



# Introduction au Cloud Azure



# Votre interlocuteur

Contact



**Dylan SINAULT**

Consultant Azure

**Mail** : [dylan.sinault@exakis-nelite.com](mailto:dylan.sinault@exakis-nelite.com)



# Introduction

Présentation de l'organisation du module

- 8 heures de cours ( cours magistral + autoformation via Microsoft Learning Path)
- 20 heures TP ( 4 TP individuel et un TP Projet en groupe ou individuel)
- Modalité d'évaluation :
  - QCM (10 questions)
  - TP Projet



# Introduction

## Présentation de la démarche

Exakis accompagne CPE Lyon sur l'éducation des principes du Cloud à travers ce cours sur l'introduction au cloud public Azure de Microsoft.

Voici les grandes parties que nous verrons dans ce cours, qui nous permettront d'appréhender l'ensemble des piliers du cloud :

- ✓ Gouvernance
- ✓ Réseau
- ✓ Sécurité
- ✓ Exploitation

Cette présentation est destinée à l'acculturation Azure des élèves concernant les enjeux des 4 piliers abordés. Cette méthode de formation du cloud Azure est basé sur une partie du Cloud Adaption Framework.

Cela donnera l'occasion de vous offrir un avant goûts des possibilités grandissantes du Cloud Azure. Des démonstrations vous seront présentées tout au long du cours et vous seront utiles durant la phase de Travaux Pratiques.



# Azure – vue d'ensemble

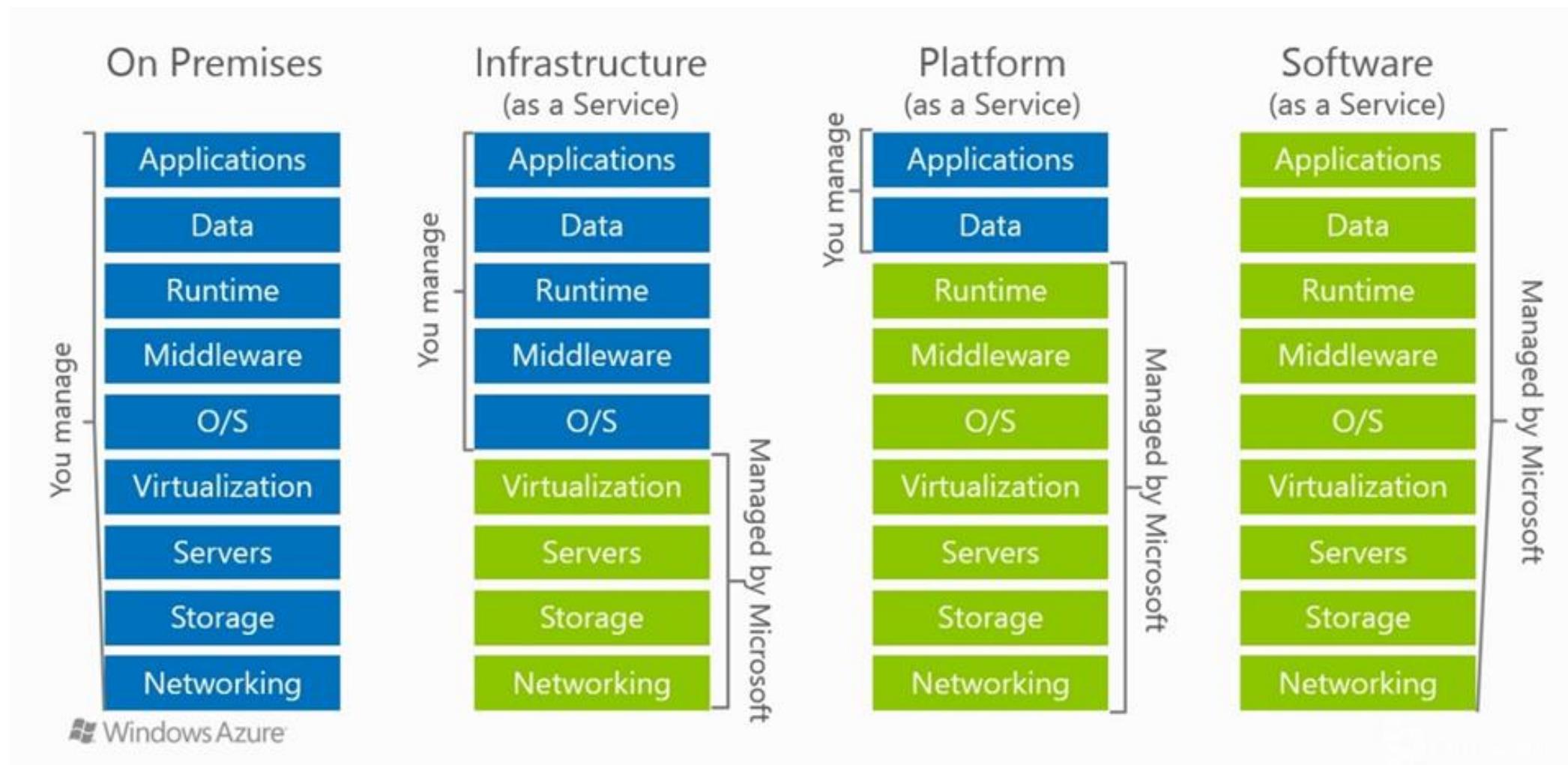
Les caractéristiques du cloud public Azure





# Concept de « As a Service »

Diagramme de distribution des responsabilités selon les types de services



## Security & Management

-  Security Center
-  Azure portal
-  Azure Active Directory
-  Azure AD B2C
-  Multi-Factor Authentication
-  Automation
-  Key Vault
-  Azure Marketplace
-  VM Image Gallery
-  REST API and CLI

## Media & CDN

-  Media Services
-  Media Analytics
-  Content Delivery Network

## Integration

-  API Management
-  Service Bus
- 

## Compute Services

-  Container Service
-  VM Scale Sets
- 
- 

## Application Platform

-  Web Apps
-  Mobile Apps
-  API Apps
-  Cloud Services
-  Service Fabric
-  Notification Hubs
-  Functions

## Data

-  SQL Database
-  Azure Synapse Analytics
-  Cosmos DB
-  SQL Server Stretch Database
-  Azure Cache for Redis
-  Table Storage
-  Azure Search

## Intelligence

-  Cognitive Services
-  Bot Services
-  Azure ML Studio

## Analytics & IoT

-  HDInsight
-  Machine Learning
-  Stream Analytics
-  Data Catalog
-  Data Lake Analytics Service
-  Data Lake Storage
-  IoT Hub
-  Event Hubs
-  Data Factory
-  Power BI Embedded

## Infrastructure Services

### Compute

-  Virtual Machines
-  Containers and Azure Kubernetes

### Storage

-  Blob
-  Queues
-  Files
-  Disks

### Networking

-  Virtual Network
-  Load Balancer
-  DNS
-  Express Route
-  Traffic Manager
-  VPN Gateway
-  App Gateway

## Datacenter Infrastructure



## Hybrid Cloud

-  Azure AD Connect Health
-  AD Privileged Identity Management
-  Domain Services
-  Backup
-  Azure Monitor
-  Import/Export
-  Azure Site Recovery
-  StorSimple



# Les datacenter Microsoft Azure

Azure est présent sur la totalité des continents



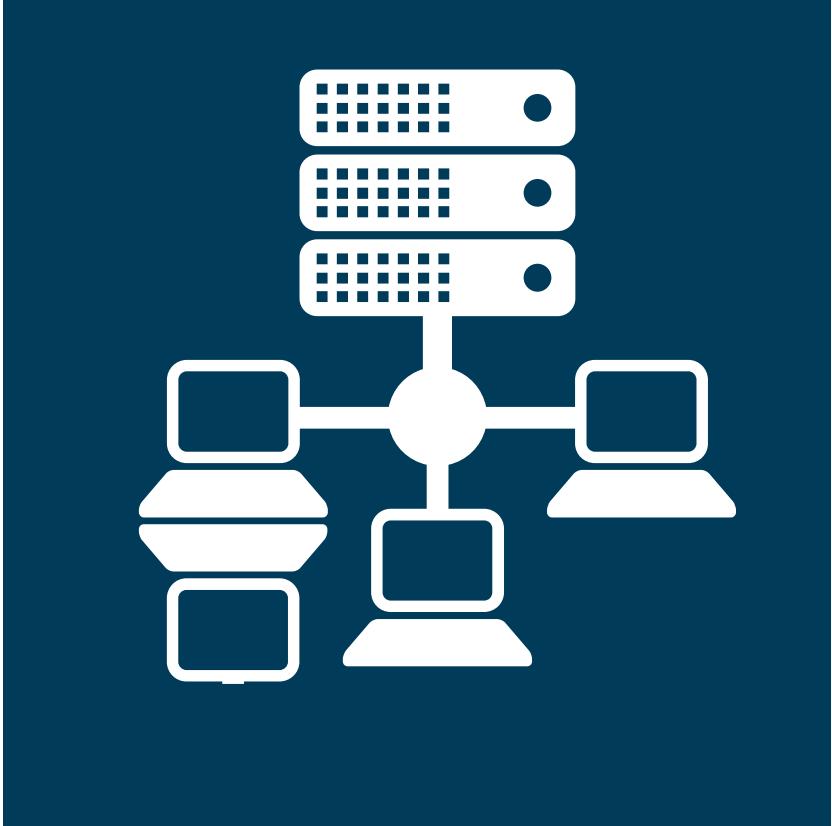
<https://azure.microsoft.com/fr-fr/regions/>

\* Trois régions Azure Government non divulguées



# Les niveaux de services attendus (SLA)

Microsoft s'engage contractuellement sur le niveau de disponibilité des services



Chaque service est caractérisé par un SLA

Résumé des SLA pour les services azure :

<https://azure.microsoft.com/fr-fr/support/legal/sla/>

**Exemple pour les machines virtuelles :**

VM	%	Equivalent temps /an
Minimum 2 instances sur 2 « Availability Zones » distinctes dans la même région azure	99,99 %	52 mn
Minimum 2 instances dans le même groupe à haute disponibilité	99,95%	4h 22mn
VM unique stockage Premium SSD (OS et Data)	99,9 %	8h 45mn
VM unique stockage SSD Standard (OS et Data)	99,5 %	1j 19h 49mn
VM unique stockage HDD Standard (OS et Data)	95%	18j 6h 17mn

## Ce qui est inclus

- ✓ Pannes matérielles (disques, CPU, mémoire)
- ✓ Pannes de datacenter – pannes réseau, pannes électriques
- ✓ Mises à jour matérielles, maintenance logicielle – maj de l'OS de l'hôte
- ✓ Arrêts planifiés – Notification de 6j, fenêtre de 6h, 25 minutes d'arrêt

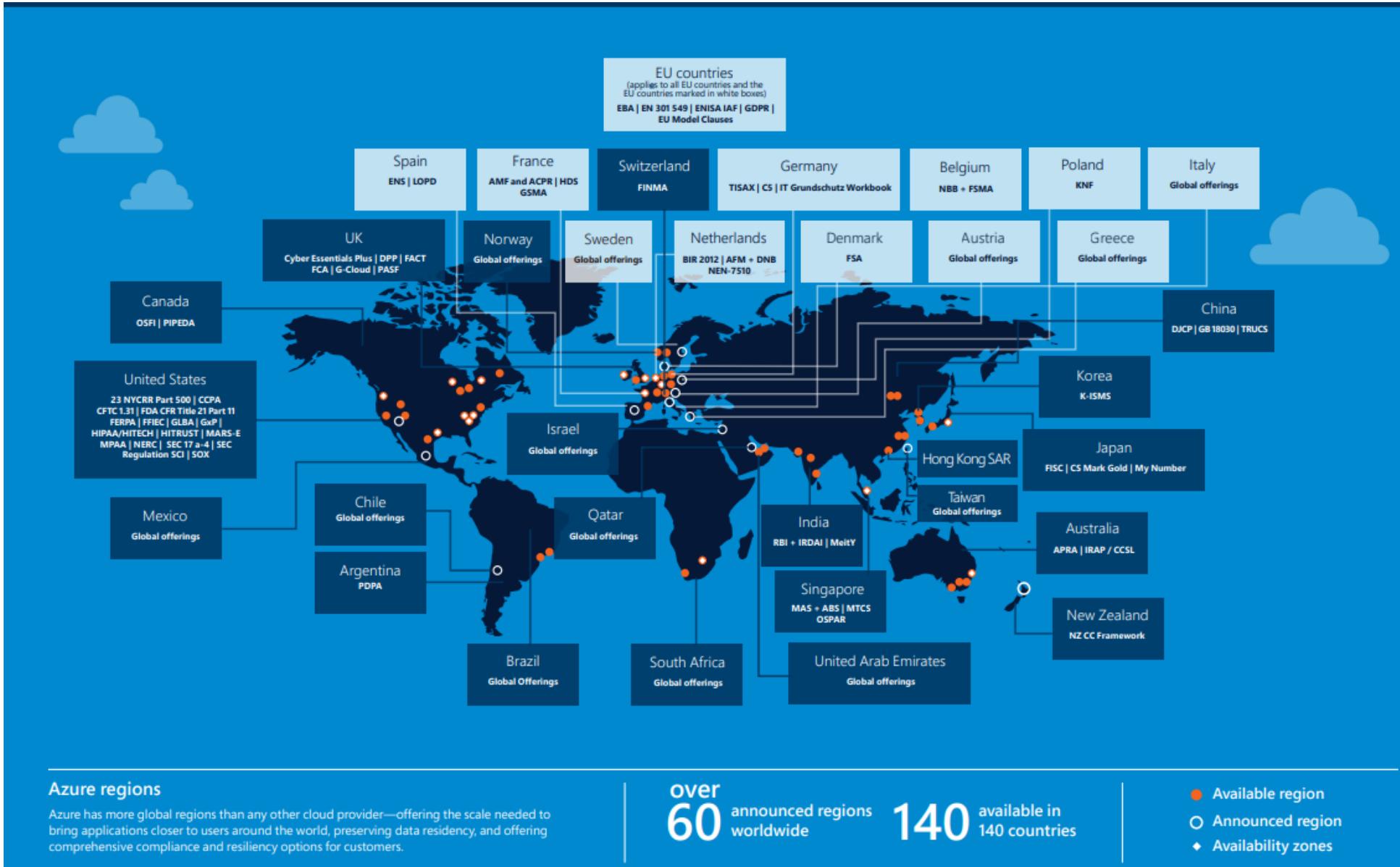
## Ce qui n'est pas inclus

- ✓ Crashes de VM dus à des logiciels tiers, maj OS invité



# Conformité et certifications

<https://docs.microsoft.com/fr-fr/compliance/regulatory/offering-home>





# Outilage pour les Admins

**Portail Azure**  
Page web dédiée à l'administration de l'environnement Azure.



Bienvenue dans Azure !  
Vous n'avez pas d'abonnement ? Consultez les options suivantes.

Commencer par un essai gratuit d'Azure  
Obtenez 200 USD de crédit gratuit sur les produits et services Azure, plus 12 mois de [services gratuits populaires](#).  
[Démarrer](#) [En savoir plus](#)

Gérer Azure Active Directory  
Gérez l'accès, définissez des stratégies intelligentes et améliorez la sécurité avec Azure Active Directory.  
[Voir](#) [En savoir plus](#)

Accéder aux avantages des étudiants  
Bénéficiez de logiciels gratuits, de crédit Azure ou d'un accès à Azure Dev Tools for Teaching après avoir vérifié votre statut scolaire.  
[Explorer](#) [En savoir plus](#)

Services Azure

- Créer une ressource
- Machines virtuelles
- App Services
- Comptes de stockage
- Bases de données SQL
- Serveurs Azure Database po...
- Azure Cosmos DB
- services Kubernetes
- Application de fonction
- Autres services

Eliot.Testing.Integration.Core.csproj - Visual Studio Code

File Edit Selection View Go Debug Terminal Help

DEBUG No Configurations VARIABLES WATCH CALL STACK

```
149 <Reference Include="PCLCrypto, Version=2.0.0.0, Culture=neutral, PublicKeyToken=null, processorArchitecture=Any" HintPath="..\packages\PCLCrypto.2.0.147\lib\net45\pclcrypto.dll" />
150 </Reference>
151 <Reference Include="PInvoke.BCrypt, Version=0.5.0.0, Culture=neutral, PublicKeyToken=null, processorArchitecture=Any" HintPath="..\packages\PInvoke.BCrypt.0.5.111\lib\net45\bcrypt.dll" />
152 </Reference>
153 <Reference Include="PInvoke.Kernel32, Version=0.5.0.0, Culture=neutral, PublicKeyToken=null, processorArchitecture=Any" HintPath="..\packages\PInvoke.Kernel32.0.5.111\lib\net45\kernel32.dll" />
154 </Reference>
155 <Reference Include="PInvoke.NCrypt, Version=0.5.0.0, Culture=neutral, PublicKeyToken=null, processorArchitecture=Any" HintPath="..\packages\PInvoke.NCrypt.0.5.111\lib\net45\ncrypt.dll" />
156 </Reference>
157 <Reference Include="PInvoke.Windows.Core, Version=0.5.0.0, Culture=neutral, PublicKeyToken=null, processorArchitecture=Any" HintPath="..\packages\PInvoke.Windows.Core.0.5.111\lib\net45\windowscore.dll" />
158 </Reference>
159 <Reference Include="RestSharp, Version=106.5.2.0, Culture=neutral, PublicKeyToken=null, processorArchitecture=Any" HintPath="..\packages\RestSharp.106.5.2\lib\net452\RestSharp.dll" />
160 </Reference>
161 <Reference Include="System" />
162 <Reference Include="System.Collections.Immutable, Version=1.5.0.0, Culture=neutral, PublicKeyToken=cc7b13ffcd2ddd51, processorArchitecture=Any" HintPath="..\packages\System.Collections.Immutable.1.5.0\lib\net45\System.Collections.Immutable.dll" />
163 </Reference>
164 <Reference Include="System.Linq, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089, processorArchitecture=Any" HintPath="..\packages\System.Linq.4.0.0\lib\net45\System.Linq.dll" />
165 </Reference>
166 <Reference Include="System.Net.Http, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089, processorArchitecture=Any" HintPath="..\packages\System.Net.Http.4.0.0\lib\net45\System.Net.Http.dll" />
167 </Reference>
168 <Reference Include="System.Threading.Tasks, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089, processorArchitecture=Any" HintPath="..\packages\System.Threading.Tasks.4.0.0\lib\net45\System.Threading.Tasks.dll" />
169 </Reference>
170 <Reference Include="System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089, processorArchitecture=Any" HintPath="..\packages\System.Xml.4.0.0\lib\net45\System.Xml.dll" />
171 </Reference>
```

Ln 164, Col 34 (9 selected) Spaces: 2 UTF-8 with BOM CRLF XML 🔍 🔔



**Visual Studio Code**  
IDE récent avec possibilité d'intégration de module Azure.

# Outilage pour les Admins



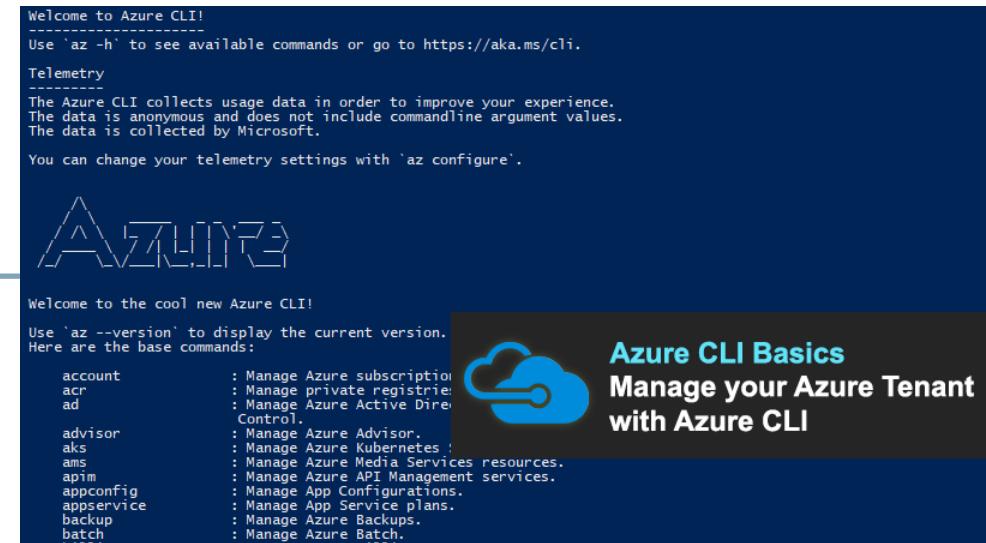
## Az Cli/ Cloud Shell

Permet uniquement l'intéraction avec les ressources Azure.



## Powershell + Module « Az » / « AzureAD »

Permet l'intéraction avec l'environnement Azure via CLI.  
Idéal pour le scripting et plus fiable que le portail.





2400 XP

## Microsoft Azure Fundamentals: Describe cloud concepts

52 min • Learning Path • 0 of 3 modules completed

Beginner   Administrator   Developer   DevOps Engineer   Solution Architect   Azure

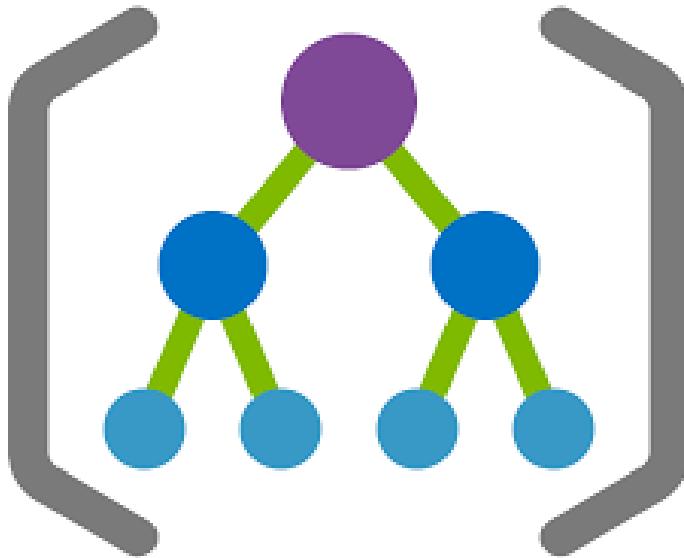
This learning path helps prepare you for [Exam AZ-900: Microsoft Azure Fundamentals](#).

### Prerequisites

- Basic familiarity with IT terms and concepts

Start >

⊕ Save





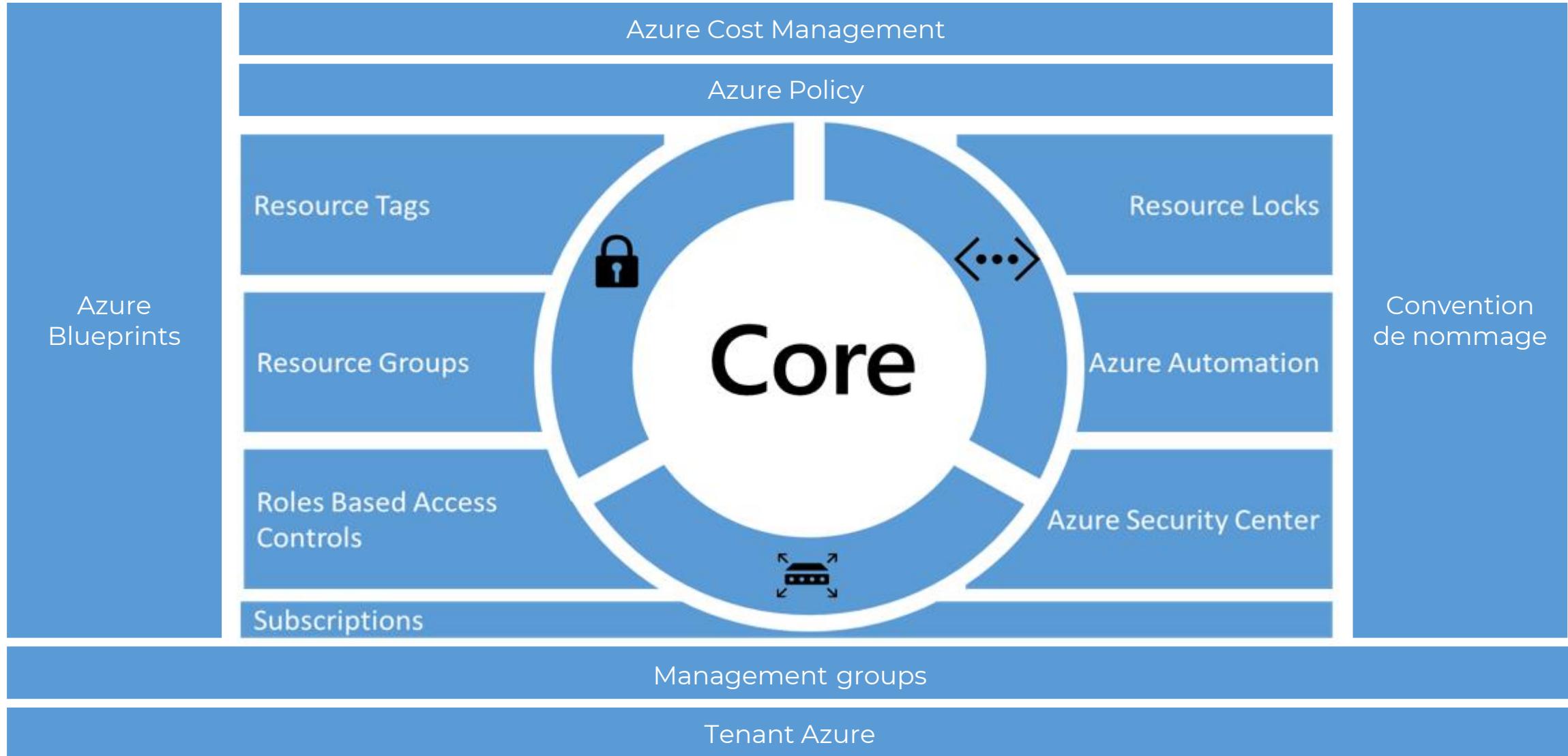
# Gouvernance

## Introduction

- ✓ La gouvernance est la mise en œuvre d'un ensemble de dispositifs (règles, normes, protocoles, conventions, contrats...) pour assurer une meilleure coordination des parties prenantes d'une organisation sur un sujet donné, chacune détenant une parcelle de pouvoir, afin de prendre des décisions consensuelles et de lancer des actions concertées.
  - ✓ La gouvernance Cloud permet de mettre en place des garde-fous permettant de respecter les contraintes de l'entreprise.
- 
- ✓ **Organisation des ressources**
    - ✓ Comment les regrouper ?
    - ✓ Comment les isoler les unes des autres ?
    - ✓ Définir des autorisations d'accès
    - ✓ Fournir des information supplémentaire sur les ressources
    - ✓ Verrouiller des ressources
  - ✓ **Définition de stratégies**
    - ✓ Création, attribution et gestion des stratégies sur les ressources
    - ✓ Orchestration du déploiement de modèles de ressources
  - ✓ **Gestion des coûts**

# Gouvernance

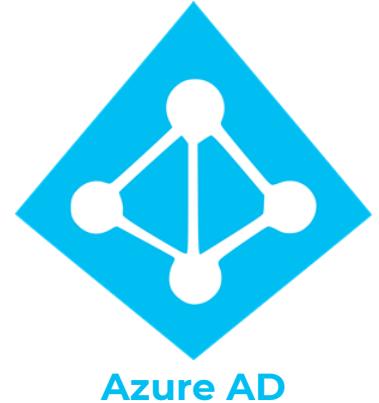
Les outils / fonctionnalités proposés par Microsoft





# Azure Active Directory

Qu'est-ce qu'est Azure AD ?



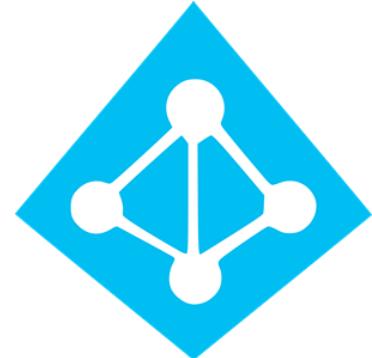
Azure AD

- Azure Active Directory (Azure AD) est le service de gestion de l'accès et des identités basé sur le cloud de Microsoft. Il permet à vos employés de se connecter et d'accéder aux ressources suivantes :
  - Ressources externes telles que Microsoft 365, le portail Azure et des milliers d'autres applications SaaS.
  - Ressources internes telles que les applications situées sur votre réseau d'entreprise et intranet ainsi que les applications cloud développées par votre propre organisation.



# Azure Active Directory

Principales fonctionnalités d'Azure AD



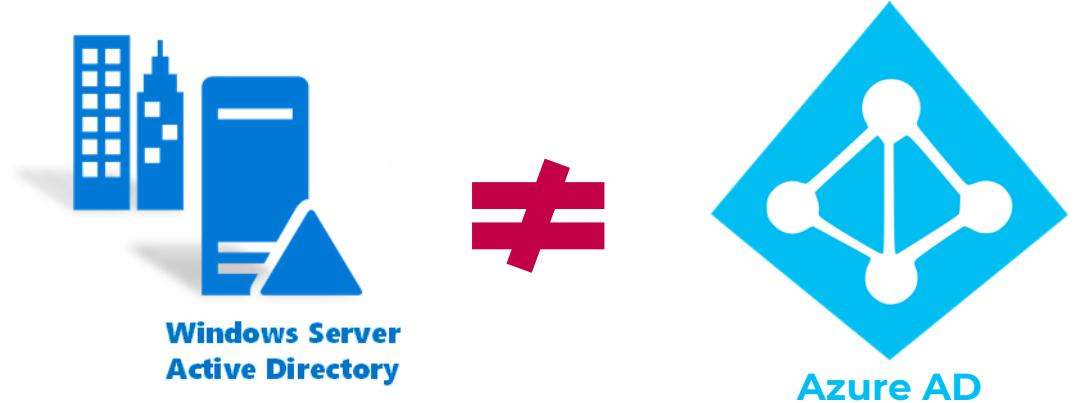
Azure AD

- ✓ Gestion des identités et des accès de base
- ✓ Gestion des applications
- ✓ Gouvernance des identités
- ✓ Azure AD Connect
- ✓ Identités gérées pour les ressources Azure



# Azure Active Directory

Qu'est-ce qu'est Azure AD ?

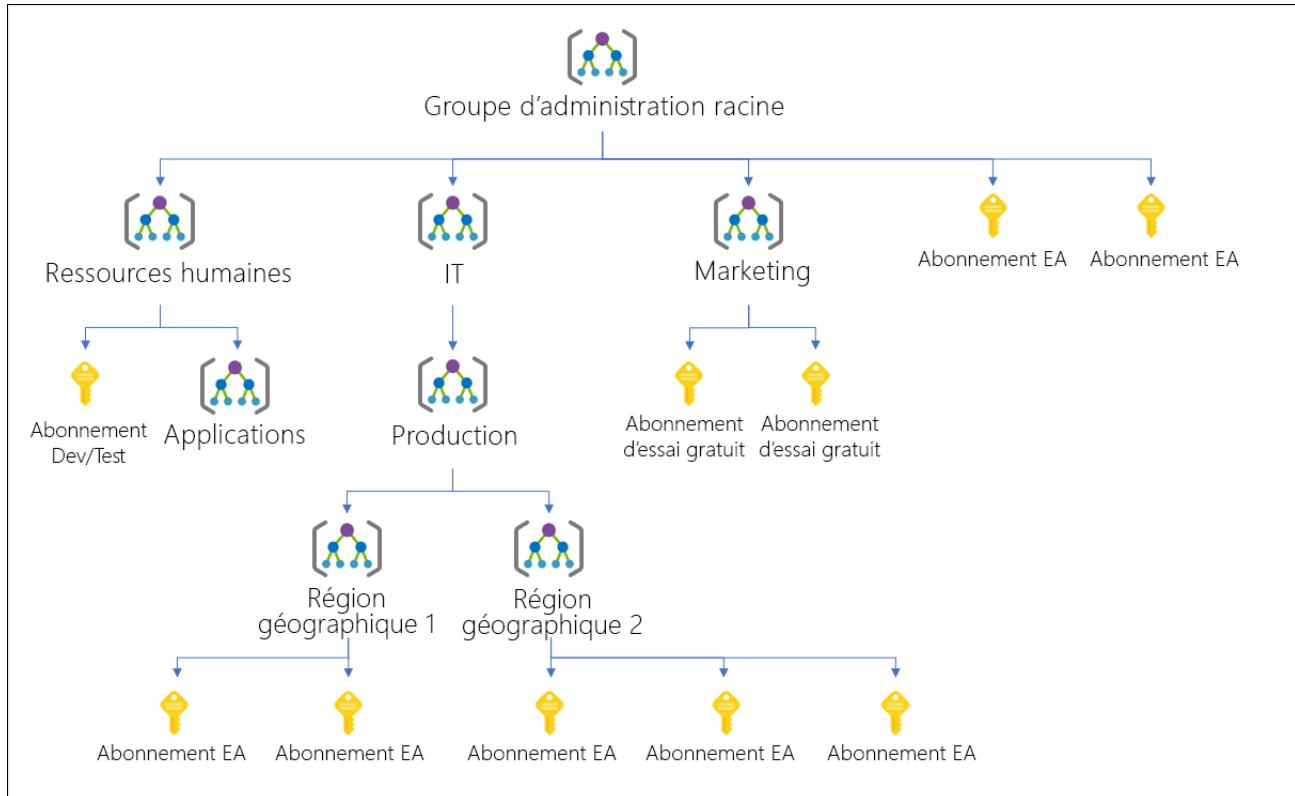


**Azure AD n'est pas un service Active Directory pour Azure !**

# Gouvernance

## Organisation des ressources - « Management Group »

- ✓ Gestion de plusieurs « Subscription »
  - ✓ Gestion des accès, stratégies et la conformité de ces « Subscription »
- ✓ Pour fournir un niveau d'étendue au-dessus des « Subscription »:
  - ✓ Organisation des « Subscription » en conteneurs et appliquer les conditions de gouvernance aux « Management Group ».
  - ✓ Héritage automatique des conditions appliquées au « Management Group » à toutes les « Subscription » membres.
  - ✓ Toutes les « Subscription » doivent approuver le même « Tenant » Azure Active Directory





# Gouvernance

## Organisation des ressources - « Subscription » - définition

- ✓ Une « Subscription » Azure correspond à un abonnement Azure spécifique permettant d'utiliser et de gérer des ressources Azure
- ✓ La séparation en différentes « Subscription » Azure intervient pour :
  - ✓ Faciliter la facturation
  - ✓ Rendre étanche des environnements
  - ✓ Réaliser de l'overlap réseau
  - ✓ Outrepasser les quotas de ressources et certaines limites
    - ✓ Exemples :
      - ✓ 25000 VM
      - ✓ 980 « Resource group »
      - ✓ 250 comptes de stockage
      - ✓ 2000 attributions de rôle
      - ✓ etc



# Gouvernance

Organisation des ressources - « Subscription » - les différents types

Liste non exhaustive :

✓ **Pay as you go**

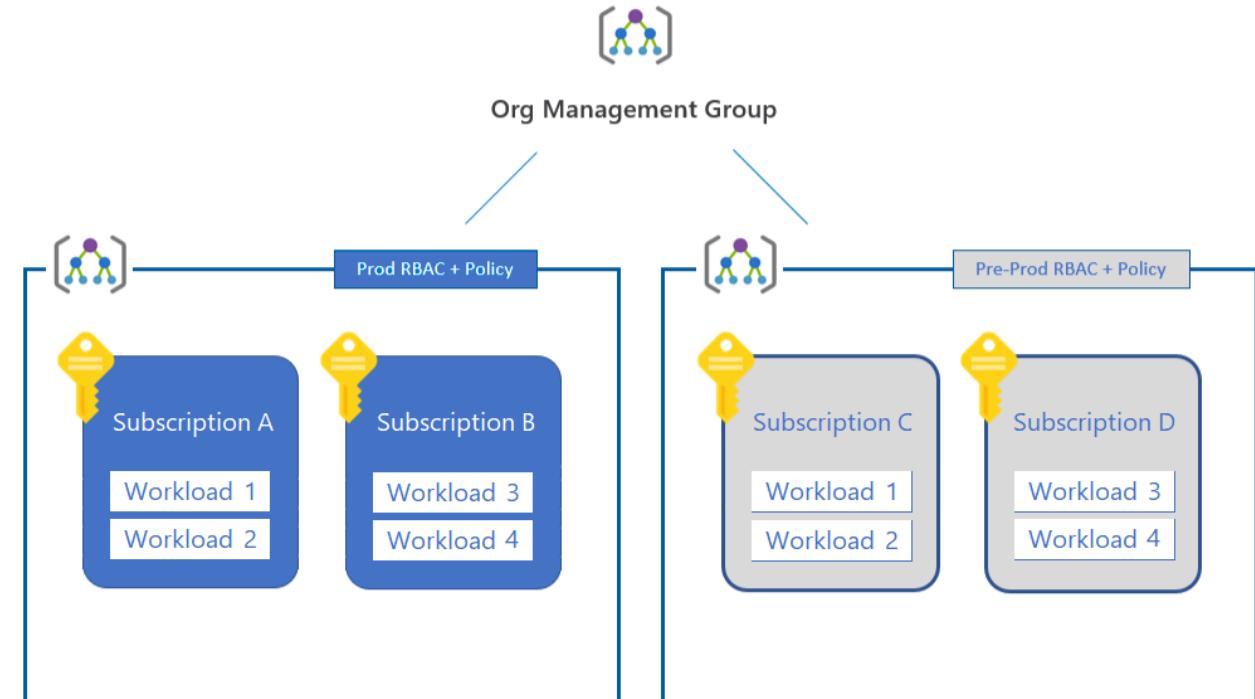
- ✓ Tarification à l'utilisation.
- ✓ Paiement chaque mois uniquement en fonction de l'utilisation, sans coût initial
- ✓ Annulation possible à tout moment.
- ✓ Nécessite l'inscription d'une Carte Bancaire.

✓ **Enterprise Agreement (EA)**

- ✓ Obtention de services en ligne avec engagement sur une période donnée
- ✓ Economies intégrées allant de 15 à 45 % en fonction des dépenses engagées

✓ **Cloud Solution Provider (CSP)**

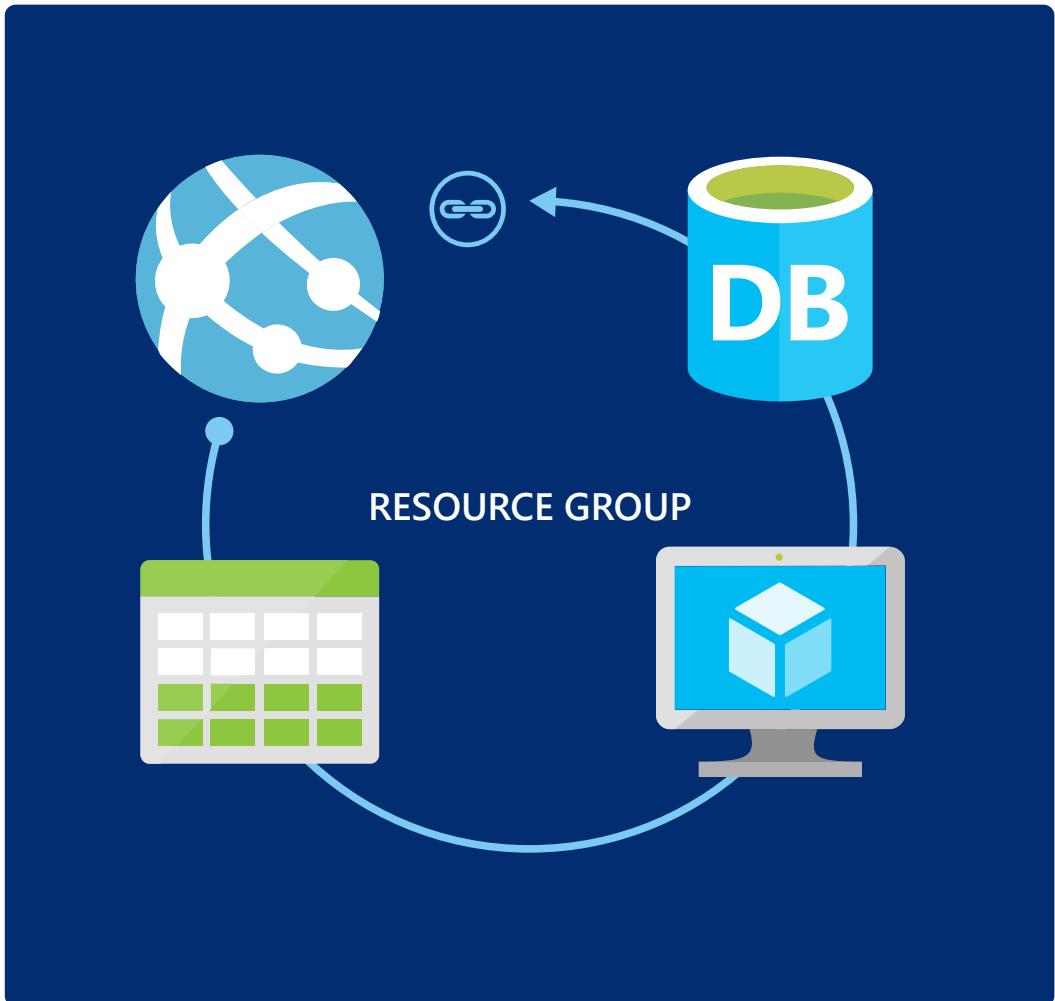
- ✓ Collaboration avec un partenaire pour concevoir et implémenter une solution complète.
- ✓ Gestion de la facturation et support technique par le partenaire.



# Gouvernance

Organisation des ressources - « Resource Group » - définition

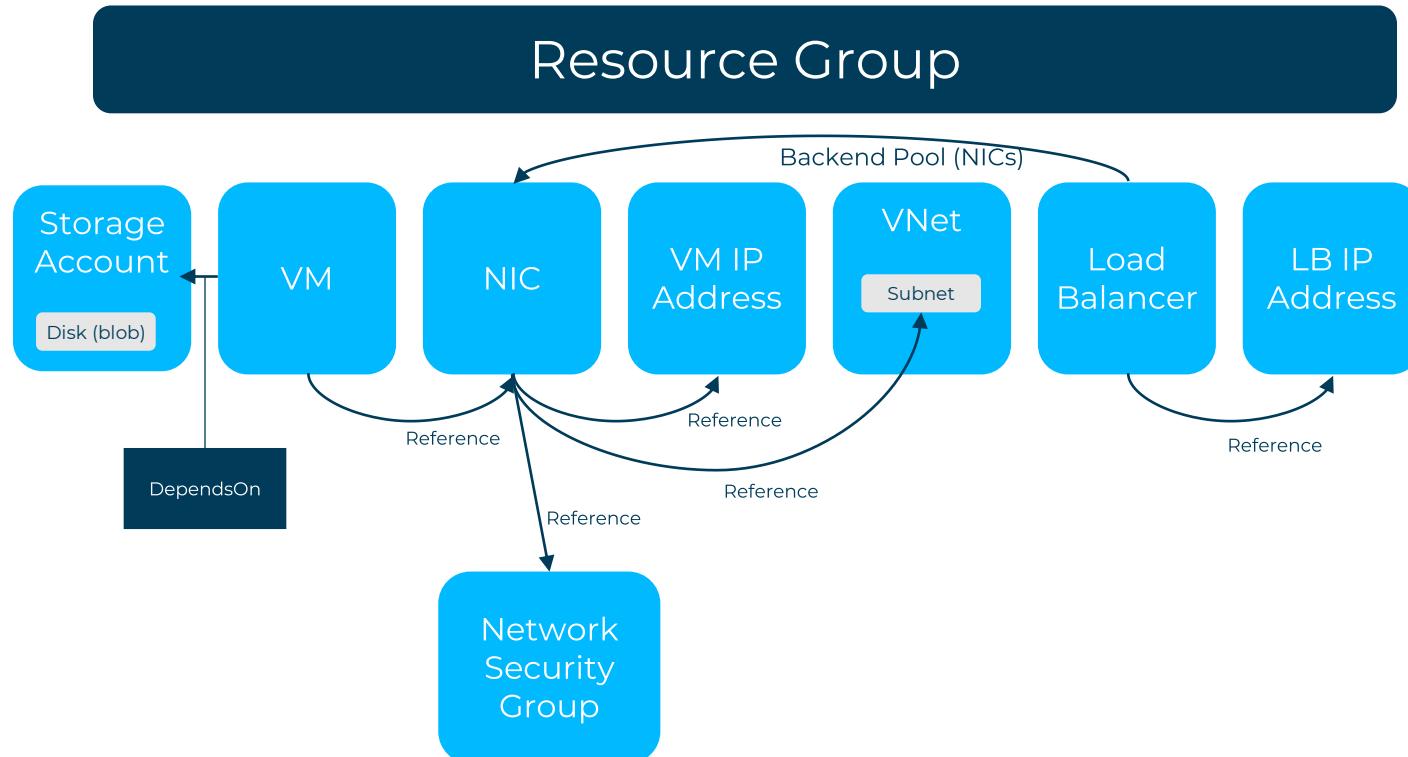
- ✓ Conteneur logique qui permet de grouper des ressources (services) au sein d'une même « Subscription » pour :
  - Segmenter une souscription Azure et limiter les droits
  - Simplifier la lecture de la facture
  - Simplifier la gestion du cycle de vie d'un service
  - Appliquer des règles d'utilisation
- ✓ Les « Resource Group » ne peuvent pas être imbriqués et une ressource n'appartient qu'à un seul et même « Resource Group »
- ✓ La suppression d'un « Resource Group » entraîne la suppression de l'ensemble des ressources qu'il contient





# Gouvernance

Organisation des ressources - « Resource Group » - Exemple pour une machine virtuelle





# Gouvernance

## Organisation des ressources - Localisation

- ✓ Choisir la zone géographique Azure selon ces 3 critères :

- ✓ Conformité et résidence des données

- ✓ Exemple Suisse :

Conformité globale

CIS Benchmark, CSA STAR Attestation, CSA STAR Certification, CSA STAR Self-Assessment, ISO 20000, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 9001, SOC 1, SOC 2, SOC 3, WCAG 2.0

Conformité régionale/nationale

HDS, EN 301 549, ENISA IAF, EU Model Clauses, EU-US Privacy Shield, GDPRConformité du secteur d'activitéAMF/ACPR, EBA, CDSA, GxP, PCI DSS, Shared Assessments, TruSight

- ✓ Disponibilité du service

- ✓ Exemple Suisse Nord : <https://azure.microsoft.com/fr-fr/global-infrastructure/services/?regions=switzerland-north%2cnon-regional&products=all>

- ✓ Tarification

- ✓ Comparer les coûts par localisation : <https://azure.microsoft.com/fr-fr/pricing/>



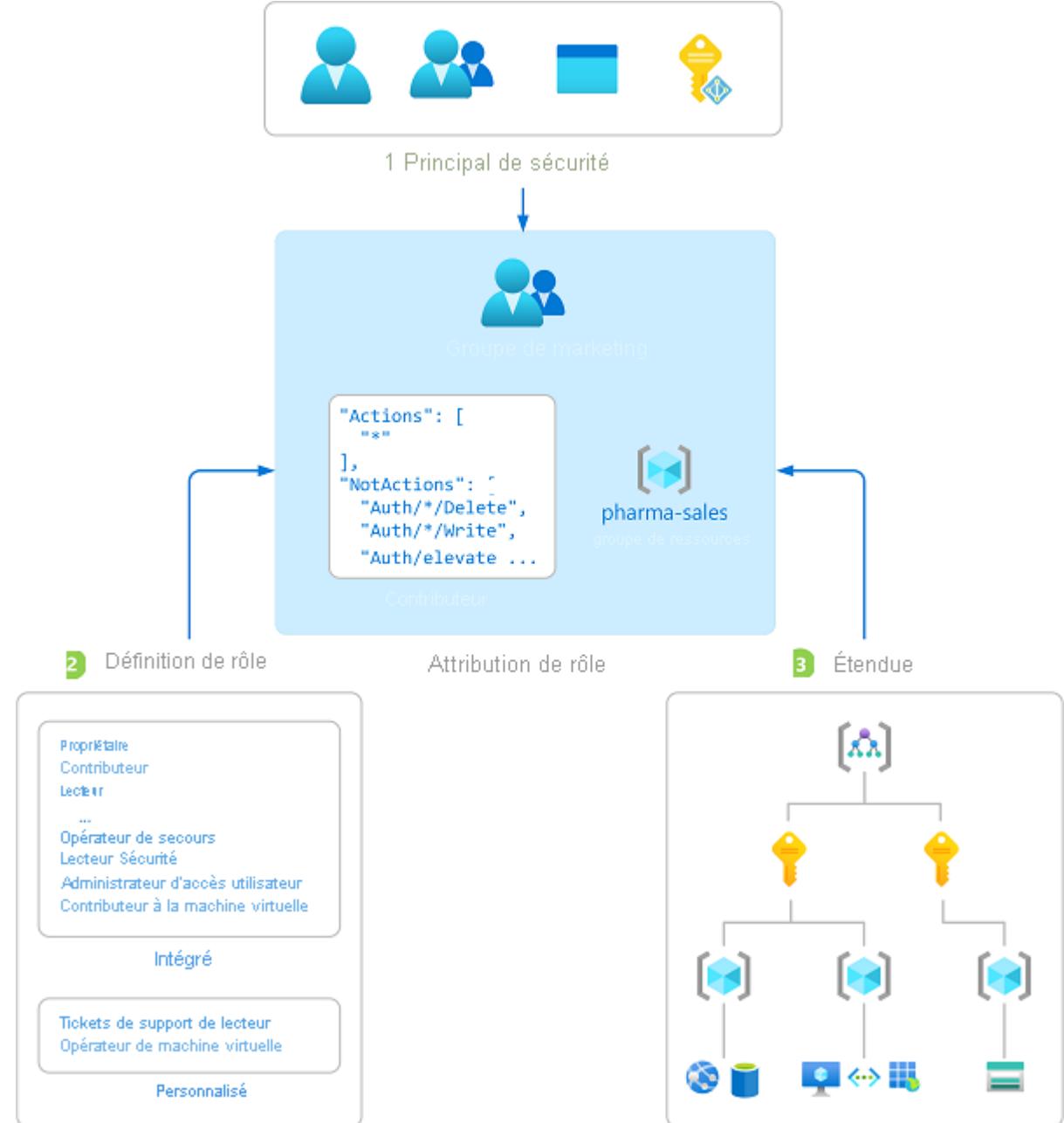
# Gouvernance

## Organisation des ressources - RBAC

- ✓ Contrôle d'accès aux ressources à l'aide du RBAC Azure.

Composition d'une attribution de rôle :

- ✓ Un **objet identité** :
  - ✓ un utilisateur, un groupe, un « Service Principal » ou une « Managed Identity » demandant l'accès à des ressources Azure
- ✓ Un **rôle** :
  - ✓ Collection d'autorisation appliquée à l'identité
- ✓ Un **périmètre** :
  - ✓ Ensemble des ressources auxquelles l'accès s'applique





# Gouvernance

## Organisation des ressources - RBAC

- ✓ 2 types de rôles
  - ✓ Natifs : règles d'accès prédéfinies sur les ressources cloud
  - ✓ Personnalisés : règles à construire

- ✓ Héritage du parent sur toutes les objets enfants

Quelques exemples d'affectation :

- ✓ Rôle « **Owner** » attribué à un utilisateur au niveau d'un « Management Group »:
  - ✓ Tous les droits sur les « Subscription » au sein du « Management Group »
- ✓ Rôle « **Reader** » attribué à un groupe au niveau d'une « Subscription »:
  - ✓ Droit de lecture sur l'ensemble des « Resource Group » et ressources au sein de la « Subscription »
- ✓ Rôle « **Contributor** » attribué à une application au niveau d'un « Resource Group »:
  - ✓ Tous les droits (sauf celui de manipuler les permissions) sur l'ensemble des ressources au sein du « Resource Group »

		Rôle			
	Lecteur	Spécifique à la ressource	Personnalisé	Contributeur	Propriétaire
Étendue					
Groupe d'administration	Lecteur				
Abonnement	Observateurs				
Groupe de ressources			Utilisateurs gérant les ressources		Administrateurs
Ressource				Processus automatisés	

# Gouvernance

## Organisation des ressources - les « Tag » - définition

- ✓ Les « Tag » vont permettre de pouvoir identifier les ressources à partir de mots-clés pouvant ensuite être utilisés dans des scripts, en facturation ou à des fins d'identification
- ✓ Les « Tag » peuvent être provisionnées sur les « Resource Group » ou les ressources
- ✓ Une balise est constituée d'un couple nom-valeur (exemple : Environment:dev)
- ✓ Chaque ressource ou « Resource Group » peut contenir jusqu'à 50 « Tag »
  - Nom limité à 512 caractères
  - Valeur limitée à 256 caractères
  - Pour les VM et Groupes d'affinités, limitation totale à 2048 caractères
- ✓ Il n'y a pas d'héritage entre « Resource Group » et ressources

# Gouvernance

Organisation des ressources - les « Tag » - exemples

✓ Exemples de « Tag » fréquemment utilisées :

- Billing : avec un code de facturation interne
- ProductOwner : avec l'adresse mail ou le nom du responsable de l'application
- ProjectName : avec le nom du projet / produit
- ProjectVersion : avec la version du projet / produit
- Environment : avec le type d'environnement (Prod, Dev, Rec...)
- Confidentiality : avec le niveau de confidentialité des données (Public, Interne, Restreint, Confidentiel...)
- Start : avec l'heure de démarrage de l'environnement
- Stop : avec l'heure d'arrêt de l'environnement
- Tier : avec le nom du tier (front, back, db, web, app...)



# Gouvernance

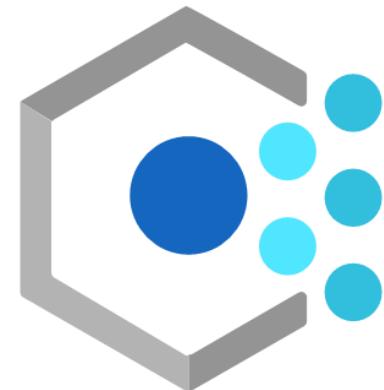
Organisation des ressources - les « Lock »

- ✓ La fonctionnalité de verrouillage des ressources permet de verrouiller une « Subscription », une ressource ou un « Resource Group » afin d'éviter toute modification ou suppression accidentelle de ressources critiques
- ✓ 2 niveaux :
  - Lecture seule : empêche les modifications
  - Supprimer : empêche les suppressions mais permet les modifications
- ✓ Application via le portail, par modèles ou par script

# Gouvernance

## Azure Policy

- ✓ Azure Policy permet de contrôler (mode « audit ») le respect de règles ou de forcer l'application de règles (mode « enforce »)
- ✓ Règles standards ou définition de règles personnalisées
- ✓ S'applique à :
  - Un « Management Group »
  - Une « Subscription »
  - Un « Resource Group »
- ✓ Exemples
  - Localisations (datacenter) Azure autorisées
  - Types de ressources autorisées
  - Storage SKUs autorisés
  - Application des tags et de leur valeur par défaut
  - Versions de Azure SQL autorisées
  - Forcer le chiffrement des comptes de stockage

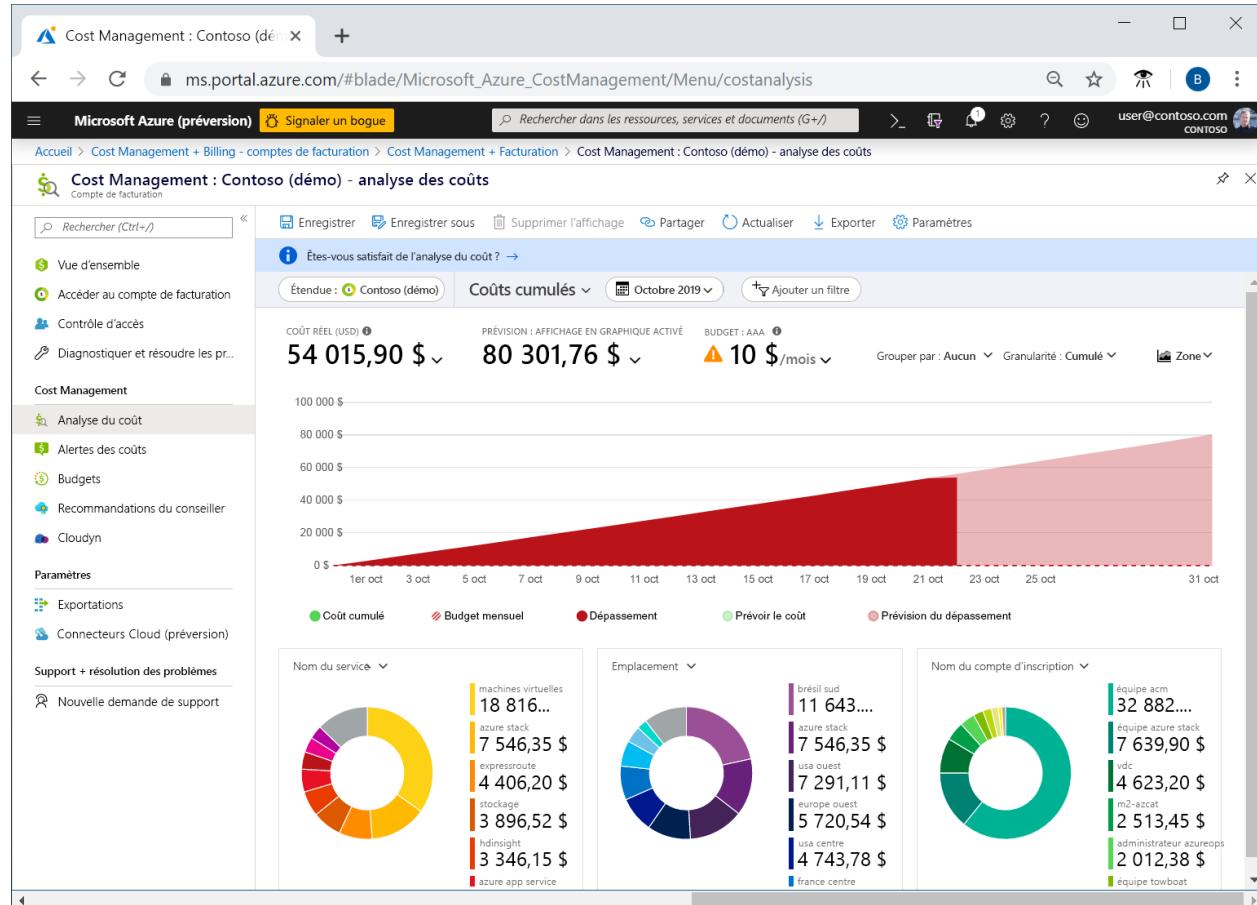




# Gouvernance

## Gestion des coûts / Azure Cost Management

- ✓ Suivre l'utilisation des ressources et gérer les coûts avec une vue unique.
- ✓ Passer en revue les **coûts par abonnements** et visualiser les données grâce aux filtres par défaut (coûts cumulés, coût réel, prévision, budget, etc...)
- ✓ Personnaliser les **vues**, les enregistrer comme modèle, les partager et exporter les données au format graphique, ou bien Excel ou CSV.
- ✓ Créer un **budget** pour gérer les coûts de manière proactive et de superviser la progression des dépenses. Des notifications peuvent être déclenchées en cas de dépassement.



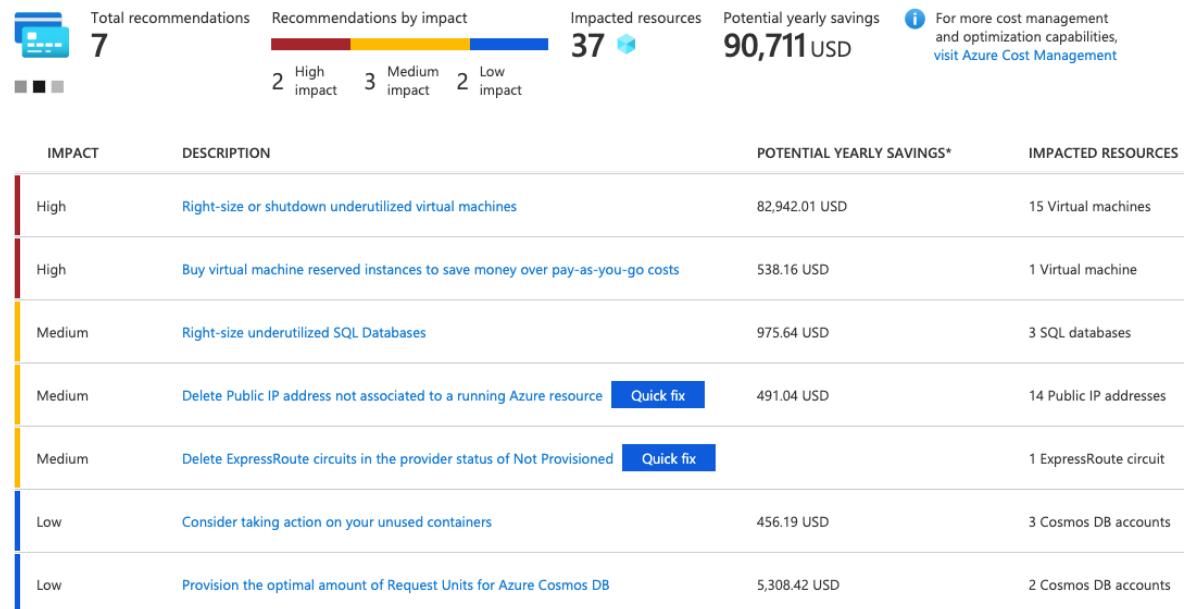


# Gouvernance

## Gestion des coûts

Quelques axes :

- ✓ Comprendre les coûts estimés avant le déploiement à l'aide de la **calculatrice Azure**
- ✓ Utiliser « **Azure Advisor** » pour superviser l'utilisation. Identifier les ressources inutilisées ou sous-utilisées.
- ✓ Choisir des régions Azure et emplacements de faible coût
- ✓ Utiliser **Azure Cost Management + Billing** pour contrôler les dépenses
- ✓ Utiliser des **limites de dépense**
- ✓ **Redimensionner** les machines virtuelles sous-utilisées
- ✓ **Libérer** les machines virtuelles en dehors des heures d'activité
- ✓ **Supprimer** les ressources inutilisées



# Gouvernance

## Convention de nommage

- ✓ Une convention de nommage efficace compose des noms de ressources à partir d'informations importantes sur les ressources
- ✓ Prérequis
  - Certaines ressources n'acceptent que des chiffres et lettres
  - Certaines ressources n'acceptent que des minuscules
  - Certaine ressources utilisent leur noms comme URL d'accès et doivent être unique pour Azure « Monde » (exemple : compte de stockage)
- ✓ Penser une convention de nommage par type de ressources est complexe

Exemples :

- ✓ Type de ressource Azure (ex : rsg, vmw, etc...)
- ✓ Projet
- ✓ Environnement (ex : prd, dev, qal, etc...)
- ✓ Région (ex : frc, swn, swe, etc...)

LYNINF Azure Subscription Naming Convention					
Version 1					
Azure resources					
<u>Location</u>	+ <u>Trigramm</u>	+ <u>Service</u>	+ <u>Projet</u>	+ <u>Type</u>	+ <u>Counter</u>
3 char	3 char	3 char	3 char	1 char	2 digits
frc	jeu	vmw	zzz	f	0
<b>frcjeuvmwzzzf0</b>					

# Discussions, questions, démonstrations



# Microsoft Learning Path



3300 XP

## Azure Fundamentals: Describe Azure management and governance

1 hr 50 min • Learning Path • 0 of 4 modules completed

Beginner Administrator Developer DevOps Engineer Solution Architect Azure

The Microsoft Azure Fundamentals training is composed of three learning paths: Microsoft Azure Fundamentals: Describe cloud concepts, Describe Azure architecture and services, and Describe Azure management and governance. Microsoft Azure Fundamentals: Describe Azure management and governance is the third learning path in Microsoft Azure Fundamentals. This learning path explores the management and governance resources available to help you manage your cloud and on-premises resources.

This learning path helps prepare you for Exam AZ-900: Microsoft Azure Fundamentals.

### Prerequisites

- Basic familiarity with IT terms and concepts

[Start >](#) [Save](#)

36



# Microsoft Learning Path



**Describe cost management in Azure**

43 min • Module • 0 of 9 units completed

★★★★★ 4.8 (2,321)

This module explores methods to estimate, track, and manage costs in Azure.

[Start >](#)

[Overview ▾](#)

[Save](#)



**Describe features and tools in Azure for governance and compliance**

34 min • Module • 0 of 8 units completed

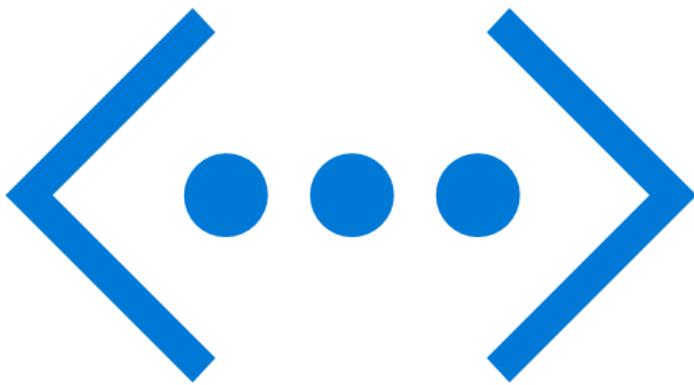
★★★★★ 4.8 (1,627)

This module introduces you to tools that can help with governance and compliance within Azure.

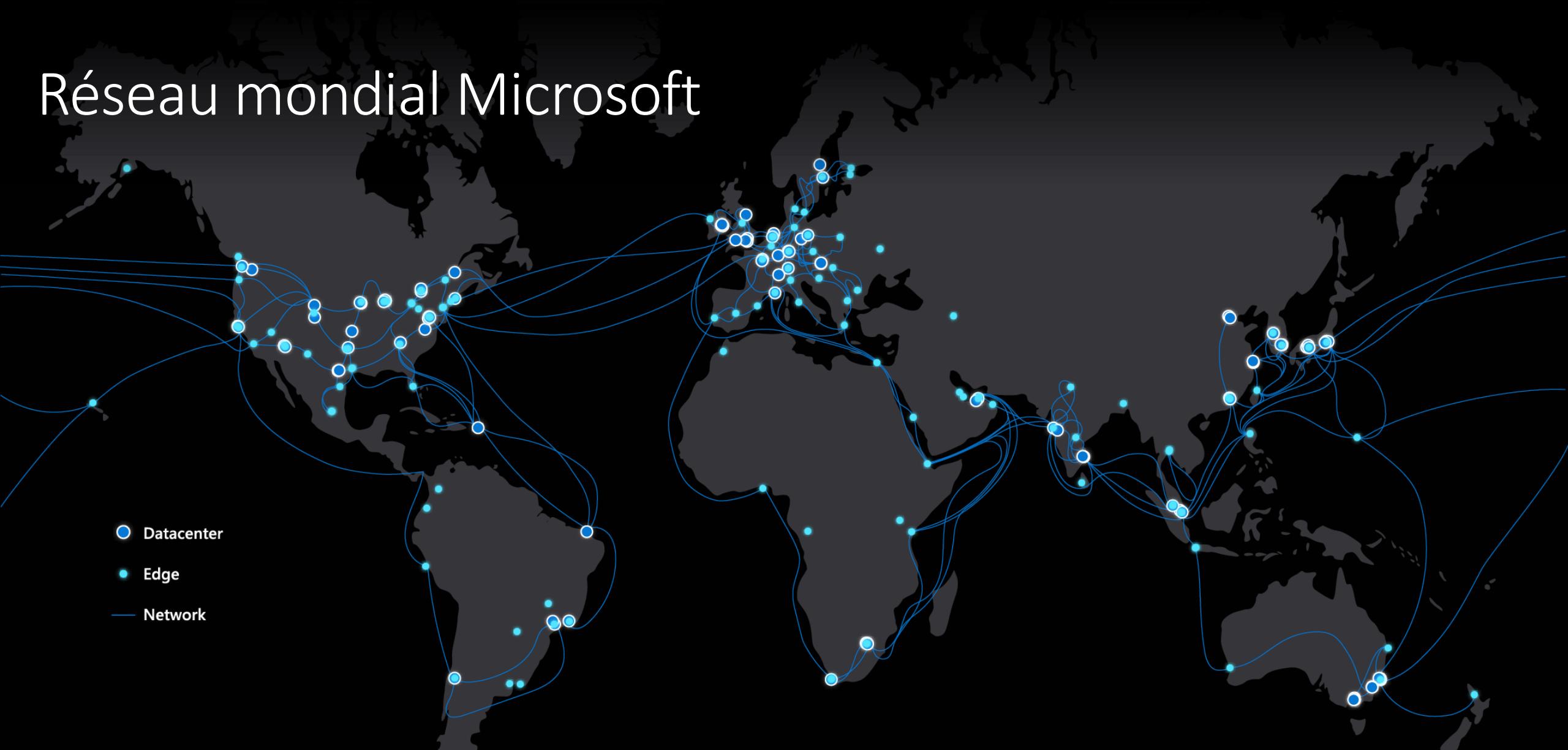
[Overview ▾](#)

[Save](#)

37



# Réseau mondial Microsoft



61 Azure regions

130K+ miles of fiber and  
subsea cables

170 edge sites

200+ ExpressRoute  
partners

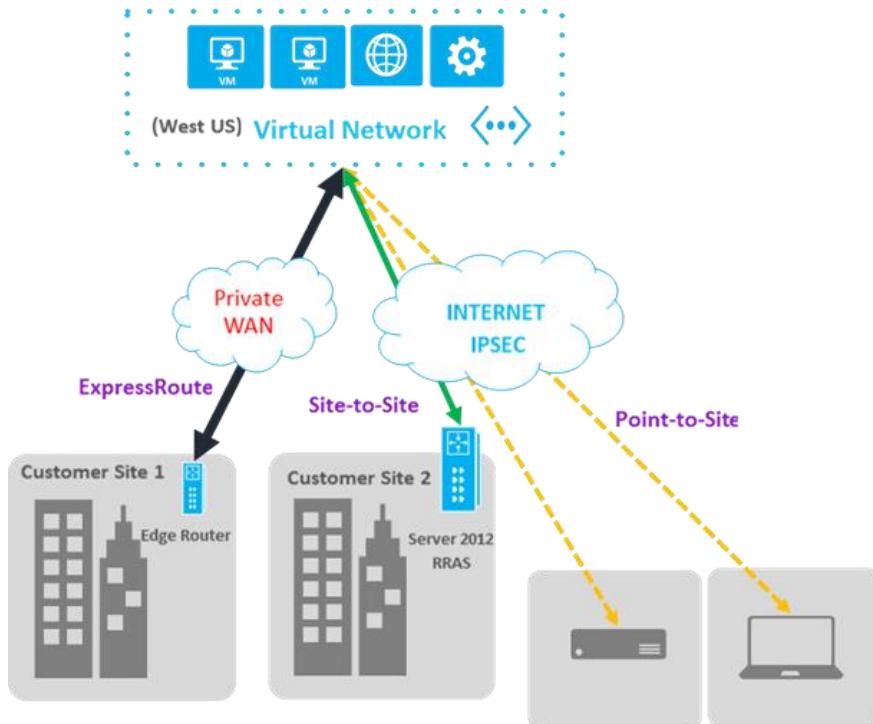
# Réseau Azure

Généralités – vue d'ensemble

**Azure virtual network** permet la communication sécurisée entre ressources Azure, avec Internet et sur des réseaux locaux.

Principaux scénarios :

- ✓ communication des ressources Azure avec **Internet**
- ✓ communication entre les **ressources Azure**
- ✓ communication avec les **ressources locales**
- ✓ **filtrage** du trafic réseau
- ✓ **routage** du trafic réseau
- ✓ **intégration** aux services Azure



# Réseau Azure

## Généralités – Les multiples possibilités

### Communication avec Internet

Par défaut, toutes les ressources d'un réseau virtuel peuvent communiquer en sortie vers Internet. Effectuer des communications entrantes vers une ressource en lui assignant une adresse IP publique ou un « Load Balancer » public.

### Communication entre les ressources Azure

- ✓ Via un « VNET »
- ✓ Via un « Service Endpoint » d'un « VNET »
- ✓ Via « Azure Private Link » sur un « VNET »
- ✓ Via un « Peering » de « VNET »

### Communication avec les ressources locales

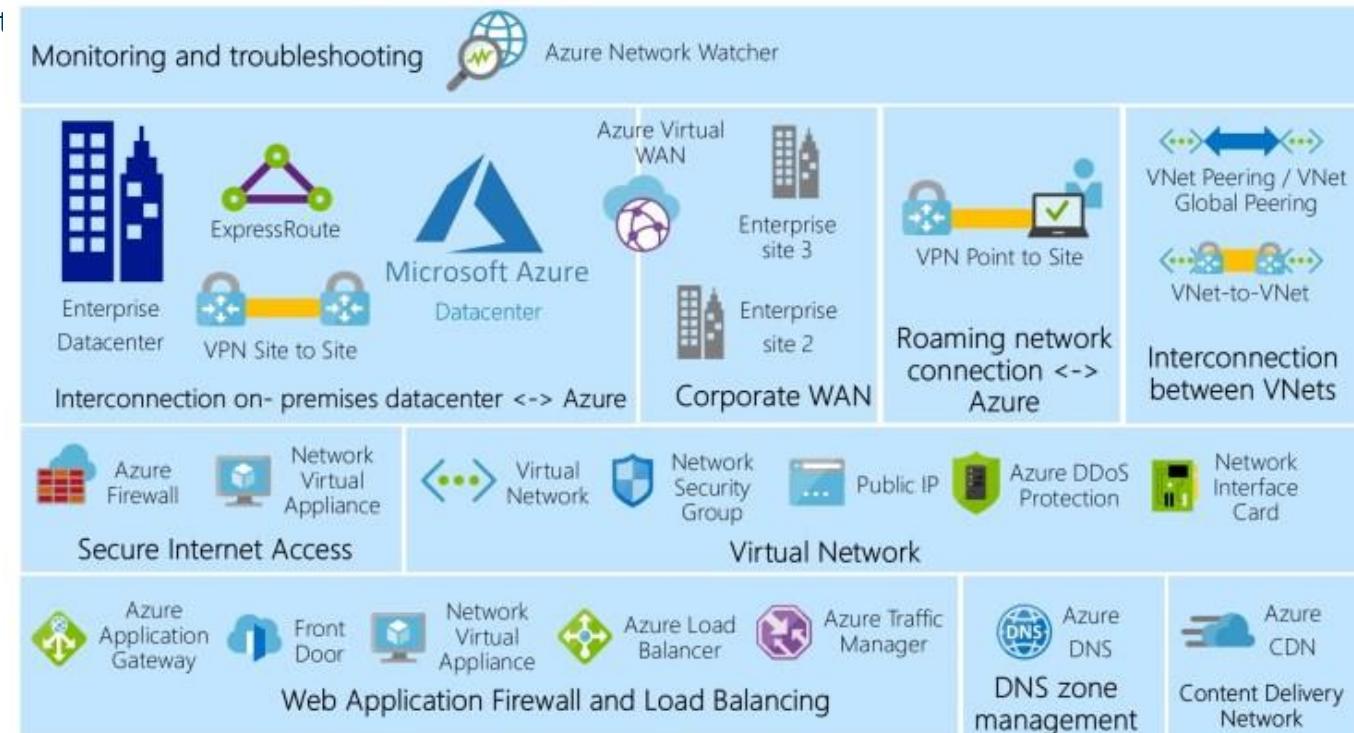
- ✓ VPN P2S
- ✓ VPN S2S
- ✓ Azure ExpressRoute

### Filtrage du trafic

- ✓ « Network Security Group »
- ✓ Azure Firewall
- ✓ « NVA » (Network Virtual Appliance)

### Routage du trafic

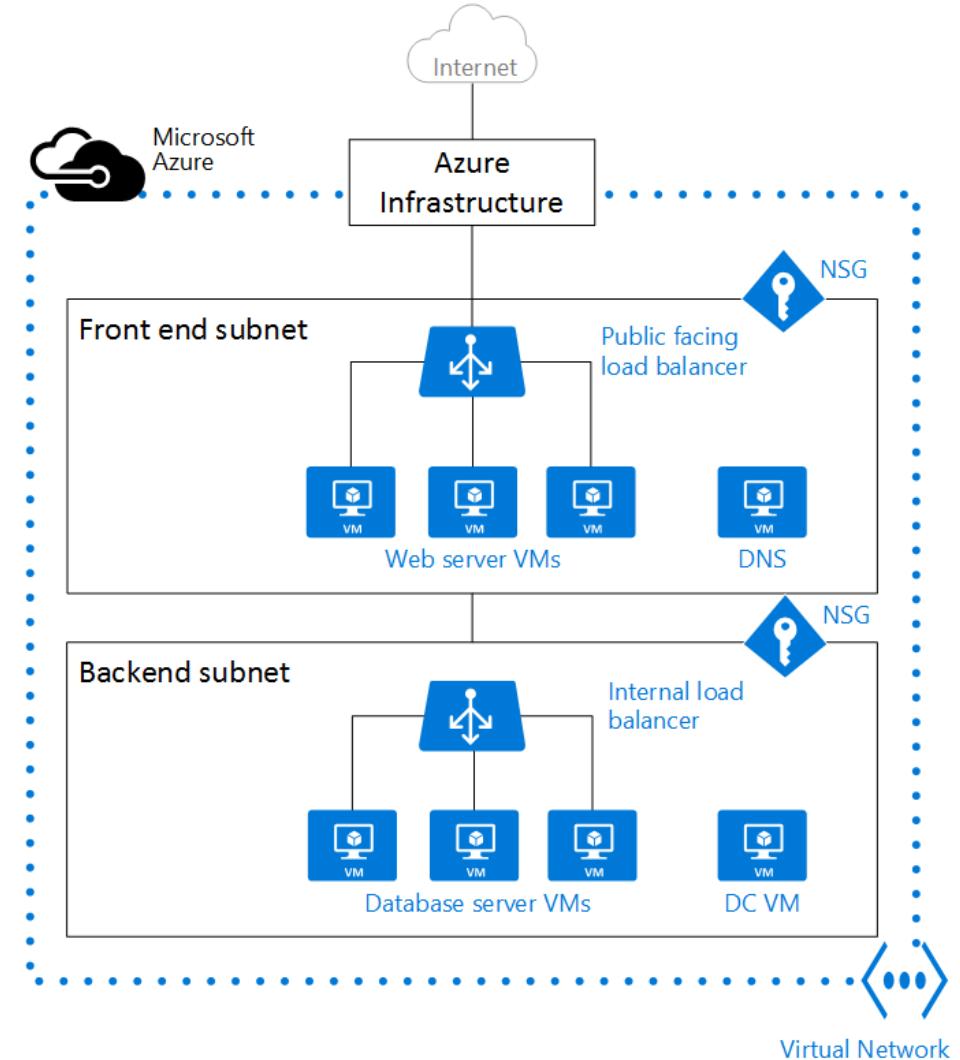
- ✓ « UDR » (User Defined Route) : créer des tables de routage personnalisées avec des itinéraires qui contrôlent où le trafic est acheminé pour chaque « Subnet »
- ✓ Itinéraires BGP : propager les itinéraires BGP locaux aux « VNET »



# Réseau Azure

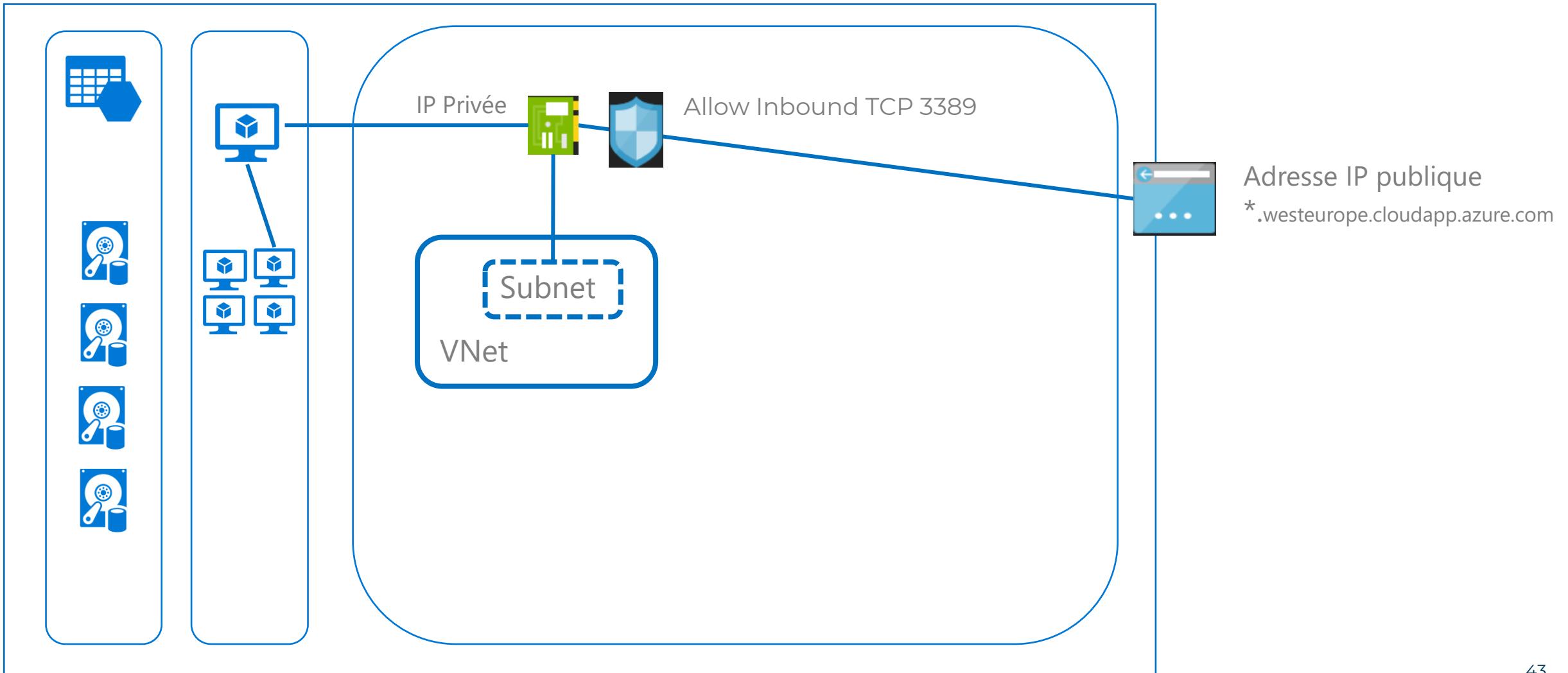
## Généralités - Virtual Network (VNET) / Subnet

- ✓ Découpé en sous-réseaux (« Subnets »)
- ✓ Routage implicite entre différents « Subnet »
- ✓ Choix du plan d'adressage (RFC1918), IPv4 ou IPv6
- ✓ Attribution dynamique des adresses IP par défaut (Réservation d'adresses IP internes statiques possible)
- ✓ 4 adresses IPv4 réservées par « Subnet » pour la « Fabric »
- ✓ Pas de support du Broadcast / Multicast
- ✓ S'étend à une seule région Azure
- ✓ Appartient à une seule « Subscription »



# Réseau Azure

Généralités – Illustration avec une machine virtuelle

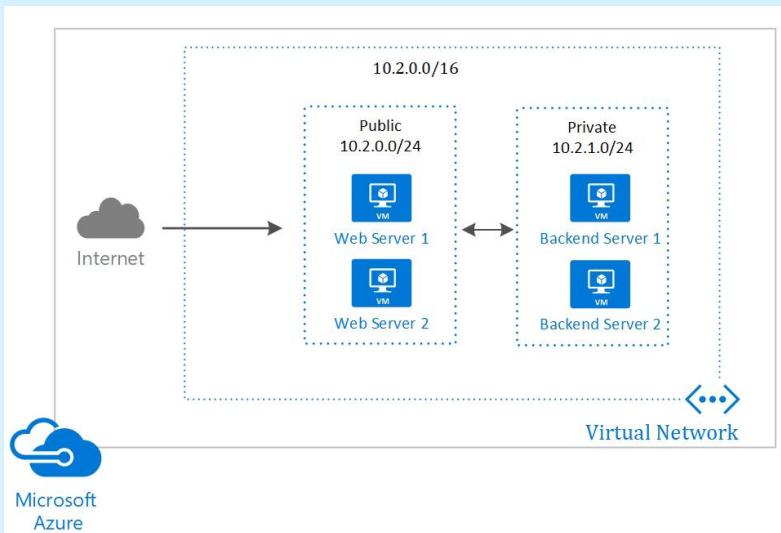


# Réseau Azure

## Focus - Communiquer entre les ressources Azure

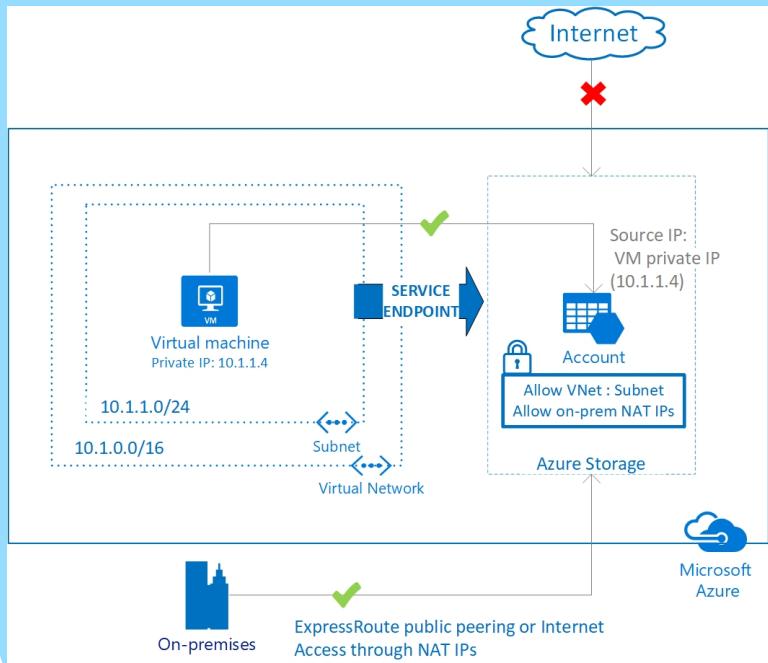
### ✓ Via un « VNET »

Faire communiquer les VMs entre elles par le biais d'adresses IP privées.



### ✓ Via un « Service Endpoint »

Les « Services Endpoint » permettent aux adresses IP privées d'un « VNET » d'atteindre le point de terminaison d'un service Azure sans « sortir » sur Internet.

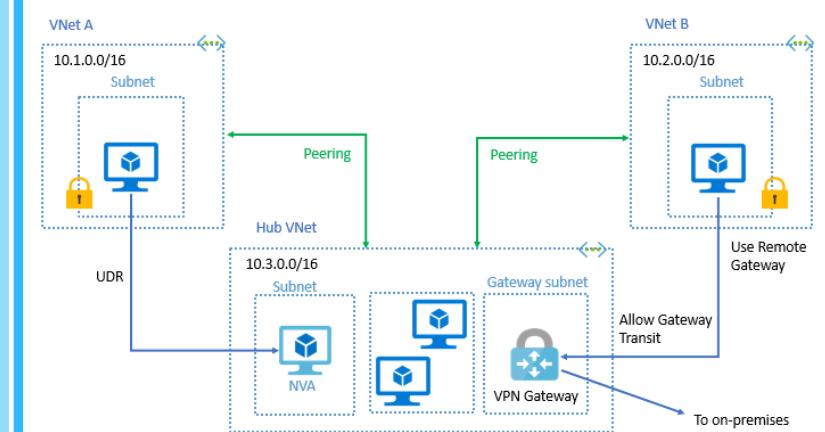


### ✓ Via un peering de réseau virtuel

Le « Peering » de « VNET » permet de connecter deux « VNET » dans Azure.

Deux types de Peering :

- « Regional Peering » : connecte des « VNET » au sein d'une même région Azure
- « Global Peering » : connecte des « VNET » entre différentes régions Azure

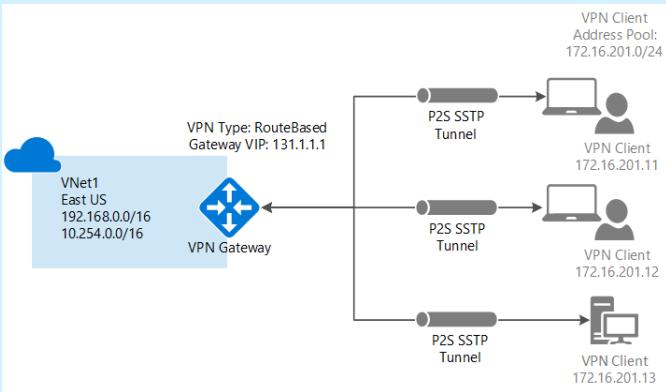


# Réseau Azure

## Focus - Communiquer avec les ressources « On-Premise »

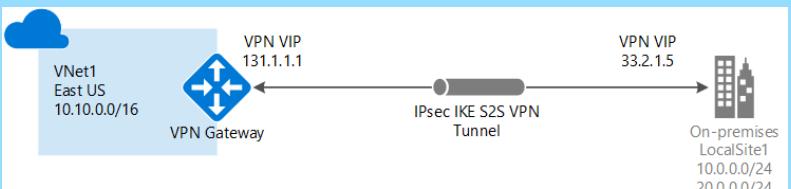
### ✓ VPN P2S

Une connexion par passerelle VPN point à site (P2S) permet de créer une connexion sécurisée à un « VNET » à partir d'un ordinateur client individuel.



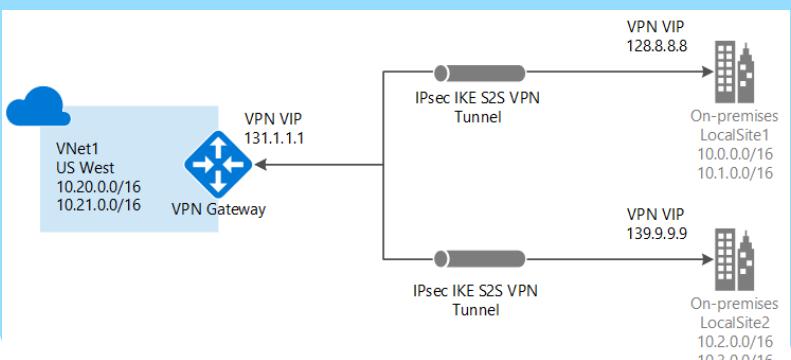
### ✓ VPN S2S

Une connexion VPN (S2S) est une connexion via un tunnel VPN IPsec/IKE. Une connexion site à site nécessite un appareil VPN local auquel est assignée une adresse IP publique.



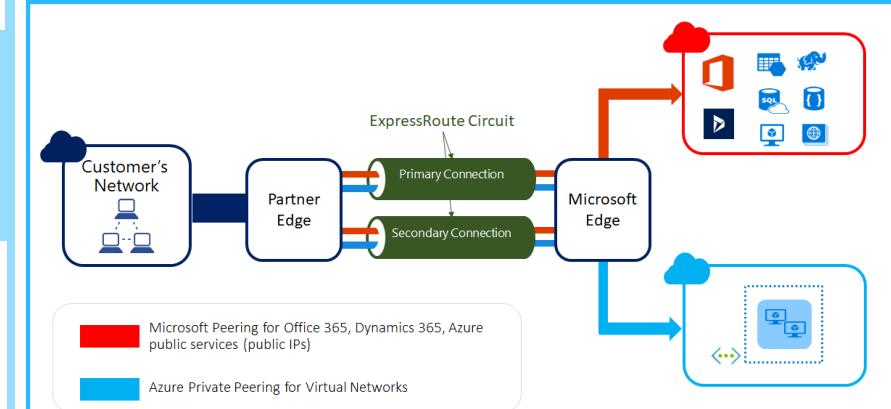
### ✓ MULTI SITE VPN S2S

Plusieurs connexions VPN à partir de votre passerelle VPN du « VNET », généralement en vous connectant à plusieurs sites locaux.



### ✓ Azure ExpressRoute

Cette connexion permet d'étendre les réseaux locaux dans le cloud Microsoft via une connexion privée avec l'aide d'un fournisseur de connectivité. Les connexions ExpressRoute ne passent pas par l'Internet public. Elles offrent ainsi une meilleure fiabilité, des vitesses supérieures, des latences cohérentes et une plus grande sécurité que les connexions classiques sur Internet.



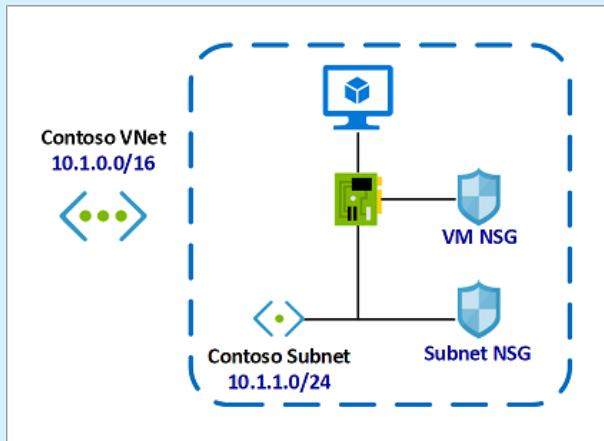
# Réseau Azure

Focus - Filtrer le trafic

## Sécurité réseau native simple

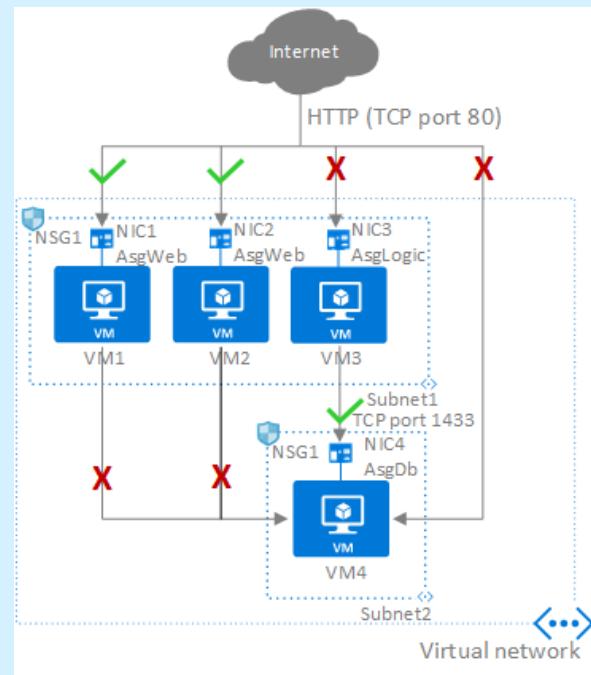
- ✓ « Network Security Group » (NSG)

Un « NSG » contient des règles de sécurité qui autorisent ou rejettent le trafic réseau entrant et sortant vers différents types de ressources Azure. Pour chaque règle, il est possible de spécifier la source et la destination, le port et le protocole.



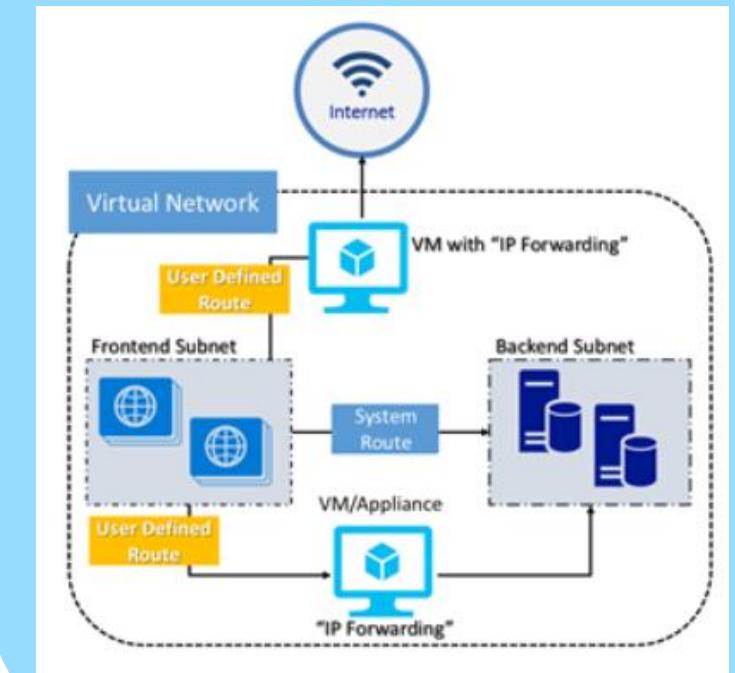
- ✓ Application Security Group (ASG)

Les « ASG » permettent de configurer la sécurité réseau comme un prolongement naturel de la structure de l'application, et donc de regrouper les machines virtuelles et définir des stratégies de sécurité réseau basés sur ces groupes.



## « Network Virtual Appliance » NVA

Une »NVA« est une machine virtuelle exécutant une fonction réseau, telle qu'un pare-feu, l'optimisation du WAN ou une autre fonction réseau.

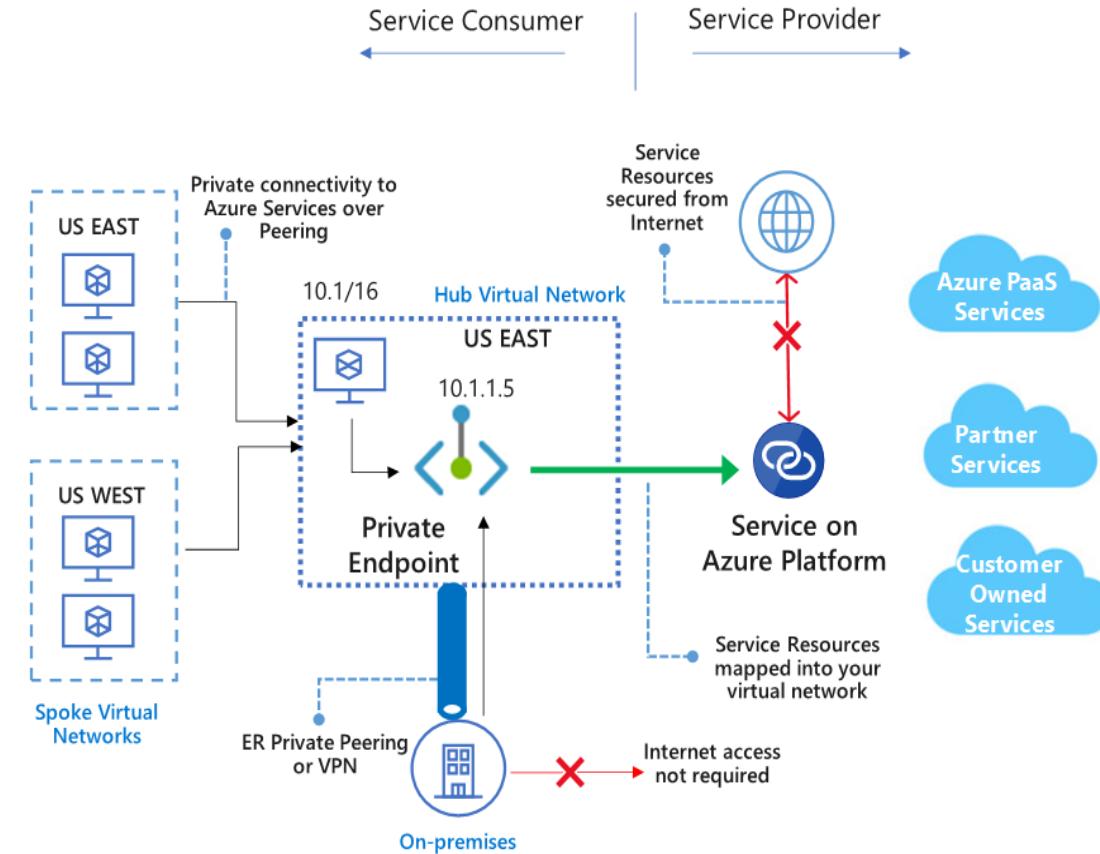




# Réseau Azure

## Focus - Azure Private Link

- ✓ Pour accéder aux services PaaS Azure et les services de partenaires/clients hébergés par Azure via un »Private Endpoint»
- ✓ Aucune passerelle Internet, périphérique NAT, adresse IP publique
- ✓ Accès privé à partir des réseaux pairés et On-premise. Utiliser le peering privé d'ER ou le VPN S2S, en supprimant le trafic via Internet
- ✓ Adresses IP prévisibles pour les ressources PaaS
- ✓ Routage sur un réseau privé.
- ✓ La configuration du NSG et du pare-feu dans l'espace d'adressage du client

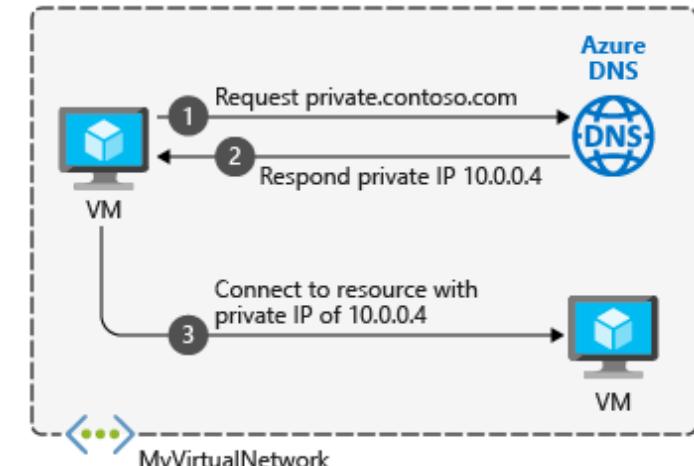




# Réseau Azure

## Présentation du composant Azure DNS

- ✓ Résolution des noms Azure :
  - Système hautement disponible
  - Adresse IP Azure DNS est **168.63.129.16**
  - Utilisé pour résoudre les « hostnames » Azure
  - Entièrement et automatiquement gérés par Azure
- ✓ Azure « DNS Private » :
  - Service DNS fiable et sécurisé pour gérer et résoudre les noms de domaine dans un Vnet
  - Pour des noms de domaine personnalisés
  - Enregistrement automatique des VMs
- ✓ Azure « DNS » (public):
  - Hautement disponible (SLA à 100%)
  - Architecture distribuée à l'échelle mondiale, résiliente aux pannes de plusieurs régions
  - Résolution rapide des noms DNS mondiaux
  - Pas de fonction de Registrar pour le moment





# Réseau Azure

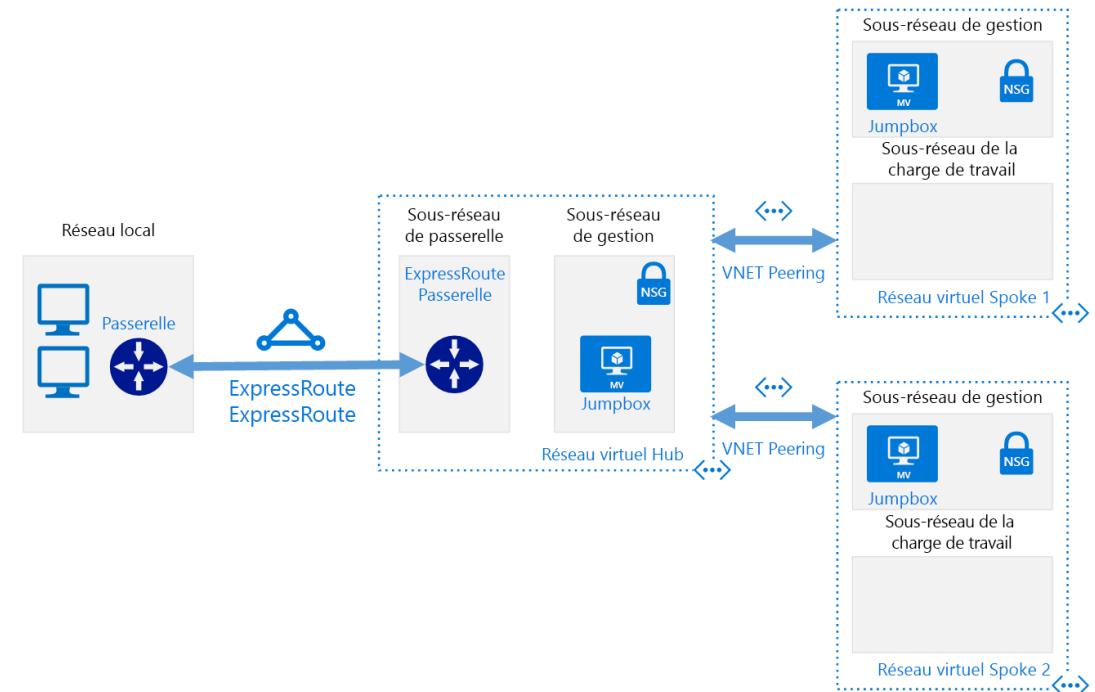
Topologie de réseau hub-and-spoke

Le hub est un « VNET » dans Azure qui centralise la connectivité au réseau local via ExpressRoute ou VPN S2S

Les membres « Spoke » sont des « VNET » homologués (« Peering ») avec le « Hub » et qui peuvent être utilisés pour isoler des environnements.

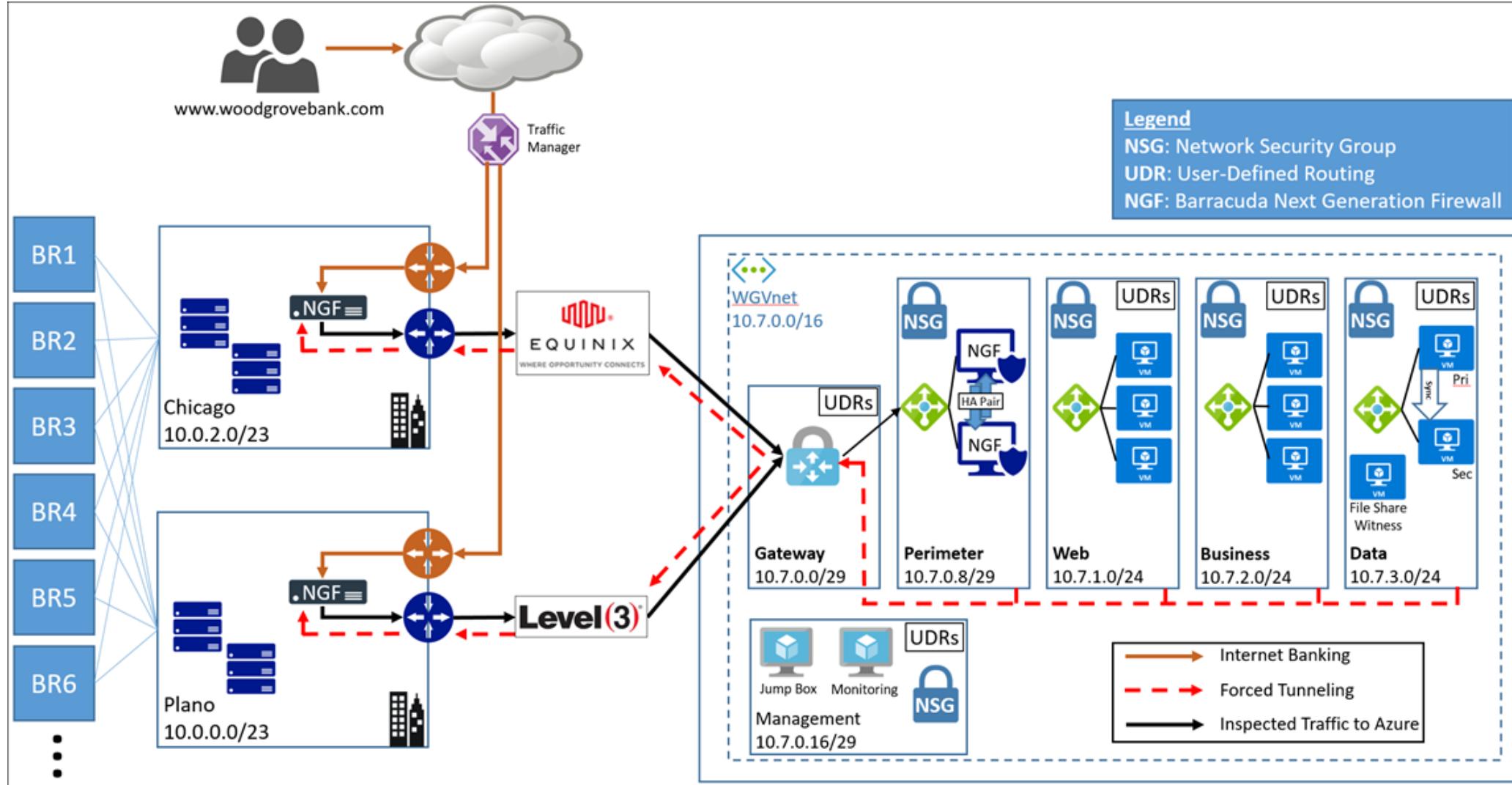
Avantages:

- **Réduction des coûts** en centralisant les services qui peuvent être partagés par plusieurs environnements (NVAs, DNS, IDS, NTP ou AD DS...)
- **Surmonter les limites des « Subscription » : Peering des VNets** de différents « Subscription » avec le « Hub » central.
- **Séparation des préoccupations** entre le service informatique central (SecOps, InfraOps) et les environnements des équipes métiers (DevOps)



# Réseau Azure

Exemple de topologie



# Discussions, questions, démonstrations



# Microsoft Learning Path



4700 XP

## Azure Fundamentals: Describe Azure architecture and services

3 hr 23 min • Learning Path • 0 of 4 modules completed

Beginner Administrator Developer DevOps Engineer Solution Architect Azure

The Microsoft Azure Fundamentals training is composed of three learning paths: Microsoft Azure Fundamentals: Describe cloud concepts, Describe Azure architecture and services, and Describe Azure management and governance. Microsoft Azure Fundamentals: Azure architecture and services is the second learning path in the Microsoft Azure Fundamentals course. This learning path explores Microsoft Azure, its architecture, and some of the most commonly used services and resources.

This learning path helps prepare you for Exam AZ-900: Microsoft Azure Fundamentals.

### Prerequisites

- Basic familiarity with IT terms and concepts

[Start >](#) [!\[\]\(d72719a91e21a20aec23a11379fae991\_img.jpg\) Save](#)



# Microsoft Learning Path



**Describe Azure compute and networking services**

58 min remaining • Module • 1 of 14 units completed

★★★★★ 4.6 (27,844)

1500 XP

This module focuses on some of the computer services and networking services available within Azure.

- Describe Azure virtual networking**  
5 min
- Describe Azure virtual private networks**  
5 min
- Describe Azure ExpressRoute**  
4 min
- Describe Azure DNS**  
3 min





# Sécurité Azure

## Introduction

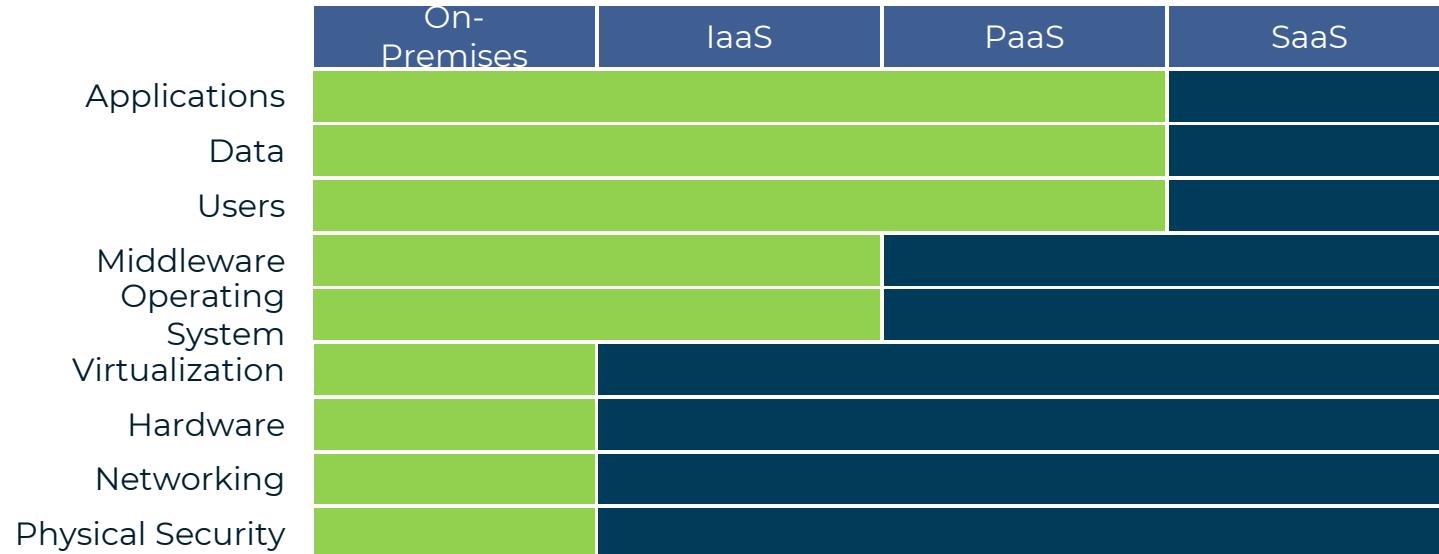
- La transformation digitale consiste à numériser les processus et les services pour que les entreprises puissent être plus agiles et fonctionner plus efficacement
- Lorsque la sécurité digitale et le cloud sont combinés, ils représentent une base solide qui prend en charge la transformation digitale. S'il en manque un, l'édifice pourrait s'effondrer
- Le cloud dans une entreprise digitale ouverte nécessite de passer d'une approche de sécurité de type « Protéger » à une approche de type « Protéger, détecter et réagir »

5 piliers pour penser efficacement la cybersécurité dans le cloud				
Leadership & Governance	Evolving Threat Environment	Cybersecurity at the speed of cloud	Cybersecurity at the new edge	People and process
<ul style="list-style-type: none"><li>• Améliorer le leadership et la gouvernance pour la prise de décision, la priorisation, l'allocation budgétaire, les rapports, la responsabilité en matière de cybersécurité</li></ul>	<ul style="list-style-type: none"><li>• En raison de la nature des menaces en constante évolution, les entreprises doivent détecter et réagir aux comportements et incidents malveillants.</li></ul>	<ul style="list-style-type: none"><li>• L'organisation doit trouver un équilibre entre la protection et la croissance de l'entreprise pour maintenir un rythme d'innovation plus rapide</li></ul>	<ul style="list-style-type: none"><li>• Les entreprises doivent faire face à la cybersécurité et aux risques liés aux technologies et aux actifs dont elles ne sont plus propriétaires ni ne sont plus contrôlées (Cloud, SaaS, mobile, etc.).</li></ul>	<ul style="list-style-type: none"><li>• L'informatique centrée sur les personnes nécessite une meilleure perception du niveau de sécurité requis et la capacité de détecter ce qui ne fonctionne pas</li></ul>



# Sécurité Azure

Modèle de responsabilité partagée en matière de sécurité



- Menaces de sécurité visant toutes les couches
- Les attaques finissent par cibler les données
- Changement de responsabilités en matière de sécurité



# Sécurité

## Généralité

Lorsque l'on parle de sécurité dans Azure, cela implique à minima de traiter les sujets suivants :

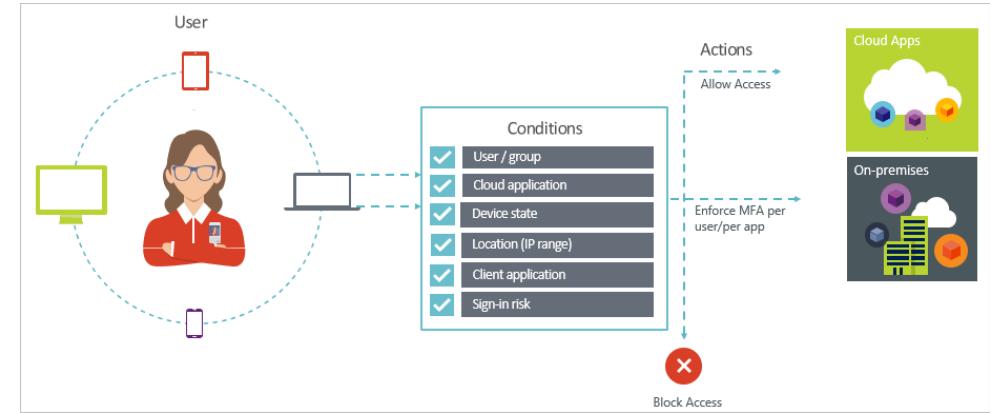
- ✓ Gestion des identités et des contrôles d'accès
- ✓ Sécurisation du réseau
- ✓ Protection des données
- ✓ Gestion des secrets (mot de passe, certificats, etc.)
- ✓ Avoir une visibilité centralisée et prévenir les attaques



# Sécurité

## Azure AD – CA / MFA

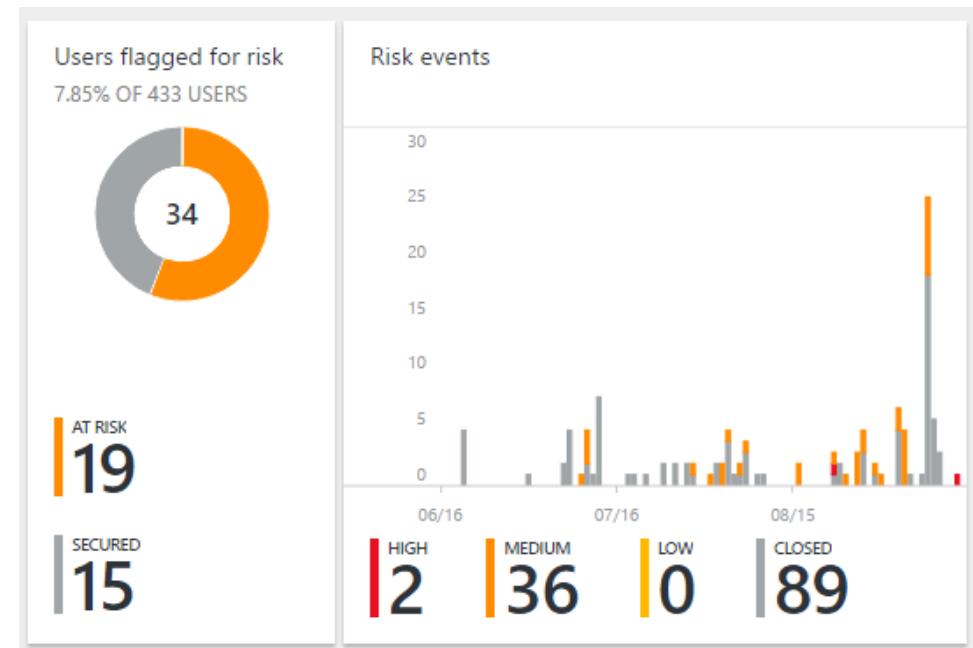
- Conditionnal Access :
  - Sign-in risk
  - Network location
  - Device management
  - Client application
- MFA
  - Utiliser plusieurs méthodes d'authentification
  - Deuxième facteur d'authentification via un téléphone mobile de confiance
  - SMS
  - Application mobile qui génère / gère des tokens logiciels (Ex: MS Authenticator)



# Sécurité

## Azure AD – Identity Protection

- Déetecter les vulnérabilités et les comptes à risque
  - Fournir des recommandations personnalisées pour améliorer la sécurité globale en mettant en évidence les vulnérabilités
  - Calcul des niveaux de risque de connexion
  - Calcul des niveaux de risque utilisateur
- Enquêter sur les événements à risque
  - Envoi de notifications d'événements de risque
  - Enquêter sur les événements à risque à l'aide d'informations pertinentes et contextuelles
  - Fournir des workflows de base pour suivre les enquêtes
  - Fournir un accès facile aux actions de correction telles que la réinitialisation du mot de passe
- Politiques d'accès conditionnel basées sur les risques
  - Politique visant à limiter les ouvertures de session risquées en les bloquant ou en exigeant des problèmes d'authentification à plusieurs facteurs
  - Politique de blocage ou de sécurisation des comptes d'utilisateurs à risque
  - Politique imposant aux utilisateurs de s'inscrire pour une authentification multifacteur





# Sécurité

## Azure AD - Privileged Identity Management

- L'objectif principal de Privileged Identity Management (PIM) est de minimiser :
  - le nombre de personnes ayant accès à des informations sécurisées
  - la durée pendant laquelle un accès privilégié est fourni à un utilisateur spécifique
- Principales fonctionnalités :
  - Fournir un accès privilégié pour une durée limitée aux ressources Azure AD et Azure
  - Exiger une approbation pour activer des rôles
  - Appliquer l'authentification multi-facteurs pour activer n'importe quel rôle
  - Utiliser la justification pour comprendre pourquoi les utilisateurs activent
  - Obtenir des notifications lorsque des rôles privilégiés sont activés
  - Effectuer des vérifications d'accès pour vous assurer que les utilisateurs ont toujours besoin de rôles
  - Télécharger l'historique d'audit pour de l'audit interne ou externe



# Sécurité

## Focus - Réseau

Voici un aperçu de quelques bonnes pratiques pour améliorer votre sécurité réseau :

- ✓ **NSG et ASG** : pour vous protéger contre le trafic non sollicité dans les sous-réseaux Azure
- ✓ **Azure Security Center**, accès JIT (just in time) : Activez l'accès au port uniquement après l'approbation du flux de travail
- ✓ **UDR** : pour pouvoir utiliser Azure Firewall ou une NVA (« Network Virtual Appliance »)
- ✓ **VPN / ExpressRoute** : Évitez toute exposition à Internet grâce à des liaisons réseau étendu dédiées
- ✓ **Désactivation** de l'accès RDP/SSH aux machines virtuelles Azure exposés sur Internet.



# Sécurité

Focus - « Encryption at rest »



- Machines virtuelles :
  - Chiffrement des disques (Windows = bitlocker, Linux = dm-crypt)
  - Fichiers & dossier - EFS dans Windows Server
- SQL Server:
  - Transparent Data and Column Level Encryption
- Storage:
  - Chiffrement des comptes de stockage
  - StorSimple avec le chiffrement AES-256
- Applications:
  - Client-Side encryption avec .NET Crypto API
  - RMS Service SDK pour le chiffrement des fichiers dans les applications

# Sécurité

## Focus - Azure Key Vault

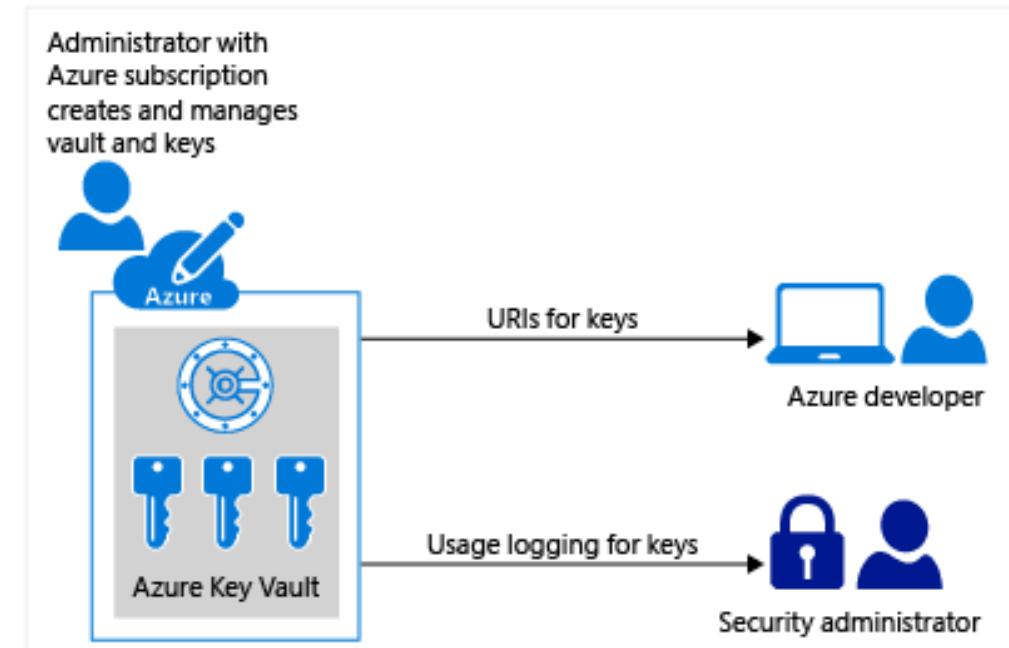
Azure Key Vault est un service cloud permettant de stocker les secrets et d'y accéder en toute sécurité. Un secret est un élément pour lequel on souhaite contrôler étroitement l'accès. Il peut s'agir de clés d'API, de mots de passe, de certificats ou de clés de chiffrement.

Il existe trois façons de s'authentifier auprès de Key Vault :

- ✓ « **Managed Identity** » pour les ressources Azure : vous pouvez attribuer une identité à votre ressource Azure qui a accès à Key Vault.
- ✓ « **Service Principal** » et **certificat** : vous pouvez utiliser un principal de service et un certificat associé qui a accès à Key Vault.
- ✓ « **Service Principal** » et **secret** : cette option n'est pas recommandée

**Exemples** de scénarios d'utilisation :

- ✓ Développeur d'une application Azure utilisant des clés pour la signature et le chiffrement, devant être externes à l'application.
- ✓ Responsable de la sécurité souhaitant que les applications soient conformes aux normes en vigueur et contrôler le cycle de vie d'une clé et la surveiller.





# Sécurité

## Azure Security Center

Azure Security center vous aide à :

- ✓ Renforcer la sécurité
- ✓ Protéger contre les menaces

Les fonctionnalités :

- ✓ **Secure Score** : évalue continuellement vos ressources, vos abonnements et votre organisation en recherchant d'éventuels problèmes de sécurité. Plus le score est élevé, plus le niveau de risque identifié est faible.
- ✓ **Compliance** : analyse les facteurs de risque dans votre environnement de cloud hybride conformément aux bonnes pratiques en matière de sécurité.
- ✓ **Azure defender** : fournit des alertes de sécurité ainsi qu'une protection avancée contre les menaces pour les ressources Azure.
- ✓ **Inventory** : affiche le nombre de machines virtuelles non analysées et un simple baromètre de vos ressources surveillées par le Centre de sécurité.
- ✓ **Insights** : offre des statistiques pour votre environnement.
- ✓ **Just-in-time VM Access**

The screenshot shows the Azure Security Center Overview page with the following data:

- Secure score:** Current score is 56.56% (33.94 points). Completed controls: 1/16. Completed recommendations: 52/287.
- Compliance:** Current compliance by passed controls:
  - HIPAA HITRUST: 0/22
  - SOC TSP: 1/13
  - ISO 27001: 2/20
  - NIST SP 800 5...: 3/29
  - PCI DSS 3.2.1: 5/45
- Azure Defender:** Resource Coverage: 93%. Alerts by severity: High (30), Medium (51), Low (31). Last update: 23 Sun.
- Inventory:** Total Resources: 2921. Unmonitored vms: 43. Status distribution: Unhealthy (1477), Healthy (1167), Not applicable (277).
- Insights:** Most prevalent recommendations (by resources):
  - Audit diagnostic setting: 686
  - Disk encryption should be applied on virt...: 118
  - A vulnerability assessment solution shou...: 117
  - Secure transfer to storage accounts shou...: 102Controls with the highest potential increase:
  - Remediate vulnerabilities: +11% (6pt)
  - Remediate security configurations: +6% (4pt)
  - Enable encryption at rest: +6% (4pt)

# Discussions, questions, démonstrations



A circular icon with a blue background, featuring a white shield with a person icon and a gear icon inside it.

**Describe Azure identity, access, and security**

43 min remaining • Module • 0 of 11 units completed

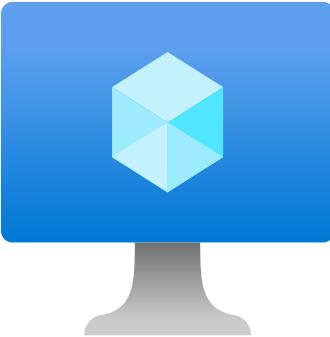
★★★★★ 4.8 (24,199)

1200 XP

This module covers some of the authorization and authentication methods available with Azure.

Overview ▾

# Exploitation





# Exploitation

## Introduction

- ✓ L'exploitation des ressources dans Azure commence tout d'abord par le type de besoin que vous recherchez au sein de votre environnement Azure et les services qui vont remplir ses attentes.
- ✓ Dans ses services d'exploitation vous retrouverez des services de type :
  - ✓ Charge de travail
  - ✓ Stockage
  - ✓ Sauvegarde et PRA
  - ✓ Supervision

# Exploitation

## Charge de calcul - Généralités

### Machine Virtuelle

- ✓ Windows Server
- ✓ Windows 10/11 (Preview)
- ✓ Linux (Ubuntu, Red Hat, CentOS, Debian)



### Containeur

- ✓ Azure Container Service
- ✓ Azure Kubernetes Service



### Serverless

- ✓ Azure function



### Application Web

- ✓ Azure Web Apps



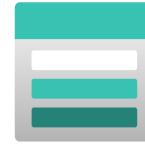


# Exploitation

## Stockage - Généralités

### Compte de Stockage

- ✓ Service de stockage PaaS standard dans Azure
- ✓ Stockage de données : relationnelles ; non-relationnelles
- ✓ Service de Queuing
- ✓ Fonctionnalité de redondance de la données
- ✓ Suppression réversible



### Service Azure SQL Managed Instance

- ✓ Service PaaS SQL
- ✓ Fonctionnalité de clustering
- ✓ Service de sauvegarde de base de données intégré
- ✓ Fonctionnalité de chiffrement avancée



# Exploitation

## Azure Backup

### Locale

- ✓ Sauvegarde planifiée
- ✓ Sauvegarde manuelle
- ✓ Rétention paramétrable jour, semaine, mois, année : coffre recovery service

### Machines virtuelles Azure

- ✓ Sauvegarde planifiée
- ✓ Sauvegarde manuelle
- ✓ Rétention paramétrable jour, semaine, mois, année : coffre recovery service
- ✓ Exclusion de disques pour limiter les coûts de stockage

### SQL Server dans une machine virtuelle Azure

- ✓ Backup full 1 par jour ou 1 par semaine
- ✓ Rétention paramétrable jour, semaine, mois, année
- ✓ Sauvegarde des logs de transaction (fréquence de 15 mn à 24 heures)

### Azure File Share

- ✓ 1 sauvegarde automatique par jour
- ✓ Rétention paramétrable en nombre jour



Azure Backup

# Exploitation

## Azure Site Recovery - Généralités

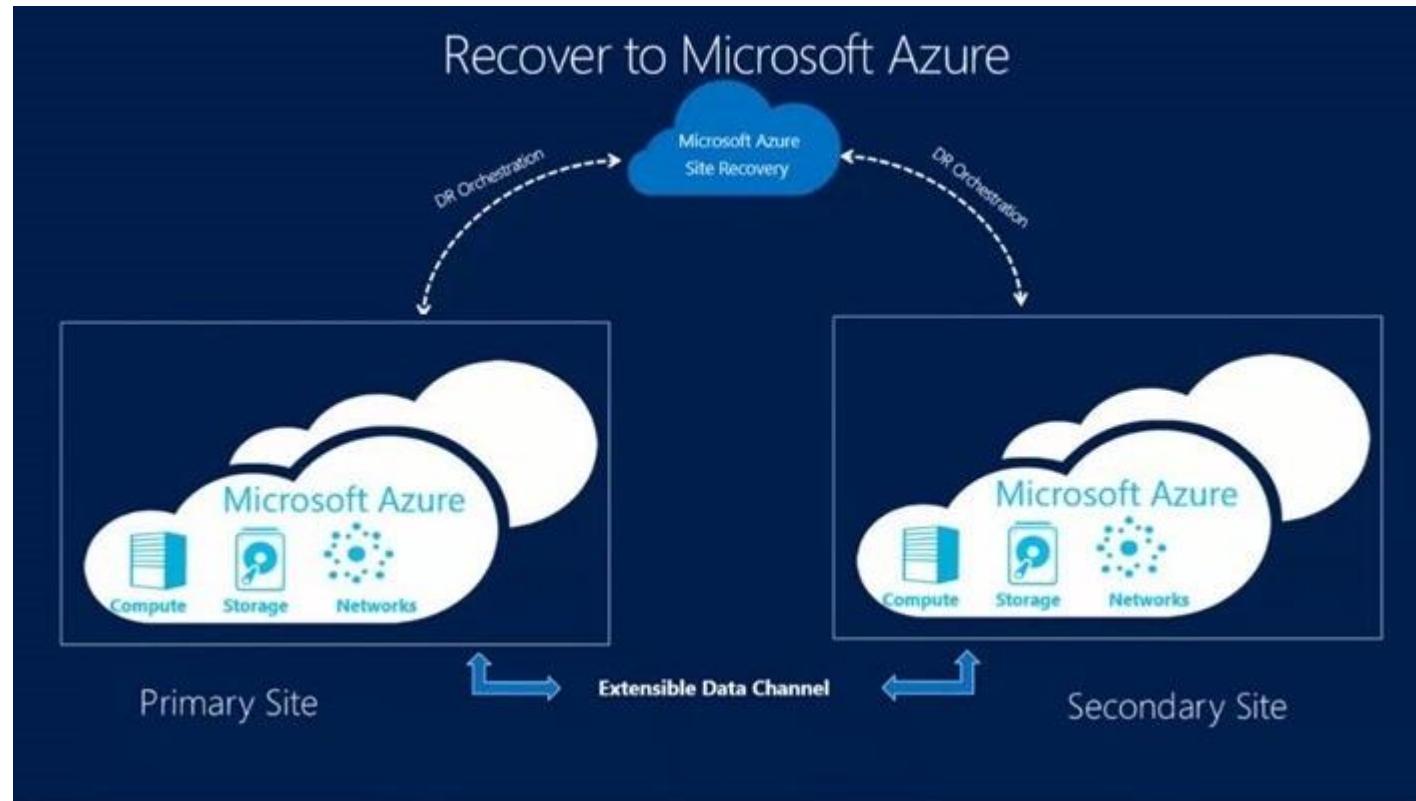
ASR contribue à mettre en œuvre une stratégie de continuité d'activité et de récupération d'urgence.

Le principe de base est de **répliquer** les charges de travail des machines virtuelles et/ou physique d'un site principal vers un **emplacement secondaire**.

En cas d'interruption de votre site principal, vous **basculez** vers l'emplacement secondaire. Lorsque le site principal est de nouveau opérationnel, vous pouvez effectuer une **restauration** automatique vers celui-ci.

La réplication peut être gérée pour :

- ✓ Les machines **virtuelles** Azure (réplication entre région)
- ✓ Machines virtuelles **locales**, Azure Stack ou serveurs physiques.

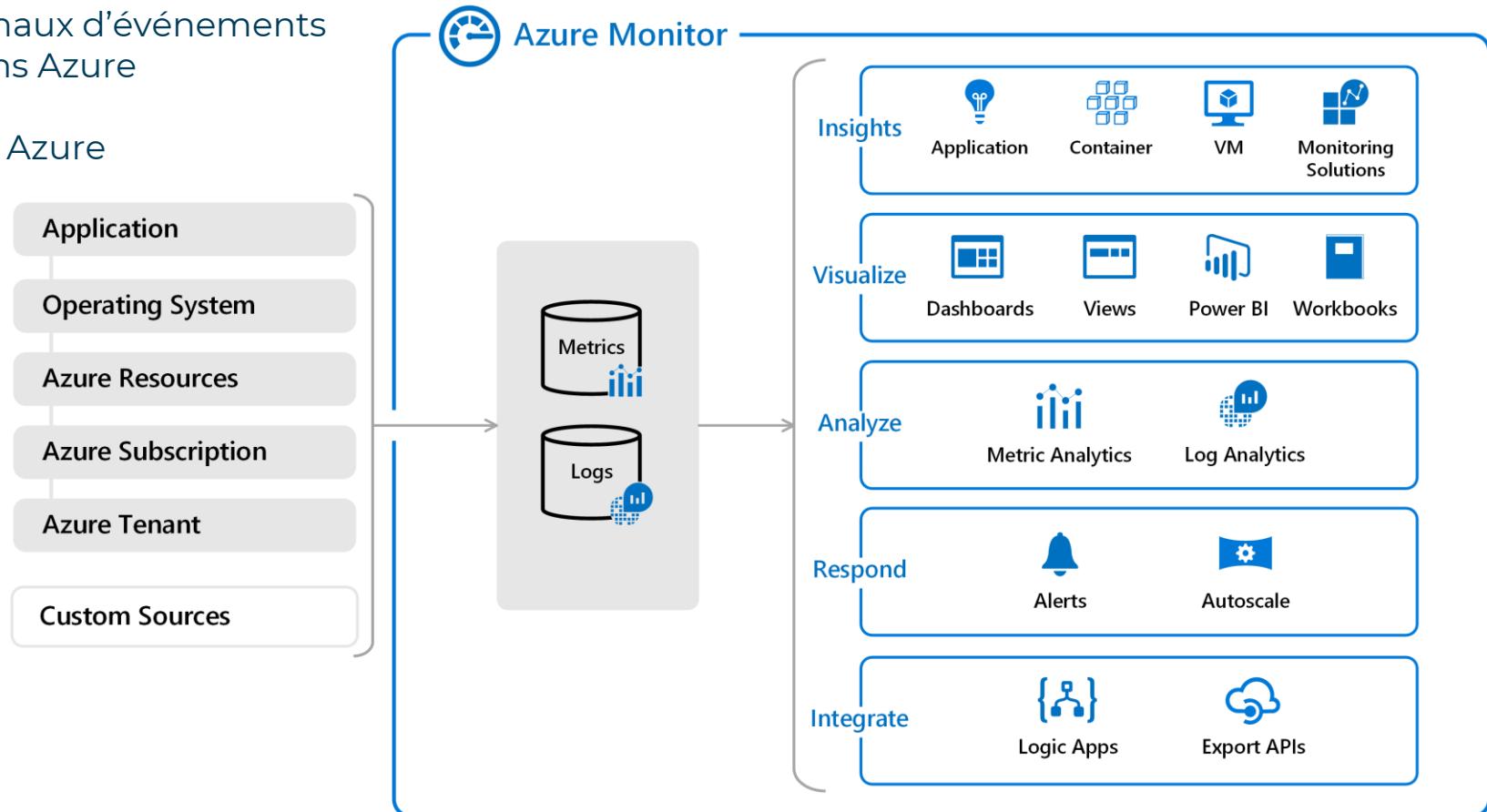




# Exploitation

## Outils de monitoring - Azure Monitor

- ✓ Outil natif de supervision dans Azure
- ✓ Utilise les métriques et les journaux d'événements issus des différents services dans Azure
- ✓ Visualisation directement dans Azure
- ✓ Alerte



# Exploitation

## Outils de monitoring - Azure Network Watcher

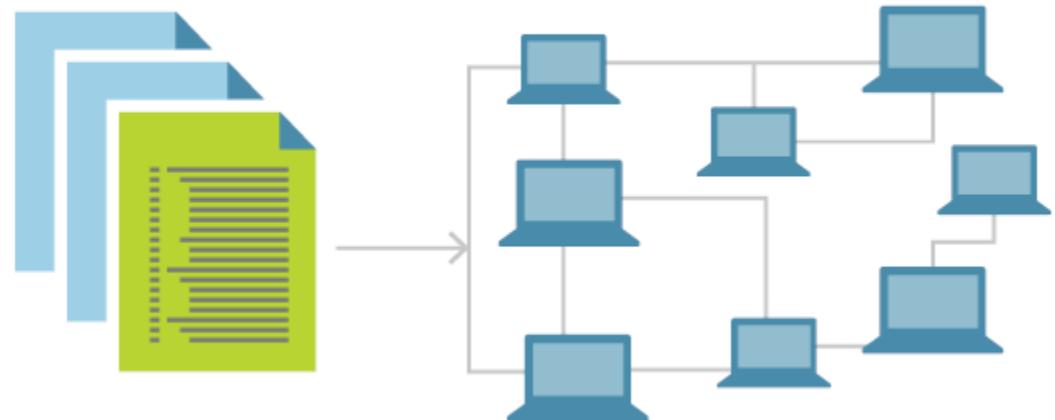
- ✓ Surveiller la communication
  - ✓ Capture de paquets
  - ✓ Définition d'alertes
- ✓ Diagnostiquer
  - ✓ Identifier les problèmes de filtrage du trafic, de routage réseau, de connexion sortantes d'une machine virtuelle
  - ✓ Identifier les problèmes de connexion sur VPN Gateway
- ✓ Afficher les ressources et les relations dans un VNET
- ✓ Afficher les métriques : synthèse du nombre de ressources réseau déployées dans un abonnement et une région, et indique la limite associée à chaque ressource
- ✓ Activer ou désactiver les journaux pour les ressources dans un VNET
- ✓ Exploiter les données de journaux
  - ✓ Avec Traffic Analytics
  - ✓ Ou autres outils :
    - ✓ Graylog
    - ✓ Grafana
    - ✓ etc



# Exploitation

## Automatisation

- ✓ Pourquoi ?
  - Pour déployer plus rapidement
  - Pour standardiser les déploiements
  - Pour limiter le risque d'erreur
  - Car IaaC (Infrastructure as a Code) est techniquement viable dans Azure
- ✓ Les outils / services
  - Azure Automation
  - Powershell et modèles ARM au format JSON
  - Terraform
  - GIT (Azure DevOps ?)



# Discussions, questions, démonstrations





**Describe Azure storage services**

36 min remaining • Module • 1 of 9 units completed

★★★★★ 4.8 (20,347)

1000 XP

This module introduces you to storage in Azure, including things such as different types of storage and how a distributed infrastructure can make your data more resilient.

[Overview](#) ▾



# Merci !