

Cloud Computing



www.imenemami.com/cloud/cours.pdf

Cloud Computing ?

☐ Utilisation du Cloud Computing ?

- Utilisation de services en lignes :
 - Courriers électroniques, films à la demande, Jeux en ligne, stockages de fichiers ou images, etc.

☐ Ce que vous pouvez faire avec le Cloud

- Créer des applications et des services
- Stocker, sauvegarder et récupérer des données
- Hébergement (sites web par exemple)
- Diffuser du contenu audio et vidéo
- Diffuser des logiciels à la demande
- Analyse des données pour en tirer des informations et faire des prévisions

Principaux avantages du Cloud Computing

☐ Coût

☐ Vitesse

☐ Elasticité et scalabilité (Mise à l'échelle)

- Scalabilité verticale (scale up) / scalabilité horizontale (scale out)

Principaux avantages du Cloud Computing

☐ Productivité

☐ Performances

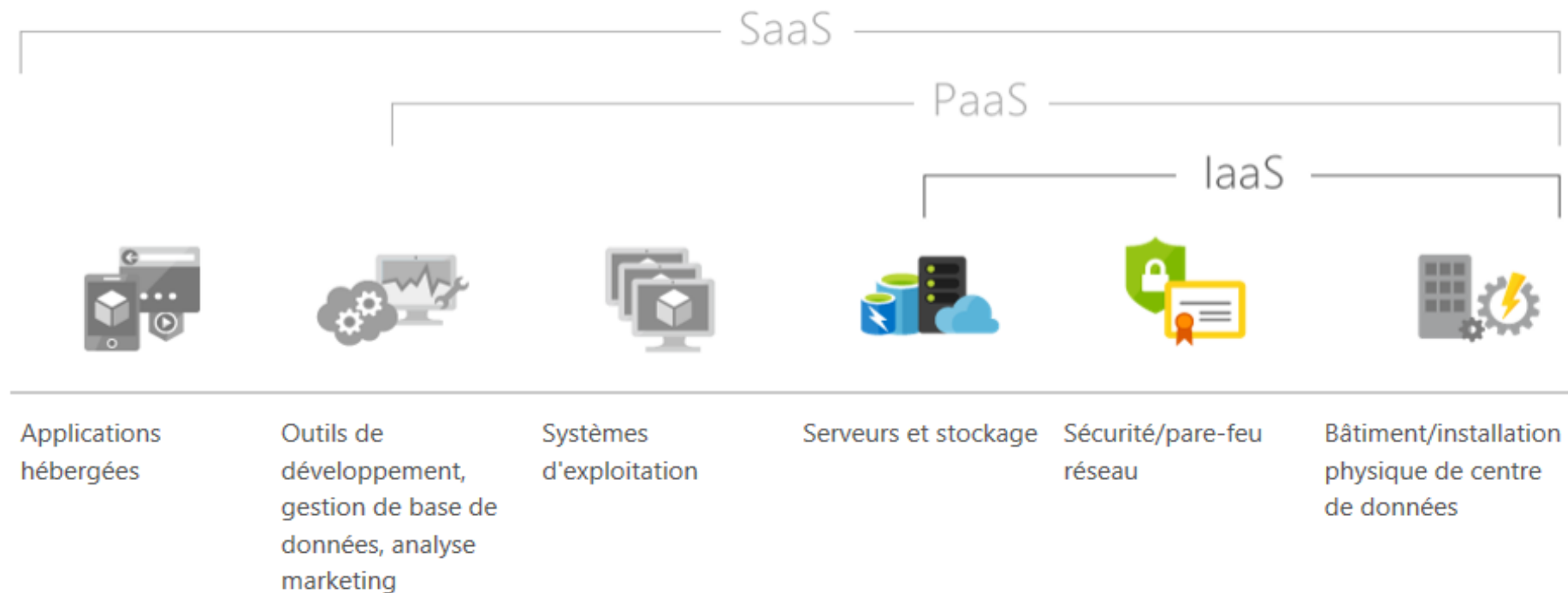
☐ Fiabilité (Haute disponibilité, Reprise sur panne)

Type de services Cloud

- ❑ L'**infrastructure** en tant que **service** (IaaS) En anglais: **Infrastructure as a Service (IaaS)**
- ❑ La **plateforme** en tant que **service** (PaaS) En anglais: **Platform as a Service (PaaS)**
- ❑ Le **logiciel** en tant que service (**SaaS**) En anglais: **Software as a Service**

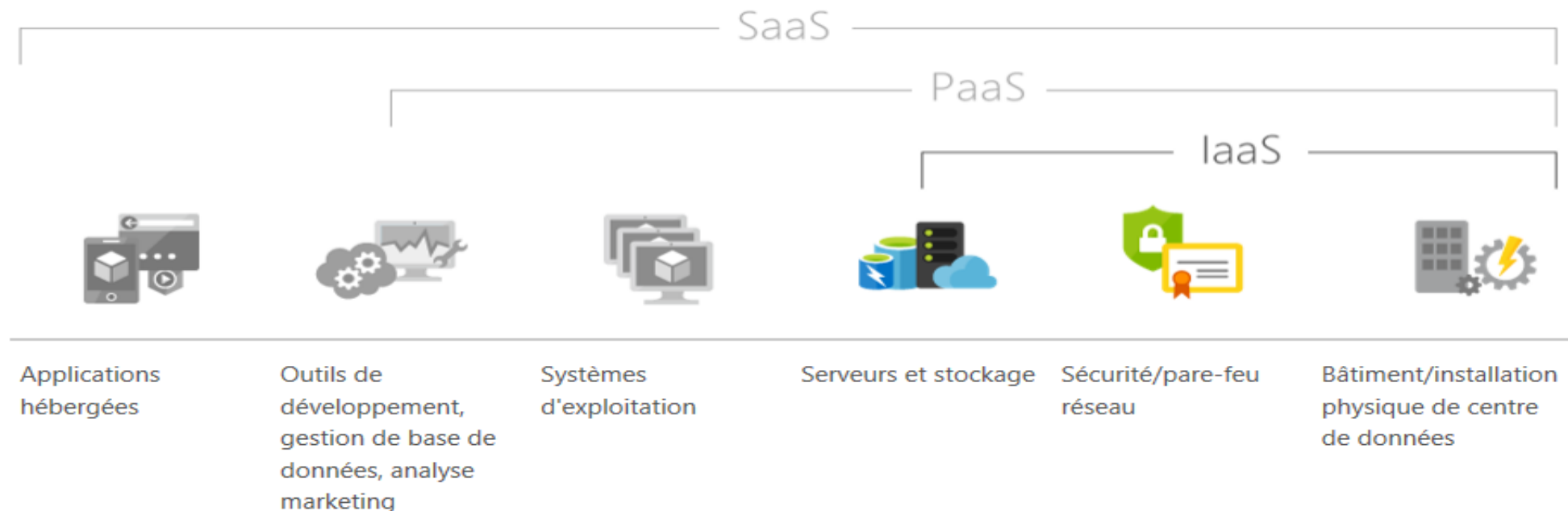
Cloud Computing : IaaS

- Paiement en fonction de l'utilisation d'une infrastructure informatique (serveur, machines virtuelles, stockage, réseaux) auprès d'un fournisseur de services cloud



Cloud Computing : PaaS

- PaaS est conçu pour offrir un environnement à la demande permettant aux développeurs de créer rapidement des applications web ou mobiles par exemple sans avoir à se préoccuper de la configuration ou de la gestion de l'infrastructure de serveurs

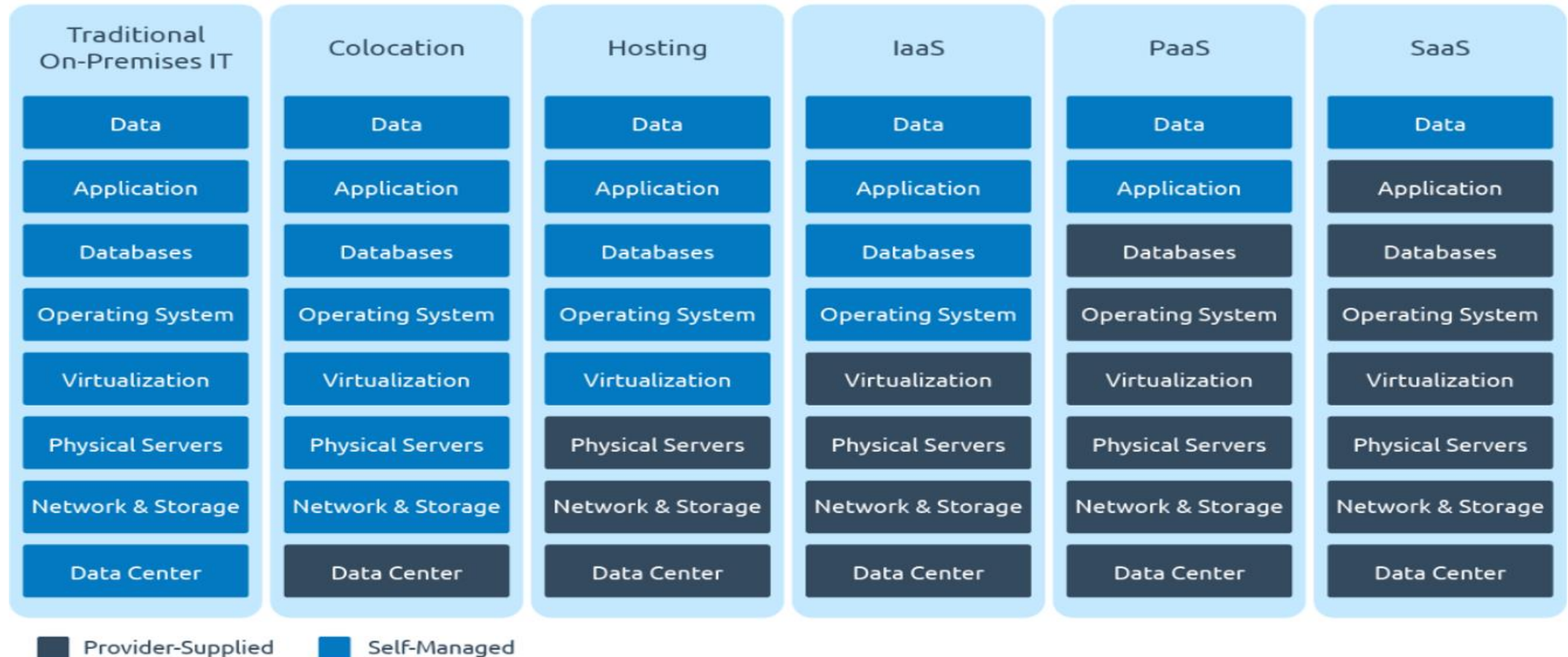


Cloud Computing : SaaS

- ❑ Avec le SaaS, les fournisseurs de services cloud hébergent et gèrent les applications logicielles et l'infrastructure sous-jacente, et gèrent la maintenance, par exemple la mise à niveau des logiciels et l'application des correctifs de sécurité.
- ❑ Le SaaS offre une solution logicielle complète pour laquelle vous payez en fonction de l'utilisation à un fournisseur de services cloud.



Cloud: les niveaux de responsabilités



Cloud computing: public, privé, hybride

☐ Cloud public

- Les clouds publics sont exploités par un fournisseur de services cloud, qui propose des ressources de calcul via Internet.

☐ Cloud privé

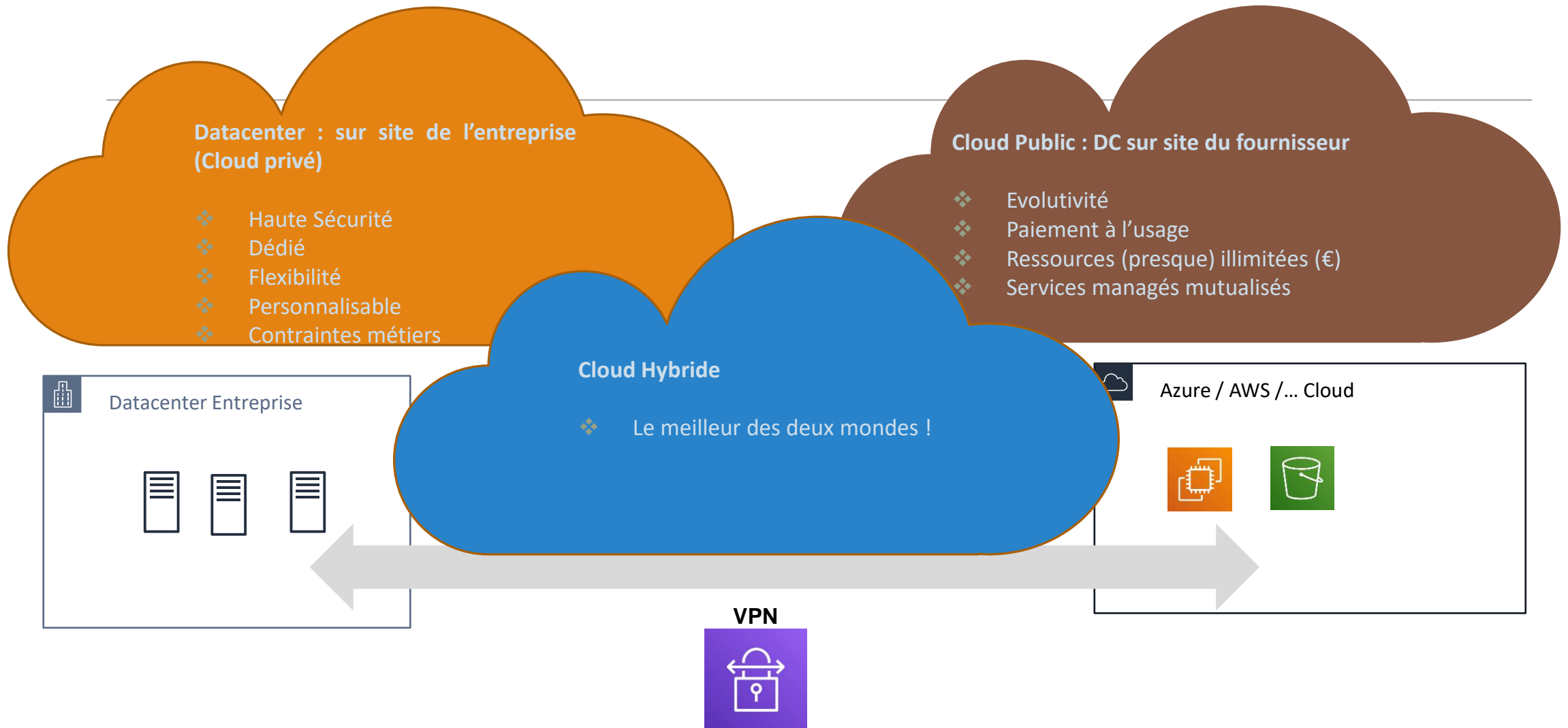
- Le cloud privé est l'ensemble des ressources de cloud computing utilisées de façon exclusive par une entreprise ou une organisation. Les services et l'infrastructure se trouvent sur un réseau privé.

☐ Cloud hybride

- Regroupe des clouds publics et privés, liés par une technologie leur permettant de partager des données et des applications.



Une architecture hybride ?



Cloud dans les entreprises

- ☐ Amazon AWS
- ☐ Microsoft Azure
- ☐ Google Cloud Plateforme
- ☐ IBM Cloud
- ☐ Oracle Cloud
- ☐ Alibaba Cloud

Microsoft Azure

Cloud Microsoft Azure est celui que nous allons étudier



Micorost Azure – Services Cloud

□ Microsoft Azure est composé d'une gamme croissante de services cloud intégrés

- Services d'infrastructure
 - ✓ Calcul (Machines virtuelles, VM Scale Sets, Containers et Azure Kubernetes)
 - ✓ Mise en réseau (Réseaux virtuels, Load balancer, App Gateway, VPN)
 - ✓ Stockage (Comptes de stockage, Sauvegarde)
- Monitoring d'infrastructure (Azure Monitor, Log Analytics Workspace)
- Sécurité et gestion (Security Center, Key Vault, Automation, Active Directory, RBAC, Policy)

Micorost Azure – Services Cloud

- Bases de données (SQL databases, CosmosDB)
- Services d'applications (Web Apps, Logic Apps, Function Apps)
- Intelligence artificielle (Services Bot)
- Analytique et IoT (PowerBI, Machine leaning, IoT Hub)
- Service de développement (Visual Studio, DevOps)

Microsoft Azure -- Régions

60+ régions à l'échelle mondiale **140** disponible dans 140 pays



Microsoft Azure -- Régions

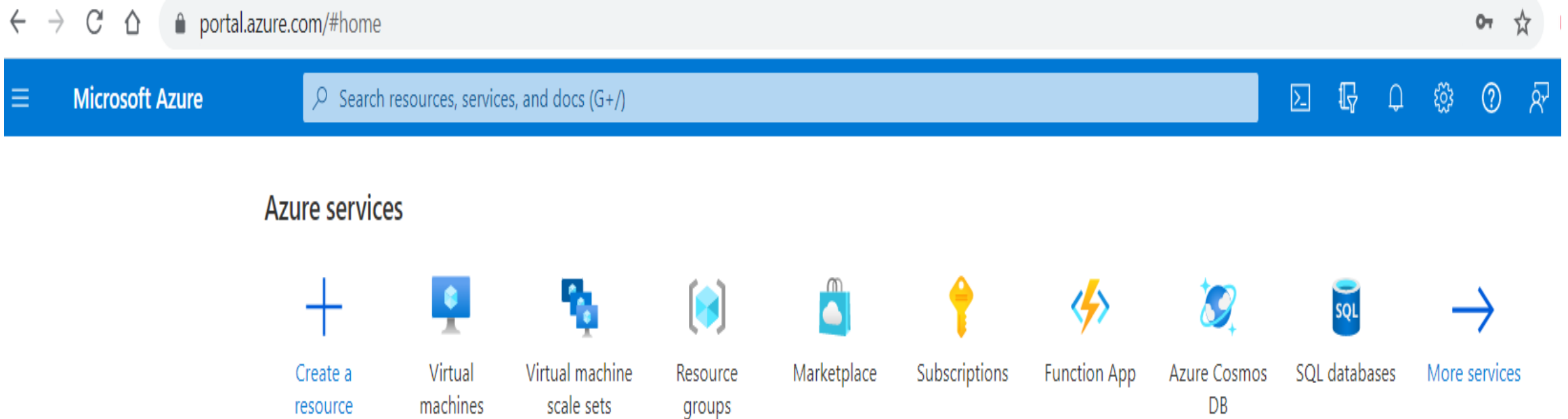
- ❑ Une région est constituée d'un ensemble de centres de données déployés dans un périmètre défini
- ❑ Azure offre aux clients la possibilité de déployer des applications là où ils en ont besoin
- ❑ Explorez les produits disponibles par région

<https://azure.microsoft.com/fr-fr/explore/global-infrastructure/products-by-region/>

Microsoft Azure -- Zones de disponibilité

- ❑ Les zones de disponibilité sont des emplacements physiquement séparés au sein d'une région Azure.
- ❑ Chaque zone de disponibilité est composée d'un ou de plusieurs datacenters équipés d'alimentation, de refroidissement et de réseau indépendants.
- ❑ Les zones de disponibilité permettent d'exécuter des applications stratégiques en bénéficiant d'une haute disponibilité et d'une réplication à faible latence.

Le portail Azure



Le portail Azure

□ Le portail vous permet d'accéder graphiquement à Microsoft Azure

- Rechercher des ressources, des services, des documents
- Manager vos ressources
- Créer vos propres tableaux de bords
- Accéder à cloud Shell
- ...

Azure Shell et Azure CLI

☐ Azure Cloud Shell est un shell interactif accessible par navigateur pour la gestion des ressources Azure

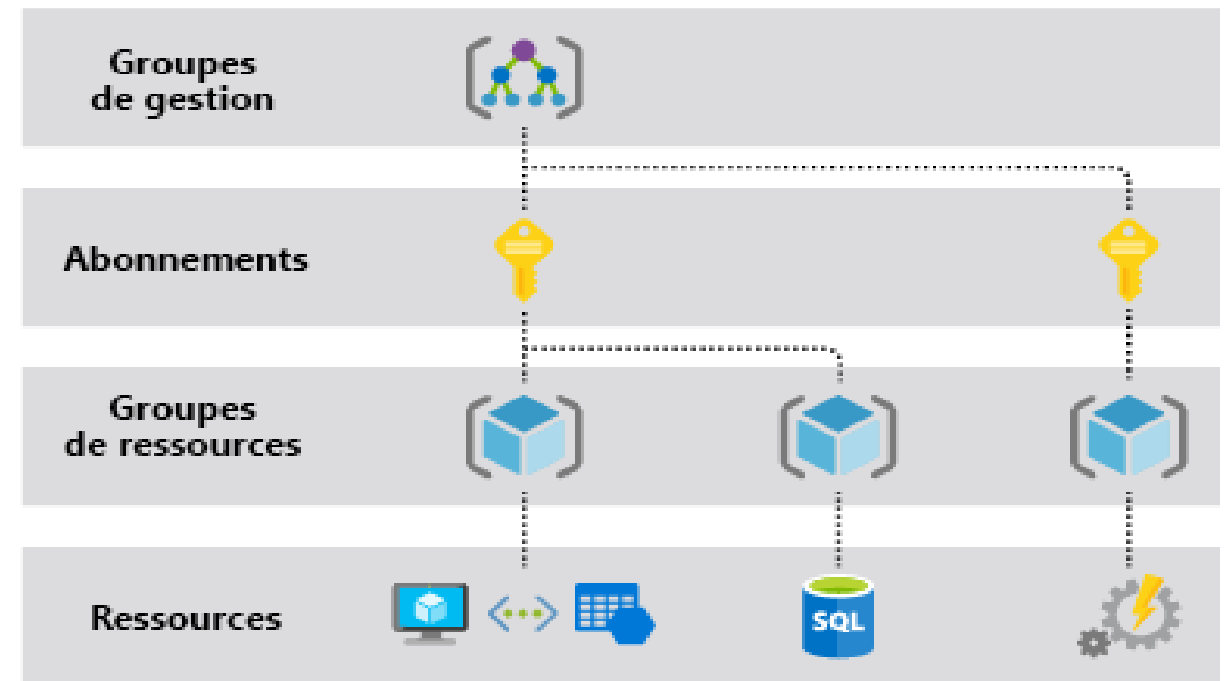
- Les utilisateurs de Linux peuvent opter pour un Bash
- Les utilisateurs de Windows peuvent opter pour PowerShell

☐ Azure CLI

- L'interface de ligne de commande Azure (Azure CLI) est un ensemble de commandes qui sert à créer et à gérer des ressources Azure.

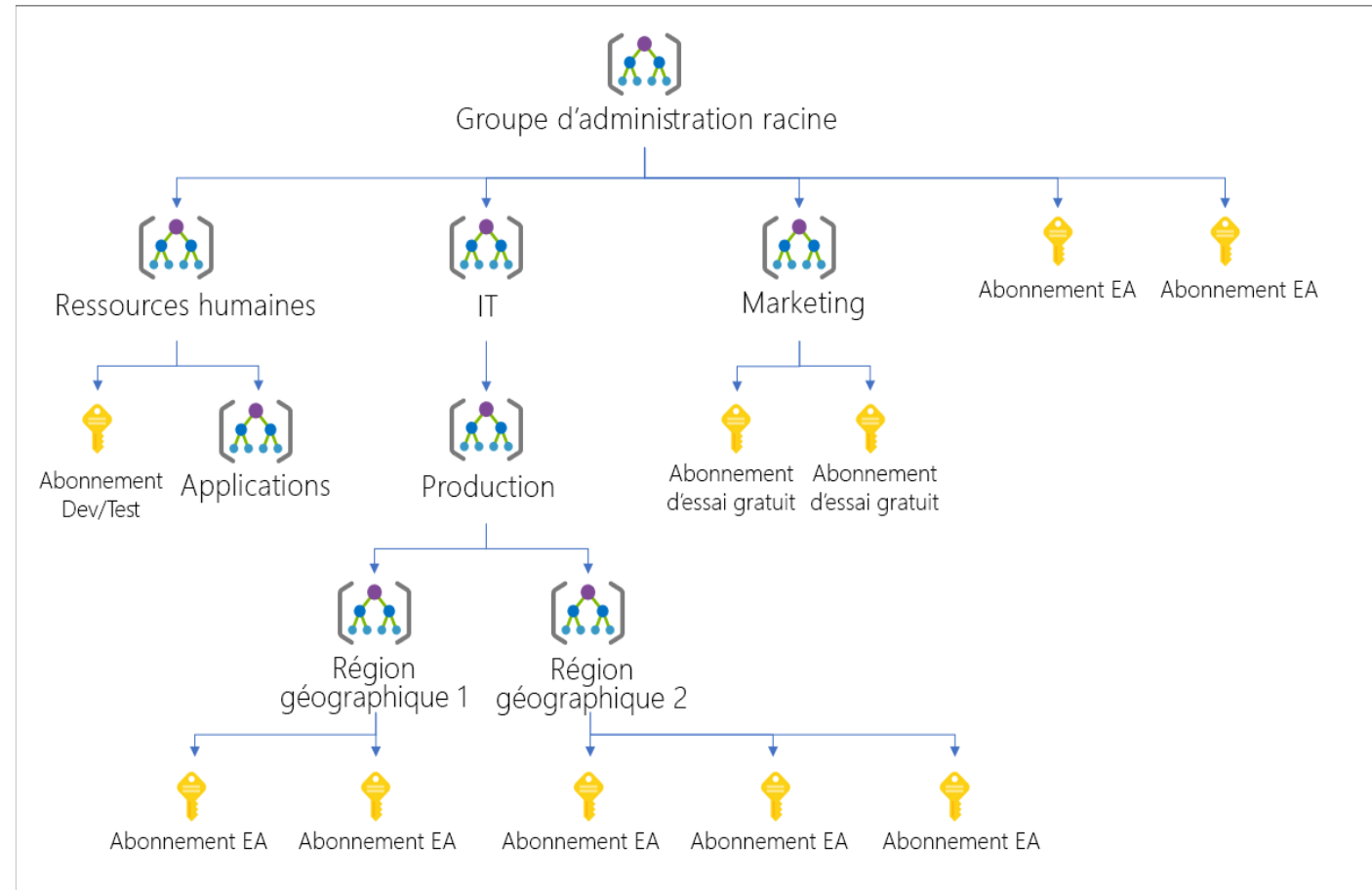
Architecture de Microsoft Azure

- ❑ Azure fournit quatre niveaux d'étendue :
 - Groupes d'administration (Management Groups)
 - Abonnements (Subscriptions)
 - Groupes de ressource (Resource Groups)
 - Ressources (Resources)



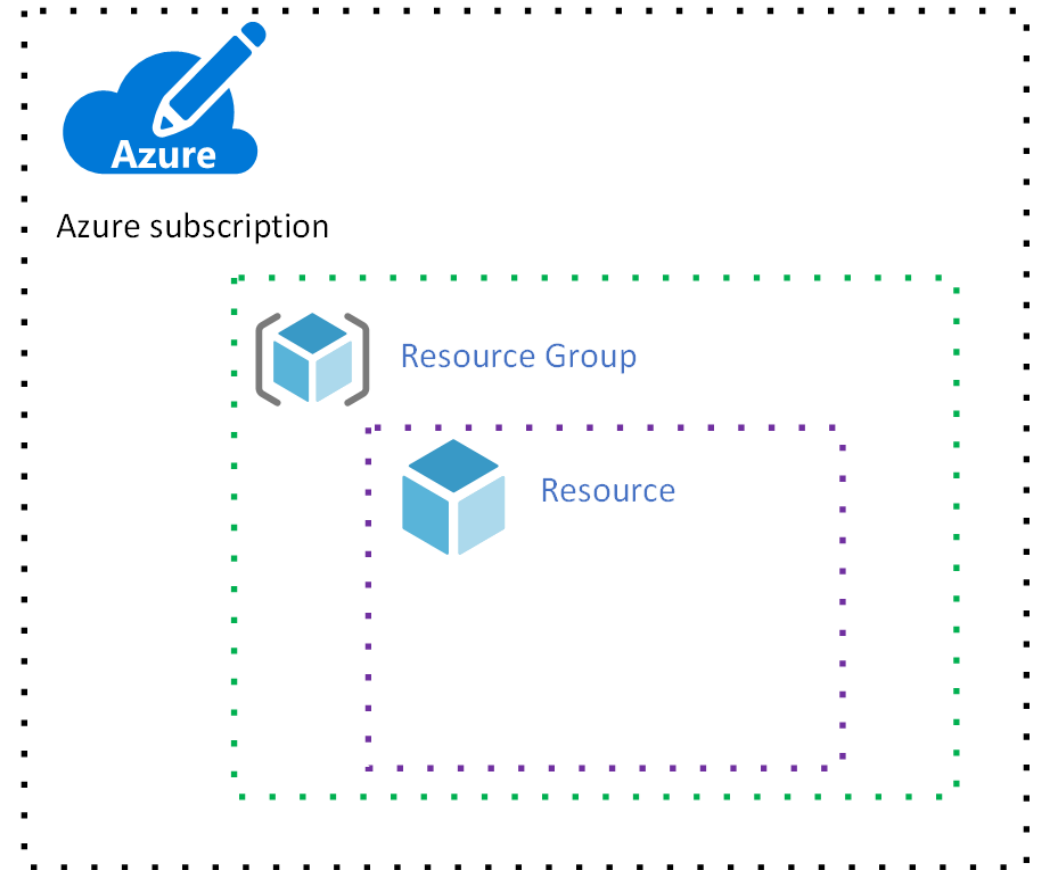
Microsoft Azure -- Les groupes d'administration (Management Group)

❑ Les groupes d'administration sont des conteneurs qui vous aident à gérer l'accès et la stratégie dans plusieurs abonnements



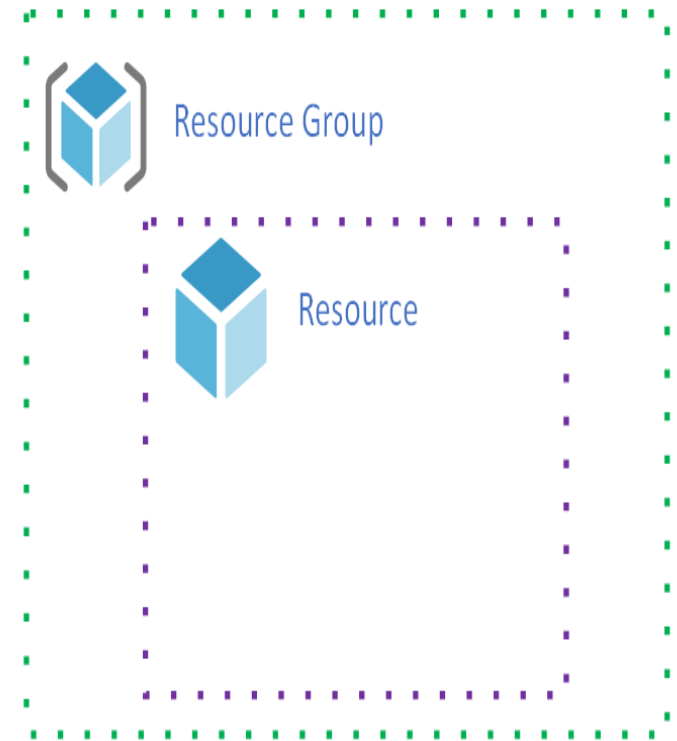
Microsoft Azure -- Les abonnements

□ Il s'agit d'une construction logique qui regroupe des groupes de ressources et leurs ressources.



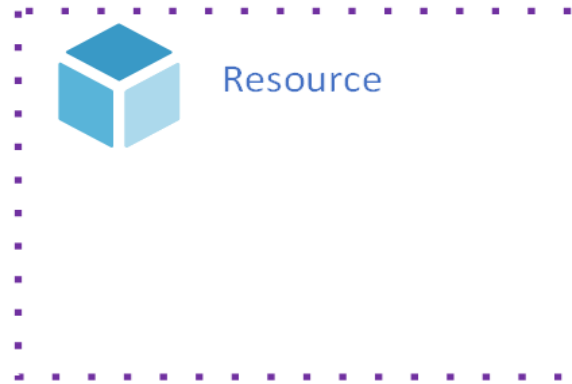
Microsoft Azure -- Les groupes de ressources

- ❑ Chaque ressource dans Azure doit appartenir à un groupe de ressources
- ❑ Un groupe de ressources est simplement une construction logique qui regroupe plusieurs ressources afin qu'elles puissent être gérées en tant qu'entité unique en fonction du cycle de vie et des aspects de sécurité. Par exemple, des ressources qui partagent un cycle de vie similaire, tels que les ressources d'une application, peuvent être créées ou supprimées en tant que groupe.



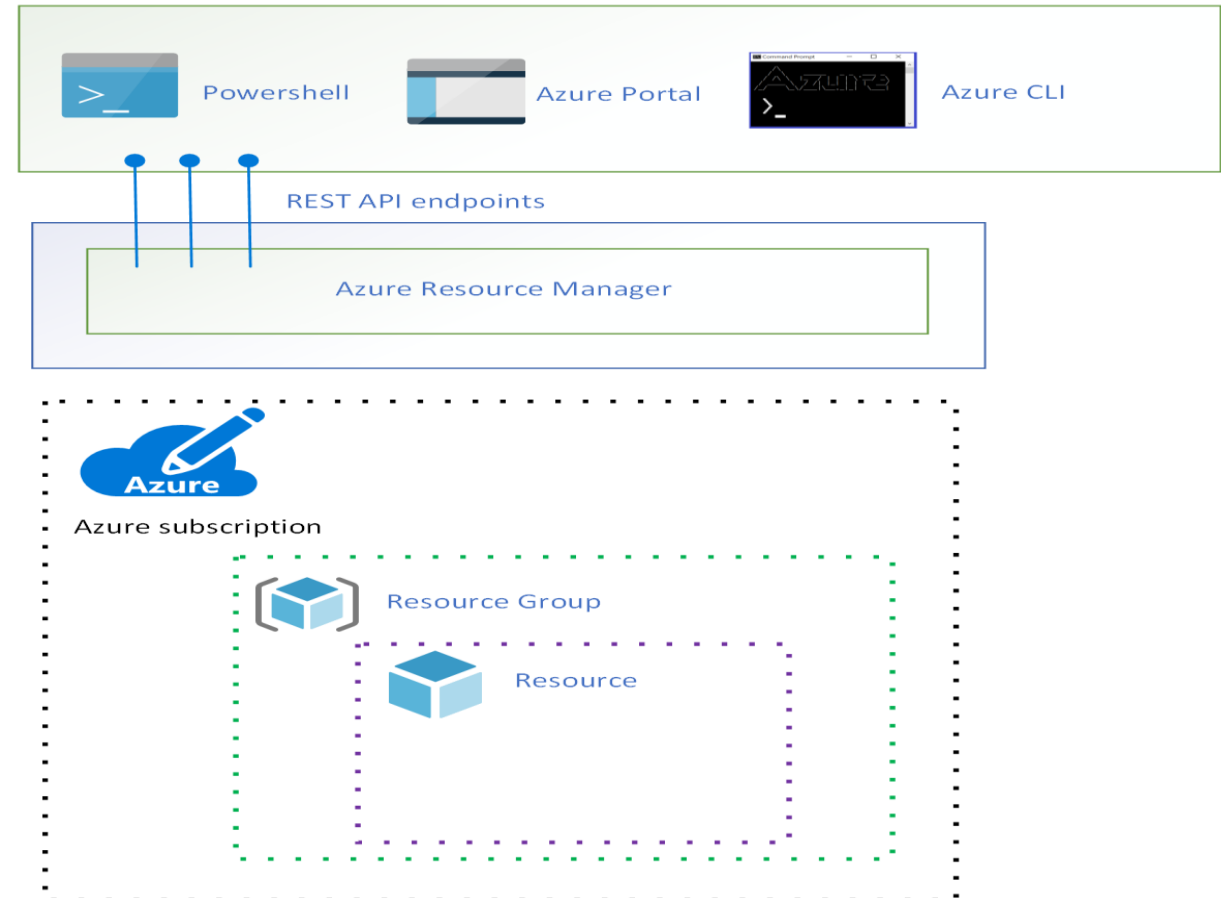
Microsoft Azure – Les ressources

- ❑ Le terme ressource fait référence à une entité gérée par Azure. Par exemple, les machines virtuelles, les réseaux virtuels et les comptes de stockage sont tous considérés comme des ressources Azure.



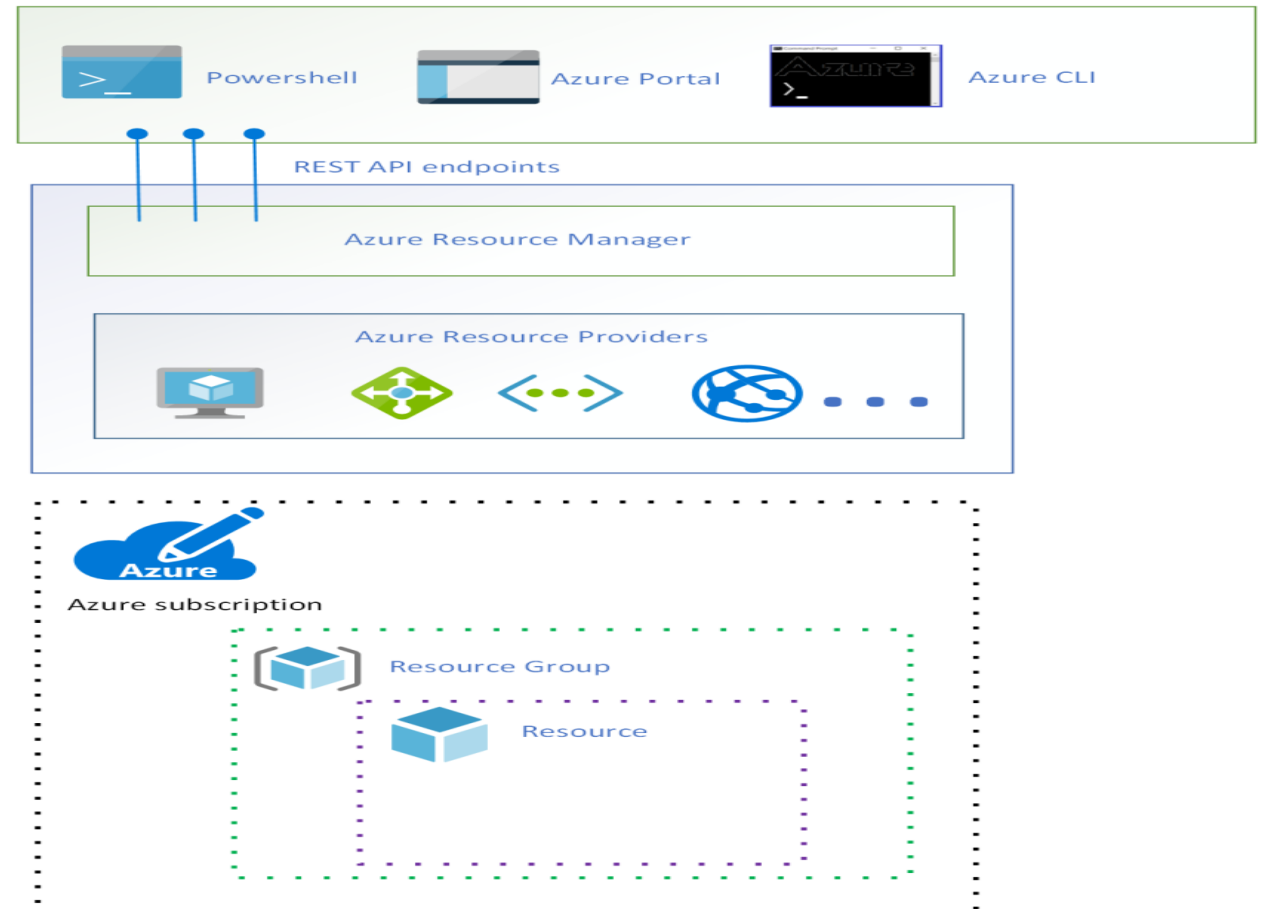
Microsoft Azure – Azure Ressource Manager

- ❑ Azure comprend un front end avec de nombreux services qui orchestrent toutes les fonctions d'Azure



Microsoft Azure – Azure Ressource Manager

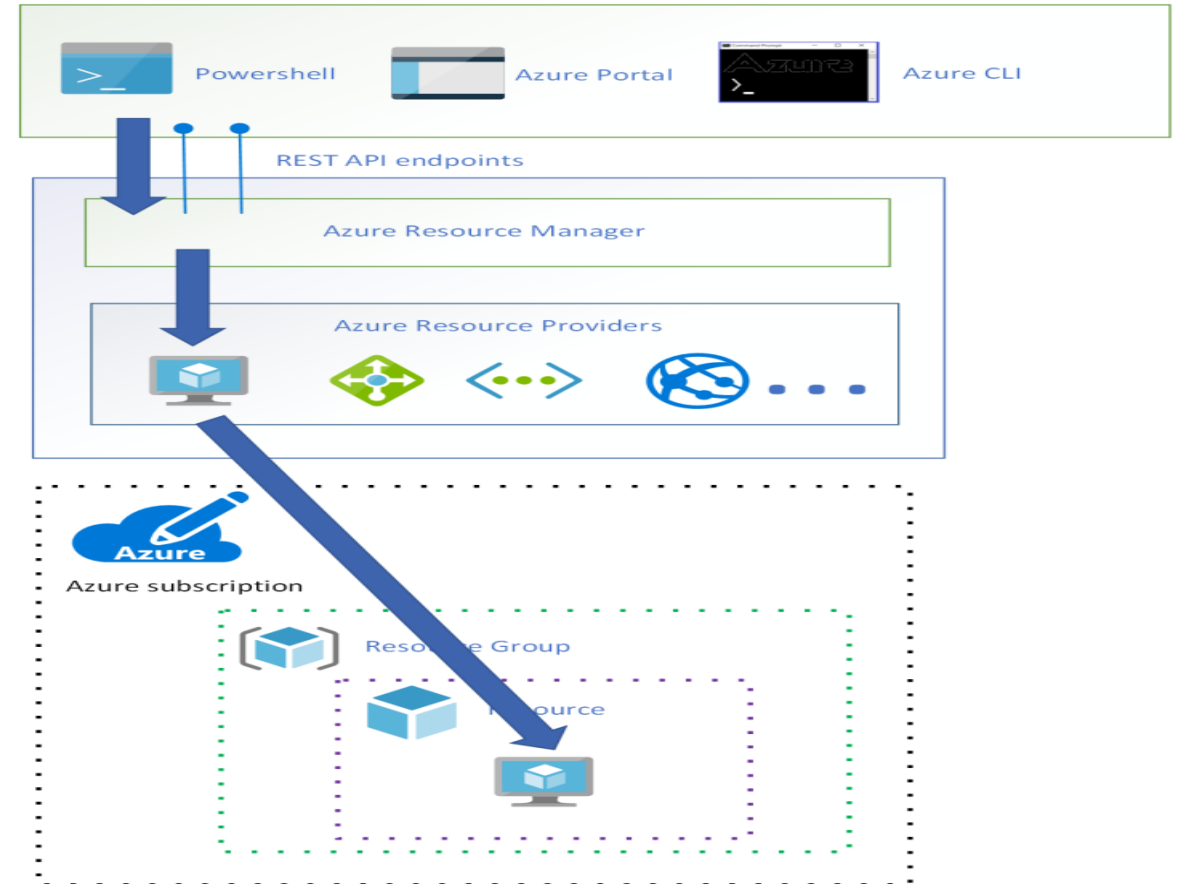
- ❑ Les clients (Portail, powershell , AZ Cli, ...) se connectent à Azure Resource Manager à l'aide de l'API REST.
- ❑ Azure Resource Manager n'inclut pas de fonctionnalités permettant de gérer directement les ressources.
 - Au lieu de cela, la plupart des types de ressources Azure ont leur propre **fournisseur de ressources** (Azure Resource Providers).



Microsoft Azure – Azure Resource Manager

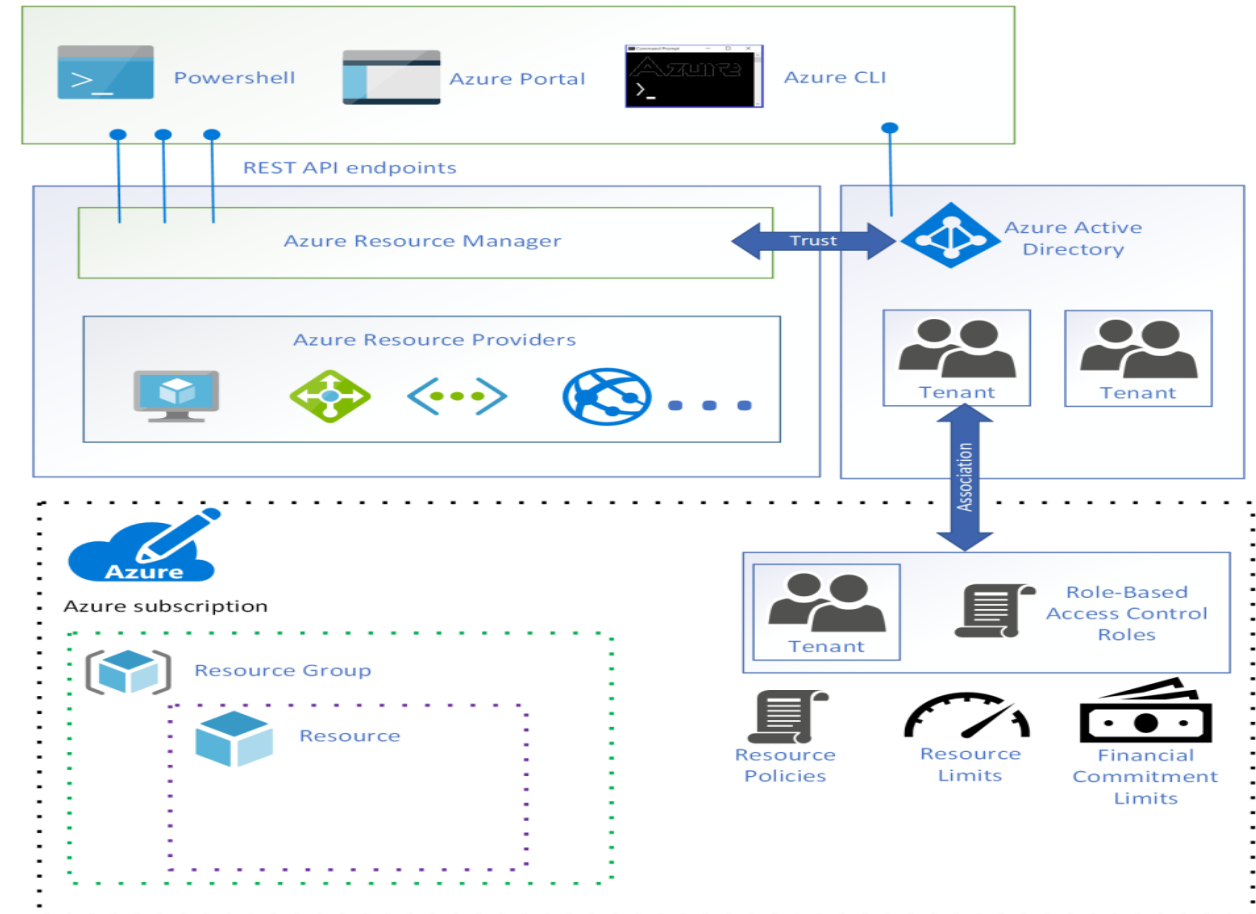
❑ Quand un client effectue une requête pour gérer une ressource spécifique, Azure Resource Manager se connecte au fournisseur de ressources pour ce type de ressources afin d'exécuter la requête.

- Par exemple, si un client effectue une requête pour gérer une ressource de machine virtuelle, Azure Resource Manager se connecte au fournisseur de ressources Microsoft.Compute



Microsoft Azure – Azure Resource Manager

- ❑ Azure Resource Manager exige du client qu'il spécifie un identificateur pour l'abonnement et le groupe de ressources, afin de gérer la ressource
- ❑ Chaque requête du client pour gérer une ressource dans un abonnement spécifique requiert que l'utilisateur dispose d'un compte dans le client Azure AD associé
- ❑ On vérifie aussi que l'utilisateur dispose des autorisations suffisantes pour effectuer la requête
- ❑ Un rôle RBAC spécifie un ensemble d'autorisations qu'un utilisateur peut utiliser pour une ressource spécifique
- ❑ Un contrôle vérifie aussi que la requête ne dépasse pas une limite d'abonnement Azure



Microsoft Azure – Déploiement

- ❑ Avec la migration vers le cloud, vous pouvez automatiser les déploiements et utiliser la pratique de l'infrastructure en tant que code
- ❑ Dans le code, vous définissez l'infrastructure qui doit être déployée
- ❑ Pour implémenter une infrastructure en tant que code pour vos solutions Azure, utilisez des modèles Azure Resource Manager (ARM).
- ❑ Modèle Resource Manager : fichier JSON (JavaScript Objet Notation) qui définit une ou plusieurs ressources à déployer vers un groupe de ressources. Il définit également les dépendances entre les ressources déployées.

Les machines virtuelles sous Azure

❑ Présentation des machines virtuelles sous Azure

❑ Les disques managés

❑ La haute disponibilité

❑ Les VMSS (Virtual Machine Scale Set)

Les machines virtuelles sous Azure

- Présentation des machines virtuelles

Présentation des machines virtuelles

- Les Machines Virtuelles Azure sont l'un des nombreux types de ressources informatiques évolutives et à la demande proposés par Azure
 - Une machine virtuelle Azure vous donne la flexibilité de la virtualisation sans que vous ayez à acheter le matériel physique qui exécute la machine virtuelle ni à en assurer la maintenance
 - Toutefois, vous devez toujours assurer la maintenance de la machine virtuelle en effectuant des tâches comme la configuration et l'installation des logiciels qui s'exécutent dessus.

Présentation des machines virtuelles

❑ A quoi dois-je penser avant de créer une machine virtuelle ?

- Le nom de vos ressources,
- L'emplacement de stockage des ressources,
- La taille de la machine virtuelle,
- Le nombre de machines virtuelles qui peuvent être créées,
- Le système d'exploitation de la machine virtuelle,
- La configuration de la machine virtuelle et les ressources liées dont a besoin la machine virtuelle

Présentation des machines virtuelles

□ Taille des machines virtuelles

- **Usage général** (B, Av2,...). Ratio processeur/mémoire équilibré. Idéal pour le test et le développement, les bases de données petites à moyennes et les serveurs web au trafic faible à moyen
- **Optimisé pour le calcul** (Fsv2, F,...). Ratio processeur/mémoire élevé. Convient pour les serveurs web au trafic moyen, les appareils réseau, les processus de traitement par lots et les serveurs d'application
- **Mémoire optimisée** (E2as, E2ads,...). Ratio mémoire/cœur élevé. Idéal pour les serveurs de base de données relationnelle, les caches moyens à grands et l'analytique en mémoire
- **Optimisée pour le stockage** (L8as, L8s,...). Débit de disque et E/S élevés. Idéale pour les bases de données NoSQL, SQL et Big Data.
- **GPU** (NC, NCsv2,...). Machines virtuelles spécialisées conçues pour les opérations graphiques lourdes et la retouche vidéo disponibles avec un ou plusieurs processeurs graphiques
- **Calcul haute performance** (H, HB,...). Nos machines virtuelles les plus rapides et dotées des processeurs les plus puissants avec interfaces réseau haut débit en option (RDMA).

Présentation des machines virtuelles

- ❑ Le support des machines virtuelles de 2e génération est disponible dans Azure
 - Les fonctionnalités incluent la mémoire augmentée, Intel Software Guard Extensions (Intel SGX) et mémoire persistante virtualisée (vPMEM)
 - Les machines virtuelles de 2e génération utilisent la nouvelle architecture de démarrage basée sur UEFI alors que les machines virtuelles de 1ère génération utilisaient l'architecture basée sur le BIOS. Comparées aux machines virtuelles de 1ère génération, les machines virtuelles de 2e génération peuvent avoir des temps d'installation et de démarrage améliorés.

Les machines virtuelles sous Azure

- Extensions: Les extensions de machines virtuelles étendent les fonctionnalités de votre machine virtuelle par le biais de la configuration post déploiement et de tâches automatisées. Ces tâches courantes peuvent être accomplies à l'aide des extensions :
 - Déployer et gérer des configurations : l'extension de configuration d'état souhaité (DSC) vous permet de configurer DSC sur une machine virtuelle pour gérer les environnements et les configurations
 - Collecter les données de diagnostic : l'extension des diagnostics Azure vous permet de configurer la machine virtuelle de sorte qu'elle collecte des données de diagnostics utilisées pour surveiller l'intégrité de votre application

Présentation des machines virtuelles

❑ Les ressources suivantes doivent généralement être créées ou exister lors de la création de la machine virtuelle

Ressource	Requis	Description
Groupe de ressources	Oui	La machine virtuelle doit être contenue dans un groupe de ressource
Compte de stockage	Oui	La machine virtuelle doit stocker ses disques durs virtuels dans le compte de stockage
Réseau virtuel	Oui	La machine virtuelle doit faire partie d'un réseau virtuel.
Adresse IP publique	Non	La machine virtuelle peut avoir une adresse IP publique pour être accessible à distance
Interface réseau	Oui	La machine virtuelle a besoin de l'interface réseau pour communiquer sur le réseau
Disques de données	Non	La machine virtuelle peut comprendre des disques de données pour développer ses capacités de stockage

Présentation des machines virtuelles

- ❑ Se connecter à la machine virtuelle
 - Vous utilisez le bouton Connecter dans le Portail Azure pour démarrer par exemple une session Bureau à distance (RDP)

- ❑ Les noms DNS sont des paramètres facultatifs qui peuvent être spécifiés sur une ressource d'adresse IP publique. Le nom de domaine complet se présente au format suivant :
<domainlabel>.<region>.cloudapp.azure.com.

Les machines virtuelles sous Azure

□ Les disques managés

Les disque managés

- ❑ La fonctionnalité Disques managés se charge de la création et de la gestion du compte de stockage Azure en arrière plan
- ❑ Vous spécifiez le disque (Standard ou Premium) et Azure crée et gère le disque
- ❑ Vous pouvez également gérer le compte de stockage et les utiliser pour les machines virtuelles

Les disque managés

□ Type de disque:

- **HDD Standard:** Sauvegarde, non critique, accès peu fréquent
 - 32 767 Gio, 500 Mo/s, 2 000 E/S par seconde
- **SSD Standard:** Serveurs web, applications d'entreprise peu utilisées et Dev/Test
 - 32 767 Gio, 750 Mo/s, 6 000 E/S par seconde
- **SSD Premium :** Charges de travail de production et sensibles aux performances
 - 32 767 Gio, 900 Mo/s, 20 000 E/S par seconde
- **SSD Premium v2:** Charges de travail de production et sensibles aux performances qui nécessitent systématiquement une latence faible et un débit élevé
 - 65 536 Gio, 1200 Mo/s, 80 000 E/S par seconde
- **Disque Ultra:** Charges de travail gourmandes en E/S, telles que les bases de données de niveau supérieur (par exemple, SQL et Oracle), et autres charges de travail très lourdes en transactions
 - 65 536 Gio, 4000 Mo/s, 160 000 E/S par seconde

Les disque managés

❑ Rôles de disque:

- **Disque de système d'exploitation:** Chaque machine virtuelle dispose d'un disque de système d'exploitation attaché. Ce disque de système d'exploitation est doté d'un système d'exploitation préinstallé qui a été sélectionnée lors de la création de la machine virtuelle.
- **Disque temporaire:** Chaque machine virtuelle contient un disque temporaire qui n'est pas un disque managé. Il fournit un stockage à court terme pour les applications et les processus, et est destiné à stocker seulement des données comme les fichiers de pagination ou d'échange. Les données présentes sur le disque temporaire peuvent être perdues lors d'un événement de maintenance ou quand vous redéployez une machine virtuelle. Lors d'un redémarrage standard réussi de la machine virtuelle, les données présentes sur le disque temporaire sont conservées.
- **Disque de données:** Un disque attaché à une machine virtuelle pour stocker des données d'application ou d'autres données que vous devez conserver.

Les disque managés

□ Chiffrement:

- Les disques managés Azure chiffrent automatiquement vos données au repos par défaut lors de leur conservation dans le cloud.
- Le chiffrement Stockage Azure n'a pas d'impact sur les performances des disques managés et n'entraîne aucun coût supplémentaire
- Le chiffrement côté serveur (chiffrement est activé sur l'hôte) protège vos données et vous aide à honorer les engagements en matière de sécurité et de conformité

Les machines virtuelles sous Azure

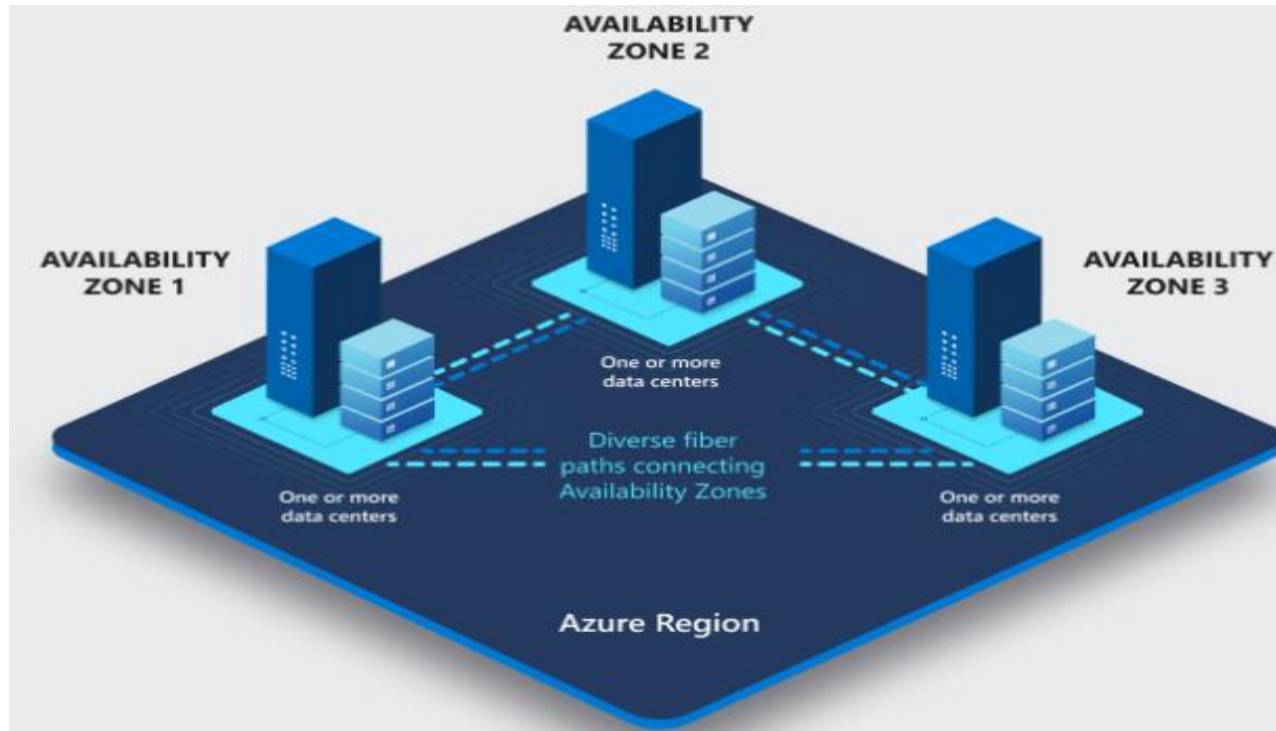
□ La haute disponibilité

Haute disponibilité

- ❑ En mettant en œuvre des solutions de hautes disponibilités (HA), les charges de travail sont généralement réparties sur différentes machines virtuelles afin d'obtenir un débit et des performances élevées, et pour créer une redondance au cas où une machine virtuelle serait affectée en raison d'une mise à jour ou d'un autre événement.
- ❑ Azure propose de nombreuses options pour obtenir une haute disponibilité.
 - Zones de disponibilité (Availability zone)
 - Groupe à haute disponibilité (Availability Set)
 - Domaines d'erreur (Fault domains)
 - Domaines de mise à jour (Update domain)

Zones de disponibilité (Availability zone)

- ❑ Une zone de disponibilité est une zone physiquement séparée au sein d'une région Azure
- ❑ On distingue trois zones de disponibilité par région Azure.



Groupe à haute disponibilité (Availability Set)

- ❑ Un groupe à haute disponibilité (Availability Set) est un regroupement logique de machines virtuelles afin de garantir la redondance et la disponibilité
- ❑ Chaque machine virtuelle de votre groupe à haute disponibilité se voit attribuer un domaine de mise à jour et un domaine d'erreur

Domaines d'erreur (Fault domains) et Domaines de mise à jour (Update domain)

❑ Domaines d'erreur

- Un domaine d'erreur est un groupe logique de matériels sous jacents qui partagent la même source d'alimentation et le même commutateur réseau, par exemple un rack dans un centre de données

❑ Domaines de mise à jour

- Un domaine de mise à jour est un groupe logique de matériels sous jacents qui peuvent faire l'objet d'une opération de maintenance ou être redémarrés en même temps
- Cette approche garantit qu'au moins une instance de votre application reste toujours en cours d'exécution, car la plateforme Azure fait l'objet d'une maintenance périodique
- Un seul domaine de mise à jour peut être redémarré à la fois.

Les groupes de placements de proximité

□ Proximity placement group

- Lors du déploiement de votre application dans Azure, la répartition des instances sur différentes régions ou zones de disponibilité crée une latence réseau, ce qui peut avoir un impact sur les performances globales de votre application
- Une seule zone de disponibilité peut s'étendre sur plusieurs centres de données physiques, ce qui peut entraîner une latence réseau qui peut affecter votre application.
- Pour que les machines virtuelles soient aussi proches que possible, avec la latence la plus faible possible, déployez-les dans un groupe de placements de proximité.

Les machines virtuelles sous Azure

□ Les VMSS (Virtual Machine Scale Set)

Les VMSS (Virtual Machine Scale Set)

- ❑ Pour offrir une redondance et de meilleures performances, les applications sont généralement réparties sur plusieurs instances
 - Un équilibreur de charge qui distribue les requêtes à l'une des instances de l'application
 - La mise à l'échelle automatique et un équilibrage de charge du trafic (Augmenter automatiquement le nombre d'instances de machine virtuelle lorsque la demande de l'application augmente, et le réduire lorsque la demande diminue)

- ❑ Toutes les instances de VM sont créées à partir de la même image d'OS de base et de la même configuration

Les réseaux virtuels sous Azure

- ❑ Présentation des réseaux virtuels
- ❑ Le peering de réseaux virtuel
- ❑ Les équilibreurs de charge (Load Balancer)
- ❑ Les NSG (Network Security Group)
- ❑ Les VPN

Les réseaux virtuels sous Azure

□ Présentation des réseaux virtuels

Présentation des réseaux virtuels

- ❑ Le réseau virtuel Azure (VNet) est le bloc de construction fondamental pour votre réseau privé dans Azure. Le réseau virtuel permet à de nombreux types de ressources Azure, telles que les VM, de communiquer de manière sécurisée entre elles, avec Internet et avec les réseaux locaux
- ❑ Un réseau virtuel est similaire à un réseau traditionnel que vous utiliseriez dans votre propre centre de données, mais avec les avantages supplémentaires de l'infrastructure Azure, tels que la mise à l'échelle et la disponibilité
- ❑ Un réseau virtuel s'étend à une seule région
- ❑ Un réseau virtuel est limité à un abonnement

Présentation des réseaux virtuels

❑ Isolement

- Les réseaux virtuels sont totalement isolés les uns des autres

❑ Accès à l'Internet public

- Toutes les VM d'un réseau virtuel ont accès à l'Internet public
- Vous pouvez contrôler l'accès grâce aux groupes de sécurité réseau (NSG)

❑ Accès aux machines virtuelles dans le réseau virtuel

- Les machines virtuelles se connectent entre elles avec des adresses IP privées, même si elles se trouvent dans des sous réseaux différents, et sans avoir recours à la configuration de routage

Présentation des réseaux virtuels

❑ Résolution de noms

- Azure fournit la résolution de noms pour les machines virtuelles déployées dans votre réseau virtuel.
- Vous pouvez également déployer vos propres serveurs DNS et configurer le réseau virtuel pour les utiliser.

❑ Sécurité

- Le trafic entrant et sortant des machines virtuelles dans un réseau virtuel peut être contrôlé à l'aide de groupes de sécurité du réseau

❑ Connectivité

- Les réseaux virtuels peuvent être connectés entre eux à l'aide de passerelles réseau.
- Les réseaux virtuels peuvent être connectés entre eux via des réseaux VPN site à site ou via Azure ExpressRoute

Présentation des réseaux virtuels

- ❑ Lors de la création d'un réseau virtuel, vous devez spécifier un espace d'adressage IP privé personnalisé
- ❑ Azure attribue aux ressources d'un réseau virtuel une adresse IP privée à partir de l'espace d'adressage que vous attribuez. Par exemple, si vous déployez une machine virtuelle dans un réseau virtuel avec l'espace d'adressage 10.0.0.0/23, la machine virtuelle reçoit une adresse IP privée telle que 10.0.0.4
- ❑ Les sous réseaux vous permettent de segmenter le réseau virtuel en sous réseaux, et d'allouer une partie de l'espace d'adressage du réseau virtuel à chaque sous réseau
- ❑ Il est recommandé d'avoir un petit nombre de grands réseaux virtuels plutôt qu'un grand nombre de petits réseaux virtuels. Cela empêche la surcharge de gestion.

Présentation des réseaux virtuels

Adresses IP

- Les adresses IP publiques permettent aux ressources Azure de communiquer avec Internet et d'autres services publics Azure
- Les adresses IP privées permettent la communication entre les ressources dans un réseau virtuel, au même titre que celles qui sont connectées via un VPN, sans utiliser des adresses IP routables par Internet.

Présentation des réseaux virtuels

❑ Les balises de services

- Microsoft gère les préfixes d'adresses englobés par l'étiquette de service et met à jour automatiquement l'étiquette de service quand les adresses changent, ce qui réduit la complexité des mises à jour fréquentes relatives aux règles de sécurité réseau
- Utilisez des étiquettes de service à la place des adresses IP spécifiques lors de la création de règles de sécurité
- En spécifiant le nom de l'étiquette de service (par exemple, **VirtualNetwork**) dans le champ Source ou Destination approprié d'une règle, vous pouvez autoriser ou refuser le trafic pour le service correspondant
- Les balises de services

<https://learn.microsoft.com/fr-fr/azure/virtual-network/service-tags-overview#available-service-tags>

Les réseaux virtuels sous Azure

- Le peering de réseaux virtuel

Le peering de réseaux virtuel

- ❑ Le peering de réseaux virtuels vous permet de connecter en toute transparence des réseaux de type virtuel network Azure
 - À l'instar du trafic entre les machines virtuelles du même réseau, le trafic est acheminé via le réseau privé de Microsoft uniquement

- ❑ Azure prend en charge les types de Peering suivants:
 - Connecte des réseaux virtuels au sein d'une même région Azure
 - Connecte des réseaux virtuels entre les différentes régions Azure

Le peering de réseaux virtuel

□ Avantages du peering de réseaux virtuels

- Connexion à latence faible et haut débit entre les ressources de différents réseaux virtuels.
- Possibilité pour les ressources d'un réseau virtuel de communiquer avec celles d'un autre réseau virtuel.
- Possibilité de transférer des données entre des réseaux virtuels dans des abonnements Azure, des locataires et des régions Azure.
- Le trafic réseau entre les réseaux virtuels est privé
- Le trafic entre les réseaux virtuels reste sur le réseau principal de Microsoft
- La latence du réseau entre des machines virtuelles de réseaux virtuels dans la même région est la même que celle d'un seul réseau virtuel

Le peering de réseaux virtuel

- Vous pouvez appliquer des groupes de sécurité réseau
 - Lors de la configuration du peering de réseaux virtuels, vous pouvez ouvrir ou fermer les règles du groupe de sécurité réseau entre les réseaux virtuels
 - Si vous ouvrez totalement la connectivité entre les réseaux virtuels appairés, vous pouvez appliquer des groupes de sécurité réseau pour bloquer ou refuser certains accès

Les réseaux virtuels sous Azure

□ Les équilibreurs de charge (Load Balancer)

Les équilibreurs de charge (Load Balancer)

□ Équilibreurs de charge Azure

- Équilibreur de charge externe

- Vous pouvez utiliser un équilibreur de charge externe pour fournir une haute disponibilité pour les machines virtuelles accessibles depuis l'Internet public

- Équilibreur de charge interne

- Vous pouvez utiliser un équilibreur de charge interne pour fournir une haute disponibilité pour les machines virtuelles accessibles depuis d'autres services sur votre réseau virtuel

Les équilibreurs de charge (Load Balancer)

□ Équilibreurs de charge Azure:

- Basic and Standard SKU

- Vous pouvez utiliser un équilibreur de charge avec SKU Basic ou Standard ou : Basic Load Balancer ou Standard Load Balancer.

<https://learn.microsoft.com/en-us/azure/load-balancer/skus>

- Gateway Load Balancer

- Des scénarios de haute performance et de haute disponibilité avec des appliances virtuelles réseau (NVA)
- Vous pouvez insérer des appliances de manière transparente pour différents types de scénarios (Firewalls, Advanced packet analytics, Intrusion detection and prevention systems, DDoS protection)

<https://learn.microsoft.com/en-us/azure/load-balancer/gateway-overview>

Les équilibreurs de charge (Load Balancer)

❑ Pourquoi utiliser Azure Load Balancer ?

- Azure Load Balancer vous permet de mettre à l'échelle vos applications et de créer des services à haut disponibilité
- Un équilibreur de charge offre une latence faible et un débit élevé, et peut augmenter l'échelle jusqu'à des millions de flux
- Équilibrer la charge du trafic interne et externe sur les machines virtuelles Azure
- Augmenter la disponibilité en répartissant les ressources au sein des zones et entre les zones
- Équilibrer la charge des services sur plusieurs ports et/ou plusieurs adresses IP
- Fournit des métriques via Azure Monitor. Elles fournissent des analyses sur les performances

Les équilibreurs de charge (Load Balancer)

□ La sécurité d'Azure Load Balancer

- Load Balancer est sécurisé par défaut
- Les équilibreurs de charge et les adresses IP publiques sont fermés aux flux entrants, sauf s'ils sont ouverts par des groupes de sécurité réseau
- Les groupes de sécurité réseau sont utilisés pour autoriser explicitement le trafic autorisé

Les réseaux virtuels sous Azure

□ Les NSG (Network Security Group)

Les NSG (Network Security Group)

- ❑ Vous pouvez utiliser un groupe de sécurité réseau Azure pour filtrer le trafic réseau à destination et en provenance des ressources Azure dans un réseau virtuel Azure
- ❑ Pour chaque règle, vous pouvez spécifier la source et la destination, le port et le protocole
- ❑ Vous pouvez associer zéro ou un groupe de sécurité réseau à chaque sous réseau de réseau virtuel et interface réseau dans une machine virtuelle
- ❑ Vous pouvez associer le même groupe de sécurité réseau à autant d'interfaces réseau individuelles et autant de sous réseaux que vous le souhaitez.

Les NSG (Network Security Group)

- ❑ Un groupe de sécurité réseau contient le nombre des règles souhaité dans les limites de l'abonnement Azure
- ❑ Chaque règle spécifie les propriétés suivantes

Les NSG (Network Security Group)

Propriété	Explication
Nom	Nom unique au sein du groupe de sécurité réseau.
Priorité	.Les règles sont traitées dans l'ordre croissant, car les nombres les plus faibles sont prioritaires.
Source ou destination	Tout, ou adresse IP (10.0.0.0/24, par exemple), une balise de service ou groupe de sécurité d'application individuelle.
Protocol	TCP, UDP, ICMP ou n'importe lequel
Sens	Indique si la règle s'applique au trafic entrant ou sortant.
Plage de ports	Vous pouvez spécifier un port individuel ou une plage de ports. Par exemple, indiquez 80 ou 10000-10005 .
Action	Autoriser ou refuser

Les NSG (Network Security Group)

❑ Exemple de règles de sécurité par défaut (Traffic entrant)

- **AllowVNetInBound**

Priority	Source	Ports source	Destination	Ports de destination	Protocol	Accès
65 000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Quelconque	Allow

- **AllowAzureLoadBalancerInBound**

Priority	Source	Ports source	Destination	Ports de destination	Protocol	Accès
65 001	AzureLoadBalancer	0-65535	0.0.0.0/0	0-65535	Quelconque	Allow

- **DenyAllInbound**

Priority	Source	Ports source	Destination	Ports de destination	Protocol	Accès
65 500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Quelconque	Deny

Les réseaux virtuels sous Azure

□ Les VPN

Les VPN

- Une passerelle VPN est un type spécifique de passerelle de réseau virtuel qui est utilisé pour envoyer du trafic chiffré entre un réseau virtuel Azure et un emplacement sur site via l'Internet public
 - Chaque réseau virtuel ne peut posséder qu'une seule passerelle VPN
 - Lorsque vous créez plusieurs connexions à la même passerelle VPN, tous les tunnels VPN partagent la bande passante de passerelle disponible

Les VPN

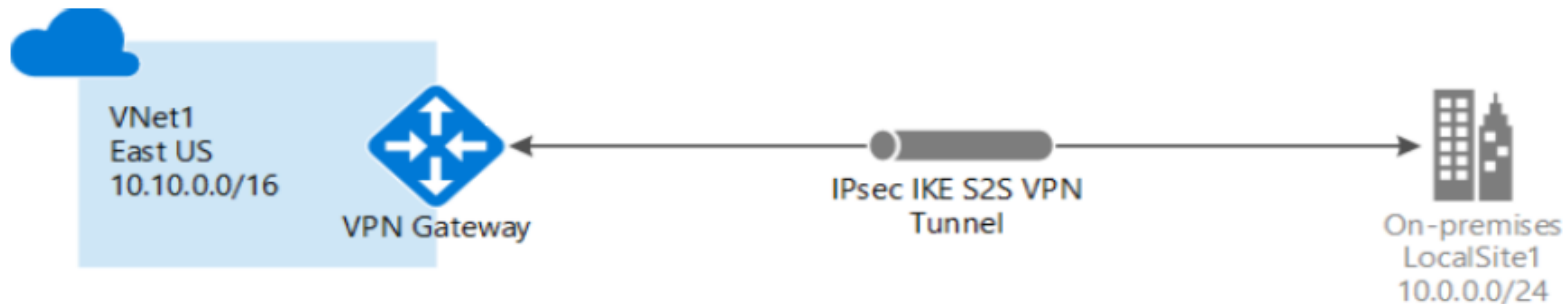
□ Les types de passerelles VPN sites à sites

- Connexions site à site (S2S)
- Connexions site à multi-sites
- Connexions point à site (P2S)
- Connexions de réseau virtuel à réseau virtuel

Les VPN

❑ Connexions site à site (S2S)

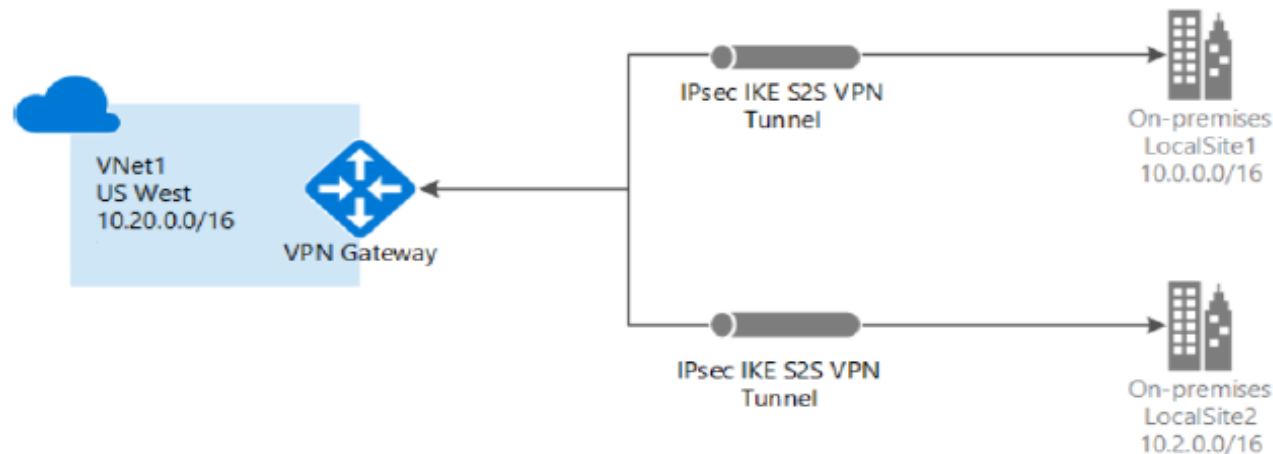
- Une connexion par passerelle VPN site à site (S2S) est une connexion via un tunnel VPN IPsec/IKE
- Les connexions S2S peuvent être utilisées entre différents locaux
- Une connexion site à site nécessite un appareil VPN local auquel est assignée une adresse IP publique



Les VPN

❏ Connexions site à multi-sites

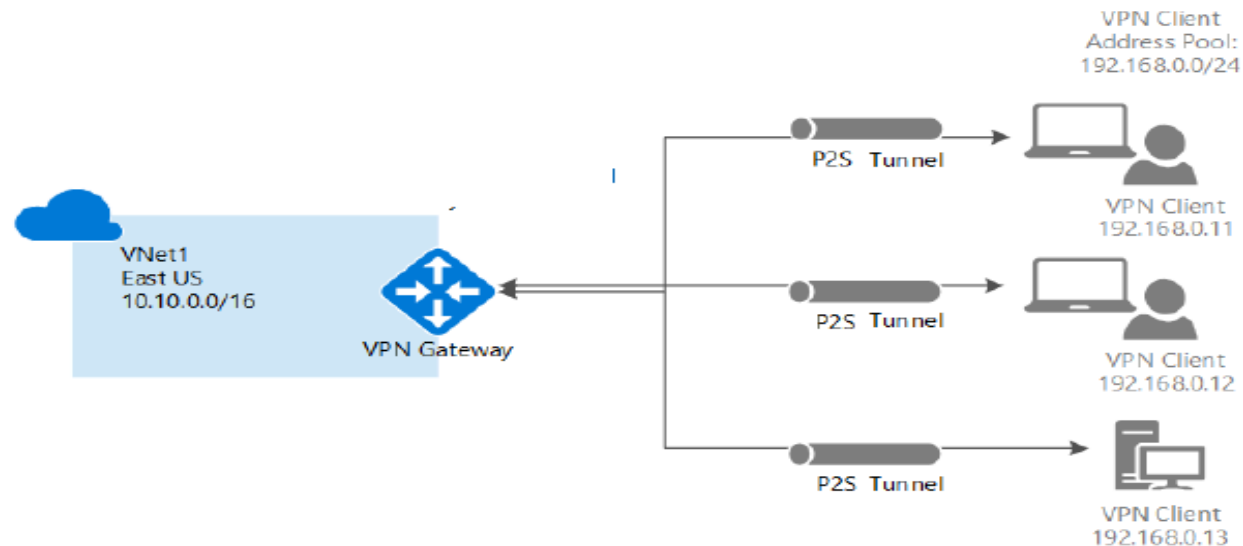
- Ce type de connexion est une variante de la connexion site à site
- Vous créez plusieurs connexions VPN à partir de votre passerelle de réseau virtuel, généralement en vous connectant à plusieurs sites locaux.



Les VPN

❏ Connexions point à site (P2S)

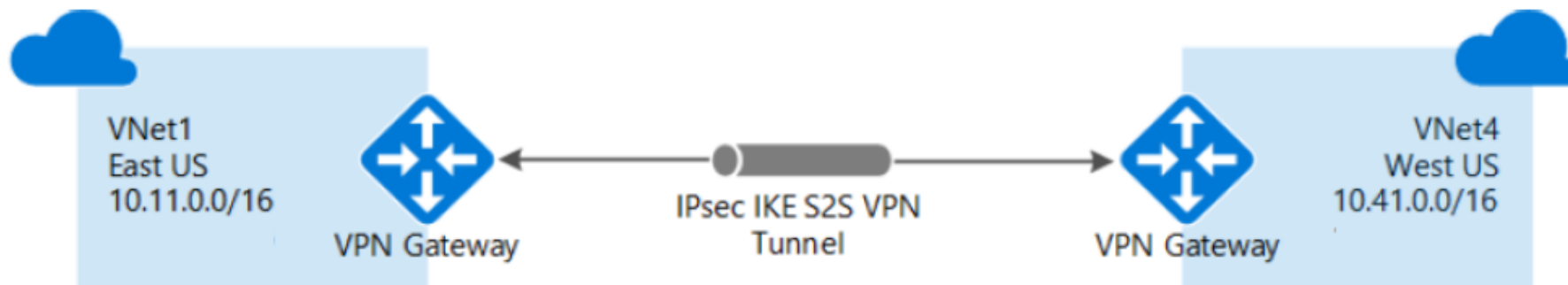
- Une connexion par passerelle VPN point à site (P2S) vous permet de créer une connexion sécurisée à votre réseau virtuel à partir d'un ordinateur de client individuel



Les VPN

☐ Connexions de réseau virtuel à réseau virtuel

- La connexion entre deux réseaux virtuels est semblable à la connexion d'un réseau virtuel à un emplacement de site local. Les deux types de connectivité font appel à une passerelle VPN pour offrir un tunnel sécurisé utilisant Ipsec/IKE
- Les réseaux virtuels que vous connectez peuvent être situés dans la même région ou dans des régions différentes, dans le même abonnement ou dans des abonnements différents



Le stockage sous Azure

❑ Présentation du modèle de stockage Azure

❑ Les comptes de stockage

❑ Les sauvegardes sous Azure

Le stockage sous Azure

□ Présentation du modèle de stockage Azure

Présentation du modèle de stockage Azure

- ❑ Un compte de stockage Azure contient tous vos objets de données de stockage Azure
- ❑ Le compte de stockage fournit pour vos données de stockage Azure un espace de noms, accessible de n'importe où dans le monde via HTTP ou HTTPS
- ❑ Les services de stockage Microsoft Azure offrent une gamme d'options pour stocker et accéder aux données.

Présentation du modèle de stockage Azure

- ❑ Azure offre des services de stockage pour faciliter la récupération et pour aider les clients à mettre en œuvre leurs objectifs de continuité d'activité et de reprise après sinistre. Ces services comprennent Azure Backup et Azure Site Recovery.
- ❑ Azure Content Delivery Network (CDN) est un autre service lié au stockage dont l'objectif principal est d'améliorer la performance des applications et services web en hébergeant des données dans des endroits proches des consommateurs
- ❑ Data Lake Storage: Référentiel hyperscale pour les charges de travail d'analyse Big Data.

Le stockage sous Azure

□ Les comptes de stockage

Les comptes de stockage

□ Les types de stockage dans un compte de stockage

- Azure Blob : magasin d'objets hautement scalable pour les données texte ou binaires. Prend également en charge l'analytique Big Data via Data Lake Storage Gen2
- Azure Files : partages de fichiers gérés pour les déploiements sur le cloud ou locaux
- Azure Queue: magasin de messagerie pour une messagerie fiable entre les composants d'application
- Azure Table : magasin NoSQL pour le stockage sans schéma de données structurées

Les comptes de stockage

□ Azure Blob

- Le stockage Blob Azure est la solution de stockage d'objet de Microsoft pour le cloud. Le stockage Blob est optimisé pour stocker de grandes quantités de données non structurées telles que des données texte ou binaires
- Le stockage Blob est idéal pour :
 - Mise à disposition d'images ou de documents directement dans un navigateur
 - Stockage de fichiers pour un accès distribué
 - Diffusion en continu de vidéo et d'audio
 - Stockage de données pour la sauvegarde et la restauration et l'archivage
 - Stockage des données pour l'analyse

Les comptes de stockage

☐ Azure Files

- Il vous permet de configurer les partages de fichiers réseau hautement disponibles qui sont accessibles à l'aide du protocole Server Message Block (SMB). Cela signifie que 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
- Les partages de fichiers peuvent être utilisés dans de nombreux scénarios courants
 - Par exemple, de nombreuses applications locales utilisent les partages de fichiers. Cette fonctionnalité simplifie la migration de ces applications qui partagent des données vers Azure
 - Les fichiers de configuration peuvent être stockés sur un partage de fichiers et sont accessibles à partir de plusieurs machines virtuelles
 - Les journaux de ressources et les métriques sont deux exemples de données qui peuvent être écrites dans un partage de fichiers et traitées ou analysées ultérieurement

Les comptes de stockage

□ Azure Queue

- Le service de files 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 en général à stocker des listes de messages qui seront traités de façon asynchrone

Les comptes de stockage

□ Azure Table

- En plus du service Stockage de tables Azure existant, il existe une nouvelle API de Table d'Azure Cosmos DB
- L'API de Table d'Azure Cosmos DB propose des tables optimisées pour le débit, la distribution globale et les index secondaires automatiques

<https://learn.microsoft.com/en-us/azure/cosmos-db/table/table-support>

Les comptes de stockage

□ Azure Table

- En plus du service Stockage de tables Azure existant, il existe une nouvelle API de Table d'Azure Cosmos DB
- L'API de Table d'Azure Cosmos DB propose des tables optimisées pour le débit, la distribution globale et les index secondaires automatiques

<https://learn.microsoft.com/en-us/azure/cosmos-db/table/table-support>

Les comptes de stockage

❑ La redondance du stockage

- Lorsque vous choisissez l'option de redondance la mieux adaptée à votre scénario, réfléchissez aux compromis possibles entre, d'une part, des coûts réduits et, de l'autre, une disponibilité et une durabilité accrues

❑ Les facteurs déterminant le choix de l'option de redondance sont les suivants

- Mode de réplication de vos données dans la région primaire
- Réplication éventuelle de vos données vers un deuxième emplacement géographiquement éloigné de la région primaire, afin d'offrir une protection contre des catastrophes régionales

Les comptes de stockage

❑ Redondance dans la région primaire

Les données d'un compte de stockage Azure sont toujours répliquées trois fois dans la région primaire. Le service Stockage Azure offre deux options pour la répllication de vos données dans la région primaire

- La répllication par stockage localement redondant (**LRS**) copie vos données de façon synchrone trois fois au sein d'un même emplacement physique dans la région primaire
 - L'option LRS est la moins coûteuse mais n'est pas recommandée pour des applications nécessitant une haute disponibilité
- La répllication par stockage redondant interzone (**ZRS**) copie vos données de façon synchrone dans trois zones de disponibilité Azure au sein de la région primaire
 - Pour les applications nécessitant une haute disponibilité, Microsoft recommande l'utilisation de l'option ZRS dans la région primaire, ainsi que la répllication vers une région secondaire

Les comptes de stockage

- ❑ Pour les applications nécessitant une haute disponibilité, vous pouvez choisir de copier en plus les données de votre compte de stockage vers une région secondaire située à des centaines de kilomètres de la région primaire.
- ❑ Le service Stockage Azure offre deux options pour la copie de vos données vers une région secondaire
 - La réplication par stockage géoredondant (**GRS**) copie vos données de façon synchrone trois fois au sein d'un même emplacement physique dans la région primaire en utilisant une réplication LRS. Elle copie ensuite vos données de façon asynchrone vers un emplacement physique unique dans la région secondaire
 - La réplication par stockage géoredondant interzone (**GZRS**) copie vos données de façon synchrone dans trois zones de disponibilité Azure au sein de la région primaire en utilisant une réplication ZRS. Elle copie ensuite vos données de façon asynchrone vers un emplacement physique unique dans la région secondaire

Les comptes de stockage

Paramètres de durabilité et de disponibilité

Paramètres	LRS	ZRS	GRS	GZRS
Pourcentage de durabilité des objets sur une année donnée	Au moins 99,999999999 % (11 chiffres 9)	Au moins 99,9999999999 % (12 chiffres 9)	Au moins 99,99999999999999 % (16 chiffres 9)	Au moins 99,99999999999999 % (16 chiffres 9)
Disponibilité pour les demandes de lecture	Au moins 99,9 % (99 % pour le niveau d'accès froid ou archive)	Au moins 99,9 % (99 % pour le niveau d'accès froid ou archive)	Au moins 99,9% (99% pour le niveau d'accès froid ou archive)	Au moins 99,9% (99% pour le niveau d'accès froid ou archive)
Disponibilité pour les demandes d'écriture	Au moins 99,9 % (99 % pour le niveau d'accès froid ou archive)	Au moins 99,9 % (99 % pour le niveau d'accès froid ou archive)	Au moins 99,9 % (99 % pour le niveau d'accès froid ou archive)	Au moins 99,9 % (99 % pour le niveau d'accès froid ou archive)

Les comptes de stockage

□ Le chiffrement du stockage

- Chiffrement au repos : Le chiffrement de Stockage Azure protège et sauvegarde vos données afin de vous permettre de respecter les engagements de votre organisation en matière de sécurité et de conformité. Stockage Azure chiffre automatiquement vos données avant de les conserver sur le compte de stockage, et les déchiffre avant leur récupération. Les processus de gestion du chiffrement, du déchiffrement et des clés sont transparents pour les utilisateurs. Vous pouvez également choisir de gérer vos propres clés à l'aide d'Azure Key Vault
- Chiffrement côté client: Stockage Azure fournit des méthodes pour chiffrer les données à partir de la bibliothèque cliente avant de les envoyer sur le réseau et de déchiffrer la réponse. Les données chiffrées via le chiffrement côté client sont également chiffrées au repos par Stockage Azure

Les comptes de stockage

□ Transfert de données vers et depuis Azure Storage

- Vous pouvez utiliser l'utilitaire de ligne de commande **AzCopy** pour copier des données d'objets blob, de fichiers et de table au sein de votre compte de stockage ou entre des comptes de stockage
- Grâce au service Azure Import/Export, vous pouvez importer des données d'objets blob dans votre compte de stockage, ou en exporter depuis celui-ci, par le biais d'un disque dur envoyé au centre de données Azure

Les comptes de stockage

□ Accès au stockage

- Lorsque vous créez un compte de stockage, Azure génère deux clés d'accès de stockage de 512 bits, qui servent à l'authentification lors de l'accès au compte de stockage
- En fournissant deux clés d'accès de stockage, Azure vous permet de régénérer les clés sans interrompre votre service de stockage

Les comptes de stockage

❑ Suppression d'un compte de stockage

- Pour supprimer un compte de stockage que vous n'utilisez plus, accédez au compte de stockage dans le portail Azure, puis cliquez sur Supprimer
- La suppression d'un compte de stockage supprime l'intégralité du compte, y compris toutes les données qu'il contient

Attention : Il n'est pas possible de restaurer un compte de stockage supprimé. Ceci vaut également pour toutes les ressources du compte : dès que vous supprimez un objet blob, une table, une file d'attente ou un fichier, la suppression est irréversible

Le stockage sous Azure

□ Les sauvegardes sous Azure

Les sauvegardes sous Azure

□ Azure Backup

- Azure Backup est le service Azure qui vous permet de sauvegarder (ou de protéger) et de restaurer vos données dans le cloud Microsoft
- Azure Backup remplace votre solution de sauvegarde locale ou hors site par une solution basée dans le cloud à la fois fiable, sécurisée et économique
- Azure Backup alloue et gère automatiquement le stockage de sauvegarde sur la base d'un modèle de paiement à l'utilisation. Avec le paiement à l'utilisation, vous payez uniquement le stockage que vous utilisez
- Azure Backup utilise la puissance et l'échelle illimitée du cloud Azure pour garantir la haute disponibilité, sans supplément de maintenance ou de surveillance. Vous pouvez configurer des alertes pour fournir des informations sur les événements, mais vous n'avez pas à vous soucier de la haute disponibilité de vos données dans le cloud

Les sauvegardes sous Azure

- Azure Backup ne limite pas la quantité de données entrantes ou sortantes transférées. Par ailleurs, les données transférées ne sont pas facturées par Azure Backup
- 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 en local et n'est jamais transmise ou stockée dans Azure. Si vous avez besoin de restaurer des données, vous êtes le seul à disposer de la phrase secrète de chiffrement ou de la clé
- Azure Backup fournit des sauvegardes cohérentes avec les applications, qui garantissent qu'aucun correctif supplémentaire n'est requis 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
- Conservation à long terme: Au lieu de basculer les copies de sauvegarde sur disque vers la sauvegarde sur bande, puis de déplacer cette dernière vers un emplacement hors site pour le stockage à long terme, vous pouvez utiliser Azure pour la rétention à court terme et à long terme.

Azure Active Directory

☐ Gestion des identités sous Azure AD

☐ Azure AD Security

☐ Azure AD Connect

Azure Active Directory

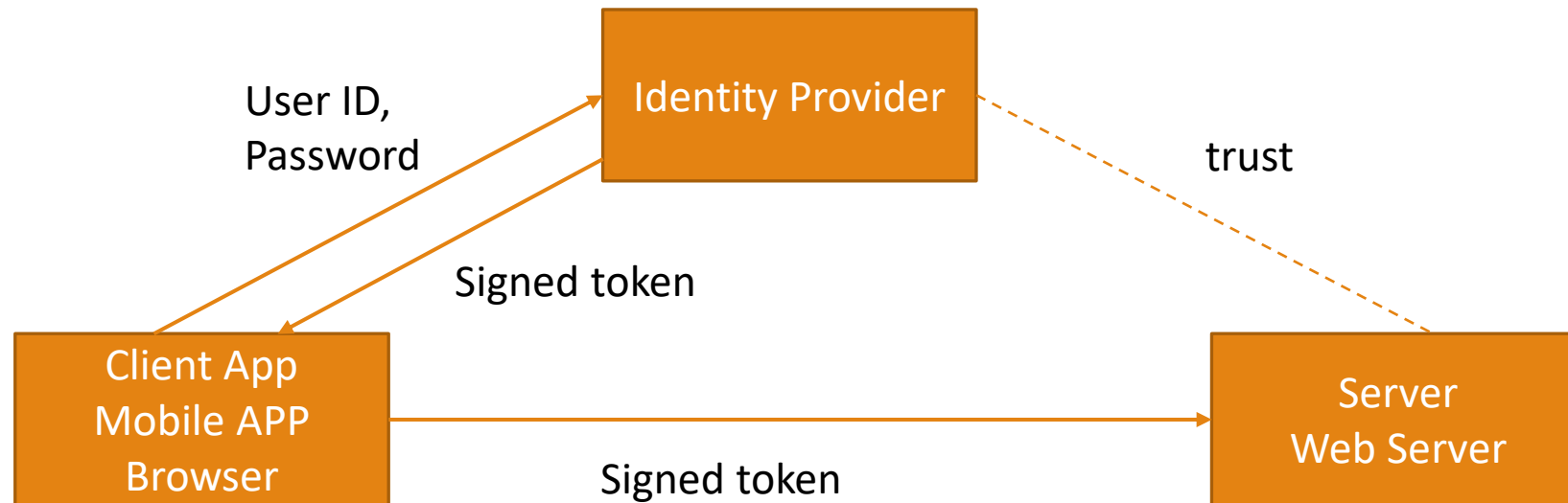
□ Gestion des identités sous Azure AD

Gestion des identités sous Azure AD

- ❑ Identité ?
- ❑ Mot de passe, clé/secret, certificat
- ❑ Azure fournit un système de gestion des identités basé sur leur Windows Active Directory
- ❑ Azure Active Directory (Azure AD or AAD) est un service dans Azure qui permet de gérer des annuaires et l'identité, il offre aux utilisateurs une authentification unique à plusieurs applications et services cloud

Gestion des identités sous Azure AD

- ❑ Identité en tant que service (Identity as a service)



Gestion des identités sous Azure AD

- ❑ La gestion des identités est le processus d'authentification des identités. Ce processus peut s'appliquer à des services, à des applications, à des utilisateurs ou à des groupes
- ❑ À l'aide des fonctionnalités de sécurité d'Azure AD, vous pouvez
 - Créer et gérer une identité unique pour chaque utilisateur de votre entreprise hybride, en synchronisant les utilisateurs, les groupes et les appareils
 - Fournir un accès à authentification unique (SSO) à vos applications
- ❑ Fournir un accès à distance sécurisé aux applications web locales via le proxy d'application Azure AD (Application proxy).
- ❑ Sécuriser l'accès aux applications locales et cloud en appliquant l'authentification multifacteur

Gestion des identités sous Azure AD

❑ Tarification AAD

- Azure AD Gratuit : Inclus avec un abonnement Azure
- Azure AD de Base (Les abonnés Microsoft 365/Office365): Conçu pour des besoins en priorité sur le cloud
- Azure AD Premium P1 : Gestion des identités au niveau de l'entreprise
- Azure AD Premium P2: toutes les fonctionnalités P1 + gestion des identités privilégiées + protection des identités

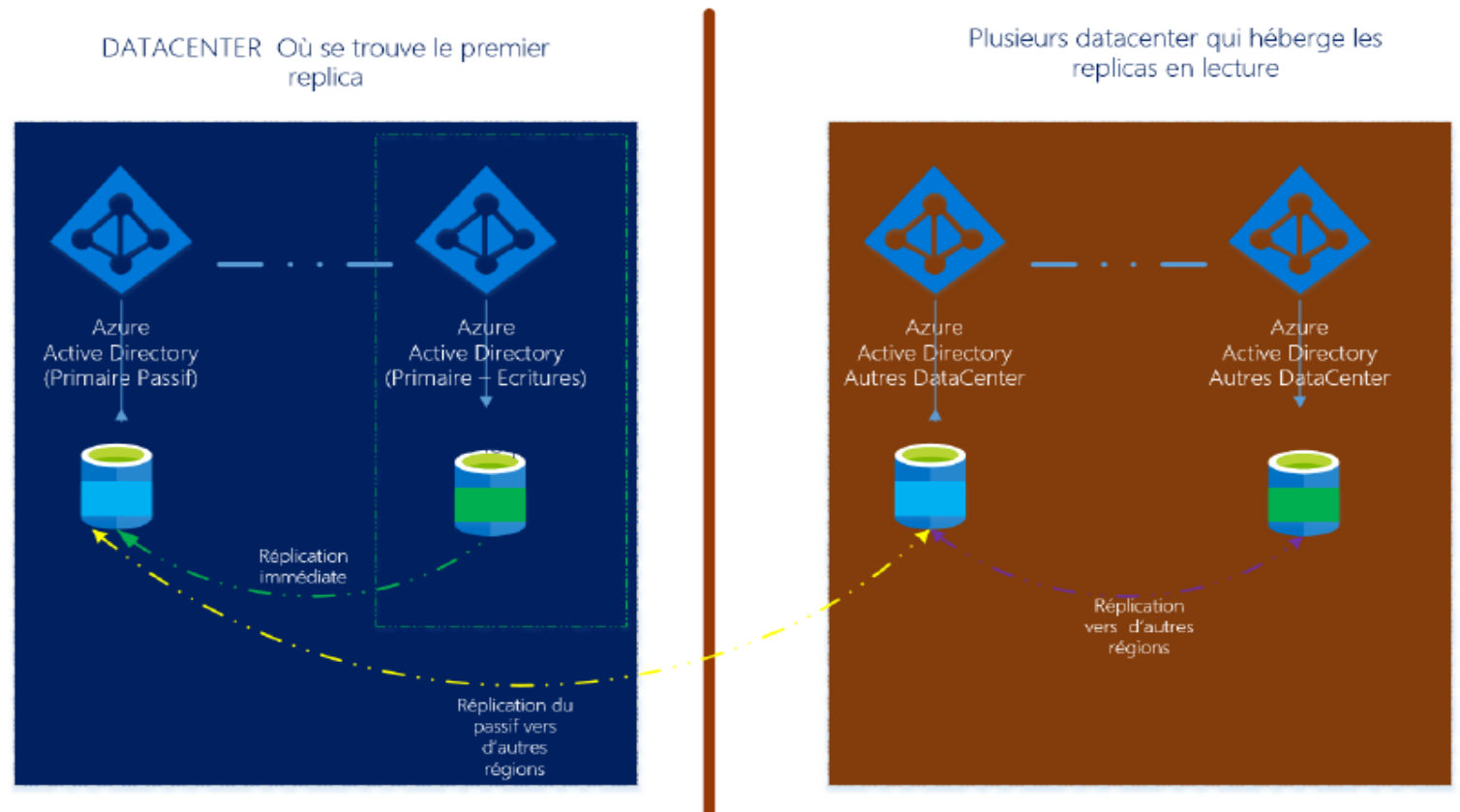
<https://azure.microsoft.com/fr-fr/pricing/details/active-directory>

Gestion des identités sous Azure AD

- ❑ Gestion des identités privilégiés (service Azure Privileged Identity Management)
 - Privileged Identity Management assure une activation de rôle basée sur l'heure et l'approbation pour atténuer les risques d'autorisations d'accès excessives, injustifiées ou malveillantes sur les ressources qui vous intéressent.
 - Fournir un accès privilégié juste-à-temps à Azure AD et aux ressources Azure
 - Affecter un accès aux ressources limité dans le temps à l'aide de dates de début et de fin
 - Exiger une approbation pour activer les rôles privilégiés
 - Appliquer l'authentification multifacteur pour l'activation des rôles
 - Utiliser la justification pour comprendre le motif d'activation des utilisateurs
 - Recevoir des notifications lors de l'activation de rôles privilégiés
 - Effectuer des révisions d'accès pour vérifier que les utilisateurs ont toujours besoin de leurs rôles
 - Télécharger l'historique des audits
 - Empêche la suppression des dernières attributions de rôle Administrateur général (Global Administrator) et Administrateur de rôle privilégié actives (Privileged Role Administrator)

Gestion des identités sous Azure AD


Architecture d'AAD



Gestion des identités sous Azure AD


☐ Azure AD tenant

- Curent directory: Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
- New Azure Ad Tenant


 **cloudimiOrg** | Overview ...
Azure Active Directory

« + Add ▾ ⚙️ Manage tenants 📄 What's new | 🛠️ Preview features | 🗨️ Got feedback? ▾

Overview Monitoring Properties Tutorials

 Search your tenant

Basic information

Name	cloudimiOrg	Users	2
Tenant ID	e75c27cc-adcf-43a1-8806-3ec197a15ab9 	Groups	0
Primary domain	cloudimi.onmicrosoft.com	Applications	0
License	Azure AD Free	Devices	0

Alerts

Manage

- Overview
- Preview features
- Diagnose and solve problems
- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Delegated admin partners
- Enterprise applications
- Devices

Gestion des identités sous Azure AD

- ❑ Chaque nouvel utilisateur Azure AD est fourni avec un nom de domaine initial, au format <nom_de_domaine>.onmicrosoft.com
- ❑ Noms de domaine personnalisé (Custom domain names)

Record type

TXT

MX

Alias or host name

@



Destination or points to address

MS=ms37377667



TTL

3600



Azure Active Directory

 Azure AD Security

Azure AD Security


☐ Protection des identités (Identity Protection)



- User risk policy
- Sign-in risk policy
- Attribution (tous les utilisateurs, certains utilisateurs/groupes)
- Niveaux de risques: Identity Protection catégorise les risques en niveaux faible, moyen et sévère
- Contrôle : Accès bloqué / permis avec conditions (changement de mot de passe, authentification multifacteur)

Azure AD Security




[Home](#) > [Identity Protection](#)

Identity Protection | User risk policy ...




 Search (Ctrl+ /)

-  Overview
-  Diagnose and solve problems


Protect

-  User risk policy
-  Sign-in risk policy
-  MFA registration policy

Report




-  Risky users
-  Risky sign-ins
-  Risk detections

Notify

-  Users at risk detected alerts
-  Weekly digest


<<

Assignments

-  Users
 - [All users](#)
-  User risk 
 - [Low and above](#)

Controls

-  Access 
 - [Block access](#)

 This view is for Azure AD Premium P2 customers to setup user risk policy. Other customers can only disable policies here.

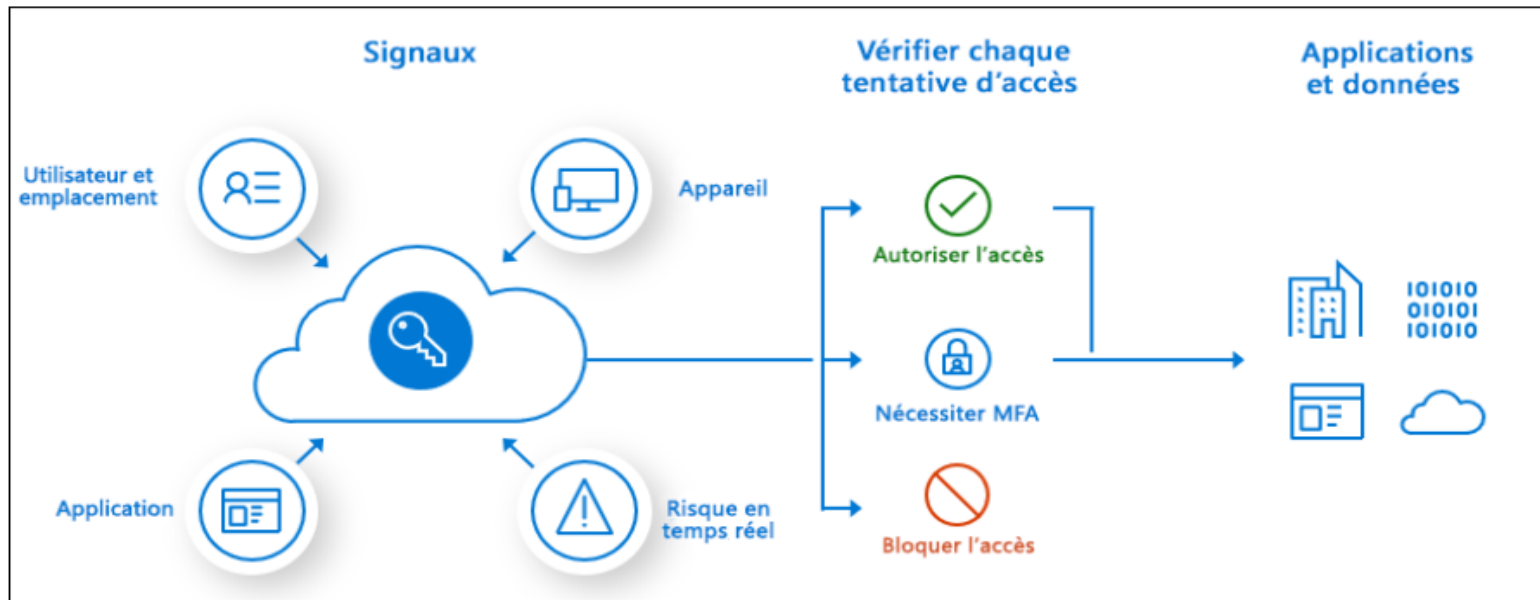
Enforce policy

☒ On ☐ Off

Azure AD Security

□ L'accès conditionnel (Conditional Access)

- Des stratégies d'accès conditionnel pour appliquer les contrôles d'accès appropriés pour garantir la sécurité de votre organisation



Azure AD Security

□ Signaux

- Appartenance des utilisateurs ou appartenance à un groupe: Les stratégies peuvent cibler des utilisateurs et des groupes spécifiques, ce qui donne aux administrateurs un contrôle plus précis sur l'accès
- Informations d'emplacement IP: Les organisations peuvent créer des plages d'adresses IP approuvées qui peuvent être utilisées pour prendre des décisions en matière de stratégie
- Appareil: Les utilisateurs disposant d'appareils de plateformes spécifiques ou marqués avec un état spécifique peuvent être utilisés lors de l'application de stratégies d'accès conditionnel.
- Application: Les utilisateurs qui tentent d'accéder à des applications spécifiques peuvent déclencher différentes stratégies d'accès conditionnel.
- Détection des risques en temps réel: L'intégration de signaux à Azure AD Identity Protection permet aux stratégies d'accès conditionnel d'identifier le comportement des connexions à risque.

Azure AD Security

❏ Décisions courantes

- Bloquer l'accès: Décision la plus restrictive
- Accorder l'accès: Décision la moins restrictive ; peut toujours nécessiter par exemple une ou plusieurs des options suivantes :
 - Exiger une authentification multifacteur
 - Exiger que l'appareil soit marqué comme conforme
 - Demander une application cliente approuvée
 - Demander un changement de mot de passe

Azure AD Security


- ❑ MultiFactor Authentication MFA (authentification multifacteur)
 - L'authentification multifacteur est un processus dans lequel l'utilisateur est invité pendant le processus de connexion à suivre une forme d'identification supplémentaire, consistant par exemple à entrer un code sur son téléphone portable
 - Un administrateur peut exiger l'inscription de ces méthodes de vérification Azure MFA, ou l'utilisateur peut accéder à sa propre page Mon profil pour modifier ou ajouter des méthodes de vérification.
 - Les formes de vérification suivantes peuvent être utilisées avec Azure MFA
 - FIDO2 security key
 - Microsoft Authenticator
 - SMS
 - Temporary Access Pass
 - Certificate-based authentication

Azure AD Security










[Home](#) > [cloudimiOrg](#) > [Users](#) > [imene](#)







imene | Authentication methods ...


User

 Diagnose and solve problems

Manage

-  Profile
-  Assigned roles
-  Administrative units
-  Groups
-  Applications
-  Licenses
-  Devices
-  Azure role assignments
-  Authentication methods

 Save  Discard |  Reset password  Require re-register MFA  Revoke MFA sessions |  Got feedback?

 Switch to the new user authentication methods experience! [Click here to use it now.](#) →

Authentication methods are the ways your users sign into Azure AD. Here, you can set the phone numbers and email addresses that users use to perform multi-factor authentication and self-service password reset, and reset a user's password.

Authentication contact info

Phone

Alternate phone

Email

Alternate email is now managed on the [Profile](#) page

Azure Active Directory

 Azure AD Connect

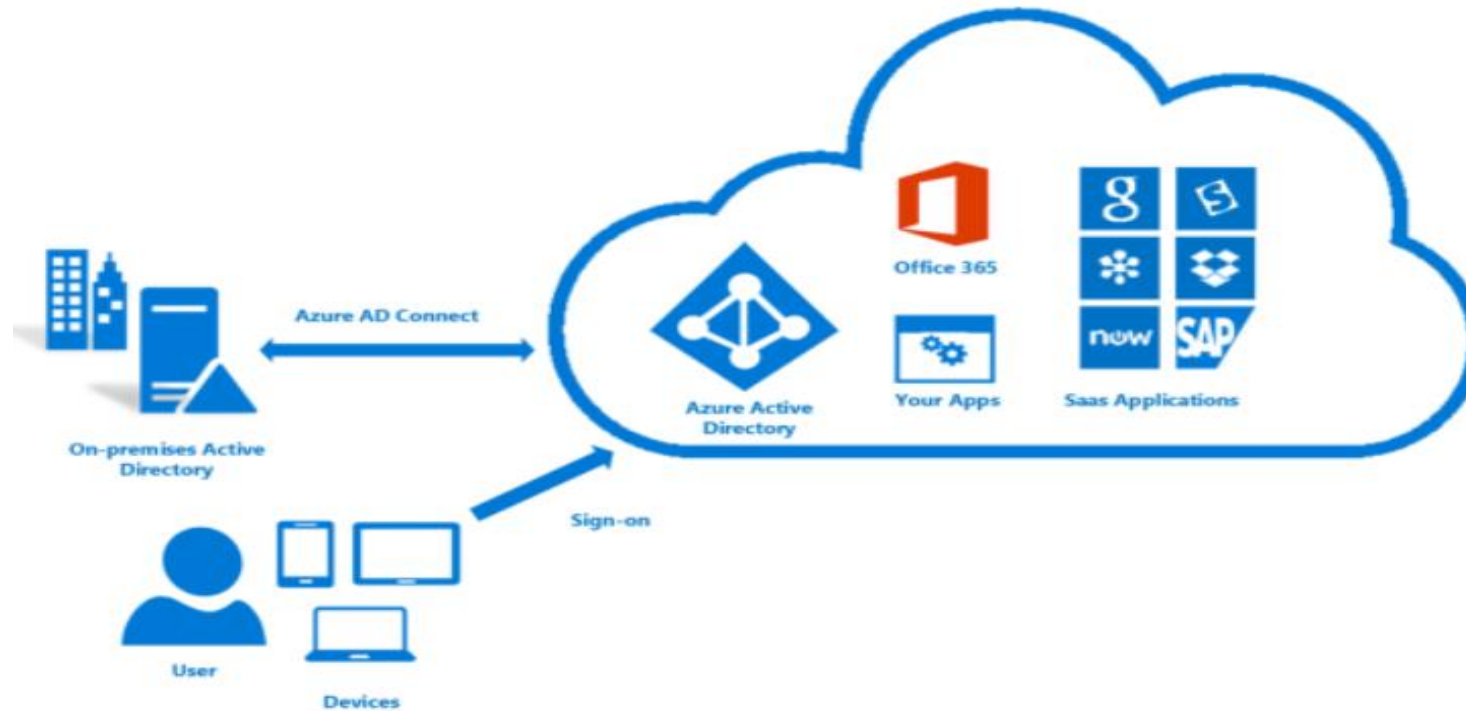
Azure AD Connect

- ❑ Identités hybrides
- ❑ Extension de votre AD Local vers Azure AD
 - Plusieurs applications pour une seule et unique identité
- ❑ Mise en œuvre
 - La synchronisation des objets d'annuaires entre votre environnement AD local et Azure AD
 - AZURE AD Connect permet cette synchronisation

Azure AD Connect

- ❑ Outil unique offrant une expérience de déploiement simple pour la synchronisation et la connexion
 - Synchroniser les comptes d'utilisateurs et de groupes dans mon AD local vers le cloud
 - Accéder aux services Cloud à l'aide du mot de passe local
 - Les utilisateurs peuvent utiliser une identité unique pour accéder aux applications locales et aux services cloud comme Microsoft 365

Azure AD Connect



Supervision et Gouvernance

☐ Supervision

☐ Gouvernance

Supervision et Gouvernance

 Supervision

Supervision

- ❑ Paramètres de diagnostic (Diagnostic settings)
 - Compteur de performance : CPU, Mémoire, Disque, Réseau,...
 - Journaux (Logs): Application, Sécurité, Système
 - Critique, Erreur, Avertissement, Informations...
 - Crash dumps: Collectez les images mémoire quand un processus se bloque

Supervision

□ Métriques

- Créer des graphiques
 - Choix du graphique (histogramme, Grille, Nuages de points,..)
 - Étendue: Choix de la ressource
 - Ajout des métriques (CPU, réseau, mémoire, disque,...)
 - Intervalle de temps

Supervision

Alertes

- Règle d'alerte
 - Etendue
 - Condition
 - Groupe d'Action
 - Notification
 - Action: (Azure Function, Logic App, Webhook, runbook)

Supervision

❑ Azure Log Analytics Workspace

- Log Analytics collecte des données de différentes sources et utilise un langage de requête puissant pour vous donner des insights sur le fonctionnement de vos ressources

❑ Azure Monitor

- ❑ Azure Monitor pour accéder à l'ensemble complet des outils servant à superviser toutes vos ressources Azure

Supervision

☐ Azure Advisor

- Advisor analyse les données de télémétrie relatives à vos configurations et à votre utilisation, et vous propose des recommandations personnalisées et réalisables pour optimiser vos ressources Azure en termes de fiabilité, de sécurité de performances et de coût

☐ Microsoft Defender for Cloud

- Gérer la sécurité de vos ressources dans le cloud

☐ Azure Cost Management : vous permet de suivre l'utilisation du Cloud et les dépenses liées à vos ressources Azure

- Gestion des coûts + facturation (Cost management + billing)
- Analyse du coût
- Alerte de coûts
- Budget

Supervision et Gouvernance

 Gouvernance

Gouvernance

- ❑ La gouvernance dans Azure est un aspect de la gestion Azure
- ❑ La gouvernance propose des mécanismes pour garder le contrôle sur vos ressources dans Azure
- ❑ La gouvernance dans Azure est principalement mise en œuvre à l'aide de Azure Policy
 - Azure Policy vous permet de gérer des définitions de stratégie afin d'appliquer des règles pour vos ressources. Cette fonctionnalité maintient ces ressources conformes aux standards de votre entreprise

Gouvernance

☐ Azure Policy vs Azure RBAC (Role-Based Access Control)

- Azure Policy garantit que l'état des ressources est conforme à vos règles d'entreprise sans se préoccuper de qui a apporté la modification ou qui a l'autorisation d'apporter une modification
- Azure RBAC est axé sur la gestion des actions des utilisateurs dans différentes étendues

Gouvernance

- ❑ Le contrôle RBAC Azure est un système d'autorisation qui permet une gestion affinée de l'accès aux ressources Azure
 - Ne pas confondre avec les rôles Azure AD qui contrôlent les autorisations pour gérer les ressources Azure Active Directory
 - <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>
 - Il y a plusieurs rôles intégrés Azure
 - <https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>
 - Owner, Contributor, Reader,...
 - Si les rôles intégrés ne répondent pas aux besoins spécifiques de votre organisation, vous pouvez créer vos propres rôles personnalisés Azure
 - Lorsque vous attribuez un rôle, vous pouvez restreindre les actions autorisées en définissant une étendue
 - Une attribution de rôle est le processus d'attachement d'une définition de rôle à un utilisateur, un groupe, un service ou une identité managée pour accorder des accès.
 - La création d'une attribution de rôle permet d'accorder un accès, qui peut être révoqué par la suppression d'une attribution de rôle.

Gouvernance

Azure Policy

- Ces règles d'entreprise, décrites au format JSON, sont appelées définitions de stratégie
- L'affectation s'applique à toutes les ressources au sein de l'étendue Resource Manager de cette affectation

Gouvernance

□ Azure Blueprints

- Permet de créer et de mettre en place rapidement de nouveaux environnements conformes aux exigences de l'organisation
- L'affectation s'applique à toutes les ressources au sein de l'étendue Resource Manager de cette affectation
- Un blueprint est composé d'artefacts: Groupe de ressource (resource group), affectation de stratégie (Policy assignment), affectation de rôle (Rôle assignment), Modèle ARM (ARM template)

Azure Key Vault

- ❑ Introduction à Azure Key Vault
- ❑ Identités managées

Azure Key Vault

□ Introduction à Azure Key Vault

Introduction à Azure Key Vault

- ❑ Azure Key Vault est un service cloud permettant de stocker les secrets et d'y accéder en toute sécurité
- ❑ Il peut s'agir de clés (keys), de mots de passe (secrets) ou de certificats (certificates)
- ❑ Azure Key Vault applique le protocole TLS (Transport Layer Security) pour protéger les données en transit entre Azure Key Vault et des clients
- ❑ Pour plus de sécurité, le service Key Vault prend en charge la gestion des clés avec HSM (Hardware Security Module)

Introduction à Azure Key Vault

- ❑ Les objets sont identifiés de façon unique dans Key Vault avec une URL.
- ❑ L'URL est constituée d'un préfixe qui identifie le coffre de clés, du type d'objet, du nom d'objet fourni par l'utilisateur et peut être complétée par une version d'objet.
 - Pour les coffres : `https://{vault-name}.vault.azure.net/{object-type}/{object-name}/{object-version}`
 - Pour les pools Managed HSM : `https://{hsm-name}.managedhsm.azure.net/{object-type}/{object-name}/{object-version}`

Introduction à Azure Key Vault

- ❑ Azure Key Vault permet de stocker en toute sécurité les secrets, mais votre code doit s'authentifier sur Key Vault pour les récupérer
- ❑ L'utilisation d'une identité managée simplifie la résolution de ce problème en donnant aux services Azure une identité automatiquement managée dans Azure AD

Azure Key Vault

❑ Identités managées

Identités managées

❑ Identités managées pour les ressources Azure

- Quand vous déployez une application sur une machine virtuelle dans Azure, vous pouvez attribuer une identité à votre machine virtuelle qui a accès à Key Vault
- L'avantage de cette approche est que l'application ou le service ne gère pas la rotation du secret. Azure fait alterner automatiquement l'identité
- Cette approche est recommandée en tant que meilleure pratique.

Create azure resource with managed identity

Grant permission

Delete resource

Identités managées

- ❑ Il existe deux types d'identités administrées (managed identity)
 - Affectation par le système (System-assigned). Lorsque vous activez une identité managée affectée par le système, une identité est créée dans Azure AD. L'identité est liée au cycle de vie de cette instance de service. Lorsque la ressource est supprimée, Azure supprime automatiquement l'identité
 - Affectation par l'utilisateur (User-assigned) . Vous pouvez également créer une identité managée en tant que ressource Azure autonome. Vous pouvez créer une identité managée affectée par l'utilisateur et l'attribuer à une ou plusieurs ressources Azure. Une identité managée affectée par l'utilisateur est gérée séparément des ressources qui l'utilisent

Application infrastructure

❑ Web App et App service plans

❑ Logic Apps et Function App

Application infrastructure

- Web App et App service plans

Web App et App service plans

- ❑ Avec App Service, vous payez pour les ressources de calcul Azure que vous utilisez
 - Les ressources de calcul que vous utilisez sont déterminées par le plan App Service sur lequel vous exécutez vos applications
- ❑ Un plan App Service définit un ensemble de ressources de calcul nécessaires à l'exécution d'une application web
- ❑ Une ou plusieurs applications peuvent être configurées pour s'exécuter sur les mêmes ressources informatiques (ou dans le même plan App Service)
- ❑ Web Apps: Fournit une plateforme commune pour le développement, la construction, l'hébergement et la gestion d'applications Web.

Web App et App service plans

- ❑ Quand vous créez un plan App Service dans une région (par exemple, Europe Ouest), un ensemble de ressources de calcul est créé pour ce plan dans cette région.
 - Toutes les applications que vous placez dans ce plan App Service s'exécutent sur ces ressources de calcul
- ❑ Chaque plan App Service définit les éléments suivants
 - Région (USA Ouest, USA Est, etc.)
 - Nombre d'instances de machine virtuelle
 - Taille des instances de machine virtuelle
 - Niveau tarifaire (Gratuit, Partagé, De base, Standard, Premium, Isolé)

Web App et App service plans

- ❑ Le niveau tarifaire d'un plan App Service détermine les fonctionnalités App Service que vous obtenez et combien vous payez pour le plan. Il existe plusieurs catégories de niveaux tarifaires : <https://azure.microsoft.com/en-gb/pricing/details/app-service/windows/>
 - Calcul partagé : Les deux niveaux Gratuit et Partagé , exécutent une application sur la même machine virtuelle Azure que les autres applications App Service, y compris les applications d'autres clients. Ces niveaux allouent des quotas d'UC à chaque application qui s'exécute sur les ressources partagées, et les ressources ne peuvent pas effectuer un scale out.
 - Calcul dédié : Les niveaux De base, Standard et Premium exécutent les applications sur des machines virtuelles Azure dédiées. Seules les applications qui se trouvent dans un même plan App Service partagent les mêmes ressources de calcul. Plus le niveau est élevé, plus vous disposez d'instances de machine virtuelle pour une mises à l'échelle.
 - Isolé : Ce niveau exécute des machines virtuelles Azure dédiées sur des réseaux virtuels Azure dédiés. Il fournit à vos applications l'isolement réseau au dessus de l'isolation du calcul. Il fournit les fonctionnalités de mises à l'échelle maximales.

Web App et App service plans

- ❑ À l'exception du niveau Gratuit , un plan App Service comporte une facturation horaire des ressources de calcul qu'il utilise.
 - Dans le niveau Partagé , chaque application reçoit un quota de minutes d'UC. Ainsi, chaque application est facturée toutes les heures pour le quota d'UC
 - Dans les niveaux de calcul dédié (De base, Standard et Premium), le plan App Service définit le nombre d'instances de machines virtuelles auquel les applications sont mises à l'échelle. Chaque instance de machine virtuelle dans le plan App Service fait l'objet d'une facturation horaire. Ces instances de machine virtuelle sont facturées dans les mêmes proportions, quel que soit le nombre d'applications en cours d'exécution sur ces instances
 - Dans le niveau Isolé , l'environnement App Service définit le nombre de workers isolés qui exécutent vos applications, et chaque worker est facturé toutes les heures. L'exécution de l'environnement App Service donne lieu à des frais horaires de base.

Web App et App service plans

- ❑ Domaines App Service : vous payez quand vous en achetez un dans Azure et quand vous le renouvelez chaque année
- ❑ Certificats App Service : vous payez quand vous en achetez un dans Azure et quand vous le renouvelez chaque année
- ❑ Si vous souhaitez utiliser le protocole TLS pour chiffrer les communications entre le navigateur Web et le serveur hébergeant l'application Web, vous devez obtenir un certificat auprès d'une autorité de certification reconnue
 - Connexions TLS basées sur IP : il existe un tarif horaire pour chaque connexion TLS basée sur IP, mais certains niveaux Standard ou supérieur vous octroient gratuitement une connexion TLS basée sur IP. Les connexions TLS basées sur SNI sont gratuites

Web App et App service plans

□ Authentification

- Vous pouvez intégrer des applications Web nécessitant une authentification et une autorisation avec Azure Active Directory (AD Azure)
- De plus, pour l'authentification, vous pouvez configurer d'autres fournisseurs d'authentification de cloud, tels que le compte Microsoft, Facebook, Twitter ou Google

Web App et App service plans

- ❑ Les applications Web nécessitent souvent un service de stockage d données et de stockage de fichiers
 - Dans Azure, vous pouvez utiliser une base de données pour héberger les données ou utiliser le stockage de table Azure

- ❑ Les applications Web incluent souvent des fichiers multimédias, tels que des images, des vidéos et des fichiers audio
 - Dans Azure, vous pouvez utiliser un compte de stockage pour ces fichiers
 - Une autre solution consiste à utiliser le système de fichiers d'une machine virtuelle pour le stockage de fichiers

Web App et App service plans

□ Il existe deux workflows de mise à l'échelle : scale up et scale out

- **Scale up:** Bénéficie d'un surcroît de capacité d'UC, de mémoire et d'espace disque, ainsi que de fonctionnalités supplémentaires, comme des machines virtuelles dédiées, des domaines et des certificats personnalisés, la mise à l'échelle automatique,... Pour monter en puissance on modifie le niveau tarifaire du plan App Service auquel appartient votre application
- **Scale out:** Augmente le nombre d'instances de machine virtuelle qui exécutent votre application. Vous pouvez effectuer le scale out selon votre niveau tarifaire

Web App et App service plans

- ❑ Sauvegarde: La fonctionnalité de sauvegarde et de restauration d'Azure App Service vous permet de créer facilement des sauvegardes d'applications manuelles ou planifiées
 - Vous pouvez configurer les sauvegardes pour qu'elles soient conservées pendant une durée indéfinie
 - Vous pouvez restaurer l'application d'après la capture instantanée d'un état précédent en remplaçant l'application existante ou en restaurant sur une autre application
 - La fonctionnalité de sauvegarde et de restauration nécessite un plan App Service de niveau Standard, Premium ou Isolé
 - Vous avez besoin d'un compte de stockage Azure dans le même abonnement que l'application que vous souhaitez sauvegarder.

Application infrastructure

□ Logic Apps et Function App

Logic Apps et Function App

❑ Logic Apps

- Active les liens rapides entre les applications basées sur le cloud, de sorte que vous puissiez créer des solutions connectées

❑ Function App

- Exécution de code

Logic App

- ❑ Son concepteur visuel modélise et automatise votre processus sous la forme d'une série d'étapes appelée workflow
- ❑ Gain de temps en créant des processus complexes à l'aide d'outils de conception faciles à comprendre
- ❑ Implémentation transparente de modèles et de workflows qui seraient sans cela difficiles à mettre en œuvre dans le code
- ❑ Logic Apps est une fonctionnalité iPaaS (integration platform as a service) entièrement gérée, qui évite aux développeurs l'obligation d'assurer l'hébergement, l'évolutivité, la disponibilité et la gestion. Logic Apps monte en puissance automatiquement pour répondre à la demande
- ❑ Logic Apps vous permet d'automatiser vos processus métier. Par exemple, surveillance de tous les tweets sur un sujet donné, analyse du sentiment et création d'alertes et de tâches pour les éléments nécessitant un suivi

Logic App

- ❑ Outils de conception faciles à utiliser : Logic Apps peut être conçu de bout en bout. Commencez par un **déclencheur** et orchestrez des **actions** à l'aide de la galerie de **connecteurs** enrichie
- ❑ Simplicité de connexion des API : Les applications logiques constituent le moyen le plus rapide et le plus fiable pour faciliter la connexion de systèmes disparates
- ❑ Prise en main rapide à partir de modèles : Une galerie de modèles qui vous permettent de créer rapidement des solutions courantes
- ❑ Extensibilité intégrée : S'il n'y a pas le connecteur dont vous avez besoin, il est possible de créer votre propre application API à utiliser en tant que connecteur personnalisé, ou appeler une fonction Azure pour exécuter du code

Function App

- Azure Functions est une solution qui permet de maintenir une infrastructure plus légère et de réduire les coûts
- Exécuter du code à mesure que des événements se produisent (déclencheur)
- Azure Functions est une solution serverless (Consumption)
- App service plan ou Function premium

Les Bases de données sous Azure

- ❑ Les modèles de bases de données
- ❑ Azure CosmosDB for NoSQL
- ❑ Azure SQL database

Les Bases de données sous Azure

- Les modèles de bases de base de données

Les modèles de bases de données

- Azure vous propose différentes méthodes de déploiement de base de données. En fonction de vos besoins et de vos architectures de données vous avez les choix entre différents modèles
 - Azure SQL: Azure SQL est une famille de produits de base de données SQL Server gérés
 - SQL Database: Base de données relationnelle SQL
 - Azure SQL Managed Instance: Migrations vers le cloud de SQL server instance
 - SQL virtual machines: Portage virtuel des charges de travail SQL Server et un accès au niveau du système d'exploitation
 - Azure Database for MySQL: Service de base de données MySQL
 - Azure Database for PostgreSQL: Service de base de données PostgreSQL
 - SQL Server Stretch Database: Étendez dynamiquement les bases de données SQL Server locales sur Azure

Les modèles de bases de données

- Table Storage: Stockage de valeurs de clés NoSQL utilisant des jeux de données semi structurés
- Azure CosmosDB: Base de données multimodèle NoSQL
 - Azure Cosmos DB for NoSQL: Base données documentaires (JSON) et utilisation possible de la syntaxe SQL pour les requêtes
 - Azure Cosmos DB for MongoDB: Service de base de données entièrement géré pour les applications écrites pour MongoDB. Recommandé si vous avez des charges de travail MongoDB existantes que vous prévoyez de migrer vers Azure Cosmos DB.
 - Azure Cosmos DB for Apache Cassandra: Service de base de données Cassandra entièrement géré pour les applications écrites pour Apache Cassandra. Recommandé si vous avez des charges de travail Cassandra existantes que vous prévoyez de migrer vers Azure CosmosDB
 - Azure Cosmos DB for Table: Service de base de données entièrement géré pour les applications écrites pour le stockage Azure Table. Recommandé si vous avez des charges de travail de stockage Azure Table existantes que vous envisagez de migrer vers Azure Cosmos DB
 - Azure Cosmos DB for Apache Gremlin: Service de base de données orientée graphes utilisant le langage de requête Gremlin. Recommandé pour les nouvelles charges de travail qui doivent stocker des relations entre les données
 - Azure Cosmos DB for PostgreSQL: Service de base de données relationnelle entièrement géré pour PostgreSQL avec exécution de requêtes distribuées, alimenté par l'extension open source Citus. Créez de nouvelles applications sur des clusters à un ou plusieurs nœuds

Les Bases de données sous Azure

- Azure CosmosDB for NoSQL

Azure CosmosDB

- ❑ Un compte CosmosDB (CosmosDB Account)
- ❑ Provisioned throughput / Serverless
- ❑ Avec le niveau gratuit d'Azure Cosmos DB, vous obtiendrez gratuitement les 1000 premières RU/s et 25 Go de stockage dans un compte
- ❑ Global Distribution
 - Geo-Redundancy, Multi-region Writes, Availability zones
- ❑ Backup policy

Azure CosmosDB

- ❑ Dans votre compte CosmosDB, il est possible de créer une ou plusieurs bases de données
- ❑ Une base de données est simplement un groupe de conteneurs
- ❑ Un conteneur Azure Cosmos DB est l'endroit où les données sont stockées
- ❑ Selon l'API cosmosDB, un conteneur est réalisé comme: une collection, table, graphique,...
- ❑ Database throughput: Required RU/s

Les Bases de données sous Azure

 Azure SQL database

Azure SQL database

- ❑ Azure SQL Database s'exécute sur le moteur de base de données SQL Server
- ❑ La base de données est créée dans un serveur logique Azure SQL Database
- ❑ Modèle d'achat
 - Modèle d'achat **DTU**: offre une combinaison de ressources de calcul, de mémoire et d'E/S réparties sur trois niveaux de service (Basic, Standard, Premium) pour prendre en charge les charges de travail de base de données, aussi bien légères qu'importantes.
 - Les tailles de calcul sont exprimées en unités de transaction de base de données (DTU, Database Transaction Unit)) pour les bases de données uniques, et en unités de transaction de base de données élastique (eDTU) pour les pools élastiques
 - Les tailles de calcul de chaque niveau fournissent une combinaison différente de ces ressources, auxquelles vous pouvez ajouter d'autres ressources de stockage

Azure SQL database

- Modèle d'achat **vCore**: vous permet de choisir le nombre de vCores, la quantité de mémoire et de stockage, ainsi que la vitesse de stockage
 - Trois niveaux de service (General purpose, Hyperscale, Business critical)
 - Hardware configuration
 - Le niveau de calcul **serverless** est disponible dans le modèle d'achat vCore lorsque vous sélectionnez le niveau de service usage général (General purpose).
 - Il met automatiquement à l'échelle les ressources de calcul en fonction de la demande de charge de travail et facture la quantité de ressources de calcul utilisée par seconde. Le niveau de calcul serverless met automatiquement en pause les bases de données pendant les périodes d'inactivité, lorsque seul le stockage est facturé, et relance automatiquement leur exécution lorsque l'activité reprend.

Azure SQL database

□ Modèles de déploiement

- Base de données unique représente une base de données isolée complètement managée
- Pool élastique représente une collection de bases de données uniques avec un ensemble partagé de ressources telles que le processeur ou la mémoire.