

Identity

On-Prem

(Sync)
Entra ID Connect

Azure

Active Directory != Entra ID

LDAP
Kerberos
NTLM

HTTP/S
X DU
X GPO

OAuth2
OpenID
WS Fed

EIDDS (Managed)

LDAP
Kerberos
NTLM

功能	免費	Microsoft 標識碼 P1	Microsoft 標識碼 P2	Microsoft Entra 套件
單一登入 (無限制)	✓	✓	✓	
雲端和同盟驗證	✓	✓	✓	
進階群組管理		✓	✓	
自助服務帳戶管理入口網站	✓	✓	✓	
多重要素驗證 (MFA)	✓	✓	✓	
條件式存取		✓	✓	
風險型條件式存取 (登入風險、使用者風險)			✓	
自動將使用者與群組佈建到應用程式		✓	✓	✓
Privileged Identity Management (PIM)			✓	✓
進階身分識別治理				✓

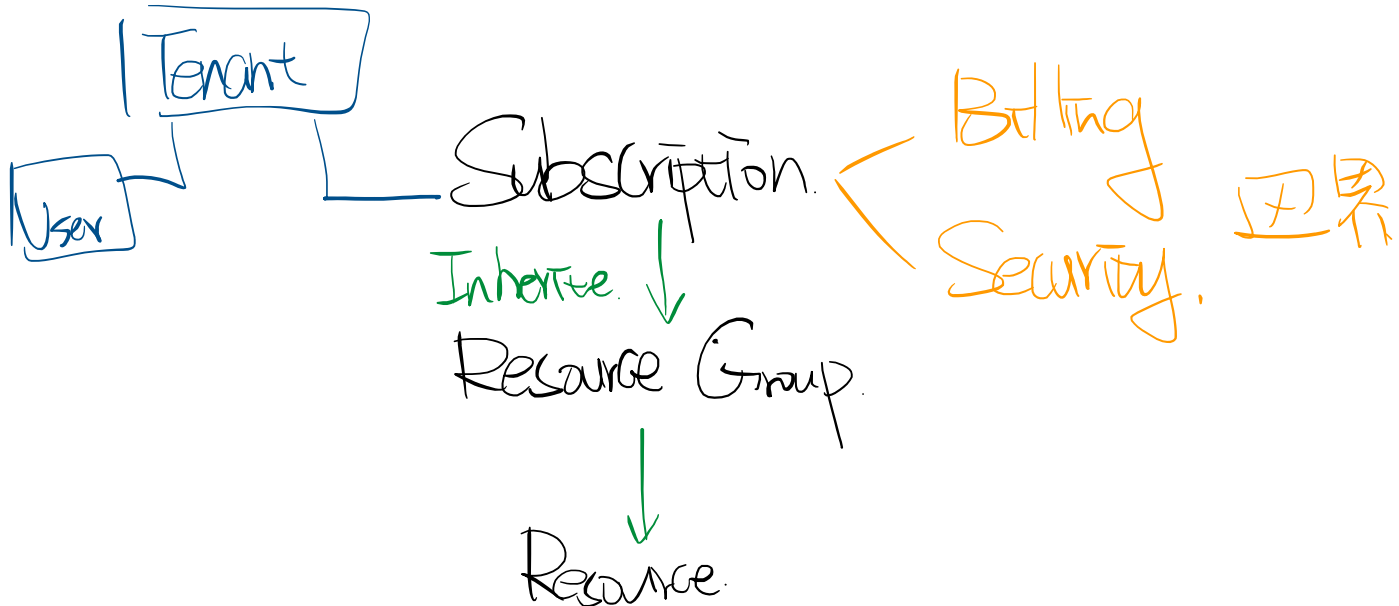
User

Entra ID

Azure

User ~~Identity~~ Azure
 Global Admin
 Group User Admin ← ~~?~~
 Global Admin

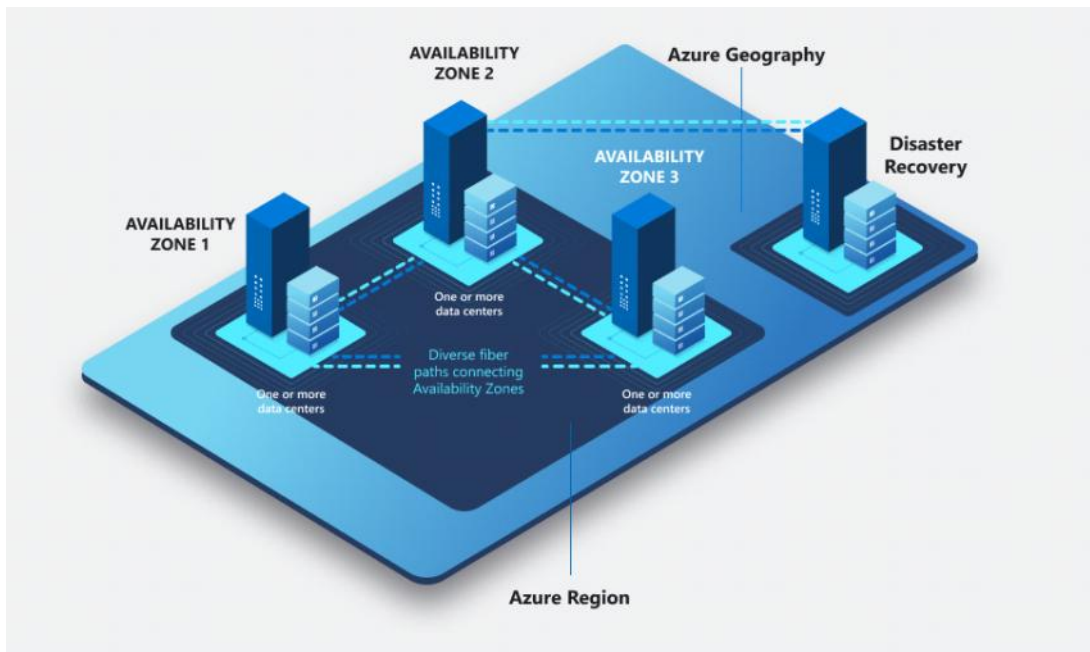
Types - Security
 ↳ MBBS
 Assign - Manual
 ↳ Dynamic Expression



Region - Availability Zone - Data Center

Region - Availability Zone - Data Center
x3. xN.

[Pair
[Coding
[Core/Net



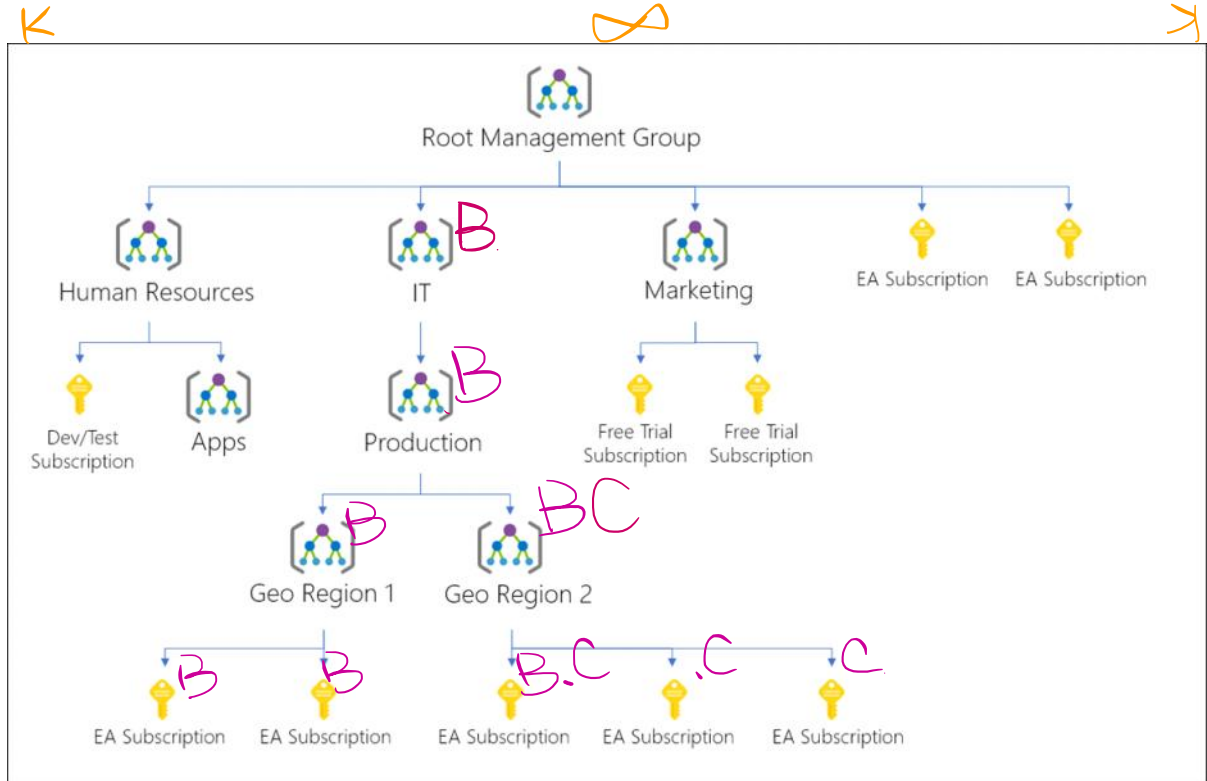
Which Region?

Region Pair.

Management Group - Inherit
- Tree Structure

- 100% STRUCTURE

- 跨 Sub



Cost Management → Service

Tag - Metadata

Azure Policy → 規則

└ Check
└ " & 強制

Definition — Policy — Built-in — Custom — JSON
 — Initiative — Policy's Folder

Assignment — MG
 — Subscription
 — RG

RBAC (Role based Access Control)

User

Group

MI

Assignment

Role = 1 ~ n Permission

— JSON
 — Built-in
 — Custom

— Action/Not
 — Data Action/Not
 — Assignable Scope

Assignment Tool

Azure Portal → Azure Cloud Shell (Container)

Azure CLI

Bash (Installer) az group subgroup command

命令 Syntax

命令式 Syntax
Azure PowerShell

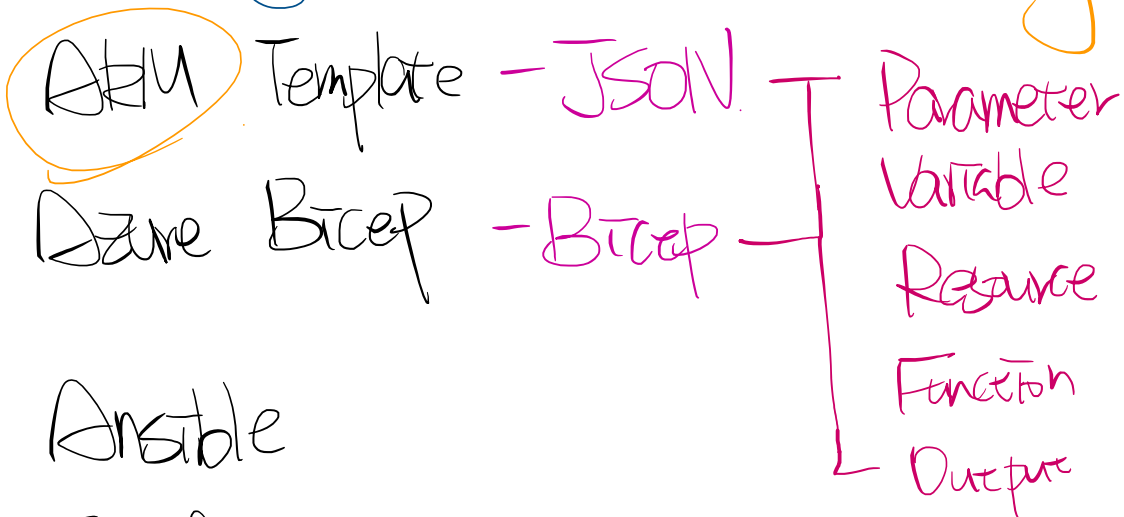
Powershell (Module)

↳ Cmdlet V.-N. New-AZRM

Azure Rest API

宣稱式 Syntax (декларатив性)

Azure Resource Manager
↳ Management Layer



Ansible

Terraform

...

Virtual Network (VNET) - Addy Space - CIDR
 L Independent SDN. 10.10.0.0/16
 L Subnet x n 192.168.10.0/24

Sub 1 10.10.10/24, $\Rightarrow 256 - 5 = \underline{251}$

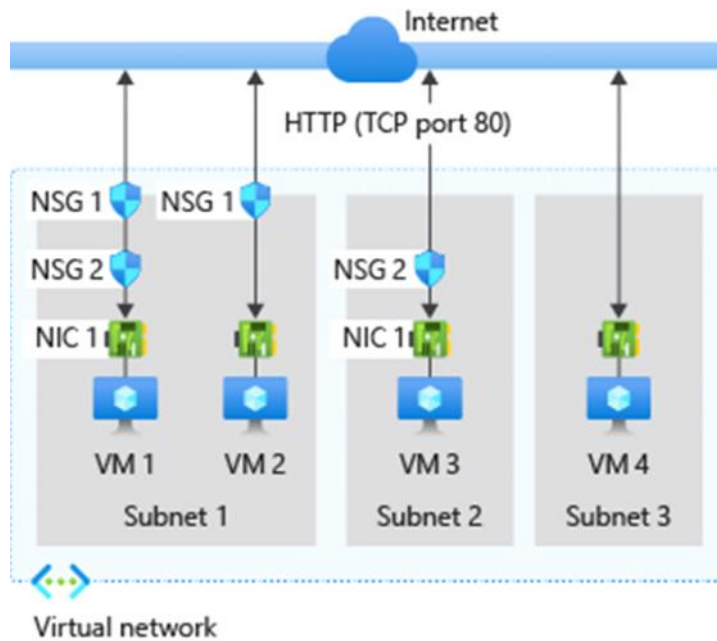
Sub 2 192.168.10.0/24

IP L Private IP - Dynamic / Static
 L Public IP - Azure Resource
 IP4/6 Static

NSG (Network Security Group) Layer 4 FW (TCP/IP)
Rules L InBound Stateless
 L OutBound Free

① 3389 . V
 ② 3389, X

Priority $\Rightarrow$ Smaller

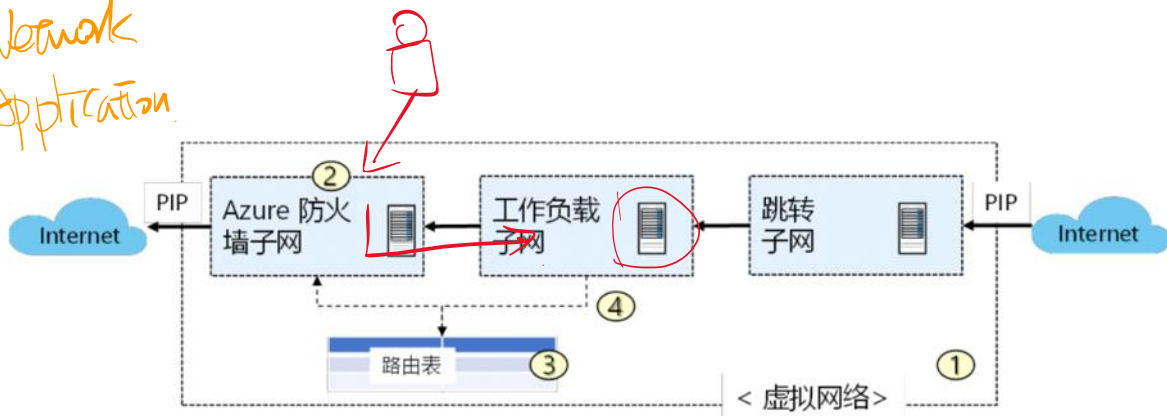


Azure Firewall (PaaS) Layer Stateful

(VM) - 数据
Subnet

HA
Scale
Maintain

NOT
Network
Application



Route

System Route (Azure)

User Define Route - Route Table

└ Route x n.
└ Link subnet

DNS

Azure DNS Zone (PaaS DNS Server)

└ Public - Internet - Child Zone a.com
└ Private - Any name money.local
└ Link vnet.

☑ Auto Registration (Discovery) By Vnet

Inter Site Connectivity

VNET $\leftrightarrow$ VNET

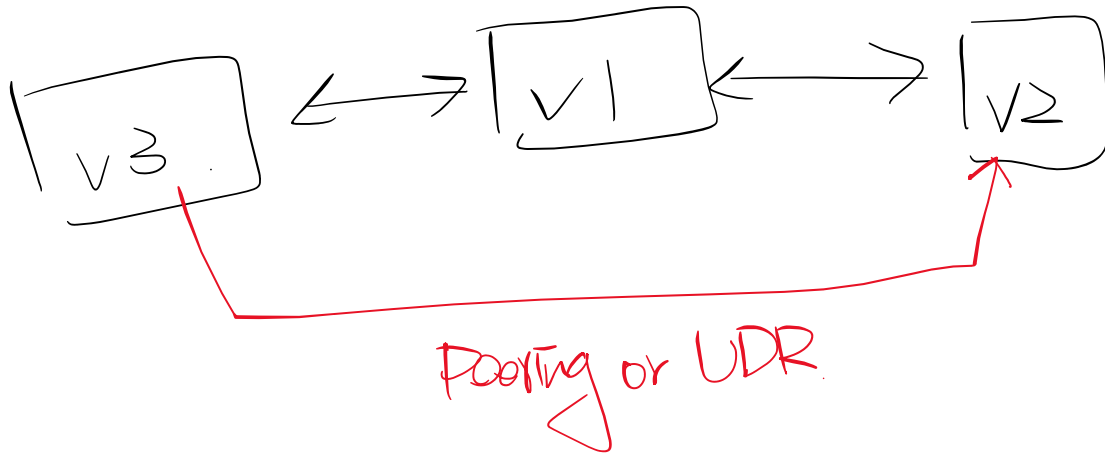
Peering (对接)
(VPN)

同 Region
跨 " "
" Sub

VNET $\leftrightarrow$ Other

On Prem
Other

Azure



Virtual Network Gateway (VPN Gateway)

└ gateway subnet

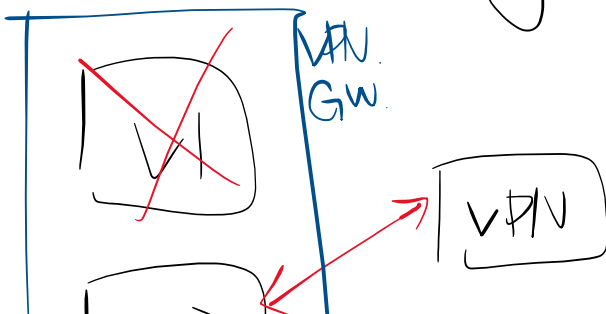
(PaaS) (VM)

└ VPN ┌ Point to Site
└ Site to Site

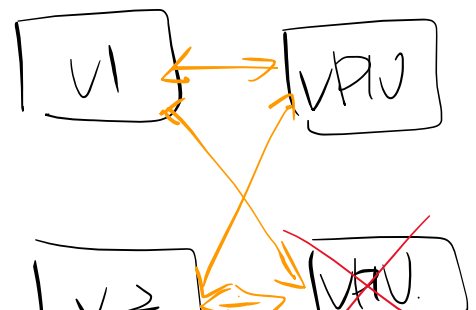
VNET
Site
Site

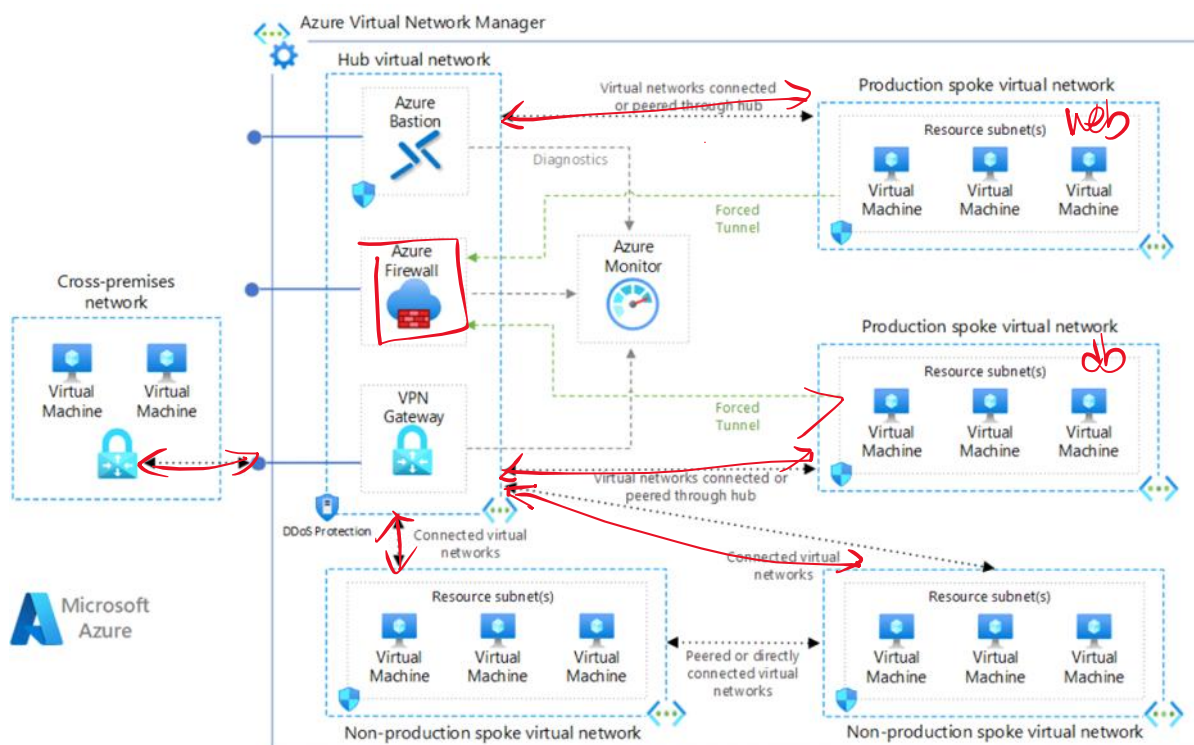
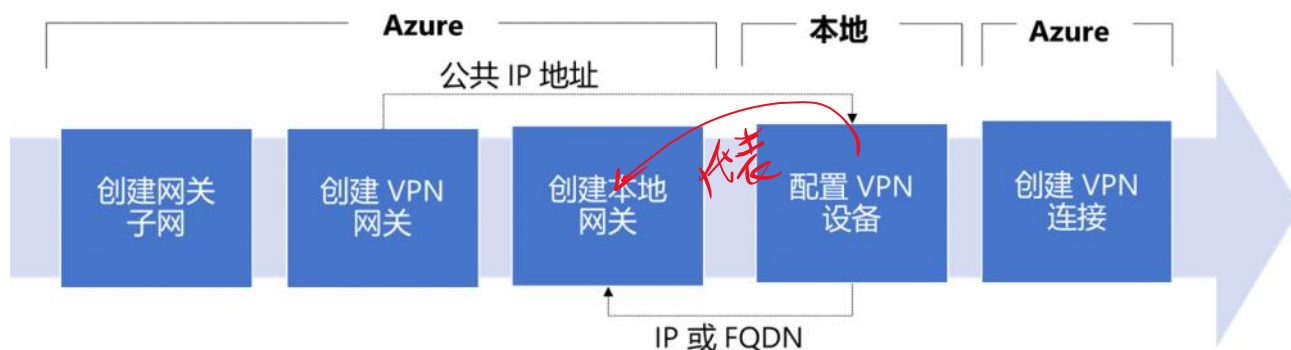
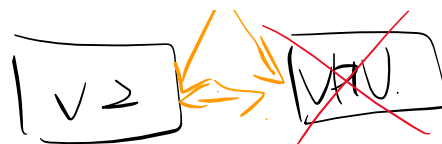
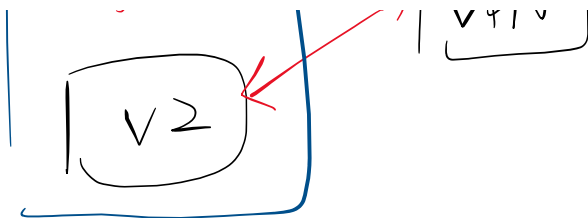
└ Express Route

Active Standby

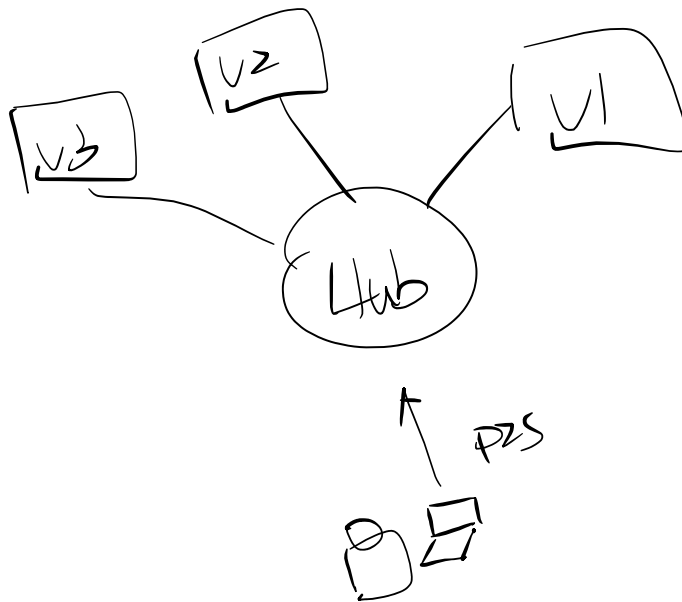
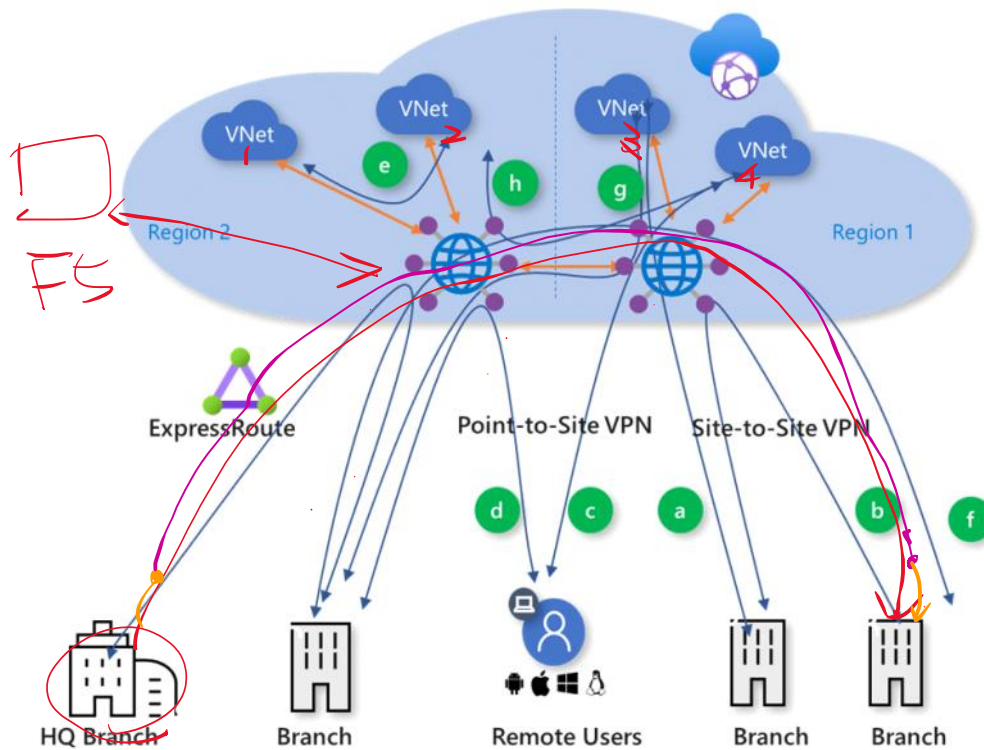


Active Active



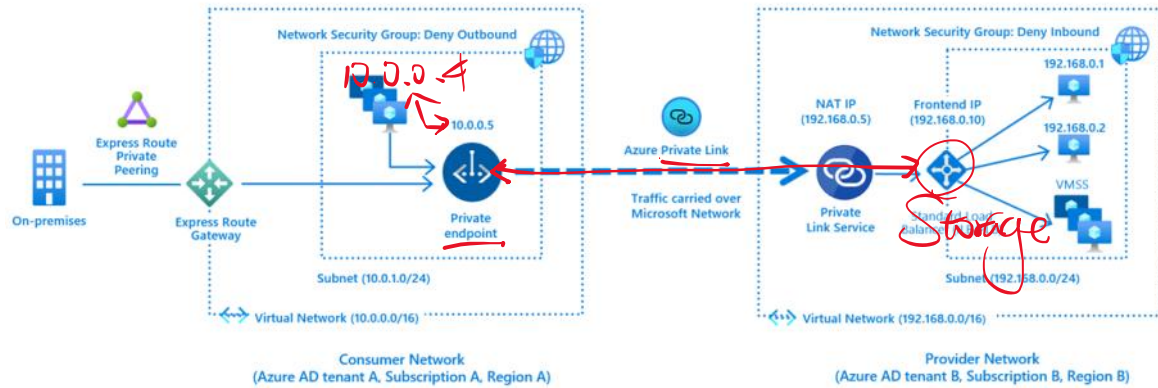


Virtual WAN. (Managed Hub-Spoke)



功能	應用程式閘道	Front Door	負載等化器	流量管理器
使用情況	使用 Web 應用程式防火牆增強應用程式安全性時，優化來自應用程式伺服器場的交付。	可縮放的安全增強型交付點，適用於基於微服務的全域 Web 應用程式。	均衡入站和出站連接以及對應用程式或伺服器終結點的請求。	在全球 Azure 區域內以最佳方式向服務分發流量，同時提供高可用性和回應性。
協議	HTTP、HTTPS、HTTP2	HTTP、HTTPS、HTTP2	TCP、UDP	Any
區域	是	✓	是	是
全局		是	是	是
Env	Azure、非 Azure 雲、本地	Azure、非 Azure 雲、本地	Azure	Azure、非 Azure 雲、本地

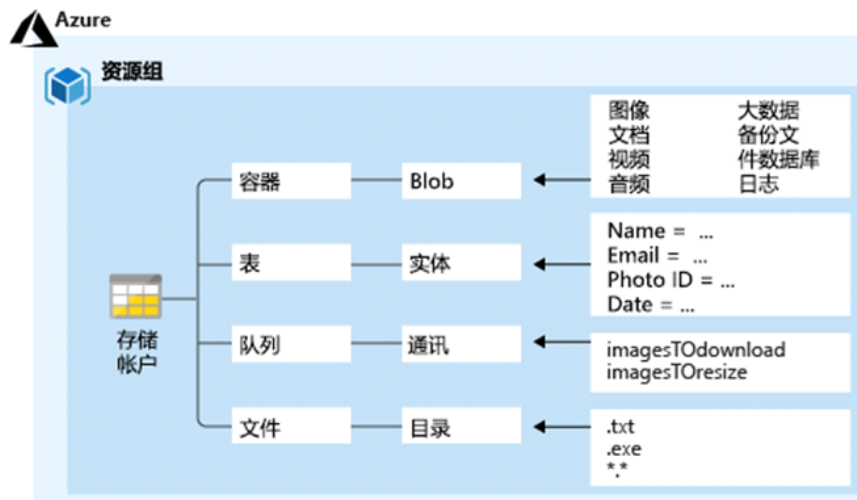
全局		是	是	是
Env	Azure、非 Azure 雲、本地	Azure、非 Azure 雲、本地	Azure	Azure、非 Azure 雲、本地
安全性	WAF	WAF、NSG	NSG	



Private Link

Azure Storage.

- Blob — HTTP/S. (SFTP)
- Files — SMB, NFS.
- Queue — MSG.
- Table — NOSQL, Key-value



⚠️ Datacenter Cooling Event - Southeast Asia

Impact Statement: Starting around 20:19 UTC on 7 February 2023, a utility power surge in the Southeast Asia region tripped a subset of the cooling units offline in one of the Availability Zones. While working to restore the cooling units, temperatures in the datacenter increased so we have proactively powered down a small subset of selected compute and storage scale units, to avoid damage to hardware and reduce cooling system load. All impacted storage and compute scale units are in the same datacenter, within one of the region's three Availability Zones (AZs). Multiple downstream services have been identified as impacted.

Current Status: We do not have an exact ETA at this time, we currently expect an extended period of time to fully restore all cooling capacity. The Azure service recovery process will commence at this time and is expected to progressively return over a number of hours. Due to the nature of this issue our storage scale units are expected to require significant recovery efforts to ensure all resources return in a consistent state. Note that any new allocations for resources will automatically avoid the impacted scale units. If your workloads are protected by Azure Site Recovery or Azure Backup, we recommend to either initiate a failover to the recovery region or recover using Cross Region Restore.

Customers using services that are zonally-aware may consider failing out of the impacted zone, physical zone AZ-03. Note that physical zones are mapped to logical zones in your Azure subscription, Refer to: <https://learn.microsoft.com/rest/api/resources/subscriptions/check-zone-peers>.

This message was last updated at 08:44 UTC on 08 February 2023

2021

Millions of websites offline after fire at French cloud services firm

By Mathieu Rosemain, Raphael Satter

3 MIN READ



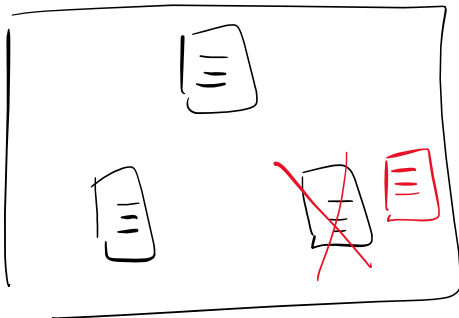
©Microsoft Corporation

Alamy

Redundancy (4+2) 3 ~ 6 Cops

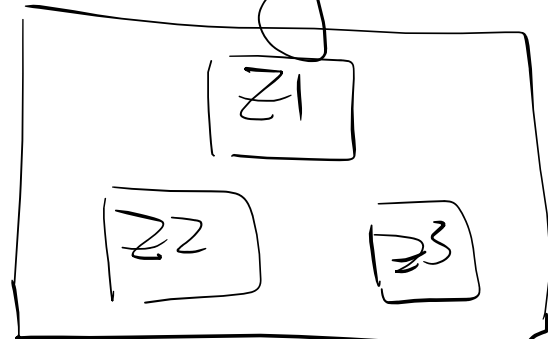
LRS (Local)

10 Region, 10 AZ
Zone



ZRS (Zone)

10 Region, 3 AZ
Region



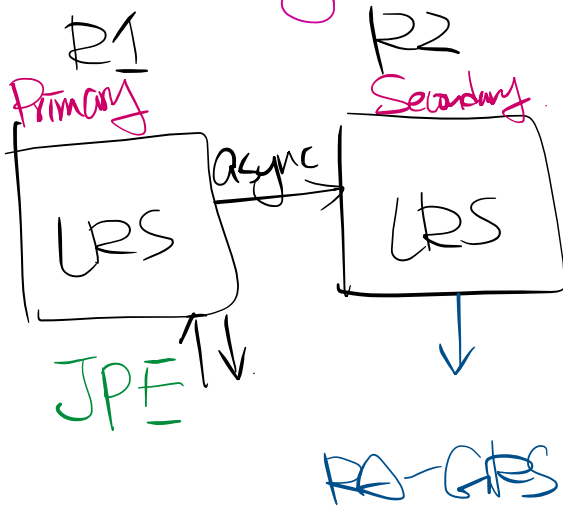
GRS (Geo)

7 AZ - 7 AZ

GZRS (Geo+Zone)

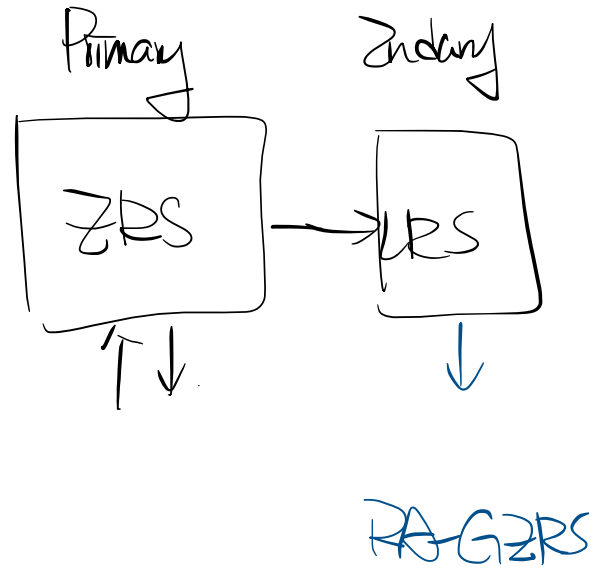
25 Region, 3 AZ

2 Region, 2 AZ
 Region Pair.



60qps

2 Region, 3+1 AZ.



Pricing — Space
 — Transaction.

Performance — Standard
 — Premium

Access Tier: Hot
 Cool
 Gold
 Archive
 By Blob
 — Lifecycle Management
 — Rules (JSON)

Blob Storage
 Single Layer

Account — Container — Blob.

images — img1.jpg → 文件夹 Folder

images - img1.jpg
 - 2025/08/img1.jpg

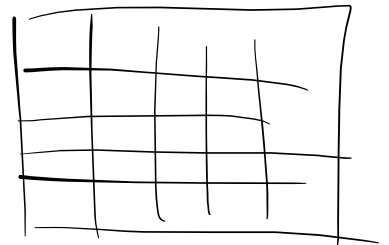
模拟 Folder name

Block Blob → 顺序 Access.

└ Append Blob (Small file)

Page Blob - Random Access
 (.VHD)

mp4 100MB, 4MB



⇒ 25 Block
 ⇒ 26 API

1KB (Log)



64K

Authn + Authz

└ Access key
 └ Entra ID

[Extra +
 Shared Access Signature

demo0821stor.blob.core.windows.net/images/IKEA.jpg

<https://demo0821stor.blob.core.windows.net/images/IKEA.jpg>

?sp=r&st=2025-08-21T03:10:51Z&se=
 2025-08-21T11:25:51Z&spr=https&sv=2024-11-04
 &sr=b&sig=vOYrk%2FDO5czxbBBIZPrPonj4%
 2Bc5iYqL708pgBhsEMk%3D

+key

] = ? (V)
 (X)

VM

Compute - Type - Series - Size
 Storage - Managed Disk -> Resource

Standard HDD

" SSD

Premium "

⋮

HA

(Resource) (Config)

()

H H

(Resource) (Contig)

Availability Set

2-3

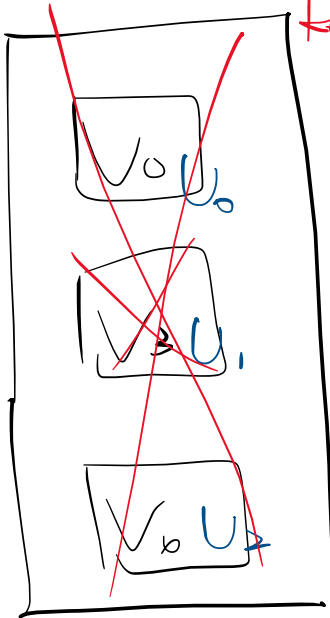
Fault Domain - Hardware

2-20

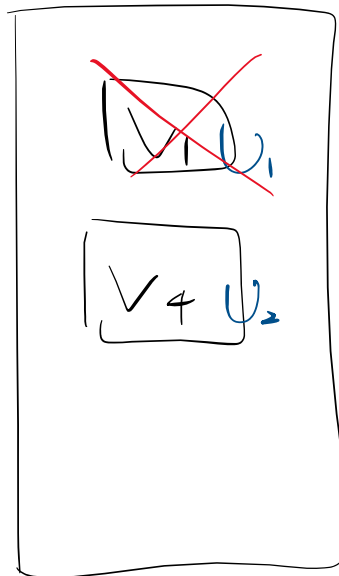
Update Domain - Update

F₀

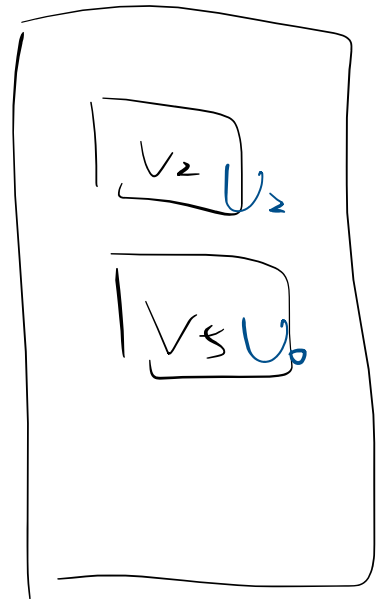
Auto
Recovery



F₁



F₂



VMSS

AV Set / Zone

Management

Scale — Flex — Manual
 — Uniform — Auto (Metric)

2 ✓

☐ Specify start/end dates ☒ Repeat specific days

☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday
☐ Friday ☒ Saturday ☒ Sunday

(UTC+08:00) Beijing, Chongqing, Hong Kon... ▾

00:00 ✓

23:59 ✓

☐ Scale based on a metric ☒ Scale to a specific instance count

1 ✓

☒ Specify start/end dates ☐ Repeat specific days

(UTC+08:00) Beijing, Chongqing, Hong Kon... ▾

08/24/2025 📅 12:00:00 AM

08/30/2025 📅 11:59:00 PM

8/24 vm?

PaaS

Azure App Service

— App Service Plan (VMSS)

— App Service (Web App) (Sandbox)

— Compute
 — Feature
 — Pricing

Container

Azure Container Registry - Docker Registry 2.0

└ Private
└ Public

VM - Nested Virtualization

Azure Container Instance (ACI)

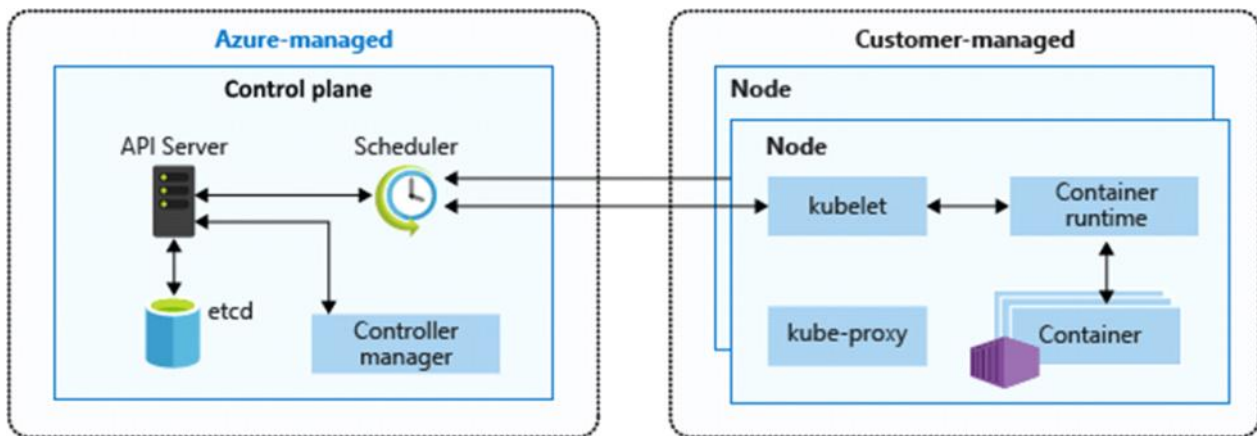
Azure Web App for Container

Azure K8S Service (AKS)

✓ Azure Container App (ACA)

K8S API (V)

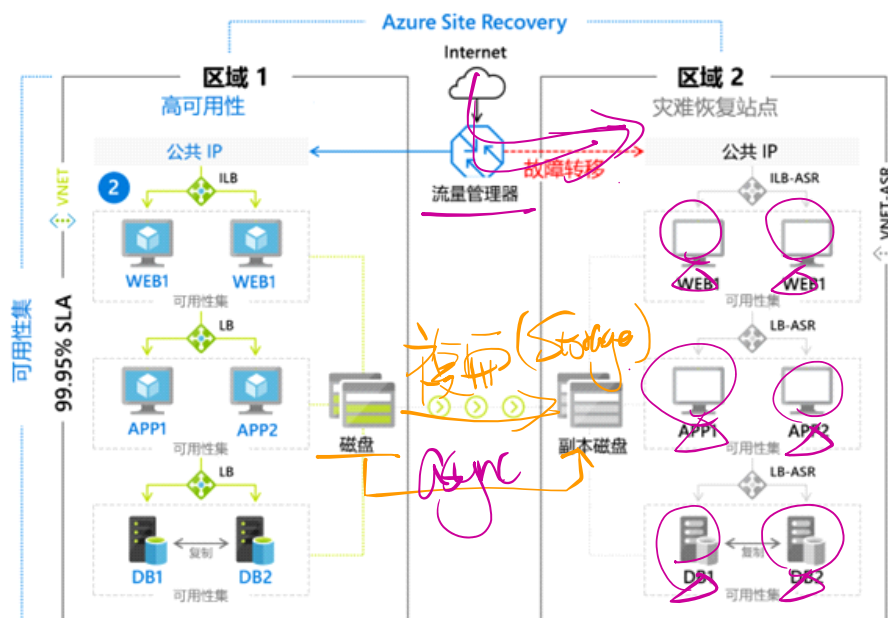
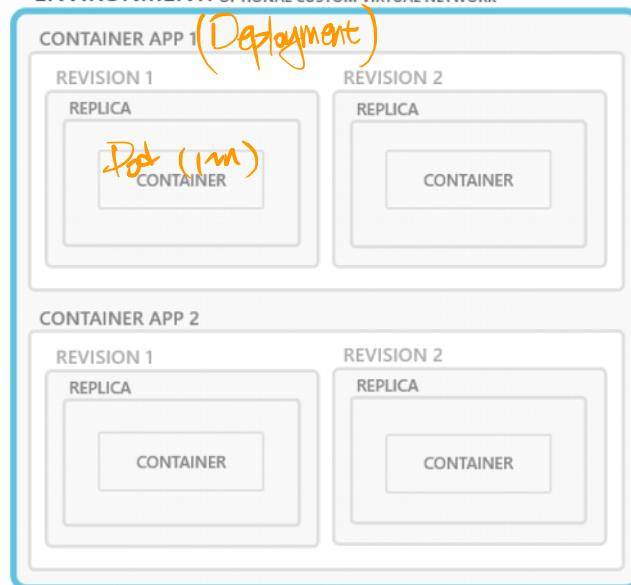
└ K8S



ENVIRONMENT: OPTIONAL CUSTOM VIRTUAL NETWORK



Environments are an isolation boundary around a collection of container apps.



Log

Log Analytics Workspace (Resource) [Metric Log] Table

└ Built in Storage (Managed)

└ Retention

└ Interactive
└ Archive

└ Visual
└ Workbook
└ KQL

Kusto Query Language
SQL like Logic

Parsing Ingest
└ Save