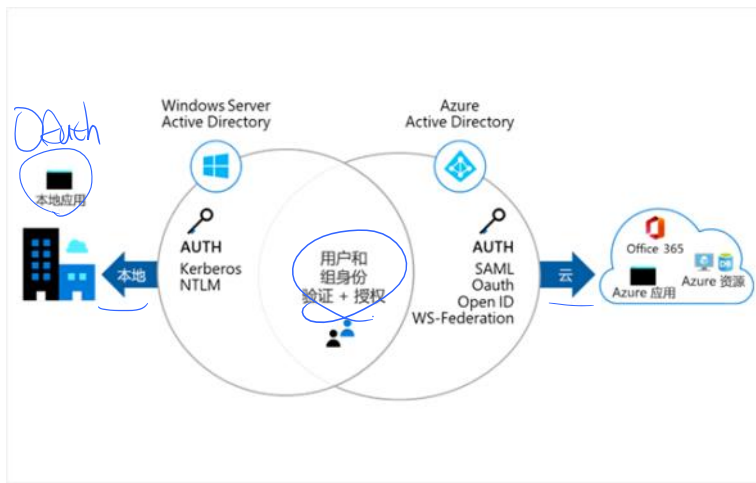
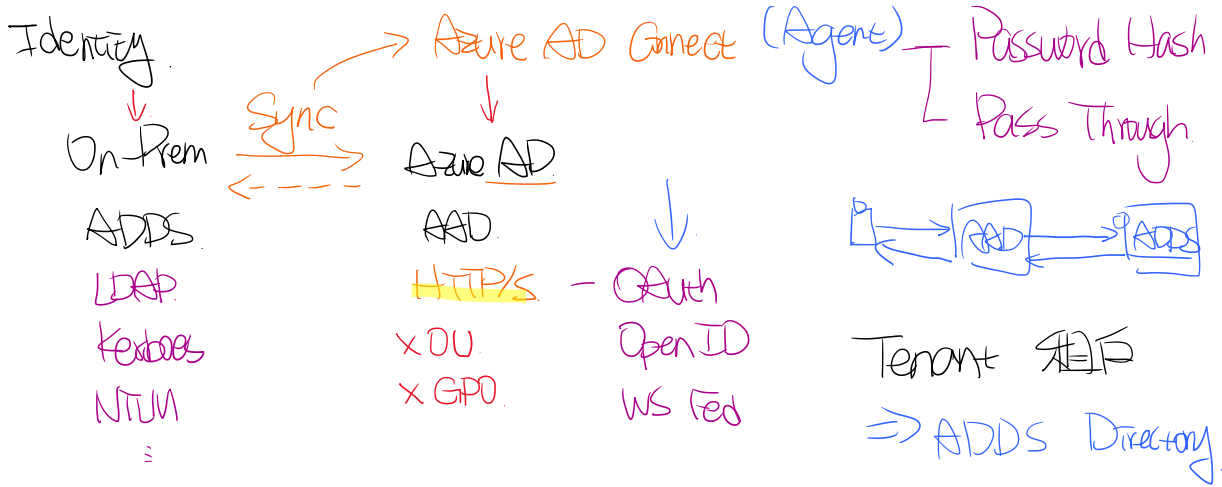




Hybrid

On Prem

AD DS

Azure

AD DS + AD

AD DS

AD + AD DS

X

AD + AD DS

Azure AD Join

(AD)

Conditional Access

AAD Join vs Register  
 Company Device  
 Control By Corp.  
 BToD  
 limited Access



1. 确定可以使用自助式密码重置的用户

Who User, Group.

2. 选择所需的身份验证方法数和可用的方法 (电子邮件、电话、问题)

3. 可以要求用户注册 SSPR (过程与 MFA 相同)

User

User & Groups.

AAD Global Admin  
 User



Azure Global Admin (X)

AAD Tenant  
 { mtc.com  
 mtc.cn  
 mtc-tw

Tenant = mtc.sg

a@mtc.com ← member

b@mtc.sg ← guest

c@mtc.cn ← member

d@hotmail.com ← guest

Group  
 { Security Group  
 M365 Group

Assign Manual

Dynamic  
 { User-App  
 Device



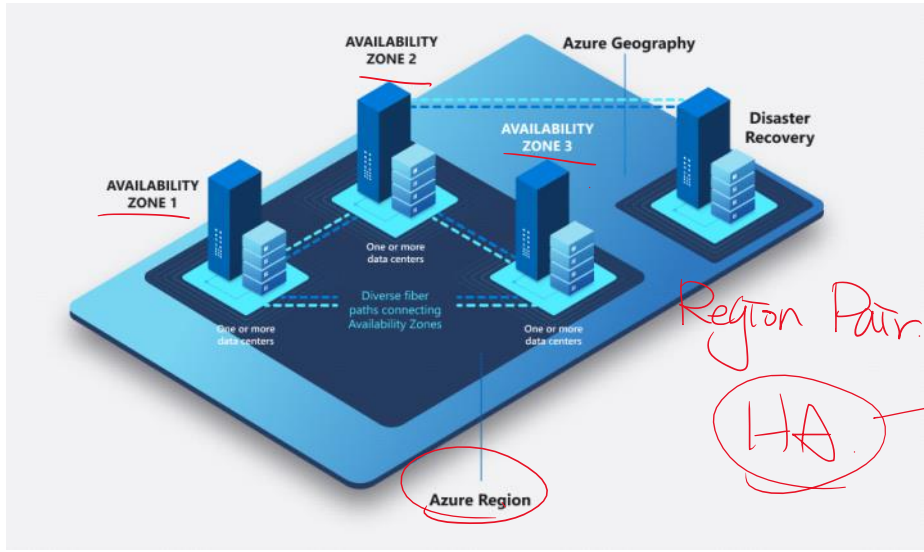
Region != Datacenter



Microsoft data center in Cheyenne, Wyoming

Region 区域 / 35 AZ 可用区域

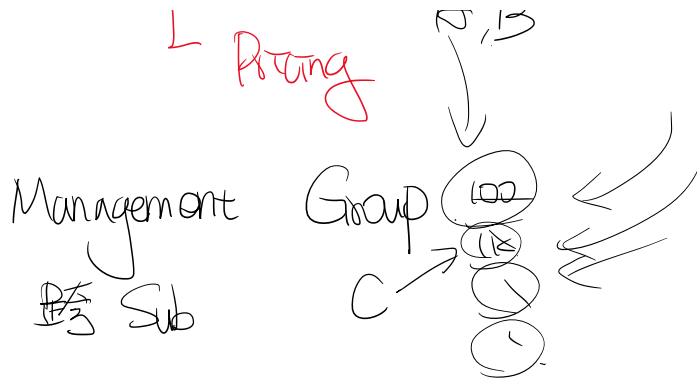
Latency  
 Pair  
 Costing  
 Core Net



Region Pair  
 HA

RTT  
 Latency  
 Geo  
 Proximity  
 A, B

Tenant = Identity Solution  
 A... C...

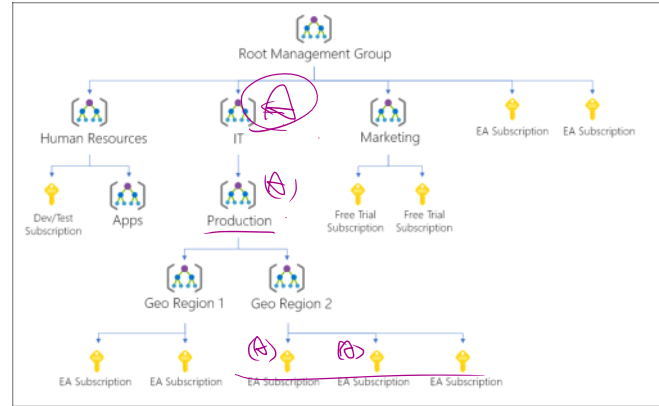


Azure = Cloud

Cost Management (Sub.)

Tag = Metadata (key-value)

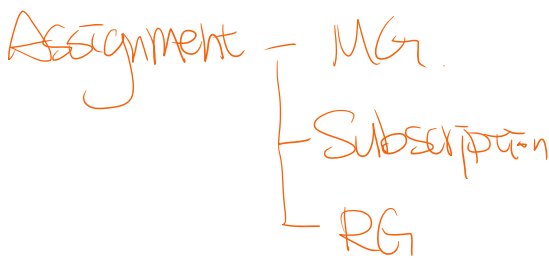
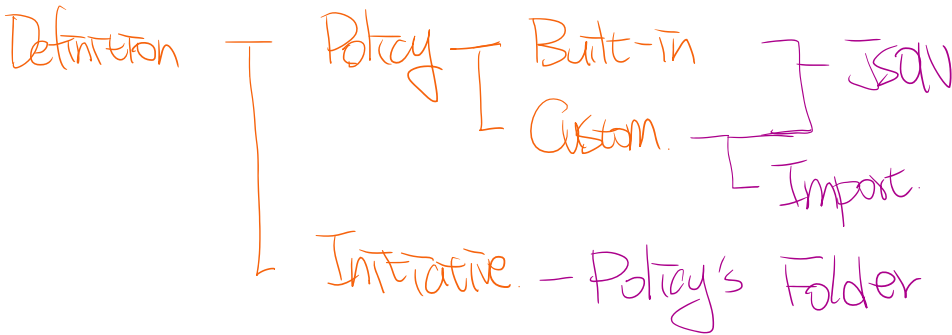
Cost Center:  
Owner



Azure Policy → 規則

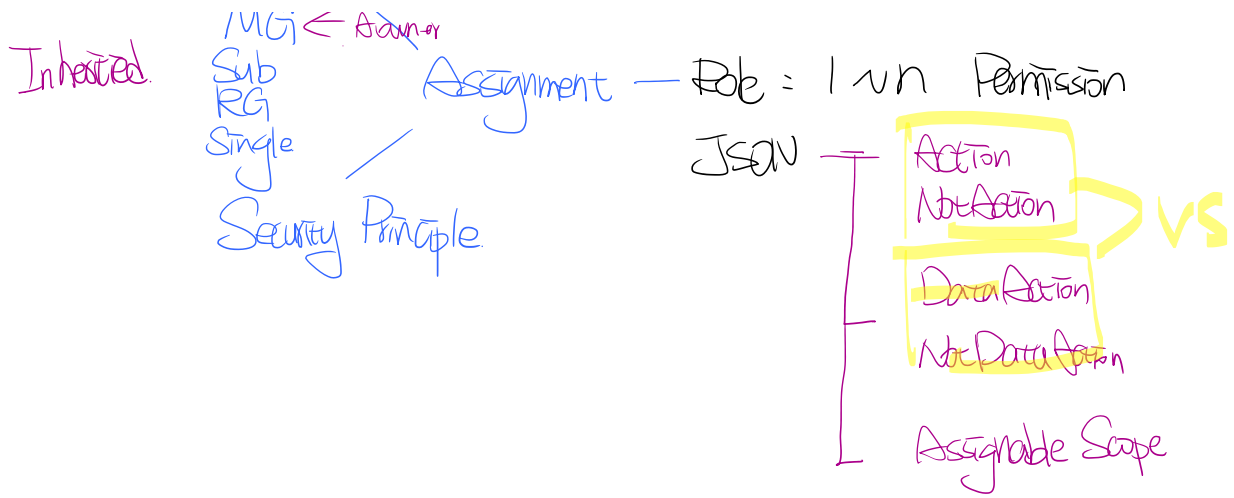


1. 檢查
2. 強制



RBAC (Role based Access Control)

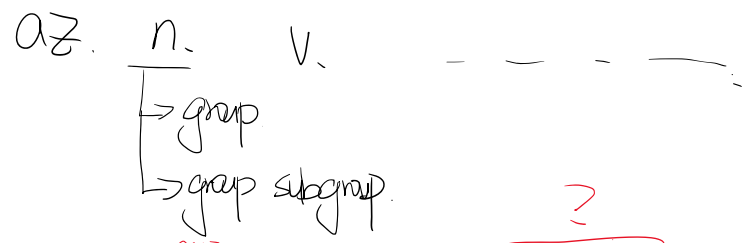
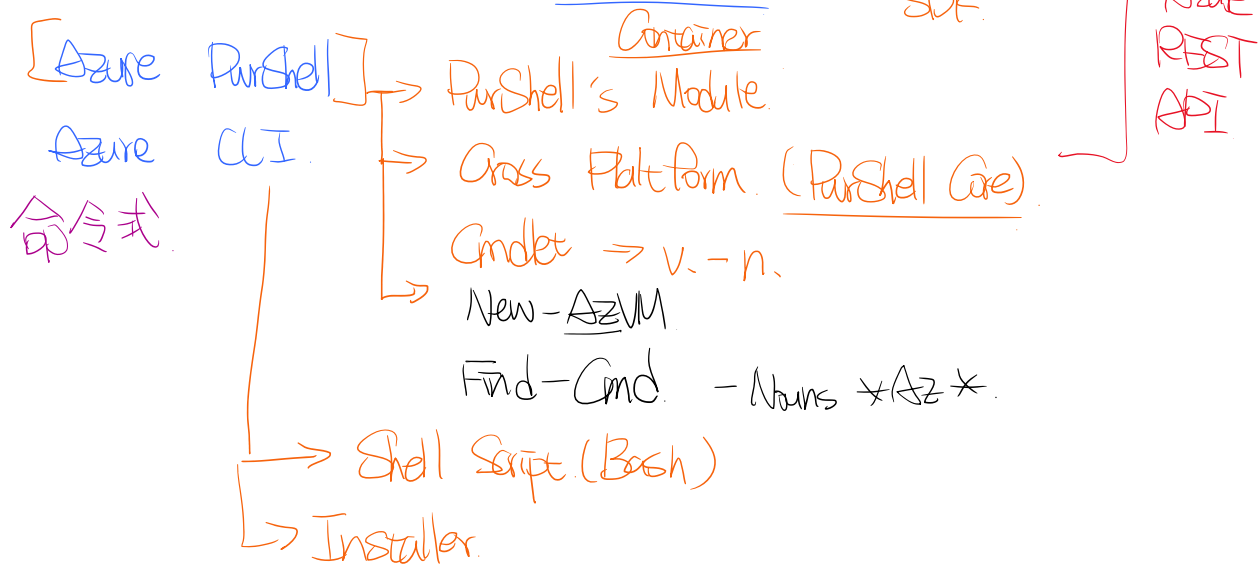




# Administration

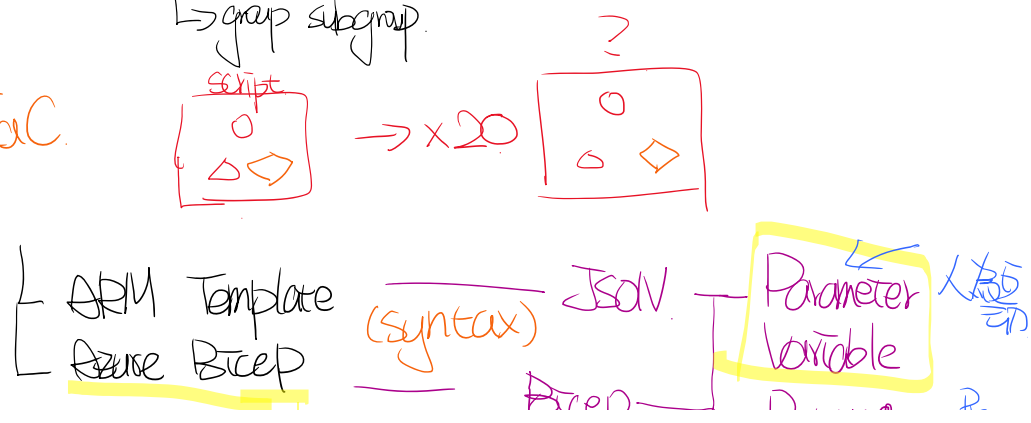
ARM - Azure Resource Manager - Management Layer

Azure Portal - Azure Cloud Shell - Tools SDK



声明式 IaC

易学性





Blank (VS Code Ext.) (→)

Export

Gallery (Azure QuickStart Temp....)

## Networking.

Virtual Network (VNET) - Addr Space - CIDR.

Independent

SDN

10.10.0.0/16

10.20.0.0/24

Subnet x n.

10.10.1.0/24  $\Rightarrow$  25110.10.2.0/24  $\Rightarrow$  29

IP - Private IP - Dynamic / Static.

④

Azure

Public IP - Azure Resource

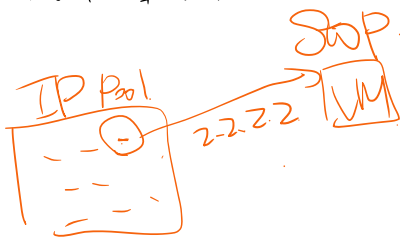
IPv4/IPv6

Basic x Dynamic

Standard AZ.

FQDN

Static



NSG (Network Security Group) Layer 4 FW (TCP/IP)

InBound  
Out Bound

Rules x n.

Priority (int)

100 ~ 4096

越小越优先

Rule 1

v RDP

400

Service Tag

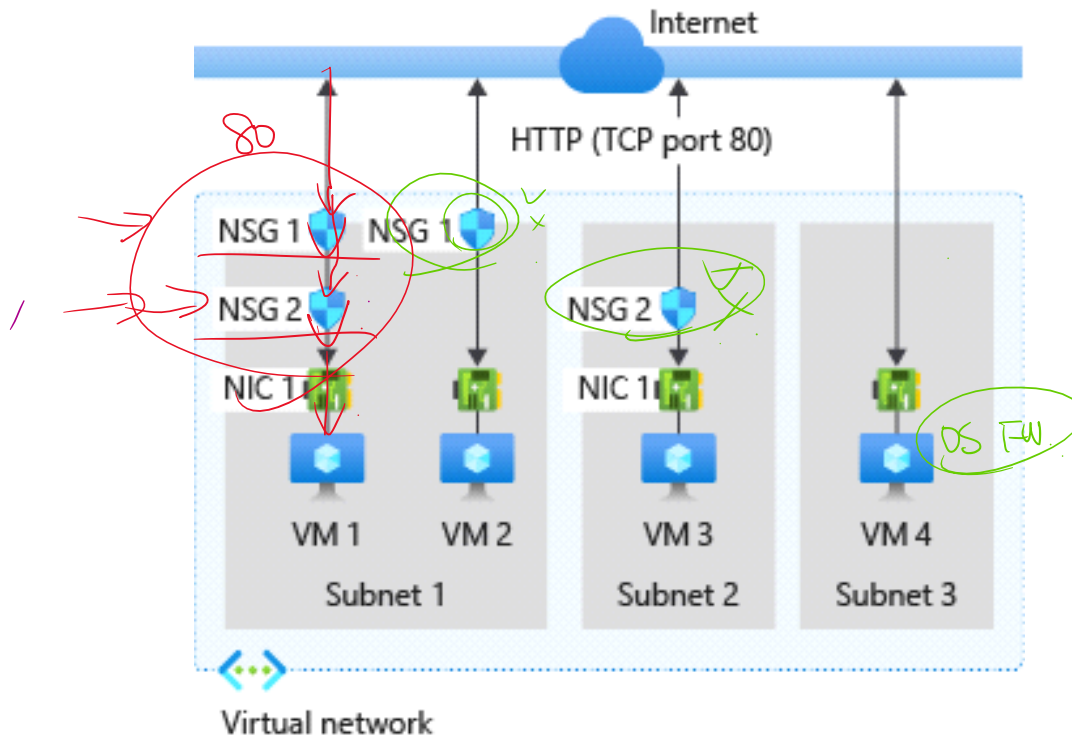
→

Rule 2

x RDP

120

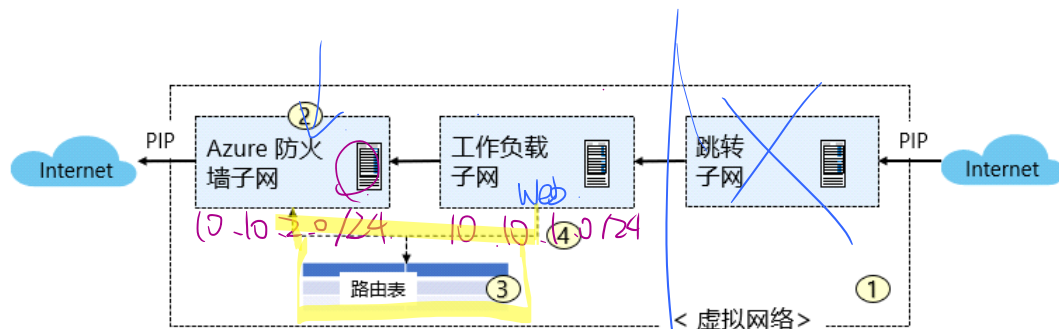
Appliance (VM)  
Subnet



Azure Firewall (Layer 7) (Pass) - (VM) → Dedicated Subnet

- NAT
- Network
- Application

HA  
Scale  
...



Route + System Route ← Azure Managed

Route

- System Route  $\leftarrow$  Azure Managed
- User Define Route (UDR) (n-)
  - Route Table - Route x n.
  - Associate - subnet x n.

Azure DNS (PaaS DNS Server)

- Public DNS Zone
  - Child Zone - RBAC.
- Private DNS Zone = Any Name
  - Link Vnet 1:n

dev-loc.

☑ Auto Registration (Discovery) By Vnet.

InterSite connectivity.

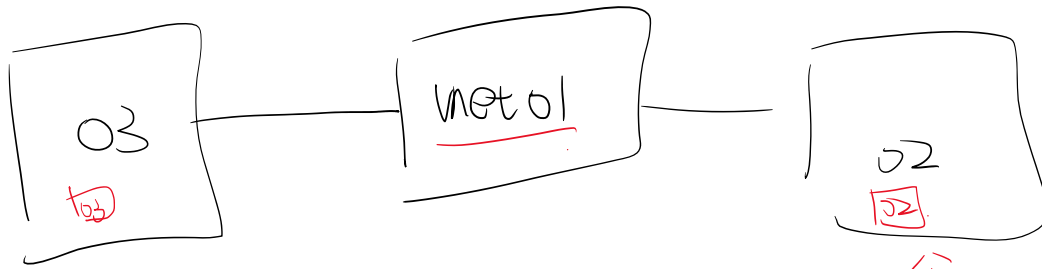
VNET  $\leftrightarrow$  VNET

VNET  $\leftrightarrow$  Other (On-Prem)  
(Other Cloud)  
(Azure).

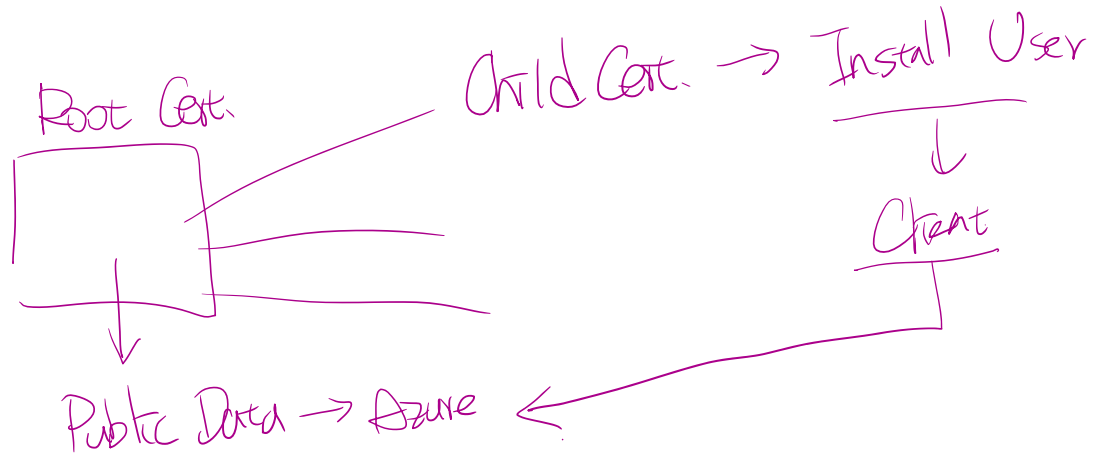
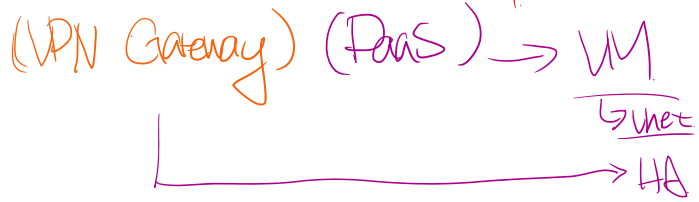
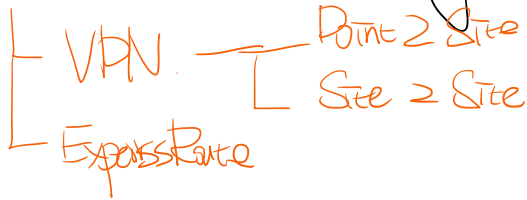
(VPC)

Peering  
(≠≠)

— Region  
Region  
Sub



Virtual Network Gateway



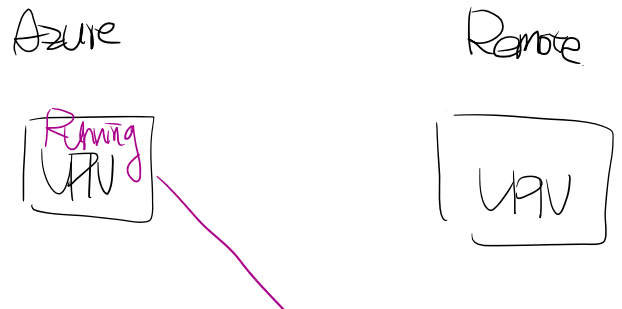
1. VNET GW
2. Config remote vpn device
3. Local Network GW - On Prem VPN Info
4. Conn.

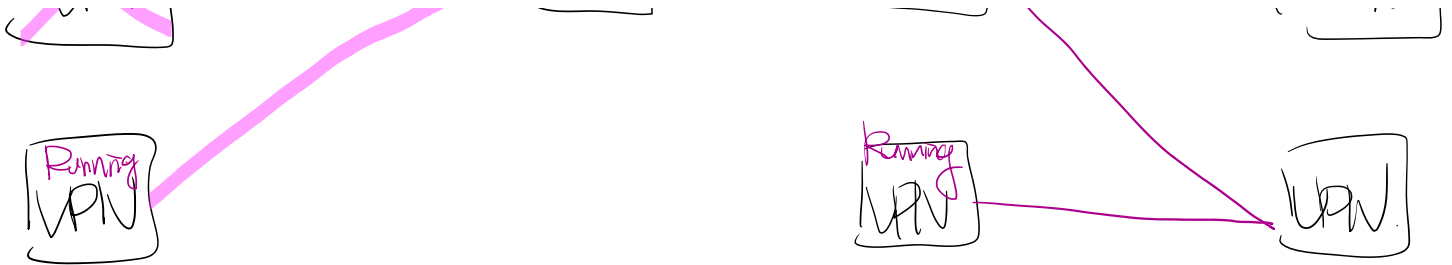
HA

Active - Standby

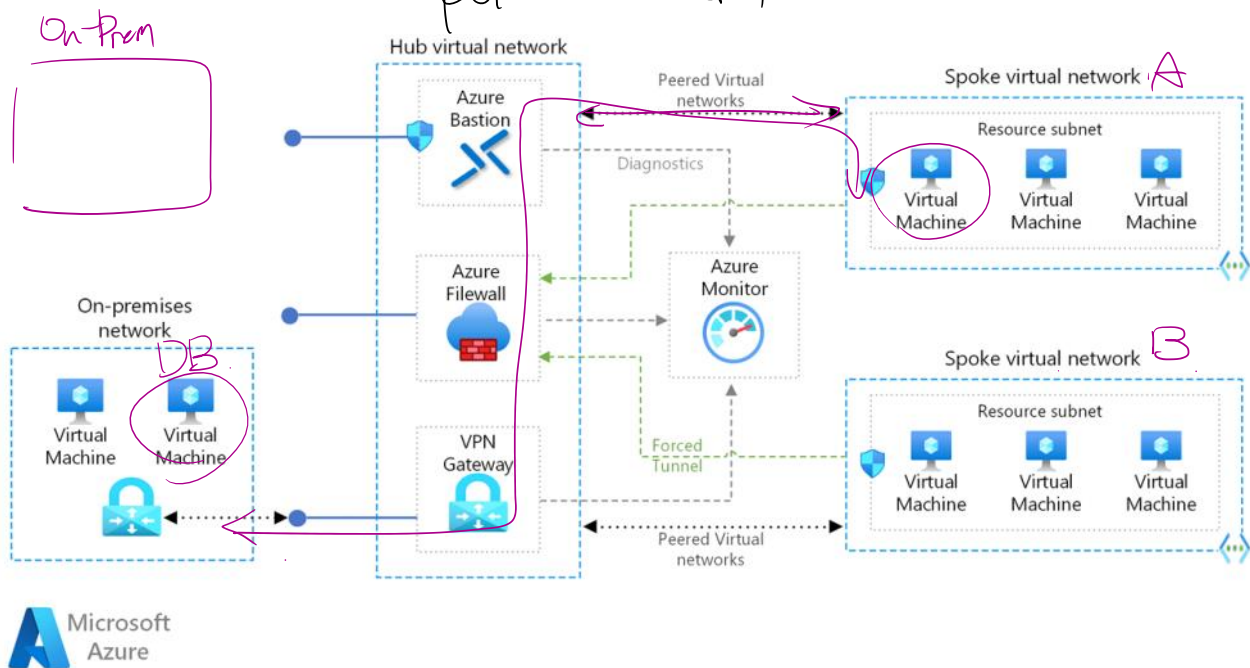


Active-Active

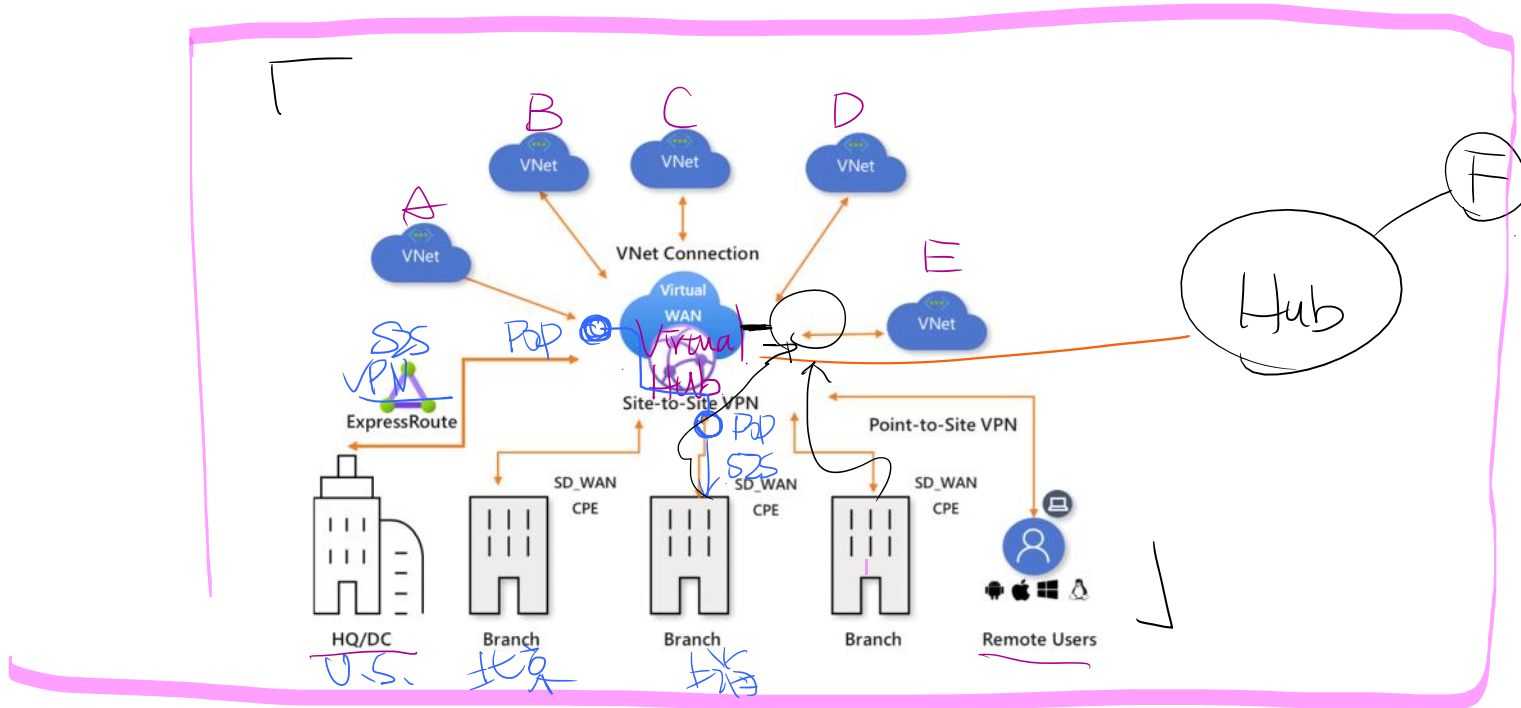




## Hub - Spoke Model



Virtual - Wan (Hub - Spoke)

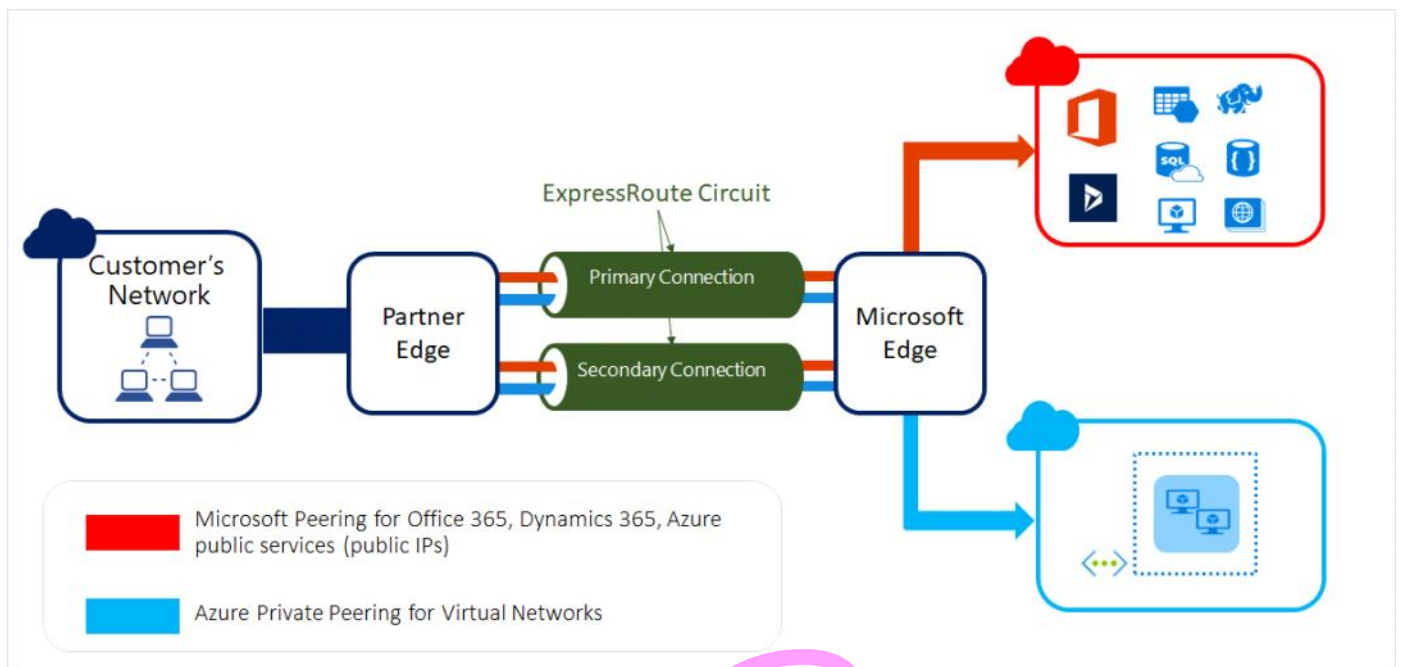


JPE Vnet a 10.10.0.0/16

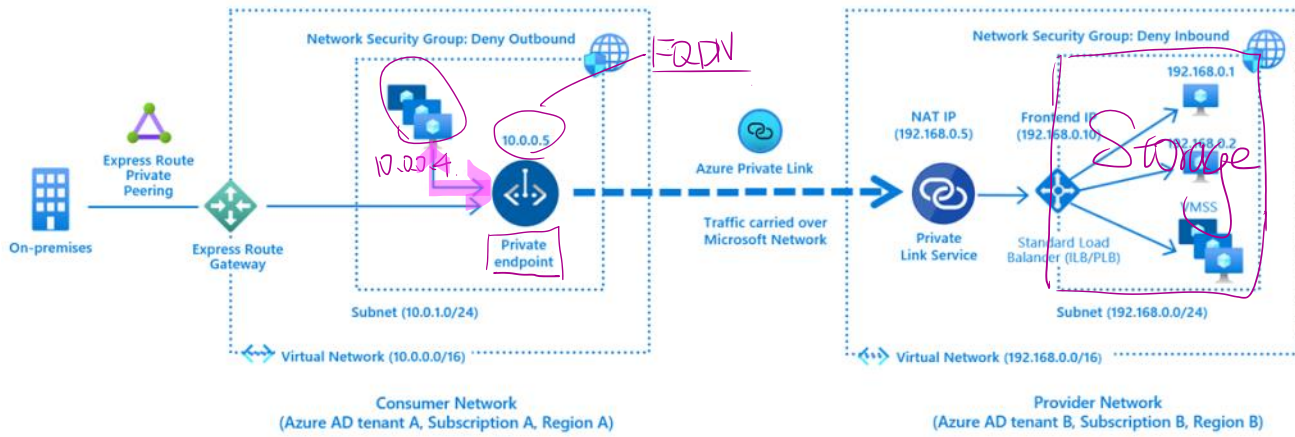
SEA Vnet b 10.11.0.0/16

(NET)

Hub - JPE 10.12.1.0/24





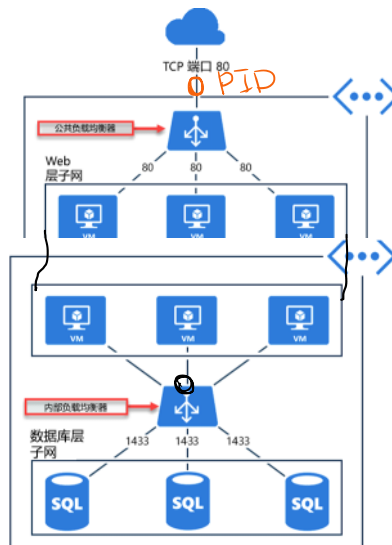


# Load Balancer

| 功能   | 应用程序网关                                    | Front Door                         | 负载均衡器                      | 流量管理器                                   |
|------|-------------------------------------------|------------------------------------|----------------------------|-----------------------------------------|
| 使用情况 | 使用 Web 应用程序防火墙增强应用程序安全性时，优化来自应用程序服务器场的交付。 | 可缩放的安全增强型交付点，适用于基于微服务的全局 Web 应用程序。 | 均衡入站和出站连接以及对应用程序或服务终结点的请求。 | 在全球 Azure 区域内以最佳方式向服务分发流量，同时提供高可用性和响应性。 |
| 协议   | HTTP、HTTPS、HTTP2                          | HTTP、HTTPS、HTTP2                   | TCP、UDP                    | Any                                     |
| 专用   | 是                                         | 是                                  | 是                          | 是                                       |
| 全球   |                                           |                                    |                            |                                         |
| Env  | Azure、非 Azure 云、本地                        | Azure、非 Azure 云、本地                 | Azure                      | Azure、非 Azure 云、本地                      |
| 安全性  | WAF                                       | WAF、NSG                            | NSG                        |                                         |

## Azure LB

Public LB — Public IP  
Internal LB — Private IP

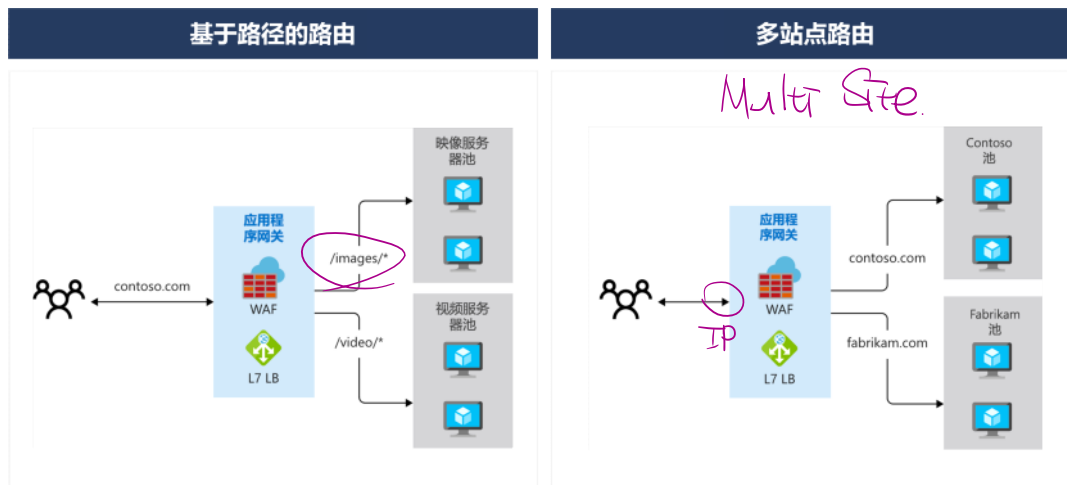


Frontend IP  $\times n$ .

Backend — VM  
Pool — Container.

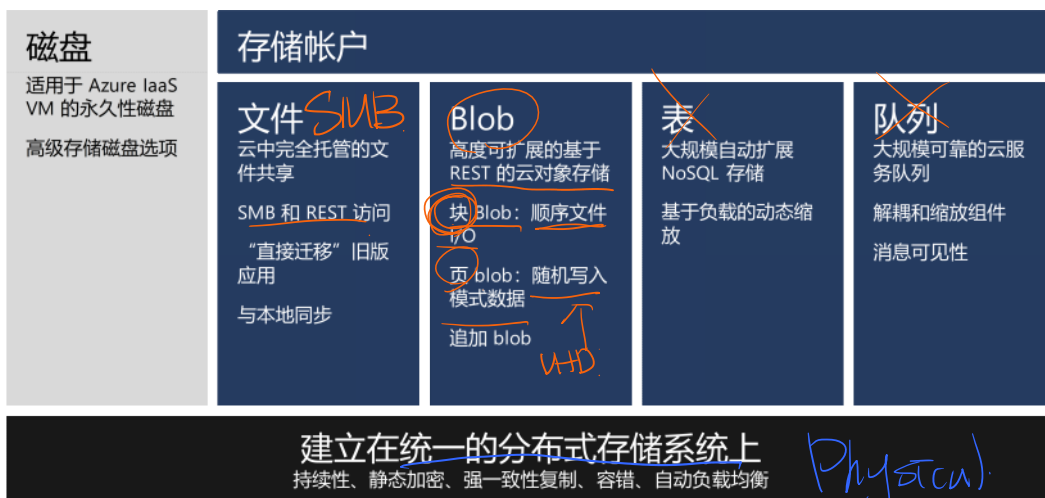
Rule

L Probe



Storage

- Blob
- Files
- Queue
- Table



| 存储帐户      | 建议用途                                       |
|-----------|--------------------------------------------|
| 标准常规用途 v2 | 包括 Blob、文件、队列、表和 Data Lake Storage 等大多数场景。 |
| 高级块 blob  | 具有高事务率的块 blob 场景，或使用较小对象或需要存储延迟始终较低的场景。    |
| 高级文件共享    | Enterprise 或高性能文件共享应用程序。                   |
| 高级页 Blob  | 高级高性能页 blob 场景。                            |

## Azure Outage as Lightning Strike Forces Data Centre Offline

By CBR Staff Writer 05 Sep 2018



Microsoft was scrambling to get a number of cloud-based services up and running this morning, after a lightning strike near one of its San Antonio data centres caused a voltage surge. This in turn forced a power-down when cooling equipment failed, triggering an Azure outage locally and issues with Office 365 globally. The outage even took the Azure service status monitor offline.

2021

## Millions of websites offline after fire at French cloud services firm

By Mathieu Rosemain, Raphael Satter

3 MIN READ

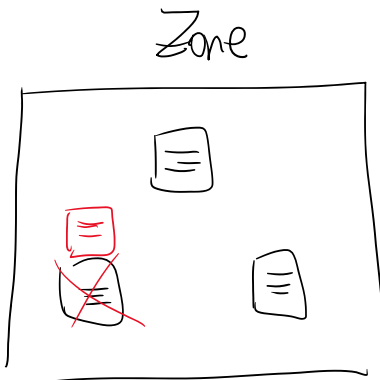


Microsoft Corporation

Getty Images

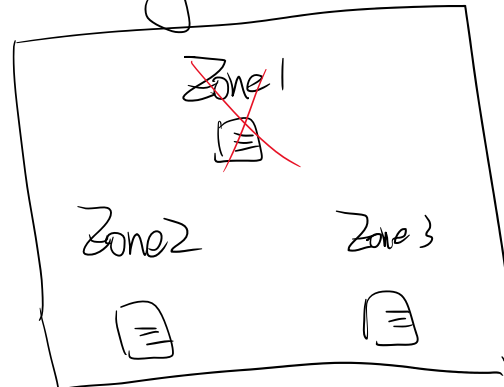
Redundancy 3 vb copies

LRS (Local)  
1 Region, 1 AZ. 3 copies

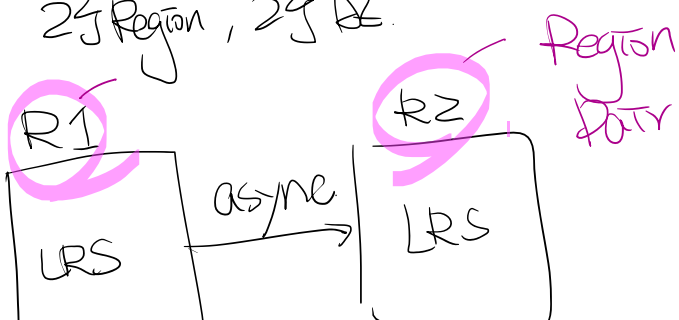


99.9-99%

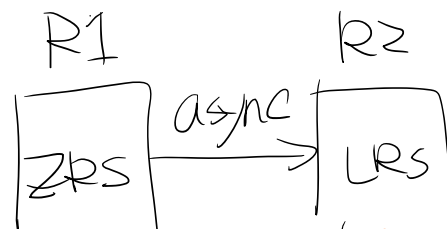
ZRS (Zone)  
1 Region, 3 AZ. 3 copies

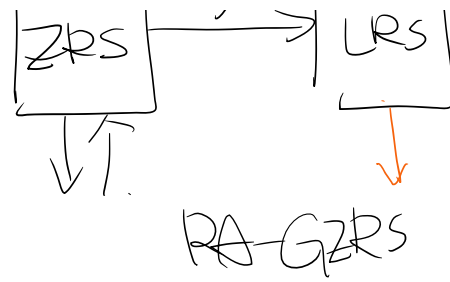
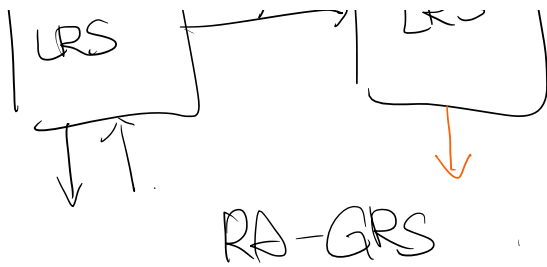


GRS (Geo)  
2 Regions, 2 AZ. 6 copies



GZRS  
2 Regions, 3+1 AZ. 6 copies





Prüfung - Space

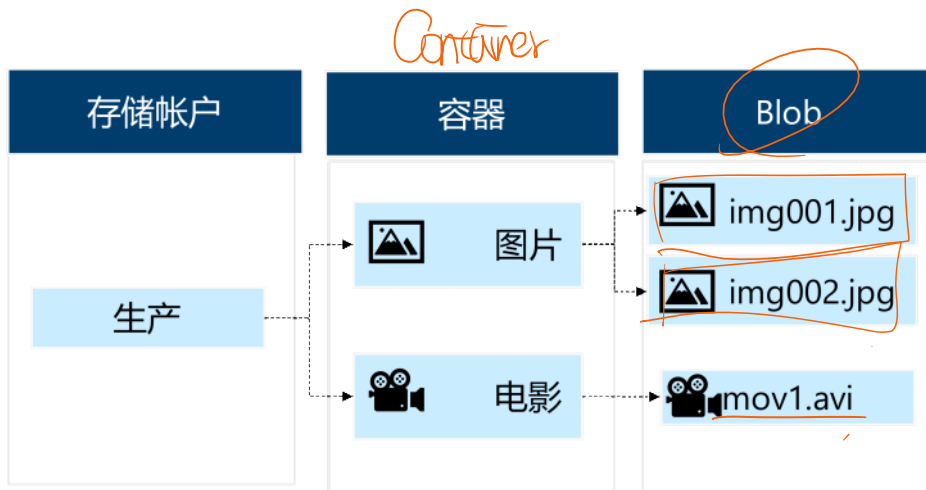
Transaction

Access Tier - Lbt  
(By Blob)

Go |  
Archive

Lifecycle Management

LRule  
↳ Code



Single Layer

2022/img.jpg

<https://demo1221stor.blob.core.windows.net/images/%E7%8C%AB%E3%81%AE%E6%81%A9%E8%BF%94%E3%81%97.jpg?sp=r&st=2022-12-21T03:23:43Z&se=2022-12-21T11:23:43Z&sr=https&sv=2021-06-08&rb&sig=NEyguOCG%2BvYNUC7FL4huNVEXKJqNwzxKqWcMHQBQm9k%3D> bbb

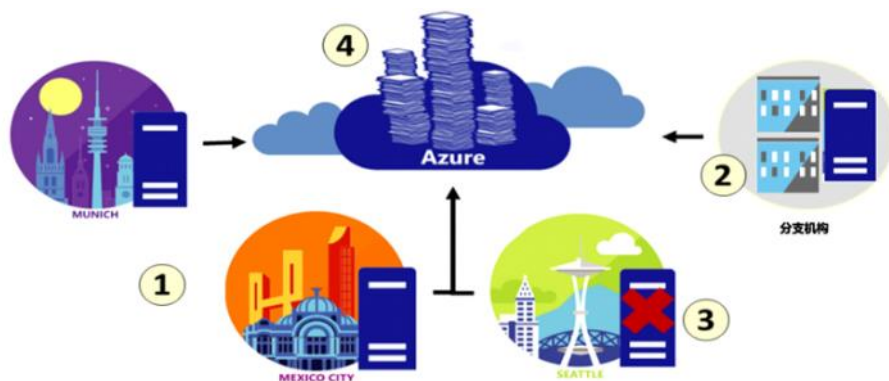


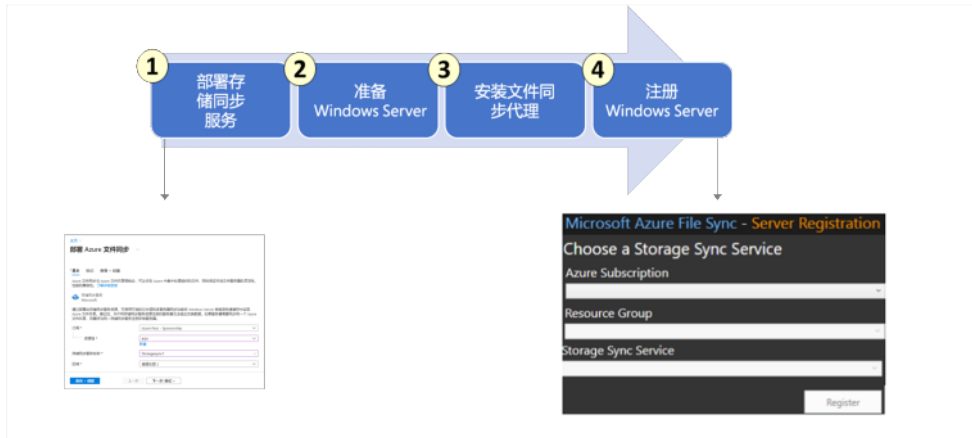
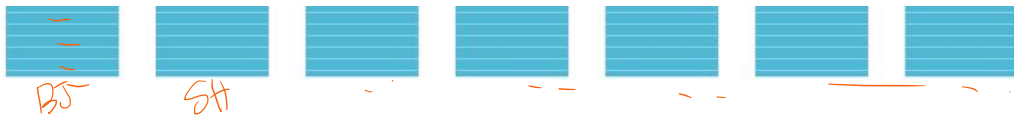
X

Access Policy. [ Pre config.  
(By Container) ] Part of the Uri

<https://demo1221stor.blob.core.windows.net/images/%E7%8C%AB%E3%81%AE%E6%81%A9%E8%BF%94%E3%81%97.jpg?si=demo1221saspolicy&spr=https&sv=2021-06-08&sr=b&sig=FHZc2g7Utg6ZTnk0rimWx4O1VRYfVIRhBR8ZyddjB%2F8%3D>

Azure File Sync





VM (IaaS)      Shutdown != Deallocated

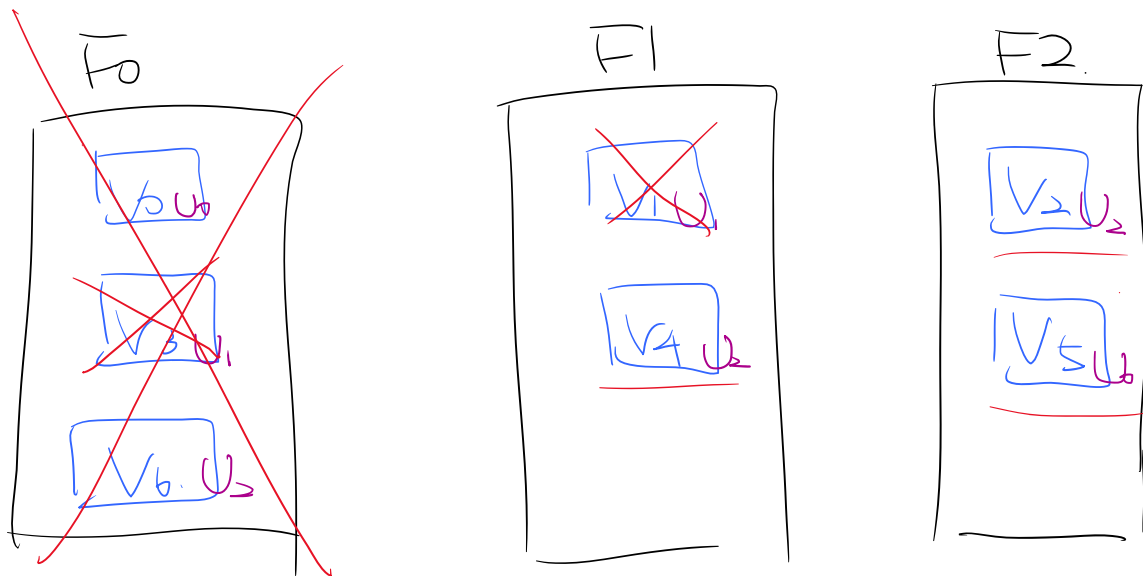
{ Computing - Type x 6 - Series - Size.  
 { Storage - Managed Disk - Azure Resource  
                     UnManaged Disk - VHD - Storage  
                                                             Page Blob.

$10 \text{ VHD} \times 500 \text{ IOPS} \Rightarrow 50,000 \text{ IOPS}$   
 Limitation.

VM

Availability Set (同一AZ)      1 ~ 3  
                                             Fault Domain - Hardware.  
                                             容错域.

Availability Zone      1 ~ 20  
 ☑ 1 ☑ 2 ☑ 3      Update Domain - Update.  
                                             更新域.



HA  $\Rightarrow$  VMSS  
VM Scale Set

- AV Set / Zone
- Management
- Scale
  - Manual
  - Auto

Azure App Service

- App Service Plan (VMSS)

- Web Appxn.

- Pricing / Feature.

Performance. =

Azure Compute Unit (ACU)

Scale
 

- Manual
- Auto

## Container

L VM

L Web App for Container.

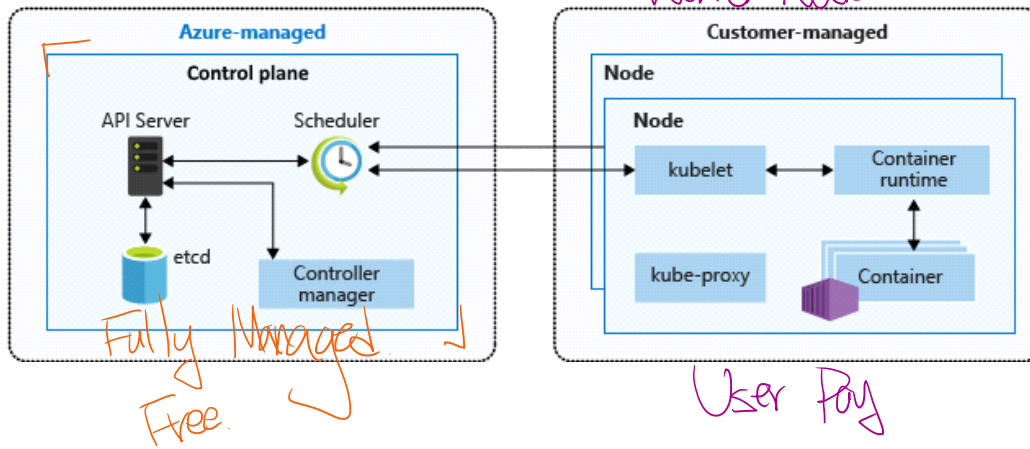
L Azure Container Instance. (Simplest)

L Azure Kubernetes Service (AKS) (PaaS)

L Pod = 1 VM Container.

Azure Container Registry - Private

L Docker Registry 2.0 L Public

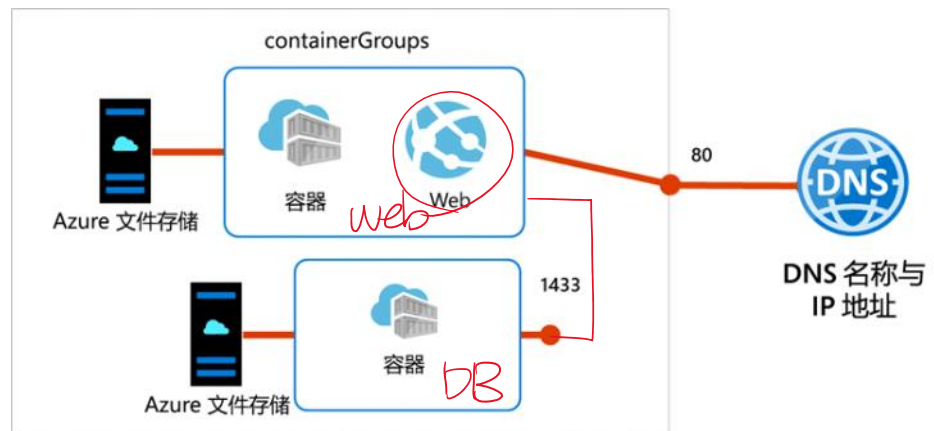


L Azure Container App (KaaS)

## Container Group

L x Portal.

L Docker Compose.



## Backup

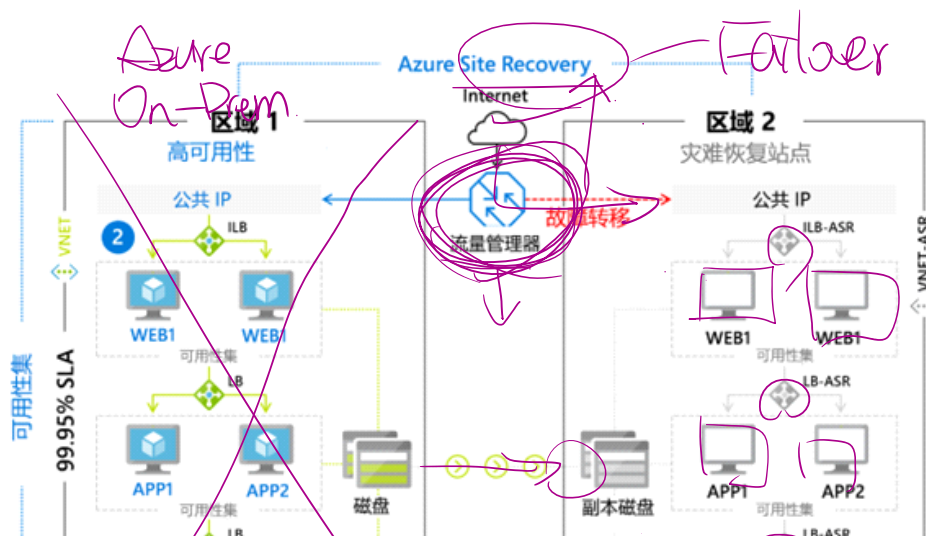
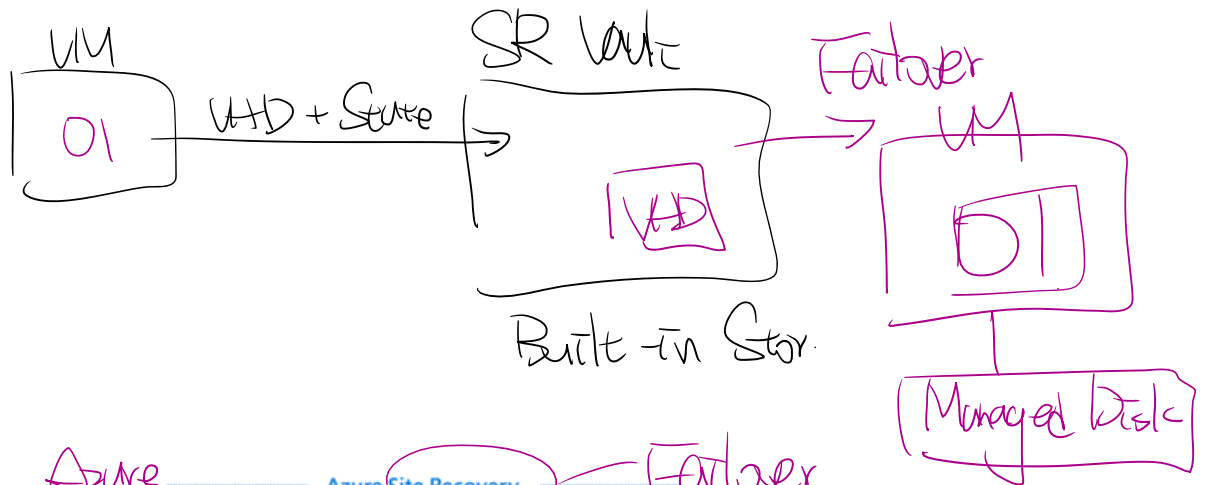
L Backup Center.

- Backup Center.

Built-in Storage | Retention  
Option

Recovery Service Vault

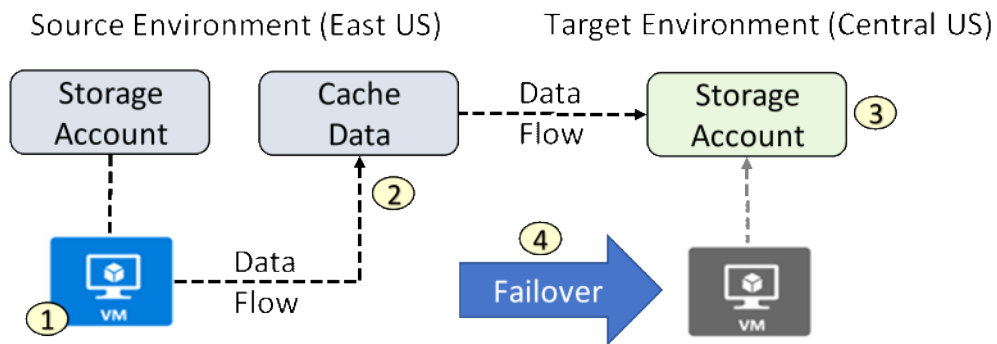
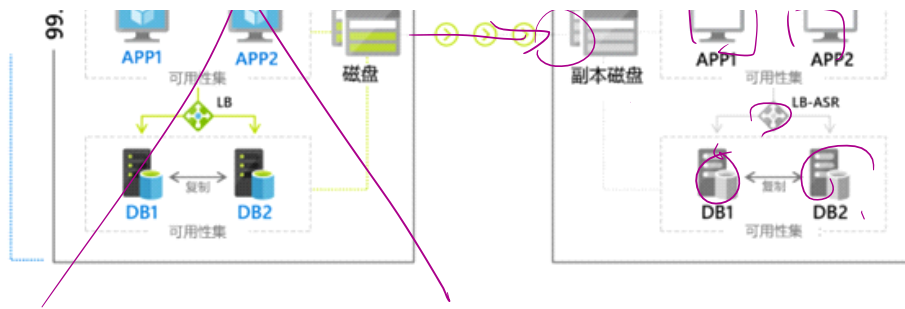
File / Volume - Win. - MARS (Agent) - 目标  
VM - 排程 (一天3次)  
DR. - Live Migration. - Job



Test Failover

Failover

Manual  
Auto



Azure Monitor

Log Analytics Workspace

- Built-in Storage
- Solution
- Log
- Tables

7~35天 - 90day

Export Storage - LTR (Linked)

Kusto Query Language (KQL)

SQL like logic