https://github.com/MicrosoftDocs/azure-docs/tree/master/articles
AZ 104 cours (backup vault , service ,storage etc)

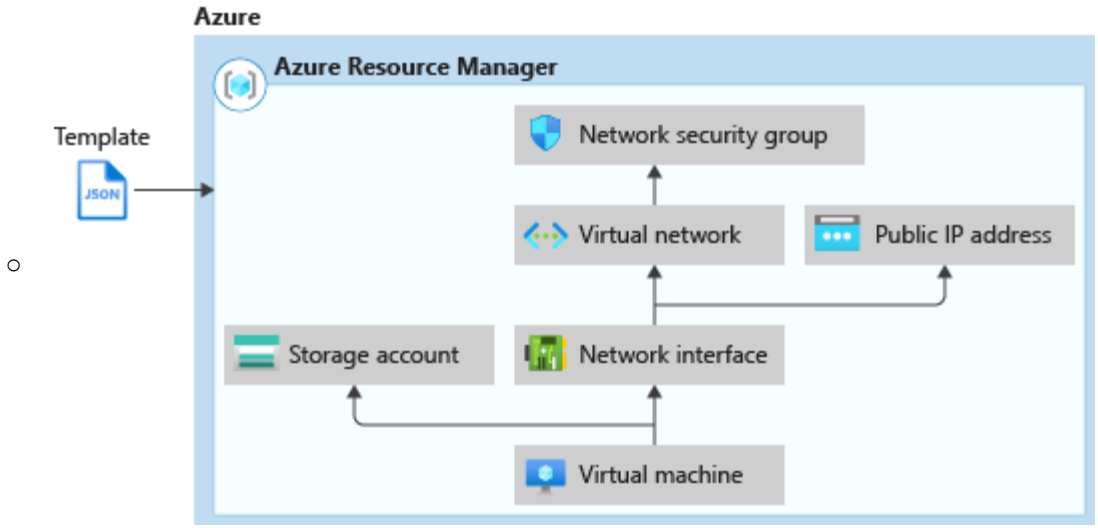
Template :

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

- The template has the **following sections**:
-
    - **$schema** : **Required -** Location of the JavaScript Object Notation (JSON) schema file that describes the version of the template language.
    - **ContentVersion Required -** Version of the template (such as 1.0.0.0). You can provide any value for this element.
    - **ApiProfile -** An API version that serves as a collection of API versions for resource types
    - **Parameters** - Provide values during deployment that allow the same templat e to be used with different environments.
    - **Variables** - Define values that are reused in your templates. They can be cons tructed from parameter values.
    - **Functions - User-defined functions** - Create customized functions that simplify your template.
    - **Resources – Required** Specify the resources to deploy.
    - **Outputs** - Returned values from the deployed resources.

#memotechnique sca pv fro

- **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**

Plan :

	Free	Basic	P1	P2	O365
Group-basedaccess managment		✖	✖	✖	✖
SSPR Cloud		✖	✖	✖	✖
Customizaion logon/ Access Panel		✖	✖	✖	✖
publicSLA		✖	✖	✖	✖
MFA	✖	✖	✖	✖	✖
Custom greetings for phone calls , Trusted Ips, Fraud alert			✖	✖	
SSPR /Unlock One premise password writeback			✖	✖	
Azure AD Sync			✖	✖	
Conditionnal access			✖	✖	
Identyti protection				✖	
Priviled Identity management				✖	

MFA and SSPR AUTH METHODE :

	SSPR	MFA
Authenticator App (Both)	×	×
SMS (Both)(Mobile phone)	×	×
Voice call (Both) (Mobile phone)	×	×
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*

Custom Voice message :

- **use your own message greetings** rather than the **default Microsoft provided message**
- **P1, P2**
- Steps:
  - **Azure Active Directory > Security > MFA > Phone call settings.**
  - **Select Add greeting.**
  - Choose the Type of greeting, such as Greeting (standard) or Authentication successful.
  - Select the Language, based on the previous section on custom message language behavior.
  - Browse for and select an .mp3 or .wav sound file to upload.
  - When ready, select Add, then Save.

MFA :

- **Trusted IPs** :
  - **P1, P2**
  - **Feature** of Azure **MFA that bypasses**
    MFA for users who **sign in** from sepcial **addresse range** and **IP** (**the company intranet, one premise**)

- **One-time bypass**
  - The one-time bypass feature allows a user to **authenticate a single time without performing two-step verification.** As an example, if a **user lost their phone**, they could not complete the two-step verification.

- **Fraud Alert :**
  - The fraud alert feature lets users report fraudulent attempts to access their r esources. When an unknown and suspicious MFA prompt is received, users can report the fraud attempt using the Microsoft Authenticator app or through their phone.
  - fraud alert configuration options are available:
    - **Automatically block users who report fraud**
    - **Code to report fraud during initial greeting**: When users receive a phone call to perform multi-factor authentication, they normally press **#** to confirm their sign -in. To report fraud, the user enters a code before pressing **#**. This code is **0** by default,

- **Remember Multi-factor Authentication**:
  - Allow to **Remembers the device**.
  - Azure Active Directory > Users and groups > All users -> MFA -> Service settings

- **Caching rules**
  - You can set a time period to allow **authentication attempts** after a user is authenticated by using the caching feature
  - It's not intended for Azure AD but on-premises.
  - Set-up: Azure Active Directory > MFA > Caching rules

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

Password writeback in SSPR :

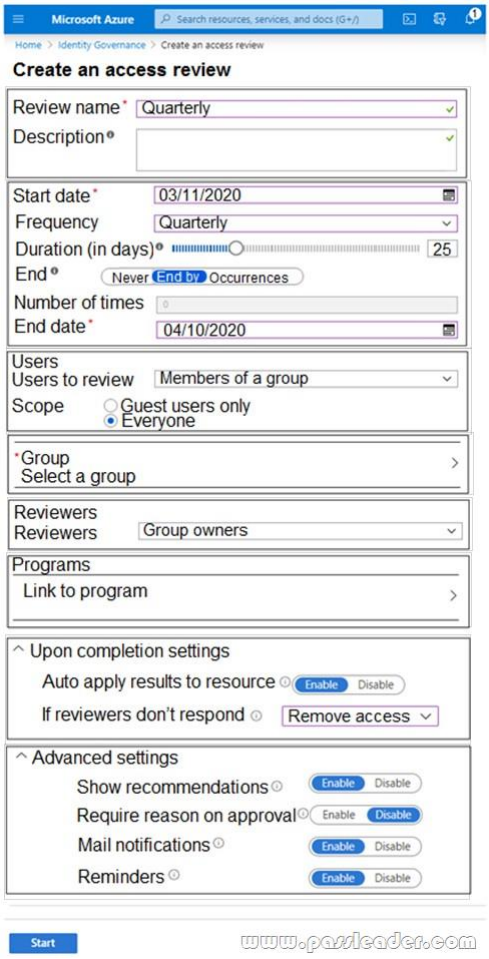
To enable password writeback in SSPR, complete the following steps:

- 1 Sign in to the Azure portal using a global administrator account.

- 2 Search for and select Azure Active Directory,
  select Password reset, then choose On-premises integration.
- 3 **Set the option for Write back passwords to your on-premises directory? to Yes.**
- 4 **Set the option**
  for Allow users to unlock accounts without resetting their password? to Yes.

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** :

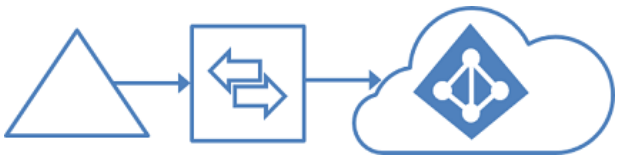
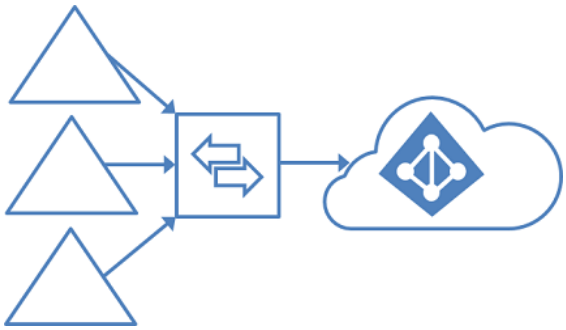
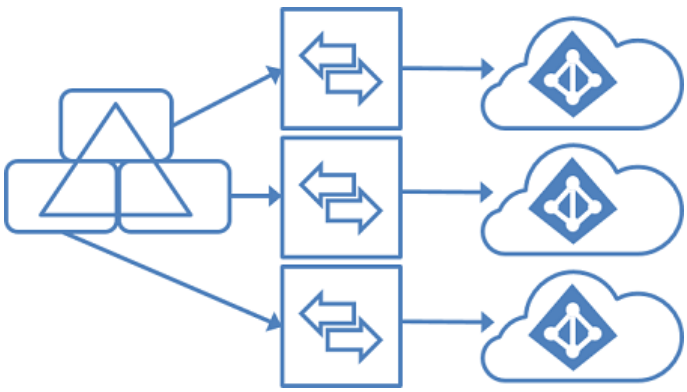


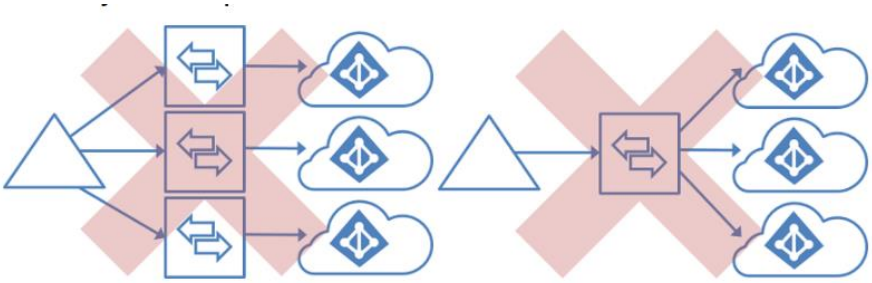
- Area 1:
  - The access review must be enforced until otherwise configured. We set **End**: **Never**.
  - The access review must be completed within two weeks. We set **Duration** (in days) to **14**.
- Area 2:
  - A lack of response must not cause changes in the operational environment. We set **If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

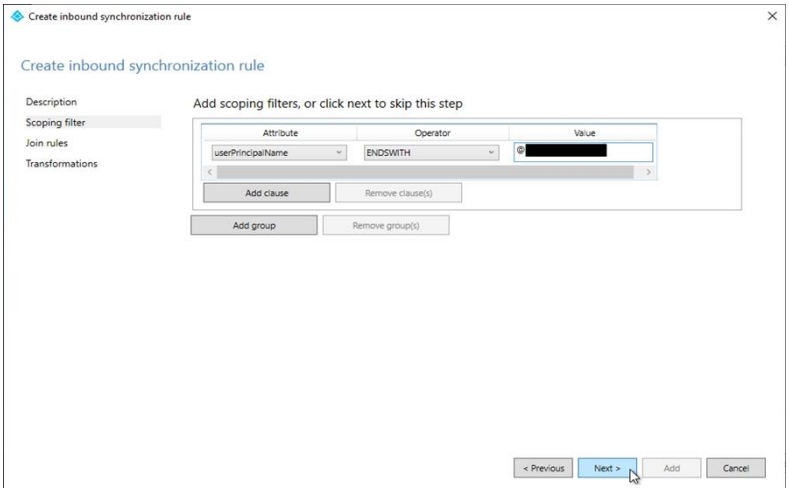
B2B users (Guest)

- **Contitional acces policy can** be aplied to guest users
- **The recommendation** for MFA for B2B users is to **always require MFA in the inviting tenant**
- **Risk-based sign-in policies cannot be applied** to **B2B users because** the risk evaluation is performed at the B2B user's home organization.
- **Guest MFA options Company responsiblility** :
    - The **inviting tenancy** is **always responsible** for **MFA** for guest user , **even if the partner organization has MFA capabilities.**
    - **The user will have to set up the mfa options from the inviting company loggin in to the inviting Azure AD**

AD Connect :

- There's a **1:1 relationship** between an **Azure AD Connect** sync server and an **Azure AD tenant**. For each Azure AD tenant, you need one Azure AD Connect sync server installation.
- Topology allowed :
    - Each object only once in an Azure AD tenant
    - 
    - 
    - The Azure AD Connect sync servers must be configured for filtering so that **each has a mutually exclusive set of objects to operate on**. You can, for example, scope each server to a **particular domain** or **organizational unit.**
    - 

-
- **Unsuported Topology** :
    - Sync the same user to multiple Azure AD tenants.
    - Make a configuration change so that users in one Azure AD tenant appear as contacts in another Azure AD tenant.
    - Modify Azure AD Connect sync to connect to multiple Azure AD tenants.
-
    - 
- If you want to add a user that is alreay synced to a tenant to a other tenant, then you should invite this user as a guest user in the tenant you can sync the same user in 2 different tenant
- *(Voir : https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies)*
- **Role for Sync**
    - 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**)
        - *https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#attribute-based-filtering*
        -



- **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 (if You must ensure that **users use their on-premise credentials** to sign-in you can use these 3 methode) :

- **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.

AD Sync User :

- You **must** use **Windows Server Active Directory** to **update** the **identity, contact info**, or **job info** for users whose **source of authority is Windows Server Active Directory**
- these property **can't be modified** from the **Azure portal** for **AD synced user**
- **you can** change the **usage location** of **any user** from **Azure AD portal** for assiged licence for exemple

Custom domain name Azure AD

- If you want add a custom domain to Azure AD
- 1 : Add Custom domaine to Azure AD
- 2 : Add a record (TXT or MX) to the registrar / public DNS Zone
- 3 : Verify the domain
- **If the verification is failing.Wait at least an hour and try again. DNS records must propagate before Azure AD can verify the domain. This process can take an hour or more.**
- **Add subdomains of a custom domain**
  - If you want to **add a subdomain name** such as '**europe.contoso.com**' to your organization, you should **first add and verify the root domain, such as contoso.com.**

- **The subdomain** is **automatically verified by Azure AD**.
  To see that the subdomain you added is verified, **refresh the domain list in the browser**.

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 :

Seamless SSO :

automatically signs users in when they are on their corporate devices connected to your corporate network.

- **Need**
  - **domain-joined (one prem)**
    - the **user's device** to be **domain-joined (one prem)** , but it is not used on Windows 10 Azure AD joined devices or hybrid Azure AD joined devices

PRT SSO :

- Need :
  - **Registred** PRT SSO
  - **Azure ADJoined-device** PRT SSO
  - **Hybrid joined** PRT SSO

- **Security Role Azure AD**
  - **Security Administrator**
    - Can read security information and reports, and manage configuration in Azure AD and Office 365.
    - **Full access to identity protection**
  - **Security Operator**
    - Creates and manages security events.
    - **View all identity Protection** reports and overview blade
    - **Dismiss user risk, confirm safe sign-in, confirm compromise**
  - **Security Reader**

- Can **read security information** and reports in Azure AD and Office 365.
- **View all identity protection reports and overview blade**

Manage action Group

- **Voice**
- **SMS**
- **Email**
    - **Alert limit**
        - **SMS: No more than 1 SMS every 5 minutes.**
        - **Voice: No more than 1 Voice call every 5 minutes.**
        - **Email: No more than 100 emails in an hour.**

- **Azure app Push Notifications**
- **Function**
    - Call a Azure function
    - Calls an existing HTTP trigger endpoint in Azure Functions.
      To handle a request, your endpoint must handle the HTTP POST verb.
    - When defining the Function action
      the the Function's httptrigger endpoint and access key are saved in the action definition.
      For example: https://azfunctionurl.azurewebsites.net/api/httptrigger?code=this_is_access_key. If you change the access key for
      the function you will need to remove and recreate the Function action in the Action Group.
    - **code / Logic App use workflow**
    - Azure Functions, you can use the
      full expressiveness of **a programming language** in a compact form.
      This lets you concisely **build complex algorithms**, or
      data lookup and parsing operations.
    - **Azure function Plan**:

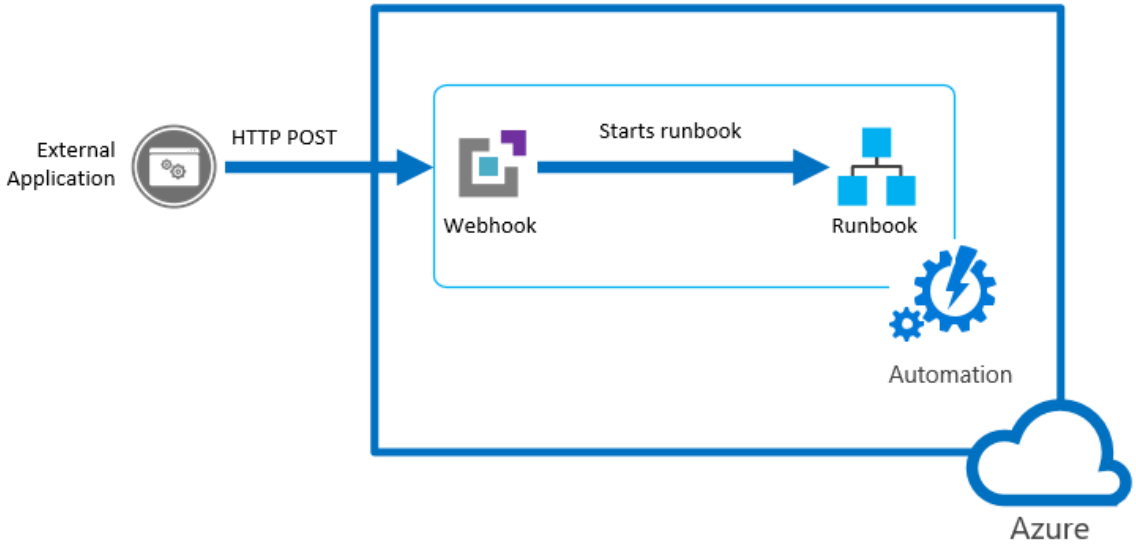
        - **Consumption plan**
            - Scale **automatically /dynamcialyt** and **only pay** for compute resources **when your functions are running**.
        - **Premium plan**
            - **Automatically scale**s based on demand using pre-warmed workers which run
              applications with no delay after being idle, runs on
              more powerful instances, and connects to virtual networks.
        - **Dedicated plan**
            - ✔ You
              have existing, underutilized VMs that are already running ot her App Service instances.

✔ You want to provide a custom image on which to run your functions.

✔ Predictive scaling and costs are required.

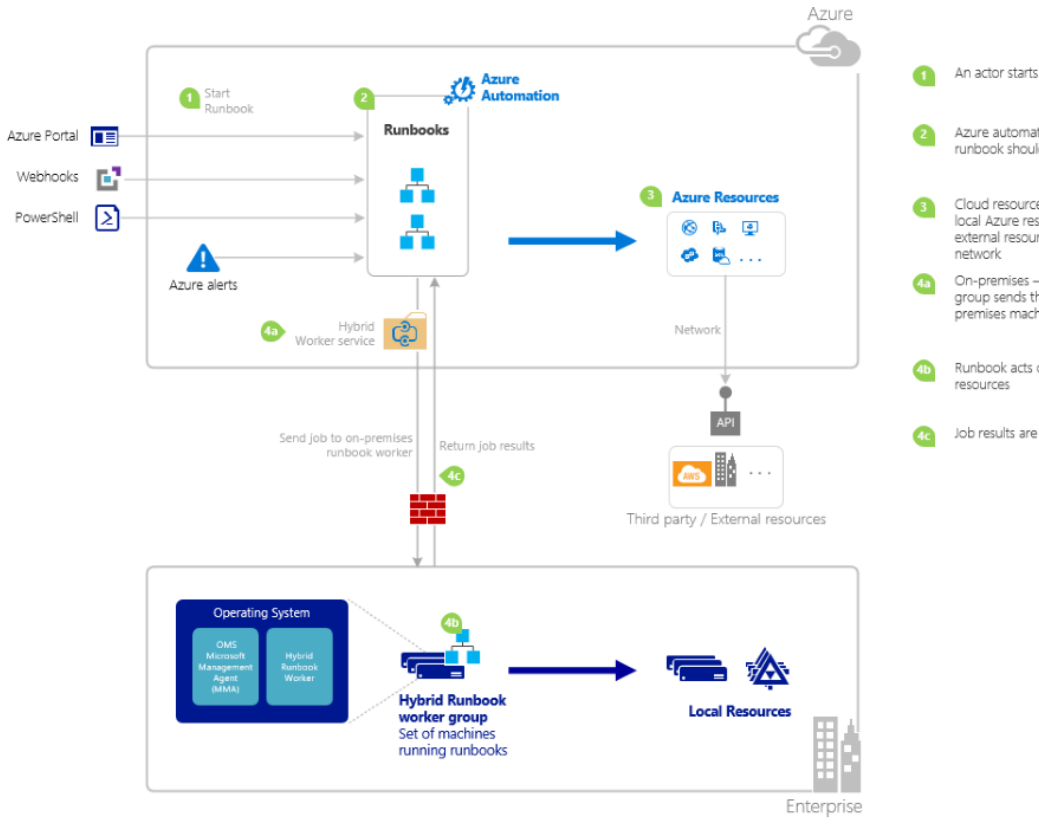
- **Logic App**
  - Cloud service the help you shcedule automate en orchestrate task, buissnesse processe, and **workflow**
  - On peut choisir dans une gallery de **pre-build connector**
  - Logic Apps excels at **connecting** a large array of disparate services via their APIs to pass and process data through many steps in a **workflow.**
  - **Can use a event grid to push event form Activity logs to triggere the logic App**
    - **Azure Event Grid trigger**
    - **A conditionnal control**
      - **to filter on the events**
    - **An action**
      - **to send the notification.**

- **Webhook** :
  - **URI**
  - A webhook allows an external service to start a particular runbook in Azure Automation through a single **HTTP request**. External services include Azure DevOps Services, GitHub, Azure Monitor logs, and custom applications.
  - Webhooks are simple HTTP callbacks used to provide event notifications. Azure Logic Apps and Power Automate both allow you to use webhooks as triggers.
  - Such a service can use a webhook to start a runbook without implementing the full Azure Automation API.



- **Secure Webhook (call of a web API Protected registred in Azure AD for protection)**
  - Action Groups Secure Webhook action enables you to take advantage of **Azure Active Directory**

to secure the connection between your action group and your protected web API (webhook endpoint).

- 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**
  - **Deploy an Azure Resource Manager template in a PowerShell runbook (flow):**
    - **Create** the Resource **Manager template**
    - **Save** the **Resource Manager template in Azure Storage (Central location)**
    - **Create** the **PowerShell runbook script**
    - **Import and publish the runbook** into your **Azure Automation account**
    - **Start** the runbook
  - 

Cost management

- **Budget** :
  - When your consumption reaches a given threshold, alerts are generated by C ost Management. There are three types

of **cost alerts**: **budget alerts**, **credit alerts**,
and department spending quota alerts.

- **Export report:**
  - You
    can create a recurring task that **automatically exports** your **Cost Manageme nt data** to Azure storage on a **daily, weekly, or monthly basis.**
    - **1 Creat a export in cost analysis**
    - **2 Configure export type as weekly**

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
- **Avset Sku** :
  - **• Aligned: For managed disks**
  - **• Classic: For unmanaged disks**

Azure monitor

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

- **Azure Dashboard**
  - Supports both metrics and logs.
  - Option
    for **personal** or **shared dashboards.** Integrated with Azure role based authen tication **(RBAC).**
  - **Automatic refresh and on demand.** Metrics refresh depends on time range with minimum of five minutes. Logs refresh every hour.

- **App insinght**
  Monitor App service
- **Container insight**
  - **Monitor the performance** of **container workloads**
  - Container insights uses a containerized version of the Log Analytics agent for Linux

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 issues on the virtual machine** like **Network Trace** . This extension installs a troubleshooting tool called PerfInsights.

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

- You can deploy the **Microsoft Monitoring agent** on **one prem VM** .
- Then you can change the **Data collection settings for your Log Analytics workspace** so that you **can send the data from the virtual machines to the workspace.**

Linux Diagnostic Extension (LAD) 3.0

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

Log analytic

- Data source :
  - For linux configure **Syslog data source** in the workspace (**Syslog** is an event logging protocol **common to Linux**)
- **Log analytic worksapce** :
  - **Capacity reservation tiers**
    - enable you to **save as much as 25%** compared to the Pay-As-You-Go price.
      The capacity reservation pricing enables you **to buy a reserv ation starting at 100 GB/day.**

Azure Monitor Logs for Service Providers

Architectures for Service Providers :

1. Distributed - Logs are stored in workspaces located in the customer's tenant

- A customer can add individual users from the service provider as **Azure Active Directory guest users (B2B).**
- For greater scalability and flexibility, service providers can use **Azure Lighthouse** to access the customer's tenant.

2. Central - Logs are stored in a workspace located in the service provider tenant

- The advantages of the centralized architecture are:
  - It is easy to manage a large number of customers and integrate them to various backend systems.
  - The service provider has full ownership over the logs and the various artifacts such as functions and saved queries.
  - The service provider **can perform analytics across all of its customers.**

- The disadvantages of the centralized architecture are:
    - This architecture is applicable only for agent-based VM data, it will **not cover PaaS, SaaS and Azure fabric data sources.**
    - It **might be hard to separate the data between the customers when they are merged into a single workspace**

3. Hybrid - Logs are stored in workspace located in the customer's tenant and some of them are pulled to a central location.

- mix between the two options. It is based on the first distributed architecture where the logs are local to each customer but using some mechanism to create a central repository of logs. A portion of the logs is pulled into a central location for reporting and analytics. This portion could be small number of data types or a summary of the activity such as daily statistics.
- here are two options to implement logs in a central location:
    - Central workspace: The service provider can create a workspace in its tenant and use a script that utilizes the **Query API** with the **Data Collection API** to bring the data from the various workspaces to this central location. Another option, other than a script, is to use **Azure Logic Apps**.
    - Power BI as a central location: Power BI can act as the central location when the various workspaces export data to it using the integration between the Log Analytics workspace and Power BI.

Peering

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

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**.
- **Container takes a long time to start**:
    - Factor :
        - **Image Size**
        - **Image location**
            - host the container image in Azure Container Registry in the same region where you intend to deploy contain er instances. This shortens the network path that the container image needs to travel, significantly shortening the download time.

Azure Container Registry

- **Store** 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 :

- Use **File** or **Disk Storage**

- **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**

- **Manifest files (yaml) :**

- **auto scale** based on **CPU utilization** :
  - apiVersion: autoscaling/v1
  - kind: HorizontalPodAutoscaler
  - metadata:
  - name: azure-app-front-hpa
  - spec:
  - **maxReplicas: 15** # define max replica count
  - **minReplicas: 3** # define min replica count
  - scaleTargetRef:
  - apiVersion: apps/v1
  - kind: Deployment
  - name: azure-app-front
  - **targetCPUUtilizationPercentage: 50** # target CPU utilization

- AKS uses the following rules to **determine if automatic repair is needed.**
  - **The node doesn't report a status within 10 minutes**
  - **The node reports status of NotReady on consecutive checks**

App Service Plan

- Create and configure App Service plan
  - Choose between Linux and Windows OS
  - App service plan are assiocied to one ore more App service
  - Auto scale and backup start to Standard plan minimum
  - Standard instance max : **10**
  - Premium v2 instance max **20**,
  - Premium v3 : instance max 30
  - **The Standard** service plan is designed for running **production workloads**
  - The app must be running in the **Standard**, Premium, or Isolated tier in order for you to enable multiple **deployment slots** and **Backup , Autoscale, VNet Integration**. Free and Shared Basic are out
  - The app must running in **Basic,**Standard premium or isolated to **be Alway on and use HTTPS (TLS/SSL binding)**. Free and Shared are out (DB).
  - The app must be running in **Shared**,Basic Strandard premium isolated for **CustomDomain**. Free is out
  - F = gratuit , D = shared

App service

- **Configure user access athentification** for **App Service or Azure function with** Azure AD Step:
  - 1- Seletc an **Identity provider** (Micrsft Azure AD, facebook, google)
  - **2- Register** the App in Azure AD
  - 3- Select App service **authentication setting**

  - Select **Account type Options** :

- **Accounts in this organizational directory (Az AD tenant) only**
    - **Azure AD only single-tenant.**
    - Select this option if you're building a line-of-business (LOB) application
    - This option **maps to Azure AD only single-tenant.**

- **Accounts in any organizational directory (Az AD tenant)**
    - **Azure AD only multi-tenant**
    - **Select this option if you would like to target all business and customers. This option maps to an Azure AD only multi-tenant.**

- **Accounts in any organizational directory (Az AD tenant) and personal Microsoft accounts**
    - Select this option to **target the widest set of customers.**
    - **Azure AD multi-tenant and personal Microsoft accounts.**

- 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)
- Configure **Access restriction** :
    - enable you to define a priority ordered allow/deny list that controls network access to your app.
    - **Ip restriction**
    - The list can include **IP addresses or Azure Virtual Network subnets.**
    - When there are one or more entries, there is then an implicit "deny all" that exists at the end of the list.

- **Autoscale :**

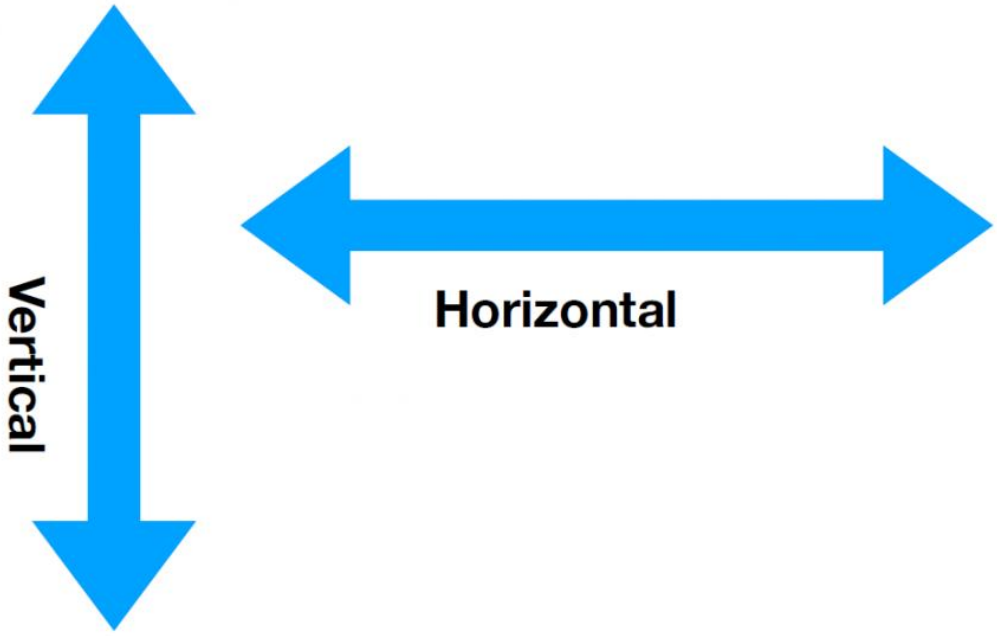
    - **Scale out -> occur if ANY condition is met ->**
    - **Scale in <- occur ONLY IF ALL condition are met**

    - **If the scal in would go under the minimum number of VM the scal in dont occure**
    - **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:
    - 3x**60** = 180 / **2** = 90.0% (>80%, no scale in occurs)
    - 3x**55** = 165 / **2** = 82.5% (>80%, no scale in occurs)
    - 3x**50** = 150 / **2** = 75.0% (<80%, scale in)
    - 3x**45** = 135 / **2** = 67.5% (<80%, scale in)
- The **estimated number of cpu after scal in** must **not triggere** the **scale o ut treshold** , if then the scale in will not occur

- **Autoscale logs** :
    - All **autoscale failures** are logged to the **Activity Log**. You can then configure an **activity log alert** so that you can be notified via email, SMS, or webhooks whenever there is an **autoscale failure.**



Azure Instance Metadata Service MDS

- is a **REST API provides 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)**

Azure Migrate :

Discover -> Assess-> Migrate

- You can create two types of assessments by using **Azure Migrate Server Assessment**:

Assessment	Details	Data
Performance-based	Assessments based on collected performance data	Recommended VM size: Based on CPU and memory utilization data. Recommended disk type (standard or premium managed disk): Based on the IOPS and throughput of the on-premises disks.
As on-premises	Assessments based on on-premises sizing	Recommended VM size: Based on the on-premises VM size. Recommended disk type: Based on the storage type setting that you select for the assessment.

-
- **Assesseemnt Type:**
  - **Servers:**
    - **Assess on-premises servers** and migrate them **to Azure virtual machines.**
  - **Databases**:

        - **Assess on-premises databases** and migrate them to **Azure SQL Database or** to **SQL Managed Instance.**
    - **Web applications:**
        - **Assess on-premises web applications** and migrate them to **Azure App Service** by using the **Azure App Service Migration Assistant**.
        - **App service** :
            - **custom Windows containe**r
                - lets you make OS changes that your app needs, so it's easy to **migr ate on-premises app that requires custom OS** and **software configuration.**
    - **Virtual desktops:**
        - **Assess your on-premises virtual desktop infrastructure (VDI)** and migrate it **to Windows Virtual Desktop in Azure**.
    - **Data**:
        - **Migrate large amounts of data** to Azure quickly and cost-effectively using **Azure Data Box products.**

- **Azure Migrate projects**
    - - Each **project** can **assess up** to **35,000 VMs in a project.**
- **Azure Migrate appliance**
    - - Following are the **limitations for each appliance.**
        - **An appliance** can only be **associated with a single Azure Migrate project.**
        - **Any number of appliances** can be associated with a **single Azure Migrate project.**

    - **Vmware**
        - **An appliance** can connect **to** a **single vCenter Server.**
        - **An appliance** can **discover up to 10,000 servers** running on **a vCenter Server.**
        - **Supported deployment :**
            - **OVA template.**
            - Deploy on an existing server running Windows Server 2016 using **PowerShell installer script.**
    - **HyperV**
        - **An appliance can connect to up to 300 Hyper-V hosts.**
        - **1 Appliance only is enough for assesse a one premise network with less than 300 hyper-v host (cluster, etc)**
        - **You will need to assign the migrate accout to the administrator group on each Hyper-v Host**
        - An appliance **can discover up to 5000 VMs running in Hyper-V environnment .**
        - **Supported deployment :**
            - **VHD template.**
            - Deploy on an existing server running **Windows Server 2016** using **PowerShell installer script**.
    - **Physical**
        - **An appliance** can discover up to **1000 physical servers.**
        - **Supported deployment**

- Deploy on an existing server running Windows Server 2016 using **PowerShell installer script.**

Database Migration :

- **Azure Database Migration Service**
  - Its is a fully managed service designed to enable seamless **migrations from multiple database sources to Azure** data platforms with **minimal downtime**

- **Data Migration Assistant**
  - helps **pinpoint potential problems blocking migration.** It **identifies unsupported features,** new features that can benefit you after migration, and the right path for database migration.

- **To assess on-premises VMware virtual machines (VMs), using the Azure Migrate: Server Assessment tool**
  - · **Create an Azure Migrate project**
  - · **Set up the Azure Migrate appliance**
  - · **Verify appliance access to Azure**
  - · **Set up an assessment**
  - · **Run an assessmen**t
  - · **Review the assessment outcome**

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"

Replicate VM to Azure

- **Replicate One premise Hyper-V VM to Azure**
- **After the Dicvovery and the Assessemtn, The Azure Migrate solution will install the Azure Recovery Services agent on each Hyper-V hots or cluster node.**
- **Ex : if you have 2 clustur of 4 node the recovery service agent will be installed and configured one the 8 machine**
-

- **(difference then Azure migrate that need only 1 appliacne for 300 host or cluster node)**
-
    - **Recovery Services vaults**
        - **Site Recovery**
        - Select one premise location -> Hyper-v
        - Create **Hyper-V Site**
        - **Add hyper-v server Step**
            - **1- Dowload** the **Microsoft Azure Site Recovery Provider** software
            - **2- Dowlorad** the **vault registration key**
            - **3 - Install it** on **each Hyper-v host (not on the VM)**
        - Select the target Env (RG)
        - Set up the **Replication policy** (copy frequency , retention point)
    - **Recovery Service Vault Role**
        - **Site Recovery Contributor**
            - permissions required to **manage Azure Site Recovery operations in a Recovery Services vault**
        - **Site Recovery Operator role!**
            - permissions to execute and **manage Failover and Failback operations.** A user with this role **can't enable or disable replication, create or delete vaults,**

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.f**

Azure Queue :

-

Azure Service Bus

- **queues :**
    - Is **FIFO** first in first Out
    - **Authorization** :
        - **AAD**
        - **SAS**
- **Topics**
    - **Multiple subscriber (consumer) can receive the message**
    - **App send message to topic, and subcribers (app) subscrip to the topic**
    - **A message send to a topic will be available to all subcribers**

Azrue Table Storage :

- **Table Storage**
- **Stocker Structuré**
- **NoSQL data**
- **Gpv1 , Gpv2**
- **Key : value paire**
-
- **Design your Table service solution to be read-efficient**
    - **Design for querying in read-heavy applications**. When you are designing your tables, think about the queries (especially the latency sensitive ones) that you will execute befor e you think about how you will update your entities. This typically results in an efficient and performant solution.
    - **Specify both PartitionKey and RowKey in your queries**.
    - Point queries such as these are the most efficient table service queries.

        - **Partitionkey** (like in cosmos DB)
            - Used to **define the partition** to store the entitites (all **member of a partition have the same value for the partion key** (classer les entité))
        - **Rowkey**
            - Help to uniquly identify an entity in the partition (**unique for each entity** like **primary key in SQL**)

    - **Consider storing duplicate copies of entities.** Table storage is cheap so consider storing the same entity multipl e times (with different keys) to enable more efficient queries.
    - **Consider denormalizing your data**. Table storage is cheap so consider denor malizing your data. For example, store summary entities so that queries for aggregate data only need to acces s a single entity.
    - **Use compound key values.** The only keys you have are PartitionKey and RowKey. For example, use compound key values to enable alternate keyed access paths to entities.
    - Use query projection. You can reduce the amount of data that you transfer over the network by using queries that select just the fields you need.

- **Design your Table service solution to be write-efficient**
    - **Do not create hot partitions.** Choose keys that enable you to spread your requests across multiple partitions at any point of time.
    - **Avoid spikes in traffic**. Smooth the traffic over a reasonable period of time and avoid spikes in traffic.
    - **Don't necessarily create a separate table for each type of entity**. When you require atomic transactions across entity types, you can store these multiple entity types in the same partition in the same table.

- **Consider the maximum throughput you must achieve.** You must be aware of the scalability targets for the Table service and ensure that your design will not cause you to exceed them.

Azure Cosmos DB :

- **Low reponse latency partout dans le monde**
- **API Intégrer**
- **Scalble**
- **ifuser in multiple country**
- **No SQL**

- **Azure Cosmis DB Creation**
  - You choose the API in the creation of the Azure Cosmos DB
  - Geo-redundancy (Enable/Disable)
  - Multi-regionwrite (Enable/Disbale)
- **Container** ;
  - Container are part of a database
  - When you create a conainrer you choose the Database or you create a new one
  - You choose then the name of the container
  - Choose th partion keys
- **Partition Keys**:
  - When you create container (DB) your specify the partion key
  - your data will be group depend of their partion keys
    (exmeple : **customer_name** , **city**)
    - For each customer with the same **name** a partion is created gro uping these user logicaly et physacaly
    - For each customer with the same **city** a partion is created grouin g these user logicaly et physacaly
    -
    - This feature allow to quilcky research in partion who have user with the same partion key
      to query efficiently withour search in the
      all db because they are physiclay grouped in partiotion

- If You plan to **change** the **partition key** for a **container** in a CosmosDB account you need to do first :
  - **Create a new Container in the DB**

  (it is **not possible to "update"** your **partition key** in an **existing container**.
  So, **create new container** with new partition key and **move the data from old container and then delete the old container.**)

- Cosmso DB API (SQL API)
  - Database (appDb)
    - Container (customer)
      - Item (who have a Partition keys (\customername))
-
- **Azure Cosmos DB** currently provides the **following APIs** :

	Core (SQL)	MongoDB	Cassandra	Table Azure	Gremlin
Nouveaux projets en cours créés à partir de zéro	✓				
Données existantes MongoDB, Cassandra, Table Azure ou Gremlin		✓	✓	✓	✓
Analyse des relations entre les données					✓
Tous les autres scénarios	✓				

- **Core (SQL) API**
  - for **JSON document** data.
  - , flexible
  - Can use **SQL command**
  - **For new project without already a DB**
- **MongoDB API**
  - for **JSON document** data.
  - If user **alreay use MongoDB one prem**
- **Cassandra** for a columnar or column-family datastore.
  - **CQL queries** (Cassandra Query Language)
  - Appache
- **Azure Table**
  - API for **key-value pair** datastore.
  - Azure table existante
- **Gremlin**
  - **(graph) API for graph data.**
  - Le format graph permet d'**analyser la relation entre les données**
  - Mettre en place une certaine forme de prévention et de détection des fraudes. Tout ce qui ne relève pas d'un comportement normal devrait être marqué

- **Cosmos DB config** :
  - ## Replicate data globaly pane :
    - You can **chose other region** where the data will be **replicated** in a **readable state**
    - You can enable **multiple-region write** so you can **write too** on the **replicated region**
    - You can **manualy and automaticlay failover**
    - **multiple-write** is available on account level not on Database level so if you have **differnt write setting (multple write region / on ly one write region)** you should create 2 **different Cosmos DB account** .
    - Microsot recommand using **one API** for **each Cosmos DB account**
    - **Configure multi-region writes** in your applications that use Azure Cosmos DB
      - Once an account has been created with multiple write regions enabled, you mu st make two changes in your application to

the ConnectionPolicy for the Cosmos client to enable the multi-region writes in Azure Cosmos DB

- **set UseMultipleWriteLocations to true**
- **pass the name of the region where the application is deployed to SetCurrentLocation.**

- **NoSQL databases consistency level**
  - ***Strong***
    - Strong consistency offers a linearizability guarantee . Linearizability refers to serving requests concurrently. The **reads are guaranteed** to return the most recent committed version of an item. **A client never sees** an **uncommitted** or **partial writ e.** Users are always **guaranteed to read the latest committed write.**
    - **Get consitensty but loose one performance because you have to wait all data are replicated before you can read so more late ncy**

  - ***Eventual***
    - Eventual consistency is the weakest form of consistency because a client may read the values that are older than the ones it had read before. Eventual consistency is ideal where the application **does not require any ordering guarantees**. **Examples include count of Retweets, Likes, or non-threaded comments**
    - **social networking database**
    - **Win on performance but loose on consistency**
  -
  - **Session**
    - Session is the best consistency setting for user data that contains **shopping basket information**. Session consistency will ensure that every **item the user put in their basket is displayed** when they review their basket.

  - ***Bounded staleness***
    - frequently chosen by globally distributed applications that expect low write latencies but require total

global order guarantee. Bounded staleness is great for applications featuring group collaboration and sharing, stock ticker, publish-subscribe/queuein

- **Beetween the strong and eventual consisenty (y ou have a defined lag**
  time allowed difference beetween primary regio n and secondary)

- **Consistent prefix**
  - ***Order***
  - *Always see in secondary the* ***most recent data*** *but the older but the* ***older are delayed***
  - **You loose on consistency**
  -

-

Azure Managed instance (MI) :

- **SQL managed Instance**
- **Cloud DDB service**
- **Combine les bénéfices de la compatibilité avec SQL Server Database avec les bénéfices du PaaS**
- **Recomander Dans la situation ou l'ont veut migrer un BD one-premise en gardant toute les fonctionaliter de SQL server**
- SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance preserves all
  PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO.
- **Fonctionnalité**
  - **Database Mail** :
    - **Solution for sending** e-mail **messages** from the **SQL Server Database Engine or Azure SQL Managed Instance.**
  - **Linked servers**
    - enable the SQL Server Database Engine and Azure SQL Managed Instance to read data from the remote data sources
      and execute commands against the remote database servers
-
- **In a Subnet VNET and have a IP adresse (delegated subnet like VnetGateway or Bastion)**
- **Advanced data security feature**
  - Advanced Threat Protection for an Azure SQL Managed Instance **detects anomalous activities** indicating **unusual and potentially harmful attempts** to **access or exploit databases.**

Azure SQL Server :

- **Paas DDB**

- **Management function (upgrad, patch,backup)**
- **Cloud version of Microsoft SQL**
- **Elastic Pool**
    - **You can create Single DB alone or in a Elsatic pool sharing the same ressource.**
    - If you **add a database** one a **pool** with **more VCores than specified one the pool** the **database Vcores would decrease** to **fit the vCore capacity of the elastic pool**.
    - The storage **size would not get impacted.**

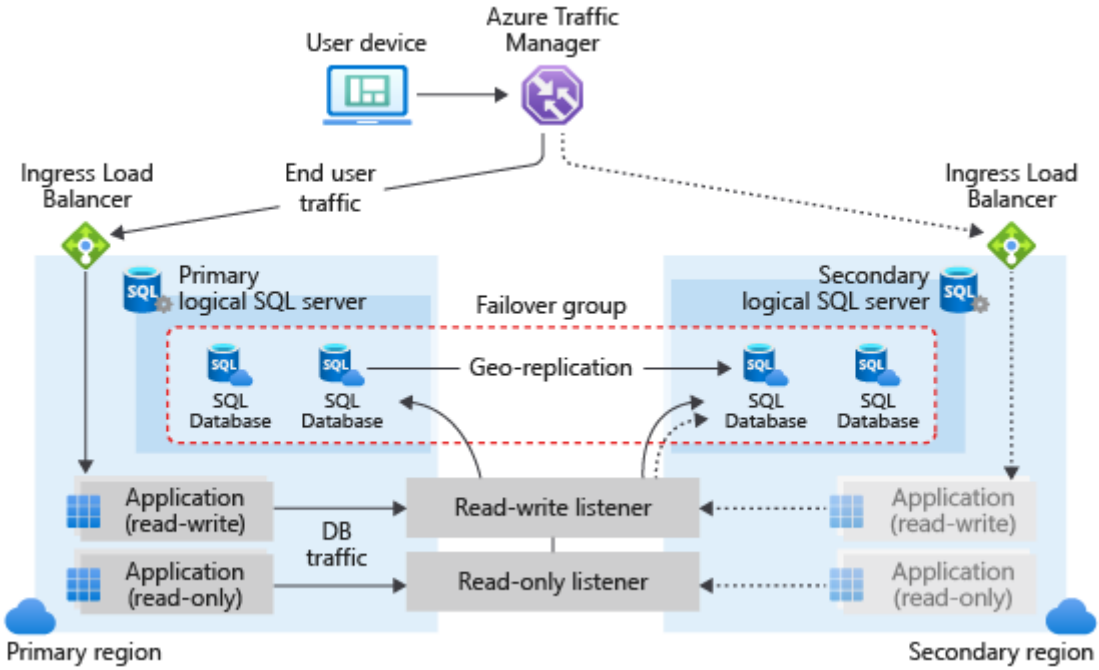
- **Moove Database**
    - You can only moove(remove and add) DB (databse) **within pool** (**elastic pool**) in the **Same SQL Server**
    - You **cant remove and add** a **DB** in a **different SQL Server** than **origine**
- **Server-side transaction Transactions acroos DB (Transaction cross multiple database)**
    - **Supported:**
        - **The Azure SQL datbase are on hte same Azure SQL Server or different Azure SQL Server (in this case you will need create link beetween server)**
        - **One Azure SQL Manage instance**
        - **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**
    - **Configure the Firewall and virtual network setting**
    - 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**

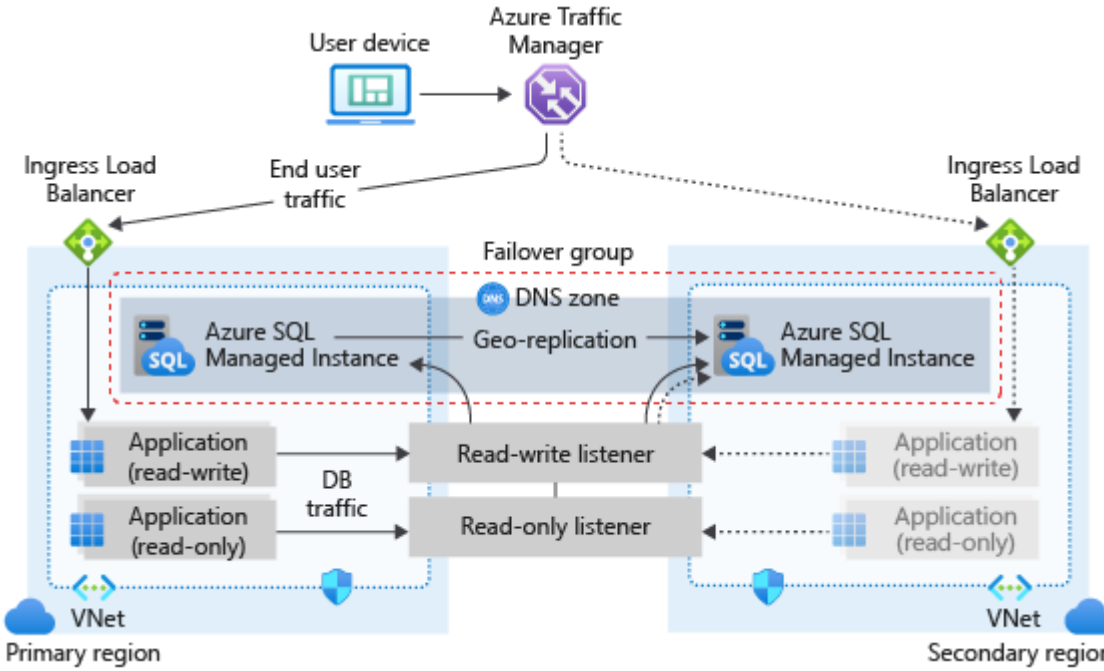
- **SQL active geo replication :**
    - **On DB level**
    - **Manually failover**
    - **Replicate readable only secondary database from a primary database**
    - **Can be one the same région or an other**
    - **The secondary db can be replicate one the same SQL server or an other**

- **Not suported in SQL Managed Instance**

- **SQL Auto Failover group** :
  - **On SQL Server Level**
  - **Replicate a groupe of DB**
  - For **Azure SQL Database and Azure SQL Managed Instance**
  - **Auto failover**
  - 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 **secondary** 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 configure** 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.

- **Always encrypted feature on Azure SQL Database**
  - Designed to **protect sensitive data stored** in specific **database columns** from access (**for example, credit card numbers, national identification numbers**,).
    This **includes database administrators or other privileged users** who are a**uthorized to access** the database to perform **management tasks**, but have **no business need to access the particular data** in the encrypted columns
  - **ensure that the external party cannot access the data in the SSN column of the Person Table.**

- **SQL Server one Azure VM** :
  - Concept of **Always On availability group :**
    -
    - Always On availability groups maximizes the availability of a set of user databases for an enterprise.
      An *availability group* supports a failover environment for a discrete set of
      user databases, known as *availability databases*, that fail over together. An availability group supports a set of read-write primary databases and one to eight sets
      of corresponding secondary databases.

- Each availability replica must reside on a different node of a single Windows Server Failover Clustering (WSFC) cluster.
- Prerequis : Both SQL Server virtual machines must **belong to the same availability set.**
- Step to create load balencer listener for the Availability group in Azure VM
    - Step 1: **Create the load balancer** and configure the IP address
    - Step 2Configure the back-end pool
        - Choose the **Avset**
    - Step 3Set the load-balancing rules
        - Protocole TCP port 1443
        - Enable **Floating IP**
    - Step 4 On the failover configuration Set the IP address listenet as the same address that you used when you set the load balancer address

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.

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.

Storage :

- In **GRS** data is copied **3 in LRS in primary** region and then **3 copy LRS** asynchronous in second region = **6 copie**
- **GZR** data is copied **3 time in ZRS primary** region and **3 copy LRS** asynchrinous in second regions = **6 copie**

Replication options

- **ZRS currently supports standard gGneral-purpose v2, FileStorage and BlockBlobStorage storage account types.**
- **You can switch a storage account from one type of replication to any other type.**
- **If you want to add or remove geo-replication or read access to the secondary region, you can use the Azure portal, PowerShell, or Azure CLI to update the replication setting.**
- **if you want to change how data is replicated in the primary region, by moving from LRS to ZRS or vice versa, then you must perform a manual migration (AzCopy)or live migration (Azure Support portal).**
- **Live migration is supported only for storage accounts that use LRS replication or GRS replications**

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

- **immutability policies for Blob storage**
    - Immutable storage for Azure Blob storage enables users to **store business-critical data** objects in a WORM (**Write Once, Read Many**) state.
    - This state makes the **data non-erasable** and **non-modifiable** for a defined **retention interval**
    - **Time based renttion policy :**
        - For the duration of the **retention interval**, blobs **can be created** and **read ,you can also change the access tier**, but **cannot be modified or deleted**.

- After the **retention interval** of the blobs has **expired**.
    - Data will continue to be in a **still non-modifiable state**,
    - **can be deleted**.

Subscription ower can't delete the time **based retention policy** once **locked**
Subcription owner can't delete the storage account that has **time based retentio policy**

- **Legal hold policy support:**
    - **Legal hold tags can be deleted**
    - If the retention interval is not known, **users can set legal holds** to store immutable data **until the legal hold is cleared**. When a legal hold policy is set, blobs **can be created** and **read ,you can also change the access tier**, but **cannot be modified or deleted**. (Like time based retention)
    -

- **User delegation SAS**
    - A SAS token for access to a container or blob may be secured by using either Azure AD credentials or an account key. A SAS secured with Azure AD credentials is called a *user delegation* SAS. Microsoft recommends that you use Azure AD credentials when possible as a security best practice, rather than using the account key, which can be more easily c ompromised

- **easy to revoke SAS**
    - **by deleting stored access policy**

        - **Storage policy** allow to **group shared access signatures wit h commun policy you can revoke group of SAS deleting the stored policy**
    - **changing period validity or**
    - **regenerate the account key**

Lifecycle management feature

- **For blob object that support access tier**
- 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

- **Advanced threat protection (Azure Defender)**
    - **Storage threat protection** is available for :
        - **Blob Storage**
        - **Azure Files**
        - **Azure Data Lake Storage Gen2**

- **Storage type Acces Autorisation**

    - **Anonymous read: Only blob**
    - **Azure AD : Blob, Queues**
    - **SAS : All exept Azure FIle (but required for Az copy)**
    - **Shared key : All**

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 of your **VMSS Template** you add :
        - You specifie in the template the SA the key and the file to use
        - The comand to execute

- **Custom Script Extension**
  - Custom Script Extension will run under the **LocalSystem Account**
  - There's **90 minutes allowed** for the script to run, anything longer will result in a failed provision of the extension.
  - **Script Location**
    - The script location **can be anywhere**, as long as the **VM can connect** to **ex** :
      - **Azure Blob storage**
      - **GitHub**
      - **internal file server**
  -

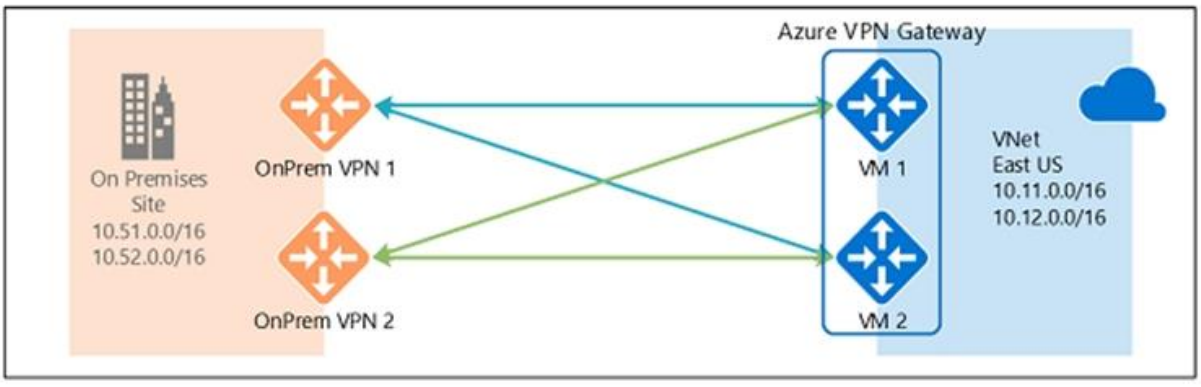
(voir : https://medium.com/charot/custom-script-extention-on-azure-vmss-e010a8c87904)

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

Virutal netwokr Gateway :

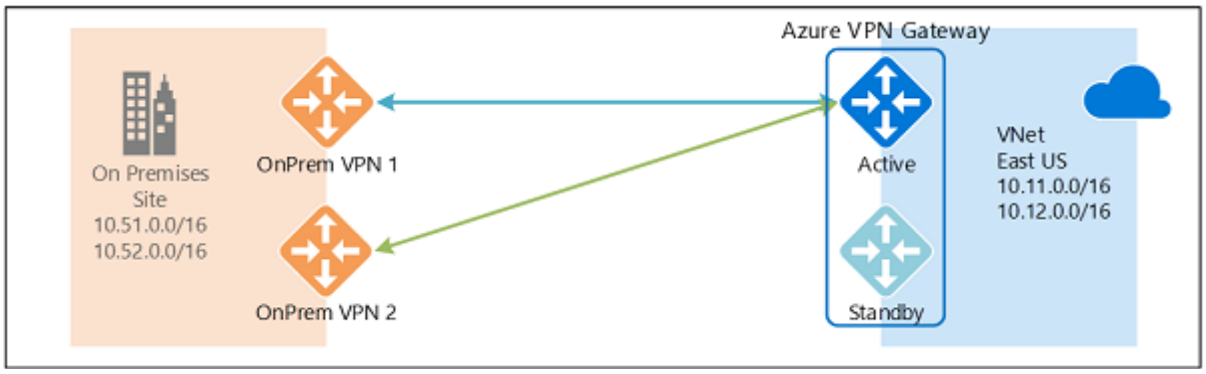
- You ca route all the traffic of a subnet to a One premise location chosing the VnetGatway as the next hop in the UDR
- **Gateway subnet already exit** as there is **ExpressRoute configured and working.**
  - So you need to create :
    - Create a **VPN gateway VpnGw1 SKU** for **coehexist** with a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

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.



Load balancer

- **Outbound rule**
  - Azure Virtual Network
    NAT can provide **outbound connectivity** for virtual machines utilizing an publ ic 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 balancer**
  - Azeure **Bacic load balancer**
  - **HEALT PROBE**
    - **TCP, HTTP**
- **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**.

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

- All load balancers are software appliances (software defined networking: SDN)
- 💡 Only Standard (not Basic) SKU allows availability zones in Load balancer

Load Balancer

- Load Balancer Role :
  - Nework contributor :
- Can manage the Load Balancer resources
- For add a healthprobe

- Bacic Load Balancer
  - 300 instance
  - BackEnd : VM in a single AvSet or Virtual machine Scale Set
  - No Availability Zone
  - No SLA
- Standar Load Balancer
  - 1000 instance
  - Any VM or Virtual Machine Scale Set in a single VNet
  - Availability zone available
  - SLA : 99.99%

- NAT Rule :
  - Create a load balancer inbound network address translation rule to forword traffic from a specific port of the front-end IP address to a specific port of a back-end VM

Azure App Gateway

- the Azure App Gateway need to be create one a subnet alone .
- if there is already virtual machine in subnet, we have to create a new subnet in Vnet

- Appp Gateway Standard v1
  - does not support static public IP addresses
  - Support only AvSet
- App Gatway Standard sku v2
  - support Static IP
  - Support Avset and AvZone
- App Gatway Support Web app and VM in Back end pool not load balancer
- Provide SLA of 99,95
- Provide SSL OFFLOADING
- One instance of Application Gateway can host up to 40 websites that are protected by a web application firewall. You just need multisite listener

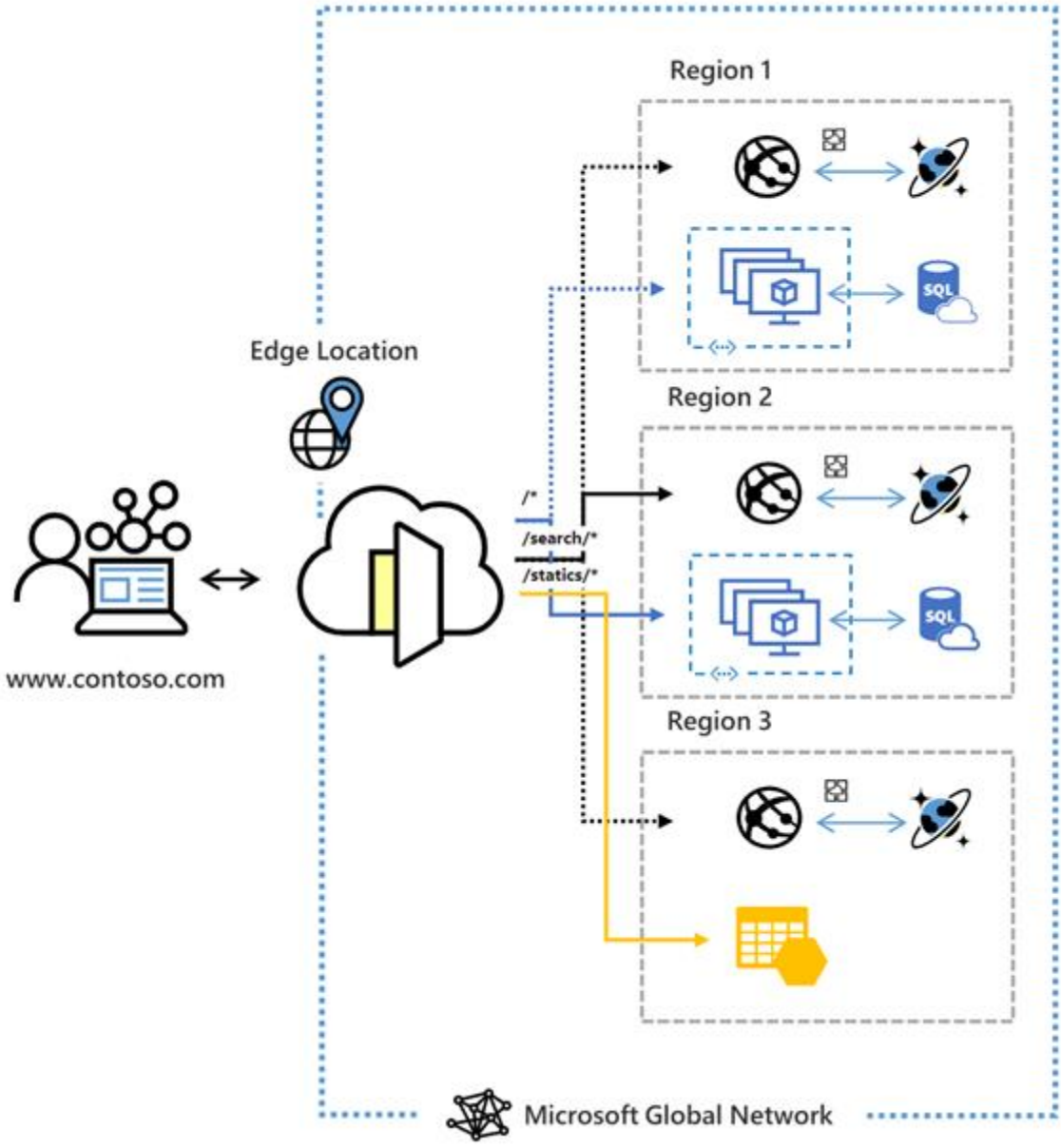
- Application Gateway can be configured with an Internet-facing VIP or with an internal endpoint that isn't exposed to the Internet
- OSI Layer 7 application
- Application Delivery Controller (ADC) as a service
- SSL offload
- Has Web Application Firewall (WAF) Integrated
  - Protection again SQL injection

        - **Provide centralized protection of your web application form common exploits and vulnerabities . SQl injection and cross-site scripting are among the most common attacks**

- **Feature**
    - **URL-based routing**
        - **If we need to route traffic based on different URL**
        - **requests for *http://contoso.com/video/** are routed to VideoServerPool, and *http://contoso.com/images/****
    - **Multiple-site hosting**
        - **If we need to direct request based on different sites**
        - **requests for *http://contoso.com* are routed to ContosoServerPool, *http://fabrikam.com* are routed to FabrikamServerPool**
    - ***Listener :***
        - ***Basic***
            - Here the listener listens to a single domain site
        - ***Multi-site.***
            - Here the listeners maps to multiple domain sites.
    - ***Backend pools***
        - These can be Network Interface cards , Virtual Machine scale sets , Public or Internal IP addresses , FQDN or backends such as App Service.
    - ***Health probes***
        - This defines how the application gateway will monitor the health of the resources in the backend pool.
    - ***Session affinity***

Azure front door :

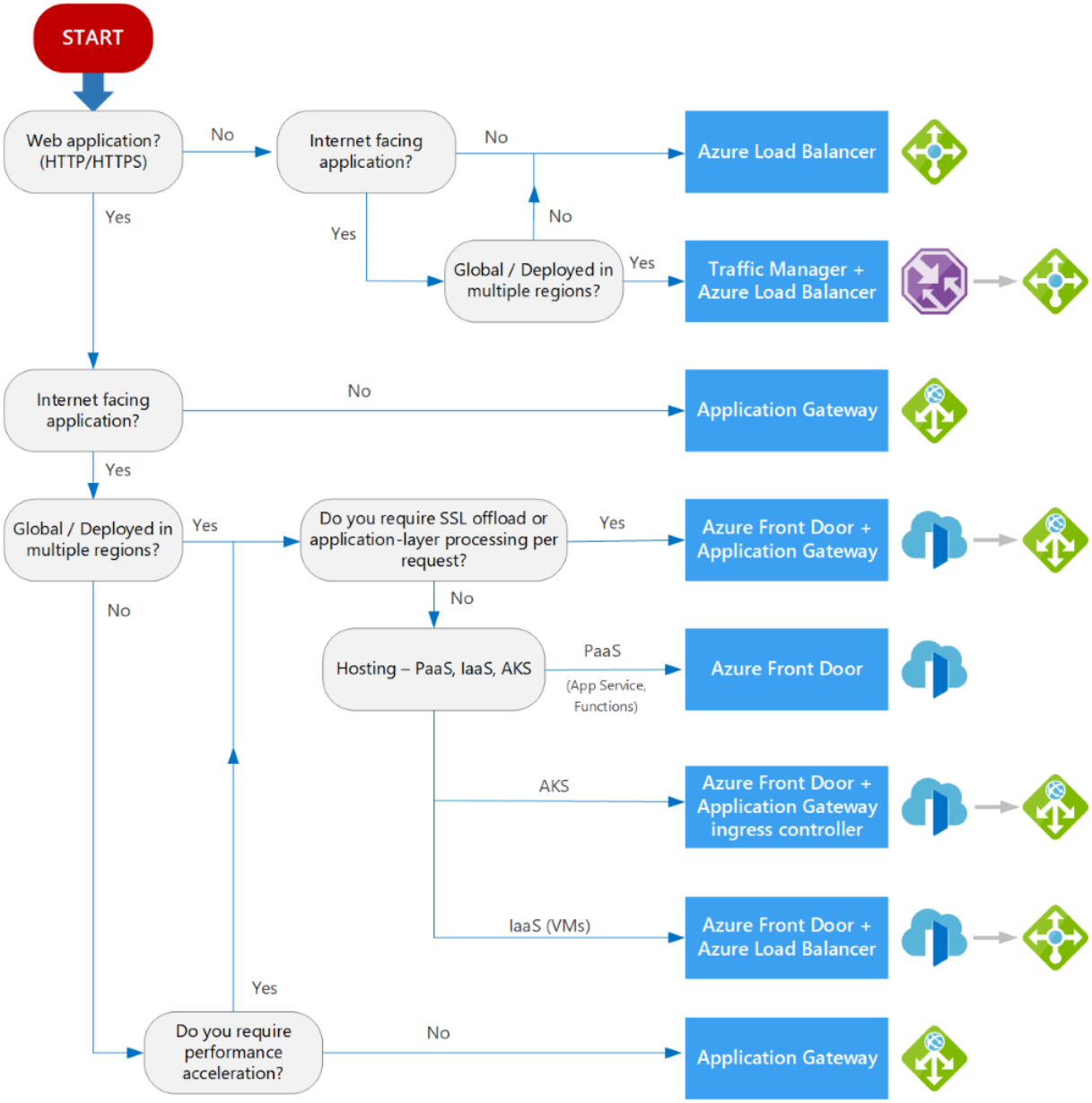
- Service permettant de **distribuer le Traffic** **entre les Azure région**
- Layer 7 (HTTP/HTTPS) load balancers (Like Applicaion Gateway)
- Application security with integrated **Web Application Firewall (WAF)**
- **Accelerated application** performance by using **split TCP-based**

- 

- 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.
- **Azure front door feature**:
    - routing methods
        - **Latency:** The latency-based routing ensures that requests are sent to the lowest latency backends
          acceptable within a sensitivity range. Basically, your user request

s are sent to the "closest" set of backends in respect to network latency.
        - **Priority:** You can assign priorities to your backends when you want to configure a primary backend to service all traffic. The secondary backend can be a backup in case the primary backend becomes unavailable.
        - **Weighted:** You can assign weights to your backends when you want to distribute traffic across a set of backends. Whether you want to evenly distribute or according to the weight coefficients.
        - **Session Affinity:** You can configure session affinity for your frontend hosts or domains to ensure requests from the same end user gets sent to the same backend.
    - **URL redirect**
        - Azure Front Door can redirect traffic at each of the following levels: protocol, hostname, path, query string. Thes e functionalities can be configured for individual microservices si nce the redirection is path-based. This can simplify application configuration by optimizing resource usage, and supports new redirection scenarios including global and path-based redirection.
        - Destination host
        - **Redirect HTTP traffic to HTTPS with URL redirect.**
        -
    - **URL-path based routing for requests**
    - **Can handle traffic for multiple site with one AFD creating** multiple Frontend host (Custom domain)
    - **Cookie-based session affinity.**

-



(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(**Its not recommended for HTTP HTTPS traffic(but you cant use it for http https web application) : TCP UDP request**)
- Service permettant de **distribuer le Traffic** entre les Azure **région**
-

- **If You want to enable Real User Measurements** to **monitor the network latency** for the application across the region :
    - **Real User management Pane ->**
    - **Generate a new Key** :
    - **Then The key** will need to be **embedded in your web application**
        - **Copy and paste the javascript code with the key to your web app**

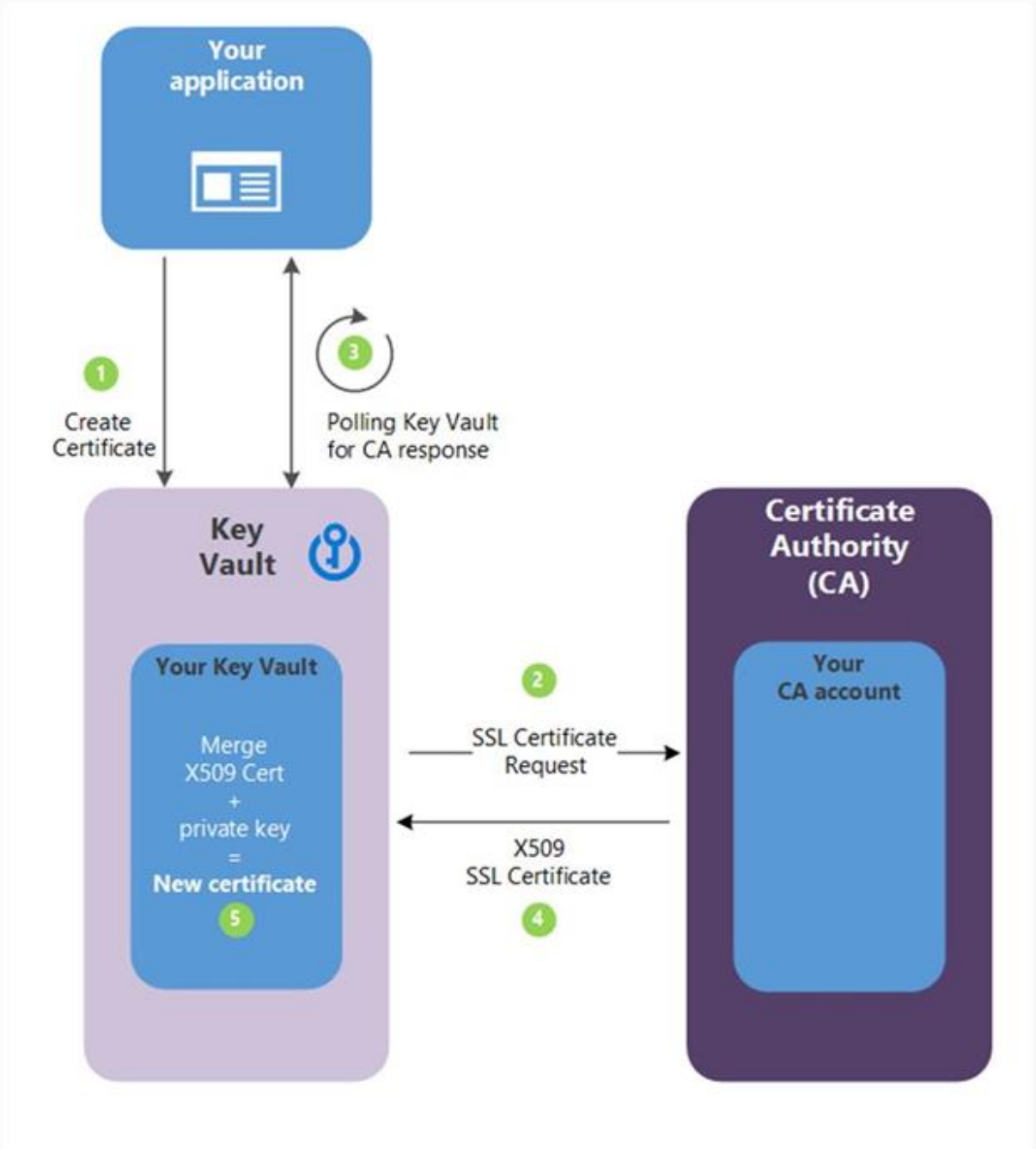
- **Routing method :**
    - **Priority** – Route traffic to another endpoint in case the primary fails.
    - **Weighted** – Route traffic to different endpoints based on weight.
    - **Performance** - you want end users to use the "closest" endpoint in terms of the lowest network latency.
    - **Geographic** - geographic location their DNS query originates fr om.
    - **Multivalue** – Here different endpoints are sent to the client. The client then selects the endpoint to send the request to.
    - **Subnet** – This maps a set of end-user IP address ranges to a specific endpoint within a Traffic Manager profile.
    -

Azure Key Vault :

- **Secret**
    - **Mot de passe**
- **Key**
    - **Can use for digitally sign blobs** in an Azure storage account
- **Certificat**
    - **CA for SSL etc , authentication**

- **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**



Azure 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.**

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)*
-
- **Scenario: Machines don't show up in the portal under Update Management**
    - Make sure that your machine is reporting to the correct workspace. For guidance on how to verify this aspect, see Verify agent connectivity to Log Analytics
    - Also **make sure that this workspace is linked to your Azure Automation account**
    - This issue can be caused by local configuration issues or by improperly configured **scope configuration.**

Azure Encryption (ADE) :

securing the data stored on the Boot and data volume of the virtual machines?

- 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**

- **Consequence of Key delete or disable** :

    - **For premium SSDs, standard SSDs, and standard HDDs:**
        - When you **disable** or **delete your key**, **any VMs with disks using that key** will **automatically shut down.** After this, the VMs will not be usable unless the key is enabled again or you assign a new key.

    - **For Ultra SSD disks**
        - The VM **won't automatically shut down**. Until you **deallocate and restart the VMs then VMs won't come back online.**

Ephemeral disks

- **do not support:**
    - Capturing VM images
    - Disk snapshots
    - **Azure Disk Encryption**
    - **Azure Backup**
    - Azure Site Recovery
    - OS Disk Swap
    - **Can't you mix ephemeral and normal OS disks in a scale set**
    - **You Can attach a Managed Disks to an Ephemeral VM (**VM that uses an ephemeral OS disk.)

Bursting (for Premium SSD) :

- **Premium SSD sizes smaller than P30** now offer disk bursting and can burst their IOPS per disk **up to 3,500 IOPS** and their bandwidth up to 170 MB/s. Bursting is **automated**

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
- Your apps need to be in a **Standard**, Premium, or PremiumV2 App Service plan.

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)

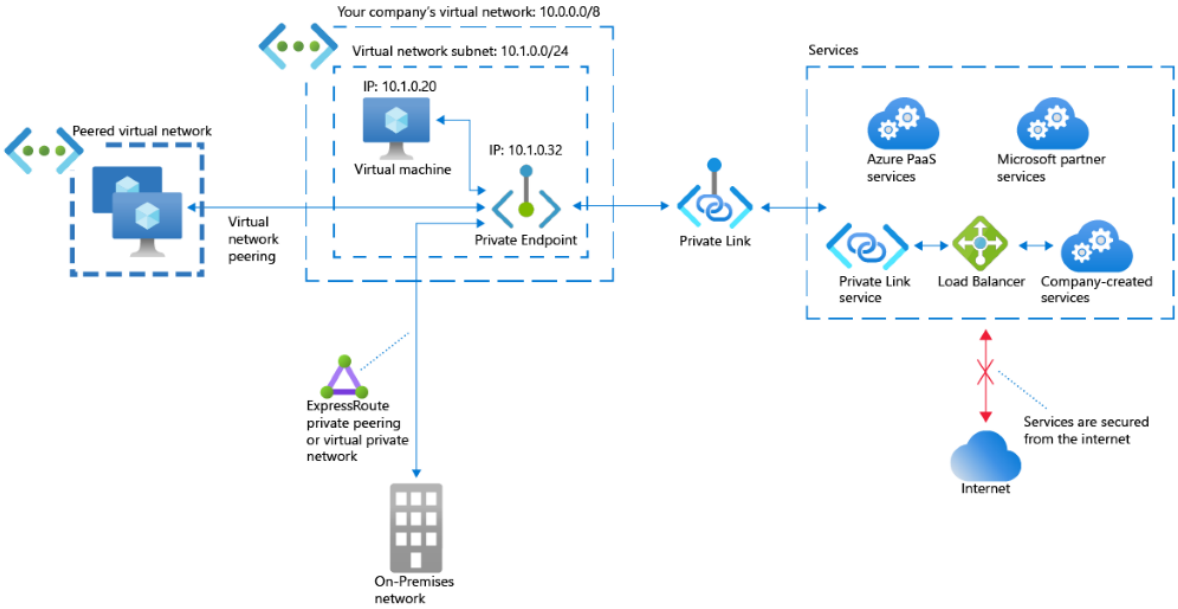
Private link endpoint :

- create a **private ip** in a **subnet** in vnet of your subscription referancing the paas service (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** targeting 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 overlapsing so you can't juse connect to the private endpoint of the peered network

- To create a **privant link** for **connect** the **private endpoint** that **customer** add to thier net work and the **private link service** that the you(**provider**) add to connect to your service running behind **Standard load balancer**
  -



  -

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%.**

Azure Sentinel

- Ingest data secuiry from service and cant make and Automatique reponse solution.

- Its a SIEM,
  SIEM aggregates security data from many **different sources(AWS,Azure)** to provide addit ional capabilities
- **Threat detection** and **reponse autamtiquely smarter and faster**
-
- **Sentinel Role**
  - Azure Sentinel Reader
    - can **view** data, incidents, workbooks, and other Azure Sentinel resources.
  - **Azure Sentinel Responder**
    - in **addition** to the above, **manage incidents** (assign, dismiss, etc.)
  - **Azure Sentinel Contributor**
    - in **addition** to the above, **create and edit workbooks, analytics rules**, and other Azure Sentinel resources.
  - **Azure Sentinel Automation Contributor**
    - allows Azure Sentinel to add **playbooks** to automation rules. It is not meant for user accounts.

- **Azure Sentinel notify**
-
  - 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.
  - Step
    - Azure Sentinel -> Playbook.->**Add Playbook**.->redirected to a **Logic App creation** page-> **select azure sentinel triggere -> select send email action**
      - Role needed is **Azure Sentinel Automation Contributor or Az sentinel contribu tor + logic app contributor**

-

Azure security center

- Unified intradructure security management system
- Renforce la securité posture des datacenters (**cloud** and **one premise**)
- Provide **security** **(compute, data, network storage , app**)
- You can define a list of allowed applications to ensure that only applications you allow can run on the VM.
- Azure Security Center can also detect and block malware from being installed on your VMs.
- just-in-time (JIT) virtual machine (VM)
- allows you to lock down inbound traffic to your Azure Virtual Machines.
  This reduces exposure to attacks while providing easy access when you need to connect t o a VM.
- **Secure score**
- **Recommandation**

- **Pricing tier**
  - **Azure Security Center free**
    - Security Center without Azure Defender
  - **Standard / Defender On**
    - **Enable Container security features**
    - **Vulnerability scanning for virtual machines and container registries**
    - **Enabling Azure Defender extends the capabilities of the free mod**
    - **Hybrid security**
    - **Just In Time**

- **Security Role Azure RBAC** :
  - **Security Admin Role**
    - **View and update permissions** for **Security Center**. Same permissions as the Security Reader role and can also **update** the **security policy** and dismiss **alerts** and **recom mendations**
  - **Security Reader**
    - V**iew permissions** for **Security Center**. Can **view recommendations, alerts**, a **security policy**, and **security states**, but **cannot make changes**

Blueprint

- Contaner for composing sets of standard, patterns and requierements for implementiatio of Azure services security and design
- Azure Blueprints allow the IT professional to orchestrate the deployment of resource templates and other Azure artifacts, including role assignments, policy assignments, resource groups, and resource manager templates
- Azure Blueprints is intended to assist with environment setup. Such environments often :
  - **Resource Groups**
  - **ARM template**
  - **Policy Assignment**
  - **Role Assignment**
- . Blueprints are essentially packages that pull these types of resources and artifacts together. These packages can then be composed, versioned, and assigned to a subscription. Such blueprint packages can also be audited and tracked.

- **dependsOn property**
  - **dependsOn** is a string array of artifact names that the particular artifact needs to be crea ted before it's created.

Azure service Health

- Notify about azure service incidenta afin d'effectuer des actions pour réduire le downtime

- You can view the **current status of the Azure services you rely on**, **upcoming planned outages**, **and services that will be sunset**. You can **set up alerts** that help you stay on top of incidents and **upcoming downtime** without having to visit the dashboard regularly.
- **Set up alert Steps:**
- **Service Health pane -> healt alerts -> add service healt alert ->**
    - **Create servic healt alert**
    - **Define alert condition**
    - **Define alert details**
    - **Define action group**

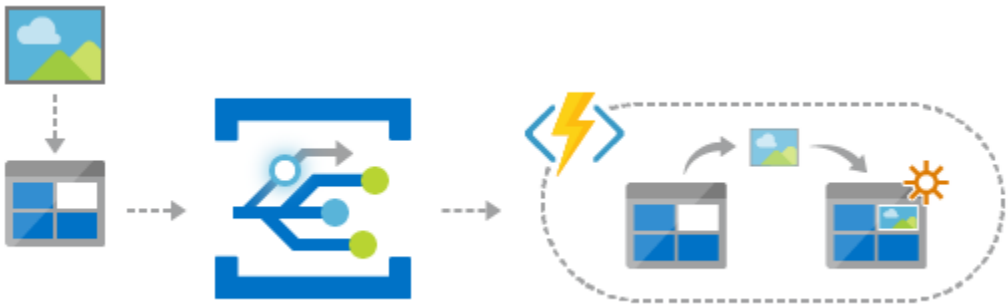
Lock

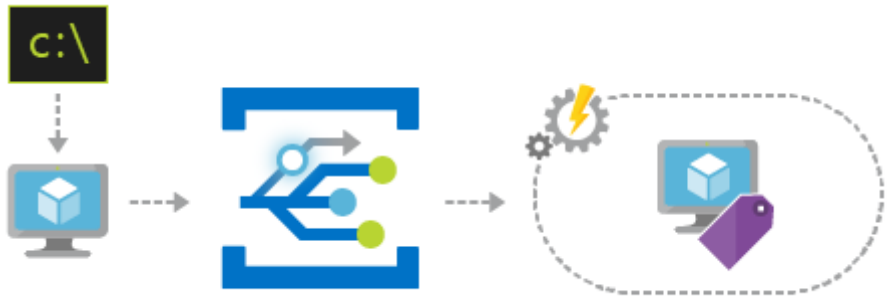
- Read only lock/delte lock on the ressource dosnt prevent the ressource to be moved to or from a rg

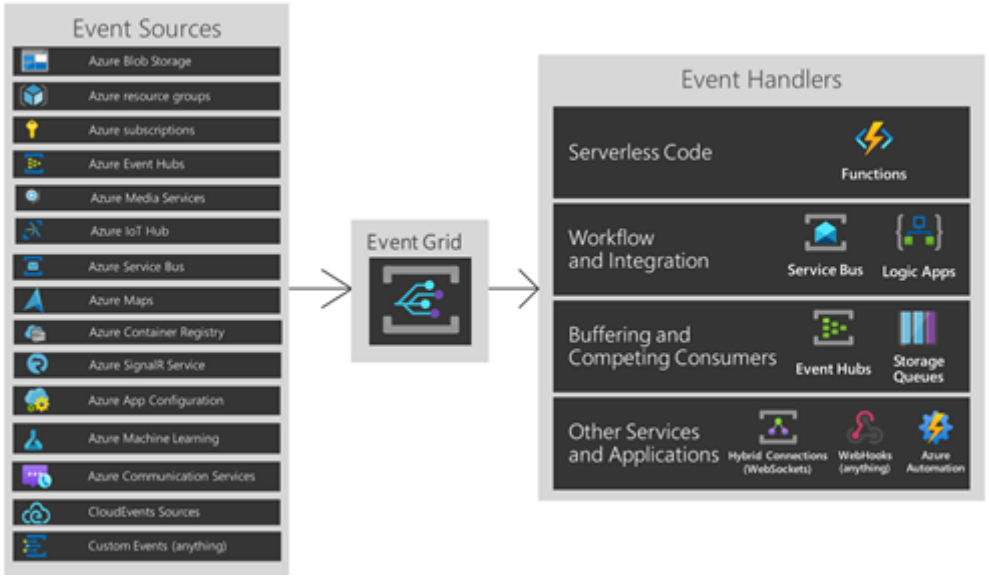
But if the **source ressource group** have a read only lock the moove operatiion is **prevented** if the destination rg have a read only lock the operaiton is alowed

- Lock
    - A read-only lock for a virtual machine prevents the users from starting or restarting the virtual m achine.
    - A read-only lock on a **storage account** prevents users from **listing the account keys.**
    - A cannot-delete lock on a **storage account** doesn't prevent **data within** that account from being delet ed or modified.
    - A read-only lock on a **storage account** **doesn't prevent** **data within** that account from being dele ted or modified.

Event Grid :

- Récupère des évènement venant de multiple Azure ressource afin de les transférer a des application ou precesse
- For example, use Event Grid to trigger a serverless function that analyzes images when added to a blob storage container
- 
- For example, use Event Grid to notify Azure Automation when a virtual machine or database in Azure SQL is created. Use the events to automatically check that service configurations are compliant, put metadata into operations tools, tag virtual machines, or file work items.





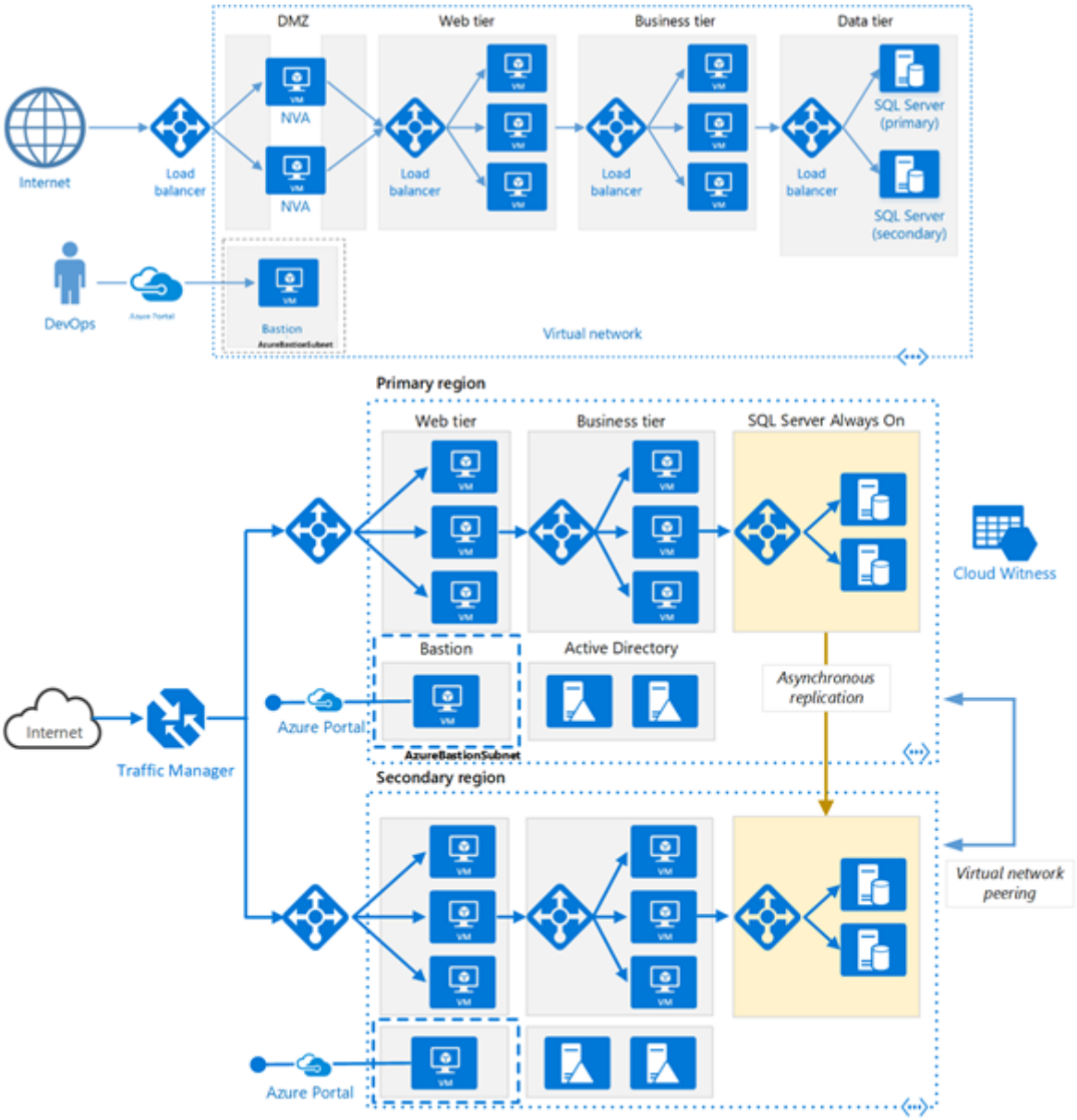
Azure Advisor

- provides **suggestions** on how to **optimize for reliability, security, performance, costs,** and operations based on **experts' best practices.**
- Recommandation
- **HA**
- **Optimise**
- **Security**
  - **Work wirth security center**
- **Money**
  - **Work wirth cost management**
  - **Go to cost management -> Advisor for recommentation related to cost optimization**

Architecture :

It would be preferential to have separate subnet for each layer of a Web appplications

- **3 tier** recomended(**at least 2**) within **1 vitual nework**
  - **3 subnet**
  - **1 virtual nework**
- **AvSet**
  - You should ideally create **availability sets** based on the **number of tiers** you have for you application (app With, **Webtier + Databasetier** = **2 Av set)**



The Azure the **initial size** of Azure a virtual hard disk (VHD) is **30 GB** for all **Windows Server images**

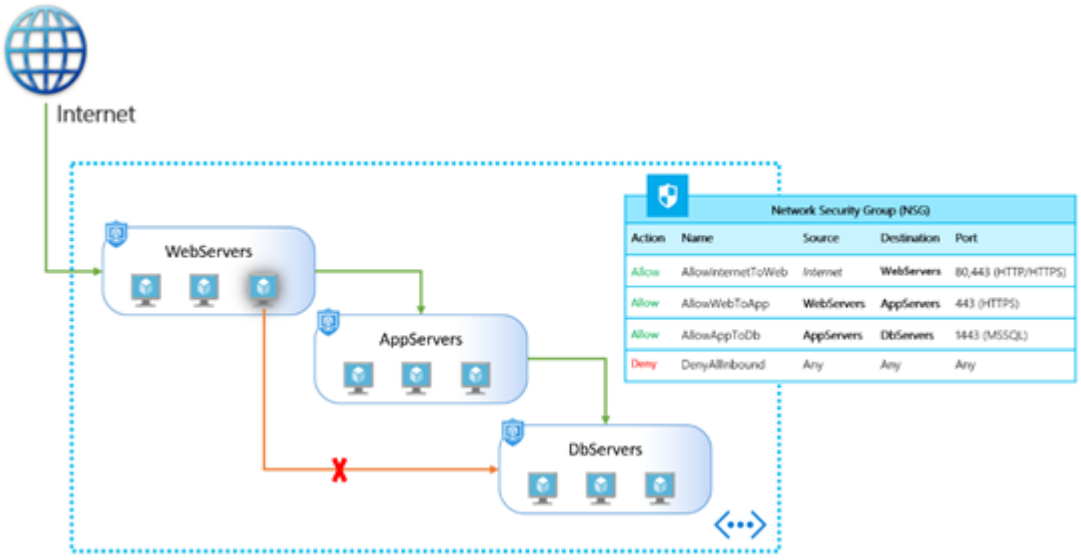
Azure Firewall :

Azure firewall and NSG are Statefull

- **There are three types of rule collections**:
  - **Application rules**:
    Configure **fully qualified domain names (FQDNs)** that can be accessed from a subnet.
  - **Network rules**: Configure rules that contain source addresses, protocols, destination ports, and destination addresses.
  - **NAT** rules: Configure DNAT rules to allow **incoming Internet connections.**

Application security Group

- Filltering traffic based on applications patterns
- Créer des groups d'application et filter le traffic en fonction de ces groupes
- allowing you to **group virtual machines** and define network security polici es based on those groups.
- Flow :
    - You **first need to create a NSG** ,
    - in the NSG you **mention the Application security group(** Webserver , App Server **)** as **source** or **destination**



Managed identity :

- **provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication. Applications may use the managed identity to obtain Azure AD tokens. For example, an application may use a managed identity to access resources like Azure Key Vault where developers can store credentials in a secure manner or to access storage accounts.**

    - **System-assigned** :
        - Created as part of an Azure resource
        - Shared life cycle with the Azure resource that the managed identity is created with.
        - When the parent resource is deleted, the managed identity is deleted as well.
    - **User-assigned**
        - Created as a stand-alone Azure resource
        - Independent life cycle.
        - Must be explicitly deleted.

You can use both types of identities for the **Azure Logic App or Azure VM**

Azure Cosmos DB Container and partition key's container Ok Udemy
Azure SQL pool, instance Ok Udemy
Microsoft Learning path module one the weak field (DATABASE Ok Udemy , SENTINEL ,SECURITY CENTER , MIGRATION , REPLICATION, QUEU , Service Bus Ok Udemy, Webhook, Proximity group , immutable storage, stored policy Ok Udemy , key vault , Update Management *)*

Selection 3: Migrate, replic recovery , load balancer, App gateway , traffic manager, front door ,
Section 6 : Keyvault

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

Personal lab :
Crate webb app with lets encryps ssl keyvault
Connection to database

If question with Avset and AVzone chose Yes even different instance

53

PAGE /33/34/37/38 LAB

Pratict Test 1

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

Pratict Test 2

- Q1 Ok, Q2 Ok,Q3, Q4 Ok,Q10 Ok, Q11 Ok ,Q12 Ok ,Q13 Ok,Q14 Ok,Q15 Ok,Q16 Ok,Q20 Ok,Q31Ok ,Q39 Ok,Q40 Ok ,Q41 Ok,Q43Ok,Q44 Ok,Q45 Ok,Q46,Q47 Ok,Q48,Q53 Ok

Pratict Test 3

Q1 Ok,Q6 Ok,

Pratist Test 4

- Q6 Ok , Q8 Ok , Q10 Ok, Q11 Ok,Q13 Ok,Q15 Ok,Q17Ok,Q18 Ok,Q20 Ok,Q21 Ok, Q24Ok, Q26 Ok,Q31 Ok,Q32 Ok,Q33 Ok,Q34 Ok,Q35 Ok,Q37 Ok,Q31,Q40 Ok, Q41 Ok, Q42 Ok, Q43 Ok,Q44 Ok,Q45 Ok,Q46 Ok

Pratice Test 5

- Q2 Ok, Q13 Ok,Q14 Ok,Q16 Ok, **Q18 Ok,**Q22 Ok ,Q24 Ok,Q26 Ok,Q27 Ok, Q28 Ok ,Q31 Ok,Q32 Ok,Q37 Ok,Q49

Praticte Test 6

- Q8 Ok, Q10 Ok, Q11 Ok, Q12 Ok, Q14 Ok , Q16 Ok, Q17 Ok, Q19 Ok, Q21, Q22 Ok, 23 Ok, 25 Ok , 26 Ok, 27 Ok,28 Ok , 29Ok , 30 Ok,31 Ok, **33 Ok,** 39 Ok, 40 Ok 41 Ok,42 Ok, 47 Ok,48 Ok ,49 Ok

Udemy alan rod 1 :
40 monitoring Ok
41 key vault Ok
42 confirmation Ok
43 migrate (migrate account ?) Ok
44 Ok
45 migrate Ok
46 recovery Ok
47 Traffic manager Ok
48 Traffic manager Ok

Udemy alan rod 2 :

14 Ok
18 Ok
22 Ok
24 Ok
27 Ok
29 Ok
45 OK
46 OK
51 Ok
52 Ok

sureh 1
sureh 2
Sureh 3
alan 2