Az 104 review

Prérequis pour les administrateurs Azure

Configurer les ressources Azure avec des outils

Azure Cloud Shell

Azure Cloud Shell est un shell interactif accessible via navigateur pour gérer les ressources Azure. Il permet aux utilisateurs de choisir entre Bash pour Linux et PowerShell pour Windows.

Fonctionnalités :

- Shell temporaire nécessitant le montage d'un partage Azure Files.
- Éditeur de texte graphique intégré basé sur Monaco.
- Authentification automatique pour un accès instantané aux ressources.
- Exécution sur un hôte temporaire pour chaque session et utilisateur.
- Expiration après 20 minutes d'inactivité.
- Nécessite un groupe de ressources, un compte de stockage et un partage de fichiers Azure.
- Partage de fichiers commun pour Bash et PowerShell.
- Persistance de $HOME avec une image de 5 Go dans le partage de fichiers.
- Permissions définies en tant qu'utilisateur Linux standard dans Bash.

Utilisation d'Azure PowerShell

Azure PowerShell est un module ajouté à Windows PowerShell ou PowerShell Core, permettant de se connecter à un abonnement Azure et de gérer les ressources. Il peut être utilisé de deux manières :

1. Via Azure Cloud Shell dans un navigateur.
2. Via une installation locale sur Linux, macOS ou Windows.

Modes :

- **Interactif :** Émettre une commande à la fois.
- **Script :** Exécuter un script de plusieurs commandes.

Module Az : Le module Az contient des applets de commande pour utiliser les fonctionnalités Azure, permettant de contrôler quasiment tous les aspects des ressources Azure.

Utiliser l'interface de ligne de commande Microsoft Azure (Azure CLI)

Azure CLI est un programme en ligne de commande pour se connecter à Azure et administrer les ressources Azure. Il peut être installé localement sur Linux, macOS, et Windows ou utilisé via Azure Cloud Shell dans un navigateur.

Utilisation :

- **Mode interactif :** Utiliser une invite de commande comme cmd.exe pour Windows ou Bash pour Linux/macOS.
- **Mode script :** Assembler des commandes Azure CLI dans un script et l'exécuter.

Commandes :

- Commandes structurées en groupes et sous-groupes (ex. : `storage` contient `account`, `blob`, `share`, `queue`).
- `az find` pour trouver des commandes spécifiques (ex. : `az find blob`).
- `--help` pour obtenir des informations détaillées sur une commande (ex. : `az storage blob --help`).

Ces outils permettent une gestion simplifiée, automatisée et cohérente des ressources Azure, favorisant ainsi l'industrialisation et l'efficacité des opérations.

Utiliser Azure Resource Manager

Avantages d'Azure Resource Manager

Azure Resource Manager (ARM) permet de gérer les ressources Azure de manière unifiée et cohérente. Voici les principaux avantages de son utilisation :

1. **Gestion par Groupe :**
    - ARM permet de travailler avec les ressources de solution sous forme de groupe. Vous pouvez déployer, mettre à jour ou supprimer toutes les ressources d'une solution en une seule opération coordonnée, simplifiant ainsi la gestion des ressources.
2. **Déploiement Répétable :**
    - Vous pouvez utiliser un modèle de déploiement unique qui fonctionne avec différents environnements (test, intermédiaire, production). Cela permet de déployer des configurations de manière répétée et cohérente tout au long du cycle de développement.
3. **Mode Déclaratif :**
    - ARM utilise une syntaxe déclarative, où vous définissez les ressources que vous souhaitez créer dans un fichier JSON. Ce mode déclaratif simplifie la gestion des infrastructures en automatisant les déploiements.
4. **Sécurité et Contrôle :**

    - ARM assure des fonctions de sécurité et de contrôle d'accès basées sur les rôles (RBAC). Vous pouvez appliquer des permissions précises aux utilisateurs pour gérer les ressources de manière sécurisée.
5. **Audit et Gestion des Ressources :**
    - ARM permet de suivre et d'auditer les opérations effectuées sur les ressources. Les tags peuvent être appliqués aux ressources pour une gestion et une facturation simplifiées.
6. **Définition des Dépendances :**
    - Vous pouvez définir les dépendances entre les ressources, garantissant qu'elles sont déployées dans l'ordre correct.
7. **Tags et Facturation :**
    - ARM permet de taguer les ressources pour les organiser et les catégoriser. La facturation peut également être effectuée sur la base de ces tags, facilitant la gestion des coûts.
8. **Cohérence de Gestion :**
    - ARM fournit une couche de gestion cohérente pour effectuer des tâches avec différents outils (Azure PowerShell, Azure CLI, portail Azure, API REST, SDK clients). Tous ces outils interagissent avec la même API ARM, garantissant une gestion uniforme des ressources.

Terminologie en lien avec les ressources Azure

1. **Ressource :**
    - Élément gérable disponible dans Azure, tel qu'une machine virtuelle, un compte de stockage, etc.
2. **Groupe de Ressources :**
    - Conteneur qui contient des ressources associées pour une solution Azure. Il facilite la gestion collective des ressources.
3. **Fournisseur de Ressources :**
    - Service qui fournit les ressources que vous pouvez déployer et gérer via ARM. Par exemple, `Microsoft.Compute` pour les machines virtuelles et `Microsoft.Storage` pour les comptes de stockage. Chaque fournisseur propose un ensemble de ressources et d'opérations pour gérer un service Azure.
4. **Modèle :**
    - Fichier JSON qui définit les ressources à déployer dans un groupe de ressources, ainsi que leurs dépendances. Il utilise une syntaxe déclarative pour spécifier les configurations souhaitées.
5. **Syntaxe Déclarative :**
    - Méthode de configuration où vous déclarez les ressources à créer et leurs configurations dans un modèle JSON, simplifiant ainsi le processus de déploiement.
6. **Type de Ressource :**

    - Le format du nom d'un type de ressource est `{fournisseur de ressources}/{type de ressource}`. Par exemple, `Microsoft.KeyVault/vaults` pour un coffre de clés.

En résumé, Azure Resource Manager offre une gestion simplifiée, sécurisée et cohérente des ressources Azure, permettant une automatisation efficace et une meilleure organisation des infrastructures cloud.

Création de Groupes de Ressources

- **Suivi des Déploiements :**
    - Permet de suivre l'exécution des déploiements. En cas d'échec, les informations fournies aident à diagnostiquer et corriger les erreurs.
    - Les déploiements sont incrémentiels : l'ajout de nouvelles ressources ne supprime pas les ressources existantes.
- **Considérations :**
    - Une ressource ne peut appartenir qu'à un seul groupe de ressources à la fois.
    - Les groupes de ressources ne peuvent pas être renommés.
    - Un groupe de ressources peut contenir différents types de ressources et des ressources de différentes régions.
- **Facteurs Importants :**
    - Les ressources d'un groupe doivent partager le même cycle de vie (déploiement, mise à jour, suppression).
    - Il est possible d'ajouter ou supprimer des ressources d'un groupe de ressources à tout moment.
    - Les ressources peuvent être déplacées d'un groupe de ressources à un autre, avec certaines limitations.

Verrous Azure Resource Manager

- **Types de Verrous :**
    - **Lecture seule :** Empêche toute modification de la ressource.
    - **Suppression :** Empêche la suppression de la ressource.
- **Héritage :**
    - Les ressources enfants héritent des verrous du groupe parent.

Réorganisation et Suppression des Ressources

- **Déplacement de Ressources :**
    - Lors du déplacement, les groupes source et cible sont verrouillés, empêchant toute modification des ressources pendant le processus.
    - Les ressources restent opérationnelles et accessibles pendant le déplacement.
- **Suppression :**

    - La suppression d’un groupe de ressources entraîne la suppression de toutes les ressources qu’il contient.
    - Commande PowerShell pour supprimer un groupe de ressources : `Remove-AzResourceGroup -Name "ContosoRG01"`.

Gestion des Limites de Ressources

- **Observation des Limites :**
    - Les limites d’utilisation des ressources peuvent être observées et comparées aux limites maximales.
    - Pour augmenter une limite, une demande peut être faite via un lien approprié.
    - Certaines limites maximales ne peuvent pas être augmentées.

Modèles Azure Resource Manager

- **Structure des Modèles :**
    - Les modèles ARM sont écrits en JSON.
    - Clés et valeurs possibles : chaîne, chiffre, expression booléenne, liste de valeurs, objet.
- **Sections des Modèles :**
    - `$schema`
    - `contentVersion`
    - `parameters`
    - `variables`
    - `functions`
    - `resources`
    - `outputs`

Ces fonctionnalités et considérations permettent de gérer efficacement et de manière cohérente les ressources Azure, facilitant leur déploiement, leur mise à jour et leur organisation.

Examen des modèles Bicep

Qu'est-ce que Bicep ?

Azure Bicep est un langage spécifique à un domaine (DSL) utilisant une syntaxe déclarative pour déployer des ressources Azure. Il offre une syntaxe concise, une gestion fiable des types et une réutilisation du code. Bicep est une abstraction sur les modèles ARM JSON, sans perte de fonctionnalités.

Fonctionnement de Bicep

- **Transpilation :** Les modèles Bicep sont convertis en modèles JSON ARM lors du déploiement, un processus appelé transpilation. Cela permet d'utiliser une syntaxe plus simple tout en conservant toutes les capacités des modèles JSON.

Avantages de Bicep par rapport à JSON

1. **Syntaxe Simplifiée :**
    - Bicep utilise une syntaxe plus intuitive que JSON. Les paramètres et variables sont référencés directement sans fonctions complexes.
    - L'interpolation de chaînes remplace la concaténation pour combiner des valeurs.
    - Les propriétés des ressources sont référencées par leur nom symbolique, simplifiant les instructions de référence.
2. **Modules :**
    - Les déploiements complexes peuvent être décomposés en modules plus petits et référencés dans un modèle principal, facilitant la gestion et la réutilisation.
3. **Gestion Automatique des Dépendances :**
    - Bicep détecte automatiquement les dépendances entre les ressources, réduisant le travail manuel de création de modèles.
4. **Validation de Type et IntelliSense :**
    - L'extension Bicep pour Visual Studio Code offre une validation riche et IntelliSense, simplifiant la création des modèles.

Modèles de Démarrage Rapide Azure

- **Composants :**
    - `README.md` : Vue d'ensemble du modèle.
    - `azuredeploy.json` : Définition des ressources à déployer.
    - `azuredeploy.parameters.json` : Valeurs nécessaires pour le modèle.

Automatisation des Tâches Azure avec PowerShell

- **Azure PowerShell :**
    - Permet d'automatiser les tâches complexes ou répétitives sur Azure.

Choix d'un Outil d'Administration

1. **Automation :**
    - Azure PowerShell et Azure CLI sont adaptés pour l'automatisation, contrairement au portail Azure.
2. **Courbe d'Apprentissage :**
    - Le portail Azure est facile à utiliser sans apprentissage préalable.

    - Azure PowerShell et Azure CLI nécessitent la connaissance des commandes et de leur syntaxe.
3. **Ensemble de Compétences de l’Équipe :**
    - Si votre équipe a déjà une expertise en PowerShell, elle sera à l’aise avec Azure PowerShell.

Outils d'Administration Azure

- **Portail Azure :** Interface web pour créer, configurer et modifier des ressources Azure sans apprendre de nouvelles commandes.
- **Azure CLI :** Outil en ligne de commande multiplateforme pour administrer des ressources Azure.
- **Azure PowerShell :** Utilisé pour l'automatisation via des scripts PowerShell.

En résumé, Azure Bicep simplifie la gestion des ressources Azure par rapport aux modèles JSON ARM, tout en offrant des avantages supplémentaires comme la modularité, la gestion automatique des dépendances et des outils de développement avancés. Choisir l'outil d'administration approprié dépend des besoins en automatisation, de la courbe d'apprentissage et des compétences de l'équipe.

Déployer l’infrastructure Azure en utilisant des modèles ARM JSON

Infrastructure en tant que Code (IaC)

L'infrastructure en tant que code (IaC) permet de décrire, via le code, l'infrastructure nécessaire pour une application. Les principaux avantages de l'IaC incluent :

- **Configurations Cohérentes :** Assure des configurations uniformes à travers différents environnements.
- **Scalabilité Améliorée :** Facilite l'extension et la réduction des ressources en fonction des besoins.
- **Déploiements Plus Rapides :** Automatise et accélère les processus de déploiement.
- **Meilleure Traçabilité :** Offre une vue d'ensemble des modifications et des déploiements d'infrastructure.

Qu'est-ce qu'un Modèle ARM ?

Les modèles Azure Resource Manager (ARM) sont des fichiers JSON qui définissent l'infrastructure et la configuration pour les déploiements Azure. Ils utilisent une syntaxe déclarative, permettant de spécifier les ressources nécessaires sans décrire les étapes de leur déploiement, contrairement à la syntaxe impérative.

Avantages de l'Utilisation des Modèles ARM

1. **Automatisation des Déploiements :**
    - Permet d'automatiser les processus de déploiement, réduisant les erreurs manuelles et augmentant l'efficacité.
2. **Pratique de l'IaC :**
    - Intègre l'infrastructure dans les projets de développement, facilitant la gestion et la version des configurations.
3. **Stockage et Versionnement :**
    - Les fichiers de modèle peuvent être stockés dans un référentiel source, permettant le contrôle de version et la collaboration.
4. **Validation Intégrée :**
    - Les modèles peuvent être validés avant le déploiement, assurant leur conformité et réduisant les risques d'erreurs.
5. **Modularité et Réutilisation :**
    - Les modèles peuvent être divisés en composants plus petits et réutilisables, favorisant la modularité et la maintenabilité.
6. **Imbrication de Modèles :**
    - Les modèles ARM peuvent être imbriqués dans d'autres modèles, permettant la création de structures complexes de manière organisée.
7. **Historique des Déploiements :**

    - Permet de consulter l'historique des déploiements et d'obtenir des informations sur leur état, facilitant la traçabilité et le dépannage.
8. **Idempotence :**
    - Les modèles ARM sont idempotents, garantissant que les déploiements répétés produisent le même résultat, assurant ainsi la consistance des ressources.

Structure d'un Modèle ARM

Les modèles ARM sont écrits en JSON et contiennent plusieurs sections clés :

- **$schema :** URL du schéma de déploiement utilisé.
- **contentVersion :** Version du contenu du modèle.
- **parameters :** Paramètres d'entrée pour le modèle.
- **variables :** Variables utilisées pour simplifier et gérer les valeurs complexes.
- **resources :** Définition des ressources à déployer.
- **outputs :** Valeurs de sortie générées par le modèle.

Exemple de Modèle ARM (Structure de Base)

```
{

  "$schema":
"http://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",

  "contentVersion": "1.0.0.0",

  "parameters": {},

  "variables": {},

  "resources": [],

  "outputs": {}

}
```

Structure des fichiers du modèle ARM

Élément	Description

schema	Une section obligatoire qui définit l'emplacement du fichier du schéma JSON qui décrit la structure des données JSON. Le numéro de version que vous utilisez dépend de l'étendue du déploiement et de votre éditeur JSON.
contentVersion	Une section obligatoire qui définit la version de votre modèle (par exemple 1.0.0.0). Vous pouvez utiliser cette valeur pour documenter les modifications importantes apportées à votre modèle pour être sûr de déployer le modèle approprié.
apiProfile	Une section facultative qui définit une collection de versions d'API pour les types de ressources. Vous pouvez utiliser cette valeur pour éviter d'avoir à spécifier les versions d'API pour chaque ressource dans le modèle.
parameters	Une section facultative où vous définissez des valeurs fournies lors du déploiement. Ces valeurs peuvent être fournies par un fichier de paramètres, par des paramètres de ligne de commande ou dans le portail Azure.
variables	Une section facultative où vous définissez des valeurs utilisées pour simplifier les expressions de langage de gabarit.
functions	Une section facultative où vous pouvez définir des fonctions définies par l'utilisateur qui sont disponibles dans le modèle. Les fonctions définies par l'utilisateur peuvent simplifier votre modèle quand des expressions compliquées y sont utilisées de façon répétée.
resources	Une section obligatoire qui définit les éléments réels que vous voulez déployer ou mettre à jour dans un groupe de ressources ou un abonnement.
output	Une section facultative où vous spécifiez les valeurs qui seront retournées à la fin du déploiement.

Implémenter et gérer le stockage dans Azure

Points à connaître sur le stockage Azure

Category	Description	Exemples de stockage
Données de la machine virtuelle	Le stockage de données de machines virtuelles comprend des disques et des fichiers. Les disques constituent un stockage de blocs persistant pour les machines virtuelles Azure IaaS. Les fichiers sont des partages de fichiers complètement managés dans le cloud.	Le stockage des données de machine virtuelle est fourni via des disques managés Azure. Les machines virtuelles se servent des disques de données pour stocker des données comme des fichiers de base de données, du contenu statique de site web ou du code d'application personnalisé. Le nombre de disques de données que vous pouvez ajouter dépend de la taille de la machine virtuelle. Chaque disque de données a une capacité maximale de 32 767 Go.
Les données non structurées	Les données non structurées sont les moins organisées. Ces données sont un mélange d'informations stockées ensemble, mais les données n'ont pas de relation claire. Le format des données non structurées est dit *non relationnel*.	Les données non structurées peuvent être stockées à l'aide du Stockage Blob Azure et de Azure Data Lake Storage. Le stockage Blob est un magasin d'objets cloud basés sur REST très évolutif. Azure Data Lake Storage est le système de fichiers DFS Hadoop (HDFS) en tant que service.

Données structurées	Les données structurées sont stockées dans un format relationnel assorti d'un schéma partagé. Les données structurées sont souvent contenues dans une table de base de données constituée de lignes, de colonnes et de clés. Les tables sont un magasin NoSQL avec mise à l'échelle automatique.	Les données structurées peuvent être stockées à l'aide du Stockage Table Azure, d'Azure Cosmos DB et de Azure SQL Database. Azure Cosmos DB est un service de base de données distribué à l'échelle mondiale. Azure SQL Database est une base de données en tant que service complètement managée reposant sur SQL.

Niveaux du compte de stockage

- Les comptes de stockage **Standard** sont sauvegardés par des disques durs (HDD). Un compte de stockage standard fournit le coût le plus bas par Go.
- Les comptes de stockage **Premium** reposent sur des disques SSD et offrent des performances homogènes à faible latence.

Explorer les services de stockage Azure

- **Stockage Blob Azure (conteneurs)** : un magasin d'objets hautement évolutifs pour les données texte et binaires.
- **Azure Files** : partages de fichiers gérés pour les déploiements sur le cloud ou locaux.
- **Stockage File d'attente Azure** : un magasin de messagerie pour une messagerie fiable entre les composants des applications.
- **Stockage Table Azure** : service qui stocke des données structurées non relationnelles (également appelées données NoSQL structurées).

Compte de stockage	Services pris en charge	Utilisation recommandée
Standard Usage général v2	Stockage Blob (y compris Data Lake Stockage), Stockage File d'attente, Stockage Table et Azure Files	Compte de stockage standard pour la plupart des scénarios, notamment les objets blob, les partages de fichiers, les files d'attente, les tables et les disques (objets blob de pages).

Premium Objets blob de bloc	Stockage Blob (y compris Data Lake Storage)	Compte de stockage Premium pour les objets blob de blocs et les objets blob d'ajout. Recommandé pour les applications avec des taux de transaction élevés. Utilisez des objets blob de blocs Premium si vous utilisez des objets plus petits ou si vous avez besoin d'une faible latence de stockage. Ce stockage est conçu pour évoluer avec vos applications.
Premium Partages de fichiers	Azure Files	Compte de stockage Premium pour les partages de fichiers uniquement. Recommandé pour l'entreprise ou des applications de mise à l'échelle hautes performances. Utilisez des partages de fichiers Premium si vous avez besoin de la prise en charge des partages de fichiers SMB (Server Message Block) et NFS.
Premium Objets blob de page	Objets blob de pages uniquement	Compte de stockage haute performance Premium pour les blobs de pages uniquement. Les objets blob de pages sont idéaux pour stocker des structures de données éparses et basées sur les index, comme le système d'exploitation et les disques de données des machines virtuelles et des bases de données.

Configurer des domaines personnalisés

- **Le mappage direct** vous permet d'activer un domaine personnalisé pour un sous-domaine sur un compte de stockage Azure. Pour cette approche, vous créez un enregistrement `CNAME` qui pointe du sous-domaine vers le compte de stockage Azure.
  - Sous-domaine : `blobs.contoso.com`
  - Compte de stockage Azure : `\<storage account>\.blob.core.windows.net`
  - Enregistrement direct `CNAME` : `contosoblobs.blob.core.windows.net`

- **Le mappage de domaine intermédiaire** est appliqué à un domaine déjà utilisé dans Azure. Cette approche peut entraîner un temps d'arrêt mineur pendant que le domaine est mappé. Pour éviter les temps d'arrêt, vous pouvez utiliser le domaine intermédiaire asverify pour valider le domaine.
    - enregistrement `CNAME` : **`asverify`**`.blobs.contoso.com`
    - Enregistrement intermédiaire `CNAME` : **`asverify`**`.contosoblobs.blob.core.windows.net`

Sécuriser les points de terminaison de stockage

Dans le Portail Azure, chaque service Azure a besoin d'étapes pour configurer les points de terminaison de service et restreindre l'accès réseau pour le service.

Informations sur la configuration des points de terminaison de service

- Les paramètres **Pare-feu et réseaux virtuels** limitent l'accès au compte de stockage à partir de sous-réseaux spécifiques sur des réseaux virtuels ou des IP publiques.
- Vous pouvez également configurer le service pour autoriser l'accès à une ou plusieurs plages d'adresses IP publiques.
- Les sous-réseaux et les réseaux virtuels doivent se trouver dans la même région Azure ou paire de régions que votre compte de stockage.

Implémenter Stockage Blob Azure

Points à connaître sur Stockage Blob Azure

- Le Stockage Blob peut stocker n'importe quel type de données texte ou binaires.
- Le Stockage Blob utilise trois ressources pour stocker et gérer vos données :
    - Un compte de stockage Azure
    - Des conteneurs dans un compte de stockage Azure
    - Objets blob dans un conteneur
- Pour implémenter le stockage Blob, vous configurez plusieurs paramètres :
    - Options de conteneur d'objets blob
    - Types d'objets blob et options de chargement
    - Niveaux d'accès de stockage d'objets blob
    - Règles de cycle de vie des objets blob
    - Options de réplication d'objets blob

Niveau de stockage chaud

Le niveau chaud est optimisé pour les lectures et écritures d'objets fréquents du compte de stockage Azure.
Ce niveau d'accès présente les coûts d'accès les plus bas, mais des coûts de stockage plus élevés que les niveaux d'accès Froid et Archive.

Niveau de stockage froid

Le niveau Froid permet de stocker de grandes quantités de données rarement utilisées. Ce niveau est prévu pour les données qui restent dans le niveau froid pendant au moins 30 jours.
Le stockage des données dans le niveau Froid est plus rentable. L'accès aux données au niveau Froid peut être plus coûteux que l'accès aux données du niveau Chaud.

Niveau de stockage archive

Le niveau archive est un niveau hors ligne optimisé pour les données qui peuvent tolérer plusieurs heures de latence de récupération. Les données doivent rester dans le niveau archive pendant au moins 180 jours ; sinon, elles sont soumises à des frais de suppression anticipée.
Ce niveau est l'option la plus économique pour le stockage des données. L'accès aux données est plus coûteux dans le niveau Archive que dans les autres niveaux.

Ce qu'il faut savoir sur la gestion du cycle de vie

- Faire passer les objets blob à un niveau de stockage plus froid (de Chaud à Froid, de Chaud à Archive ou de Froid à Archive) pour optimiser les performances et le coût.
- Supprimer les objets blob à la fin de leurs cycles de vie.
- Définissez des conditions basées sur des règles à exécuter une fois par jour au niveau du compte de stockage Azure.
- Appliquez des conditions basées sur des règles aux conteneurs ou à un sous-ensemble d'objets blob.

Configurer des règles de stratégie de gestion de cycle de vie

Dans le Portail Azure, vous créez des règles de stratégie de gestion du cycle de vie pour votre compte de stockage Azure en spécifiant plusieurs paramètres. Pour chaque règle, vous créez des conditions **If - Then** pour faire transitionner ou expirer les données en fonction de vos spécifications.

- **If** : la clause **If** définit la clause d'évaluation pour la règle de stratégie. Lorsque la clause **If** est évaluée à true, la clause **Then** est exécutée. Utilisez la clause **If** pour définir la période à appliquer aux données d'objet blob. La fonctionnalité de gestion du cycle de vie vérifie si les données ont fait l'objet d'un accès ou d'une modification en fonction de l'heure spécifiée.

    - **Plus de (jours)** : nombre de jours à utiliser dans la condition d'évaluation.
- **Then** : la clause **Then** définit la clause d'action pour la règle de stratégie. Lorsque la clause **If** est évaluée à true, la clause **Then** est exécutée. Utilisez la clause **Then** pour définir l'action de transition pour les données d'objet

blob. La fonctionnalité de gestion du cycle de vie fait transitionner les données en fonction du paramètre.

    - **Déplacer vers le stockage Froid** : les données d'objet blob sont transférées vers le stockage de niveau Froid.
    - **Déplacer vers le stockage Archive** : les données d'objet blob sont transférées vers le stockage de niveau Archive.
    - **Supprimer l'objet blob** : les données d'objet blob sont supprimées.

Ce qu'il faut savoir sur la réplication d'objets blob

- La réplication d'objets implique que le contrôle de version des objets blob soit activé sur les comptes source et de destination.
- La réplication d'objets ne prend pas en charge les captures instantanées d'objets blob. Les instantanés d'un objet blob du compte source ne sont pas répliqués vers le compte de destination.
- La réplication d'objets est prise en charge lorsque les comptes source et de destination se trouvent au niveau chaud ou froid. Les comptes source et de destination peuvent se trouver dans des niveaux différents.
- Lorsque vous configurez la réplication d'objets, vous créez une stratégie de réplication qui spécifie le compte Stockage Azure source et le compte de destination.
- Une stratégie de réplication comprend une ou plusieurs règles qui spécifient un conteneur source et un conteneur de destination. La stratégie identifie les objets blob dans le conteneur source à répliquer.

Charger des objets blob

- **Objets blob de blocs**. Un objet blob de blocs se compose de blocs de données assemblés pour créer un objet blob. La plupart des scénarios de stockage d'objets blob utilisent des objets blob de blocs. Les objets blob de blocs sont idéaux pour le stockage des données texte et binaires dans le cloud, telles que des fichiers, des images et des vidéos.
- **Objets blob d'ajout**. Un objet blob d'ajout est similaire à un objet blob de blocs, car l'objet blob d'ajout se compose également de blocs de données. Les blocs de données d'un objet blob d'ajout sont optimisés pour les opérations d'*ajout*. Les objets blob d'ajout sont utiles pour les scénarios de journalisation, où la quantité de données peut augmenter à mesure que l'opération de journalisation se poursuit.
- **Objets blob de pages**. La taille d'un objet blob de pages peut atteindre 8 To. Les objets blob de pages sont plus efficaces pour les opérations de lecture/écriture fréquentes. Les machines virtuelles Azure utilisent des objets blob de pages pour les disques du système d'exploitation et les disques de données.

- Le type d'objet blob de blocs est le type par défaut d'un nouvel objet blob. Lorsque vous créez un objet blob, si vous ne choisissez pas de type spécifique, le nouvel objet blob est créé en tant qu'objet blob de blocs.
- Après avoir créé un objet blob, vous ne pouvez pas modifier son type

Déterminer la tarification du Stockage Blob

- **Niveaux de performances**. À mesure que le niveau de performance devient froid, le coût par gigaoctet diminue.
- **Coûts d'accès aux données**. les frais d'accès aux données augmentent à mesure que le niveau refroidit.
- **Coûts des transactions**. Il existe des frais par transaction pour tous les niveaux. Les frais augmentent au fur et à mesure que le niveau devient froid.
- **Coûts de transfert de données de géoréplication**. Ces coûts s'appliquent uniquement aux comptes pour lesquels la géoréplication est configurée, notamment GRS et RA-GRS. Le transfert de données de géoréplication implique des frais par gigaoctet.
- **Coûts de transfert de données sortantes**. Les transferts de données sortants (données transférées hors d'une région Azure) entraînent une facturation de l'utilisation de la bande passante au gigaoctet.
- **Modifications apportées au niveau de stockage**. Passer d'un niveau de stockage de compte froid à un niveau de stockage chaud implique des frais correspondant à la lecture de toutes les données existantes du compte de stockage.

Passer en revue les stratégies de sécurité de Stockage Azure

- **Chiffrement**. Toutes les données écrites dans le Stockage Azure sont automatiquement chiffrées à l'aide du chiffrement du Stockage Azure.
- **Authentification**. Azure Active Directory (Azure AD) et le contrôle d'accès en fonction du rôle (RBAC) sont pris en charge dans le Stockage Azure à la fois pour les opérations de gestion des ressources et les opérations de données.
    - Attribuez des rôles RBAC limités au compte de stockage Azure à des principaux de sécurité et utilisez Azure AD pour autoriser les opérations de gestion des ressources comme la gestion des clés.
    - L'intégration d'Azure AD est prise en charge pour les opérations de données sur Stockage Blob Azure et Stockage File d'attente Azure.
- **Données en transit**. Les données peuvent être sécurisées en transit entre une application et Azure au moyen du chiffrement côté client, de HTTPS ou de SMB 3.0.
- **Chiffrement de disque**. Les disques de système d'exploitation et les disques de données utilisés par Machines virtuelles Azure peuvent être chiffrés à l'aide du service Azure Disk Encryption.

- **Signatures d'accès partagé**. Il est possible d'accorder un accès délégué aux objets de données Stockage Azure en utilisant une signature d'accès partagé (SAS).
- **Autorisation**. Chaque demande auprès d'une ressource sécurisée dans le Stockage Blob, Azure Files, Stockage File d'attente ou Azure Cosmos DB (Stockage Table Azure) doit être autorisée. L'autorisation garantit que les ressources de votre compte de stockage sont accessibles uniquement quand vous le souhaitez, et uniquement pour les utilisateurs ou les applications autorisées.

Créer des signatures d'accès partagé

- Une signature SAS vous offre un contrôle précis sur le type d'accès que vous accordez aux clients qui la possèdent.
- Une signature SAS au niveau du compte peut déléguer l'accès à plusieurs services de Stockage Azure, comme des objets blob, des fichiers, des files d'attente et des tables.
- Vous pouvez spécifier l'intervalle de temps pendant lequel une signature SAS est valide, notamment la date et l'heure de début et d'expiration.
- Vous spécifiez les autorisations accordées par la signature SAS. Une signature SAS pour un objet blob peut accorder des autorisations en lecture et en écriture sur cet objet blob, mais pas d'autorisations de suppression.
- La signature SAS offre un contrôle au niveau du compte et au niveau du service.
    - La signature SAS **au niveau du compte** délègue l'accès aux ressources dans un ou plusieurs services Stockage Azure.
    - La signature SAS **au niveau du service** délègue l'accès à une ressource dans un seul service Stockage Azure.
- Il existe des paramètres de configuration SAS facultatifs :
    - **Adresses IP**. Vous pouvez identifier une adresse IP ou plage d'adresses IP à partir de laquelle le Stockage Azure accepte la signature SAS. Configurez cette option pour spécifier une plage d'adresses IP appartenant à votre organisation.
    - **Protocoles**. Vous pouvez spécifier le protocole sur lequel Stockage Azure accepte la signature SAS. Configurez cette option pour restreindre l'accès aux clients à l'aide du protocole HTTP.

Configurer une signature d'accès partagé

- **Méthode de signature** : choisissez la méthode de signature : clé de compte ou clé de délégation utilisateur.
- **Clé de signature** : sélectionnez la clé de signature dans votre liste de clés.
- **Autorisations** : sélectionnez les autorisations accordées par la signature SAS, comme la lecture ou l'écriture.

- **Date/heure de début et d'expiration** : spécifiez l'intervalle de temps de validité de la signature SAS. Définissez l'heure de début et l'heure d'expiration.
- **Adresses IP autorisées** : (facultatif) identifiez une adresse IP ou une plage d'adresses IP à partir de laquelle le Stockage Azure accepte la signature SAS.
- **Protocoles autorisés** : (facultatif) sélectionnez le protocole via lequel le Stockage Azure accepte la signature SAS.

Déterminer le chiffrement du Stockage Azure

- Les données sont chiffrées automatiquement avant d'être conservées dans Disques managés Azure, Stockage Blob Azure, Stockage File d'attente Azure, Azure Cosmos DB, Stockage Table Azure ou Azure Files.
- Les données sont déchiffrées automatiquement avant d'être récupérées.
- Le chiffrement du Stockage Azure, le chiffrement au repos, le déchiffrement et la gestion des clés sont transparents pour les utilisateurs.
- Toutes les données écrites dans le Stockage Azure sont chiffrées avec le chiffrement AES (Advanced Encryption Standard) 256 bits. AES (Advanced Encryption Standard) est l'un des chiffrements par blocs les plus sécurisés.
- Azure Disk Encryption est activé pour tous les comptes de stockage nouveaux et existants, et il ne peut pas être désactivé.

Créer des clés gérées par le client

- En créant vos propres clés (appelées clés *gérées par le client*), vous disposez d'une plus grande flexibilité et d'un meilleur contrôle.
- Vous pouvez créer, désactiver, auditer, effectuer une rotation et définir des contrôles d'accès pour vos clés de chiffrement.
- Les clés gérées par le client peuvent être utilisées avec le chiffrement du Stockage Azure. Vous pouvez utiliser une nouvelle clé ou un coffre de clés et une clé existants. Le compte de stockage Azure et le coffre de clés doivent se trouver dans la même région, mais ils peuvent appartenir à des abonnements différents.

Configurer les clés gérées par le client

- **Type de chiffrement** : choisissez si la clé de chiffrement est gérée par Microsoft ou par vous-même (le client).
- **Clé de chiffrement** : spécifiez une clé de chiffrement en entrant un identificateur URI ou sélectionnez une clé dans un coffre de clés existant.

Configurer Azure Files et Azure File Sync

Azure Files (partages de fichiers)	Stockage Blob Azure (objets blob)	Azure Disks (objets blob de pages)
Azure Files fournit les protocoles SMB et NFS, des bibliothèques clientes, et une interface REST permettant d'accéder aux fichiers stockés à partir de n'importe quel emplacement.	Stockage Blob Azure fournit des bibliothèques clientes ainsi qu'une interface REST permettant de stocker des données non structurées, et d'y accéder, à une grande échelle dans des objets blob de blocs.	Azure Disks est similaire au service Stockage Blob Azure. Azure Disks fournit une interface REST permettant de stocker des données structurées ou indexées, et d'y accéder, dans des objets blob de pages.
- Les fichiers dans un partage Azure Files sont de véritables objets de répertoire. - Les données dans Azure Files sont accessibles via des partages de fichiers sur plusieurs machines virtuelles.	- Les objets blob dans Stockage Blob Azure sont un espace de noms plat. - Les données blob dans Stockage Blob Azure sont accessibles via un conteneur.	- Les objets blob de pages dans Azure Disks sont stockés sous forme de pages de 512 octets. - Les données d'objet blob de pages sont propres à une machine virtuelle unique.
Azure Files *est idéal pour la migration lift-and-shift d'une application vers le cloud qui utilise déjà les API du système de fichiers natif. Partagez des données entre l'application et d'autres applications s'exécutant dans Azure.* *Azure Files est une bonne option pour stocker les outils de développement et de débogage qui doivent être accessibles à partir de nombreuses machines virtuelles.*	***Stockage Blob Azure*** *est idéal pour les applications qui doivent prendre en charge les scénarios de streaming et d'accès aléatoire.* *Stockage Blob Azure est une bonne option lorsque vous souhaitez pouvoir accéder aux données d'application de n'importe quel endroit.*	*Les solutions* ***Azure Disks*** *sont idéales lorsque vos applications exécutent fréquemment des opérations de lecture/écriture aléatoires.* *Azure Disks est une bonne option lorsque vous souhaitez stocker des données relationnelles pour les disques de système d'exploitation et de données dans des machines virtuelles et bases de données Azure.*

Créer des instantanés de partage de fichiers

- La fonctionnalité d'instantané de partage Azure Files est fournie au niveau du partage de fichiers.
- Les instantanés de partage sont incrémentiels par nature. Seules les données modifiées depuis le dernier instantané de partage sont enregistrées.
- Les instantanés incrémentiels réduisent le temps nécessaire à la création d'instantané de partages et permettent de réaliser des économies sur les coûts de stockage.
- Bien que les instantanés de partage soient enregistrés de façon incrémentielle, vous ne devez conserver que le dernier instantané de partage pour restaurer le partage.
- Vous pouvez récupérer un instantané de partage pour un fichier individuel. Ce niveau de prise en charge permet de restaurer des fichiers individuels plutôt que d'avoir à restaurer l'intégralité du partage de fichiers.
- Si vous voulez supprimer un partage contenant des instantanés de partage, vous devez commencer par supprimer tous les instantanés.

Implémenter Azure File Sync

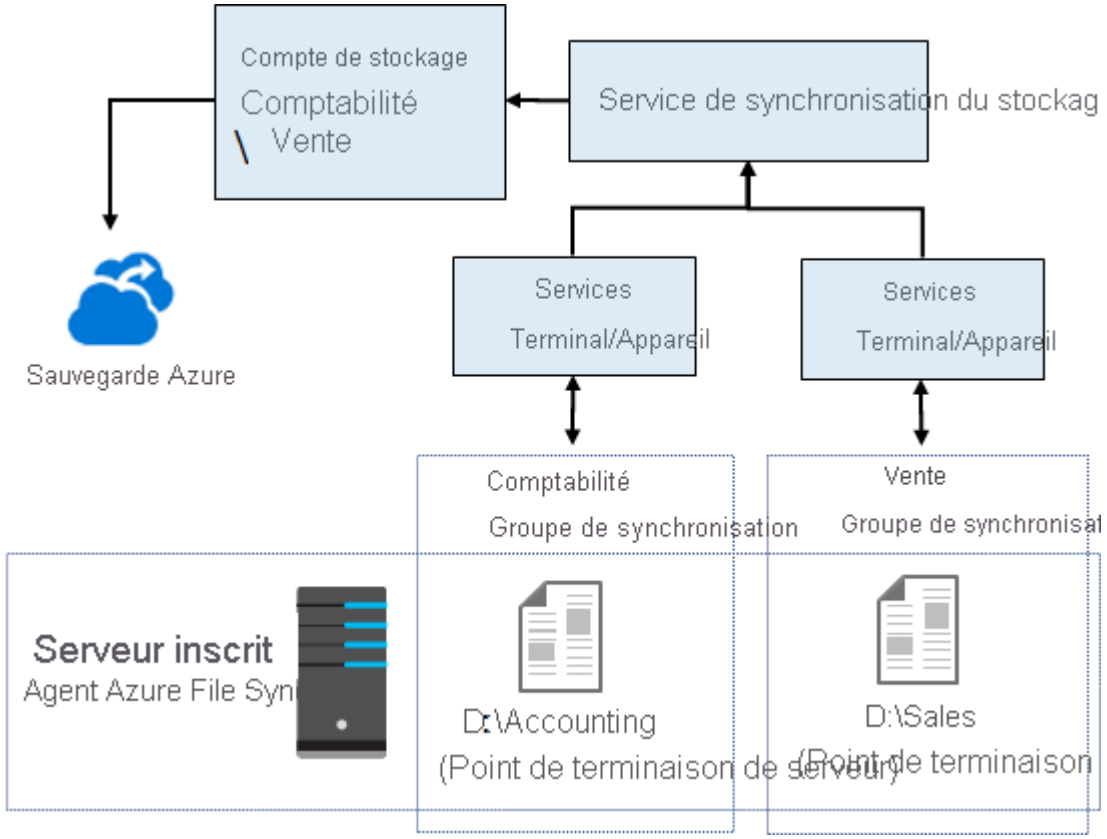
Azure File Sync vous permet de mettre en cache plusieurs partages Azure Files sur un Windows Server local ou sur une machine virtuelle cloud. Vous pouvez utiliser Azure File Sync pour centraliser les partages de fichiers de votre organisation dans Azure Files tout en conservant la flexibilité, le niveau de performance et la compatibilité d'un serveur de fichiers local.

- Azure File Sync transforme votre Windows Server en un cache rapide de vos partages Azure Files.
- Vous pouvez utiliser tout protocole disponible dans Windows Server pour accéder à vos données localement avec Azure File Sync, notamment SMB, NFS et FTPS.
- Azure File Sync prend en charge autant de caches que nécessaire dans le monde entier.

Hiérarchisation cloud

- Quand un fichier est hiérarchisé, Azure File Sync remplace le fichier localement par un pointeur. Un pointeur est communément appelé *point d'analyse*. Le point d'analyse représente une URL vers le fichier dans Azure Files.
- Lorsqu'un utilisateur ouvre un fichier hiérarchisé, Azure File Sync rappelle les données du fichier à partir d'Azure Files avec fluidité, sans que l'utilisateur ait besoin de savoir que le fichier est stocké dans Azure.

- Les fichiers de hiérarchisation cloud ont des icônes grisées avec un attribut de fichier 0 hors connexion pour permettre à l'utilisateur de savoir que le fichier est uniquement dans Azure.



Service de synchronisation du stockage

Le service de synchronisation de stockage est la ressource Azure de premier niveau pour Azure File Sync. Cette ressource est équivalente à la ressource de compte de stockage et peut être déployée de manière similaire.

- Le service de synchronisation de stockage crée les relations de synchronisation entre plusieurs comptes de stockage au moyen de différents groupes de synchronisation.
- Le service nécessite une ressource de premier niveau distincte de la ressource de compte de stockage pour prendre en charge les relations de synchronisation.
- Un abonnement peut avoir plusieurs ressources de service de synchronisation de stockage déployées.

Groupe de synchronisation

Un groupe de synchronisation définit la topologie de synchronisation d'un ensemble de fichiers. Les points de terminaison dans un groupe de synchronisation sont synchronisés entre eux. Considérons ce scénario : vous voulez gérer deux

ensembles distincts de fichiers avec Azure File Sync et, dans ce but, vous créez deux groupes de synchronisation et vous ajoutez des points de terminaison différents dans chacun de ces groupes. Une instance du service de synchronisation de stockage peut héberger autant de groupes de synchronisation que nécessaire.

Serveur inscrit

L'objet serveur inscrit représente une relation d'approbation entre votre serveur (ou cluster) et la ressource du service de synchronisation de stockage. Vous pouvez inscrire autant de serveurs que vous souhaitez auprès d'une ressource du service de synchronisation de stockage.

Agent Azure File Sync

L'agent Azure File Sync est un package téléchargeable qui permet à Windows Server de rester synchronisé avec un partage Azure Files. L'agent Azure File Sync a trois composants principaux :

- **FileSyncSvc.exe** : ce fichier est le service Windows en arrière-plan qui gère le monitoring des changements sur les points de terminaison de serveur, ainsi que le démarrage des sessions de synchronisation dans Azure.

- **StorageSync.sys** : ce fichier est le filtre du système de fichiers Azure File Sync qui prend en charge la hiérarchisation cloud. Le filtre gère la hiérarchisation des fichiers dans Azure Files quand la hiérarchisation cloud est activée.

- **Applets de commande PowerShell** : ces applets de commande de gestion PowerShell vous permettent d'interagir avec le fournisseur de ressources Azure `Microsoft.StorageSync`. Ces applets de commande se trouvent aux emplacements (par défaut) suivants :

    - `C:\\Program Files\\Azure\\StorageSyncAgent\\StorageSync.Management.PowerShell.Cmdlets.dll`
    - `C:\\Program Files\\Azure\\StorageSyncAgent\\StorageSync.Management.ServerCmdlets.dll`

Point de terminaison de serveur

Un point de terminaison de serveur représente un emplacement spécifique sur un serveur inscrit, comme un dossier sur un volume de serveur. Plusieurs points de

terminaison de serveur peuvent coexister sur le même volume si leurs espaces de noms sont uniques (par exemple, `F:\\sync1` et `F:\\sync2`).

Point de terminaison cloud

Un point de terminaison cloud est un partage Azure Files qui fait partie d'un groupe de synchronisation. En tant que membre d'un groupe de synchronisation, le point de terminaison cloud entier (partage Azure Files) est synchronisé.

- Un partage Azure Files ne peut être membre que d'un seul point de terminaison cloud.
- Un partage de fichiers Azure ne peut être membre que d'un seul groupe de synchronisation.
- Considérez le scénario où vous avez un partage contenant déjà des fichiers. Si vous ajoutez le partage comme point de terminaison cloud à un groupe de synchronisation, les fichiers dans le partage sont fusionnés avec les fichiers sur les autres points de terminaison dans le groupe de synchronisation.

Utiliser l'Explorateur Stockage Azure

L'Explorateur Stockage Azure est une application autonome qui vous permet d'utiliser facilement les données Stockage Azure sur Windows, macOS et Linux. Avec l'Explorateur Stockage Azure, vous pouvez accéder à plusieurs comptes et abonnements et gérer l'ensemble de votre contenu de stockage.

Points à connaître sur l'Explorateur Stockage Azure

- Explorateur Stockage Azure nécessite des autorisations de gestion (Azure Resource Manager) et de couche de données pour autoriser l'accès complet à vos ressources. Vous devez disposer d'autorisations Azure Active Directory (Azure AD) pour avoir accès à votre compte de stockage, aux conteneurs du compte et aux données dans les conteneurs.
- Explorateur Stockage Azure vous permet de vous connecter à différents comptes de stockage.
    - Vous connecter à des comptes de stockage associés à vos abonnements Azure.
    - Vous connecter à des comptes de stockage et à des services partagés à partir d'autres abonnements Azure.
    - Vous connecter au stockage local et le gérer à l'aide de l'émulateur de stockage Azure.

Attachement à un compte de stockage externe

Pour créer la connexion, vous avez besoin du **Nom du compte** et de la **Clé du compte** du stockage externe. Dans le portail Azure, la clé du compte est appelée **key1**.

Pour utiliser un nom de compte de stockage et une clé d'un cloud Azure national, utilisez le menu déroulant **Domaine des points de terminaison de stockage** pour sélectionner **Autre**, puis entrez le domaine de point de terminaison du compte de stockage personnalisé.

Clés d'accès

Les clés d'accès fournissent un accès à l'ensemble du compte de stockage. Deux clés d'accès vous sont fournies pour vous permettre de maintenir les connexions avec une clé, pendant que vous régénérez l'autre.

Quand vous régénérez vos clés d'accès, vous devez mettre à jour les ressources et applications Azure qui accèdent à ce compte de stockage pour que celles-ci utilisent les nouvelles clés. Cette action n'interrompt pas l'accès aux disques à partir de vos machines virtuelles.

Utiliser le service Azure Import/Export

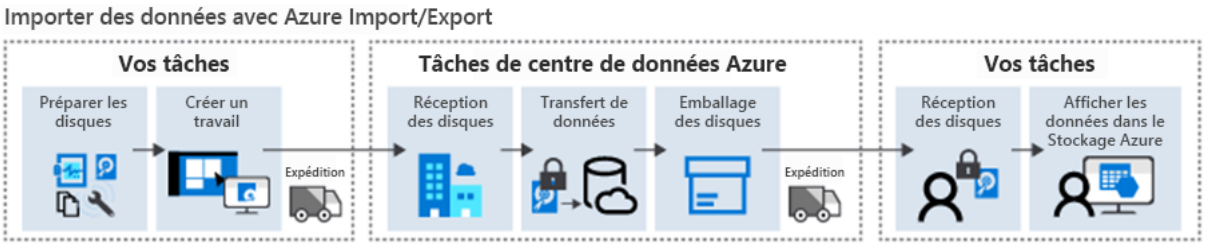
Le service Azure Import/Export est utilisé pour importer de manière sécurisée des volumes importants de données dans Stockage Blob Azure et Azure Files en expédiant des lecteurs de disque vers un centre de données Azure. Vous pouvez également utiliser ce service pour transférer des données de Stockage Blob Azure vers des lecteurs de disque et les expédier vers vos sites locaux.

Éléments à savoir sur le service Azure Import/Export

- Les données de vos lecteurs de disque peuvent être importées dans Stockage Blob Azure ou Azure Files dans votre compte de stockage Azure.
- Les données de Stockage Azure dans votre compte de stockage Azure peuvent être exportées vers des lecteurs que vous fournissez.
- Créez un travail Azure Import pour importer des données à partir de disques physiques dans Stockage Blob Azure ou Azure Files.
- Créez un travail Azure Export pour exporter des données de Stockage Azure vers des disques durs.
- Vous pouvez créer des travaux directement du portail Azure ou programmatiquement avec l'API REST Azure Import/Export.

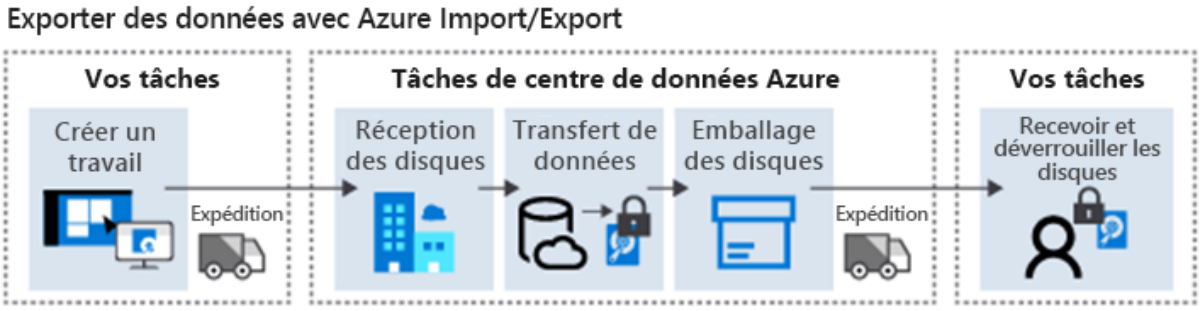
Travaux Azure Import

Les travaux Azure Import transfèrent en toute sécurité de grandes quantités de données vers Stockage Blob Azure (objets blob de blocs ou objets blob de pages) ou Azure Files. Vous expédiez des lecteurs de disque à un centre de données Azure, le personnel copie les données spécifiées dans le stockage Azure, puis vous les retourne.



Travaux Azure Export

Les travaux Azure Export transfèrent les données depuis le Stockage Azure vers des lecteurs de disques durs et les expédient à vos sites locaux.



Utiliser l'outil WAImportExport

WAImportExport est l'outil du service Azure Import/Export. L'outil est utilisé pour préparer les lecteurs avant d'importer des données et pour réparer les fichiers endommagés ou manquants après le transfert de données.

L'outil WAImportExport est disponible dans deux versions :

- La version 1 est idéale pour l'importation et l'exportation de données dans Stockage Blob Azure.
- La version 2 est idéale pour importer des données dans Azure Files.

L'outil WAImportExport est compatible uniquement avec le système d'exploitation Windows 64 bits. Pour obtenir la liste des versions et systèmes d'exploitation pris en charge, consultez Configuration requise pour Azure Import/Export.

Éléments à savoir sur l'outil WAImportExport

- Avant de créer une tâche Azure Import, utilisez l'outil WAImportExport pour copier des données sur les disques durs que vous envisagez d'expédier à Microsoft.
- Une fois votre travail Azure Import terminé, utilisez l'outil WAImportExport pour réparer les objets blob endommagés, manquants ou ayant des conflits avec d'autres objets blob dans votre stockage Azure.
- Après avoir reçu les disques durs d'un travail Azure Export terminé, utilisez l'outil WAImportExport pour réparer tout fichier corrompu ou manquant sur les disques.

- L’outil WAImportExport gère la copie des données, le chiffrement des volumes et la création de fichiers journaux. Les fichiers journaux sont nécessaires à la création d’un travail Azure Import/Export et permettent de garantir l’intégrité du transfert de données.

Utiliser l’outil AzCopy

L’outil **AzCopy** constitue une autre méthode de transfert de données. AzCopy v10 est l’utilitaire de ligne de commande nouvelle génération permettant de copier des données vers et depuis Stockage Blob Azure et Azure Files. AzCopy v10 offre une interface de ligne de commande (CLI) repensée et une nouvelle architecture pour des transferts de données fiables et performants. Avec AzCopy, vous pouvez copier des données entre un système de fichiers et un compte de stockage, ou entre comptes de stockage.

Ce que vous devez savoir sur AzCopy

- Chaque instance d'AzCopy crée un ordre de travail et un fichier journal associé. Vous pouvez afficher et redémarrer les travaux précédents et reprendre les travaux ayant échoué.
- Vous pouvez utiliser AzCopy pour répertorier ou supprimer des fichiers ou des objets blob dans un chemin d’accès donné. AzCopy prend en charge des modèles à caractères génériques dans un chemin, les indicateurs `--include` et les indicateurs `--exclude`.
- AzCopy retente automatiquement un transfert en cas de défaillance.
- Lorsque vous utilisez Stockage Blob Azure, AzCopy vous permet de copier l’intégralité d’un compte vers un autre compte. Aucun transfert de données vers le client n'est nécessaire
- AzCopy prend en charge les API Azure Data Lake Storage Gen2.
- AzCopy est intégré à l’Explorateur Stockage Azure.
- AzCopy est disponible sur Windows, Linux et macOS.

Options d’authentification

Authentification	Support	Description

Azure Active Directory (Azure AD)	Le Stockage Blob Azure et Azure Data Lake Storage Gen2	L'utilisateur entre la commande de connexion `.\\azcopy` pour se connecter à l'aide d'Azure AD. L'utilisateur doit disposer du rôle *Contributeur aux données Blob du stockage* pour écrire dans le Stockage Blob en utilisant l'authentification Azure AD. Lorsque l'utilisateur se connecte à partir d'Azure AD, il ne fournit ses informations d'identification qu'une seule fois. Cette option permet à l'utilisateur de contourner l'ajout d'un jeton SAP à chaque commande.
Jetons SAS	Stockage Blob Azure et Azure Files	Sur la ligne de commande, l'utilisateur ajoute un jeton SAS au chemin d'accès de l'objet blob ou du fichier pour chaque commande qu'il entre.

Type de compte

Le *type* de compte de stockage est un ensemble de stratégies qui déterminent les services de données que vous pouvez inclure dans le compte et le prix de ces services. Il existe quatre types de comptes de stockage :

- **Standard - StorageV2 (v2 universel)** : offre actuelle qui prend en charge tous les types de stockage et toutes les fonctionnalités les plus récentes
- **Premium - Objets blob de pages** : type de compte de stockage Premium pour les objets blob de pages uniquement
- **Premium - Objets blob de blocs** : type de compte de stockage Premium pour les objets blob de blocs et les objets blob d'ajout
- **Premium - Partages de fichiers** : type de compte de stockage Premium pour les partages de fichiers uniquement

Microsoft recommande d'utiliser l'option **Usage général v2** pour les nouveaux comptes de stockage.

Qu'est-ce que l'Explorateur Stockage ?

L'Explorateur Stockage est une application GUI que Microsoft a développée dans le but de faciliter l'accès aux données stockées dans des comptes de stockage Azure, ainsi que leur gestion. L'Explorateur Stockage est disponible sur Windows, macOS et Linux.

Voici quelques-uns des avantages de l'utilisation de l'Explorateur Stockage :

- Vous pouvez vous connecter rapidement à plusieurs comptes de stockage et les gérer facilement.
- L'interface vous permet de vous connecter à Data Lake Storage.
- Vous pouvez également utiliser l'interface pour mettre à jour et afficher les entités incluses dans vos comptes de stockage.
- Vous pouvez télécharger et utiliser gratuitement l'Explorateur Stockage.

Types de stockage Azure

L'Explorateur Stockage Azure peut accéder à de nombreux types de données différents issus de services comme les suivants :

- **Stockage Blob Azure**. Le stockage Blob s'utilise pour stocker des données non structurées sous forme d'objets blob.
- **Stockage Table Azure**. Le stockage Table s'utilise pour stocker des données semi-structurées/NoSQL.
- **Stockage File d'attente Azure**. Le stockage File d'attente sert à stocker les messages dans une file d'attente, qui sont ensuite accessibles et traités par les applications via des appels HTTP(S).
- **Azure Files**. Azure Files est un service de partage de fichiers qui permet un accès par le biais du protocole SMB (Server Message Block), de manière similaire aux serveurs de fichiers traditionnels.
- **Azure Data Lake Storage**. Azure Data Lake, basé sur Apache Hadoop, est conçu pour de gros volumes de données ; il peut stocker des données structurées et non structurées. Azure Data Lake Storage Gen1 est un service dédié. Azure Data Lake Storage Gen2 correspond à Stockage Blob Azure avec la fonctionnalité d'espace de noms hiérarchique activée sur le compte.

Gérer plusieurs comptes de stockage dans différents abonnements

Si vous avez plusieurs comptes de stockage associés à des abonnements différents dans votre locataire Azure, leur gestion avec le portail Azure peut s'avérer chronophage. Avec l'Explorateur Stockage, vous pouvez gérer plus facilement les données qui sont stockées dans plusieurs comptes de stockage Azure et abonnements Azure.

Types de connexion

Il existe de nombreuses façons de connecter une instance de l'Explorateur Stockage Azure à vos ressources Azure. Par exemple :

- Ajouter des ressources à l'aide d'Azure Active Directory (Azure AD)
- Utiliser une chaîne de connexion
- Utiliser un URI de signature d'accès partagé
- Utiliser un nom et une clé

- Attacher un émulateur local
- Attacher une ressource Azure Data Lake Storage au moyen d'un URI

Déployer et gérer les ressources de calcul Azure

Configurer des machines virtuelles

Ce qu'il faut savoir sur la configuration des machines virtuelles

Passons en revue une check-list des éléments à prendre en compte lors de la configuration d'une machine virtuelle.

- **Commencez par le réseau** : la configuration réseau peut passer par des réseaux virtuels pour permettre une connexion privée entre les machines virtuelles Azure et les autres services Azure. Le réseau peut être configuré pour autoriser l'accès aux services externes.
- **Choisissez un nom pour la machine virtuelle** :
    - le nom de la machine sert de nom d'ordinateur dans l'OS
    - longueur **max Windows est de 16 caractères** et **64 pour Linux**
    - définir une convention de nommage qui peut être une combinaison de ces données (Environnement ou usage, Lieu, numéro d'instance, produit ou service, rôle) ***devusc-webvm01***
- **Décidez de l'emplacement de la machine virtuelle** : tenir compte des facteurs de conformité ou fiscales, des configurations et capacités disponibles, du prix et de la distance avec les utilisateurs cibles
- **Déterminez la taille de la machine virtuelle** : tenir compte de la charge de travail que la machine virtuelle doit exécuter
- **Passez en revue le modèle de tarification et estimez vos coûts** :
    - Les coûts de ***calcul*** : sur une base horaire pour le nombre de minutes d'utilisation avec un mode de *paiement à la consommation* ou des *Instances machines virtuelle réservée (avec une réduction et un engagement)*
    - *Les coûts de* ***stockage*** : les frais de stockage sont indépendants de l'utilisation ou non de la machine virtuelle
- **Identifiez le stockage Azure à utiliser avec la machine virtuelle** : Azure gère en arrière plan la création et la gestion des comptes de stockage des des disques managés. Vous spécifiez la taille de disque et le niveau de performance (Standard ou Premium).
- **Sélectionnez un système d'exploitation de la machine virtuelle** : Azure intègre le coût de licence du système d'exploitation dans le prix. Il existe sur la place de marché Azure des images d'OS avec des logiciels préinstallés. Vous pouvez créer votre propre image d'OS (uniquement les systèmes d'exploitation 64 bits) et la stocker dans le Stockage Azure.

Déterminer le dimensionnement des machines virtuelles

Le dimensionnement d'une machine virtuelle dépend de sa charge de travail. Azure fournit des tailles de machines virtuelles qui proposent des variations de configurations (la puissance de traitement, la mémoire et la capacité de stockage).

- **Usage général** :
    - Tests et développement
    - Bases de données de taille petite à moyenne
    - Serveurs web ayant un trafic faible à moyen
- **Optimisé pour le calcul** :
    - Serveurs web ayant un trafic moyen
    - Appliances réseau
    - Processus de traitement par lots
    - Serveurs d'applications
- **Mémoire optimisée :**
    - Serveurs de base de données relationnelle
    - Caches de taille moyenne à grande
    - Analytique en mémoire
- **Optimisé pour le stockage** :
    - Big Data
    - Bases de données SQL et NoSQL
    - Entreposage des données
    - Bases de données transactionnelles volumineuses
- **GPU** :
    - Entraînement des modèles
    - Inférence avec Deep Learning
- **Calcul haute performance** :
    - Charges de travail qui nécessitent un haut niveau de performance
    - Réseaux à fort trafic

Azure fournit la possibilité de redimensionner la taille d'une machine virtuelle si la configuration actuelle l'autorise.

Déterminer le stockage des machines virtuelles

Toutes les machines virtuelles comportent au moins deux disques : **un disque d'OS et un disque temporaire et peuvent comporter des disques de données.** Les disques sont stockés en temps que disques durs virtuels (VHD).

- **Disque de système d'exploitation** : est préinstallé sur le disque du système d'exploitation sélectionné à la création de la VM. Il est inscrit en tant que lecteur SATA et étiqueté comme lecteur C: par défaut.
- **Disque temporaire** : les données sur ce disque peuvent être perdues lors d'une maintenance ou d'un redéploiement. Elles ne doivent donc pas être des données critiques. Ce disque est étiqueté comme :

    - sur Windows lecteur *D:* par défaut et est utilisé pour **stocker le fichier pagefile.sys**
    - sur Linux */dev/sdb* et est formaté et monté sur /mnt par **l'agent Linux Azure**
- **Disques de données** : sert à stocker des données d'application ou des données à conserver. Ils sont inscrits en tant que **disques SCSI** et étiquetés avec la lettre de notre choix. La taille de la VM détermine le nombre de disques de données que vous pouvez attacher et le type de stockage que vous pouvez utiliser pour héberger les disques de données.

Se connecter aux machines virtuelles

La connexion vers des VM peut être faite avec Azure Bastion avec les protocoles SSH et RDP, à Cloud Shell.

Ce qu'il faut savoir sur la connexion de machines virtuelles Windows

- Utilisez l'application Bureau à distance Microsoft avec le protocole RDP
- Établit une session d'interface utilisateur graphique avec une VM Azure
- Requiert l'adresse IP de la VM
- En option le port à utiliser
- Un fichier RDP téléchargeable à utiliser pour la connexion est fourni par le système

Ce qu'il faut savoir sur la connexion de machines virtuelles Linux

- Utilise le protocole SSH

Azure Bastion fournit une connectivité RDP et SSH sécurisée à toutes les machines virtuelles du réseau virtuel dans lequel il est provisionné.
Azure Bastion vous permet de vous connecter à la machine virtuelle directement dans le portail Azure.

Planifier la maintenance et les temps d'arrêt

- Un événement de **maintenance matérielle non planifiée** se produit quand la plateforme Azure prédit que le matériel ou tout composant de plateforme associé à une machine physique est sur le point d'échouer. Azure utilise la technologie de Migration dynamique pour migrer vos machines virtuelles. La migration dynamique est une opération de conservation de machine virtuelle qui n'interrompt la machine virtuelle que pendant un court moment, mais ses performances peuvent être réduites avant ou après l'événement
- Un **temps d'arrêt inattendu** se produit lorsque le matériel ou l'infrastructure physique de votre machine virtuelle échoue de manière inattendue. Les temps d'arrêt inattendus comprennent les défaillances du réseau local, du disque local ou au niveau du rack. Lorsqu'une défaillance de ce type est

détectée, la plateforme Azure migre automatiquement (répare) votre machine virtuelle vers une machine physique saine dans le même centre de données. Lors de la procédure de réparation, les machines virtuelles subissent des temps d'arrêt (redémarrage) et, dans certains cas, une perte du lecteur temporaire.
- Les événements de **maintenance planifiée** sont des mises à jour périodiques effectuées par Microsoft sur la plateforme sous-jacente Azure en vue d'améliorer la fiabilité, les performances et la sécurité de l'infrastructure hébergeant vos machines virtuelles. La plupart de ces mises à jour se déroulent sans aucune incidence sur vos machines virtuelles ou services cloud.

Créer des groupes à haute disponibilité

Un groupe à haute disponibilité est une fonctionnalité logique que vous pouvez utiliser pour vous assurer qu'un groupe de machines virtuelles associées sont déployées ensemble. Le regroupement permet d'éviter qu'un point de défaillance unique n'affecte toutes vos machines. Le regroupement garantit que toutes les machines ne sont pas mises à niveau en même temps lors d'une mise à niveau du système d'exploitation hôte dans le centre de données.

Ce qu'il faut savoir sur les groupes à haute disponibilité

- Toutes les machines virtuelles d'un groupe à haute disponibilité doivent exécuter le même ensemble de fonctionnalités.
- Les mêmes logiciels doivent être installés sur toutes les machines virtuelles d'un groupe à haute disponibilité.
- Azure veille à ce que les machines virtuelles d'un groupe à haute disponibilité s'exécutent sur plusieurs serveurs physiques, racks de calcul, unités de stockage et commutateurs réseau.
  En cas de défaillance matérielle ou logicielle Azure, seul un sous-ensemble des machines virtuelles du groupe à haute disponibilité est affecté. Votre application reste opérationnelle et accessible à vos clients.
- Vous pouvez créer une machine virtuelle et un groupe à haute disponibilité en même temps.
  Une machine virtuelle ne peut être ajoutée à un groupe à haute disponibilité qu'au moment de la création de la machine virtuelle. Pour changer le groupe à haute disponibilité d'une machine virtuelle, vous devez supprimer la machine virtuelle et la recréer.
- Vous pouvez créer des groupes à haute disponibilité en utilisant le portail Azure, des modèles ARM (Azure Resource Manager), des scripts ou des outils d'API.

- Microsoft fournit des contrats de niveau de service (SLA) robustes pour les machines virtuelles Azure et les groupes à haute disponibilité. Pour plus d'informations, consultez Contrat SLA pour Machines Virtuelles Azure.

Passer en revue les domaines de mise à jour et les domaines d'erreur

Azure Virtual Machine Scale Sets implémente deux concepts de nœud pour aider Azure à maintenir la haute disponibilité et la tolérance de panne lors du déploiement et de la mise à niveau d'applications : les *domaines de mise à jour* et les *domaines d'erreur*. Chaque machine virtuelle dans un groupe à haute disponibilité est placée dans un domaine de mise à jour et un domaine d'erreur.

Éléments à savoir sur les domaines de mise à jour

Un domaine de mise à jour est un groupe de nœuds qui sont mis à niveau ensemble durant le processus de mise à niveau d'un service (ou *lancement*). Un domaine de mise à jour permet à Azure d'effectuer des mises à niveau incrémentielles ou propagées dans le cadre d'un déploiement. Voici quelques autres caractéristiques des domaines de mise à jour.

- Chaque domaine de mise à jour contient un groupe de machines virtuelles et le matériel physique associé que vous pouvez mettre à jour et redémarrer en même temps.
- Pendant une maintenance planifiée, un seul domaine de mise à jour est redémarré à la fois.
- Par défaut, il existe cinq domaines de mise à jour (non configurables par l'utilisateur).
- Vous pouvez configurer jusqu'à 20 domaines de mise à jour.

Éléments à savoir sur les domaines d'erreur

Un domaine d'erreur est un groupe de nœuds représentant une unité physique de défaillance. Vous pouvez considérer un domaine d'erreur comme étant un ensemble de nœuds qui appartiennent au même rack physique.

- Un domaine d'erreur définit un groupe de machines virtuelles qui partagent un ensemble commun de composants matériels (ou *commutateurs*) et un point de défaillance unique. Par exemple, il peut s'agir d'un rack de serveurs desservi par un ensemble de commutateurs d'alimentation ou réseau.
- Deux domaines d'erreur collaborent afin d'atténuer les défaillances matérielles, les pannes de réseau, les coupures de courant ou les mises à jour logicielles.

Passer en revue les zones de disponibilité

Les zones de disponibilité constituent une offre à haute disponibilité qui protège vos applications et données des pannes des centres de données. Une zone de disponibilité dans une région Azure est une combinaison d'un domaine d'erreur et d'un domaine de mise à jour.

Ce qu'il faut savoir sur les zones de disponibilité

- Les Zones de disponibilité sont des emplacements physiques uniques au sein d'une région Azure.
- Chaque zone est composée d'un ou de plusieurs centres de données qui sont équipés d'une alimentation, d'un système de refroidissement et d'un réseau indépendant.
- Pour garantir la résilience, un minimum de trois zones distinctes sont activées dans toutes les régions.
- La séparation physique des zones de disponibilité dans une région protège les applications et les données des défaillances dans le centre de données. Des services redondants interzone répliquent vos applications et données dans des zones de disponibilité afin de vous protéger contre les points de défaillance uniques.

Comparer la mise à l'échelle verticale et horizontale

Une configuration de machine virtuelle robuste inclut la prise en charge de la scalabilité. La scalabilité autorise un débit pour une machine virtuelle proportionnel à la disponibilité des ressources matérielles associées. Une machine virtuelle scalable peut gérer les augmentations de requêtes sans affecter le temps de réponse et le débit. Pour la plupart des opérations de mise à l'échelle, il existe deux options d'implémentation : *verticale* et *horizontale*.

Informations à connaître sur la mise à l'échelle verticale

La mise à l'échelle verticale, également désignée par les termes ***scale-up et scale-down*, nécessite d'augmenter ou de diminuer la taille des machines virtuelles en réponse à une charge de travail**. La mise à l'échelle verticale rend une machine virtuelle plus (scale-up) ou moins (scale-down) puissante.

Informations à connaître sur la mise à l'échelle horizontale

La mise à l'échelle horizontale, également appelée ***scale-out et scale-in*, est utilisée pour ajuster le nombre de machines virtuelles dans votre configuration afin de prendre en charge l'évolution de la charge de travail**. Lorsque vous implémentez la mise à l'échelle horizontale, le nombre d'instances de machine virtuelle augmente (scale-out) ou diminue (scale-in).

Implémenter Azure Virtual Machine Scale Sets

Les groupes de machines virtuelles identiques Azure sont une ressource de calcul Azure qui vous permet de déployer et de gérer un groupe de machines virtuelles **identiques**.

Virtual Machine Scale Sets augmente automatiquement le nombre d'instances de vos machines virtuelles à mesure que la demande d'application augmente, et réduit le nombre d'instances de machines à mesure que la demande diminue.

Ce qu'il faut savoir sur Azure Virtual Machine Scale Sets

- Toutes les instances de machines virtuelles sont créées à partir de la même configuration et de la même image de système d'exploitation de base. Cette approche vous permet de gérer facilement des centaines de machines virtuelles sans tâches de configuration ou de gestion de réseau supplémentaires.
- Virtual Machine Scale Sets prend en charge l'utilisation d'Azure Load Balancer pour la distribution élémentaire du trafic de couche 4, et d'Azure Application Gateway pour l'arrêt SSL et la distribution plus avancée du trafic de couche 7.
- Vous pouvez utiliser Virtual Machine Scale Sets pour exécuter plusieurs instances de votre application. Si l'une des instances de machines virtuelles rencontre un problème, les clients continuent d'accéder à votre application via une autre instance de machine virtuelle avec une interruption minimale.
- La demande des clients pour votre application peut changer pendant la journée ou la semaine. Pour répondre à la demande des clients, Virtual Machine Scale Sets implémente la mise à l'échelle automatique afin d'augmenter et de diminuer automatiquement le nombre de machines virtuelles.
- Virtual Machine Scale Sets prend en charge jusqu'à 1000 instances de machines virtuelles. Si vous créez et chargez vos propres images de machines virtuelles, la limite est de 600 instances de machines virtuelles.

Créer des groupes de machines virtuelles identiques

- **Mode d'orchestration** : choisissez la façon dont les machines virtuelles sont gérées par le groupe identique. **En mode d'orchestration flexible, vous créez et ajoutez manuellement une machine virtuelle de n'importe quelle configuration au groupe identique**. En **mode d'orchestration uniforme, vous définissez un modèle de machine virtuelle, et Azure va générer des instances identiques basées sur ce modèle**.
- **Image** : choisissez le système d'exploitation ou l'application de base pour la machine virtuelle.

- **Architecture de machine virtuelle** : Azure offre un choix de machines virtuelles x64 ou Arm64 pour exécuter vos applications.
- **Exécuter avec une remise Azure Spot** : Azure Spot offre une capacité Azure inutilisée à un tarif réduit par rapport au prix du paiement à l'utilisation. Les charges de travail doivent être tolérantes aux pertes d'infrastructure, car Azure peut récupérer la capacité.
- **Taille** : sélectionnez une taille VM adaptée à la charge de travail que vous voulez exécuter. La taille que vous choisissez détermine ensuite des facteurs comme la puissance de traitement, la mémoire et la capacité de stockage. Azure propose différentes tailles vous permettant de prendre en charge de nombreux types d'utilisation. Azure facture un prix horaire basé sur la taille et le système d'exploitation de la machine virtuelle.

Sous l'onglet **Avancé**, vous pouvez également sélectionner les éléments suivants :

- **Activer une mise à l'échelle de plus de 100 instances** : identifiez votre préférence d'allocation de mise à l'échelle. Si vous sélectionnez **Non**, **votre implémentation de Virtual Machine Scale Sets est limitée à un seul groupe de placement d'une capacité maximale de 100**. Si vous sélectionnez **Oui**, v**otre implémentation peut s'étendre sur plusieurs groupes de placement d'une capacité allant jusqu'à 100**. La sélection de **Oui** modifie également les caractéristiques de disponibilité de votre implémentation.
- **Algorithme de diffusion** : Microsoft recommande d'allouer la **Diffusion maximale** pour votre implémentation. Cette approche procure une diffusion optimale.

Implémenter la mise à l'échelle automatique

La *mise à l'échelle automatique* est le processus qui permet d'augmenter ou diminuer automatiquement le nombre d'instances de machines virtuelles qui exécutent votre application.

Configurer la mise à l'échelle automatique

Lorsque vous créez une implémentation d'Azure Virtual Machine Scale Sets dans le portail Azure, vous pouvez activer la mise à l'échelle automatique. Pour des performances optimales, **vous devez définir un nombre minimal, maximal et par défaut d'instances de machines virtuelles à utiliser pendant le processus de mise à l'échelle automatique**.
Stratégie de mise à l'échelle : la mise à l'échelle manuelle conserve un nombre d'instances fixe. La mise à l'échelle automatique personnalisée met à l'échelle la capacité selon n'importe quelle planification, en fonction de n'importe quelle métrique.

Scale-out

- **Seuil du processeur** : spécifiez le seuil de pourcentage d'utilisation du processeur auquel déclencher la règle d'augmentation automatique du nombre d'instances.
- **Durée en minutes** : la durée en minutes est la période de temps prise en compte par le moteur de mise à l'échelle automatique pour l'examen des métriques. Par exemple, 10 minutes signifie qu'à chaque exécution d'une mise à l'échelle automatique, il va interroger les métriques sur les 10 dernières minutes. Ce délai permet à vos métriques de se stabiliser et évite de réagir à des pics temporaires.
- **Nombre de machines virtuelles à augmenter de** : spécifiez le nombre de machines virtuelles à ajouter à votre implémentation de Virtual Machine Scale Sets lorsque la règle d'augmentation automatique du nombre d'instances est déclenchée.

Scale-in

- **Seuil du processeur pour le scale-in** : spécifiez le seuil de pourcentage d'utilisation du processeur auquel déclencher la règle de diminution automatique du nombre d'instances.
- **Nombre de machines virtuelles à diminuer de** : spécifiez le nombre de machines virtuelles à retirer de votre implémentation lorsque la règle de diminution automatique du nombre d'instances est déclenchée.

Stratégie de scale-in : la fonctionnalité de stratégie de scale-in offre aux utilisateurs un moyen de configurer l'ordre dans lequel les machines virtuelles font l'objet du scale-in.

Configurer des extensions de machine virtuelle

Implémenter des extensions de machine virtuelle

Les extensions de machine virtuelle Azure sont de petites applications permettant d'exécuter des tâches de configuration et d'automatisation post-déploiement pour Machines Virtuelles Azure. Les extensions concernent la gestion de vos machines virtuelles.

Ce qu'il faut savoir sur les extensions de machine virtuelle

- Vous pouvez gérer les extensions de machine virtuelle avec Azure CLI, PowerShell, des modèles ARM (Azure Resource Manager) et le portail Azure.

- Les extensions de machine virtuelle peuvent être associées à un nouveau déploiement de machine virtuelle ou s'exécuter sur tout système existant.

- Il existe différentes extensions de machine virtuelle pour les machines Windows et Linux. Vous pouvez choisir parmi un large éventail d'extensions de machine virtuelle internes et tierces.

Implémenter des extensions de script personnalisé

Les extensions de script personnalisé peuvent être **utilisées pour lancer et exécuter automatiquement des tâches de personnalisation de machine virtuelle après la configuration initiale de la machine**. Votre extension de script peut effectuer des tâches simples, **telles que l'arrêt de la machine virtuelle ou l'installation d'un composant logiciel**. Les scripts peuvent également être plus complexes et effectuer une série de tâches.

Ce qu'il faut savoir sur les extensions de script personnalisé

- Vous pouvez installer des extensions de script personnalisé à partir du portail Azure en accédant à la page **Extensions** de votre machine virtuelle.

- Une fois la ressource Extensions de script personnalisé créée pour votre machine virtuelle, vous fournissez un fichier de script PowerShell avec les commandes à exécuter sur la machine. Vous pouvez également spécifier des arguments facultatifs, en fonction des besoins de votre scénario. Une fois votre fichier PowerShell chargé, votre script est exécuté immédiatement.

- Les scripts peuvent être téléchargés à partir de Stockage Azure ou de GitHub, ou fournis dans le portail Azure lors de l'exécution de l'extension.
- Vous pouvez également utiliser la commande PowerShell `Set-AzVmCustomScriptExtension` pour exécuter des scripts avec Extensions de script personnalisé. Cette commande nécessite l'URI du script dans le conteneur d'objets blob.

```
Set-AzVmCustomScriptExtension -FileUri
https://scriptstore.blob.core.windows.net/scripts/Install_IIS.ps1 -Run
"PowerShell.exe" -VmName vmName -ResourceGroupName resourceGroup
-Location "location"
```

- Gardez à l'esprit que l'exécution des extensions de script personnalisé ont seulement 90 minutes pour s'exécuter

Implémenter Desired State Configuration

Desired State Configuration est une **plateforme de gestion de Windows PowerShell**. Desired State Configuration **permet de déployer et de gérer les données de configuration de services logiciels, et de gérer l'environnement**

dans lequel ces services s'exécutent. La plateforme vous permet également de tenir à jour et de gérer des configurations existantes.

Éléments à savoir sur la création de votre configuration d'état souhaité

- Vous pouvez utiliser Desired State Configuration lorsque les extensions de script personnalisé ne répondent pas aux exigences de l'application pour votre machine virtuelle.
- Desired State Configuration est axé sur la création de *configurations* spécifiques à l'aide de scripts.
- Une configuration est un script facile à lire qui décrit un environnement d'ordinateurs (ou nœuds) ayant des caractéristiques spécifiques. Ces caractéristiques peuvent être aussi simples que de vérifier qu'une fonctionnalité spécifique de Windows est activée, et aussi complexes que de déployer SharePoint.
- Le script de configuration se compose d'un bloc de configuration, d'un bloc de nœud et d'un ou plusieurs blocs de ressources.
    - le bloc de configuration est le bloc de script le plus à l'extérieur. Vous définissez le bloc avec le mot clé `Configuration` et fournissez un nom.
    - Les blocs de nœuds définissent les ordinateurs ou machines virtuelles que vous configurez. Vous définissez un nœud avec le mot clé `Node` et fournissez un nom pour la ressource.
    - Les blocs de ressources configurent les propriétés des ressources (ordinateurs ou machines virtuelles). Vous fournissez le nom du rôle ou de la fonctionnalité Windows dont vous voulez garantir l'ajout ou la suppression. Le mot clé `Ensure` est utilisé pour indiquer si le rôle ou la fonctionnalité est ajouté.
- Desired State Configuration fournit un ensemble d'extensions de langage Windows PowerShell, d'applets de commande Windows PowerShell et de ressources. Vous pouvez utiliser ces fonctionnalités pour spécifier de manière déclarative la façon dont vous souhaitez configurer votre environnement logiciel.
- La configuration d'état souhaité Windows PowerShell est fournie avec un ensemble de ressources de configuration intégrées, telles que `File Resource`, `Log Resource` et `User Resource`.

```
configuration IISInstall

{

   Node "localhost"

   {
```

```
        WindowsFeature IIS
        {
            Ensure = "Present"
            Name = "Web-Server"
        }
    }
}
```

Configurer des plans Azure App Service

Implémenter des plans Azure App Service

Dans Azure App Service, une application s'exécute dans un plan Azure App Service. Un plan App Service définit un ensemble de ressources de calcul nécessaires à l'exécution d'une application web. Les ressources de calcul sont analogues à une batterie de serveurs dans l'hébergement web classique. Une ou plusieurs applications peuvent être configurées pour s'exécuter sur les mêmes ressources informatiques (ou dans le même plan App Service).

Ce qu'il faut savoir sur les plans App Service

- Lorsque vous créez un plan App Service dans une région, un ensemble de ressources de calcul est créé pour le plan dans la région spécifiée. Toutes les applications que vous placez dans le plan s'exécutent sur les ressources de calcul définies par le plan.

- Chaque plan App Service définit trois paramètres :

    - **Région** : région pour le plan App Service, par exemple USA Ouest, Inde Centre, Europe Nord, etc.
    - **Nombre d'instances de machine virtuelle** : nombre d'instances de machine virtuelle à allouer pour le plan.
    - **Taille des instances de machine virtuelle** : taille des instances de machine virtuelle dans le plan (notamment Petite, Moyenne ou Grande).
- Vous pouvez continuer à ajouter de nouvelles applications à un plan existant tant que le plan a suffisamment de ressources pour gérer l'augmentation de charge.

Fonctionnement et mise à l'échelle des applications dans les plans App Service

Le plan Azure App Service est l'unité d'échelle des applications App Service. En fonction du niveau tarifaire de votre plan Azure App Service, vos applications s'exécutent et sont mises à l'échelle de manière différente. Si votre plan est configuré pour exécuter cinq instances de machine virtuelle, toutes les applications dans le plan s'exécutent sur les cinq instances. Si votre plan est configuré pour une mise à l'échelle automatique, toutes les applications dans le plan sont mises à l'échelle ensemble conformément aux paramètres de mise à l'échelle.

Voici un récapitulatif de l'exécution et de la mise à l'échelle des applications dans les niveaux tarifaires des plans Azure App Service :

- **Niveau Gratuit ou Partagé** :
    - les applications s'exécutent en recevant des minutes de processeur sur une instance de machine virtuelle partagée.
    - Les applications ne peuvent pas être soumises à un scale-out.
- **Niveau De base, Standard, Premium ou Isolé** :
    - Les applications s'exécutent sur toutes les instances de machine virtuelle configurées dans le plan App Service.
    - Plusieurs applications du même plan partagent les mêmes instances de machine virtuelle.
    - Si vous avez plusieurs emplacements de déploiement pour une application, tous les emplacements de déploiement s'exécutent sur les mêmes instances de machine virtuelle.
    - Si vous activez les journaux de diagnostic, effectuez des sauvegardes ou exécutez des tâches web, ces tâches utilisent des cycles de processeur et de la mémoire sur les mêmes instances de machine virtuelle.

Déterminer les tarifs d'un plan Azure App Service

Fonctionnalité	Gratuit	Partagé	De base	Standard	Premium	Isolé
Usage	Développement, Test	Développement, Test	Développement, Test dédié	Charges de travail de production	Scalabilité et performances améliorées	Haute performance, sécurité, isolation

Applications web, mobiles ou API	10	100	Illimité	Illimité	Illimité	Illimité
Espace disque	1 Go	1 Go	10 Go	50 Go	250 Go	1 To
Mise à l'échelle automatique	n/a	n/a	n/a	Prise en charge	Prise en charge	Pris en charge
Emplacements de déploiement	n/a	n/a	n/a	5	20	20
Nombre maximal d'instances	n/a	n/a	Jusqu'à 3	Jusqu'à 10	Jusqu'à 30	Jusqu'à 100

Isolé

Le plan de service Isolé est conçu pour exécuter des charges de travail critiques qui doivent s'exécuter dans un réseau virtuel. Le plan Isolé permet aux clients d'exécuter leurs applications dans un environnement privé dédié dans un centre de données Azure. L'environnement privé utilisé avec un plan Isolé est appelé App Service Environment.

Effectuer un scale-up et un scale-out d'un plan Azure App Service

Il existe deux méthodes pour mettre à l'échelle votre plan et vos applications Azure App Service : le *scale-up* et le *scale-out*. Vous pouvez mettre à l'échelle vos applications manuellement ou choisir une *mise à l'échelle automatique*.

Ce qu'il faut savoir sur la mise à l'échelle d'Azure App Service

- La méthode par scale-up augmente la capacité de processeur, de mémoire et d'espace disque. Le scale-up vous permet d'obtenir de nombreuses fonctionnalités supplémentaires, comme des machines virtuelles dédiées, des domaines et des certificats personnalisés, des emplacements de préproduction, la mise à l'échelle automatique, entre autres. Le scale-up

s’effectue en changeant le niveau tarifaire du plan Azure App Service dans lequel se trouve votre application.

- La méthode par scale-out augmente le nombre d’instances de machine virtuelle qui exécutent votre application. Vous pouvez effectuer le scale-out de 30 instances au maximum, selon le niveau tarifaire de votre plan App Service. Dans les environnements App Service de niveau Isolé, bénéficiez d’une capacité de scale-out supplémentaire pouvant aller jusqu’à 100 instances. Le nombre d’instances de mise à l’échelle peut être configuré manuellement ou automatiquement (mise à l’échelle automatique).
- Grâce à la mise à l’échelle automatique, vous pouvez augmenter automatiquement le nombre d’instances de mise à l’échelle pour la méthode par scale-out. La mise à l’échelle automatique est basée sur des règles et des planifications prédéfinies.
- Vous pouvez faire un scale-up et un scale-down de votre plan App Service à tout moment en changeant le niveau tarifaire du plan.

Configurer la mise à l’échelle automatique Azure App Service

Ce que vous devez savoir sur la mise à l’échelle automatique

- Pour utiliser la mise à l’échelle automatique, vous spécifiez le nombre minimal et maximal d’instances à exécuter à l’aide d’un ensemble de règles et de conditions.
- Lorsque votre application s’exécute dans des conditions de mise à l’échelle automatique, le nombre d’instances de machine virtuelle est ajusté automatiquement en fonction de vos règles. Lorsque les conditions relatives aux règles sont remplies, une ou plusieurs actions de mise à l’échelle automatique sont déclenchées.
- Un paramètre de mise à l’échelle automatique est lu par le moteur de mise à l’échelle automatique afin de déterminer s’il faut effectuer un scale-out ou un scale-in. Les paramètres de mise à l’échelle automatique sont regroupés en profils.
- Les règles de mise à l’échelle automatique comprennent un déclencheur et une action de mise à l’échelle (scale-in ou scale-out). Le déclencheur peut être basé sur des métriques ou sur l’heure.
    - Les règles **basées sur des métriques** mesurent la charge de l’application et ajoutent ou suppriment des machines virtuelles en fonction de la charge, par exemple « effectuer cette action lorsque l’utilisation du processeur est supérieure à 50 % ». Parmi les exemples de métriques, citons Temps processeur, Temps de réponse moyen et Requêtes.
    - Les règles **basées sur l’heure** (ou sur une planification) vous permettent d’effectuer une mise à l’échelle lorsque vous voyez des schémas horaires dans votre charge et que vous souhaitez effectuer la

mise à l'échelle avant qu'une augmentation ou diminution de charge possible ne se produise. Vous pourriez par exemple avoir comme règle : « déclencher un webhook chaque samedi à 8 heures dans un fuseau horaire donné. »

- Le moteur de mise à l'échelle automatique utilise des paramètres de notification.

  Un paramètre de notification définit quelles notifications doivent se produire lorsqu'un événement de mise à l'échelle automatique a lieu en fonction de la satisfaction des critères d'un profil de paramètre de mise à l'échelle automatique. La mise à l'échelle automatique peut notifier une ou plusieurs adresses e-mail ou appeler un ou plusieurs webhooks.

Configurer Azure App Service

Implémenter Azure App Service

Azure App Service réunit tout ce dont vous avez besoin pour créer des sites web, des back-ends mobiles et des API web pour n'importe quelle plateforme ou n'importe quel appareil. Les applications s'exécutent et se mettent à l'échelle facilement dans les environnements Windows et Linux.

Avantage	Description
Plusieurs langages et frameworks	App Service offre une prise en charge de première classe pour ASP.NET, Java, Ruby, Node.js, PHP et Python. Vous pouvez également exécuter PowerShell et d'autres scripts ou exécutables comme services en arrière-plan.
Optimisation DevOps	App Service prend en charge l'intégration et le déploiement continus avec Azure DevOps, GitHub, BitBucket, Docker Hub et Azure Container Registry. Vous pouvez promouvoir des mises à jour avec des environnements de test et de préproduction. Gérez vos applications dans App Service à l'aide d'Azure PowerShell ou de la CLI interplateforme.

Mise à l'échelle globale avec haute disponibilité	App Service vous permet d'effectuer un scale-up ou un scale-out manuellement ou automatiquement. Vous pouvez héberger vos applications n'importe où dans l'infrastructure mondiale des centres de données Microsoft, et bénéficier de la haute disponibilité offerte par le contrat SLA App Service.
Connexions aux plateformes SaaS et aux données locales	App Service vous permet de choisir parmi plus de 50 connecteurs pour des systèmes d'entreprise (comme SAP), des services SaaS (comme Salesforce) et des services Internet (comme Facebook). Vous pouvez accéder aux données locales en utilisant des connexions hybrides et des réseaux virtuels Azure.
Sécurité et conformité	App Service est conforme aux normes ISO, SOC et PCI. Vous pouvez authentifier les utilisateurs avec Azure Active Directory ou avec des connexions sociales via Google, Facebook, Twitter ou Microsoft. Créez des restrictions par adresse IP et gérez les identités de service.
Modèles d'application	Faites votre choix parmi une liste complète de modèles d'application dans la Place de marché Azure, tels que WordPress, Joomla et Drupal.
Intégration de Visual Studio	App Service offre des outils dédiés dans Visual Studio pour permettre de rationaliser le travail de création, de déploiement et de débogage.
Fonctionnalités API et mobiles	App Service offre une prise en charge CORS clé en main pour les scénarios d'API RESTful. Vous pouvez simplifier vos scénarios d'application mobile en activant l'authentification, la synchronisation des données hors connexion, les notifications Push, etc.
Code serverless	App Service vous permet d'exécuter un extrait de code ou un script à la demande sans avoir à provisionner ou gérer explicitement l'infrastructure. Vous payez uniquement pour le temps de calcul utilisé par votre code.

Paramètres post-création

Certains paramètres de configuration supplémentaires peuvent être ajoutés dans le code du développeur, tandis que d'autres peuvent être configurés dans votre application. Voici quelques paramètres d'application supplémentaires.

- **Always On** : vous pouvez garder l'application chargée même s'il n'y a pas de trafic. Ce paramètre est nécessaire pour les WebJobs continus ou pour les WebJobs déclenchés avec une expression CRON.
- **Affinité ARR** : dans un déploiement multi-instance, vous pouvez faire en sorte que le client soit routé vers la même instance pendant toute la session.
- **Chaînes de connexion** : les chaînes de connexion pour votre application sont chiffrées au repos et transmises sur un canal chiffré.

Explorer l'intégration et le déploiement continus

- Le **déploiement automatisé** (intégration continue) est un processus utilisé pour pousser de nouvelles fonctionnalités et des correctifs de bogues selon un modèle rapide et répétitif, avec un impact minimal sur les utilisateurs finaux. Azure prend en charge le déploiement automatisé directement à partir de plusieurs sources :
    - **Azure DevOps** : poussez votre code sur Azure DevOps (anciennement Visual Studio Team Services), générez votre code dans le cloud, exécutez des tests, générez une version à partir du code et, enfin, poussez votre code sur une application web Azure.
    - **GitHub** : Azure prend en charge le déploiement automatisé directement à partir de GitHub. Quand vous connectez votre dépôt GitHub à Azure pour le déploiement automatisé, les changements que vous poussez sur votre branche de production sur GitHub sont déployés automatiquement pour vous.
    - **Bitbucket** : de façon similaire à GitHub, vous pouvez configurer un déploiement automatisé avec Bitbucket.
- Le **déploiement manuel** vous permet de pousser manuellement votre code sur Azure. Il y a plusieurs options pour pousser manuellement votre code :
    - **Git** : la fonctionnalité App Service Web Apps propose une URL Git que vous pouvez ajouter comme dépôt distant. En poussant le code sur le dépôt distant, vous déployez votre application.
    - **Interface CLI** : la commande `webapp up` est une fonctionnalité de l'interface de ligne de commande qui package votre application et la déploie. Le déploiement peut inclure la création d'une nouvelle application web App Service.
    - **Visual Studio** : Visual Studio propose un Assistant de déploiement App Service qui peut vous guider tout au long du processus de déploiement.

- **FTP/S** : FTP ou FTPS est un moyen traditionnel d'envoyer (push) votre code à de nombreux environnements d'hébergement, notamment App Service.

Créer des emplacements de déploiement

Ce qu'il faut savoir sur les emplacements de déploiement

- Les emplacements de déploiement sont des applications en production qui ont leurs propres noms d'hôtes.
- Les emplacements de déploiement sont disponibles dans les niveaux tarifaires App Service Standard, Premium et Isolé. Votre application doit s'exécuter dans l'un de ces niveaux pour utiliser des emplacements de déploiement.
- Les niveaux Standard, Premium et Isolé offrent différents nombres d'emplacements de déploiement.
- Les éléments de contenu et de configuration des applications web peuvent être échangés entre deux emplacements de déploiement, y compris l'emplacement de production.

Ce qu'il faut savoir sur la création d'emplacements de déploiement

- Les nouveaux emplacements de déploiement peuvent être vides ou clonés.

- Les paramètres d'emplacement de déploiement sont divisés en trois catégories :

    - Les paramètres d'application et les chaînes de connexion propres à l'emplacement (si applicable)
    - Les paramètres de déploiement continu (si activé)
    - Les paramètres d'authentification App Service (si activée)
- Lorsque vous clonez une configuration depuis un autre emplacement de déploiement, la configuration clonée est modifiable. Certains éléments de configuration suivent le contenu pendant l'échange. D'autres éléments de configuration propres à l'emplacement restent dans l'emplacement source après l'échange.

Paramètres échangés et paramètres propres à l'emplacement

***** Le paramètre peut être configuré pour être propre à l'emplacement.

****** La fonctionnalité n'est actuellement pas disponible.

Paramètres échangés	Paramètres propres à l'emplacement

Paramètres généraux, par exemple versions du framework, 32/64 bits, sockets web	Noms de domaine personnalisés
Paramètres d'application *	Certificats non publics et paramètres TLS/SSL
Chaînes de connexion *	Paramètres de mise à l'échelle
Mappages de gestionnaires	Always On
Certificats publics	Restrictions d'adresse IP
Contenu WebJobs	Planificateurs WebJobs
Connexions hybrides **	Paramètres de diagnostic
Points de terminaison de service **	Partage des ressources cross-origin (CORS)
Azure Content Delivery Network **	Intégration du réseau virtuel
Mappage de chemin	Identités managées
	Paramètres se terminant par le suffixe _EXTENSION_VERSION

Ce qu'il faut savoir sur la sécurité des applications avec App Service

- Le module de sécurité d'authentification et d'autorisation dans Azure App Service s'exécute dans le même environnement que le code de votre application, mais séparément.
- Le module de sécurité est configuré en utilisant des paramètres d'application. Aucun Kit de développement logiciel (SDK), aucun langage spécifique ni aucune modification du code de l'application ne sont nécessaires.
- Quand vous activez le module de sécurité, chaque requête HTTP entrant passe par le module avant d'être gérée par le code de votre application.
- Le module de sécurité gère plusieurs tâches pour votre application :
    - Authentifier les utilisateurs avec le fournisseur spécifié
    - Valider, stocker et actualiser les jetons
    - Gérer la session authentifiée
    - Injecter les informations d'identité dans les en-têtes de demande

Ce qu'il faut savoir quand vous utilisez App Service pour la sécurité des applications

- **Autoriser les requêtes anonymes (aucune action)** : Confier l'autorisation du trafic non authentifié à votre code d'application. Dans le cas des demandes authentifiées, App Service transmet également les informations d'authentification dans les en-têtes HTTP. Cette fonctionnalité permet de traiter de manière plus souple les demandes anonymes. Avec cette fonctionnalité, vous pouvez présenter plusieurs fournisseurs de connexion à vos utilisateurs.
- **Autoriser uniquement les demandes authentifiées**. Rediriger toutes les demandes anonymes vers `/.auth/login/<provider>` pour le fournisseur choisi. La fonctionnalité équivaut à **Se connecter avec le <fournisseur>**. Si la demande anonyme provient d'une application mobile native, la réponse

retournée est un message `HTTP 401 Unauthorized`. Avec cette fonctionnalité, vous n'avez pas besoin d'écrire du code d'authentification dans votre application.

- **Journalisation et suivi**. Consulter les traces d'authentification et d'autorisation directement dans vos fichiers journaux. Si une erreur d'authentification inattendue se produit, vous trouverez facilement tous les détails dans les journaux d'activité existants. Si vous activez le suivi des demandes ayant échoué, vous pouvez voir exactement comment le module de sécurité a participé à l'échec d'une demande. Dans les journaux d'activité de suivi, recherchez les références à un module nommé `EasyAuthModule_32/64`.

Créer des noms de domaine personnalisés

Configurer un nom de domaine personnalisé pour votre application

Pour mapper un nom DNS personnalisé à votre application, **vous avez besoin d'un plan App Service de niveau payant pour votre application**.

'**Réservez votre nom de domaine**. Si vous n'avez pas encore de nom de domaine externe enregistré pour votre application, le moyen le plus simple de configurer un domaine personnalisé est d'en acheter un directement dans le portail Azure. (Ce nom n'est pas le nom attribué par Azure `\*.azurewebsites.net`.) Le processus d'enregistrement vous permet de gérer le nom de domaine de votre application web directement dans le portail Azure au lieu d'accéder à un site tiers. La configuration du nom de domaine dans votre application web est également un processus simple dans le portail Azure.

1. **Créez des enregistrements DNS pour mapper le domaine à votre application web Azure**. Le système DNS (Domain Name System) utilise des enregistrements de données pour mapper les noms de domaine aux adresses IP. Il existe plusieurs types d'enregistrements DNS.

    - Pour les applications web, vous créez un enregistrement `A` (adresse) ou un enregistrement `CNAME` (nom canonique).

        - Un enregistrement `A` (adresse) mappe un nom de domaine à une adresse IP.
        - Un enregistrement `CNAME` mappe un nom de domaine à un autre nom de domaine. DNS utilise le deuxième nom pour rechercher l'adresse. Les utilisateurs voient toujours le premier nom de domaine dans leur navigateur. Par exemple, vous

pouvez mapper `contoso.com` à votre URL `webapp.azurewebsites.net`.

- Si l'adresse IP change, l'entrée `CNAME` reste valide alors que l'enregistrement `A` doit être mis à jour.

- Certains bureaux d'enregistrement de domaines n'autorisent pas les enregistrements `CNAME` pour le domaine racine ou pour les domaines génériques. Dans ce cas, vous devez utiliser un enregistrement `A`.

2. **Activez le domaine personnalisé**. Une fois que vous avez votre domaine et avez créé votre enregistrement DNS, utilisez le portail Azure pour valider votre domaine personnalisé et l'ajouter à votre application web. Veillez à tester votre domaine avant de le publier.

Ce qu'il faut savoir sur Sauvegarde et restauration

- Pour utiliser la fonctionnalité Sauvegarde et restauration, vous avez besoin du plan App Service de niveau Standard ou Premium pour votre application ou site.
- Vous avez besoin d'un compte de stockage Azure et d'un conteneur dans le même abonnement que l'application à sauvegarder.
- Azure App Service peut sauvegarder les informations suivantes dans le compte de stockage Azure et le conteneur que vous avez configurés pour votre application :
  - Paramètres de configuration d'application
  - le contenu d'un fichier ;
  - Toute base de données connectée à votre application (SQL Database, Azure Database pour MySQL, Azure Database pour PostgreSQL, MySQL in-app)
- Dans votre compte de stockage, chaque sauvegarde se compose d'un fichier zip et d'un fichier XML :
  - Le fichier zip contient les données de sauvegarde de votre application ou site.
  - Le fichier XML contient un manifeste du contenu du fichier zip.
- Vous pouvez configurer des sauvegardes manuellement ou selon une planification.
- Les sauvegardes complètes sont la valeur par défaut.
- Les sauvegardes partielles sont prises en charge. Vous pouvez spécifier des fichiers et des dossiers à exclure d'une sauvegarde.
- Vous restaurez des sauvegardes partielles de votre application ou site de la même façon que vous restaurez une sauvegarde normale.
- Les sauvegardes peuvent contenir jusqu'à 10 Go de contenu d'application et de base de données.

- Les sauvegardes de votre application ou site sont visibles dans la page **Conteneurs** de votre compte de stockage et de votre application (ou site) dans le portail Azure.

Ce qu'il faut savoir sur Application Insights

Examinons certaines caractéristiques d'Application Insights pour Azure Monitor.

- Application Insights fonctionne sur diverses plateformes, notamment .NET, Node.js et Java EE.
- La fonctionnalité peut être utilisée pour les configurations hébergées localement, dans un environnement hybride ou dans n'importe quel cloud public.
- Application Insights s'intègre à votre processus DevOps, et a des points de connexion sur de nombreux outils de développement.
- Vous pouvez monitorer et analyser les données des applications mobiles en intégrant Visual Studio App Center.

Configurer Azure Container Instances

Ce qu'il faut savoir sur Azure Container Instances

- **Temps de démarrage rapides**. Les conteneurs peuvent démarrer en quelques secondes sans devoir provisionner et gérer des machines virtuelles.
- **Connectivité IP publique et noms DNS**. Les conteneurs peuvent être directement exposés sur Internet avec une adresse IP et un nom de domaine complet (FQDN).
- **Tailles personnalisées**. Les nœuds de conteneur peuvent être mis à l'échelle de manière dynamique pour répondre aux demandes de ressources réelles pour une application.
- **Stockage persistant**. Les conteneurs prennent en charge le montage direct des partages de fichiers Azure Files.
- **Conteneurs Windows et Linux**. Container Instances peut planifier les conteneurs Windows et Linux. Spécifiez le type de système d'exploitation quand vous créez vos groupes de conteneurs.
- **Groupes coplanifiés**. Le service Container Instances prend en charge la planification de groupes multiconteneurs qui partagent des ressources de machine hôte.
- **Déploiement d'un réseau virtuel**. Le service Container Instances peut être déployé dans un réseau virtuel Azure.

Informations importantes sur les groupes de conteneurs

- Un groupe de conteneurs est similaire à un pod dans Kubernetes. Un pod correspond généralement à un mappage 1:1 avec un conteneur, mais un pod

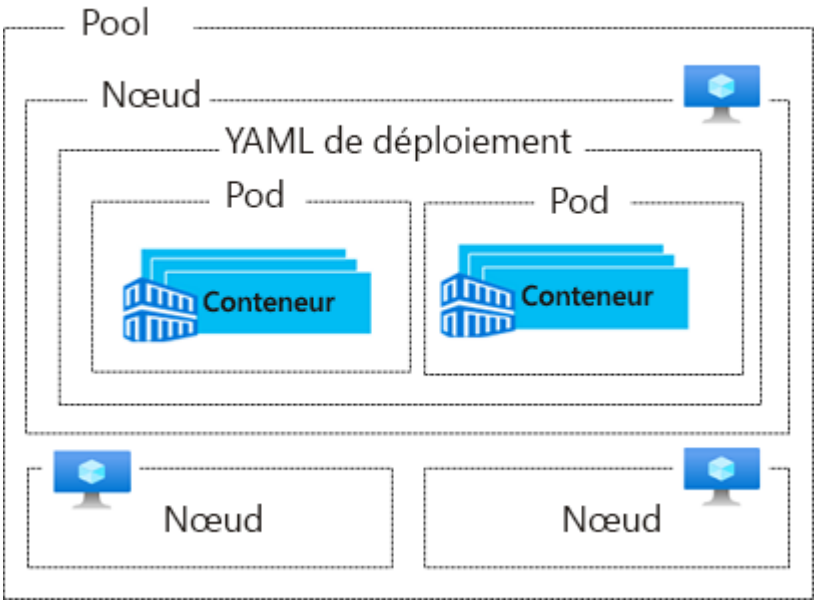
peut contenir plusieurs conteneurs. Les conteneurs d'un pod multiconteneur peuvent partager des ressources associées.

- Azure Container Instances alloue des ressources à un groupe multiconteneur en ajoutant les demandes de ressources de tous les conteneurs du groupe. Les ressources peuvent inclure des éléments comme des processeurs, de la mémoire et des GPU.

  Imaginons un groupe de conteneurs qui comporte deux conteneurs nécessitant chacun des ressources du processeur. Chaque conteneur nécessite un processeur. Azure Container Instances alloue deux processeurs pour le groupe de conteneurs.
- Il existe deux méthodes courantes pour déployer un groupe multiconteneur : à l'aide d'un modèle Resource Manager (ARM) ou de fichiers YAML.
    - **Modèle ARM**. Un modèle ARM est recommandé pour le déploiement d'autres ressources de service Azure quand vous déployez vos instances de conteneur, comme un partage de fichiers Azure Files.
    - **Fichier YAML**. En raison de la nature concise du format YAML, un fichier YAML est recommandé quand le déploiement comprend uniquement des instances de conteneur.
- Les groupes de conteneurs peuvent partager une adresse IP externe, un ou plusieurs ports sur l'adresse IP et une étiquette DNS avec un nom de domaine complet (FQDN).
    - **Accès client externe**. Vous devez exposer le port sur l'adresse IP et à partir du conteneur pour que les clients externes puissent atteindre un conteneur de votre groupe.
    - **Mappage de ports**. Le mappage de ports n'est pas pris en charge, car les conteneurs d'un groupe partagent un espace de noms de port.
    - **Groupes supprimés**. Quand un groupe de conteneurs est supprimé, son adresse IP et son nom de domaine complet sont libérés.

Configurer Azure Kubernetes Service

Explorer la terminologie Azure Kubernetes Service



Ce qu'il faut savoir sur les concepts AKS

- **Pools** : Un pool est un groupe de nœuds qui ont une configuration identique.
- **Nœuds** : Un nœud est une machine virtuelle individuelle qui exécute des applications conteneurisées.
- **Pods** : Un pod représente une seule instance d'une application. Un pod peut contenir plusieurs conteneurs.
- **Conteneur** : Un conteneur est une image exécutable légère et portable qui contient les logiciels et toutes leurs dépendances.
- **Déploiement** : Un déploiement a un ou plusieurs pods identiques managés par Kubernetes.
- **Manifeste** : Le manifeste est le fichier YAML qui décrit un déploiement.

Explorer l'architecture des clusters et des nœuds AKS

Un cluster Azure Kubernetes Service est divisé en deux composants : les nœuds managés par Azure et les nœuds managés par le client. Les nœuds managés par Azure fournissent les services Kubernetes de base et l'orchestration des charges de travail d'application dans votre cluster AKS. Les nœuds managés par le client exécutent vos charges de travail d'application dans votre cluster AKS.

Ce qu'il faut savoir sur les clusters, nœuds et pools AKS

- Pour exécuter vos applications et services annexes, vous avez besoin d'un nœud Kubernetes pour votre cluster AKS. Chaque cluster AKS contient un ou

plusieurs nœuds qui exécutent les composants de nœud Kubernetes et le runtime de conteneur.

- Les nœuds sont des instances de Machines Virtuelles Azure. Les nœuds d'une même configuration sont regroupés dans des pools de nœuds. Un cluster Kubernetes contient un ou plusieurs pools de nœuds.
- Le nombre et la taille initiaux des nœuds sont définis quand vous créez un cluster AKS, opération qui engendre la création du nœud de pools par défaut. Le pool de nœuds par défaut dans AKS contient les machines virtuelles sous-jacentes qui exécutent vos nœuds d'agent.
- Quand vous créez un cluster AKS, un nœud de cluster managé par Azure est automatiquement créé et configuré. Ce nœud est fourni en tant que ressource Azure managée qui est à l'écart de l'utilisateur.
- Le kubelet est l'agent Kubernetes qui traite les requêtes d'orchestration en provenance du nœud managé par Azure ainsi que la planification de l'exécution des conteneurs demandés.
- Le composant kube-proxy gère le réseau virtuel sur chaque nœud. Le proxy route le trafic réseau et gère l'adressage IP pour les services et les pods.
- Le runtime de conteneur permet aux applications conteneurisées de s'exécuter et d'interagir avec d'autres ressources telles que le réseau virtuel et le stockage.
    - Les clusters AKS avec des pools de nœuds Kubernetes version 1.19 et ultérieure utilisent `containerd` comme runtime de conteneur.
    - Les clusters AKS avec des pools de nœuds qui utilisent des versions de Kubernetes antérieures à v1.19 implémentent Moby (Docker en amont) comme runtime de conteneur.
- Lorsque vous implémentez des clusters Azure Kubernetes Service, vous payez uniquement pour l'exécution de nœuds d'agent dans votre cluster.

Configuration de la mise en réseau Azure Kubernetes Service

Kubernetes utilise des pods pour exécuter une instance de votre application et fournit différents services pour regrouper logiquement les pods. Cette disposition offre un accès direct via une adresse IP ou un système de noms de domaine (DNS) et sur un port spécifique.

Ce qu'il faut savoir sur les réseaux virtuels Kubernetes

- Les nœuds Kubernetes sont connectés à un réseau virtuel qui fournit une connectivité entrante et sortante pour les pods.
- Le composant kube-proxy s'exécute sur chaque nœud afin de fournir les fonctionnalités réseau.
- Les stratégies réseau configurent la sécurité et le filtrage du trafic réseau pour les pods.
- Le trafic réseau peut être distribué à l'aide d'un équilibreur de charge.

- Vous pouvez effectuer le routage complexe du trafic des applications avec des contrôleurs d'entrée.

Azure Kubernetes Service

La plateforme Azure permet de simplifier les réseaux virtuels pour les clusters Azure Kubernetes Service.

Quand vous créez un équilibreur de charge Kubernetes, la ressource Azure Load Balancer sous-jacente est créée et configurée. Quand vous ouvrez des ports réseau sur les pods, les règles de groupe de sécurité réseau Azure correspondantes sont configurées. Pour le routage d'applications HTTP, Azure peut configurer un DNS externe quand de nouvelles routes d'entrée sont configurées.

Ce qu'il faut savoir sur les types de service Kubernetes

Type de service	Description	Scénario
IP du cluster	Créez une adresse IP interne à utiliser dans un cluster Azure Kubernetes Service.	*Implémenter des applications internes uniquement qui prennent en charge d'autres charges de travail au sein du cluster*
NodePort	Créez un mappage de port sur le nœud sous-jacent.	*Autoriser un accès direct à l'application avec l'adresse IP et le port du nœud*
LoadBalancer	Créez une ressource Azure Load Balancer, configurez une adresse IP externe et connectez les pods demandés au pool de back-ends de l'équilibreur de charge.	*Autoriser le trafic des clients à atteindre l'application en créant des règles d'équilibrage de charge sur les ports souhaités*
ExternalName	Créez une entrée DNS spécifique.	*Prendre en charge un accès plus facile aux applications*

Voici quelques détails sur ces options de configuration réseau :

- Vous pouvez créer des équilibreurs de charge internes et externes.
- L'adresse IP pour les services et les équilibreurs de charge peut être attribuée dynamiquement, ou vous pouvez spécifier une adresse IP statique existante.

- Les équilibreurs de charge internes ne recevant qu'une adresse IP privée, ils ne sont pas accessibles à partir d'Internet.
- Des adresses IP statiques internes et externes peuvent être affectées. L'adresse IP statique existante est souvent liée à une entrée DNS.

Ce qu'il faut savoir sur les pods Kubernetes

Kubernetes utilise des pods pour exécuter une instance de votre application, où un pod représente une instance unique de votre application.

- Les pods ont généralement un mappage 1:1 avec un conteneur, bien qu'il existe des scénarios avancés où un pod peut contenir plusieurs conteneurs.
- Ces pods multiconteneurs sont planifiés ensemble sur le même nœud et permettent aux conteneurs de partager des ressources connexes.
- Quand vous créez un pod, vous pouvez définir des limites de ressources pour demander une certaine quantité de ressources en UC ou mémoire. Le planificateur Kubernetes tente de planifier les pods afin qu'ils s'exécutent sur un nœud ayant les ressources disponibles pour répondre à la requête.
- Vous pouvez spécifier des limites de ressources maximales qui empêchent un pod donné de consommer trop de ressources de calcul à partir du nœud sous-jacent.
- Un pod est une ressource logique, tandis qu'un conteneur est l'endroit où s'exécutent les charges de travail des applications.

Ce qu'il faut savoir sur les volumes de stockage

- Les volumes de stockage traditionnels qui stockent et récupèrent les données sont créés en tant que ressources Kubernetes gérées par le Stockage Azure.
- Vous pouvez créer manuellement des volumes de stockage en vue de les attribuer directement à des pods, ou vous pouvez laisser Kubernetes les créer automatiquement.
- Les volumes de stockage peuvent utiliser des disques Azure ou Azure Files :
    - Utilisez **Disques Azure** pour créer une ressource *DataDisk* Kubernetes. Les disques peuvent utiliser un stockage Azure Premium, assorti de disques SSD hautes performances, ou le stockage Azure Standard, assorti de disques HDD standards. Pour la plupart des charges de travail de production et de développement, utilisez le stockage Premium. Les disques Azure sont montés avec des autorisations *ReadWriteOnce*, donc ils ne sont disponibles que pour un seul nœud. Pour les volumes de stockage accessibles par plusieurs nœuds simultanément, utilisez Azure Files.
    - Utilisez **Azure Files** pour monter un partage SMB 3.0 géré par un compte Stockage Azure sur des pods. Avec Azure Files, vous pouvez partager des données entre plusieurs nœuds et plusieurs pods. Les fichiers peuvent utiliser un stockage Azure Standard, assorti de

disques HDD standard, ou un stockage Azure Premium, assorti de disques SSD hautes performances.

Ce qu'il faut savoir sur les volumes persistants

Les volumes sont définis et créés dans le cadre du cycle de vie d'un pod et existent tant que le pod n'est pas supprimé. Le stockage d'un pod est censé être conservé si le pod est replanifié sur un autre hôte pendant un événement de maintenance, en particulier dans les configurations `StatefulSets`. Un volume persistant (`PersistentVolume`) est une ressource de stockage créée et gérée par l'API Kubernetes qui peut exister au-delà de la durée de vie d'un pod donné.

- Vous pouvez utiliser des disques Azure ou Azure Files pour fournir un volume persistant. Le choix d'utiliser des disques Azure ou Azure Files est souvent déterminé par le niveau de performance ou le besoin d'un accès simultané aux données.
- Un volume persistant peut être créé de façon statique par un administrateur de cluster, ou de façon dynamique par le serveur d'API Kubernetes.
- Si un pod est planifié et demande un stockage qui n'est pas disponible actuellement, Kubernetes peut créer les disques Azure ou un stockage Azure Files sous-jacents. Kubernetes attache également le volume de stockage au pod.
- Le provisionnement dynamique utilise un type `StorageClass` pour identifier quel type de Stockage Azure doit être créé.

Ce qu'il faut savoir sur les classes de stockage

Pour définir différents niveaux de stockage, tels que Premium et Standard, vous pouvez configurer un type `StorageClass`. Le type `StorageClass` définit également les actions `reclaimPolicy` pour le stockage. La définition `reclaimPolicy` contrôle le comportement de la ressource de Stockage Azure sous-jacente quand le pod est supprimé et que le volume persistant risque de ne plus être nécessaire. La ressource de stockage sous-jacente peut être supprimée ou conservée en vue d'être utilisée par un futur pod.
Dans Azure Kubernetes Service, quatre types `StorageClasses` initiaux sont créés pour un cluster à l'aide de plug-ins de stockage dans l'arborescence :

Type StorageClass	Description	Action reclaimPolicy
`default`	Utilisez le stockage Azure StandardSSD pour créer un disque managé Azure.	Garantit que le disque Azure sous-jacent est supprimé lorsque le volume persistant qui a utilisé le disque est supprimé.

`managed-premium`	Utilisez le stockage Azure Premium pour créer un disque managé Azure.	Garantit que le disque Azure sous-jacent est supprimé lorsque le volume persistant qui a utilisé le disque est supprimé.
`azurefile`	Utilisez le stockage Azure Standard pour créer un partage de fichiers Azure Files.	Garantit que le partage de fichiers Azure Files sous-jacent est supprimé lorsque le volume persistant qui a utilisé le partage de fichiers est supprimé.
`azurefile-premium`	Utilisez le stockage Azure Premium pour créer un partage de fichiers Azure Files.	Garantit que le partage de fichiers Azure Files sous-jacent est supprimé lorsque le volume persistant qui a utilisé le partage de fichiers est supprimé.

Si aucun type `StorageClass` n'est spécifié pour un volume persistant, le type `default` est utilisé.

Ce qu'il faut savoir sur les revendications de volumes persistants

Une revendication de volume persistant (`PersistentVolumeClaim`) demande un stockage sur des disques Azure ou Azure Files d'une taille, d'un mode d'accès et d'une `StorageClass` particuliers.

- Le serveur d'API Kubernetes peut provisionner dynamiquement la ressource de stockage sous-jacente dans Azure si aucune ressource existante ne satisfait à la revendication selon le type de `StorageClass` défini.
- La définition du pod inclut le montage du volume une fois que ce dernier a été connecté au pod.
- Un volume persistant est *lié* à une revendication de volume persistant une fois qu'une ressource de stockage disponible a été affectée au pod qui demande le volume.
- Les volumes persistants sont liés aux revendications par un mappage 1 à 1.

Ce qu'il faut savoir sur les techniques de mise à l'échelle

Technique de mise à l'échelle	Description	Configuration requise pour la version

Mettre à l’échelle manuellement les pods ou les nœuds	Mettez à l’échelle vos réplicas (pods) et vos nœuds manuellement pour tester la façon dont votre application répond à des changements de ressources disponibles et d’état. La mise à l’échelle manuelle des ressources vous permet de définir un nombre spécifique de ressources à utiliser pour maintenir un coût fixe, par exemple le nombre de nœuds. Pour effectuer une mise à l’échelle manuelle, vous devez définir le nombre de réplicas ou de nœuds. L’API Kubernetes planifie ensuite la création de pods ou le drainage de nœuds.	Toutes les versions de Kubernetes
Mettre à l’échelle automatiquement les pods	Utilisez l’autoscaler de pods horizontal (HPA, horizontal pod autoscaler) pour surveiller la demande en ressources et adapter automatiquement le nombre de vos réplicas. Par défaut, le HPA vérifie l’API de métriques toutes les 30 secondes à la recherche d’un changement à apporter dans le nombre de vos réplicas. Lorsque des modifications sont nécessaires, le nombre de réplicas est augmenté ou diminué en conséquence.	Clusters AKS qui déploient Metrics Server pour Kubernetes 1.8 ou ultérieur

Mettre à l'échelle automatiquement les clusters	Répondez aux demandes changeantes de pods avec l'autoscaler de cluster, qui ajuste le nombre de vos nœuds en fonction des ressources de calcul demandées dans le pool de nœuds. Par défaut, l'autoscaler de cluster vérifie le serveur d'API toutes les 10 secondes à la recherche d'un changement à apporter dans le nombre de nœuds. Si l'autoscaler de cluster détermine qu'un changement est nécessaire, le nombre de nœuds de votre cluster AKS est augmenté ou diminué en conséquence.	Clusters AKS activés pour RBAC qui exécutent Kubernetes 1.10.x ou ultérieur

Ce qu'il faut savoir lors de l'utilisation de la mise à l'échelle horizontale

- **Prenez en compte le nombre de pods (réplicas)**. Lorsque vous configurez le HPA pour un déploiement donné, vous définissez le nombre minimal et maximal de pods (réplicas) qui peuvent s'exécuter.
- **Envisagez de mettre à l'échelle les métriques**. Pour utiliser le HPA, définissez la métrique à surveiller et à utiliser comme base pour les décisions de mise à l'échelle, comme l'utilisation du processeur.
- **Envisagez un ralentissement pour les événements de mise à l'échelle**. Comme le HPA vérifie l'API de métriques toutes les 30 secondes, les événements de mise à l'échelle précédents risquent de ne pas être terminés avant les vérifications suivantes. Le HPA risque de changer le nombre de réplicas avant que l'événement de mise à l'échelle précédent ne reçoive les demandes de charges de travail d'application et de ressources pour les ajuster en conséquence.
- Pour minimiser la course aux événements, définissez des valeurs de ralentissement ou de délai pour définir la durée pendant laquelle le HPA doit attendre après un événement de mise à l'échelle avant qu'un autre événement de mise à l'échelle ne soit déclenché. Par défaut, le délai pour un scale-up des événements est de 3 minutes, tandis qu'il est de 5 minutes pour un scale-down.
- **Envisagez d'ajuster les valeurs de ralentissement**. Vous devrez probablement ajuster les valeurs de ralentissement. Les valeurs de ralentissement par défaut peuvent donner l'impression que le HPA n'adapte

pas le nombre de réplicas assez rapidement. Pour augmenter plus rapidement le nombre de réplicas utilisés, réduisez la valeur `--horizontal-pod-autoscaler-upscale-delay` lorsque vous créez vos définitions HPA à l'aide de l'outil `kubectl` Azure CLI.

Ce qu'il faut savoir lors de l'utilisation de la mise à l'échelle automatique de clusters

- **Envisagez une combinaison avec le HPA**. L'autoscaler de cluster est généralement utilisé parallèlement à l'autoscaler de pods élastique. Lorsque les deux techniques de mise à l'échelle sont combinées, le HPA augmente ou diminue le nombre de pods en fonction de la demande de l'application. L'autoscaler de cluster ajuste le nombre de nœuds en fonction des besoins pour exécuter les pods supplémentaires en conséquence.
- **Envisagez un scale-out des événements**. Si les ressources de calcul d'un nœud sont insuffisantes pour l'exécution d'un pod demandé, ce pod ne peut pas avancer dans le processus de planification. Le pod ne peut pas démarrer, sauf si d'autres ressources de calcul sont disponibles dans le pool de nœuds.

  Quand l'autoscaler de cluster remarque des pods qui ne peuvent pas être planifiés en raison de contraintes liées aux ressources du pool de nœuds, le nombre de nœuds du pool est augmenté pour fournir les ressources de calcul supplémentaires. Lorsque les nœuds supplémentaires sont correctement déployés et utilisables au sein du pool de nœuds, les pods sont alors planifiés pour s'exécuter dessus.
- **Envisagez une mise à l'échelle en rafale sur Azure Container Instances**. Si votre application doit être mise à l'échelle rapidement, certains pods risquent de rester à l'état d'attente de planification jusqu'à ce que les nouveaux nœuds déployés par l'autoscaler de cluster puissent accepter les pods planifiés. Pour les applications qui présentent des demandes de croissance extrêmement forte et rapide, vous pouvez mettre à l'échelle au moyen de nœuds virtuels et d'Azure Container Instances. Nous examinerons de plus près la mise à l'échelle en rafale rapide dans la section suivante.
- **Envisagez un scale-in des événements**. L'autoscaler de cluster surveille le statut de planification des pods pour les nœuds qui n'ont pas reçu récemment de nouvelles demandes de planification. Ce scénario indique que le pool de nœuds détient plus de ressources de calcul que nécessaire, et que le nombre de nœuds peut donc être réduit.

  Un nœud, qui transmet un seuil indiquant pendant 10 minutes qu'il n'est pas nécessaire, est planifié pour suppression par défaut. Lorsque cette situation se produit, les pods sont planifiés pour s'exécuter sur d'autres nœuds au sein du pool de nœuds tandis que l'autoscaler de cluster réduit le nombre de nœuds.

- **Envisagez d'éviter les pods uniques**. Vos applications risquent de rencontrer quelques perturbations au moment où les pods sont planifiés sur des nœuds différents et que l'autoscaler de cluster diminue le nombre de nœuds. Pour limiter ces perturbations, évitez les applications qui utilisent une seule instance de pod.

Informations à connaître sur la mise à l'échelle en rafale rapide

- Azure Container Instances vous permet de déployer rapidement votre instance de conteneur sans infrastructure supplémentaire. Lorsque vous vous connectez à AKS, votre instance de conteneur devient une extension logique et sécurisée de votre cluster AKS.
- Le composant Virtual Kubelet est installé dans votre cluster AKS. Le composant présente votre instance de conteneur sous la forme d'un nœud Kubernetes virtuel.
- Kubernetes planifie l'exécution des pods en tant qu'instances de conteneur via des nœuds virtuels, plutôt que des pods sur des nœuds de machine virtuelle directement dans votre cluster AKS.
- Votre application n'a besoin d'aucune modification pour utiliser les nœuds virtuels.
- Les déploiements peuvent être mis à l'échelle sur AKS et Container Instances. Il n'existe pas de délai quand l'autoscaler de cluster déploie de nouveaux nœuds sur votre cluster AKS.
- Les nœuds virtuels sont déployés sur un autre sous-réseau dans le même réseau virtuel que votre cluster AKS. Cette configuration de réseau virtuel permet au trafic entre Container Instances et AKS d'être sécurisé. À l'instar d'un cluster AKS, une instance de conteneur est une ressource de calcul logique et sécurisée, qui est isolée des autres utilisateurs.

Qu'est-ce qu'Azure Automation State Configuration ?

Azure Automation State Configuration est un service Azure basé sur PowerShell. Il vous permet de déployer, de surveiller de façon fiable et de mettre à jour automatiquement l'état souhaité de toutes vos ressources. Azure Automation fournit les outils permettant de définir des configurations et de les appliquer à des machines, qu'elles soient réelles ou virtuelles.

Pourquoi utiliser Azure Automation State Configuration ?

Azure Automation State Configuration utilise le DSC PowerShell pour aider à résoudre ces problèmes. Il gère de manière centralisée vos artefacts DSC et le processus DSC.

Azure Automation State Configuration a un serveur Pull intégré. Vous pouvez cibler des nœuds pour qu'ils reçoivent automatiquement les configurations de ce serveur Pull, conformes à l'état souhaité et qu'ils indiquent leur conformité. Vous pouvez

cibler des machines physiques ou virtuelles Windows ou Linux, dans le cloud ou en local.

Qu’est-ce que DSC PowerShell ?

DSC PowerShell est une plateforme de gestion déclarative utilisée par Azure Automation State Configuration pour configurer, déployer et contrôler des systèmes.

```
Configuration Create_Share
{
  Import-DscResource -Module xSmbShare
  # A node describes the VM to be configured

  Node $NodeName
  {
        # A node definition contains one or more resource blocks
        # A resource block describes the resource to be configured on the node
        xSmbShare MySMBShare
        {
        Ensure        = "Present"
        Name          = "MyFileShare"
        Path          = "C:\Shared"
        ReadAccess  = "User1"
        FullAccess  = "User2"
        Description = "This is an updated description for this share"
        }
  }
}
```

Qu’est-ce que le Gestionnaire de configuration locale ?

Le Gestionnaire de configuration local est un composant de Windows Management Framework (WMF) sur un système d’exploitation Windows. Le Gestionnaire de configuration local est responsable de la mise à jour de l’état d’un nœud, comme une machine virtuelle, pour le faire correspondre à l’état souhaité. Chaque fois que le Gestionnaire de configuration local s’exécute, il effectue les étapes suivantes :

1. **Obtenir** : obtient l’état actuel du nœud.
2. **Tester** : compare l’état actuel d’un nœud à l’état souhaité en utilisant un script DSC compilé (fichier .mof).
3. **Définir** : met à jour le nœud pour qu’il corresponde à l’état souhaité décrit dans le fichier .mof.

Vous configurez le Gestionnaire de configuration local quand vous inscrivez une machine virtuelle auprès d’Azure Automation.

Architectures Envoi (push) et Tirage (pull) dans DSC

Le Gestionnaire de configuration local sur chaque nœud peut fonctionner en deux modes.

- **Mode push** : Un administrateur envoie manuellement ou *pousse* (push) les configurations vers un ou plusieurs nœuds. Le Gestionnaire de configuration local s'assure que l'état de chaque nœud correspond à ce qui est spécifié par la configuration.
- **Mode Tirage (pull)** : un *serveur Pull* contient les informations de configuration. Le Gestionnaire de configuration local sur chaque nœud interroge le serveur Pull à intervalles réguliers, par défaut toutes les 15 minutes, pour obtenir les informations de configuration les plus récentes. Ces requêtes constituent l'étape 1 dans le diagramme ci-dessous. À l'étape 2, le serveur Pull renvoie les détails de toutes les modifications de la configuration à chaque nœud.

Les deux modes présentent des avantages :

- Le mode Envoi (push) est facile à configurer. Il n'a pas besoin de sa propre infrastructure dédiée et peut s'exécuter sur un ordinateur portable. Le mode Envoi (push) est utile pour tester les fonctionnalités de DSC. Vous pouvez également utiliser le mode Envoi (push) pour obtenir une machine nouvellement mise en image avec l'état souhaité pour la base de référence.
- Le mode Tirage (pull) est pratique quand vous avez un déploiement d'entreprise qui s'étend sur un grand nombre de machines. Le Gestionnaire de configuration local interroge régulièrement le serveur Pull et vérifie que les nœuds sont dans l'état souhaité. Si un outil ou une équipe externe applique des correctifs logiciels qui aboutissent à des écarts de la configuration sur des machines individuelles, ces machines sont rapidement annulées en ligne et la configuration est rétablie à celle que vous avez définie. Ce processus vous permet d'obtenir un état de conformité continue pour vos obligations réglementaires et de sécurité.

Plateformes et systèmes d'exploitation pris en charge

Azure Automation DSC est pris en charge par le cloud Azure et d'autres fournisseurs cloud, par votre infrastructure locale ou par une combinaison hybride couvrant tous ces environnements.

Azure Automation DSC prend en charge les systèmes d'exploitation suivants :

- Windows
    - Server 2019
    - Server 2016

    - Server 2012 R2
    - Server 2012
    - Server 2008 R2 SP1
    - 11
    - 10
    - 8.1
    - 7
- Linux
    - L'extension Linux DSC prend en charge toutes les distributions Linux listées dans la documentation DSC PowerShell.

DSC PowerShell est installé sur toutes les machines Linux prises en charge par Azure Automation DSC.

Autres exigences de DSC

Si vos nœuds se trouvent sur un réseau privé, le port et les URL suivants sont nécessaires pour que DSC communique avec Automation :

- **Port** : seul le port TCP 443 est nécessaire pour l'accès Internet sortant.
- **URL globale** : *.azure-automation.net
- **URL globale de US Gov Virginia** : *.azure-automation.us
- **Service de l'agent** : https://`<workspaceId>`.agentsvc.azure-automation.net

Configurer et gérer des réseaux virtuels pour les administrateurs Azure

Configurer des réseaux virtuels

Ce que vous devez savoir sur les sous-réseaux

- Chaque sous-réseau contient une plage d'adresses IP qui appartient à l'espace d'adressage du réseau virtuel.
- La plage d'adresses d'un sous-réseau doit être unique dans l'espace d'adressage du réseau virtuel.
- La plage d'un sous-réseau ne peut pas chevaucher d'autres plages d'adresses IP de sous-réseau dans le même réseau virtuel.
- L'espace d'adressage IP d'un sous-réseau doit être spécifié en utilisant la notation CIDR.
- Vous pouvez segmenter un réseau virtuel en un ou plusieurs sous-réseaux dans le portail Azure. Les caractéristiques des adresses IP des sous-réseaux sont listées.

Adresses réservées

Pour chaque sous-réseau, Azure réserve cinq adresses IP. Les quatre premières adresses et la dernière adresse sont réservées.
Examinons les adresses réservées dans la plage d'adresses IP `192.168.1.0/24`.

Adresse réservée	Motif
`192.168.1.0`	Cette valeur identifie l'adresse de réseau virtuel.
`192.168.1.1`	Azure configure cette adresse comme passerelle par défaut.
`192.168.1.2 et 192.168.1.3`	Azure mappe ces adresses IP Azure DNS à l'espace de réseau virtuel.
`192.168.1.255`	Cette valeur fournit l'adresse de diffusion du réseau virtuel.

Créer des réseaux virtuels

- Quand vous créez un réseau virtuel, vous devez définir l'espace d'adressage IP du réseau.
- Prévoyez d'utiliser un espace d'adressage IP qui n'est pas déjà utilisé dans votre organisation.
    - L'espace d'adressage du réseau peut être local ou dans le cloud, mais pas les deux.
    - Vous ne pouvez pas redéfinir l'espace d'adressage IP d'un réseau après sa création. Même si vous planifiez votre espace d'adressage pour des réseaux virtuels cloud uniquement, vous pouvez décider par la suite de connecter un site local.
- Pour créer un réseau virtuel, vous devez définir au moins un sous-réseau.
- Vous pouvez créer un réseau virtuel dans le portail Azure. Fournissez l'abonnement Azure, le groupe de ressources, le nom du réseau virtuel et la région du service pour le réseau.

Planifier l'adressage IP

Les **adresses IP privées** permettent de communiquer dans un réseau virtuel Azure et dans votre réseau local. Vous créez une adresse IP privée pour votre ressource quand vous utilisez une passerelle VPN ou un circuit Azure ExpressRoute pour étendre votre réseau à Azure.

Les **adresses IP publiques** permettent à votre ressource de communiquer avec Internet. Vous pouvez créer une adresse IP publique pour vous connecter aux services publics Azure.

Ce qu'il faut savoir sur les adresses IP

- Les adresses IP peuvent être attribuées de manière statique ou dynamique.
- Vous pouvez séparer les ressources IP attribuées de manière dynamique et statique dans différents sous-réseaux.
- Les adresses IP statiques ne changent pas et sont idéales pour certaines situations, comme :
    - Résolution de noms DNS, où un changement de l'adresse IP nécessite la mise à jour des enregistrements de l'hôte.
    - Modèles de sécurité basés sur une adresse IP qui nécessitent que les applications ou les services aient une adresse IP statique
    - Certificats TSL/SSL liés à une adresse IP.
    - Règles de pare-feu qui autorisent ou refusent le trafic en utilisant des plages d'adresses IP.
    - Machines virtuelles basées sur un rôle, comme les contrôleurs de domaine et les serveurs DNS.

Créer un adressage IP public

- **Version IP** : choisissez une adresse **IPv4** ou **IPv6**, ou **Les deux** adresses. L'option **Les deux** crée deux adresses IP publiques : une adresse IPv4 et une adresse IPv6.
- **Référence SKU** : sélectionnez la référence SKU de l'adresse IP publique, notamment **De base** ou **Standard**. La valeur doit correspondre à la référence SKU de l'équilibreur de charge Azure avec lequel l'adresse est utilisée.
- **Nom** : entrez un nom pour identifier l'adresse IP. Le nom doit être unique au sein du groupe de ressources que vous avez sélectionné.
- **Attribution d'adresse IP** : identifiez le type d'attribution d'adresse IP à utiliser.
    - Les adresses **dynamiques** sont affectées une fois qu'une adresse IP publique est associée à une ressource Azure, et que la ressource est démarrée pour la première fois. Les adresses dynamiques peuvent changer si une ressource, telle qu'une machine virtuelle, est arrêtée (libérée), puis redémarrée via Azure. L'adresse reste la même si une machine virtuelle est redémarrée ou arrêtée à partir du système d'exploitation invité. Lorsqu'une ressource d'adresse IP publique est supprimée d'une ressource, l'adresse dynamique est libérée.
    - Les adresses **statiques** sont attribuées durant la création d'une adresse IP publique. Les adresses statiques ne sont pas libérées tant qu'une ressource d'adresse IP publique n'est pas supprimée. Si l'adresse n'est pas associée à une ressource, vous pouvez changer la

méthode d’attribution après la création de l’adresse. Si l’adresse est associée à une ressource, vous risquez de ne pas pouvoir changer la méthode d’attribution.

Associer des adresses IP publiques

***** Les adresses IP statiques sont disponibles sur certaines références SKU uniquement.

Ressource	Association d’adresses IP publiques	Adresse IP dynamique	Adresse IP statique
Machine virtuelle	Carte d’interface réseau	Oui	Oui
Équilibrage de charge	Configuration frontale	Oui	Oui
passerelle VPN	Configuration IP de passerelle VPN	Oui	Oui *
passerelle d’application	Configuration frontale	Oui	Oui *

Références SKU d’adresse IP publique

Fonctionnalité	Référence SKU De base	Référence SKU standard
Attribution d’adresse IP	Statique ou dynamique	statique
Sécurité	Ouverte par défaut	Sécurisée par défaut, et fermée au trafic entrant
Ressources	Interfaces réseau, passerelles VPN, passerelles applicatives et équilibreurs de charge accessibles sur Internet	Interfaces réseau ou équilibreurs de charge standard publics
Redondance	Ne sont pas redondantes dans une zone	Redondance dans une zone par défaut

Affectation d’adresses IP privées

Une adresse IP privée est allouée à partir de la plage d’adresses du sous-réseau de la machine virtuelle dans lequel la ressource est déployée. Il existe deux options : dynamique et statique.

- **Dynamique** : Azure attribue la première adresse IP non attribuée ou non réservée de la plage d’adresses du sous-réseau. La méthode d’allocation par défaut est dynamique.
- **Statique** : vous sélectionnez et attribuez n’importe quelle adresse IP non attribuée ou non réservée de la plage d’adresses du sous-réseau.

Ce qu’il faut savoir sur les groupes de sécurité réseau

- Un groupe de sécurité réseau contient une liste de règles de sécurité qui autorisent ou rejettent le trafic réseau entrant et sortant.
- Un groupe de sécurité réseau peut être associé à un sous-réseau ou à une interface réseau.
- Un groupe de sécurité réseau peut être associé plusieurs fois.
- Vous créez un groupe de sécurité réseau et définissez des règles de sécurité dans le portail Azure.

Groupes de sécurité réseau et sous-réseaux

Vous pouvez attribuer des groupes de sécurité réseau à un sous-réseau et créer un sous-réseau filtré protégé (également appelé zone démilitarisée ou *DMZ*). Une zone DMZ agit comme un tampon entre les ressources de votre réseau virtuel et Internet.

- Utilisez le groupe de sécurité réseau pour limiter le flux de trafic sur toutes les machines qui résident dans le sous-réseau.
- Chaque sous-réseau peut avoir seulement un groupe de sécurité réseau associé.

Groupes de sécurité réseau et interfaces réseau

Vous pouvez attribuer des groupes de sécurité réseau à une carte d’interface réseau.

- Définissez des règles de groupe de sécurité réseau pour contrôler tout le trafic qui transite par une carte réseau.
- Chaque interface réseau existant dans un sous-réseau peut avoir zéro ou un groupe de sécurité réseau associé.

Ce qu’il faut savoir sur les règles de sécurité

- Azure crée plusieurs règles de sécurité par défaut au sein de chaque groupe de sécurité réseau, notamment pour le trafic entrant et le trafic sortant.

Exemples de règles par défaut : `DenyAllInbound` et `AllowInternetOutbound`.

- Azure crée les règles de sécurité par défaut dans chaque groupe de sécurité réseau que vous créez.
- Vous pouvez ajouter d'autres règles de sécurité à un groupe de sécurité réseau en spécifiant des conditions pour n'importe lequel des paramètres suivants :
    - **Nom**
    - **Priorité**
    - **Port**
    - **Protocole** (N'importe lequel, TCP, UDP)
    - **Source** (N'importe laquelle, Adresses IP, Étiquette de service)
    - **Destination** (N'importe laquelle, Adresse IP, Réseau virtuel)
    - **Action** (Autoriser ou Refuser)
- Une valeur de priorité est attribuée à chaque règle de sécurité. Toutes les règles de sécurité d'un groupe de sécurité réseau sont traitées par ordre de priorité. Quand une règle a une valeur de priorité basse, elle est prioritaire dans l'ordre de traitement.
- Vous ne pouvez pas supprimer les règles de sécurité par défaut.
- Vous pouvez remplacer une règle de sécurité par défaut en créant une autre règle de sécurité qui a un paramètre de priorité plus élevé pour votre groupe de sécurité réseau.

Règles de trafic entrant

Azure définit trois règles de sécurité de trafic entrant par défaut pour votre groupe de sécurité réseau. Ces règles **refusent tout le trafic entrant**, sauf le trafic provenant de votre réseau virtuel et des équilibreurs de charge Azure.
Quand un NSG est créé, Azure crée la règle de sécurité par défaut `DenyAllInbound` pour le groupe. Le comportement par défaut refuse tout le trafic entrant provenant d'Internet.

Règles de trafic sortant

Azure définit trois règles de sécurité de trafic sortant par défaut pour votre groupe de sécurité réseau. Ces règles **autorisent uniquement le trafic sortant** vers Internet et vers votre réseau virtuel.
Quand un NSG est créé, Azure crée la règle de sécurité par défaut `AllowInternetOutbound` pour le groupe.

Déterminer les règles de sécurité effectives du groupe de sécurité réseau.

- Pour le trafic entrant, Azure traite d'abord les règles de sécurité du groupe de sécurité réseau de tous les sous-réseaux associés, puis de toutes les interfaces réseau associées.
- Pour le trafic sortant, le processus est inversé. Azure évalue d'abord les règles de sécurité des groupes de sécurité réseau de toutes les interfaces réseau associées, puis des sous-réseaux associés.
- Pour le processus d'évaluation du trafic entrant et sortant, Azure vérifie également comment appliquer les règles pour le trafic interne au sous-réseau.

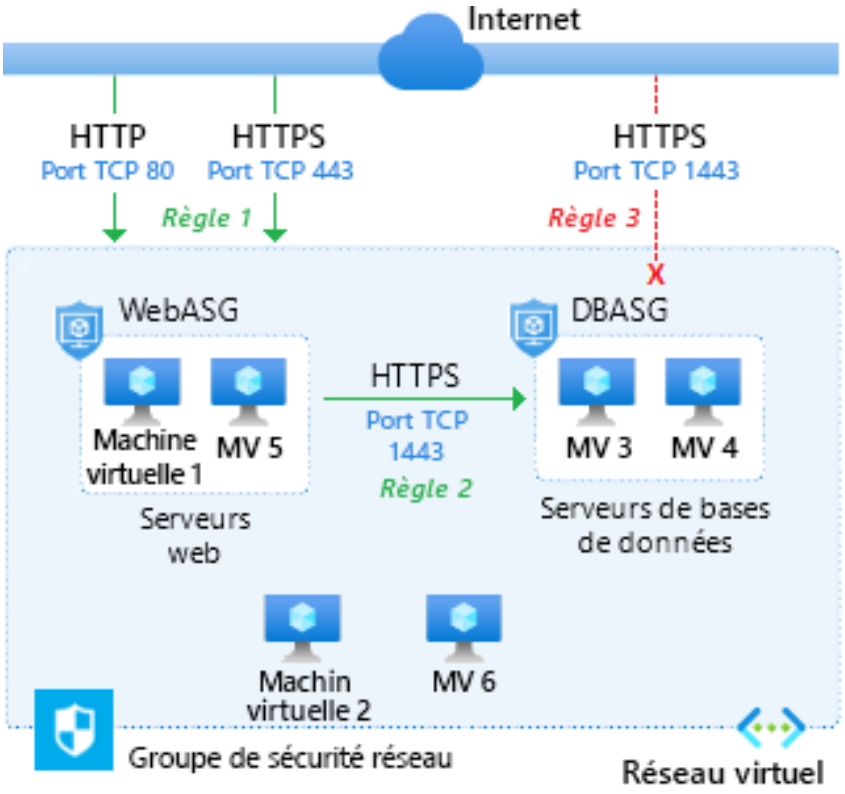
Pour qu'une règle de sécurité particulière soit toujours traitée, attribuez-lui la valeur de priorité la plus basse possible.

Créer des règles pour le groupe de sécurité réseau

- **Source** : identifie comment la règle de sécurité contrôle le trafic **entrant**. La valeur spécifie une plage d'adresses IP source spécifique autorisée ou refusée. Le filtre de la source peut être n'importe quelle ressource, une plage d'adresses IP, un groupe de sécurité d'application ou une étiquette par défaut.
- **Destination** : identifie comment la règle de sécurité contrôle le trafic **sortant**. La valeur spécifie une plage d'adresses IP de destination spécifique autorisée ou refusée. La valeur du filtre de destination est similaire à celle du filtre de source. La valeur peut être n'importe quelle ressource, une plage d'adresses IP, un groupe de sécurité d'application ou une étiquette par défaut.
- **Service** : spécifie le protocole de destination et la plage de ports pour la règle de sécurité. Vous pouvez choisir un service prédéfini, comme RDP ou SSH, ou fournir une plage de ports personnalisée. Vous pouvez choisir parmi un grand nombre de services.
- **Priorité** : attribue la valeur d'ordre de priorité de la règle de sécurité. Les règles sont traitées par ordre de priorité parmi toutes les règles d'un groupe de sécurité réseau, y compris un sous-réseau et une interface réseau. Plus la valeur est basse, plus la priorité de la règle est haute.

Implémenter des groupes de sécurité d'applications

Les groupes de sécurité d'application fonctionnent de la même façon que les groupes de sécurité réseau, mais ils fournissent un moyen centré sur l'application d'examiner votre infrastructure. Vous regroupez vos machines virtuelles dans un groupe de sécurité d'application. Ensuite, vous utilisez le groupe de sécurité d'application comme source ou destination dans les règles de groupe de sécurité réseau.



Déterminer les cas d’usage pour Pare-feu Azure

Pare-feu Azure est un service de sécurité réseau informatique géré qui protège vos ressources réseau virtuel Azure. Il s’agit d’un service de pare-feu avec état intégral, doté d’une haute disponibilité intégrée et d’une scalabilité illimitée dans le cloud. Vous pouvez créer, appliquer et consigner des stratégies de connectivité réseau et d’application de façon centralisée entre les abonnements et les réseaux virtuels.

Éléments à connaître concernant le service Pare-feu Azure

Fonctionnalité	Description
Adresse IP publique	Le service Pare-feu Azure utilise une adresse IP publique statique pour vos ressources de réseau virtuel. Les pare-feu externes identifient le trafic provenant de votre réseau virtuel grâce à l’adresse IP. **Remarque** : **vous pouvez associer plusieurs adresses IP publiques à votre pare-feu.**
Haute disponibilité intégrée	Avec Pare-feu Azure, vous bénéficiez d’une haute disponibilité intégrée sans aucune configuration supplémentaire requise. Il n’est pas nécessaire d’implémenter d’autres équilibreurs de charge.

Zones de disponibilité	Configurez Pare-feu Azure pendant le déploiement pour qu'il couvre plusieurs zones de disponibilité afin d'augmenter la disponibilité.
Extensibilité du cloud sans limites	Pare-feu Azure offre une scalabilité cloud illimitée permettant une mise à l'échelle selon les besoins et la prise en charge des flux de trafic réseau qui varient. Il est inutile de prévoir un budget pour les pics de trafic.
Règles de filtrage des noms de domaine complets de l'application	Pare-feu Azure permet de limiter le trafic HTTP/S sortant ou le trafic Azure SQL à une liste spécifiée de noms de domaine complets (FQDN), notamment des caractères génériques.
Règles de filtrage du trafic réseau	Créez des règles de filtrage réseau dans Pare-feu Azure pour autoriser ou refuser le trafic par adresse IP source et de destination, port et protocole. Pare-feu Azure est un service avec état intégral. Le service peut distinguer les paquets légitimes pour différents types de connexions. Les règles sont appliquées et consignées entre plusieurs abonnements et réseaux virtuels.
Renseignement sur les menaces	Pare-feu Azure prend en charge le filtrage basé sur le renseignement sur les menaces. Configurez votre pare-feu pour donner l'alerte et refuser le trafic depuis ou vers des adresses IP et des domaines malveillants connus. Ces adresses IP et domaines proviennent du flux Microsoft Threat Intelligence.
Intégration d'Azure Monitor	Le Pare-feu Azure est totalement intégré à Azure Monitor pour la journalisation et les analyses.

Par défaut, Pare-feu Azure refuse tout le trafic via votre réseau virtuel. Le comportement par défaut a pour objectif de fournir le niveau de protection le plus élevé contre les accès malveillants ou inconnus. Pour autoriser le trafic pour une ressource ou un service donné, vous devez définir des règles afin de contrôler le trafic spécifique.

Vous pouvez configurer **trois types de règles pour Pare-feu Azure : NAT, réseau et application**. Les règles sont définies dans le portail Azure.

Traitement des règles par Pare-feu Azure

Quand un paquet arrive sur un port désigné de votre réseau, il est inspecté afin de déterminer s'il est autorisé. Pare-feu Azure traite le paquet en l'évaluant selon vos règles dans l'ordre suivant :

1. Règles de réseau
2. Règles d'application (pour le réseau et les applications)

Si une règle autorisant l'acheminement du paquet est trouvée, aucune règle de réseau ou d'application restante n'est vérifiée pour ce paquet.

Une fois qu'un paquet est autorisé, Pare-feu Azure vérifie les règles NAT qui définissent la manière d'acheminer le trafic autorisé.

Éléments à connaître concernant les règles NAT

Vous pouvez configurer le NAT ou le DNAT (Destination Network Address Translation) du Pare-feu Azure pour traduire et filtrer le trafic entrant vers vos sous-réseaux. Chaque règle de la collection de règles NAT est ensuite utilisée pour traduire l'adresse IP et le port public de votre pare-feu en adresse IP et port privés. Une règle NAT qui route le trafic doit être accompagnée d'une règle de réseau correspondante pour autoriser le trafic.

Éléments à connaître concernant les règles de réseau

Tout trafic non-HTTP/S qui est autorisé à passer via le pare-feu doit disposer d'une règle de réseau. Imaginons un scénario dans lequel les ressources d'un sous-réseau doivent communiquer avec des ressources d'un autre sous-réseau. Dans ce cas, vous pouvez configurer une règle de réseau de la source vers la destination.

Éléments à connaître concernant les règles d'application

Les règles d'application définissent des noms de domaine complets (FQDN) qui sont accessibles depuis un sous-réseau. C'est le cas par exemple quand vous devez autoriser le trafic réseau de Windows Update via le pare-feu.

Configurer Azure DNS

Identifier les domaines et les domaines personnalisés

- Quand vous créez un abonnement Azure, Azure crée automatiquement un domaine Azure Active Directory (Azure AD) pour votre abonnement.
- Azure applique un **nom de domaine initial** à votre instance de domaine initial.

Le nom de domaine initial est de la forme `<Your Domain Name>`, suivie de `.onmicrosoft.com`. Par exemple : `yourdomainname.onmicrosoft.com`.

- L'objectif d'un **nom de domaine personnalisé** est de fournir une forme simplifiée de votre nom de domaine pour prendre en charge des utilisateurs ou des tâches spécifiques.

  Les organisations implémentent généralement des noms de domaine personnalisés pour permettre aux utilisateurs d'accéder à leur domaine en utilisant des informations d'identification qui leur sont familières.

  Prenons l'exemple du domaine Azure AD Azure Administrator Incorporated. Azure crée le nom de domaine initial pour l'instance Azure AD en tant que `azureadminincorg.onmicrosoft.com`. Un nom de domaine personnalisé pour l'instance peut être `azureadmininc.org`.
- Le nom de domaine initial est destiné à être utilisé jusqu'à ce que votre nom de domaine personnalisé soit *vérifié*.
- Avant de pouvoir être utilisé par Azure AD, un nom de domaine personnalisé doit être ajouté à votre annuaire et vérifié.
- Dans Azure AD, **les noms de domaine doivent être globalement uniques**. Quand un annuaire Azure AD a vérifié un nom de domaine spécifique, les autres annuaires Azure AD ne peuvent pas utiliser ce nom de domaine.

Vérifier les noms de domaine personnalisés

Quand un administrateur ajoute un nom de domaine personnalisé à une instance Azure Active Directory, celui-ci se trouve initialement dans un état *non vérifié*. Azure AD ne va autoriser aucune des ressources d'annuaire à utiliser un nom de domaine personnalisé qui est non vérifié.

Comment vérifier votre nom de domaine personnalisé

Après avoir ajouté un nom de domaine personnalisé pour votre instance Azure AD dans le portail Azure, vous devez vérifier la propriété de votre nom de domaine personnalisé.
Vous lancez le processus de vérification en ajoutant un enregistrement DNS pour votre nom de domaine personnalisé. Le type d'enregistrement DNS peut être MX ou TXT.
L'enregistrement `MX` (ou *Mail eXchange*) liste les serveurs d'échange de messagerie qui acceptent les e-mails pour votre domaine. L'enregistrement `TXT` (ou *Text*) indique du texte lisible par l'humain ou des données lisibles par une machine à propos de votre domaine. Ces types d'enregistrements sont définis dans RFC 1035.

Après avoir ajouté un enregistrement DNS à votre nom de domaine personnalisé, Azure interroge le domaine DNS quant à la présence de l'enregistrement DNS.

Créer des zones Azure DNS

Une zone DNS **Azure** héberge les enregistrements DNS pour un domaine. Pour héberger votre domaine dans Azure DNS, vous devez d'abord créer une zone DNS pour votre nom de domaine. Chaque enregistrement DNS pour votre domaine est ensuite créé à l'intérieur de cette zone DNS.

Dans le portail, vous spécifiez le nom de la zone DNS, le nombre d'enregistrements, le groupe de ressources, l'emplacement de la zone, l'abonnement associé et les serveurs de noms DNS.

- Dans un groupe de ressources, le nom d'une zone DNS doit être unique. Le fait de fournir un nom unique quand vous créez une zone DNS permet à Azure de garantir que la zone DNS n'existe pas déjà dans le groupe de ressources.
- Plusieurs zones DNS peuvent avoir le même nom, mais les zones DNS doivent exister dans des groupes de ressources différents ou des abonnements Azure différents.
- Quand plusieurs zones DNS partagent le même nom, chaque instance de zone DNS est affectée à une adresse de serveur de noms DNS différente.
- Le domaine racine/parent est inscrit auprès du bureau d'enregistrement et pointe vers Azure DNS.
- Les domaines enfants sont inscrits directement dans Azure DNS.

Déléguer des domaines DNS

Pour déléguer votre domaine à Azure DNS, vous devez identifier les serveurs de noms DNS pour votre zone DNS. Chaque fois qu'une zone DNS est créée, Azure DNS alloue des serveurs de noms DNS à partir d'un pool. Une fois les serveurs de noms DNS affectés, Azure DNS crée automatiquement des enregistrements faisant autorité `NS` (ou *Name Server*) dans votre zone DNS.

Le processus de délégation pour votre domaine implique plusieurs étapes :

1. Identifier vos serveurs de noms DNS
2. Mettre à jour votre domaine parent
3. Déléguer des sous-domaines (facultatif)

Comment trouver vos serveurs de noms DNS

Le moyen le plus simple de trouver les serveurs de noms affectés à votre zone DNS est d'utiliser le portail Azure.

Comment mettre à jour votre domaine parent

Une fois votre zone DNS créée et que vous pouvez identifier vos serveurs de noms DNS, vous devez mettre à jour votre domaine parent.

Voici un processus de base que vous pouvez suivre pour mettre à jour les informations de votre domaine parent auprès de votre bureau d'enregistrement :

1. Accédez à la page de gestion de DNS de votre bureau d'enregistrement.
2. Recherchez les enregistrements `NS` existants pour votre domaine parent.
3. Remplacez les enregistrements `NS` existants par les enregistrements `NS` créés pour votre domaine par Azure DNS.

Les étapes de configuration de la délégation d'une zone DNS enfant sont similaires au processus de délégation classique. La différence principale est que vous ne travaillez pas avec votre bureau d'enregistrement pour déléguer un sous-domaine. Vous déléguez la zone DNS enfant dans le portail Azure.

Voici les étapes pour déléguer un sous-domaine :

1. Accédez à la zone DNS parent pour votre domaine dans le portail Azure.
2. Recherchez les enregistrements `NS` existants pour votre domaine parent.
3. Créez de nouveaux enregistrements `NS` pour votre zone DNS enfant (sous-domaine).

Ce qu'il faut savoir sur les jeux d'enregistrements DNS

- Tous les enregistrements d'un jeu d'enregistrements DNS doivent avoir le même nom et le même type d'enregistrement.
- Un jeu d'enregistrements DNS ne peut pas contenir deux enregistrements identiques.
- Un jeu d'enregistrements de type `CNAME` ne peut contenir qu'un seul enregistrement.
  Un enregistrement `CNAME` (ou *enregistrement Canonical NAME*) fournit un alias d'un nom de domaine à un autre. Cet enregistrement est utilisé pour fournir un autre nom pour votre domaine. L'opération DNS `lookup` tente de trouver votre domaine en réessayant l'opération `lookup` avec l'autre nom spécifié dans l'enregistrement `CNAME`.
- Vous pouvez créer un jeu d'enregistrements qui n'a aucun enregistrement. Cet ensemble est appelé *jeu d'enregistrements vide*.
- Si vous avez un jeu d'enregistrements vide pour votre domaine, ce jeu n'apparaît pas sur vos serveurs de noms Azure DNS.

Planifier des zones DNS privées Azure

Vous pouvez créer des zones DNS privées Azure en utilisant vos propres noms de domaine personnalisés au lieu des noms fournis par Azure. Avec vos propres noms de domaine personnalisés, vous pouvez adapter votre architecture de réseau virtuel en fonction des besoins de votre organisation. Vous bénéficiez de la résolution de noms pour les machines virtuelles au sein d'un réseau virtuel et entre plusieurs réseaux virtuels. Vous pouvez configurer des noms de zones DNS avec une vue *à horizon partagé*, qui permet à une zone DNS privée et une zone DNS publique de partager le même nom.

Ce qu'il faut savoir sur les avantages du DNS privé Azure

Avantage	Description
Aucune solution DNS personnalisée n'est nécessaire	Auparavant, un grand nombre de clients devaient créer des solutions DNS personnalisées pour gérer les zones DNS dans leur réseau virtuel. Vous pouvez maintenant assurer la gestion de zones DNS à l'aide de l'infrastructure Azure native. Le DNS privé Azure élimine la charge de travail liée à la création et à la gestion de solutions DNS personnalisées.
Prise en charge des types d'enregistrements DNS courants	Le DNS privé Azure prend en charge tous les types d'enregistrements DNS courants, y compris `A`, `AAAA`, `CNAME`, `MX`, `PTR`, `SOA`, `SRV` et `TXT`.
Gestion automatique des enregistrements de nom d'hôte	En plus d'héberger vos enregistrements DNS personnalisés, le DNS privé Azure gère automatiquement les enregistrements de noms d'hôte pour les machines virtuelles dans les réseaux virtuels spécifiés. Dans ce scénario, vous pouvez optimiser les noms de domaine que vous utilisez sans avoir à créer de solutions DNS personnalisées ni modifier les applications.
Résolution des noms d'hôte entre des réseaux virtuels	Contrairement aux noms d'hôtes fournis par Azure, les zones DNS privées Azure peuvent être partagées entre des réseaux virtuels. Cette fonctionnalité simplifie les scénarios de détection de services et réseaux croisés, tels que le peering de réseaux virtuels.

Outils et expérience utilisateur familiers	Pour réduire la courbe d'apprentissage, le DNS privé Azure utilise des outils Azure DNS bien connus, y compris le portail Azure, Azure PowerShell, Azure CLI, les modèles Azure Resource Manager (ARM) et l'API REST.
Prise en charge du DNS à horizon partagé	Avec le DNS privé Azure, vous pouvez créer des zones portant le même nom qui sont résolues avec des réponses différentes au sein d'un réseau virtuel et à partir de l'Internet public. Un scénario classique de DNS à horizon partagé est de fournir une version dédiée d'un service pour une utilisation au sein du réseau virtuel.
Prise en charge des régions Azure	Les zones DNS privées Azure sont disponibles dans toutes les régions Azure du cloud public Azure.

Configurer un peering de réseaux virtuels Azure

Déterminer les utilisations de l'appairage de réseaux virtuels Azure

Le moyen le plus simple et le plus rapide de connecter vos réseaux virtuels est sans doute d'utiliser l'appairage de réseaux virtuels Azure. L'appairage de réseaux virtuels vous permet de connecter deux réseaux virtuels Azure en toute transparence. Une fois les réseaux appairés, les deux réseaux virtuels fonctionnent comme un seul réseau, à des fins de connectivité.

Ce qu'il faut savoir sur l'appairage de réseaux virtuels Azure

- Il existe deux types d'appairage de réseaux virtuels Azure : *régional* et *global*.
- **L'appairage régional de réseaux virtuels** connecte des réseaux virtuels Azure qui existent dans la même région.
- **L'appairage global de réseaux virtuels** connecte des réseaux virtuels Azure qui existent dans des régions différentes
- Vous pouvez créer un appairage régional de réseaux virtuels dans la même région de cloud public Azure, dans la même région de cloud Chine, ou dans la même région de cloud Microsoft Azure Government.
- Vous pouvez créer un appairage global de réseaux virtuels dans n'importe quelle région de cloud public Azure ou dans n'importe quelle région cloud Chine.
- L'appairage global de réseaux virtuels dans différentes régions de cloud Azure Government n'est pas autorisé..

- Une fois que vous avez créé un appairage entre des réseaux virtuels, les réseaux virtuels individuels sont toujours gérés en tant que ressources distinctes.

Déterminer le transit par passerelle et la connectivité

Quand des réseaux virtuels sont appairés, vous pouvez configurer une passerelle VPN Azure dans le réseau virtuel appairé comme *point de transit*.

Ce qu'il faut savoir sur la passerelle VPN Azure

- Un réseau virtuel ne peut avoir qu'une seule passerelle VPN.
- Le transit via la passerelle est pris en charge pour l'appairage régional et global de réseaux virtuels.
- Quand vous autorisez le transit via la passerelle VPN, le réseau virtuel peut communiquer avec les ressources situées en dehors de l'appairage. Dans notre exemple, la passerelle de sous-réseau de passerelle au sein du réseau virtuel hub peut effectuer des tâches comme :
    - Utiliser un VPN de site à site pour vous connecter à un réseau local.
    - Utiliser une connexion de réseau virtuel à réseau virtuel vers un autre réseau virtuel.
    - Utiliser un VPN de point à site pour vous connecter à un client.
- Le transit par passerelle permet aux réseaux virtuels appairés de partager la passerelle et d'accéder aux ressources. Avec cette implémentation, vous n'avez pas besoin de déployer de passerelle VPN dans le réseau virtuel pair.
- Vous pouvez appliquer des groupes de sécurité réseau dans un réseau virtuel pour bloquer ou autoriser l'accès à d'autres réseaux virtuels ou sous-réseaux. Quand vous configurez l'appairage de réseaux virtuels, vous pouvez choisir d'ouvrir ou de fermer les règles de groupe de sécurité réseau entre les réseaux virtuels.

Ce qu'il faut savoir sur la création de l'appairage de réseaux virtuels

- Pour implémenter l'appairage de réseaux virtuels, votre compte Azure doit être affecté au rôle `Network Contributor` ou `Classic Network Contributor`. Vous pouvez également affecter votre compte Azure à un rôle personnalisé autorisé à effectuer les actions d'appairage nécessaires. Pour plus d'informations, consultez Autorisations.
- Pour créer un appairage, vous avez besoin de deux réseaux virtuels.
- Le deuxième réseau virtuel de l'appairage est appelé *réseau distant*.
- Initialement, les machines virtuelles de vos réseaux virtuels ne peuvent pas communiquer entre elles. Une fois l'appairage établi, les machines peuvent communiquer au sein du réseau appairé en fonction de vos paramètres de configuration.

Comment créer un appairage de réseaux virtuels

- Créez deux réseaux virtuels à inclure dans l'appairage. N'oubliez pas qu'au moins un des réseaux virtuels doit être déployé à l'aide d'Azure Resource Manager.
- Choisissez le premier réseau virtuel à utiliser dans l'appairage, puis sélectionnez **Paramètres**>**Ajouter** (appairage).
- Configurez les paramètres d'appairage pour le premier réseau virtuel. La partie supérieure de la boîte de dialogue **Ajouter un appairage** affiche les paramètres de *ce réseau virtuel*. La partie inférieure de la boîte de dialogue affiche les paramètres du réseau virtuel distant dans l'appairage.
- **Nom du lien d'appairage** : fournissez un nom pour identifier l'appairage sur ce réseau virtuel. Le nom doit être unique au sein du réseau virtuel.
- **Trafic vers un réseau virtuel distant** : spécifiez comment contrôler le trafic vers le réseau virtuel distant.
    - **Autoriser** : autoriser la communication entre les ressources connectées à vos deux réseaux virtuels au sein du réseau appairé.
    - **Bloquer** : bloquer tout le trafic vers le réseau virtuel distant. Vous pouvez toujours autoriser un trafic vers le réseau virtuel distant si vous ouvrez explicitement le trafic via une règle de groupe de sécurité réseau.
- **Trafic transféré à partir d'un réseau virtuel distant** : spécifiez comment contrôler le trafic qui provient de l'extérieur de votre réseau virtuel distant.
    - **Autoriser** : transférer le trafic extérieur du réseau virtuel distant vers ce réseau virtuel au sein de l'appairage. Ce paramètre vous permet de transférer le trafic de l'extérieur du réseau virtuel distant, notamment le trafic d'une appliance virtuelle réseau, vers ce réseau virtuel.
    - **Bloquer** : bloquer le transfert du trafic externe du réseau virtuel distant vers ce réseau virtuel au sein de l'appairage. Là encore, certains trafics peuvent toujours être transférés en ouvrant explicitement le trafic via une règle de groupe de sécurité réseau. Lorsque vous configurez le transfert du trafic entre des réseaux virtuels via une passerelle VPN Azure, ce paramètre n'est pas applicable.
- **Passerelle de réseau virtuel ou serveur de routage** : spécifiez si votre appairage de réseaux virtuels doit utiliser une passerelle VPN Azure. La valeur par défaut consiste à ne pas utiliser de passerelle VPN (aucune).

Configurez les paramètres d'appairage pour votre réseau virtuel distant.

Dans le portail Azure, vous configurez le réseau virtuel distant dans l'appairage dans la boîte de dialogue **Ajouter un appairage**. La partie inférieure affiche les paramètres du réseau virtuel distant. Les paramètres sont similaires aux paramètres décrits pour le premier réseau virtuel.

Comment vérifier le statut de votre appairage ?

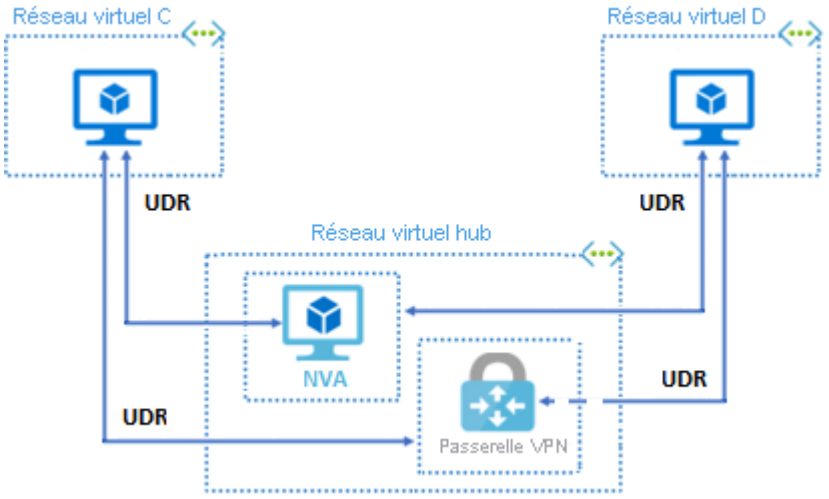
- Pour le déploiement avec Azure Resource Manager, les deux conditions d'état principales sont **Initié** et **Connecté**. Pour le modèle de déploiement classique, la condition **Mise à jour** de l'état est également utilisée.
- Quand vous créez l'appairage initial *vers* le deuxième réseau virtuel (distant) à partir du premier réseau virtuel, l'état de l'appairage pour le premier réseau virtuel indique **Initié**.
- Lorsque vous créez l'appairage suivant *du* deuxième réseau virtuel vers le premier réseau virtuel, l'état de l'appairage pour le premier réseau virtuel et les réseaux virtuels distants indique **Connecté**. Dans le portail Azure, vous pouvez voir que l'état de la première modification du réseau virtuel passe de **Initié** à **Connecté**.

Étendre l'appairage avec des routes définies par l'utilisateur et le chaînage de services

Le peering de réseaux virtuels n'est pas transitif. Les fonctionnalités de communication d'un appairage sont disponibles uniquement pour les réseaux virtuels et les ressources de l'appairage. D'autres mécanismes doivent être utilisés pour autoriser le trafic vers et depuis les ressources et les réseaux en dehors du réseau de l'appairage privé.

Éléments à savoir sur l'extension de l'appairage

Le diagramme suivant montre un réseau virtuel hub-and-spoke avec une appliance virtuelle réseau et une passerelle VPN. Le réseau hub-and-spoke est accessible à d'autres réseaux virtuels via des itinéraires définis par l'utilisateur et un chaînage de services.



Mécanisme	Description
Réseau hub-and-spoke	Quand vous déployez un réseau de type hub-and-spoke, le réseau virtuel hub peut héberger des composants d'infrastructure tels que l'appliance virtuelle réseau (NVA) ou la passerelle VPN Azure. Tous les réseaux virtuels spoke peuvent ensuite être homologués avec le réseau virtuel hub. Le trafic peut transiter via des appliances virtuelles réseau ou des réseaux VPN sur le réseau virtuel hub.
Itinéraire défini par l'utilisateur (UDR)	Le peering de réseaux virtuels permet de définir le tronçon suivant dans un itinéraire défini par l'utilisateur sur l'adresse IP d'une machine virtuelle du réseau virtuel appairé ou une passerelle VPN.
Chaînage de services	Le chaînage de services vous permet de définir des itinéraires définis par l'utilisateur. Ces itinéraires dirigent le trafic d'un réseau virtuel vers une passerelle NVA ou VPN.

Déterminer les utilisations d'Azure VPN Gateway

Une passerelle VPN est un type spécifique de passerelle de réseau virtuel utilisée pour envoyer du trafic chiffré entre votre réseau virtuel Azure et un emplacement local sur l'Internet public. Une passerelle VPN peut aussi être utilisée pour envoyer du trafic chiffré entre vos réseaux virtuels Azure sur le réseau Microsoft.

Ce qu'il faut savoir sur les passerelles VPN

- Quand vous implémentez une passerelle VPN, le service VPN intercepte vos données et applique un chiffrement avant qu'elles n'atteignent Internet.
- Le service VPN utilise une voie sécurisée (appelée *tunnel VPN*) pour le déplacement de vos données entre votre appareil et Internet. Le tunnel VPN est ce qui permet votre connexion sécurisée à Internet.
- Un réseau virtuel ne peut avoir qu'une seule passerelle VPN.
- Vous pouvez créer plusieurs connexions à la même passerelle VPN.
- Lorsque vous créez plusieurs connexions à la même passerelle VPN, tous les tunnels VPN partagent la bande passante de passerelle disponible.
- Une passerelle VPN peut être déployée dans des zones de disponibilité Azure pour bénéficier de la résilience, de l'extensibilité et d'une disponibilité plus élevée. Les zones de disponibilité Azure permettent de séparer physiquement et logiquement les passerelles au sein d'une région, tout en protégeant la connectivité de votre réseau local à Azure contre les défaillances au niveau des zones.

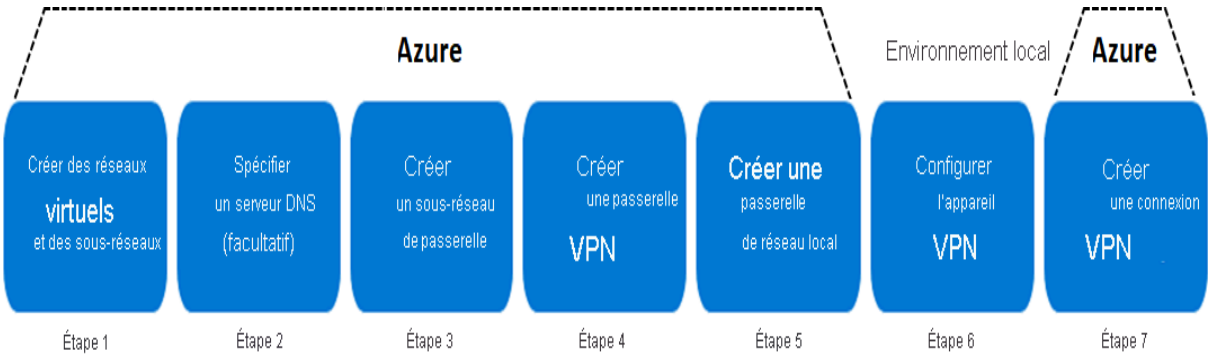
Passerelle de réseau virtuel

Une passerelle de réseau virtuel est composée de deux machines virtuelles ou plus, déployées sur un sous-réseau spécifique que vous créez, appelé *sous-réseau de passerelle*.

- Les machines virtuelles sont créées quand vous créez la passerelle de réseau virtuel.
- Les machines virtuelles contiennent des tables de routage et exécutent des services de passerelle spécifiques.
- Vous ne pouvez pas configurer directement les machines virtuelles qui font partie d'une passerelle de réseau virtuel.

Créer des connexions de site à site

L'organigramme suivant met en évidence les sept grandes étapes de cette configuration. Six des sept étapes sont effectuées dans Azure et une est effectuée localement.



Le processus complet de création d'une passerelle VPN pour une connexion de site à site peut prendre jusqu'à 45 minutes.

Ce qu'il faut savoir sur la configuration d'une connexion de site à site

- **Étape 6 : Configurer l'appareil VPN**. L'étape qui s'effectue localement est nécessaire seulement lors de la configuration d'une connexion de site à site. Si vous suivez ces étapes pour créer un autre type de configuration de passerelle VPN, vous n'aurez peut-être pas besoin d'effectuer cette étape.

Ce qu'il faut savoir sur le sous-réseau de passerelle

- Vous déployez une passerelle dans votre réseau virtuel en ajoutant un sous-réseau de passerelle.
- Votre sous-réseau de passerelle doit être nommé *GatewaySubnet*.
- Le sous-réseau de passerelle contient les adresses IP utilisées par vos ressources et vos services de passerelle de réseau virtuel.

- Quand vous créez votre sous-réseau de passerelle, les machines virtuelles de la passerelle sont déployées dans le sous-réseau de passerelle et configurées avec les paramètres requis de la passerelle VPN.

Ce qu'il faut savoir sur le type de passerelle VPN

- Les **VPN basés sur des routes** utilisent des *routes* dans le transfert ou la table de routage des adresses IP pour diriger les paquets dans leurs interfaces de tunnel correspondantes. Les interfaces de tunnel chiffrent ou déchiffrent ensuite les paquets en entrée et en sortie des tunnels VPN. La stratégie (ou le sélecteur de trafic) pour les VPN basés sur des routes est configurée en tant que « universel » (ou générique).
    - La plupart des configurations de passerelle VPN nécessitent un VPN basé sur des routes.
    - Utilisez une passerelle basée sur des routes quand votre réseau virtuel coexiste avec une passerelle Azure ExpressRoute ou si vous devez utiliser le protocole IKEv2.
- Les **VPN basés sur des stratégies** chiffrent et dirigent les paquets via des tunnels IPsec en fonction des stratégies IPsec. Les stratégies sont configurées avec les combinaisons de préfixes d'adresses entre votre réseau local et le réseau virtuel Azure. La stratégie (ou le sélecteur de trafic) est définie sous la forme d'une liste d'accès dans la configuration d'appareil VPN.

  Gardez à l'esprit les limitations suivantes des VPN basés sur des stratégies :
    - Un VPN basé sur des stratégies peut être utilisé seulement sur la référence SKU de passerelle De base. Le type de VPN basé sur des stratégies n'est pas compatible avec les autres références SKU de passerelle.
    - Quand vous utilisez un VPN basé sur des stratégies, vous ne pouvez avoir qu'un seul tunnel VPN.
    - Vous pouvez utiliser des VPN basés sur des stratégies seulement pour des connexions S2S et seulement pour certaines configurations.

Déterminer la référence SKU de passerelle et la génération

Les tableaux identifient les informations suivantes pour chaque type et génération de référence SKU :

- **Tunnels** : le nombre maximal de tunnels de site à site (S2S) et de réseau à réseau virtuel qui peuvent être créés pour la référence SKU.
- **Connexions** : le nombre maximal de connexions IKEv2 de point à site (P2S) qui peuvent être créées pour la référence SKU.
- **Point de référence du débit agrégé** : le point de référence du débit agrégée est basé sur les mesures de plusieurs tunnels VPN agrégés via une même passerelle. Le point de référence du débit agrégé pour une passerelle VPN

est S2S + P2S combinés. Le point de référence du débit agrégé n'est pas garanti en raison des conditions du trafic Internet et du comportement de votre application.

Créer la passerelle de réseau local

La passerelle de réseau local fait généralement référence à l'emplacement local. Pour créer une passerelle locale, **vous spécifiez un nom pour le site ainsi que l'adresse IP ou le nom de domaine complet de l'appareil VPN local pour la connexion**. **Vous spécifiez aussi les préfixes des adresses IP à router via la passerelle VPN vers l'appareil VPN**. **Les préfixes d'adresses que vous spécifiez sont les préfixes situés sur le réseau local**.

Ce qu'il faut savoir sur la création d'une passerelle de réseau local

- **Nom** : spécifiez un nom pour votre site. Azure utilise ce nom pour faire référence à votre passerelle de réseau local.
- **Point de terminaison** : spécifiez l'adresse IP ou le nom de domaine complet de l'appareil VPN local pour la connexion.
- **Adresse IP**. Identifiez l'adresse IP publique de votre passerelle de réseau local.
- **Espace d'adressage**. Spécifiez une ou plusieurs plages d'adresses IP (en notation CIDR) pour définir l'espace d'adressage de votre réseau local.
  Notes
  Si vous envisagez d'utiliser cette passerelle de réseau local dans une connexion activée avec le protocole BGP (Border Gateway Protocol), le préfixe minimal que vous devez déclarer est l'adresse d'hôte de l'adresse IP de votre pair BGP sur votre appareil VPN.
- **Configurer les paramètres BGP** : si nécessaire, cochez cette case pour configurer les paramètres BGP pour la passerelle de réseau local.

Ce qu'il faut savoir sur la configuration de votre appareil VPN

- Consultez la liste des appareils validés pour y rechercher votre appareil. Pour visualiser la liste, consultez Appareils VPN validés et guides de configuration des appareils.
  Notes
  Si votre appareil n'est pas présent dans la liste des appareils VPN validés, votre appareil peut néanmoins fonctionner. Contactez le fabricant de votre appareil pour obtenir une prise en charge et des instructions de configuration.
- Pour configurer votre appareil VPN, vous avez besoin des informations suivantes :
  - **Une clé partagée**. Cette clé est la clé partagée que vous avez spécifiée lors de la création de la connexion VPN.
  - **Adresse IP publique de votre passerelle VPN**. L'adresse IP peut être nouvelle ou existante.

- Des **scripts de configuration** sont disponibles pour certains appareils. Consultez Télécharger les scripts de configuration d'appareil VPN pour les connexions VPN S2S pour rechercher un script téléchargeable pour votre appareil VPN.

Configurer Azure ExpressRoute et Azure Virtual WAN

Déterminer les utilisations d'Azure ExpressRoute

Azure ExpressRoute vous permet d'étendre vos réseaux locaux dans le cloud Microsoft. La connexion est facilitée par un fournisseur de connectivité. Avec ExpressRoute, vous pouvez établir des connexions aux services de cloud computing Microsoft comme Microsoft Azure, Microsoft 365 et les applications Microsoft Dynamics CRM.
Le réseau Microsoft opère les connexions primaires et secondaires des circuits Azure ExpressRoute en mode actif/actif. Les administrateurs peuvent forcer leurs connexions redondantes d'un circuit ExpressRoute à opérer en mode actif/passif.

Azure ExpressRoute est pris en charge dans tous les emplacements et régions Azure.

Ce qu'il faut savoir sur Azure ExpressRoute

- Microsoft utilise le protocole BGP (Border Gateway Protocol) pour échanger des routes entre votre réseau local, vos instances dans Azure et les adresses publiques Microsoft afin de fournir une connectivité de couche 3. Plusieurs sessions BGP sont créées pour les différents profils de trafic.
- Chaque circuit ExpressRoute se compose de deux connexions à deux routeurs MSEE (Microsoft Enterprise Edge) entre le fournisseur de connectivité et la périphérie de votre réseau. Microsoft nécessite une double connexion BGP entre le fournisseur de connectivité et la périphérie de votre réseau, une pour chaque routeur MSEE. Les connexions BGP doubles assurent la redondance.
- Les connexions ExpressRoute permettent d'accéder aux services Microsoft Azure, aux services Microsoft 365 et à Microsoft Dynamics CRM. Microsoft 365 étant conçu pour être accessible de façon fiable et sécurisée sur Internet, ExpressRoute nécessite l'autorisation de Microsoft.
- Vous vous connectez à Microsoft dans un de nos emplacements d'appairage et vous accédez à toutes les zones de la région géopolitique.
  Supposons que vous vous connectiez à Microsoft à Amsterdam par le biais d'ExpressRoute. Vous pouvez accéder à tous les services cloud de Microsoft hébergés dans les régions Europe Nord et Europe Ouest.
- La fonctionnalité du module complémentaire Premium d'ExpressRoute vous permet d'étendre la connectivité au-delà des frontières géopolitiques.

Supposons que vous vous connectiez à Microsoft à Amsterdam par le biais d'ExpressRoute. Quand vous activez la fonctionnalité du module complémentaire Premium d'ExpressRoute, vous pouvez accéder à tous les services cloud de Microsoft hébergés dans toutes les régions du monde, à l'exception des clouds nationaux.

- **ExpressRoute Global Reach** vous permet d'échanger des données entre vos sites locaux en connectant vos circuits ExpressRoute.
  Supposons que vous disposiez d'un centre de données privé en Californie connecté à ExpressRoute dans la Silicon Valley. Vous configurez un autre centre de données privé au Texas connecté à ExpressRoute à Dallas et activez ExpressRoute Global Reach. Vous pouvez connecter vos centres de données privés entre eux au moyen de deux circuits ExpressRoute. Le trafic entre vos centres de données transite alors par le réseau de Microsoft.
- Vous pouvez acheter des circuits ExpressRoute pour un large éventail de bandes passantes. Contactez votre fournisseur de connectivité pour déterminer les bandes passantes prises en charge.
- Microsoft propose plusieurs options tarifaires pour ExpressRoute.

Faire coexister des réseaux de site à site et Azure ExpressRoute

Azure ExpressRoute est une connexion directe et privée à partir de votre WAN (elle ne transite pas par l'Internet public) vers les services Microsoft, y compris Azure. Le trafic VPN site à site transite chiffré par l'Internet public. La possibilité de configurer des connexions VPN site à site et ExpressRoute pour le même réseau virtuel présente plusieurs avantages.

Ce qu'il faut savoir sur les modèles de connexion ExpressRoute

Modèle de connexion	Fonctionnement	Prise en charge des couches
Colocalisation avec un échange cloud	Si vous êtes colocalisé dans une installation avec un échange cloud, vous commandez des interconnexions virtuelles au cloud Microsoft par le biais de l'échange Ethernet du fournisseur de colocalisation.	Les fournisseurs de colocalisation offrent des interconnexions de couche 2 ou des interconnexions de couche 3 gérées entre votre infrastructure dans l'installation de colocalisation et le cloud Microsoft.

Connexions Ethernet point à point	Vous connectez vos centres de données et bureaux locaux au cloud Microsoft par le biais de liaisons Ethernet point à point.	Les fournisseurs Ethernet point à point offrent des connexions de couche 2 ou des connexions de couche 3 gérées entre votre site et le cloud Microsoft.
Réseaux universels (IPVPN)	Vous intégrez votre réseau étendu au cloud Microsoft. Les fournisseurs IPVPN, généralement un VPN MPLS (Multiprotocol Label Switching), offrent une connectivité Any-to-Any entre vos succursales et vos centres de données. Le cloud Microsoft peut être interconnecté à votre réseau étendu afin qu'il apparaisse comme n'importe quelle autre succursale.	Les fournisseurs de réseaux étendus offrent généralement une connectivité de couche 3 gérée.

Ce qu'il faut savoir sur les connexions intersites

Plusieurs services Azure peuvent prendre en charge des configurations de connexions intersites diverses.

Connexion	Services Azure	Bande passante	Protocoles	Scénarios
Réseau virtuel et point à site (VPN utilisateur)	Services Azure IaaS, Machines virtuelles Azure	Basé sur la référence SKU de passerelle	actif / passif	*Environnements de développement, test et lab pour les services cloud* *Environnements de développement, test et lab pour les machines virtuelles*

Réseau virtuel et site à site	Services Azure IaaS, Machines virtuelles Azure	En règle générale < 1 Gbit/s (agrégation)	actif / passif actif / actif	*Environnements de développement, test et lab* *Charges de travail de production à petite échelle et machines virtuelles*
Circuit ExpressRoute	Services Azure IaaS et PaaS, Services Microsoft 365	De 50 Mbits/s jusqu'à 100 Gbits/s	actif/actif (recommandé) actif/passif (forcé manuellement)	*Charges de travail de niveau entreprise et stratégiques* *Solutions de Big Data*

Déterminer les utilisations d'Azure Virtual WAN

Azure Virtual WAN (Wide Area Network) est un service réseau qui fournit une connectivité optimisée et automatisée des branches à Azure et via Azure. Les régions Azure servent de hubs auxquels vous pouvez connecter vos branches. Vous utilisez le backbone Azure pour connecter des branches et profiter de la connectivité de branche à réseau virtuel.

Ce qu'il faut savoir sur Azure Virtual WAN

- Azure Virtual WAN regroupe de nombreux services de connectivité cloud Azure, comme un VPN site à site (S2S), un VPN utilisateur (P2S) et Azure ExpressRoute, dans une même interface opérationnelle.
- La connectivité aux réseaux virtuels Azure est établie à l'aide de connexions de réseau virtuel.
- L'architecture réseau de transit mondial est basée sur un modèle de connectivité hub-and-spoke. Le *hub* réseau hébergé dans le cloud permet une connectivité transitive entre les points de terminaison qui peuvent être répartis sur différents types de *spokes*.
- Il existe deux types de réseaux étendus (WAN) :
    - **De base** : un WAN virtuel de base ne peut être implémenté que dans une connexion VPN S2S.
    - **Standard** : un WAN virtuel standard peut être implémenté avec Azure ExpressRoute et un VPN utilisateur (P2S). Vous pouvez également

utiliser un WAN standard avec un VPN S2S, un inter-hub et une connexion de réseau virtuel à réseau virtuel transitant par le hub virtuel.

- Vous pouvez trouver des partenaires qui prennent en charge l'automatisation de la connectivité avec un VPN Azure Virtual WAN. Pour plus d'informations, consultez Partenaires, régions et localisations de hub virtuel pour Virtual WAN.

Configurer le routage et les points de terminaison réseau

Ce que vous devez savoir sur les routes système

- Azure utilise des routes système pour contrôler le trafic des machines virtuelles dans plusieurs scénarios :
  - Trafic entre des machines virtuelles dans le même sous-réseau
  - Trafic entre des machines virtuelles dans différents sous-réseaux du même réseau virtuel
  - Trafic des machines virtuelles vers Internet
- Une table de routage contient un ensemble de règles (appelées *routes*), qui spécifie comment les paquets doivent être routés dans un réseau virtuel.
- Les tables de routage enregistrent des informations sur les routes système, où les tables sont associées aux sous-réseaux.
- Chaque paquet quittant un sous-réseau est géré en fonction de la table de routage associée.
- Les paquets sont mis en correspondance avec les routes en utilisant la destination. La destination peut être une adresse IP, une passerelle de réseau virtuel, une appliance virtuelle ou Internet.
- Quand une route correspondante est introuvable, le paquet est supprimé.

Ce que vous devez savoir sur les routes définies par l'utilisateur

- Les routes définies par l'utilisateur contrôlent le trafic réseau en définissant des routes qui spécifient le *tronçon suivant* du flux du trafic.
- Le tronçon suivant peut être l'une des cibles suivantes :
  - Passerelle de réseau virtuel
  - Réseau virtuel
  - Internet
  - Appliance virtuelle réseau
- À l'instar des routes système, les routes définies par l'utilisateur accèdent également aux tables de routage.
- Chaque table de routage peut être associée à plusieurs sous-réseaux.
- Chaque sous-réseau peut être associé à une seule table de routage.
- La création de tables de routage dans Microsoft Azure n'occasionne aucuns frais.

Déterminer les utilisations des points de terminaison de service

Avec les points de terminaison de service, le trafic de service change pour utiliser des adresses privées de réseau virtuel en tant qu'adresses IP source lors de l'accès au service Azure à partir d'un 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.

Ce que vous devez savoir sur les points de terminaison de service

- Les points de terminaison de service peuvent étendre votre identité de réseau virtuel à vos services Azure pour sécuriser vos ressources de service.
- Vous sécurisez vos ressources de service Azure sur votre réseau virtuel à l'aide de règles de réseau virtuel.
- Les règles de réseau virtuel peuvent supprimer l'accès Internet public aux ressources et autoriser le trafic uniquement à partir de votre réseau virtuel.
- Les points de terminaison de service acheminent toujours le trafic de service directement à partir de votre réseau virtuel vers le service sur le réseau principal de Microsoft Azure.
- Les points de terminaison de service sont configurés via le sous-réseau. La gestion des points de terminaison n'entraîne aucune surcharge supplémentaire.

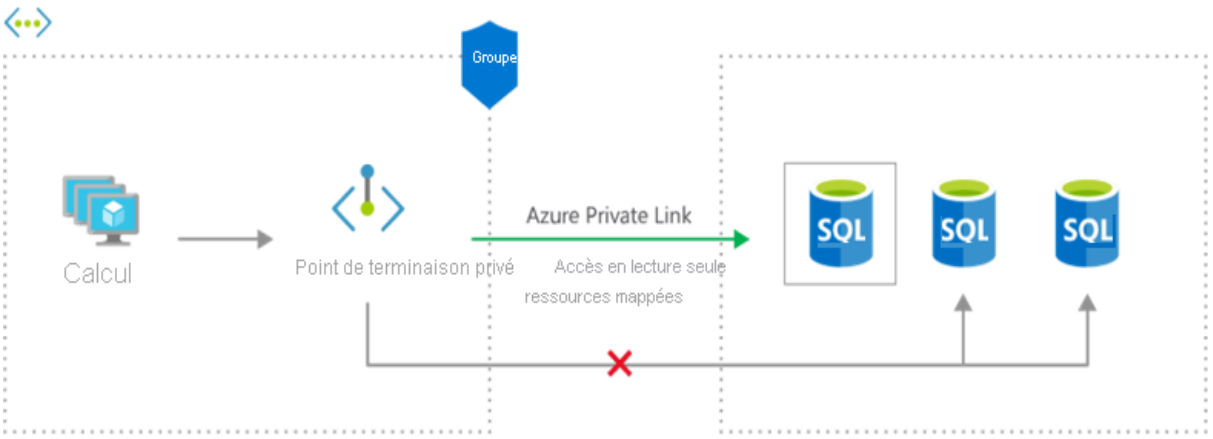
Identifier les utilisations des liaisons privées

Azure Private Link fournit une connectivité privée entre un réseau virtuel et la plateforme Azure en tant que service (PaaS), appartenant à un client ou à des services partenaires Microsoft. Il simplifie l'architecture réseau et sécurise la connexion entre les points de terminaison dans Azure en éliminant l'exposition des données à l'internet public.

Ce que vous devez savoir sur Azure Private Link

- Azure Private Link conserve l'ensemble du trafic sur le réseau mondial Microsoft. Il n'y a pas d'accès à l'Internet public.
- Private Link est mondial et n'a pas de restrictions régionales. Vous pouvez vous connecter en privé à des services s'exécutant dans d'autres régions Azure.
- Le mappage de votre réseau à un point de terminaison privé permet de délivrer les services sur Azure dans votre réseau virtuel privé.

- Private Link peut délivrer vos propres services de façon privée dans les réseaux virtuels de votre client.
- Tout le trafic vers le service peut être routé par le biais du point de terminaison privé. Aucune passerelle, aucun appareil NAT, aucune connexion Azure ExpressRoute ou VPN ni aucune adresse IP publique ne sont nécessaires.



Configurer Azure Load Balancer

Déterminer les usages d'Azure Load Balancer

L'équilibrage de charge Azure offre une haute disponibilité et des performances réseau élevées pour vos applications. Les administrateurs utilisent l'équilibrage de charge pour distribuer efficacement le trafic réseau entrant parmi les ressources et les serveurs du back-end. Un équilibreur de charge est implémenté à l'aide de règles d'équilibrage de charge et de sondes d'intégrité.

Ce qu'il faut savoir sur Azure Load Balancer

- Azure Load Balancer peut être utilisé pour les scénarios entrants et sortants.
- Vous pouvez implémenter un équilibreur de charge **public** ou **interne**, ou utiliser les deux types dans une configuration combinée.
- Pour implémenter un équilibreur de charge, vous devez configurer quatre composants :
    - Configuration IP front-end
    - Pools de back-ends
    - Sondes d'intégrité
    - Règles d'équilibrage de la charge
- La configuration front-end spécifie l'IP publique ou l'IP interne à laquelle votre équilibreur de charge répond.
- Les pools de back-ends sont vos services et ressources, y compris Machines Virtuelles Azure ou les instances dans Azure Virtual Machine Scale Sets.

- Les règles d’équilibrage de charge déterminent comment le trafic est distribué aux ressources de back-end.
- Les sondes d’intégrité garantissent l’intégrité des ressources du back-end.
- Load Balancer peut être mis à l’échelle jusqu’à plusieurs millions de flux d’application TCP et UDP.

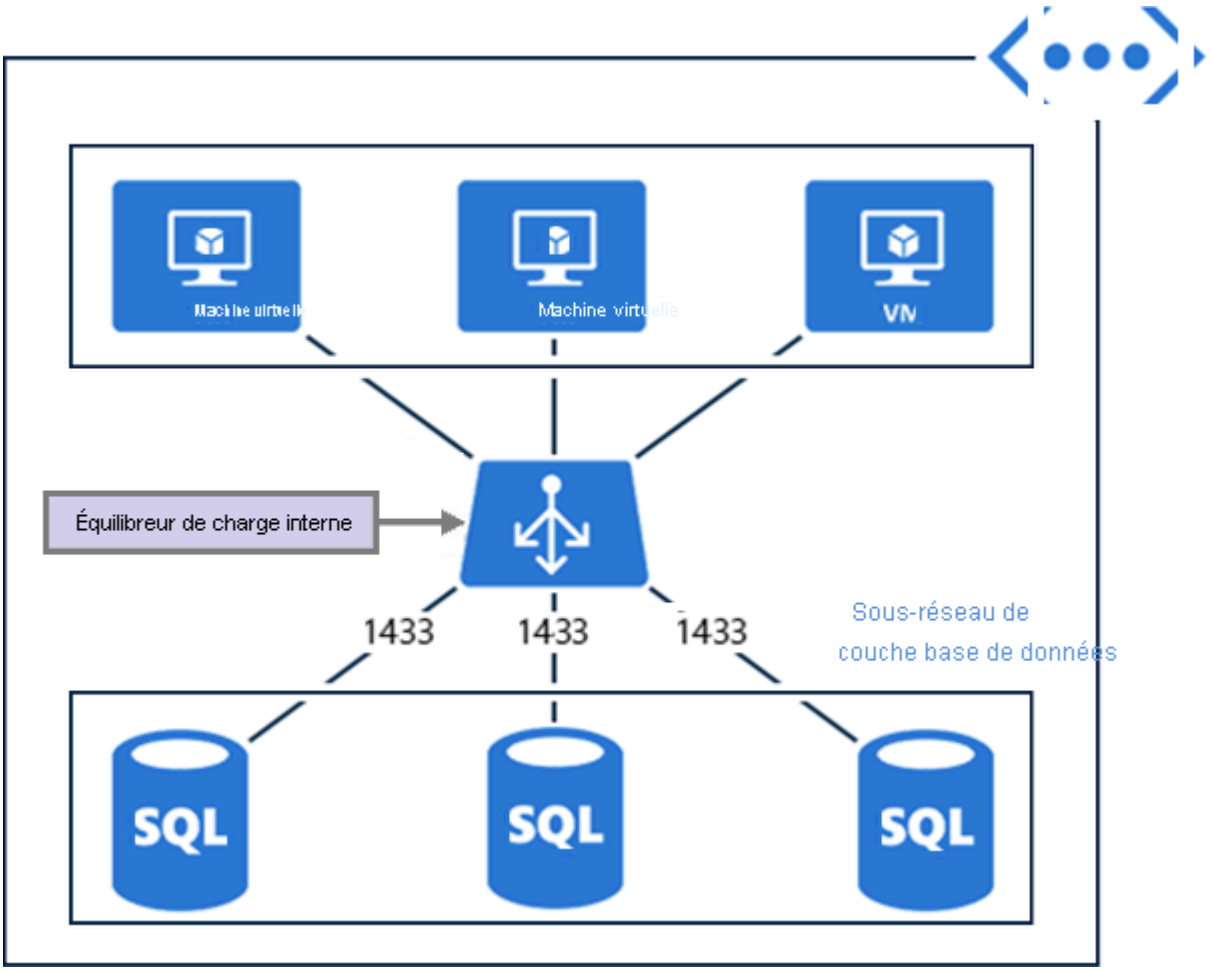
Implémenter un équilibreur de charge public

Les administrateurs utilisent des équilibreurs de charge publics pour mapper les adresses IP publiques et les numéros de port du trafic entrant aux adresses IP privées et aux numéros de port de machines virtuelles. Le mappage peut également être configuré pour le trafic de réponse provenant des machines virtuelles.

Les règles d’équilibrage de charge servent à spécifier comment distribuer des types de trafic spécifiques parmi plusieurs services ou machines virtuelles. Vous pouvez adopter cette approche pour partager la charge du trafic de requêtes web entrantes entre plusieurs serveurs web.

Implémenter un équilibreur de charge interne

Les administrateurs utilisent des équilibreurs de charge internes pour diriger le trafic vers des ressources qui résident dans un réseau virtuel, ou vers des ressources qui utilisent un VPN pour accéder à l’infrastructure Azure. Dans cette configuration, les adresses IP de front-end et les réseaux virtuels ne sont jamais directement exposés à un point de terminaison Internet.



Ce qu'il faut savoir sur les références SKU Azure Load Balancer

- Standard Load Balancer est le produit le plus récent. Il s'agit essentiellement d'un surensemble de Basic Load Balancer.
- La référence SKU Standard offre un ensemble de fonctionnalités étendu et plus précis que la référence SKU De base.
- Vous pouvez mettre à niveau la référence SKU De base vers la référence SKU Standard. Toutefois, les nouvelles conceptions et architectures doivent utiliser la référence SKU De base.
- La référence SKU Passerelle prend en charge des scénarios de haute performance et de haute disponibilité avec des appliances virtuelles réseau tierces.

Comparaison des fonctionnalités des références SKU De base et Standard

Fonctionnalité	Référence SKU De base	Référence SKU standard
Sondes d'intégrité	HTTP, TCP	HTTPS, HTTP, TCP

Zones de disponibilité	Non disponible	Front-ends redondants interzones et zonaux pour le trafic entrant et sortant
Plusieurs serveurs frontaux	Entrant uniquement	Trafic entrant et sortant
Sécurité	- Ouverts par défaut - (Facultatif) Contrôle via des groupes de sécurité réseau (NSG)	- Fermeture aux flux entrants, sauf autorisation d'un groupe NSG - Le trafic interne du réseau virtuel vers l'équilibreur de charge interne est autorisé

Créer des pools de back-ends

Chaque équilibreur de charge a un ou plusieurs pools de back-ends qui sont utilisés pour distribuer le trafic. Les pools de back-end contiennent les adresses IP des cartes réseau virtuelles connectées à votre équilibreur de charge. Vous configurez ces paramètres de pool dans le portail Azure.

Ce qu'il faut savoir sur les pools de back-ends

- La référence SKU De base autorise jusqu'à 300 pools, et la référence SKU Standard autorise jusqu'à 1000 pools.
- Lorsque vous configurez les pools de back-ends, vous pouvez vous connecter à des groupes à haute disponibilité, à des machines virtuelles ou à Microsoft Azure Virtual Machine Scale Sets.
- Pour la référence SKU De base, vous pouvez sélectionner des machines virtuelles dans un groupe à haute disponibilité unique ou des machines virtuelles dans une instance d'Azure Virtual Machine Scale Sets.
- Pour la référence SKU Standard, vous pouvez sélectionner des machines virtuelles ou des instances Virtual Machine Scale Sets dans un réseau virtuel unique. Votre configuration peut inclure une combinaison de machines virtuelles, de groupes à haute disponibilité et d'instances Virtual Machine Scale Sets.

Créer des sondes d'intégrité

Une sonde d'intégrité permet à votre équilibreur de charge de superviser l'état de votre application. La sonde ajoute ou supprime dynamiquement des machines virtuelles de la rotation de votre équilibreur de charge en fonction de leur réponse aux vérifications d'intégrité. Lorsqu'une sonde ne répond pas, l'équilibreur de charge n'envoie plus de nouvelles connexions à l'instance défaillante.

Choses à savoir sur les sondes d'intégrité

- Dans une **sonde HTTP**, l'équilibreur de charge sonde vos points de terminaison de pool de back-ends toutes les 15 secondes. Une instance de machine virtuelle est considérée comme *saine* si elle répond avec un message HTTP 200 dans les délais spécifiés (le délai par défaut est de 31 secondes). Si un état autre que HTTP 200 est retourné, l'instance est considérée comme *non saine*, et la sonde échoue.
- Une **sonde TCP** s'appuie sur l'établissement d'une session TCP réussie sur un port défini. Si l'écouteur spécifié sur la machine virtuelle existe, l'exécution de la sonde réussi. Si la connexion est refusée, la sonde échoue.
- Pour configurer une sonde, vous spécifiez des valeurs pour les paramètres suivants :
    - **Port** : port de back-end
    - **URI** : URI pour demander l'état d'intégrité au back-end
    - **Intervalle** : durée entre les tentatives de la sonde (la valeur par défaut est de 15 secondes)
    - **Seuil non sain** : nombre d'échecs qui doivent se produire pour que l'instance soit considérée comme non saine
- Une **sonde d'agent invité** est une troisième option qui utilise l'agent invité à l'intérieur de la machine virtuelle. Cette option n'est pas recommandée lorsqu'une configuration de sonde personnalisée HTTP ou TCP est possible.

Points à connaître sur les règles d'équilibrage de charge

- Pour configurer une règle d'équilibrage de charge, vous devez disposer d'un front-end, d'un back-end et d'une sonde d'intégrité pour votre équilibreur de charge.
- Pour définir une règle dans le portail Azure, vous configurez plusieurs paramètres :
    - **Version IP** (IPv4 ou IPv6)
    - **Adresse IP front-end**, **Port* et **Protocole** (TCP ou UDP)
    - **Pool de back-ends** et **Port de back-end**
    - **Sonde d'intégrité**
    - **Persistance de session**
- Par défaut, Azure Load Balancer répartit le trafic réseau équitablement sur plusieurs machines virtuelles.
  Azure Load Balancer utilise un hachage à cinq tuples pour mapper le trafic aux serveurs disponibles. Le tuple se compose de l'adresse IP source, du port source, de l'adresse IP de destination, du port de destination et du type de protocole. L'équilibreur de charge fournit l'adhérence uniquement dans une session de transport.
- La **persistance de sessions** spécifie comment gérer le trafic en provenance d'un client. Par défaut, les requêtes successives d'un client sont gérées par n'importe quelle machine virtuelle de votre pool.

Vous pouvez modifier le comportement de persistance de session comme suit :
    - **Aucune (par défaut)** : n'importe quelle machine virtuelle peut gérer la requête.
    - **Adresse IP cliente** : les requêtes successives provenant de la même adresse IP cliente sont gérées par la même machine virtuelle.
    - **Adresse IP cliente et protocole** : les requêtes successives provenant de la même combinaison adresse IP cliente/protocole sont gérées par la même machine virtuelle.
- Vous pouvez utiliser les règles d'équilibrage de charge en combinaison avec les règles NAT.

Configurer Azure Application Gateway

Implémenter une passerelle Azure Application Gateway

Les administrateurs utilisent Azure Application Gateway pour gérer les demandes des applications clientes vers leurs applications web. Une passerelle applicative écoute le trafic entrant à destination d'applications web et vérifie les messages envoyés via des protocoles comme HTTP. Les règles de passerelle dirigent le trafic vers les ressources d'un pool back-end.

Ce qu'il faut savoir sur l'acheminement du trafic

- Azure Application Gateway propose deux méthodes principales d'acheminement du trafic :
    - L'**acheminement basé sur le chemin** envoie des requêtes avec différents chemins d'URL à différents pools de serveurs back-end.
    - L'acheminement **multisite** configure plusieurs applications web sur la même instance de passerelle applicative.
- Vous pouvez configurer votre passerelle applicative pour qu'elle **redirige** le trafic.
  Application Gateway peut rediriger le trafic reçu sur un écouteur vers un autre écouteur ou vers un site externe. Cette approche est couramment utilisée par les applications web afin de rediriger automatiquement les requêtes HTTP pour qu'elles communiquent via HTTPS. La redirection garantit que toutes les communications entre votre application web et les clients se produisent sur un chemin chiffré.
- Vous pouvez implémenter Application Gateway pour **réécrire les en-têtes HTTP**.
  Les en-têtes HTTP permettent au client et au serveur de passer des informations de paramètre dans la requête ou la réponse. Dans ce scénario, vous pouvez traduire les URL ou interroger des paramètres de chaîne, et modifier des en-têtes de requête et de réponse. Ajoutez des conditions pour

vous assurer que les URL ou les en-têtes sont réécrits uniquement pour certaines conditions.
- Application Gateway vous permet de créer des pages d'erreur personnalisées au lieu d'afficher les pages d'erreur par défaut. Vous pouvez utiliser votre marque et votre mise en page personnalisées à l'aide d'une page d'erreur personnalisée.

Configurer des composants Azure Application Gateway

Azure Application Gateway dispose d'une série de composants qui s'associent pour acheminer les requêtes vers un pool de serveurs web et pour vérifier l'intégrité de ces serveurs web. Ces composants incluent l'adresse IP front-end, les pools back-end, les règles d'acheminement, les sondes d'intégrité et les écouteurs. En option, la passerelle peut également implémenter un pare-feu.

Éléments à connaître concernant les composants Application Gateway

- **L'adresse IP front-end** reçoit les requêtes clientes (adresse IP publique ou privée)
- Un **pare-feu** facultatif vérifie la présence de menaces courantes dans le trafic entrant avant que les requêtes n'atteignent les écouteurs.
- Un ou plusieurs **écouteurs** reçoivent le trafic et acheminent les requêtes vers le pool back-end. (Un écouteur de base route uniquement une requête selon le chemin de l'URL. Un écouteur multisite peut également acheminer les requêtes à l'aide de l'élément hostname de l'URL)
- **Les règles d'acheminement** définissent comment analyser la requête pour la diriger vers le pool back-end approprié.
- Un **pool back-end** contient des serveurs web pour des ressources telles que des machines virtuelles ou des Virtual Machine Scale Sets. Chaque pool dispose d'un équilibreur de charge pour distribuer la charge de travail entre les ressources.
- Les **sondes d'intégrité** déterminent quels serveurs dans le pool back-end sont disponibles pour l'équilibrage de charge.

Superviser et sauvegarder les ressources Azure

Configurer des sauvegardes de fichiers et de dossiers

Décrire les avantages de Sauvegarde Azure

Azure Backup est le service Azure qui vous permet de sauvegarder (ou de protéger) et de restaurer vos données dans le cloud Microsoft. Il remplace votre solution de sauvegarde locale ou hors site par une solution cloud à la fois fiable, sécurisée et économique.

Avantage	Description
Déplacer la sauvegarde locale	Le service Sauvegarde Azure offre une solution simple pour la sauvegarde de vos ressources locales dans le cloud. Obtenez une sauvegarde à court terme et à long terme sans avoir besoin de déployer des solutions de sauvegarde locale complexes.
Sauvegarder les machines virtuelles Azure IaaS	Le service Sauvegarde Azure fournit des sauvegardes indépendantes et isolées pour éviter une destruction accidentelle des données d'origine. Les sauvegardes sont stockées dans un coffre Azure Recovery Services avec gestion intégrée des points de récupération. La configuration et la scalabilité sont simples : les sauvegardes sont optimisées, et vous pouvez facilement effectuer des restaurations en fonction des besoins.
Obtenir un transfert de données illimitées	Le service Sauvegarde Azure ne limite pas la quantité de données entrantes ou sortantes transférées, et ne facture pas les données transférées. Les données sortantes sont les données transférées à partir d'un coffre Recovery Services pendant une opération de restauration. Si vous effectuez une sauvegarde initiale hors connexion à l'aide du service Azure Import/Export pour importer de grandes quantités de données, des coûts sont associés aux données entrantes.
Sécuriser les données	Le chiffrement des données garantit une transmission et un stockage sécurisés de vos données dans le cloud public. La phrase secrète de chiffrement est stockée localement, elle n'est jamais transmise ou stockée dans Azure. Si vous devez restaurer des données, vous seul disposez de la phrase secrète ou de la clé de chiffrement.
Obtenir des sauvegardes cohérentes avec les applications	Une sauvegarde cohérente au niveau application signifie qu'un point de récupération dispose de toutes les données nécessaires pour restaurer la copie de sauvegarde. Le service Sauvegarde Azure fournit des sauvegardes cohérentes avec les applications. Ainsi, aucun correctif supplémentaire n'est nécessaire pour restaurer les données. La restauration de données cohérentes avec les applications réduit le délai de restauration, ce qui permet de rétablir rapidement le fonctionnement normal.

Conserver des données à court terme et à long terme	Vous pouvez utiliser les coffres Azure Recovery Services pour la conservation des données à court terme et à long terme. Azure ne limite pas la durée de conservation des données dans un coffre Recovery Services. Vous pouvez les conserver dans un coffre aussi longtemps que vous le souhaitez. Sauvegarde Azure se limite à 9 999 points de récupération par instance protégée.
Gestion automatique du stockage	Les environnements hybrides nécessitent souvent un stockage hétérogène avec des instances locales et des instances dans le cloud. Avec Sauvegarde Azure, l'implémentation de dispositifs de stockage locaux est gratuite. Sauvegarde Azure alloue et gère automatiquement le stockage de sauvegarde. Le service utilise un modèle de paiement à l'utilisation : vous payez donc uniquement pour le stockage que vous consommez.
Diverses options de stockage	Sauvegarde Azure propose deux types de réplication pour maintenir votre stockage et vos données hautement disponibles. Le **stockage localement redondant (LRS)** réplique vos données trois fois (il crée trois copies de vos données) dans une unité d'échelle de stockage d'un centre de données. Toutes les copies des données existent dans la même région. Le stockage LRS est une option à faible coût qui protège vos données contre les défaillances matérielles locales. Le **stockage géoredondant (GRS)** est l'option de réplication par défaut : c'est l'option recommandée. Le stockage géo-redondant réplique vos données vers une région secondaire, distante de plusieurs centaines de kilomètres de l'emplacement principal des données sources. Le stockage GRS est plus onéreux que le stockage LRS, mais il offre une durabilité des données supérieure, même en cas de panne au niveau régional.

Configurer les options de sauvegarde du coffre Azure Recovery Services

Le **coffre Recovery Services** est une entité de stockage dans Azure qui stocke des données. Les coffres Recovery Services facilitent l'organisation de vos données de sauvegarde, tout en réduisant le temps de gestion.

Choses à savoir sur les coffres Recovery Services

- Le coffre Recovery Services peut être utilisé pour sauvegarder des partages de fichiers Azure Files, ou des fichiers et dossiers locaux.
- Les coffres Recovery Services stockent les données de sauvegarde de différents services Azure, par exemple les machines virtuelles IaaS (Linux ou Windows) et Azure SQL dans des machines virtuelles Azure.
- Les coffres Recovery Services prennent en charge System Center Data Protection Manager, Windows Server, le serveur de sauvegarde Azure et d'autres services.
- Dans le portail Azure, vous pouvez créer un coffre Recovery Services à partir du tableau de bord du Centre de sauvegarde.

Choses à savoir sur la configuration des coffres Recovery Services

- Si vous utilisez le service Sauvegarde Azure pour les partages de fichiers Azure Files, vous n'avez pas besoin de configurer le type de réplication de stockage. La sauvegarde Azure Files est basée sur des captures instantanées, aucune donnée n'est transférée vers le coffre. Les captures instantanées sont stockées dans le même compte Stockage Azure que votre partage de fichiers sauvegardé.
  Vous pouvez configurer la réplication de vos coffres Recovery Services à partir du tableau de bord du Centre de sauvegarde sous **Propriétés**>**Configuration de la sauvegarde**>**Mettre à jour**.
- Il existe trois options de réplication de stockage : géoredondant, localement redondant et redondant interzone. Le tableau suivant fournit des recommandations pour les types de réplication.

Utiliser l'agent MARS (Microsoft Azure Recovery Services)

Le service Sauvegarde Azure utilise l'agent MARS (Microsoft Azure Recovery Services) pour sauvegarder les fichiers, les dossiers et les données système de vos machines locales et des machines virtuelles Azure. L'agent MARS est un agent complet qui offre de nombreux avantages pour la sauvegarde et la restauration de vos données.

Choses à savoir sur l'agent MARS

- Le service Sauvegarde Azure pour les fichiers et les dossiers repose sur l'installation de l'agent MARS sur votre client Windows ou votre serveur Windows.
- Les données disponibles pour la sauvegarde dépendent de l'emplacement où vous installez et exécutez l'agent MARS.
- Vous pouvez sauvegarder des fichiers et des dossiers sur des machines virtuelles ou des machines physiques Windows. Les machines virtuelles peuvent être situées localement ou dans Azure.

- L’agent MARS ne nécessite pas de serveur de sauvegarde distinct.
- L’agent MARS ne reconnaît pas les applications. Vous pouvez restaurer des fichiers et des dossiers à partir de sauvegardes, ou effectuer une restauration au niveau du volume.

Configurer des sauvegardes de fichiers et de dossiers locaux.

Étape 1. Créer un coffre Recovery Services

Étape 2. Télécharger l’agent MARS et le fichier d’informations d’identification

Étape 3. Installer et inscrire l’agent MARS

Étape 4. Configurer des sauvegardes

Configurer des sauvegardes de machines virtuelles

Explorer les options possibles pour protéger les données des machines virtuelles

Informations à connaître sur les options de sauvegarde pour les machines virtuelles

Option Sauvegarde Azure	Scénarios de configuration	Description
Azure Backup	*Sauvegarder des machines virtuelles Azure exécutant des charges de travail de production* *Créer des sauvegardes cohérentes avec les applications pour les machines virtuelles Windows et Linux*	Sauvegarde Azure prend un instantané de votre machine virtuelle et stocke les données en tant que points de récupération dans des coffres de récupération géoredondants. Quand vous effectuez une restauration à partir d’un point de récupération, vous pouvez restaurer une machine virtuelle entière ou des fichiers spécifiques uniquement.

Azure Site Recovery	*Récupérer rapidement et facilement des applications spécifiques* *Répliquer vers la région Azure de votre choix*	Azure Site Recovery protège vos machines virtuelles d'un scénario de sinistre majeur où une région entière connaît une panne en raison d'une grande catastrophe naturelle ou d'une interruption de service généralisée.
Disques managés Azure - capture instantanée	*Sauvegarder rapidement et facilement vos machines virtuelles qui utilisent des disques managés Azure, à tout moment* *Prendre en charge des environnements de développement et de test*	La capture instantanée de disques managés Azure est une copie en lecture seule d'un disque managé qui est stockée comme disque managé standard par défaut. Une capture instantanée existe indépendamment du disque source et peut être utilisée pour créer des disques managés par la suite. Chaque instantané est facturé selon la taille réelle utilisée. Si vous créez un instantané d'un disque managé d'une capacité de 64 Go et que vous n'utilisez que 10 Go, vous serez facturé pour 10 Go.
Disques managés Azure - image	*Créer une image à partir de votre disque dur virtuel personnalisé dans un compte de stockage Azure ou directement à partir d'une machine virtuelle généralisée (via Sysprep)* *Créer des centaines de machines virtuelles en utilisant votre image personnalisée sans copier ni gérer de compte de stockage*	Les disques managés Azure prennent également en charge la création d'une image personnalisée gérée. Ce processus capture une image unique qui contient tous les disques gérés associés à une machine virtuelle, incluant à la fois le système d'exploitation et les disques de données.

Créer des captures instantanées des machines virtuelles dans Sauvegarde Azure

Un travail Sauvegarde Azure crée un instantané pour votre machine virtuelle en deux phases :

- Phase 1 : Prendre un instantané des données de machine virtuelle
- Phase 2 : Transférer l'instantané vers un coffre Azure Recovery Services

Informations à connaître sur les instantanés et les points de récupération

- Par défaut, Sauvegarde Azure conserve les instantanés pendant deux jours pour réduire les temps de sauvegarde et de restauration. La rétention locale réduit le temps nécessaire à la transformation et à la copie des données à partir d'un coffre Azure Recovery Services.
- Vous pouvez définir une valeur de rétention d'instantané par défaut comprise entre un et cinq jours.
- Les instantanés incrémentiels sont stockés sous forme d'objets blob de pages Azure (disques Azure).
- Les points de récupération d'un instantané de machine virtuelle ne sont disponibles qu'une fois les deux phases du travail Sauvegarde Azure terminées.
- Les points de récupération sont répertoriés pour l'instantané de la machine virtuelle dans le portail Azure et étiquetés avec un *type de point de récupération*.
- Lorsqu'un instantané est créé pour la première fois, les points de récupération sont identifiés avec le type de point de récupération **instantané**.
- Une fois l'instantané transféré vers un coffre Azure Recovery Services, le type de point de récupération devient **snapshot and vault** (instantané et coffre).

Configurer les options de sauvegarde dans un coffre Azure Recovery Services

Un coffre Azure Recovery Services est une entité de stockage dans Azure qui héberge des données. Les données sont généralement des copies de données ou des informations de configuration pour des machines virtuelles, des charges de travail, des serveurs ou des stations de travail. Vous pouvez utiliser des coffres Recovery Services pour organiser vos données de sauvegarde et réduire la surcharge de gestion.

Sauvegarder vos machines virtuelles

Étape 1. Créer un coffre Recovery Services

La première étape consiste à créer un coffre Azure Recovery Services pour les sauvegardes de machines virtuelles. Vous devez créer le coffre dans votre abonnement Azure et dans la région où vous souhaitez stocker les données.

Étape 2. Définir les options de votre stratégie de sauvegarde

Après avoir créé le coffre, vous devez définir votre stratégie de sauvegarde. La stratégie définit quand déclencher les captures instantanées des données et combien de temps conserver ces captures instantanées.

Étape 3. Sauvegarder votre machine virtuelle

La dernière étape consiste à exécuter le processus de travail Sauvegarde Azure et à créer vos sauvegardes.

Pour exécuter le travail de sauvegarde, l'extension Sauvegarde Azure nécessite que l'agent de machine virtuelle Microsoft Azure soit présent sur votre machine virtuelle Azure.

- Si votre machine virtuelle a été créée à partir de la galerie Azure, l'agent a été installé par défaut sur la machine.
- Si votre machine virtuelle a été migrée à partir d'un centre de données local, vous devez installer manuellement l'agent sur la machine.

Restaurer vos machines virtuelles

Après la sauvegarde de votre machine virtuelle, les captures instantanées et points de récupération de sauvegarde sont stockés dans votre coffre Recovery Services. Vous pouvez récupérer votre machine en accédant à sa capture instantanée, ou restaurer les données à un point précis dans le temps en utilisant les points de récupération.

Choses à savoir sur la restauration des machines virtuelles

- Vous pouvez sélectionner des points de récupération de vos captures instantanées de machines virtuelles dans le portail Azure.
- Quand vous déclenchez une opération de restauration, Sauvegarde Azure crée un travail pour suivre l'opération de restauration.
- Sauvegarde Azure crée et affiche temporairement des notifications concernant l'opération de restauration.
- Vous pouvez suivre l'opération de restauration en surveillant les notifications de travail dans le portail Azure.

Implémenter System Center DPM et Azure Backup Server

Une autre option possible pour sauvegarder vos machines virtuelles est d'utiliser System Center Data Protection Manager (DPM) ou Microsoft Azure Backup Server (MABS). Ces services vous permettent de sauvegarder des charges de travail spécialisées, des machines virtuelles ou des fichiers, des dossiers et des volumes. Les charges de travail spécialisées peuvent inclure des données de Microsoft SharePoint, Microsoft Exchange et SQL Server.

Choses à savoir sur l'utilisation de System Center DPM et de MABS

- Quand vous configurez la protection d'une machine ou d'une application avec le service System Center DPM ou MABS, vous choisissez de faire la sauvegarde sur le disque local DPM ou MABS pour un stockage à court terme, et sur Azure pour une protection en ligne. Vous spécifiez quand déclencher la sauvegarde sur le stockage DPM ou MABS local et quand déclencher la sauvegarde en ligne sur Azure.
- Pour assurer la protection de vos machines locales, l'instance System Center DPM ou MABS doit être exécutée localement.
- Pour protéger vos machines virtuelles Azure, l'instance MABS doit être exécutée en tant que machine virtuelle Azure dans Azure.
- L'agent de protection System Center DPM/MABS doit être installé sur chaque machine que vous souhaitez protéger. Pour plus d'informations, consultez Déployer l'agent de protection System Center DPM et Installer l'agent de protection DPM (pour MABS).
- Les machines que vous souhaitez sauvegarder doivent être ajoutées à un *groupe de protection* System Center DPM.
- Au déclenchement de la sauvegarde, le disque de la charge de travail protégée est sauvegardé sur les disques DPM ou MABS locaux, selon la planification que vous avez spécifiée. Les disques DPM ou MABS sont ensuite sauvegardés dans le coffre Recovery Services par l'agent MARS en cours d'exécution sur l'instance DPM ou MABS.

Implémenter la suppression réversible pour vos machines virtuelles

Le service Stockage Azure propose maintenant la fonctionnalité de *suppression réversible* pour les objets Blob Azure. Avec cette fonctionnalité, vous pouvez récupérer plus facilement vos données qui ont été modifiées ou supprimées par erreur par une application ou un autre utilisateur du compte de stockage.

La fonctionnalité de suppression réversible pour les machines virtuelles protège les sauvegardes de vos machines virtuelles contre les suppressions involontaires. Même après leur suppression, les sauvegardes sont conservées à l'état de suppression réversible pendant encore 14 jours.

Choses à savoir sur la suppression réversible des sauvegardes

- **Arrêter le travail de sauvegarde**. Avant de pouvoir supprimer ou conserver les données de sauvegarde de votre machine virtuelle, vous devez arrêter le travail de sauvegarde en cours. Après avoir arrêté le travail de sauvegarde dans le portail Azure, vous avez le choix entre supprimer vos données de sauvegarde ou les conserver.
- **Appliquer l'état de suppression réversible**. Empêchez la suppression définitive des données de sauvegarde de votre machine virtuelle en sélectionnant **Supprimer les données de sauvegarde**, puis **Arrêter la sauvegarde**. L'état de suppression réversible est alors appliqué à vos données de sauvegarde, et les données sont conservées durant 14 jours. Si vous appliquez l'état à une machine virtuelle, la machine est affichée comme étant *supprimée de manière réversible*.
- **Afficher les données de suppression réversible dans le coffre**. Pendant la période de conservation de 14 jours, le coffre Recovery Services affiche votre machine virtuelle supprimée de manière réversible avec une icône de **suppression réversible** rouge.
- **Annuler la suppression des éléments de sauvegarde**. Avant de pouvoir restaurer une machine virtuelle qui a été supprimée de manière réversible, vous devez annuler la suppression des données de sauvegarde.
- **Restaurer les éléments**. Après avoir annulé la suppression des éléments de sauvegarde, vous pouvez restaurer votre machine virtuelle en sélectionnant **Restaurer la machine virtuelle** à partir du point de récupération choisi dans la sauvegarde.
- **Reprendre les sauvegardes**. Quand le processus d'annulation de la suppression est terminé, l'état du travail de sauvegarde est redéfini sur **Arrêter la sauvegarde avec conservation des données**. Vous pouvez choisir **Reprendre la sauvegarde**. L'opération de reprise récupère les éléments de sauvegarde dans l'état *actif* en fonction de la stratégie de sauvegarde sélectionnée par l'utilisateur. La stratégie définit les planifications de sauvegarde et de conservation des données.

Implémenter Azure Site Recovery

Azure Site Recovery permet d'assurer la continuité de l'activité en maintenant l'exécution des charges de travail et applications métier lors des interruptions. Site Recovery réplique les charges de travail s'exécutant sur des machines virtuelles et physiques depuis un site principal vers un emplacement secondaire. Si une interruption se produit sur votre site principal, Site Recovery implémente un basculement vers l'emplacement secondaire pour maintenir l'accès à vos applications. Quand le site principal redevient opérationnel, vous pouvez reprendre l'accès aux applications sur la machine principale.

Choses à savoir sur Azure Site Recovery

- Répliquer des machines virtuelles Azure d'une région Azure vers une autre
- Répliquer des machines virtuelles VMware locales, des machines virtuelles Hyper-V, des serveurs physiques (Windows et Linux) et des machines virtuelles Azure Stack vers Azure
- Répliquer des instances Windows AWS sur Azure
- Répliquer des machines virtuelles VMware locales, des machines virtuelles Hyper-V managées par System Center VMM et des serveurs physiques vers un site secondaire

Configurer Azure Monitor

Décrire les fonctionnalités clés d'Azure Monitor

Choses à savoir sur Azure Monitor

- **Superviser et visualiser les métriques** : Azure Monitor collecte des valeurs de métriques numériques à partir de vos ressources Azure en fonction de vos préférences. Azure Monitor propose différentes méthodes d'affichage de vos données de métriques pour vous aider à comprendre l'intégrité, le fonctionnement et les performances de votre système.
- **Interroger et analyser les journaux** : les journaux Azure Monitor (Log Analytics) génèrent des journaux d'activité, des journaux de diagnostic et des informations de télémétrie à partir de vos solutions de monitoring. Le service fournit des requêtes analytiques que vous pouvez utiliser pour faciliter la résolution des problèmes et la visualisation de vos données de journal.
- **Configurer des alertes et des actions** : Azure Monitor vous permet de configurer des alertes pour vos données collectées afin de vous avertir en cas de conditions critiques. Vous pouvez configurer des actions en fonction des conditions d'alerte, et prendre des mesures correctives automatisées basées sur les déclencheurs de vos métriques ou journaux.

Éléments à savoir sur le monitoring avec Azure

- Les services de monitoring et de diagnostic offerts dans Azure sont divisés en **catégories** globales telles que Noyau, Application, Infrastructure et Capacités partagées.
- Les **magasins de données** dans Azure Monitor contiennent vos métriques et journaux. Les métriques Azure Monitor et les journaux Azure Monitor sont les deux types de données de base utilisés par le service.

- Différentes **sources de monitoring** fournissent à Azure Monitor les données de métriques et de journaux à analyser. Ces sources peuvent inclure votre

abonnement et votre locataire Azure, vos instances de service Azure, vos ressources Azure, les données de vos applications, etc.

- Azure Monitor Insights effectue différentes fonctions avec les données collectées, notamment l'analyse, le déclenchement d'alertes et le streaming vers des systèmes externes.
    - **Obtenir des insights** : accédez à l'extension Azure Application Insights d'Azure Monitor afin d'utiliser les fonctionnalités APM (Application Performance Monitoring). Vous pouvez utiliser les outils APM pour superviser les performances de votre application et collecter des données de journalisation du suivi. Application Insights est disponible pour de nombreux services Azure, tels que Machines Virtuelles Azure et Azure Virtual Machine Scale Sets, Azure Container Instances, Azure Cosmos DB et Azure IoT Edge.
    - **Visualiser** : utilisez les nombreuses options d'Azure Monitor pour afficher et interpréter vos métriques et journaux collectés. Vous pouvez utiliser Power BI avec la fonctionnalité Classeurs Azure d'Azure Monitor, et accéder à des tableaux de bord et des vues configurables.
    - **Analyser** : utilisez les journaux Azure Monitor (Log Analytics) dans le portail Azure pour écrire des requêtes de journal pour vos données. Vous pouvez analyser de manière interactive vos données de journal à l'aide des métriques Azure Monitor et du puissant moteur d'analyse.
    - **Répondre** : configurez des règles d'alerte de journal dans Azure Monitor pour recevoir des notifications relatives aux performances de votre application. Vous pouvez configurer le service pour qu'il prenne des mesures automatisées lorsque les résultats de vos requêtes et alertes correspondent à certaines conditions ou résultats.
    - **Intégrer** : Ingérez et exportez les résultats des requêtes de journal à partir d'Azure CLI, des applets de commande Azure PowerShell et de diverses API. Configurez l'exportation automatisée de vos données de journal vers votre compte Stockage Azure ou vers Azure Event Hubs. Créez des workflows pour récupérer vos données de journal et les copier vers des emplacements externes avec Azure Logic Apps.

Définir les métriques et les journaux

Toutes les données collectées par Azure Monitor sont de l'un des deux types fondamentaux, métriques et journaux :

Les **métriques** sont des valeurs numériques décrivant un aspect d'un système à un moment précis dans le temps. Les métriques sont légères et capables de prendre en charge des scénarios en quasi temps réel.

Les **journaux d'activité** contiennent différents types de données organisées en enregistrements, avec différents jeux de propriétés pour chaque type. Les données telles que les événements et les traces sont stockées sous forme de journaux avec

des données de performances afin que toutes les données puissent être combinées à des fins d'analyse.

Ce qu'il faut savoir sur les métriques Azure Monitor

- Pour de nombreuses ressources Azure, les données de métriques collectées par Azure Monitor sont affichées dans la page **Vue d'ensemble** de la ressource dans le portail Azure. Considérez la vue d'ensemble d'une machine virtuelle Azure qui comporte plusieurs graphiques montrant les métriques de performances.
- Vous pouvez utiliser **Metrics Explorer** d'Azure Monitor pour afficher les métriques de vos services et ressources Azure.
- Dans le portail Azure, sélectionnez un graphique pour une ressource afin d'ouvrir les données de métriques associées dans Metrics Explorer. Cet outil vous permet de représenter sous forme de graphique les valeurs de plusieurs métriques au fil du temps. Vous pouvez travailler avec les graphiques de manière interactive, ou les épingler à un tableau de bord pour les afficher avec d'autres visualisations.

Ce qu'il faut savoir sur les journaux Azure Monitor

- Dans le portail Azure, les données de journal collectées par Azure Monitor sont stockées dans Log Analytics.
- Log Analytics inclut un langage de requête riche pour vous aider à rapidement récupérer, consolider et analyser vos données collectées.
- Vous pouvez utiliser Log Analytics pour créer et tester des requêtes. Utilisez les résultats de requêtes pour analyser directement les données, enregistrer vos requêtes, visualiser les données et créer des règles d'alerte.
- Azure Monitor utilise une version du langage de requête Data Explorer. Ce langage est adapté aux requêtes de journal simples, mais inclut également des fonctionnalités avancées telles que les agrégations, les jointures et l'analytique intelligente. Vous pouvez rapidement apprendre le langage de requête en suivant plusieurs leçons disponibles. Des conseils particuliers sont fournis aux utilisateurs qui connaissent déjà SQL et Splunk.

Identifier les données et les niveaux de monitoring

Ce qu'il faut savoir sur la collecte de données

- Azure Monitor commence à collecter des données dès que vous créez votre abonnement Azure et que vous ajoutez des ressources.
- Lorsque vous créez ou modifiez des ressources, ces données sont stockées dans des journaux d'activité Azure Monitor.
- Les données de performances relatives aux ressources, ainsi que la quantité de ressources consommées, sont stockées sous forme de métriques Azure Monitor.

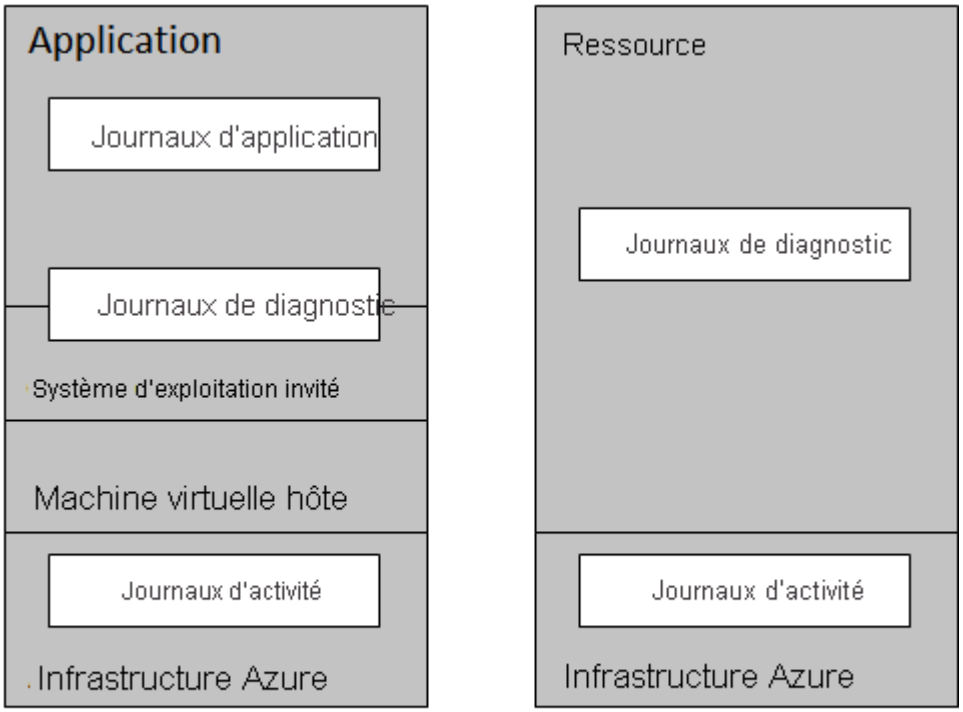
- Étendez les données que vous collectez en activant les diagnostics et en ajoutant l'agent Azure Monitor aux ressources de calcul. L'extension de vos sources de données vous permet de collecter des données relatives au fonctionnement interne des ressources.
- L'agent Azure Monitor vous permet également de configurer différentes sources de données afin de collecter les journaux et les métriques des systèmes d'exploitation invités Windows et Linux.
- Azure Monitor peut collecter des données de journal à partir de n'importe quel client REST à l'aide de l'API de collecteur de données. L'API de collecte de données vous permet de créer des scénarios de supervision personnalisés, et d'étendre cette supervision aux ressources qui n'exposent pas de données via d'autres sources.

Décrire les événements du journal d'activité

Le journal d'activité Azure Monitor est un journal lié à l'abonnement, qui fournit des insights sur tous les événements au niveau de l'abonnement qui se produisent dans Azure. Les événements peuvent inclure différentes données, qui vont des données opérationnelles d'Azure Resource Manager aux mises à jour des événements d'intégrité de service Azure.

Ce qu'il faut savoir sur les journaux d'activité

- Vous pouvez utiliser les informations contenues dans les journaux d'activité pour comprendre l'état des opérations de ressources et d'autres propriétés pertinentes.
- Les journaux d'activité peuvent vous aider à déterminer « quoi, qui et quand » pour toutes les opérations d'écriture (PUT, POST, DELETE) effectuées sur des ressources dans votre abonnement.
- Les journaux d'activité sont conservés pendant 90 jours.
- Vous pouvez interroger n'importe quelle plage de dates dans un journal d'activité, à condition que la date de début ne remonte pas à plus de 90 jours.
- Vous pouvez récupérer des événements à partir de votre journal d'activité à l'aide du portail Azure, d'Azure CLI, des applets de commande PowerShell et de l'API REST Azure Monitor.



Ressources de calcul uniquement

Ressources non liées au cal ressources uniquement

Éléments à savoir sur les filtres de journal d'activité

Examinons certains des filtres que vous pouvez définir pour contrôler les données à examiner dans votre journal d'activité :

- **Abonnement** : afficher les données d'un ou plusieurs noms d'abonnements Azure spécifiés.
- **Intervalle de temps** : afficher les données pour une heure spécifiée en choisissant l'heure de début et de fin des événements, par exemple une période de six heures.
- **Gravité de l'événement** : afficher les événements aux niveaux de gravité sélectionnés, à savoir *Information*, *Avertissement*, *Erreur* ou *Critique*.
- **Groupe de ressources** : afficher les données d'un ou plusieurs groupes de ressources spécifiés dans vos abonnements spécifiés.
- **Ressource (nom)** : afficher les données des ressources spécifiées.
- **Type de ressource** : afficher les données des ressources d'un type spécifié, comme `Microsoft.Compute/virtualmachines`.
- **Nom de l'opération** : afficher les données d'une opération Azure Resource Manager sélectionnée, telle que `Microsoft.SQL/servers/Write`.
- **Événement lancé par** : afficher les données d'opération d'un utilisateur spécifié qui a effectué l'opération, nommé « appelant ».

Éléments à savoir sur les catégories d'événements

Catégorie d'événements	Données d'événement	Exemples

Administrative	Toutes les opérations de création, de mise à jour, de suppression et d'action effectuées via Azure Resource Manager, ainsi que toutes les modifications apportées au contrôle d'accès en fonction du rôle (RBAC) dans vos abonnements filtrés	`create virtual machine`
		
		`delete network security group`

Service Health	Tous les événements d'intégrité du service pour les services et ressources Azure connectés à vos abonnements filtrés, y compris *Action requise*, *Récupération assistée*, *Incident*, *Maintenance*, *Informations* ou *Sécurité*	`SQL Azure in East US is experiencing downtime`
		
		`Azure SQL Data Warehouse Scheduled Maintence Complete`

Resource Health	Tous les événements d'intégrité des ressources pour vos ressources Azure filtrées, y compris *Disponible*, *Indisponible*, *Dégradé* ou *Inconnu*, et identifiés comme *Lancé par la plateforme* ou *Lancé par l'utilisateur*	`Virtual Machine health status changed to unavailable`
		
		`Web App health status changed to available`

Alert	Toutes les activations d'alertes Azure pour vos abonnements et ressources filtrés	`CPU % on devVM001 has been over 80 for the past 5 minutes`
		
		`Disk read LessThan 100000 in the last 5`

		`minutes`
Autoscale	Tous les événements liés au fonctionnement du moteur de mise à l'échelle automatique, sur la base des paramètres de mise à l'échelle automatique définis pour vos abonnements filtrés	`Autoscale scale up action failed`
Recommandation	Événements de recommandation pour certains types de ressources Azure, tels que les sites web et les serveurs SQL, en fonction de vos abonnements et ressources filtrés	*Recommandations pour mieux utiliser vos ressources*
Sécurité	Toutes les alertes générées par Microsoft Defender pour le cloud affectent vos abonnements et ressources filtrés	`Suspicious double extension file executed`
Stratégie	Toutes les opérations d'action d'effet effectuées par Azure Policy pour vos abonnements et ressources filtrés, où chaque action effectuée par Azure Policy est modélisée comme une opération sur une ressource	`Audit` et `Deny`

Ce qu'il faut savoir sur les alertes Azure

- Dans le portail Azure, vous configurez Azure Monitor pour capturer les données de télémétrie de vos services, ressources et applications Azure.
- Vous créez des alertes pour que votre configuration Azure fonctionne avec les données de télémétrie capturées.
- Une alerte se compose de *règles d'alerte* qui combinent les paramètres et les conditions que vous souhaitez monitorer, notamment :
    - Ressources à monitorer
    - Signaux ou données de télémétrie à collecter à partir des ressources
    - Conditions à remplir
- Une règle d'alerte spécifie des *groupes d'actions* pour effectuer des étapes réactives quand une alerte se déclenche, comme l'envoi de notifications.
- Chaque alerte surveille vos données de télémétrie et capture un signal concernant les modifications apportées à une ressource spécifiée.

- La règle d'alerte capture le signal et vérifie s'il correspond aux critères de votre condition.
- Quand vos données de télémétrie remplissent les conditions de votre règle, une alerte se déclenche et appelle les groupes d'actions spécifiés.
- Si vous monitorez plusieurs ressources, le système évalue vos conditions et déclenche des alertes séparément pour chaque ressource.

Ce qu'il faut savoir sur les types d'alertes

- **Alertes de métrique** : évaluez les données de métriques de vos ressources à intervalles réguliers. Collectez les données de métriques à partir de votre plateforme, de journaux Azure Monitor convertis en métriques, d'Azure Application Insights et de métriques personnalisées. Les alertes de métrique peuvent appliquer plusieurs conditions et seuils dynamiques.
- **Alertes de journal** : utilisez des requêtes Log Analytics dans le portail Azure pour évaluer les journaux de ressources à une fréquence prédéfinie.
- **Événements du journal d'activité** : implémentez des alertes à déclencher quand un nouvel événement du journal d'activité répondant à vos conditions se produit. Les alertes *Resource Health* et *Service Health* sont deux types d'alertes de journal d'activité.
- **Alertes de détection intelligente** : recevez des avertissements automatiques sur d'éventuels problèmes de performances et anomalies d'échecs dans vos applications web en utilisant la détection intelligente sur vos ressources Application Insights. Migrez la détection intelligente sur vos ressources Application Insights afin de créer des règles d'alerte pour les différents modules de détection intelligente.

Ce qu'il faut savoir sur les états d'alerte

- Il existe trois états d'alerte :
    - **Nouveau** : le problème est nouveau (ouvert) et n'est pas en cours de révision.
    - **Reconnu** : le problème est en cours de révision et le travail a commencé.
    - **Fermé** : le problème est résolu.
- Pendant le processus de monitoring des alertes, quand les conditions d'une règle d'alerte correspondent aux données de télémétrie de la ressource spécifiée, une alerte se déclenche et appelle les groupes d'actions spécifiés. Le système définit l'état d'alerte sur *Nouveau*.
- Quand le système définit un état d'alerte sur *Nouveau*, vous pouvez modifier l'état pour spécifier l'emplacement du problème associé dans le processus de résolution.

  Seul l'état *Nouveau* initial d'une alerte est défini par le système. C'est vous, en tant qu'administrateur, qui effectuez tous les autres changements d'état.

- Quand le problème de l'alerte est en cours de révision, vous pouvez définir l'état d'alerte sur *Reconnu*.
- Une fois le problème d'une alerte résolu, vous pouvez faire passer l'état d'alerte à *Fermé*.
- Si l'état d'une alerte est *Fermé*, vous pouvez « rouvrir » l'alerte en remplaçant l'état d'alerte par *Nouveau* ou *Reconnu*. |
- L'historique de l'alerte stocke tous les changements d'état.

État d'alerte et condition Azure Monitor

- Au moment du déclenchement initial d'une alerte, le système fait passer l'état d'alerte à *Nouveau*. Tous les autres changements de l'état d'alerte sont effectués par un administrateur local.
- Pour toutes **les mises à jour de la condition Azure Monitor pour la même alerte**, **le système effectue tous les changements**.
- Au moment du déclenchement d'une alerte, la condition Azure Monitor de l'alerte passe à ***déclenchée***.
- Quand le problème de l'alerte est résolu, la condition Azure Monitor de l'alerte passe à ***résolue***.

Alertes sans état et avec état

- Les **alertes sans état** se déclenchent chaque fois que la condition de votre règle d'alerte correspond à vos données, même si la même alerte existe déjà. Vous pouvez configurer les alertes de journal et les alertes de métrique en tant qu'alertes sans état.
- Les **alertes avec état** se déclenchent quand la condition de votre règle d'alerte correspond à vos données et que la même alerte n'existe pas. Une alerte avec état ne déclenche aucune autre action tant que les conditions de la règle d'alerte actuelle sont remplies. Vous pouvez configurer les alertes de journal et les alertes de métrique en tant qu'alertes avec état. Les alertes de journal d'activité sont toujours sans état.

Ce qu'il faut savoir sur les règles d'alertes

- Une règle d'alerte se compose de plusieurs attributs clés : la ressource cible, un signal d'alerte, les critères de règle, la gravité du problème, ainsi qu'un nom et une description.
- Votre **ressource cible** définit l'étendue et les signaux disponibles pour votre opération d'alerte. Une cible peut être n'importe quelle ressource Azure, telle qu'une machine virtuelle, un compte Stockage Azure ou une instance Virtual Machine Scale Sets. Une cible peut également être un espace de travail Log Analytics ou une ressource Azure Application Insights. Pour certaines ressources telles que les machines virtuelles Azure, vous pouvez spécifier plusieurs ressources comme cible pour votre règle d'alerte.

- La ressource cible de votre alerte émet un **signal** en fonction du type de ressource sélectionné. Le signal émis peut être *Métrique*, *Journal d'activité*, *Application Insights* ou *Journal*.
- Vous définissez des **critères** pour votre règle d'alerte qui combinent votre signal avec la logique de traitement. Les critères s'appliquent à votre ressource cible. `\* Percentage CPU > 70%; Server Response Time > 4 ms; and Result count of a log query > 100` est un exemple de combinaison de critères.
- Vous pouvez spécifier le niveau de **gravité** de votre règle d'alerte, qui correspond au problème relatif à votre alerte. La gravité peut être comprise entre 0 et 4.
- Lorsqu'un problème correspond à vos conditions de règle, le système appelle les **actions** pour votre règle d'alerte. Les actions sont les étapes réactives relatives au problème, telles que l'envoi de notifications.
- Par défaut, le système définit une nouvelle règle d'alerte sur *Activée*. Si vous ne souhaitez pas qu'une alerte se déclenche, définissez la règle d'alerte sur *Désactivée*.
- Une alerte ne peut se déclencher que lorsque la règle d'alerte est à l'état *Activée*.

Ce qu'il faut savoir sur les groupes d'actions

- Plusieurs alertes peuvent utiliser le même groupe d'actions ou des groupes d'actions différents selon les besoins de l'utilisateur.
- Les notifications spécifient comment notifier les utilisateurs quand votre groupe d'actions se déclenche.
- Les actions spécifient comment appeler vos actions définies quand votre groupe d'actions se déclenche.

Notifications

Dans le portail Azure, vous pouvez sélectionner l'option **Envoyer un e-mail au rôle Azure Resource Manager** pour envoyer des notifications par e-mail aux membres du rôle de votre abonnement Azure.

Actions

Vous affectez à chaque action un nom unique et des détails, et vous définissez les notifications à envoyer ou les actions à effectuer. Vous pouvez spécifier des actions pour envoyer un appel vocal, un SMS ou un e-mail.

Points à connaître concernant Log Analytics

- Log Analytics dans Azure Monitor offre des fonctionnalités et des outils de requête permettant de répondre à quasiment toutes les questions sur votre configuration supervisée.

- Log Analytics prend en charge le langage de requête Kusto. Vous pouvez créer des requêtes simples ou complexes avec KQL, notamment :
    - Rechercher et trier par valeur, heure, état de propriété, etc.
    - Joindre des données à partir de plusieurs tables
    - Agréger de grands ensembles de données
    - Effectuer des opérations complexes avec un minimum de code
- Quand vos journaux Azure Monitor ont collecté suffisamment de données et que vous comprenez comment construire la requête appropriée, vous pouvez utiliser Log Analytics pour effectuer une analyse détaillée et résoudre les problèmes.

Points à connaître concernant l'espace de travail Log Analytics

Pour commencer à utiliser Log Analytics dans Azure Monitor, vous devez créer votre espace de travail. Un espace de travail a un ID d'espace de travail et un ID de ressources uniques. Après avoir créé votre espace de travail, vous configurez vos sources de données et solutions pour stocker leurs données dans votre espace de travail.

Pour créer votre espace de travail Log Analytics, configurez les paramètres suivants :

- **Nom** : spécifiez un nom pour votre nouvel espace de travail Log Analytics. Le nom de votre espace de travail doit être unique au sein de votre groupe de ressources.
- **Abonnement** : spécifiez l'abonnement Azure à associer à votre espace de travail.
- **Groupe de ressources** : spécifiez le groupe de ressources à associer à votre espace de travail. Vous pouvez choisir un groupe de ressources existant ou en créer un. Le groupe de ressources doit contenir au moins une instance Machines virtuelles Azure.
- **Région** : sélectionnez la région où déployer vos machines virtuelles.
  Notes
  La région doit prendre en charge Log Analytics. Vous pouvez passer en revue les régions qui prennent en charge Log Analytics. Dans la zone **Rechercher un produit**, entrez « Azure Monitor ».
- **Tarification** : le niveau tarifaire par défaut d'un nouvel espace de travail est le *paiement à l'utilisation*. Les frais incombent uniquement une fois que vous avez commencé à collecter des données.

Configurer Network Watcher

Décrire les fonctionnalités d’Azure Network Watcher

Azure Network Watcher offre des outils permettant d’effectuer un monitoring et des diagnostics, d’afficher les métriques et d’activer et de désactiver les journaux d’activité pour les ressources se trouvant sur un réseau virtuel Azure. Network Watcher est un service régional qui vous permet de superviser et de diagnostiquer les conditions au niveau d’un scénario réseau.

Éléments à connaître concernant Network Watcher

Fonctionnalité	Description	Scénarios
Vérification du flux IP	Diagnostiquez rapidement les problèmes de connectivité depuis ou vers Internet, et depuis ou vers votre environnement local.	*Déterminer si une règle de sécurité bloque le trafic entrant ou sortant vers ou depuis une machine virtuelle* *Résoudre les problèmes pour déterminer si une autre exploration est nécessaire*
Tronçon suivant	Affichez le point de connexion suivant (ou *tronçon suivant*) dans votre route réseau et analysez la configuration de votre routage réseau.	*Déterminer s’il existe un tronçon suivant et affichez la cible, le type et la table de routage du tronçon suivant* *Vérifier que le trafic atteint une destination cible prévue*

Résolution des problèmes de VPN	Diagnostiquez et résolvez les problèmes d'intégrité de votre passerelle de réseau virtuel ou de votre connexion avec les données collectées. Affichez les statistiques de connexion, les informations sur le processeur et la mémoire, les erreurs de sécurité IKE, les paquets ignorés ainsi que les mémoires tampons et événements.	*Afficher les diagnostics récapitulatifs dans le portail Azure* *Passer en revue les diagnostics détaillés dans les fichiers journaux générés stockés dans votre compte de stockage Azure* *Résoudre simultanément les problèmes de plusieurs passerelles ou connexions*
Diagnostics NSG	Utilisez les journaux de flux pour mapper le trafic IP par le biais d'un groupe de sécurité réseau (NSG) et collectez des données de diagnostic. Une implémentation courante pour les journaux de flux NSG consiste à satisfaire aux réglementations de conformité de sécurité et aux exigences d'audit.	*Définir des règles de groupe de sécurité réseau prescriptives pour votre organisation et effectuer des audits de conformité périodiques* *Comparer vos règles de groupe de sécurité réseau prescriptives aux règles effectives pour chaque machine virtuelle de votre réseau*

Résolution des problèmes de connexion	« Résolution des problèmes de connexion Azure Network Watcher » est un ajout récent à la suite d'outils et de fonctionnalités réseau de Network Watcher. Vérifiez une connexion TCP ou ICMP directe d'une machine virtuelle, d'une passerelle d'application ou d'un hôte Azure Bastion à une machine virtuelle, à un nom de domaine complet (FQDN), à un URI ou à une adresse IPv4.	*Résoudre vos problèmes de connectivité et de performances réseau dans Azure* *Résoudre les problèmes de connexion pour une machine virtuelle, une passerelle d'application ou un hôte Azure Bastion*

(!) Notes

Pour utiliser Network Watcher, vous devez être Propriétaire, Contributeur ou Contributeur de réseaux. Si vous créez un rôle personnalisé, il doit être en mesure de lire, d'écrire et de supprimer le service Network Watcher.

Passer en revue les diagnostics de vérification des flux IP

La fonctionnalité de **vérification des flux IP** dans Azure Network Watcher vérifie la connectivité depuis ou vers Internet et depuis ou vers votre environnement local. Cette fonctionnalité vous aide à déterminer si une règle de sécurité bloque le trafic à destination ou en provenance de votre machine virtuelle ou d'Internet.

Ce qu'il faut savoir sur la vérification des flux IP

- Vous configurez la fonctionnalité de vérification des flux IP avec les propriétés suivantes dans le portail Azure :
    - Vos abonnement et groupe de ressources
    - Adresse IP locale (source) et numéro de port local
    - Adresse IP distante (de destination) et numéro de port distant
    - Protocole de communication (TCP ou UDP)
    - Sens du trafic (entrant ou sortant)
- La fonctionnalité teste la communication pour une machine virtuelle cible avec des règles de groupe de sécurité réseau (NSG) associées en exécutant des paquets entrants et sortants vers et depuis la machine.
- Une fois les séries de tests terminées, la fonctionnalité vous indique si la communication avec la machine réussit (autorise l'accès) ou échoue (refuse l'accès).
- Si la machine cible refuse le paquet en raison d'un groupe de sécurité réseau, la fonctionnalité retourne le nom de la règle de sécurité de contrôle.

Passer en revue les diagnostics de tronçon suivant

La fonctionnalité de **tronçon suivant** dans Azure Network Watcher vérifie si le trafic est dirigé vers la destination prévue. Cette fonctionnalité vous permet d'afficher le point de connexion suivant (ou *tronçon suivant*) dans votre route réseau et vous aide à vérifier une configuration réseau correcte.

Ce qu'il faut savoir sur la fonctionnalité de tronçon suivant

- Vous configurez la fonctionnalité de tronçon suivant avec les propriétés suivantes dans le portail Azure :
    - Vos abonnement et groupe de ressources
    - Machine virtuelle et interface réseau
    - Adresse IP source
    - Adresse IP de destination (si vous souhaitez vérifier qu'une cible spécifiée est accessible)
- La fonctionnalité teste le point de connexion suivant dans la configuration de votre route réseau.
- Le test du tronçon suivant retourne trois éléments :
    - Type de tronçon suivant
    - Adresse IP du tronçon suivant (si disponible)
    - Table de routage pour le tronçon suivant (si disponible)
- Le type de tronçon suivant peut être *Internet*, *VirtualAppliance*, *VirtualNetworkGateway*, *VirtualNetwork*, *VirtualNetworkPeering*, *VirtualNetworkServiceEndpoint*, *MicrosoftEdge* ou *None*.
- Si le tronçon suivant est une route définie par l'utilisateur, le processus retourne cette route. Sinon, la fonctionnalité de tronçon suivant retourne la route système.
- Si le tronçon suivant est de type *None*, il peut y avoir une route système valide vers l'adresse IP de destination, mais aucun tronçon suivant n'existe pour acheminer le trafic vers la cible.

Visualiser la topologie du réseau

Azure Network Watcher fournit un outil de **topologie** de supervision réseau pour aider les administrateurs à visualiser et à comprendre l'infrastructure.

Choses à savoir sur l'outil de topologie

- L'outil Topologie de Network Watcher permet de générer un diagramme visuel des ressources d'un réseau virtuel.
- L'affichage graphique montre les ressources du réseau, leurs interconnexions et leurs relations les unes avec les autres.
- Vous pouvez afficher les sous-réseaux, les machines virtuelles, les interfaces réseau, les adresses IP publiques, les groupes de sécurité réseau, les tables de routage, etc.

- Pour générer une topologie, vous avez besoin d’une instance Azure Network Watcher dans la même région que le réseau virtuel.