fonctions serverless

L'architecture *serverless* fait évoluer les plateformes du Cloud vers du code natif Cloud pur en faisant abstraction du code de l'infrastructure qu'il doit exécuter.Azure Functions est une option de calcul serverless qui prend en charge les *fonctions*, de petits morceaux de code qui effectuent des opérations uniques.

Les avantages de l'utilisation d'architectures serverless avec des applications Functions sont les suivants :

- L'infrastructure Azure fournit automatiquement tous les serveurs mis à jour dont les applications ont besoin pour s'exécuter à grande échelle.
- Les ressources de calcul sont allouées dynamiquement et se mettent à l'échelle automatiquement et instantanément pour répondre aux demandes élastiques. Serverless, cela ne signifie pas « aucun serveur », mais « moins de serveur », car les serveurs s'exécutent uniquement en fonction des besoins.
- La micro-facturation permet d'économiser les coûts en facturant uniquement les ressources de calcul et la durée d'exécution du code.
- Les *liaisons* de fonctions simplifient l'intégration en fournissant un accès déclaratif à une large gamme de services Azure et tiers.

Les fonctions sont *pilotées par les événements*. Un événement externe comme une requête web HTTP, un message, une planification ou une modification des données *déclenche* le code de la fonction. Une application Functions ne code pas le déclencheur, mais uniquement la réponse au déclencheur. Avec une barrière inférieure à l'entrée, les développeurs peuvent se concentrer sur la logique métier, plutôt que sur l'écriture de code pour gérer les problèmes liés à l'infrastructure tels que la messagerie.

Azure Functions est un service géré dans Azure et Azure Stack. Le runtime Functions open source fonctionne dans de nombreux environnements, notamment Kubernetes, Azure IoT Edge, localement et d'autres Clouds.

Serverless et Functions nécessitent de nouvelles méthodes de pensée et de nouvelles approches pour la création d'applications. Ils ne constituent pas les solutions adaptées à chaque problème.

Étapes d'implémentation des fonctions serverless

La réussite de l'implémentation de technologies serverless avec Azure Functions nécessite les actions suivantes :

- Décider et planifier
- Les architectes et décideurs techniques (TDM) effectuent une évaluation des applications, dirigent des ateliers et des formations techniques ou y assistent, exécutent des projets pilote ou preuve de concept (PoC), et dirigent des sessions de conception architecturale en fonction des besoins.
- Développer et déployer des applications
- Les développeurs implémentent des modèles et pratiques de développement d'applications Functions serverless, configurent des pipelines DevOps et utilisent les meilleures pratiques SRE (Site Reliability Engineering).
- Gestion des opérations
- Les professionnels de l'informatique identifient les configurations d'hébergement, la scalabilité durable en automatisant l'approvisionnement de l'infrastructure et maintiennent la disponibilité en planifiant la continuité d'activité et la reprise d'activité.
- Applications sécurisées
- Les professionnels de la sécurité gèrent les notions de base en matière de sécurité Azure Functions, sécurisent la configuration de l'hébergement et fournissent des conseils en matière de sécurité des applications.

PARTIE 5

Déployer la conteneurisation

Dans ce module, vous allez :

- Connaitre les concepts de base de la conteneurisation
- Gérer les images des conteneurs

6 heures

CHAPITRE 1

Connaitre les concepts de base de la conteneurisation

Ce que vous allez apprendre dans ce chapitre :

- Comprendre le concept de la conteneurisation
- Gérer des images des conteneurs
- Implémenter un conteneur

2 heures

CHAPITRE 1

Connaitre les concepts de base de la conteneurisation

1. **Utilisation de Dockerfile**
2. Différentiation entre les registres privés et publiques

Migrer une application vers Azure App Service à l'aide d'un conteneur personnalisé

App Services utilise la technologie de conteneur Docker pour héberger à la fois des images prédéfinies et des images personnalisées. Pour voir une liste d'images prédéfinies, exécutez la commande Azure CLI az webapp list-runtimes --os linux . Si ces images ne répondent pas à vos besoins, vous pouvez générer et déployer une image personnalisée.

1. Configurer votre environnement initial
2. Examiner le fichier Docker
3. Générer et tester l'image localement
4. Créer un groupe de ressources
5. Envoyer l'image vers Azure Container Registry
6. Configurer App Service pour déployer l'image à partir du registre
7. Déployer l'image et tester l'application

01- Configurer votre environnement initial

- Installer Docker, que vous utilisez pour générer des images Docker :

L'installation peut se faire en téléchargeant le fichier d'installation à travers le site www.docker.com

Après avoir installé Docker, ouvrez une fenêtre de terminal et vérifiez que Docker est installé

docker –version

- Cloner l'exemple de dépôt :

Sur un invité de commande, exécutez la commande suivante :

git clone https://github.com/Azure-Samples/docker-django-webapp-linux.git --config core.autocrlf=input

L'argument --config core.autocrlf=input est pour garantir des fins de ligne appropriées dans les fichiers qui sont utilisés dans le conteneur Linux.

- Accéder ensuite au dossier :

cd docker-django-webapp-linux

02. Examiner le fichier Docker

```
FROM tiangolo/uwsgi-nginx-flask:python3.6
RUN mkdir /code
WORKDIR /code
ADD requirements.txt /code/
RUN pip install -r requirements.txt --no-cache-dir
ADD . /code/
ENV SSH_PASSWD "root:Docker!"
RUN apt-get update \
    && apt-get install -y --no-install-recommends dialog \
    && apt-get update \
&& apt-get install -y --no-install-recommends openssh-server \
&& echo "$SSH_PASSWD" | chpasswd
COPY sshd_config /etc/ssh/
COPY init.sh /usr/local/bin/
RUN chmod u+x /usr/local/bin/init.sh
•EXPOSE 8000 2222
• ENTRYPOINT ["init.sh"]
```

- Le premier groupe de commandes installe la configuration requise de l'application dans l'environnement.
- Le deuxième groupe de commande crée un serveur SSH pour sécuriser la communication entre le conteneur et l'hôte.
- Dans `ENTRYPOINT ["init.sh"]`, la dernière ligne appelle `init.sh` pour démarrer le service SSH et le serveur Python.

03- Générer et tester l'image localement

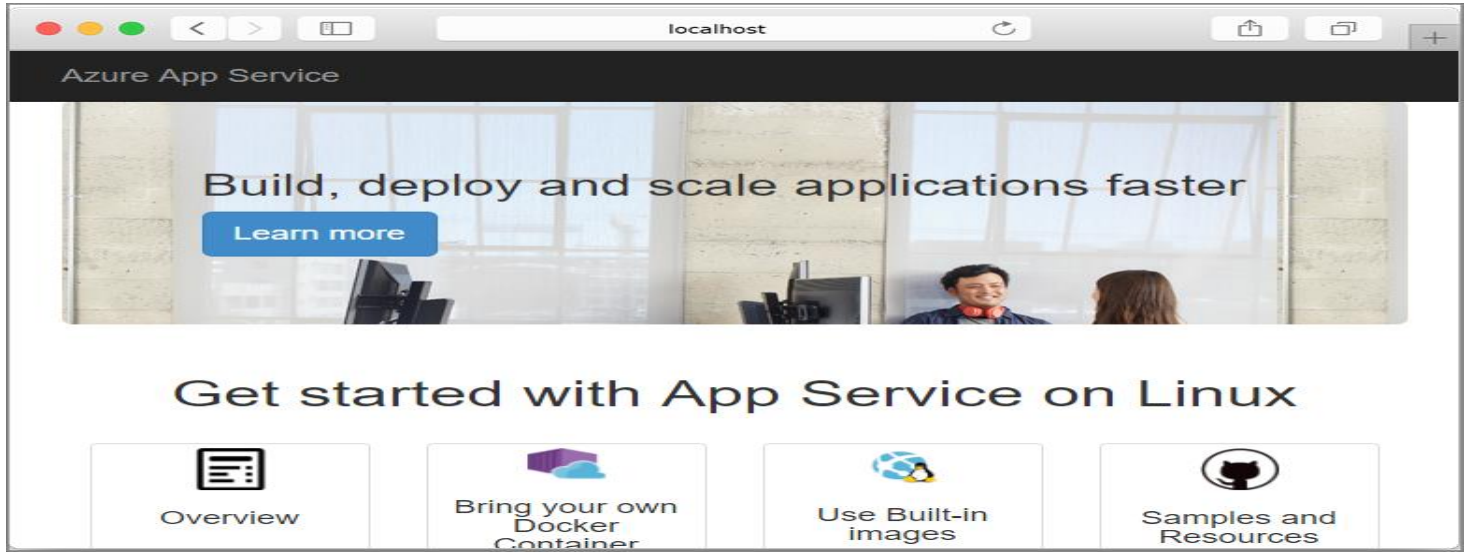
- Exécuter la commande suivante pour générer l'image :

```
docker build --tag appsvc-tutorial-custom-image .
```

- Vérifier que la build fonctionne en exécutant le conteneur Docker localement :

```
docker run -it -p 8000:8000 appsvc-tutorial-custom-image
```

- Cette commande `docker run` spécifie le port avec l'argument `-p` suivi du nom de l'image. `-it` vous permet de l'arrêter avec `Ctrl+C`.
- Accéder à `http://localhost:8000` pour vérifier que l'application web et le conteneur fonctionnent correctement.



04- Créer un groupe de ressources sur Azure

- Dans cette section et celles qui suivent, vous préparez des ressources dans Azure vers lesquelles vous allez envoyer (push) l'image, puis déployer un conteneur sur Azure App Service. Vous allez commencer par créer un groupe de ressources dans lequel collecter toutes les ressources.
- Exécuter la commande az group pour créer un groupe de ressources :

```
az group create --name myResourceGroup --location westeurope
```

- Vous pouvez changer la valeur `--location` pour spécifier une région proche de chez vous.

05- Envoyer l'image vers Azure Container Registry

1. Exécuter la commande az acr creat pour créer un registre de conteneurs Azure (Azure Container Registry) :

```
az acr create --name <registry-name> --resource-group myResourceGroup --sku Basic --admin-enabled true
```

2. Remplacer `<registry-name>` par un nom approprié pour votre registre. Le nom ne doit contenir que des lettres et des chiffres, et doit être unique dans tout Azure.

Exécutez la commande az acr show afin de récupérer les informations d'identification pour le registre :

```
az acr credential show --resource-group myResourceGroup --name <registry-name>
```

La sortie JSON de cette commande fournit deux mots de passe, ainsi que le nom d'utilisateur du registre.

3. Utiliser la commande `docker login` pour vous connecter au registre de conteneurs :

```
docker login <registry-name>.azurecr.io --username <registry-username>
```

Remplacer `<registry-name>` et `<registry-username>` par les valeurs des étapes précédentes. Lorsque vous y êtes invité, tapez l'un des mots de passe de l'étape précédente.

Vous utilisez le même nom de registre dans toutes les étapes restantes de cette section.

4. Une fois la connexion établie, étiqueter votre image Docker locale dans le registre :

```
docker tag appsvc-tutorial-custom-image <registry-name>.azurecr.io/appsvc-tutorial-custom-image:latest
```

5. Utiliser la commande `docker push` pour envoyer (push) l'image vers le registre :

```
docker push <registry-name>.azurecr.io/appsvc-tutorial-custom-image:latest
```

06- Configurer App Service pour déployer l'image à partir du registre

Pour déployer un conteneur sur Azure App Service, vous commencez par créer une application web sur App Service, puis vous connectez l'application web au registre de conteneurs. Quand l'application web démarre, App Service tire (pull) automatiquement l'image du registre.

- Créer un plan App Service à l'aide de la commande az appservice plan create:
- `az appservice plan create --name myAppServicePlan --resource-group myResourceGroup --is-linux`

Un plan App Service correspond à la machine virtuelle qui héberge l'application web.

- Créer l'application web à l'aide de la commande `az webapp create` :
- `az webapp create --resource-group myResourceGroup --plan myAppServicePlan --name <app-name> --deployment-container-image-name <registry-name>.azurecr.io/appsvc-tutorial-custom-image:latest`

Remplacer `<app-name>` par le nom de l'application web, qui doit être unique dans tout Azure. Remplacez également `<registry-name>` par le nom de votre registre spécifié à la section précédente.

- Utiliser `az webapp config appsettings set` pour définir la variable d'environnement `WEBSITES_PORT` conformément aux attentes du code d'application :

```
az webapp config appsettings set --resource-group myResourceGroup --name <app-name> --settings WEBSITES_PORT=8000
```

06- Configurer App Service pour déployer l'image à partir du registre

- Activer l'identité gérée attribuée par le système pour l'application Web en utilisant la commande az webapp identity assign :

  az webapp identity assign --resource-group myResourceGroup --name <app-name> --query principalId --output tsv

Remplacez <app-name> par le nom que vous avez utilisé à l'étape précédente. La sortie de la commande (filtrée par les arguments --query et --output) est le principal du service de l'identité affectée, que vous utiliserez sous peu.

L'identité managée vous permet d'accorder des autorisations à l'application web pour accéder à d'autres ressources Azure sans qu'aucune information d'identification spécifique ne soit nécessaire.

- Récupérer votre ID d'abonnement avec la commande az account show Vous en aurez besoin à la prochaine étape :
- az account show --query id --output tsv

- Accorder à l'identité managée l'autorisation d'accéder au registre de conteneurs :
- az role assignment create --assignee <principal-id> --scope /subscriptions/<subscription-id>/resourceGroups/myResourceGroup/providers/Microsoft.ContainerRegistry/registries/<registry-name> --role "AcrPull"

Remplacer les valeurs suivantes :

- <principal-id> par l'ID de principal du service récupéré à partir de la commande az webapp identity assign.
- <registry-name> avec le nom de votre registre de conteneurs.
- <subscription-id> avec l'ID d'abonnement récupéré à partir de la commande az account show.

06- Configurer App Service pour déployer l'image à partir du registre

- Configurer votre application pour qu'elle utilise l'identité managée pour effectuer une extraction à partir d'Azure Container Registry.

Azure CLICopier

Essayer

```
az resource update --ids /subscriptions/<subscription-id>/resourceGroups/myResourceGroup/providers/Microsoft.Web/sites/<app-name>/config/web --set properties.acrUseManagedIdentityCreds=True
```

Remplacer les valeurs suivantes :

- `<subscription-id>` avec l'ID d'abonnement récupéré à partir de la commande `az account show`.
- `<app-name>` avec le nom de votre application web.
-

07- Déployer l'image et tester l'application

Vous pouvez effectuer ces étapes une fois que l'image est envoyée (par push) au registre de conteneurs et qu'App Service est entièrement provisionné.

1. Utiliser la commande az webapp config container set pour spécifier le registre de conteneurs et l'image à déployer pour l'application web :

az webapp config container set --name <app-name> --resource-group myResourceGroup --docker-custom-image-name <registry-name>.azurecr.io/appsvc-tutorial-custom-image:latest --docker-registry-server-url https://<registry-name>.azurecr.io

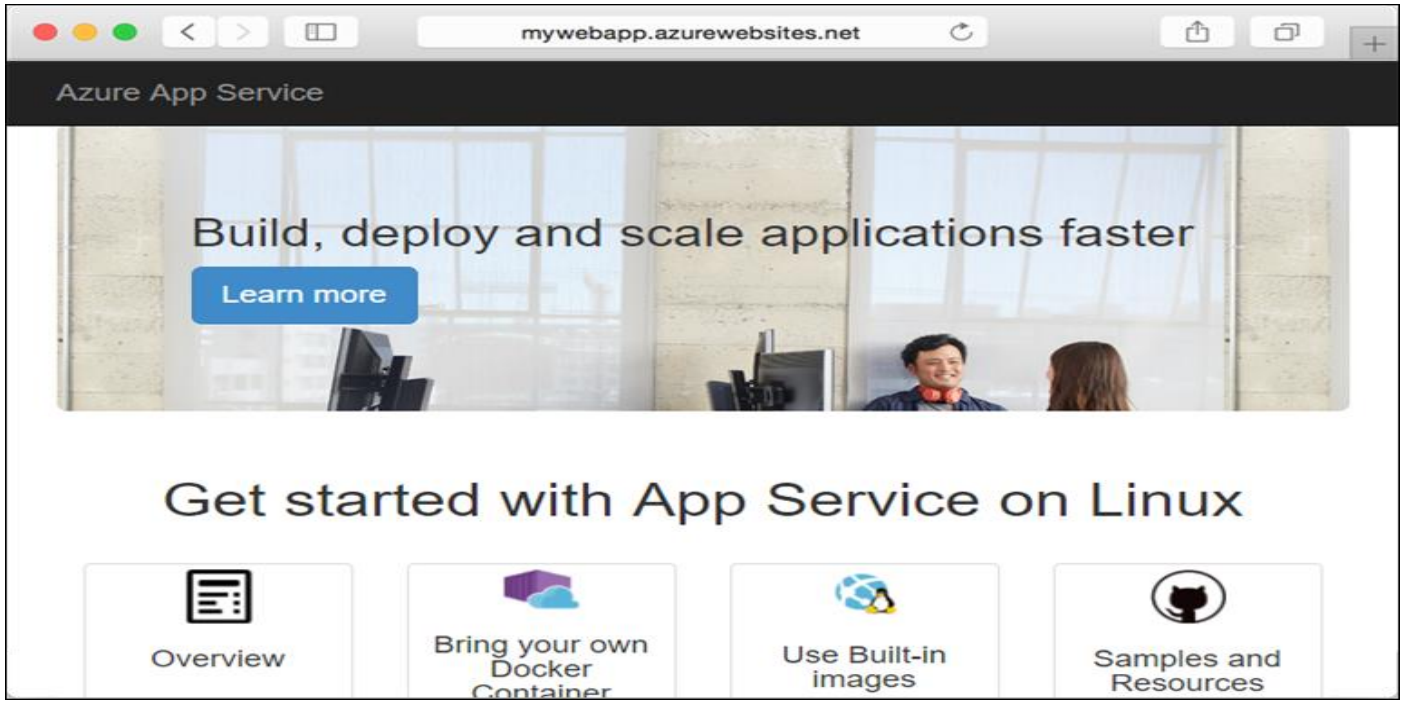
Remplacer <app-name> par le nom de votre application web et remplacer <registry-name> à deux endroits par le nom de votre registre.

- Quand vous utilisez un registre autre que Docker Hub (comme le montre cet exemple), --docker-registry-server-url doit être au format https:// suivi du nom de domaine complet du registre.
- Le message « No credential was provided to access Azure Container Registry. Trying to look up... » (Aucune information d'identification n'a été fournie pour accéder à Azure Container Registry. Tentative de recherche... ») indique qu'Azure utilise l'identité managée de l'application pour s'authentifier auprès du registre de conteneurs au lieu de demander un nom d'utilisateur et un mot de passe.
- Si vous rencontrez l'erreur, « AttributeError: 'NoneType' object has no attribute 'reserved' » (AttributeError : l'objet «NoneType » n'a pas d'attribut « reserved »), vérifiez que votre <app-name> est correct.

Pour tester l'application, accédez à https://<app-name>.azurewebsites.net, en remplaçant <app-name> par le nom de votre application web. Lorsque l'utilisateur accède à l'application pour la première fois, celle-ci peut mettre un certain temps à répondre, car App Service doit tirer (pull) l'image entière du registre. En cas d'expiration du délai d'attente du navigateur, actualisez simplement la page. Une fois l'image initiale tirée (pull), les tests suivants s'exécutent beaucoup plus rapidement.

07- Déployer l'image et tester l'application

2. Pour tester l'application, accédez à https://<app-name>.azurewebsites.net , en remplaçant <app-name> par le nom de votre application web. Lorsque l'utilisateur accède à l'application pour la première fois, celle-ci peut mettre un certain temps à répondre, car App Service doit tirer (pull) l'image entière du registre. En cas d'expiration du délai d'attente du navigateur, actualisez simplement la page. Une fois l'image initiale tirée (pull), les tests suivants s'exécutent beaucoup plus rapidement.



CHAPITRE 1

Connaitre les concepts de base de la conteneurisation

1. Utilisation de Dockerfile
2. **Différentiation entre les registres privés et publiques**

Définitions

- Registre de conteneurs :

  Un registre de conteneurs est un référentiel, ou un ensemble de référentiels, utilisé afin de stocker des images de conteneurs pour le développement d'applications conteneurisées, Kubernetes et le DevOps.

- Image de conteneur :
  - Une image de conteneur est une copie d'un conteneur (les fichiers et composants constitutifs d'une application), qui peut ensuite être multipliée pour une mise à l'échelle horizontale rapide ou déplacée vers d'autres systèmes selon les besoins. Une fois l'image de conteneur générée, elle devient un modèle à partir duquel il est possible de créer des applications ou de faire évoluer une application existante.
  - Pour pouvoir être utilisées, les images de conteneurs doivent d'abord être enregistrées quelque part. C'est là que le registre de conteneurs intervient. Ce registre est un emplacement qui sert à stocker des images de conteneurs et à les partager par le biais d'un processus de chargement (pushing) et de téléchargement (pulling). Une fois l'image transférée vers un autre système, l'application qu'elle contient peut y être exécutée.

Différence entre les registres privés et publiques

Les registres publics constituent une option idéale pour les individus ou les petites équipes qui souhaitent commencer à utiliser un registre aussi vite que possible. Ils offrent des capacités et des fonctions de base et sont faciles à prendre en main.

Parmi les registres publics on trouve **Docker Hub**, qui est un registre Docker et hébergé dans le Cloud. Il peut gérer le partage et le stockage des images Docker.

À l'aide de Docker Hub, les développeurs peuvent y accéder pour exploiter des images de centeneurs publiques.

Les registres privés fournissent un espace de stockage d'images de conteneurs sûr et confidentiel spécialement pensé pour les entreprises, hébergé sur site ou à distance.

Une entreprise peut choisir de créer et déployer son propre registre de conteneurs ou opter pour un service de registre privé disponible sur le marché. Ces registres privés intègrent souvent des fonctions de sécurité avancées et une assistance technique, comme la solution **Azure Container Registry**.

Azure Container Registry (En français : registres de conteneurs dans Azure) est un service de registre managé basé sur le registre Docker open source 2.0. Créez et tenez à jour des registres de conteneurs Azure pour stocker et gérer vos images de conteneur et les artefacts associés.

Les images conteneur peuvent être envoyées (push) et tirées (pull) avec Container Registry à l'aide de l'interface Docker CLI ou Azure CLI. Grâce à l'intégration au portail Azure, vous pouvez inspecter visuellement les images conteneur dans votre registre de conteneurs. Dans des environnements distribués, la fonctionnalité de géoréplication de Container Registry permet de distribuer des images conteneur aux différents centres de données Azure locaux.

Niveaux de service Azure Container Registry

Azure Container Registry est disponible dans plusieurs niveaux de service. Ces niveaux offrent une tarification prévisible et plusieurs options pour l'alignement en fonction de la capacité et des modèles d'utilisation de votre registre Docker privé dans Azure :

Niveau	Description
De base	Point d'entrée au coût optimisé pour les développeurs apprenant Azure Container Registry. Les registres De base ont les mêmes fonctionnalités de programmation que les registres Standard et Premium . Toutefois, le stockage inclus et le débit d'image sont parfaitement appropriés pour des scénarios d'utilisation inférieure.
Standard	Les registres Standard offrent les mêmes fonctionnalités que la version De base, avec un stockage inclus et un débit d'image accrus. Les registres Standard devraient satisfaire les besoins de la plupart des scénarios de production.
Premium	Les registres Premium fournissent la quantité la plus élevée de stockage inclus et d'opérations simultanées, permettant des scénarios impliquant des volumes importants. En plus d'un débit d'image plus élevé.

CHAPITRE 2

Gérer les images des conteneurs

Ce que vous allez apprendre dans ce chapitre :

- Gérer des registres des images
- Automatiser des déploiements

2 heures

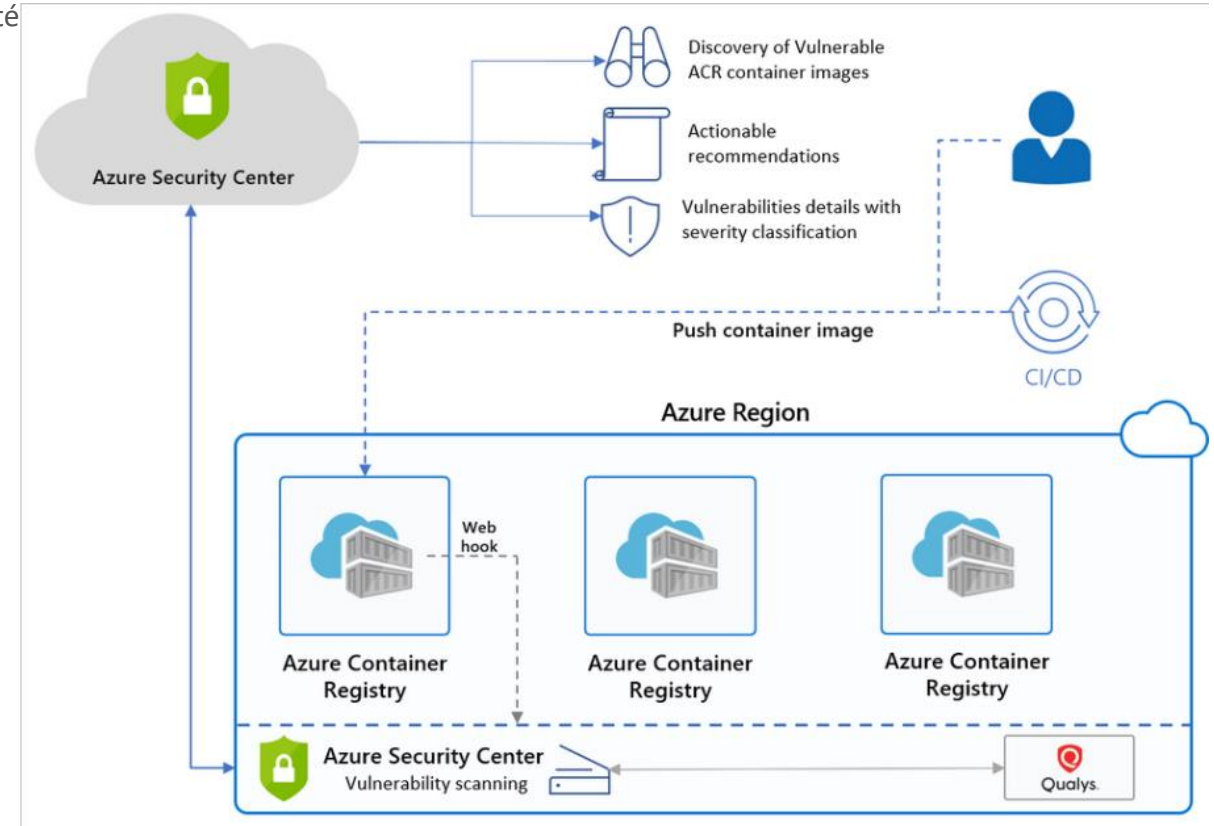
CHAPITRE 2

Gérer les images des conteneurs

1. **Gestion des registres des images**
2. Automatisation des déploiements

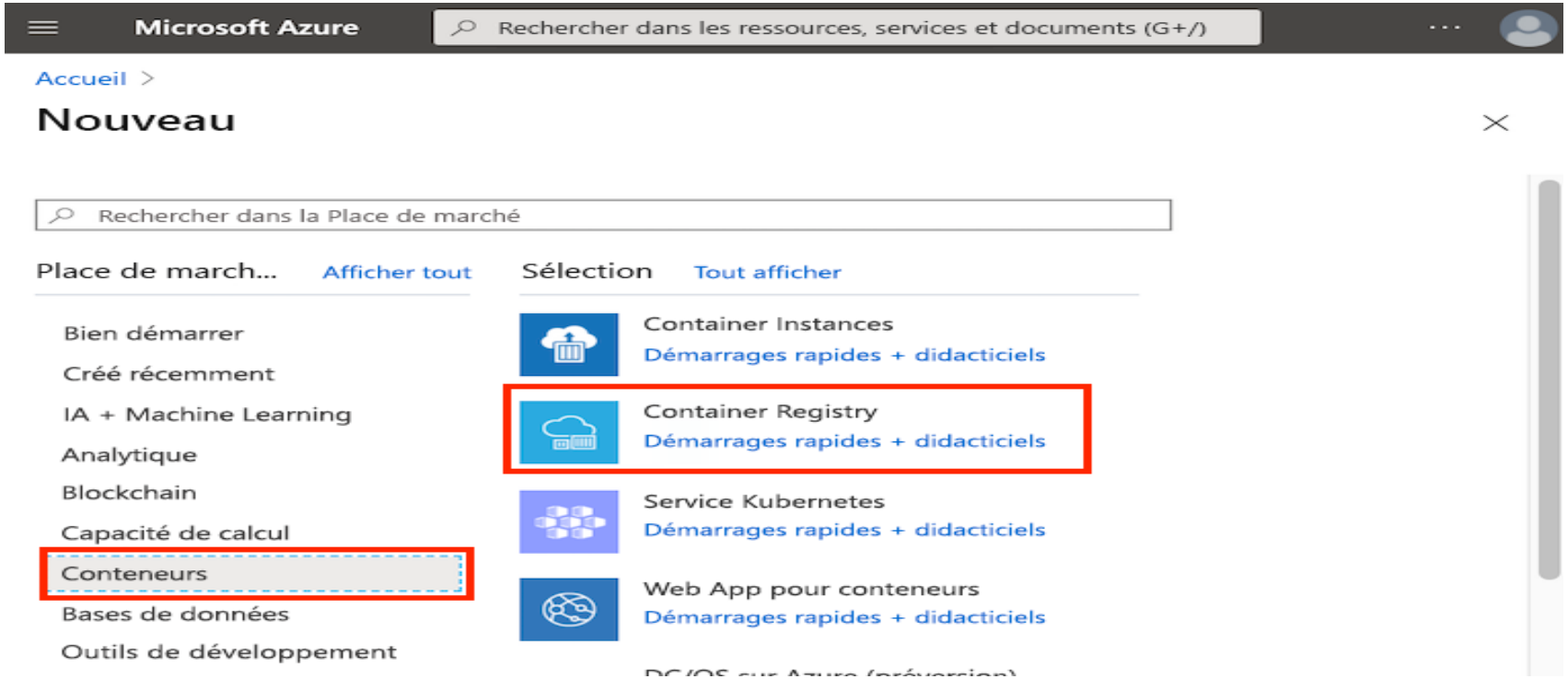
Azure Container Registry ACR

Azure Container Registry (ACR) est un service du Cloud public Azure. L'ACR se présente sous forme d'un registre privé d'images Docker. Ce dernier vous permet de générer et déployer les applications conteneurisées en toute sécurité



Créer un registre de conteneurs Azure à l'aide du portail Azure

Sélectionner **Créer une ressource**>**Conteneurs**>**Container Registry**.



PARTIE 5

Créer un registre de conteneurs Azure à l'aide du portail Azure

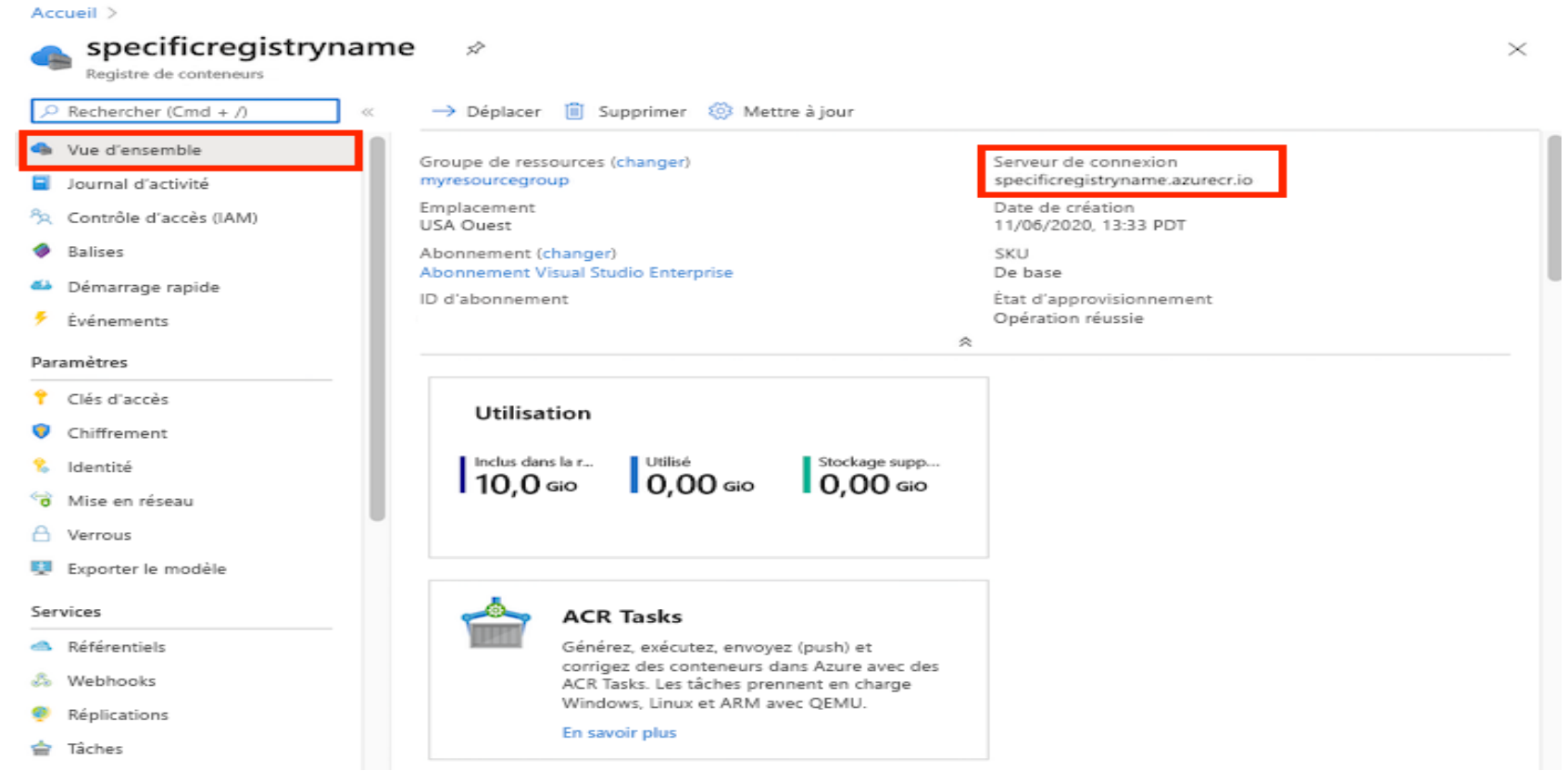
Sous l'onglet **Informations de base**, entrez les valeurs appropriées pour **Groupe de ressources** et **Nom du registre**. Le nom du registre doit être unique dans Azure et contenir entre 5 et 50 caractères alphanumériques. Pour ce guide de démarrage rapide, créez un groupe de ressources dans l'emplacement West US nommé myResourceGroup, et sélectionnez « De base » pour **SKU**.

Accepter les valeurs par défaut pour les autres paramètres. Sélectionnez ensuite **Passer en revue + créer** . Après avoir passé en revue les paramètres, sélectionnez **Créer**.

PARTIE 5

Créer un registre de conteneurs Azure à l'aide du portail Azure

Quand le message **Déploiement réussi** s'affiche, sélectionnez le registre de conteneurs dans le portail.



PARTIE 5

Se connecter au registre

Avant d'envoyer (push) et de tirer (pull) des images conteneur, vous devez vous connecter à l'instance du registre. Connectez-vous à Azure PowerShell sur votre ordinateur local, puis exécutez la cmdlet Connect-AzContainerRegistry. Spécifiez seulement le nom du registre au moment de la connexion avec Azure PowerShell. N'utilisez pas le nom complet du serveur de connexion.

```
Connect-AzContainerRegistry -Name <registry-name>
```

Une fois l'opération terminée, la commande renvoie Login Succeeded.

Envoyer l'image au registre

Pour envoyer une image dans un registre Azure Container Registry, vous devez tout d'abord disposer d'une image. Si vous n'avez pas encore d'images conteneur locales, exécutez la commande docker pull suivante pour tirer (pull) une image publique existante. Pour cet exemple, tirez l'image hello-world à partir de Microsoft Container Registry.

```
docker pull mcr.microsoft.com/hello-world
```

Avant d'envoyer (push) une image vers le registre, vous devez la marquer avec le nom complet de votre serveur de connexion au registre. Le nom du serveur de connexion est au format *<nom-registre>.azurecr.io* (obligatoirement tout en minuscules). Par exemple : *monregistreconteneurs.azurecr.io*.

Étiquetez l'image en utilisant la commande docker tag. Remplacez <login-server> par le nom du serveur de connexion de votre instance ACR.

```
docker tag mcr.microsoft.com/hello-world <login-server>/hello-world:v1
```

Exemple :

```
docker tag mcr.microsoft.com/hello-world  mycontainerregistry.azurecr.io/hello-world:v1
```

Pour finir, utilisez la commande docker push pour envoyer l'image vers l'instance du registre. Remplacez <login-server> par le nom du serveur de connexion de votre instance de registre. Cet exemple crée le référentiel **hello-world** qui contient l'image hello-world:v1.

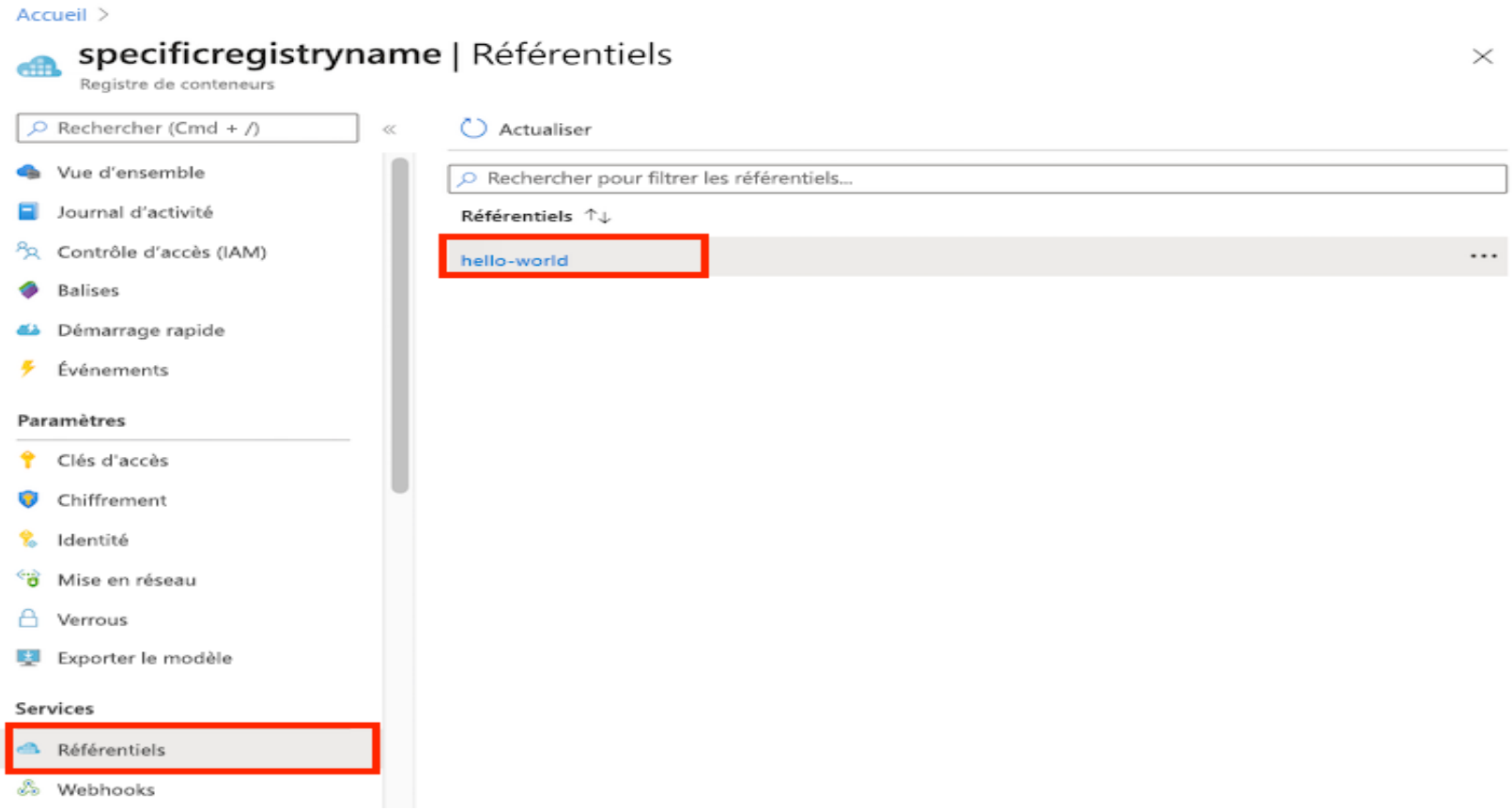
```
docker push <login-server>/hello-world:v1
```

Après avoir envoyé (push) l'image à votre registre de conteneurs, supprimez l'image hello-world:v1 de votre environnement Docker local. (Notez que cette commande docker rmi ne supprime pas l'image du référentiel **hello-world** dans votre registre de conteneurs Azure.)

```
docker rmi <login-server>/hello-world:v1
```

Répertorier les images conteneur

Pour lister les images de votre registre, accéder à ce registre dans le portail, sélectionnez **Référentiels**, puis le référentiel **hello-world** que vous avez créé avec docker push.



Exécuter l'image à partir du registre

Vous pouvez à présent extraire (pull) et exécuter l'image conteneur `hello-world:v1` à partir de votre registre de conteneurs à l'aide de docker run :

```
docker run <login-server>/hello-world:v1
```

Exemple de sortie :

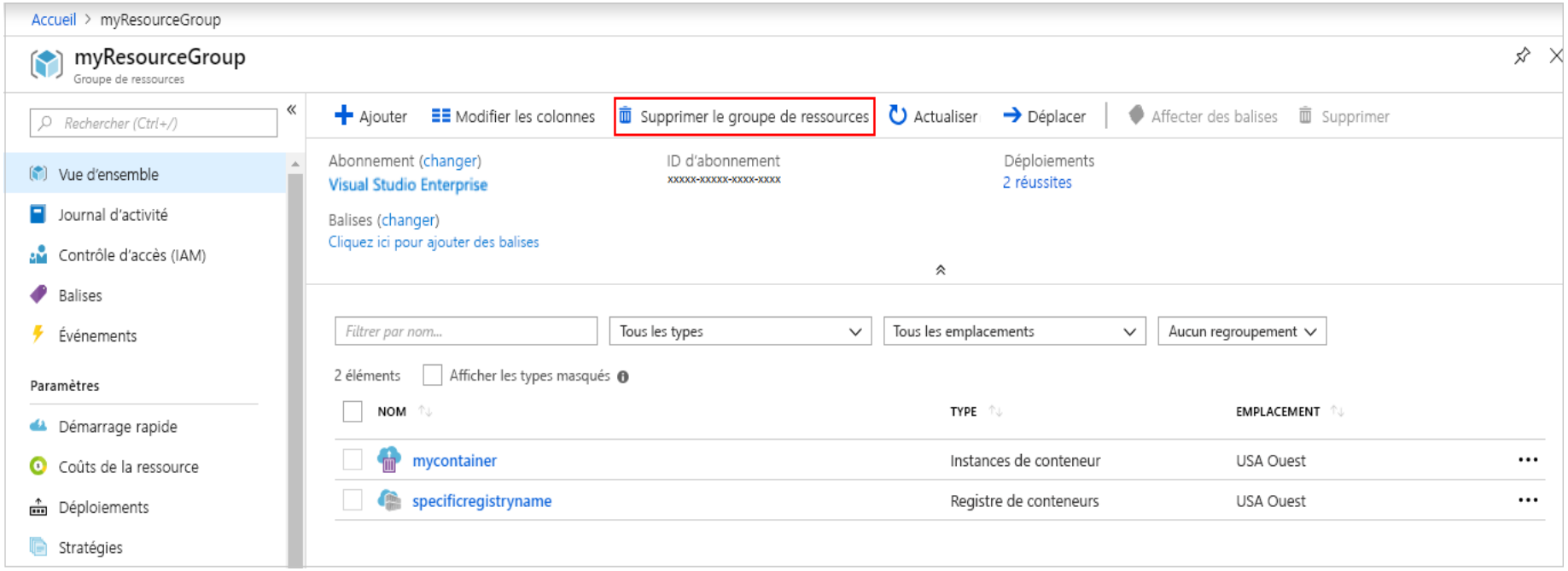
```
Unable to find image 'mycontainerregistry.azurecr.io/hello-world:v1' locally
v1: Pulling from hello-world
Digest: sha256:662dd8e65ef7ccf13f417962c2f77567d3b132f12c95909de6c85ac3c326a345
Status: Downloaded newer image for mycontainerregistry.azurecr.io/hello-world:v1

Hello from Docker!
This message shows that your installation appears to be working correctly.
```

PARTIE 5

Nettoyer les ressources

Pour supprimer vos ressources, accéder au groupe de ressources **myResourceGroup** dans le portail. Une fois le groupe de ressources chargé, cliquez sur **Supprimer le groupe de ressources** pour supprimer le groupe de ressources, le registre de conteneurs et les images conteneur stockées à cet endroit.



CHAPITRE 2

Gérer les images des conteneurs

1. Gestion des registres des images
2. **Automatisation des déploiements**

Automatisation des déploiements

L'automatisation du déploiement vous permet de déplacer des logiciels entre les environnements de test et de production à l'aide d'un processus automatisé. Cela garantit la reproductibilité et la fiabilité des déploiements tout au long du cycle de distribution.

L'automatisation du déploiement permet de lancer de nouvelles fonctions et applications plus rapidement et fréquemment, sans intervention humaine.

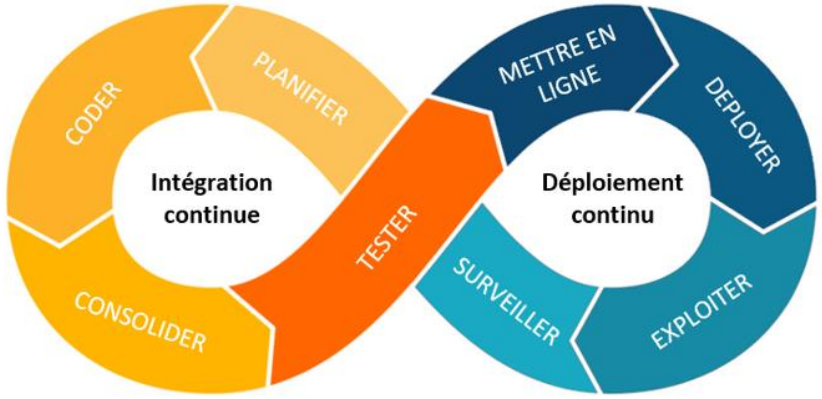
L'automatisation au service du DevOps

L'application des méthodologies CI/CD nécessite que les équipes de développement et d'exploitation travaillent ensemble de manière agile dans le cadre d'une approche DevOps ou d'ingénierie de la fiabilité des sites.

Une approche agile du développement logiciel raccourcit les cycles de publication, réduit les temps d'arrêt et vous permet de résoudre les problèmes au fur et à mesure qu'ils surviennent sans attendre les nouvelles versions.

Si les équipes de développement et d'exploitation ne sont pas d'accord sur la façon dont l'application doit être déployée ou sur la façon dont l'environnement doit être configuré, le déploiement automatisé est impossible.

Pour automatiser votre environnement, vous devez être cohérent. En outre, le même processus de déploiement doit être appliqué à tous les environnements, y compris les environnements de production.



PARTIE 5

Azure Pipelines : Automate tests, builds, and delivery

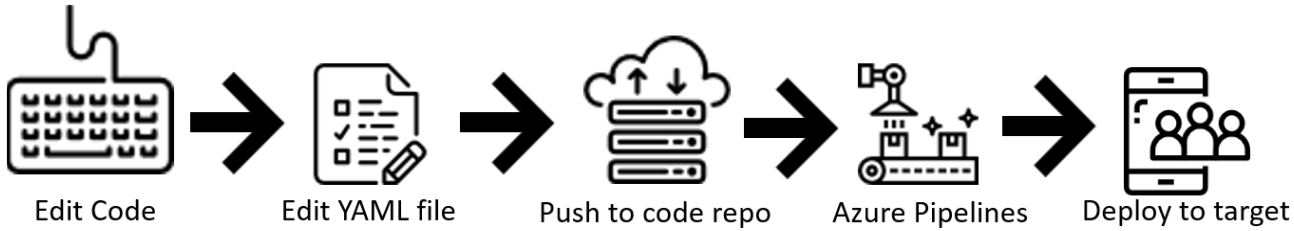
L'intégration continue (CI) automatise les tests et les builds pour votre projet. CI aide à détecter les bogues ou les problèmes au début du cycle de développement, lorsqu'ils sont plus faciles et plus rapides à corriger. Les éléments connus sous le nom d'artefacts sont produits à partir de systèmes CI. Ils sont utilisés par les pipelines de livraison continue pour piloter les déploiements automatiques.

La livraison continue déploie et teste automatiquement le code en plusieurs étapes pour favoriser la qualité. Les systèmes d'intégration continue produisent des artefacts déployables, qui incluent l'infrastructure et les applications. Les pipelines de publication automatisés utilisent ces artefacts pour publier de nouvelles versions et des correctifs sur la cible de votre choix.

Intégration Continue ((CI)	Livraison continue (CD)
- Augmentez la couverture du code - Construisez plus rapidement en divisant les tests et les builds - Assurez-vous automatiquement que vous n'envoyez pas de code cassé - Exécuter des tests en continu	- Déployer automatiquement le code en production - Assurez-vous que les cibles de déploiement disposent du dernier code - Utiliser le code testé du processus CI

Azure Pipelines : Define pipelines using YAML syntax

Vous définissez votre pipeline dans un fichier YAML appelé azure-pipelines.yml avec le reste de votre application.



Le pipeline est versionné avec votre code. Il suit la même structure de ramification. Vous obtenez la validation de vos modifications par le biais de revues de code dans les demandes d'extraction et les politiques de création de branche.

Chaque branche que vous utilisez peut modifier le pipeline en modifiant le fichier azure-pipelines.yml.

Une modification du processus de génération peut provoquer une interruption ou entraîner un résultat inattendu. Étant donné que le changement est dans le contrôle de version avec le reste de votre base de code, vous pouvez identifier plus facilement le problème.

Suivre ces étapes de base :

Configurer Azure Pipelines pour utiliser votre dépôt Git.

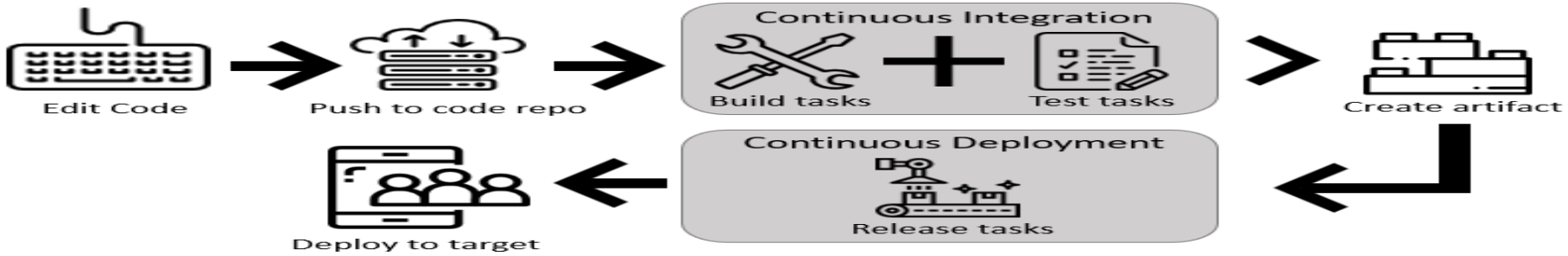
Modifier votre fichier azure-pipelines.yml pour définir votre build.

Pousser votre code vers votre référentiel de contrôle de version. Cette action lance le déclencheur par défaut pour créer et déployer, puis surveiller les résultats.

Votre code est maintenant mis à jour, construit, testé et empaqueté. Il peut être déployé sur n'importe quelle cible.

Azure Pipelines : Define pipelines using the Classic interface

Créer et configurez des pipelines dans le portail web Azure DevOps avec l'éditeur d'interface utilisateur classique. Vous définissez un pipeline de build pour générer et tester votre code, puis pour publier des artefacts. Vous définissez également un pipeline de publication pour consommer et déployer ces artefacts sur des cibles de déploiement.



Suiver ces étapes de base :

Configurer Azure Pipelines pour utiliser votre dépôt Git.

Utiliser l'éditeur classique d'Azure Pipelines pour créer et configurer vos pipelines de build et de publication.

Poussez votre code vers votre référentiel de contrôle de version. Cette action déclenche votre pipeline et exécute des tâches telles que la création ou le test de code.

Le build crée un artefact qui est utilisé par le reste de votre pipeline pour exécuter des tâches telles que le déploiement en préproduction ou en production.

- Votre code est maintenant mis à jour, construit, testé et empaqueté. Il peut être déployé sur n'importe quelle cible

Azure Pipelines : Create your first pipeline

Pour commencer, bifurquer le référentiel suivant dans votre compte GitHub.

- Obtenez l'exemple de code Java

https://github.com/MicrosoftDocs/pipelines-java

- Créer votre premier pipeline Java
- Connectez-vous à votre organisation Azure DevOps et accédez à votre projet.
- Accéder à Pipelines, puis sélectionnez Nouveau pipeline.
- Suiver les étapes de l'assistant en sélectionnant d'abord GitHub comme emplacement de votre code source.
- Vous serez peut-être redirigé vers GitHub pour vous connecter. Si tel est le cas, saisissez vos informations d'identification GitHub.
- Lorsque vous voyez la liste des référentiels, sélectionnez votre référentiel.
- Vous pouvez être redirigé vers GitHub pour installer l'application Azure Pipelines. Si tel est le cas, sélectionnez Approuver et installer.
- Azure Pipelines analysera votre référentiel et recommandera le modèle de pipeline Maven.
- Lorsque votre nouveau pipeline apparaît, jetez un œil au YAML pour voir ce qu'il fait. Lorsque vous êtes prêt, sélectionnez Enregistrer et exécuter.

Azure Pipelines : Create your first pipeline

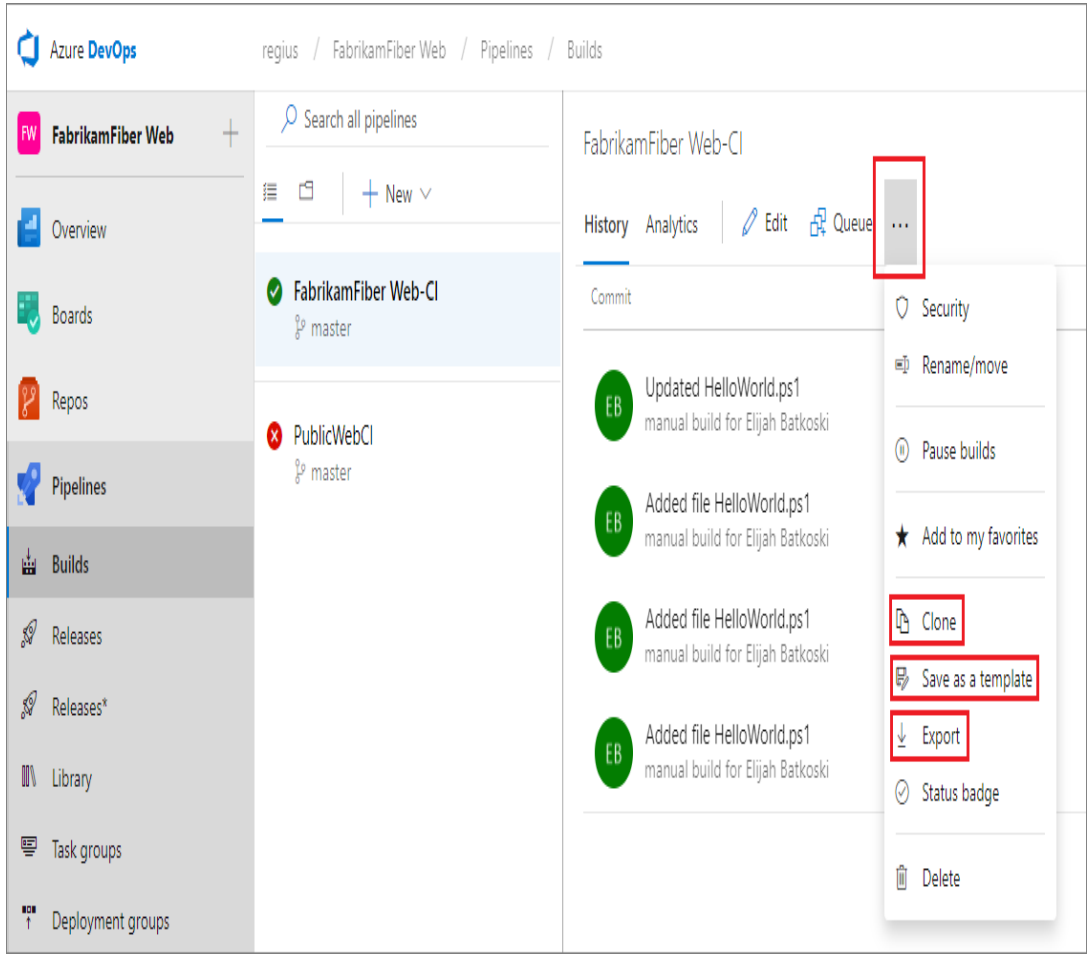
Vous êtes invité à valider un nouveau fichier azure-pipelines.yml dans votre référentiel. Une fois que vous êtes satisfait du message, sélectionnez Enregistrer et exécuter à nouveau.

Si vous souhaitez observer votre pipeline en action, sélectionnez la tâche de build.

Vous venez de créer et d'exécuter un pipeline que nous avons créé automatiquement pour vous, car votre code semblait correspondre au modèle Maven.

Vous avez maintenant un pipeline YAML fonctionnel (azure-pipelines.yml) dans votre référentiel que vous pouvez personnaliser !

Lorsque vous êtes prêt à apporter des modifications à votre pipeline, sélectionnez-le dans la page Pipelines, puis modifiez le fichier azure-pipelines.yml.



PARTIE 5

CHAPITRE 3

Déployer des conteneurs

Ce que vous allez apprendre dans ce chapitre :

- Créer une instance de conteneur
- Déployer des instances de conteneur dans un réseau virtuel Azure
- Activer ou désactiver le stockage persistant intégré

2 heures

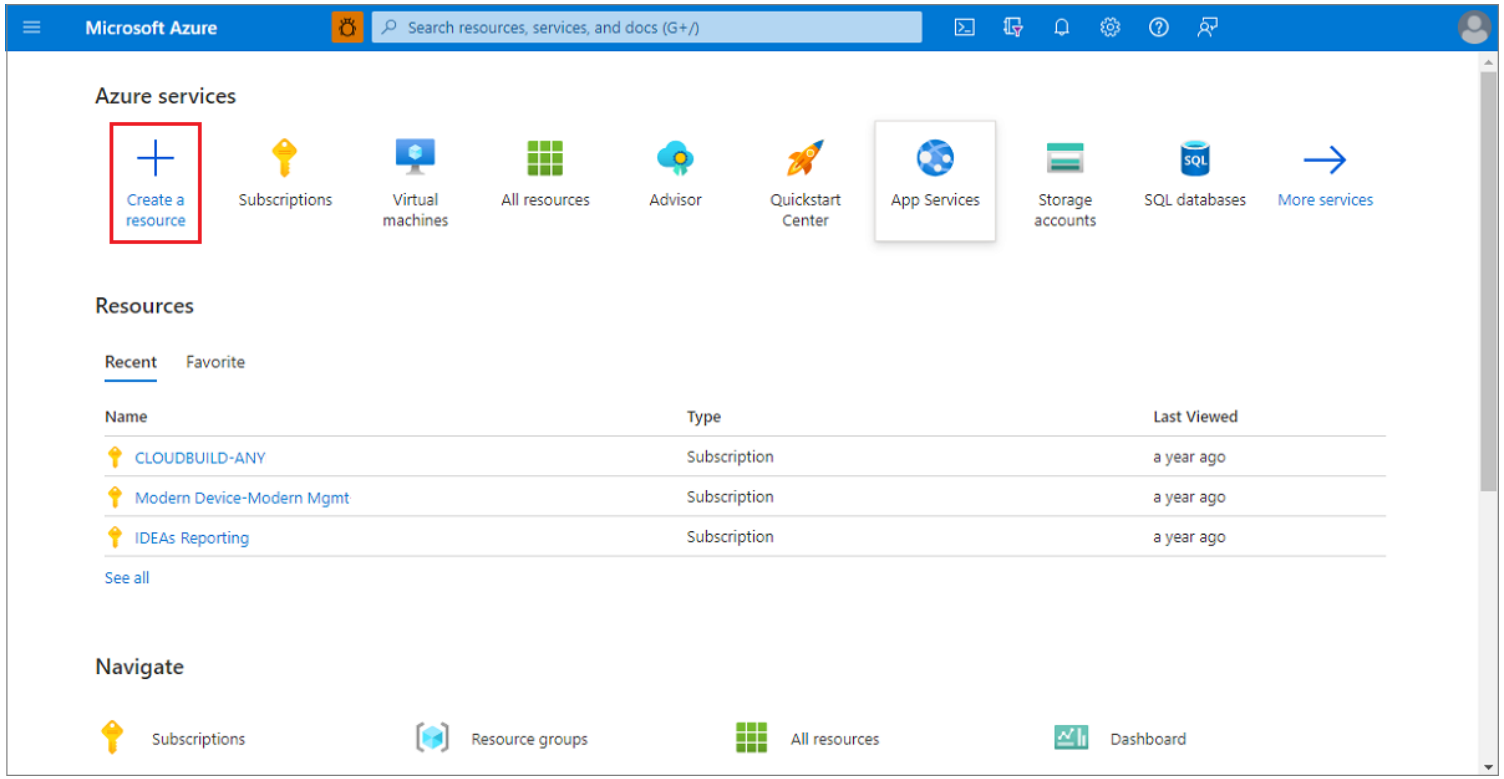
CHAPITRE 3

Déployer des conteneurs

1. **Allocation des ressources**
2. Mise en réseau
3. Stockage persistant des données

Allocation des ressources : Créer une instance de conteneur

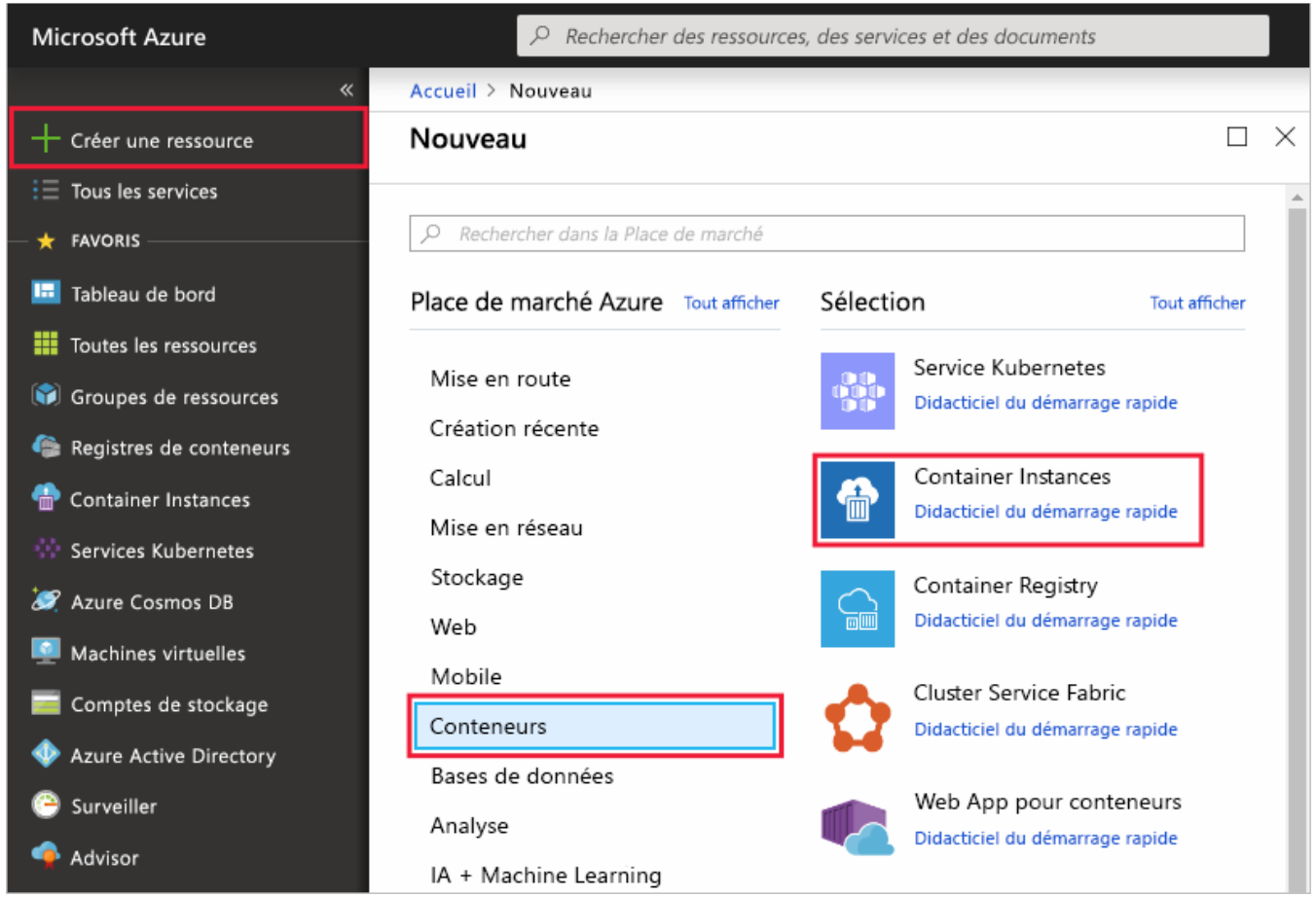
Dans la page d'accueil du portail Azure, sélectionner **Créer une ressource**.



PARTIE 5

Allocation des ressources : Créer une instance de conteneur

Sélectionner **Conteneurs**>**Container Instances**.



PARTIE 5

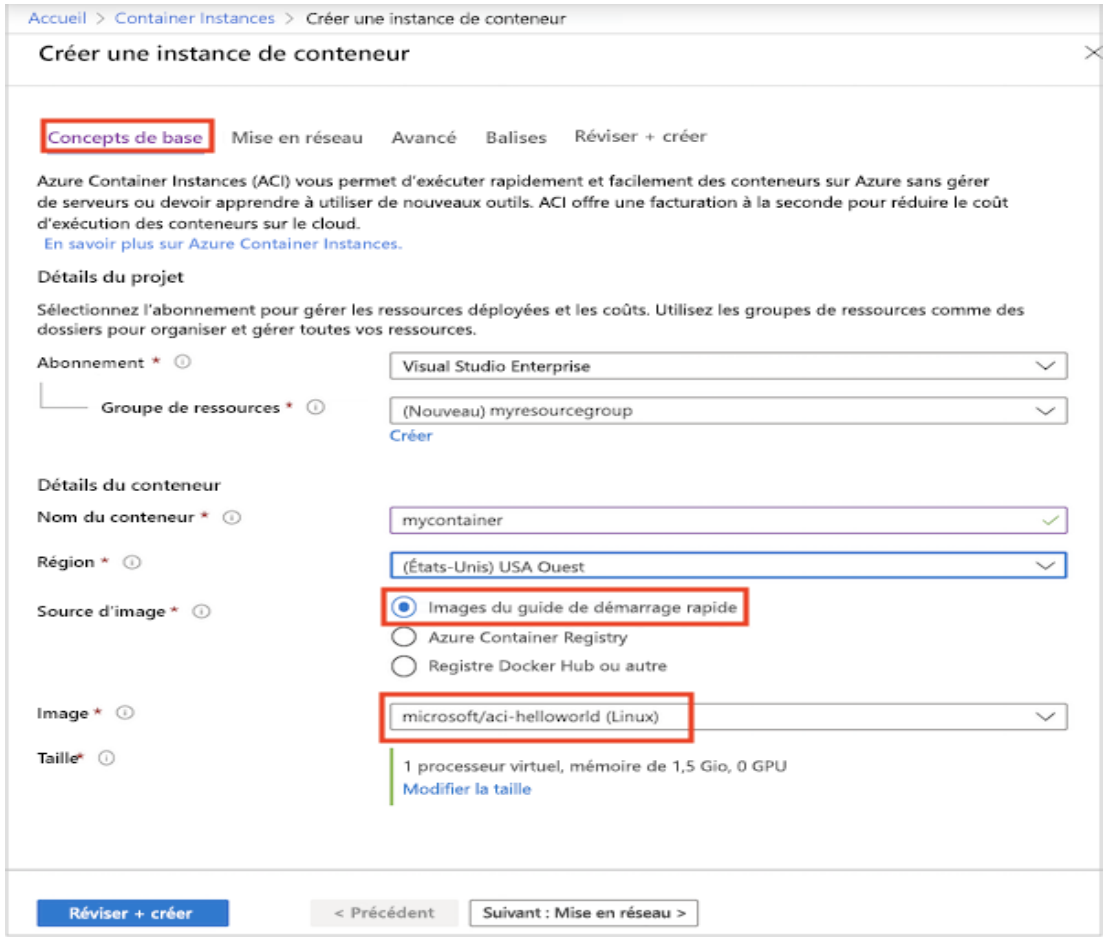
Allocation des ressources : Créer une instance de conteneur

Dans la page **De base**, choisissez un abonnement et entrez les valeurs suivantes pour le **Groupe de ressources**, le **Nom de conteneur**, la **Source d'image** et l'**Image conteneur**.

- Groupe de ressources : **Créer**>myresourcegroup
- Nom du conteneur : mycontainer
- Source d'image : **Images du guide de démarrage rapide**
- Image conteneur : mcr.microsoft.com/azuredocs/aci-helloworld:latest (Linux)

Conserver les autres valeurs par défaut, puis sélectionner **Suivant : Mise en réseau**.

Dans la page **Mise en réseau**, spécifier une **Étiquette du nom DNS** pour votre conteneur. Le nom doit être unique au sein de la région Azure dans laquelle vous créez l'instance de conteneur. Votre conteneur sera publiquement accessible avec <dns-name-label>.<region>.azurecontainer.io. Si vous recevez un message d'erreur « Étiquette de nom DNS indisponible », essayer d'utiliser une autre étiquette de nom DNS.



PARTIE 5

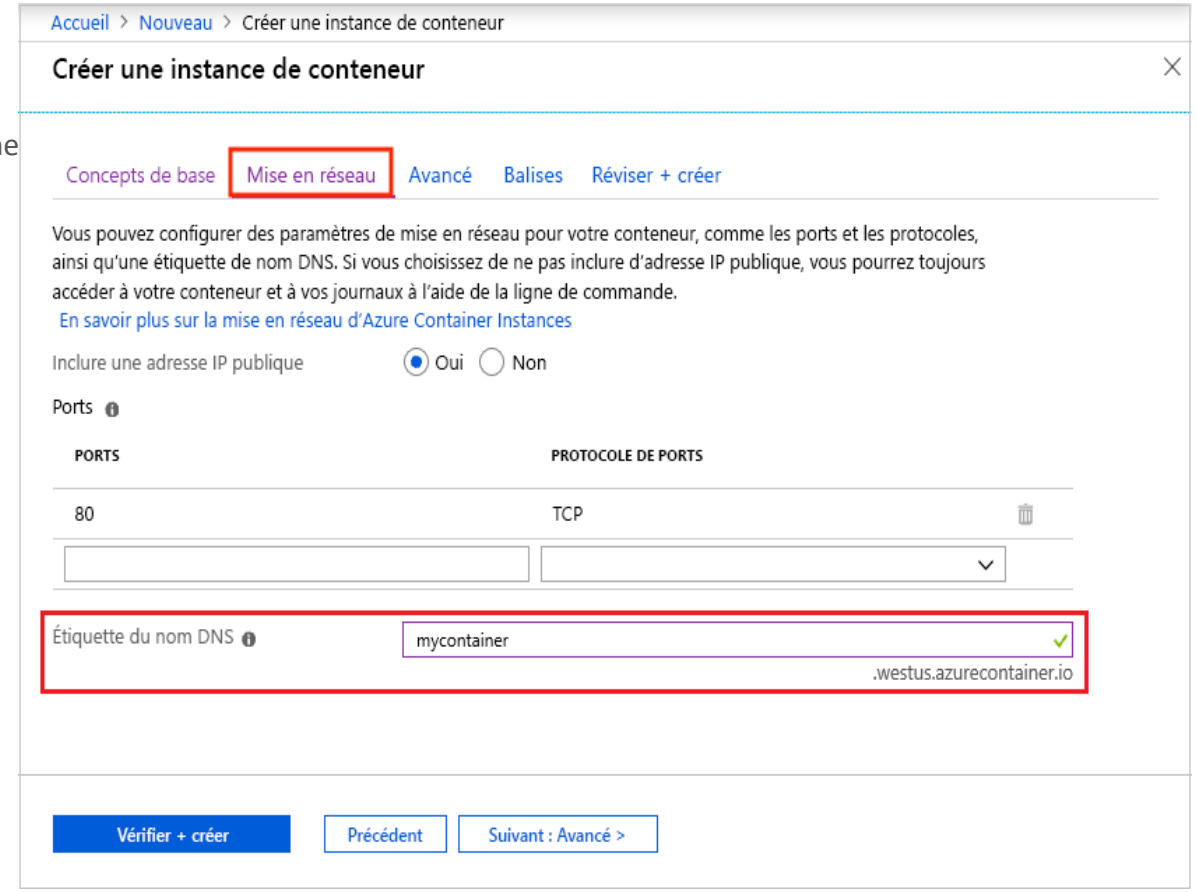
Allocation des ressources : Créer une instance de conteneur

Un hachage généré automatiquement est ajouté en tant qu'étiquette de nom DNS au nom de domaine complet (FQDN) de votre instance de conteneur, empêchant toute prise de contrôle malveillante du sous-domaine. Spécifiez la **réutilisation de l'étendue d'étiquette de nom DNS** pour le nom de domaine complet (FQDN). Vous pouvez choisir une de ces options :

- Locataire
- Abonnement
- Groupe de ressources
- Aucune réutilisation
- Toute réutilisation (cette option est la moins sécurisée.)

Dans cet exemple, sélectionnez **Locataire**.

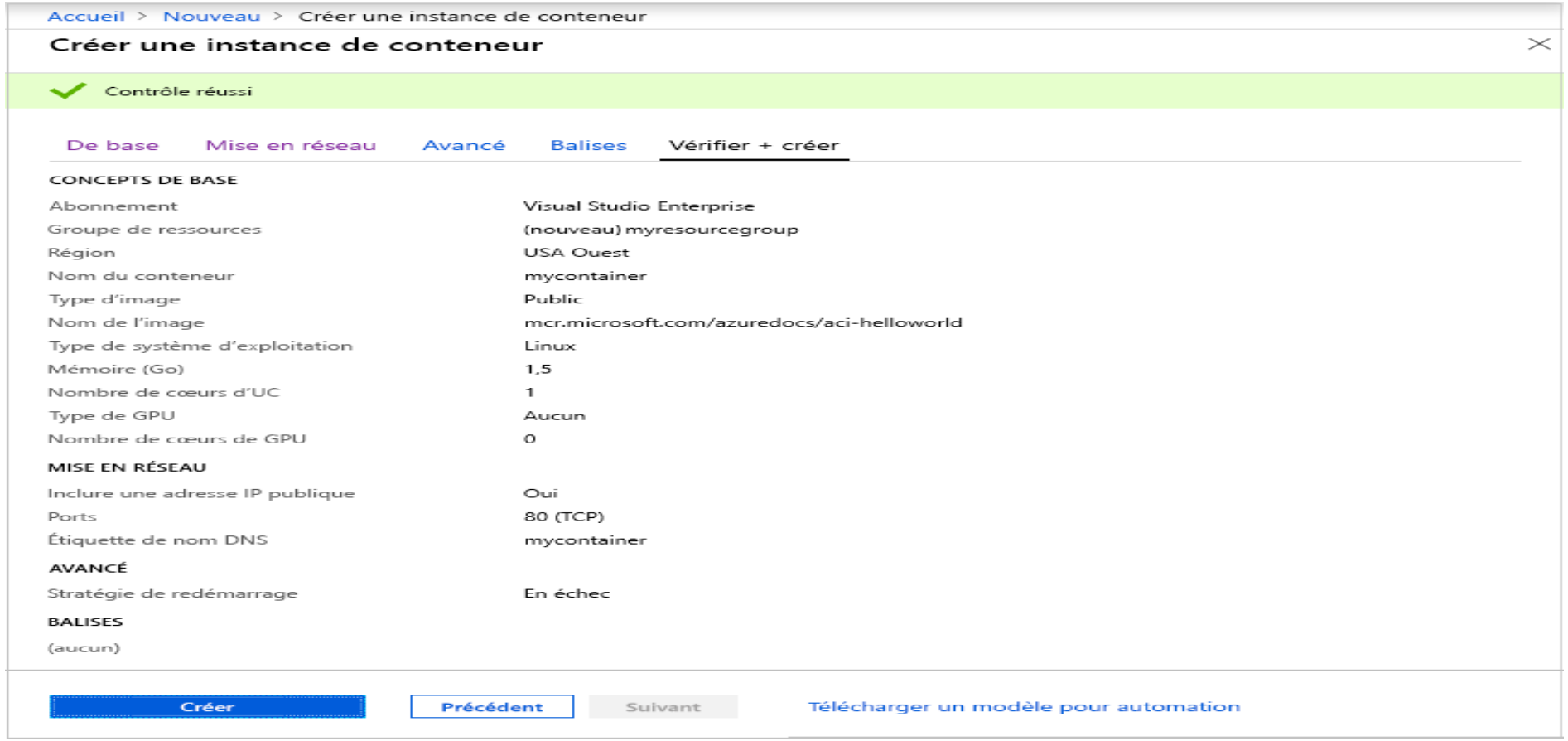
Conserver les autres paramètres par défaut, puis sélectionnez **Vérifier + créer**.



PARTIE 5

Allocation des ressources : Créer une instance de conteneur

Une fois la validation terminée, un résumé des paramètres de votre conteneur s'affiche. Sélectionnez **Créer** pour envoyer votre demande de déploiement de conteneur.

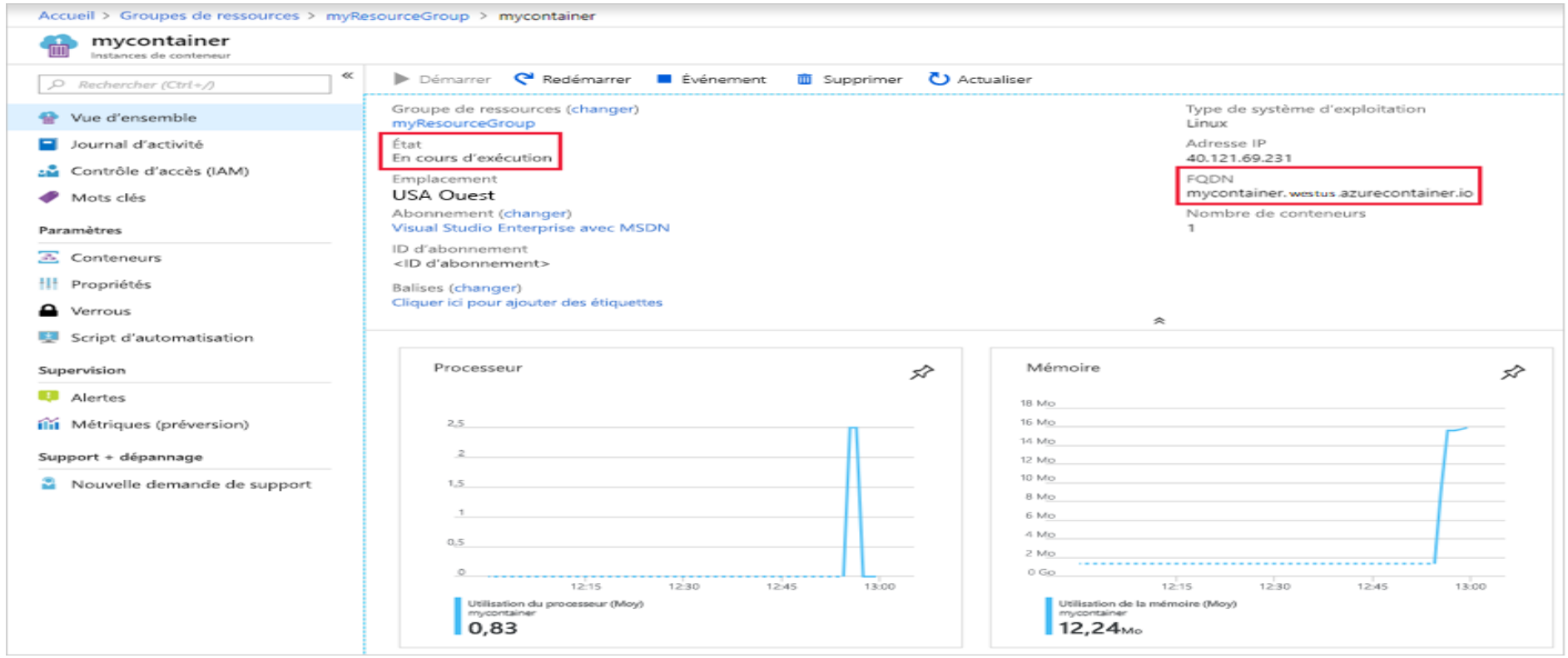


PARTIE 5

Allocation des ressources : Créer une instance de conteneur

Quand le déploiement commence, une notification s'affiche, indiquant que le déploiement est en cours. Une autre notification s'affiche lorsque le groupe de conteneurs a été déployé.

Ouvrez la vue d'ensemble du groupe de conteneurs en accédant à **Groupes de ressources**>**myresourcegroup**>**mycontainer**. Notez le **FQDN** de l'instance de conteneur et son **État**.



PARTIE 5

Allocation des ressources : Créer une instance de conteneur

Une fois que son **État** est *En cours d'exécution*, accédez au nom de domaine complet du conteneur dans votre navigateur.

OFPPT
La Voie de l'Avenir

WEBFORCE
BE THE CHANGE

CHAPITRE 3

Déployer des conteneurs

1. Allocation des ressources
2. **Mise en réseau**
3. Stockage persistant des données

Déployer des instances de conteneur dans un réseau virtuel Azure

Pour déployer dans un nouveau réseau virtuel et laisser Azure créer automatiquement les ressources réseau, spécifiez les éléments suivants lorsque vous exécutez as container create :

- Nom du réseau virtuel
- Préfixe d'adresse de réseau virtuel au format CIDR
- Nom du sous-réseau
- Préfixe d'adresse de sous-réseau au format CIDR

Le réseau virtuel et les préfixes d'adresse de sous-réseau spécifient les espaces d'adressage du réseau virtuel et du sous-réseau, respectivement. Ces valeurs sont représentées en notation CIDR (Classless Inter-domain Routing), par exemple 10.0.0.0/16.

Une fois que vous avez déployé votre premier groupe de conteneurs avec cette méthode, vous pouvez déployer dans le même sous-réseau en spécifiant les noms du réseau virtuel et du sous-réseau, ou le profil réseau créé automatiquement par Azure pour vous. Comme Azure délègue le sous-réseau à Azure Container Instances, vous ne pouvez déployer *que* des groupes de conteneurs dans le sous-réseau.

Déployer des instance de conteneur dans un réseau virtuel Azure

Exemple

La commande az container create suivante spécifie les paramètres pour un nouveau réseau virtuel et un nouveau sous-réseau. Fournissez le nom d'un groupe de ressources créé dans une région où des déploiements de groupe de conteneurs dans un réseau virtuel sont disponible . Cette commande déploie le conteneur Microsoft aci-helloworld public qui exécute un petit serveur web Node.js qui gère une page web statique. Dans la section suivante, vous allez déployer un deuxième groupe de conteneurs dans le même sous-réseau et tester la communication entre les deux instances de conteneur.

```
az container create \
 --name appcontainer \
 --resource-group myResourceGroup \
 --image mcr.microsoft.com/azuredocs/aci-helloworld \
 --vnet aci-vnet \
 --vnet-address-prefix 10.0.0.0/16 \
 --subnet aci-subnet \
 --subnet-address-prefix 10.0.0.0/24
```

Lorsque vous déployez dans un nouveau réseau virtuel avec cette méthode, l'opération peut prendre quelques minutes, le temps de créer les ressources réseau. Après le déploiement initial, les déploiements de groupe de conteneurs sur le même sous-réseau sont accomplis plus rapidement.

CHAPITRE 3

Déployer des conteneurs

1. Allocation des ressources
2. Mise en réseau
3. **Stockage persistant des données**

Stockage persistant des données

Les conteneurs Windows utilisent par défaut un stockage éphémère. Toutes les E/S de conteneur se produisent dans un « espace de travail » et chaque conteneur reçoit son propre travail. La création de fichier et les écritures de fichier sont capturées dans l'espace de travail et n'échappent pas à l'hôte. Lors de l'arrêt d'une instance de conteneur, toutes les modifications apportées à l'espace de travail sont écartées. Lors du démarrage d'une nouvelle instance de conteneur, un nouvel espace de travail est fourni pour l'instance.

Stockage par niveaux

Comme décrit dans la Vue d'ensemble des conteneurs , les images de conteneur sont un ensemble de fichiers qui se présente sous la forme d'une série de couches. Le stockage en couches englobe tous les fichiers intégrés dans le conteneur. Chaque fois que vous effectuez un docker pull, puis un docker run de ce conteneur, vous obtenez un résultat identique.

Où sont stockées les niveaux et comment modifier cette configuration

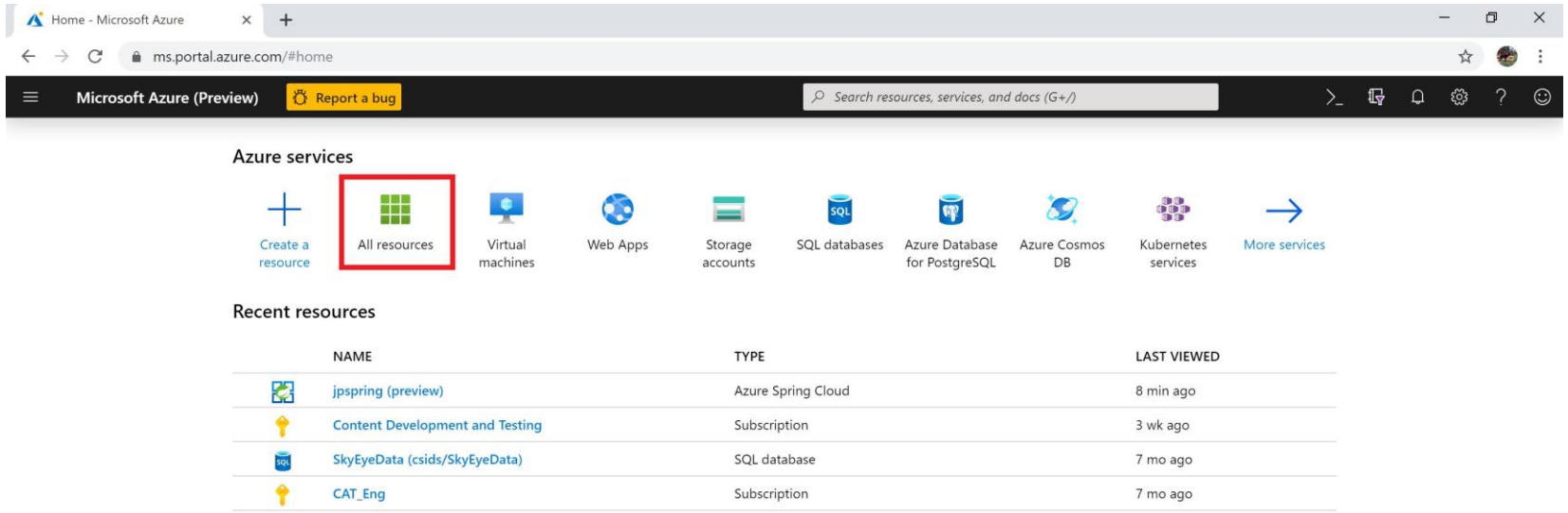
Dans une installation par défaut, les niveaux sont stockés dans C:\ProgramData\docker et répartis dans les répertoires « image » et « windowsfilter ».

Vous ne devez pas modifier les fichiers contenus dans les répertoires des niveaux : ils sont gérés avec soin à l'aide de commandes telles que :

- docker images
- docker rmi
- docker pull
- docker load
- docker save

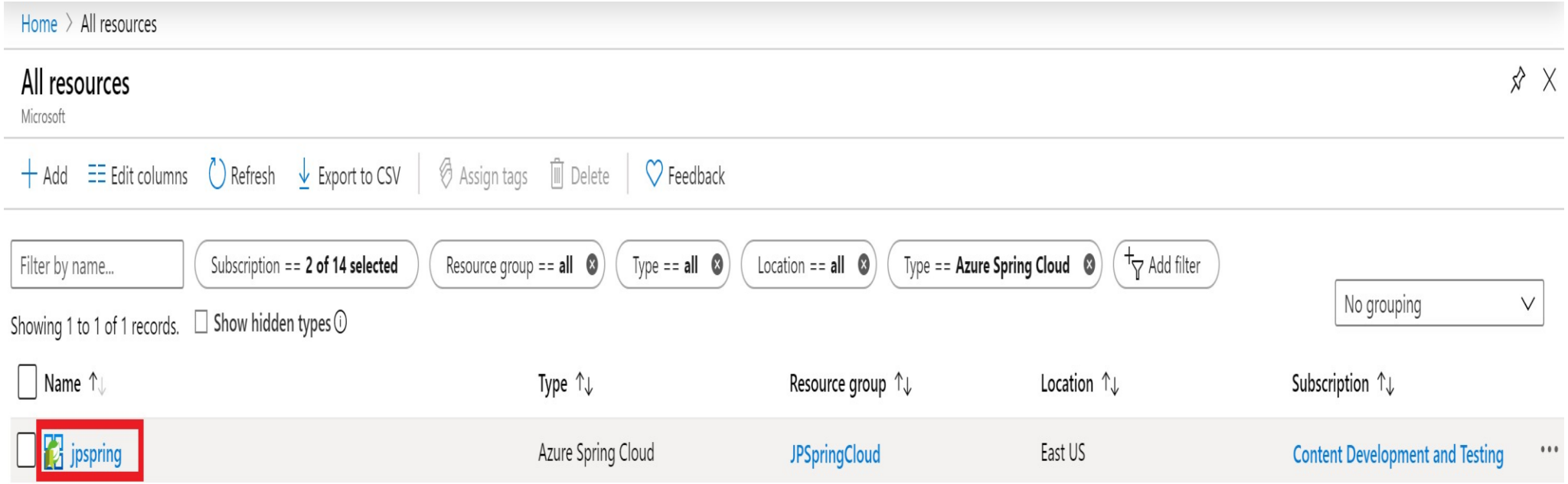
Activer ou désactiver le stockage persistant intégré

Vous pouvez modifier l'état du stockage persistant intégré à l'aide du Portail Azure ou à l'aide d'Azure CLI.



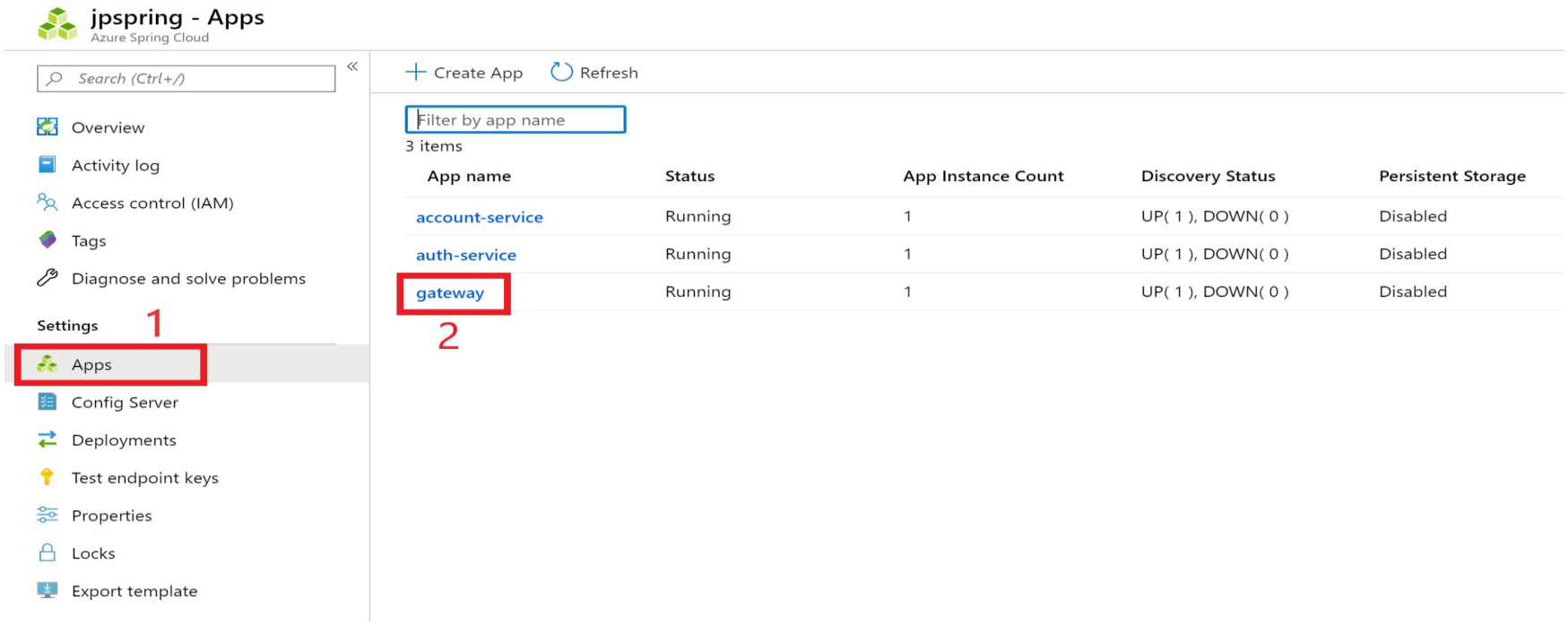
Activer ou désactiver le stockage persistant intégré

Sélectionner la ressource Azure Spring Apps qui nécessite un stockage persistant. Dans notre exemple, l'application sélectionnée est appelée **upspring**.



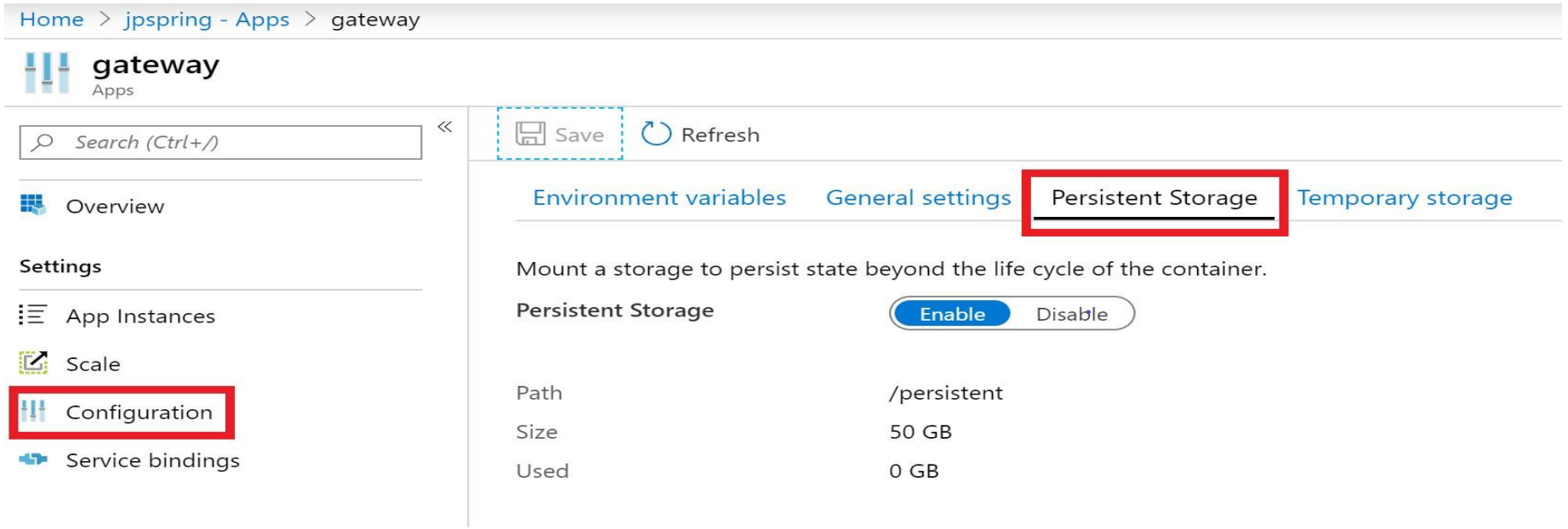
Activer ou désactiver le stockage persistant intégré

- Sous l'en-tête **Paramètres**, sélectionnez **Applications**.
- Vos services Azure Spring Apps apparaissent dans un tableau. Sélectionnez le service auquel vous souhaitez ajouter un stockage persistant. Dans cet exemple, le service **passerelle** est sélectionné.



Activer ou désactiver le stockage persistant intégré

- Dans la page de configuration du service, sélectionnez **Configuration**
- Sélectionner l'onglet **Stockage persistant** et sélectionnez **Activer** pour activer le stockage persistant, ou sélectionnez **Désactiver** pour désactiver le stockage persistant.



- Une fois le stockage persistant activé, sa taille et son chemin d'accès sont affichés dans l'onglet **Stockage persistant**.

PARTIE 5

PARTIE 6

Maintenir un environnement de production

Dans ce module, vous allez :

- Gouverner les ressources Cloud
- Assurer le bon fonctionnement des ressources

5 heures

CHAPITRE 1

Gouverner les ressources Cloud

Ce que vous allez apprendre dans ce chapitre :

- Contrôler avec vigilance des déploiements des ressources
- Assurer la maintenance productive des ressources déployées

3 heures

CHAPITRE 1

Gouverner les ressources Cloud

1. **Stratégie de déploiement**
2. Blueprints
3. Étiquetage des ressources

Stratégies de déploiement bleu-vert dans Azure Spring Apps

Azure Spring Apps est le nouveau nom du service Azure Spring Cloud. Bien que le service ait un nouveau nom, vous verrez l'ancien nom à divers endroits pendant un certain temps, car nous travaillons à mettre à jour les ressources telles que les captures d'écran, les vidéos et les diagrammes.

Azure Spring Apps (niveau Standard et supérieur) autorise deux déploiements pour chaque application, un seul reçoit le trafic de production. Ce modèle est connu sous le nom de déploiement bleu-vert. La prise en charge par Azure Spring Apps du déploiement bleu-vert, avec un pipeline de livraison continue (CD) et des tests automatisés rigoureux, permet des déploiements d'applications agiles avec un niveau de confiance élevé.

Déploiements alternés

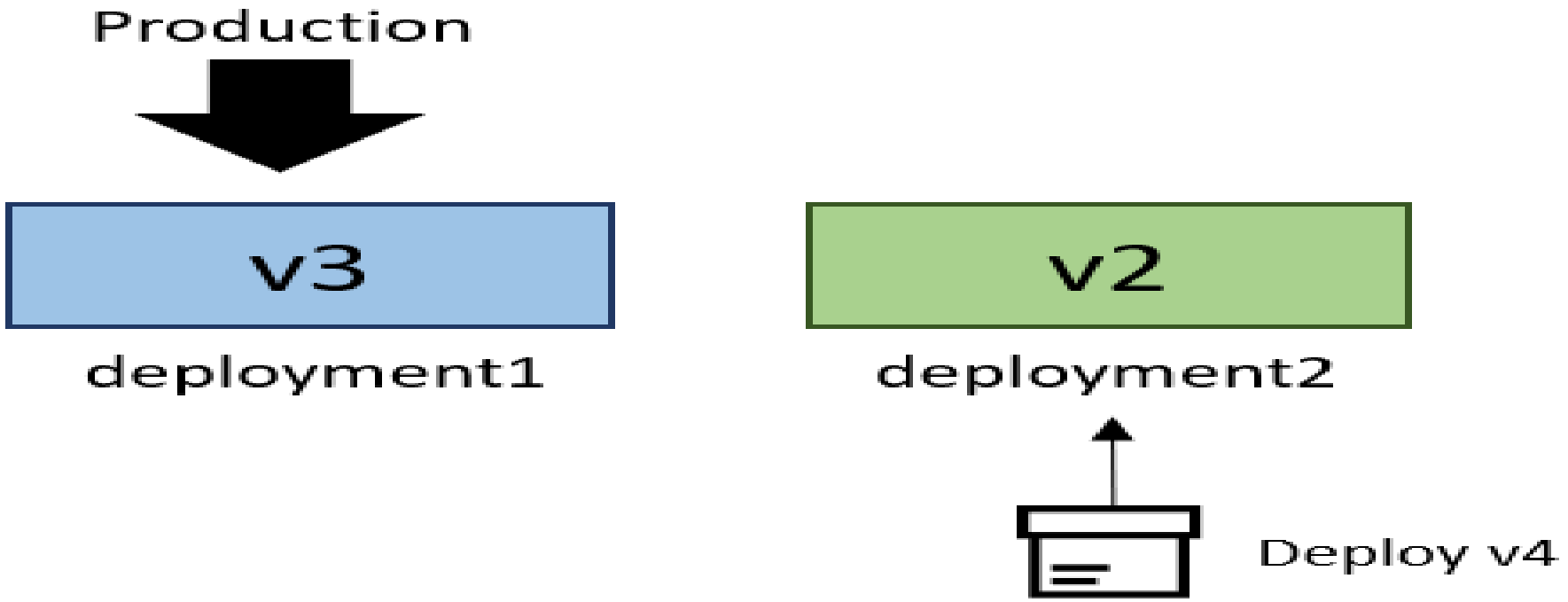
Le moyen le plus simple d'implémenter un déploiement bleu-vert avec Azure Spring Apps consiste à créer deux déploiements fixes et à toujours déployer sur le déploiement qui ne reçoit pas de trafic de production. Avec la tâche , vous pouvez déployer de cette façon, juste en affectant à l'indicateur UseStagingDeployment la valeur true.

Voici comment fonctionne l'approche des déploiements alternés dans la pratique :

Supposons que votre application a deux déploiements : deployment1 et deployment2. Actuellement, deployment1 est défini en tant que déploiement de production et exécute la version v3 de l'application.

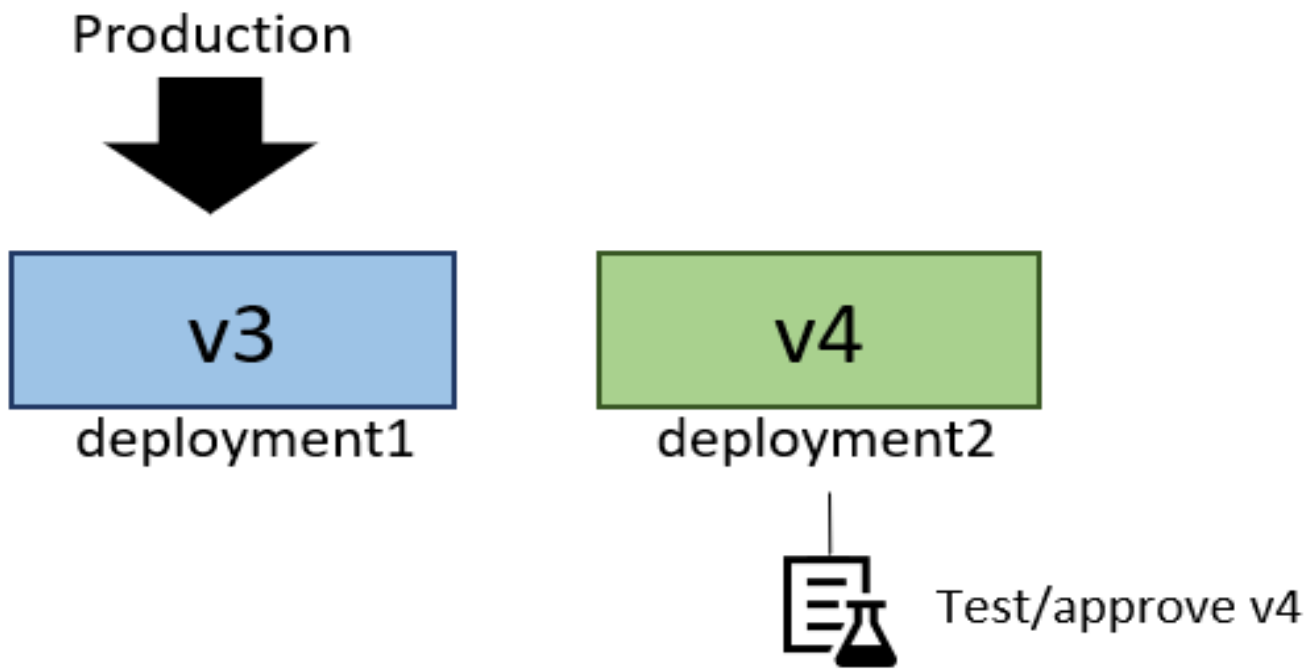
Ce qui fait de deployment2 le déploiement de préproduction. Ainsi, lorsque le pipeline de livraison continue (CD) est prêt à être exécuté, il déploie la version suivante de l'application, la version v4, sur le déploiement de préproduction deployment2.

Stratégies de déploiement bleu-vert dans Azure Spring Apps



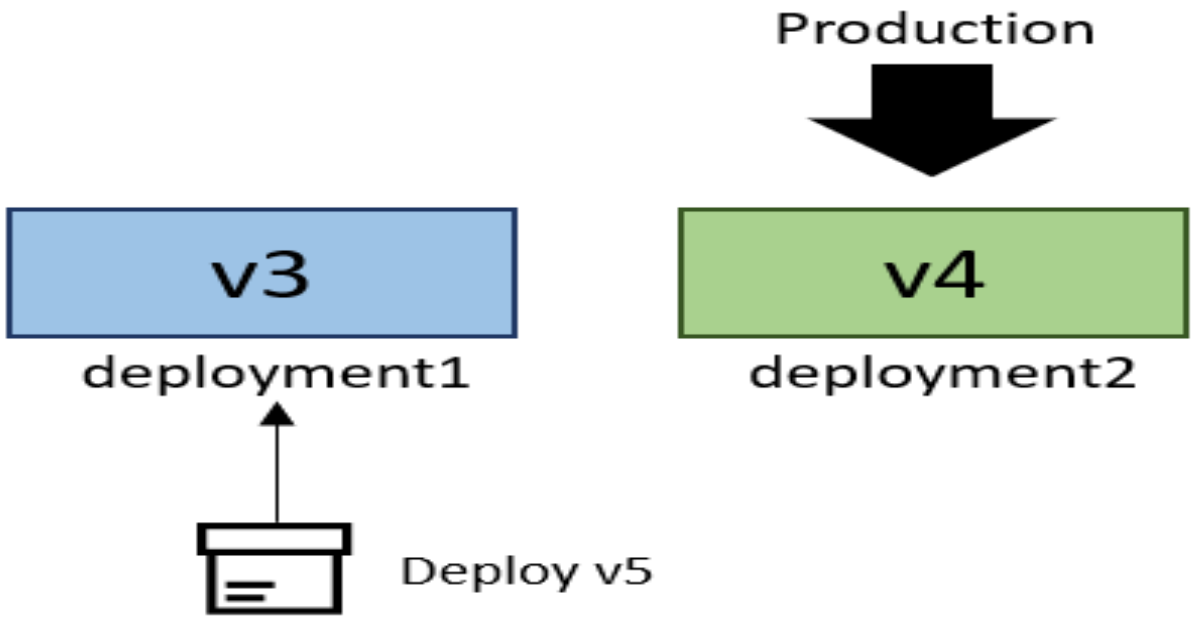
Stratégies de déploiement bleu-vert dans Azure Spring Apps

Une fois que v4 a démarré sur deployment2, vous pouvez exécuter des tests automatisés et manuels sur ce dernier via un point de terminaison de test privé pour garantir que v4 répond à toutes les attentes.



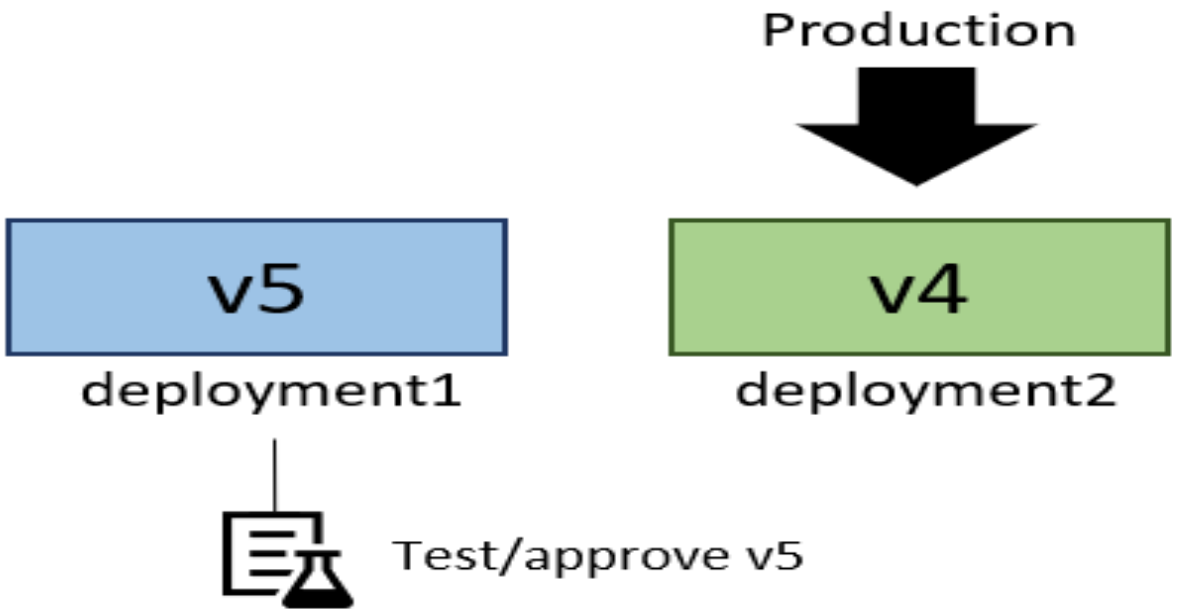
Stratégies de déploiement bleu-vert dans Azure Spring Apps

Maintenant, deployment1 est le déploiement de préproduction. Par conséquent, la prochaine exécution du pipeline de déploiement se déploie sur deployment1.



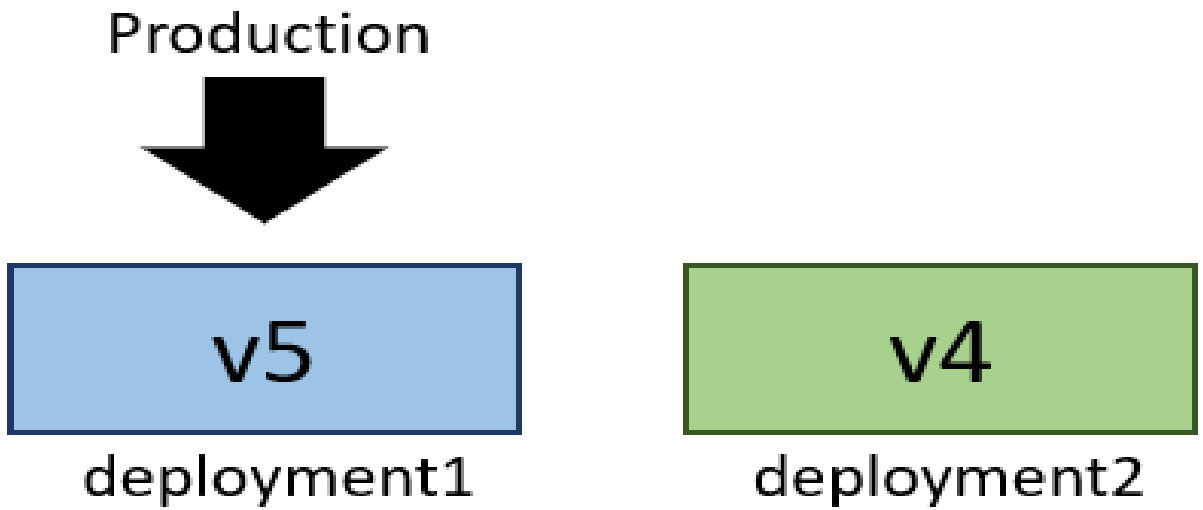
Stratégies de déploiement bleu-vert dans Azure Spring Apps

Vous pouvez maintenant tester V5 sur le point de terminaison de test privé de `deployment1`.



Stratégies de déploiement bleu-vert dans Azure Spring Apps

Enfin, une fois que v5 répond à toutes vos attentes, vous définissez deployment1 à nouveau comme déploiement de production afin que v5 reçoive tout le trafic de production.



CHAPITRE 1

Gouverner les ressources Cloud

1. Stratégie de déploiement
2. **Blueprints**
3. Éiquetage des ressources

Qu'est-ce qu'Azure Blueprint ?

Les **blueprints** permettent aux ingénieurs et aux architectes de définir les paramètres de conception d'un projet, les blueprints Azure permettent aux architectes Cloud et aux principaux groupes informatiques d'implémenter des normes, des modèles et des exigences organisationnels. Vous pouvez définir un ensemble de ressources Azure reproductibles conformes à Azure Blueprints, les équipes de développement peuvent rapidement créer et mettre en place de nouveaux environnements avec la confiance nécessaire pour renforcer la conformité organisationnelle avec un ensemble de composants intégrés tels que la mise en réseau pour accélérer le développement et le déploiement.

Les Blueprints sont un moyen déclaratif d'orchestrer le déploiement de divers modèles de ressources et d'autres artefacts tels que :

- Attributions de rôles
- Affectations de stratégie
- Modèles Azure Resource Manager (modèles ARM)
- Groupes de ressources

Le service **Azure Blueprints** s'appuie sur la base de données **Azure Cosmos DB** distribuée dans le monde entier . Les objets Blueprint sont répliqués dans plusieurs régions Azure. Cette réplication offre une faible latence, une haute disponibilité et un accès cohérent à vos objets Blueprint, quelle que soit la région dans laquelle Azure Blueprints déploie vos ressources.

Définition de blueprint

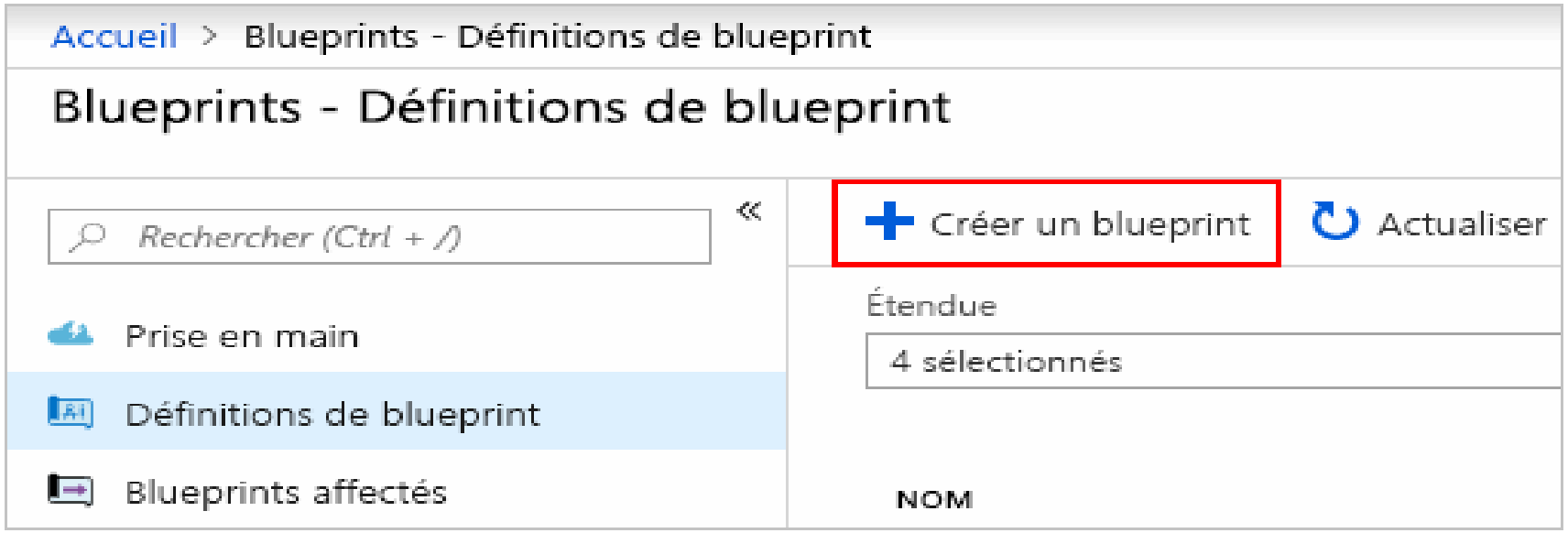
Un blueprint est composé d'*artefacts*. Azure Blueprints prend actuellement en charge les ressources suivantes comme artefacts :

Ressource	Options de hiérarchie	Description
Groupes de ressources	Abonnement	Crée un groupe de ressources pour une utilisation par d'autres artefacts dans le blueprint. Ces groupes de ressources réservés vous permettent d'organiser les ressources en totale conformité avec la structure souhaitée. Ils fournissent aussi un limiteur d'étendue pour les artefacts de stratégie et d'attribution de rôle inclus, et des modèles Resource Manager.
Modèle ARM	Abonnement, groupe de ressources	Des modèles, tels que les modèles imbriqués et liés, sont utilisés pour composer des environnements complexes. Exemples d'environnements : une batterie de serveurs SharePoint, une configuration de l'état Azure Automation ou un espace de travail Log Analytics.
Affectation de rôle	Abonnement, groupe de ressources	Permet l'affectation d'une stratégie ou d'une initiative à l'abonnement auquel le blueprint est affecté. La stratégie ou l'initiative doit se trouver à l'intérieur de l'étendue de l'emplacement de définition du blueprint. Si la stratégie ou l'initiative comporte des paramètres, ceux-ci sont affectés au moment de la création du blueprint ou durant son affectation.
Attribution de rôle	Abonnement, groupe de ressources	Ajoutez un utilisateur ou un groupe existant à un rôle intégré pour vous assurer que les personnes adéquates disposent d'un accès approprié à vos ressources. Vous pouvez définir des attributions de rôle pour l'ensemble de l'abonnement ou les imbriquer dans un groupe de ressources spécifique inclus dans le blueprint.

Créer un blueprint

La première étape de la définition d'un modèle standard à des fins de conformité est de composer un blueprint à partir des ressources disponibles. Vous allez créer un blueprint nommé *MyBlueprint* pour configurer les attributions de rôles et de stratégies de l'abonnement. Ensuite, vous ajouterez un groupe de ressources, un modèle ARM et une attribution de rôle sur le groupe de ressources.

- Sélectionnez **Tous les services** dans le volet gauche. Recherchez et sélectionnez **Blueprints**.
- Sélectionnez **Définitions de blueprint**, puis **+ Créer un blueprint**.



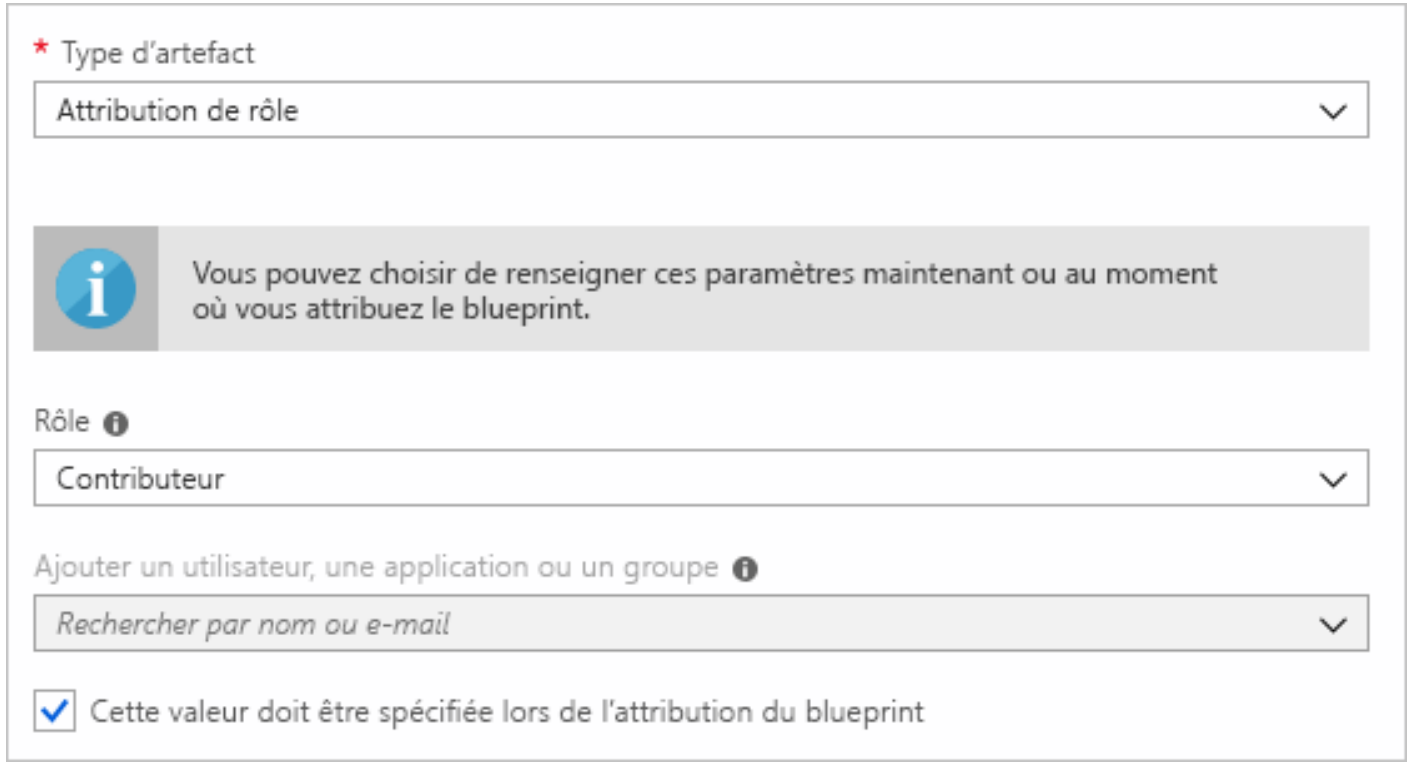
PARTIE 6

Créer un blueprint

- Vous pouvez également sélectionner **Prise en main**>**Créer** pour accéder directement à la création d'un blueprint.
- Sélectionnez **Commencer par un blueprint vide** à partir de la carte dans la partie supérieure de la liste des blueprints intégrés.
- Donnez un nom au blueprint, par exemple *MyBlueprint*. (Vous pouvez utiliser 48 lettres et chiffres maximum, sans espaces ni caractères spéciaux.) Laissez le champ **Description du blueprint** vide pour le moment.
- Dans la zone **Emplacement de la définition**, sélectionnez les points de suspension à droite. Sélectionnez ensuite le groupe d'administration ou l'abonnement dans lequel vous souhaitez enregistrer le blueprint, puis choisissez **Sélectionner**.
- Vérifiez que les informations sont correctes. Une fois définis, les champs **Nom du blueprint** et **Emplacement de définition** ne peuvent plus être modifiés. Sélectionnez ensuite **Suivant : Artefacts** en bas de la page ou l'onglet **Artefacts** en haut de la page.
- Ajoutez une attribution de rôle au niveau de l'abonnement :
  - Sous **Abonnement**, sélectionnez **+ Ajouter un artefact**. La fenêtre **Ajouter un artefact** s'ouvre sur la droite.
  - Dans le champ **Type d'artefact**, sélectionnez **Attribution de rôle**.
  - Pour **Rôle**, sélectionnez **Contributeur**. N'entrez rien dans le champ **Ajouter un utilisateur, une application ou un groupe** sous lequel la case cochée indique qu'il s'agit d'un paramètre dynamique.
  - Sélectionnez **Ajouter** pour ajouter cet artefact au blueprint.

Créer un blueprint

- Sélectionnez **Ajouter** pour ajouter cet artefact au blueprint.



Créer un blueprint

- Ajoutez une attribution de stratégie au niveau de l'abonnement :
  - Sous l'artefact d'attribution de rôle, sélectionnez **+ Ajouter un artefact**.
  - Dans le champ **Type d'artefact**, sélectionnez **Attribution de stratégie**.
  - Définissez le **Type** sur **Intégré**. Dans la zone **Recherche**, entrez **étiquette**.
  - Enlevez le focus de la fonction **Rechercher** pour appliquer le filtre. Sélectionnez **Ajouter l'étiquette et sa valeur aux groupes de ressources**.
  - Sélectionnez **Ajouter** pour ajouter cet artefact au blueprint.
- Sélectionnez la ligne d'attribution de stratégie **Ajouter l'étiquette et sa valeur aux groupes de ressources**.
- La fenêtre qui s'ouvre vous permet de fournir des paramètres à l'artefact dans le cadre de la définition de blueprint. Vous pouvez définir les paramètres de toutes les attributions (paramètres statiques) en fonction de ce blueprint, plutôt que pendant l'attribution (paramètres dynamiques). Cet exemple utilise des paramètres dynamiques durant l'affectation du blueprint. Veillez donc à conserver les valeurs par défaut et à sélectionner **Annuler**.
- Ajoutez un groupe de ressources au niveau de l'abonnement :
  - Sous **Abonnement**, sélectionnez **+ Ajouter un artefact**.
  - Dans le champ **Type d'artefact**, sélectionnez **Groupe de ressources**.
  - Laissez les zones **Nom complet de l'artefact**, **Nom du groupe de ressources** et **Emplacement** vides. Vérifiez que la case est cochée pour chacune des propriétés de paramètre afin de les transformer en paramètres dynamiques.
  - Sélectionnez **Ajouter** pour ajouter cet artefact au blueprint.

Créer un blueprint

- Ajoutez un modèle sous le groupe de ressources :
  - Sous **ResourceGroup**, sélectionnez **+ Ajouter un artefact**.
  - Dans le champ **Type d'artefact**, sélectionnez **Modèle Azure Resource Manager**. Définissez **Nom complet de l'artefact** sur **StorageAccount** et laissez la zone **Description** vide.
  - Sous l'onglet **Modèle** dans la zone de l'éditeur, collez le modèle Resource Manager suivant. Après avoir collé le modèle, sélectionnez l'onglet **Paramètres** et notez que les paramètres du modèle storageAccountType et location ont été détectés. Chaque paramètre est automatiquement détecté et renseigné, mais configuré en tant que paramètre dynamique.

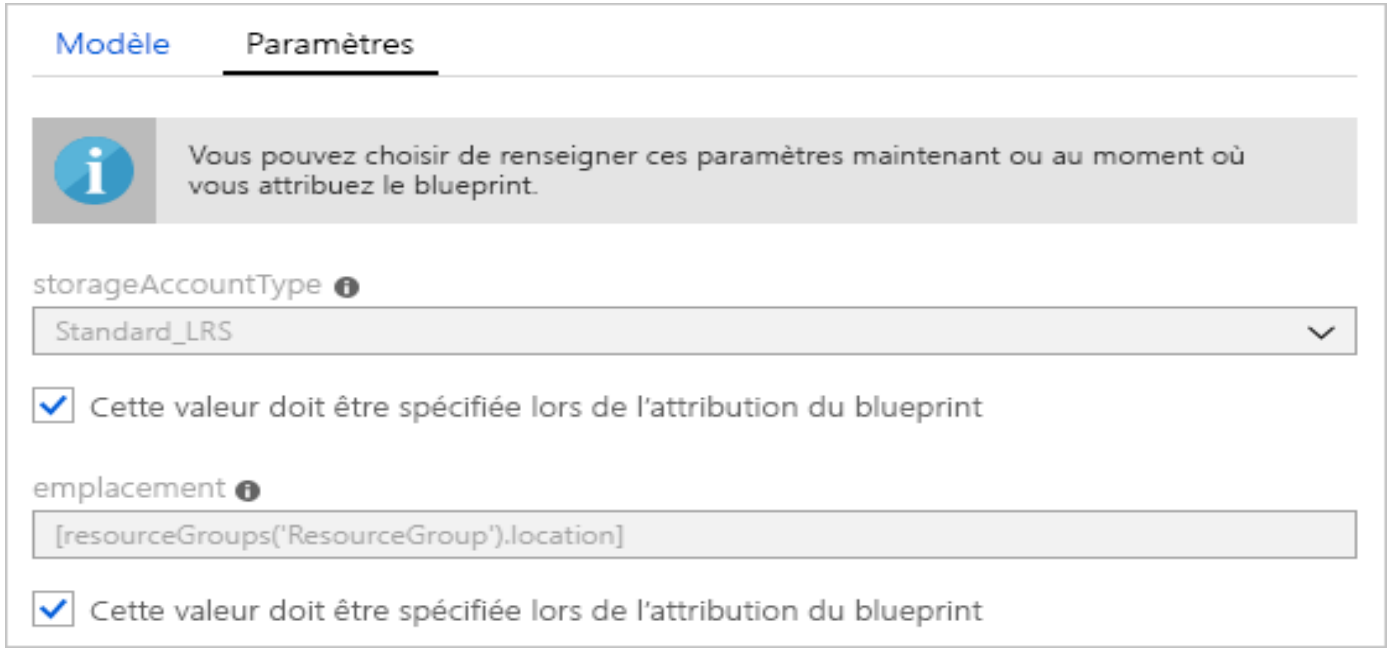
JSON Copier

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "storageAccountType": {
            "type": "string",
            "defaultValue": "Standard_LRS",
            "allowedValues": [
                "Standard_LRS",
                "Standard_GRS",
                "Standard_ZRS",
                "Premium_LRS"
            ],
            "metadata": {
                "description": "Storage Account type"
            }
        },
        "location": {
            "type": "string",
            "defaultValue": "[resourceGroup().location]",
            "metadata": {
                "description": "Location for all resources."
            }
        }
    },
    "variables": {
        "storageAccountName": "[concat('store', uniquestring(resourceGroup().id))]"
    },
    "resources": [{
        "type": "Microsoft.Storage/storageAccounts",
        "name": "[variables('storageAccountName')]",
        "location": "[parameters('location')]",
        "apiVersion": "2018-07-01",
        "sku": {
            "name": "[parameters('storageAccountType')]"
        },
        "kind": "StorageV2",
        "properties": {}
    }],
    "outputs": {
        "storageAccountName": {
            "type": "string",
            "value": "[variables('storageAccountName')]"
        }
    }
}
```

PARTIE 6

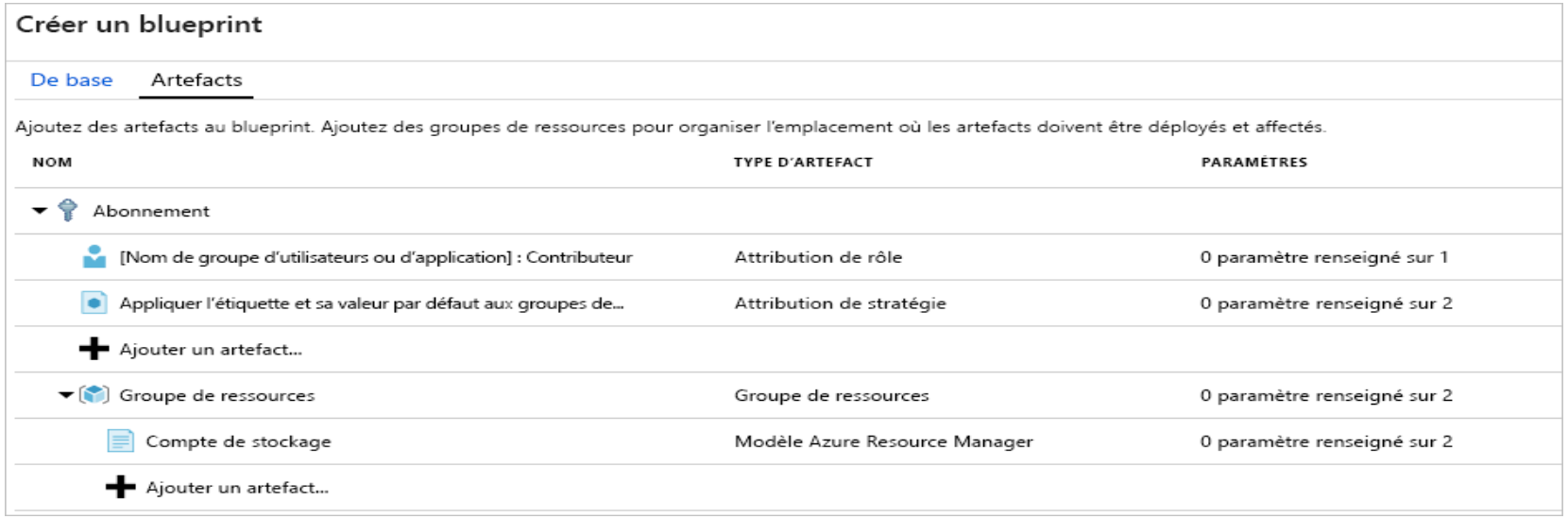
Créer un blueprint

- Décochez la case **storageAccountType** et notez que la liste déroulante contient uniquement les valeurs incluses dans le modèle ARM, sous allowedValues. Cochez la case pour redéfinir le paramètre en paramètre dynamique.
- Sélectionnez **Ajouter** pour ajouter cet artefact au blueprint.



Créer un blueprint

- Votre blueprint terminé doit ressembler à ce qui suit. Dans la colonne **Paramètres**, notez que chaque artefact présente ***x* paramètres renseignés sur *y***. Les paramètres dynamiques sont définis à chaque affectation du blueprint.



- Une fois que vous avez ajouté tous les artefacts planifiés, sélectionnez **Enregistrer le brouillon** en bas de la page.

PARTIE 6

CHAPITRE 1

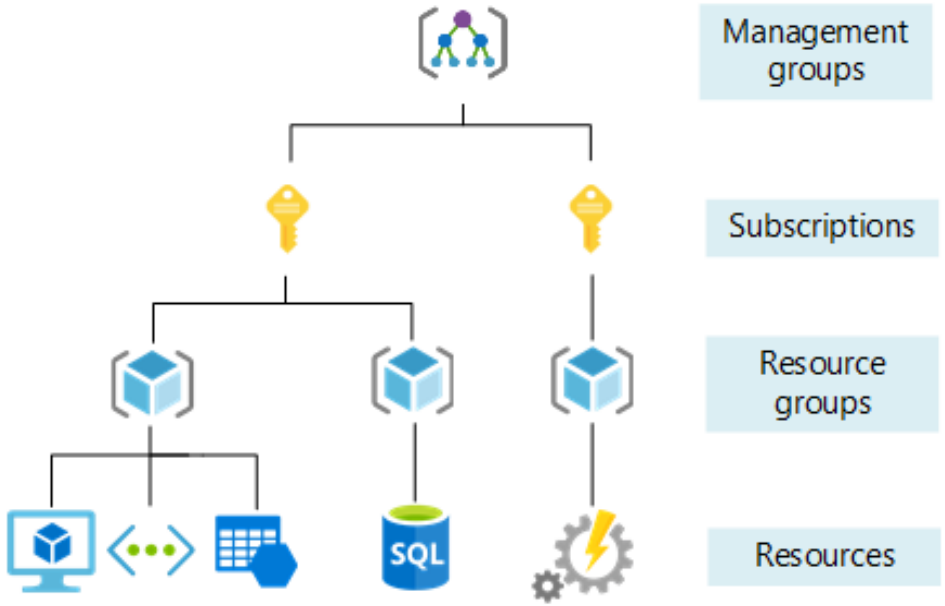
Gouverner les ressources Cloud

1. Stratégie de déploiement
2. Blueprints
3. **Étiquetage des ressources**

Utiliser des étiquettes pour organiser vos ressources Azure et votre hiérarchie de gestion

- Les étiquettes sont des éléments de métadonnées que vous appliquez à vos ressources Azure. Il s'agit de paires clé-valeur qui permettent d'identifier les ressources en fonction de paramètres liés à votre organisation. Ajoutez une clé appelée Environnement si vous souhaitez suivre l'environnement de déploiement de la ressource. Pour identifier les ressources utilisées en production, affectez-leur des valeurs de production. La paire clé-valeur Environnement = Production est maintenant entièrement formée.

- Les étiquettes de ressource prennent en charge tous les services engendrant des coûts. Pour vous assurer que les services engendrant des coûts sont approvisionnés à l'aide d'une étiquette, utilisez l'une des stratégies d'étiquette.



Appliquer des étiquettes

Azure PowerShell propose deux commandes pour appliquer des étiquettes : New-AzTag et Update-AzTag. Vous devez disposer de la Az.Resources version 1.12.0 du module ou ultérieure. Vous pouvez vérifier votre version avec Get-InstalledModule -Name Az.Resources. Vous pouvez installer ce module ou installer Azure PowerShell 3.6.1 ou version ultérieure.

New-AzTag remplace toutes les étiquettes de la ressource, du groupe de ressources ou de l'abonnement. Lorsque vous appelez la commande, transmettez l'ID de ressource de l'entité que vous souhaitez baliser.

L'exemple suivant applique un ensemble d'étiquettes à un compte de stockage :

```
$tags = @{"Dept"="Finance"; "Status"="Normal"}
$resource = Get-AzResource -Name demoStorage -ResourceGroup demoGroup
New-AzTag -ResourceId $resource.id -Tag $tags
```

Une fois la commande terminée, notez que la ressource a deux étiquettes.

Sortie

Properties :

```
Name    Value
======  =======
 Dept    Finance
Status  Normal
```

CHAPITRE 2

Assurer le bon fonctionnement des ressources

Ce que vous allez apprendre dans ce chapitre :

- Soutien technique aux clients utilisateurs
- Interopérabilité entre les services offerts par les autres fournisseurs Cloud

2 heures

CHAPITRE 2

Assurer le bon fonctionnement des ressources

1. **Soutien technique aux clients utilisateurs**
2. Interopérabilité entre les services offerts par les autres fournisseurs Cloud

Aperçu du soutien Azure

Où est disponible le support Azure ?

Le support en lien avec la gestion de la facturation et des abonnements est disponible pour tous les clients Azure dans les marchés où Azure est proposé. Le support technique est disponible pour les clients qui ont acheté un plan de support. Certains services peuvent ne pas être couverts dans toutes les régions immédiatement après la mise à disposition générale.

Dans quelles langues Microsoft fournit-il le support technique ?

Microsoft fournit un support en neuf langues : anglais, espagnol, français, allemand, italien, portugais, chinois traditionnel, coréen et japonais. Le support est disponible 24 heures sur 24, 7 jours par semaine, en anglais pour toutes les gravités et en japonais pour la gravité A uniquement.

Pour toutes les autres langues prises en charge, le support est disponible pendant les heures ouvrées locales. Le support en dehors de ces heures est fourni en anglais (avec des services de traduction si besoin). Vous pouvez également attendre le jour ouvré suivant pour bénéficier du support dans votre langue.

Quelles sont les heures d'ouverture du support ?

En Amérique du Nord, les heures d'ouverture du support sont de 06 h 00 à 18 h 00 (heure du Pacifique) du lundi au vendredi, à l'exclusion des jours fériés. Les heures d'ouverture et les jours fériés varient selon le pays ou la région, mais les heures d'ouverture du support sont généralement de 9 h 00 à 17 h 00 (heure locale), du lundi au vendredi, sauf les jours fériés.

Comment accéder au support technique ?

Les ressources de base en auto-assistance sont incluses pour tous les clients Azure sans coût supplémentaire. Pour un support technique individualisé, vous devez disposer d'un plan de support payant (https://azure.microsoft.com/fr-ca/support/plans/).

Aperçu du soutien Azure

Comment puis-je obtenir de l'aide si je n'ai pas de plan de support ?

Obtenez des réponses à vos questions techniques dans Azure sur Q&A, un canal de la communauté où vous pouvez échanger des idées avec des experts de la communauté, des ingénieurs Microsoft et d'autres clients. L'outil de recherche robuste retourne les réponses de diverses sources, ce qui en fait une ressource d'auto-assistance précieuse.

Si vous êtes membre du Microsoft Partner Network, du Microsoft Developer Network ou du programme Microsoft for Startups, vous pouvez bénéficier d'un support Azure limité même si vous n'avez pas de plan de support payant. Pour connaître les avantages et options de support technique, consultez les conditions générales du service.

Votre abonnement Azure inclut gratuitement l'accès au support relatif à la gestion des abonnements (par exemple, facturation, ajustement des quotas et transfert de compte) via le portail Azure. Il permet également d'accéder au tableau de bord des états Azure, au forum de support de la communauté Azure et à Azure sur Q&A.

Comment contacter le support Azure ?

Accédez au portail Azure et créez une demande de support. Le support relatif à la gestion et à la facturation des abonnements est inclus avec votre abonnement Azure. En outre, le support technique est fourni via l'un des plans de support Azure. Pour obtenir des instructions pas à pas, consultez la page sur la création d'une demande de support Azure.

Nous vous recommandons de soumettre des demandes de support en ligne pour vous aider à obtenir l'expertise technique la plus efficace possible. En raison de la nature détaillée des demandes, il est plus facile d'apporter des informations pertinentes en ligne que par téléphone. Le processus simple et intuitif élimine également les délais imprévus, car les problèmes sont acheminés plus rapidement vers l'ingénieur le plus qualifié.

CHAPITRE 2

Assurer le bon fonctionnement des ressources

1. Soutien technique aux clients utilisateurs
2. **Interopérabilité entre les services offerts par les autres fournisseurs Cloud**

Stockage

Cloud Storage est compatible avec d'autres plates-formes de stockage d'objets. Vous pouvez ainsi intégrer facilement des données provenant de différentes sources. Cette page décrit les outils Cloud Storage permettant de gérer les données d'objets multiplates-formes.

API XML

L'API XML Google Cloud Storage est compatible avec des outils et des bibliothèques fonctionnant avec des services tels que Amazon Simple Storage Service (Amazon S3). Pour utiliser ces outils et bibliothèques avec Cloud Storage, remplacez le point de terminaison de la requête utilisé par l'outil ou la bibliothèque par l'URI Cloud Storage https://storage.googleapis.com, puis configurez l'outil ou la bibliothèque pour utiliser vos clés HMAC Cloud Storage. Pour obtenir des instructions détaillées sur la mise en route, consultez la page Migration simple depuis Amazon Simple Storage Service (Amazon S3).

S'authentifier avec le processus de signature V4

Le processus de signature V4 vous permet de créer des requêtes signées pour l'API XML Cloud Storage. Lorsque vous effectuez le processus de signature V4, vous créez une signature qui peut être utilisée dans un en-tête de requête pour vous authentifier. Vous pouvez effectuer le processus de signature à l'aide d'une signature RSA, ou en utilisant votre workflow Amazon S3 et vos identifiants HMAC.

Importer des données avec le service de transfert de stockage

Le service de transfert de stockage vous permet d'importer de grandes quantités de données en ligne dans Cloud Storage à partir de buckets Amazon S3, de conteneurs Microsoft Storage Azure et d'emplacements HTTP/HTTPS généraux. Ce service permet aussi de planifier des transferts récurrents, de supprimer des objets sources et de sélectionner les objets à transférer.

Ligne de commande

L'outil gsutil vous permet d'accéder à Cloud Storage à partir de la ligne de commande. Il permet également d'accéder à d'autres services de stockage dans le Cloud utilisant l'authentification HMAC, tels qu'Amazon S3, et d'utiliser ces services. Après avoir ajouté vos identifiants Amazon S3 à ~/.aws/credentials, vous pouvez commencer à utiliser gsutil pour gérer les objets de vos buckets Amazon S3. Exemple :

La commande suivante répertorie les objets dans le bucket Amazon S3 example-bucket :

```
gsutil ls s3://example-bucket
```

La commande suivante synchronise les données entre un bucket Amazon S3 et un bucket Cloud Storage :

```
gsutil rsync -d -r s3://my-aws-bucket gs://example-bucket
```