Azure Activity Log :

- **Can connect** to **l**og analytic workspace
- **Can enable diagnostic setting like VM (SA, LaWorkspace, event hub)**

Azure monitor :

- **Service health pane :**

get status of functionality on Azure Service

  - **Security adivosry pane**

Azure monitor alerte :

- **Target Resource** - Defines the scope and signals available for alerting.
  - A target can be any Azure resource. Example targets:
    - Virtual machines.
    - Storage accounts.
    - **Log Analytics workspace**.
    - Application Insights.
    - **Subcription**
- **Signal** -
  - Emitted by the target resource. Signals can be of the following types: **metric**, **activity log**, Application Insights, and **Log (is selected Log analtytic workspace**.
- **Log analytic query**
  - **You can use query that ask a gorupe of Az VM so you can create 1 alert rule for multipe VM event**

Service healt alerte :

- Service health notifications are stored in the **Azure activity log**
- there is a separate user interface (**Sevice healt alert pane**) to make it easier to view and set up alerts on service health notification (instead of create a alert on subcription based on siganl type (activity log)

Database Monitor :

- Query Performance Insight
  - provides intelligent query analysis for single and pooled databases. It helps **identify** thening **top resource consuming and long-run queries i**n your workload
- Azure SQL Database Auditing
  - You can enable auditing in your DB Service

- **Enable Auditing for your SQL DB**
  - Storage location for the audit must be in the **same region** as the SQLSevr

- **You can send diagnostic log (SQL Insight, VM) to :**
  - **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)**

Automatic tuning :

- to improve the **performance of SQL DB**
- intelligent performance service that uses built-in intelligence to continuously monitor queries executed on a database, and it automatically improves their performance.

Power bi :

- To perfom **real time reporting from data send to log analytic workspae**:
  - Use E**vent Hubs, Stream Analytics**, and **Power BI** to transform your diagnostics data into near real-time insights on your Azure services."

SQL Analytics :

- Data streamed to a Log Analytics workspace can be consumed by SQL Analytics. SQL Analytics is a cloud only monitoring solution that provides intelligent monitoring of your databases that includes performance reports, alerts, and mitigation recommendations

Azure AD monitoring

- AAD => Monitioring =>**Diagnositc setting**
  - **Add diagnostic setting (like VM or SQL DB)**
    - **Select the log type**
      - **Audit log**
      - **Sign in log**
      - **Etc**
    - **Select the destination**
      - **Log an workspace**

- **Sto Account**
- **Event hub**

Azure Monitor Alerte :

- **Metric : ressource usage (disk, ram , cpu , Iops)**

- **Treshold**
  - **Static**
  - **Dynamic**
    - based on **historic usage patterns.**

Azure Service Map

- **Vizualise relationship** beetween app componnement

App insight :

automatically detect performance anomalies, and includes powerful analytics tools to help you diagnose issues and to understand what users actually do with your app.

track requests and exceptions to specific lines of code within the application

- **App Insights feature :**
  - **Users, Sessions, and Events**
    - Users tool: How many people used your app and its features.
    - Sessions tool: How many sessions of user activity have included certain pages and features of your app
    - Events tool: How often certain pages and features of your app are used
  - **Funnel feature**
    - If your application involves multiple stages, you need to know if most **customers are progressing through** **the entire process**, or if they are ending the process at some point. The progression through a **series of steps** in a web application is known as a funnel.
    - You can use Azure Application Insights Funnels to gain insights into your users, and monitor step-by-step conversion rates.
  - **Cohort**
    - A cohort is a **set of users, sessions, events**, or operations that have **something in common.**
  - **Impact**
    - Impact **analyzes** how **load times** and other properties influence **conversion rates** for various parts of your app
  - **Retention**
    - The retention feature in Azure Application Insights helps you analyze **how** **many users return** to your a

pp, and how often they **perform particular tasks** or achieve goals

- **User Flows**
  - The User Flows **tool visualizes** how users **navigate** between **the pages** and **features** of your site.
    - How do users navigate away from a page on your site?
    - What do **users click on a page** on your site?
    - Where are the places that **users churn most** from your site?
    - Are there places where users repeat the **same action over and over?**
- **Continuous export**
  - **The events** you see in the Application Insights portal **can be exported** to **storage** in Microsoft Azure in **JSON format**. From there, you can download your data and write whatever code you need to process it.
  - **Continuous export is supported for Azure Storage accounts.**

IT Service Management Connector

- **IT Service Management Connector (ITSMC) allows you to connect Azure to a supported IT Service Management (ITSM) product or service. (Sysetem center One-premises)**
- **With ITSMC, you can create work items in ITSM tool, based on your Azure alerts (metric alerts, Activity Log alerts and Log Analytics alerts).**
- **ITSMC provides a bi-directional connection between Azure and ITSM tools to help you resolve issues faster**

- **Azure Hybrid Benefit**
  - allows you to use your **on-premises Windows Server licenses** and run Windows virtual machines on Azure at a **reduced cost.**
- **Azure Reserved VM Instances**
  - you r**eserve virtual machines in advance** and **save up to 80 percent.**
  - **Select a term for 1 or 3 year and billing frequency Monthly**
- **Stop VM after buget limit target**:
  - Create **buget alert** :
  - 1. Azure Monitor > Alerts > Manage Actions > create action groups with action type "Automation Runbook" > stop VM
    2. Create budgets scoped by the resource groups > in the alert section choose the previously created **action groups.**

Template :

- **Deploy with keyvault secret for password :**
  - Set the **--enabled-for-template-deployment** to **true** creating the key vault
  - 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.**

- **Azure Key Vault :**

- **Secret**
  - **Mot de passe**
- **Key**
  - **Can use for digitally sign blobs** in an Azure storage account
  - **Sign encrypt the operating system** disks and data disks of the virtual machine
- **Certificat**
  - **CA for SSL etc , authentication**

- Sku
  - **Standard**
    - Geo Aval
  - **Premmium** (**premium is the max)**
    - Geo Aval

        - HSM (Hardware Security Modules)
  - Advise :
    - **You can increase the number of keyvault to ensure the various applications can distribute their requests across them**
  - **Backup and restore :**
    - **A backup taken** of a key from a **key vault** in one Azure region **can be restore**d to a key vault in another Azure region, as long as both of these conditions are true:
      - Both of the Azure regions belong to **the same geography.**
      - Both of the key vaults belong to the **same Azure subscription.**
    -

Storage :

(app insigh) Continuous export is supported for Azure Storage accounts.

  - **Storage type Acces Autorisation**
    - **Anonymous read: Only blob**
    - **Azure AD : Blob, Queues (Azure file with Azure AD DS)**
    - **SAS : All exept Azure FIle (but required for Az copy)**
    - **Shared key : All**

Storage tiering :

- General Purpose V2
- Blob storage accounts.

  - in **archive** access tier, **you can get the file back within 15 hours.**
  - Access tier can be set **on container or data level**

Access data cost is minimum for

- **Access tier:**
  i. **Hot Tier: Frequent reads**
     - **Lower data access costs**
     - **Higher data storage costs**
  ii. **Cool Tier: Accessed less frequently**
     - **Higher data access costs**
     - **Lower data storage costs**
     - **Optimized for data that's stored 30 days**
  iii. **Archive Tier: Take hours to get data available**
     - **Even Highest data access cost**
     - **Lowest data storage cost**

        - **Optimized for data that's stored 180 days**

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

- **Access policy :**

    - **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 pol icy**
    - **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)
    -
- **Container Access level :**
        - **private non anonymous access**
        - **Anonymous read acces container**
        - **Anonymous read acces blob**

- **Stored access policy :**

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

Encryption :

  - Data in a new storage account is encrypted with Microsoft-managed keys by default.
  - you can **only manage encryption with your own keys** for these following services :
    - **Blob storage, Azure Files**
    - **Azure Key Vault must be in the same region as the SA**

VPN

- **Point to site**
  - **Certificat based auth**
    - **One user laptop**
      - Trusted Root Certification Authorities certificate store
        - **Root CA with public key**
      - Personal store
        - **User Certificate with private key**
    - **Azure VPN Gateway :**
      - **Root CA with public key**

When you create VPN (VNET VNET, P2S S2S) you need o create a new subet (azurebastionsubnet, firewall subnet)on the vnet for implement it **at leats /28**

Force tunnelign :

Force tunneling :

- Forced tunneling lets you redirect or "force" all **Internet-bound traffic back to your on-premises location** via a Site-to-Site VPN tunnel for inspection and auditing. This is a critical security requirement for most enterprise IT policies.
- Without forced tunneling, Internet-bound traffic from your VMs in Azure will always traverse from Azure network infrastructure directly out to the Internet, without the option to allow you to inspect or audit the traffic.
- Flow ;
  - **Create route table** en create a defaut route to root all traffic 0000/0 to "VirtualNetworkGateway"
  - Associate the roote table to the VNET
  - Carte a Virtual network gateway
  - Create a local Netwrok gateway Objetc and associate it with the VNET with the -GatewayDefaultSite parameter
  - Create the S2S Connection

- **If you use a VNETGetway Type Expresse route you must use BGP**

BGP :

- ExpressRoute: You must use BGP to advertise on-premises routes to the Microsoft Edge router. **You cannot create user-defined routes to force traffic to the ExpressRoute virtual network gateway if you deploy a virtual network gateway deployed as type: ExpressRoute**. You can use user-defined routes for forcing traffic from the Express Route to, for example, a Network Virtual Appliance

https://docs.microsoft.com/en-us/azure/vpn-gateway/bgp-howto

- **Microsoft does not support any router redundancy protocols (for example, HSRP, VRRP)** for **high availability configurations**. We rely on a **redundant pair of BGP sessions** per peering for high availability.

Express Route :

- **Redundant :**
  - **Each ExpressRoute** circuit has a **redundant pair of cross connections configured** to provide **high availability.**
- **BGP :**
  - **Routing to the closet available**
  - **Automatic routing configuration**

Access review :

- **P2**
- **User type**
  - **User**
  - **Guest**
  - **Service (managed identity)**

- **Identitdy governance :**
  - **Review group membershib**
  - **Review App assignement**

- **PIM/Identitdy governance**
  - **Review AAD Role**
  - **Review ARM Role**

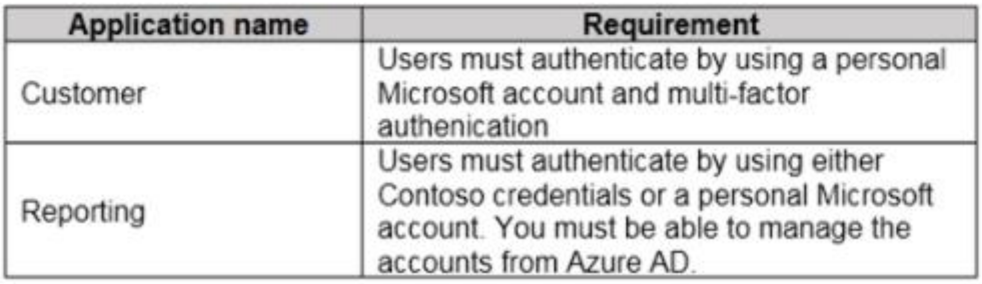
- **Setting**
  - **Reviewer (person who do the review allow deny)**
  - **Frenqueny (when the review is done, monthly , weekly email will be send)**

App Service

App Service Plan

- Create and configure App Service plan
  - Choose between **Linux** and **Windows OS**
  - you can deploy **container-based applications**
  - 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



Application name	Requirement
Customer	Users must authenticate by using a personal Microsoft account and multi-factor authenication
Reporting	Users must authenticate by using either Contoso credentials or a personal Microsoft account. You must be able to manage the accounts from Azure AD.

Box 1: **B2C**

- **personal accounts** are obviously supported, also enable B2C for **MFA** seems possible,
- AAD v1 or v2 requires premium P1 license to enable MFA, we have only Basic (https://docs.microsoft.com/en-us/azure/active-directory-b2c/multi-factor-authentication?pivots=b2c-user-flow)

Box 2: **AAD v2.0**

- v1.0 does not support personal accounts, v2 - does.
- At the same time, integrating internal Contoso accounts to B2C would be more difficult.
- B2C local accounts can't be named as Contoso accounts, as there would be limited use of these accounts when managing Azure, or other usually internal services

Azure AD App Registration Pane :

- Pane where you can enable **AAD authentification** for **your app** and enable **SSO**
- **You can configure App registration for enable multitenant for un single App**

  - **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**

Azure App registration 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 (with this iption in App Registration user from other Tenant can sign to this App no need guest)**
    - **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**
    - **Azure AD only Multi-tenant**
    - Select this option to **target the widest set of customers.**
    - **Azure AD multi-tenant and personal Microsoft accounts.**

- **Personal Microsft accounts only**

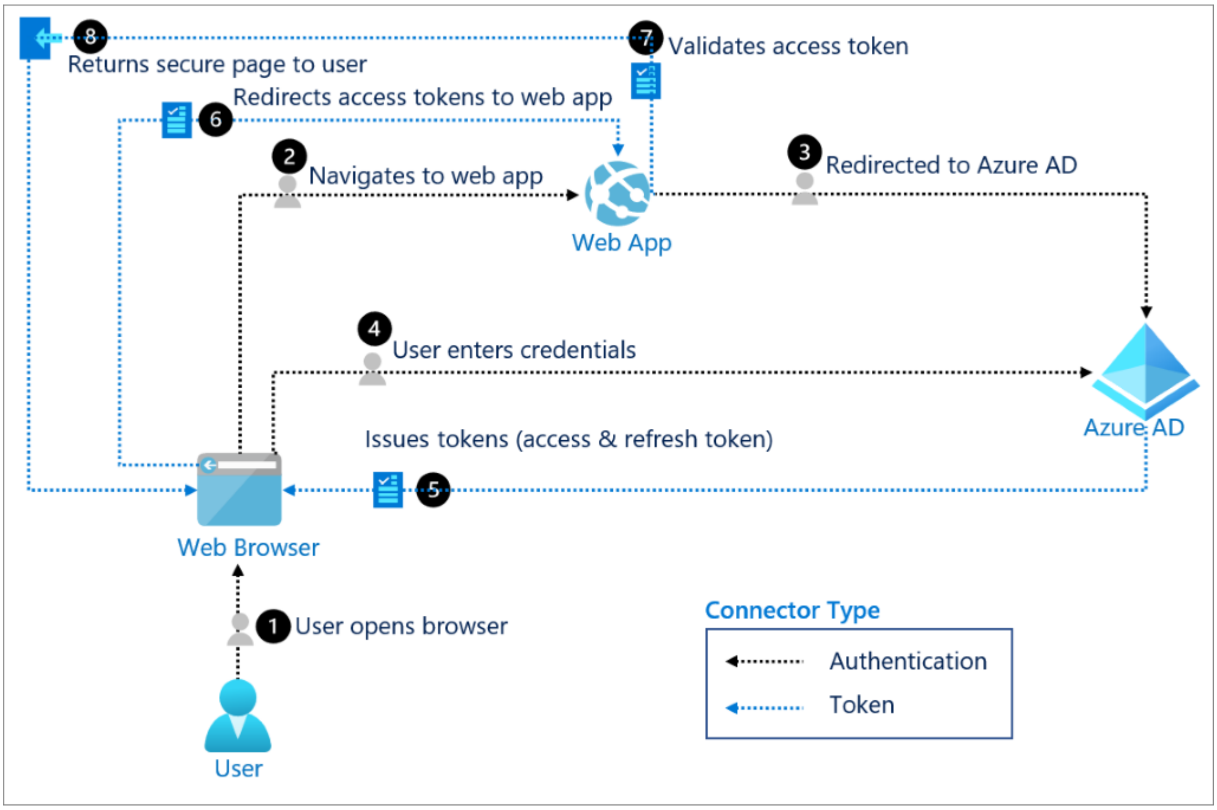
For connect your App to your **Registered App object**

- you **need to copy** your **Application code** the :
    - **Application ID:** A unique identifier assigned by the Microsoft identity platform.
    - **Application Secret :** A password or a public/private key pair that your app uses to authenticate with the Microsoft identity platform.

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 registred)**
    - **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)**
- Use case :
    - A app can then get sql dp password from keyvault in the code

Authentification OAuth 2,0 avec Azure Active Directory :



User -> webb app -> rediret Azure AD auth

User -> puth credentiel

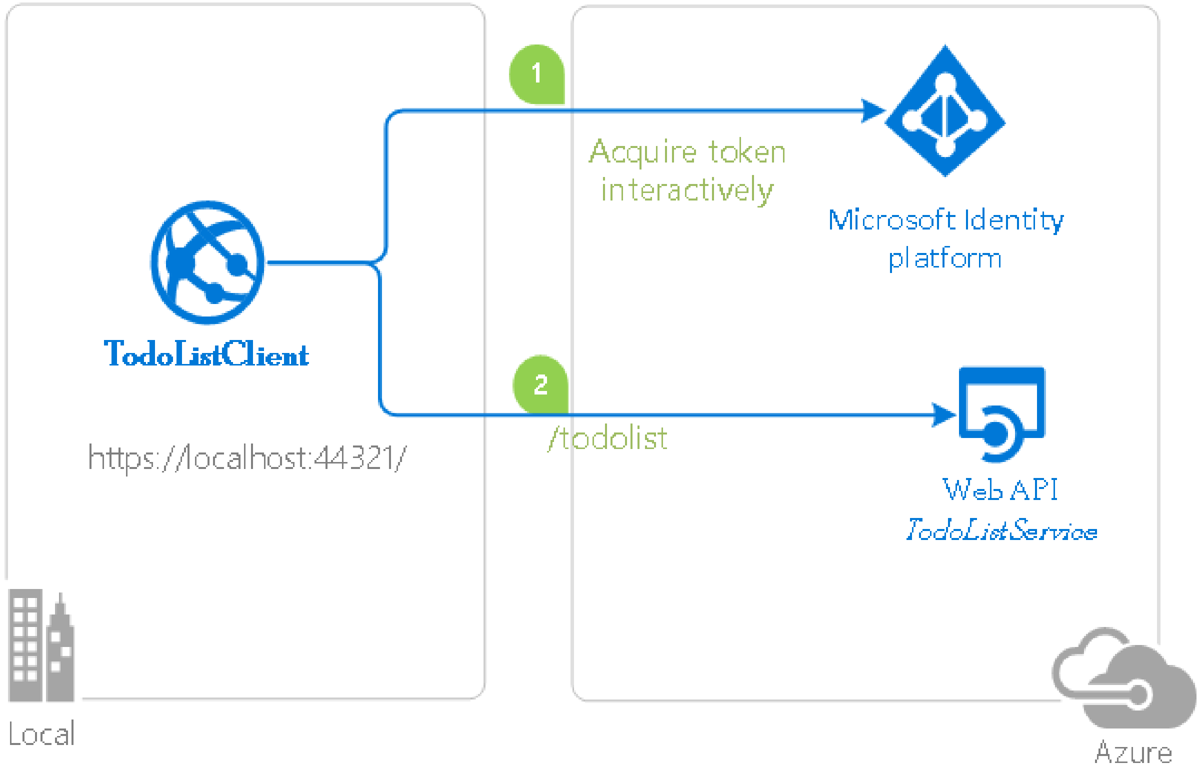
AzureAD=> Give token

Web API -> authorize make the authorization decisions

Policy => Api management

Protect a web API backend

https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad



- 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 to validate the OAuth token** for every incoming request.

Azure AD Application Proxy :

- **on-premises legacy** applications **published for cloud access**
- Application Proxy is a feature of Azure AD that enables users to **access on-premises web applications from a remote client**. Application Proxy includes both the Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server.

Managed identity :

- **VM with MI enabled can access Keyvault, Azure SQL, Cosmos DB with RBAC Authaurization type.**

- **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 policy :

- Scope
    - **MG ,Sub, RG**

- **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

You can get the ARM templates of a ressource and. Then you can use the templates in Azure Blueprints to deploy the same ressource across multiple Azure subscriptions.

- **Assignement Scope**
    - **MG ,Sub**

- **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 group 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.

Blue print definition

- When **creating a blueprint definition**, you'll **define where the blueprint is saved.** Blueprints **can be saved to a management group or subscription** that you have **Contributor** access to.

- **Blue print Assingment**

    - If the **location is defined in a management group**,
      the **blueprint is available to assign to any child subscription or MG of that management group.**

Blueprint Locking modes :

- Locking mode are applied on artifact and **dont inherit like ressource lock lock(Template, RG, RBAC, Policy**)
  - **Don't Lock**
  - **Read Only one RG artificat**
    - The resource group is read only and **tags on the resource group can't be modified**.
    - **Not Locked** resources can be added, moved, changed, or deleted from this **resource group(if applied on RG artifact)**.
  - **Read Only**,
    - The resource **can't be altered** in any way. No changes and it **can't be deleted.**
  - **Do Not Delete**
    - The resources **can be altered**, but **can't be deleted**.
    - **Not Locked** resources can be added, moved, changed, or deleted from this **resource group (if applied on RG artifact)**

An Azure RBAC deny assignments deny action is applied to artifact resources during assignment of a blueprint if the assignment selected the **Read Only** or **Do Not Delete** option. The deny action is added by the managed identity of the blueprint assignment and can only be removed from the artifact resources by the same managed identity. This security measure enforces the locking mechanism and **prevents removing the blueprint lock outside Azure Blueprints** for **any user even the Owner of subcription.**

Management group :

- Management group arboresence **cant** be associated in **multiple AAD Tenant**
  - So if multiple tenant => Multiple Root Management group

____

IdFix :

- identifies errors such as **duplicates and formatting problems** in your **Active Directory Domai**n Services (AD DS) domain before you **synchronize to Azure AD.**

Azure AD Connect Health :

- You **can configure** the Azure AD Connect Health service to **send email notifications when alerts indicate that your identity infrastructure is not healthy.**

Azure AD Domain service

- provides managed domain services such as **domain join**, group policy, LDAP, Kerberos/NTLM authentication that is fully compatible with Windows Server Active Directory
- **Azure file Azure AD user authentification**

AKS

- **AKS Load balance solution**
  - **Application gatewayer ingress controller**
  - **Frond Door**

- **Virtual nodes with Virtual Kubelet ACI** :
  - To **rapidly scale application workloads** in an AKS cluster, you can use virtual nodes

ACI :

- has networking controls (public, private)
- **supports Restart policies set to "OnFailure" by default.**
- **Minimized cost compared to AKS**

Container :

- **Modernized approach** for application **development and deployment** is to use **container-based technologies**
- Ideal deployment strategy is to use Azure container services

Azure Container registry :

Pricing tier :

- **Basic/ Standard**
  - Azure Active Directory authentication integration, image deletion, and webhooks
- **Premium**
  - **Geo-replication**
    - for managing a **single registry across multiple regions**
  - **private link with private endpoints**
    - to restrict access to the registry.

- **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**

Azure Instance Metadata Service MDS

- is a **REST API provides information** about currently **running virtual machine** instances(**Auth token, 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

---

- **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
- Network Subscription Limits
- Role Based Access Control
- In Portal you can search for Network Watcher and enable it on VMs
  - Network Performance Monitor
    - E.g. top network health events, ExpressRoute monitor, service endpoint monitor, performance monitor
    - It ties in logs/metrics with Log Analytics.
    - Part of Insights & Analytics Azure management solution.
    - Works with installing Microsoft Monitoring Agent (MMA) in VM.
    - Flow
    - Deploy Insight & Analytics and then select Network Performance Monitor
    - Choose VM and click on "Connect", it'll install MicrosoftMonitoringAgent

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), flow logs to provide insights into traffic flow in your Azure cloud. With traffic analytics, you can:
- Visualize network activity
- Identify security threats to, and secure your network, with information such as open-ports, applications attempting internet access, and virtual machines (VM) connecting to rogue networks.
- Understand traffic flow patterns across Azure regions and the internet to optimize your network deployment for performance and capacity.

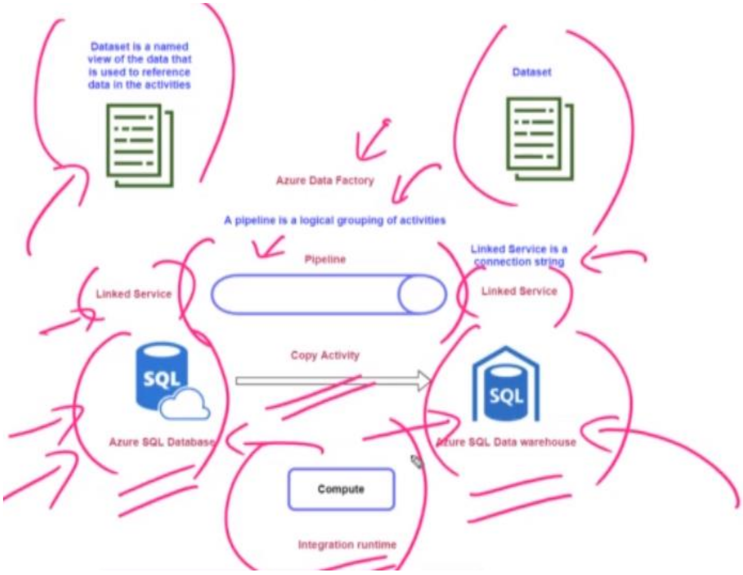
- **Pinpoint network misconfigurations leading to failed connections in your network.**

Storage :

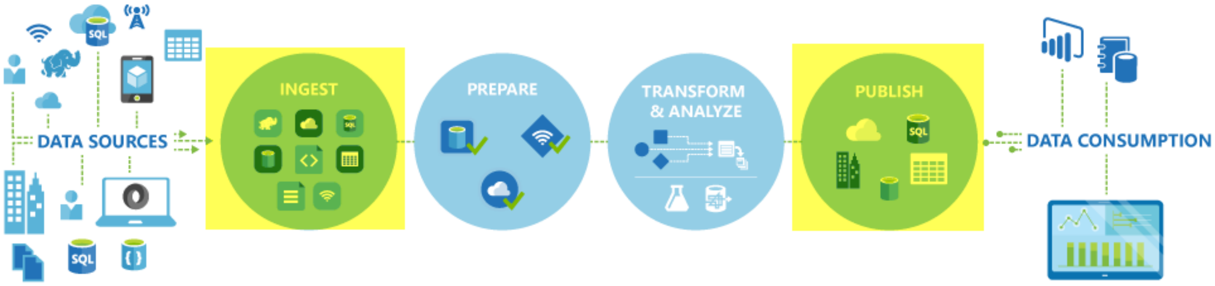
- **Azure Data factory**
  - Cloud based ETL (**Extract transfrom and load your data**)
  - For cloud and hybrid environnement
  - If your file is in **consistent format**, **no ETL is required**. The files **can be copied directly using the AzCopy command.**
  - **Can create data workflow**
  - **Can be used** to **transfer data** from an **on-premise area to an Azure storage account.**
  - to **transfer the data** 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*)
  - 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.**

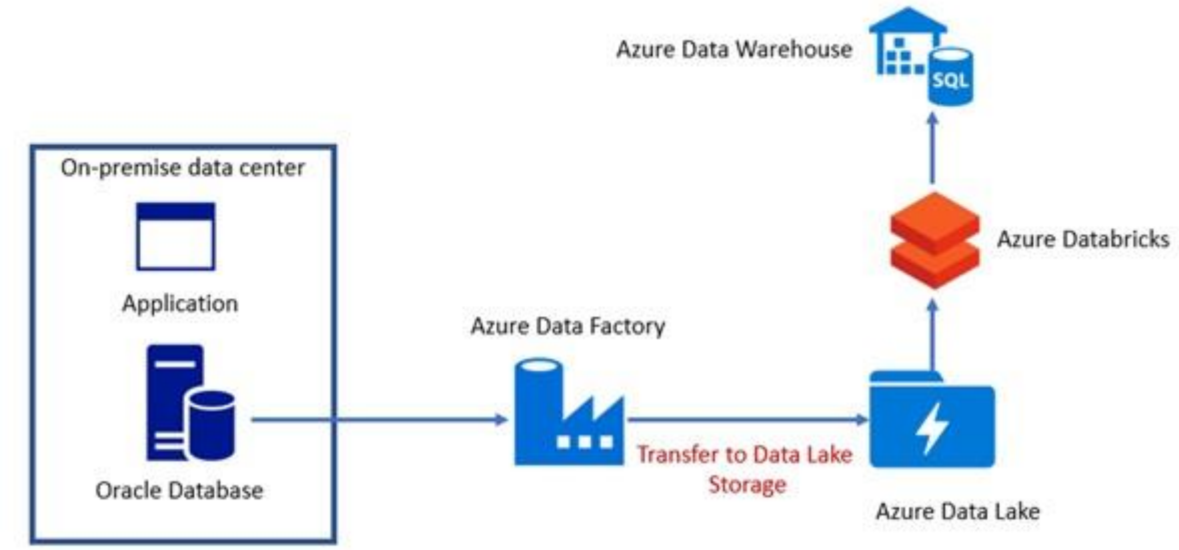
  - **Linked service :**
    - Connectivity from data source or data destination
  - **Data set :**
    - Represent the data structre within the data store being referenced in the Linked service object
    - There is source and output dataset for the source and destination
  - **Pipeline** :
    - A pipeline 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**

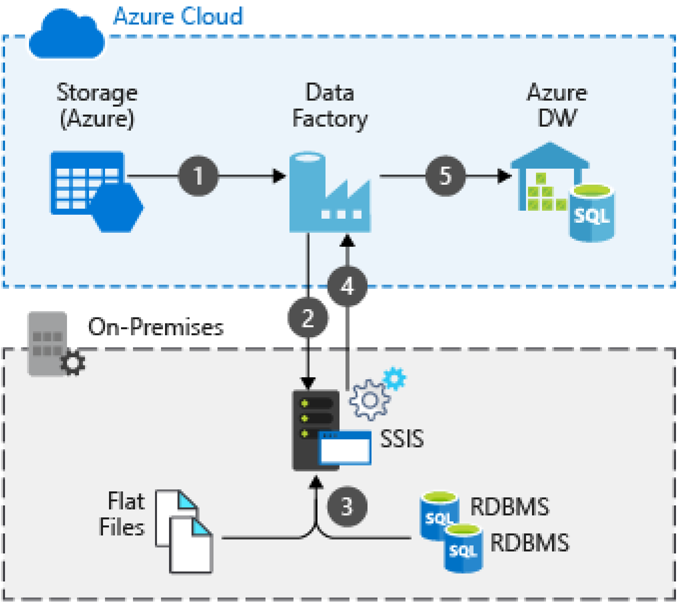
and transform data from t**he blob storage** to an **Azure Synapse Analytics pool**

- 
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.**







Even HBub :

Send event to Event HuB from Application :

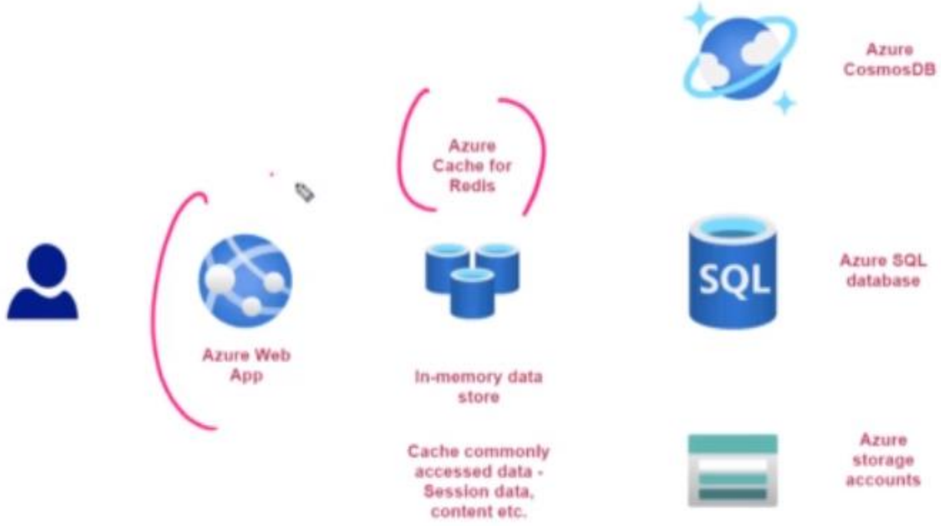
- **AMQP Protocol**
  - If we send **many events & throughput** is a concern: use **AMQP**.
  - Compared to HTTP, AMQP is **easy to scale.**
- **HTTP/REST**
  - If we send **few events** and **latency** is a concern: use **HTTP / REST.**

Web App :

- **Support :**

    - **read and write to the local file system**
    - **write to the Windows Application event log**

Azure Redis Cache :

- **Store frequent acccess data closest to the application in a cache** to **improve the performance** (CDN closest tu user)
- Data from :
    - **Azure cosmsos DB**
    - **SQL Database**
    - **Storage account**
    - 

Accelerated Networking

- Accelerated networking enables single root I/O virtualization (SR-IOV) to a **VM,** greatly **improving its networking performance**
    - enables **single root I/O virtualization (SR-IOV)** to a VM (**improving its networking performance**)
- **Supported on** :
    - D/DSv2 , **F/Fs**, D/Dsv3, E/Esv3, Fsv2, Lsv2, Ms/Mms and Ms/Mmsv2.
-
-

Azure Content Delivery Network :

- https://www.udemy.com/course/exam-az-microsoft-azure-exam-role1/learn/lecture/17563312#overview
- (when a **first user in a region make a request** to the APP ,
  the **CDN will find the closest edges server** and will **cache** the
  app response in it, then other request to the app
  in this region will be send to these **edges server with minmal latency**)

- 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**

Autorisation methode :

- Keyvault : RBAC
- Azure SQL Rbac
- Cosmis DB HMAC

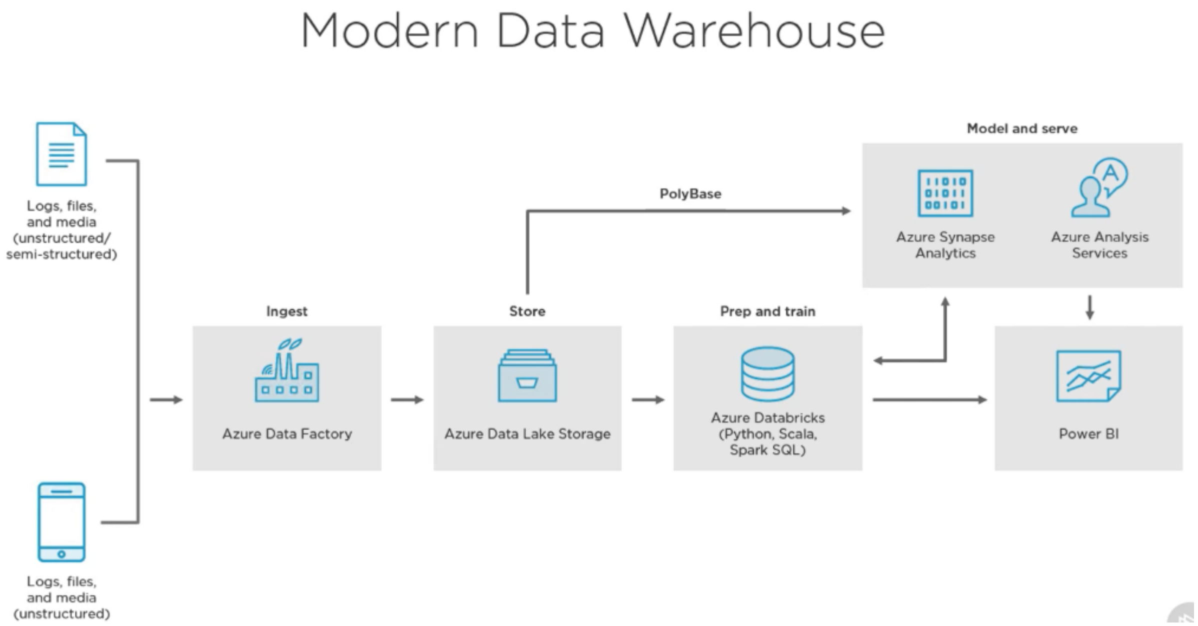
Just in Time :

- 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**

- **Data Warehouse (stocker des donné massive BIG DATA, Big data analyitic) :**
  - **Data Lake**
    - **Unstructured data**
    - **Pour le Big data Analytic**
    - **Et l'intelligence artificiel**
    - **Moins chère qu'une DDB Relationnel**
    - **Store organize et analyze**
    - **Diver type de donné provenant de diverses sources**
    - **Large volume de donnée peu chère**

        - infrequently used data is stored in cooler tiers to lower costs.
    - Synapse Analytics/ SQL data werehouse
        - Structured Data , SQL
        - Pour le Big data Analytic
        - Service d’analyse intégré
        - Ingest data
        - Wharehousing data
        - Analtic
        - One of the benefits of Azure SQL Data Warehouse is that high availability is built into the platform.
        - Afin de répondre aux besoins immédiats en Machine Learning et en Business Intelligence.
        - Old name : Azure SQL data werehouse
    - HDinsignt
        - structured or unstructured data
        - Pour le Big data Analytic
        - Big data clusters
        - Cloud distribution Of hadoop
        - Composant rendant plus facile et cost effective l’exécution d’une massive amont de donnée
        - Support popular open-source Framework
        - Hadoop, Spark, Kafka
    - Data Brick
        - structured or unstructured data
        - Pour le Big data Analytic
        - Big data clusters
        - based on Apache Spark
        - An other data Analytics platform
        - based on Apache Spark
        - Offer 2 enviromment for devolpping data intensive applications

- Cluster :
    - Used to run the data processing job
- Notbook
    - Web interface allow you interact with data en vizualization
- Libraries
    - Use built-in library or your third party library to run on the cluster



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**

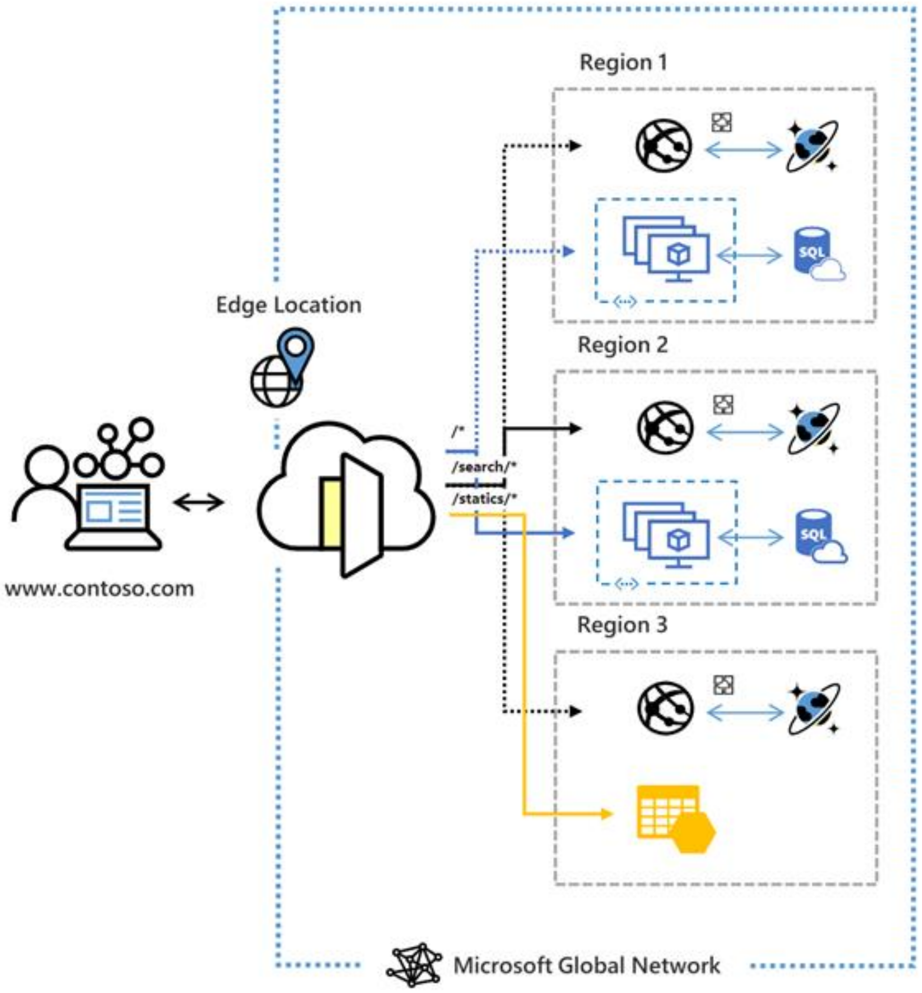
- Appp Gateway Standard v1
  - **does not** support **static public IP** addresses
  - Support **only AvSet**
- **App Gatway Standard** sku **v2**
  - **support Static IP**
  - **Support Avset and AvZone**
- App Gatway **Support Web app and VM in Back end pool** not load balancer
- Provide **SLA** of **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 VideoServer Pool, 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 :

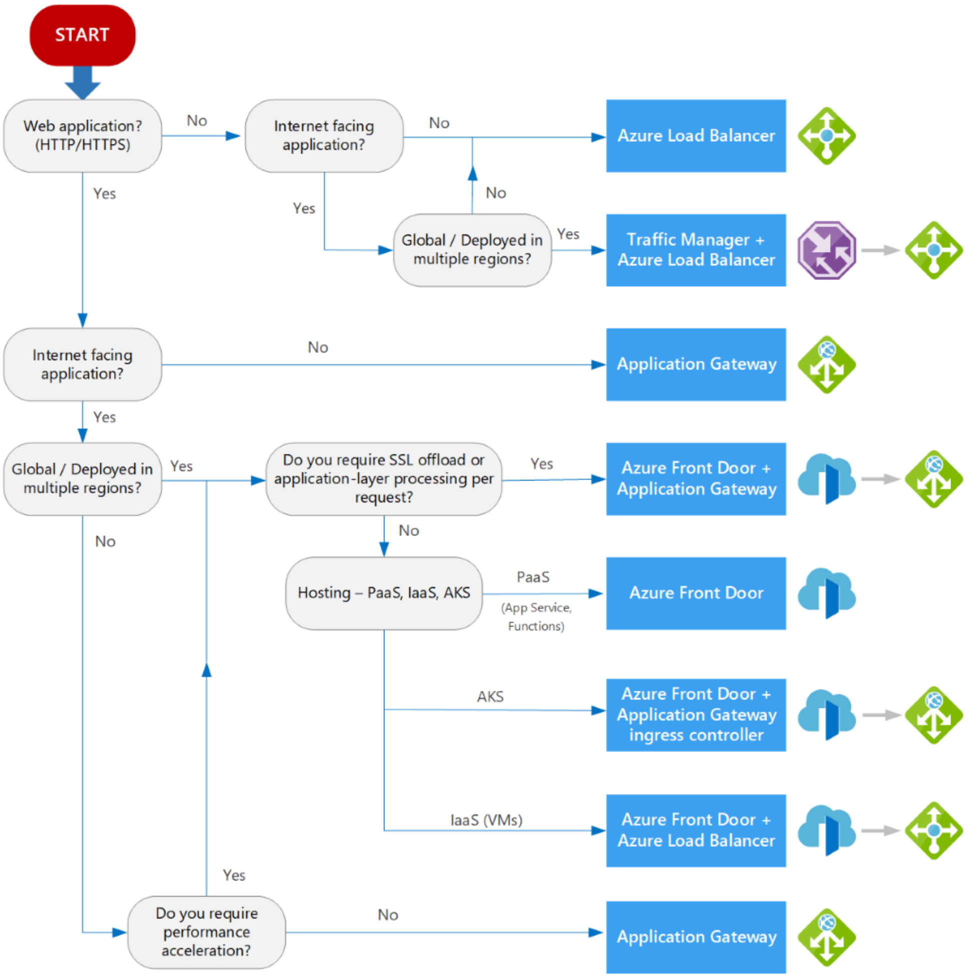
- Service permettant de **distribuer le Traffic** entre les Azure région
- Layer 7 (HTTP/HTTPS) load balancers (**Like Applicaion Gateway**)
- **SSL offloading capabilitie**s so that the **SSL encryption can be managed by Azure Front Door itself.**
- Application security with integrated **Web Application Firewall (WAF)**
  - **Rate limit rule (not in traffic mangaer)**
    - **controls the number of requests allowed** from clients during a one-minute duration
- **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 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. (active /standby , change to other methode for active/active)**
  - **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.

    - **Endpoint monitoring (like healthprobe)**
        - **set the monitoring endpoint**
        - **If the endpoint fails, then Traffic Manager will fail over to the secondary**
-

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 additional 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.

Flow :

- You **first need** to create a **log analytic workspace connected** to the **Azure sentinel**
- **Collect** data using **various collector** from Azure ressource **(VM , AD, Activity log, Ressource) or tier or one prem**
- Then **use prebuilt Workbook** (permet de **travailler les donné pour afficher des graphic dashbord**)

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 creatio**n page-> **select azure sentinel triggere** -> **select send email action**
        - Role needed is **Azure Sentinel Automation Contributor or Az sentinel contributor + logic app contributor**

You can't use the same workspace used by Azure security center
Once you have enabled azure sentinel on a workspace you cant moove the workkpae to a other RG or subcription

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 c onnect to 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 **recommendations**

- **Security Reader**
    - View **permissions** for **Security Center**.
      Can **view recommendations, alerts**, a **security policy**,
      and **security states**, but **cannot make changes**

Azure cosmos DB :

- has the ability to work with **multiple consistency levels**. It can virtually store unlimited amounts of data. IT can also accept multi-region reads and writes

Azure SQL Database

- **Tiers :**
    - **Standard**
        - **locally redundant onyl**
    - **Basic**
        - **locally redundant only**
    - **General Purpose**
        - **Serverless and Provisionned**
            - **zone redundancy (** This feature is **not available in SQL Managed Instance)**
    - **Premium**
        - **Offers highest resilience to failures and fast failovers**
        - **zone redundancy**
        - dynamic scaling
    - **Hyperscale**
        -

- **Dynamic Data Masking**
    - limit the sensitive data to the non-privileged users by **hiding the data of a column.**
- **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 **authorized 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 running on Premium Storage VM

- **Cache polices** :

  - **Log disk : None Cache** —Log files have primarily write-heavy operations. Therefore, they do not benefit from the ReadOnly cache.
  - **Data disk : Readonly Cache**—If you have separate storage pools for the log and data files, enable read caching only on the storage pool for the data files.

Long-term retention (LTR) backups in Azure SQL and Azure SQL Managed Instance

- Many applications have regulatory, compliance, or other business purposes that **require you to retain database backups beyond the 7-35 days provided by Azure SQL Database and Azure SQL Managed Instance automatic backups.** By using the **long-term retention (LTR) feature,** you can store specified SQL Database and SQL Managed Instance full backups in Azure Blob storage with configured redundancy for **up to 10 years**

vCore-based Azure SQL database

- **can also use long term retention** to ensure database backups are retained for seven years
- **can save on costs by using existing licenses** that are based on the Microsoft Enterprise Agreement.

Database Migration service :

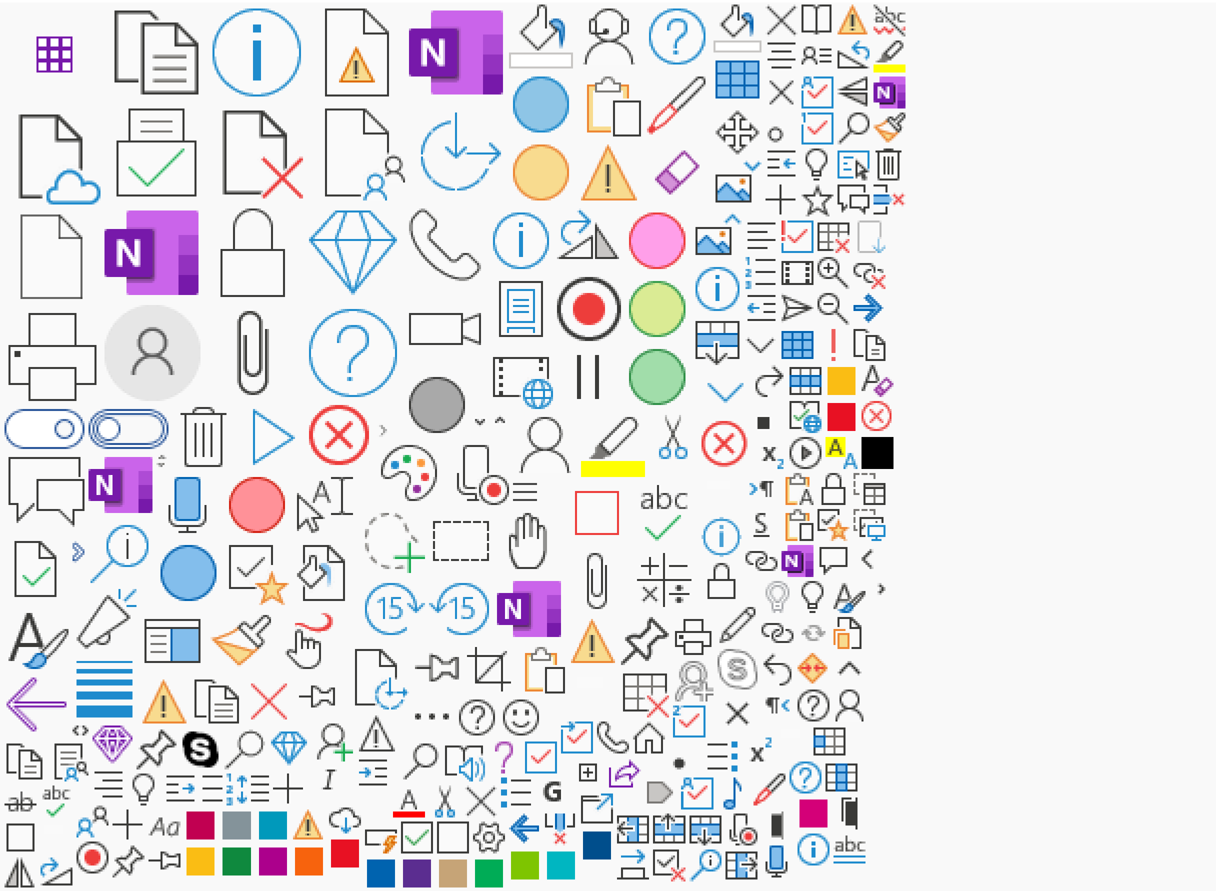
- You can use the Database Migration service to carry out an online migration. Here you don't need to have a storage account.

Azure SQL Database Managed Instance :

- option makes it easier for existing SQL Server customers to simply lift and shift their on-premise databases to Azure with the **least amount of database changes.**

Microsft Graph API (LOURD) :

- Managing with Microsoft Graph (and PowerShell)
-



-
- https://developer.microsoft.com/en-us/graph/graph-explorer
-
- **Is the web api allowing to manages globaly for automation (get / post) with rest ressource :**
    - **Azure AD, Microsoft 365 (teams, exchange, intune ,sharepoint.. etc) , Windows 10, and Enterprise Mobility + Security**
- Https://graph.microsoft.com
- You can manage **access review**
- **If you have a application that need to use access review api you must :**
    - **Register the application in Azure AD**
    - **Then delegate permission to the Microsoft Graph API**
        - **Go the thte app registred object**
            - **API Permission pane**
            - **Add permission => sekect " Microsoft Graph API "**
            - **Select delegate permission or** *App permission for your user if the application will be run with your user log in*
                - *Select the autozization needed (access review for exemple)*

Ligne 21 grpah powerhsell sdk module :

https://github.com/johnthebrit/RandomStuff/blob/master/AzureAD/MGAADDemo.ps1

https://github.com/microsoftgraph/msgraph-sdk-powershell/tree/dev/samples

Azure Batch :

- Use :
    - **Run large-scale parallel** en h**igh performance computing batch jobs**
    - **Image and video processing** to be **done in parallel**
- **Node** are used in Az Batch account to run the applications thats would process your workloads
- Nodes are run in a pool that are defined in the Az Batch account
- Storage account :
    - Store application you wan to process (ps, bat)
- Scrips ore executable can run on the nodes :
    - Exe, cmd, bat, PS , shell, python

Requirement :
Perform calculations in Azure.
Each node must communicate data to every other node.
Maximize the number of nodes to calculate multiple scenes as fast as possible.

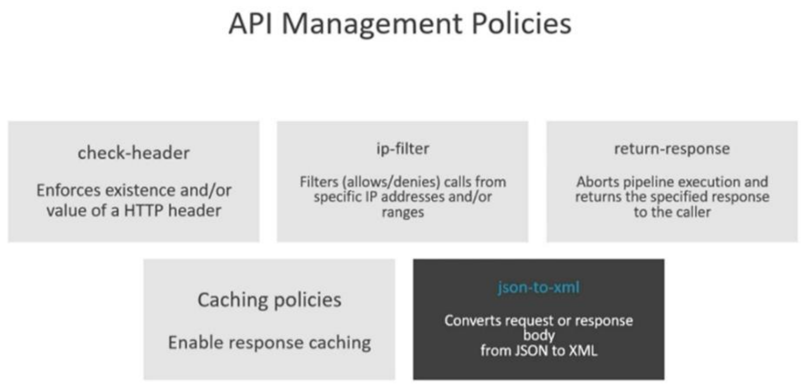
- Create a **render farm** that uses Azure Batch.
- **Enable parallel task** execution

- **low-priority VMs**
    - to **reduce the cost of Batch workloads**. Low-priority VMs make new types of Batch workloads possible by **enabling a large amount of compute power to be used for a very low cost.**
    - Low-priority VMs take advantage of **surplus capacity in Azure**. When you specify low-priority VMs in your pools, Azure Batch can **use this surplus, when available.**
    -

https://www.udemy.com/course/exam-az-microsoft-azure-exam-role1/learn/lecture/26975318#overview

Azure API Management Service :

- Its a API Gateway is a componement a APIM (beetwen your clien app and your api)
- API Gateway :
    - Accept client call and direct to backend api
    - Transofrm API at runtime without modification code (polcicy)
    - Verify API key and token
    - Optionaly cahce backend response
    - Enforce usase quotas and request rate limite
    - Logs API call detais for analytic and auditing purpose

    -
- Developer Portal
    - Dev can test the API in the interactive console
    - Read API documentation
    - Create an account and subscripe to the API by getting a API key
- Publish your API
- Organize en managae your API that you created
- **Feature :**
    - **Cache responses result**
        - Faster response
    - **Rate limit and qotas**
        - Ensure **no flooding of your api calls ddos**
    - **Provide secure way to access API**
    - **Policy**
    - In Azure API Management (APIM), policies are a powerful capability of the system that allow the publisher to change the behavior of the API through configuration.
    - Popular Statements include format conversion from XML to JSON and call
      rate limiting to restrict the amount of incoming calls from a developer
        - **For exemple :**
            - **Check-header policies**
                - **You want to ensure that aspnet-version header is removed form the repsponse of pulished APIS**
            - **Json-to-xml polices**
                - **You want to convert the data to JSON**
    - **Policy exemple :**
        -
        - 

          API Management Policies

          check-header
          Enforces existence and/or value of a HTTP header

          ip-filter
          Filters (allows/denies) calls from specific IP addresses and/or ranges

          return-response
          Aborts pipeline execution and returns the specified response to the caller

          Caching policies
          Enable response caching

          json-to-xml
          Converts request or response body from JSON to XML
        -
    - **Can use VNET integration for secure request and not public IP with premium tier**
    - **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**

-

Add API to APIM flow :

APIMS-> APIS pane-> Add New API (can add logic app and azure function as API)-> enter API url , API name-> Create
In APIS pane-> select your API , you can add polices :

- **inbound policies :**
  - **be alied to the request**
  - **Like ip-filter policis to restrict the usage of the API to a specific IP address range.**
- **backend**
  - **Be applied before request is forwaded to the backend**
- **outboud policies**
  - **Be applied to the response (ex convert response to json if the client requier json)**
- **On error**
  - **Applie if a error occure**

Add API to protduct for publish and make it acceccible for client

APIMS -> Product Pane -> Add ->Give a Name , Selct State(published or not published) , select "require subcription" or not (open for evryonne) , select the API you previously Added , Create.

Modify access to the product

Product Pane -> select you product -> Access control -> select the group allowed
Member of the group can now access the API thourgut the Gatway url (in APIMS Overview pane)
From APIMS -> user , you can add user and then add them to Group

- If there is only **1 API**, we just need to add that **1 API**
- **2 Products** need to be published, one for the **internal applications** and one for the **partner applications**

OAuth2:

- **Authtorization grant type :**
  - **Auhtorization code**

        - The Authorization **Code Grant Type** is used by both **web apps and native apps** to get an access token after a user authorizes an app.
    - **Support state parameter :**
        - to include additional client data
          In case you need to store additional details about a client that don't fit into the standard parameter

---

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**:

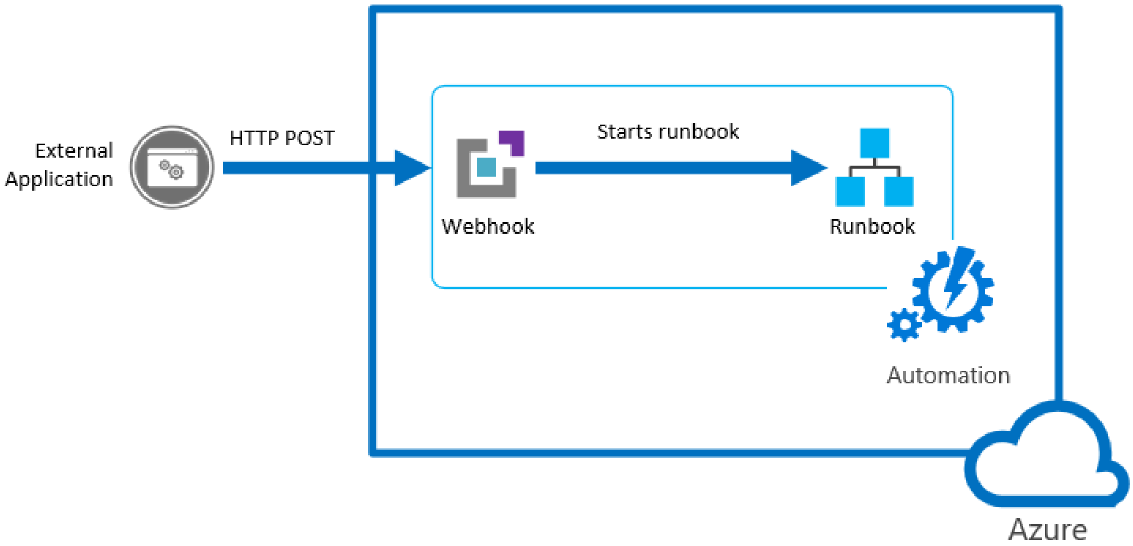
- **Consumption plan**

    - 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**
    - **Virtual network integration (if your functionn must call a App private IP)**
    - ✓ You have existing, underutilized VMs that are already running other 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.**
- **Connect to on-premises data sources from Azure Logic Apps**
    - One premise install :
        - **One premise data gaetway**
    - Azure install
        - **A connectio gateway resource**

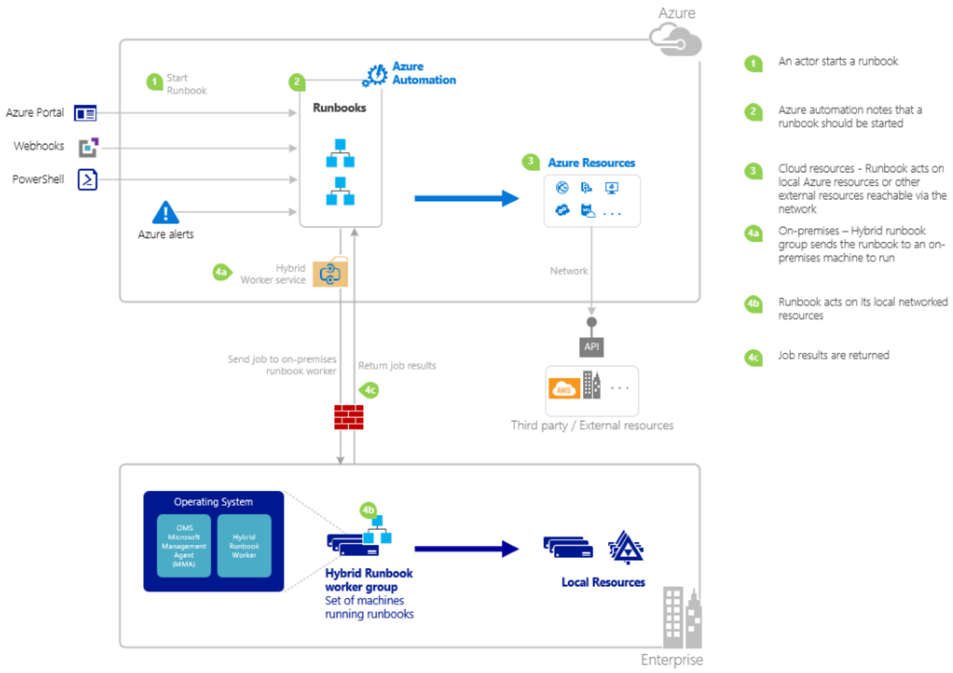
  https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-gateway-connection
- **Webhook :**
    - **URI**
    - A webhook allows an external service to start a particular runbook in Azure Automation through a single **HTTP request**. External services include Azure DevOps Services, GitHub, Azure 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.
-
-

- 

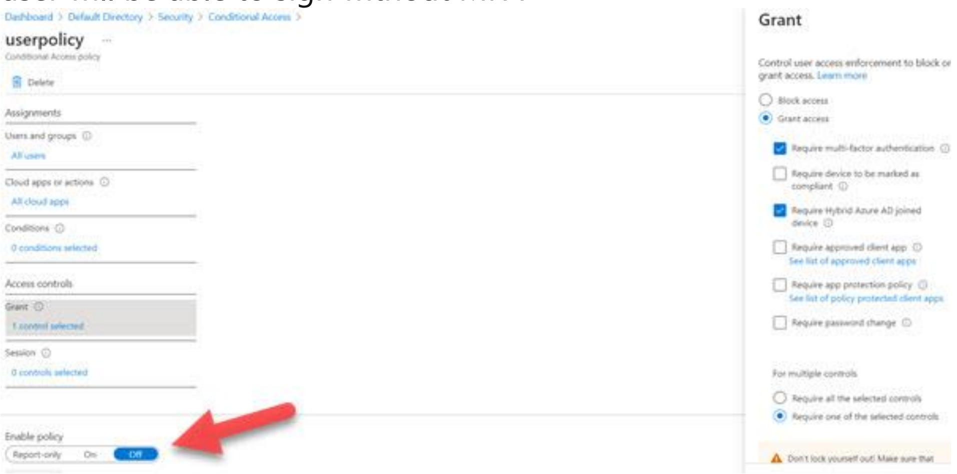
  - **Send Grid**
    - Its a **connector** that you can connect to **logic app or Azure function** for
      - **Send email.**
      - Add recipients to lists.
      - Get, add, and manage global suppression.
      -

- **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
  -
  -
  -

- 
Azure
Start Runbook
Azure Automation
Runbooks
Azure Portal
Webhooks
PowerShell
Azure alerts
Azure Resources
Network
Hybrid Worker service
Send job to on-premises runbook worker
Return job results
API
Third party / External resources
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 on local Azure resources or other external resources reachable via the network
4a On-premises – Hybrid runbook group sends the runbook to an on-premises machine to run
4b Runbook acts on its local networked resources
4c Job results are returned
-

Conditional access :

- If **policy enabled state is off the policy will not apply** and user will be able to sign without MFA
- 
Dashboard > Default Directory > Security > Conditional Access >

userpolicy ...

Conditional Access policy

Delete

Assignments

Users and groups
All users

Cloud apps or actions
All cloud apps

Conditions
0 conditions selected

Access controls

Grant
1 control selected

Session
0 controls selected

Enable policy
Report-only | On | **Off**

Grant

Control user access enforcement to block or grant access. Learn more

○ Block access
● Grant access

☑ Require multi-factor authentication
□ Require device to be marked as compliant
☑ Require Hybrid Azure AD joined device
□ Require approved client app
See list of approved client apps
□ Require app protection policy
See list of policy protected client apps
□ Require password change

For multiple controls
○ Require all the selected controls
● Require one of the selected controls

Don't lock yourself out! Make sure that
-

Premium managed disk

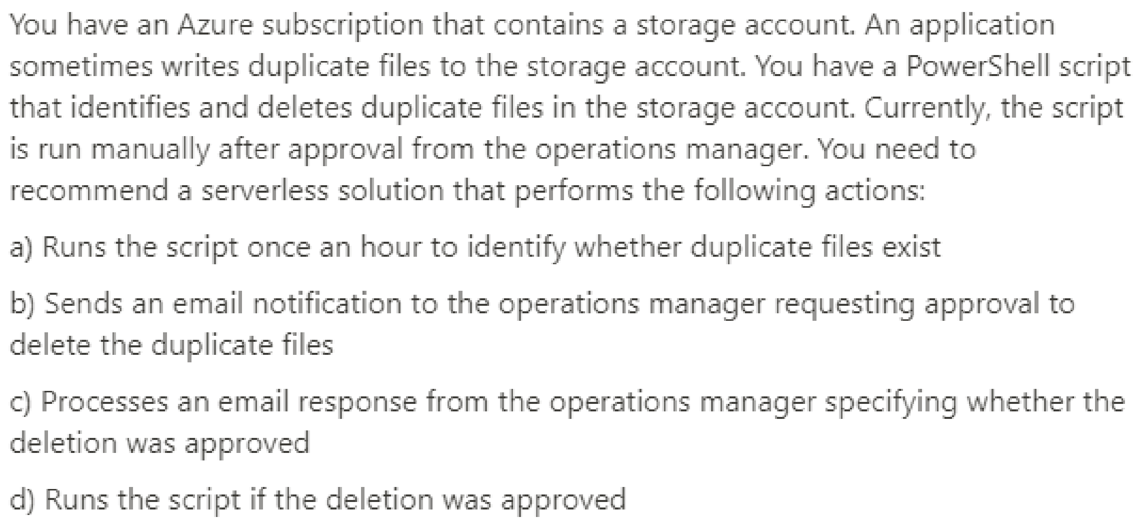
- provides **faster throughput and I/O capabilities**. And the **availability of the disks is managed by Azure.**
- Microsoft recommends not to use geo-redundant storage account for storing disks for SQL Databases.

With a locally-redundant storage account, you can actually use un-managed disks.
This is **cheapest option**

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**

Design :



You have an Azure subscription that contains a storage account. An application sometimes writes duplicate files to the storage account. You have a PowerShell script that identifies and deletes duplicate files in the storage account. Currently, the script is run manually after approval from the operations manager. You need to recommend a serverless solution that performs the following actions:

a) Runs the script once an hour to identify whether duplicate files exist

b) Sends an email notification to the operations manager requesting approval to delete the duplicate files

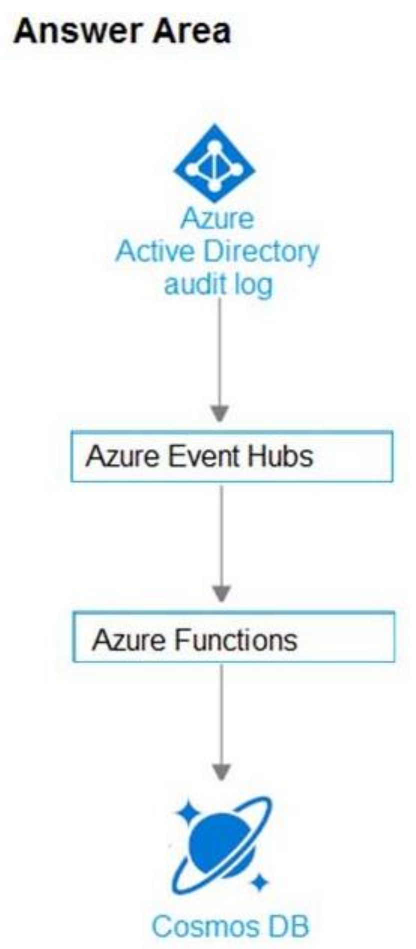
c) Processes an email response from the operations manager specifying whether the deletion was approved

d) Runs the script if the deletion was approved

- **Azure function (mail http trigger aprove or deny) -> Azure logic App -> azure automation runbook (powershell script)**

Design Azure AD log to Cosmos DB

https://docs.microsoft.com/en-us/azure/azure-functions/functions-event-hub-cosmos-db?tabs=bash



- https://www.examtopics.com/exams/microsoft/az-304/view/17/

____

Azure migrate

- **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.**

Replicate VM

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)

Azure Service Fabric :

- distributed systems platform that makes it **easy to package**, **deploy**, and manage scalable and reliable microservices and containers.

You can use Azure Service Fabric to create Service Fabric clusters on any virtual machines or computers running Windows Server.

Azure Virtual Desktop :

- **Scale session hosts** using **Azure Automation**
  - You can reduce your total AVD cost by **shutting down and deallocating session host VMs during off-peak usage hours,** then turning them back on and reallocating them during peak hours.
    - Flow :
      - Scale session hosts Azure Automation - Azure | Microsoft Docs

46 Study case

Alan 50

Faire les case study
Alan 2 : 4 , 5 , 9 , 58 , 59, 61, 62, 63 , 77, 78

API Management service

Autentification

https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-v2-protocols

Lire la liste de protocols

Alan 2 42