SOMMAIRE

RAPPEL : REGIONS UTILISABLES POUR LES LABS AU VUE DES PASS AZURE (EAST US + WEST EUROPE)

AZ-100.1 (Day 1) – Managing Azure Subscriptions

Overview of azure Subcriscription

Notion de délégation

Management group

Access control

RBAC -> Des rôles prédéfinis

Exemple :

- Owner (Habiliter à tout faire)
- Contributeur (Habiliter à tout faire sauf définir des autorisations)
- Reader (Droit de lecture)

La définition des autorisations peut se faire à 4 niveaux :

Management groups

Subscriptions

Resource groups

Object

RG (objet organisationnel) sert à :

- Faciliter la délégation
- Connaître les couts
- Mettre en place des stratégies

Advisor

Aide dans les recommandations de coût de sécurité d'implémentation

Log Analytics

Log Analytics vous aide à collecter, corréler, rechercher et agir sur les données de journalisation et de performance générées par les systèmes d'exploitation et les applications. Il vous donne des informations opérationnelles en temps réel à l'aide de tableaux de bord de recherche et de tableaux de bord personnalisés pour analyser facilement des millions d'enregistrements sur l'ensemble de vos charges de travail et de vos serveurs, quel que soit leur emplacement physique. Log Analytics vous offre une interface unique pour la consommation et la corrélation des données, couvrant à la fois Linux et Windows Server.

AZ-100.2 (Day 2) – Implementing and Managing Storage

Les comptes de stockage

Le compte de stockage est un conteneur hébergeur de disques gérés et/ou non gérés

Il est limité par défaut à 200 comptes de stockage par abonnement. Puis possibilité d'en avoir 50 en plus via Microsoft.

Il existe deux types de Storage Account :

- Standard (Usage général – Hébergé sur du disque mécanique))
- Premium (Pour les VHD – Hébergé sur SSD). En preview,*Ultra SSD* -> 64 To et 160000 IOPS

STANDARD	PREMIUM
HDD	**SSD**
Entre 20000 et 40000 IOPS	**80000 IOPS**
5 Po	**Entre 32 To et 60 To**

Au sein d'un Storage Account, création au minimum d'un container (sorte de dossier) qui peut contenir

A quoi sert un storage account :

- A usage général (500 To max et 20000 IOPS) -> écrire tout type de données possibles (V1 ou V2)
- V2 -> Blob Block
    - Méthode d'accès de type
        - **Hot** « 1 centime/go/mois »
        - **Cool** « 0,5 centimes/Go/mois »
        - **Archive** « 0.25 centimes /Go/mois »
- A usage de type blob (5 Po et 50000 IOPS)

Les 4 types de stockage de données :

- **BLOB STORAGE**
- **TABLE STORAGE**
- **QUEUE STORAGE**
- **FILE STORAGE**

1. Le BLOB (Binary Large Object) STORAGE

Le voir comme un fichier (Accessible via les ports 80 et 443)

Nous avons 3 méthodes d'écriture :

Page : Ecriture du fichier par page (512 octets). Taille Max -> 4095 Go depuis Juillet 2017. A terme 32 voire 64 To

Optimisé pour la lecture et l'écriture aléatoire.

Exemple : VHD

Block : Ecriture du fichier par block (100 Mo). Taille Max -> 50000 blocks (Max 4 To)

Non supporté pour de la VM

Optimisé pour de la lecture séquentielle

Exemple : Données Utilisateurs sauvegardées, Films.

Append :Ecriture (Ajout) du fichier par block (4 Mo)

Optimisé pour l'ajout de données..

Exemple : Logs

2. Le TABLE STORAGE (No SQL)

Similaire à une feuille de calcul excel. Possibilité de poser un index.

Avantages : rapidité de lecture et écriture des données

Inconvénients : le traitement des données.

Création d'un système de table et de magasins de données semi-structurées avec maximum 256 colonnes avec des lignes /enregistrements (nommées entity sous Azure)

1 entity -> Taille max = 1 Mo

3. Le QUEUE STORAGE

Magasin temporaire pour les échanges asynchrones des messages applicatives.

4. Le FILE STORAGE

Ecriture de fichier SMB 2.1 et SMB 3.X par block (4 Mo).

Maximum 5 To et 1 fichier maximum 1 To.

Partage SMB dans Azure. Accessible de partout via le port 445.

5. Web static (En preview)

6. HDFS « Big data » (En preview) Actuellement nommé DATA LAKE STORAGE

Les Disques

BASIC TIER	STANDARD TIER
300 IOPS	500 IOPS
5 Tailles **-> A0 à A4**	Plus de **80** Tailles
	A -> D : HDD
	DS, GS, etc… SSD (appelés aussi **Disk Premium**)

Possibilité de passer du Basic au Standard.

Scale up -> Augmentation ou diminution de la taille, avec un redémarrage automatique.

Avec 2012R2, Tiering SSD (data chaudes) et HDD (data froides)

Choix entre :

Disques gérés (Depuis Février 2017)	Disques non gérés
Prise en charge par Microsoft **Payant et par mois**	**A moi de gérer toute la chaîne de disque**

Les 4 méthodes de redondances des comptes de stockage

- LOCALLY REDUNDANT STORAGE (LRS)

  Le plus bas niveau et le moins cher (1centime du Go)

  Réplication **synchrone** des données du Storage Account sur **3** baies physiques dans le même batiment (Facility)

  4 URL (car 4 types de données)

  Idéal pour les VM

  En Storage Account Premium, que du LRS

- GEO REDUNDANT STORAGE (GRS)

  Réplication **asynchrone** du Storage Account vers la deuxieme région pairée de la même zone géographique

  Les data secondaires ne sont accessibles que lorsque le primary est HS.

  Dorénavant la distance max entre les deux régions = 300 km (exemple : la Suisse)

  2 centimes du go

  Données copies x **SIX**

  4 URL (car 4 types de données)

  Pas de latence garantie

  Les VM ne sont pas adaptées pour le GRS

  Les données secondaires sont inaccessibles (tant que les principales sont IN)

- RA-GEO REDUNDANT STORAGE (RA-GRS)

  Identique au GRS avec un accès en lecture aux données secondaires

  Réplication asynchrone

  Données copies x **SIX**

  7 URL (car la partie **"FILE" est indisponible**)

- ZONE REDUNDANT STORAGE (ZRS)

    Ne se choisit qu'à la création du compte de stockage

    Réplication asynchrone de manière générale et synchrone dans les régions dotées de **3** Datacenters

    Données copies x **TROIS**

    6 URL

    Réplication des données sur **3** baies physiques mais dans des bâtiments (facility) differents

    Soit au sein de la même région (France Central : Auber + Montlery + les Ulis)

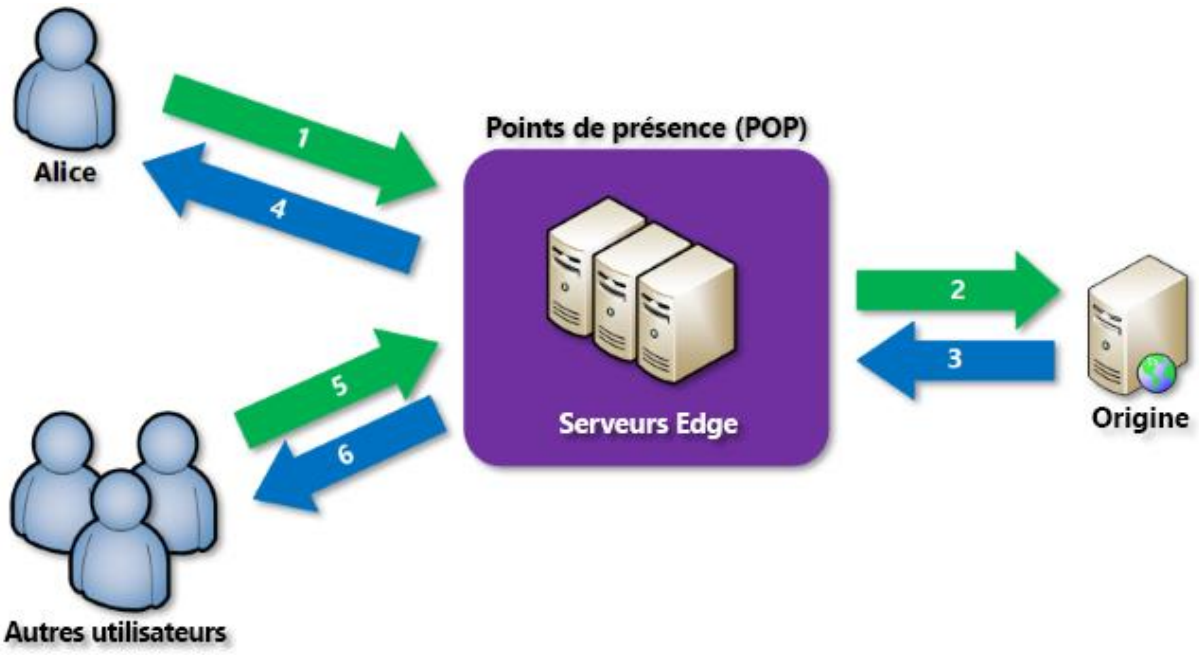
    Soit dans des régions pairées (France Central et France Sud) → **Avaibility Zone**

GRS n'est pas une solution de Disaster Recovery pour les VM

Solution de Disaster Recovery :

- Recovery Services (OMS ou Recovery Services Vault)
- Azure Backup (VM)
- Azure Site Recovery (PRA)

Les CDN (Content Delivery Network)



Un réseau de diffusion de contenu (CDN) est un réseau distribué de serveurs capables de fournir efficacement du contenu web aux utilisateurs. Il stocke le contenu en cache sur des serveurs Edge dans un point de présence (POP) proches des utilisateurs finaux afin de réduire la latence.

Les fournisseurs de la solution CDN

- MICROSOFT
- AKAMAI
- VERIZON

Exemple : Netflix , Streaming jeux olympiques

AZ-100.3 (Day 3) – Deploying and Managing Azure Virutal Machines

Introduction

Nous sommes en mode **IaaS**

DHCP ne fonctionne pas en mode **IaaS** (Hyper-V DHCP Guard) au premier niveau.

Idem pour le WDS et PXE

Par contre au second niveau avec la **Nested Virtualisation** -> Oui

Les Sizes de VM pour la Nested Virtulisation : **Dv3 ou Ev3**

NB : Nombre de VCPU limité par le quota en fonction de la région

Les caractéristiques du disque dur de la VM

- Type FIXE uniquement
- Génération 1 uniquement
- Taille max 4 To (depuis 15 Janvier 2017
- Extension VHD uniquement

Pour Uploader des VHD locaux dans Azure

Add-AzureVHD

Add-AzureRMVHD

Prix Compute VM

- Réseau sortant
- Stockage (SSD plus cher que le HDD)
- Processeur
- RAM

AZURE AVABILITY - Garanties SLA sur les VMs auprès de Microsoft (garantie de disponibilité et non de performance)

- 1er Niveau -> 0% (Tout dépend de votre configuration)
- 2ème niveau -> 99,9% (1 VM dans un storage premium)
- 3 ème niveau -> 99,95 % (au moins 2 VMs dans AVSet)

AVSet (Solution gratuite) , des vm hébergeant le même service.

Attention cela se fait à la creation de la VM. Prévoyez la création du AVSet au préalable.

- 4 ème niveau -> 99,99 % (dispo que dans certaines regions = Il s'agit du AZone). Il faut au moins 2 VM

App Service – Web App

Pour assurer 99,95% de disponibilité, recommander de prendre au minimum 1 Plan Basic

L'appli Web App sera hébergée dans DEUX régions et avec le TRAFFIC MANAGER (DNS) faire du Load Balancer.

Storage

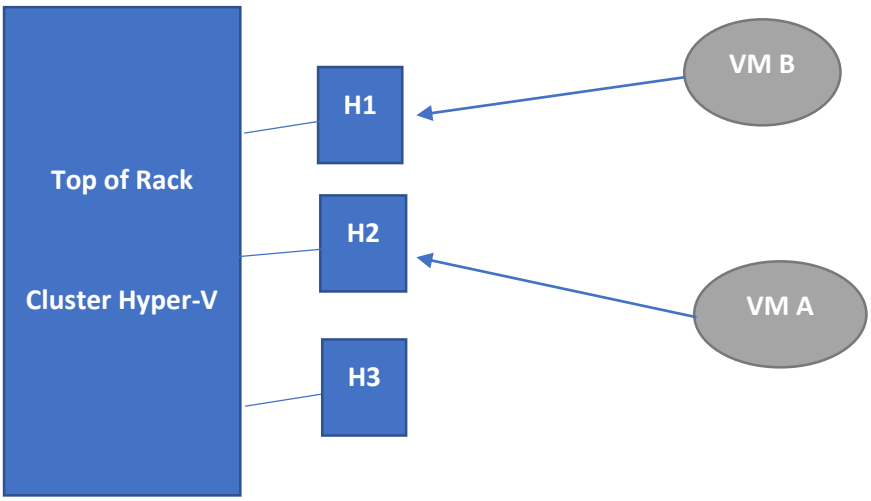
STANDARD (redondance DATA)		PREMIUM
V1	**V2**	
LRS	**LRS**	**LRS**
GRS	**GRS**	
RA-GRS	**RA-GRS**	
ZRS		

VM

AVAIBILITY SET – 99,95% HA	STORAGE ACCOUNT	AVAIBILITY ZONE – 99,99% HA
Au minimum 2 VMs	**Standard ou Premium**	**Réplication synchrone**

Avaibility Set (Organisation intelligente)

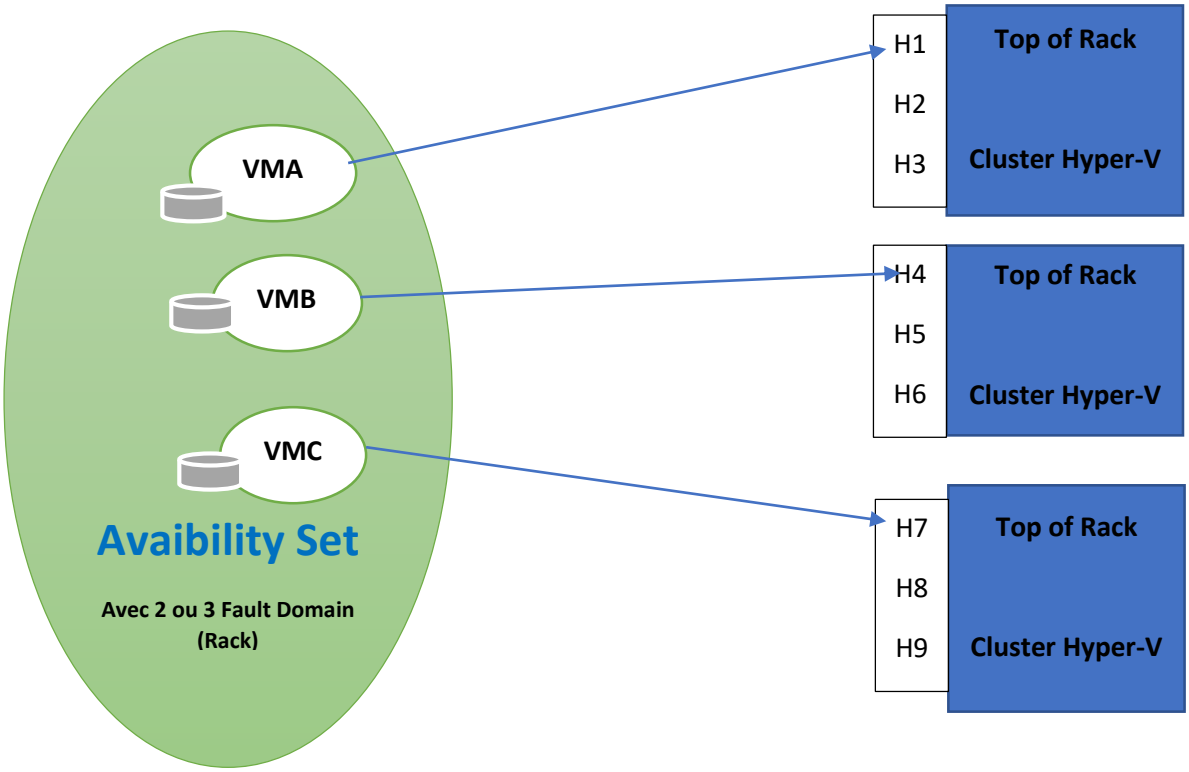
- Aucune mise en place de l'Avaibility Set



En cas de crash d'un nœud (Hx) -> Failover de ma VMx vers un autre nœud.

En cas de crash de mon Top of rack (Cluster Hyper-V) -> Perte de mes VMs

- Mise en place de l'Avaibility Set



Si les VHDs sont dans le même Storage Account Non géré -> SPOF

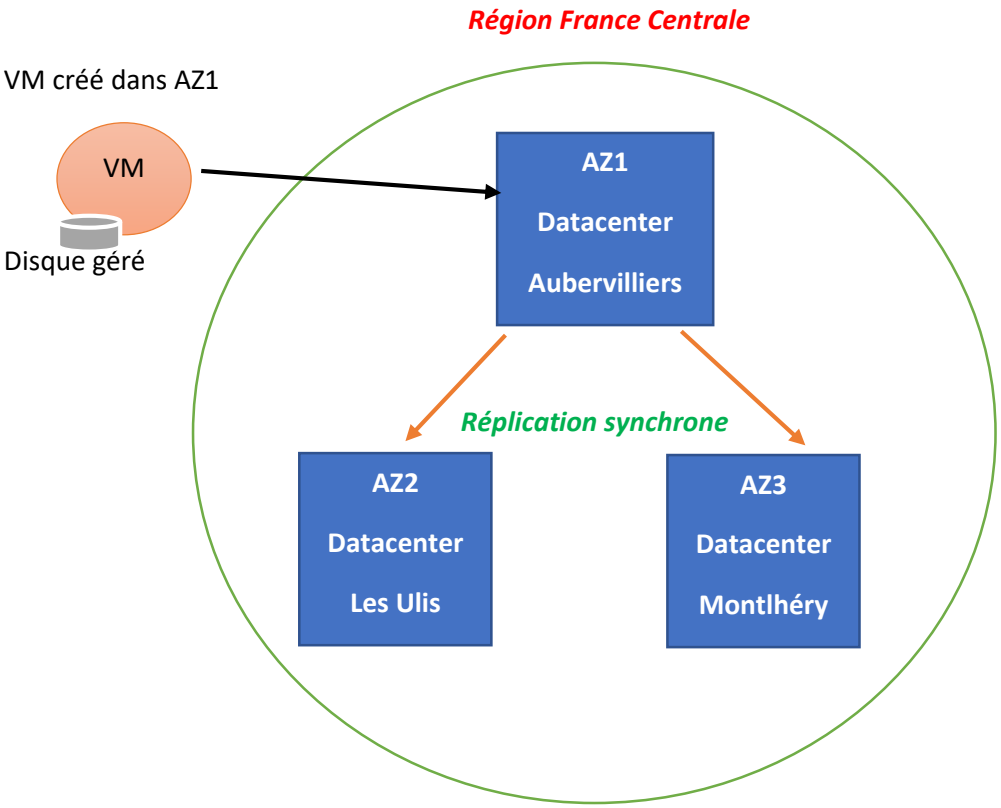
Si les VHD sont dans un Storage Account géré -> Pas de SPOF

Les Update Domain ne sont utiles que dans le mode de gestion ASM (Ancien mode de gestion), dans la mesure où il est de votre responsabilité de patcher vous-mêmes les VMs.

Avaibility Zone

Mise en place gratuite, sauf le trafic de réplication.

Se met en place au sein d'1 seule région (et dans les régions où il y a 3 Datacenters)



VM Scale Set (VMSS)

- Scale out (Montée en charge automatique)
- Scale in (Diminution en charge automatique

Scalability

- Augmentation de la size de la VM
- Diminution de la Size de la VM (NB : Prendre en compte les limitations de la size choisie)

Les Extensions des VMs

- **Custom Script Extension**

Exécution d'un fichier PowerShell qu'après le premier déploiement de la VM.

Intérêt : Finalisation de l'infrastructure.

- **PowerShell Desirate State**

A chaque redémarrage de la VM, vérification de la configuration OS et éventuellement installation de composants.

- **Extension Windows / Linux Chef**

Géré par Cook Book.

- **VMAccess Extension**

Permet la réinitialisation du mot de passe

Set-AzureVMAccessExtension

Set-AzureRmVMAccessExtension

- **BGInfo**

Set-AzureVMBGInfoExtension

Set-AzureRmVMBginfoExtension

AZ-100.4 (Day 4) – Configuring and Manage Virtual Networks

Règles générales

- TOUT TRAFIC INTRA VNET → GRATUIT

  vmA (VNet1) peut communiquer avec vmB (VNet1) -> Trafic non payant

- TOUT TRAFIC SORTANT & INTER VNET → PAYANT

  vmA (VNet 1) ne peut pas communiquer nativement avec vmC (VNet2). La mise en place d'une communication entre 2 VNets est payante.

Les composants réseaux

VNET

1 VNET EST REGIONAL (1 Virtual Network est associé à 1 région)

On peut comparer un Virtual Network à un Switch.

1 MACHINE VIRTUELLE ne peut pas changer de Virtual Network → Obligation de suppression de la MACHINE VIRTUELLE puis recréer la MACHINE VIRTUELLE.

ON NE PEUT PAS CHANGER VNET, MAIS DE SOUS-RESEAU VIA 1 REBOOT

Le VNET existe en mode ASM et ARM.

Best Practice → 1 maximum par mode.

C'est une limite de sécurité réseau / 1 VNET par région (Largement suffisant)

50 VNETs maximum par abonnement

/! \ Voir Limites Azure sur site web via google.

VNET : composant servant à connecter les MACHINES VIRTUELLES.

IP PRIVEES, ADDRESS SPACE & SUBNET

Fournir des adresses IP Privés aux MACHINES VIRTUELLES (4096 @ IP Privés) / RFC 1918

Fournir des sous-réseaux différents (Préconisation des sous-réseaux IP Privés).

Par défaut, le routage des sous-réseaux est activé.

Par défaut, l'Address Space est défini dans le routeur.

ADDRESS SPACE (10.1.0.0/16)	ADDRESS SPACE (192.168.0.0/16)
Sous-réseau A → 10.1.0.0/24	Sous-réseau C → 192.168.1.0/24)
Sous-réseau B → 10.1.1.0/24	

Dans Azure, le nombre utilisable d'adresses IP est bien précise.

Exemple : Pour 1 sous-réseau 192.168.1.0/24, les adresses .1, .2, .3 sont réservés par Microsoft (sans oublier les .0 et .255)

Dans Azure, le plus grand masque possible est 255.255.255.248 (/29)

Gestion du trafic sortant (/ ! \ Le TRAFIC SORTANT EST PAYANT)

Route Table ou UDR - Premier niveau de sécurisation (ROUTAGE DU TRAFIC)

Exploitation & Mise en service gratuit

Route Table ou User Define Route (Trafic sortant) en mode **Stateless**.

Se met en place sur les sous-réseaux.

- ➔ Destination
  0.0.0.0/0
  10.1.1.1/32
  10.2.1.0/24

- ➔ Action (5 possibles)
  None ou Null (Droppé, éjecté)
  Internet
  VNET
  VNET Gateway (permet l'interconnexion entre 2 VNETs via 1 tunnel = Force tunneling)
  Vers 1 Virtual Appliance (Barracuda, Fortinet (€)).

Forced Tuneling

Imposer le trafic via un tunnel (Vnet Gateway)

NSG - Deuxième niveau de sécurisation (FILTRAGE DU TRAFIC)

NSG (Network Security Group) équivalent à un pare-feu. → En mode **Statefull**

Il gère le trafic entrant et sortant.

Il se met en place sur les sous-réseaux et sur les NIC associés aux MACHINES VIRTUELLES.

Lors de la mise en place d'un NSG, il crée par défaut :

➔ 3 règles de Trafic entrant
➔ 3 règles de Trafic sortant

Remarque : Par défaut, il n'y a pas de NSG. Conclusion, open bar. A vous de gérer le trafic entrant et sortant.

Type de trafic	
Entrant	Source
Sortant	Destination
	TCP / UDP
	Port
	Action

Virtual network Connectivity

Cross-Premises

- **Express Route**

Mise en place de la connexion entre On-Premises et le Réseau Public Microsoft

Attente entre 6 mois et 1 an (L'attente peut être longue pour des raisons de validation technique).

MPLS -> Lien nécessaire & le bon fournisseur ayant la technologie MPLS

3 circuits

- Public MS <-> SaaS (Office 365)
- Public Azure <-> PaaS (PaaS SQL)
- Private Azure <-> IaaS (Au sein d'un VNET, donc MACHINES VIRTUELLES mise en place)

- **Point-To-Site VPN (P2S VPN)**

Mettre entre place un tunnel SSTP entre une machine et un VNET Azure

Fonctionne avec des CA Self-Sign, Privé, Public

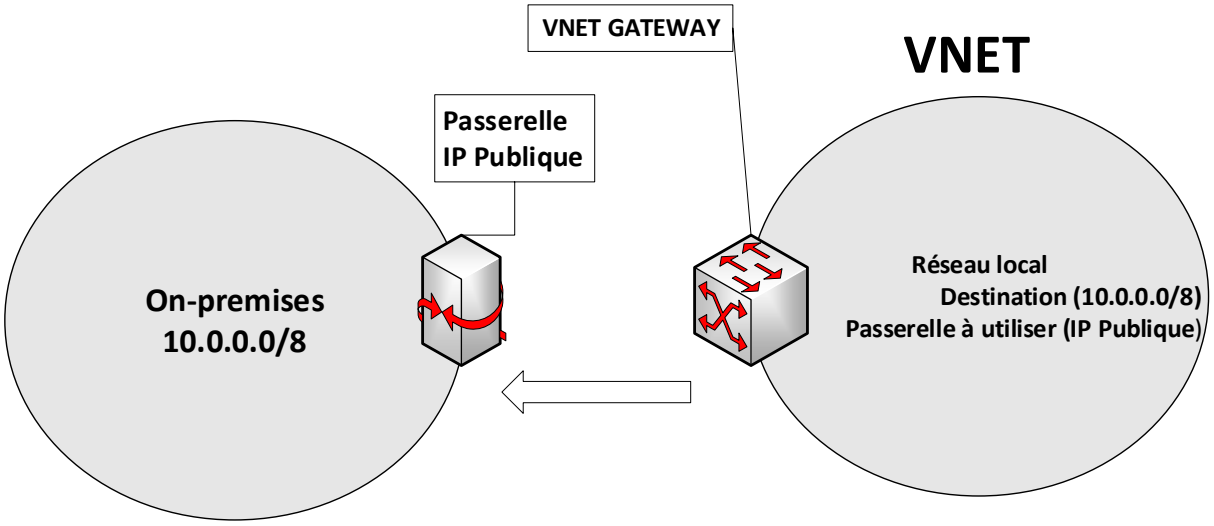
- **Site-To-Site VPN (S2S VPN)**

Connexion entre le réseau On-premises et un VNET Azure. Protocole Tunnel IPSec.

Tunnel VPN entre on-premises et Vnet Azure (via une Vnet Gateway)

Dependance de votre lien Internet

Temps de mise en place = environ 1h

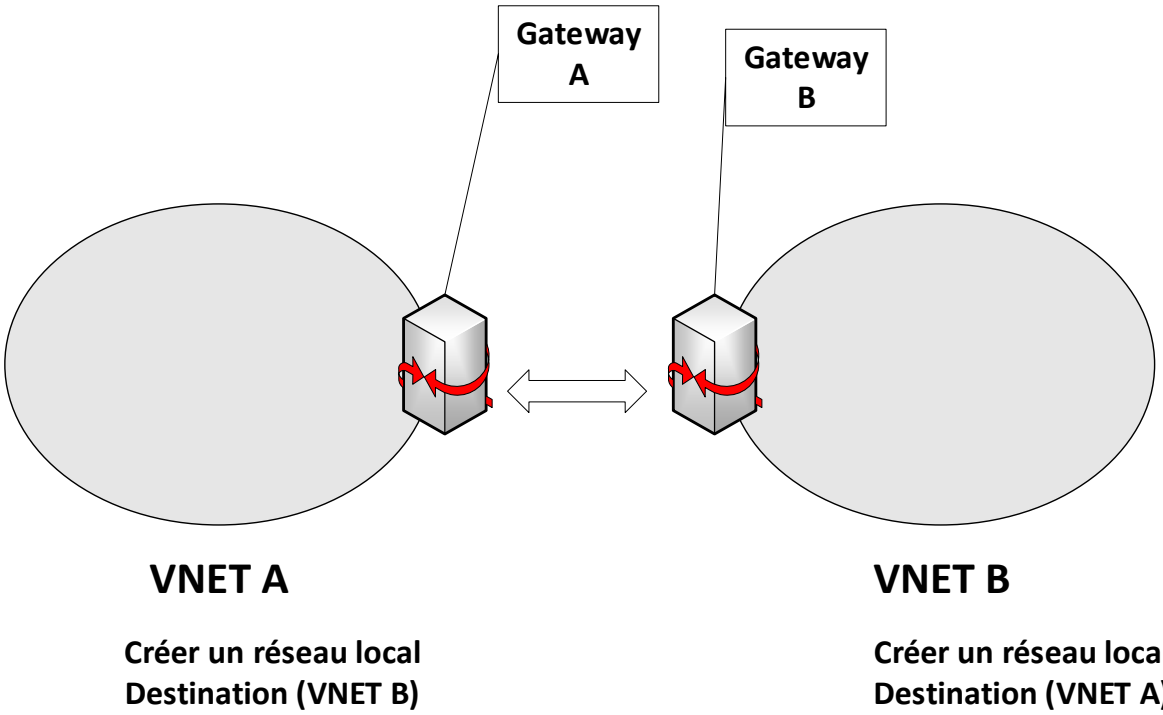


Cross-Vnet

Si les ordinateurs résident sur un autre réseau virtuel Azure, vous pouvez utiliser l'une des méthodes suivantes

- **VNET-To-VNET**

Transitif partout !!!



- **VNET peering**

Non Transitif !!!

Si deux réseaux virtuels résident dans la même région Azure, vous pouvez les connecter directement en tirant parti de la fonctionnalité de VNET Peering. Cela permet une connectivité directe entre eux sans avoir à déployer des passerelles VPN, ce qui élimine les coûts supplémentaires et l'impact sur les performances. Au moins un des réseaux virtuels dans la mise en place du VNET peering doit être une ressource Azure Resource Manager; il n'est pas possible d'utiliser le VNET peering pour connecter deux réseaux virtuels classiques.

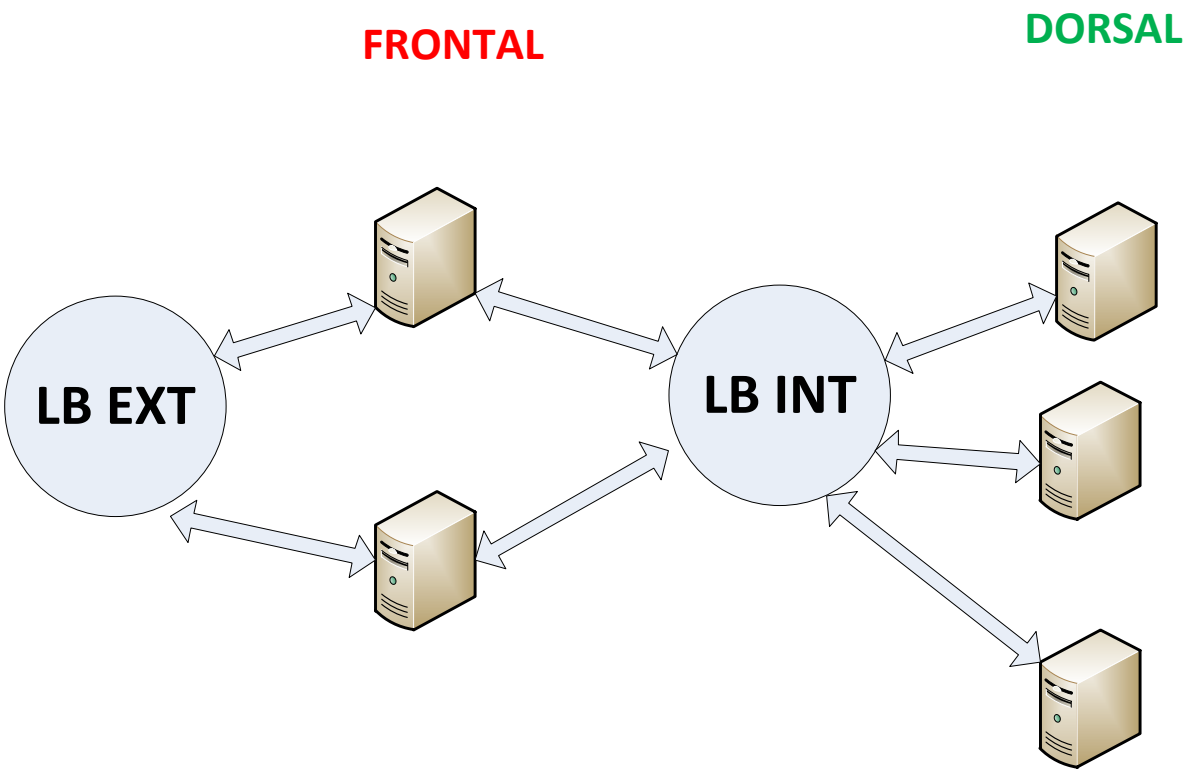
Equilibrage de charge

Load Balancing

- Application Gateway (HTTP & HTTPS) → Couche 7
- Traffic Manager (DNS)

Equipement

- Load Balancer (Interne et Externe) → Couche 4



AZ-100.5 (Day 5) – Implementing and Managing Hybrid Identities

AZURE DATABASE

PaaS SQL ou Azure SQL Database (/!\ -> Différent de SQL Server dans un VM IaaS)

Non connectable à Active Directory.

Plus il y a de **DTU**, plus la DB sera rapide.

1 Serveur SQL PaaS fournit par Microsoft peut atteindre maximum 45 000 **DTU**

SGDBR (Système de gestion de BDR)	NO SGDBR
SQL	**No SQL**
Transactionnel	**No Transactionnel**
ACID	**No ACID**
Relationnel	**No Relationnel**
Schema fixe	**Schema fixe**
SQL SERVER	**CASSANDRA**
ORACLE	**MangoDB**
POSTGRES	**Redis**
DB2	**Couchbase**
MySQL (Oracle gratuit)	

Big Data

- HDInsight (Microsoft)
- EMR (AWS)
- Hadoop (Apache Software Foundation)

Tous utilisent le système de fichiers **Hadoop Distributed File System (HDFS)**