Azure AZ104

01 Manage Azure identities and governance

Manage Azure Active Directory (Azure AD) objects

Azure AD Plan

	Free	Basic	P1	P2	O365
Group-basedaccess managment		✖	✖	✖	✖
SSPR Cloud		✖	✖	✖	✖
Customizaion logon/ Access Panel		✖	✖	✖	✖
SLA		✖	✖	✖	✖
MFA	✖	✖	✖	✖	✖
SSPR /Unlock One premise password writeback			✖	✖	
Azure AD Sync			✖	✖	
Conditionnal access			✖	✖	
Identyti protection				✖	
Priviled Identity management				✖	

Azure Active Directory

- **Add licence**
  - **From the Licenses blade of Azure AD, assign a license**
- **Add role to user**
  - **Select Azure Active Directory, select Users, and then select a specific user from the list.**
  - **3. For the selected user, select Directory role, select Add role, and then pick the appropriate admin roles from the Directory roles list, such as Conditional access administrator.**

User condit

You can update location information on all user(AD, Guest AAD)

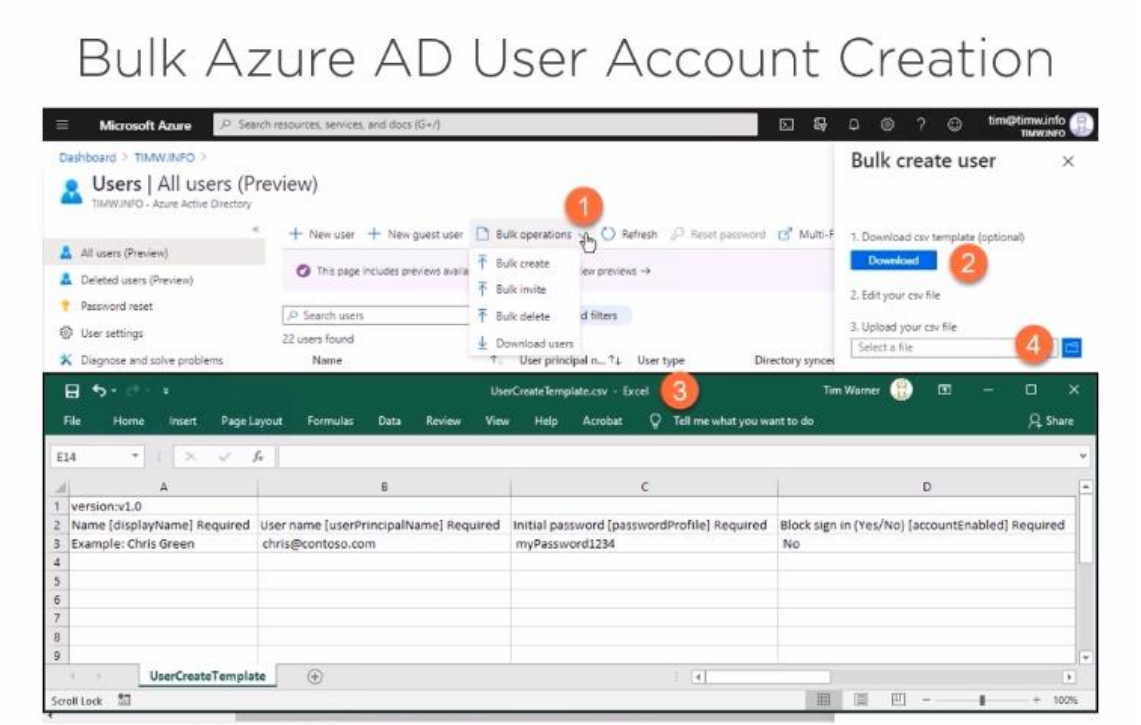
A user account can be restored when it's deleted within the last 30 days

- **AD user**

- You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server ActiveDirectory.

- Custom domain name Azure AD
  - If you want add a custom domain to Azure AD
    - 1 : Add Custom domaine to Azure AD
    - 2 : Add a record (TXT or MX) to the registrar / public DNS Zone
    - 3 : Verify the domain (fore Azure verify that you do own the domain name)

- create users
- Role : User Administrator or Global Administrator
  - Create users Powershell
    - `Install-Module` -Name AzureAD
    - `Connect-AzureAD`
    - `New-AzureADUser` -DisplayName -PasswordProfile -UserPrincipalName « flo.iedom.fr» -AccontEnabled $true
  - create users Cli
    - az ad user create –display-name
  - Buld Azure AD user creation
    - Csv



  - cloud identities
    - local Azure AD
    - Hybryd identities (synchrinized)
    - Guest identités

      For add guest user you can modify the External collaboration settings in User settings.

      - Azure AD B2B collaboration

        - définie in a other Azure AD instance, can invite user from a other AAD instance, B2B
    - External identities
        - Identiis like google, facebook etc

- manage guest accounts
    - Require Azure AD Premum P2
        - Guest identités
            - Azure AD B2B collaboration
                - définie in a other Azure AD instance, can invite user from a other AAD instance, B2B
            - External identities
                - Identiis like google, facebook etc
    - Can be invited by :
        - Administrator
        - Users
    - Role required for guest review :
        - Global administrator
        - User administaror

    - Create group
        - Create group powershell
            - `New-AzureADGRroup` -Description -DisplayName -MailEnabled -Security Enabled -MailNickName
        - Create group CLI
            - Az ad group create
            - Az ad group memeber checj
            - Az ad group member add
        - Type de groupe :
            - Security group
                - ressource access, application access
            - M365 group
                - with M365 licence, list email, distribution list
        - Groupe concept :
            - Group Owner
                - delegate groupe owenerhsip , charged of pupulate the group
            - Membership assigned
                - Manualy add user
            - Dynamic membership
                - Azure ad control group membreship based on user properties exemple (city= guadeloupe)
                - Dynamic still have owner that can change dynamic rule, add licence, remove licence
                - Cannot manulay add user/device to dynamic group
            - Group-assigned roles and licences

        - Automate distribution of licences by assigned licence to the groupe
    - Role needed to add or modified group
        - Global administartor , user administartor
        - User administrator role has the permission to update group membership. He can add users, devices, other groups to any group in Azure AD (Cloud device administartor can't update groupe membership even of device)

- Confiure bulk user update

```
Import -AzureAD-Module

Connect-AzureAD

        $adGroupId = "<Azure AD Group Id here>"


        $users = Get-AzureADGroupMember -ObjectId $adGroupId


        foreach ($u in $users)
        {
            Write-Host $u.DisplayName
            Set-AzureADUser -ObjectId $u.Mail -Department "<New Value to update here>"
        }
```

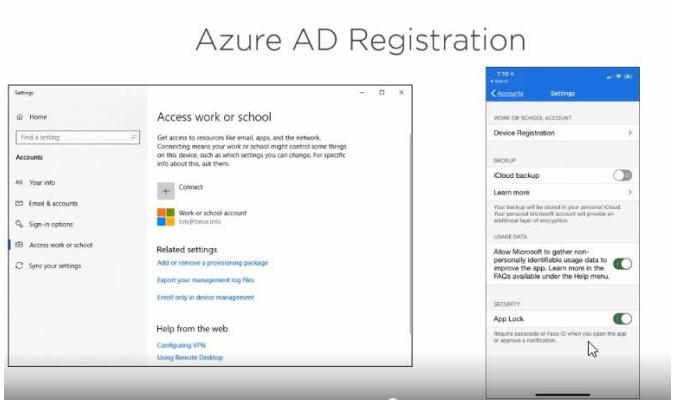
- Bulk update Azure AD with user attributes from CSV
    - https://timw.info/akh

- manage user and group properties
- manage device settings
    - Device
        - System that can be registrer or join AzureAD and be managed with Azure MDM tools
            - Possibility of create group of device
    - BYOD
        - Bring your own device, personly owend device signed with personnal Microsoft account
    - MDM
        - Mobile device managemnt, Org Owned device that support AAD device singin
    - Local Administrators group of a device
        - The user that Join the device
        - Global administrator
        - When a device is joined to azure AD the user who join the computer to the domain is added as the local administrator. Also the global administrator will be added as an administrator to the system
- Maange device role
    - Cloud device administrator

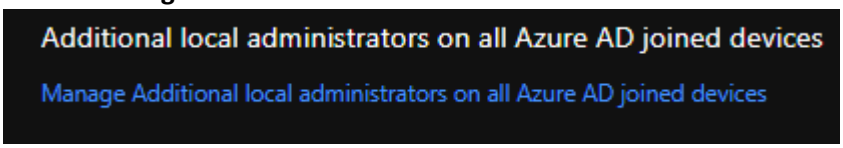
        - Add, enable, disable delete devices in Azure AD
        - CANNOT modify properties of device in the device
            - Cloud device administrators can manage devices(delete, disable, & enable devices), not group membership, but Group Ower, Global administartor , user administartor can
        -

    - Device administrator
        - Local machine administrator, connot modify object in Azrue AD
        - Can modify local device propeties
    -

- configure Azure AD join
    - Azure AD registred
        - Persnaly owen device, Windows 10, iOS, iPadOS, Android, and macOS.
        - W'ont be subject to full contraol policy but at least SSO experience
        - Microsoft authenticator App
        - You can select None or All that can register device
        - Can select MFA auth required for join registred device

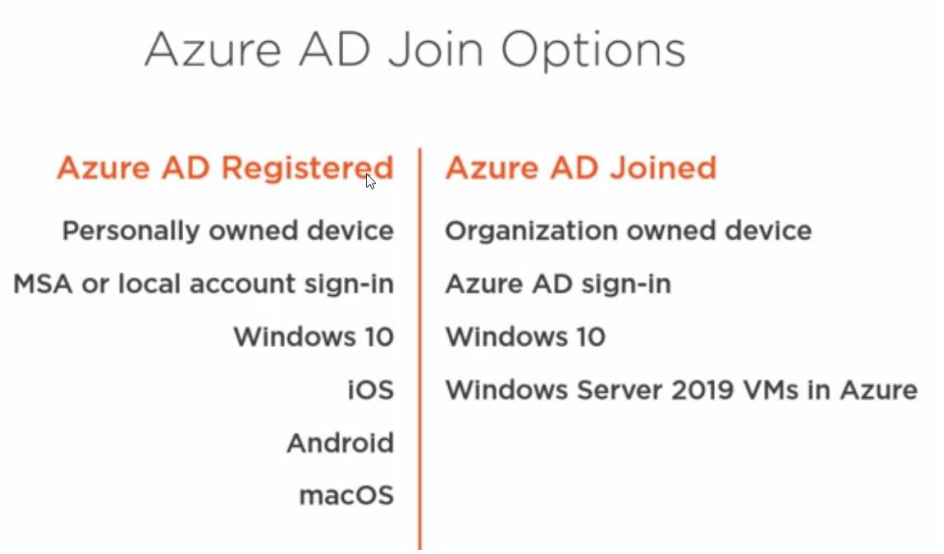


    - Azure AD join
        - Organization owned , azure ad sign-in , Win10, Win server 2019 VMs in Azure
        - You can select None, All, or selected user or group that can join device
        - Can select MFA auth required for join device
        - Can choose to Add Additional local administrators (en plus du Global administrator et de l'user qui a join le device par default)
        - add a user as an administrator on all the computers that will be joined to the Azure AD domain
            - Device settings from the Devices blade



            - And add Device Administrators (en plus du Global administrator et de l'user qui a join le device par default qui sont parfault Local admin des PC Joint)

- **Azure AD join supports Windows 10 or Windows Server 2019 devices where users sign in by using their work account with a password or Windows Hello. Azure AD Multi-Factor Authentication is also supported.**
- **three choices for how devices are provisioned and joined to Azure AD**
  - **Self-service in OOBE or in Windows Settings**
  - **Windows Autopilot**
  - **bulk enrollment**



- **Hybrid AAD Join**
  - **Company thta have one premise AD and SCCM**
  - **Need to support AAD apps and service**
  - **Org owned device**
  - **AAD synchro with AD Connect**
  - **Windows 7, 8.1, 10**
  - **Windows server 2008 or newer**
- **AAD sign-in to Azure VM**
  - **Win Server 2019**
  - **Wi 10 1809**
  - **Must be AAD joined**
  - **RBAC on the user VM Role (Virtual Macine User login or Administrator Login roles)**
  - **System assigned manged identity « On»**
  - **Login with AAD credentials « On »**
  - **AzureAD\floria@iedom.fr « mot de passe »**
- **Azure AD Device Management**
  - **After Joined device what you can do :**
    - **SSO to Saas apps en Azure**
    - **Etreprise state roaming**
      - **Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device**
    - **Windows hello**

        - In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.
    - Conditional acces policy
- Microsoft Intune
    - Part of Microsoft endpoint manager product family :
        - SCCM
        - Windows autopilot
            - Reimage système
            - Deploy windows setting
            - Migrate user state
    - MDM and MAM (mobile device management, mobile application management)
    - Use case :
        - AAD joined mobile device (Win10, IOS)
        - Need to do policy management,
        - Wipe
        - Geolocation
        - Allow/deny app
    - Microsoft intne company portal
        - For Dowlaoad Allowed App

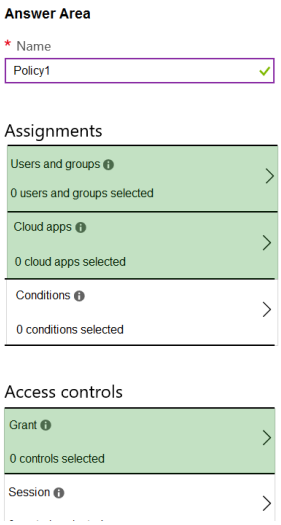
- Configure self-service Password reset (SSPR)
    - Reduce support desk paswword change issues
    - Minimum AzAD Premium P1 licence
    - Password writeback(Up if you want that AAD Password change update to one-premise)
    - Administrator don’t have the ability to use security questions for SSPR.
    - Even without SSPR enabled, users can change their password when they're signed in to Azure AD.
    - If the user passes the authentication tests, then they can reset their password.
    - A user is considered registered for SSPR when they've registered at least the number of methods that you've required to reset a password. You can set this number in the Azure portal.
    - Enable two or more of these methods :
        - Mobile app notification
        - Mobile app code
        - Email
        - Mobile phone
        - Office phone
        - Security questions

Configure self-service password reset

	Azure AD Free	Azure AD Premium P1 or P2
Cloud-only password change	✸	✸
Cloud-only password reset		✸
Hybrid password change or reset with on-prem writeback		✸

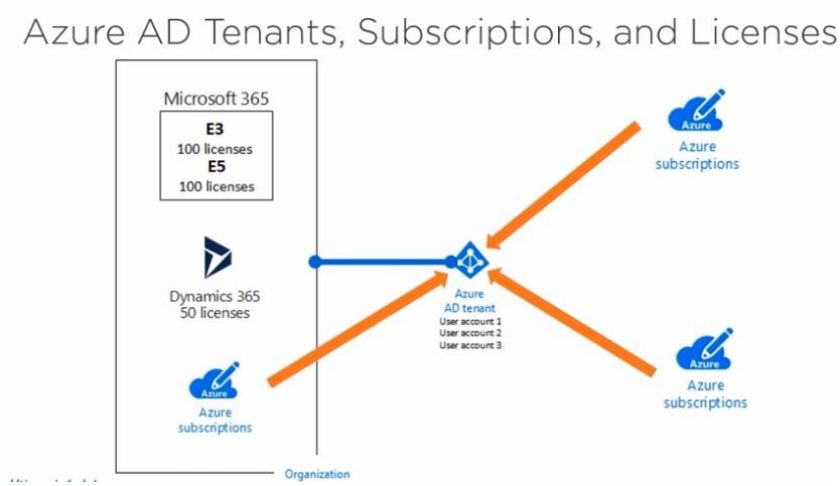
- **MFA**
  - **Free for global admin Administrators but need AzAD Premium p1 licence for other user**
  - **Recomended enforce MFA with conditonnal acces**
- **Conditionnal acces**
  - **AzAD Premium 1 licence**
  - **Condition that the user have to meet for succecfull authentified (location, network, AD device join)**
  - **Chose user group, App, condition (location, device,client apps, device state)**
  - **Actions (block grant MFA, ADjoined, compliant)**
  - **conditional access policy that requires all users to use multi-factor authentication when they access the Azure portal. three settings should you configure**

Answer Area



  -
- **My App portal**
  - **https://myapplications.microsoft.com/**
- **Manage multiple directories**

- Change subscription of tenant/direcorty,
  - need to be owner of the subscriptions and global Administrator of the tenant

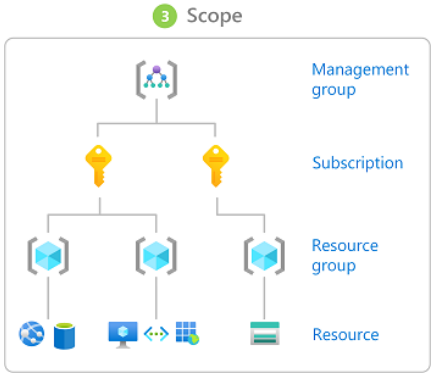


Manage role-based access control (RBAC)

- RBAC
  - Assign permission to
    - User
      - Who has un profil in Azure AD , can be assigned to users in other tenants
    - Groups
    - Applications
  - Scope
    - Management group, subscription,RG, Ressources
  - Use Case
    - Allow one user to manager VM,and other to manage VNET
    - Allow DBA group to manage SQL Database in a sub
    - Allow an application to access all ressource in a resource group
  - Principe
    - Role assigned to group impact all user
    - You can also assign roles to users in other tenants (ex gest user B2B)
    - Service principal
      - Secuirity ID for applications or services
    - Manged identity
      - In Azure AD
      - Used in developping cloud applications to handle credential management (ex Azure Keyvault)
      - 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.

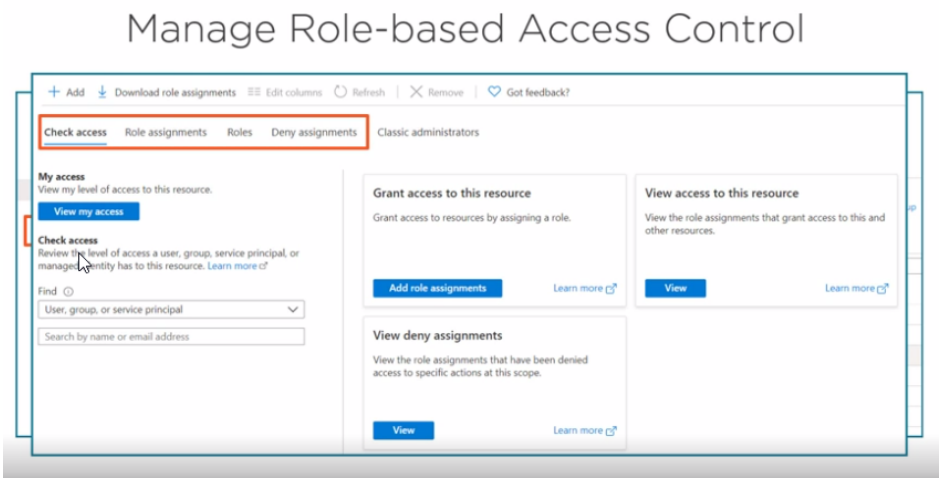
-

- **Diffèrent des Azure AD Rôles** ou on ne peut pas créer de role custom**(Owner / Global Administarteur)**
- **Possibilité de créer des role customisé**
- **Role intégré** :
  - **Contributeur** : **CRUD**, but **cannot grant acccess**
    - **Only apply to ressoruce itself but not the data**
    - **(ex storage acc contributor can manage it but have not acces to the data in the storage acces)**
  - **Owner** : **CRUD** + Allow **attribuer des rôles (grant access)** dans Azure RBAC.
  -
  - **Reader** : **Read only** existing resources
  - **User access Administrateur** : gérer **l'accès utilisateur aux ressources** Azure **grant access**.
  - **Under role**
    - **Ex : (Network contributer, VM contributor , Vnet Owner etc)**
    - **Allow to define a role in a lower scope for more security**
- Azure RBAC can be applied on all scope, **Management groupe, Suscription Ressource Groupe, Ressource**
- Les Rôles **RBAC s'hérite** du scope supérieur



- **Deny Assignements**
  - **Block user** for performing **specific** actions **even if** a **role assignment allow it**
  - Created and managed in azure to **protect ressources**
  - Can **only be created** using **Azure Blue Prints** or **managed apps**

Manage Role-based Access Control



- **Use 'Set-AzRoleDefinition' to update a custom role by using Azure PowerShell.**
- **Add role assigenemts Powershell**
  - `New-AzRoleAssignement` – SignInName flor@iedom.fr -RoleDefinition « Contributor » -RessourceGroupName Rgtest
- **Verify role assigenemnt PS**
  - `Get-AzRoleAssignement` -ResourceGroupName RGtest
- **Verify role assigenemnt Az CLI**
  - **Az role assignment list -ressource-group rgtest**

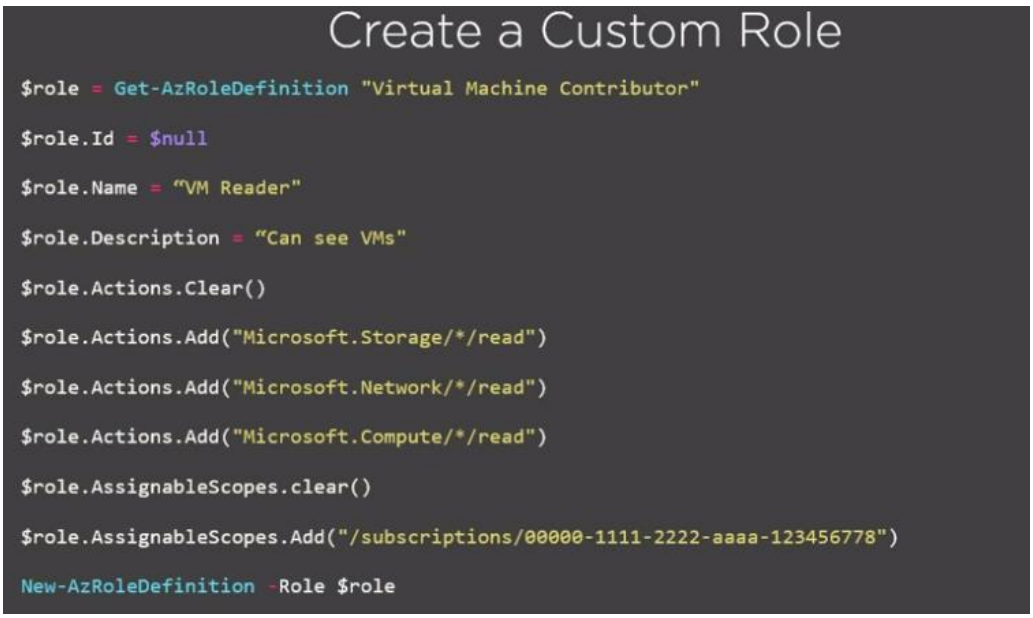
- **create a custom role**

Role Action Examples

Operation String	Action
*/read	Grants read access to all resource types of all resource providers
Microsoft.compute/*	Grants access to all operations for all resource types in the Microsoft.Compute resource provider
microsoft.web/sites/restart/Action	Grants access to restart a web app

  - **from portal**
  - **from arm template**
  - **Powerhsell**
    - **Modifing existing role**
    - **See actions of a role :**
      - **(`Get-AzRoleDefinition` " virutal machine contributor ").actions**
    - **Create new role using existant definition Powershell**
      - **$role = `Get-AzRoleDefinition` " Role name "**
      - **$role.id = $null**
      - **$role.Name = " New role Name "**
      - **$role.Actions.Clear()**
      - **$role.Actions.Add(" Microsoft.Storage/*/read ")**
      - **$role.AssignableScopes.clear()**
      - **$role. AssignableScopes.Add("/subscriptions/subscription-id ")**

- `New-AzRoleDefinition` -Role $role



- provide access to Azure resources by
- assigning roles at different scopes
- interpret access assignments

Manage subscriptions and governance

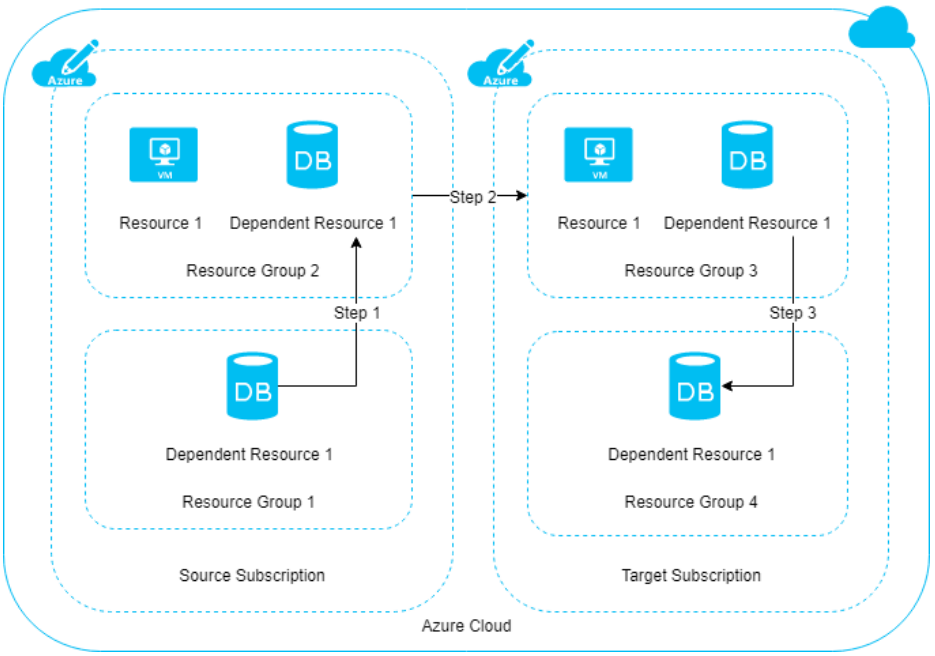
- Subscription
  - Free Trial
  - Support Plan
  - MSDN
  - Visual Studio
  - Pay-as-you-go
  - Entreorise Agreelent
- Ability
  - You can move resource between subscription
  - You can transfer subsscitption beetween different tenants
  - A single tenant can have multiple subscriptions
- Subscriptions panel
  - Cost Overview
  - Acitivity log
  - RBAC
  - etc
- Configure Azure policies
- Configure ressource locks
  - Ressource lock
    - read-only
    - delete
      - doesnt prenvent the data, file or database wihtin the ressource to be deleteted
  - lock concepts
    - can apply to all ressouce and resource groups

        - can be inherited from parent scopes
            - for both existing and new resources
        - applies to all user and roles
        - can you move a ressource in a read only lock ressource group?
            - yes you can and the ressource will inertih the read only lock
        - Read only lock on a ressource doesn't prevent us from moving a resource from one ressourge group to another , this would be prevented if the RG Source had a read only lock not the Rg destination
        -
    - Scope lock
        - Subscritpion , RG, Ressource
    - Lock Powershell
        - `New-AzResourceLock` -Locklevel ConNoteDelete -LockName LockSite
    - Lock CLI
        - Az lock create –name LockGroup –lock-type CanNotDelete –resource-group exemplerg
- apply and manage tags on resources
    - Tags
        - Organize resource
        - Consit of a name and a value pair
        - Must ahve the write access to « Microsoft.Ressources/tags »
        - Ressource can have mutlipte tag
        - Tag ar not ineritable
        - Not all resources support tag
        - Tags Powerhsell
            - Show all ressource assiciated with the tag « departement »
                - (`Get-AzTag` -TagName departement).name
            - Add a tag to ressource
                - $tags = @{'project' = « ux » }
                - $rg = `Get-AZressourcegroup` -Name rgtest
                - `New-Aztag` -RessoourceId $rg.ressourceID
- manage resource groups

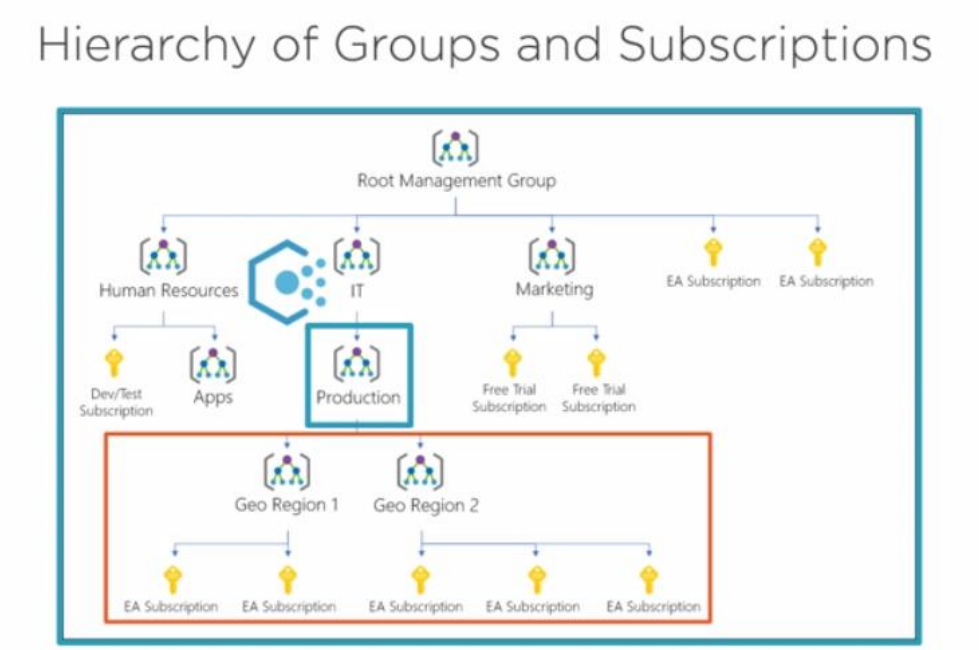
    - Ressourc group
        - Container that hold related Azre resources
        - Ressource can be moved from one resource group to another and across subciption if that is supported by that resource
        - Ressource can be moved from one region to another if that is supported by that resource
        - Both the source group and the target group are locked during the move operation. Write and delete operations are blocked on the resource groups until the move completes. This lock means you can't add, update, or delete resources in the resource groups. It doesn't mean the resources are frozen
    - Historique Deployement

        - From the RG1 blade, click Deployments. You see a history of deployment for the resource group. And the template used for the deployement
        - date and time when the resources were created

        - To see the template that you used for the deployment, select View template.
    -



        - Moving resource does not change the location/region where it was originaly created
        - Delete a rg delete all resource in that resource group
    - Ressource group Powershell
        - `New-AzResourceGroup` -name -location
    - Ressource group CLI
        - Az group create –name exemple –location eastus2
- manage subscriptions
- Manage Costs
    - Cost management blade
        - Cost Analyze cost and trends using (can access on subscription level)
            - Filter by different field like tags
        - Cost alert can be generted when treshold you define is met
            - Can send sms or mail
            - Can stop the VM when a treshold is meet for save money
        - Apply budgets to apply cost thresholds and limits to contrôle your spend
        - Recommendations displays ways to control cost through indentifying trends in your usage
    - Budget
        - Budget or cost alert should be created in cost managment in the portal not subscription
        - Can be create in subscirption or cost management pane
- configure management groups
    - Management group
        - Efficienttly manage access, policies and compliance
        - Provide level of scope over subscriptions
        - Subscirpitons withtin a group inherit polices applied to the group



- **Rout management group**
  - **Each directory has a singl top levl group called the root**
  - **Allow for global policies en RBAC assignement**
  - **AD global admin need to elevate to user acces administrator role or Owen in the root management group to asCsign RBAC to other user in other management group (none is by default have right in the root management group)**
  - **Root managemnt group cant be deleted**
- **Can moove created mangament group or subscirption under other manegemtn group parent**
- **Azure policy**
  - **Used to create assign and manage polices in Azure**
  - **Enforce rules to ensure tour resource remain compliant**
  - **Dont apply remediation to resource that are not compliant but suggest that he is not compliant**
- **Poicly concepts**
  - **Policy definition is a rule (allow or not allow location , ressource type)**
  - **An assigement is an application of an initiative or a policy to a specific scope (MG,Sub,RG)**
  - **An initiavive is a collection of policy defintions**
- **Policy pane**
  - **See ressource non compliance**
  - **Assing**
  - **Create initiative**
- **Azure policy Powerhsell**
  - **$rg = `Get-AzResourceGroup` -Name**
  - **Get a polcy deinition**
    - **$definition = `Get-AzpolicyDefinition` | Where-Object {$_ .Properties.DisplayName -eq 'Audit VMs that do not use managed disk' }**

        - Create the policy assignement
            - `New-AzPolicyAssigement` -Name 'adudit-vm-manageeddisk' -Scope $rg.RessourceId -PolicyDefiniton $definition

02 Implement and manage storage

Secure storage

Microsoft Defender for Storage detects anomalies in account activity. It then notifies you of potentially harmful attempts to access your account.

- configure network access to storage accounts
    - Firewalls and virtual netwoks pane
        - **The default network rule is to allow all connections from all networks.**
        - Layered security model for controlling acces to the storage
        - Secure and control access based of the need of app an infra
        - We can specify the VNET, Subnet allowed to acces the storage account or allow all Networks
            - When you slect the VNET a service endpoint is automaticlay created
        - We can specify Pulbic IP range of the One-premise Network allowed to acces the storage account
        - Select Allow trusted Microsoft services to access this storage account as an exception to enable Azure Backup service to access the network restricted storage account.
        - Limit access by rules
            - IP addresses
            - IP ranges
            - Subnets in Azure VNets
            - Trusted microsoft services
            - Can be Used for limiting
                - private network traffic in azure
                - Traffic from internet
                - One premise connecion (like Express route)
        - Configured throught firewala and virtual netwokrs blade from the storage account you want protect
        - Service Endpoints in azure services like vNETS
        - Require Ahtorizaton
            - Even if you put the firewal and vent rule in place the traffic accesing the storage account need to still have the proper autorisation
            - Azure AD Credentilas (Blob and Queue)
            - Shared account keys
            - SAS Token(shared acces signature)
- create and configure storage accounts
    - Storage account

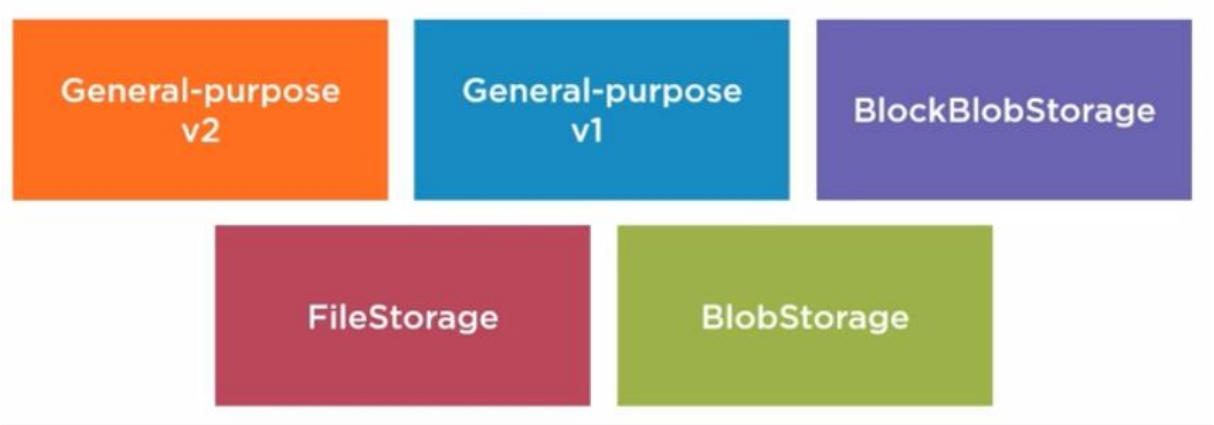
- **The storage account name is used as part of the URI for API access, so it must be globally unique.**
- **Contains all Azure storage objects**
- **Unique namespace acces to storage resources**
  - https://stblobstorage001.blob.core.windows.net/demo/az-104-outline.pdf
- **Create storage account Powershell**

```
$resourceGroup = "storage-resource-group"
$location = "westus"
```

  - `New-AzResourceGroup -Name $resourceGroup -Location $location`
  - `New-AzStorageAccount -ResourceGroupName MyResourceGroup -AccountName mystorageaccount -Location westus -SkuName Standard_GRS`
- **Create storage account CLI**

```
az group create --name storage-resource-group    --location westus
az account storage create --name storag
```

- **Storage accounts type**



Blob Storage Account

- **Supported services: Blob storage**
- **Supported blob types: Block blobs, append blobs**
- **Supports blob storage access tiers (hot, cool, archive)**
- **❗ Does not support ZRS**

General Purpose V1

- **Supported services: Blob storage**
- **❗ Does not support blob storage access tiers (hot, cool, archive)**
- **❗ Classic deployment & ARM**
- **❗ Does not support ZRS (Zone Redundant Storage) replication**

- **Slightly cheaper storage transaction costs, can be converted to V2.**

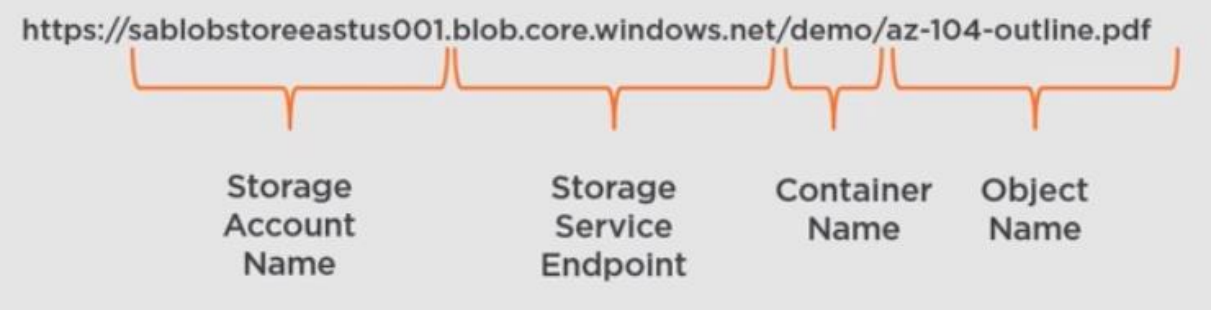
General Purpose V2

- **Supports all latest features.**
  - **Including anything in General Purpose V1 and blob storage access tiers.**
- **Recommended choice when creating storage account.**
- **Lower storage costs than V1**
- **Has a changing soft limit (as of now 500 TB)**
  - **You can contact Azure support and request higher limits (as of now 5 PB). Same for ingress/egress limits to.**

Azure Storage Account Capabilities

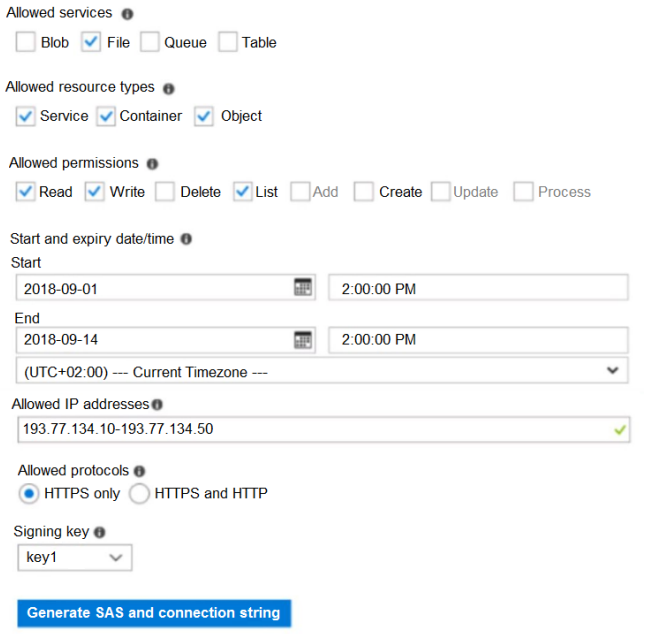
	Supported Services	Performance Tiers	Access Tiers	Replication Options
General Purpose v2	Blob, File, Table, Disk, Queue, & Data Lake Gen2	Standard Premium (Disk Only)	Hot, Cool, Archive	LRS, GRS, RA-GRS, ZRS, GZRS (preview), RA-GZRS (preview)
General Purpose v1	Blob, File, Queue, Table, and Disk	Standard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

- **Azure storage Endpoint for BlobStorage**



- **Generate shared access signature (SAS) tokens**
  - **Shared access signature(SAS)**

- provide time-limited access to ressource in a storage account
- A shared access signature (SAS) provides secure delegated access to resources in your storage account without compromising the security of your data. With a
- SAS, you have granular control over how a client can access your data. You can control what resources the client may access, what permissions they have on those resources, and how long the SAS is valid, among other parameters.

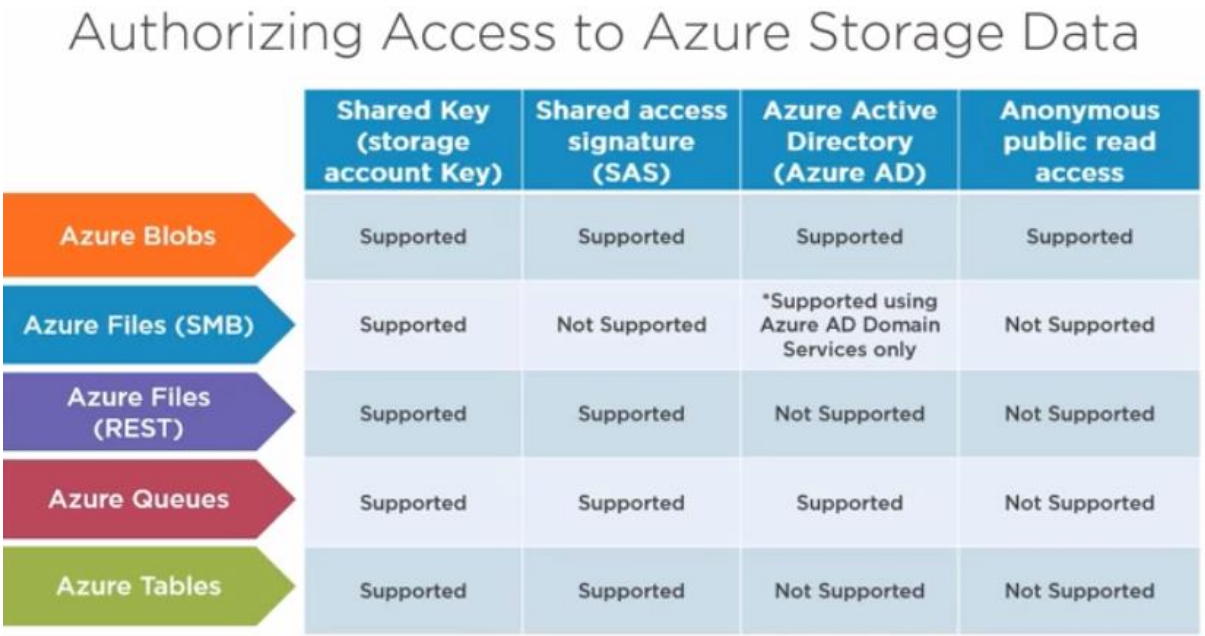


- allow grannular permission (read write delete)
- can be applied at storage account or data object level
- generate SAS keys in multuple tools
  - azure portal, azure storage explorer
- easy to revoke SAS
  - by deleting stored policy or
  - changing period validity or
  - regenerate the account key
- Contains permissions and start & end validity period.
- Set read and/or write permissions.
- Grant permissions to access only partition + row key ranges.
- You can restrict access to IP Address(es)
- Enforce HTTPS
- Net use for File share dont support SAS

- manage access keys Shared access Key
  - access keys Shared access Key

  - Access to entire storage account (root password)
  - Used in scenarios needed limited number of secrets
  - Protect your keys
  - Consied use Azure AD instead of shared key MS recommanded
  - Use Azure Key Vault

-
- Configure Azure AD authentication for a storage account
  - Azure AD authentication
  - Supported for Blob and Queu storage
  - UsinG RBAC
  - Microsoft recommanded approach instead of share key
- Storage type Acces Autorisation
  - Anonymous read: Only blob
  - Azure AD : Blob, Queues
  - SAS : All exept Azure FIle (but required for Az copy)
  - Shared key : All



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

Switching	...to LRS	...to GRS/RA-GRS	...to ZRS	...to GZRS/RA-GZRS
...from LRS	N/A	Use Azure portal, PowerShell, or CLI to change the replication setting[1,2]	Perform a manual migration OR Request a live migration	Perform a manual migration OR Switch to GRS/RA-GRS first and then request a live migration[1]
...from GRS/RA-GRS	Use Azure portal, PowerShell, or CLI to change the replication setting	N/A	Perform a manual migration OR Switch to LRS first and then request a live migration	Perform a manual migration OR Request a live migration
...from ZRS	Perform a manual migration	Perform a manual migration	N/A	Request a live migration
...from GZRS/RA-GZRS	Perform a manual migration	Perform a manual migration	Use Azure portal, PowerShell, or CLI to change the replication setting	N/A

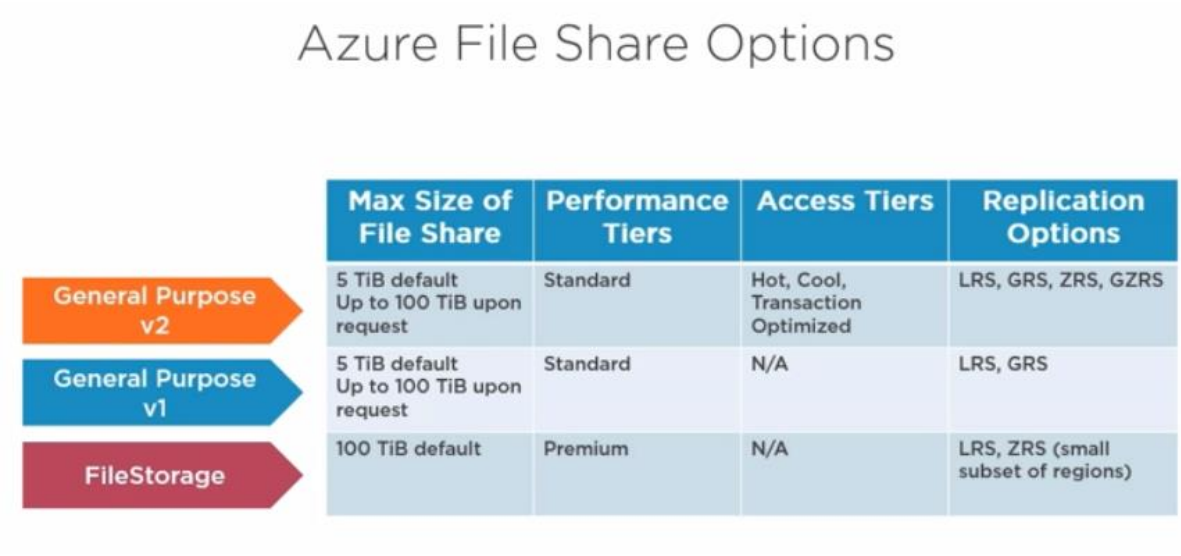
- **LRS and ZRS**
  - **replication wihtin a region**
  - **ZRS provides replication across datacenter**
- **GRS and GZR**
  - **Cross-region replication**
  - **GZR give ZRS in the primary region**
- **RA-GRS and RA-GRZRS**
  - **Provide read-only access to the replicated data to the secondary region**

Outage scenario	LRS	ZRS	GRS/ RA-GRS	GZRS/ RA-GZRS
Data center node becomes unavailable	Yes	Yes	Yes	Yes
Entire datacenter becomes unavailable	No	Yes	Yes	Yes
Primary region-wide outage	No	No	Yes	Yes
Read access in secondary region when primary is unavailable	No	No	Yes (with RA-GRS)	Yes (with RA-GZRS)

    - Replication can be re-confifured on Storage Account
- configure blob object replication

Configure Azure files and Azure Blob Storage

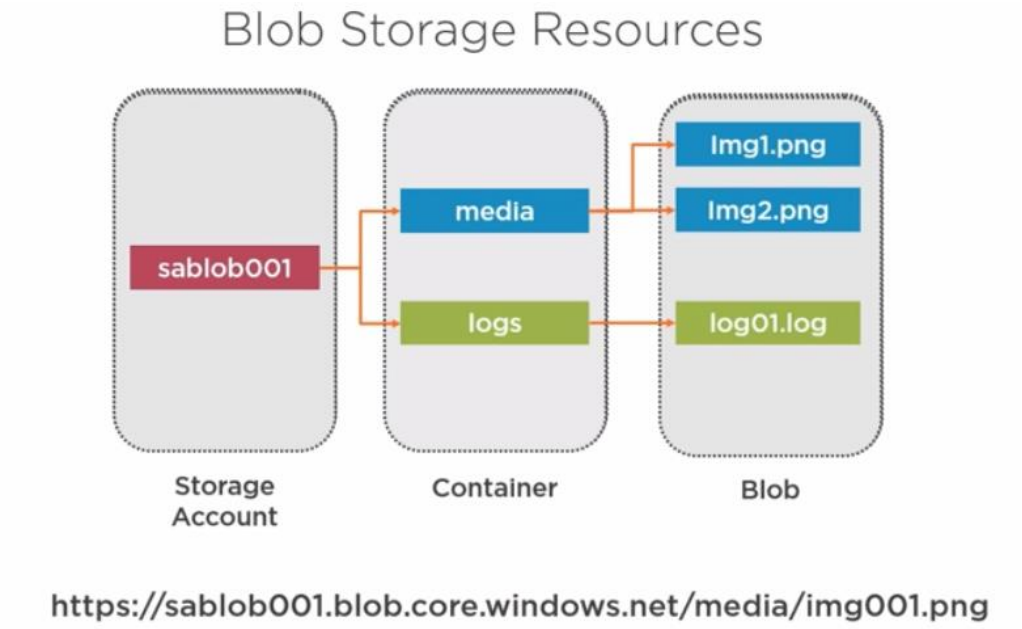
- create an Azure file share
    - Cloud-based SMB or NFS file share
    - Create share through azure portal or code
    - Client use port 445
    - Recommended to use with express route or site to site vpn not from internet
    - Support Storage account : GPv1, GPv2, FileStorage



- Configure Access to Azure Files
    - Autheitification for file share
        - Azure Active DirectorRY Domain Services or Active DirectorRY Domain Services
            - Provides identidy-baes acces for hybrid envrionment
            - Allow granular share-level and file-level permission
            - Best pratice recommanded for file share
        - Storage Account Key or Shared Access Signature

        - Less granular control
        - Secure the keys
    - Net use dont support the use of SAS

- Configure Azure Blob Storage
    - Unscrutured data objects of various types
    - Use a unique URI-based namespace
    - Storage account supported : BlobStorage, GPv1, GPv2
    - Manage cost with tiering
    - Support various replication depending of the storage account



- configure storage tiers for Azure Blob Storage
    - tiers can be applied when uploading blobs to Azure
    - Change tiers at blob level
    - Archive requiers rehydration for access
    - Use lifecycle managment for automation of blob tier dépend of usage
    - configure blob lifecycle management

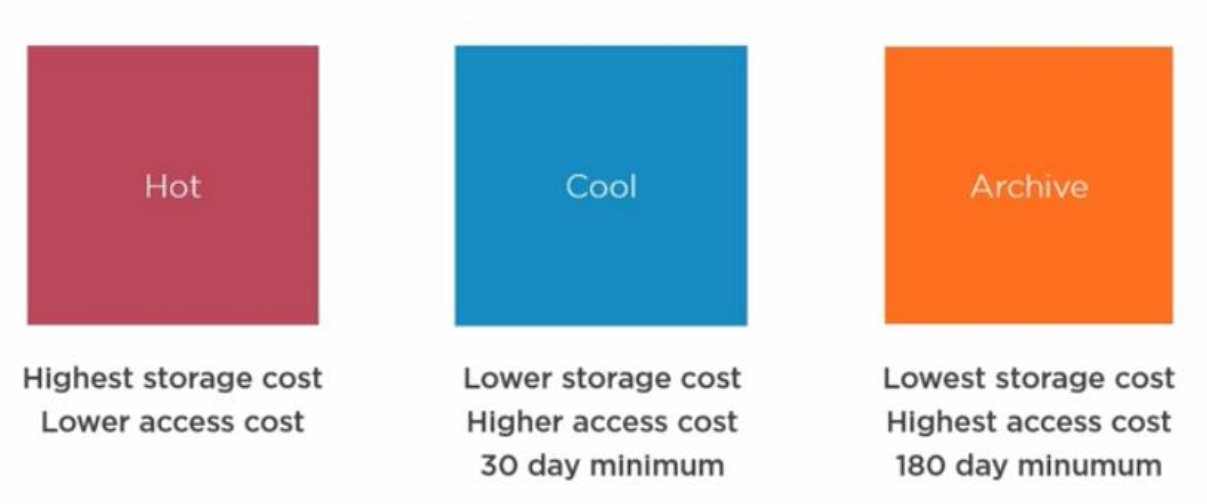
Blob Storage Access Tiers

- Only the General Purpose V2 and Blob storage account types support the Archive access tier.

- Set on blob level.
- Three tiers:
    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
        - Highest data access cost
        - Lowest data storage cost
        - Optimized for data that's stored 180 days
        - ❗ Only supported for Block Blobs
- Changing storage tiers incurs charges
- ❗ Can't change the Storage Tier of a Blob that has snapshots

- Azure Blob Storage Lifecycle Management Policies
    i. E.g. configure a policy to move a blob directly to the archive storage tier X days after it's uploaded
    ii. In portal: Storage Account → Blob Service → Lifecycle Management
    iii. Executed daily



Manage storage

- Export/ import with Azure job
    - Securely import/export large amounts of data with physical drives
    - Create jobs (import or export) using Azure portal or rest API
    - Import job : import to Azure BlobStorage and Azure File
    - Export job : export from Azure BlobStrorage Only
    - Driv shipped to microsoft
    - WAImportExportTool
        - WaImportExportV1 for import to blob:
        - WaImportExportV2 for import to FileStorage

```
.\WAImportExport.exe PrepImport
    /j:<JournalFile>
    /id:<SessionId>
    [/logdir:<LogDirectory>]
    [/sk:<StorageAccountKey>] [/silentmode]
    [/InitialDriveSet:<driveset.csv>]
    /DataSet:<dataset.csv>
```

WAImportExportTool

- CLI tool run on 64-bit Windows Only!
- Encryption, decryption and data copy
- Creation of journal files
- Determine number of drives needed for export job
- Understand uses for driveset.csv and dataset.csv)

Importing data

- Create import job
  - i. Create storage account
  - ii. Prepare the drives
    - Connect disk drives to the Windows system via SATA connectors
    - Create a single NTFS volume on each drive
    - Prepare data using WAImportExportTool
      - Modify dataset.csv to include files/folders
      - Modify driveset.csv to include disks & encryption settings
      - Copy access key from storage account
  - iii. In Azure → Create import/export job → Import into Azure → Select container RG → Upload JRN (journal) file created from *WAImportExportTool* → Choose import destination to the storage account → Fill return shipping info
  - iv. Ship the drives to the Azure data center & update status with tracking number
- Costs
  - i. Charged: fixed price per device, return shipping costs
  - ii. Free: for the data transfer in Azure
- ❗ No SLAs on shipping
  - i. Estimated: 7-10 days after arrival

Exporting data

- Import/Export Job

1. In portal: Azure → Create Import/Export Job → Choose Export from Azure
2. Select storage account and optionally containers

3. Type shipping info
4. Ship blank drives to Azure
5. Azure encrypts & copies files
    - Provides recovery key for encrypted drive.

Azure Data Box

- Microsoft ships Data Box storage device
    - Each storage device has a maximum usable storage capacity of 80 TB.
- It lets you send terabytes of data into Azure in a quick, inexpensive, and reliable way

Data Box Disk

- 35 Tb max the single disk

Data Box Gateway

- This device is an entirely virtual appliance. It's based on a virtual machine that you provision in your on-premises environment.

- Online data transfer is ideal when you need a continuous link to transfer a massive amount of data.

Azure Stack Edge device

- Azure Stack Edge devices are online physical appliances that provide data preprocessing and machine learning before transfer to the cloud.

- Install and use Azure Storage Explorer
    - Azure Storage Explorer
    - Manage Azure storage from your desktop
    - Cross-platform client application to administer/view storage and Cosmos DB accounts.
        - Can be downloaded with Storage Account → Open in Explorer in Portal.
        - Available in Azure portal as well (preview & simpler)
    - Can manage accounts across multiple subscriptions
    - Allows you to
        - Run storage emulator in local environment.
        - Manage SAS, CORS, access levels, meta data, files in File Share, stored procedures in Cosmos DB
        - Move data to and from Azure thought internet

        - Manage soft delete:
            - Enables recycle bin (retention period) for deleted items.
    - Connecting and authentication
        - Admin access with account log-in
        - Limited access with account level SAS

- Copy data by using AZCopy
    - AZCopy

    - Copy blobs or file to or from storage account
    - Installed by dowloadinf from Microsft
    - SAS, Access Key and Azure AD Auhtentifcation

    - You can use AzCopy command-line utility tool.
    - No limit to # of files in batch
    - Pattern filters to select files
    - Can continue batch after connection interruption
        - Uses internal journal file to handle it
    - Copy newer/older source files.
    - Throttle # of concurrent connections
    - Modify file name and metadata during upload.
    - Generate log file
    - You Copy files between storage accounts
    - You can aloso sync files beetween stroage account

AzCopy

- Command-line utility that you can use to copy blobs or files only to or from a storage account.
- Copy the contents of a folder to the public container in an Azure Storage account
    - azcopy cp "/path/to/dir" "https://[account].blob.core.windows.net/[container]/[path/to/directory]?[SAS]" –recursive
- Create a container or file share represented by the given resource URL.
    - azcopy make https://[account-name].[blob,file,dfs].core.windows.net/[top-level-resource-name]
- Sync files beetween stroage account

  azcopy sync `'https://<source-storage-account-name>.file.core.windows.net/<file-share-name><SAS-token>' 'https://<destination-storage-account-`

    - Blobs
        - You can provide authorization credentials by using Azure Active Directory (AD), or by using a Shared Access Signature (SAS) token.
    - Files

- **Only Shared Access Signature (SAS) token is supported for authorization of copy File storage.**

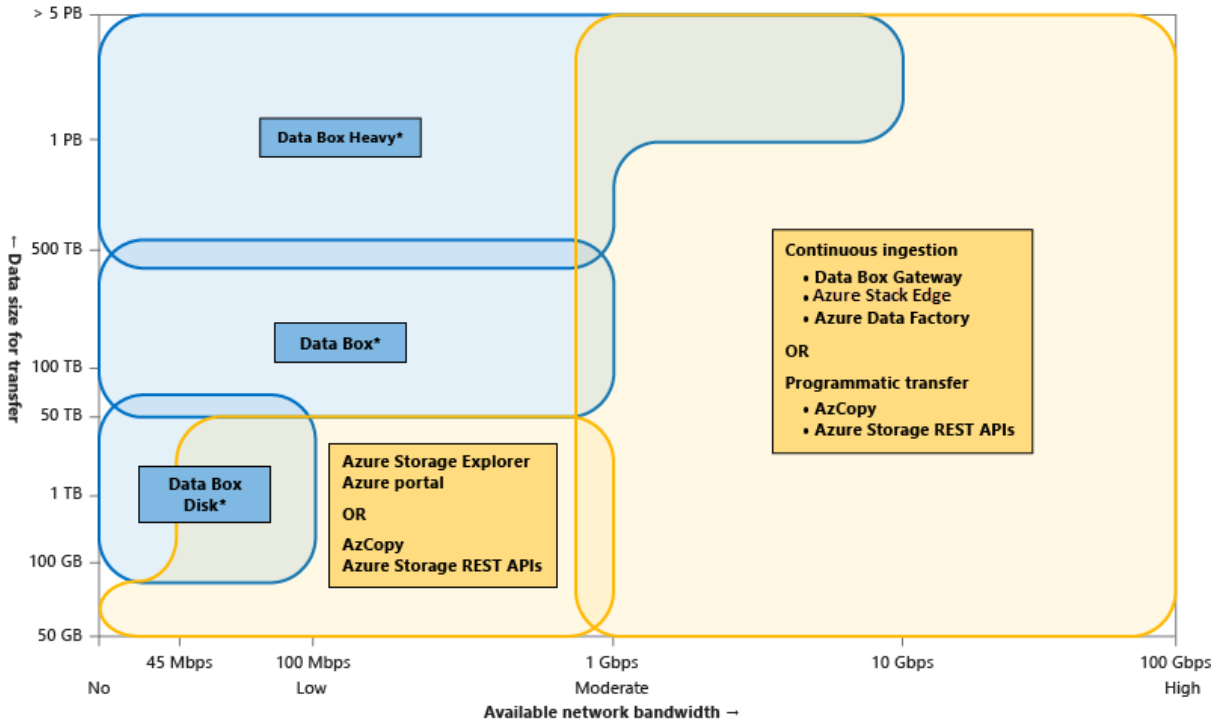
AUTHORIZE PY

Storage typeAZCO	Currently supported method of authorization
Blob storage Azure	Azure AD & SAS
Blob storage (hierarchical namespace)	Azure AD & SAS
File storage	SAS only

```
azcopy [command] [arguments]
--[flag-name]=[flag-value]
```

AzCopy Syntax

```
azcopy copy 'H:\data'
'https://sablobstore001.blob.core.windows.net/blobdata' --
recursive
```



- Create and configure Azure File Sync service
  - Azure File Sync service
    - Over SSL 443
  - Cloud Endpoint
    - Azure file share being sync
  - Server Endpont
    - Windows server
  - Sync Group
    - Définie the relationship beetween cloud endpont and server endpoint
    - Only 1 cloud endpoint
    - Multiple server endpont

    Cloud tiering allows frequently accessed files to be cached on the local server. Infrequently accessed files are tiered, or archived, to the Azure file share according to the policy you create.

  - **Cloud endpoint** is **scanned by the detection job every 24 hours** so if you add file to cloud endpoint you will need to wait 24h to see the files in the one-premise (server endpoint)

  - **Servers endpoint (on-premises)** file is scanned and **synced automatically after it's being added**, so if you add file to server endpint you will see it imediatly in the cloud endpoint

    Azure needs to have port 445 open to connect to Azure datacenters.

    Your on-premises server need to support SMB encryption.

Workflow for replication

0. Step 0 : **Check server compaltibility** : Install the **Azure PowerShell module** on the **server** and use the cmdlet **Invoke-AzStorageSyncCompatibilityCheck.**

1. **Deploy a storage account**
2. **Deploy a Azure File Share**
3. **Deploy Storage Sync service**
    - **Must be in same region as storage account**
4. **Create a sync group and cloud endpoint**
    - **Sync group has:**
        - **Storage account & file share**
        - **Server endpoints**
        - **Cloud endpoints**
5. **Register server**
    - **On portal: Sync Service → Registered Service → Download Azure File Sync Agent**
    - **Install the service and register the server**
6. **Add file share into the** sync group **as server endpoint**
    - **You can have only 1 cloud endpoint for the same sync group**
    - **You can enable/disable cloud tiering**
7. **Install agent on file server**
    - **Supported >Windows Server 2012**
    - **Selected files can be skipped**
8. **Register server to the *storage sync service* as server endpoint**

Scale and Limits

- 15 **storage sync services per subscription**
- 30 **sync groups per storage service**

- 1 **cloud endpoint and** 50 **server endpoints per sync group**
- 4 **TB maximum space**
- 100 **GB maximum file size**
- 64 **KB minimum file size to be tiered**

  -

-

03 Deploy and manage Azure compute resources

Automate deployment of virtual machines (VMs) by using Azure Resource Manager Templates

  - **ARMS Templates**
    - **Json Format**
    - **Use to create or modify resources in Azure**
    - **Submit template to the Azure Resource Manager**
  - **Modify ARMS Template**
    - **Can modify existing template in portal**
      - **Choose Export template under Automation Section**
      - **Select Delploy and chose to edit template**
      - **Make change and save**

- **save a deployment as an Azure Resource Manager template**
  - **1) Go to resource group in portal**
  - **2)go to demployemnt -> template in the rg level**
  - **3) Download the template and parameters files**
  - **4) You can also add the template to library**

- **deploy from a template**
  - **go to templtares**
  - **select the template you saved and click « redeploy »**

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

- **modify an Azure Resource Manager template**
  - **1) Generate a template in the portal**
  - **2) Donwload the template**
  - **3) Edit en deploy modified template**

- **Automate configuration managmenet by using custom Script extension**
  - **Scripts can be located anyware as long as the VM has acces to it**
  - **Scripts can also be deployed with ARM templates as well**
  - **The provider will be Microsoft.Compute/virtualMachines/**
  - **Script will only run once**

- What is an Azure custom script extension?
  - An Azure custom script extension downloads and runs a script on an Azure VM. It can automate the same tasks on all the VMs in a scale set.

  - Store your custom scripts in Azure Storage or in GitHub. To add one to a VM, you can use the Azure portal. To run custom scripts as part of a templated deployment, combine a custom script extension with Azure Resource Manager templates."

- configure a virtual hard disk (VHD) IMAGE
  - as a managed image
  - you're adding an app, configuration, updates and the you sysprep and create the image
  - use waagent for prep linux machine
  - managed image can support 20 simultaneous deployments
  - Snapshots
    - Read-only full copy of a managed disks
    - You can create new VMs based on snapshots
  - Images
    - Generalized VM disk images
    - Snapshots can be converted into imag
  - Capture an imag
    - 1) first thing to do is to Sysrep with the generalize option
    - 2) then we capture the image provide a name for the image
    - 3) the you can choose to delete automaticlelly the VM after creating the image
    - 4) write the name of the captured VM to confirm that we want to proceed
  - Get a snapshot image
    - Go to Disks → Select OS disk → Create snapshot
    - In snapshot → Click on Export → You will get SAS url → Download VHD
    - Generalize the image

- deploy virtual machine extensions
- Azure Automation State Configuration
  - It is an Azure configuration management service that allows you to write, manage, and compile PowerShell Desired State Configuration (DSC) configurations
  - for nodes in any cloud or on-premises datacenter.
  - Variety
    - Azure virtual machines
    - Physical/virtual Windows machines on-premises, or in a cloud other than Azure (including AWS EC2 instances)
    - Physical/virtual Linux machines on-premises, in Azure, or in a cloud other than Azure
  - Flow :
    - Step 1: Upload a configuration to Azure Automation State Configuration.
    - Step 2: Compiling a configuration into a node configuration
    - Step 3: Onboard the virtual machines to Azure State Configuration
    - Step 4: Assign the node configuration.

        - Step 5: Check the compliance status of the node.

Configure VMs

- Configure Azure Disk Encryption(ADE)
    - Full disk encryption of the OS and data disk
    - Azure disk encryption is integrated with azure Key Vault
    - VM's must be able to connect to either AzureAD or the KeyVault endpoint
- VM Disk Encryption
    - Use Bitlocker feature
    - Use DM-Crypt system in Linux
    - Requiere that Encroypted VM must be backed up to Recovery service Vault

- Move VMs from one resource group to another
    - Moving a VM to anotger subscription requieres moving all dependent items
    - VM scale sets with standard load balancers and standars public IP cannot be moved
    - Vm integrated with key vault for disk encryption cannot be moved
    - Move VM Powerhshell
        - `Move-AzResource` -DestinationResourceGroupName -ResourceId
        - `Move-AzResource` -DestinationSubscriptionId -DestinationResourceGroupName -ResourceId
- Manage VM sizes
    - VM will reboot afeter being resized that cause downtime
    - You can do it live but best paritice is to shudown the vm before resize
- add Data disks
    - can add a new or existing data disk
    - adding managed disk allows you to chose from source types of BLOB or Snapshots
    - Managed disk provide a SLA a 99,95 %
    - Your VMs should use managed disks if you want to move them to an Availability Zone
    - a disk added can be detached and add to a other VM
    - only 1 VM can be atached to 1 disk a the same time
    - they have a limit of disk you can add dépend of the VM size
- Step to Add data disk to an virtual Machin VM Powershell
    - Create the VM
        - `New-AzVm`
    - Create the Disk configuration (diskset)
        - `New-AzDiskConfig`
    - Create the Data Disk
        - `New-AzDisk`
    - Add the disk to the VM
        - `Add-AzVMDataDisk`
    - Update the VM
        - `Update-AzVM`
- Configure networking of VM
    - Vnet
        - Role needed for manage VNET

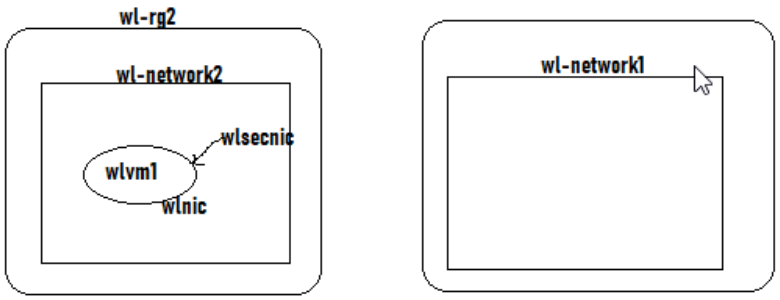
- Network contributor
  - When creating an azure VM you must create a virutal nework or use and existing Vnet
  - There is no security boundary between subnets by default
  - it's possible add multiple address spaces within an Azure VNET that can be disjointed. For example, 10.0.0.0/8 and 192.168.0.0/16 could be within the same virtual network. Azure will automatically enable routing between VMs that are part of virtual subnets in different address spaces within a virtual network.

- NIC
  - To add a nic to an existing Vm it must first be deallocated(must stop the vm from the portal before add the nic)
  - A deallocated VM release dynamically assigned public IPs
  - A NIC can only be assigned to a vritual network that exists in the same location as the NIC
  - Th public IP is only allocated when the VM is running state if not the ip is relase and you will not see it in the nic pane
  - 

: VM is running
  - 

: VM is stopped
  - In order to attach a Network interface to a vitrual machine, it must be created in the same région as the virtual machine .it also is a part of the same virtual network hosting the virtual machine
  - The network interface for à Virtual Machine can have both a private and a public IP adress
  - To add a nic to an existing Vm it must first be deallocated(must stop the vm from the portal before add the nic)

  - You can associate multiple NICs on a VM to multiple subnets, but those subnets must all reside in the same virtual network (vNet)
  - You can change the subnet a VM is connected to after it's created, but you cannot change the VNet.
  - For change of VNET you must delete the VM (keep tje disk) and recreate it in the Vnet



  -

- Redeploy VMs
  - Use when you cannot connect vira RDP or SSH
  - Redeploy shutdown the VM and move to a new node and powers back up

- Redeploy Windows virtual machine
  - If you have been facing difficulties troubleshooting Remote Desktop (RDP) connection or application access to Windows-based Azure virtual machine (VM), redeploying the VM may help. When you redeploy a VM, Azure will shut down the VM, move the VM to a new node within the Azure infrastructure, and then power it back on, retaining all your configuration options and associated resources.
- Disk D in default VM deployement
  - D is temporory disk
  - Redeploy - Try redeploying your virtual machine, which will migrate it to a new Azure host. If you continue, the virtual machine will be restarted and you will lose any data on the temporary drive. While the redeployment is in progress, the virtual machine will be unavailable.
- Redeploy Powerhsell
  - `Set-AzVM` -Redeploy -RessourceGroupName -Name
- Redeploy CLI
  - Az vm redeploy –resource-Group --name

- Configure high Availability
  - Availabilty option
    - Availability Zone
      - Availability zone distribute VM across Azure regions
      - Azure regions of 3 zone
      - Standars SKU Load Balancer Only can accept AZ
      - Standars SKU Public IP requiered for Az
      - SLA : All VM that have 2 or more instance in AvZone have 99,99 of SLA
    - Avalability Sets (Fault Domains, Update Domains)
    - Distribute across a single data center
    - 5 udpate domains by default (can up to 20)
    - Connot add a VM to AvailSet post deployment (Must be done at creation)
    - SLA : All VM that have 2 or more instance in AvSet have 99,95 of SLA
      - Fault Domaine
        - 3 max
        - Rack of servers in Azure that share power source and physical switch
        - Protect again Rack failure
      - Update Domains
        - 20 max
        - Protect against normal maintenance updates
        - VMS in the same update domain restart together during planned maintenance
        - Only one update domain restart at a time
- deploy and configure scale sets
- VM Scale Sets
  - SLA
    - Scale Sets is a free service,
    - it does not have a financially backed SLA itself.

        - However, if the Virtual Machine Scale Sets includes Virtual Machines in at least 2 Fault Domains (AvSet, Az), the availability of the underlying Virtual Machines SLA for two or more instances applies.
    - can be vertical :
        - https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-vertical-scale-reprovision
    - And horizontal (classic add vm instance)

    - Scalability options
        - Scale Sets
            - Group of load balanced virtual machines
            - 2 or more VMs recommended
            - Can sclae automatically based on demand or schedule
            - Can be delpoyed across multiple update/fault domains

Create and configure containers

- Azure container networking interface
    - Availabe for AKS and Az Container
    - With AzCNI every pod gets an IP address from the subnet and can be accessed directly

- Azure container instance is the quiquest way to deploy conatainer to azure en comparaison a aks ou il faudra créer un cluster et gerer l'orchestration
- ACI is for smallest application without need of cluster or scalling
- Configure sizing and scaling for Azure Container Instances
- Configure container groups for 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)
    - Create AZ Container CLI
        - az group create –name --location
        - az container create --resource-group myResourceGroup --name myContainer –image mrc.microsoft.com/azuredocs/aci-helloword –dns-name-label az104-demo –port 80 –restart-policy Always
- Configure storage for Azure Kubernetes Service (AKS)
- Create and configure AKS
    - You dont pay for the Master or the pod only for the node VM
    - Vous payez uniquement les instances de machine virtuelle, le stockage et les ressources réseau consommés par votre cluster Kubernetes.
    - The AKS Cluster must use virutal machien scale sets for the nodes for autoscalling and multiple node pools
    - All node pool must reside in the same Vnet

    - AKS cluster must use the Standar SKU load balancer to use multiple node pools
    - Create AKS Cluster CLI
        - az group create –name --location
        - az aks create --resource-group myResourceGroup --name myAKSCluster --node-count 1 --enable-addons monitoring --generate-ssh-keys
    - Create a AKS Single Node Cluster
        - Az aks create –resource-group –name –vm-set-type VirutalMachineScaleStes –node-count 2 –generate-ssh-keys –load-balancer-sku standart
- Configure scaling for AKS
    - Increase the number of pode
        - Kubectl scale –recplicas=3 «name of the pods service »
    - Increse the number of nodes
        - az aks scale --resource-group $RESOURCE_GROUP --name $AKS_CLUSTER --node-count 2
        - From the portal => node pools => Scale
    - Autoscal :
        - Kubectl autoscale
- Upgrade an AKS cluster
    - `az aks get-upgrades`
    - `az aks upgrade`
- Azure Kubernetes node
    - A node in Kubernetes is a virtual machine.
- Kubernetes pods
    - Pods are known to be the smallest deployable units of computing. It simply means that a pod can contain at least one container.
    - Pods are in the nodes like VM in Hyper-v host
- Kubectl
    - Kubectl is a command-line client that provides you with the ability to manage your Kubernetes instance. There are a lot of commands, and here I presented only a small subset of them:
        - Install Kubetcl with cli
            - az aks install -cli
        - First you connect to the AKS Cluster in CLI :
            - Az aks get-credenials –resource-group --name
        - To show all your nodes you can use this command.
            - kubectl get nodes
        - A similar command is used to display information about your pods:
            - kubectl get pods
        - Get servcice running on nodes
            - Kubetcl get service
        - To create resources defined in the YAML file you should use:
            - kubectl apply -f ./myFile.yaml
        - When you want to manually scale the resources to 5 you can do it by this command:
            - kubectl scale --replicas=5 -f ./myFile.yaml
- Configure network Networking AKS
    - kubenet :

- with kubenet nodes get an IP address from the subnet's VNET,and pods receive an ip address from a logically different address space to the subnet's VNET of the nodes NAT is then configured so the pods can reach ressources on the VNET the ip address is NAT'd to the nodes ip address

- **Azure Container Netwok interface** :
  - with ACNI every pod gets and IP address directly from the subnet and can be accessed directly

Create and configure Azure App Service

- **Create and configure App Service plan**
  - **Choose between Linux and Windows OS**
  - **App service plan are assiocied to one ore more App service**
  - **Auto scale and backup start to Standard plan minimum**
  - **Standard instance max : 5**
  - **Premium v2 instance max 20,**
  - **Premium v3 : instance max 30**
  - **The app must be running in the Standard, Premium, or Isolated tier in order for you to enable multiple deployment slots and Backup , Autoscale. Free and Shared Basic are out**
  - **The app must running in Basic,Standard premium or isolated to be alway on. Free and Shared are out.**
  - **The app must be running in Shared,Basic Strandard premium isolated for CustomDomain. Free is out**

Create and Configure App Service Plans

Features	Free/shared	Standard	Premium v2	Premium v3
Custom domain	Shared D, B	Yes	Yes	Yes
Scale	B manual (3)	Auto 10	Auto 20	Auto 30
Staging slots	--	5	20	20
Daily backups	--	10	50	50
Traffic Manager	--	Yes	Yes	Yes

The backup and restore option is available with the Standard App Service Plan. This is also mentioned in the Microsoft documentation.

	FREE	SHARED	BASIC	STANDARD	PREMIUM	ISOLATED	APP SERVICE LINUX
64-bit			✓	✓	✓	✓	✓
App Service Advisor			✓	✓	✓	✓	✓
Always On			✓	✓	✓	✓	
Authentication & Authorization	✓	✓	✓	✓	✓	✓	
Backup/Restore				✓	✓	✓	✓

- **Create App Servuce using Azure CLI**

- **Create and configure App Service**
  - **Web app and App Service plan need to be in the same region**
  - **You can't mix Windows and linux apps i the same App service plan (choose eteher linux plan or windows plan)**
  - **« .Net core » is supported on both Windows and linux (other .Net than core support only windows)**
  - **Autoscalling is determined by rules based on treshold metrics defined**
  - **Create App Servuce using Azure CLI**
    - **Create the RG : Az groupe create –name –location**
    - **Create the App servuce plan : Az appservice plan create –name psap –resource-group ps-app-rg –sku F1 –is-linux**
    - **Create the Web app : Az webapp create –name dotnetapp –resource-group ps-app-rg –plan psasp**
  - **App/OS Association**
    - **.NET Core**
      - **Windows**
      - **Linux**
    - **PHP All versions**
      - **Windows**
      - **Linux**
    - **ASP.NET**
      - **Windows**
    - **Ruby**
      - **Linux**
- **create an App Service plan**
- **configure scaling settings in an App Service plan**

    - Scale up pane
        - Increase to a biggest service plan
    - Scale out pane
        - Increase instance
    - Autoscale
        - Atoscale start to the Standard plan (S)
        - Autoscale is only to Scale out
        - Create rule based on metric
        - Add scale down rule
- create an App Service
- secure an App Service
- Configure custom domain names
    - Custom domains pane
        - Can force HTTPS Only
        - Can add custom domain
    - 1 - Verify your Domain with TXT record
    - 2 - record or an A record to map a custom DNS name to App Service (IP Name association)
- Configure backup for an App Service
- Configure networking settings
    - Networking pane
        - Confivire Vnet integration
            - Outbound connection from the web app to ressource in a VNet
            - Permettant a L'app d'acceder a des VM ou des Base de donné presente sur le VNET autorisé
        - Azure front door
            - Load balancer fonctinnant a l'echel mondial
- Configure deployment settings
- Deployement slots :
    - Lorsque vous déployez votre dans Azure App Service, vous pouvez utiliser un autre emplacement de déploiement que l'emplacement de production par défaut
    - Accessible au niveau de plan Standard, Premium ou Isolé d'App Service.
    - Les emplacements de déploiement sont des applications en production pourvues de leur propre nom d'hôte. Les éléments de contenu et de configuration des applications peuvent être échangés entre deux emplacements de déploiement, y compris l'emplacement de production.
- Swap
    - When you swap deployment slots, Azure swaps the Virtual IP addresses of the source and destination slots, thereby swapping the URLs of the slots.
    - We can easily revert the deployment by swapping back.
- Deployement slots options :
    - The app must be running in the Standard, Premium, or Isolated tier in order for you to enable multiple deployment slots.

    - You can specify that 80% of the workload will be sent to the old (production) version and 20% to the new version:

- Dans la colonne % de trafic de l'emplacement vers lequel vous souhaitez acheminer le trafic, spécifiez un pourcentage (compris entre 0 et 100) pour représenter la quantité totale de trafic à diriger. Sélectionnez Enregistrer.
- You can also set that new version of the app won't be available to the users before it is verified by a QA team. After the testing, you can swap the versions:

- Azure Automated deployement
  - currently supports Azure DevOps, GitHub, Bitbucket, OneDrive, Dropbox, FTP, local Git and external Git repositories.for automated deployment

04 Configure and manage virtual networking

Implement and manage Virtual networking

- create and configure virtual networks, including peering

Connecting VNets

- You don't need to have a Layer 3 router to route traffic from subnet to subnet
- Azure system routes take care of the routing for you automatically

Options

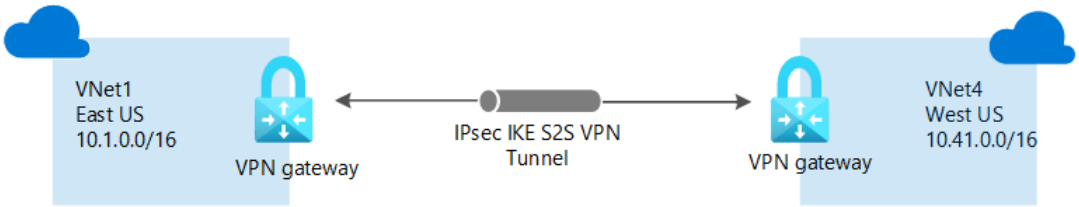
- VPN Gateway

- Creates IPsec/IKEv2 tunnel and always-on connection
- Used for connecting VPNs in cloud or hybrid scenario.

Inside Azure

- VNet-to-VNet VPN

  - You can connect VNET to VNET creating a virtual network gateway and a GatewaySubnet for each VNET and etablish a tunel encrypted :



You need to have enought of ip mask for create a Gateway subnet /27 in each VNET

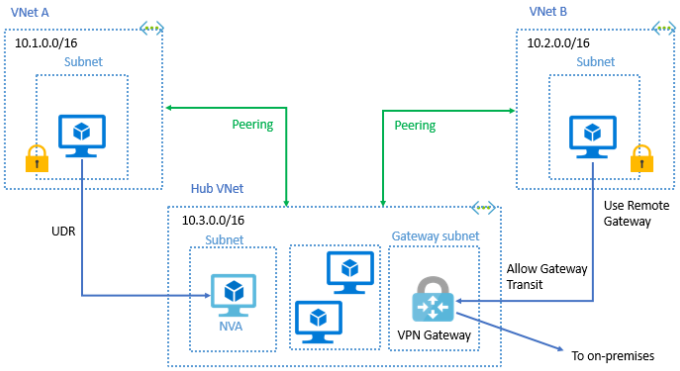
- Create isolation or administrative boundaries
- Provide cross-region geo-redundancy and replication securely
- No traffic crosses the public internet
- Separate VPN gateways costs while VNet peering is free.

- 💡 **Make sure your VNet address spaces do not overlap.**
- **Troubleshooting**
  - **Verify connectivity through peering**
    - **Set up Azure DNS**

- **VNet peering**

  - **Peering is bidirectional the peering is not established if you set up the peering only in 1 direction**

  - **VNET PEERING Scope**
    - **Across RG**
    - **Across subscription**
    - **Across region using Gloval peering**
      - **You can peer across VNets in any Azure public regions with non-overlapping address spaces**



  - **❗ Seamless connection between two Azure VNets.**
    - **The peered networks appear as one, for connectivity purposes.**
    - **Name resolution does not flow, requires own DNS zone**
  - **Runs on Azure backbone**
  - 💡 **You can peer across regions and subcriptions**
  - **Peering can overcome misplaced VMs**
- **Save money with service chaining (e.g. services' communication are chained through a subnet)**
- **❗ Peering must be done on both sites**
  - **VNet1 <=> VNet2 and VNet2 <=> VNet1**
- Configuration
  - Allow forwarded traffic
    - **Am I peering from a hub VNet that'll have IP-forwarder?**
    - **Allow peers (other VNets) to forward traffic to go through.**
  - Allow gateway transit
    - **Am I hosting a VPN gateway?**
  - Use remote gateways
    - **Is this network use peers gateway?**

        - ❗ **VNets must be in same region**
- **Enables** force tunnelling
    - **E.g. when all Internet traffic must go through on-premises firewall device.**
    - **You can use *user defined routes* for all outbound traffic to go back through VPN gateway to on-premises.**
- ❗ **Peerings are not transitive**
    - **If you peer spoke1 <=> spoke2 and spoke2 <=> spoke3 then spoke1 cannot communicate with spoke3 automatically.**
    - **Common solution is transiting VNet with** Hub and Spoke topology**.**
        - **Topology is a segmentation**
            - When to segment with VNets and when with subnets?
                - **Depends on bureaucratic reasons**
                - **E.g. different VNets when**
                    - **Different cost centers/groups need management autonomy**
                    - **You want to completely isolate different workloads**
        - **Name resolution needs configurations**
            - **You can't do with Azure provided DNS as all your hosts have then internal.cloudapp.net**
            - **In peering azure provided DNS won't work**

- **Hybrid Connections**

    - **Site-to-site VPN**

        - **Two VPN devices connect to each other.**
        - Flow
            i. **Deploy a VPN Gateway resource in Azure**
                - **Requires gateway subnet (or DMZ subnet).**
                - **Different SKUs: Basic, VpnGw1, VpnGw2, VpnGw3**
                    - **You get more bandwidth, site-to-site and point-to-site points.**
                    - **Don't use basic for production**
                - **You can see the deployed VPN Gateway in *Connected Devices* in subnet.**

            ii. **Deploy a Local Network Gateway as well.**
                - **For your on-prem gateway device, you need to set up one of the route table configurations:**
                    - **PolicyBased**
                        - **Handle route tables manually**
                        - ❗ **Does not work with BGP failover, active-to-active configurations**
                    - **RouteBased**
                        - 💡 **Always use if possible**

        - Some VPN devices do not support it
        - What's compatible is documented on Microsoft docs.

    iii. Create a connection between two gateways
        - Create local-to-azure in Local Network Gateway
        - Create azure-to-local in VPN Gateway
        - In Shared Key in connection blade, specify a key.

- Modify local network gateway IP after a change of local public IP steps :
    - 1 – Remove the connection
    - 2 – Modify the local network gateway
    - 3 – Recreate the connexion

    - Point-to-site VPN

        - Allows access to Azure resources through VPN tunnel from a client agent.
        - More portable way
        - Flow
            i. On Azure deploy VPN gateway
            ii. In Point-to-site configuration blade download VPN client
            iii. Deploy agent (a VPN Client) from VPN gateway
            iv. Install on individual endpoints (e.g. laptops)
        - Allows connection outside network perimeter

    P2S VPN client

    - SKU
        - Basic dont support IKEv2 and OpenVPN Connections
        - VpnGwx support all the protocal
        - The VPN type must be Route-based.
        - Policy-based VPN gateways are not supported for point-to-site VPN connections.
            - If you have created a PolicyBased VPN Gateway you must delete it and create a RouteBased VPN Gateway if you want create a P2S Connexion
    - Protocol
        - OpenVPN (SSL/TLS)
            - Windows, Linux Mac
            - Client
                - OpenVPN Client, Azure VPN client
        - Secure Socket Tunneling Protocol (SSTP)
            - Windows 7 and later
            - Client
                - Native VPN client of windows
        - IKEv2 VPN

        - Mac device
        - Client
            - Native VPN client of MAC
- Authent methode
    - Using AAD
        - (Requiere of use Azure VPN client throught OpenVPN protocol)
    - Using certificate
        - (Windows VPN client package, OpenVPN Client, SSTP, IKev2)
        - Step
            - 1st confiig
                - Generate root certificat from client or AD
                - Generate the client cert
                - Copy the root cert key and past it to the root certificat on the P2S configuration page
                - Save
            - Client Cert
                - You can ether 1 :
                    - Generate en new client cert from the root cert if you have it installed on your pc and install it
                - Or you can 2 :
                    - Export a client cert generated from a other PC
                    - you need the password that was created when the client certificate was exported.
                    - Copy the client to yout pc and install it
    - Using AD (need RADIUS)
        - IKEv2 and SSTP and OpenVPN through PowerShelle

- Express route

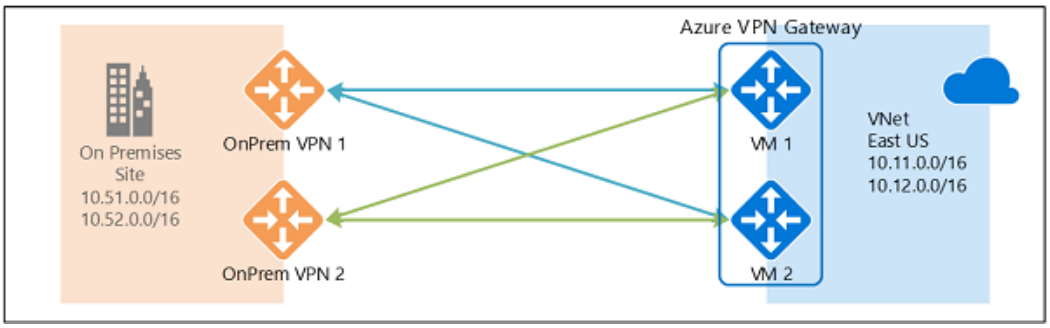
    - SKU :
        - VpnGw1 SKU is required since ExpressRoute is not supported by Basic SKU

    - High speed secure connection between on-prem and cloud

    Best practices for High Availability

    - Combine ExpressRoute and VPN
        - In gateway subnet
            - Deploy ExpressRoute gateway

        - **Deploy VPN Gateway**
    - **Both gateways gives access to front-end tier and a jumpbox in a management subnet**
    - **If ExpressRoute goes down VPN gateway gets activated**
- Deploy two VPNs
    - **Requires enabling BGP in gateway link**
        - **Robust routing**
        - **Enable active-to-active connection configuration**
        - **Only allowed RouteBased routing configuration**



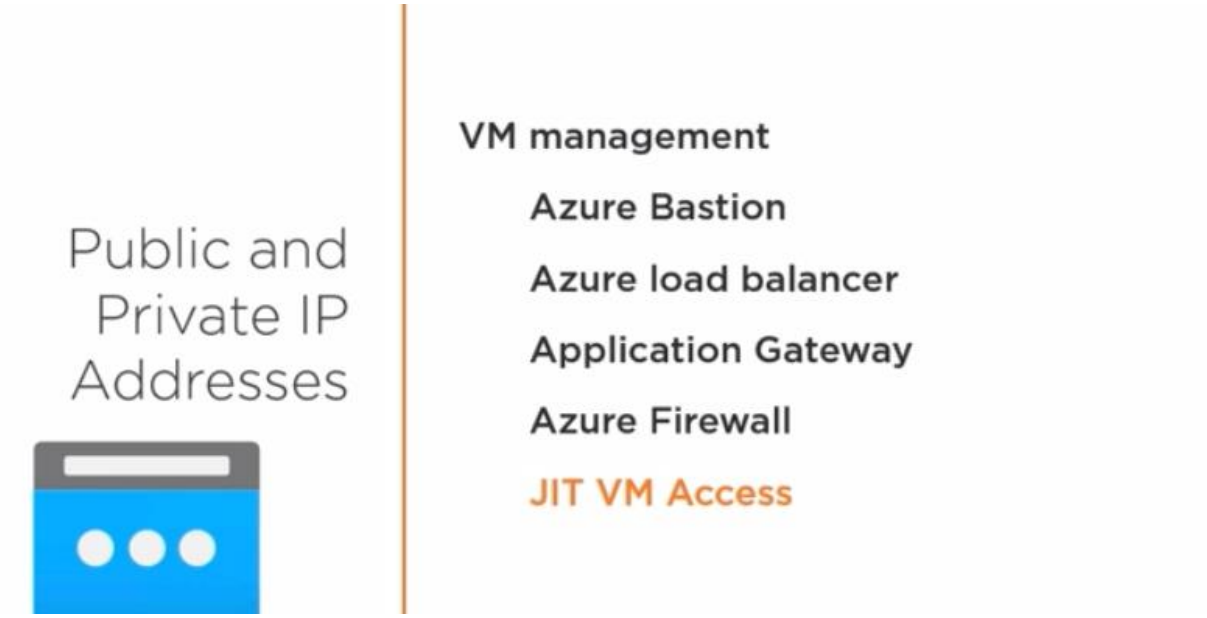
    - **Two VPN gateways on-prem**
        - **Allows redundant active-to-active connection to single gateway.**
        - **You have one active and one stand-by gateway**
- **Exress route direct**
    - **New function allow to connect directly to one of microsoft backbon instead of connect to provider**

- **System Routes vs. User-defined Routes**

- Situations
    - **You need to move one VM to another VNet.**
        - **It requires re-deploying**
    - **Isolation & segmentations**
        - **E.g. development / production VNet**
    - **Hub & Spoke Topology**
        - ***Hub*: VNet have Virtual Network Appliance (e.g. firewall), or gateway**
            - **You don't want to have *Virtual Network Appliance* as it costs both money and resources.**
        - ***Spokes***
            - **Other VNets (e.g. front-end, back-end)**
            - **You can force communicates with each other through Hub.**
- **Internet calls and calls from internet**
    - **Handled by Azure using system routes**
    - **You don't need to manipulate them**

- If you want to override system routes (e.g. for Hub & Spoke topology)
    - You need User Defined Routing
    - For network appliance you need to configure IP forwarding
        - Enables it to pass on traffic that it's not destined for itself.

- Configure private and public IP addresses



- Configure user-defined network routes
- implement subnets
    - Azure réserve 5 adresses IP dans chaque sous-réseau. Il s'agit des adresses x.x.x.0-x.x.x.3 et de la dernière adresse du sous-réseau. Dans chaque sous-réseau, la plage x.x.x.1-x.x.x.3 est réservée aux services Azure.
- Configure endpoints on subnets
- Configure private endpoints
- Configure Azure DNS, including custom DNS settings and private or public DNS zones

DNS & Name Resolution

Azure-provided name resolution

- No configuration required
- Name Given from azure by default
- All VMs within a VNet can resolve each others' host names
- ❗ Limitations
    - Cross-VNet name resolution
    - Issue: No custom DNS suffix
- You can add custom DNS server IP addresses

- E.g. in hybrid cloud if you want Azure VMs to have IP addresses from on-premises DNS server or vice versa.
- E.g. stand up own DNS servers in VNet instead.
- E.g. configure DNS forwarding between one DNS server in one VNet to another DNS server in another VNet

- Azure DNS

  - Azure DNS is a hosting service for DNS domains that provides name resolution
  - By hosting your domains in Azure, you can manage your DNS records by using the same credentials, APIs, tools, and billing as your other Azure services.
  - You can't use Azure DNS to buy a domain name. For an annual fee, you can buy a domain name by using App Service domains or a third-party domain name registrar.
  - Your domains then can be hosted in Azure DNS for record management. For more information, see Delegate a domain to Azure DNS.
  - To start hosting your domain in Azure DNS, you need to create a DNS zone for that domain name. Each DNS record for your domain is then created inside this DNS zone

- Allows VNETs to resolve each others host names.
- Host your public DNS domain in Azure
  - Use Azure geo-distributed name servers for high speed name resolution
  - Delegate a domain:
    a. Create a DNS Zone
    b. Copy an Azure DNS name server from the zone
    c. In the registrar's DNS management page, edit the NS records and replace the NS records with the Azure DNS name servers.
  - Azure public DNS zone
    a. You can configure Azure DNS to resolve host names in your public domain. For example, if you purchased the contoso.xyz domain name from a domain name registrar, you can configure Azure DNS to host the contoso.xyz domain and resolve www.contoso.xyz to the IP address of your web server or web app.

  - Azure private DNS :
- Create private DNS zones
  - Allows you to not route names in public DNS
  - Eclusive for VM (App service cannot get a Private dns name)
  a. To publish a private DNS zone to your virtual network, you specify the list of virtual networks that are allowed to resolve records within the zone. These are called linked virtual networks. When autoregistration is enabled, Azure DNS also updates the zone records whenever a virtual machine is created, changes its' IP address, or is deleted.

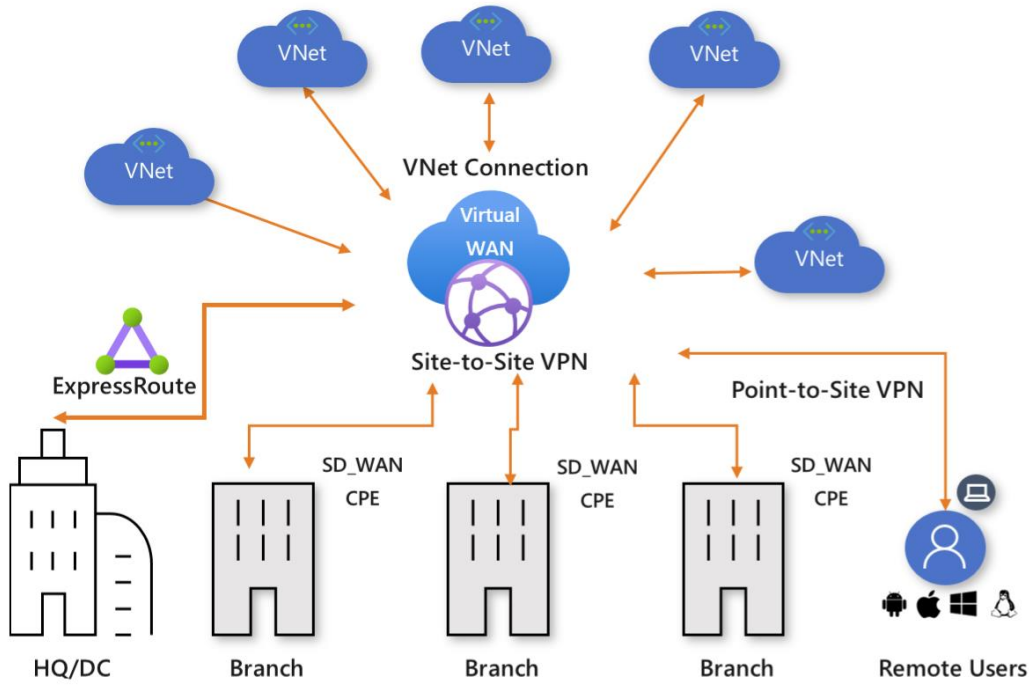
  -
  - Linked to VNets
    a. Lets you avoid setting up own DNS infrastructure

- Registration VNet
    a. You create private DNS zone and registration VNet
    b. Any VMs within that VNet will automatically have their names registered and DNS records created in Azure DNS
- Resolution VNet
    a. Allows you to have name resolution across VNets
    b. Other VNets will be resolution VNets
    c. Allows you to create records (hosts, alias) for VMs and it'll support name resolution across VNets

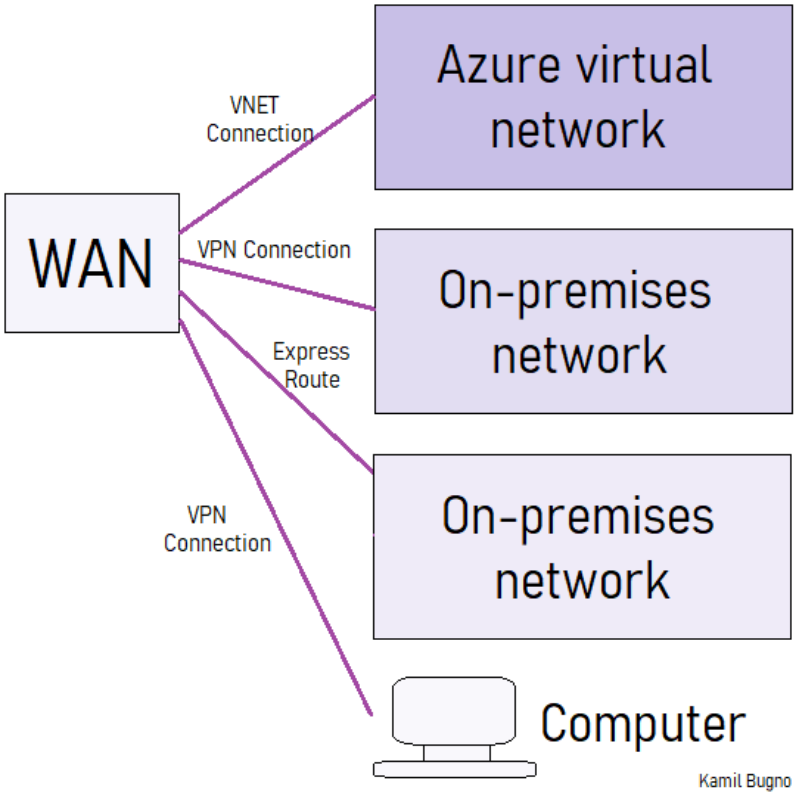
- You manage in Portal -> Private DNS zone
    - Each DNS zone has
        a. VNets of associated with it
        b. Record-sets: IP addresses and host names of VMs (A record for name resolution of VM)

Integrate an on-premises network with an Azure virtual network

- create and configure Azure VPN Gateway
-
- create and configure Azure ExpressRoute
    - High speed secure connection between on-prem and cloud
- configure Azure Virtual WAN
    - Concept de Base
        - You ahve 2 ore more office that need to comunicate to each other
        - You use Azure has a Hub for allow that
        - Its like a Site to site Vpn but for transitif connection cross multiple site



- If you have a highly developed network architecture that contains P2S VPN connections, S2S VPN connections, ExpressRoute and Azure virtual networks and you want to have the ability to connect it all together, you can use WAN:



  - Configure WAN
    - Hubs panes
      - Central point
      - Basicaly a Vpn gateway within Auzre

Secure access to virtual networks

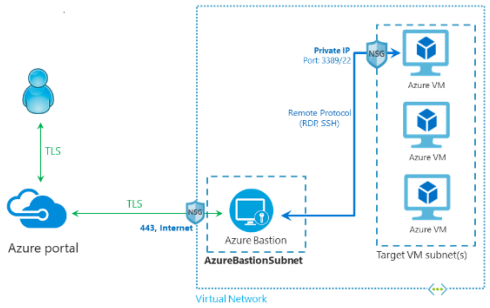
- Create Networks Security Rules
- NSG
  - The NSGs in Azure are Stateful. Meaning that if you open an incoming port, the outgoing port will be open automatically to allow the traffic.
  - The default rules in a Network Security Group allow for outbound access and inbound access is denied by default. Access within the VNet is allowed by default.
  - Like normal ACLs the rules are processed based on a priority. Lower is prior
  - NSGs can only be used in the Azure region that it was created in.
  - There is a soft limit of 100 NSGs per subscription and a soft limit of 200 rules per NSG.
  - You can't delete a default rules
  - Default rule
    - Inbout
      - Vnet
      - LoadBalancer
      - Deny all other

        - **Outbound**
            - **Vnet**
            - **Internet**
            - **Deny all other**

- **associate a network security group (NSG) to a subnet or network interface**
    - **pest pratice is too create role basec nsg like frontVM , backend etc**
      Go to network security groupe -> create your NSG
    - **NIC/subnets -> Network security groupe pane ->**
- **evaluate effective security rules**
    - **NIC/subnet-> effective security rules pane -> Edit -> choose the NSG created you want applied -> Save**
    - **Show all seucirty rule applied**
- **implement Azure Firewall**
    - **Configure Azure firewall**
        - **Userd defined route**
            - **Need to confugure a used defined route on a subnet**
            - **Select virutal apliance en put the privite ip of the firewall**
            - **If you wan to force the traffic of the subnet pass trhought the firewall**
        - **Rule :**
        - **Rule that are not specificly allow are deny**
            - **Application rule**
                - **Allow/deny traffic sortant vers un site (google.fr) /port**
            - **Networking rule**
                - **Allow/deny traffic sortant vers une IP / port**
            - **Nat Rule**
                - **Nat traffic from internet to Subnet VM (RDP)**
- **implement Azure Bastion**

  Azure Bastion Host

    - **Azure Bastion is a service you deploy that lets you connect to a virtual machine through RDP/SSH over TLS using the Azure portal.**
    - **secure and seamless connectivity.**
    - **PaaS service inside your virtual network in a subnet.**
    - **your virtual machines do not need a public IP address, agent, or special client software.**
    - **To create an Azure Bastion host you need to have the AzureBastionSubnet created as part of the virtuak network**



-

Configure load balancing

- **Configure Azure Application Gateway**

  - **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 vulnerabilities . 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***
    - ***Multi-site.***
  - ***Backend pools***
  - ***Health probes***
  - ***Session affinity***

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

Load Balancer

- Load Balancer Role :
    - Nework contributor :
        - Can manage the Load Balancer resources
        - For add a healthprobe
- Bacic Load Balancer
    - 300 instance
    - BackEnd : VM in a single AvSet or Virtual machine Scale Set
    - No Availability Zone
    - No SLA
- Standar Load Balancer
    - 1000 instance
    - Any VM or Virtual Machine Scale Set in a single VNet
    - Availability zone available
    - SLA : 99.99%

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

    - public load balancer
        - OSI Layer 4 TCP and UDP
        - Internet-facing, has public IP address
        - Offers two distribution modes
        - Set-up public load balancer
            - Settings -> Back-end-pools-> Add VMs
            - Settings -> Health-probe -> Add health probe
                - E.g. tcp-80-probe (HTTP) probe
                - Set interval -> time between prop events
                - Set unhealth threshold (e.g. 2) before VM is dropped out from the pool
                - Add load balancing port
                - Incoming request from port 80 (port) will be passed to TCP passed 80 (back-end port)
                - Select backend pool & health-probe
                - Set session persistance
                    - If you need to ensure that The same web server services all client for each request
                - Floating IP (direct server return)

        - Use with internal load balancers
        - Use with SQL server always on cluster
        - Used when same back-end port needs to be used across multiple rules in a single Load Balancer.
    - Add inbound NAT rule
        - Create a load balancer inbound network address translation rule to forword traffic from a specific port of the front-end IP address to a specific port of a back-end VM
    -
        - Map TCP 5000 to a VMs RDP port (3389)
        - Map TCP 5000 to a VMs RDP port (3389)
- internal load balancer
    - OSI Layer 4 TCP and UDP
    - Applies to traffic only within a virtual network
        - No public IP address
    - Good for applying load balancing to n-tier application services (database)

-
- troubleshoot load balancing

Monitor and troubleshoot virtual networking

- Monitor on-premises connectivity
- Configure and use Network Performance Monitor
- Use Azure Network Watcher
- troubleshoot external networking
- troubleshoot virtual network connectivity

Troubleshooting tips

- Azure blocks ICMP between Vnets and the Internet
    - ICMP is used for ping
    - Microsoft blocks it because of DDoS attacks.
- Simplify NSGs as much as possible to reduce troubleshooting friction
- Azure portal Diagnose and solve problems/Resource health blade is useful
- Network Watcher and Network Permormance Monitor make troubleshooting much easier
    - 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

05 Monitor and back up Azure resources

Monitor resources by using Azure Monitor

Azure Monitor :

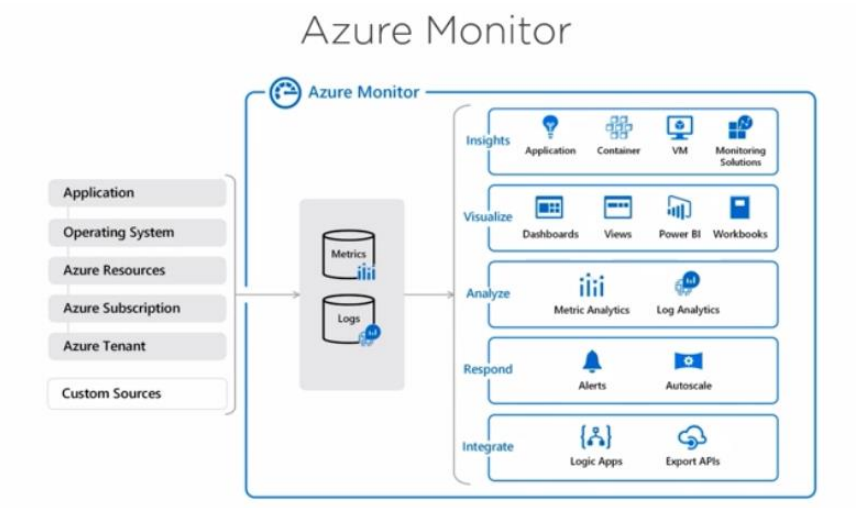
- **Diagnostic setting (Under Azure minitor) :**
    - Often done from resource level
    - Allow to generate log of different workload or metric
    - And store them to log analytics worksapce or storage account
    - In the creation of the VM you must « enable » monitoring for the monitoring agent to be installed and the log send to a storage account, l'agent peut etre reintstallé
    - You can select the treshoold logged the frequency and custom them

- **Alert :**
    - Alerts in Azure Monitor can identify important information in your Log Analytics repository. They are created by alert rules that automatically run log searches at regular intervals, and if results of the log search match particular criteria, then an alert record is created and it can be configured to perform an automated response
    - You can create alerts in resouce level
    - For creating an alert when error event are logged to the systeem log on a virtual machine you have to record the events in a logs analytics workspace, and then configure alerts in Azure monitor based on the azure log analytic worksapce
    - Alerts are created by alert rules in Azure Monitor and can automatically run saved queries or custom log searches at regular intervals. You can create alerts based on specific performance metrics or when certain events are created, absence of an event, or a number of events are created within a particular time window. For example, alerts can be used to notify you when average CPU usage exceeds a certain threshold, when a missing update is detected, or when an event is

generated upon detecting that a specific Windows service or Linux daemon is not running. If the results of the log search match particular criteria, then an alert is created. The rule can then automatically run one or more actions, such as notify you of the alert or invoke another process.

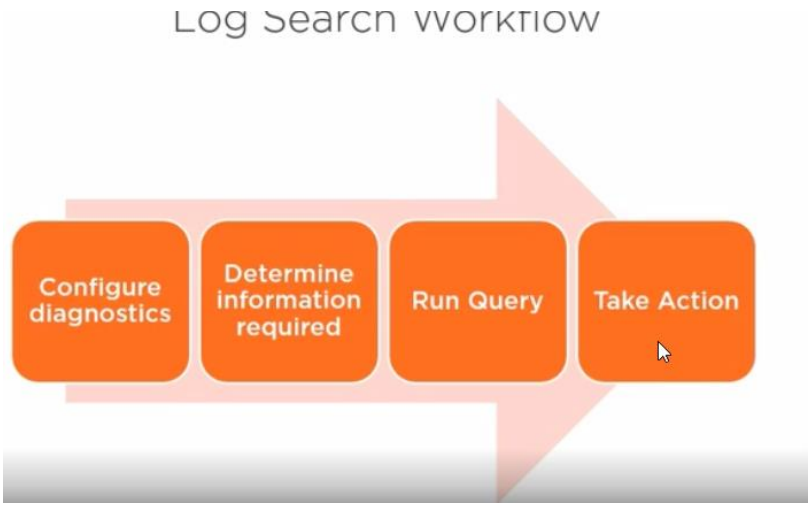
- set up alerts and actions
  - first Define the scope pf the alert (what target resource will be monitored)
  - Select the condition that need to be met for an alert to be triggered
    - Configure signal logic (static , frequency, dynamic)
  - Selct Action Group
    - Notification to send (email, sms, voice,text)
    - Action type to perform (initiating a logic app, Azure Function or an automation run book, emails SMS)
  - Define rule detail (name , descirption , enable/disable)
  - Test rule (You can lunch a test)

- Metric :
  - configure and interpret metrics (feature of Azur monitor)
    - Metric are real-time numbers like CPU%n disk usage
    - Use metric explorer to visualize & analyze the data
    - Use filters to refine data
    - Change views in metrics Explorer
    - Pin to dashborard for regular use
    - Create a alert rule based on a metrics view that you created within metric explorer
  - Linux Diagnostic Extension (LAD) 3.0
    - The Linux Diagnostic Extension helps a user monitor the health of a Linux VM running on Microsoft Azure.

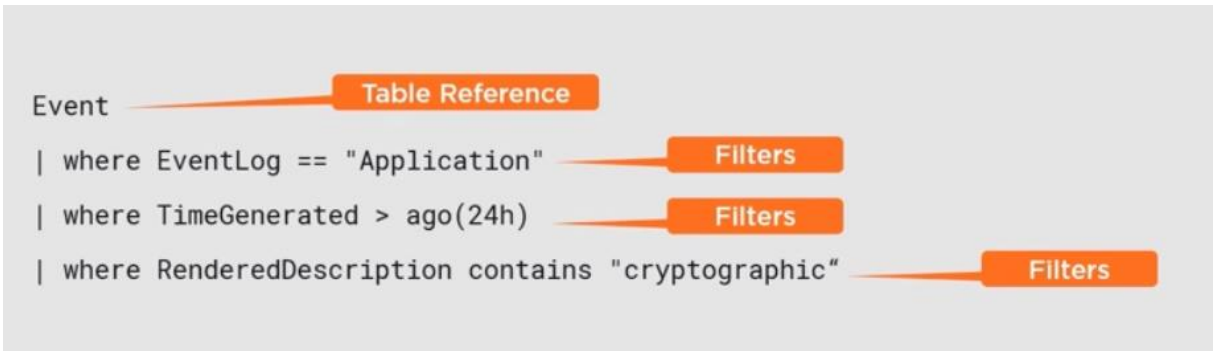


- ClouDyn
  - Microsoft service for globaly monitoring Azure, Amazaon AWS and Google Cloud
- Configure Log Anaytic
  - Create log analytic workspace

        - Containeur pour stocker les logs
        - Work across regions
        - Worksapce data source :
            - Connecte ressource to provide their log into the workspace
    - Enale connection beetwen log analytic and resurce in Azure
        - Form VM thourght Log An portal and enable log analytic vm extension
        - For windows servers one premise, use Mircrosot Management Agent
    - Collect information such as CPU metrics , event on Vm
- Query and Analyze logs in Log Analytic
    - Help for diagnostic for search on a specific event occured at a specific period running query
    - Log search Workflow



        - Configuure diagnostic
            - Grabbing an event logs grom Azure VMs running windows server
        - Determinine information requiered
        - Run Query
        - Take action
            - Review the results
            - Creating an alert rule
    - Create a Query with Kusto Query Language



```
Perf
| where ObjectName =="Processor" and CounterName == "% Processor Time"
| where TimeGenerated between (startofweek(ago(9d)) .. endofweek(ago(2d)))
| summarize avg(CounterValue) by Computer , bin(TimeGenerated, 5min)
| render timechart
```

  - Graph that has avg(CounterValue) on the Y axis and Computer Values on x axis

- configure Azure Monitor logs
- configure Application Insights
  - monitoring service for live applications
  - need to aenable application insights for the application
  - Azure Application Insights helps you gain powerful insights into how people use your app. Every time you update your app, you can assess how well it works for users. With this knowledge, you can make data driven decisions about your next development cycles.
  - 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 app, 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?

-

Implement backup and recovery

- create a Recovery Services vault
  - Storage Entity for backuo and resovery resources
  - Linux and Windows Virtual Machines Azure SQL Databases are common services
  - Centralized management (Backup, restore, site replication, reporting)
  - Work with on-premises and cloud bases workload like AWS
  - Backup resource in the same region as RSV
  - Site recovery resources in deffenrent Azure regions
- create and configure backup policy
  - Stored in recovery service vault in region of resources
  - Defines how a backup plan is implemented
  - Setup asks for backuo confiuration
    - What
      - Azure VM
      - Azure files share
      - SQL Server on Azure VM
      - Sap HANA on Azure VM
    - Create a backup Policy
    - Backuo schedule
    - Instant restre snapshots
    - Renteion range
    - Policy for each resource type
- perform backup by using Azure Backup
  - Support one-premise and Azure and eveen AWS workloads
  - App consistent backup (a recovery point has all required data to restore)
  - Require resource and vault in same region
  - Can initiate backup manually or scheduled
  - For backup Azure VM Backup agent are installed one aure vm
    - Backup Agent
      - Azure VM : Azure Backup extensions is auto installed during first backup
      - One premise or AWS VMs you need to install and agent MARS (Microsoft Azure Recovery Service)
        - To connect the aent to the RSV you need to dowload the credential file from RSV
  - Another tool : Virtual Machine Soft Delete
    - Protect against unintended VM deletions
    - Soft delete : Even after the backuo are deleted ther preserved for 14 days
    - Only preserve backup data, if a v mis deleted without ever being backedup the soft delete feature wont preserve the data
- Perform restore operation by using Azure Backup
  - Point-in-time restores
  - VM Restore Options
    - Entire VM(original location recovery or alternate location recovery)
    - Restore just a disks
    - Files

            - Choose specifi restore point, browse a mounted copy of the disk, select the files and then restore them
            - Dowload a script from azure portal to allow you to auto moint the restored data from azure for 12 hours on your local system
        - Restoring File share
            - Based on snapshots
            - Incorporares soft delete for 14 days of retention by default on the storage account
            - File share backup data is stored in storage account
            -

- perform site-to-site recovery by using Azure Site Recovery
    - 1st Set up site recovery at VM lelvel or in recovery services Vault
    - RSV en VM resources for replication must be in different regions
    - Exemple
        - Vm in Eeast US and West US Regions
        - Existing RSV in West US Régions
        - Only East US VMs can be preotected with Site Recovery
    - You can perform test failovers or production failovers
- configure and review backup reports
    - for Azure VMs, Azure files on other that can be backed up with azure backup
    - requiere log analytic worskpase for collecting the data used by the back up report
    - configure diagnostic setting in recovery service vault
    - view the report in recvery service vault

Azure Backup

- Backs up to Recovery Services Vault
- Online storage entity in Azure used to hold data such as backup copies, recovery points and backup policies.
- Storage account is automatically created an configured
    - Comes with LRS and GRS storage account
        - Configure in Vault → Backup Infrastructure → Backup Configuration
- All backups are listed and globally controlled in *Backup Jobs*
    - You can monitor status and get reports
    - You can filter the jobs
- Backup policy
    - Settings
        - Policy type
            - Azure VM
            - Azure File Share
            - SQL Server in Azure VM
        - Backup frequency
        - Retention range: daily, weekly, monthly, yearly
- You can set inbuilt RBAC roles to vault
    - Backup Operator
        - Manage backups but cannot remove backup, create vault, give any roles.
    - Others e.g. • Backup Reader • Monitoring Reader

- Backup Alerts
  - Vault → Backup Alerts → Configure notifications → Enable e-mail notifications → Choose severities (critical, warning, information) → Select notification (per alert or hourly digest)
- Enable MFA
  - Properties → Security settings → Enable
  - ❗ Cannot be disabled when enabled once.
- You generate Security PIN for critical options and Azure Backup will prompt for the pin (Properties → Security settings)
- When creating a VM back-up you can enable back-ups and choose a vault and policy.
  - ❗ VM must be in same location as recovery vault
- To delete a vault, ensure all backups are stopped, delete backup agents/servers
- Azure Backup Reports
  - On portal: Vault → Backup Reports → Diagnostic Settings → Turn on diagnostics
  - You can save reports in you can archive reports in *storage accounts*, *stream to event hubs*, *send to Log Analytics*
  - After you configure a storage account for reports by using a Recovery Services vault, you can connect Azure Backup from Power BI and get a dashboard.

Benefits

- Automatic storage management
- Unlimited scaling
- Application-consistent backup
  - Each and every recovery point it has information for what it needs to go back to recovery point
- Data encryption both in-rest and in-transit
- Unlimited data transfer
- Long-term retention without any time limit

Pricing

- Pay as you go storage model
- You pay per Protected Instance
  - Protected instance is an application server/workload or computer that's been configured to back up to Microsoft Azure

Components

1) Microsoft Azure IaaS VM Backup

   Can Backup
   a. Virtual Machine
   b. Azure file share
   c. SQL server in Azure VM
   d. SAP HANA in Azure VM

e. **Blobs cannot be backup up to service vaults.**

Storage location

f. **Storage must be in the same location as the Vault(pas besoin d'etre dans la même RG)**

g. **location and subscription where this Log Analytics workspace can be created is independent of the location and subscription where your vaults exist.**

Recovery and restore critere :

h. **File recovery**
   i. **can be done from any machine on internet.**

i. **Restoring the VM,**
   i. **You can restore the backed up disk and either restore the disk before the malware (VM) or create a any virtual machine**
   ii. **For Restore with the replace option the VM have t be stopped or deallocated state to replace the VM extisting disks**

- **Features**
  - Policy-driven backup and retention
    - **Scheduled and on-demand backups, multiple recovery points**
    - **You can hwoever use to backup directly with *Backup Now***
  - Application-consistent backup
    - **No impact on production environment and no shutdown of VMs**
  - Fabric level backup
    - **Multiple backups, centralized management, detailed tracking**
- **❗ New VM created by backup won't have backup policy associated with it.**
- **Restoring and file-recovery manually**
  - **Go to back-up blade for VM.**
    - **Two alternatives:**
      a. **Back-up items → Select backup → Restore VM → Select snapshot**
      b. **VM → Back-up**
  - **Different alternatives:**
    - **Restore VM**
      a. **Two alternatives:**
         a. **Create new VM**
         b. **Restore disks**
    - **File recovery**
      a. **Select recovery point**
      b. **Download script and execute on VM**
         a. **Mounts disks from the selected recovery point**
         b. **💡 If files are larger than 100 GB, restore whole VM instead**
      c. **Unmount disks after recovery**

2) Microsoft Azure Backup MARS Agent

For backing up on-premises computers to Azure
Windows Only
Install back-up agent on local machine
Need connectivity to Microsoft Azure
If you want to restore the folder on another virutal machine. You should install the Microsft Azure Recovery Services Agent on the destionation virtual machine

- **Called also** Recovery Services Agent
- **For backing up on-premises computers to Azure**
  - **Install back-up agent on local machine**
  - **Need connectivity to Microsoft Azure**
- **Same configuration and control**
  - **Centralized management of all on-premises back-ups**
- **Secure backup and recovery**
  - **Protected Instance is registered with Azure**
- **Flow**
  - **In recovery services in portal**
    a. **Back-up**
       - **Where is your workload running: On-premises**
       - **What do you want to back-up:**
         - **• Files and folders • Hyper-V • VMware • Microsoft SQL Server • Sharepoint • Exchange • System State • Bare Metal Recovery**

    b. **Backup *files and folders* and *system state***
    c. **Download** Recovery Services Agent **from link provided**
    d. **Download credentials to enter in the workstation**
    e. **Transfer credentials & agents to the workstation**
  - **Install the Azure backup client**
    a. **Select a password for encryption**

  iii. **Setup the backup**
    a. **Click on *Schedule Backup* in agent**
    b. **Select files/folders**
    c. **Specify retention settings and policy**

  iv. **Backup and restore file**
    a. **Click on** Backup Now **in agent**
    b. **Click on** Recover Now **in agent**

3) Microsoft Azure Backup Server (MABS)

For backing up on-premises computers to Azure
Windows and Linux
requires installation of a dedicated server,
Azure Backup Server is more powerful than MARs
App-aware backups for SQL Server, Exhchange etc
Can be installed on a server in Azure or on-premises

- **Centralized installation**
  - **Can be installed on a server in Azure or on-premises**
- **Free**
- **Similar functionality as *Data Protection Manager (DPM)***
- **Backup a variety of instances**
  - **Workloads, VMWare and Hyper-V VMs, hosts, files, application workloads and barebone backups**
- **Flow**
  - **Create Backup in Site Recovery Service**
    - **Go to Vault → Backup**
    - **Get link for Azure Backup Server**
  - **Install Azure Backup Server**
    - **Installs SQL server**
  - **Configure Azure Backup Server**
    - **Select management**
    - **Protection Servers → Register a server**
    - **Disk Servers → Add a disk for configuration files**
    - **Create protection group**
      - **Add servers, workstations and workloads to the group**
      - **Can back-up to online and/or locally**
    - **Enable disk for backup data**

iv. **Recover with Azure Backup Server**
  - **Select server → Click on Recover Now**

Ressource can acces and be connected to ressorce in different Ressource roupe (ext VM(RG1), VNET(RG2),storrage), bust must be in same location

Azure Active Directory

- **Add licence**
  - **From the Licenses blade of Azure AD, assign a license**
- **Add role to user**
  - **Select Azure Active Directory, select Users, and then select a specific user from the list.**
  - **3. For the selected user, select Directory role, select Add role, and then pick the appropriate admin roles from the Directory roles list, such as Conditional access administrator.**

User

You can update location information on all user(AD, Guest AAD)

- **AD user**
    - **You must use Windows Server Active Directory to update the identity, contact info, or job info for users whose source of authority is Windows Server ActiveDirectory.**

Powershell

- `Set-AzMarketplaceTerms` **cmdlet**
    - **Accept or reject terms for a given publisher id(Publisher), offer id(Product) and plan id(Name).**
- **Install-Module -Name Az**
- **Connect-AzAccount**
- **Get-AzSubscription**
- **$context = Get-AzSubscription -SubscriptionId**
- **Set-AzContext = $context**
- **New-Az « ressource »**
- **Get-Az « ressource »**
- **Remove-Az « ressource »**

CLI

- **Az « ressource » create**
- **Az « ressource » list**
- **Az « ressource » delete**

IT Service Management Connector

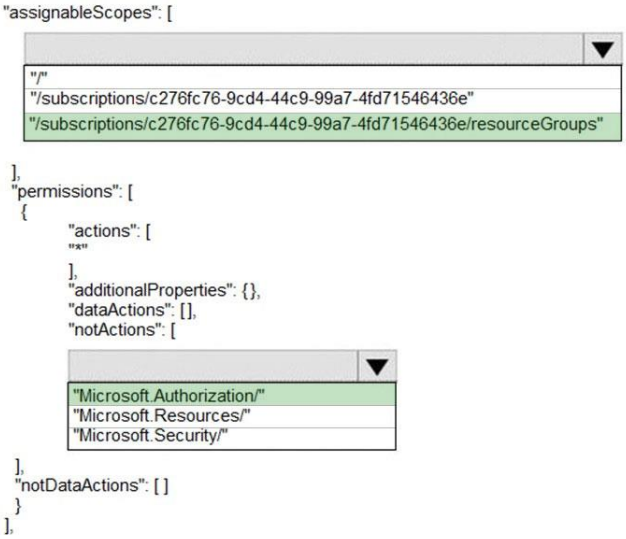
- **IT Service Management Connector (ITSMC) allows you to connect Azure to a supported IT Service Management (ITSM) product or service. (Sysetem center One-premises)**
- **With ITSMC, you can create work items in ITSM tool, based on your Azure alerts (metric alerts, Activity Log alerts and Log Analytics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

RBAC :

- **Owner role**
    - **Allow the user to assing role**
- **DevTest Labs**
    - **only lets you connect, start, restart, and shutdown virtual machines in your Azure DevTest Labs.**
- **Logic App Contributor role**
    - **Lets you manage logic apps, but not change access to them.**
- **Logic App Operator**
    - **Lets you read, enable, and disable logic apps, but not edit or update them.**
- **Custom RBAC JSon:**
    - **Can be assigned only to the resource groups in Subscription1**
        - **AssignableSclopes :[« /subscriptions/subcription_id/resourceGroups/* »]**
    - **Allows the viewing, creating, modifying, and deleting of resources within the resource groups**
        - **Action : [« * »]**

- Prevents the management of the access permissions for the resource groups
  - notActions : [« Microsoft.Authorization/* »]

Answer Area



- Elevate your access
  - Azure AD Global Administrators are the only users that can elevate themselves to gain access on subscription and management group
  - When you elevate your access, you will be assigned the User Access Administrator role in Azure at root scope (/). This allows you to view all resources and assign access in any subscription or management group in the directory, then you can assing yourself Owner role.

- Role to enable Traffic Analytics for an Azure subscription.
  - owner, contributor, reader, or network contributor.
- Virtual Machine Contributor
  - Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.
- Virtual Machine Administrator Login
  - View Virtual Machines in the portal and login as administrator

Log Analatytic

- Commande
  - view the error from a table named Event.
    - Event | search "error"

Traffic Analytics

- Correlate data of network traffic
- 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.
- Role to enable Traffic Analytics
    - owner, contributor, reader, or network contributor.

AzCopy

- Command-line utility that you can use to copy blobs or files only to or from a storage account.
- Copy the contents of a folder to the public container in an Azure Storage account
    - azcopy cp "/path/to/dir" "https://[account].blob.core.windows.net/[container]/[path/to/directory]?[SAS]" –recursive
- Create a container or file share represented by the given resource URL.
    - azcopy make "https://[account-name].[blob,file,dfs].core.windows.net/[top-level-resource-name]"
    - Blobs
        - You can provide authorization credentials by using Azure Active Directory (AD), or by using a Shared Access Signature (SAS) token.
    - Files
        - Only Shared Access Signature (SAS) token is supported for authorization of copy File storage.

Az Container

- Azure Container Instances do support mounting Azure File Shares into the container as volumes.
- When we need persistent storage in container instances we use File Shares which is already made compatible with container instances.

Availability Set

- Microsoft updates, which Microsoft refers to as planned maintenance events,
    - update domains to ensure that not all VMs are rebooted at the same time.

- Delete recovery service vault

    - First you need Disable soft delete feature
    - You can't delete a Recovery Services vault if it is registered to a server and holds backup data. If you try to delete a vault, but can't, the vault is still configured to receive backup data.
    - Remove vault dependencies and delete vault
    - In the vault dashboard menu, scroll down to the Protected Items section, and click Backup Items. In this menu, you can stop and delete Azure File Servers, SQL

- Servers in Azure VM, and Azure virtual machines.
- **You can't delete a Recovery Services vault with any of the following dependencies:**
  - **You can't delete a vault that contains protected data sources (for example, IaaS VMs, SQL databases, Azure file shares).**
  - **You can't delete a vault that contains backup data. Once backup data is deleted, it will go into the soft deleted state.**
  - **You can't delete a vault that contains backup data in the soft deleted state.**
  - **You can't delete a vault that has registered storage accounts.**

Azure Storage

3 copie minimum

Azure storage offers different access tiers, which allow you to store blob object data in the most cost-effective manner

Storage account type	Supported services	Supported performance tiers	Replication options
BlobStorage	Blob (block blobs and append blobs only)	Standard	LRS, GRS, RA-GRS
General-purpose V1	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS
General-purpose V2	Blob, File, Queue, Table, and Disk	Standard, Premium	LRS, GRS, RA-GRS, ZRS, ZGRS (preview), RA-ZGRS (preview)
Block blob storage	Blob (block blobs and append blobs only)	Premium	LRS, ZRS (limited regions)
FileStorage	Files only	Premium	LRS, ZRS (limited regions)

General-purpose v1 accounts (Storage). Legacy account type for blobs, files, queues, and tables. Use general-purpose v2 accounts instead when possible.

General-purpose v2 accounts (StorageV2). Basic storage account type for blobs, files, queues, and tables. Recommended for most scenarios using Azure Storage.

Block blob storage accounts (BlockBlobStorage). Blob-only storage accounts with premium performance characteristics. Recommended for scenarios with high transactions rates, using smaller objects, or requiring consistently low storage latency.

FileStorage storage accounts (FileStorage). Files-only storage accounts with premium performance characteristics. Recommended for enterprise or high performance scale applications.

Blob storage accounts (BlobStorage). Blob-only storage accounts. Use general-purpose v2 accounts instead when possible.

✓ All storage accounts are encrypted using Storage Service Encryption (SSE) for data at rest.

- **Blop Storage acces tier** (**only** in **General Purpose v2 (GPv2) accounts**)
  - **Hot** : accecced (frequently)
  - **Cool** : Medium pas acces fréquent accessed and stored for at least 30 days.
  - **Archive** : storing data that is rarely accessed and stored for at least 180 days

General-purpose v2 accounts deliver the lowest per-gigabyte capacity prices for Azure Storage, as well as industry-competitive transaction prices.

- **Azure Files share UNC Path format**
  - **Net use **[storageaccountname].file.core.windows.net/[FileShareName]
- **Azure Import/Export service**
  - **Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter.**
  - **The maximum size of an Azure Files Resource of a file share is 5 TB.**

- **Import**
  - **Azure Blob Storage / Azure File Storage**
- **Export**
  - **Azure Blob Storage**
- **Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter.**
- **To Transfer the data From the Server one-premises to the storage account by using the Azure Import/Export service.**
  - **Step 1 : Attach an external disk to Server1 and then run waimportexport.exe**
    Determine data to be imported, number of drives you need, destination blob location for your data in Azure storage.
    Modify the dataset.csv file in the root folder where the tool is.
    Modify the driveset.csv file in the root folder where the tool is.
    Use the PrepImport option to copy and prepare data to the disk drive.
    .\WAImportExport.exe PrepImport
  - **Step 2 : From the Azure portal, create an import job.**
    Create an import job in your target storage account in Azure portal. Upload the drive journal files.
  - **Step 3 : Detach the external disks from Server1 and ship the disks to an Azure data center.**
    Provide the return address and carrier account number for shipping the drives back to you.
    Ship the disk drives to the shipping address provided during job creation.
  - **Step 4 : From the Azure portal, update the import job**
    Update the delivery tracking number in the import job details and submit the import job.
    The drives are received and processed at the Azure data center.
    The drives are shipped using your carrier account to the return address provided in the import job.
- **Supports the following of storage accounts:**
  - **Standard General Purpose v2 storage accounts (recommended for most scenarios)**
  - **Blob Storage accounts**
  - **General Purpose v1 storage accounts (both Classic or Azure Resource Manager deployments),**
- **Azure Import/Export service supports the following storage types:**
  - **Import supports Azure Blob storage and Azure File storage**
  - **Export supports Azure Blob storage**

- **Azure File Sync**
  - **To synchronize the files in the file share to an on-premises server**
    - **Step 0 : Check server compaltibility :** Install the Azure **PowerShell module** on the **server** and use the cmdlet **Invoke-AzStorageSyncCompatibilityCheck.**
    - **Step 0 ,5 ; Create the Azure file share**
    - **Step 1 (C): Install the Azure File Sync agent on Server1**

        - Step 2 : Register Windows Server with Storage Sync Service establishes a trust relationship between your server and the Storage Sync Service.
        - Step3 : Create a sync group and a cloud endpoint and a server Endpoint.
            - A sync group defines the sync topology for a set of files. Endpoints within a sync group are kept in sync with each other. A sync group must contain one cloud endpoint, which represents an Azure file share and one or more server endpoints. A server endpoint represents a path on registered server.
    - A sync group must contain only one cloud endpoint
    - One or more server endpoints can be added to the sync group.

    - Cloud endpoint is scanned by the detection job every 24 hours so if you add file to cloud endpoint you will need to wait 24h to see the files in the one-premise (server endpoint)

    - Servers endpoint (on-premises) file is scanned and synced automatically after it's being added, so if you add file to server endpint you will see it imediatly in the cloud endpoint

    - Files are never overwritten. If the file exists, it will get a new name on the endpoint (file1(1).txt)

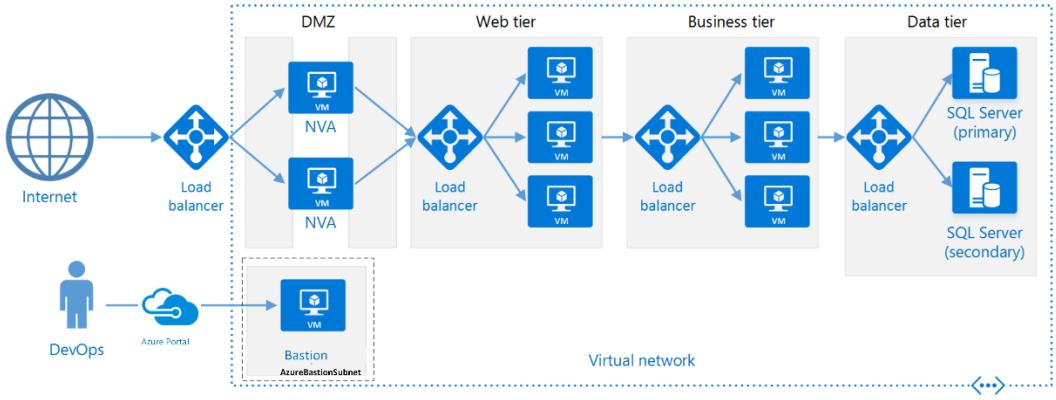
    - Ressource
        - can be moved beetwen RG and subscritpion within the same locations
        - you cant move a App service(Webb app) to a rg that already contain a App service (Web app)
        - VM -> Vnet = same region required
        - Recovery Vault -> VM/SA /DB = same region required
        - Recovery Vault-> Storage = same région required
        - VNIC -> VM = same région and same VNET same susbscirption
        - AKS node = same VNET
        - Webb App -> App service plan = same région

- Azurz VM
    - VM one premise to Azure
        - Before you upload a Windows virtual machine (VM) from on-premises to Microsoft Azure, you must prepare the virtual hard disk (VHD or VHDX). Azure supports only generation 1 VMs that are in the VHD file format and have a fixed sized disk. The maximum size allowed for the VHD is 1,023 GB. You can convert a generation 1 VM from the VHDX file system to VHD and from a dynamically expanding disk to fixed-sized.

Architecture :

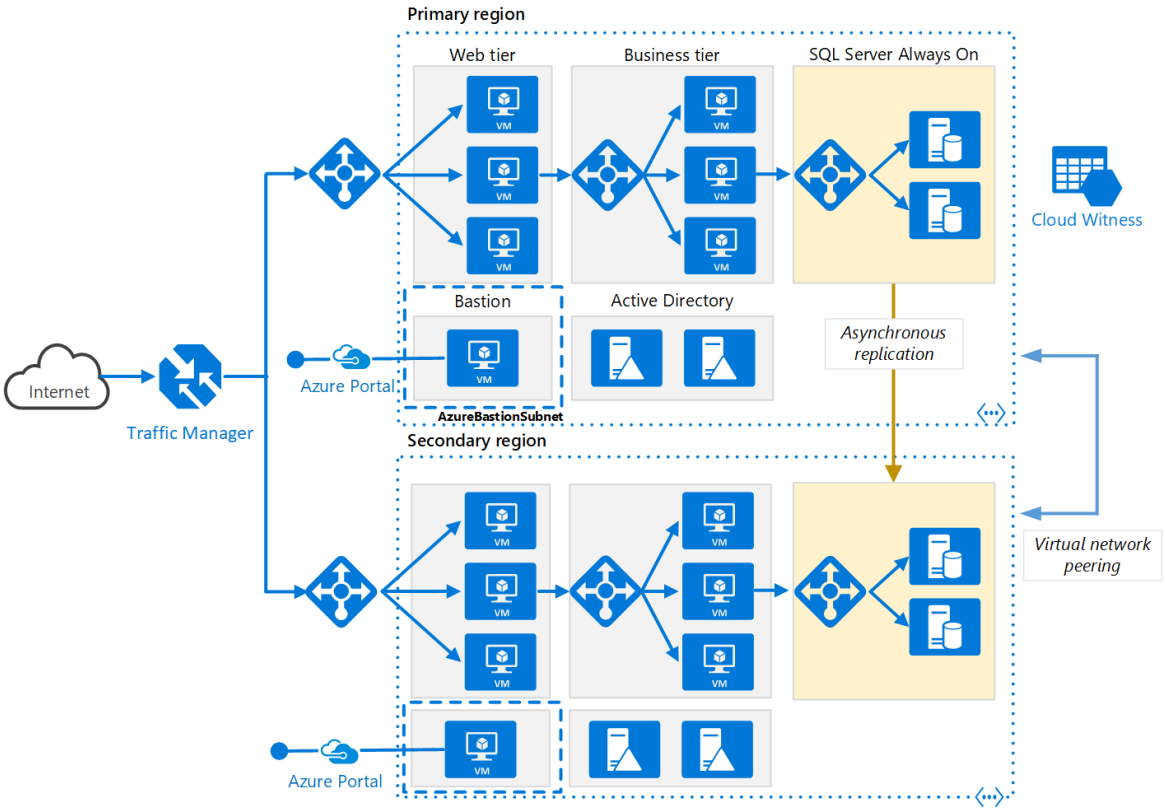
It would be preferential to have separate subnet for each layer of a Web appplications

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



    - **SLA**
        - **Deploy 2 or mor instance of VM behind availability zone assure SLA of 99.99% or whith avaiblityset SLA of 99.95% for the service**
        - **Adding load balancer for redundancy increase the SLA too 99,99 % with AZ**
        - **Single VM SLA :**
            - **Virtual Machine using Premium SSD 99,9 %**
            - **Virtual Machine using Standard SSD Managed Disks for Operating System Disk and Data Disks 99.5%**
            - **Virtual Machine using Standard HDD Managed Disks for Operating System Disks and Data Disks 95%.**
    - **Security admin role**
        - **Only for manage the Security center**
        - **Not ressource like vnet vm etc**
        - **Not assing permission**

DNS : port 53 TCP/UDP



Classic shit

- **Lock**
- **Availibtyt Zone**
- **Availibity set**
- **Pricing calculator**
- **Azure policy**
- **Ressource group**
- **AKS Az Container**
- **Vnet peering**
- **VNIC**
- **Policy**
- **Manaement group**
- **Budget**
- **AD connect, passtrhought**
- **SLA AvaiZon AvaiSet**
- **Microsot advisor (cost)**
- **Peering (global peering)**
- **SLA sclae sets**

Add code couleur pour les gros titres

Add code couleur pour les topic pas encore parcourue et role

Udemy :

- **Manage Azure VM**
- **Manage VM Backups**

- Azure App Services
- AKS
- Manage Virtual Networking
- Implement and manage virtual networking
- Configure name resolution
- Secure access to virtual networks
- Implement multi-factor
- Configure load balancing
- Monitor and troubleshoot virtual
- Networking
- sla

Faiire les Quiz du cours udemy sur les modules