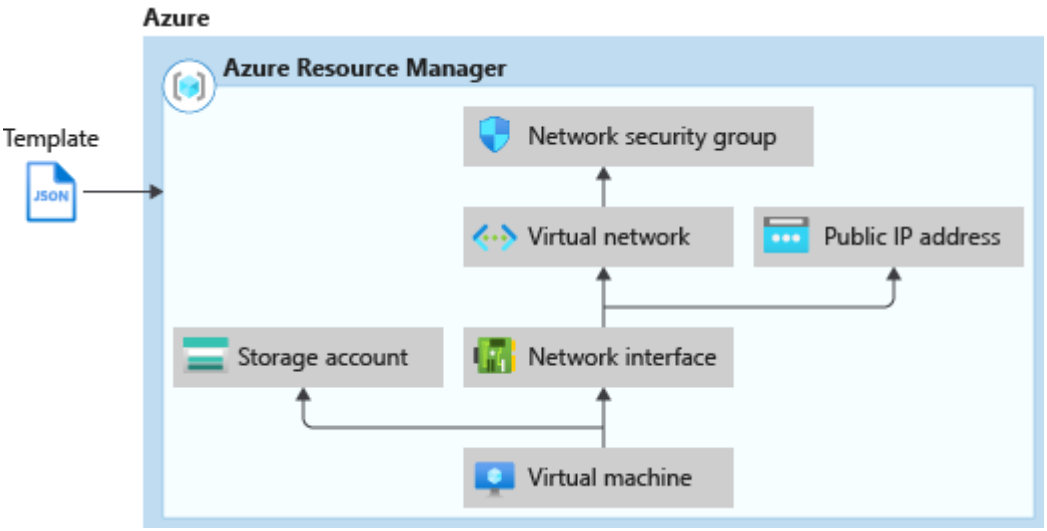
https://github.com/MicrosoftDocs/azure-docs/tree/master/articles
AZ 104 cours

Template :

- **Depandancies** :
  -
  -
  - 

  - VM depend on **Storage account** and **NetInterface**
  - Network interface depend on **VNET** and **public IP**
  - **VNET** depend on **NSG**

  - When deploying a virtual machine from a template, you must specify:
    - the **Resource Group name** and **location** for the VM
    - the **administrator username** and **password**
    - an unique DNS **name** for the public IP

- **Template Copy field**:
  - Mean "**count**" **instance of the ressource will be deployed**

Parameter and variable :

1. If template in question
   has below then location from the **variables** in **template** file will be used.

"resource":["location":"[variables('location')]]

2. If template in question has below then location from the **parameters** file
   or manually will be used.

"resource":["location": "[parameters('location')]"]

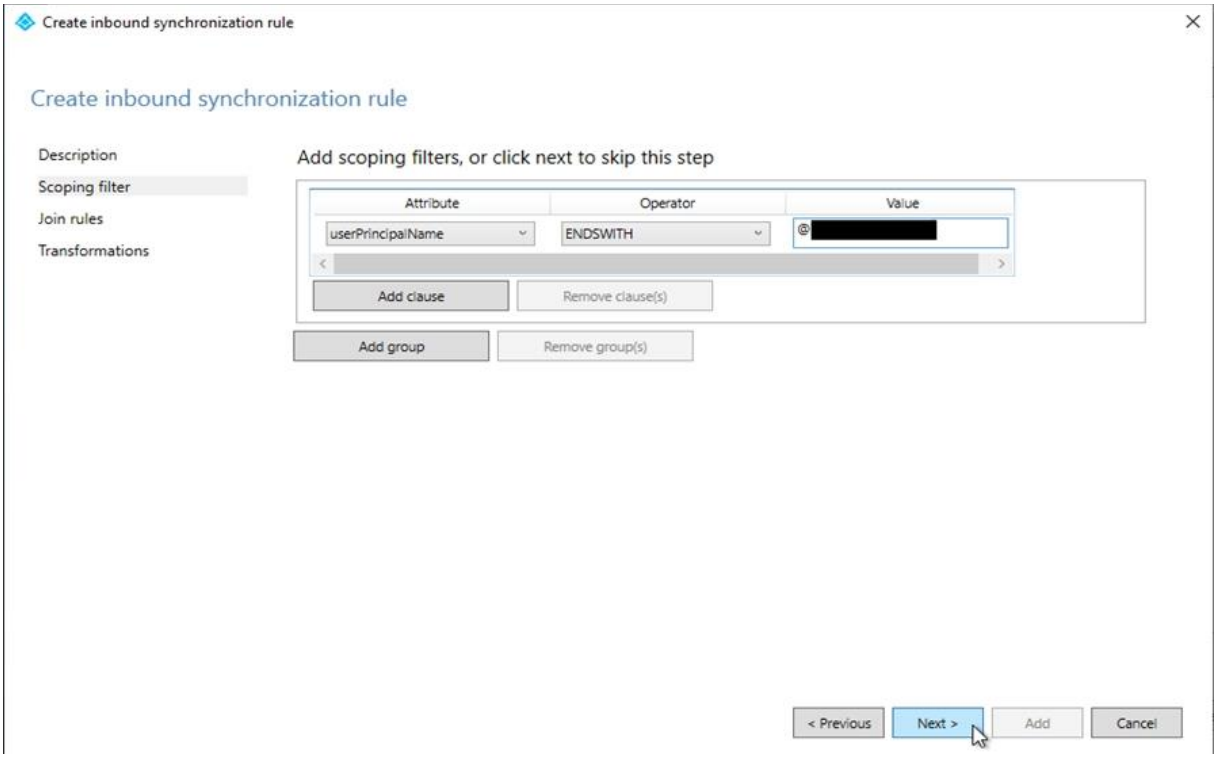
Custome role JSON:

- Field obligatoire
  - IsCustom
  - AssignableScopes
  - Description

AD Connect :

- Least privilege for **sync** :
  - AAD : Global administrator

        - ADDS : Enterprise Admins (EA) group
    - Lest privilege for **enable SSO**
        - ADDS : Domain Admin
    - Sync user to Azure Ad based one rule like the upn of the account
        - GUI (**Synchronization Rules Editor**) or PowerShell **not the syncronization options .**



    - **Staging** mode
        - In staging mode, the server is active for import and synchronization, but it **does not run** any exports, not running password sync or password writeback
        - **Need to disable** stagging mode for starts exporting, enables password sync, and enables password writeback.

Hybrid solution :

- **Hash syncronization**:
    - AD Connect sync the **Hash** of the Password **Hash in Azure AD** and Azure AD accepts both the user name and password validate it with the synced hash.

- **Pass-throught** :
    - Auhtehnticate directmty too Azure One premises
    - Azure AD accepts the user name and password and send it **On-Premise Auth**N agent server which will authenticate with AD and return the successful authentication to Azure AD
    - If 365 can't reach your pass through agent you won't be able to authenticate until it comes back online.

- **ADFS**
    - Authent diretclty to AD one premise

- MFA for ADFS :
  - you can select Certificate Authentication (in other words, **smart card-based authentication**) as an additional authentication method.

Azure Automation runbook

- Can use it in **action group** after a **alert rule** **is trigered** for lunch task like **powershell script** test
- **Or restart a VM**

Budget :

- When your consumption reaches a given threshold, alerts are generated by Cost Ma nagement. There are three types of **cost alerts**: **budget alerts**, **credit alerts**, and department spending quota alerts.

Avset

- VM and Availability Set **must be** in the **same region** and **same RG**
- Maintain application performance accross different VM
- Calcul AvSet :
  - (Number of VM / (fault or update))* (numer of fault or update available)
  - AvSet VM must be in same region and have same RG

Log analytic

- Data source :
  - For linux configure **Syslog data source** in the workspace (**Syslog** is an event logging protocol **common t o Linux**)

Devices feature :

Enterprise State Roaming (ESR)

- Permet de repercuter les changements fait (pour un user ayant la fonctionnalité activé)sur un poste utilisateur vers un autre poste (Azure AD join)
- **Applicable uniquement aux utilisateur ou a groupe d'utilsateur** pas a un Device
- Requierement :
  - **Windows 10**
  - The device is **Azure AD joined** or hybrid Azure AD joined
  - You can enable roaming for all users or for only a selected group of users.(**all or group not single like SSPR**)
  - Enterprise State Roaming is enabled for the tenant in Azure AD
  - The **user is assigned** an Azure Active Directory **Premium license P1** or **P2**
  - The device must be restarted and the user must sign in again

SSO :

- **Registred** PRT
- **Joined-device** PRT
- **Hybrid joined** Seamless

Peering

- Need to recreate peering when adding addresse space
- Must not overlapse

Advanced threat protection

- Storage threat protection is available for **blob** service

Container :

- You need to add a file named File1.txt from Server1 (container host.)to a folder named C:\Folder1 in the container image.
  - You can add the following line to the **Dockerfile** (all these option is valid)(**No Copy-Item** and **XCOPY commands** allowed) :
    - COPY test1.txt /temp/
    - COPY test1.txt c:/temp/
    - ADD test1.txt /temp/
    - ADD test1.txt c:/temp/
  - Dockerfile :
    - text file that contains the instructions needed to create a new container image.

Azure Container Registry

- Storge where you can push docker image that container can use
- Push docker image you created to container registry

Deploy container image to a AKS Cluster

- Run docker tagwith the right ACR.
  - **docker tag mcr.microsoft.com/oss/nginx/nginx:1.15.5-alpine myregistry.azurecr.io/samples/nginx**
- Docker push
  - Push the Container image to the ACR
  - **docker push myregistry.azurecr.io/samples/nginx**
- - create kubectl apply with the right deployment and right ACR.

AKS :

- **Step to ma Manage AKS**
  - **1) az aks create**
  - **2) Install Kubetcl with cli**
    - **az aks install -cli**
  - **3) First you connect to the AKS Cluster in CLI :**
    - **Az aks get-credenials –resource-group --name**
  - **To show all your nodes you can use this command.**
    - **kubectl get nodes**
  - **A similar command is used to display information about your pods:**
    - **kubectl get pods**
  - **Get servcice running on nodes**
    - Kubetcl get service
  - **To create resources defined in the YAML file you should use:**
    - **kubectl apply -f ./myFile.yaml**
  - **When you want to manually scale the resources to 5 you can do it by this command:**
    - **kubectl scale --replicas=5 -f ./myFile.yaml**
- **Continuous Deployment in AKS**
  - Using **Azure Pipelines**
-

App service

- Configure **TLS** mutual authentication
  - Must be minimum Basic , Standard, Premium, isolated
  - ASP.NET : Client cert is in the **http request header**
  - For other (Nodejs,php..) the client cert in in a **base64** encoded value
- Configure a **WebJobs**
  - You can choose to develop a WebJob that runs as either a **.NET Core** app (**ASP.NET** or .NET Core)
- **Autoscale :**
  - **Scale out** occur if **ANY condition is met**
  - **Scale in** occur ONLY IF **ALL condition are met**
  -
  - **Scale in (know when a scale in wile occure) Use case :**

    - Taken current number of instances: 3
    - Scale rule
      - **Increase** the instance count by one when the CPU percentage is greater or equal to **80.**
      - **Decrease** the instance count by one when the CPU percentage is less than or equal to **60.**
    - instances after scale in: **2**
    - **60, 55, 50, 45 are CPU%**
    - We have:
      - **3**x**60** = 180 / **2** = 90.0% (>80%, no scale in occurs)
      - **3**x**55** = 165 / **2** = 82.5% (>80%, no scale in occurs)
      - **3**x**50** = 150 / **2** = 75.0% (<80%, scale in)
      - **3**x**45** = 135 / **2** = 67.5% (<80%, scale in)
    - The **estimated number of cpu after scal in** must **not t riggere** the **scale out treshold** , if then the scale in will not occur

Azure Instance Metadata Service MDS

- is a REST API p**rovides information** about currently **running virtual machine** instances(**Auth to ken**, SKU, storage, network configurations, and upcoming maintenance events) you can use it to manage and configure your virtual machines.
- You can only access it from within the VM with the **169.254.169.254** non routable
  - Ex : http://169.254.169.254/metadata/identity/oauth2/token

VM Migration

- **BitLocked disk Not supported**
  - **Vmware**
    - OS disk must be a basic disk
    - Data disks can be dynamic disks
      - **OS Disk** :

        - Up to **2,048 GB** (**2T**) for Generation 1 machines
    - **Datadisk** :
        - Up to **32,767 GB** (**32T**) Replicating to managed dis k
        - Up to 4,095 GB (4T) Replicating to storage account

- **Hyper-V**
    - Generation 1
      Generation 2—Windows only, OS disk only
        - **Os Disk**
            - Up to **2,048 GB** (**2T**) for generation 1 VMs.
            - Up to 300 GB for generation 2 VMs
        - **Data disk**
            - **VHD size Up to 4,095 GB (4T)**

Upload a Windows virtual machine (VM) from on-premises to Azure

- **Step**
    - Run `sfc.exe /scannow` on the VM
    - Update remote desktop registry settings
    - Configure Windows Firewall rules
    - Install Windows updates
    - **Generalize** a VHD (**Sysprep**)
    - **Convert the virtual disk** to a fixed size **VHD** Using **Hyper-V** Manager or **Powoershell**
    - Uploads a VHD from an on-premises to a **blob** in storage account in Azure.
        - **Add-AzVhd -Destination** "http://contosoaccount.blob.core.windows.net/vhdstore/win7baseimage.vhd" -**LocalFilePath** "C:\vhd\Win7Image.vhd"

Azure monitor

- From **Workbooks**, create a **workbook**
    - **graph visualization** to display the **traffic flow between the virtual machines.**

Azure Bastion

- provides secure and seamless **RDP** and **SSH** access to your virtual machine
- Connect to a vrm from **RDP** throught a **shared external public IP** addresse
- Bastion **can view all the VMs** if the **VNETs are peered.**

Azure Queue :

-

Azure Service Bus queues :

- Is FIFO first in first Out

- **Authorization** :
    - **AAD**
    - **SAS**

Azure Cosmos DB :

- If You plan to change the partition key for a container in a CosmosDB account you need to do first :
    - **Create a new Azure Cosmos DB account**
- **Azure Cosmos DB** currently provides the **following APIs** :
    - **Core (SQL) API** for **JSON document** data.
    - **MongoDB API** for **JSON document** data.
    - Cassandra for a columnar or column-family datastore.
    - Azure Table API for key-value datastore.
    - Gremlin (graph) API for graph data.
- **Cosmos DB config** :
    - **multiple-write** is available on account level not on Database level so if you have **differnt write setting (multple write region / only one write region)** you should create 2 **different Cosmos DB account** .
    - Microsot recommand using **one API** for **each Cosmos DB account**

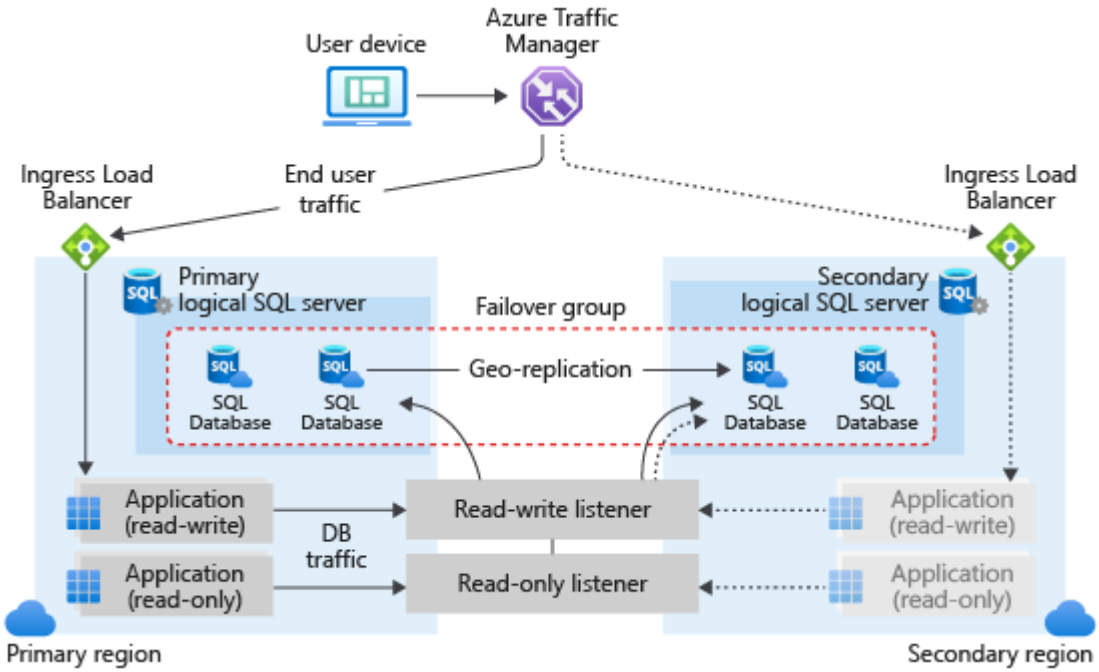
Azure Managed instance :

- **In a Subnet VNET and have a IP adresse**

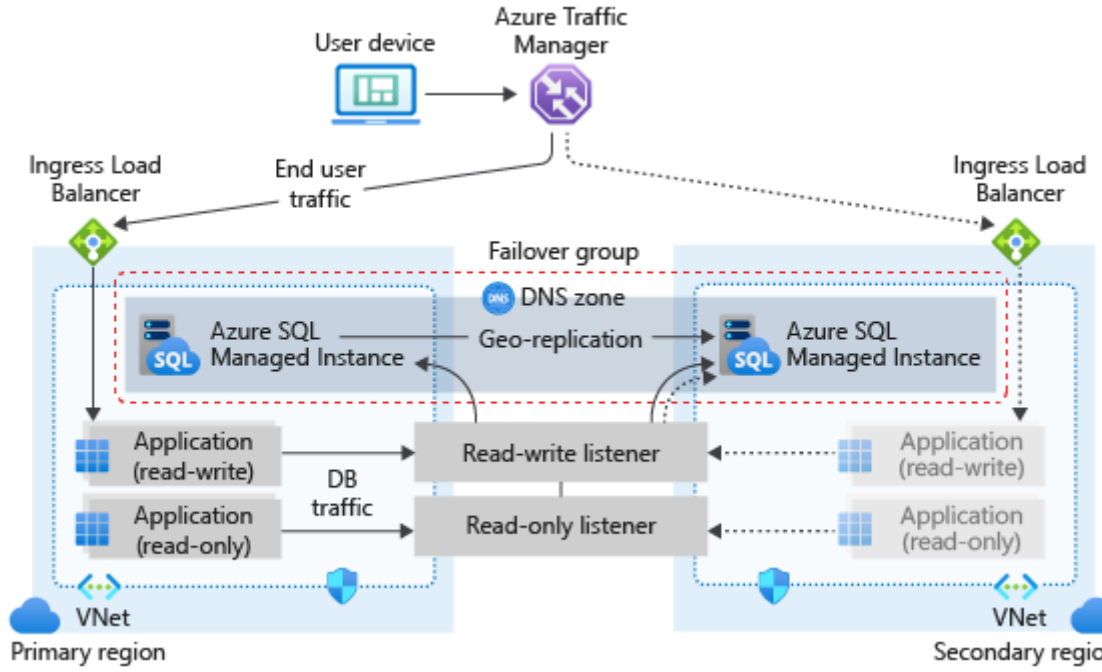
Azure SQL Server :

- **Paas DDB**
- **Management function (upgrad, patch,backup)**
- **Cloud version of Microsoft SQL**
- **Moove Database**
    - You can only moove(remove and add) DB (databse) **within pool** (**elastic pool**) in the **Same SQL Server**
    - You **cant remove and add** a **DB** in a **different SQL Server** than **origine**
- **Transactions acroos DB**
    - **server-side transaction** are **supported** when the **DBs** are hosted on the same **SQL Server** deployed in a **virtual machine.**
    - **client-side transactions** are **supported** when the **DBs** are hosted on the same **Azure SQL Server**
- **Query editor**
    - query an Azure SQL Database Step :
    - Go to Query editor pane
    - Establish a connection to the database
        - Even though you're signed into the portal, you still need to provide credentials to access the databas e (login/password)
    - Run Query
    - *Your **local network settings** might be preventing the Query Editor from issuing queries.*
        - Configure local network settings
        - Open **Windows Defender Firewall**
        - Add outbound rule for **443, 1443**
- **SQL Failover group** :
    - For **Azure SQL Database and Azure SQL Managed Instance**

- The **secondary** SQL DB Server
  or SQL managed instanc must be in **different regions**
- To do auto-failover, you must
  have **primary** and **secondary servers** in **different regions**. If you want
  to **failover databases in an elastic pool**, then the **secondar**y server
  must have the **same pool name**. You can also failover
  a database that is **not part of a pool** to a **secondary server.**
- If your **SQL Managed instance** are in **different VNET** you **must confi gure** a global **peering** ore
  a **VPN beetween** the **VNET** beacause the Instance in a same failover group should be able to communicate .
-



-



-
- Creating failover groups between two servers in different subscriptions is not currently supported for Azure SQL Database
- You can create a failover group between SQL Managed Instances in two different subscriptions, as long as subscriptions are associated to the same Azure Active Directory Tenant.

Automated Backup v2

- Azure configuration **backup option** for **Azure SQL Server virtual machines,**
- Store the backu up in an Azure **Storage account in Blob** storage.

Storage :

- In **GRS** data is copied **3 in LRS in primary** region and then **3 copy** **LRS** asynchronous in second region
- **GZR** data is copied **3 time in ZRS primary** region and **3 copy** **LRS** asynchrinous in second regions

Premium and Standard SA :

- **Premium only** storage account : **File share , Block blob**
- **Standard only** storage acount : **Blob storage**
- **Prem and Stand** Storage account : **General v1 Genera l v2**
  - **Prem** : support **only page blob**
  - **Stand** : page blob, block blob, append blob, files shares, tables queu

- **Hirarshical namescpae**
  - Setting that need to be enabled on storage account for set Azure AD permission in indivudual blob

VMSS

- Be aware minim , max and inital VM instance

the **managed disk** feature allow you :

- This feature further increases the scalability of virtual machine scale sets by allowing you to create up to 1,000 VMs in a virtual machine scale set using a Marketplace image.
- When deployed VMSS with automation if you want to automticely install Feature and app in the deployement you need to :
  - **Upload** a PS script in a storage account
  - In the **CustomScriptExtension** in properties you add :
    - You specifie in the template the SA the key and the file to use
    - The comand to execute

(voir : https://medium.com/charot/custom-script-extention-on-azure-vmss-e010a8c87904)

- **NSG**
  - **NSG** for VMSS are configured at **NIC** level of each **VM instance**

- **Load balancer rule**
    - If the app **must be accessed from** http and https you have to create **2 load balancer rule** On for the **HTTP traffic**, and one for the **HTTPs traffic**.

Virutal netwokr Gateway :

- You ca route all the traffic of a subnet to a One premise location chosing the VnetGatway as the next hop in the UDR
- **Gateway subnet already exit** as there is **ExpressRoute configured and working.**
    - So you need to create :
        - Create a **VPN gateway VpnGw1 SKU** for **coehexist** with a **Expresse route.**
        - Create a **local network gateway (** local site VPN gateway) -
        - Create a **VPN connection**

Azure Performance Diagnostics :

- Go to VM panne -> Extensions -> Chose Azure Performance Diagnostics
    - Azure Performance Diagnostics VM Extension helps collect performance diagnostic data from Windows VMs. The extension performs analysis, and provides a report of findings and recommendations to **identify** and **resolve performance issue s on the virtual machine** like **Network Trace** . This extension installs a troubleshooting tool called PerfInsights.

SLA

- Deploy 2 or mor instance of VM behind availability zone assure SLA of 99.99% or whith **avaiblityset** SLA of **99.95**% for the service
- Adding load balancer for redundancy increase the SLA too **99,99** % with **AZ**

- **Single VM SLA** :
    - Virtual Machine using **Premium** SSD **99,9 %**
    - Virtual Machine using Standard SSD Managed Disks for Operating System Disk and Data Disks 99.5%
    - Virtual Machine using Standard HDD Managed Disks for Operating System Disks and Data Disks 95%.

VM Windows DiagSetting :

- Enable
- Install monitoring agent
- Log analytic workspace as destination of logs
- Create a alert in alert monitor
- Selec the log analytic workspace as source

Linux Diagnostic Extension (LAD) 3.0

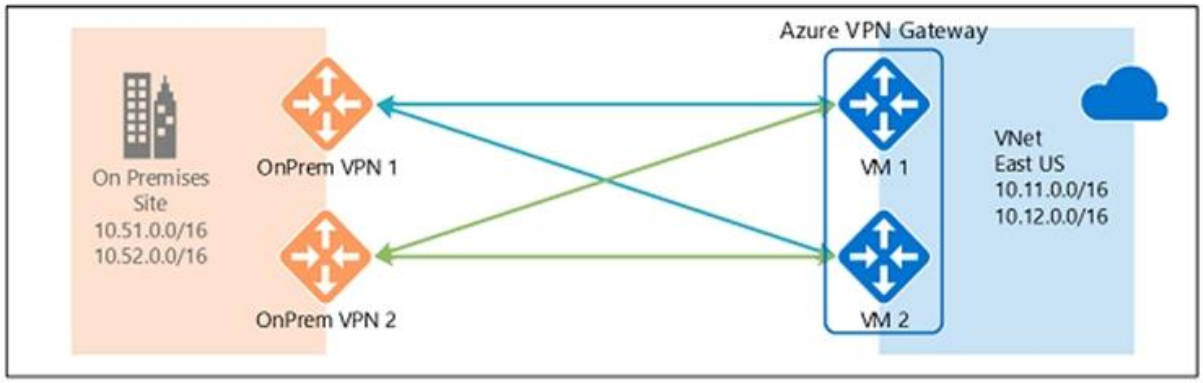
- The Linux Diagnostic Extension helps a user **monitor the health** of a **Linux VM running on Microsoft Azure.**

Replicate VM to Azure

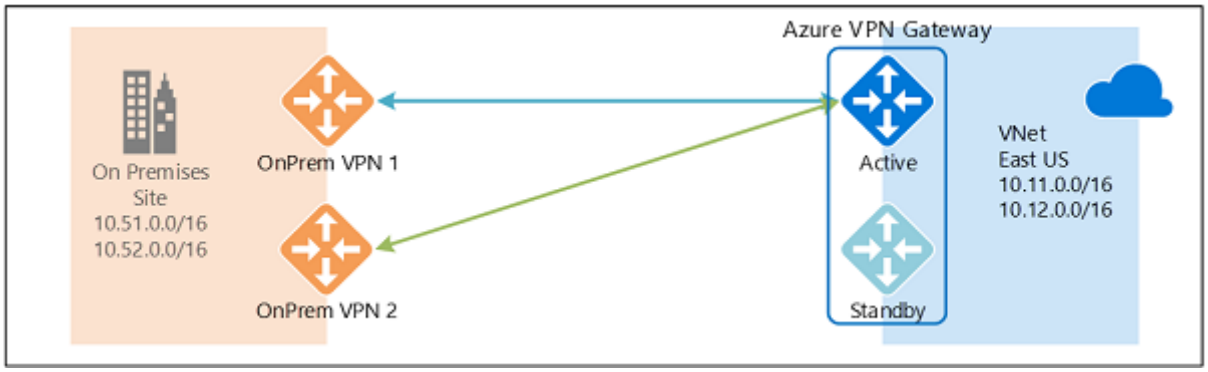
- **Replicate One premise Hyper-V VM to Azure**

- **Recovery Services vaults**
  - **Site Recovery**
  - Select one premise location -> Hyper-v
  - Create **Hyper-V Site**
  - Add hyper-v server
    - Dowload the Microsoft Azure Site Recovery Provider software
    - Dowlorad the key
    - Install it on each Hyper-v host
  - Select the target Env (RG)
  - Set up the **Replication policy** (copy frequency , retention point)

Highly Available Cross-Premises and VNet-to-VNet Connectivity



4 public IP
2 local network gateway
1 Vnet gateway
if a single instance of an Azure VPN gateway fails, or a single on-premises VPN device fails, the failure will not cause an interruption that is longer than two minutes.
PS :
You can also do this but with this config with one VPN gateway and 3 IP but
For any planned maintenance or unplanned disruption that happens to the active instance, the standby instance would take over (failover) automatically, and resume the S2S VPN or VNet-to-VNet connections. The switch over will cause a interruption.that can be about 1 to 3 minutes in the worst case.



Azure Sentinel workspace

- there is no built-in functionality that notifies you via email
  if there is an incident that is generated in Azure Sentinel. However, you can set up an Azure
  Logic App playbook to send incident information to your email.

Load balancer

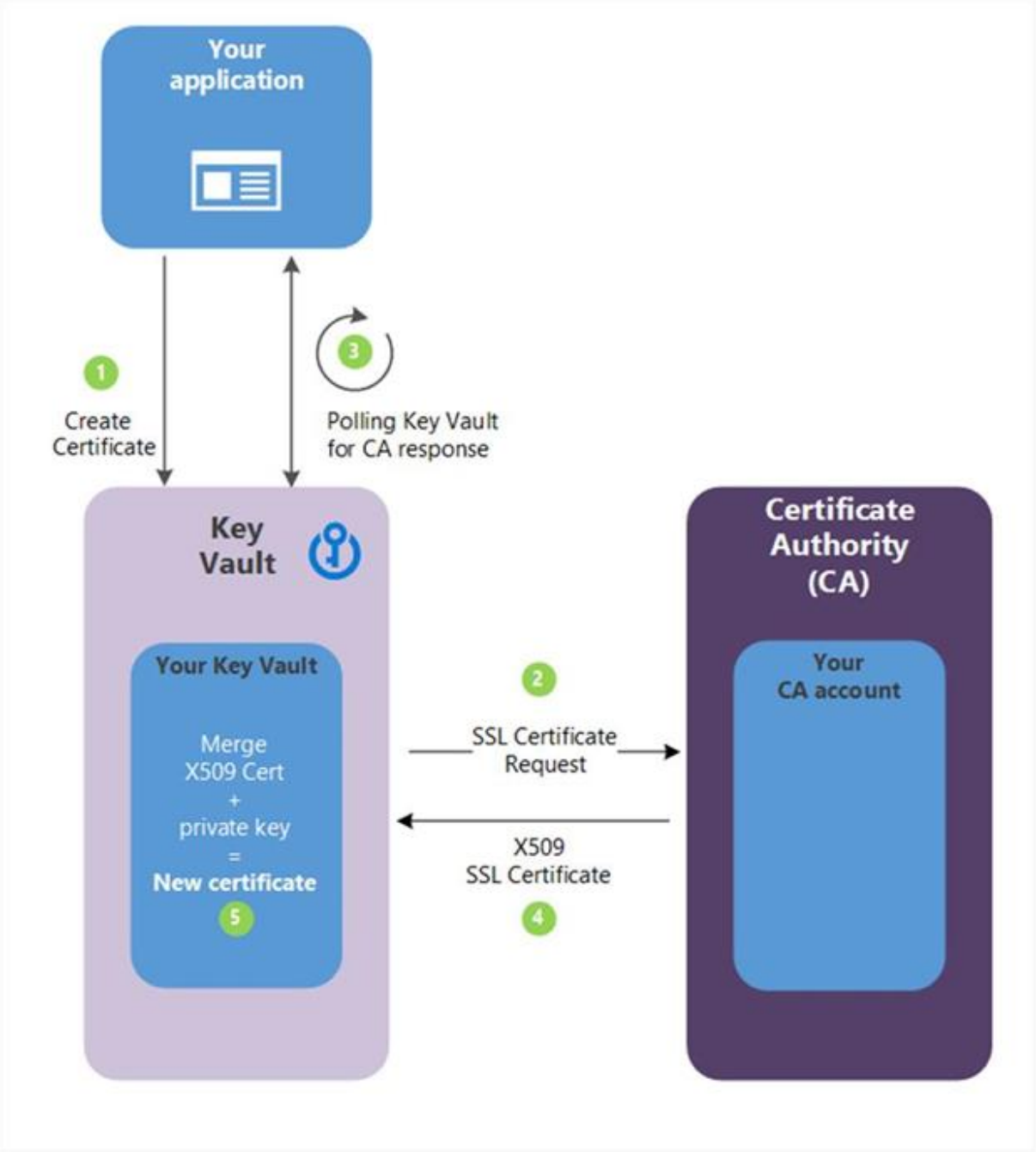
- Outbound rule
  - Azure Virtual
    Network NAT can provide outbound connectivity for virtual machines utilizin g an public standard load balancer Step
    - Add the **network interfaces** of the **virtual machines** to the backend pool of LB1.
    - Add an **outbound rule** to LB
    - Associate a network security group (**NSG**) to Subnet1.
  - Azure **Standard load balancer**
    - **HEALT PROBE**
      - **TCP, HTTP**, **HTTPS**
      - **Https** is **only allowed** in **standars sku load balan cer**
  - Azeure **Bacic load balancer**
  - **HEALT PROBE**
    - **TCP, HTTP**

Backing up your databases in Microsoft Azure

- Backup to URL
  - Backup Azure and one premise
  - Store the backu up in an Azure **Storage account in Blob** storage.

Azure Key Vault :

- **Firewalls and virtual networks pane**
  - **Like in SA** you cant limite access to a Network and IP with this feature
  - Default is disabled and allow all
  - Trusted Services feature like in SA
  - Can configure private endpoint (private link)
- **Generate deploy and manage Certificate from keyVault creating a trusted partnership with (DigiCert or other provider) certificate authority - Step**
  - Obtain the CA account credentials. (recuperer les information d'identification obtenue a l'inscription sur le site de l'authorité de certification)
  - Create a certificate issuer from key Vault
    - **Add the Certificate Authority to keyvault (you have to create a account in the CA site)**
    - **Enter a name, the account ID , your password**
    - **Click Create**



MFA and SSPR AUTH METHODE :

	SSPR	MFA
Authenticator App	×	×
SMS	×	×
Voice call	×	×
Windows Hello		×
FIDO2 security key		×
OATH software/hardware tokens		×

Security question	**×**	
Email addresses	**×**	

Also for MFA : App passwords ***(****used for old applications) that don't support modern authentication*

MFA :

- **Trusted IPs** :
  - **Feature** of Azure **MFA that bypasses**
    MFA for users who **sign in** from sepcial **addresse range** and **IP** (**the company intranet, one premise**)

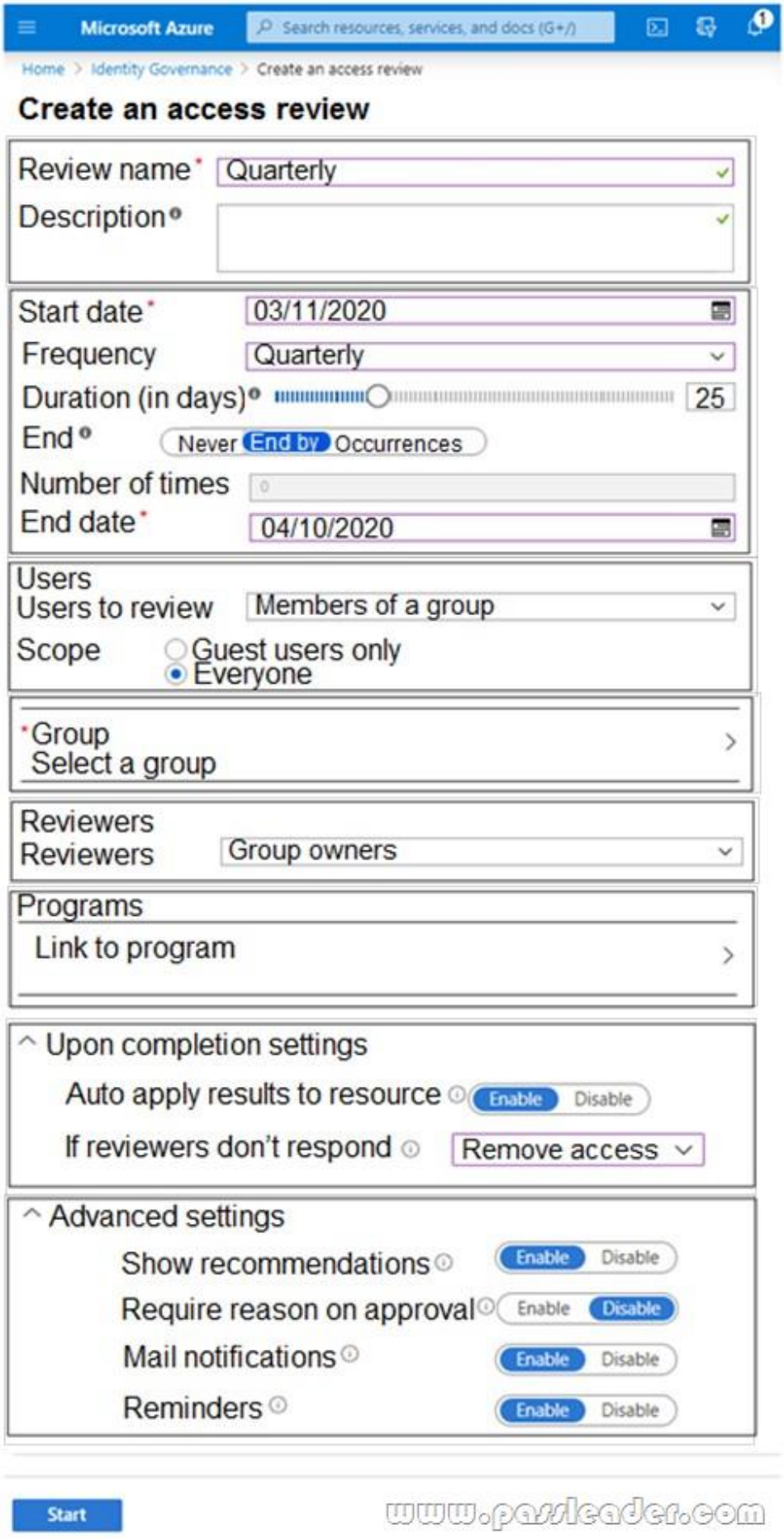
SSPR :

- Option Set **Notify users on password resets** option to *Yes*.
  - These notifications can cover both regular user accounts and admin accounts.

- Option **Notify all admins when other admins reset their password** to *Yes*
  - only 'global administrators' get notifications about admin password change, not all kinds of administrators
-

Azure AD access review :

- 1. Azure AD **Premium P2**
- Azure AD **Privileged Identity Management (PIM)**.
- 2. be a **Global administrator** or a **User administrator**
- onboard the Tenant to allow for access reviews.
- **Access review pane** :



- Area 1:
    - The access review must be enforced until otherwise configured. We set **End**: **Never**.
    - The access review must be completed within two weeks. We set **Duration** (in days) to **14**.
- Area 2:
    - A lack of response must not cause changes in the operational environment. We set **If reviewers don't respond**: **No change** (which leave user's access unchanged).

Azure AD RBAC :

- You **cannot remove inherited roles, Be aware**
    - you will get this error "Inherited role assignments cannot be removed.
    - Open the scope where the role was assigned and remove it from there.

Azure Load Balancer

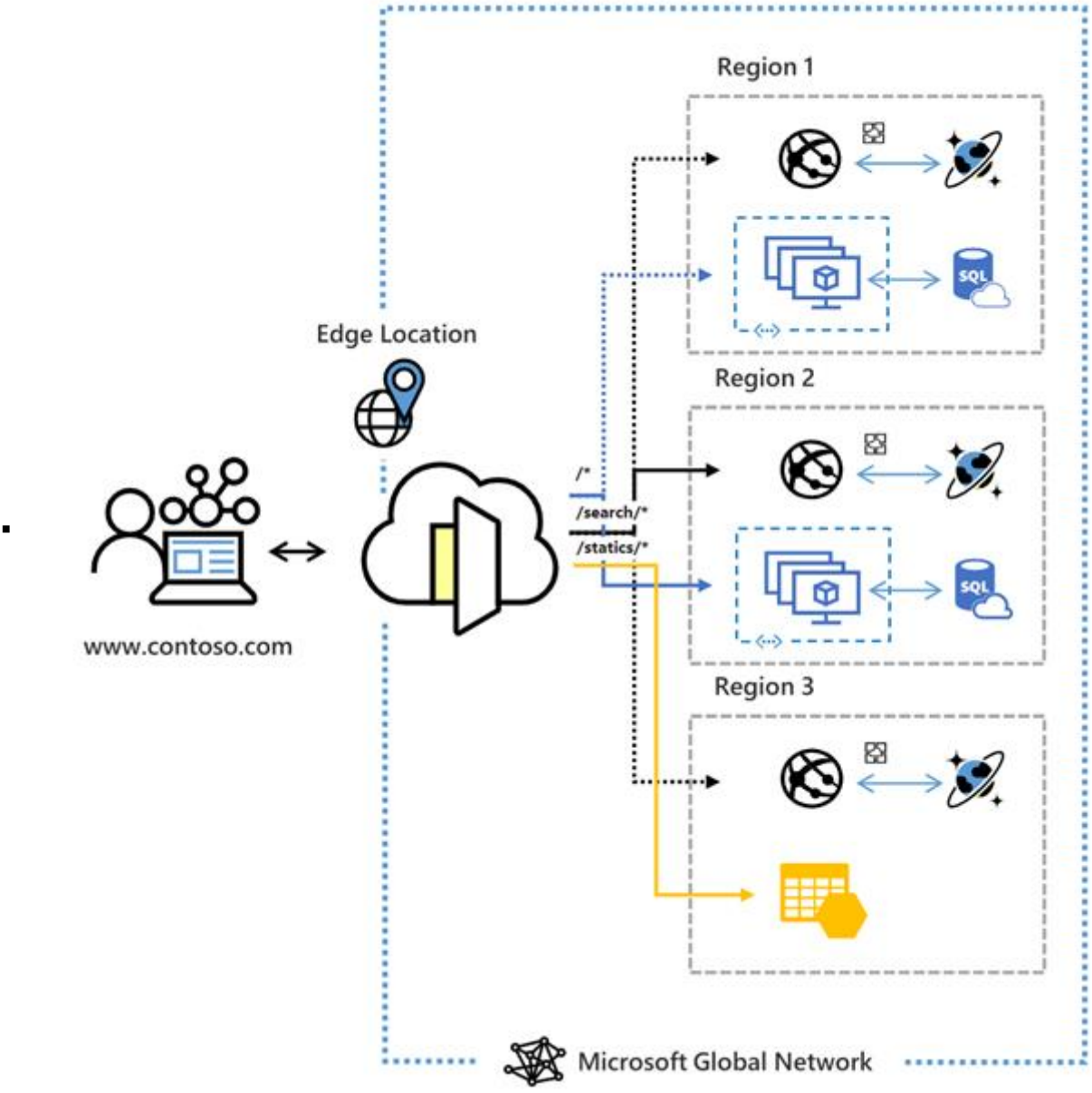
- **All load Load balancer** type support **support static public IP addresses**
- Load balancer support Virtual Machine in Back end pool
- **dont support webb app in Back end pool**

Azure App Gateway

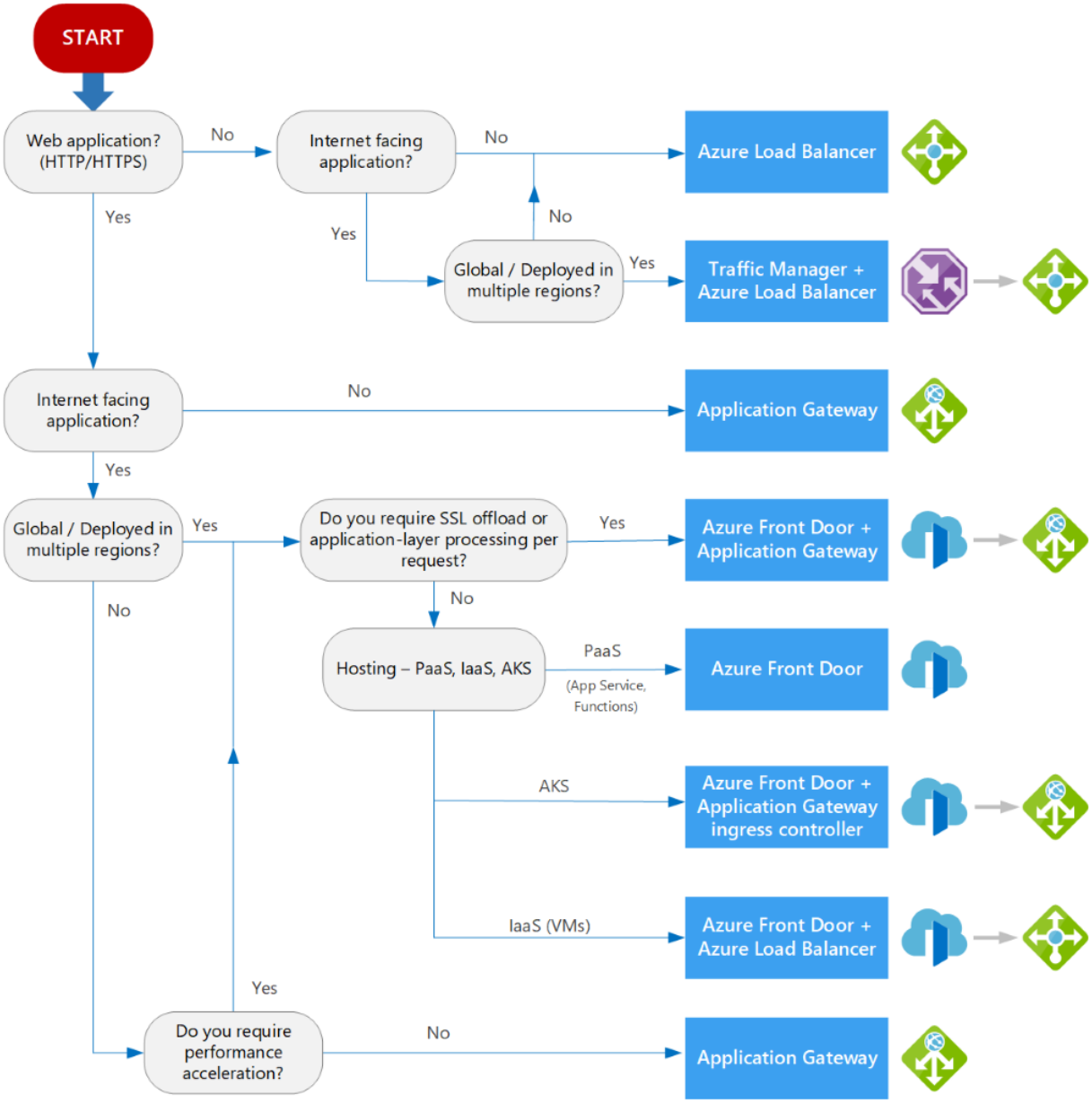
- Appp Gateway Standard does not support static public IP addresses
- **App Gatway Standard** sku **v2 support Static IP**
- App Gatway **Support Web app in Back end pool** not load balancer **VM too**
- Provide **SLA** of **99,95**

Azure front door :

- Service permettant de **distribuer le Traffic** entre les Azure **région**
- Layer 7 (HTTP/HTTPS) load balancers (Like Applicaion Gateway)
- Application security with integrated **Web Application Firewall (WAF)**
- **Accelerated application** performance by using **split TCP-based**



- Azure Front Door is a **global (cross région)**, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications
- Based on your routing method you can ensure that Front Door will route your client requ ests to the fastest and most available application backend. An **application backend is** any **Internet-facing service hosted inside or outside of Azure.**
- Azure Front Door needs a **public VIP** or a **publicly available DNS** name to route the traffic to. Deploying an **Azure Load Balancer behind Front Door** is a **common u se** case.



(Voir : https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview#decision-tree-for-load-balancing-in-azure

https://docs.microsoft.com/en-us/azure/frontdoor/front-door-overview

https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq#can-azure-front-door-load-balance-or-route-traffic-within-a-virtual-network
)

Azure traffic manger

- DNS based tarffic load balancer(**Not for HTTP HTTPS** traffic : **TCP UDP request**)
- Service permettant de **distribuer le Traffic** entre les Azure **région**

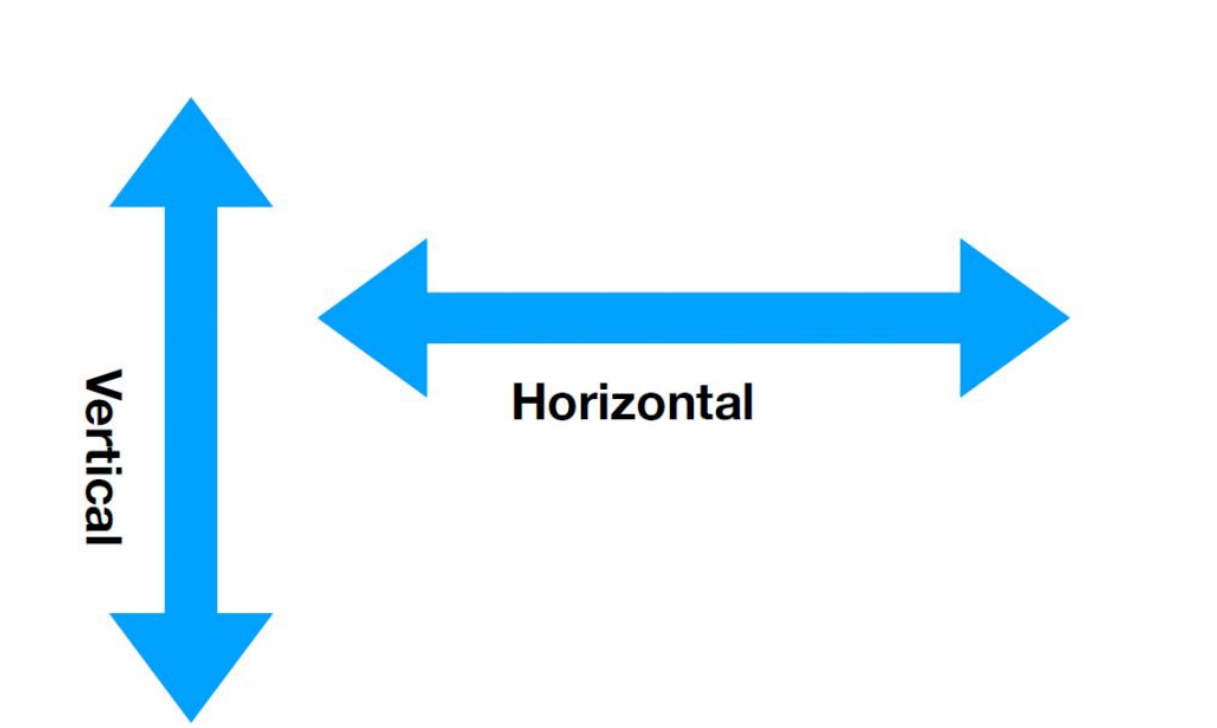
Update Management :

- You can enable it one VM for manage the update
- **Update deployments**

        - Must created **1 for each OS Global type** (windows ore linux) (**2** if you have the 2 kind)
    - *(Voir : https://docs.microsoft.com/en-us/azure/automation/update-management/deploy-updates)*

Azure Encryption (ADE) :

- Azure Encryption is supported on **all types of disks**
- To encrypt, a secret is sufficient
- To **sign** something, it needs to be related to an entity so a **certificate**



A Marketplace image :

- **A Marketplace image** in Azure has the following attributes :

*Publisher: The organization that created the image. Examples:
Canonical, MicrosoftWindowsServer

*Offer: The name of a group of related images created by
a publisher. Examples: UbuntuServer, WindowsServer

*SKU: An instance of an offer, such as a major release of a distribution. Examples: 18.04-LTS, 2019-Datacenter Version: The version number of an image SKU.

"storageProfile":{
"imageReference":{
"publisher":"MicrosoftWindowsServer",
"offer":"WindowsServer",
"sku":"2016-Datacenter",

"version":"latest"
}

VNET Integration :

- Vnet integration for app service **Integrate the app** in a **particular subnet** of the vnet delagated to the app and is instance

Service.endpoint :

- Allow a **Subnet** in a vnet to **connect to a service** in your subscription but thought public Adresses and optimized route(Azure backbone)
- Service endpoint **enable endpoint** for **all the service, all the storage account**
- Service endpoint **work only on the particular subnet**
- **vnet peered** or **on premise** network **Will not connect trought it** (but you csn use a app getaway in the vnet with the serv endpoint to make it work)

Private link endpoint :

- create a **private ip** in a **subnet** in vnet of your subscription referancing the paas s ervice (sa, web app, database..)
- Private endoint **enable endpoint** for **a particular storage account** and a **particular service** (blob file)for the private endpoint
- Other **vnet peering**, **vnetvnet** or **one premise** can **then acces the service** targeti ng the **private endpoint ip**

Private link service :

- **Private link service** create in a **standard load balancer** behind app **for create a private endpoint** on a **other subscription/Tennant** vnet Usefull if you cant peer the vnet if overlapsin g so you can't juse connect to the private endpoint of the peered network

Service tag :

- Service tag **allow nsg** for allow internet access for **particular Azure service** For exemple if your nsg is prevented to acces internet by nsg you can use service tag for allow in the nsg the vm to access a particule public Azure service (sa database paas) Service tags group the public ip of Azure service

- **SLA**
  - **Deploy 2 or mor instance of VM behind availability zone assure SLA of 99.99% Deploy 2 or mor instance of VM whith avaiblityset assure SLA of 99.95% for the service**
  - **Single VM SLA :**
    - **Virtual Machine using Premium SSD 99,9 %**
    - **Virtual Machine using Standard SSD Managed Disks for Operating System Disk and Data Disks 99.5%**
    - **Virtual Machine using Standard HDD Managed Disks for Operating System Disks and Data Disks 95%.**

Lifecycle management feature

- Available in all Azure regions for
  - **General Purpose v2** (**GPv2**) **accounts**,
  - **blob storage accounts**,
  - **Premium Block Blob storage accounts**
  - **Azure Data Lake Storage Gen2 accounts**
- **Not General Purpose (GPv1)** you can upgrade to Gpv1 to Gp2

Azure Cosmos DB Container and partition key's container
Azure SQL pool, instance

- https://www.examtopics.com/exams/microsoft/az-303/view/53/

53

PAGE /33/34/37/38 LAB

Pratict Test 1

- Q 11,17,29,37,49,56 OK

Pratict Test 2