

# AZ-104

## Domaines de connaissance de l'examen :

- Gérer les identités et la gouvernance Azure (15–20 %)
- Implémenter et gérer le stockage (15–20 %)
- Déployer et gérer les ressources de calcul Azure (20–25%)
- Configurer et gérer des réseaux virtuels (20–25 %)
- Superviser les ressources Azure et en assurer la maintenance (10–15 %)

## Prérequis pour les administrateurs Azure

### Objectifs d'apprentissage

Dans ce module, vous allez découvrir comment :

- Gérer les ressources avec le portail Azure.
- Gérer les ressources avec Azure Cloud Shell.
- Gérer les ressources avec Azure PowerShell.
- Gérer les ressources avec Azure CLI.

### Configurer les ressources Azure avec des outils

#### Azure Cloud Shell

Azure Cloud Shell est un shell interactif, accessible par navigateur pour la gestion des ressources Azure. Les utilisateur **Linux** peuvent choisir d'utiliser **Bash**, et les utilisateurs **Windows** l'option **Powershell**

#### Fonctionnalités d'Azure Cloud Shell

- Est temporaire et nécessite le montage d'un partage Azure Files nouveau ou existant.
- Offre un éditeur de texte graphique intégré, basé sur l'éditeur open source Monaco.
- S'authentifie automatiquement pour accéder instantanément à vos ressources.
- S'exécute sur un hôte temporaire fourni en fonction de chaque session et de chaque utilisateur.
- Expire après 20 minutes en l'absence d'activité interactive.
- Nécessite un groupe de ressources, un compte de stockage et un partage de fichiers Azure.
- Utilise le même partage de fichiers Azure pour Bash et PowerShell.
- Est affecté à une seule machine par compte d'utilisateur.

- Persiste \$HOME en utilisant une image de 5 Go stockée dans votre partage de fichiers.
- Les autorisations sont définies en tant qu'utilisateur Linux standard dans Bash.

### Utilisation d'Azure PowerShell

Azure PowerShell est un module que vous ajoutez à Windows PowerShell ou PowerShell Core. Il vous permet de vous connecter à votre abonnement Azure et de gérer les ressources. Azure PowerShell a besoin de PowerShell pour fonctionner. PowerShell propose des services comme la fenêtre shell et l'analyse des commandes. Azure PowerShell ajoute les commandes spécifiques à Azure.

Azure PowerShell est également disponible sous deux formes :

- dans un navigateur via Azure Cloud Shell
- dans une installation locale sur les systèmes d'exploitation Linux, macOS ou Windows

Il propose **deux modes** :

- le mode **interactif** qui permet d'émettre une commande à la fois
- le mode **script** qui permet d'exécuter un script composé de plusieurs commandes

Qu'est-ce que le module Az?

**Az** est le nom officiel **du module Azure Powershell contenant les applets de commande qui permettent d'utiliser les fonctionnalités Azure**. Il contient des centaines d'applets de commande qui vous permettent de contrôler quasiment tous les aspects de chaque ressource Azure.

Utiliser l'interface de ligne de commande Microsoft Azure

Azure CLI est un programme en ligne de commande qui permet de se connecter à Azure et d'exécuter des commandes d'administration sur les ressources Azure. Il s'exécute sur Linux, macOS et Windows.

Vous pouvez installer l'interface CLI localement sur les ordinateurs qui exécutent les systèmes d'exploitation Linux, macOS ou Windows. Vous pouvez également utiliser Azure CLI à partir d'un navigateur via Azure Cloud Shell.

Dans les deux cas, Azure CLI peut être utilisé de manière interactive ou via des scripts :

- **Mode interactif**. Tout d'abord, pour les systèmes d'exploitation Windows, lancez un interpréteur de commandes tel que cmd.exe, ou utilisez Bash pour Linux ou macOS. Émettez ensuite la commande à l'invite de l'interpréteur de commandes.
- **Mode script**. Assemblez des commandes Azure CLI dans un script d'interpréteur de commandes à l'aide de la syntaxe de script de l'interpréteur de commandes de votre choix. Exécutez ensuite le script.

Les commandes de l'interface CLI sont structurées en *groupes* et *sous-groupes*. Chaque groupe représente un service fourni par Azure, et les sous-groupes séparent les commandes pour ces services en regroupements logiques. Par exemple, le groupe **storage** contient des sous-groupes, incluant **compte**, **blob**, **partage** et **file d'attente**.

La commande **az find** permet de trouver des commandes particulières : `az find blob`.

L'argument **-help** permet d'obtenir des informations détaillées sur une commande : `az storage blob -help`.

## Utiliser Azure Resource Manager

### Objectifs d'apprentissage

Dans ce module, vous allez découvrir comment :

- Identifier les fonctionnalités et les cas d'usage Azure Resource Manager.
- Décrire chaque composant Azure Resource Manager et son utilisation.
- Organiser vos ressources Azure avec des groupes de ressources.
- Appliquer des verrous Azure Resource Manager.
- Déplacer des ressources Azure entre des groupes, des abonnements et des régions.
- Supprimer des ressources et des groupes de ressources.
- Appliquer et suivre les limites des ressources.

### Passer en revue les avantages d'Azure Resource Manager

Azure Resource Manager vous permet de travailler avec les ressources de solution sous forme de groupe. Vous pouvez déployer, mettre à jour ou supprimer toutes les ressources de votre solution dans le cadre d'une opération unique et coordonnée. Vous utilisez un modèle de déploiement pouvant fonctionner avec différents environnements (environnements de test, intermédiaire et de production). Azure Resource Manager assure des fonctions de sécurité, d'audit et de catégorisation pour vous aider à gérer vos ressources après le déploiement.

### Couche de gestion cohérente

Azure Resource Manager fournit une couche de gestion cohérente pour effectuer des tâches avec Azure PowerShell, Azure CLI, le portail Azure, l'API REST et les kits SDK clients.

Les outils interagissent avec la même API Azure Resource Manager. L'API transmet les requêtes au service Azure Resource Manager, qui les authentifie et les autorise. Ensuite, Azure Resource Manager route les requêtes vers les fournisseurs de ressources appropriés.

## Avantages

- Déployer, gérer et surveiller toutes les ressources de votre solution comme un groupe
- Déployé de manière répétée tout au long du cycle de développement
- Mode déclaratif
- Définir les dépendances entre les ressources pour l'ordre de déploiement
- Appliquer le RBAC dans les définitions de ressources
- Tags des ressources
- Facturation sur la base de tag

## Réviser la terminologie en lien avec les ressources Azure

- Ressource : élément gérable disponible dans Azure
- Groupe de ressources : conteneur qui contient des ressources associées pour une solution Azure
- Fournisseur de ressources : service qui fournit les ressources que vous pouvez déployer et gérer via Resource Manager. Microsoft.Compute, qui fournit la ressource de machine virtuelle ; Microsoft.Storage, qui fournit la ressource du compte de stockage. Chaque fournisseur de ressource propose un ensemble de ressources et d'opérations permettant de gérer un service Azure/\$.
- Modèle : fichier JSON qui définit les ressources à déployer sur un groupe de ressources avec leur dépendance
- syntaxe déclarative : qui permet de déclarer voici ce que je souhaite créer

Le nom d'un type de ressource est au format : **{fournisseur de ressources}/{type de ressource}**. Par exemple, le type de coffre de clés est **Microsoft.KeyVault\vaults**.

## Créer des groupes de ressources

Le déploiement de ressources dans un groupe de ressources devient un travail qui vous permet de suivre l'exécution du modèle. Si le déploiement échoue, **la sortie du travail peut décrire la raison de l'échec du déploiement**. Que le déploiement **soit effectué d'une ressource unique à un groupe ou d'un modèle à un groupe, vous pouvez utiliser ces informations pour corriger les erreurs et redéployer**. Les **déploiements sont incrémentiels** : si un groupe de ressources contient deux applications web et que vous décidez d'en déployer un troisième, les applications web existantes ne sont pas supprimées.

## Considérations

- Les ressources peuvent appartenir à un seul groupe de ressources à la fois.
- Les groupes de ressources ne peuvent pas être renommés.
- Les groupes de ressources peuvent avoir des ressources de types différents (services).

- Les groupes de ressources peuvent avoir des ressources provenant de différentes régions.

#### Création de groupes de ressources

La création d'un rg doit considérer des facteurs importants :

- Toutes les ressources de votre groupe doivent partager le même cycle de vie. Les opérations de déploiement, de mise à jour et de suppression porteront sur toutes les ressources du groupe.
- Vous pouvez à tout moment ajouter ou supprimer une ressource au niveau d'un groupe de ressources.
- Vous pouvez déplacer une ressource d'un groupe de ressources vers un autre groupe. Les limitations s'appliquent au [déplacement de ressources](#).

#### Créer des verrous Azure Resource Manager

- Vous pouvez associer le verrou à un abonnement, à un groupe de ressources ou à une ressource.
- Les ressources enfants héritent des verrous.

#### Types de verrou

- **Verrous en lecture seule**, qui empêchent toute modification apportée à la ressource.
- **Verrous de suppression**, qui empêchent la suppression.

#### Réorganiser les ressources Azure

Lors du déplacement de ressource vers un autre groupe de ressource, le groupe source et le groupe cible sont verrouillés. Vous ne pouvez pas **ajouter, mettre à jour ou supprimer des ressources dans le groupe de ressources**. Les **ressources restent opérationnelles et accessibles**.

#### Suppression de ressources et de rg

La suppression d'un rg => la suppression de toutes les ressources qu'elle contient.

#### Suppression d'un rg avec powershell

```
Remove-AzResourceGroup -Name "ContosoRG01"
```

#### Déterminer les limites des ressources

L'utilisation des ressources peut être observée par rapport aux limites.

- Lorsque vous avez besoin d'augmenter une limite par défaut, il existe un lien Demander une augmentation.
- Toutes les ressources ont une limite maximale répertoriée dans les [limites Azure](#).
- Si vous êtes à la limite maximale, la limite ne peut pas être augmentée.

# Configurer des ressources avec des modèles Azure Resource Manager

## Explorer le schéma des modèles Azure Resource Manager

Les modèles Azure Resource Manager sont écrits en JSON. Chaque clé est une chaîne, dont la valeur peut être :

- Chaîne
- un chiffre
- Une expression booléenne
- Une liste de valeurs
- Un objet (qui est une collection d'autres paires clé/valeur)

Un modèle Resource Manager peut contenir des sections exprimées en notation JSON, mais qui ne sont pas liées au langage JSON lui-même :

```
{
  "$schema":
"http://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.js
on#",
  "contentVersion": "",
  "parameters": {},
  "variables": {},
  "functions": [],
  "resources": [],
  "outputs": {}
}
```

Nom de l'élément	Obligatoire	Description
\$schema	Oui	Emplacement du fichier de schéma JSON qui décrit la version du langage du modèle. Utilisez l'URL indiquée dans l'exemple précédent.
contentVersion	Oui	Version du modèle (par exemple, 1.0.0.0). Vous pouvez fournir n'importe

		quelle valeur pour cet élément. Utilisez cette valeur pour documenter les modifications importantes dans votre modèle. Cette valeur peut être utilisée pour s'assurer que le bon modèle est utilisé.
parameters	Non	Valeurs fournies lors de l'exécution du déploiement pour personnaliser le déploiement des ressources.
variables	Non	Valeurs utilisées en tant que fragments JSON dans le modèle pour simplifier les expressions du langage du modèle.
functions	Non	Fonctions définies par l'utilisateur et disponibles dans le modèle.
les ressources	Oui	Types de ressource déployés ou mis à jour dans un groupe de ressources.
outputs	Non	Valeurs retournées après le déploiement.

## Explorer les paramètres des modèles Azure Resource Manager

C'est dans la section des paramètres du modèle que vous pouvez spécifier les valeurs que vous pouvez saisir lors du déploiement des ressources. Les propriétés disponibles pour un paramètre sont :

```
"parameters": {
  "<parameter-name>" : {
    "type" : "<type-of-parameter-value>",
    "defaultValue": "<default-value-of-parameter>",
```

```

    "allowedValues": [ "<array-of-allowed-values>" ],
    "minValue": <minimum-value-for-int>,
    "maxValue": <maximum-value-for-int>,
    "minLength": <minimum-length-for-string-or-array>,
    "maxLength": <maximum-length-for-string-or-array-parameters>,
    "metadata": {
      "description": "<description-of-the parameter>"
    }
  }
}

```

Voici un exemple qui montre deux paramètres, un pour le nom d'utilisateur d'une machine virtuelle et un pour son mot de passe :

```

"parameters": {
  "adminUsername": {
    "type": "string",
    "metadata": {
      "description": "Username for the Virtual Machine."
    }
  },
  "adminPassword": {
    "type": "securestring",
    "metadata": {
      "description": "Password for the Virtual Machine."
    }
  }
}
}

```

## Examen des modèles Bicep

[Azure Bicep](#) est un langage spécifique à un domaine (DSL) qui utilise la syntaxe déclarative pour déployer des ressources Azure. Il fournit une syntaxe concise, une cohérence des types fiable et une prise en charge de la réutilisation du code.

Vous pouvez utiliser Bicep au lieu de JSON pour développer vos modèles Azure Resource Manager (modèles ARM).

Bicep est une abstraction transparente sur un modèle ARM JSON et ne perd aucune des fonctionnalités de modèle JSON.

### Comment fonctionne Bicep ?

Lorsque vous déployez une ressource ou une série de ressources sur Azure, les outils intégrés à Bicep convertissent votre modèle Bicep en modèle JSON. On parle alors de transpilation. La transpilation est le processus qui consiste à convertir le code source écrit dans un langage dans un autre langage.

Les avantages de Bicep par rapport à JSON :



- **Syntaxe plus simple** : Bicep fournit une syntaxe plus simple pour l'écriture de modèles. Vous pouvez référencer des paramètres et des variables directement, sans utiliser de fonctions complexes. L'interpolation de chaîne est utilisée à la place de la concaténation pour combiner des valeurs pour les noms et d'autres éléments. Vous pouvez référencer directement les propriétés d'une ressource à l'aide de son nom symbolique au lieu d'instructions de référence complexes. Ces améliorations de syntaxe permettent de créer et de lire des modèles Bicep.
- **Modules** : vous pouvez décomposer des déploiements de modèles complexes en fichiers de modules plus petits et les référencer dans un modèle principal. Ces modules facilitent la gestion et la réutilisation accrue.
- **Gestion automatique des dépendances** : dans la plupart des cas, Bicep détecte automatiquement les dépendances entre vos ressources. Ce processus supprime une partie du travail impliqué dans la création de modèles.
- **Validation de type et IntelliSense** : l'extension Bicep pour Visual Studio Code intègre une validation riche et IntelliSense pour toutes les définitions d'API de type de ressource Azure. Cette fonctionnalité permet d'obtenir une expérience de création plus simple.

Les [modèles de démarrage rapide Azure](#) sont des modèles Resource Manager qui sont fournis par la communauté Azure.

- Le fichier README.md fournit une vue d'ensemble de ce que fait le modèle.
- Le fichier azuredeploy.json définit les ressources qui seront déployées.
- Le fichier azuredeploy.parameters.json fournit les valeurs dont le modèle a besoin.

## Automatiser des tâches Azure à l'aide de scripts avec PowerShell

Décider si Azure PowerShell convient à vos tâches

Qu'est-ce que le portail Azure ?

Le portail Azure est un site web qui vous permet de créer, configurer et modifier des ressources dans votre abonnement Azure.

Qu'est-ce qu'Azure CLI ?

Azure CLI est un programme en ligne de commande multiplateforme permettant de se connecter à Azure et d'exécuter des commandes d'administration sur des ressources Azure.

Comment choisir un outil d'administration

- **Automation** : Avez-vous besoin d'automatiser un ensemble de tâches complexes ou répétitives ? Azure PowerShell et Azure CLI prennent l'automatisation en charge, contrairement au portail Azure.
- **Courbe d'apprentissage** : Avez-vous besoin d'effectuer une tâche rapidement sans apprendre de nouvelles commandes ou une nouvelle syntaxe ? Le portail Azure ne nécessite pas d'apprentissage de syntaxe ou de mémorisation de commandes. Dans Azure PowerShell et Azure CLI, vous devez connaître la syntaxe détaillée de chaque commande que vous utilisez.
- **Ensemble de compétences de l'équipe** : Votre équipe a-t-elle déjà une expertise ? Par exemple, votre équipe a peut-être utilisé PowerShell pour administrer Windows. Dans ce cas, elle sera rapidement à l'aise avec Azure PowerShell.

Installer PowerShell

Nous allons passer en revue les instructions d'installation proprement dites dans l'unité suivante, mais examinons les deux composants qui constituent Azure PowerShell.

- **Produit PowerShell de base** Il existe deux variantes : Windows PowerShell et PowerShell 7.x, que vous pouvez installer sur Windows, macOS et Linux.
- **Module Azure Az PowerShell** Ce module supplémentaire doit être installé pour permettre l'ajout à PowerShell des commandes spécifiques à Azure.

```
curl https://packages.microsoft.com/keys/microsoft.asc | sudo apt-key add -  
sudo curl -o /etc/apt/sources.list.d/microsoft.list  
https://packages.microsoft.com/config/ubuntu/18.04/prod.list  
sudo apt-get update  
sudo apt-get install -y powershell  
pwsh
```

Créer une ressource Azure à l'aide de scripts dans Azure PowerShell

Que sont les applets de commande PowerShell ?

Une commande PowerShell est appelée une **cmdlet** (prononcez « command-let »). Une cmdlet est une commande qui manipule une fonctionnalité unique. Le terme

**cmdlet** désigne une « petite commande ». Par convention, les auteurs de cmdlets sont encouragés à créer des cmdlets simples et à fonction unique.

Le produit PowerShell de base est fourni avec des cmdlets qui travaillent avec des fonctionnalités telles que des sessions et des tâches d'arrière-plan. Vous pouvez ajouter des modules à votre installation PowerShell pour obtenir des applets de commande qui manipulent d'autres fonctionnalités.

Les applets de commande suivent une convention de nommage de type **verbe-nom**, par exemple `Get-Process`, `Format-Table` et `Start-Service`. Il existe également une convention quant au choix du verbe : « **get** » pour récupérer des données, « **set** » pour insérer ou mettre à jour des données, « **format** » pour mettre en forme des données, « **out** » pour diriger une sortie vers une destination, etc.

Qu'est-ce qu'un module PowerShell ?

Les applets de commande sont livrées dans des *modules*. Un module PowerShell est une DLL comprenant le code pour traiter chaque applet de commande disponible. Vous chargez des applets de commande dans PowerShell en chargeant le module qui les contient. Vous pouvez obtenir la liste des modules chargés en utilisant la commande `Get-Module`.

Qu'est-ce que le module Az PowerShell ?

**Az** est le nom officiel du module Azure PowerShell qui contient les applets de commande qui permettent d'utiliser les fonctionnalités Azure. Il contient des centaines d'applets de commande qui vous permettent de contrôler quasiment tous les aspects de chaque ressource Azure.

Installer le module Az PowerShell

`pwsh`

`Install-Module -Name Az -Scope CurrentUser -Repository PSGallery -Force`

Mettre à jour un module PowerShell

`Update-Module -Name Az`

Connecter

`Connect-AzAccount`

Utiliser des abonnements

`Set-AzContext -Subscription '00000000-0000-0000-0000-000000000000'`

Obtenir la liste de tous les groupes de ressources

`Get-AzResourceGroup`

Pour une liste plus concise

## Get-AzResourceGroup | Format-Table

Création d'une machine virtuelle avec PowerShell

```
New-AzVm -ResourceGroupName learn-0a18bc7f-2912-495f-9a15-ac6a0333b7a6  
-Name "testvm-eus-01" -Credential (Get-Credential) -Location "eastus" -Image  
Canonical:0001-com-ubuntu-server-focal:20_04-lts:latest -OpenPorts 22  
-PublicIpAddressName "testvm-01"  
User : dino  
Password : Test1234
```

Récupérer les informations d'une VM

```
$vm = (Get-AzVM -Name "testvm-eus-01" -ResourceGroupName  
learn-0a18bc7f-2912-495f-9a15-ac6a0333b7a6)  
$vm.HardwareProfile  
$vm.StorageProfile.OsDisk
```

Passez l'objet de machine virtuelle à d'autre applet

```
$vm | Get-AzVMSize
```

Pour obtenir l'adresse IP publique

```
Get-AzPublicIpAddress -ResourceGroupName  
learn-0a18bc7f-2912-495f-9a15-ac6a0333b7a6 -Name "testvm-01"
```

Arrêter une machine virtuelle

```
Stop-AzVM -Name $vm.Name -ResourceGroupName $vm.ResourceGroupName
```

Supprimer une machine virtuelle

```
Remove-AzVM -Name $vm.Name -ResourceGroupName  
$vm.ResourceGroupName
```

Lister les ressources dans un groupe de ressource

```
Get-AzResource -ResourceGroupName $vm.ResourceGroupName | Format-Table
```

Supprimer l'interface réseau

```
$vm | Remove-AzNetworkInterface -Force
```

Supprimer les disques de système d'exploitation managés

```
Get-AzDisk -ResourceGroupName $vm.ResourceGroupName -DiskName  
$vm.StorageProfile.OSDisk.Name | Remove-AzDisk -Force
```

Supprimer le réseau virtuel

```
Get-AzVirtualNetwork -ResourceGroupName $vm.ResourceGroupName |  
Remove-AzVirtualNetwork -Force
```

Supprimer le groupe de sécurité réseau

```
Get-AzNetworkSecurityGroup -ResourceGroupName $vm.ResourceGroupName |  
Remove-AzNetworkSecurityGroup -Force
```

Supprimer l'adresse IP publique

```
Get-AzPublicIpAddress -ResourceGroupName $vm.ResourceGroupName |  
Remove-AzPublicIpAddress -Force
```

## Créer et enregistrer des scripts dans Azure PowerShell

Qu'est-ce qu'un script PowerShell ?

Un script PowerShell est un fichier texte contenant des commandes et des constructions de contrôle. Les commandes sont des cmdlets. Les constructions de contrôle sont des fonctionnalités de programmation telles que des boucles, des variables, des paramètres, des commentaires, etc., fournies par PowerShell.

Les fichiers de script PowerShell ont une extension de fichier **.ps1**.

Après avoir écrit le script, exécutez-le à partir de la ligne de commande PowerShell en spécifiant le nom du fichier précédé d'un point et d'une barre oblique inverse :

```
.\myScript.ps1
```

### Variables

```
$loc = "East US"
```

```
$iterations = 3
```

```
$adminCredential = Get-Credential
```

```
$loc = "East US"
```

```
New-AzResourceGroup -Name "MyResourceGroup" -Location $loc
```

Boucles

```
For ($i = 1; $i -lt 3; $i++)
```

```
{
```

```
    $i
```

```
}
```

Paramètres

Passez des paramètres à un script :

```
.\setupEnvironment.ps1 -size 5 -location "East US"
```

Capturez les valeurs des paramètres dans des variables avec des correspondances par nom :

```
param([string]$location, [int]$size)
```

Passez des paramètres sans noms :

```
.\setupEnvironment.ps1 5 "East US"
```

Dans le script la capture dépend de la position :

```
param([int]$size, [string]$location)
```

Authentification

```
Connect-AzAccount
```

Script

```
param([string]$resourceGroup)
```

```
$adminCredential = Get-Credential -Message "Enter a username  
and password for the VM administrator."
```

```
For ($i = 1; $i -le 3; $i++)
```

```
{
```

```
    $vmName = "ConferenceDemo" + $i
```

```
    Write-Host "Creating VM: " $vmName
```

```
    New-AzVm -ResourceGroupName $resourceGroup -Name $vmName  
-Credential $adminCredential -Image
```

```
Canonical:0001-com-ubuntu-server-focal:20_04-lts:latest
```

```
}
```

Exécution du script

```
./ConferenceDailyReset.ps1 learn-0a18bc7f-2912-495f-9a15-ac6a0333b7a6
```

Suppression d'un groupe de ressource

```
Remove-AzResourceGroup -Name MyResourceGroupName
```

## Contrôler les services Azure avec l'interface de ligne de commande

Qu'est-ce qu'Azure CLI ?

```
variable="value"
```

```
variable=integer
```

Azure CLI vous permet de contrôler presque tous les aspects de chaque ressource Azure. Vous pouvez travailler avec des groupes de ressources, du stockage, des

machines virtuelles, Azure Active Directory (Azure AD), des conteneurs, l'apprentissage automatique, etc.

Les commandes de l'interface CLI sont structurées en *groupes* et *sous-groupes*. Chaque groupe représente un service fourni par Azure, et les sous-groupes séparent les commandes pour ces services en regroupements logiques. Par exemple, le groupe **storage** contient des sous-groupes, dont **account**, **blob** et **queue**.

Trouver les commandes avec az find

```
az group create --name <name> --location <location>
```

Filtrer les valeurs de retour

```
az group list --query "[?name == '$RESOURCE_GROUP']"
```

Création de ressource

```
# création d'un groupe de ressource : az group create
az appservice plan create --name $AZURE_APP_PLAN --resource-group
$RESOURCE_GROUP --location $AZURE_REGION --sku FREE
# vérification de la ressource créée
az appservice plan list --output table
# création de la webapp
az webapp create --name $AZURE_WEB_APP --resource-group
$RESOURCE_GROUP --plan $AZURE_APP_PLAN
# verification que l'app a bien été créée
az webapp list --output table
# déploiement du code
az webapp deployment source config --name $AZURE_WEB_APP --resource-group
$RESOURCE_GROUP --repo-url
"https://github.com/Azure-Samples/php-docs-hello-world" --branch master
--manual-integration
```

## Déployer l'infrastructure Azure en utilisant des modèles ARM JSON

Explorer la structure du modèle Azure Resource Manager

Qu'est ce que l'infrastructure en tant que code ?

L'infrastructure en tant que code vous permet de décrire, par le biais du code, l'infrastructure dont vous avez besoin pour votre application. Les avantages de l'infrastructure en tant que code sont les suivants :

- Configurations cohérentes
- Scalabilité améliorée
- Déploiements plus rapides
- Meilleure traçabilité

Qu'est ce qu'un modèle ARM?

Les modèles ARM sont des fichiers JavaScript Object Notation (JSON) qui définissent l'infrastructure et la configuration de votre déploiement. Le modèle utilise une *syntaxe déclarative*. La syntaxe déclarative est un moyen de générer la structure et les éléments qui soulignent les ressources qui ressembleront sans décrire son flux de contrôle. La syntaxe déclarative est différente de la *syntaxe impérative*, qui utilise des commandes que l'ordinateur doit exécuter. Les scripts impératifs se concentrent sur la spécification de chaque étape du déploiement des ressources.

Avantages de l'utilisation des modèles ARM

Les modèles ARM vous permettent:

- d'automatiser les déploiements
- d'utiliser la pratique de l'infrastructure en tant que code (IaC)
- Le code du modèle devient partie intégrante de vos projets d'infrastructure et de développement
- vous pouvez stocker les fichiers IaC dans un référentiel source et la mettre en version.
- validation intégrée de vérification du modèle avant son déploiement
- peuvent être scindés en composants ARM plus petits et réutilisables
- imbriquer des modèles dans d'autres modèles
- consulter l'historique des déploiements et des informations sur leur état

Les modèles ARM sont **idempotents**, ce qui signifie que vous pouvez déployer plusieurs fois le même modèle et récupérer les mêmes types de ressource dans le même état.

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.
<b>apiProfile</b>	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.
<b>parameters</b>	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.
<b>variables</b>	Une section facultative où vous définissez des valeurs utilisées pour simplifier les expressions de langage de gabarit.
<b>functions</b>	Une section facultative où vous pouvez définir des <a href="#">fonctions définies par l'utilisateur</a> 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.
<b>resources</b>	Une section obligatoire qui définit les éléments réels que vous voulez déployer ou mettre à jour dans un groupe de ressources ou un abonnement.
<b>output</b>	Une section facultative où vous spécifiez les valeurs qui seront retournées à la fin du déploiement.

## Déployer un modèle ARM sur Azure

Vous pouvez déployer un modèle ARM sur Azure de l'une des manières suivantes :

- Déployer un modèle local.
- Déployer un modèle lié.
- Déployer dans un pipeline de déploiement continu.

Pour le déploiement local il faut Azure PowerShell ou Azure CLI localement.

Se connecter au préalable : `az login`

Définir un groupe de ressources, soit en utilisant un existant ou en créant un. Vous

peuvent obtenir les valeurs de localisation disponibles à partir de : `az account`

`list-locations` (CLI) ou `Get-AzLocation` (PowerShell). Vous pouvez

configurer le lieu par défaut en utilisant `az configure --defaults`

`location=<location>`.

```
az group create \
```

```
  --name {name of your resource group} \
```

```
  --location "{location}"
```

Pour démarrer un déploiement de modèle au niveau du groupe de ressources, utilisez la commande Azure CLI [az deployment group create](#) ou la commande Azure PowerShell [New-AzResourceGroupDeployment](#).

Les deux commandes **nécessitent le groupe de ressources, la région et le nom du déploiement** pour pouvoir l'identifier facilement dans l'historique de déploiement.

```
templateFile="{provide-the-path-to-the-template-file}"
az deployment group create \
  --name blanktemplate \
  --resource-group myResourceGroup \
  --template-file $templateFile
```

Pour ajouter une ressource à votre modèle, vous devez connaître le fournisseur de ressources et ses types de ressources. La syntaxe de cette combinaison se présente sous la forme de **{fournisseur-de-ressources}/{type-de-ressources}**. Une fois que vous avez défini le fournisseur et le type de ressource, vous devez comprendre les propriétés de chaque type de ressource que vous voulez utiliser. Pour plus d'informations, consultez [Définir des ressources dans les modèles Azure Resource Manager](#). Affichez la liste dans la colonne de gauche pour rechercher la ressource. Notez que les propriétés sont triées par version de l'API.

```
{
  "$schema":
  "https://schema.management.azure.com/schemas/2019-04-01/deploy
mentTemplate.json#",
  "contentVersion": "1.0.0.1",
  "apiProfile": "",
  "parameters": {},
  "variables": {},
  "functions": [],
  "resources": [
    {
      "type": "Microsoft.Storage/storageAccounts",
      "apiVersion": "2019-06-01",
      "name": "learntemplatestorage123",
      "location": "westus",
      "sku": {
        "name": "Standard_LRS"
      },
      "kind": "StorageV2",
      "properties": {
        "supportsHttpsTrafficOnly": true
      }
    }
  ]
}
```

```

    }
  ],
  "outputs": {}
}

```

Ajouter de la flexibilité à votre modèle Azure Resource Manager à l'aide de paramètres et de sorties

Paramètres de modèle ARM

Les paramètres de modèle ARM vous permettent de personnaliser le déploiement en fournissant des valeurs adaptées à un environnement particulier.

Dans la section `parameters` du modèle, vous spécifiez les valeurs que vous pouvez entrer quand vous déployez les ressources. Vous êtes **limité à 256 paramètres dans un modèle**. Les définitions de paramètre **peuvent utiliser la plupart des fonctions de modèle**.

```

"parameters": {
  "<parameter-name>": {
    "type": "<type-of-parameter-value>",
    "defaultValue": "<default-value-of-parameter>",
    "allowedValues": [
      "<array-of-allowed-values>"
    ],
    "minValue": <minimum-value-for-int>,
    "maxValue": <maximum-value-for-int>,
    "minLength": <minimum-length-for-string-or-array>,
    "maxLength":
<maximum-length-for-string-or-array-parameters>,
    "metadata": {
      "description": "<description-of-the-parameter>"
    }
  }
}

```

Les types de paramètres autorisés sont les suivants :

- chaîne
- secureString
- entiers
- booléen
- objet

- secureObject
- tableau

Les paramètres de modèle avec les types *secureString* ou *secureObject* ne peuvent pas être lus ni collectés après le déploiement de la ressource.

Utiliser des paramètres dans un modèle ARM

Définition :

```
"parameters": {
  "storageAccountType": {
    "type": "string",
    "defaultValue": "Standard_LRS",
    "allowedValues": [
      "Standard_LRS",
      "Standard_GRS",
      "Standard_ZRS",
      "Premium_LRS"
    ],
    "metadata": {
      "description": "Storage Account type"
    }
  }
}
```

Utilisation :

```
"resources": [
  {
    "type": "Microsoft.Storage/storageAccounts",
    "apiVersion": "2019-04-01",
    "name": "learntemplatestorage123",
    "location": "[resourceGroup().location]",
    "sku": {
      "name": "[parameters('storageAccountType')]"
    },
    "kind": "StorageV2",
    "properties": {
      "supportsHttpsTrafficOnly": true
    }
  }
]
```

Instanciation :

```
templateFile="azuredeploy.json"
az deployment group create \
  --name testdeployment1 \
  --template-file $templateFile \
  --parameters storageAccountType=Standard_LRS
```

Sorties d'un modèle ARM

Dans la section outputs de votre modèle ARM, vous pouvez spécifier des valeurs qui seront retournées après un déploiement réussi. Voici les éléments qui composent la section Sorties.

```
"outputs": {
  "<output-name>": {
    "condition": "<boolean-value-whether-to-output-value>",
    "type": "<type-of-output-value>",
    "value": "<output-value-expression>",
    "copy": {
      "count": <number-of-iterations>,
      "input": <values-for-the-variable>
    }
  }
}
```

Élément	Description
<b>output-name</b>	Doit être un identificateur JavaScript valide.
<b>condition</b>	(Facultatif) Une valeur booléenne qui indique si cette valeur de sortie est retournée. Si la valeur est true, elle est incluse dans la sortie du déploiement. Si elle est false, la valeur de sortie est ignorée pour ce déploiement. En l'absence de spécification, la valeur par défaut est true.

<b>type</b>	Le type de la valeur de sortie.
<b>value</b>	(Facultatif) Une expression de langage de gabarit évaluée et retournée sous forme de valeur de sortie.
<b>copy</b>	(Facultatif) La copie est utilisée pour retourner plusieurs valeurs pour une sortie.

Utiliser des sorties dans un modèle ARM

```
"outputs": {
  "storageEndpoint": {
    "type": "object",
    "value":
"[reference('learntemplatestorage123').primaryEndpoints]"
  }
}
```

Notez la partie `reference` de l'expression. Cette fonction obtient l'état d'exécution du compte de stockage.

Redéployer un modèle ARM

Rappelez-vous que les modèles ARM sont **idempotents**, ce qui signifie que vous pouvez **redéployer le modèle dans le même environnement et que, si rien n'a été modifié dans le modèle, rien ne changera dans l'environnement**. Si une modification a été apportée au modèle, par exemple **si vous avez modifié une valeur de paramètre, seule cette modification sera déployée**. Votre modèle peut contenir toutes les ressources dont vous avez besoin pour votre solution Azure et vous pouvez réexécuter sans danger un modèle. Les ressources sont **créées seulement si elles n'existent pas déjà et mises à jour seulement s'il y a une modification**.

## Gérer les identités et la gouvernance dans Azure

### Objectifs d'apprentissage

Dans ce module, vous allez découvrir comment :

- Définir les concepts d'Azure AD, notamment les identités, les comptes et les locataires.
- Décrire les fonctionnalités d'Azure AD qui prennent en charge différentes configurations.
- Comprendre les différences entre Azure AD et Active Directory Domain Services (AD DS).
- Choisir parmi les éditions prises en charge d'Azure AD.

- Implémenter la fonctionnalité de jonction Azure AD.
- Utilisez la fonctionnalité de réinitialisation de mot de passe en libre-service d'Azure AD.

## Décrire les avantages et les fonctionnalités Azure Active Directory

[Azure Active Directory \(Azure AD\)](#) est le service de gestion des identités et d'annuaire cloud multilocataire de Microsoft. Azure AD permet de prendre en charge l'accès utilisateur aux ressources et aux applications, comme :

- Les ressources internes et les applications situées sur votre réseau d'entreprise.
- Les ressources externes comme Microsoft 365, le portail Azure et les applications SaaS.
- Les applications cloud développées pour votre organisation.

Choses à savoir sur les fonctionnalités Azure AD

### Fonctionnalité Azure AD Description

**Accès authentification unique (SSO)** **avec** Azure AD fournit une authentification unique sécurisée aux applications web cloud et aux applications locales. Les utilisateurs peuvent se connecter avec les mêmes informations d'identification pour toutes leurs applications.

**Prise en charge des appareils omniprésents** Azure AD fonctionne sur les appareils iOS, macOS, Android et Windows, et offre la même expérience sur tous. Les utilisateurs peuvent lancer des applications à partir d'un panneau d'accès web personnalisé, d'une application mobile, de Microsoft 365 ou de portails d'entreprise personnalisés avec leurs informations d'identification professionnelles existantes.

<b>Accès à distance sécurisé</b>	Azure AD fournit un accès à distance sécurisé pour les applications web locales. L'accès sécurisé peut inclure l'authentification multifactor (MFA), des stratégies d'accès conditionnel ainsi que la gestion des accès en fonction du groupe. Les utilisateurs peuvent accéder aux applications Web sur site depuis n'importe où, y compris depuis le même portail.
<b>Extensibilité cloud</b>	<b>du</b> Azure AD peut s'étendre au cloud pour vous aider à gérer un ensemble cohérent d'utilisateurs, de groupes, de mots de passe et d'appareils dans différents environnements.
<b>Protection des données sensibles</b>	<b>des</b> Azure AD offre des fonctionnalités uniques de protection des identités permettant de sécuriser vos données et applications sensibles. Les administrateurs peuvent surveiller les activités de connexion suspectes et les vulnérabilités potentielles dans une vue consolidée des utilisateurs et des ressources dans l'annuaire.
<b>Support libre-service</b>	<b>en</b> Azure AD vous permet de déléguer des tâches aux employés de l'entreprise qui seraient généralement effectuées par des administrateurs disposant de privilèges d'accès plus élevés. L'accès aux applications libre-service et la gestion des mots de passe via des étapes de vérification peuvent réduire les appels au support technique et améliorer la sécurité.

Les choses à considérer lors de l'utilisation des fonctionnalités d'Azure AD

Azure AD offre de nombreuses fonctionnalités et avantages. Pensez aux fonctionnalités qui peuvent être utilisées pour mieux prendre en charge vos scénarios d'entreprise.

- **Activation de l'accès avec l'authentification unique.** Activez l'accès à l'authentification unique pour permettre à vos utilisateurs de se connecter au cloud ou d'utiliser des applications locales. L'authentification unique Azure AD prend en charge Microsoft 365 et des milliers d'applications SaaS telles que Salesforce, Workday, DocuSign, ServiceNow et Box.
- **Pensez à l'expérience utilisateur et à la prise en charge des appareils.** Créez une expérience utilisateur cohérente qui fonctionne sur tous les appareils et tous les points d'accès de l'annuaire. Vous pouvez concevoir des



portails d'entreprise personnalisés et un accès web personnalisé qui permette à vos employés de se connecter à l'aide de leurs informations d'identification professionnelles.

- **Avantages de l'accès à distance sécurisé.** Protégez vos applications web locales en implémentant un accès à distance sécurisé à l'aide de l'authentification multifacteur et de stratégies d'accès.
- **Avantages de l'extensibilité cloud.** Connectez Active Directory et d'autres annuaires locaux dans le cloud à Azure AD en quelques étapes seulement. Vous pouvez faciliter la gestion des mêmes utilisateurs, groupes, mots de passe et appareils pour vos administrateurs à travers tous les environnements pris en charge.
- **Utilisation de la protection avancée pour les données sensibles.** Améliorez la sécurité de vos données et applications sensibles à l'aide des fonctionnalités de protection intégrées d'Azure AD. Les administrateurs peuvent utiliser des rapports de sécurité avancés, des notifications, des recommandations de correction et des stratégies basées sur les risques.
- **Réduction des coûts et options libre-service.** Profitez des fonctionnalités libre-service d'Azure AD pour aider à réduire les coûts pour votre organisation. Déléguez à vos utilisateurs non administrateurs certaines tâches comme la réinitialisation des mots de passe, ou la création et la gestion de groupes.

Décrire les concepts Azure Active Directory

<b>Concept Azure AD</b>	<b>Description</b>
<b>Identité</b>	Une <i>identité</i> est un objet qui peut être authentifié. L'identité peut être un utilisateur avec un nom d'utilisateur et un mot de passe. Les identités peuvent également être des applications ou d'autres serveurs qui exigent une authentification à l'aide de clés secrètes ou de certificats. Azure AD est le produit sous-jacent qui fournit le service d'identité.

<b>Compte</b>	Un <i>compte</i> est une identité à laquelle sont associées des données. Pour avoir un compte, vous devez d'abord avoir une identité valide. Vous ne pouvez pas avoir de compte sans identité.
<b>Compte Azure AD</b>	Un <i>compte Azure AD</i> est une identité qui est créée par le biais d'Azure AD ou d'un autre service cloud Microsoft comme Microsoft 365. Les identités sont stockées dans Azure AD et sont accessibles aux abonnements de service cloud de votre organisation. Ce compte est également appelé <i>compte professionnel ou scolaire</i> .
<b>Locataire (annuaire) Azure</b>	Un <i>locataire Azure</i> est une instance dédiée et approuvée d'Azure AD. Chaque locataire (également appelé <i>annuaire</i> ) représente une seule organisation. Quand votre organisation s'inscrit à un abonnement de service cloud Microsoft, un locataire est automatiquement créé. Étant donné que chaque locataire est une instance dédiée et approuvée d'Azure AD, vous pouvez créer plusieurs locataires ou instances.
<b>Abonnement Azure</b>	Un abonnement Azure est utilisé pour payer les services cloud Azure. Chaque abonnement n'est joint qu'à un seul locataire. Vous pouvez avoir plusieurs abonnements.

## Comparer Azure Active Directory à Azure Active Directory Domain Services

Active Directory Domain Services (AD DS) est le déploiement traditionnel d'Active Directory basé sur Windows Server sur un serveur physique ou virtuel. Active Directory Domain Services (AD DS) comprend également Active Directory Certificate Services (AD CS), Active Directory Lightweight Directory Services (AD LDS), Active Directory Federation Services (AD FS) et Active Directory Rights Management Services (AD RMS).

Éléments à prendre en compte lorsque vous utilisez Azure AD plutôt qu'AD DS

Lorsque vous planifiez votre stratégie d'identité, tenez compte des caractéristiques suivantes qui différencient Azure AD et AD DS.

- **Solution d'identité** : AD DS est avant tout un service d'annuaire, tandis qu'Azure AD est une solution d'identité complète. Azure AD est conçu pour les applications basées sur Internet qui utilisent des communications HTTP et

HTTPS. Les fonctionnalités d'Azure AD permettent une gestion forte des identités.

- **Protocoles de communication** : étant donné qu'Azure AD est basé sur HTTP et HTTPS, il n'utilise pas l'authentification Kerberos. Azure AD utilise les protocoles HTTP et HTTPS comme SAML, WS-Federation et OpenID Connect pour l'authentification (et OAuth pour l'autorisation).
- **Services de fédération** : Azure AD comprend des services de fédération et de nombreux services tiers comme Facebook.
- **Structure plate** : les utilisateurs et les groupes Azure AD sont créés dans une structure plate. Il n'existe aucune unité organisationnelle (UO) ni aucun objet de stratégie de groupe (GPO).
- **Service managé** : Azure AD est un service managé. Vous gérez uniquement les utilisateurs, les groupes et les stratégies. Si vous déployez AD DS avec des machines virtuelles à l'aide d'Azure, vous gérez de nombreuses autres tâches, notamment le déploiement, la configuration, les machines virtuelles, la mise à jour corrective et d'autres processus back-end.

## Sélectionner des éditions Azure Active Directory

Azure Active Directory se décline en quatre éditions : **Gratuit**, **Microsoft 365 Apps**, **Premium P1** et **Premium P2**. L'édition gratuite fait partie de tout abonnement Azure. Les éditions Premium sont disponibles via un Contrat Entreprise Microsoft, le programme Open Volume License et le programme Fournisseurs de solutions cloud. Les abonnés Azure et Microsoft 365 peuvent également acheter Azure Active Directory Premium P1 et P2 en ligne.

## Choses à savoir sur les éditions Azure AD

Fonctionnalité	Gratuit	Microsoft 365 Apps	Premium P1	Premium P2
Objets d'annuaire	500 000	Illimité	Illimité	Illimité
Authentification unique	Illimité	Illimité	Illimité	Illimité
Gestion de base des identités et des accès	X	X	X	X
Collaboration interentreprises	X	X	X	X
Gestion des identités et des accès		X	X	X

**pour les applications  
Microsoft 365**

<b>Fonctionnalités Premium</b>	X	X
<b>Identités hybrides</b>	X	X
<b>Gestion avancée des accès aux groupes</b>	X	X
<b>Accès conditionnel</b>	X	X
<b>Identity Protection</b>		X
<b>Gouvernance des identités</b>		X

**Azure Active Directory Microsoft 365 Apps** prend en charge pour Microsoft 365 :

- Une prise en charge supplémentaire inclut la personnalisation
- l'authentification multifacteur
- la gestion des accès aux groupes
- la réinitialisation de mot de passe en libre-service pour les utilisateurs cloud

**Azure Active Directory Premium P1** prend en charge :

- les groupes dynamiques
- la gestion des groupes libre-service
- les fonctionnalités d'écriture différée dans le cloud.
- comprend Microsoft Identity Manager, qui est une suite locale de gestion des identités et des accès
- autorisent la réinitialisation de mot de passe en libre-service pour vos utilisateurs locaux.

**Azure Active Directory Premium P2** comprend :

- Azure AD Identity Protection, qui fournit un accès conditionnel basé sur les risques à vos applications et à vos données critiques d'entreprise
- Privileged Identity Management est inclus pour permettre la découverte, la restriction et le monitoring des administrateurs et de leur accès aux ressources, ainsi que pour fournir un accès juste-à-temps si nécessaire

## Implémenter la jonction Azure Active Directory

La fonctionnalité de jonction Azure AD utilise l'authentification unique afin de fournir un accès aux ressources et aux applications de l'organisation, et afin de simplifier les déploiements Windows des appareils appartenant à l'entreprise.

## Choses à savoir sur la fonctionnalité de jonction Azure AD

<b>Avantage</b>	<b>Description</b>
<b>Authentification unique (SSO)</b>	Les appareils joints offrent un accès SSO à vos applications et services SaaS gérés par Azure. Vos utilisateurs n'auront pas d'autres invites d'authentification lorsqu'ils accéderont aux ressources de travail. La fonctionnalité d'authentification unique est disponible, même lorsque les utilisateurs ne sont pas connectés au réseau du domaine.
<b>Enterprise State Roaming</b>	À compter de Windows 10, vos utilisateurs peuvent synchroniser de façon sécurisée leurs paramètres utilisateur ainsi que les données des paramètres d'application sur les appareils joints. L'Enterprise State Roaming réduit le temps de configuration des nouveaux appareils.
<b>Accès au Microsoft Store pour Entreprises</b>	Lorsque vos utilisateurs accèdent au Microsoft Store pour Entreprises à l'aide d'un compte Azure AD, ils peuvent choisir parmi une gamme d'applications présélectionnées par votre organisation.
<b>Windows Hello</b>	Fournissez à vos utilisateurs un accès pratique et sécurisé aux ressources de travail à partir des appareils joints.
<b>Restriction de l'accès</b>	Autorisez les utilisateurs à accéder aux applications uniquement à partir des appareils joints qui répondent à vos stratégies de conformité.
<b>Accès facile aux ressources locales</b>	Les appareils joints bénéficient d'un accès facile aux ressources locales lorsqu'ils disposent d'une visibilité sur le contrôleur de domaine local.

### Éléments à prendre en compte lors de l'utilisation d'appareils joints

- **Options de connexion.** Vous pouvez connecter votre appareil à Azure AD de deux façons :

- **Inscrivez** votre appareil dans Azure AD afin de pouvoir gérer l'identité de l'appareil. Azure AD Device Registration fournit à l'appareil une identité qui sera utilisée pour l'authentifier lorsqu'un utilisateur se connectera à Azure AD. Vous pouvez utiliser cette identité pour activer ou désactiver l'appareil.
- **Joignez** votre appareil, ce qui correspond à l'extension de l'inscription d'un appareil. La jonction offre les avantages de l'inscription et change l'état local de l'appareil. Modifier l'état local permet à vos utilisateurs de se connecter à un appareil à l'aide du compte professionnel ou scolaire d'une organisation au lieu d'un compte personnel.
- **Combinaison de l'inscription et d'autres solutions.** Combinez l'inscription avec une solution MDM comme Microsoft Intune pour fournir d'autres attributs d'appareil dans Azure AD. Vous pouvez créer des règles d'accès conditionnel qui exigent que l'accès à partir des appareils réponde aux standards de sécurité et de conformité de votre organisation.
- **Autres scénarios d'implémentation.** Même si la jonction AD est destinée aux organisations qui ne disposent pas d'une infrastructure Windows Server Active Directory locale, elle peut être utilisée pour d'autres scénarios comme ceux impliquant des succursales.

## Implémenter la réinitialisation de mot de passe en libre-service dans Azure Active Directory

### Choses à savoir sur la fonctionnalité de réinitialisation de mot de passe en libre-service d'Azure AD

- Pour gérer les options de la réinitialisation de mot de passe en libre-service, vous aurez besoin d'un compte Azure AD disposant de privilèges d'administrateur général. Ce compte pourra toujours réinitialiser ses propres mots de passe, quelle que soit la configuration des options.
- Un groupe de sécurité est utilisé afin de limiter le nombre d'utilisateurs qui disposent de privilèges de réinitialisation de mot de passe en libre-service.
- Tous les comptes d'utilisateur de votre organisation doivent avoir une licence valide pour utiliser la réinitialisation de mot de passe en libre-service.

### Éléments à prendre en compte lors de l'utilisation de SSPR

- **Qui peut réinitialiser ses mots de passe ?** Décidez des utilisateurs de votre organisation que vous autorisez à utiliser la fonctionnalité. Dans le portail Azure, il existe trois options pour la fonctionnalité de réinitialisation de mot de passe en libre-service : **Aucun**, **Sélectionné** et **Tous**.
- **Méthodes d'authentification.** Déterminez le nombre de méthodes d'authentification qui sont nécessaires pour réinitialiser un mot de passe, et sélectionnez les options d'authentification pour les utilisateurs.

- Votre système doit exiger au moins une méthode d'authentification pour réinitialiser un mot de passe.
- Un plan de réinitialisation de mot de passe en libre-service fort doit proposer plusieurs méthodes d'authentification à l'utilisateur. Les options incluent la notification par e-mail, la notification par SMS ou l'envoi d'un code de sécurité sur le téléphone mobile ou de bureau de l'utilisateur. Vous pouvez également proposer à l'utilisateur un ensemble de questions de sécurité.
- Vous pouvez exiger que des questions de sécurité soient enregistrées pour les utilisateurs de votre locataire Azure AD.
- Vous pouvez configurer le nombre de questions de sécurité auxquelles il faudra répondre correctement pour réussir la réinitialisation du mot de passe.
- Combinaison de méthodes pour une sécurité renforcée. Les questions de sécurité peuvent être moins sécurisées que les autres méthodes d'authentification. Certains utilisateurs peuvent connaître les réponses aux questions d'un utilisateur, ou les questions peuvent être faciles à deviner. Si vous utilisez les questions de sécurité, combinez cette option avec d'autres méthodes d'authentification.

## Configurer des comptes d'utilisateurs et de groupes

### Objectifs d'apprentissage

Dans ce module, vous allez découvrir comment :

- Configurer des comptes d'utilisateurs et leurs propriétés.
- Créer des comptes d'utilisateurs.
- Importer des comptes d'utilisateurs en bloc avec un modèle.
- Configurer des comptes de groupes et les types d'affectation.

### Créer des comptes d'utilisateur

**Compte  
d'utilisateur**

**Description**

<b>Identité cloud</b>	Un compte utilisateur avec une <i>identité cloud</i> est défini uniquement dans Azure AD. Ce type de compte d'utilisateur comprend les comptes d'administrateur et les utilisateurs gérés dans le cadre de votre organisation. Une identité cloud peut être destinée aux comptes d'utilisateur définis dans votre organisation Azure AD, ainsi qu'aux comptes d'utilisateur définis dans une instance Azure AD externe. Lorsqu'une identité cloud est supprimée de l'annuaire principal, le compte d'utilisateur est supprimé.
<b>Identité synchronisée avec l'annuaire</b>	Les comptes d'utilisateur qui ont une <i>identité synchronisée avec l'annuaire</i> sont définis dans un annuaire Active Directory local. Une activité de synchronisation se produit via Azure AD Connect pour importer ces comptes d'utilisateur dans Azure. La source de ces comptes est Windows Server Active Directory.
<b>Utilisateur invité</b>	Les <i>comptes d'utilisateur invités</i> sont définis en dehors d'Azure. Il s'agit par exemple de comptes d'utilisateur d'autres fournisseurs de cloud et de comptes Microsoft, tels qu'un compte Xbox LIVE. La source des comptes d'utilisateur invité est Utilisateur invité. Les comptes d'utilisateur invité sont utiles lorsque des fournisseurs ou prestataires externes ont besoin d'accéder à vos ressources Azure.

#### Éléments à prendre en compte lors du choix des comptes d'utilisateur

- **Considérez l'emplacement où les utilisateurs sont définis.** Déterminez où vos utilisateurs sont définis. Tous vos utilisateurs sont-ils définis au sein de votre organisation Azure AD, ou certains sont-ils définis dans des instances Azure AD externes ? Avez-vous des utilisateurs externes à votre organisation ? Il est courant pour les entreprises de prendre en charge plusieurs types de comptes dans leur infrastructure.
- **Pensez à la prise en charge des contributeurs externes.** Autorisez les contributeurs externes à accéder aux ressources Azure dans votre organisation en prenant en charge le type de compte **Utilisateur invité**. Lorsque le contributeur externe n'a plus besoin d'un accès, vous pouvez supprimer le compte d'utilisateur et ses privilèges d'accès.
- **Envisagez une combinaison de comptes d'utilisateur.** Implémentez les types de comptes d'utilisateur qui permettent à votre organisation de répondre



à ses besoins métier. Prenez en charge les comptes d'utilisateur à identité synchronisée avec l'annuaire pour les utilisateurs définis dans Windows Server Active Directory. Prenez en charge les identités cloud pour les utilisateurs définis dans votre structure Azure AD interne ou pour ceux définis dans une instance Azure AD externe.

## Gérer les comptes d'utilisateurs

Il existe plusieurs façons d'ajouter des comptes d'utilisateur d'identité cloud dans Azure AD (Azure Active Directory). Une approche courante consiste à utiliser le **portail Azure**. Vous pouvez également utiliser le **Centre d'administration Microsoft 365, la console Administrateur Microsoft Intune et Azure CLI pour ajouter des comptes d'utilisateur à Azure AD**.

- Un nouveau compte d'utilisateur doit avoir un nom complet et un nom de compte d'utilisateur associé. **Aran Sawyer-Miller** est un exemple de nom complet, et **asawmill@contoso.com** pourrait être le nom de compte d'utilisateur associé.
- Les informations et les paramètres qui décrivent un utilisateur sont stockés dans le profil de compte d'utilisateur.
- Le profil peut avoir d'autres paramètres comme le poste d'un utilisateur et son adresse e-mail de contact.
- Un utilisateur disposant de privilèges d'Administrateur général ou d'Administrateur d'utilisateurs peut prédéfinir des données de profil dans les comptes d'utilisateur, telles que le numéro de téléphone principal de l'entreprise.
- Les utilisateurs non administrateurs peuvent définir certaines de leurs propres données de profil, mais ils ne peuvent pas modifier leur nom d'affichage ou le nom de leur compte.

## Éléments à prendre en compte lors de la gestion des comptes d'identité cloud

- **Considérez les données de profil utilisateur.** Autorisez les utilisateurs à définir leurs informations de profil pour leurs comptes, en fonction des besoins. Les données de profil utilisateur, y compris l'image, le poste et les informations de contact de l'utilisateur, sont facultatives. Vous pouvez également fournir certains paramètres de profil pour chaque utilisateur en fonction des exigences de votre organisation.

- **Pensez aux options de restauration pour les comptes supprimés.** Incluez des scénarios de restauration dans votre plan de gestion des comptes. Les opérations de restauration pour un compte supprimé sont disponibles jusqu'à 30 jours après la suppression d'un compte. Après 30 jours, un compte d'utilisateur supprimé ne peut pas être restauré.
- **Réfléchissez aux données de compte collectées.** Collectez les informations de connexion et de journal d'audit pour les comptes d'utilisateur. Azure AD vous permet de collecter ces données afin de vous aider à analyser et à améliorer votre infrastructure.

## Créer des comptes d'utilisateurs en bloc

Azure AD (Azure Active Directory) prend en charge plusieurs opérations en bloc, notamment la création et la suppression en bloc pour les comptes d'utilisateur. L'approche la plus courante pour ces opérations consiste à utiliser le portail Azure. Azure PowerShell peut être utilisé pour le chargement en bloc de comptes d'utilisateur.

### Informations à connaître concernant les opérations de compte en bloc

- Seuls les administrateurs généraux et les administrateurs d'utilisateurs ont les privilèges nécessaires pour créer et supprimer des comptes d'utilisateur dans le portail Azure.
- Pour effectuer des opérations de création ou de suppression en bloc, l'administrateur remplit un modèle de valeurs séparées par des virgules (CSV) des données pour les comptes d'utilisateur.
- Des modèles d'opérations en bloc peuvent être téléchargés à partir du portail Azure AD.
- Des listes en bloc de comptes d'utilisateur peuvent être téléchargées.

### Éléments à prendre en compte lors de la création de comptes d'utilisateur

- **Pensez aux conventions de nommage**
- **Envisagez l'utilisation de mots de passe initiaux**
- **Pensez aux stratégies pour réduire les erreurs**

## Créer des comptes de groupes

Azure AD (Azure Active Directory) permet à votre organisation de définir deux types de comptes de groupes différents. Les **groupes de sécurité permettent de gérer l'accès de membres et d'ordinateurs aux ressources partagées d'un groupe**

**d'utilisateurs.** Vous pouvez créer un groupe de sécurité pour une stratégie de sécurité spécifique, et appliquer les mêmes autorisations à tous les membres d'un groupe. Les groupes Microsoft 365 offrent des opportunités de collaboration. Les membres du groupe ont accès à une boîte aux lettres, un calendrier, des fichiers et un site SharePoint partagés, et bien plus encore.

- Utilisez des groupes de sécurité afin de définir des autorisations pour tous les membres du groupe en même temps, plutôt que d'ajouter des autorisations à chaque membre individuellement.
- Ajoutez des groupes Microsoft 365 afin d'activer l'accès aux groupes pour les utilisateurs invités en dehors de votre organisation Azure AD.
- Les groupes de sécurité peuvent être implémentés uniquement par un administrateur Azure AD.
- Les utilisateurs normaux et les administrateurs Azure AD peuvent tous utiliser des groupes Microsoft 365.

Éléments à prendre en compte lors de l'ajout de membres à un groupe

**Droits  
d'accès**

**Description**

**Affecté**

Ajoutez des utilisateurs spécifiques en tant que membres d'un groupe, où chaque utilisateur peut disposer d'autorisations uniques.

**Utilisateur  
dynamique**

Utilisez des règles d'appartenance dynamique pour ajouter et supprimer automatiquement des membres de groupe. Quand les attributs d'un membre changent, Azure examine les règles de groupe dynamique pour l'annuaire. Si les attributs du membre répondent aux exigences de la règle, le membre est ajouté au groupe. Si les attributs du membre ne répondent plus aux exigences de règle, le membre est supprimé.

**Appareil dynamique** (*Groupes de sécurité uniquement*) Appliquez des règles de groupe dynamiques pour ajouter et supprimer automatiquement des appareils dans des groupes de sécurité. Quand les attributs d'un appareil changent, Azure examine les règles de groupe dynamique pour l'annuaire. Si les attributs de l'appareil répondent aux exigences de la règle, l'appareil est ajouté au groupe de sécurité. Si les attributs de l'appareil ne répondent plus aux exigences de la règle, l'appareil est supprimé.

Éléments à prendre en compte lors de l'utilisation d'unités administratives

- **Pensez aux outils de gestion.** Passez en revue vos options de gestion des unités administratives. Vous pouvez utiliser le portail Azure, des applets de commande et des scripts PowerShell, ou Microsoft Graph.
- **Prenez en compte les exigences de rôle dans le portail Azure.** Planifiez votre stratégie pour les unités administratives en fonction des privilèges de rôle. Dans le portail Azure, seuls les utilisateurs Administrateur général ou Administrateur de rôle privilégié peuvent gérer les unités administratives.
- **Pensez à l'étendue des unités administratives.** Reconnaissez le fait que l'étendue d'une unité administrative s'applique uniquement aux autorisations de *gestion*. Les membres et les administrateurs d'une unité administrative peuvent exercer leurs autorisations *utilisateur* par défaut pour parcourir d'autres utilisateurs, groupes ou ressources en dehors de leur unité administrative.

## Configurer des abonnements

Identifier les régions Azure

Éléments à prendre en compte pour l'utilisation des régions et des paires régionales

- **Réfléchissez au déploiement des ressources et des régions.** Planifiez les régions où déployer vos ressources.
- **Tenez compte de la prise en charge du service par région.** Vérifiez la disponibilité des régions et des services.
- **Tenez compte des services qui ne nécessitent pas de régions.** Identifiez les services qui n'ont pas besoin de prise en charge régionale.
- **Réfléchissez aux exceptions du jumelage de régions.** Consultez le site web Azure pour connaître la disponibilité actuelle des régions et les exceptions.
- **Prenez en compte les avantages de la résidence des données.** Prenez parti des avantages de la résidence des données offerts par les paires

régionales. Cette fonctionnalité permet de répondre aux exigences en matière de compétence fiscale et juridique.

Visitez le site web de l'infrastructure mondiale Azure pour trouver les régions prises en charge pour votre zone géographique métier. Vous pouvez effectuer une recherche par nom de pays ou de région, ou par produit Microsoft. Une liste des paires de régions prises en charge et des exceptions est également disponible.

## Implémenter des abonnements Azure

Un abonnement Azure est une unité logique de services Azure qui est liée à un compte Azure.

Les abonnements vous permettent d'organiser l'accès aux ressources des services Azure et de contrôler la façon dont l'utilisation des ressources est rapportée, facturée et payée.

### Points à connaître sur les abonnements

- Chaque service cloud Azure appartient à un abonnement.
- Chaque abonnement peut avoir une configuration de facturation et de paiement différente.
- Plusieurs abonnements peuvent être liés au même compte Azure.
- Plusieurs comptes Azure peuvent être liés au même abonnement.
- La facturation des services Azure est effectuée par abonnement.
- Si votre compte Azure est le seul compte associé à un abonnement, vous êtes responsable des exigences de facturation.
- Les opérations programmatiques pour un service cloud peuvent nécessiter un ID d'abonnement.

### Éléments à prendre en compte pour l'utilisation des abonnements

- **Tenez compte des types de comptes Azure nécessaires.** Déterminez les types de comptes Azure que vos utilisateurs lieront à des abonnements Azure.
- **Utilisez plusieurs abonnements.** Configurez différents abonnements et options de paiement en fonction des services, projets, bureaux régionaux, etc. de votre entreprise.
- **Prenons l'exemple d'un abonnement dédié pour les services partagés.** Planifiez la façon dont les utilisateurs peuvent partager des ressources allouées dans un seul abonnement.
- **Réfléchissez à l'accès aux ressources.** Chaque abonnement Azure peut être associé à un annuaire Azure AD.

## Obtenir un abonnement Azure

Pour utiliser Azure, vous devez avoir un abonnement Azure. Il existe plusieurs façons d'obtenir un abonnement Azure. Vous pouvez obtenir un abonnement Azure dans le cadre d'un :

- **Contrat d'Entreprise** : Tous les clients d'un [Contrat Entreprise](#) peuvent ajouter Azure à leur contrat en payant d'avance un engagement financier envers Azure. L'engagement est consommé tout au long de l'année en utilisant n'importe quelle combinaison de la grande variété de services cloud proposés par Azure.
- **Revendeur Microsoft** : Achetez Azure par le biais du [programme de licence Open](#), qui offre un moyen simple et flexible d'acheter des services cloud auprès de votre revendeur Microsoft. Si vous avez déjà acheté une clé Azure en licence Open, [activez un nouvel abonnement ou ajoutez des crédits maintenant](#).
- **Partenaire Microsoft** : Trouvez un [partenaire Microsoft](#) qui peut concevoir et implémenter votre solution cloud Azure. Ces partenaires ont l'expertise métier et technologique pour recommander des solutions qui répondent aux besoins uniques de votre entreprise.
- **Compte gratuit personnel** : pour un abonnement d'essai avec la possibilité d'effectuer une mise à niveau

## Identifier l'utilisation de l'abonnement Azure

Azure propose des options d'abonnement gratuites et payantes pour répondre à différents besoins et exigences. Les abonnements les plus courants sont : **Gratuit, Paiement à l'utilisation, Accord Entreprise et Étudiant.**

Vous pouvez choisir une combinaison d'options d'obtention et différents abonnements.

## Éléments à prendre en compte pour la création d'abonnements Azure

- **Essayez Azure gratuitement.** Un abonnement Azure gratuit comprend un crédit financier valable pour **n'importe quel service pendant les 30 premiers jours**. Vous obtenez un **accès gratuit aux produits Azure les plus utilisés pendant 12 mois et un accès à plus de 25 produits toujours gratuits**.
- **Payez mensuellement pour les services utilisés.** Un abonnement avec paiement à l'utilisation facture tous les mois les services utilisés lors de cette période de facturation
- **Utilisez un Accord Entreprise Azure.** Un Accord Entreprise permet d'acheter des licences logicielles et des services cloud dans le cadre d'un contrat unique. Le contrat comprend des remises pour les nouvelles licences et la Software Assurance. Ce type d'abonnement cible les organisations de type entreprise.

- **Prenez en charge Azure pour les étudiants.** Un abonnement Azure for Students comprend un crédit financier valable pendant les 12 premiers mois.

## Implémenter Microsoft Cost Management

Microsoft Cost Management prend en charge les tâches de facturation administratives et vous aide à gérer l'accès à la facturation pour voir les coûts.

### Choses à savoir sur Microsoft Cost Management

- Microsoft Cost Management montre les modèles de coût et d'utilisation de l'organisation avec une analytique avancée. Les coûts sont basés sur les prix négociés et prennent en compte la réservation et les remises Azure Hybrid Benefit. Des analyses prédictives sont aussi disponibles.
- Les rapports dans Microsoft Cost Management montrent les coûts basés sur l'utilisation consommés par les services Azure et les offres tierces de la Place de marché. Les rapports vous aident à comprendre vos dépenses et votre utilisation des ressources, et à trouver des anomalies dans les dépenses. Les frais, comme les achats de réservation, le support et les taxes, peuvent ne pas être visibles dans les rapports.
- Le produit utilise des groupes d'administration, des budgets et des recommandations Azure pour montrer clairement comment vos dépenses sont organisées et comment réduire les coûts.
- Vous pouvez utiliser le portail Azure ou différentes API pour automatiser l'exportation visant à intégrer les données de coût à des processus et systèmes externes. Vous avez aussi à disposition une exportation automatisée des données de facturation ainsi que des rapports planifiés.

### Choses à prendre en compte en cas d'utilisation de Microsoft Cost Management

- **Analysez les coûts.** Tirez parti des fonctionnalités d'analyse de coûts de Microsoft Cost Management pour explorer et analyser vos coûts organisationnels. Vous pouvez voir les coûts agrégés par organisation pour comprendre où ils ont augmenté et pour identifier les tendances de dépenses. Monitorer les coûts cumulés au fil du temps pour estimer les tendances de coûts mensuelles, trimestrielles ou même annuelles par rapport à un budget.
- **Évaluez les options budgétaires.** Utilisez les fonctionnalités de Microsoft Cost Management pour établir et gérer les budgets. Les budgets empêchent de dépasser les plafonds ou les limites de coût.
- **Tenez compte des recommandations.** Passez en revue les recommandations Microsoft Cost Management pour découvrir comment optimiser et améliorer l'efficacité en identifiant les ressources inactives et sous-utilisées.
- **Exportez les données de gestion des coûts.** Microsoft Cost Management vous aide à utiliser vos informations de facturation.

## Appliquer l'étiquetage des ressources

Vous pouvez appliquer des étiquettes à vos ressources Azure pour les organiser de façon logique par catégories. Les étiquettes sont utiles pour le tri, la recherche, la gestion et l'analyse de vos ressources.

### Points à connaître sur les balises de ressource

- Chaque étiquette de ressource a un nom et une valeur.
- Le nom de l'étiquette reste constant pour toutes les ressources auxquelles elle est appliquée.
- La valeur de l'étiquette peut être sélectionnée dans un ensemble de valeurs défini ou être unique pour une instance de ressource spécifique.
- Chaque ressource ou groupe de ressources peut avoir un maximum de 50 paires nom/valeur d'étiquette.
- Les étiquettes appliquées à un groupe de ressources ne sont pas héritées par les ressources dans le groupe.

### Éléments à prendre en compte pour la création des étiquettes de ressource

- **Recherchez en fonction des données d'étiquette.** Recherchez des ressources dans votre abonnement en interrogeant le nom et la valeur de l'étiquette.
- **Recherchez les ressources associées.** Récupérez les ressources associées dans d'autres groupes de ressources en recherchant le nom ou la valeur de l'étiquette.
- **Regroupez les données de facturation.** Regroupez les groupes de ressources comme les machines virtuelles par centre de coût et environnement de production. Quand vous téléchargez le fichier CSV d'utilisation de vos ressources pour vos services, les étiquettes apparaissent dans la colonne **Tags**.
- **Créez des étiquettes avec PowerShell ou Azure CLI.** Créez de nombreuses étiquettes de ressource programmatiquement en utilisant Azure PowerShell ou Azure CLI.

## Réaliser des économies

**Réduction des  
coûts**

**Description**



<b>Réservations</b>	Économisez de l'argent en payant à l'avance. Vous pouvez payer un ou trois ans de machine virtuelle, de capacité de calcul SQL Database, de débit Azure Cosmos DB ou d'autres ressources Azure. Le prépaiement vous permet d'obtenir une remise sur les ressources que vous utilisez. Les réservations peuvent réduire sensiblement les coûts de machine virtuelle, de calcul SQL Database, d'Azure Cosmos DB ou d'autres ressources, jusqu'à hauteur de 72 % sur les tarifs des paiements à l'utilisation. Des réservations permettent de bénéficier d'une remise sur la facturation et n'ont aucune incidence sur l'état de runtime de vos ressources.
<b>Avantages Azure Hybrid</b>	Accédez aux avantages tarifaires si vous disposez d'une licence avec <i>Software Assurance</i> . Azure Hybrid Benefit permet d'optimiser la valeur des investissements existants en termes de licences Windows Server ou SQL Server locales lors de la migration vers Azure. La calculatrice Azure Hybrid Benefit peut vous aider à déterminer les économies que vous pouvez réaliser.
<b>Crédits Azure</b>	Utilisez l'avantage de crédit mensuel pour développer, tester et expérimenter de nouvelles solutions sur Azure. En tant qu'abonné Visual Studio, vous pouvez utiliser Microsoft Azure sans frais supplémentaires. Avec votre crédit Azure mensuel, Azure est votre bac à sable personnel pour le développement et les tests.
<b>Régions Azure</b>	Comparez les tarifs entre les régions. Les prix peuvent varier d'une région à l'autre, même au sein des États-Unis. Vérifiez les prix des différentes régions pour voir si vous pouvez économiser en sélectionnant une autre région pour votre abonnement.
<b>Budgets</b>	Appliquez les fonctionnalités budgétaires de Microsoft Cost Management pour planifier et favoriser la responsabilité organisationnelle. Avec les budgets, vous pouvez prendre en compte les services Azure que vous consommez ou auxquels vous vous abonnez pendant une période spécifique. Monitorisez les dépenses au fil du temps et informez les autres utilisateurs de leurs dépenses pour gérer les coûts de manière proactive. Utilisez des budgets pour comparer et suivre les dépenses dans le cadre de l'analyse des coûts.

**Calculatrice de prix** La [calculatrice de prix](#) fournit des estimations dans tous les domaines d'Azure (calcul, réseau, stockage, web et bases de données).

## Configurer Azure Policy

### Créer des groupes d'administration

Les organisations qui utilisent plusieurs abonnements ont besoin de pouvoir gérer efficacement l'accès, les stratégies et la conformité. Les [groupes d'administration Azure](#) offrent un niveau d'étendue et de contrôle au-delà des abonnements. Vous pouvez utiliser des groupes d'administration comme conteneurs pour gérer l'accès, la stratégie et la conformité de vos abonnements.

### Points à connaître sur les groupes d'administration

- Par défaut, tous les nouveaux abonnements sont placés sous le groupe d'administration de niveau supérieur, ou *groupe racine*.
- Tous les abonnements d'un groupe d'administration héritent automatiquement des conditions appliquées à ce groupe d'administration.
- Une arborescence de groupes d'administration peut prendre en charge jusqu'à six niveaux de profondeur.
- L'autorisation du contrôle d'accès en fonction du rôle Azure pour les opérations de groupe d'administration n'est pas activée par défaut.

### Éléments à prendre en compte pour l'utilisation des groupes d'administration

- **Utilisez les hiérarchies et les groupes personnalisés.** Alignez vos abonnements Azure en utilisant des hiérarchies et des regroupements personnalisés qui répondent à la structure organisationnelle et aux scénarios métier de votre entreprise.
- **Tenez compte de l'héritage de stratégie.** Tous les abonnements d'un groupe d'administration héritent des conditions appliquées au groupe d'administration.
- **Tenez compte des règles de conformité.**
- **Utilisez les rapports sur les coûts.** Utilisez des groupes d'administration pour effectuer des rapports sur les coûts par service ou pour des scénarios métier spécifiques.

Un groupe d'administration a un identificateur unique (ID) de répertoire et un nom complet. L'ID est utilisé pour envoyer des commandes sur le groupe d'administration. La valeur d'ID ne peut pas être changée après sa création, car elle est utilisée dans l'ensemble du système Azure pour identifier le groupe d'administration. Le nom complet du groupe d'administration est facultatif et peut être changé à tout moment.

## Implémenter des stratégies Azure

Azure Policy est un service Azure que vous pouvez utiliser pour créer, affecter et gérer des stratégies. Vous pouvez utiliser des stratégies pour appliquer des règles à vos ressources afin de répondre aux standards de conformité de l'entreprise et aux contrats de niveau de service. Azure Policy exécute des évaluations et des analyses sur vos ressources pour vérifier qu'elles sont conformes.

### Points à connaître sur Azure Policy

Avantage	Description
<b>Appliquer les règles et la conformité</b>	Activez des stratégies intégrées ou créez des stratégies personnalisées pour tous les types de ressources. Prenez en charge l'évaluation et l'application de stratégies en temps réel, ainsi que l'évaluation périodique ou à la demande de la conformité.
<b>Appliquer des stratégies à grande échelle</b>	Appliquez des stratégies à un groupe d'administration avec un contrôle sur l'ensemble de votre organisation. Appliquez plusieurs stratégies, et agrégez les états de stratégie avec une initiative de stratégie. Définissez une étendue d'exclusion.
<b>Effectuer une correction</b>	Appliquer une correction en temps réel et une correction sur vos ressources existantes.
<b>Pratiquer la gouvernance</b>	Implémentez des tâches de gouvernance pour votre environnement : <ul style="list-style-type: none"><li>- Prendre en charge plusieurs équipes d'ingénierie (déploiement et fonctionnement dans l'environnement)</li><li>- Gérer plusieurs abonnements</li><li>- Standardiser et appliquer la configuration des ressources cloud</li><li>- Gérer la conformité réglementaire, le contrôle des coûts, la sécurité et la cohérence de la conception</li></ul>

### Éléments à prendre en compte lors de l'utilisation d'Azure Policy

- **Utilisez des ressources déployables.** Spécifiez les types de ressource que votre organisation peut déployer en utilisant Azure Policy.
- **Tenez compte des restrictions de localisation.** Limitez les localisations que vos utilisateurs peuvent spécifier au moment du déploiement des ressources.

- **Tenez compte de l'application des règles.** Appliquez des règles de conformité et des options de configuration pour vous aider à gérer vos ressources et vos options utilisateur.
- **Effectuez des audits d'inventaire.** Utilisez Azure Policy avec le service Sauvegarde Azure sur vos machines virtuelles et exécutez des audits d'inventaire.

## Créer des stratégies Azure

Une *définition de stratégie* décrit les conditions de conformité d'une ressource et les actions à effectuer quand les conditions sont remplies. Une ou plusieurs définitions de stratégie sont regroupées dans une *définition d'initiative* pour contrôler l'étendue de vos stratégies et évaluer la conformité de vos ressources.

### Étape 1 : Créer des définitions de stratégie

Une définition de stratégie exprime une condition à évaluer et les actions à effectuer quand la condition est remplie. Vous pouvez créer vos propres définitions de stratégie ou choisir parmi les définitions intégrées d'Azure Policy. Vous pouvez créer une définition de stratégie pour empêcher le déploiement des machines virtuelles de votre organisation si elles sont exposées à une adresse IP publique.

### Étape 2 : Créer une définition d'initiative

Une définition d'initiative est un ensemble de définitions de stratégie qui vous permettent de suivre l'état de conformité de votre ressource pour atteindre un objectif plus large. Vous pouvez créer vos propres définitions d'initiative ou utiliser les définitions intégrées d'Azure Policy. Vous pouvez utiliser une définition d'initiative pour que les ressources soient conformes aux réglementations de sécurité.

### Étape 3 : Définir l'étendue de la définition d'initiative

Azure Policy vous permet de contrôler la façon dont vos définitions d'initiative sont appliquées aux ressources de votre organisation. Vous pouvez limiter l'étendue de la définition d'initiative à des groupes d'administration, abonnements ou groupes de ressources spécifiques.

### Étape 4 : Déterminer la conformité

Une fois que vous avez attribué une définition d'initiative, vous pouvez évaluer l'état de conformité de toutes vos ressources. Les ressources individuelles, les groupes de ressources et les abonnements dans une étendue peuvent être définis pour ne pas être affectés par les règles de stratégie.

## Créer des définitions de stratégie

Accéder aux définitions de stratégie intégrées

Vous pouvez trier la [liste des définitions intégrées](#) par catégorie pour rechercher des stratégies répondant à vos besoins métier.

Voici quelques exemples de définitions de stratégie intégrées :

- **Références SKU de tailles de machine virtuelle autorisées** : spécifiez un ensemble de références SKU de tailles VM que votre organisation peut déployer. Cette stratégie se trouve sous la catégorie Calcul.
- **Localisations autorisées** : limitez les localisations que les utilisateurs peuvent spécifier au moment du déploiement des ressources..

Ajouter de nouvelles définitions de stratégie

Si vous ne trouvez pas de stratégie intégrée pour répondre à vos besoins métier, vous pouvez ajouter ou créer une définition. Les définitions de stratégie peuvent également être importées dans Azure Policy à partir de [GitHub](#). (format JSON)

## Créer une définition d'initiative

Ajouter une nouvelle définition d'initiative

Quand vous créez une définition d'initiative, vérifiez que la définition utilise le format JSON spécifique demandé par Azure. Pour plus d'informations, consultez la [structure de définition d'initiative Azure Policy](#).

Utiliser une définition d'initiative intégrée

Voici quelques exemples de définitions d'initiative intégrées :

- **Auditer les machines avec des paramètres de sécurité de mot de passe non sécurisés** : utilisez cette initiative pour déployer une stratégie d'audit sur des ressources spécifiées dans votre organisation.
- **Configurer les machines Windows pour exécuter l'agent Azure Monitor et les associer à une règle de collecte de données** : utilisez cette initiative pour superviser et sécuriser vos machines virtuelles Windows, vos Virtual Machine Scale Sets et vos machines Arc.

## Délimiter l'étendue de la définition d'initiative

L'étape suivante consiste à attribuer l'initiative pour établir l'étendue des stratégies. L'étendue détermine les ressources ou regroupements de ressources qui sont affectés par les conditions des stratégies.

Pour établir l'étendue, vous sélectionnez les abonnements affectés. En option, vous pouvez également choisir les groupes de ressources affectés.

## Configurer le contrôle d'accès en fonction du rôle

### Implémenter un contrôle d'accès en fonction du rôle

Le contrôle d'accès en fonction du rôle (RBAC) est un mécanisme qui peut vous aider à gérer qui peut accéder à vos ressources Azure.

#### Points à connaître sur Azure RBAC

- Permettre à une application d'accéder à toutes les ressources d'un groupe de ressources.
- Permettre à un utilisateur de gérer les machines virtuelles d'un abonnement, et à un autre de gérer les réseaux virtuels.
- Permettre à un groupe d'administrateurs de base de données de gérer les bases de données SQL d'un abonnement.
- Permettre à un utilisateur de gérer toutes les ressources d'un groupe de ressources (machines virtuelles, sites web et sous-réseaux).

#### Concepts du contrôle d'accès en fonction du rôle (RBAC) Azure

Concept	Description	Exemples
<b>Principal de sécurité</b>	Objet représentant quelque chose qui demande l'accès à des ressources.	Utilisateur, groupe, principal de service, identité managée
<b>Définition de rôle</b>	Ensemble d'autorisations qui répertorie les opérations autorisées. RBAC Azure est fourni avec des définitions de rôles intégrées, mais vous pouvez également créer vos propres définitions de rôle personnalisées.	Certaines définitions de rôle intégrées : <i>Lecteur</i> , <i>Contributeur</i> , <i>Propriétaire</i> , <i>Administrateur de l'accès utilisateur</i>
<b>Étendue</b>	Limite pour le <i>niveau</i> d'accès demandé ou « combien » d'accès sont accordés.	Racine, groupe d'administration, abonnement, groupe de ressources, ressource

<b>Cession</b>	Une <b>attribution</b> attache une <b>définition de rôle</b> à un <b>principal de sécurité</b> au niveau d'une <b>étendue</b> particulière. Les utilisateurs peuvent accorder l'accès décrit dans une définition de rôle en créant (attachant) une attribution pour le rôle.	<ul style="list-style-type: none"> <li>- Attribuer le rôle <i>Administrateur de l'accès utilisateur</i> à un groupe d'administration limité à un groupe d'administration</li> <li>- Attribuer le rôle <i>Contributeur</i> à un utilisateur limité à un abonnement</li> </ul>
----------------	--	--

### Éléments à prendre en compte lors de l'utilisation d'Azure RBAC

- **Prenez vos demandeurs en considération.** Planifiez votre stratégie pour prendre en charge tous les types d'accès à vos ressources.
- **Prenez vos rôles en considération.** Examinez les types de responsabilités et de scénarios de travail de votre organisation.
- **Prenez l'étendue des autorisations en considération.** Réfléchissez à la façon dont vous pouvez garantir la sécurité en contrôlant l'étendue des autorisations pour les attributions de rôles.
- **Envisagez des définitions intégrées ou personnalisées.** Passez en revue les définitions de rôle intégrées dans RBAC Azure.

### Créer une définition de rôle

Une définition de rôle se compose d'ensembles d'autorisations définis dans un fichier JSON. Chaque ensemble d'autorisations a un nom, tel que *Actions* ou *NotActions*, qui décrit l'objectif des autorisations. Voici quelques exemples d'ensembles d'autorisations :

- Les autorisations *Actions* identifient les actions autorisées.
- Les autorisations *NotActions* spécifient les actions qui ne sont pas autorisées.
- Les autorisations *DataActions* indiquent comment les données peuvent être modifiées ou utilisées.
- Les autorisations *AssignableScopes* répertorient les étendues où une définition de rôle peut être attribuée.

Les autorisations *Actions* indiquent que le rôle *Contributeur* dispose de tous les privilèges d'action. Le caractère générique astérisque "\*" signifie « tout ». Les autorisations *NotActions* réduisent les privilèges fournis par l'ensemble *Actions* et refusent trois actions :

- *Authorization/\*/Delete* : non autorisé à supprimer ou effacer pour « tout ».
- *Authorization/\*/Write* : non autorisé à écrire ou à modifier pour « tout ».

- **Authorization/elevateAccess/Action** : non autorisé à augmenter le niveau ou l'étendue des privilèges d'accès.

Le rôle *Contributeur* dispose également de deux autorisations *DataActions* pour spécifier la façon dont les données peuvent être affectées :

- **"NotDataActions"** : [ ] : aucune action spécifique n'est répertoriée. Par conséquent, toutes les actions peuvent affecter les données.
- **"AssignableScopes"** : [ "/" ] : le rôle peut être attribué pour toutes les étendues qui affectent les données.

Informations à connaître sur les définitions de rôle

- RBAC Azure fournit des ensembles d'autorisations et des rôles intégrés. Vous pouvez également créer des rôles et des autorisations personnalisés.
- Le rôle intégré *Propriétaire* dispose du niveau de privilège d'accès le plus élevé dans Azure.
- Le système soustrait les autorisations *NotActions* des autorisations *Actions* pour déterminer les *autorisations effectives* pour un rôle.
- Les autorisations *AssignableScopes* pour un rôle peuvent être des groupes d'administration, des abonnements, des groupes de ressources ou des ressources.

Autorisations des rôles

Utilisez ensemble les autorisations *Actions* et *NotActions* pour accorder et refuser les privilèges exacts pour chaque rôle. Les autorisations *Actions* peuvent fournir l'étendue de l'accès et les autorisations *NotActions* peuvent limiter l'accès.

Nom de rôle	Description	Autorisations Actions	Autorisations NotActions
<i>Propriétaire</i>	Autoriser toutes les actions	*	n/a



<i>Contributeur</i>	Autoriser toutes les actions, à l'exception de l'écriture ou de la suppression d'une attribution de rôle	*	- Microsoft.Authorization/* /Delete - Microsoft.Authorization/* /Write - Microsoft.Authorization/elevateAccess/Action
<i>Lecteur</i>	Autoriser toutes les actions de lecture	/*/read	n/a

#### Étendues de rôle

- Définissez l'étendue d'un rôle comme disponible pour l'attribution dans deux abonnements :  
"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e",  
"/subscriptions/e91d47c4-76f3-4271-a796-21b4ecfe3624"
- Définir l'étendue d'un rôle comme disponible pour l'attribution uniquement dans le groupe de ressources Réseau :  
"/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e/resourceGroups/Network"
- Définir l'étendue d'un rôle comme disponible pour l'attribution pour tous les demandeurs : "/"

#### Éléments à prendre en considération lors de la création de rôles

- **Envisagez d'utiliser des rôles intégrés.**
- **Envisagez de créer des définitions personnalisées.**
- **Envisagez de limiter l'étendue de l'accès.**
- **Envisagez de contrôler les modifications apportées aux données.**
- **Envisagez d'appliquer des attributions de refus.**

#### Création d'une affectation de rôle

Une attribution de rôle est le processus de définition de l'étendue d'une définition de rôle pour limiter les autorisations d'un demandeur, tel qu'un utilisateur, un groupe, un principal de service ou une identité managée.

- **L'objectif d'une attribution de rôle est de contrôler l'accès.**
- **L'étendue limite les autorisations définies pour un rôle disponibles pour le demandeur affecté.**
- **Vous révoquez l'accès en supprimant une attribution de rôle.**
- **Une ressource hérite des attributions de rôles de sa ressource parente.**
- **Les autorisations effectives pour un demandeur sont une combinaison des autorisations pour les rôles attribués par le demandeur et des autorisations pour les rôles attribués aux ressources demandées.**

Comparer les rôles Azure aux rôles Azure Active Directory

Trois types de rôles sont disponibles pour la gestion des accès dans Azure :

- Rôles d'administrateur d'abonnements classique
- Rôles de contrôle d'accès en fonction du rôle (RBAC) Azure
- Rôles d'administrateur Azure Active Directory (Azure AD)

	<b>Rôles RBAC Azure</b>	<b>Rôles d'administrateur Azure AD</b>
<b>Gestion de l'accès</b>	Gère l'accès aux ressources Azure	Gère l'accès aux ressources Azure AD
<b>Affectation d'étendue</b>	L'étendue peut être spécifiée à plusieurs niveaux, notamment les groupes d'administration, les abonnements, les groupes de ressources et les ressources	L'étendue est spécifiée au niveau du locataire
<b>Définitions de rôles</b>	Les rôles peuvent être définis via le portail Azure, Azure CLI, Azure PowerShell, les modèles Azure Resource Manager et l'API REST	Les rôles peuvent être définis via le portail d'administration Azure, le portail d'administration Microsoft 365 et Microsoft Graph Azure AD PowerShell

Appliquer le contrôle d'accès en fonction du rôle

- **Les rôles d'administrateur Azure AD** permettent de gérer des ressources dans Azure AD, comme des utilisateurs, des groupes et des domaines. Ces

rôles sont définis pour le locataire Azure AD au niveau racine de la configuration.

- **Les rôles RBAC Azure** offrent une gestion des accès plus granulaire pour les ressources Azure. Ces rôles sont définis pour un demandeur ou une ressource et peuvent être appliqués à plusieurs niveaux : racine, groupes d'administration, abonnements, groupes de ressources ou ressources.

Passer en revue les rôles RBAC Azure fondamentaux

<b>Rôle fondamental</b>	<b>Description</b>
<i>Propriétaire</i>	Le rôle <i>Propriétaire</i> dispose d'un accès total à toutes les ressources, ainsi que du droit de déléguer l'accès à d'autres personnes. Les rôles <i>Administrateur de services</i> et <i>Coadministrateur</i> se voient attribuer le rôle <i>Propriétaire</i> dans l'étendue de l'abonnement.
<i>Contributeur</i>	Le rôle <i>Contributeur</i> peut créer et gérer tous les types de ressources Azure. Ce rôle ne peut pas accorder l'accès à d'autres personnes.
<i>Lecteur</i>	Le rôle <i>Lecteur</i> peut voir les ressources Azure existantes.
<i>Administrateur de l'accès utilisateur</i>	Le rôle <i>Administrateur de l'accès utilisateur</i> peut gérer l'accès des utilisateurs aux ressources Azure.

## Créer des utilisateurs et des groupes Azure dans Azure Active Directory

Pourquoi utiliser Azure AD B2B au lieu de la fédération ?

Avec Azure AD B2B, vous n'avez pas à vous préoccuper de la gestion et de l'authentification des informations d'identification et des identités des partenaires. Vos partenaires peuvent collaborer avec vous même s'ils ne disposent pas d'un service informatique. Par exemple, vous pouvez collaborer avec un sous-traitant qui possède seulement une adresse e-mail personnelle ou professionnelle et qui n'utilise aucune solution de gestion des identités gérée par un service informatique.

## Implémenter la réinitialisation de mot de passe en libre-service Azure AD

Avant de commencer à configurer SSPR, les éléments suivants doivent être en place :

- Une organisation Azure AD. Cette organisation doit avoir au moins une licence d'essai activée.
- Un compte Azure AD avec des privilèges d'administrateur général. Vous utiliserez ce compte pour configurer SSPR.
- Un compte d'utilisateur nonadministrateur. Vous utiliserez ce compte pour tester SSPR. Il est important que ce compte ne soit pas un administrateur, car Azure AD impose des conditions supplémentaires sur les comptes d'administration à SSPR. Cet utilisateur et tous les comptes d'utilisateur doivent disposer d'une licence valide pour utiliser SSPR.
- Un groupe de sécurité avec lequel tester la configuration. Le compte d'utilisateur non-administrateur doit être membre de ce groupe. Vous utiliserez ce groupe de sécurité pour limiter les personnes pour lesquelles vous effectuez le déploiement de SSPR.

### Étendue du déploiement de SSPR

Il existe trois paramètres pour la propriété **Réinitialisation du mot de passe en libre-service activée** :

- **Désactivé** : aucun utilisateur de l'organisation Azure AD ne peut utiliser SSPR. Il s'agit de la valeur par défaut.
- **Activé** : tous les utilisateurs de l'organisation Azure AD peuvent utiliser SSPR.
- **Sélectionné** : Seuls les membres du groupe de sécurité spécifié peuvent utiliser SSPR. Vous pouvez utiliser cette option pour activer SSPR pour un groupe d'utilisateurs ciblé, qui peut le tester et vérifier qu'il fonctionne comme prévu. Quand vous êtes prêt à le déployer de façon plus large, définissez la propriété sur **Activé** afin que tous les utilisateurs aient accès à SSPR.

### Configurer SSPR

- Accédez au [Portail Azure](#), puis à **Active Directory>Réinitialisation de mot de passe**.
- Propriétés :
  - Activer SSPR.
  - Vous pouvez l'activer pour tous les utilisateurs de l'organisation Azure AD ou pour des utilisateurs sélectionnés.
  - Pour l'activer pour des utilisateurs sélectionnés, vous devez spécifier le groupe de sécurité. Les membres de ce groupe peuvent utiliser SSPR.
- Méthodes d'authentification :
  - Choisissez d'exiger une ou deux méthodes d'authentification.

- Choisissez les méthodes d'authentification que les utilisateurs peuvent utiliser.
- Inscription :
  - Spécifiez si les utilisateurs doivent s'inscrire à SSPR lors de leur prochaine connexion.
  - Spécifiez la fréquence à laquelle les utilisateurs sont invités à reconfirmer leurs informations d'authentification.
- Notifications : Indiquez si les utilisateurs et les administrateurs de réinitialisation de mot de passe doivent être avertis.
- Personnalisation : Indiquez une adresse e-mail ou une URL de page web où vos utilisateurs peuvent obtenir de l'aide.

## Implémenter et gérer le stockage dans Azure

### Objectifs d'apprentissage

Dans ce module, vous allez découvrir comment :

- Identifier les fonctionnalités et les cas d'utilisation des comptes de stockage Azure.
- Choisir parmi les différents types de stockage Azure et créer des comptes de stockage.
- Sélectionner une stratégie de réplication du stockage.
- Configurer l'accès réseau sécurisé aux points de terminaison de stockage.

### Configurer des comptes de stockage

#### Implémenter le Stockage Azure

Points à connaître sur le stockage Azure

**Category**

**Description**

**Exemples de stockage**

<b>Données de la machine virtuelle</b>	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.
<b>Les données non structurées</b>	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 <i>non relationnel</i> .	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.
<b>Données structurées</b>	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. Vous pouvez utiliser le stockage de niveau standard pour les applications qui

nécessitent un stockage en bloc ou lorsque les données sont rarement consultées.

- Les comptes de stockage **Premium** reposent sur des disques SSD et offrent des performances homogènes à faible latence. Vous pouvez utiliser le stockage de niveau Premium pour les disques de machine virtuelle Azure avec des applications gourmandes en E/S comme les bases de données.

### Réflexions nécessaires lors de l'utilisation du Stockage Azure

- **Considérer la durabilité et la disponibilité.** Le stockage Azure est durable et hautement disponible. La redondance garantit que vos données sont sécurisées lors de pannes matérielles temporaires. Vous répliquez les données entre centres de données ou régions géographiques afin de les protéger contre les catastrophes locales ou les catastrophes naturelles. Les données répliquées restent hautement disponibles en cas de panne inattendue.
- **Envisagez l'accès sécurisé.** Toutes les données écrites dans le Stockage Azure sont chiffrées par le service. Le Stockage Azure vous permet de contrôler de manière très précise les utilisateurs qui ont accès à vos données.
- **Considérer la scalabilité.** Le Stockage Azure est conçu pour être hautement évolutif afin de répondre aux besoins de stockage de données et de performances des applications modernes.
- **Envisagez la facilité de gestion.** Microsoft Azure gère la maintenance du matériel, les mises à jour et les problèmes critiques pour vous.
- **Envisagez l'accessibilité des données.** Les données dans le Stockage Azure sont accessibles n'importe où dans le monde via HTTP ou HTTPS. Microsoft fournit des Kits de développement logiciel (SDK) pour le stockage Azure dans différents langages. Vous pouvez utiliser .NET, Java, Node.js, Python, PHP, Ruby, Go et l'API REST. Le Stockage Azure prend en charge l'écriture de scripts dans Azure PowerShell ou l'interface de ligne de commande Azure. Le portail Azure et l'Explorateur Stockage Azure offrent des solutions visuelles simples pour utiliser vos données.

### 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).

## Stockage Blob Azure (conteneurs)

Le Stockage Blob Azure est la solution de stockage d'objets de Microsoft pour le cloud. Le Stockage Blob est optimisé pour le stockage d'immenses quantités de données non structurées ou non relationnelles, comme les données texte ou binaires.

## Azure Files

Azure Files vous permet de configurer des partages de fichiers en réseau à haute disponibilité. Les partages sont accessibles via le protocole SMB (Server Message Block) et NFS (Network File System). Plusieurs machines virtuelles peuvent partager les mêmes fichiers avec accès en lecture et en écriture. Vous pouvez également consulter les fichiers à l'aide de l'interface REST ou des bibliothèques clientes de stockage.

## Stockage File d'attente Azure

Le Stockage File d'attente Azure sert à stocker et à récupérer des messages. La taille maximale des messages de file d'attente est de 64 Ko et une file d'attente peut contenir des millions de messages. Les files d'attente servent à stocker des listes de messages qui seront traités de façon asynchrone.

## Stockage Table Azure (Azure Cosmos DB)

Le Stockage Table Azure est un service de base de données NoSQL complètement managé pour le développement d'applications modernes. En tant que service entièrement géré, Azure Cosmos DB prend en charge l'administration de la base de données avec la gestion, les mises à jour et l'application de correctifs automatiques. Il traite également la gestion de la capacité avec des options économiques de mise à l'échelle automatique et serverless qui répondent aux besoins de l'application pour faire correspondre la capacité à la demande.

## Éléments à prendre en compte lors du choix de services Stockage Azure

- **Envisagez l'optimisation du stockage pour les données massives.** Stockage Blob Azure est optimisé pour stocker des quantités massives de données non structurées. Les objets du stockage Blob sont accessibles où que vous soyez dans le monde via HTTP ou HTTPS. Le stockage blob est idéal pour servir les données directement dans un navigateur, diffuser en continu des données et stocker des données pour la sauvegarde et la restauration.
- **Envisagez le stockage avec une haute disponibilité.** Azure Files prend en charge les partages de fichiers réseau hautement disponibles. Les applications locales utilisent des partages de fichiers pour faciliter la migration. En utilisant Azure Files, tous les utilisateurs peuvent accéder aux données et outils partagés. Les informations d'identification du compte de



stockage fournissent l'authentification du partage de fichiers pour garantir que tous les utilisateurs qui ont monté le partage de fichiers disposent de l'accès en lecture/écriture correct.

- **Envisagez de stocker des messages.** Stockage File d'attente Azure permet de stocker de grandes quantités de messages. Stockage File d'attente est couramment utilisé pour créer un backlog de travail à traiter de manière asynchrone.
- **Envisagez de stocker des données structurées.** Le Stockage Table Azure est idéal pour stocker des données non relationnelles structurées. Il fournit des tables optimisées pour le débit, une distribution globale et des index secondaires automatiques. Étant donné que le Stockage Table Azure fait partie d'Azure Cosmos DB, vous avez accès à un service de base de données NoSQL complètement managé pour le développement d'applications modernes.

## Déterminer les types de comptes de stockage

Compte de stockage	Services pris en charge	Utilisation recommandée
<a href="#"><u>Standard Usage général v2</u></a>	Stockage Blob (y compris Data Lake Storage), 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).
<a href="#"><u>Premium Objets blob de bloc</u></a>	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.

Tous les types de comptes de stockage sont chiffrés à l'aide de Storage Service Encryption (SSE) pour les données au repos.

### Déterminer les stratégies de réplication

- Stockage localement redondant (LRS)
- Stockage redondant dans une zone (ZRS)
- Stockage géo-redondant (GRS)
- Stockage géoredondant interzone (GZRS)

### Accéder au stockage

<b>Service</b>	<b>Point de terminaison par défaut.</b>
<b>Service de conteneur</b>	<code>//mystorageaccount.blob.core.windows.net</code>
<b>Service de Table</b>	<code>//mystorageaccount.table.core.windows.net</code>
<b>Service File d'attente</b>	<code>//mystorageaccount.queue.core.windows.net</code>

**Service Fichier**                    `//mystorageaccount.file.core.windows.net`

Pour accéder aux données *myblob* à l'emplacement *mycontainer* dans votre compte de stockage, nous utilisons l'adresse URL suivante :

`//mystorageaccount.blob.core.windows.net/mycontainer/myblob.`

Configurer des domaines personnalisés

Le stockage Azure ne fournit actuellement pas de prise en charge native du protocole HTTPS avec des domaines personnalisés. Vous pouvez implémenter un réseau de distribution de contenu Azure (CDN) pour accéder aux blobs à l'aide de domaines personnalisés via HTTPS.

Il existe deux façons de configurer un domaine personnalisé : le mappage direct et le mappage de domaine intermédiaire.

- **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.

L'exemple suivant montre comment un sous-domaine est mappé à un compte de stockage Azure pour créer un enregistrement **CNAME** dans le système DNS (Domain Name System) :

- Sous-domaine : `blobs.contoso.com`
- Compte de stockage Azure : `\<storageaccount>\.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. En ajoutant le mot clé **asverify** à votre propre sous-domaine, vous permettez à Azure de reconnaître votre domaine personnalisé sans modifier l'enregistrement DNS du domaine. Une fois que l'enregistrement DNS pour le domaine a été modifié, il est mappé au point de terminaison blob sans aucun temps d'arrêt.

L'exemple suivant montre comment un domaine en cours d'utilisation est mappé à un compte de stockage Azure dans le DNS avec le domaine

intermédiaire `asverify` :

- 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.

Pour accéder à ces paramètres pour votre compte de stockage, vous utilisez les paramètres Pare-feu et réseaux virtuels . Vous ajoutez les réseaux virtuels qui doivent avoir accès au service pour le compte.

### Informations sur la configuration des points de terminaison de service

Voici quelques points à prendre en compte pour configurer les paramètres d'accès au 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.

## Configurer Stockage Blob Azure

### Implémenter Stockage Blob Azure

Blob est l'acronyme de Binary Large Object.

#### 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

Éléments à prendre en compte lors de l'implémentation de Stockage Blob Azure

- **Envisagez les chargements dans les navigateurs.** Utilisez le stockage Blob pour servir des images ou des documents directement dans un navigateur.
- **Envisagez l'accès distribué.** Le Stockage Blob peut stocker des fichiers pour un accès distribué, par exemple pendant un processus d'installation.
- **Envisagez de diffuser des données en continu.** Diffusez en continu de la vidéo et de l'audio à l'aide du stockage Blob.
- **Envisagez l'archivage et la récupération.** Le stockage d'objets blob est une solution idéale pour stocker des données pour la sauvegarde et la restauration, la récupération d'urgence et l'archivage.
- **Envisagez l'accès aux applications.** Vous pouvez stocker des données dans le Stockage Blob pour l'analyse par un service local ou hébergé par Azure.

Créer des conteneurs d'objets blob

- Tous les objets blob doivent figurer dans un conteneur.
- Un conteneur peut stocker un nombre illimité d'objets blob.
- Un compte de stockage Azure peut contenir un nombre illimité de conteneurs.
- Vous pouvez créer le conteneur dans le portail Azure.
- Vous chargez des objets blob dans un conteneur

Dans le Portail Azure, vous configurez deux paramètres pour créer un conteneur pour un compte de stockage Azure.

- **Nom** : Saisissez un nom pour votre conteneur. Le nom du compte de Stockage Azure doit être unique dans Azure.
  - Le nom ne peut contenir que des lettres minuscules, des chiffres et des traits d'union.
  - Le nom doit commencer par une lettre ou un chiffre
  - La longueur minimale du nom est de trois caractères.
  - La longueur maximale du nom est de 63 caractères.
- **Niveau d'accès public** : le niveau d'accès spécifie si le conteneur et ses objets blob sont accessibles publiquement. Par défaut, les données de conteneur sont privées et visibles uniquement par le propriétaire du compte. Il existe trois choix de niveau d'accès :

- **Privé** : (par défaut) Interdit l'accès anonyme au conteneur et aux objets blob.
- **Blob** : autoriser un accès en lecture publique anonyme aux objets blob uniquement.
- **Conteneur** : autoriser l'accès public anonyme permettant de lire et de répertorier l'ensemble du conteneur, notamment les blobs

## Affecter des niveaux d'accès aux 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.

Comparer	Niveau de stockage chaud	Niveau de stockage froid	Niveau de stockage archive
Disponibilité	99,9 %	99 %	Hors connexion
Disponibilité (lectures RA-GRS)	99,99 %	99,9 %	Hors connexion

<b>Latence (temps jusqu'au premier octet)</b>	millisecondes	millisecondes	heures
<b>Durée de stockage minimale</b>	N/A	30 jours	180 jours
<b>Coûts d'utilisation</b>	Coûts de stockage supérieurs, coûts d'accès et de transaction inférieurs	Coûts de stockage plus faibles, coûts de transaction et d'accès plus élevés	Coûts de stockage les plus faibles, coûts de transaction et d'accès les plus élevés

Vous pouvez également modifier le niveau d'accès aux objets blob pour votre compte à tout moment.

## Ajouter des règles de gestion de cycle de vie des objets blob

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.

## Déterminer la réplification d'objets blob

Pendant le processus de réplification, le contenu suivant est copié du conteneur source vers le conteneur de destination :

- Contenu de l'objet blob
- Métadonnées et propriétés de l'objet blob
- Toutes les versions des données associées à l'objet blob

## Ce qu'il faut savoir sur la réplification d'objets blob

- La réplification d'objets implique que le contrôle de version des objets blob soit activé sur les comptes source et de destination.
- La réplification 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 réplification 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 réplification d'objets, vous créez une stratégie de réplification qui spécifie le compte Stockage Azure source et le compte de destination.
- Une stratégie de réplification 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.

Éléments à prendre en compte lors de l'utilisation des outils de chargement d'objets blob

Outil de chargement	Description
<b>AZCopy</b>	Outil en ligne de commande facile à utiliser pour Windows et Linux. Vous pouvez copier des données vers et depuis le stockage Blob, entre conteneurs et entre comptes de stockage.
<b>Azure Data Box Disk</b>	Un service permettant de transférer des données locales vers le stockage Blob quand des gros jeux de données ou des contraintes réseau rendent infaisable le chargement de données via le réseau. Vous pouvez utiliser Azure Data Box Disk pour demander des disques SSD à Microsoft. Vous pouvez copier vos données sur ces disques et les expédier à Microsoft qui les chargera dans le stockage Blob.
<b>Azure Import/Export</b>	Un service qui vous aide à exporter de grandes quantités de données depuis votre compte de stockage vers les disques durs que vous fournissez, et que Microsoft vous retourne ensuite avec vos données.

Déterminer la tarification du Stockage Blob

- **Niveaux de performances.** Le niveau Stockage Blob détermine la quantité de données stockées et le coût du stockage de ces données. 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. Pour les données des niveaux Froid et Archive, des frais d'accès aux données en lecture vous sont facturés par gigaoctet.
- **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. Cette facturation est cohérente avec celle des comptes Stockage Azure universels.
- **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. La modification du niveau de stockage de compte chaud vers un niveau de stockage froid induit des frais équivalents à l'écriture de toutes les données dans le niveau froid (comptes GPv2 uniquement).

## Configurer la sécurité du Stockage Azure

### 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.

Éléments à prendre en compte pour la sécurité de l'autorisation

<b>Stratégie d'autorisation</b>	<b>Description</b>
<b>Azure Active Directory</b>	Azure AD est le service cloud de Microsoft qui gère les identités et les accès. Avec Azure AD, vous pouvez attribuer un accès de granularité fine aux utilisateurs, groupes ou applications à l'aide du contrôle d'accès en fonction du rôle (RBAC).
<b>Clé partagée</b>	L'autorisation de clé partagée s'appuie sur les clés d'accès de votre compte Azure et d'autres paramètres pour produire une chaîne de signature chiffrée. La chaîne est transmise à la demande dans l'en-tête d'autorisation.
<b>Signatures d'accès partagé</b>	Une signature SAS délègue l'accès à une ressource particulière de votre compte avec les autorisations spécifiées et pour un intervalle de temps spécifié.
<b>Accès anonyme aux conteneurs et objets blob</b>	Vous pouvez éventuellement rendre publiques des ressources blob au niveau du conteneur ou de l'objet blob. Un conteneur ou un objet blob public est accessible à tout utilisateur avec un accès en lecture anonyme. Les demandes de lecture sur les conteneurs et objets blob publics ne nécessitent aucune autorisation.

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.

#### Identifier les paramètres URI et SAS

Quand vous créez votre signature SAS, un identificateur URI (Uniform Resource Identifier) est créé à l'aide de paramètres et de jetons. L'URI se compose de votre URI de ressource Stockage Azure et du jeton SAS.

## Uniform Resource Identifier

.Ressource Stockage Azure

`https://...`

.Jeton de signature d'accès partagé

`?sv=...`

```
https://myaccount.blob.core.windows.net/?restype=service&comp=
properties&sv=2015-04-05&ss=bf&st=2015-04-29T22%3A18%3A26Z&se=
2015-04-30T02%3A23%3A26Z&sr=b&sp=rw&sip=168.1.5.60-168.1.5.70&
spr=https&sig=F%6GRVAZ5Cdj2Pw4tgU7I1STkWgn7bUkkAg8P6HESXwmf%4B
```

Paramètre	Exemple	Description
URI de ressource	<code>https://myaccount.<b>blob</b>.core.windows.net/ ?restype=<b>service</b> &amp;comp=properties</code>	Définit le point de terminaison de Stockage Azure et d'autres paramètres. Cet exemple définit un point de terminaison pour le Stockage Blob et indique que la signature SAS s'applique aux opérations au niveau du service. Quand l'URI est utilisé avec <b>GET</b> , les propriétés de stockage sont récupérées. Quand l'URI est utilisé avec <b>SET</b> , les propriétés de stockage sont configurées.

<b>Version du Stockage</b>	<b>sv=2015-04-05</b>	Pour la version du Stockage Azure 2012-02-12 et les versions ultérieures, ce paramètre indique la version à utiliser. Cet exemple indique que la version 2015-04-05 (5 avril 2015) doit être utilisée.
<b>Service de stockage</b>	<b>ss=bf</b>	Spécifie le Stockage Azure auquel la signature SAS s'applique. Cet exemple indique que la signature SAS s'applique au Stockage Blob et à Azure Files.
<b>Heure de début</b>	<b>st=2015-04-29T22%3A18%3A26Z</b>	(Facultatif) Spécifie la date et l'heure de début de la signature SAS en heure UTC. Cet exemple montre comment définir l'heure de début sur le 29 avril 2015 22:18:26 UTC. Si vous voulez que la signature d'accès partagé soit valide immédiatement, omettez l'heure de début.
<b>Heure d'expiration</b>	<b>se=2015-04-30T02%3A23%3A26Z</b>	Spécifie l'heure d'expiration de la signature SAS en heure UTC. Cet exemple montre comment définir l'heure d'expiration sur le 30 avril 2015 02:23:26 UTC.

<b>Ressource</b>	<b>sr=b</b>	Spécifie les ressources qui sont accessibles via la signature SAS. Cet exemple spécifie que la ressource accessible se trouve dans le Stockage Blob.
<b>autorisations</b>	<b>sp=rw</b>	Répertorie les autorisations à accorder. Cet exemple permet l'accès aux opérations de lecture et d'écriture.
<b>Plage d'adresses IP</b>	<b>sip=168.1.5.60-168.1.5.70</b>	Spécifie une plage d'adresses IP à partir desquelles les demandes sont acceptées. Cet exemple définit la plage d'adresses IP allant de 168.1.5.60 à 168.1.5.70.
<b>Protocole</b>	<b>spr=https</b>	Spécifie les protocoles à partir desquels le Stockage Azure accepte la signature SAS. Cet exemple indique que seules les requêtes via le protocole HTTP sont acceptées.

## Signature

`sig=F%6GRVAZ5Cdj2Pw4tgU7I1  
STkWgn7bUkkAg8P6HESXwmf%4B`

Spécifie que l'accès à la ressource est authentifié à l'aide d'une signature HMAC. La signature est calculée sur une chaîne de signature avec une clé à l'aide de l'algorithme SHA256, puis encodée en Base64.

## 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.

Dans le portail Azure, vous configurez le chiffrement du Stockage Azure en spécifiant le type de chiffrement. Vous pouvez gérer les clés vous-même ou utiliser des clés gérées par Microsoft. Tenez compte de la façon dont vous pouvez implémenter le chiffrement du Stockage Azure pour la sécurité de votre stockage.

## 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.

## Appliquer les meilleures pratiques de sécurité de Stockage Azure

<b>Recommandation</b>	<b>Description</b>
<b>Toujours utiliser le protocole HTTPS pour la création et la distribution</b>	Si une signature SAS est transmise via le protocole HTTP et interceptée, un attaquant risque de l'intercepter et de l'utiliser. Ces <i>attaques de l'intercepteur</i> peuvent compromettre des données sensibles ou permettre à l'utilisateur malveillant d'altérer les données.
<b>Référencer les stratégies d'accès stockées si possible</b>	Les stratégies d'accès stockées vous donnent la possibilité de révoquer les autorisations sans avoir à régénérer les clés de compte de stockage Azure. Définissez une date d'expiration éloignée dans le futur pour la clé du compte de stockage.
<b>Définir des délais d'expiration à court terme pour une signature SAS non planifiée</b>	Si une signature SAS est compromise, vous pouvez atténuer les attaques en limitant la validité de la signature SAS à une période courte. Cette pratique est importante si vous ne pouvez pas référencer une stratégie d'accès stockée. Des heures d'expiration avec une échéance à court terme permettent également de limiter la quantité de données pouvant être écrites dans un objet blob en limitant le temps disponible pour le chargement vers ce dernier.
<b>Demander aux clients de renouveler automatiquement la signature SAS</b>	Demandez aux clients de renouveler la signature SAS bien avant la date d'expiration. En la renouvelant de manière anticipée, vous leur laissez le temps de réessayer si le service fournissant la signature SAS n'est pas disponible.

**Planifier soigneusement la date de début de la signature SAS**

Si vous définissez la date de début d'une signature SAS sur l'heure actuelle, des défaillances peuvent être observées par intermittence pendant les premières minutes en raison des variations d'horloge (différences de l'heure actuelle sur différentes machines). En règle générale, définissez une heure de début située au moins 15 minutes dans le passé. Vous pouvez également ne définir aucune heure de début spécifique, ce qui entraîne la validité immédiate de la signature SAS dans tous les cas. Les mêmes conditions s'appliquent généralement à l'heure d'expiration. Vous pouvez observer jusqu'à 15 minutes de variation d'horloge (dans un sens ou dans l'autre) sur une demande. Pour les clients qui utilisent une version d'API REST antérieure à 2012-02-12, la durée maximale pour une signature SAS qui ne référence pas une stratégie d'accès stockée est d'une heure. Toutes les stratégies spécifiant une période plus longue échouent.

**Définissez les autorisations d'accès minimales pour les ressources**

Une bonne pratique en matière de sécurité consiste à fournir à l'utilisateur les privilèges minimaux requis. Si un utilisateur a besoin d'un accès en lecture à une seule entité, accordez-lui un accès en lecture à cette seule entité, plutôt qu'un accès en lecture/écriture/suppression à toutes les entités. Cette pratique permet également de limiter les dégâts si une signature SAS est compromise, car son pouvoir est moindre si elle tombe entre les mains d'un attaquant.

**Comprendre la facturation des comptes pour l'utilisation, notamment une signature SAS**

Si vous fournissez un accès en écriture à un objet blob, un utilisateur peut choisir de charger un objet blob de 200 Go. Si vous lui avez également accordé un accès en lecture, il peut choisir de le télécharger 10 fois, ce qui entraîne des coûts de sortie pour l'équivalent de 2 To. Accordez des autorisations limitées pour atténuer les risques liés aux actions éventuelles d'utilisateurs malveillants. Utilisez une signature SAS à durée de vie limitée pour limiter cette menace, sans oublier de prendre en compte les variations d'horloge pour l'heure de fin.

**Valider les données écrites avec une signature SAS**

Quand une application cliente écrit des données dans votre compte de stockage Azure, n'oubliez pas que ces données peuvent être une source de problèmes. Si votre application nécessite des données validées ou autorisées, validez les données après leur écriture, mais avant leur utilisation. Cette pratique assure également une protection contre l'écriture de données endommagées ou malveillantes dans votre compte, soit par un utilisateur qui a acquis correctement la signature d'accès partagé, soit par un utilisateur qui exploite sa divulgation.

**Ne pas partir du principe qu'une signature SAS est toujours la meilleure option**

Dans certains scénarios, les risques associés à une opération particulière sur votre compte de stockage Azure sont plus importants que les avantages de l'utilisation d'une signature SAS. Pour ces opérations, créez un service de niveau intermédiaire qui écrit dans votre compte de stockage après avoir effectué la validation des règles métier, l'authentification et un audit. Il est également parfois plus simple de gérer l'accès par d'autres moyens. Si vous souhaitez que l'ensemble des objets blob dans un conteneur soient lisibles publiquement, vous pouvez rendre le conteneur public, au lieu de fournir une signature SAS d'accès à chaque client.

**Superviser vos applications avec Azure Storage Analytics**

Vous pouvez utiliser la journalisation et les métriques pour observer tout pic des échecs d'authentification. Vous pouvez constater des pics dus à une interruption de votre service fournisseur SAS ou à la suppression accidentelle d'une stratégie d'accès stockée.

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.

- 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.

**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 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.

- 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.

**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.

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 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.

**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.

## Gérer les partages Azure Files

Pour accéder à vos fichiers, vous avez besoin d'un compte de stockage Azure. Une fois que vous avez un compte de stockage, vous pouvez créer et configurer un partage de fichiers en utilisant Azure Files dans le portail Azure.

Éléments à prendre en compte quand vous utilisez des partages Azure Files

- **Ouvrir le port 445.** Azure Files utilise le protocole SMB. SMB communique via le port TCP 445. Vérifiez que le port 445 est ouvert. Assurez-vous également que votre pare-feu ne bloque pas le port TCP 445 de la machine cliente.
- **Activer le transfert sécurisé.** Le paramètre **Secure transfer required** améliore la sécurité de votre compte de stockage en acceptant uniquement les requêtes à votre compte de stockage qui proviennent de connexions sécurisées.

## 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.

Éléments à prendre en compte lors de l'utilisation des instantanés de partages de fichiers

### Avantage

### Description

***Protection contre l'altération des données et les erreurs d'application***

Les applications qui utilisent des partages de fichiers effectuent des opérations telles que l'écriture, la lecture, le stockage, la transmission et le traitement de données. Quand une application présente un défaut de configuration ou qu'un bogue involontaire est introduit, l'altération ou le remplacement accidentel de quelques blocs de données peuvent se produire. Pour vous protéger contre ces scénarios, vous pouvez prendre un instantané de partage avant de déployer le nouveau code d'application. Quand un bogue ou une erreur d'application est introduit dans le nouveau déploiement, vous pouvez revenir à une version précédente de vos données sur ce partage de fichiers.

***Protection contre une suppression accidentelle ou une modification involontaire***

Supposons que vous travailliez sur un fichier texte dans un partage de fichiers. Une fois le fichier texte fermé, vous ne pouvez plus annuler les modifications apportées. Dans ce scénario, vous avez besoin de récupérer une version antérieure de votre fichier. Vous pouvez utiliser les instantanés de partage pour récupérer des versions précédentes du fichier s'il est renommé ou supprimé accidentellement.

***Prise en charge de la sauvegarde et de la récupération***

Après avoir créé un partage de fichiers, vous pouvez régulièrement créer un instantané de ce partage de fichiers en vue de l'utiliser à des fins de sauvegarde de données. Pris régulièrement, un instantané de partage facilite la conservation de versions antérieures de données à des fins d'audit ou de récupération d'urgence.

## 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

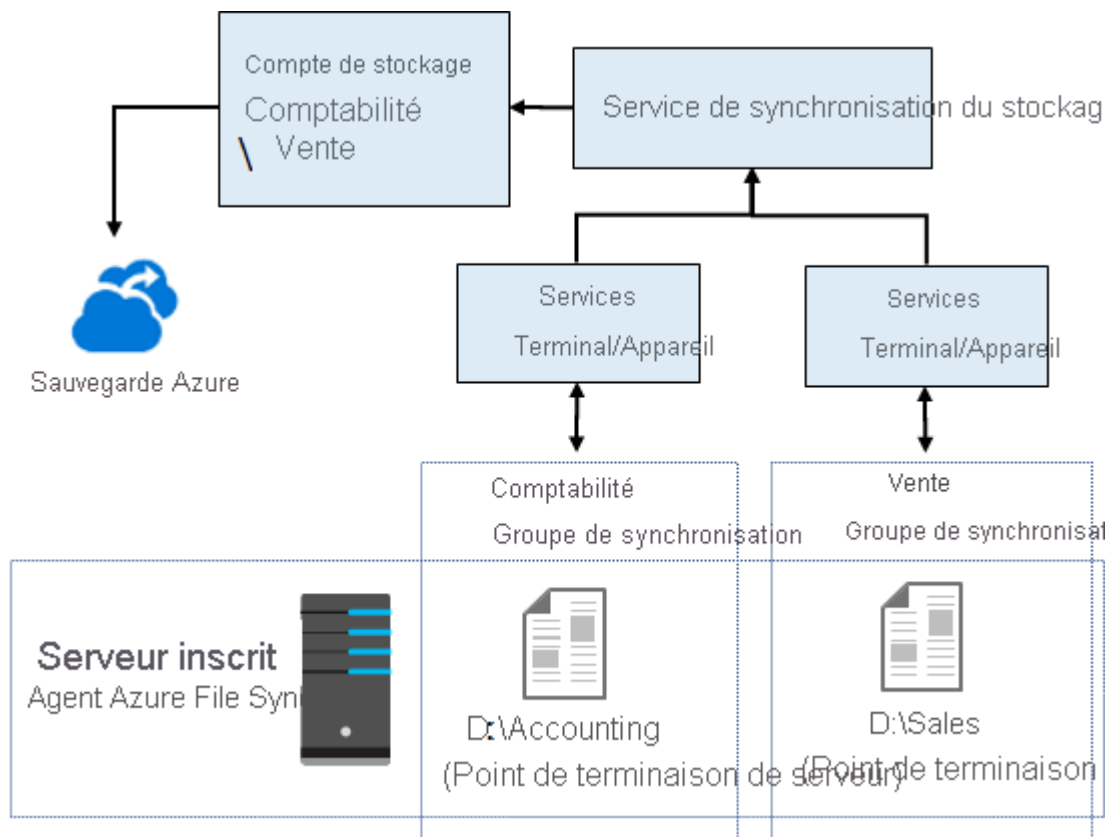
- Quand un fichier est hiérarchisé, Azure File Sync remplace le fichier localement par un pointeur. Un pointeur est communément appelé *point d'analyse*. Le point d'analyse représente une URL vers le fichier dans Azure Files.
- Lorsqu'un utilisateur ouvre un fichier hiérarchisé, Azure File Sync rappelle 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 **O** hors connexion pour permettre à l'utilisateur de savoir que le fichier est uniquement dans Azure.

## Aspects à prendre en compte lors de l'utilisation d'Azure File Sync

- **Envisagez d'opérer un lift-and-shift d'application.** Utilisez Azure File Sync pour déplacer des applications qui nécessitent un accès entre Azure et des systèmes locaux. Donnez un accès en écriture aux mêmes données sur les serveurs Windows et Azure Files.
- **Envisagez un support pour les filiales.** Fournissez un support aux filiales qui doivent sauvegarder des fichiers à l'aide de Azure File Sync. Utilisez le service pour configurer un nouveau serveur qui se connecte à un stockage Azure.
- **Envisagez la sauvegarde et la récupération d'urgence.** Après avoir implémenté Azure File Sync, le service Sauvegarde Azure sauvegarde vos données locales. Restaurez les métadonnées de fichier immédiatement et rappelez les données selon le besoin pour une récupération d'urgence rapide.
- **Envisagez l'archivage de fichiers avec la hiérarchisation cloud.** Azure File Sync stocke uniquement les données récemment utilisées sur les serveurs locaux. Implémentez la hiérarchisation cloud afin que les données non utilisées migrent vers Azure Files.

## Identifier les composants d'Azure File Sync

Azure File Sync présente quatre composants principaux qui fonctionnent ensemble pour fournir la mise en cache des partages Azure Files sur une machine Windows Server locale ou une machine virtuelle cloud.



### 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.

## Déployer Azure File Sync

### Étape 1 : Déployer le service de synchronisation du stockage

Vous pouvez déployer le service de synchronisation du stockage à partir du portail Azure. Vous configurez les paramètres suivants :

- Nom du déploiement du service de synchronisation du stockage
- ID d'abonnement Azure à utiliser pour le déploiement
- Groupe de ressources pour le déploiement
- Emplacement du déploiement

### Étape 2 : Préparer Windows Server à l'utilisation d'Azure File Sync

Après avoir déployé le service de synchronisation du stockage, vous configurez chaque Windows Server ou machine virtuelle cloud que vous envisagez d'utiliser avec Azure File Sync, y compris les nœuds serveurs dans un cluster de basculement.

### Étape 3 : Installer l'agent Azure File Sync

Une fois la configuration de Windows Server terminée, vous êtes prêt à installer l'agent Azure File Sync. L'agent est un package téléchargeable qui permet à Windows Server de rester synchronisé avec un partage Azure Files. Le package d'installation de l'agent Azure File Sync devrait s'installer relativement vite.

### Étape 4 : Inscrire chaque Windows Server auprès du service de synchronisation du stockage

Une fois l'installation de l'agent Azure File Sync terminée, la fenêtre **Inscription du serveur** s'ouvre.

Le fait d'inscrire le Windows Server auprès d'un service de synchronisation du stockage établit une relation d'approbation entre votre serveur (ou cluster) et le service de synchronisation du stockage. Pour l'inscription, vous avez besoin de votre ID d'abonnement Azure et de certains des paramètres de déploiement que vous avez configurés à la première étape :

- Nom du déploiement du service de synchronisation du stockage
- Groupe de ressources pour le déploiement

## Notes

Un serveur (ou cluster) ne peut être inscrit qu'auprès d'un seul service de synchronisation à la fois.

## Configurer le Stockage Azure avec des outils

### 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.

### Réflexions nécessaires lors de l'utilisation de l'Explorateur Stockage Azure

<b>Scénario</b>	<b>Description</b>
<b>Connexion à un abonnement Azure</b>	Gérez les ressources de stockage appartenant à votre abonnement Azure.

<b>Utilisation du stockage de développement local</b>	Gérez le stockage local à l'aide de l'émulateur de stockage Azure.
<b>Attachement au stockage externe</b>	Gérez les ressources de stockage qui appartiennent à un autre abonnement Azure ou qui sont dans des clouds Azure nationaux en utilisant les points de terminaison, la clé et le nom du compte de stockage. Ce scénario est décrit plus en détail dans la section suivante.
<b>Attacher un compte de stockage à une signature d'accès partagé</b>	Gérez les ressources de stockage qui appartiennent à un autre abonnement Azure à l'aide d'une signature d'accès partagé (SAP).
<b>Attacher un service à une signature d'accès partagé</b>	Gérez un service de Stockage Azure spécifique (conteneur d'objets blob, file d'attente ou table) appartenant à un autre abonnement Azure à l'aide d'une signature SAS (signature d'accès partagé).

#### 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.

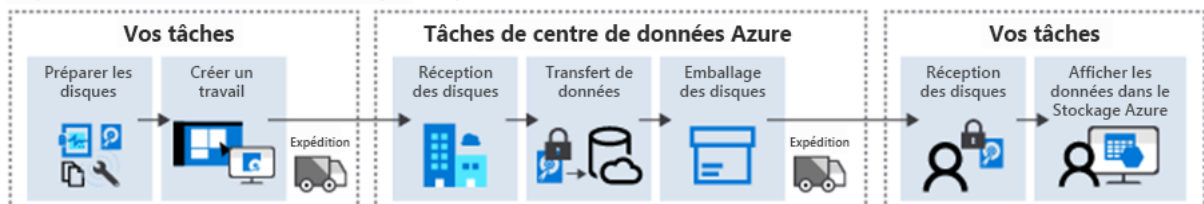
### Éléments à savoir sur le service Azure Import/Export

- 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.

#### Importer des données avec Azure Import/Export



### Créer un travail Azure Import.

Suivez ces étapes pour créer un travail Azure Import.

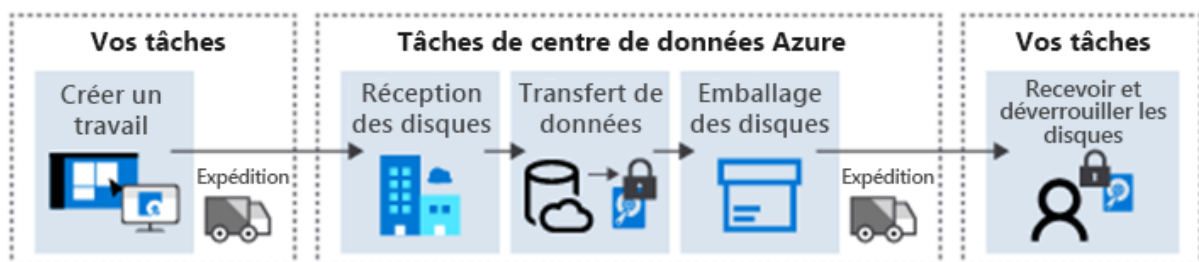
1. Si vous n'avez pas de compte de stockage Azure, [créez un compte](#) à utiliser pour la tâche d'importation.
2. Déterminez le nombre de disques nécessaires pour accueillir les données à transférer.
3. Identifiez l'ordinateur à utiliser pour effectuer la copie des données et joignez les disques physiques que vous envisagez d'expédier à Microsoft.

4. Installez l'outil WAImportExport sur les disques. Nous allons examiner de plus près l'outil WAImportExport dans l'unité suivante.
5. Exécutez l'outil WAImportExport pour copier les données sur les disques.
  1. Chiffrer les lecteurs de disque avec BitLocker.
  2. Générez des fichiers journaux pour documenter le transfert de données.
6. Dans le Portail Azure, créez un travail Azure Import et fournissez les informations suivantes :
  1. Compte de stockage Azure à utiliser pour le travail d'importation
  2. Adresse de retour pour l'expédition de vos disques
  3. Votre numéro de compte de transporteur d'expédition
  4. Adresse du centre de données de la région Azure qui héberge le compte de stockage Azure
7. Expédiez le nombre requis de disques au centre de données de la région Azure hébergeant le compte de stockage. Notez le numéro de suivi des expéditions.
8. Mettez à jour le travail d'importation pour inclure le numéro de suivi des expéditions.
9. Une fois les disques arrivés au centre de données Azure, le personnel effectue les tâches suivantes :
  1. Les données sur les disques fournis sont copiées dans le compte de stockage spécifié.
  2. Les disques vous sont renvoyés.

## 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.

### Exporter des données avec Azure Import/Export



## Créer un travail Azure Export

Identifiez les données à exporter dans Stockage Blob Azure.

Déterminez le nombre de disques nécessaires pour accueillir les données à transférer.

Dans le Portail Azure, créez un travail Azure Export et fournissez les informations suivantes :

Compte de stockage Azure à utiliser pour le travail d'exportation

Données blob à exporter

Adresse de retour pour l'expédition de vos disques

Votre numéro de compte de transporteur d'expédition

Expédiez le nombre requis de disques au centre de données de la région Azure hébergeant le compte de stockage. Notez le numéro de suivi des expéditions.

Mettez à jour le travail d'exportation pour inclure le numéro de suivi des expéditions.

Une fois les disques arrivés au centre de données Azure, le personnel effectue les tâches suivantes :

Les données spécifiées dans le compte de stockage sont copiées sur les disques que vous avez fournis.

Les volumes de disque sont chiffrés à l'aide de BitLocker.

Les disques vous sont renvoyés.

Les clés BitLocker utilisées pour chiffrer vos disques sont stockées avec le compte de stockage spécifié dans le Portail Azure. Vous pouvez déchiffrer le contenu des disques et copier les données dans votre stockage local.

## 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.

#### Éléments à prendre en compte lors de l'utilisation de l'outil WAImportExport

- **Tenez compte des lecteurs de disque pris en charge.** Pour les disques durs, le service Azure Import/Export nécessite des disques durs SATA II/III internes ou des disques SSD. Gardez cette exigence à l'esprit lors de la sélection de vos disques durs.
- **Envisagez le chiffrement BitLocker.** Lorsque vous préparez un disque pour un travail Azure Import, vous devez chiffrer le volume NTFS de chaque lecteur de disque avec BitLocker.
- **Envisagez la version du système d'exploitation.** Pour préparer un lecteur de disque, vous devez le connecter à un ordinateur exécutant une version 64 bits du système d'exploitation Windows client ou serveur. Vous exécutez l'outil WAImportExport à partir de cet ordinateur.

#### 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
<b>Azure Active Directory (Azure AD)</b>	Le Stockage Blob Azure et Azure Data Lake Storage Gen2	L'utilisateur entre la commande de connexion <code>.\azcopy</code> pour se connecter à l'aide d'Azure AD. L'utilisateur doit disposer du rôle <i>Contributeur aux données Blob du stockage</i> 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 SAS à chaque commande.
<b>Jetons SAS</b>	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.

## AzCopy et l'Explorateur Stockage Azure

L'Explorateur Stockage Azure utilise l'outil AzCopy pour tous ses transferts de données.

L'Explorateur Stockage Azure utilise votre clé de compte pour effectuer des opérations. Une fois connecté à l'Explorateur Stockage Azure, vous n'avez plus besoin de fournir vos informations d'autorisation.

Éléments à prendre en compte lors de l'utilisation de AzCopy

- **Considérez la synchronisation de données.** Utilisez AzCopy pour synchroniser un système de fichiers avec le Stockage Blob Azure et vice versa. AzCopy est idéal pour les scénarios de copie incrémentielle.
- **Envisagez la gestion des travaux.** Gérez vos opérations de transfert avec AzCopy. Affichez et redémarrez les travaux précédents. Reprenez les travaux ayant échoué.
- **Tenez compte de la résilience de transfert.** Fournissez une résilience des données pour vos transferts de données. En cas d'échec d'un travail de copie, AzCopy retente automatiquement la copie.
- **Envisagez une copie rapide de compte à compte.** Utilisez AzCopy avec le Stockage Blob Azure pour la fonctionnalité de copie de compte à compte. Étant donné que les données ne sont pas transférées au client, le transfert est plus rapide.

Prise en main de l'interface CLI AzCopy

La syntaxe CLI de base pour AzCopy commence par la commande `azcopy` suivie du type de travail à effectuer, par exemple `copy`. Pour la commande `copy`, vous spécifiez le chemin `[source]` des fichiers à copier, le chemin `[destination]` des fichiers copiés et les options `[flags]` à appliquer au travail de transfert.

```
azcopy copy [source] [destination] [flags]
azcopy --help
```

## Créer un compte de stockage

Un *compte de stockage* est un conteneur qui regroupe un ensemble de services de stockage Azure. Seuls les services de données du stockage Azure peuvent être inclus dans un compte de stockage (objets blob, fichiers, files d'attente et tables Azure).

La combinaison de services de données dans un seul compte de stockage vous permet de les gérer comme un groupe. Les paramètres que vous spécifiez quand vous créez le compte ou les changements que vous effectuez après la création s'appliquent à tous les services dans le compte de stockage.

La suppression du compte de stockage supprime toutes les données qui y sont stockées.

## Paramètres du compte de stockage

Un compte de stockage définit une stratégie qui s'applique à tous les services de stockage dans le compte.

- **Abonnement** : abonnement Azure auquel les services seront facturés dans le compte.
- **Emplacement** : centre de données qui stocke les services dans le compte.
- **Performances** : option qui détermine les services de données accessibles au compte de stockage et le type de disque matériel utilisé pour stocker les données.
  - **Standard** vous permet de disposer de tous les services de données (Blob, Fichier, File d'attente, Table) et utilise des lecteurs de disque magnétiques.
  - **Premium** fournit plus de services pour le stockage des données. Par exemple, le stockage de données d'objets non structurés comme les objets blob de blocs ou d'ajout et le stockage de fichiers spécialisés utilisé pour stocker et créer des partages de fichiers Premium. Ces comptes de stockage utilisent des disques SSD pour le stockage.
- **Réplication** : stratégie utilisée pour effectuer des copies des données dans une optique de protection contre une défaillance matérielle ou une catastrophe naturelle. Azure gère automatiquement au moins trois copies de vos données dans le centre de données associé au compte de stockage. La réplication minimale est appelée stockage localement redondant (LRS) et vous protège contre les pannes matérielles. Elle ne protège pas en cas d'événement affectant l'ensemble du centre de données. Vous pouvez effectuer une mise à niveau vers les autres options, comme le stockage géoredondant (GRS), pour effectuer la réplication sur différents centres de données à travers le monde.
- **Niveau d'accès** : contrôle la rapidité avec laquelle vous pouvez accéder aux blobs dans un compte de stockage. Le niveau d'accès chaud est optimisé pour stocker les données qui sont fréquemment consultées ou modifiées et offre un accès plus rapide que l'accès sporadique, mais à un coût de stockage plus élevé. Le niveau d'accès sporadique est optimisé pour stocker des données rarement consultées ou modifiées et a un coût de stockage inférieur. Le niveau d'accès chaud s'applique uniquement aux blobs et sert de valeur par défaut pour les nouveaux blobs.
- **Transfert sécurisé requis** : fonctionnalité de sécurité qui détermine les protocoles pris en charge pour l'accès. Quand elle est activée, la fonctionnalité exige le protocole HTTPS, quand elle est désactivée, autorise le protocole HTTP.
- **Réseaux virtuels** : fonctionnalité de sécurité qui n'autorise que les requêtes d'accès entrant provenant du ou des réseaux virtuels spécifiés.

Le nombre de comptes de stockage nécessaires est généralement déterminé par la diversité de vos données, la sensibilité aux coûts et la tolérance du temps de gestion.

### Sensibilité aux coûts

Un compte de stockage en lui-même n'a aucun coût financier ; toutefois, les paramètres que vous choisissez pour le compte influencent le coût des services dans le compte.

### Choisir les paramètres de votre compte

Les trois paramètres qui s'appliquent au compte proprement dit :

- Nom
- Modèle de déploiement
- Type de compte

### Modèle de déploiement

Un *modèle de déploiement* est le système utilisé par Azure pour organiser vos ressources. Le modèle définit l'API qui vous permet de créer, configurer et gérer ces ressources. Azure fournit deux modèles de déploiement :

- **Resource Manager** : modèle actuel qui utilise l'API Azure Resource Manager
- **Classique** : offre héritée qui utilise le modèle de déploiement classique

Le modèle Resource Manager ajoute le concept d'un *groupe de ressources*, qui n'est pas disponible dans le modèle Classic. Un groupe de ressources vous permet de déployer et de gérer une collection de ressources sous la forme d'une seule unité.

Microsoft recommande l'utilisation de **Resource Manager** pour toutes les nouvelles ressources.

### 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.

## Contrôler l'accès au Stockage Azure avec des signatures d'accès partagé

### Options d'autorisation pour le Stockage Azure

Les clients accèdent aux fichiers stockés dans le Stockage Azure via HTTP/HTTPS. Azure vérifie chaque demande d'autorisation du client pour accéder aux données stockées. Quatre options sont disponibles pour le stockage Blob :

- Accès public
- Azure Active Directory (Azure AD)
- Clé partagée
- Signature d'accès partagé (SAP)

#### Accès public

L'accès public est également connu comme accès en lecture public anonyme pour les conteneurs et les blobs.

Il existe deux paramètres distincts qui affectent l'accès public :

- **Le compte de stockage.** Configurez le compte de stockage pour autoriser l'accès public en définissant la propriété *AllowBlobPublicAccess*. Quand la valeur est true, les données de blob sont disponibles en accès public uniquement si le paramètre d'accès public du conteneur est également défini.
- **Le conteneur.** Vous pouvez activer l'accès anonyme uniquement s'il a été autorisé pour le compte de stockage. Un conteneur a deux paramètres possibles pour l'accès public : *Accès en lecture public pour les blobs* ou *Accès en lecture public pour un conteneur et ses blobs*. L'accès anonyme est contrôlé au niveau du conteneur et pas sur chaque blob. Cela signifie que pour sécuriser certains fichiers, vous devez les placer dans un conteneur distinct qui n'autorise pas l'accès en lecture publique.

#### Azure Active Directory

Utilisez l'option Azure AD pour accéder de manière sécurisée au Stockage Azure sans avoir à stocker des informations d'identification dans votre code. L'autorisation AD se déroule en deux étapes. D'abord, vous authentifiez un principal de sécurité

qui retourne un jeton OAuth 2.0 en cas de réussite. Ensuite, ce jeton est transmis au Stockage Azure pour autoriser l'accès à la ressource demandée.

Utilisez cette méthode d'authentification si vous exécutez une application avec des identités managées ou des principaux de sécurité.

### Clé partagée

Le Stockage Azure crée deux clés d'accès 512 bits pour chaque compte de stockage créé. Vous partagez ces clés pour accorder aux clients l'accès au compte de stockage. Ces clés accordent à chaque personne autorisée l'équivalent d'un accès racine à votre stockage.

Nous vous recommandons de gérer les clés de stockage avec Azure Key Vault, car il est facile de permuter les clés selon une planification régulière pour assurer la sécurité de votre compte de stockage.

### Signature d'accès partagé

Une signature SAS vous permet d'accorder un accès granulaire aux fichiers dans le Stockage Azure, comme un accès en lecture seule ou un accès en lecture-écriture, et un délai d'expiration au bout duquel la signature SAS n'autorise plus le client à accéder aux ressources choisies. Une signature d'accès partagé est une clé qui accorde une autorisation à une ressource de stockage et doit être protégée de la même manière qu'une clé de compte.

Le service Stockage Azure prend en charge trois types de signatures d'accès partagé :

- **SAS de délégation d'utilisateur** : peut être utilisée seulement pour le stockage Blob et est sécurisée avec des informations d'identification Azure AD.
- **SAS de service** : une signature SAS de service est sécurisée avec une clé de compte de stockage. Une signature SAS de service délègue l'accès à une ressource dans un des quatre services de stockage Azure : Blob, File d'attente, Table ou Fichier.
- **SAS de compte** : une signature SAS de compte est sécurisée avec une clé de compte de stockage. Une signature SAS de compte a les mêmes contrôles qu'une signature SAS de service, mais elle contrôle aussi l'accès aux opérations de niveau service, comme l'obtention des statistiques du service.

Vous pouvez créer une signature SAS ad hoc en spécifiant toutes les options que vous devez contrôler, y compris l'heure de début, l'heure d'expiration et les autorisations.

Si vous prévoyez de créer une signature SAS de service, une autre option possible est de l'associer à une stratégie d'accès stockée. Une stratégie d'accès stockée peut être associée à un maximum de cinq SAS actives. Vous pouvez contrôler l'accès et l'expiration au niveau de la stratégie d'accès stockée. Il s'agit d'une bonne approche si vous devez avoir un contrôle granulaire afin de changer l'expiration ou révoquer une signature SAS. La seule façon de révoquer ou de changer une signature SAS ad hoc est de changer les clés du compte de stockage.

Que sont les stratégies d'accès stockées ?

Vous pouvez créer une stratégie d'accès stockée dans quatre types de ressources de stockage :

- Conteneurs d'objets blob
- Partages de fichiers
- Files d'attente
- Tables

La stratégie d'accès stockée que vous créez pour un conteneur d'objets blob peut s'appliquer à tous les objets blob qu'il contient en plus du conteneur lui-même. Une stratégie d'accès stockée est créée avec les propriétés suivantes :

- **Identificateur** : nom que vous utilisez pour référencer la stratégie d'accès stockée.
- **Heure de début** : Valeur DateTimeOffset pour la date et l'heure auxquelles la stratégie peut commencer à être utilisée. Cette valeur peut être null.
- **Heure d'expiration** : Valeur DateTimeOffset pour la date et l'heure auxquelles la stratégie expire. Passé ce délai, les demandes au stockage échoueront avec un message de code d'erreur 403.
- **Autorisations** : liste d'autorisations sous la forme d'une chaîne pouvant inclure tout ou partie des autorisations **acdlrw**.

Une stratégie d'accès stockée fournit un niveau de contrôle supplémentaire sur les signatures d'accès partagé au niveau du service (SAP) côté serveur. L'établissement d'une stratégie d'accès stockée sert à regrouper des signatures d'accès partagé et à fournir des restrictions supplémentaires pour les signatures liées par la stratégie.

## Charger, télécharger et gérer des données avec l'Explorateur Stockage Azure

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

### Objectifs d'apprentissage

Dans ce module, vous allez découvrir comment :

- Déterminez les responsabilités des fournisseurs de services cloud et des clients dans un environnement de cloud computing.
- Identifiez les principales considérations et facteurs impliqués dans la planification des machines virtuelles. Les considérations incluent les exigences en matière de charge de travail, l'allocation des ressources et l'accès sécurisé.
- Configurez le dimensionnement et le stockage des machines virtuelles.
- Créer une machine virtuelle dans le portail Azure
- Pratiquez le déploiement d'une machine virtuelle Azure et vérifiez la configuration.

## Configurer des machines virtuelles

### Passer en revue les responsabilités des services cloud

Responsabilité	SaaS	PaaS	IaaS	Local-ment	
Informations et données	Client	Client	Client	Client	<b>RESPONSABILITÉ TOUJOURS CONSERVÉE PAR LE CLIENT</b>
Appareils (mobiles et PC)	Client	Client	Client	Client	
Comptes et identités	Client	Client	Client	Client	
Infrastructure d'identité et d'annuaire	Microsoft	Client	Client	Client	<b>LA RESPONSABILITÉ VARIE SELON LE TYPE DE SERVICE</b>
Applications	Microsoft	Client	Client	Client	
Contrôles réseau	Microsoft	Client	Client	Client	
Système d'exploitation	Microsoft	Microsoft	Client	Client	<b>TRANSFERTS DE RESPONSABILITÉ AU FOURNISSEUR DE CLOUD</b>
Hôtes physiques	Microsoft	Microsoft	Microsoft	Client	
Réseau physique	Microsoft	Microsoft	Microsoft	Client	
Centre de données physique	Microsoft	Microsoft	Microsoft	Client	

Microsoft
  Client

## Planifier 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
- **Passer 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 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.

Éléments à prendre en compte lors du choix du stockage pour vos machines virtuelles

- **Utilisez le Stockage Premium Azure** : adapté aux charges de travail gourmande en E/S et stockent les données sur des disques SSD
- **Utilisez plusieurs disques de stockage** :
  - permet aux applications d'atteindre **256 To de stockage** par VM
  - avec le stockage Premium de réaliser
    - jusqu'à **80000 opérations E/S par seconde** par VM
    - un débit de disque maximal de **2000 Mo/s** par VM
- **Utilisez des disques managés Azure** :
  - sont stockés en tant qu'objets blob de page
  - les disques SSD, SSD Premium, SSD Standard et les lecteurs de disque dur (HDD) standard sont disponibles
- **Effectuez une migration vers le Stockage Premium** : pour bénéficier de performances optimales pour les charges de travail nécessitant un nombre élevé d'E/S

## 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
- Requier 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.

# Configurer la disponibilité des machines virtuelles

## 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**. Lorsque vous implémentez des groupes de machines virtuelles identiques et configurez toutes vos machines virtuelles de la même façon, vous obtenez une véritable *mise à l'échelle automatique*. 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**, votre implémentation peut s'étendre sur plusieurs groupes de placement d'une capacité allant jusqu'à 1000. 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.

- **Nombre minimal de machines virtuelles** : spécifiez le nombre minimal de machines virtuelles qui doivent être disponibles lorsque la mise à l'échelle automatique est appliquée à votre implémentation de Virtual Machine Scale

Sets.

- **Nombre maximal de machines virtuelles** : spécifiez le nombre maximal de machines virtuelles qui peuvent être disponibles lorsque la mise à l'échelle automatique est appliquée à votre implémentation.

### 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.

## Créer un groupe de machines virtuelles identiques

Informations de base   Disques   Réseau   **Mise à l'échelle**   Gestion   Intégrité   Avancé

Nombre initial d'instances \* ⓘ

### Mise à l'échelle

Stratégie de mise à l'échelle ⓘ

- Mise à l'échelle manuelle  
 Mise à l'échelle automatique

Nombre minimal d'instances \* ⓘ

Nombre maximal d'instances \* ⓘ

### Scale-out

Seuil du processeur (%) \* ⓘ

Durée en minutes \* ⓘ

Nombre d'instances à augmenter de \* ⓘ

 ✓

### Scale-in

Seuil du processeur (%) \* ⓘ

Nombre d'instances à diminuer de \* ⓘ

 ✓

### Stratégie de scale-in

Configurez l'ordre dans lequel les machines virtuelles sont sélectionnées pour la suppression pendant une opération de scale-in.

Stratégie de scale-in

- Par défaut : équilibre les zones de disponibilité et les domaines d'erreur, puis supprime la machine...
- Machine virtuelle la plus récente : équilibre les zones de disponibilité, puis supprime la dernière m...
- Machine virtuelle la plus ancienne : équilibre les zones de disponibilité, puis supprime la plus ancie...

## 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.

Éléments à prendre en considération lors de l'utilisation d'extensions de machine virtuelle

- **Réfléchissez au déploiement.** De petites applications d'extension de machine virtuelle peuvent être un sous-ensemble d'un déploiement plus important pour vos machines virtuelles.
- **Réfléchissez au provisionnement.** Vous pouvez utiliser des extensions de machine virtuelle en tant qu'applications de configuration pour faciliter le provisionnement de vos machines virtuelles.
- **Réfléchissez au post-déploiement.** Les extensions de machine virtuelle peuvent être exécutées sur tous les systèmes gérés par une extension prise en charge après le déploiement.

## 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"
```

Éléments à prendre en compte lors de l'utilisation d'extensions de script personnalisé

- **Réfléchissez aux tâches qui peuvent dépasser le délai d'expiration.** Gardez à l'esprit que l'exécution des extensions de script personnalisé ont seulement 90 minutes pour s'exécuter. Si votre déploiement prend plus de 90 minutes, votre tâche est marquée comme ayant *dépassé le délai d'attente*. Tenez compte du délai d'expiration lors de la conception de vos scripts. Votre machine virtuelle doit être en cours d'exécution pour pouvoir effectuer les tâches désignées.
- **Tenez compte des dépendances.** Identifiez les dépendances dans la configuration de votre tâche de machine virtuelle. Si votre extension de script personnalisé nécessite un accès réseau ou au stockage, vérifiez que le contenu est disponible.
- **Tenez compte des événements d'échec.** Planifiez en tenant compte des erreurs qui peuvent se produire lors de l'exécution de votre script. Identifiez les scénarios où vous risquez de manquer d'espace disque, ou les zones qui ont des restrictions de sécurité et d'accès. Établissez une stratégie pour la façon dont votre script répond aux erreurs.
- **Tenez compte des données sensibles.** Votre extension de script personnalisé peut avoir besoin d'informations sensibles telles que des informations d'identification, des noms de compte de stockage et des clés d'accès à des comptes de stockage. Réfléchissez à la façon dont vous protégez ou chiffrez vos informations sensibles.

## 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.

### Éléments à prendre en considération lors de l'utilisation de plans Azure App Service

- **Réfléchissez aux économies en termes de coûts.** Étant donné que vous payez pour les ressources informatiques allouées par votre plan App Service, vous pouvez potentiellement faire des économies en plaçant plusieurs applications dans le même plan App Service.
- **Pensez à placer plusieurs applications dans un même plan.** Créez un plan unique pour prendre en charge plusieurs applications, afin de faciliter la configuration et la gestion des instances de machine virtuelle partagées. Étant donné que les applications partagent les mêmes instances de machine

virtuelle, vous devez gérer soigneusement les ressources et la capacité de votre plan.

- **Réfléchissez à la capacité du plan.** Avant d'ajouter une nouvelle application à un plan existant, déterminez les besoins en ressources de la nouvelle application et identifiez la capacité restante de votre plan.
- **Réfléchissez à l'isolation des applications.** Isolez votre application dans un nouveau plan App Service lorsque :
  - L'application est gourmande en ressources.
  - Vous souhaitez mettre à l'échelle l'application indépendamment des autres applications dans le plan existant.
  - L'application a besoin de ressources dans une région géographique différente.

### 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.

Paramètres

Scale-out (plan App Service)

Choisir comment mettre à l'échelle votre ressource

Mise à l'échelle manuelle  Conserver un nombre d'instances fixe

Mise à l'échelle automatique personnalisée  Mettre à l'échelle selon n'importe quelle planification, en fonction des métriques

Profil 1 [✎](#) [🗑️](#)

Mode de mise à l'échelle  Mettre à l'échelle...  Mettre à l'échelle vers un nombre...

Nombre d'instances \*

Planification  Spécifier des dates de début/fin  Répéter des jours spécifiques

Fuseau horaire  ▼

Date de début

Date de fin

- 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.

Éléments à prendre en compte lors de la configuration de la mise à l'échelle automatique

- **Nombre minimal d'instances.** Définissez un nombre minimal d'instances pour faire en sorte que votre application s'exécute toujours même en l'absence de charge.
- **Nombre maximal d'instances.** Définissez un nombre maximal d'instances afin de plafonner votre coût horaire total possible.
- **Marge de mise à l'échelle adéquate.** Vérifiez que vos valeurs de nombre maximal et minimal d'instances sont différentes, et définissez une marge adéquate entre les deux valeurs. Vous pouvez mettre à l'échelle automatiquement entre le minimum et le maximum à l'aide de règles que vous créez.
- **Combinaisons de règles de mise à l'échelle.** Utilisez toujours une combinaison de règles de scale-out et de scale-in qui amènent à une augmentation et une diminution. Si vous ne définissez pas de règle de scale-out, votre application risque d'échouer ou les performances peuvent se dégrader en cas d'augmentation de la charge. Si vous ne définissez pas de règle de scale-in, vous risquez d'encourir des coûts inutiles et élevés en cas

de diminution de la charge.

- **Statistiques de métriques.** Choisissez soigneusement les statistiques appropriées pour vos métriques de diagnostic, notamment Moyenne, Minimum, Maximum et Total.
- **Nombre d'instances par défaut.** Sélectionnez toujours un nombre raisonnable d'instances par défaut. Le nombre d'instances par défaut est important, car la mise à l'échelle automatique utilise le nombre que vous spécifiez pour mettre à l'échelle votre service quand les métriques ne sont pas disponibles.
- **Notifications.** Configurez toujours des notifications de mise à l'échelle automatique. Il est important de rester conscient des performances de votre application à mesure que la charge évolue.

## 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
<b>Plusieurs langages et frameworks</b>	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.
<b>Optimisation DevOps</b>	App Service prend en charge l'intégration et le déploiement continu 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.

<b>Mise à l'échelle globale avec haute disponibilité</b>	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.
<b>Connexions aux plateformes SaaS et aux données locales</b>	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.
<b>Sécurité et conformité</b>	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.
<b>Modèles d'application</b>	Faites votre choix parmi une liste complète de modèles d'application dans la Place de marché Azure, tels que WordPress, Joomla et Drupal.
<b>Intégration de Visual Studio</b>	App Service offre des outils dédiés dans Visual Studio pour permettre de rationaliser le travail de création, de déploiement et de débogage.
<b>Fonctionnalités API et mobiles</b>	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.
<b>Code serverless</b>	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 continu

- 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.

## Ajouter des emplacements de déploiement

### 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.

<b>Paramètres échangés</b>	<b>Paramètres propres à l'emplacement</b>
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 <code>_EXTENSION_VERSION</code>

## Sécuriser votre application App Service

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.

## Sauvegarder et restaurer votre application App Service

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.

## Utiliser Azure Application Insights

Azure Application Insights est une fonctionnalité d'Azure Monitor qui vous permet de monitorer vos applications en production. Vous pouvez intégrer Application Insights à votre configuration App Service pour détecter automatiquement les anomalies de performances dans vos applications.

Application Insights est conçue pour vous aider à améliorer en permanence les performances et la convivialité de vos applications. La fonctionnalité offre des outils analytiques puissants pour vous aider à diagnostiquer les problèmes et comprendre ce que les utilisateurs font réellement avec vos applications.

## 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

### Passer en revue 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.

#### Implémenter des groupes de conteneurs

La ressource de niveau supérieur dans Azure Container Instances est un **groupe de conteneurs**. Un groupe de conteneurs est une collection de conteneurs qui sont planifiés sur le même ordinateur hôte. Les conteneurs d'un groupe de conteneurs partagent un cycle de vie, des ressources, un réseau local et les volumes de stockage.

#### 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.

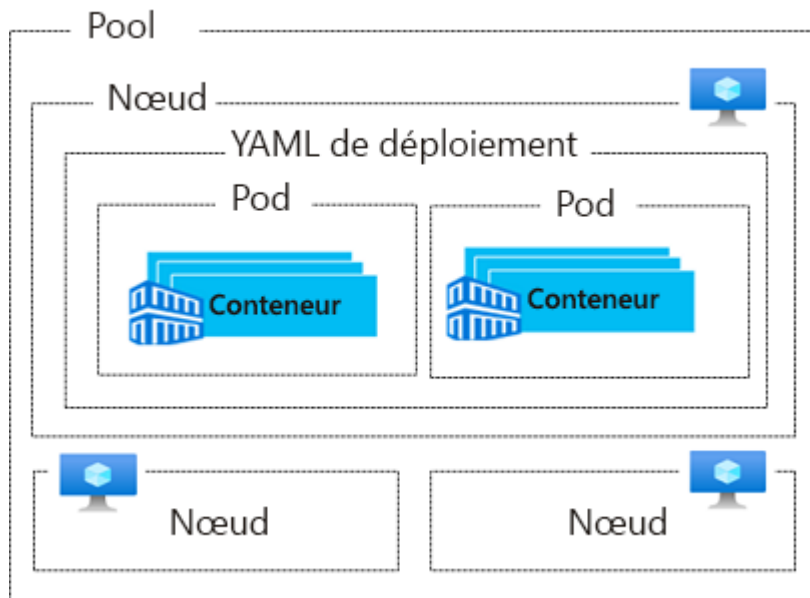
Imaginons un groupe de conteneurs qui comporte deux conteneurs nécessitant chacun des ressources du processeur. Chaque conteneur nécessite un processeur. Azure Container Instances alloue deux processeurs pour le groupe de conteneurs.

- 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

Azure fonctionne comme un service Kubernetes hébergé et exécute des fonctions critiques telles que la surveillance et la maintenance de l'intégrité. AKS utilise des composants, tels que des nœuds, des pods et des pools, pour vous aider à déployer et à gérer vos applications de conteneur dans des clusters Kubernetes.



Ce qu'il faut savoir sur les concepts AKS

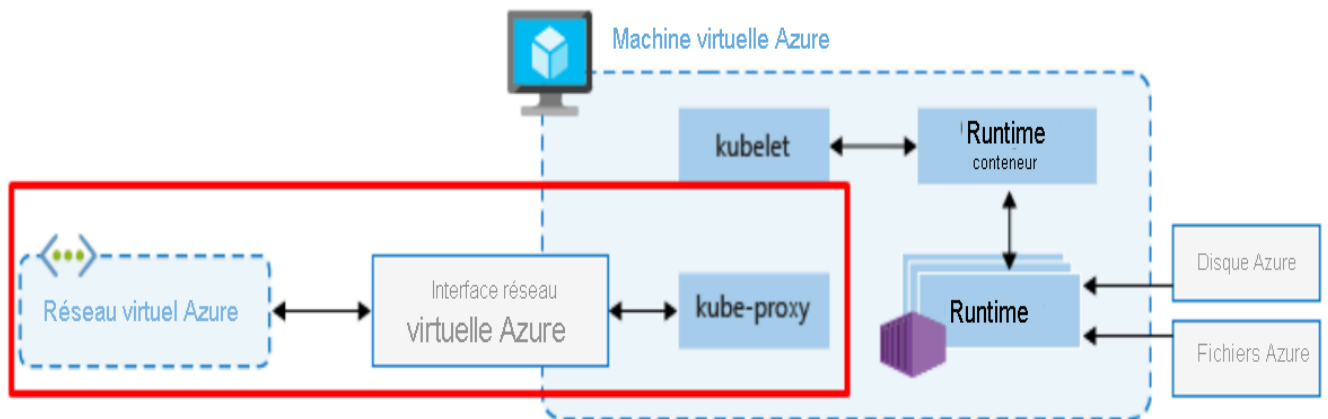
- **Pools** : Un pool est un groupe de nœuds qui ont une configuration identique.
- **Nœuds** : Un nœud est une machine virtuelle individuelle qui exécute des applications conteneurisées.
- **Pods** : Un pod représente une seule instance d'une application. Un pod peut contenir plusieurs conteneurs.
- **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.

L'illustration suivante montre un exemple de cluster AKS. Le nœud managé par Azure dispose d'un planificateur, d'un contrôleur, d'un serveur d'API et d'un stockage. Le nœud managé par le client a un runtime de conteneur, un conteneur, un agent kubelet et un composant kube-proxy. Nous allons examiner ces éléments dans la section suivante.





### 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
-----------------	-------------	----------

<b>IP du cluster</b>	Créez une adresse IP interne à utiliser dans un cluster Azure Kubernetes Service.	<i>Implémenter des applications internes uniquement qui prennent en charge d'autres charges de travail au sein du cluster</i>
<b>NodePort</b>	Créez un mappage de port sur le nœud sous-jacent.	<i>Autoriser un accès direct à l'application avec l'adresse IP et le port du nœud</i>
<b>LoadBalancer</b>	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.	<i>Autoriser le trafic des clients à atteindre l'application en créant des règles d'équilibrage de charge sur les ports souhaités</i>
<b>ExternalName</b>	Créez une entrée DNS spécifique.	<i>Prendre en charge un accès plus facile aux applications</i>

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.

Les pods sont généralement des ressources éphémères et jetables. Les pods planifiés de manière individuelle ne bénéficient pas de certaines des fonctionnalités de haute disponibilité et de redondance fournies par Kubernetes. À la place, les pods sont généralement déployés et managés par des contrôleurs Kubernetes, par exemple le contrôleur de déploiement.

## Configurer le stockage Azure Kubernetes Service

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 <code>StorageClass</code>	Description	Action <code>reclaimPolicy</code>
<code>default</code>	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.
<code>managed-premium</code>	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.

<code>azurefile</code>	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.
<code>azurefile-premium</code>	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.

## Configurer la mise à l'échelle Azure Kubernetes Service

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. Ce comportement permet au nouveau nombre de réplicas d'être pris en compte, et à l'API de métriques de refléter la charge de travail distribuée. 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 `kubect1` 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.

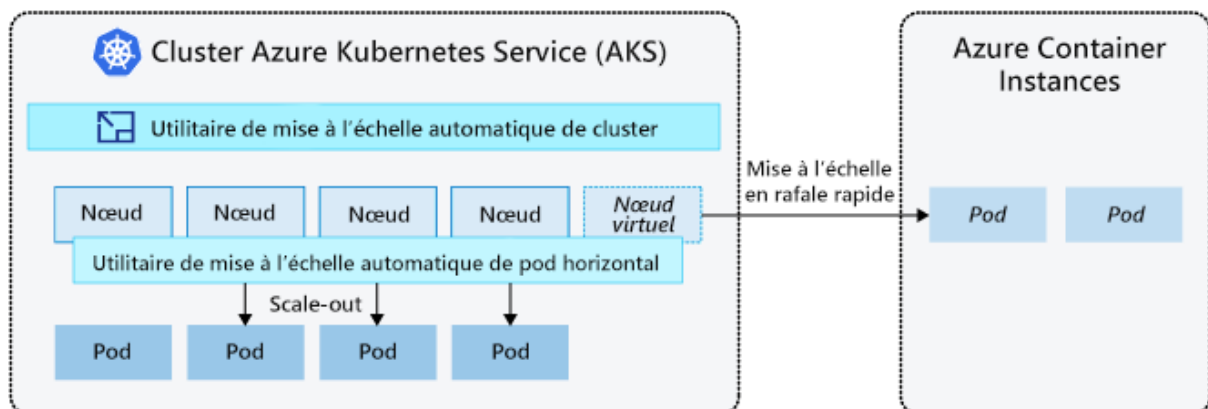
- **Envisagez une mise à l'échelle en rafale sur Azure Container Instances.** Si votre application doit être mise à l'échelle rapidement, certains pods risquent de rester à l'état d'attente de planification jusqu'à ce que les nouveaux nœuds déployés par l'autoscaler de cluster puissent accepter les pods 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.

## Configurer la mise à l'échelle en rafale d'AKS sur Azure Container Instances



### 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.

## Protéger les paramètres de vos machines virtuelles avec Azure Automation State Configuration

Azure Automation State Configuration résout la plupart des problèmes liés au déploiement à grande échelle et à la gestion des dérives de configuration.

### 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"  
    }  
}  
}
```

L'exemple précédent utilise le module `xSmbShare` qui indique à DSC *comment* vérifier l'état d'un partage de fichiers. Le kit de ressources DSC compte actuellement plus de 80 modules de ressources, notamment un pour l'installation d'un site IIS.

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.

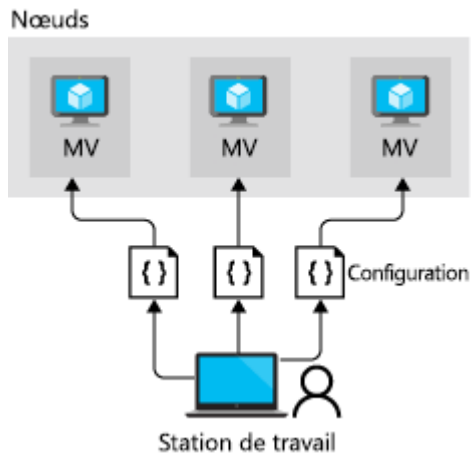
Vous configurez le Gestionnaire de configuration local quand vous inscrivez une machine virtuelle auprès d'Azure Automation.

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

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

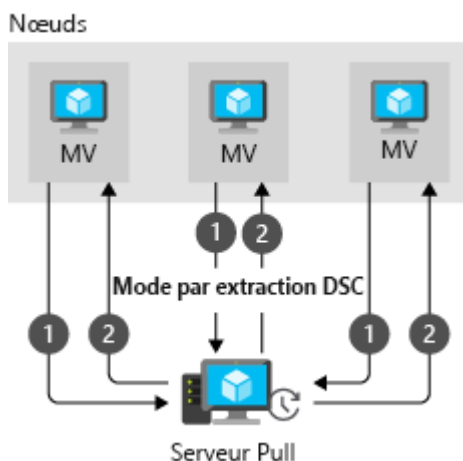
- **Mode push** : Un administrateur envoie manuellement ou *pousse* (push) les configurations vers un ou plusieurs nœuds. Le Gestionnaire de configuration

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.

Quand vous utilisez cette approche, chaque nœud doit être inscrit auprès du service Tirage (pull).



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

## Objectifs d'apprentissage

Dans ce module, vous allez découvrir comment :

- Décrivez les composants et les fonctionnalités du réseau virtuel Azure.
- Identifier les fonctionnalités et les cas d'usage des sous-réseaux et de leur mise en œuvre
- Identifier les cas d'usage des adresses IP privées et publiques
- Créez un réseau virtuel et attribuez une adresse IP.

## Configurer des réseaux virtuels

### Planifier des réseaux virtuels

- Un réseau virtuel Azure est une isolation logique du cloud Azure dédiée à votre abonnement.
- Vous pouvez utiliser des réseaux virtuels pour provisionner et gérer des réseaux privés virtuels (VPN) dans Azure.
- Chaque réseau virtuel a son propre bloc CIDR (Classless Inter-Domain Routing), et peut être lié à d'autres réseaux virtuels et réseaux locaux.
- Vous pouvez lier des réseaux virtuels à une infrastructure informatique locale pour créer des solutions hybrides ou intersites, quand les blocs CIDR des réseaux de connexion ne se chevauchent pas.
- Vous contrôlez les paramètres du serveur DNS pour les réseaux virtuels et la segmentation du réseau virtuel en sous-réseaux.

### Créer des sous-réseaux

#### 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.
  - Chaque sous-réseau contient une plage d'adresses IP qui appartient à l'espace d'adressage du réseau virtuel.
  - La plage d'adresses de chaque 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.
- 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

## Allouer ou attribuer des adresses IP privées

Éléments à prendre en compte lors de l'association d'adresses IP privées

Ressource	Association d'adresse IP privée	Adresse IP dynamique	Adresse IP statique
Machine virtuelle	Carte d'interface réseau	Oui	Oui
Équilibreur de charge interne	Configuration frontale	Oui	Oui
passerelle d'application	Configuration frontale	Oui	Oui

## 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.

Supposons que les adresses 10.0.0.4 à 10.0.0.9 soient déjà allouées à d'autres ressources. Dans ce cas, Azure alloue l'adresse 10.0.0.10 à une nouvelle ressource.

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

Supposons que la plage d'adresses d'un sous-réseau est 10.0.0.0/16 et que les adresses 10.0.0.4 à 10.0.0.9 sont déjà allouées à d'autres ressources. Dans ce scénario, vous pouvez allouer n'importe quelle adresse comprise entre 10.0.0.10 et 10.0.255.254.

## Configurer des groupes de sécurité réseau

### Implémenter des groupes de sécurité 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.

## Déterminer les règles du groupe de sécurité réseau

### 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 équilibrateurs de charge Azure.

### Règles de trafic sortant

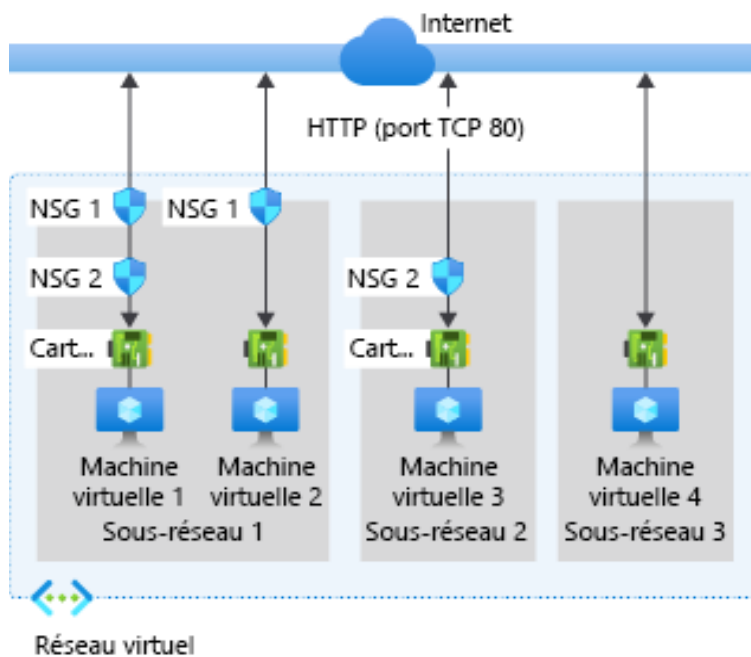
Azure définit trois règles de sécurité de trafic sortant par défaut pour votre groupe de sécurité réseau. Ces règles **autorisent uniquement le trafic sortant** vers Internet et vers votre réseau virtuel.

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.

La façon dont Azure applique vos règles de sécurité définies pour une machine virtuelle détermine l'effectivité générale de vos règles.

Ce qu'il faut savoir sur les règles de sécurité effectives



Évaluation	NSG de sous-réseau	NSG de carte réseau	Règles de trafic entrant	Règles de trafic sortant
VM 1	Sous-réseau 1 NSG 1	Carte d'interface réseau NSG 2	Les règles de sous-réseau NSG 1 sont prioritaires sur les règles de carte réseau NSG 2	Les règles de carte réseau NSG 2 sont prioritaires sur les règles de sous-réseau NSG 1

<b>Machine virtuelle 2</b>	Sous-réseau 1 <i>NSG 1</i>	Carte d'interface réseau <i>Aucune</i>	Les règles de sous-réseau <i>NSG 1</i> s'appliquent à la fois au sous-réseau et à la carte réseau	Les règles par défaut Azure s'appliquent à la carte réseau et les règles de sous-réseau <i>NSG 1</i> s'appliquent uniquement au sous-réseau
<b>VM 3</b>	Sous-réseau 2 <i>Aucune</i>	Carte d'interface réseau <i>NSG 2</i>	Les règles par défaut Azure s'appliquent au sous-réseau et les règles <i>NSG 2</i> s'appliquent à la carte réseau	Les règles de carte réseau <i>NSG 2</i> s'appliquent à la carte réseau et au sous-réseau
<b>VM 4</b>	Sous-réseau 3 <i>Aucune</i>	Carte d'interface réseau <i>Aucune</i>	Les règles Azure par défaut s'appliquent à la fois au sous-réseau et à la carte réseau et tout le trafic entrant est autorisé	Les règles Azure par défaut s'appliquent à la fois au sous-réseau et à la carte réseau et tout le trafic sortant est autorisé

#### Règles effectives de trafic entrant

- 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. Si un NSG a un sous-réseau ou une carte réseau, les règles du sous-réseau ou de la carte réseau peuvent remplacer les règles de sécurité Azure par défaut.
- Les règles de trafic entrant NSG d'un sous-réseau de machine virtuelle sont prioritaires sur les règles de trafic entrant NSG d'une carte réseau de la même machine virtuelle.

#### Règles effectives de trafic sortant

- Quand un NSG est créé, Azure crée la règle de sécurité par défaut **AllowInternetOutbound** pour le groupe. Le comportement par défaut autorise tout le trafic sortant vers Internet. Si un NSG a un sous-réseau ou une carte réseau, les règles du sous-réseau ou de la carte réseau peuvent

remplacer les règles de sécurité Azure par défaut.

- Les règles de trafic sortant NSG d'une carte réseau de machine virtuelle sont prioritaires sur les règles de trafic sortant NSG d'un sous-réseau de la même machine virtuelle.

Pour qu'une règle de sécurité particulière soit toujours traitée, attribuez-lui la valeur de priorité la plus basse possible. La bonne pratique est de laisser des « trous » dans la numérotation de vos priorités, par exemple, 100, 200, 300, etc. Les trous dans la numérotation vous permettent d'ajouter de nouvelles règles sans avoir à modifier les règles existantes.

## Créer des règles pour le groupe de sécurité réseau

Source ⓘ

N'importe lequel

Plages de ports sources ⓘ

\*

Destination ⓘ

N'importe laquelle

Service ⓘ

Personnalisée

Plages de ports de destination ⓘ

8080

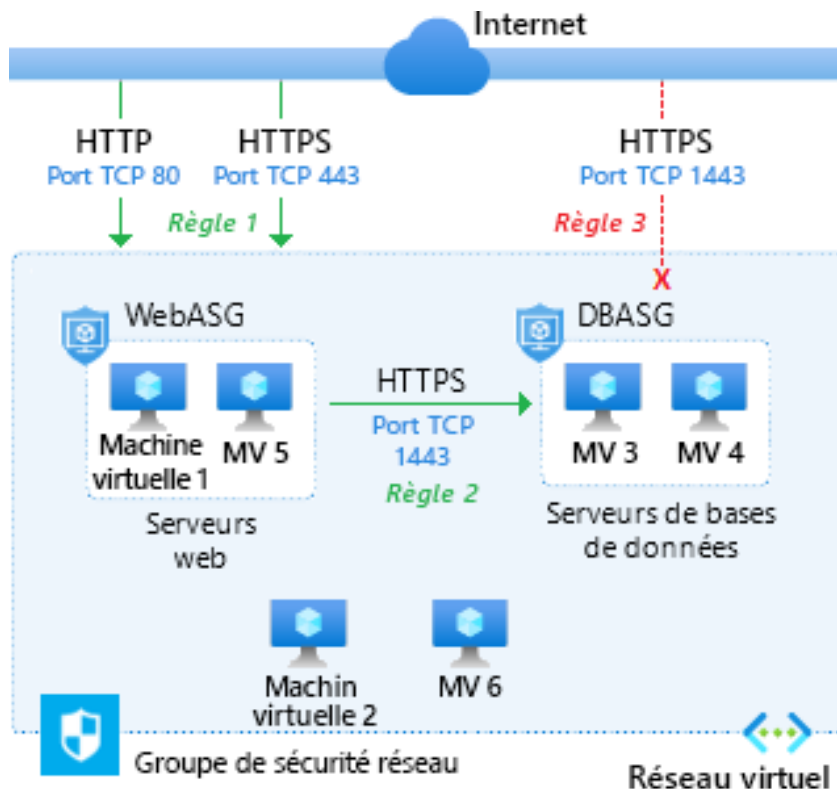
- **Source** : identifie comment la règle de sécurité contrôle le trafic **entrant**. La valeur spécifie une plage d'adresses IP source spécifique autorisée ou refusée. Le filtre de la source peut être n'importe quelle ressource, une plage d'adresses IP, un groupe de sécurité d'application ou une étiquette 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.

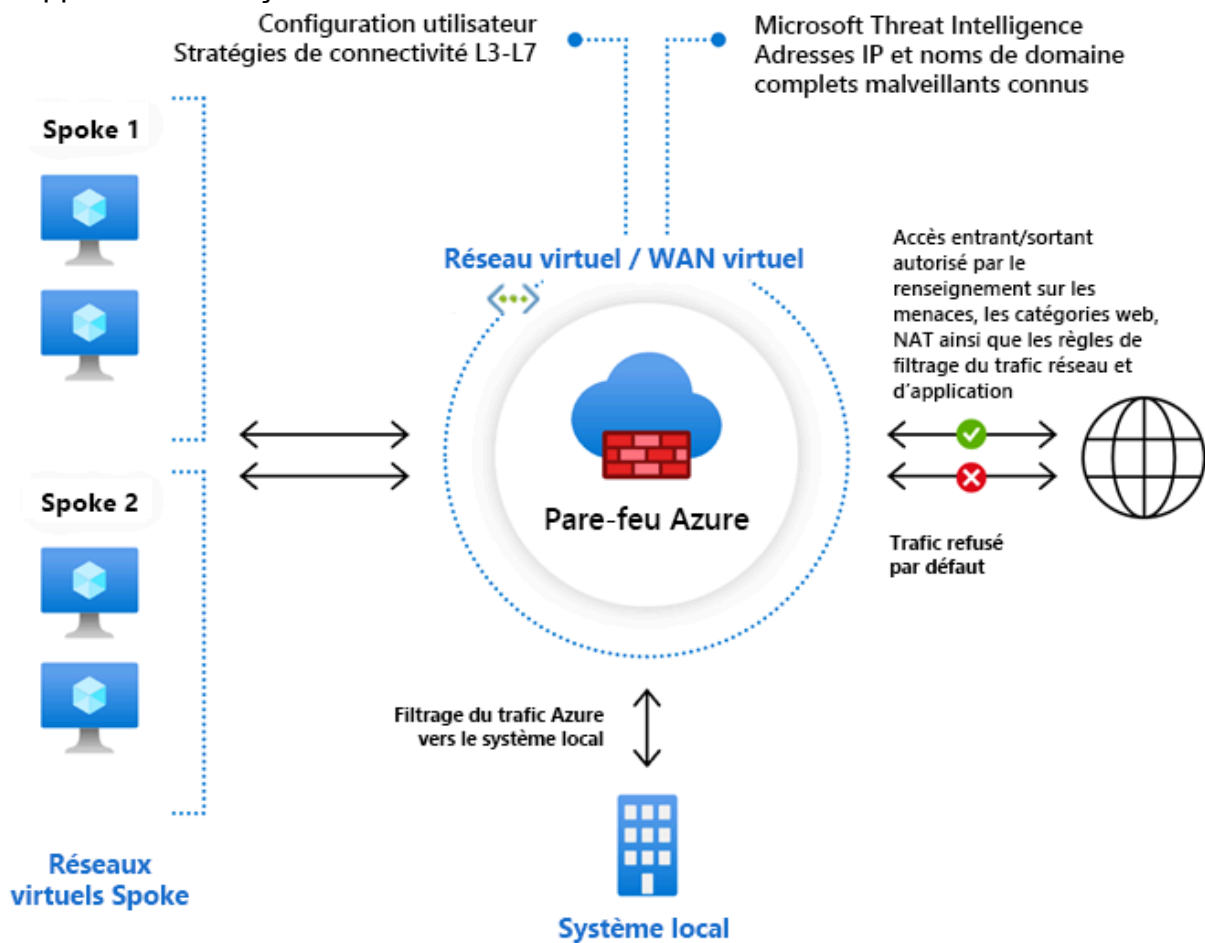


## Configurer le Pare-feu Azure

### 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
<b>Adresse IP publique</b>	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.  <b>Remarque</b> : vous pouvez associer plusieurs adresses IP publiques à votre pare-feu.
<b>Haute disponibilité intégrée</b>	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.

<b>Zones de disponibilité</b>	Configurez Pare-feu Azure pendant le déploiement pour qu'il couvre plusieurs zones de disponibilité afin d'augmenter la disponibilité.
<b>Extensibilité du cloud sans limites</b>	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.
<b>Règles de filtrage des noms de domaine complets de l'application</b>	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.
<b>Règles de filtrage du trafic réseau</b>	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.
<b>Renseignement sur les menaces</b>	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.
<b>Intégration d'Azure Monitor</b>	Le Pare-feu Azure est totalement intégré à Azure Monitor pour la journalisation et les analyses.

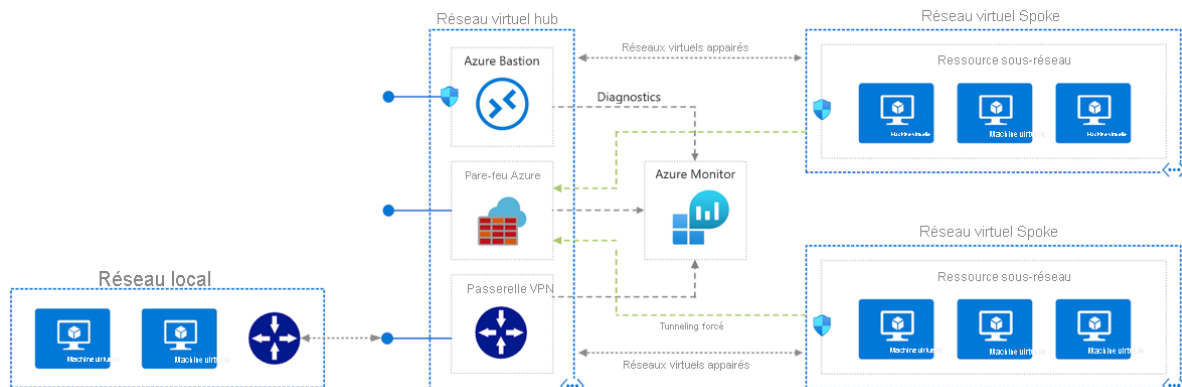
## Créer une implémentation Pare-feu Azure

Quand vous déployez un pare-feu, l'approche recommandée consiste à implémenter une topologie de réseau **hub-and-spoke**.

Le **hub** est un réseau virtuel d'Azure qui centralise la connectivité à votre réseau local.

Les **spokes** sont des réseaux virtuels appairés avec le hub et qui peuvent être utilisés pour isoler les charges de travail.

Le trafic circule entre un centre de données local et le réseau hub via une connexion Azure, comme Azure ExpressRoute, la passerelle VPN Azure ou Azure Bastion.



## Créer des règles Pare-feu Azure

**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 publics 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.**

Paramètres de configuration d'une règle NAT :

- **Nom** : fournissez une étiquette pour la règle.
- **Protocole** : choisissez le protocole TCP ou UDP.
- **Adresse source** : identifiez l'adresse comme \* (Internet), une adresse Internet spécifique ou un bloc CIDR (Classless Inter-Domain Routing).
- **Adresse de destination** : spécifiez l'adresse externe du pare-feu pour la règle à inspecter.
- **Ports de destination** : fournissez les ports TCP ou UDP que la règle écoute sur l'adresse IP externe du pare-feu.
- **Adresse traduite** : spécifiez l'adresse IP du service (machine virtuelle, équilibreur de charge interne, etc.) qui héberge ou présente le service en privé.
- **Port traduit** : identifiez le port vers lequel le trafic entrant est acheminé par Pare-feu Azure.

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.

Voici les paramètres de configuration d'une règle de réseau :

- **Nom** : fournissez un intitulé convivial pour la règle.
- **Protocole** : choisissez le protocole pour la règle, par exemple TCP, UDP, ICMP (ping et traceroute) ou celui de votre choix.
- **Adresse source** : identifiez l'adresse ou le bloc CIDR de la source.
- **Adresses de destination** : spécifiez les adresses ou blocs CIDR de la ou des destinations.
- **Ports de destination** : fournissez le port de destination du trafic.

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.

Voici les paramètres de configuration d'une règle d'application :

- **Nom** : fournissez un intitulé convivial pour la règle.

- **Adresses sources** : identifiez l'adresse IP de la source.
- **Protocole** : **port** : spécifiez **HTTP** ou **HTTPS**, ainsi que le port sur lequel le serveur web écoute.
- **Noms de domaine complets cibles** : fournissez le nom de domaine du service, comme **www.contoso.com**. Des caractères génériques (\*) peuvent être utilisés. Une étiquette FQDN représente un groupe de noms FQDN associés à des services Microsoft bien connus. Les étiquettes de nom de domaine complet peuvent être par exemple **Windows Update**, **App Service Environment** et **Azure Backup**.

## 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.

- Le nom de domaine initial ne peut pas être modifié ou supprimé, mais vous pouvez ajouter un nom de domaine personnalisé routable que vous contrôlez.
- 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, comme illustré dans l'image suivante :

Accueil > Fabrikam - Noms de domaine personnalisés > contoso.com

**contoso.com** ×  
Nom de domaine personnalisé

 Supprimer

 Pour utiliser contoso.com avec votre compte Azure AD, créez un enregistrement TXT auprès de votre bureau d'enregistrement de noms de domaine selon les informations ci-dessous.

TYPE D'ENREGISTREMENT	<input checked="" type="radio"/> TXT <input type="radio"/> MX
ALIAS OU NOM D'HÔTE	<input type="text" value="@"/> 
ADRESSE DE DESTINATION OU...	<input type="text" value="MS=ms64983159"/> 
TTL	<input type="text" value="3600"/> 

[Partager ces paramètres par e-mail](#)

Vérifier le domaine

La vérification ne réussira pas tant que vous n'aurez pas configuré votre domaine avec votre bureau d'enregistrement comme décrit ci-dessus.

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

Azure DNS fournit un service DNS fiable et sécurisé pour gérer et résoudre les noms de domaine dans un réseau virtuel, sans qu'il soit nécessaire d'ajouter une solution DNS personnalisée.

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.

contosotest.com  
Zone DNS

Rechercher (Ctrl+F)

Vue d'ensemble

Journal d'activité

Contrôle d'accès (IAM)

Balises

Diagnostiquer et résoudre les problèmes

Paramètres

Propriétés

Vous

Jeu d'enregistrements Zone enfant Déplacer

Essentials

Groupe de ressources (modifier)  
**azurednsrg**

Abonnement (modifier)  
Abonnement Azure

Identifiant d'abonnement

Étiquettes (changer)  
Cliquer ici pour ajouter des balises

Serveur de noms 1  
**ns1-04.azure-dns.com.**

Serveur de noms 2  
**ns2-04.azure-dns.net.**

Serveur de noms 3  
**ns3-04.azure-dns.org.**

Serveur de noms 4  
**ns4-04.azure-dns.info.**

## 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.

Chaque bureau d'enregistrement a ses propres outils de gestion DNS pour gérer les enregistrements de serveur de noms DNS pour un domaine. Le terme *bureau d'enregistrement* fait référence au bureau d'enregistrement de domaines de tiers, qui est la société où vous avez inscrit votre domaine.

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.

## Éléments à prendre en compte lors de l'utilisation d'enregistrements NS

Plusieurs considérations importantes sont à prendre en compte lors de l'utilisation d'enregistrements **NS** et de serveurs de noms pour une zone DNS.

- Quand vous copiez un enregistrement **NS** (une adresse de serveur de noms DNS), veillez à inclure le point final ( . ) à la fin de l'adresse. Le point final indique la fin d'un nom de domaine complet, comme **ns1-02.azure-dns.com.** et **ns3-02.azure-dns.org..**

- Pour déléguer votre domaine à Azure DNS, vous devez utiliser les noms exacts des serveurs de noms DNS tels qu'ils ont été créés par Azure DNS.
- Nous vous recommandons de toujours copier **tous** les enregistrements **NS** des serveurs de noms DNS de votre domaine dans le domaine parent, quel que soit le nom de domaine réel. Dans notre exemple de scénario, supposons que nous n'attendons pas de trafic sur le serveur de noms DNS `ns4-02.azure-dns.info`. Bien que nous ne prévoyons pas de trafic sur cette adresse de serveur de noms DNS, la bonne pratique est de copier aussi cet enregistrement **NS** dans le domaine parent auprès du bureau d'enregistrement avec les autres adresses de serveur de noms.

### Comment déléguer des sous-domaines

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).

### Notes

Les zones DNS parent et enfant peuvent être dans le même groupe de ressources ou dans des groupes de ressources différents.

### Ajouter des jeux d'enregistrements DNS

Un jeu d'enregistrements DNS (également appelé *jeu d'enregistrements de ressource*) est une collection d'enregistrements dans une zone DNS.

Accueil > Zones DNS privées >

## Zones DNS privées

Microsoft

+ Créer ⚙️ Gérer la vue ...

Filtrer sur n'importe quel champ...

Nom

privatelink.servicebus.windows.net

### Ajouter un jeu d'enregistrements

privatelink.servicebus.windows.net

Nom

.privatelink.servicebus.windows.net

Type

A – Enregistrement d'adresse

TTL \* Unité de durée de vie

1 Heures

Adresse IP

### 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.

Prenons l'exemple suivant, où nous avons deux enregistrements dans un jeu d'enregistrements. Tous les enregistrements ont le même nom, [www.contoso.com](http://www.contoso.com). Tous les enregistrements ont le même type d'enregistrement, **A**. Chaque enregistrement du jeu a une valeur différente. Dans le cas présent, chaque enregistrement fournit une adresse IP différente.

- 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
<b>Aucune solution DNS personnalisée n'est nécessaire</b>	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.
<b>Prise en charge des types d'enregistrements DNS courants</b>	Le DNS privé Azure prend en charge tous les types d'enregistrements DNS courants, y compris <b>A</b> , <b>AAAA</b> , <b>CNAME</b> , <b>MX</b> , <b>PTR</b> , <b>SOA</b> , <b>SRV</b> et <b>TXT</b> .
<b>Gestion automatique des enregistrements de nom d'hôte</b>	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.
<b>Résolution des noms d'hôte entre des réseaux virtuels</b>	Contrairement aux noms d'hôte 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.

Passer en revue les scénarios avec des zones DNS privées Azure

<https://learn.microsoft.com/fr-fr/training/modules/configure-azure-dns/8-determine-private-zone-scenarios>

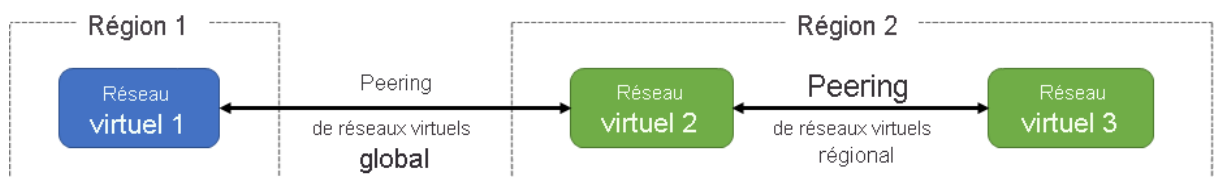
## Configurer un peering de réseaux virtuels Azure

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.

Éléments à prendre en considération lors de l'utilisation de l'appairage de réseaux virtuels Azure

Avantage	Description
<b>Connexions réseau privées</b>	Lorsque vous implémentez l'appairage de réseaux virtuels Azure, le trafic réseau entre les réseaux virtuels appairés est privé. Le trafic entre les réseaux virtuels reste sur le réseau principal de Microsoft Azure. Aucun chiffrement et aucune connexion Internet publique, ni passerelle ne sont nécessaires pour que les réseaux virtuels communiquent.
<b>Performances élevées</b>	Comme l'appairage de réseaux virtuels Azure utilise l'infrastructure Azure, vous bénéficiez d'une connexion à faible latence et à bande passante élevée entre les ressources de différents réseaux virtuels.
<b>Communication simplifiée</b>	L'appairage de réseaux virtuels Azure permet aux ressources d'un réseau virtuel de communiquer avec les ressources d'un autre réseau virtuel, une fois que les réseaux virtuels sont homologués.

<b>Transfert de données transparent</b>	Vous pouvez créer une configuration d'appairage de réseaux virtuels Azure pour transférer des données entre des abonnements Azure, des modèles de déploiement et des régions Azure.
<b>Aucune interruption des ressources</b>	L'appairage de réseaux virtuels Azure ne nécessite aucun temps d'arrêt des ressources du réseau virtuel pendant ou après la création de l'appairage.

## 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.

## Créer le peering de réseaux virtuels

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

Il existe quelques points à prendre en compte avant de créer l'appairage dans le portail Azure.

- 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

1. 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.
2. Choisissez le premier réseau virtuel à utiliser dans l'appairage, puis sélectionnez **Paramètres>Ajouter** (appairage).
3. 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.

[Accueil](#) > [Réseaux virtuels](#) > [Peerings](#) >

## Ajouter un peering ...

Ce réseau virtuel

Nom du lien de peering \*

Trafic vers le réseau virtuel distant ⓘ

- Autoriser (par défaut)
- Bloquer tout le trafic vers le réseau virtuel distant

Trafic transféré à partir du réseau virtuel distant ⓘ

- Autoriser (par défaut)
- Bloquer le trafic provenant de l'extérieur du réseau virtuel distant

Passerelle de réseau virtuel ou Serveur de routes ⓘ

- Utiliser la passerelle de ce réseau virtuel ou le Serveur de routes
- Utiliser la passerelle du réseau virtuel distant ou le Serveur de routes
- Aucun (par défaut)

- **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.

Créez au moins une machine virtuelle dans chaque réseau virtuel.

Testez la communication entre les machines virtuelles au sein de votre réseau appairé.

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.

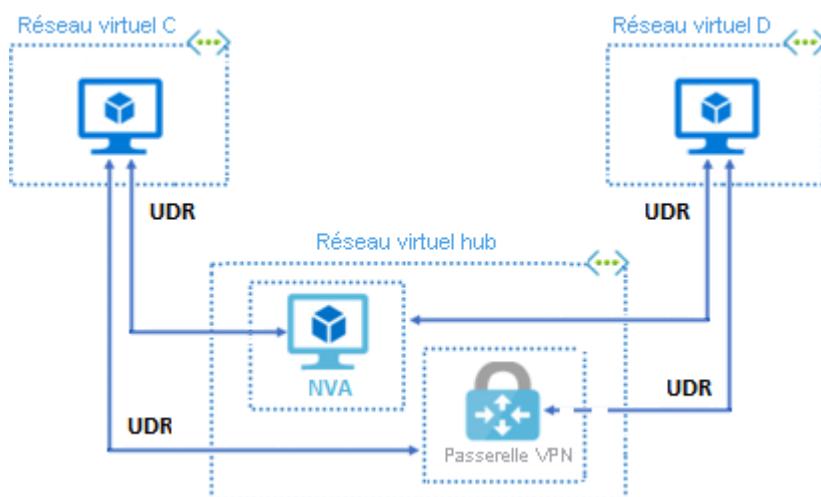
- Quand vous créez l'appairage initial vers le deuxième réseau virtuel (distant) à partir du premier réseau virtuel, l'état de l'appairage pour le premier réseau virtuel indique **Initié**.
- Lorsque vous créez l'appairage suivant *du* deuxième réseau virtuel vers le premier réseau virtuel, l'état de 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.



Il existe plusieurs façons d'étendre les fonctionnalités de votre appairage pour les ressources et les réseaux virtuels en dehors de votre réseau d'appairage :

---

Mécanisme	Description
<b>Réseau hub-and-spoke</b>	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.
<b>Itinéraire défini par l'utilisateur (UDR)</b>	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.
<b>Chaînage de services</b>	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.

## Configurer une passerelle VPN Azure

### 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.

Éléments à prendre en compte lors de l'utilisation de passerelles VPN

### Configuration

### Scénarios

#### Site à site (S2S)

- Connecter vos centres de données locaux à vos réseaux virtuels Azure via un tunnel VPN IPsec/IKE (IKEv1 ou IKEv2)
- Prendre en charge des configurations intersites et hybrides
- Configurer le VPN S2S et Azure ExpressRoute pour le même réseau virtuel
- Configurer le VPN S2S en tant que chemin de basculement sécurisé pour ExpressRoute
- Utiliser des VPN S2S pour se connecter à des sites en dehors de votre réseau qui sont connectés via ExpressRoute

#### Point à site (P2S ou VPN utilisateur)

- Connecter des appareils individuels à vos réseaux virtuels Azure
- Créer une connexion sécurisée à votre réseau virtuel à partir d'un ordinateur client individuel
- Utile pour les travailleurs distants ou itinérants qui veulent se connecter à des réseaux virtuels Azure depuis leur emplacement actuel
- Prendre en charge quelques clients qui doivent se connecter à un réseau virtuel

## Réseau virtuel à réseau virtuel

(Réseau virtuel à réseau virtuel)

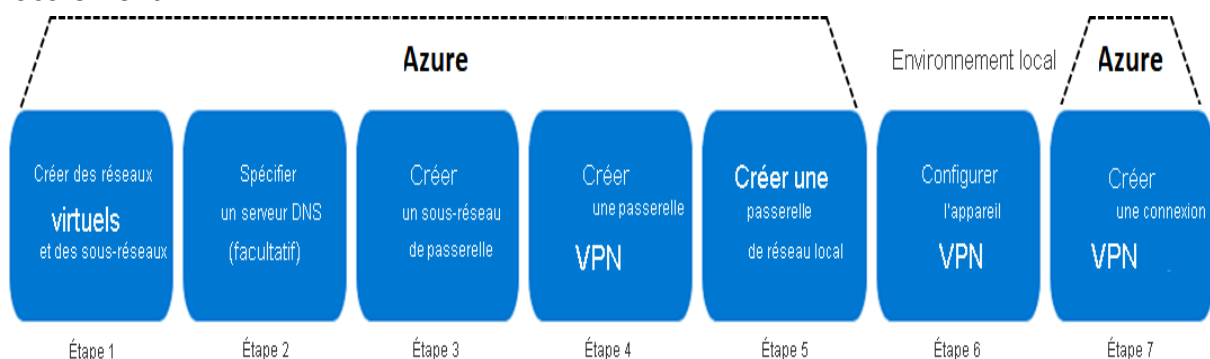
- Connecter un réseau virtuel à un autre réseau virtuel via un tunnel VPN IPsec/IKE
- Créer un réseau qui intègre la connectivité intersite à la connectivité réseau entre réseaux virtuels en combinant la communication de réseau virtuel à réseau virtuel avec des configurations de connexion multisites
- Connecter des réseaux virtuels dans la même région ou dans des régions différentes
- Connecter des réseaux virtuels dans le même abonnement ou dans des abonnements différents
- Connecter des réseaux virtuels qui ont le même modèle de déploiement ou des modèles de déploiement différents

## Hautement disponible

- Prendre en charge la haute disponibilité pour les connexions intersites et de réseau virtuel à réseau virtuel
- Implémenter la haute disponibilité pour plusieurs appareils VPN locaux
- Implémenter la haute disponibilité pour une passerelle VPN Azure active-active
- Implémenter la haute disponibilité pour une combinaison de plusieurs appareils VPN locaux et d'une passerelle VPN Azure active-active

## 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.

## Créer le sous-réseau de passerelle

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.

## Créer la passerelle VPN

Éléments à considérer lors de la création d'une passerelle VPN

### Détails du projet

- **Abonnement** : utilisez le menu déroulant pour sélectionner l'abonnement à utiliser pour la création de la ressource de passerelle de réseau virtuel.
- **Groupe de ressources** : utilisez le menu déroulant pour sélectionner le groupe de ressources de la ressource de passerelle de réseau virtuel.

### Détails de l'instance

- **Nom** : spécifiez un nom pour identifier votre passerelle VPN.
- **Région** : utilisez le menu déroulant pour sélectionner l'emplacement de la région (et l'abonnement) Azure pour la passerelle VPN. L'emplacement est l'endroit où vont se trouver les ressources que vous déployez sur cette passerelle de réseau virtuel.
- **Type de passerelle** : sélectionnez le type de passerelle à créer, **VPN** (passerelle VPN Azure) ou **ExpressRoute** (Azure ExpressRoute).
- **Type de VPN** : sélectionnez le type de VPN à créer, **Basé sur des routes** ou **Basé sur des stratégies**. Le type de VPN que vous choisissez dépend de la marque et du modèle de votre appareil VPN ainsi que du type de connexion VPN que vous envisagez de créer. Dans l'unité suivante, nous examinons en détail les options pour les valeurs de ce paramètre.
  - Les passerelles VPN basées sur des routes sont les plus courantes. Les scénarios classiques incluent les connexions de point à site, entre réseaux virtuels ou de site à site multiples. Sélectionnez « Basé sur

des routes » quand votre réseau virtuel coexiste avec une passerelle Azure ExpressRoute ou si vous devez utiliser le protocole IKEv2.

- Les passerelles VPN basées sur des stratégies prennent en charge seulement le protocole IKEv1.
- **Référence SKU** : utilisez le menu déroulant pour sélectionner une référence SKU de passerelle. Passez en revue les options de référence SKU dans l'unité [Déterminer la référence SKU et la génération de la passerelle](#).

Votre choix affecte le nombre de tunnels que vous pouvez avoir et le point de référence du débit agrégé. La valeur de référence est basée sur les mesures de plusieurs tunnels agrégés via une même passerelle. Le débit n'est pas garanti en raison des conditions de trafic Internet et du comportement de votre application.

- **Génération** : utilisez le menu déroulant pour sélectionner la génération de passerelle, **Génération1** ou **Génération2**. Génération2 offre des performances et un contrat SLA améliorés pour le même prix que Génération1.
  - Génération1 prend en charge les références SKU De base et VpnGw1 ainsi que la plupart des autres références SKU prises en charge dans Génération2.
  - Génération2 prend en charge la plupart des références SKU disponibles dans Génération1 ainsi que VpnGw4 et VpnGw5.
- **Réseau virtuel** : utilisez le menu déroulant pour sélectionner un réseau virtuel existant pour la passerelle VPN, ou sélectionnez **Créer un réseau virtuel** pour configurer un nouveau réseau virtuel. Gardez à l'esprit qu'un réseau virtuel ne peut pas être associé à plusieurs passerelles. Le réseau virtuel envoie et reçoit le trafic via la passerelle VPN.

## Adresse IP

Dans le portail Azure, vous pouvez voir l'adresse IP affectée à la passerelle VPN. Votre passerelle doit normalement apparaître en tant qu'appareil connecté.

## Déterminer le type de passerelle VPN

Le type de VPN que vous choisissez dépend de la topologie de connexion que vous voulez créer. Pour créer une **connexion de point à site (P2S)**, vous devez créer un **VPN basé sur des routes**. Le **type de VPN peut également dépendre de votre matériel**. Pour une **configuration de site à site (S2S)**, vous avez besoin d'un **appareil VPN**. Certains périphériques VPN ne prennent en charge qu'un certain type de 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.

## Génération1

SKU	Tunnels	Connexions	Référence
VpnGw1/Az	Bande passante 30	Bande passante 250	650 Mbits/s
VpnGw2/Az	Bande passante 30	Bande passante 500	< 1,0 Gbits/s
VPNGw3/Az	Bande passante 30	Bande passante 1 000	1,25 Gbits/s

## Génération2

SKU	Tunnels	Connexions	Référence
VpnGw2/Az	Bande passante 30	Bande passante 500	1,25 Gbits/s
VPNGw3/Az	Bande passante 30	Bande passante 1 000	2,5 Gbits/s
VPNGw4/Az	Bande passante 100	Bande passante 5 000	< 5,0 Gbits/s
VPNGw5/Az	Bande passante 100	Bande passante 10000	10,0 Gbits/s

## 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.

## Configurer l'appareil VPN local

Une liste validée d'appareils VPN standard qui fonctionnent bien avec la passerelle VPN est disponible pour les développeurs. La liste a été créée en partenariat avec des fabricants d'appareils comme Cisco, Juniper, Ubiquiti et Barracuda Networks.

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.

## Créer la connexion VPN

- **Nom** : entrez un nom pour votre connexion VPN.
- **Type de connexion** : utilisez le menu déroulant pour sélectionner une connexion de site à site (IPsec).
- **Passerelle de réseau virtuel** : la valeur de ce paramètre est fournie par Azure. La valeur est définie sur la passerelle de réseau virtuel pour laquelle vous établissez la connexion VPN.
- **Passerelle de réseau local** : définissez cette valeur sur la passerelle de réseau local que vous avez créée à l'étape 5 du processus de connexion de site à site.
- **Clé partagée (PSK)**. Spécifiez une clé partagée à utiliser pour votre connexion. Vous pouvez générer ou créer vous-même la clé partagée. Pour établir une connexion de site à site, vous avez besoin d'une clé partagée, qui

est la même que celle que vous utilisez pour votre appareil VPN local et votre connexion de passerelle de réseau virtuel.

## 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.

Ce qu'il faut savoir pour utiliser Azure ExpressRoute

#### **Avantage**

#### **Description**

#### **Scénarios**

**Bénéficiaire de connexions rapides, fiables et privées**

Les connexions Azure ExpressRoute ne passant pas par l'Internet public, elles offrent une plus grande fiabilité, des débits plus importants et des latences moindres par rapport aux connexions Internet classiques. Dans certains cas, les connexions ExpressRoute qui transfèrent des données entre des systèmes locaux et Azure peuvent dégager des économies significatives.

*Créer des connexions privées entre les centres de données Azure et l'infrastructure pour vos ressources locales ou dans un environnement de colocation*

*Établir des connexions à Azure au niveau d'un emplacement ExpressRoute, par exemple l'installation d'un fournisseur d'échange*

*Se connecter directement à Azure à partir d'un réseau WAN existant, comme un VPN MPLS (Multiprotocol Label Switching) fourni par un fournisseur de services réseau*

**Accéder à un cloud privé virtuel pour le stockage, la sauvegarde et la récupération**

Azure ExpressRoute vous offre une connexion rapide et fiable à Azure avec des bandes passantes allant jusqu'à 100 Gbits/s. Les vitesses de connexion élevées en font une excellente option pour les scénarios qui nécessitent l'intégrité et la disponibilité des données. ExpressRoute est une option rentable pour transférer de grandes quantités de données.

*Prendre en charge la migration périodique des données, la reprise d'activité après sinistre et la réplication pour la continuité d'activité*

*Transférer de grandes quantités de données comme des jeux de données pour des applications de calcul hautes performances*

*Déplacer des machines virtuelles volumineuses entre vos environnements de développement et de test*

**Étendre et connecter vos centres de données**

Azure ExpressRoute offre un débit élevé et de faibles latences. Une implémentation ExpressRoute fonctionne comme une extension naturelle vers ou entre vos centres de données.

*Se connecter et ajouter de la capacité de calcul et de stockage à vos centres de données existants*

*Profiter de l'échelle et de l'économie du cloud public sans avoir à faire de compromis sur les performances du réseau*

## **Créer des applications hybrides**

Azure ExpressRoute fournit les fonctionnalités qui vous permettent de créer des applications couvrant l'infrastructure locale et Azure sans compromettre la confidentialité ou les performances.

*Exécuter une application intranet d'entreprise dans Azure qui authentifie vos clients auprès d'un service Azure Active Directory local*

*Desservir tous vos clients d'entreprise sans que le trafic ne passe jamais par l'Internet public*

## Déterminer les fonctionnalités d'Azure ExpressRoute

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.

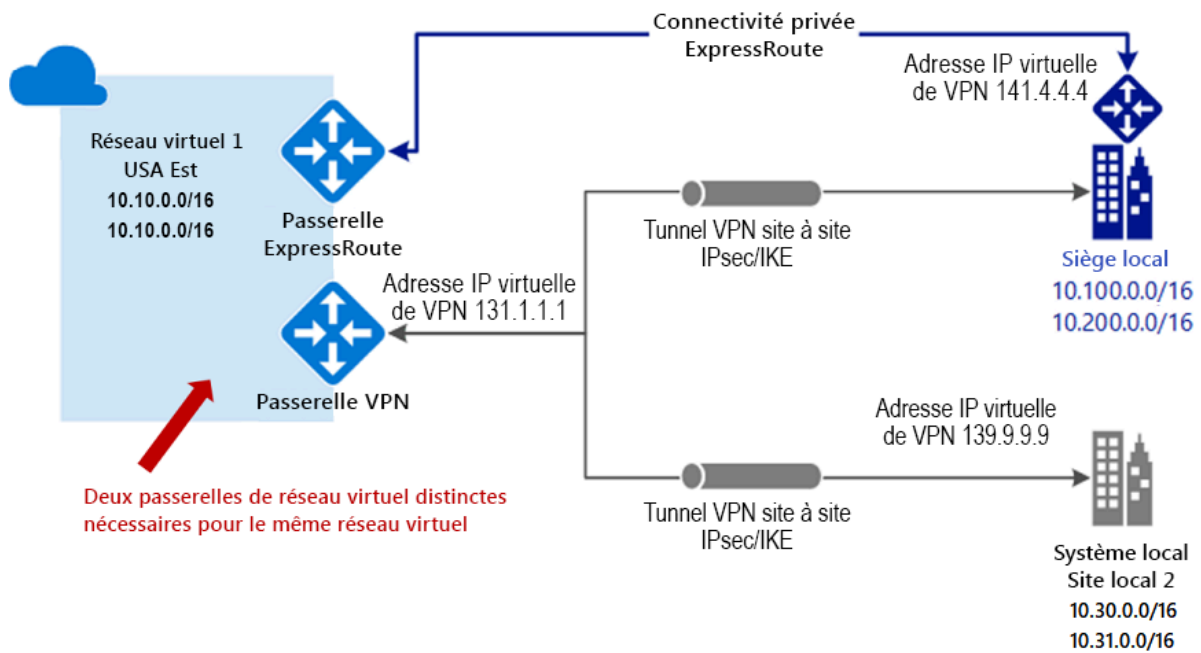
- Vous pouvez acheter des circuits ExpressRoute pour un large éventail de bandes passantes. Contactez votre fournisseur de connectivité pour déterminer les bandes passantes prises en charge.
- Microsoft propose plusieurs [options tarifaires](#) pour ExpressRoute.

## 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.

Vous configurez un VPN site à site comme un chemin de basculement sécurisé pour ExpressRoute. Vous pouvez également utiliser des VPN site à site pour vous connecter à des sites qui ne font pas partie de votre réseau, mais qui sont connectés par le biais d'ExpressRoute. Notez que cette configuration nécessite deux passerelles de réseau virtuel pour le même réseau virtuel. Un réseau utilise le type de passerelle *VPN*, tandis que l'autre utilise le type de passerelle *ExpressRoute*.





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

Modèle de connexion	Fonctionnement	Prise en charge des couches
<b>Colocalisation avec un échange cloud</b>	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.
<b>Connexions Ethernet point à point</b>	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.

## Comparer les options de connexion intersite

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. Pour améliorer la haute disponibilité, nous vous recommandons d'opérer les deux connexions d'un circuit ExpressRoute en mode actif/actif. Quand vous autorisez les connexions à opérer en mode actif/actif, le réseau Microsoft équilibre la charge du trafic sur les connexions flux par flux.

## Ce qu'il faut savoir sur les connexions intersites

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

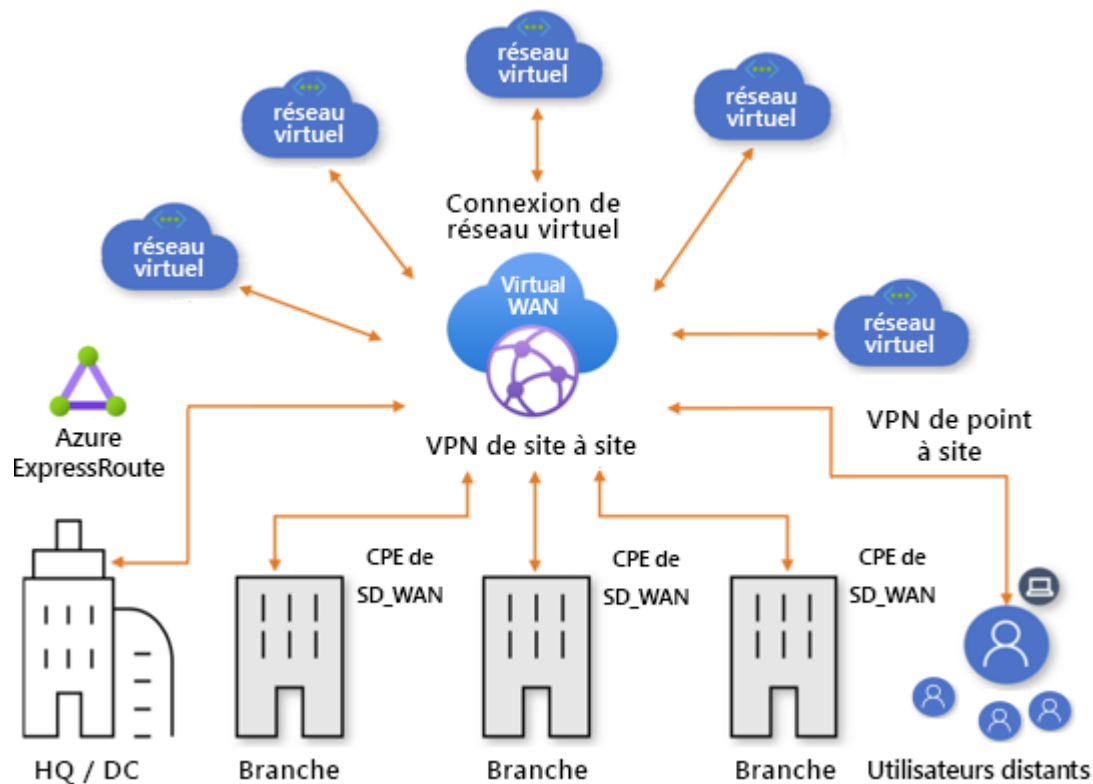
Connexion	Services Azure	Bande passante	Protocoles	Scénarios
<b>Réseau virtuel et point à site (VPN utilisateur)</b>	Services Azure IaaS, Machines virtuelles Azure	Basé sur la référence SKU de passerelle	actif / passif	<i>Environnements de développement, test et lab pour les services cloud</i>  <i>Environnements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

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

## 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.

L'illustration suivante montre les connexions intersites établies par le biais d'Azure Virtual WAN pour accéder aux réseaux virtuels Azure. Une connexion est établie à partir de l'emplacement local en utilisant Azure ExpressRoute. Plusieurs branches se connectent par le biais d'une configuration site à site, et les utilisateurs distants se connectent par le biais d'une connexion point à site (VPN utilisateur).



### 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

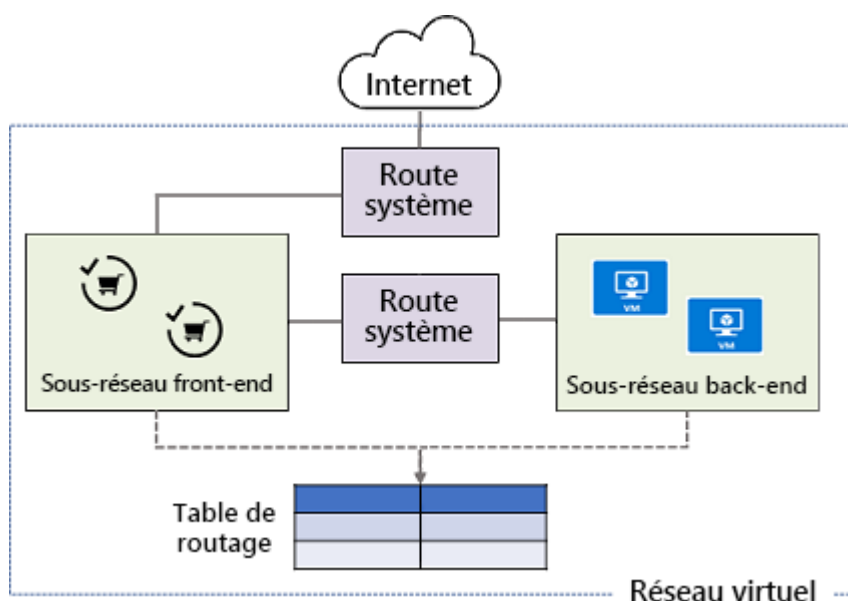
## Passer en revue les routes système

Azure utilise des *routes système* pour diriger le trafic réseau entre des machines virtuelles, des réseaux locaux et Internet. Les informations relatives aux routes système sont enregistrées dans une *table de routage*.

## 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.

## Scénario d'entreprise

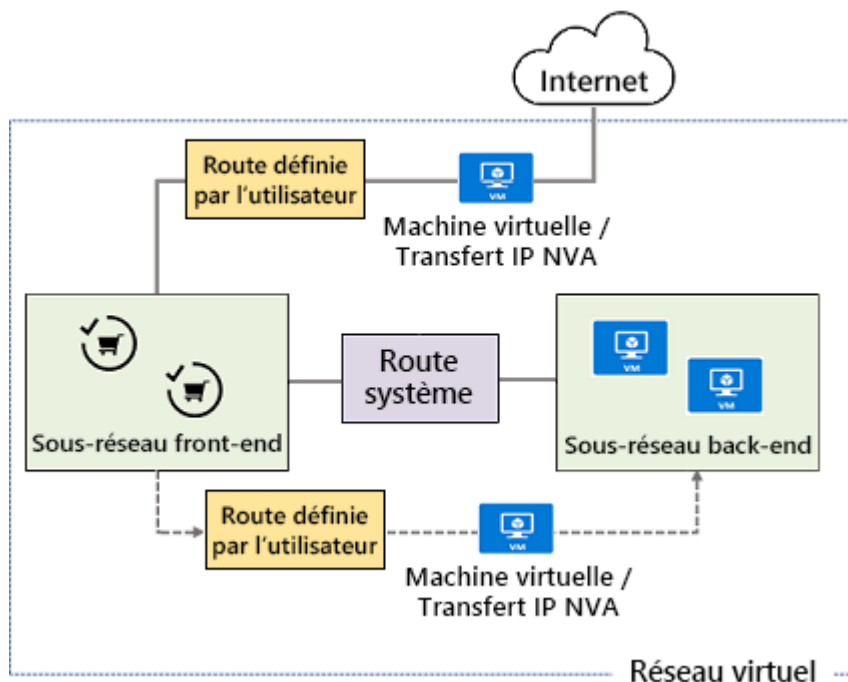


## Identifier les routes définies par l'utilisateur

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.

Scénario d'entreprise



Déterminer les utilisations des points de terminaison de service

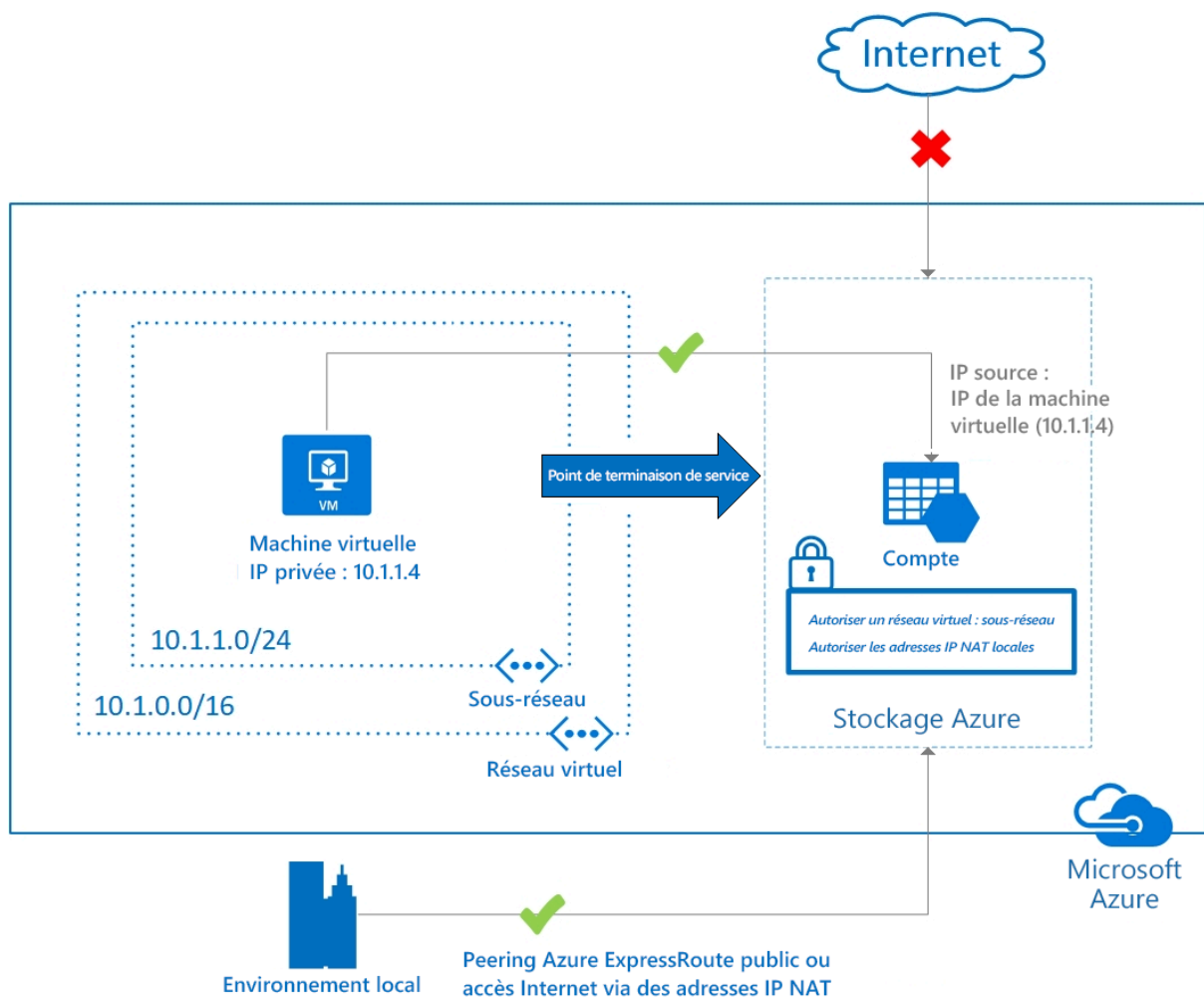
Un *point de terminaison de service* de réseau virtuel fournit l'identité de votre réseau virtuel au service Azure.

Aujourd'hui, le trafic du service Azure à partir d'un réseau virtuel utilise des adresses IP publiques en tant qu'adresses IP source. 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. Ce changement permet d'accéder aux services sans avoir besoin d'adresses IP publiques réservées, généralement utilisées dans les pare-feux IP.

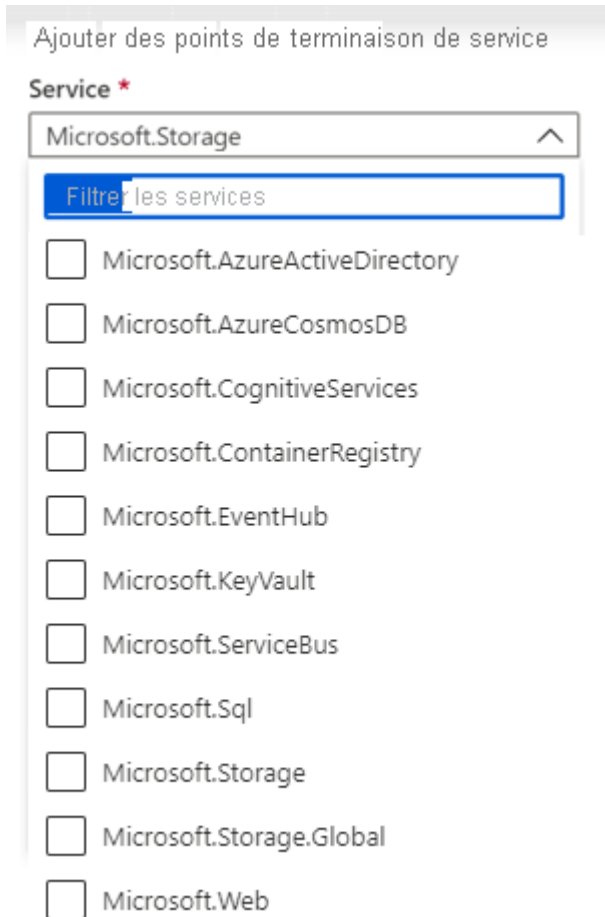
Ce que vous devez savoir sur les points de terminaison de service

- 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.



## Déterminer les services des points de terminaison de service

Il est facile d'ajouter un point de terminaison de service au réseau virtuel. Dans le portail Azure, vous sélectionnez le service Azure pour lequel créer le point de terminaison.



Service	Disponibilité	Description
<b>Stockage Azure</b>	Disponibilité générale dans toutes les régions Azure	Ce point de terminaison donne au trafic une route optimale vers le service Stockage Azure. Chaque compte de stockage prend en charge jusqu'à 100 règles de réseau virtuel.



**Azure SQL Database et Azure SQL Data Warehouse**

Disponibilité générale dans toutes les régions Azure

Une fonctionnalité de sécurité du pare-feu contrôle si votre base de données accepte la communication à partir de sous-réseaux spécifiques dans des réseaux virtuels. Cette fonctionnalité s'applique au serveur de base de données pour vos bases de données uniques et votre pool élastique dans SQL Database ou vos bases de données dans SQL Data Warehouse.

**Azure Database pour PostgreSQL et Azure Database pour MySQL**

Disponibilité générale dans les régions Azure où le service de base de données est disponible

Les règles et points de terminaison de services de réseau virtuel étendent l'espace d'adressage privé d'un réseau virtuel à vos serveurs Azure Database pour PostgreSQL et Azure Database pour MySQL.

**Azure Cosmos DB**

Disponibilité générale dans toutes les régions Azure

Vous pouvez configurer le compte Azure Cosmos DB pour autoriser l'accès uniquement à partir d'un sous-réseau spécifique d'un réseau virtuel. Autorisez les points de terminaison de service à accéder à Azure Cosmos DB sur le sous-réseau dans un réseau virtuel. Le trafic provenant du sous-réseau est envoyé à Azure Cosmos DB avec l'identité du sous-réseau et du réseau virtuel. Quand le point de terminaison de service Azure Cosmos DB est activé, vous pouvez limiter l'accès au sous-réseau en l'ajoutant à votre compte Azure Cosmos DB.

<b>Azure Key Vault</b>	Disponibilité générale dans toutes les régions Azure	Les points de terminaison de service de réseau virtuel pour Key Vault permettent de restreindre l'accès à un réseau virtuel spécifié. Les points de terminaison vous permettent également de restreindre l'accès à une liste de plages d'adresses IPv4 (Internet Protocol version 4). L'accès est refusé à tout utilisateur se connectant à votre coffre de clés en dehors de ces sources.
<b>Azure Service Bus et Azure Event Hubs</b>	Disponibilité générale dans toutes les régions Azure	L'intégration de Service Bus à des points de terminaison de service de réseau virtuel permet un accès sécurisé aux fonctionnalités de messagerie à partir de charges de travail, notamment celles de machines virtuelles liées à des réseaux virtuels. Le chemin du trafic réseau est sécurisé aux deux extrémités.

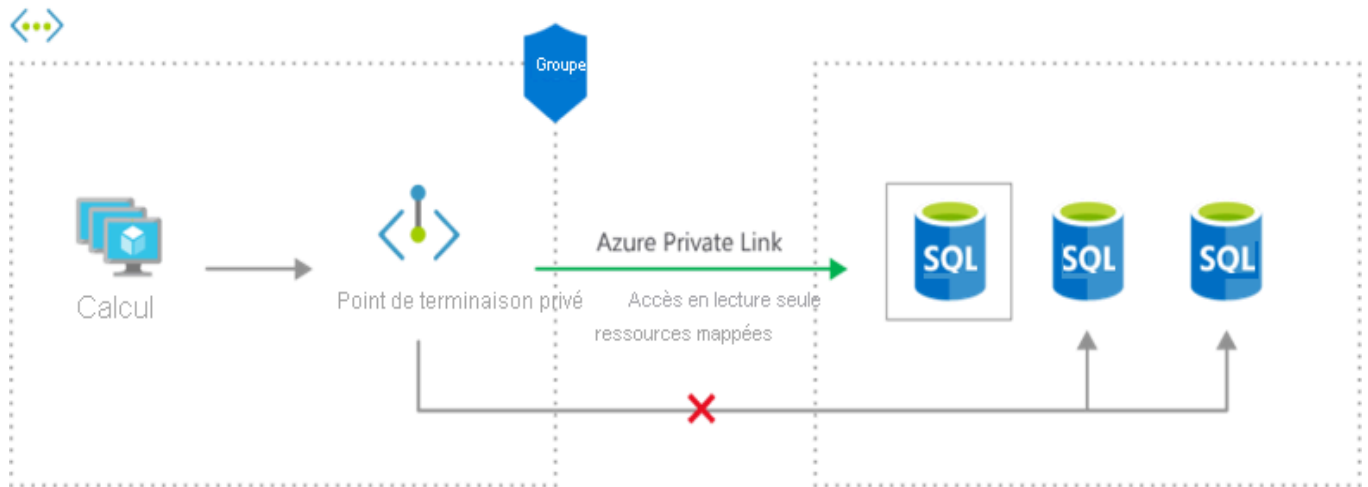
## Identifier les utilisations des liaisons privées

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

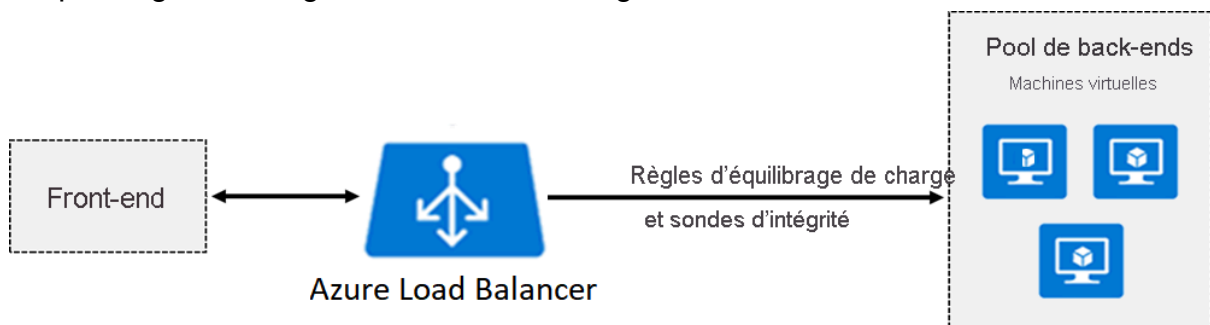
nécessaires.



## 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

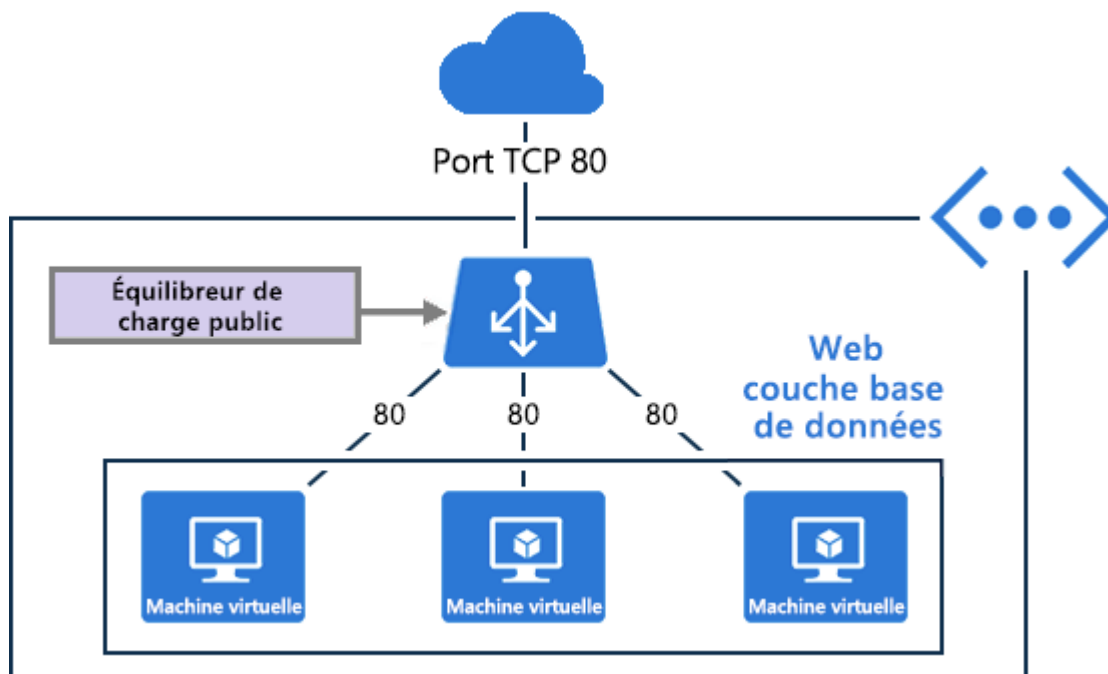
- Azure Load Balancer peut être utilisé pour les scénarios entrants et sortants.
- Vous pouvez implémenter un équilibreur de charge **public** ou **interne**, ou utiliser les deux types dans une configuration combinée.
- Pour implémenter un équilibreur de charge, vous devez configurer quatre composants :
  - 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.

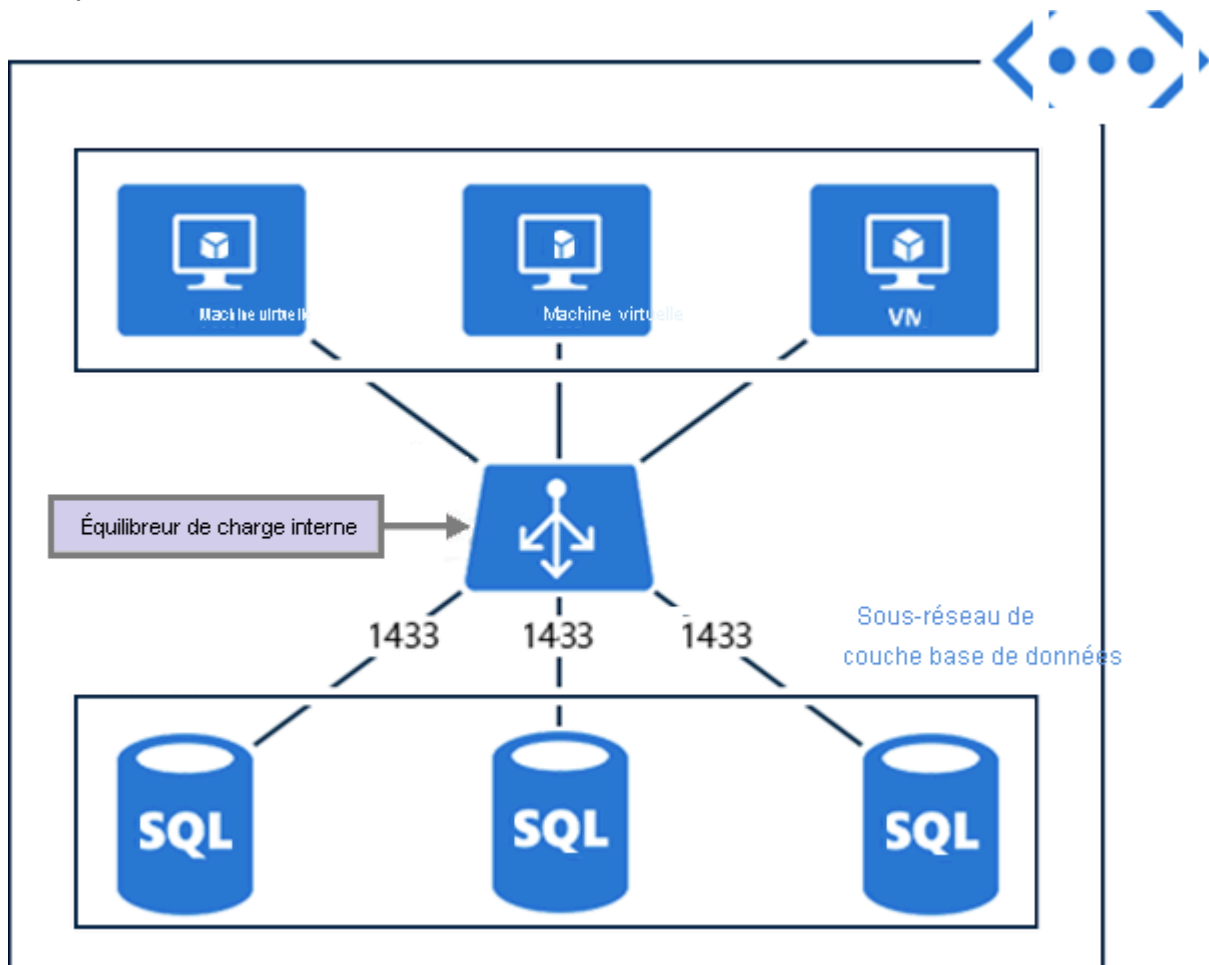
Les règles d'équilibrage de charge servent à spécifier comment distribuer des types de trafic spécifiques parmi plusieurs services ou machines virtuelles. Vous pouvez adopter cette approche pour partager la charge du trafic de requêtes web entrantes entre plusieurs serveurs web.



## 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.



## Déterminer les références SKU de l'équilibreur de charge

Lorsque vous créez un équilibreur de charge Azure dans le portail Azure, vous sélectionnez le type d'équilibreur de charge à créer (interne ou public) et la référence SKU. Azure Load Balancer prend en charge trois options de référence SKU : De base, Standard et Passerelle. Chaque référence SKU fournit des fonctionnalités, une mise à l'échelle de scénario et des tarifs différents.

### 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

<b>Fonctionnalité</b>	<b>Référence SKU De base</b>	<b>Référence SKU standard</b>
<b>Sondes d'intégrité</b>	HTTP, TCP	HTTPS, HTTP, TCP
<b>Zones de disponibilité</b>	Non disponible	Front-ends redondants interzones et zonaux pour le trafic entrant et sortant
<b>Plusieurs serveurs frontaux</b>	Entrant uniquement	Trafic entrant et sortant
<b>Sécurité</b>	<ul style="list-style-type: none"> <li>- Ouverts par défaut</li> <li>- (Facultatif) Contrôle via des groupes de sécurité réseau (NSG)</li> </ul>	<ul style="list-style-type: none"> <li>- Fermeture aux flux entrants, sauf autorisation d'un groupe NSG</li> <li>- Le trafic interne du réseau virtuel vers l'équilibreur de charge interne est autorisé</li> </ul>

#### 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.

Microsoft Azure

Accueil > LoadBalancer1

## LoadBalancer1 | Pools de back-ends ...

Équilibreur de charge

Rechercher

+ Ajouter Actualiser Envoyer des commentaires

Paramètres

- Configuration d'adresse IP front-end
- Pools de back-ends**
- Sondes d'intégrité
- Règle d'équilibrage de charge
- Règles NAT de trafic entrant
- Propriétés
- Verrous

### Ajouter un pool de back-ends ...

LoadBalancer1

Nom \*

Réseau virtuel

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 réussit. 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.

## Créer des règles d'équilibreur de charge

Vous pouvez définir des règles d'équilibrage de charge pour spécifier la façon dont le trafic est distribué à vos pools de back-ends. Chaque règle mappe une combinaison d'adresses IP et de port de front-end à un ensemble de combinaisons d'adresses IP et de ports de back-end.

## 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



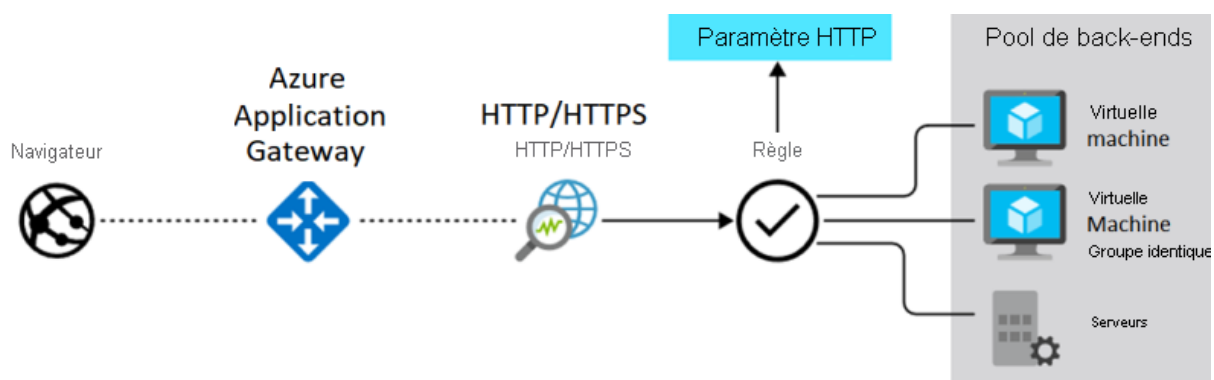
aux serveurs disponibles. Le tuple se compose de l'adresse IP source, du port source, de l'adresse IP de destination, du port de destination et du type de protocole. L'équilibreur de charge fournit l'adhérence uniquement dans une session de transport.

- La **persistance de session** 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.  
Envisagez un scénario où vous utilisez NAT à partir de l'adresse publique d'un équilibreur de charge vers le port TCP 3389 sur une machine virtuelle spécifique. En combinant votre règle NAT avec des règles d'équilibrage de charge, vous pouvez activer l'accès Bureau à distance à partir d'en dehors d'Azure.

## 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.



## Éléments à connaître concernant Azure Application Gateway

<b>Avantage</b>	<b>Description</b>
<b>Routage de la couche Application</b>	Utilisez le routage de la couche Application pour acheminer le trafic vers un pool back-end en fonction de l'URL de la demande. Le pool back-end peut comprendre des machines virtuelles Azure, Azure Virtual Machine Scale Sets, Azure App Service et même des serveurs locaux.
<b>Équilibrage de charge par tourniquet (round robin)</b>	Utilisez l'équilibrage de charge par tourniquet (round robin) pour distribuer le trafic entrant sur plusieurs serveurs. Envoyer des demandes d'équilibrage de charge aux serveurs de chaque pool back-end. Les demandes des clients sont transférées dans un cycle via un groupe de serveurs afin de créer un équilibre efficace pour la charge du serveur.
<b>Adhérence de session</b>	Appliquez l'adhérence de session à votre passerelle applicative pour vous assurer que les requêtes des clients d'une même session sont acheminées vers le même serveur principal.
<b>Protocoles pris en charge</b>	Créez une passerelle applicative pour prendre en charge les protocoles HTTP, HTTPS, HTTP/2 ou WebSocket.
<b>Protection par pare-feu</b>	Implémentez un pare-feu d'applications web pour vous protéger des vulnérabilités des applications web.
<b>Chiffrement</b>	Prise en charge du chiffrement de bout en bout des requêtes pour vos applications web.
<b>Mise à l'échelle automatique de la charge</b>	Ajustez dynamiquement la capacité selon les variations de la charge du trafic web.

## Déterminer l'acheminement Azure Application Gateway

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.

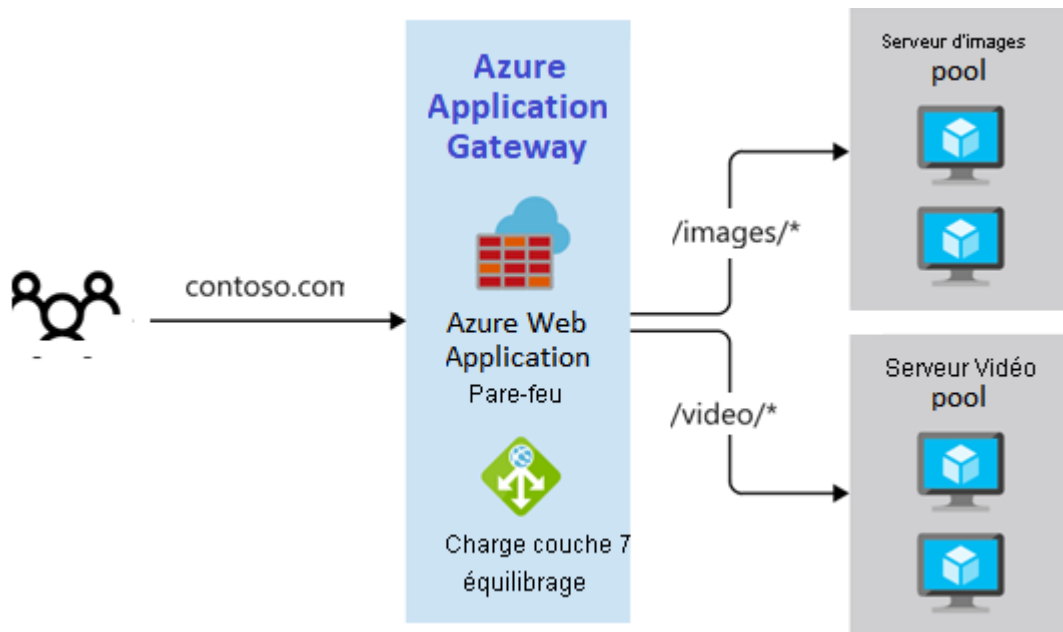
- L'acheminement **multisite** configure plusieurs applications web sur la même instance de passerelle applicative.
- Vous pouvez configurer votre passerelle applicative pour qu'elle **redirige** le trafic.

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.

### **Routage basé sur le chemin**

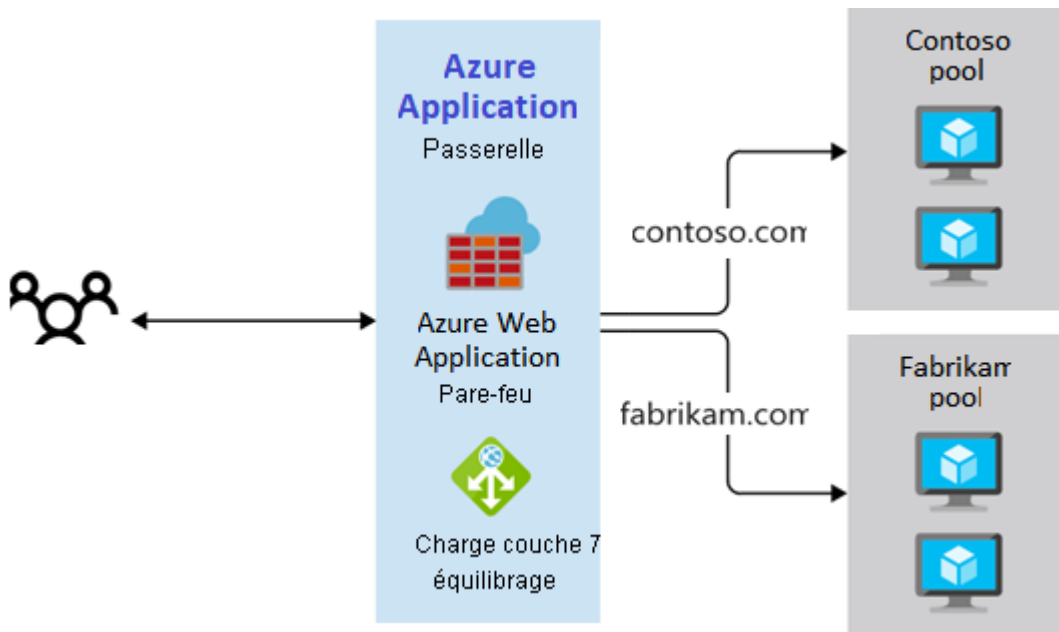
Vous pouvez implémenter l'acheminement basé sur le chemin pour diriger les requêtes de chemins d'URL spécifiques vers le pool back-end approprié. Prenons l'exemple d'un scénario où votre application web reçoit des requêtes de vidéos ou d'images. Vous pouvez utiliser l'acheminement basé sur le chemin pour diriger les requêtes portant sur le chemin `/video/*` vers un pool back-end de serveurs optimisés pour gérer le streaming vidéo. Les requêtes d'images portant sur le chemin `/images/*` peuvent être dirigées vers un pool de serveurs qui gèrent la récupération d'images. L'illustration suivante illustre cette méthode d'acheminement :



### Acheminement multisite

Lorsque vous devez prendre en charge plusieurs applications web sur la même instance de passerelle applicative, l'acheminement multisite est la meilleure option. Les configurations multisites sont utiles pour prendre en charge les applications multilocataires, où chaque locataire dispose de son propre groupe de machines virtuelles ou autres ressources hébergeant une application web.

Dans cette configuration, vous inscrivez plusieurs noms DNS (CNAME) pour l'adresse IP de votre passerelle applicative et vous spécifiez le nom de chaque site. Application Gateway utilise différents écouteurs pour attendre les requêtes de chaque site. Chaque écouteur passe la requête à une règle qui peut router la requête vers les serveurs d'un autre pool de back-ends.

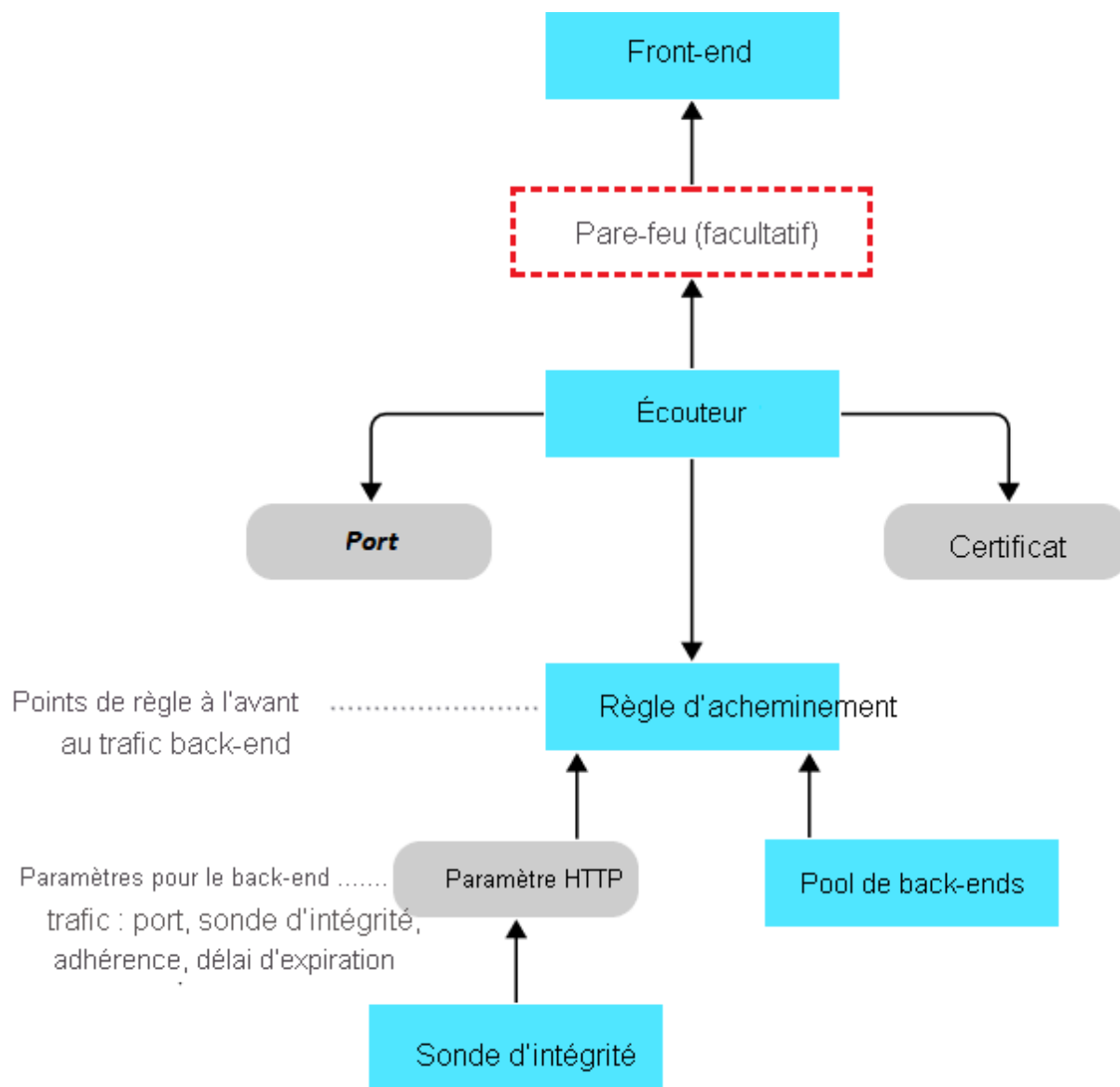


## Configurer des composants Azure Application Gateway

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.
- 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.
- **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.



### Adresse IP front-end

Les requêtes clientes sont reçues via votre adresse IP front-end. Votre passerelle applicative peut avoir une adresse IP publique ou privée, ou les deux. Vous ne pouvez avoir qu'une seule adresse IP publique et une seule adresse IP privée.

### Écouteurs

Les écouteurs acceptent le trafic arrivant sur une combinaison spécifiée de protocole, port, hôte et adresse IP. Chaque écouteur achemine les requêtes vers un pool back-end de serveurs en fonction de vos règles d'acheminement. Un écouteur peut être *de base* ou *multisite*. 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 écouteurs gèrent également les certificats TLS/SSL pour sécuriser votre application entre l'utilisateur et Application Gateway.

## **Règles de routage**

Une règle d'acheminement lie vos écouteurs aux pools back-end. Une règle spécifie comment interpréter les éléments hostname et path de l'URL d'une requête, puis comment diriger la requête vers le pool de back-ends approprié. Une règle de routage est également associée à un ensemble de paramètres HTTP. Ces paramètres HTTP indiquent si le trafic est chiffré entre Application Gateway et les serveurs de back-end (et si oui, de quelle manière). D'autres informations de configuration incluent le protocole, l'adhérence de session, le drainage de connexion, le délai d'expiration des requêtes et les sondes d'intégrité.

## **Pools de back-ends**

Un pool de back-ends référence une collection de serveurs web. Lors de la configuration du pool, vous fournissez l'adresse IP de chaque serveur web et le port sur lequel il écoute les requêtes. Chaque pool peut spécifier un ensemble fixe de machines virtuelles, de Virtual Machine Scale Sets, une application hébergée par Azure App Services ou une collection de serveurs locaux. Chaque pool de back-ends est associé à un équilibreur de charge qui répartit le travail au sein du pool.

## **Sondes d'intégrité**

Les sondes d'intégrité déterminent les serveurs dans votre pool back-end qui sont disponibles pour l'équilibrage de charge. Application Gateway utilise une sonde d'intégrité pour envoyer une requête à un serveur. Quand le serveur retourne une réponse HTTP avec un code d'état compris entre 200 et 399, le serveur est considéré comme sain. Si vous ne configurez pas de sonde d'intégrité, Application Gateway crée une sonde par défaut qui attend 30 secondes avant d'identifier un serveur comme indisponible (non sain).

## **Pare-feu (facultatif)**

Vous pouvez activer Azure Web Application Firewall pour permettre à Azure Application Gateway de gérer les requêtes entrantes avant qu'elles n'atteignent votre écouteur. Le pare-feu vérifie dans chaque requête la présence de menaces d'après les recommandations de l'Open Web Application Security Project (OWASP). Les menaces courantes incluent l'injection SQL, le scripting inter-site, l'injection de commandes, le trafic de requêtes HTTP et le fractionnement de réponse, et l'inclusion de fichiers distants. D'autres menaces peuvent provenir des bots, des crawlers, des scanneurs et des violations et anomalies du protocole HTTP.

## Concevoir un schéma d'adressage IP pour votre déploiement Azure

Adressage IP réseau et intégration

<https://learn.microsoft.com/fr-fr/training/modules/design-ip-addressing-for-azure/2-network-ip-addressing-integration>

Adressage IP public et privé dans Azure

<https://learn.microsoft.com/fr-fr/training/modules/design-ip-addressing-for-azure/3-azure-public-private-ip-addressing>

Planifier l'adressage IP de vos réseaux

<https://learn.microsoft.com/fr-fr/training/modules/design-ip-addressing-for-azure/4-plan-design-ip-addressing>

## Distribuer vos services sur des réseaux virtuels Azure et les intégrer avec le peering de réseaux virtuels

Connecter des services par peering de réseaux virtuels

<https://learn.microsoft.com/fr-fr/training/modules/integrate-vnets-with-vnet-peering/2-connect-services-using-vnet-peering>

## Héberger votre domaine sur Azure DNS

Présentation d'Azure DNS

<https://learn.microsoft.com/fr-fr/training/modules/host-domain-azure-dns/2-what-is-azure-dns>

## Gérer et contrôler le flux de trafic dans votre déploiement Azure à l'aide de routes

Qu'est-ce qu'une appliance virtuelle réseau ?

<https://learn.microsoft.com/fr-fr/training/modules/control-network-traffic-flow-with-routes/4-network-virtual-appliances>



## Améliorer la scalabilité et la résilience des applications en utilisant Azure Load Balancer

<https://learn.microsoft.com/fr-fr/training/modules/improve-app-scalability-resiliency-with-load-balancer/2-load-balancer-features>

Configurer un équilibreur de charge public

<https://learn.microsoft.com/fr-fr/training/modules/improve-app-scalability-resiliency-with-load-balancer/3-public-load-balancer>

## Superviser et sauvegarder les ressources Azure

### Objectifs d'apprentissage

Dans ce module, vous allez découvrir comment :

- Décrivez les composants et les fonctionnalités du réseau virtuel Azure.
- Identifier les fonctionnalités et les cas d'usage des sous-réseaux et de leur mise en œuvre
- Identifier les cas d'usage des adresses IP privées et publiques
- Créez un réseau virtuel et attribuez une adresse IP.

### 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.

Azure Backup propose plusieurs composants que vous pouvez télécharger et déployer sur l'ordinateur ou sur le serveur approprié, ou dans le cloud. Vous déployez un composant (ou un agent) en fonction de ce que vous souhaitez protéger. Vous pouvez utiliser tous les composants de Sauvegarde Azure (que vous protégez des données en local ou dans le cloud) pour sauvegarder des données dans un coffre Recovery Services d'Azure.

Choses à savoir sur Sauvegarde Azure

#### **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.

Pour effectuer la configuration initiale, vous devez spécifier l'abonnement, le groupe de ressources et la région géographique ainsi qu'un nom permettant d'identifier le coffre.

## 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.

Type de réplication	Recommandation
<b>Géoredondant (GRS)</b>	(Par défaut) Utilisez la réplication GRS quand Azure est votre point de terminaison de stockage de sauvegarde principal.
<b>Localement redondant (LRS)</b>	Si Azure <b>n'est pas</b> votre point de terminaison de stockage de sauvegarde principal, utilisez la réplication LRS pour réduire vos coûts de stockage.

**Redondant dans une zone**

Si vous avez besoin d'une disponibilité des données sans temps d'arrêt dans une région, et si vous devez garantir la résidence des données, utilisez la réplication ZRS.

- Vous pouvez également spécifier le mode de restauration des données dans une région jumelée Azure secondaire en activant la **restauration interrégionale**.

## 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

La première étape consiste à créer un coffre Recovery Services pour vos sauvegardes. Le coffre doit être créé dans votre abonnement Azure, comme indiqué dans la [section précédente](#).

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

Dans le tableau de bord du Centre de sauvegarde, la page du coffre Recovery Services fournit un lien permettant de télécharger l'agent MARS (agent Recovery Services). Pour effectuer l'installation de l'agent MARS, vous devez également télécharger le fichier des *informations d'identification du coffre*. Pour plus d'informations, consultez [Télécharger l'agent MARS](#).

### Étape 3. Installer et inscrire l'agent MARS

Le programme d'installation de l'agent MARS fournit un Assistant qui permet de configurer l'emplacement d'installation, le serveur proxy et les informations relatives à la phrase secrète. Le fichier d'informations d'identification téléchargé est utilisé pour inscrire l'agent. L'agent MARS est installé sur votre machine locale.

### Étape 4. Configurer des sauvegardes

Vous êtes désormais prêt à utiliser l'agent MARS pour créer une stratégie de sauvegarde. Vous pouvez spécifier le moment où la sauvegarde doit être effectuée, les données à sauvegarder, la durée de conservation des éléments de sauvegarde ainsi que d'autres paramètres tels que la limitation de bande passante du réseau.

## 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

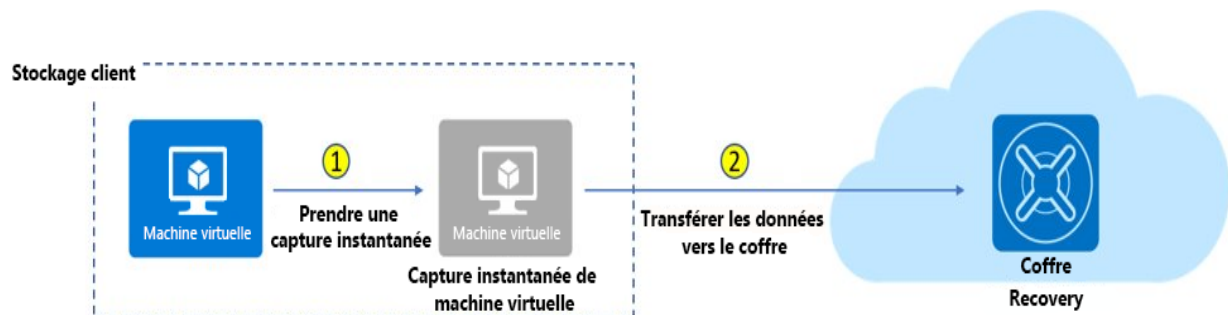
<b>Option Sauvegarde Azure</b>	<b>Scénarios de configuration</b>	<b>Description</b>
<b>Azure Backup</b>	<i>Sauvegarder des machines virtuelles Azure exécutant des charges de travail de production</i>  <i>Créer des sauvegardes cohérentes avec les applications pour les machines virtuelles Windows et Linux</i>	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.

<b>Azure Site Recovery</b>	<p><i>Récupérer rapidement et facilement des applications spécifiques</i></p> <p><i>Répliquer vers la région Azure de votre choix</i></p>	<p>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.</p>
<b>Disques managés Azure - capture instantanée</b>	<p><i>Sauvegarder rapidement et facilement vos machines virtuelles qui utilisent des disques managés Azure, à tout moment</i></p> <p><i>Prendre en charge des environnements de développement et de test</i></p>	<p>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.</p>
<b>Disques managés Azure - image</b>	<p><i>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)</i></p> <p><i>Créer des centaines de machines virtuelles en utilisant votre image personnalisée sans copier ni gérer de compte de stockage</i></p>	<p>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.</p>

## 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.

### Choses à savoir sur les coffres Recovery Services

- Un coffre Recovery Services stocke des données de sauvegarde pour divers services Azure, comme des machines virtuelles IaaS (Linux ou Windows) et des bases de données Azure SQL.
- Les coffres Azure Recovery Services prennent en charge System Center Data Protection Manager (DPM), Windows Server, Microsoft Azure Backup Server (MABS) et d'autres services.
- Dans le portail Azure, vous pouvez utiliser un coffre Azure Recovery Services pour y sauvegarder vos machines virtuelles Azure
- Vous pouvez utiliser un coffre Recovery Services pour y sauvegarder vos machines virtuelles locales, par exemple, les machines Hyper-V et VMware, l'état du système et la récupération complète

## 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.

Vous devez également spécifier le mode de réplication du stockage : géoredondant (par défaut) ou localement redondant.

- **Géoredondant** (GRS) : (par défaut) utilisez la réplication GRS si Azure est le point de terminaison de stockage des sauvegardes principal.
- **Localement redondant** (LRS) : si Azure **n'est pas** le point de terminaison de stockage des sauvegardes principal, utilisez la réplication LRS pour réduire vos coûts de stockage.

### 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.

Votre machine virtuelle est protégée grâce aux captures instantanées de vos données effectuées à des intervalles définis. Les captures instantanées créent des points de récupération qui sont stockés dans votre coffre Recovery Services.

S'il s'avère nécessaire de réparer ou de recréer votre machine virtuelle, vous pouvez restaurer cette machine à partir des points de récupération sauvegardés. Dans votre stratégie de sauvegarde, vous pouvez spécifier de déclencher une sauvegarde entre une à cinq fois par jour.

### 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.

### Comparer l'agent MARS et Azure Backup Server

<b>Composant</b>	<b>Avantages</b>	<b>Limites</b>	<b>Données protégées</b>	<b>Sauvegardes stockées</b>
------------------	------------------	----------------	--------------------------	-----------------------------

**Agent de sauvegarde MARS**

*Sauvegarder les fichiers et dossiers sur des machines physiques ou virtuelles exécutant Windows*

*Aucun serveur de sauvegarde distinct n'est requis*

- Sauvegardes déclenchées trois fois par jour
- Non-prise en compte des applications
- Restauration des fichiers, dossiers et volumes uniquement
- Pas de prise en charge pour Linux

Fichiers et dossiers

Coffre Azure Recovery Services

<b>Azure Backup Server</b>	<i>Captures instantanées tenant compte des applications</i>  <i>Choix flexible du moment auquel déclencher les sauvegardes</i>  <i>Granularité de récupération</i>  <i>Prise en charge de Linux sur les machines virtuelles Hyper-V et VMware</i>  <i>Sauvegarder et restaurer les machines virtuelles VMware</i>  <i>Pas de licence System Center requise</i>	- Nécessite toujours un abonnement Azure actif - Pas de sauvegardes des charges de travail Oracle - Pas de prise en charge des sauvegardes sur bande	Fichiers, dossiers, volumes, machines virtuelles, applications et charges de travail	Coffre Azure Recovery Services ou disque attaché localement
----------------------------	--	--	--	---

## 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.

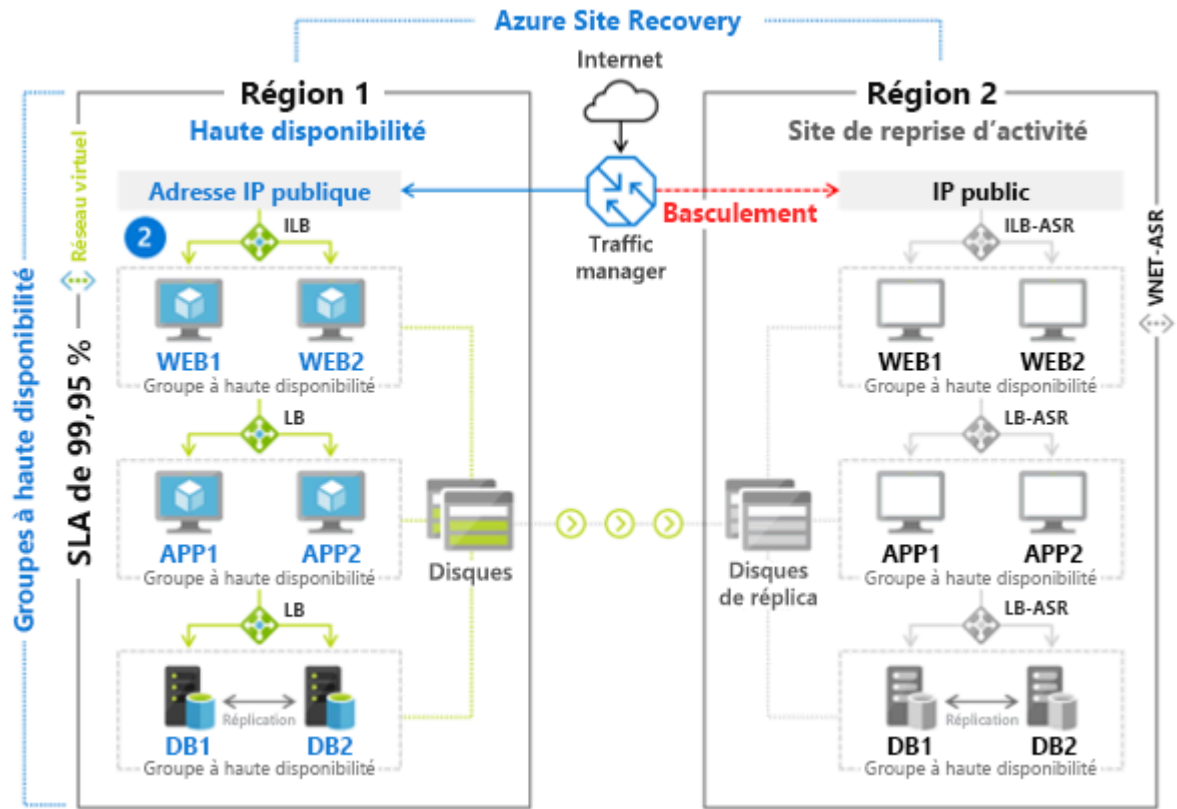
La fonctionnalité de suppression réversible pour les machines virtuelles protège les sauvegardes de vos machines virtuelles contre les suppressions involontaires. Même après leur suppression, les sauvegardes sont conservées à l'état de suppression réversible pendant encore 14 jours.

## 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

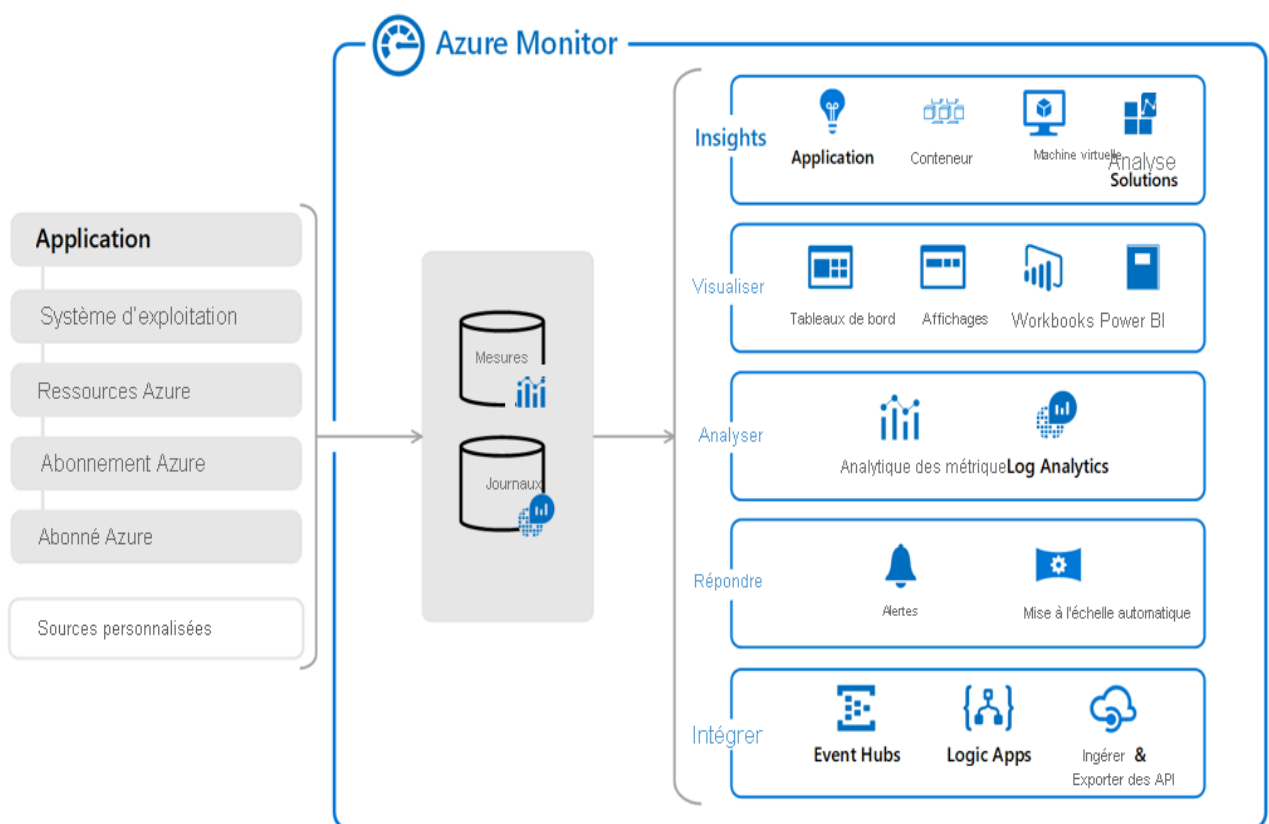
### Décrire les fonctionnalités clés d'Azure Monitor

#### 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 les visualisations 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.

Décrire les composants Azure Monitor



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

## Monitoring des niveaux de données

<b>Couche Données</b>	<b>Description</b>
<b>Application</b>	Le niveau Application contient des données de monitoring sur les performances et les fonctionnalités de votre code d'application. Ces données sont collectées quelle que soit votre plateforme.
<b>SE invité</b>	Les données de monitoring relatives au système d'exploitation sur lequel votre application s'exécute sont organisées dans le niveau Système d'exploitation invité. Votre application peut s'exécuter dans Azure, dans un autre cloud, ou localement.
<b>Ressource Azure</b>	Le niveau de ressources Azure contient des données de monitoring relatives au fonctionnement de toute ressource Azure que vous utilisez, y compris des détails sur la consommation de la ressource.
<b>Abonnement Azure</b>	Le niveau d'abonnement Azure contient des données de monitoring relatives au fonctionnement et à la gestion de votre abonnement Azure. Ce niveau contient également des données sur l'intégrité et le fonctionnement d'Azure proprement dit.

## **Locataire Azure**

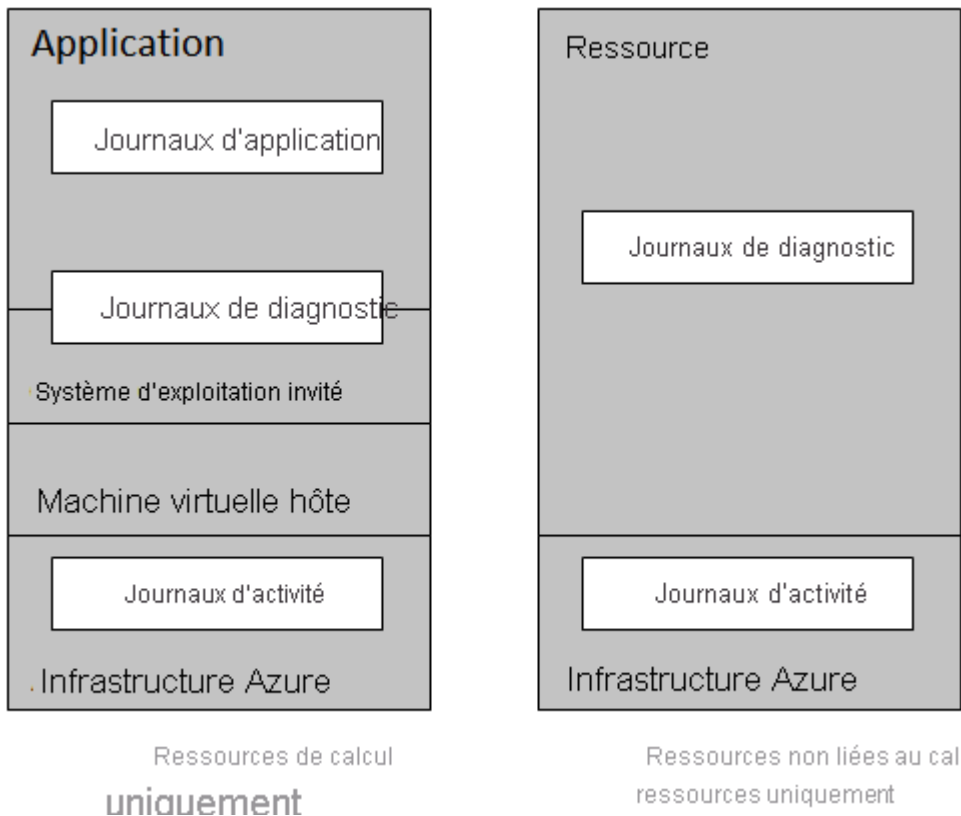
Les données relatives au fonctionnement de vos services Azure au niveau locataire, comme Azure Active Directory, sont organisées dans le niveau de locataire Azure.

## 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.



## Interroger le journal d'activité

### 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 ».

Après avoir défini un ensemble de filtres, vous pouvez l'épingler au tableau de bord Azure Monitor. Vous pouvez également télécharger les résultats de votre recherche dans le journal d'activité sous forme de fichier CSV.

En plus des filtres, vous pouvez entrer une chaîne de texte dans la zone **Rechercher**. Azure Monitor tente de faire correspondre votre chaîne de recherche aux données retournées pour tous les champs de tous les événements qui correspondent à vos paramètres de filtre.

Éléments à savoir sur les catégories d'événements

Catégorie d'événements	Données d'événement	Exemples
<b>Administrative</b>	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	<code>create virtual machine</code>  <code>delete network security group</code>
<b>Service Health</b>	Tous les événements d'intégrité du service pour les services et ressources Azure connectés à vos abonnements filtrés, y compris <i>Action requise, Récupération assistée, Incident, Maintenance, Informations</i> ou <i>Sécurité</i>	<code>SQL Azure in East US is experiencing downtime</code>  <code>Azure SQL Data Warehouse Scheduled Maintenance Complete</code>

<b>Resource Health</b>	Tous les événements d'intégrité des ressources pour vos ressources Azure filtrées, y compris <i>Disponible</i> , <i>Indisponible</i> , <i>Dégradé</i> ou <i>Inconnu</i> , et identifiés comme <i>Lancé par la plateforme</i> ou <i>Lancé par l'utilisateur</i>	Virtual Machine health status changed to unavailable  Web App health status changed to available
<b>Alert</b>	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
<b>Autoscale</b>	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
<b>Recommandation</b>	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	<i>Recommandations pour mieux utiliser vos ressources</i>
<b>Sécurité</b>	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

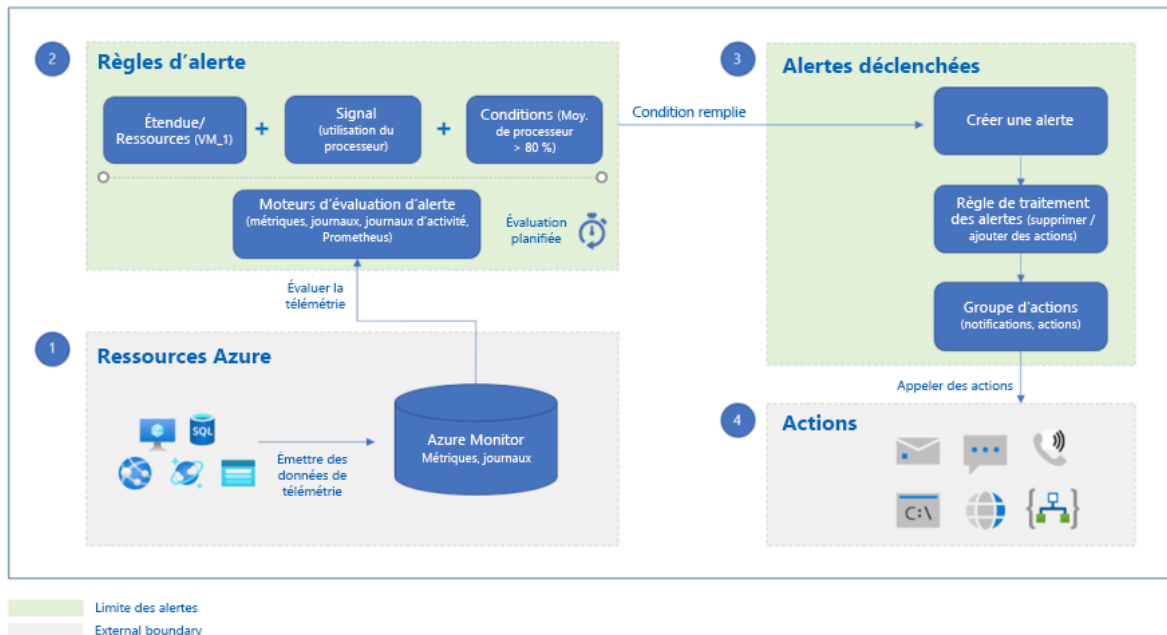
## Configurer des alertes Azure

### Décrire les alertes Azure Monitor

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 monitoriez plusieurs ressources, le système évalue vos conditions et déclenche des alertes séparément pour chaque ressource.





## Gérer les alertes Azure Monitor

### 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 « ouvrir » 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.

## Créer des règles d'alerte

Créer une règle - Microsoft Azure

portal.azure.com/#blade/Microsoft\_Azure\_Monitoring/Azure...

Microsoft Azure Rechercher dans les ressour...

Accueil > Superviser - Vue d'ensemble > Créer une règle

### Créer une règle

Gestion des règles

**\* RESSOURCE** **HIÉRARCHIE**

Sélectionnez la ou les cibles que vous souhaitez superviser

Sélectionner

**\* CONDITION**

Aucune condition n'est définie. Cliquez sur « Ajouter une condition » pour sélectionner un signal et définir sa logique

Ajouter

**ACTIONS**

Nom du groupe d'actions Contenir des actions

Aucun groupe d'actions sélectionné

Sélectionner un groupe d'actions Créer un groupe d'actions

Créer une règle d'alerte

### 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*.

## Créer des groupes d'actions

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. Le système envoie des e-mails aux utilisateurs Azure Active Directory (Azure AD) qui sont membres du rôle uniquement, et non aux groupes Azure AD ou aux principaux de service.

Vous pouvez également sélectionner l'option **E-mail/SMS/Push/Voix** pour spécifier les actions par e-mail, SMS, push ou voix.

## 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.

### Actions

Configurez la méthode selon laquelle les actions sont exécutées quand le groupe d'actions est déclenché. Sélectionnez les types d'actions, renseignez les détails associés et ajoutez une description unique. Cette étape est facultative.

Type d'action ⓘ	Nom ⓘ	Sélectionné ⓘ
<input type="text" value=""/> ^	<input type="text"/>	
Runbook Automation		
Fonction Azure		
ITSM		
Application logique		
Webhook sécurisé		
Webhook		

Vous pouvez configurer le groupe d'actions pour qu'il utilise une action automatisée par le biais de l'attribut **Type d'action**. Voici quelques options automatisées :

- **Runbook automation** : un runbook automation est la capacité à définir, créer, orchestrer, gérer et créer des rapports sur les workflows qui prennent en charge les processus système et réseau opérationnels. Un workflow de runbook peut potentiellement interagir avec tous les types d'éléments d'infrastructure, tels que les applications, les bases de données et le matériel.
- **Azure Functions** : Azure Functions est un service de calcul serverless qui vous permet d'exécuter du code déclenché par des événements sans avoir à provisionner ou à gérer explicitement l'infrastructure.
- **ITSM** : l'action peut connecter Azure et un produit ou service de gestion des services informatiques (ITSM) pris en charge. Cette action nécessite une connexion ITSM.
- **Logic Apps** : Azure Logic Apps connecte vos applications et services critiques pour l'entreprise en automatisant vos workflows.
- **Webhook** : un webhook est un point de terminaison HTTPS ou HTTP qui permet aux applications externes de communiquer avec votre système.

## Configurer Log Analytics

## Déterminer les utilisations de Log Analytics

### 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 prendre en compte lors de l'utilisation de 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.

## Créer un espace de travail Log Analytics

Quand vous capturez des journaux et des données dans Azure Monitor, Azure stocke les informations collectées dans un espace de travail Log Analytics. Votre espace de travail Log Analytics est l'environnement de gestion de base pour les journaux Azure Monitor.

## 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 ressource 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 ».

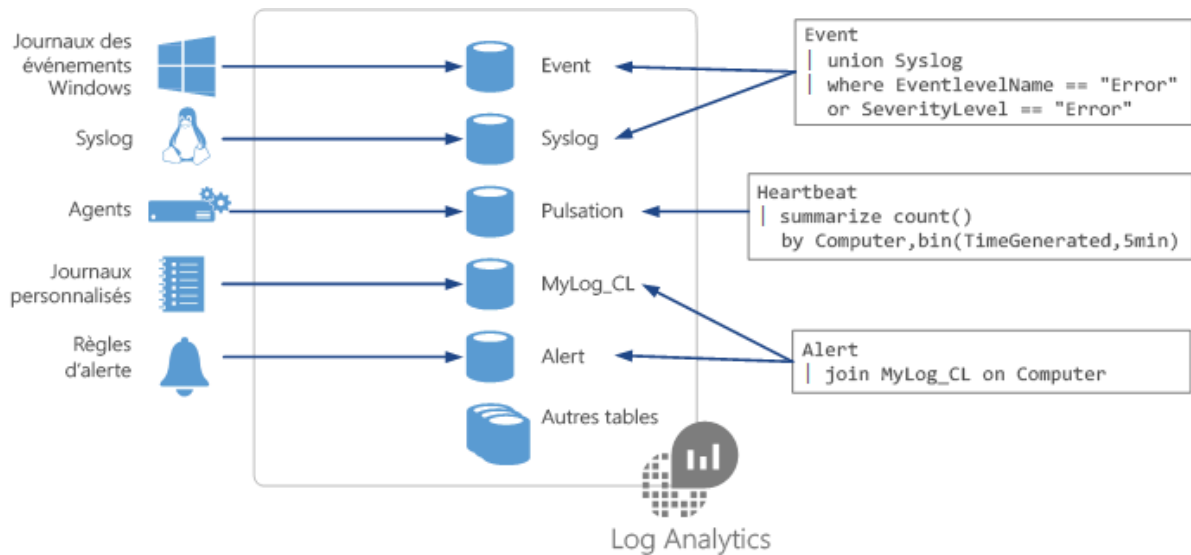
- **Tarifcation** : le niveau tarifaire par défaut d'un nouvel espace de travail est le *paiement à l'utilisation*. Les frais incombent uniquement une fois que vous avez commencé à collecter des données.

Chaque espace de travail Log Analytics d'Azure Monitor peut présenter un niveau tarifaire différent. Vous pouvez modifier le niveau tarifaire d'un espace de travail et effectuer le suivi des modifications.

## Structurer des requêtes Log Analytics

Les administrateurs génèrent des requêtes Log Analytics à partir de données stockées de tables dédiées dans un espace de travail Log Analytics. Voici quelques tables dédiées courantes : Event, Syslog, Heartbeat et Alert. Quand vous générez une requête KQL (Langage de requête Kusto), vous commencez en déterminant quelles tables du référentiel de journaux Azure Monitor contiennent les données que vous recherchez.

L'illustration suivante met en évidence comment les requêtes KQL utilisent les données de table dédiées pour vos services et ressources supervisés.



### Points à connaître sur la structure de requête KQL

- Chaque source de données et solution sélectionnée stocke ses données dans des tables dédiées dans votre espace de travail Log Analytics.
- La documentation de chaque source de données et solution inclut le nom du type de données qu'elle crée et une description de chacune de ses propriétés.
- La structure de base d'une requête est une table source suivie d'une série de commandes (appelées *opérateurs*).
- Une requête peut avoir une chaîne de plusieurs opérateurs permettant d'affiner vos données et d'effectuer des fonctions avancées.
- Chaque opérateur d'une chaîne de requête commence par un caractère de barre verticale |.
- De nombreuses requêtes nécessitent les données d'une seule table uniquement, mais d'autres requêtes peuvent utiliser diverses options et inclure des données provenant de plusieurs tables.

## 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
<b>Vérification du flux IP</b>	Diagnostiquez rapidement les problèmes de connectivité depuis ou vers Internet, et depuis ou vers votre environnement local.	<p><i>Déterminer si une règle de sécurité bloque le trafic entrant ou sortant vers ou depuis une machine virtuelle</i></p> <p><i>Résoudre les problèmes pour déterminer si une autre exploration est nécessaire</i></p>
<b>Tronçon suivant</b>	Affichez le point de connexion suivant (ou <i>tronçon suivant</i> ) dans votre route réseau et analysez la configuration de votre routage réseau.	<p><i>Déterminer s'il existe un tronçon suivant et affichez la cible, le type et la table de routage du tronçon suivant</i></p> <p><i>Vérifier que le trafic atteint une destination cible prévue</i></p>
<b>Résolution des problèmes de VPN</b>	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.	<p><i>Afficher les diagnostics récapitulatifs dans le portail Azure</i></p> <p><i>Passer en revue les diagnostics détaillés dans les fichiers journaux générés stockés dans votre compte de stockage Azure</i></p> <p><i>Résoudre simultanément les problèmes de plusieurs passerelles ou connexions</i></p>

**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.

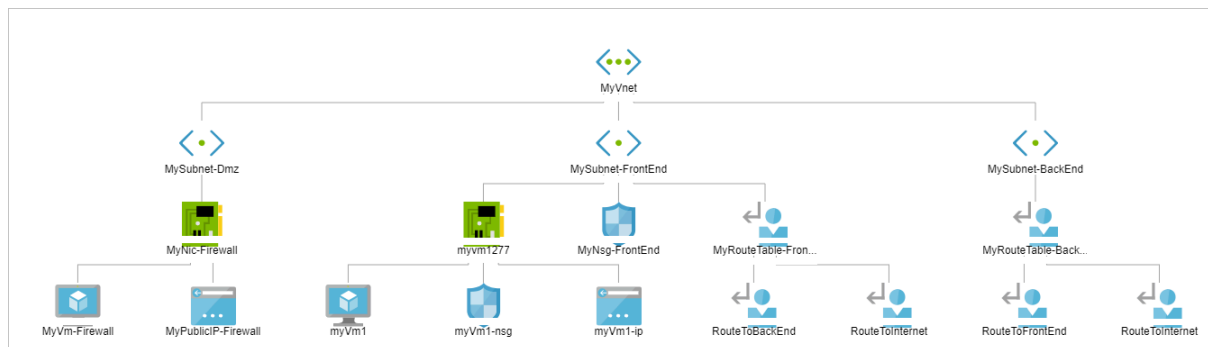
### Ce qu'il faut savoir sur la fonctionnalité de tronçon suivant

- 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. L'image suivante montre un exemple de diagramme de topologie pour un réseau virtuel dans Network Watcher.



## 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.

## Améliorer la réponse aux incidents à l'aide des alertes dans Azure

Utiliser les alertes de journal pour signaler des événements de votre application

Composition des règles de recherche dans les journaux

Chaque alerte de journal a une règle de recherche associée. La composition de ces règles est la suivante :

- **Requête de journal** : requête qui s'exécute chaque fois que la règle d'alerte se déclenche.

- **Période** : intervalle de temps pour la requête.
- **Fréquence** : fréquence d'exécution de la requête.
- **Seuil** : point de déclenchement pour la création d'une alerte.

Les résultats de la recherche dans les journaux sont de deux types : nombre d'enregistrements ou mesure de métriques.

#### Nombre d'enregistrements

Utilisez ce type de recherche dans les journaux pour un événement ou pour des données basées sur un événement. Les réponses provenant de syslog ou d'applications web en sont des exemples.

Ce type de recherche dans les journaux retourne une seule alerte quand le nombre d'enregistrements d'un résultat de la recherche atteint ou dépasse le nombre d'enregistrements (seuil). Par exemple, quand le seuil de la règle de recherche est supérieur ou égal à cinq, les résultats de la requête doivent retourner au moins cinq lignes de données pour que l'alerte se déclenche.

#### Mesure de métriques

Les journaux de mesure de métriques offrent les mêmes fonctionnalités de base que les journaux d'alertes de métriques.

Contrairement à un certain nombre de journaux de recherche d'enregistrements, les journaux de mesure de métriques nécessitent la définition de critères supplémentaires :

- **Fonction d'agrégation** : définit le calcul qui doit être effectué sur les données de résultat. Par exemple, le nombre ou la moyenne. Le résultat de la fonction se nomme **AggregatedValue**.
- **Champ de groupe** : champ selon lequel le résultat est regroupé. Ce critère est utilisé avec la valeur agrégée. Par exemple, vous pouvez spécifier une moyenne regroupée par ordinateur.
- **Intervalle** : intervalle de temps pendant lequel les données sont agrégées. Par exemple, si vous spécifiez 10 minutes, un enregistrement d'alerte est créé pour chaque bloc agrégé de 10 minutes.
- **Seuil** : point défini par une valeur agrégée et le nombre total de violations.

Utilisez ce type d'alerte quand vous devez ajouter un niveau de tolérance aux résultats trouvés. Ce type d'alerte est utilisé notamment pour envoyer une réponse en cas de détection d'une tendance ou d'un modèle particulier. Par exemple, si le nombre de violations est égal à cinq, et si l'un des serveurs de votre groupe dépasse 85 % de taux d'utilisation du processeur plus de cinq fois au cours d'une période donnée, une alerte se déclenche.

Comme vous pouvez le constater, les mesures de métriques réduisent considérablement le volume des alertes générées. Il convient toutefois d'accorder une attention particulière à la définition des paramètres de seuil pour éviter de rater les alertes critiques.

#### Nature sans état des alertes de journal

L'une des principales considérations à prendre en compte durant l'évaluation de l'utilisation des alertes de journal est qu'elles sont sans état (les alertes de journal avec état sont [actuellement en préversion](#)). Une alerte de journal génère de nouvelles alertes chaque fois que les critères de la règle se déclenchent, que l'alerte ait été enregistrée précédemment ou non.

### Utiliser les alertes du journal d'activité pour signaler des événements dans votre infrastructure Azure

#### Quand utiliser les alertes du journal d'activité

Jusqu'à présent, vous avez vu les deux différents types d'alerte pris en charge dans Azure Monitor. Les *alertes de métriques* conviennent parfaitement à la supervision des violations de seuil ou à la détection des tendances, tandis que les *alertes de journal* permettent une supervision analytique plus importante des données historiques.

Les alertes du journal d'activité sont conçues pour fonctionner avec des ressources Azure. En règle générale, vous créez ce type de journal pour recevoir des notifications quand des changements spécifiques se produisent sur une ressource de votre abonnement Azure.

Il existe deux types d'alertes du journal d'activité :

- **Opérations spécifiques** : s'applique aux ressources de votre abonnement Azure et dispose souvent d'une étendue composée de ressources spécifiques ou d'un groupe de ressources. Vous utilisez ce type d'alerte quand vous devez recevoir une alerte qui signale un changement dans l'un des aspects de votre abonnement. Par exemple, vous pouvez recevoir une alerte si une machine virtuelle est supprimée ou si de nouveaux rôles sont attribués à un utilisateur.
- **Événements Service Health** : ils incluent la notification des incidents et la maintenance des ressources cibles.

#### Composition d'une alerte du journal d'activité

Il est important de noter que les alertes du journal d'activité supervisent uniquement les événements de l'abonnement où l'alerte de journal a été créée.

Les alertes de journal d'activité sont basées sur des événements. La meilleure approche pour les définir consiste à utiliser Azure Monitor afin de filtrer tous les événements de votre abonnement, jusqu'à ce que vous trouviez celui que vous souhaitez. Pour lancer le processus de création, vous sélectionnez ensuite **Ajouter une alerte de journal d'activité**.

À l'instar des alertes précédentes, les alertes du journal d'activité ont leurs propres attributs :

- **Catégorie** : administration, intégrité du service, mise à l'échelle automatique, stratégie ou recommandation
- **Étendue** : niveau de ressource, de groupe de ressources ou d'abonnement
- **Groupe de ressources** : emplacement où la règle d'alerte est enregistrée
- **Type de ressource** : espace de noms de la cible de l'alerte
- **Nom de l'opération** : nom de l'opération
- **Niveau** : commentaires, information, avertissement, erreur ou critique
- **État** : démarré, échec ou réussi
- **Événement lancé par** : adresse e-mail ou identificateur Azure Active Directory (ou « appelant ») de l'utilisateur

Créer une alerte de journal spécifique à une ressource

Quand vous créez votre alerte de journal d'activité, vous sélectionnez le type de signal **Journal d'activité**. Vous voyez alors toutes les alertes disponibles pour la ressource sélectionnée. L'image suivante montre toutes les alertes administratives pour les machines virtuelles Azure. Dans cet exemple, une alerte est déclenchée quand une machine virtuelle est hors tension.

Apportez des changements au service de supervision pour réduire la liste des options. La sélection de l'option **Administration** filtre tous les signaux pour afficher uniquement les signaux liés à l'administration.

**Configurer la logique du signal** ✕

Choisissez un signal ci-dessous et configurez la logique sur l'écran suivant pour définir la condition d'alerte.

**Tous les signaux (15)**

Type de signal ⓘ Analyser le service ⓘ

Journal d'activité Journal d'activité – Administratif

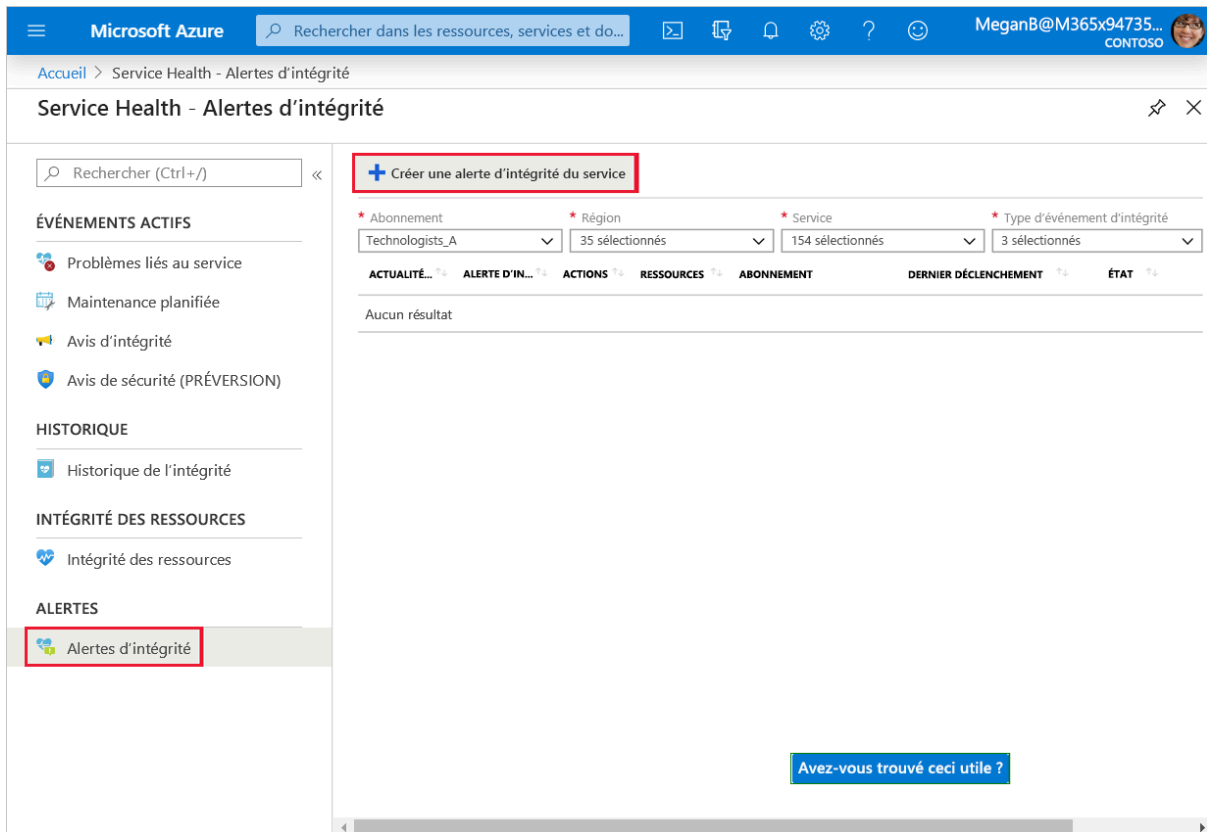
🔍 Rechercher par nom de signal

NOM DU SIGNAL	↑↓	TYPE DE SIGNAL	↑↓	ANALYSER LE SERVICE	↑↓
Toutes les opérations d'administration		Journal d'activité		Administratif	
Obtenir la machine virtuelle (virtualMachines)		Journal d'activité		Administratif	
Créer ou mettre à jour une machine virtuelle (virtualMachines)		Journal d'activité		Administratif	
Supprimer la machine virtuelle (virtualMachines)		Journal d'activité		Administratif	
Démarrer une machine virtuelle (virtualMachines)		Journal d'activité		Administratif	
Mettre hors tension la machine virtuelle (virtualMachines)		Journal d'activité		Administratif	
Redéployer la machine virtuelle (virtualMachines)		Journal d'activité		Administratif	
Redémarrer une machine virtuelle (virtualMachines)		Journal d'activité		Administratif	
Libérer une machine virtuelle (virtualMachines)		Journal d'activité		Administratif	
Généraliser la machine virtuelle (virtualMachines)		Journal d'activité		Administratif	
Capter la machine virtuelle (virtualMachines)		Journal d'activité		Administratif	
Exécuter une commande sur la machine virtuelle (virtualMachines)		Journal d'activité		Administratif	
Convertir les disques de machine virtuelle en disques managés (vir...		Journal d'activité		Administratif	
Effectuer le redéploiement de maintenance (virtualMachines)		Journal d'activité		Administratif	
Réimager la machine virtuelle (virtualMachines)		Journal d'activité		Administratif	

## Créer une alerte d'intégrité du service

Les alertes d'intégrité de service ne ressemblent pas aux autres types d'alerte que vous avez vus jusqu'à présent dans ce module. Pour créer une alerte, recherchez et sélectionnez **Service Health** dans le portail Azure. Sélectionnez ensuite **Alertes d'intégrité**. Une fois que vous avez sélectionné **Créer une alerte d'intégrité du service**, les étapes de création de l'alerte sont similaires à celles que vous avez suivies pour créer d'autres alertes.





La seule différence est que vous n'avez plus besoin de sélectionner une ressource, car l'alerte concerne une région entière dans Azure. Vous pouvez sélectionner le genre d'événement d'intégrité pour lequel vous souhaitez être alerté. Vous pouvez sélectionner des événements relatifs à des problèmes de service, à une maintenance planifiée, à des avis d'intégrité ou tous les événements. Les étapes restantes pour effectuer des actions et nommer les alertes sont les mêmes.

Utiliser des groupes d'actions et des règles de traitement des alertes pour envoyer des notifications quand une alerte est déclenchée

Quand une alerte est déclenchée, Azure Monitor, Azure Service Health et Azure Advisor utilisent des groupes d'actions pour informer les utilisateurs de l'alerte et effectuer une action. Un groupe d'actions est une collection de préférences de notification et d'actions qui sont exécutées quand l'alerte est déclenchée. Vous pouvez exécuter une ou plusieurs actions pour chaque alerte déclenchée.

Azure Monitor peut effectuer n'importe laquelle des actions suivantes :

- Envoyer un e-mail
- Envoyer un SMS
- Créer une notification Push Azure App
- Effectuer un appel vocal vers un numéro
- Appeler une fonction Azure
- Déclencher une application logique

- Envoyer une notification à un webhook
- Créer un ticket ITSM
- Utiliser un runbook (pour redémarrer une machine virtuelle ou pour effectuer un scale-up ou un scale-down d'une machine virtuelle)

Une fois que vous avez créé un groupe d'actions, vous pouvez réutiliser ce groupe d'actions aussi souvent que vous le souhaitez. Par exemple, une fois que vous avez créé une action pour envoyer un e-mail à l'équipe des opérations de votre société, vous pouvez ajouter ce groupe d'actions à tous les événements d'intégrité du service.

Quand vous créez la règle d'alerte, vous pouvez créer un groupe d'actions ou ajouter un groupe d'actions existant à la règle d'alerte. Vous pouvez également modifier une alerte existante pour ajouter un groupe d'actions.

### Règles de traitement des alertes

Utilisez des règles de traitement des alertes pour remplacer le comportement normal d'une alerte déclenchée en ajoutant ou en supprimant un groupe d'actions. Vous pouvez utiliser des règles de traitement des alertes pour ajouter des groupes d'actions ou supprimer des groupes d'actions de vos alertes déclenchées. Les règles de traitement des alertes sont différentes des règles d'alerte. Les règles d'alerte déclenchent des alertes quand une condition est remplie dans vos ressources monitorées. Les règles de traitement des alertes modifient les alertes quand elles sont déclenchées.

Vous pouvez utiliser des règles de traitement des alertes pour :

- Supprimer les notifications pendant les fenêtres de maintenance planifiée
- Implémenter la gestion à grande échelle, en spécifiant la logique couramment utilisée dans une seule règle, au lieu d'avoir à la définir systématiquement dans toutes vos règles d'alerte.
- Ajouter un groupe d'actions à tous les types d'alerte

Vous pouvez appliquer des règles de traitement des alertes à différentes étendues de ressources, d'une ressource unique ou à un abonnement entier. Vous pouvez également les utiliser pour appliquer différents filtres ou faire en sorte que la règle fonctionne selon une planification prédéfinie.

Vous pouvez contrôler quand appliquer la règle de traitement des alertes. Par défaut, la règle est toujours active, mais vous pouvez sélectionner une fenêtre ponctuelle pour que cette règle s'applique, ou vous pouvez définir une périodicité, par exemple, toutes les semaines.

# Analyser votre infrastructure Azure avec des journaux Azure Monitor

Que sont les journaux Azure Monitor et les insights sur les machines virtuelles d'Azure Monitor ?

Quel est le lien entre tous les outils de supervision natifs d'Azure ?

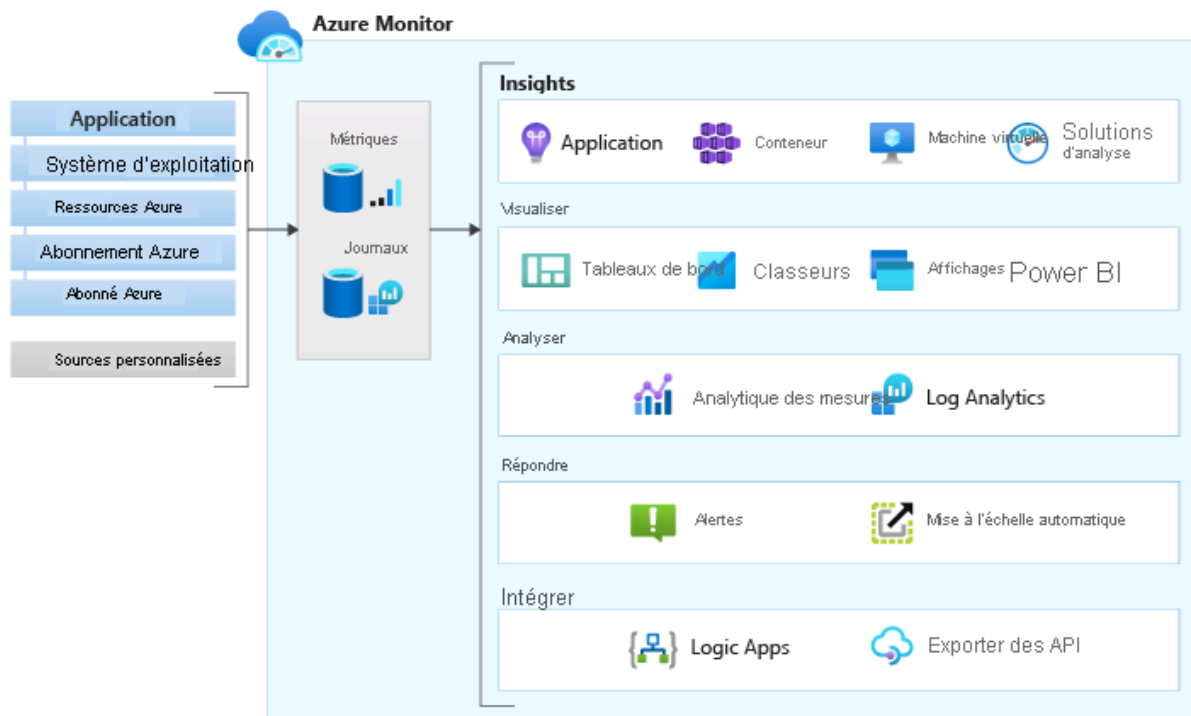
Il existe quelques ressources et services différents qui complètent le kit d'outils de supervision dans Azure. Azure Monitor devient le service de premier niveau, qui s'étend sur tous les autres outils d'analyse, tandis que tout le reste demeure sous-jacent. Le service collecte et analyse les données générées par les ressources Azure. Azure Monitor capture les données de supervision issues des sources suivantes :

- Application
- SE invité
- Ressources Azure
- Abonnements Azure
- Client Azure

Les données collectées par Azure Monitor se composent de métriques dans Azure Monitor Metrics et de journaux dans Azure Monitor Logs. Azure Monitor Metrics sont des valeurs numériques légères qui sont stockées dans une base de données de série chronologique et qui peuvent être utilisées pour les alertes en quasi-temps réel. Les métriques capturées sont, par exemple, les pourcentages IOPS et les cycles processeur.

Comme nous l'avons vu précédemment, la fonctionnalité Journaux Azure Monitor collecte et organise les données de journal générées par les ressources Azure. La principale différence entre les métriques Azure Monitor et les journaux Azure Monitor tient à la structure des données générées. Les métriques Azure Monitor stockent uniquement des données numériques ayant une structure spécifique. Les journaux Azure Monitor peuvent stocker des données relatives aux métriques Azure Monitor et une variété d'autres types de données, utilisant toutes leur propre structure.

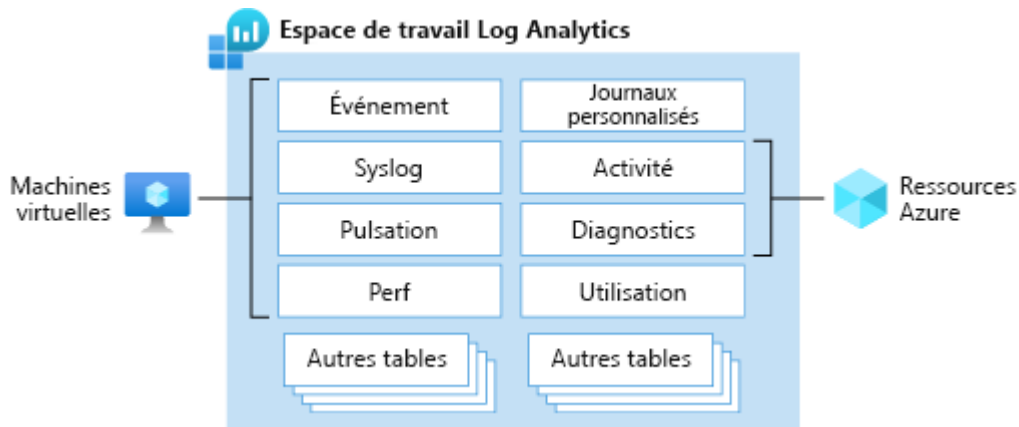
L'illustration suivante montre comment les flux des applications, des ressources, des charges de travail, des données de locataire et des sources personnalisées sont transmis à Azure Monitor (vers les métriques ou les journaux). Une fois que les données générées se trouvent dans les métriques ou les journaux, il y a plusieurs façons de visualiser, d'analyser, de répondre, d'intégrer et d'afficher l'intégrité globale des ressources.



En plus des journaux et des métriques, les ressources Azure génèrent aussi des journaux de plateforme Azure, qui sont collectés par Azure Monitor. Les journaux de plateforme fournissent des informations complètes de diagnostic et d'audit pour les ressources Azure et la plateforme Azure sous-jacente. Ils correspondent aux journaux des ressources (anciennement appelés journaux de diagnostic), aux journaux d'activité et aux journaux Azure Active Directory. Toutes les ressources génèrent automatiquement des journaux de plateforme. Les administrateurs peuvent avoir besoin de configurer le transfert de certains journaux de plateforme devant être conservés vers une ou plusieurs destinations (par exemple, Log Analytics).

### Planifier le déploiement d'un espace de travail Log Analytics

L'une des tâches dans un déploiement de Log Analytics est le choix d'une conception adaptée. Les espaces de travail Log Analytics sont des conteneurs dans lesquels les données Azure Monitor sont collectées, agrégées et analysées. Pour vous aider à comprendre ce que sont les espaces de travail Log Analytics, le diagramme suivant détaille les différents types de journaux qui peuvent être ingérés. Ces journaux incluent tout depuis des événements, des journaux syslog, des journaux des pulsations et ainsi de suite. Il y a ensuite les ressources Azure qui peuvent aussi envoyer des journaux de plateforme et des journaux d'activité Azure à l'espace de travail.



Plusieurs fonctionnalités Azure facilitent la mise en place des espaces de travail Log Analytics dans les entreprises. Les espaces de travail Log Analytics proposent désormais différents niveaux de contrôle d'accès aux journaux collectés.

Fonctionnalité	Description	Notes
Mode d'accès	Détermine de quelle manière les utilisateurs accèdent à un espace de travail Log Analytics, et définit l'étendue des données	Il existe deux options. <i>Contexte de l'espace de travail</i> permet d'accéder à tous les journaux dans un espace de travail où l'autorisation est attribuée. Les requêtes sont étendues à toutes les données de toutes les tables. <i>Contexte de la ressource</i> : permet d'accéder aux journaux des ressources dans toutes les tables auxquelles vous avez accès. Les requêtes sont étendues aux seules données associées à la ressource en question.

Mode de contrôle d'accès	Définit le fonctionnement des autorisations pour un espace de travail Log Analytics donné	<i>Exiger des autorisations d'espace de travail</i> signifie qu'un utilisateur a accès à toutes les données dans toutes les tables autorisées, ce qui ne permet pas un contrôle d'accès en fonction du rôle (RBAC) précis. <i>Utiliser les autorisations de ressource ou d'espace de travail</i> permet un contrôle RBAC précis, où les utilisateurs peuvent uniquement voir les données de journal pour les ressources autorisées. Les autorisations peuvent être attribuées à un seul utilisateur ou à des groupes d'utilisateurs pour l'espace de travail ou la ressource.
Table-level RBAC	Fournit un mécanisme permettant de définir un contrôle de données plus précis à l'intérieur d'un espace de travail Log Analytics avec d'autres autorisations indiquées dans la table	Avec cette fonctionnalité, un administrateur peut définir quels types de données spécifiques sont accessibles à un ensemble d'utilisateurs. La configuration du contrôle RBAC au niveau de la table nécessite des rôles personnalisés Azure pour accorder ou refuser l'accès à des tables spécifiques. Ces rôles sont appliqués à des espaces de travail Log Analytics, où les modes d'accès « contexte de l'espace de travail » ou « contexte de la ressource » sont configurés.

La meilleure stratégie consiste à limiter le nombre total d'espaces de travail nécessaires pour les opérations quotidiennes. Avec un nombre réduit d'espaces de travail, les tâches d'administration et de requête seront plus rapides et plus simples. Certaines entreprises auront besoin d'une conception avec des espaces de travail multiples. C'est le cas, par exemple, dans une entreprise globale où la souveraineté des données est une exigence.

Azure collecte les données de supervision des ressources de calcul à l'aide d'agents

Pour les ressources de calcul dans Azure, plusieurs agents sont nécessaires pour faciliter la collecte des données d'analyse dans Log Analytics et Azure Monitor. Chaque agent permet aux clients de mesurer les performances, la réactivité et la

disponibilité des systèmes d'exploitation invités et des charges de travail sous-jacentes.

Le tableau suivant décrit chaque agent :

<b>Agent</b>	<b>Description</b>	<b>Notes</b>
Agent Azure Monitor	Collecte les données d'analyse des systèmes d'exploitation invités sur les machines virtuelles et remet les données aux journaux et/ou aux métriques Azure Monitor	Au fil du temps, cet agent remplace l'agent Log Analytics et l'extension de diagnostic Azure listés ci-dessous. Bien que cet agent introduise de nouvelles fonctionnalités, il ne prend pas en charge tous les scénarios d'analyse couverts par les agents précédents. Vous devez comprendre les <a href="#">inconvenients</a> avant de basculer vers l'agent Azure Monitor.
Agent Log Analytics	Collecte les journaux et des données de niveau de performance pour les machines virtuelles dans Azure, dans d'autres clouds ou en local	Permet d'intégrer les insights sur les machines virtuelles d'Azure Monitor, Microsoft Defender pour le cloud et Microsoft Sentinel. L'agent fonctionne aussi avec les comptes Azure Automation pour intégrer Azure Update Management, Azure Automation State Configuration avec externe suivi des modifications et inventaire Azure Automation.
Extension Diagnostics Azure	Permet aux clients de recevoir des données supplémentaires des systèmes d'exploitation invités et des charges de travail qui résident sur les ressources de calcul	Les données principalement capturées avec cette extension sont ensuite envoyées dans les métriques Azure Monitor. Si nécessaire, ces données peuvent également être envoyées à un outil tiers à l'aide d'Azure Event Hubs ou envoyées au stockage Azure à des fins d'archivage. Vous pouvez également collecter les diagnostics de démarrage, ce qui vous aide à effectuer des investigations pour les problèmes de démarrage de la machine virtuelle.

Agent de dépendances	Collecte les données découvertes relatives à certains processus exécutés sur les machines virtuelles	Mappe toutes les dépendances entre les machines virtuelles et les dépendances de processus externes.
----------------------	--	--

Comme nous l'avons dit précédemment, les insights sur les machines virtuelles d'Azure Monitor doivent être configurés pour l'espace de travail Log Analytics. Les insights sur les machines virtuelles d'Azure Monitor sont un service récent qui améliore la visibilité et fournit des fonctionnalités supplémentaires pour la collecte de données des machines virtuelles.

Dans l'unité suivante, nous vous montrerons comment déployer un espace de travail Log Analytics avec le contrôle d'accès adapté. Nous allons maintenant voir en détail comment activer les insights sur les machines virtuelles d'Azure Monitor. Cela implique également d'intégrer les machines virtuelles à un espace de travail Log Analytics.