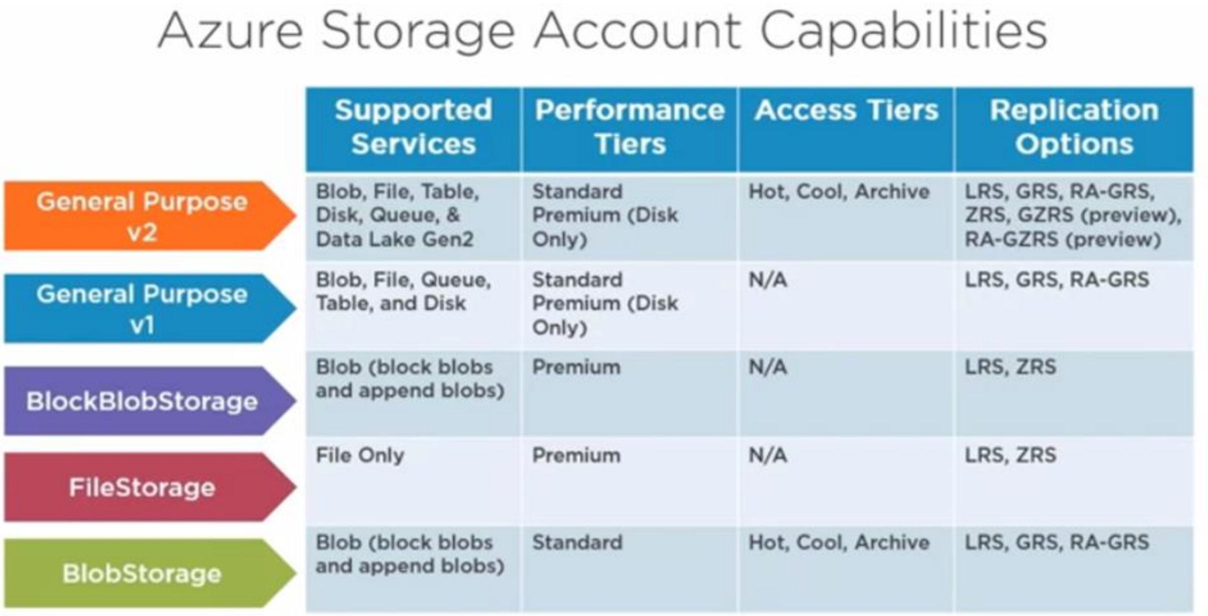
Storage account :

- You need to design a storage solution for an app that will store large amounts of frequently used data. The solution must meet the following requirements:
  ✑ Maximize data throughput.
  ✑ Prevent the modification of data for one year.
  ✑ Minimize latency for read and write operations.
  - **BlockBlobSorage**
    - **Premium** blob storage (**faster thant GPv2 Premium only for disque**)
  - **Blob**
    - One big file is splitted in "blobs" that are processed in parallel (for **read and write**)
    - immutability requirement through a Time-Based Retention Policy at the **container-level.** That will prevent write and delete operations for all blobs in the container for a given period (in this case, 1 year).
- Premium: **Premium file shares** are backed by solid-state drives **(SSDs**) and provide consistent **high performance and low latency**



Azure Storage Account Capabilities

	Supported Services	Performance Tiers	Access Tiers	Replication Options
General Purpose v2	Blob, File, Table, Disk, Queue, & Data Lake Gen2	Standard Premium (Disk Only)	Hot, Cool, Archive	LRS, GRS, RA-GRS, ZRS, GZRS (preview), RA-GZRS (preview)
General Purpose v1	Blob, File, Queue, Table, and Disk	Standard Premium (Disk Only)	N/A	LRS, GRS, RA-GRS
BlockBlobStorage	Blob (block blobs and append blobs)	Premium	N/A	LRS, ZRS
FileStorage	File Only	Premium	N/A	LRS, ZRS
BlobStorage	Blob (block blobs and append blobs)	Standard	Hot, Cool, Archive	LRS, GRS, RA-GRS

- **GPV2 hierarchical anmesace enabled :**
  - **unlock capabilities such as file and directory-level security on an Azure storage account**
    - Fine-grain AAD based Access Control at the directory/sub-directory level

- **Service Endpoints**
  - are enabled on subnets configured in Azure virtual networks. **Endpoints can't be used for traffic from your premises to Azure services.**

(allow connectivuty throught azure backbon from other azure service or vnet still use SA name)

- **Private Endpoint**
    - securely connect to storage accounts from **on-premises networks** that connect to the **VNet using VPN or ExpressRoutes with private-peering.(create a private IP on the VNET)**

Azure Data Lake Storage Gen2 :

- Azure Data Lake Storage is optimized storage for **big data analytics workloads**.
- Use cases: Batch, interactive, streaming analytics and machine learning data such as log files, IoT data, click streams, large datasets

Backup :

- SQL server on Azure VM
    - The solution must meet the following requirements: Provide the ability to recover in the event of a regional outage. Support a recovery time objective (RTO) of 15 minutes. Support a recovery point objective (RPO) of 24 hours. Support automated recovery. Minimize costs
        - **Azure site recovery**
            - Replication with Azure Site Recover:
            - **RTO is typically less than 15 minutes**.
            - **RPO: One hour for application consistency and five minutes for crash consistency.**

Azure AD Aplication Proxy :

- **Enable users to access on-premise web app from a remote client**

Azure AD DS

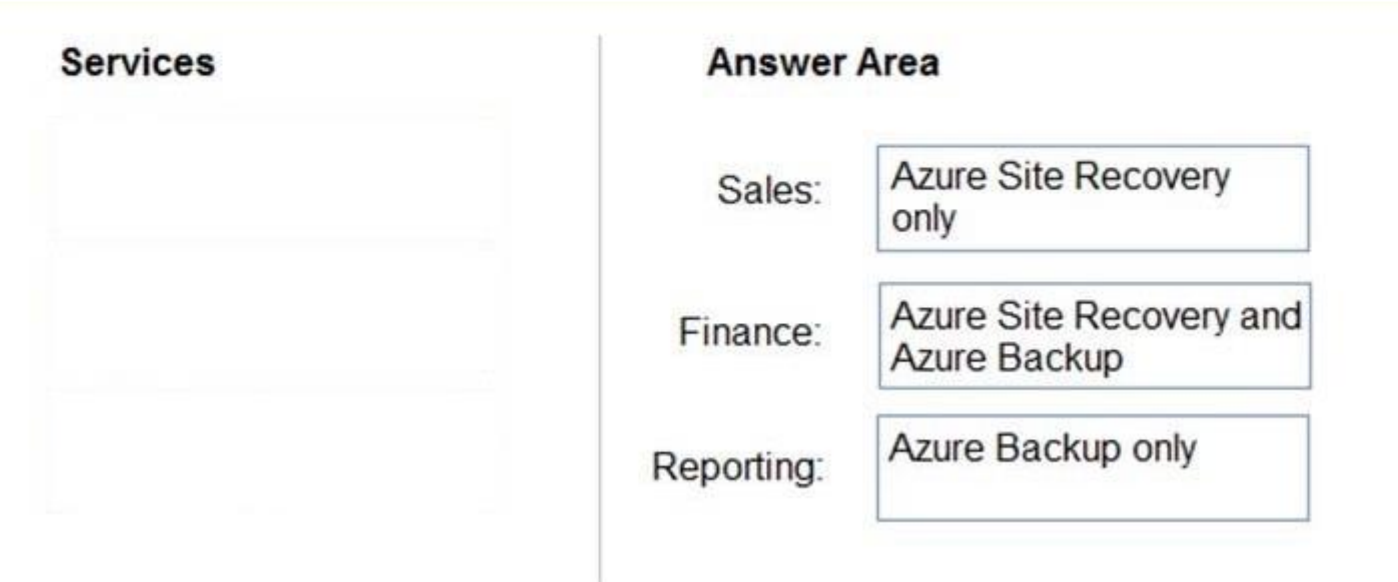
- allow to use legacy protocols like **LDAP**. Kerberos and NTLM

Azure Synapse Analytics Dedicated SQL pool. :

- Hava **limit of 128 concurrent queries**

Azure Firewall :

- Firewall **Parent policy** must be in the **same region** as child policy



Services

Answer Area

Sales:	Azure Site Recovery only
Finance:	Azure Site Recovery and Azure Backup
Reporting:	Azure Backup only

- **Backup** ensures that your **data** is safe and recoverable while Site Recovery keeps your workloads available when/if an outage occurs.

Network Watcher

- **Need to Enable Network Watcher in the region**
- **Shows where's the traffic is captured/denied**
- **Suite of tools**
    - **Topology**:
        - **e.g. VNETs, subnets, VMs, NICs**
    - **Variable Packet Capture:**
        - **Captures TCP packages at NIC level as wireshark files.**
        - **Inspect network traffic between VM**
    - **IP Flow Verify:**
        - **Troubleshoots NSG**
        - **Chek if a packet is allowed or denied to or from a Virtual machine**
        - **If the packet is denied by a security group the name of the rule that denied the packet is returned**
        - **Quiclick diagnose connectivity issues**
            - **From or to a virtual machine**
            - **From or to the internet**
            - **From or to the on-premises environnement**
            - **The information consist of**
                - **Direction**
                - **Protocal**
                - **Local IP**
                - **Remote IP**
                - **Local Port**

            - **Remort Port**
- **Next hop:**
    - **Troubleshoots route tables**
- **Connection troubleshoot:**
    - **Why it does not connect?**
- **Diagnostics Logging**
- **Security Group View**
- **NSG Flow Logging**
    - **Log network traffic to and from a virtual machine**
    - **log network traffic that flows through an NSG with Network Watcher's NSG flow log capability**
    - **Create a VM with a network security group**
    - **Step :**
        - **1 . Enable Network Watcher in the region**
        - **2 . register the Microsoft.Insights provider**
        - **3 . Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability**
        - **Create a storage accoutn for store the log**
        - **4 . Download logged data**
        - **5. View logged data**
- **Connection Monitor**
    - **connection monitoring in Azure Network Watcher.**
    - **monitor, diagnose, and view connectivity-related metrics for your Azure deployments.**
    - **VPN Gateway Troubleshooting**

Azure API Management :

- helps organizations **publish APIs to external, partner**, and internal developers to unlock the potential of their data and services. You **can secure API** Management using the **OAuth 2.0 client credentials** flow

- **Azure API Management Premium** tier supports **virtual network integration**, which allows you to restrict **ingress access** to the microservices to a single **private IP** address within the virtual network. This tier also supports mutual **TLS authentication**, **rate-limiting policies**, and provides a solution for exposing the microservices to the consumer apps while minimizing costs.

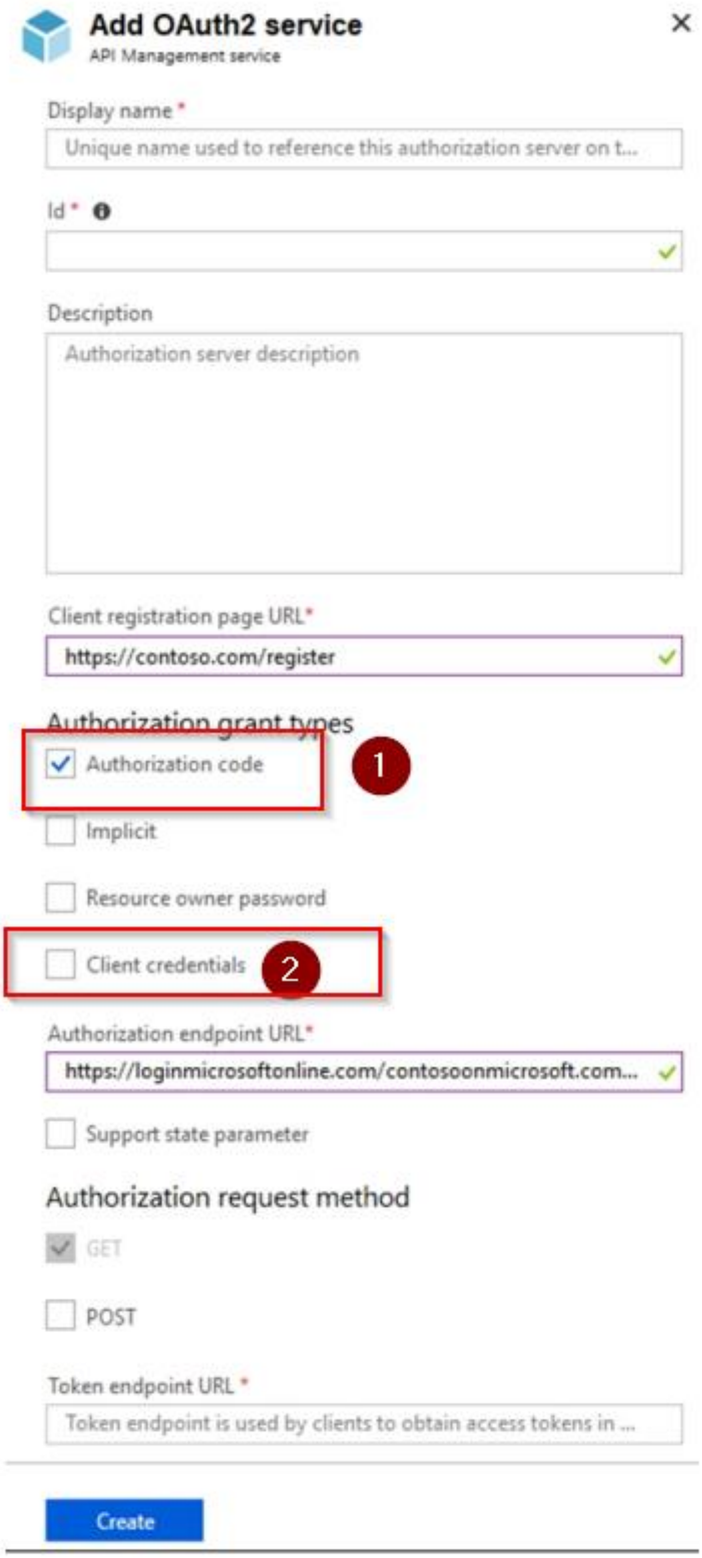
- **Protect a web API backend** c

(front end App connecting back end app (API) configuration flow)

    - 1 - In Azure AD, register an application (backend-app) to represent the API.
    - 2 - In Azure AD, register another application (client-app) to represent a client application that needs to call the API.

        - 3 - **In Azure AD, grant permissions to allow the client-app to call the backend-app.**
        - 4 - In APIM, configure the Developer Console to call the API using OAuth 2.0 user authorization.
        - 5 - **In APIM, add the validate-jwt policy (JSON Web Token) to validate the OAuth token** for every incoming request.

    - **API** ar **accesible from internet** when they are deployed on a VNET but **configured** to be **"External" (No VPN are needed to acces the API if he is external)**
    - API on a subnet can access data from ohere subnet in the same VNET if NSG doesent prevent it (**default is open beeteen subnet**)



Add OAuth2 service

API Management service

Display name *

Unique name used to reference this authorization server on t...

Id *

Description

Authorization server description

Client registration page URL*

https://contoso.com/register

Authorization grant types

☑ Authorization code

□ Implicit

□ Resource owner password

□ Client credentials

Authorization endpoint URL*

https://loginmicrosoftonline.com/contosoonmicrosoft.com...

□ Support state parameter

Authorization request method

☑ GET

□ POST

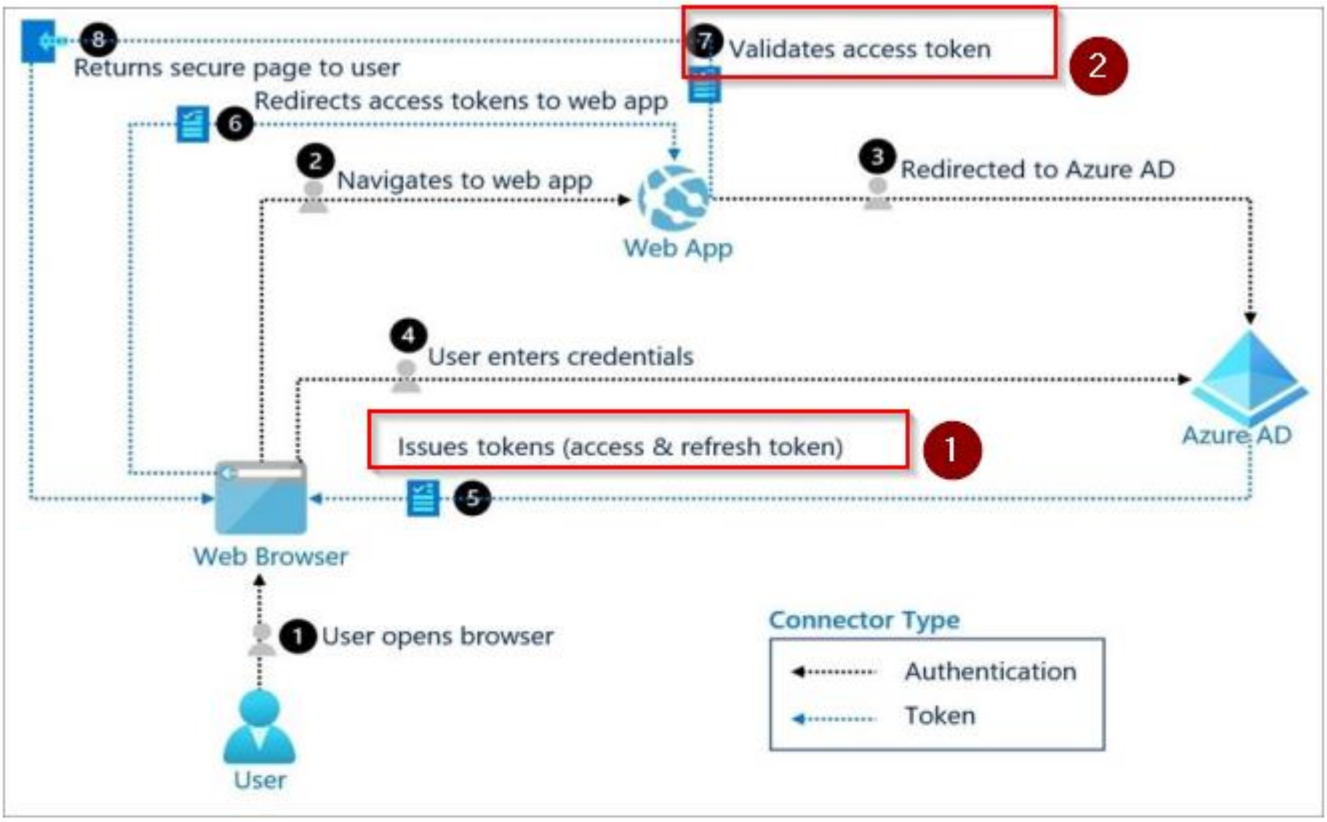
Token endpoint URL *

Token endpoint is used by clients to obtain access tokens in ...

- **1) Authorization Code** Grant Type is **used by** both **web apps** and native apps to get an access token after a user authorizes an app.
- **2)Client Credentials** : How to enable **custom data in grant flo** In case you need to store additional details about a client that don't fit into the standard parameter

- For **remove AspNet-Version** from the **response** of the published APIs
  - **Create e new policy**
    - https://docs.microsoft.com/en-us/azure/api-management/transform-api

APIM users conntecion flow (OAuth 2.0):



- **The access tokens will be genrated by Azure AD**
- **Authorization decission will be perfomed by the web API**

- **You can send diagnostic log (SQL Insight, VM) to (Database Metric monitoring) :**
  - **Event Hub**
  - **Storage account**
  - **Log analytic workspace**
- **Azure SQL Diag setting**
  - **Like diag setting for VM**
  - **Can store multipe data type**:
    - **SQL Insight, Erros,Querrystoreruntime , timeout, block ,deadlocks**

        - **Maximum rentention days** for log :
            - **730 days**
        - **Multiple Diag setting one same DB to multipe storage destination**:
            - **you can have multiple diagnostic settings that send the data into different destinations(storage , log analytic , event hub)**

Azure Service Map

- **Vizualise relationship** beetween app componnement

- **Azure Hybrid Benefit**
    - allows you to use your **on-premises Windows Server licenses** and run Windows virtual machines on Azure at a **reduced cost.**

Template :

- **Deploy ARM Template with keyvault secret for password :**
    - Set the **--enabled-for-template-deployment** to **true** creating the key vault (**enable access to the ARM Template in Keyvaylt policy** *)*
    - assign the persson who deploy the template the **Microsoft.KeyVault/Vaults/Deploy/Action permission**.

Keyvault :

- Only **1 keyvault is needed for HA an DR** : Azure already makes the Key highly available and **automatically failover** on case of an outage to a **paired region**
- In the event of a region failover, it may take a few minutes for the service to fail over.
- **During failover,** your key vault is in **read-only mode.** Requests that are supported in this mode are:
    - **List certificates /secrert/key**
    - **Get certificates /secets /key**
    - **Encrypt**
    - **Decrypt**
    - **Wrap**
    - **Unwrap**
    - **Verify**
    - **Sign**
    - **Backup**

Not : Delete

- During failover, you will not be able to make changes to key vault properties. You will not be able to change access policy or firewall configurations and settings.
- **After a failover** is failed back, all request types (including **read *and* write** requests) are **available.**

- **RBAC can assign permission to a specific secret, but the access policy assigns permissions for all secrets or keys, not as granular as RBAC**

Azure Redis Cache :

- **Store frequent acccess data closest to the application in a cache** to **improve the performance**
- Redis **improves the performance** and scalability of an **application** that uses **backend data** stores heavily. It's able to process **large volumes of application requests** by keeping **frequently accessed data in the server memory,**
- Data from :
    - **Azure cosmsos DB**
    - **SQL Database**
    - **Storage account**

- **Azure Content Delivery Network :**
    - https://www.udemy.com/course/exam-az-microsoft-azure-exam-role1/learn/lecture/17563312#overview
    -
    - For effective **delivery of static content across the world,**
    - . Place all of the content in an Azure **Blob storage account.**
    - **Enable Contend delivery Network** on the **Storage Account**
    - Since users access the content via a **domain name,** ensure the **domain name is assigned to the Azure Content Delivery Network domain.**
    - **Flow :**
        - **Create a CDN profile (with a princintier) :**
        - **Create a CDN endpoint en name it (this will assiociete the CDN profile ressource to the CDN enpoint ressrouce)**
            - **Storage account**
            - **Cloud service**
            - **Web apps**
            - **Custom origine**
                - **Web app on one premise or in a VM**
        - **You can add a Custom domain to the endpoint**

Just in Time :

- for providing **access whenever required** for **virtual machines.**
- available in **Azure Security Center**
- **Flow :**
    - **Azure security -> defender**
    - **Create JIT on a VM**
        - **Select the public port , select the time allowed**
        - **Requet access => select "my Ip" or ip of somewhone**
    - **This will create a NSG rule for the requered access during the time definied**

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**

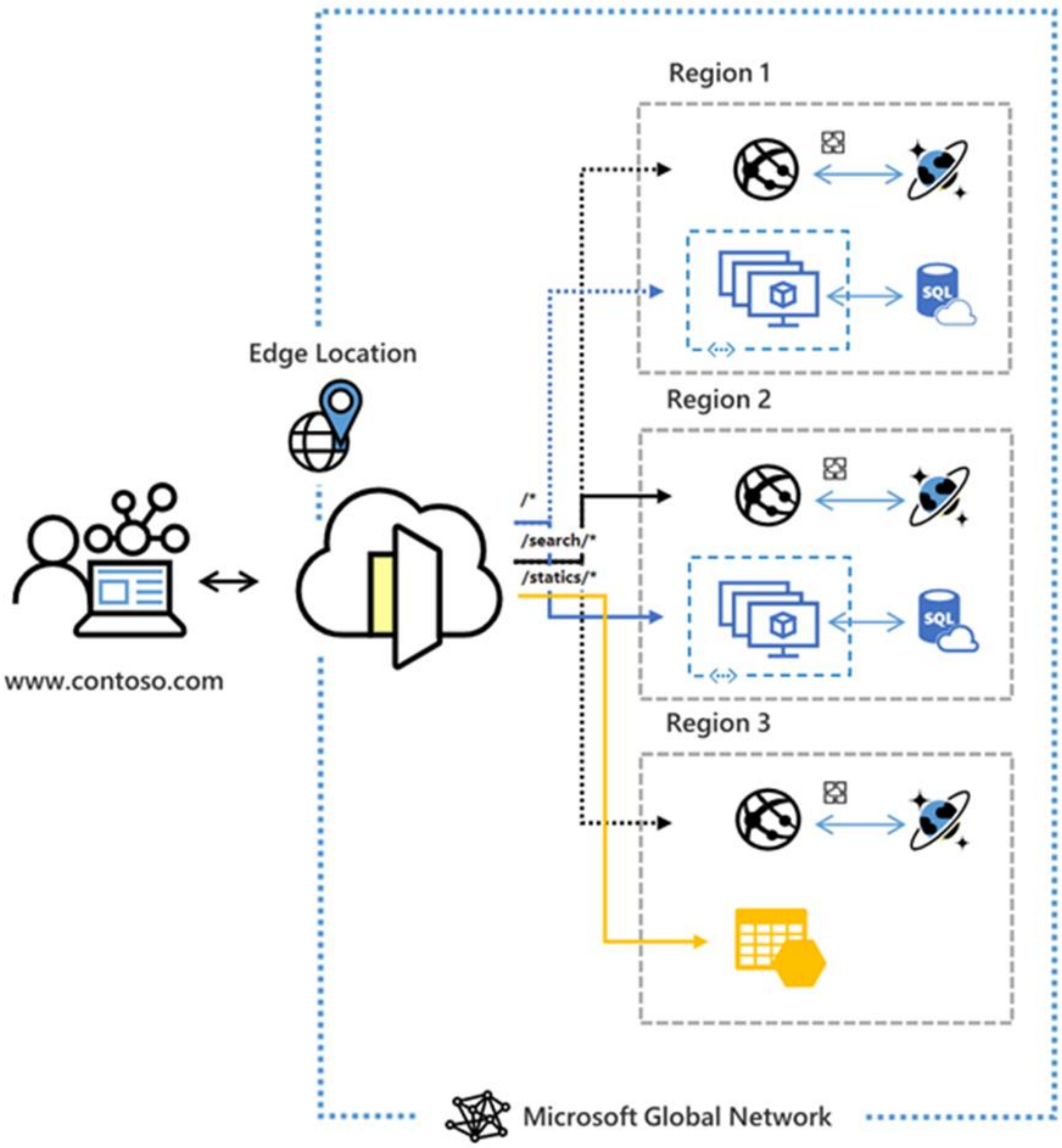
- **Application Gateway can be configured with an Internet-facing VIP or with an internal endpoint that isn't exposed to the Internet**
- **OSI Layer 7 application**
- **Application Delivery Controller (ADC) as a service**
- **SSL offload**
- **Has Web Application Firewall (WAF) Integrated**
    - **Protection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

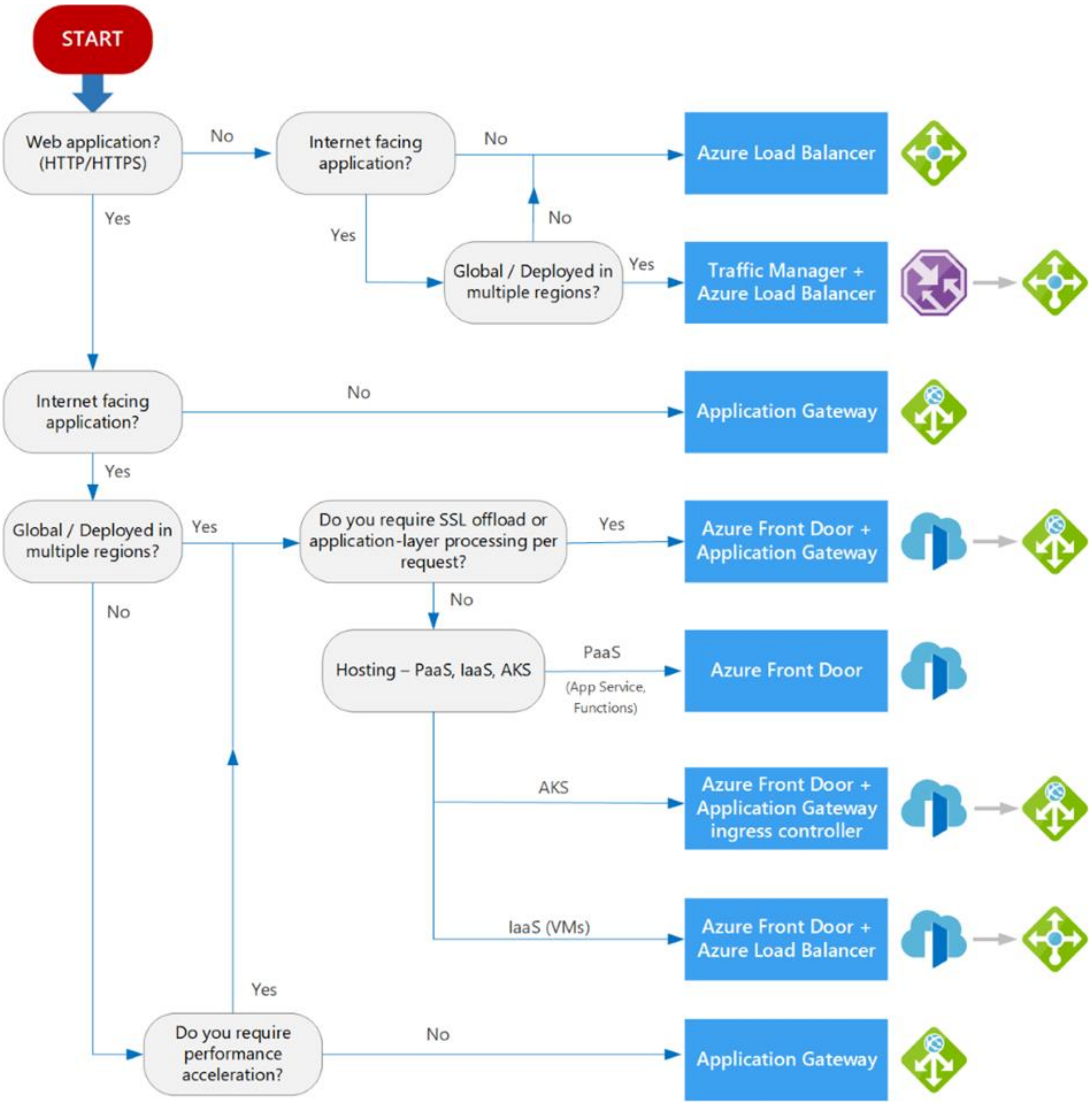
Azure front door :

- Service permettant de **distribuer le Traffic** **entre les Azure région**
- Layer 7 (HTTP/HTTPS) load balancers **(Like Applicaion Gateway**)
- **SSL offloading capabilitie**s so that the **SSL encryption can be managed by Azure Front Door itself.**
- **Recommended for https**
- Application security with integrated **Web Application Firewall (WAF)**
- **Accelerated application** performance by using **split TCP-based**
- **Can route to AKS , Web APP, ore Azure VM**



- 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 requests 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 use** 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 requests 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. These functionalities can be configured for individual microservices since 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.**


START
Web application? (HTTP/HTTPS)
No
Internet facing application?
No
Azure Load Balancer
Yes
Yes
No
Global / Deployed in multiple regions?
Yes
Traffic Manager + Azure Load Balancer
Internet facing application?
No
Application Gateway
Yes
Global / Deployed in multiple regions?
Yes
Do you require SSL offload or application-layer processing per request?
Yes
Azure Front Door + Application Gateway
No
No
Hosting – PaaS, IaaS, AKS
PaaS
(App Service, Functions)
Azure Front Door
AKS
Azure Front Door + Application Gateway ingress controller
IaaS (VMs)
Azure Front Door + Azure Load Balancer
Yes
Do you require performance acceleration?
No
Application Gateway

Azure traffic manger

- DNS based tarffic load balancer(**Its not recommended for HTTP HTTPS traffic(but you can use it for http https web application) : TCP UDP request**)
- Service permettant de **distribuer le Traffic** **entre les Azure région**
- deploy two Azure virtual machines to two Azure regions, and you create a Traffic Manager profile.

- **If You want to Provide redundancy** to en **app** if an Azure **region fails** you can :
  - deploy two Azure **virtual machines to two Azure regions**, and you **create a Traffic Manager** profile.

- **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. (active /standby , change to other methode for active/active)**
        - **set the monitoring endpoint**
        - **If the endpoint fails, then Traffic Manager will fail over to the secondary**
    - **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 from.
    - **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 Container Instances :

- **Restart policies**
    - **Always**
        - **Restar the Container evrytime the process running exit**
    - **On failure**
        - **Restart the container evrytime the process exit with exit code 0**
    - **Never**
        - **Never Restart the Container**
    - **(afin de chaner la restart policy il faut recrer le container)**

- **Premium SKU Azure Container Registry** :
    - Enable geo-replication for container images. Best practice: Store your container images in Azure Container Registry and geo-replicate the registry to each AKS region. To deploy and run your applications in AKS, you need a way to store and pull the container images. **Container Registry integrates with AKS**, **so it can securely store your container images or Helm charts**. Container Registry **supports multimaster geo-replication to automatically replicate your images to Azure regions** around the world. G**eo-replication is a feature of Premium SKU container registries.**

AKS

- **Azure API Management**

- to manage the **communication between the microservices and the clients** that consume them
- **Azure API Management Premium tier with virtual network connection**

- **AKS Load balance solution**
  - **Application Gateway Ingress Controller**
    - which makes it possible for Azure Kubernetes Service (AKS) customers to leverage Azure's native Application Gateway L7 load-balancer to expose cloud software to the Internet.
      - **Support App Gateay feature:**
      - **URL routing**
      - **Cookie-based affinity**
      - **TLS termination**
      - **End-to-end TLS**
      - **Support for public, private, and hybrid web sites**
      - **Integrated web application firewall**

- Pods are an abstraction of executable code, nodes are abstractions of computer hardware, so the comparison is a bit apples-and-oranges.

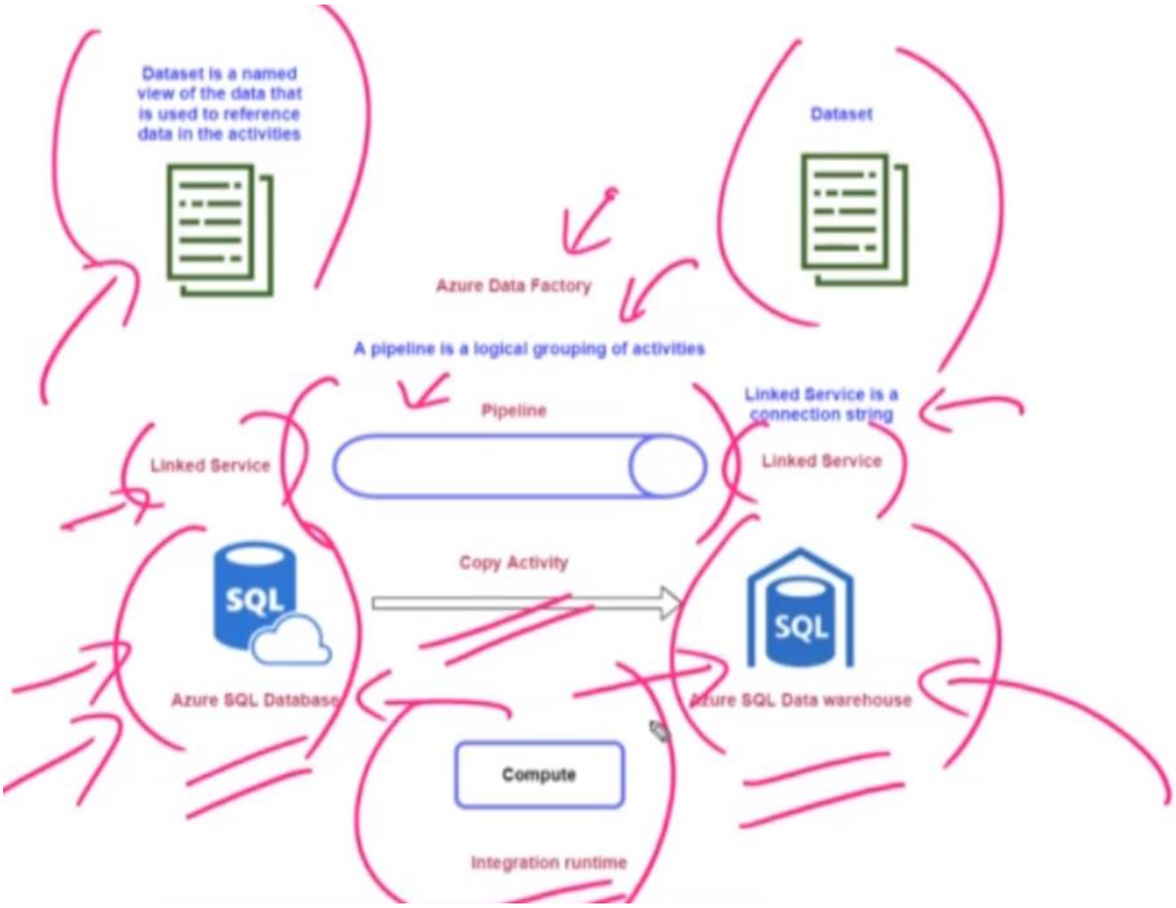
Pods are simply the smallest unit of execution in Kubernetes, consisting of one or more containers, each with one or more application and its binaries.
Nodes are the physical servers or VMs that comprise a Kubernetes Cluster
A Pod always runs on a Node. A Node is a worker machine
in Kubernetes and may be either a virtual or a physical machine, depending on the cluster.

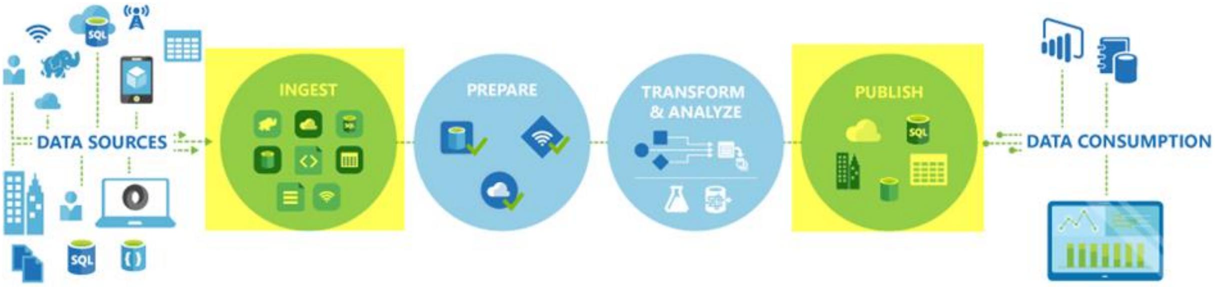
- AKS clusters can scale in one of two ways: *
  - **The "cluster autoscaler" For Windows, "AKS Virtual Nodes" for Linux**
  - watches
    for pods that can't be scheduled on nodes because of resource con straints. The
    cluster then **automatically increases the number of nodes (cont ainer).**

  - The **horizontal pod autoscaler** uses the Metrics Server in a Kubernetes cluster to monitor the resource demand of pods. If an application needs more resources,
    the number of pods is automatically increased to meet the dem and

Storage :

- **Azure Data factory**
  - Cloud based ETL (**Extract transfrom and load your data**)
  - If your file is in **consistent format**, **no ETL is required**. The files **can be copied directly using the AzCopy command.**
  - **Can create data workflow**
  - **Can be used** to **transfer data** from an **on-premise area** **to an Azure storage account.**
  - to **transfer the data (for exemple log)** on a **monthly basis(you can shcedule)** from **Azure Blob storage to an Azure SQL database.**
  - Workflow to orchestrate data movement
  - **Data soruce or destination can be multipe from multipe source of data from azure ,tier or one prem (**[*https://docs.microsoft.com/fr-fr/azure/data-factory/copy-activity-overview*](https://docs.microsoft.com/fr-fr/azure/data-factory/copy-activity-overview) *)*
  - I**f your data store is located inside an on-premises network, an Azure virtual network, or Amazon Virtual Private Cloud, you need to configure a self-hosted integration runtime to connect to it.**
  - Azure Data Factory hosts the runtime engine for **SSIS(SQL server integration service) packages on Azure.**
  - **Linked service :**
    - Connectivity from data source or data destination
  - **Data set :**
    - Represent the data structre within the data store being referenced in the Linked service object
  - **Pipeline** :
    - A pipeline is a logical grouping of activities that together perform a task.
    - **Activity**
      - The activities in a pipeline define actions to perform on your data. For example, you may use a **copy activity** to copy data from SQL Server to an Azure Blob Storage. Then, use a **data flow activity** or a **Databricks Notebook activity** to **process and transform data** from t**he blob storage** to an **Azure Synapse Analytics pool**
-

- 
Dataset is a named view of the data that is used to reference data in the activities
Dataset
Azure Data Factory
A pipeline is a logical grouping of activities
Pipeline
Linked Service is a connection string
Linked Service
Linked Service
Copy Activity
SQL
SQL
Azure SQL Database
Azure SQL Data warehouse
Compute
Integration runtime
-
- **Step** :
  - **Connect** required **data source**
  - **Ingest the data** from the source
  - **Transform** the data if required
  - **Publish the data into destination** like(can be multipe source or data azure ,tier or one prem)   :
    - **Azure Data wareahouse (Azure Synapse Analysis)**
    - **Azure SQL DB**
    - **Azure Cosmis DB**
    - **Azure Data Lake Storage.**



Azure Service Fabric :

- **Microservices architecture**

- Enables you to create Service Fabric clusters **on premises or in Azure** or other clouds.
- Azure Service Fabric is **low-latency** and (**hyper-scale operation)** scales up to thousands of machines.

Traffic Analytics

- Correlate data of network traffic
- Send data to log analytic workspace

cloud-based solution that provides visibility into user and application activity in cloud networks.

Traffic analytics **analyzes Network Watcher, network security group (NSG),**

Azure policy :

- Scope
    - **MG ,Sub, RG**
- **Azure policy for** ensure that the **Azure SQL databases have Transparent Data Encryption (TDE) enabled**
    - **Create an Azure policy** definition that uses the **deployIfNotExists**
    - **Create an Azure policy assignment**
    - **Invoke a remediation task**

- **Effect**
    - **Modify** :
        - Modify is used to add, update, or remove properties or **tags** on a subscription or resource during creation or update
        - **Existing non-compliant** resources **can be remediated** with a **remediation task**

Append:

- used to add additional fields to the requested resource during creation or update. A common example is specifying allowed IPs for a storage resource.
- Append is intended for use with **non-tag properties**.
- The append effect **dont modify** the value but only **add field during the creation** ore update of a ressource
- **Audit**
    - used to create a warning event in the activity log when evaluating a non-compliant rs
- **Deny**
    - Deny is used to prevent a resource request that doesn't match defined standards through a policy definition

Blueprint

- **Scope Creation**
    - **MG ,Sub**
- **Scope Assignemt**
    - **Subcription**

Blueprints remain connected to the deployed resources :

- the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved. This connection supports improved tracking and auditing of deployments. Azure Blueprints can also upgrade several subscriptions at once that are governed by the same blueprint.
- **Setting :**
  - **State**:
    - **Draft**
      - When a blueprint is first created, it's considered to be in Draft mode
      - In drat state the blueprint **cant be assigned**
      - When it's ready to be assigned, it needs to be **Published**.
  - **Artifacts** :
    - Artificat are object in Blueprint
      - **Resource Groups**
      - **ARM template**
      - **Policy Assignment**
      - **Role Assignment**
    - **Artifcats parameter :**
      - **Certain afterfcat requiere parameter that you need to pupulated**
      - **Ex:**
        when you assing a Bluprint with ressourge gr oup you will need to provide the ressource group name if the Rg paramet are not set
- **dependsOn property**
  - **dependsOn** is a string array of artifact names that the particular artifact needs to be created before it's created.

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** :
  - **It can only be associated with a single Azure resource.**
  - 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**
    - **can be shared**. **The same user-assigned managed identity can be associated with more than one Azure resource.**
    - Created as a stand-alone Azure resource
    - Independent life cycle.
    - Must be explicitly deleted.

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 (multi-master)** (Enable/Disbale)
- **Replicate data globaly pane :**

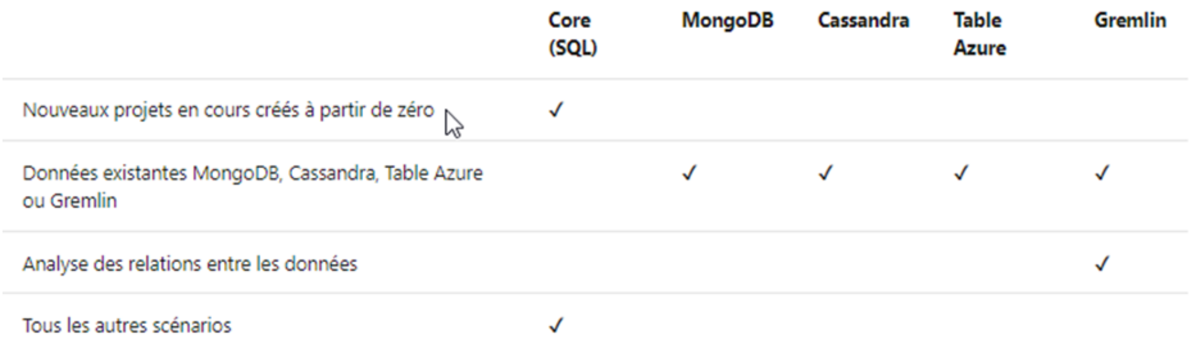
- You can **chose other region** where the data will be **replicated** in a **readable state**
- You can enable **multiple-region write** so you can **write too** on the **replicated region**
- You can **manualy and automaticlay failover**

- **multiple-write** is available on account level not on Database level so if you have **diffrent 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**

- **Configure multi-region writes** in your applications that use Azure Cosmos DB
    - Once an account has been created with multiple write regions enabled, you must 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.**

- **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

- **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 write.** 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 latency**

- ***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 (across region)** that expect **low write latencie**s 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 (you have a defined lag time allowed difference beetween primary region 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 Cosmos DB:**
    - Each partition **across all the regions** is replicated. Each region contains all the data partitions of an Azure Cosmos container and **can serve reads** as well as **serve writes** when **multi-region writes is enabled.**

- Incorrect Answers: B, D: **Storage account or Datalake in GZRS** protects against failures. Geo-redundant storage (with GRS or GZRS)
    - replicates your data to another physical location in the secondary region to protect against regional outages. However, that data is **available to be read only if the customer or Microsoft initiates a failover** from the primary to secondary region.

Azure SQL Database in Active geo-replication

- is designed as a business continuity solution that **lets you perform quick disaster recovery of individual databases in case of a regional disaster** or a large scale outage. Once geo-replication is set up, you can **initiate a geo-failover** to a geo-secondary in a different Azure region. The geo-failover is

initiated programmatically by the application or manually by the user.
Reference

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**
- Lift and shif with Minimal application and datanse changes
- Keep Paas capailiy (auto ptach update backup ha) that **reduces management o**verhead
- **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** indicatin**g unusual and potentially harmful attempt**s to **access or exploit databases.**

Azure SQL Database

- **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**

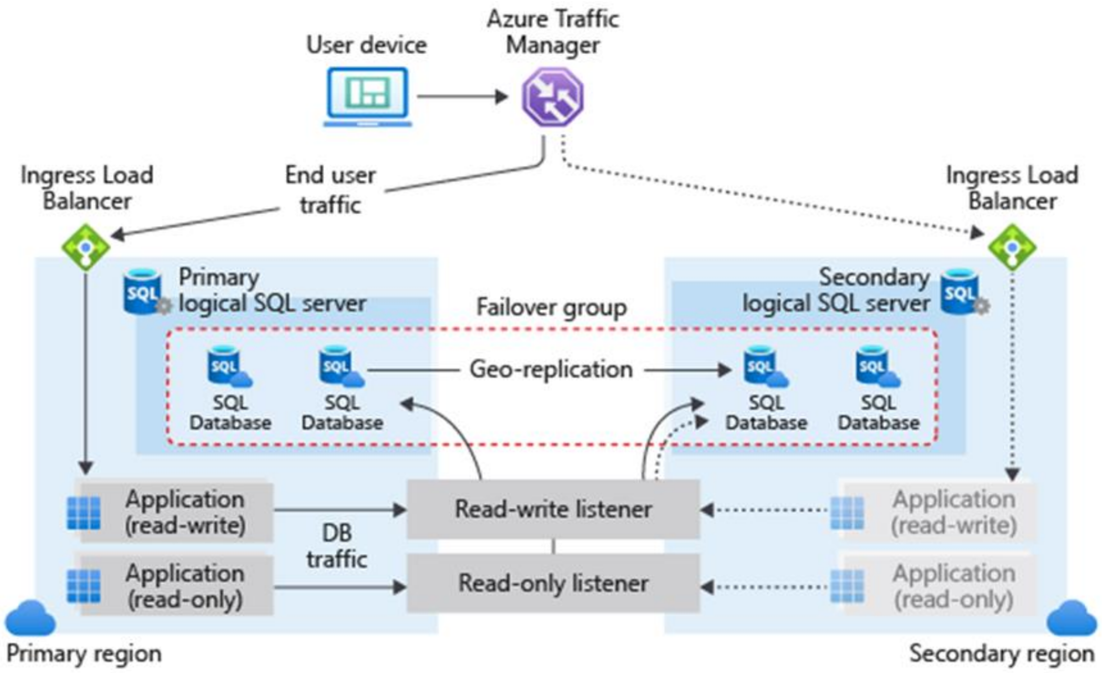
- **Query editor**
    - **Configure the Firewall and virtual network setting**
    - query an Azure SQL Database Step :
    - Go to Query editor pane
    - Establish a connection to the database
        - Even though you're signed into the portal, you still need to provide credentials to access the database (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** :

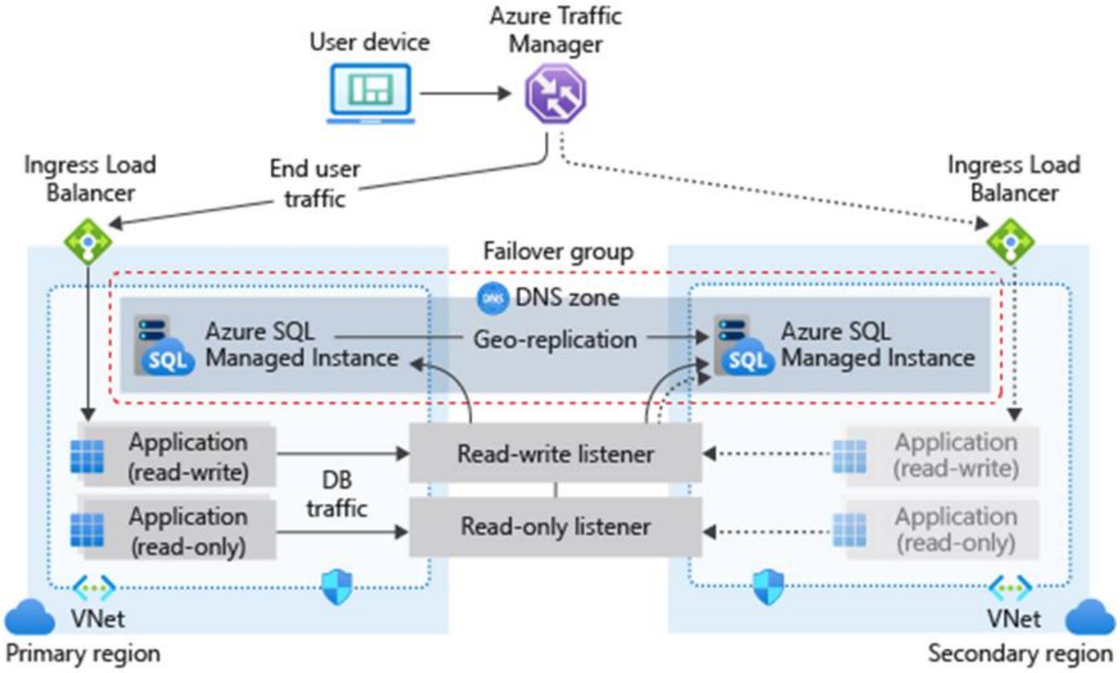
    - **On SQL Server Level**
    - **Replicate a groupe of DB**
    - For **Azure SQL Database and Azure SQL Managed Instance**
    - **Auto failover**
    - The **secondary** SQL DB Server or SQL managed instanc must be in **different regions**
    - To do auto-failover, you must have **primary** and **secondary 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 user**s 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 Managed Instance** / SQL **Azure SQL Database**
    - **SQL Auto Failover group** :
        - Supports multiple automatically **replicated instances across Azure regions**
    - Azure SQL Managed instances & Auto Failover Group - **supports User Initiated Backups** and **minimizes administrative effort for business continuity**
    - **Online Migration :**

        - If Minimize downtime required, needs to be an online migration.
        - For online migrations from SQL Server to SQL Managed Instance using Azure Database Migration Service, you must provide the full database backup and subsequent log backups in the SMB network share that the service can use to migrate your databases
        - When configuring the migration, you **need to select** the **Azure Storage Account** that DMS can upload the backup files from the SMB network share to and use for database migration
        - **Managed instance** db **size max** : limit is 2-**8TB max.**
        - **Azure SQL Database** size max is **100 TB with Hyperscale** service tier model

    - **Server-side transaction Transactions acroos DB**

(Transaction cross multiple database)

    - **Supported:**
        - **The Azure SQL datbase are on the same Azure SQL Server**
        - **In or different Azure SQL Server (in this case you will need create link beetween server)**
        - **On the same 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**

SQL Managed instance tiers :

- General purpose: Designed for applications with typical performance and I/O latency requirements.
- **Business critical:** Designed for applications with **low I/O latency** requirements and minimal impact of underlying maintenance operations on the workload.

Azure SQL Database Service tier :

- **vCore tiers** allow serverless and **auto-pause,** which matches perfect to "only used first day of month". Rest of the month, the service is paused and does not generate compute costs. **Azure automatically pauses and resumes** the database based on workload activity **During the pause period, Azure does not charge you for the compute resources**

- In DTU service tier, you need to add min. 100 DTUs to get possibility for 400GB DB size. Below you only have 250GB.

- **Database Business Critical :**

        - **The primary node constantly pushes changes to the secondary nodes** in order and **ensures that the data is persisted to at least one secondary replica** before committing each transaction. This process **guarantees that if the primary node crashes for any reason, there is always a fully synchronized node to fail over to.**
- **Premium :**
    - **Allow Azure Avaibilty zone**
- **Hyperscale :**
    - **(support up to 100TB).**
    - **Suppot scaling compute resources up and down based on your workload requirements.**
    - **Azure SQL Database Hyperscale :**
        - Azure SQL Database Hyperscale is a highly scalable service tier that is designed to provide high performance, and supports **up to 100 TB of data.**
        - provides high throughput and performance, as well as r**apid scaling to adapt to the workload requirements**. Connectivity, **query processing**, database engine features, etc. work like any other database in Azure SQL Database.
    -

Long-term retention policy (LTR) :

- to automatically r**etain the database backups** in separate **Azure Blob storage** containers for **up to 10 years.**

Database Migration :

- **Azure Database Migration Service**
    - Its is a fully managed service designed to enable seamless **migrations from multiple database sources to Azure Managed Instrance** data platforms with **minimal downtime**
- **Data Migration Assistant**
    - **For migrate SQL Databse to Azure SQL Database**
    - 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.
- **Azure CosmosDB Data Migration tool**
    - **For migrate SQL Databse to Azure Cosmoss DB**
- **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

Azure Logic App:

- For **allow to handle high load**
    - In **Worklow Setting** enable : High troughpout

Microsoft identity platform Endpoint meaning :

- **Managed identities** provide an identity for applications to use when connecting to **Azure resources that support Azure Active Directory (Azure AD) authentication (Storage account, keyvault etc...)** . Applications may use the managed identity to **obtain Azure AD tokens**

Asynchronous messaging option :

- **Azure Servcie bus Qeu:**
    - well suited for transferring commands from **producers to consumers**. **Data is transferred** between different applications and services using messages. A message is a container decorated with metadata, and contains data. The data can be any kind of information, including structured data encoded with the common formats such as the following ones: JSON, **XML,** Apache Avro, Plain Text.
    - process **asynchronously**
    - recommend a solution to process the messages by using a First in. First out (FIFO) pattern
        - **Azure Service Bus queues** with **sessions enabled**
            - Azure Service Bus supports a FIFO pattern through the use of sessions. A session is a sequence of ordered messages. All messages in a session are handled in the order they arrive. This ensures that messages are processed in the order they were added to the queue.

            Asur sevruc bus queue :

            - A queue allows processing of a message by a single consumer.

            Azure service bus topic :

            - In contrast to queues, topics and subscriptions provide a **one-to-many** form of communication in a publish and subscribe pattern

- EventGrid
- EventBus

Azure CycleCloud :

- an enterprise-friendly **tool for orchestrating and managing High Performance Computing (HPC)** environments on Azure. With CycleCloud, users can provision infrastructure for HPC systems, deploy familiar HPC schedulers

Azure Function :

- **code / Logic App use workflow**
- **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.
        - **VNET ingetrgation private endpoint**

- **Migration** efforts based on Azure Cloud Adoption Framework include the incremental approaches to the workloads. Each migration iteration is a batch of migration waves - the smallest workload that produces tangible results. Usually, the iteration consists of the **three phases:**

    - **Assess workloads** - these workloads help to evaluate costs, architecture, and deployment tools.
    - **Deploy workloads** - these workloads replicate the current functionality in a cloud using lift and shift, lift, and optimize approaches.
    - **Release workloads** - these workloads provide test, optimization, documentation, and release of the cloud migration efforts.

Web APP :

- **Azure Web App can write Application event log**
- **can read/write files to local file system**
- **is less expansive that a VM scale set**
- **Azure App Service supports AAD authentication to app users**
-
- App service have **already local storage storage accout is not a must** for web site content stirage
- **Deployment slots:**

  . Deployment slots are live apps with their own host names. App content and configurations elements can be swapped between two deployment slots, including the production slot. Deploying your application to a non-production slot has the following benefits: * You can validate app changes in a staging deployment slot before swapping it with the production slot

SSO method :

- **Password-based**

Azure Virtual WAN :

- Basic : it can connect to only site to site VPN,
- **Standard: to connect to Express route it needs to be upgraded to standard.**

BGP (Border Gateway Protocol can do) :

- Routing **from the virtual networks to the on-premises location** :
  - BGP is a dynamic routing protocol that enables automatic route updates between ExpressRoute circuits and the on-premises sites.
- The **automatic routing configuration following a failover :**
  - It can dynamically detect when a site fails and automatically reroute traffic to the other available site.

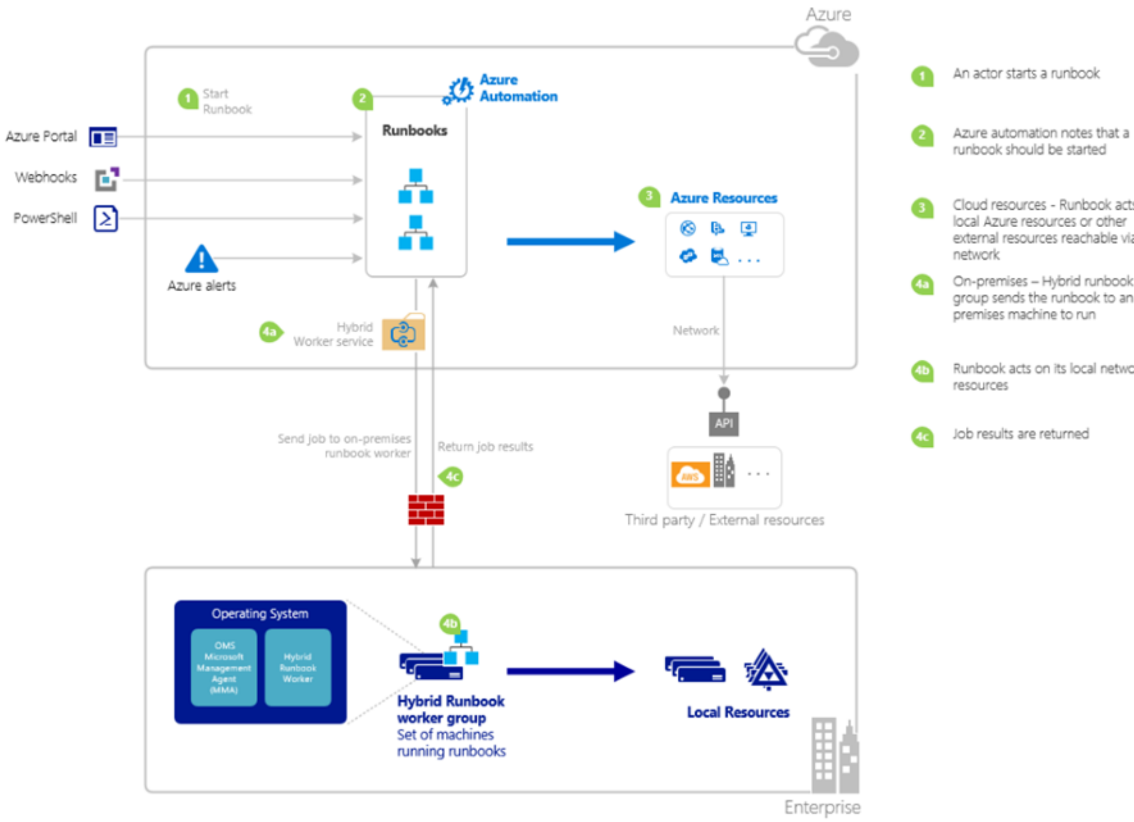
Azure monitor :

- **Configure rule and alerte group**
  - You can kep the s**ame action group** for **multipe alerte rule** (ex, **3 rule , 1 action group**)

Azure Bach :

- **rendering of images for 3D scenes,**
- **Enable parallel task execution on compute nodes**

- **Azure Automation runbook**
  - **For exemple Can be used in action group to atomaticaly start and sto Virtual Desktop based on business hours**
  - 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
  -

- 
Azure
Start Runbook
Azure Automation
Runbooks
Azure Portal
Webhooks
PowerShell
Azure alerts
Hybrid Worker service
Azure Resources
Network
API
Third party / External resources
Send job to on-premises runbook worker
Return job results
Operating System
OMS Microsoft Management Agent (MMA)
Hybrid Runbook Worker
Hybrid Runbook worker group
Set of machines running runbooks
Local Resources
Enterprise
1 An actor starts a runbook
2 Azure automation notes that a runbook should be started
3 Cloud resources - Runbook acts local Azure resources or other external resources reachable via network
4a On-premises – Hybrid runbook group sends the runbook to an premises machine to run
4b Runbook acts on its local netwo resources
4c Job results are returned

-

o

- ,**Azure Time Series Insights :**
  performs the roles of stream processing, data store, and analytics and reporting. It accepts streaming data from either **IoT Hub** or Event Hubs and stores, processes, analyzes
- **Azure Datalake**
  - Data of datalake data **can be load directly** to **Azure Synapse Analytics SQL**
- Azure AD **Identy protection** :
  - Detect risks
  - Force MFA registration :
    - **Force** selected user or group
      to **register** for **MFA authentificatoon**

Entreprise Application :

- After the App have been **registred** a Object
  in **Entreprise Application** is **created**
- The object created referencing the **entreprise app** is caled a **service principal (for App)**
  - **RBAC Role** :
    - You
      can then assing **RBAC role** to the **Service princpal** created
      to access other Az ressource like **Keyvault** **(like for MI in VM or other Rssrce)**

ACCEUIL OPEN –6EM recuper badge