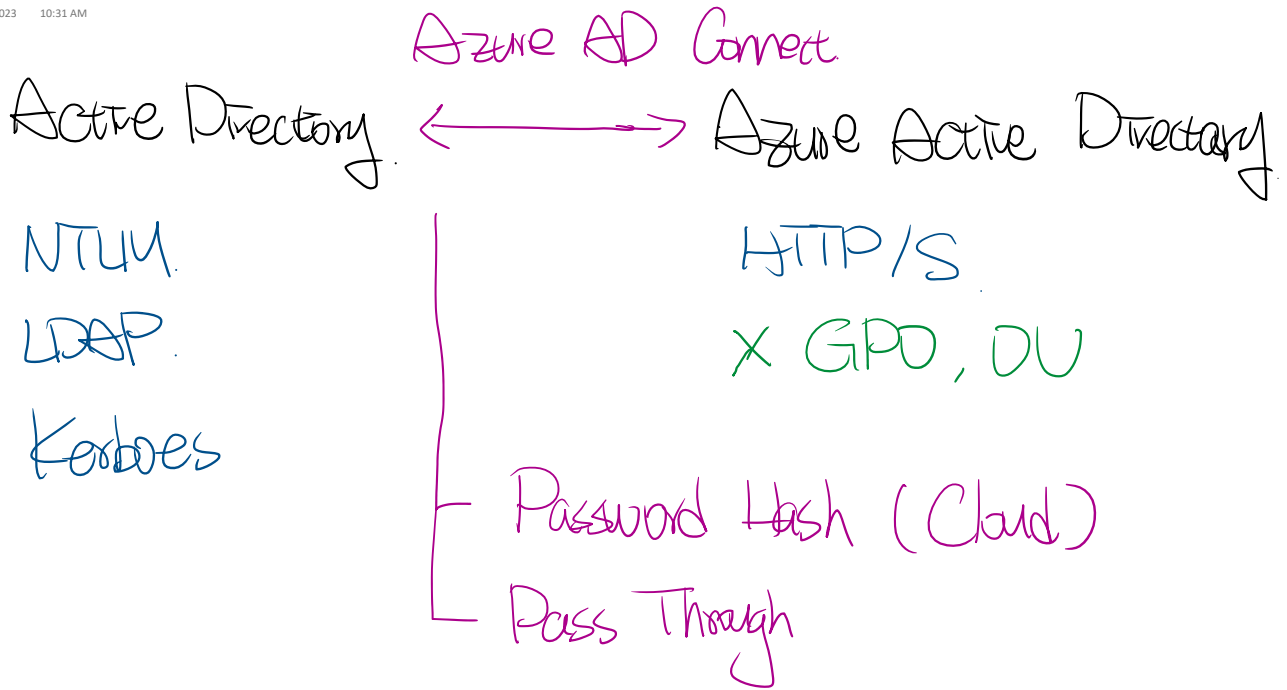




Tenant ~~租戶~~ = Directory 目錄

Azure AD Domain Service

User

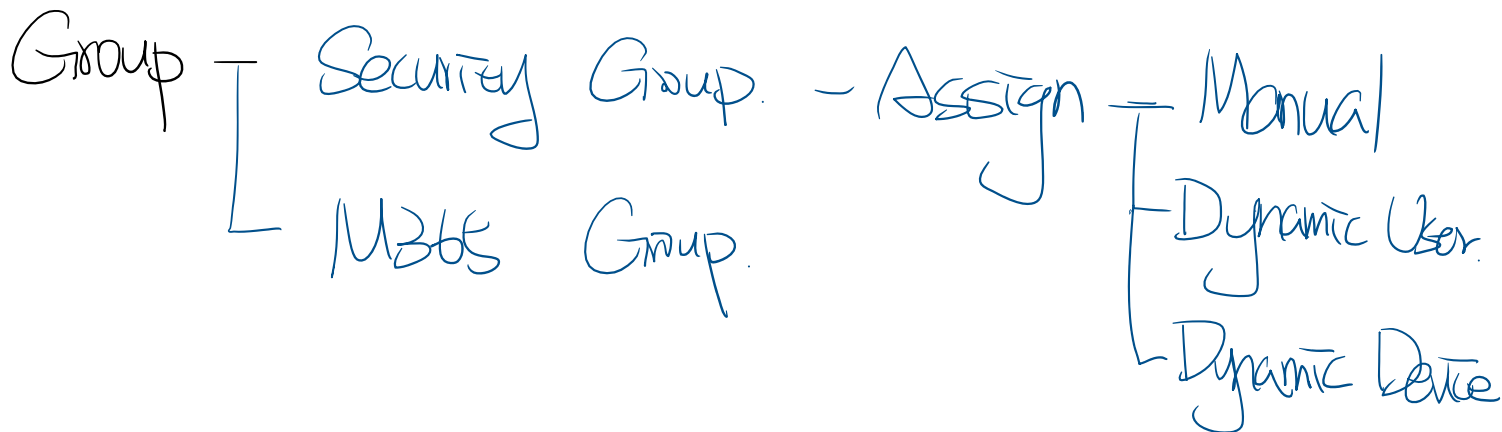
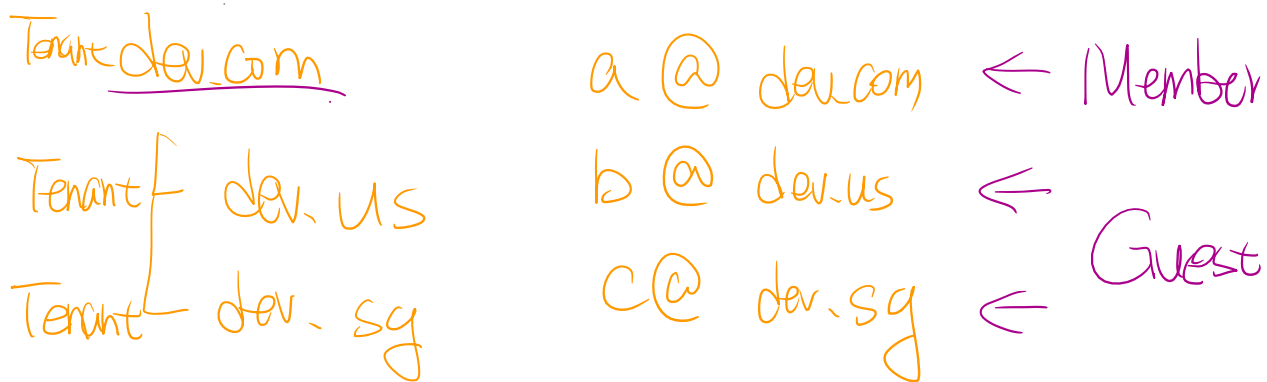
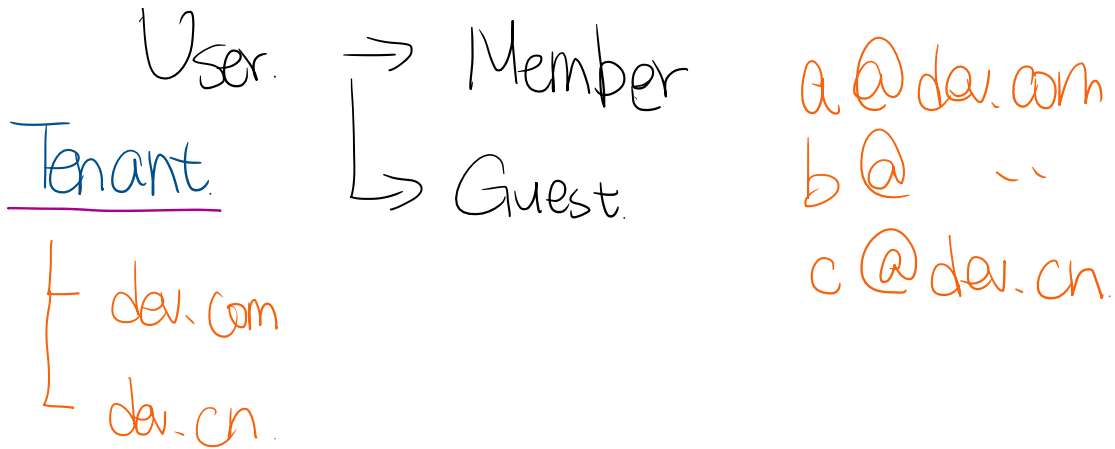
[Global Admin AAD
User Admin

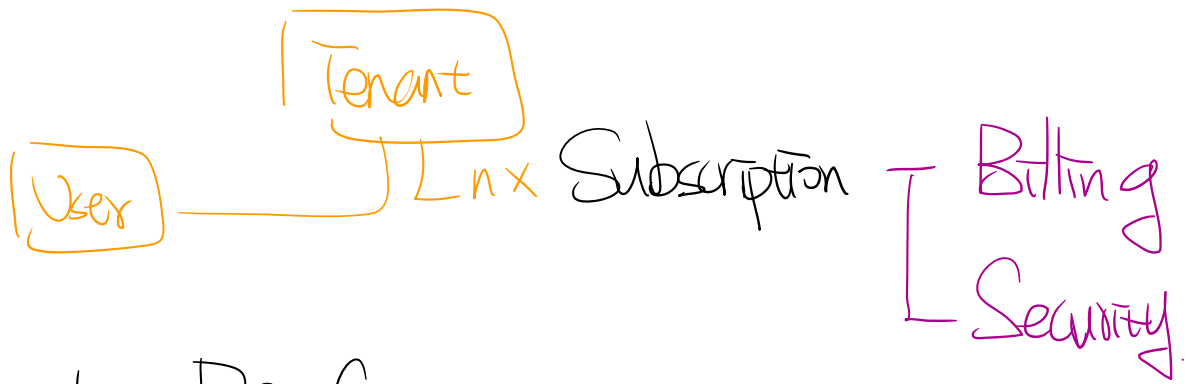
Azure Global Admin. → No.

! = Azure AD

Azure AD Join

Registered (BYOD)





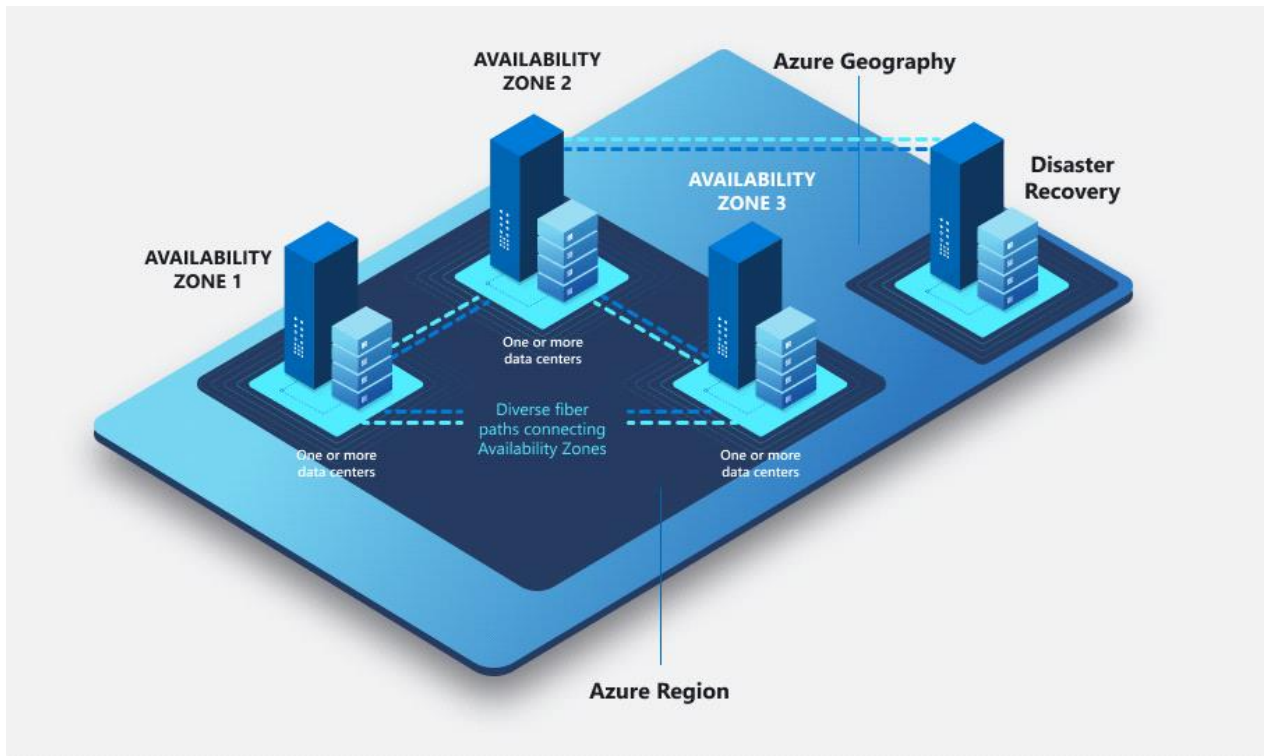
Region 1 = DataCenter.

Pay as U Go

CSP

ED



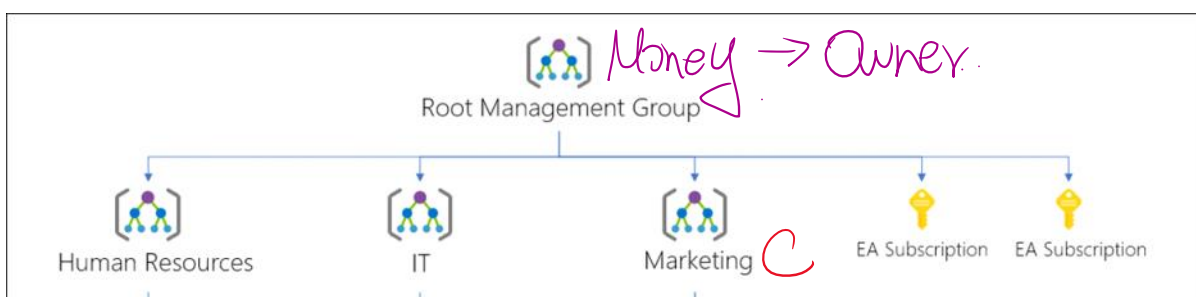


Region Pair.

Ltense

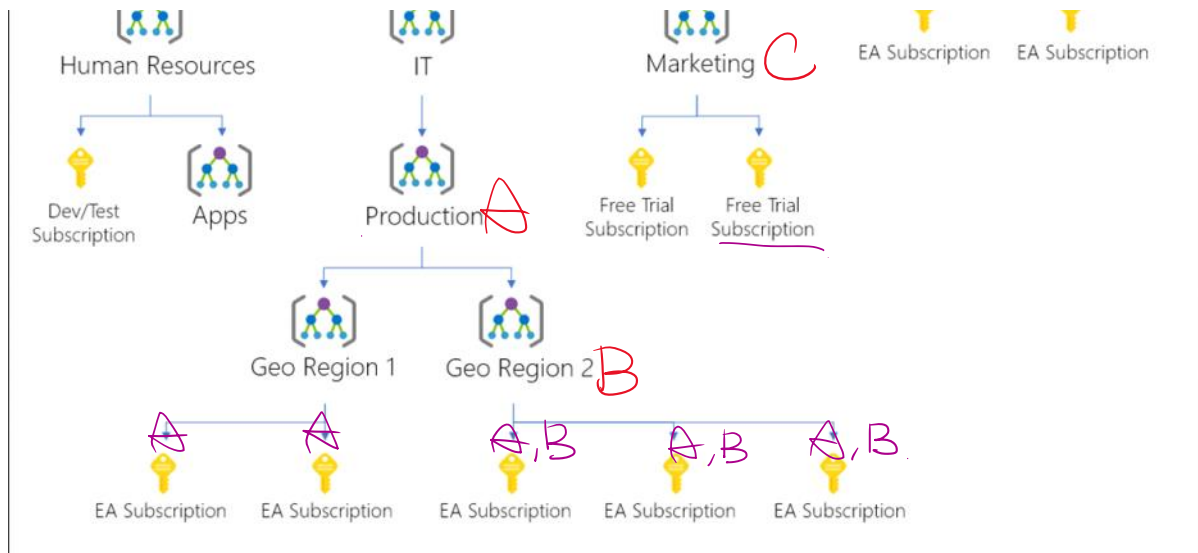
BYOL (Win, SQL SW)

Management Group — Tree Inherited



500 max





6

Tag - Metadata

Azure Policy ⇒ 規則

檢查 or 強制

定義 [Policy - Built-in
Custom - JSON
Initiative - Policy's Folder

Assignment | Subscription
| RG

ARM → Azure Resource Manager.

→ Management Layer | RBAC
Scope
Sub, UG, RG, Res...

User | Assignment | Role based Access Control.

Security Principle 安全原理

| In Permission.
JSON

| User Principle
| Service Principle

| Action / NotAction
| DataAction / NotDataAction
| Assignable Scope

Azure Portal

| Azure Cloud Shell

Azure PowerShell

PowerShell's Module

PowerShell's Module

跨平台

Cmdlet $\Rightarrow$ v.-n.

New - AZUM

Azure CLI

Shell Script

跨平台, Installer

AZ. n. V. $\rightarrow$ Action.

SDK group (sub)

Azure REST API

命令式

宣告式 $\rightarrow$ декларативность

ARM Template - JSON

Azure Bicep

Parameter

Variable

Resource

Function

Output

Pre Define
User Define

Blank + VS Code Ext.
Gallery

Export

Networking.

Virtual Network (VNET) - Addr Space - CIDR

Independent

10.10.0.0/16

Subnet x N.

10.10.1.0/24 → .0, .1, .2, .3, .255
256 - 5 ⇒ 251

10.10.2.0/29 → 32 - 5 ⇒ 27

IP - Private IP - Dynamic, Static

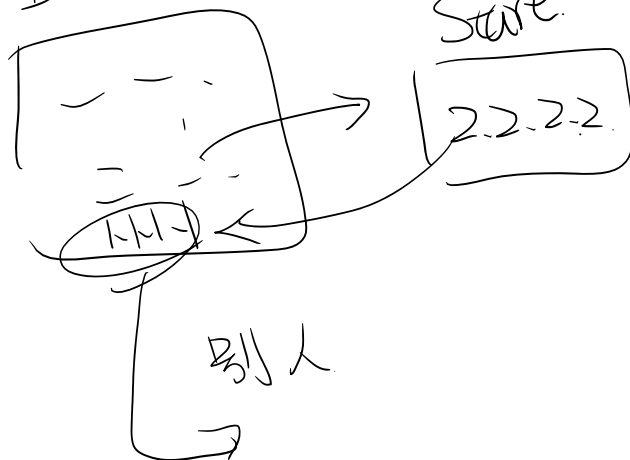
Public IP - Azure Resource

→ FQDN

Pricing

Basic Dynamic
Standard (AZ) Static

IP Pool



NSG (Network Security Group)

Layer 4 FW (TCP/IP)

NSG (Network Security Group)

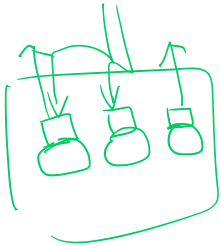
Layer 4 FW (TCP/IP)

[InBand
OutBand]

Rule x n

Priority (int)
100~4096

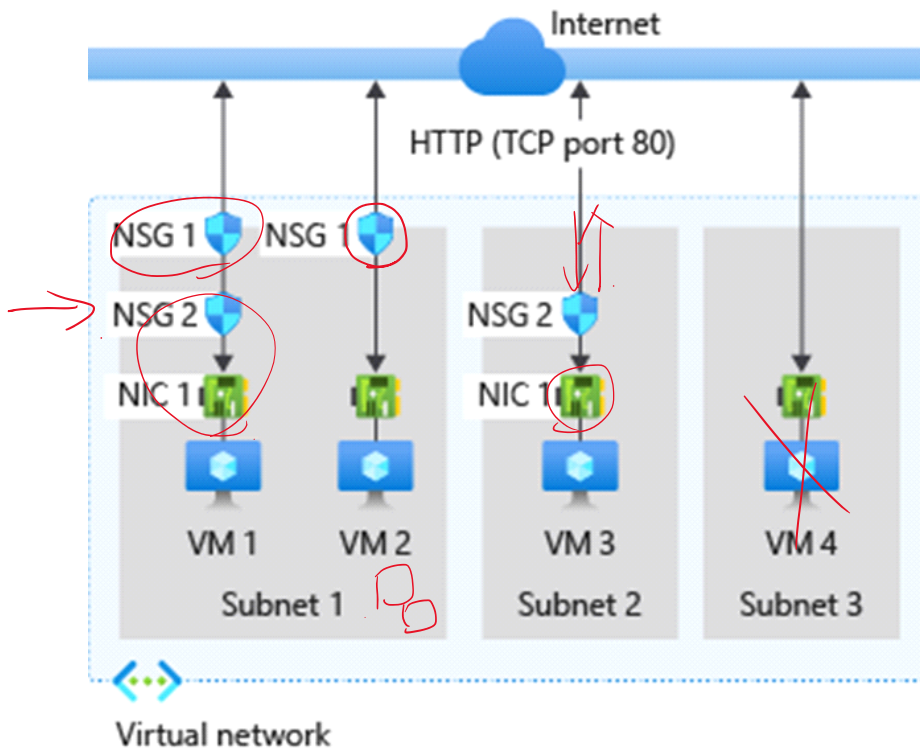
越小越优先



Rule1 → RDP V 400

Rule2 → RDP X 300

+ VM
Subnet.



Azure Firewall

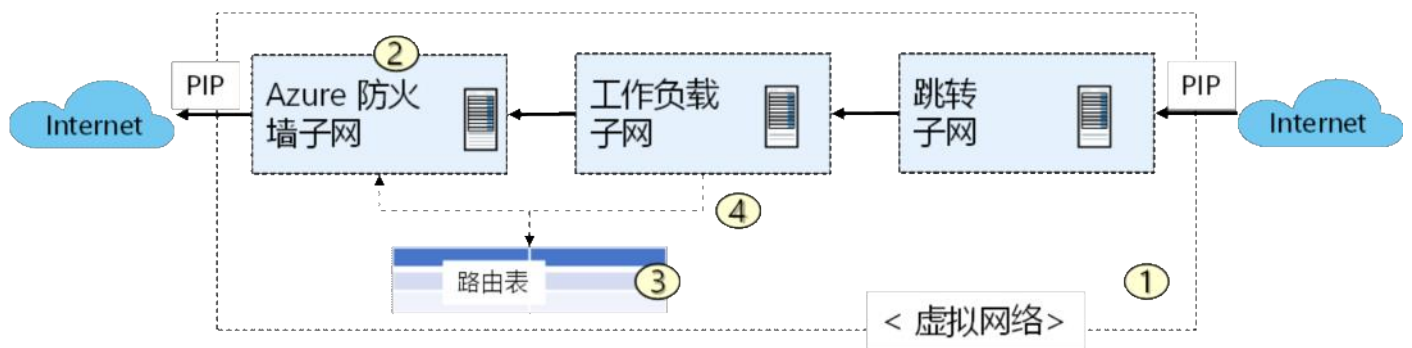
(Layer 4)

(VM) → 専用 Subnet.

Azure Firewall (Layer 1) (VM) → 専用 Subnet.

Managed
└ HA
└ Scale.

└ NAT.
└ Network (TCP/IP)
└ Application



Route └ System Route ← Azure Managed

└ User Define Route. (UDR) (n.)

└ Create Route Table - Routes.

└ Resource.

└ Associate Subnet

Azure DNS (PaaS DNS Svr)

└ Public DNS Zone

Public DNS Zone

Access Control

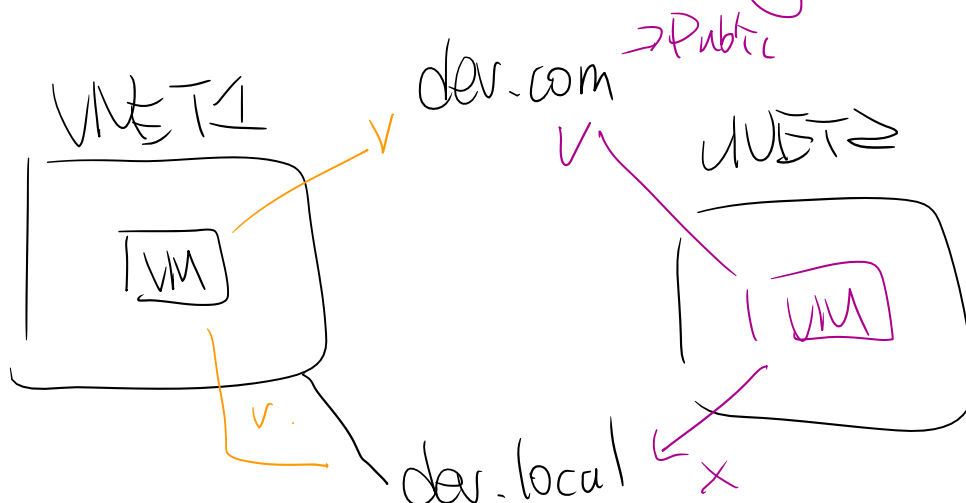
Child Zone

Private DNS Zone = Any name

dev.local
corp.com

link vnet.

Auto Registration (Discovery)



InterSite Connectivity

VNET $\leftrightarrow$ VNET

VNET $\leftrightarrow$ Other (On-Prem)

(Other Cloud)

Peering (対等)

VNET $\leftrightarrow$ VNET

同 Region
異 Region

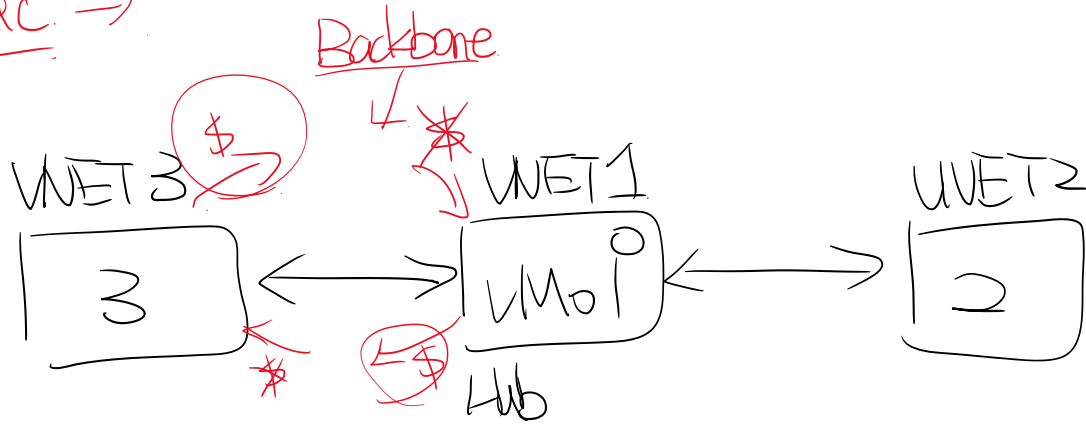
NET ↔ NET

Free

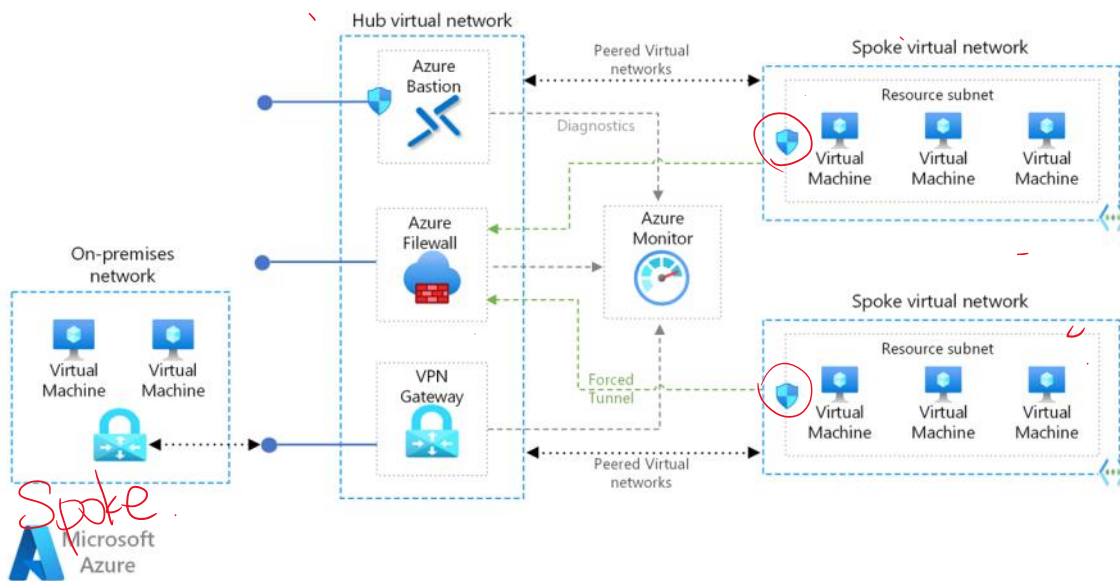
跨 - Region

跨 Subscription

Traffic →



Hub - Spoke



Virtual Network Gateway (VPN Gateway)

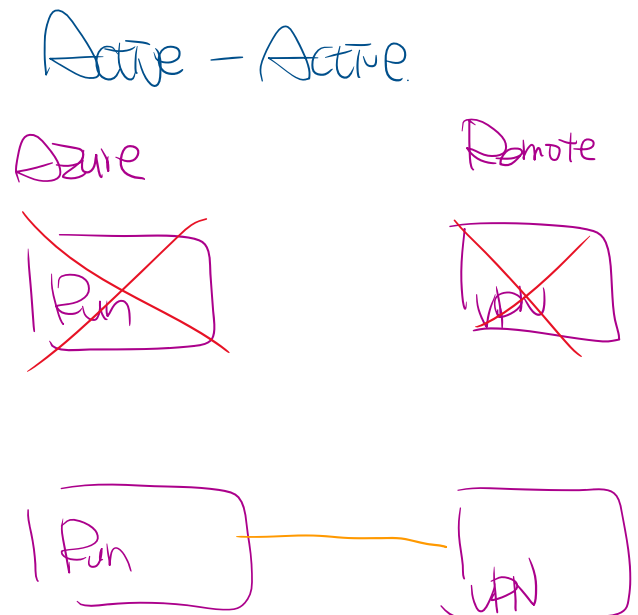
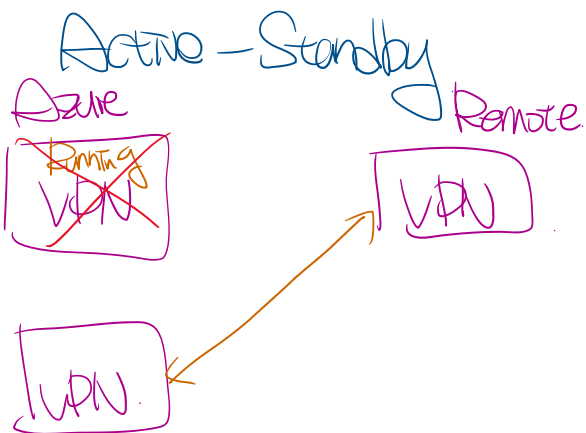
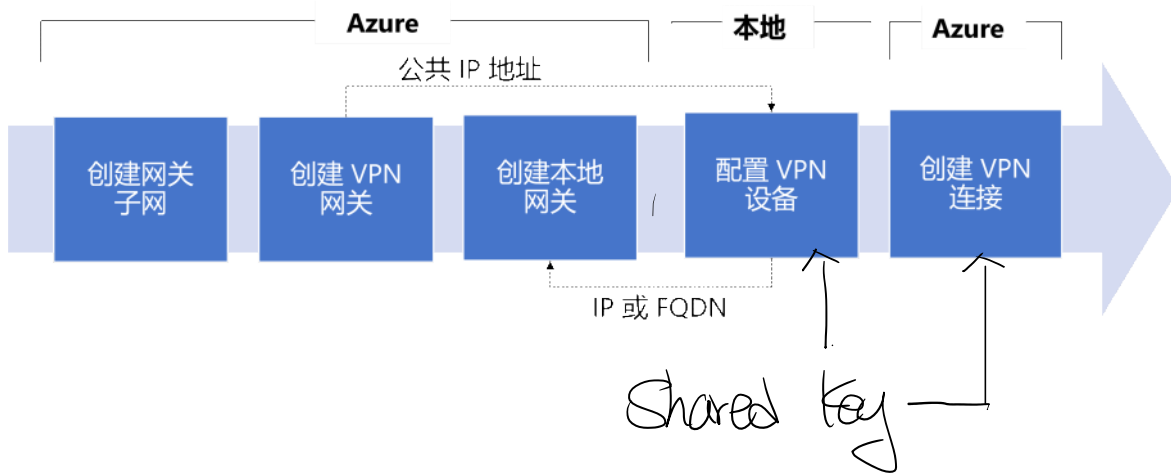
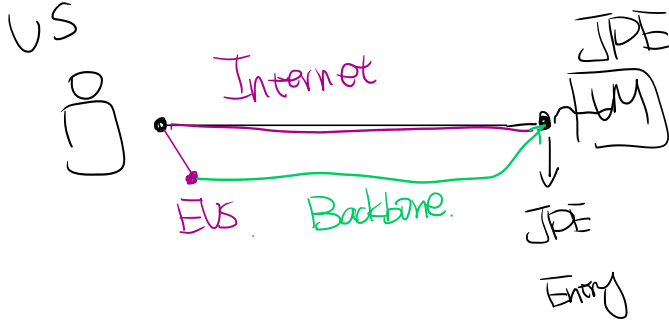
(PaaS)

VPN Point to Site

VM → HA
gateway subnet

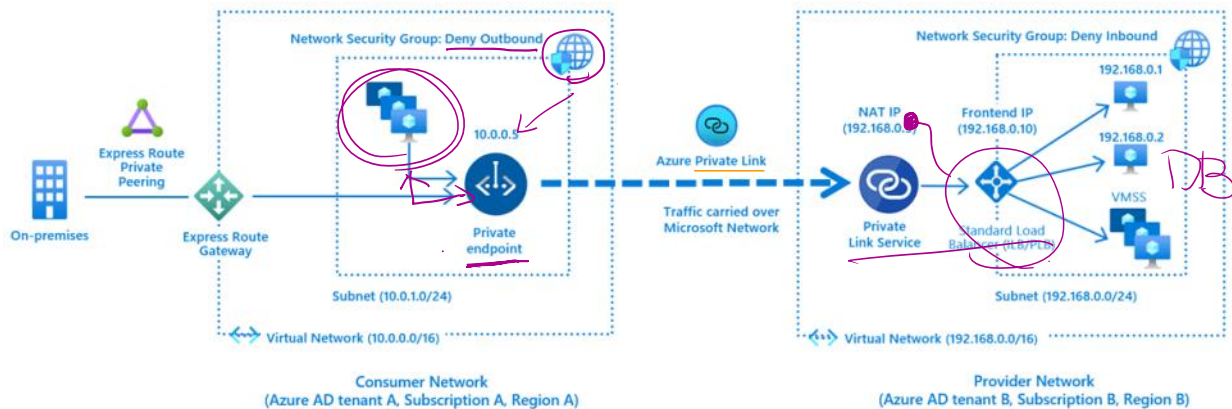
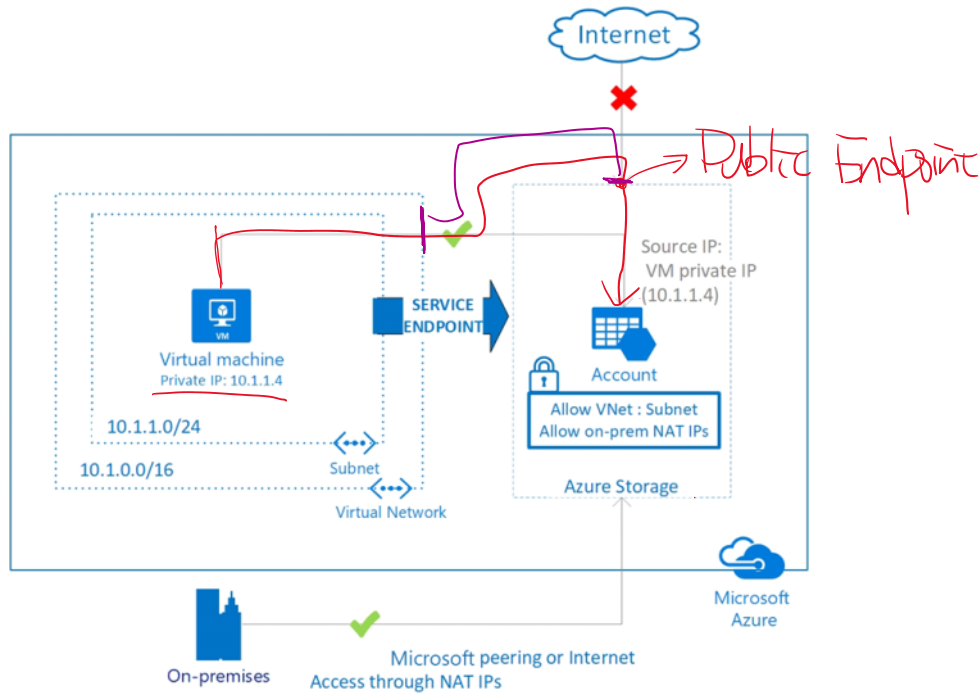
VPN. Tunnel < Site
 Site > Site
 Express Route.

Gateway Subnet



17 Note Endpoint / Link.

Service Endpoint.



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	可缩放的安全增强型交付点，适用于基于微服务的全	均衡入站和出站连接以及对应用程序或服务器终结	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

	务器场的交付。	局 Web 应用 程序。	点的请求。	用性和响应性。
协议	HTTP、HTTPS、HTTP2	HTTP、HTTPS、HTTP2	TCP、UDP	Any
专用	是		是	
全球		是		是
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	