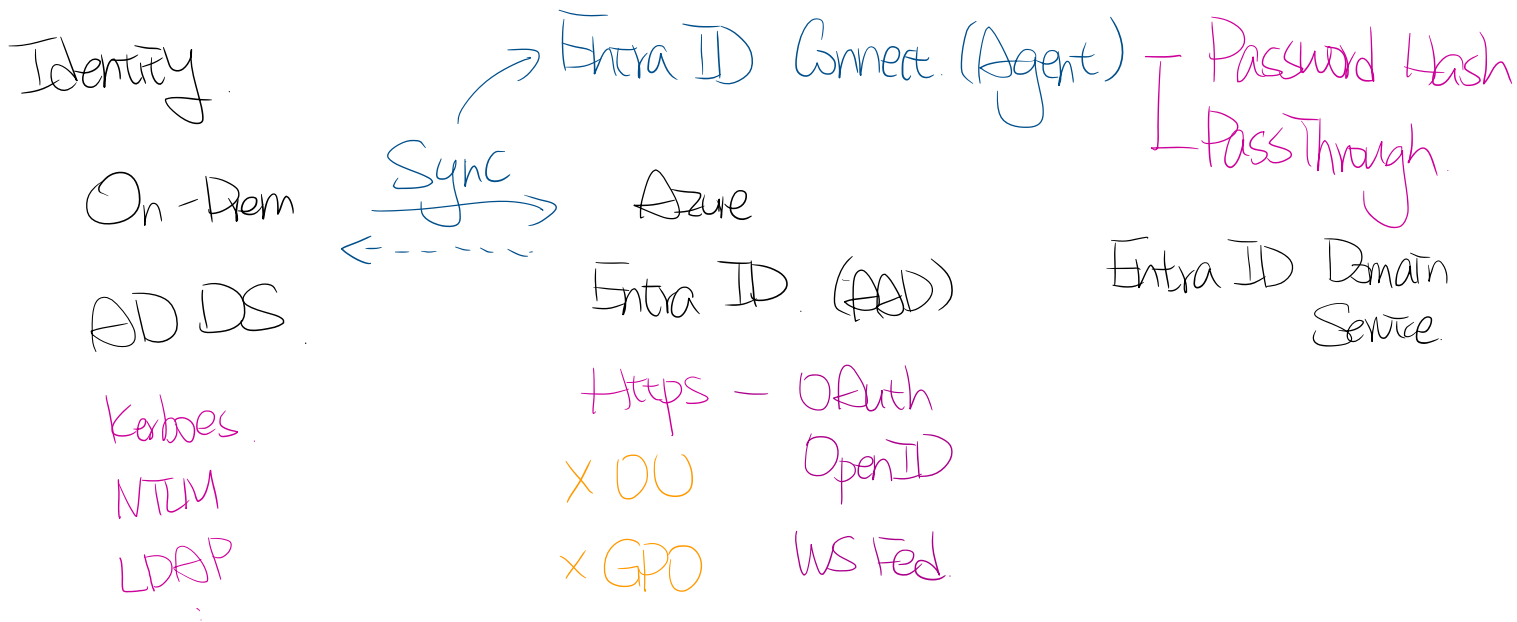




Entra ID Join

Org
Join

vs

BTOD
Register

vs

EntraID / AD
Hybrid Join

User / Groups

Entra ID Global Admin

User Admin



Azure Global Admin

User

Member

Guest

→ Tenant

mtt.com

mtt.org

mtt.dev

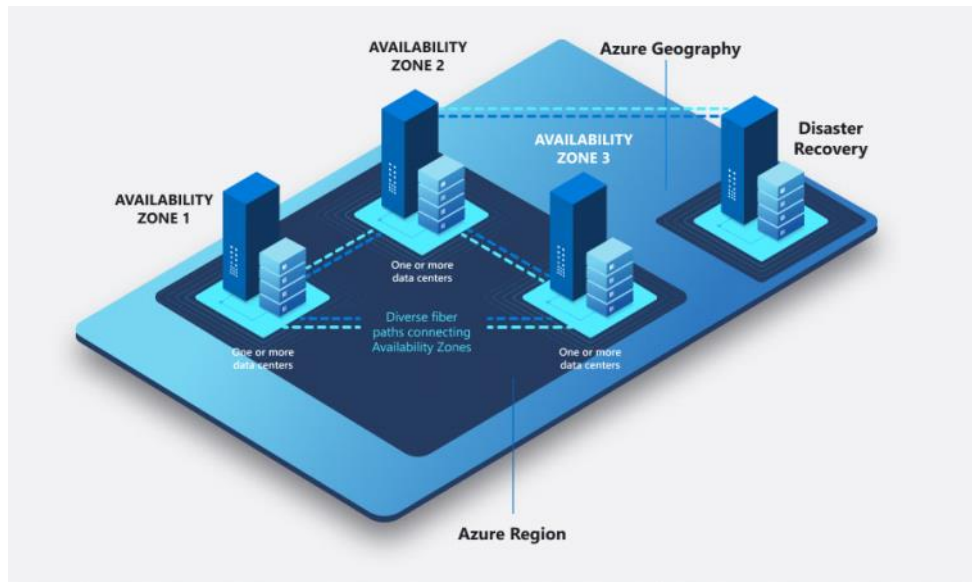
usera@met.com → member
userb@met.org →
... @met.dov → Guest

Group | Security Group - Assign | Manual
| M365 Group | Dynamic | User
| | Device

Security Principle | User Principle
| Service Principle

Region ! = Data Center





Region Pair

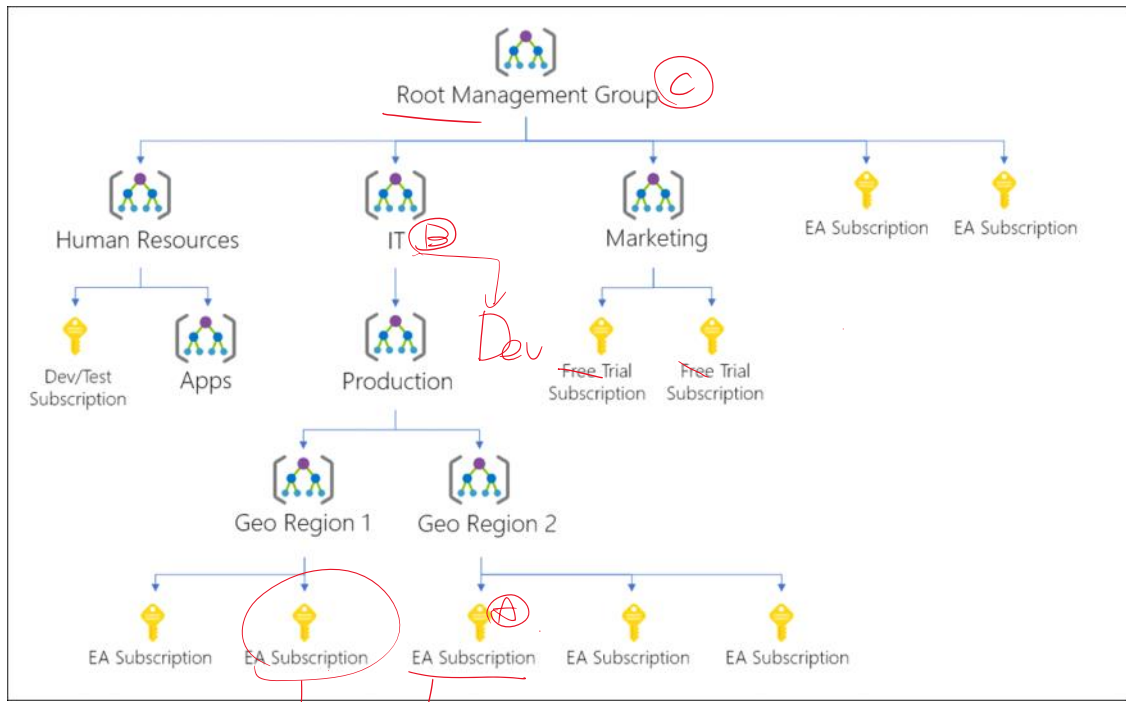
Region

- Latency
- Hybrid Benefit (BYOL)
- Reserved Instance

Subscription - Billing

Security

Management Group, Inherited (Tree)



B, C
A, B, C

Tag = Metadata. (Key-Value)
Department
Owner.

Azure Policy → 規則

[Check
" & Enforce

10P → 1S
x3 ⇒ 4S ⇒ 4

Definition [Policy [Built-In
Custom]] JSOIN
Initiative - Policy's Folder. Import

↳ Initiative — Policy's Folder. ^{Import}

Assignment —
└─ IUG
└─ Sub
└─ RG.

Role based Access Control (RBAC)

Role = 1 or n Permission

JSON —
└─ Action
└─ Not Action
└─ Data Action
└─ Not Data Action
└─ Assignable Scope

> v.s.?

Tools

ARM — Azure Resource Manager — Management Layer.
└─ Resource Group.
└─ Template.

template.
Validation (Azure Policy)

Azure Portal - Azure Cloud Shell - Container.

Azure PowerShell → PowerShell's Module

Cross Platform. (PowerShell Core)

Cmdlet → V. - n.

New - AZVM

命令式 Script

Azure CLI

Shell Script (Bash)

Installer

AZ ^{n.} group ^{v.} subgroup action

AZ vm create

disk
↓
sub group

声明式 Script (IaC)



ARM Template - JSON

Azure Bicep - Bicep

Parameter → Deploy & Sub

Variable

Resources

Function

Output

Virtual Network (VNET) (SDN) - Addr Space (CIDR)

Independent

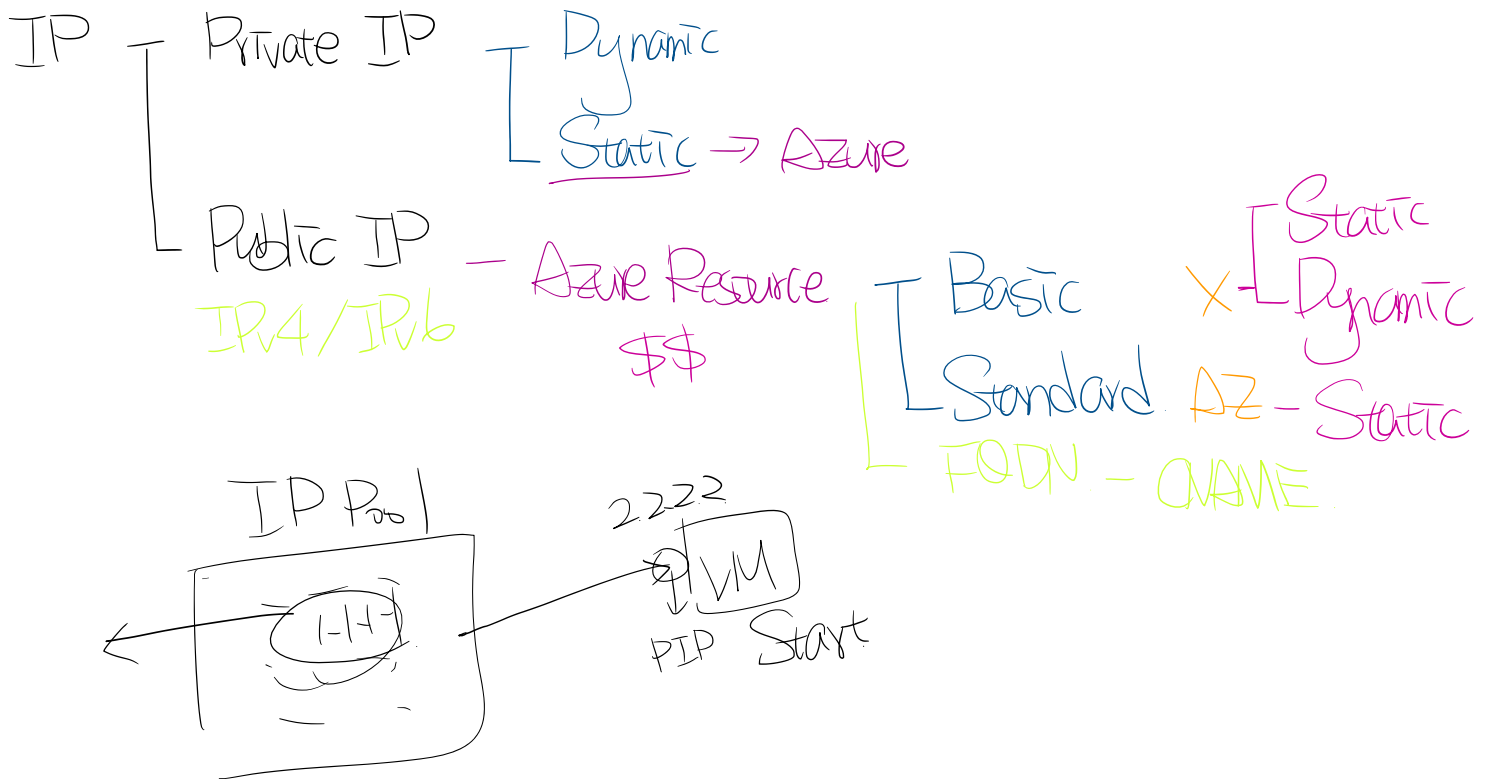
Subnet x n (Reserved IP)

10.10.0.0/16

10.11.0.0/24

10.10.1.0/24 $\Rightarrow 256 - 5 = 251$

10.10.2.0/24 $\Rightarrow 32 - 5 = 27$



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

InBound

OutBound

Rules - Priority

Stateless

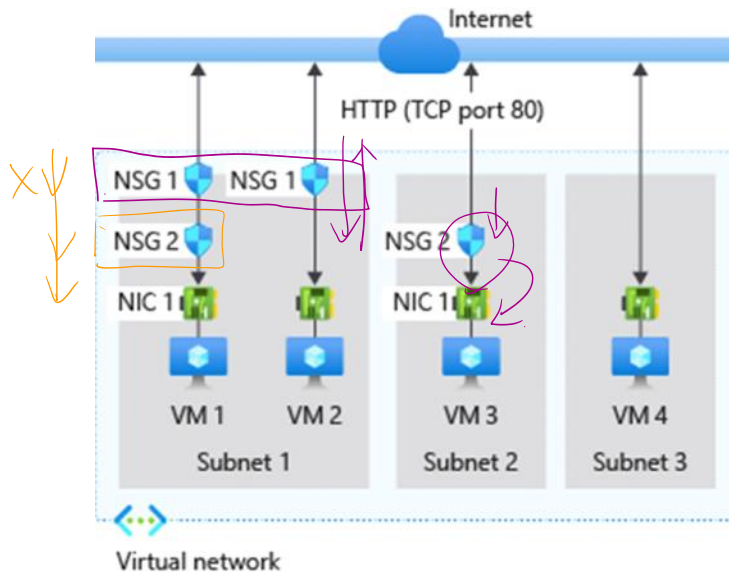
Free

Associate

Subnet

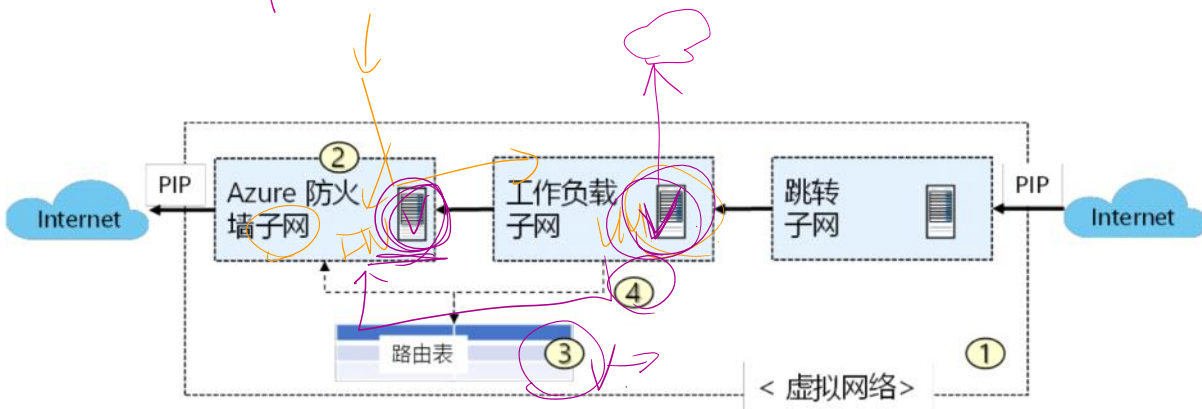
Associate (VM)

Appliance (VM)



Azure Firewall Layer 7 Stateful Paas

- HA
- Scale
- NAT
- Network
- Application



Route System Route ← Azure Managed

menu.
 L system menu. - Azure managed
 L User Define Route (UDR)
 L Route Table (Resource)
 L Route x n
 L Associate - Subnet x n

Azure DNS (PaaS DNS Server)

L (Public) DNS Zone
 L Child Zone - RBAC
 L Private DNS Zone = Any Name
 L link vnet 1:n
☒ Auto Registration (Discovery)

Inter-site Connectivity

VNET $\leftrightarrow$ VNET

VNET $\leftrightarrow$ Other - On-Prem

Other Cloud

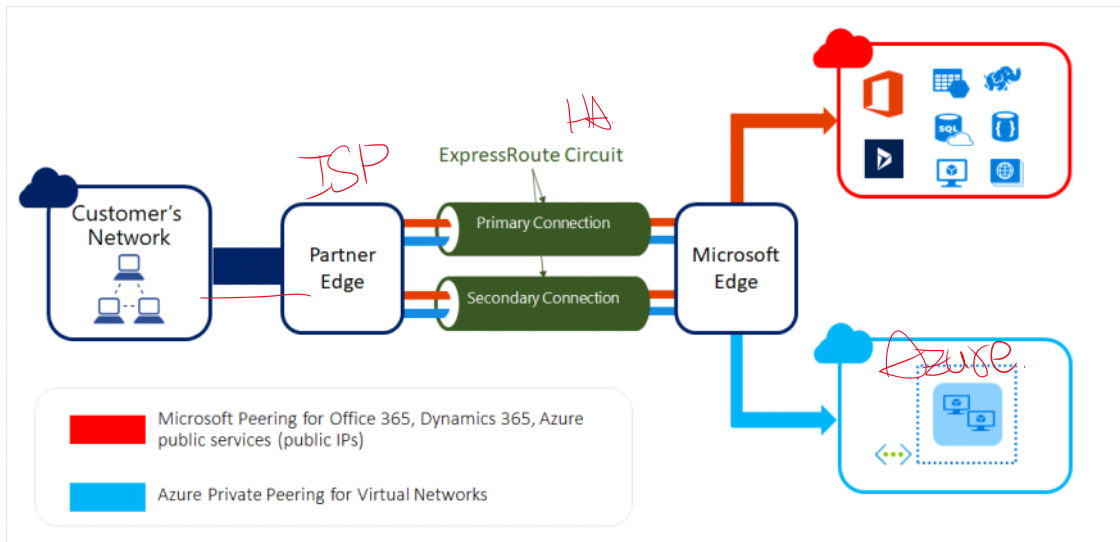
(VPN)
 Peering - 同 Region
 跨 Region
 跨 Sub

Azure

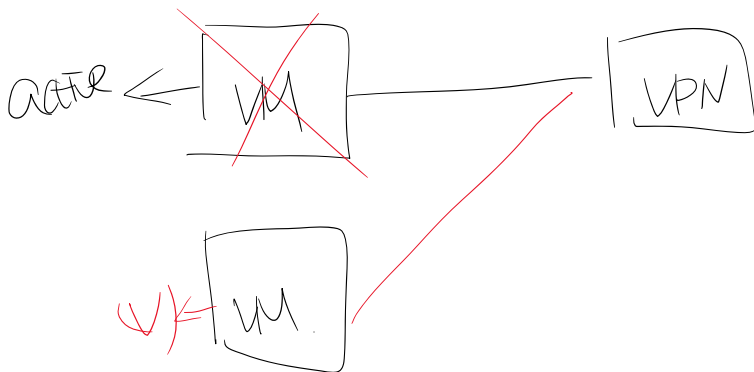
Virtual Network Gateway

PaaS - HA
Scale - Tier

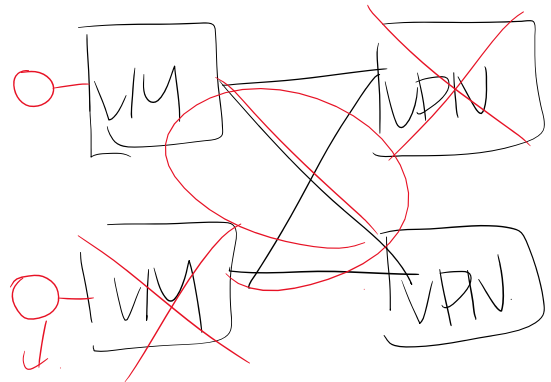
VPN - Point 2 Site
Site 2 Site
ExpressRoute



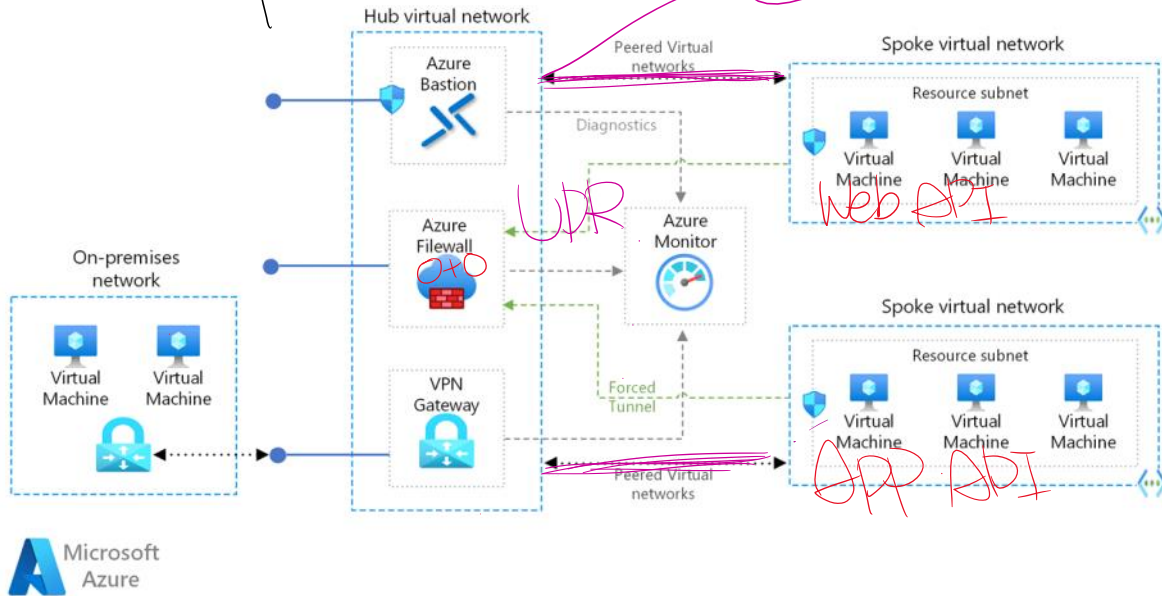
Active - Standby



Active - Active

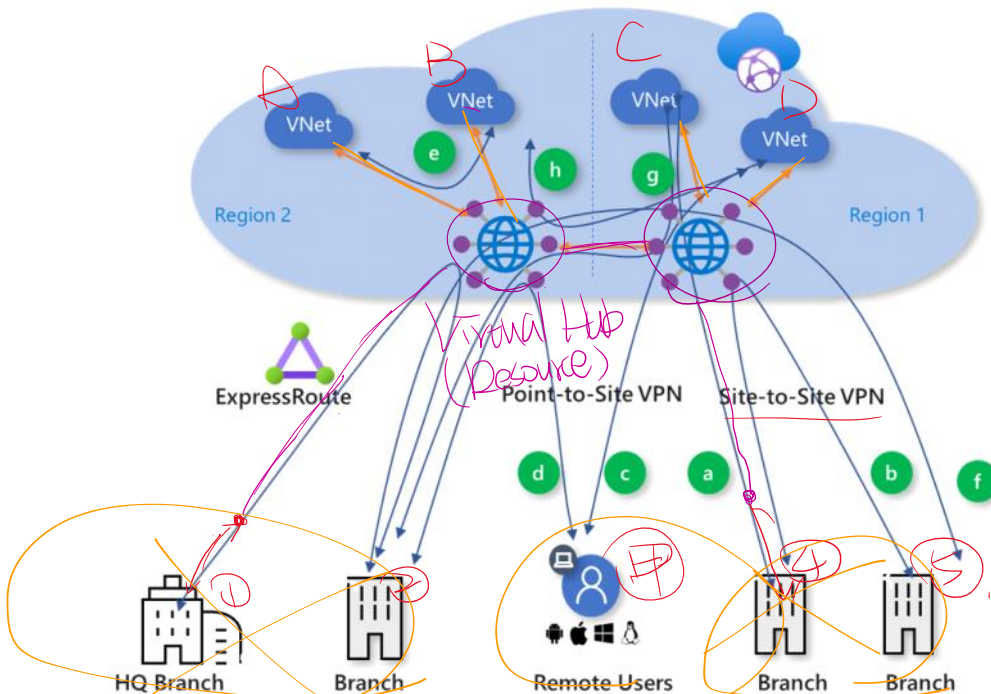


Hub-Spoke Model



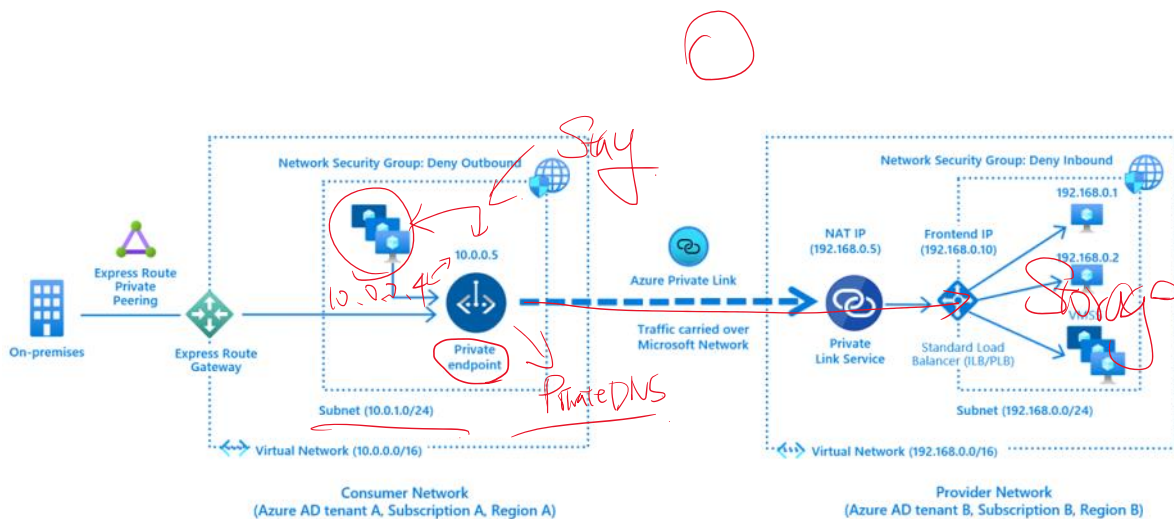
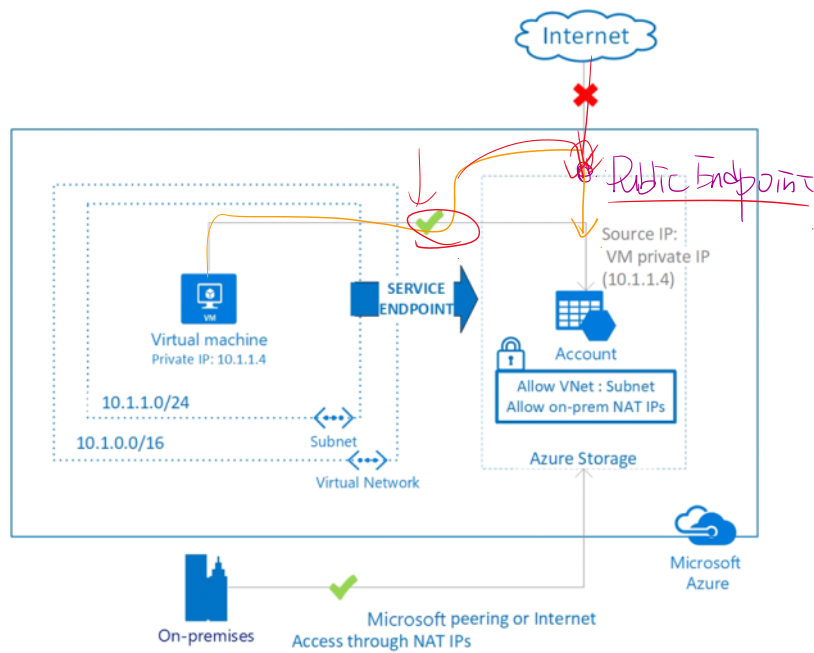
Virtual-WAN

based on Hub-Spoke model

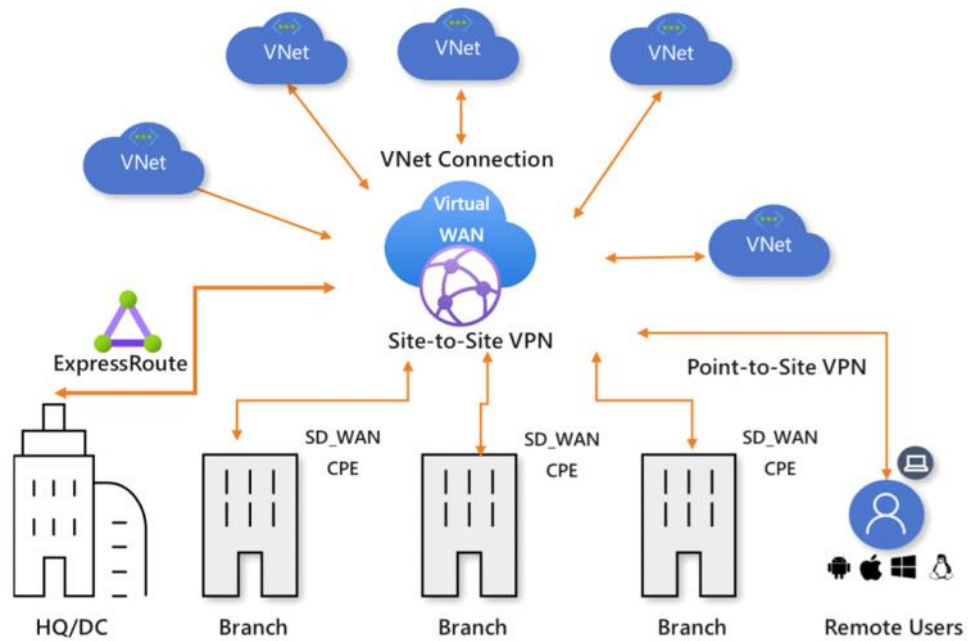


Service Endpoint

Private Endpoint / Link



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端场的交付。	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器终结点的请求。	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
区域	是		是	
全球		是	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	



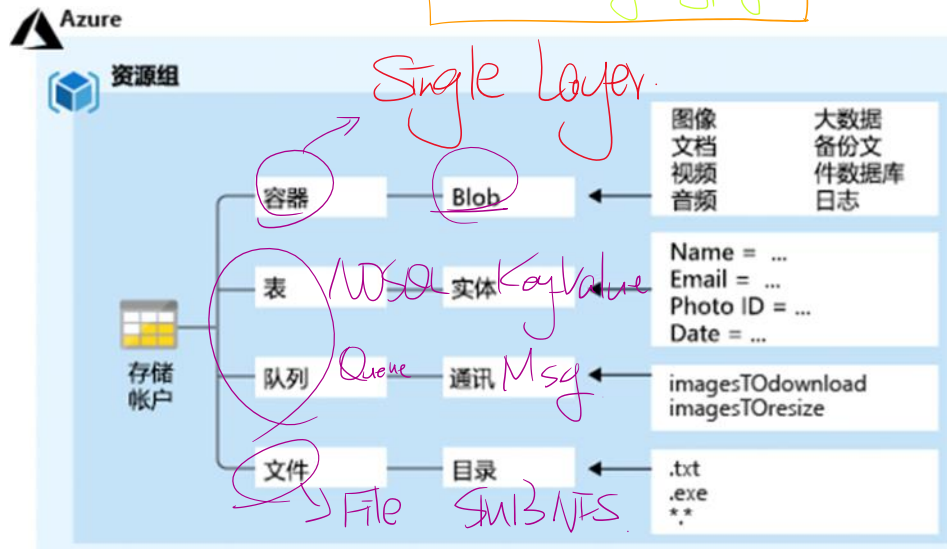
Storage

Images

img1.png

Blob Name

2023/img2.jpg



Redundancy

3 ~ 6 Gigs

⚠ Datacenter Cooling Event - Southeast Asia - Extended Mitigation

Impact Statement:

Starting around 20:19 UTC on 7 February 2023, a utility power surge in the Southeast Asia region tripped a subset of cooling units offline in one of the Availability Zones. While working to restore the cooling units, temperatures in the datacenter increased and we have proactively powered down a small subset of compute and storage 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 – 01:00 UTC

We are continuing to focus our efforts on mitigation for services which were impacted due to this incident. The core storage and compute services restoration have been completed successfully.

We have several other key services fully recovered and for some of which we are still working on post recovery checks. We are closely monitoring the datacenter metrics for storage and compute resources which continue to show healthy thresholds.

We will continue to provide updates as we have further progress towards service restoration. We will share our next update in 2 hours or as events warrant.

This message was last updated at 01:04 UTC on 09 February 2023

2021 Millions of websites offline after fire at French cloud services firm

By Mathieu Rosemain, Raphael Satter

3 MIN READ



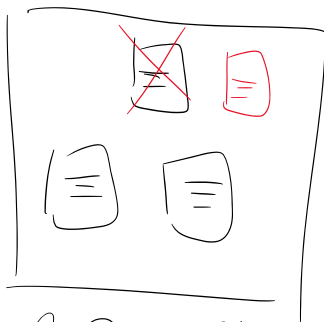
©Microsoft Corporation

Alamy

LRS (Local)

1 Region, 1 AZ 3 copies

Zone



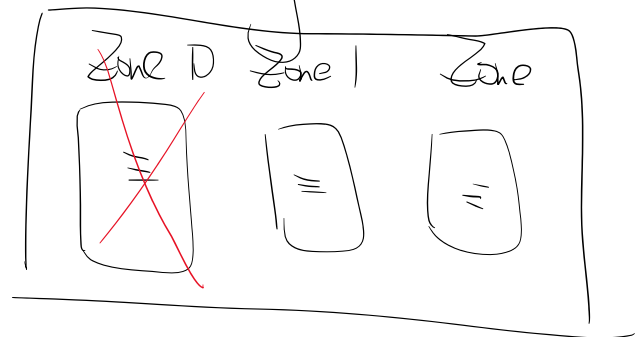
99.9...9%
a

ZRS (Zone)

1 Region, 3 AZ 3 copies

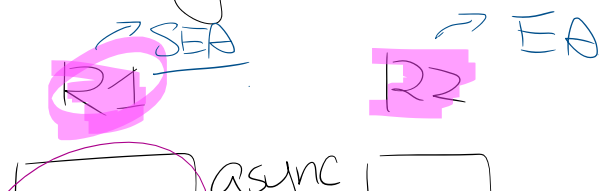
3 copies

Region



GRS (Geo)

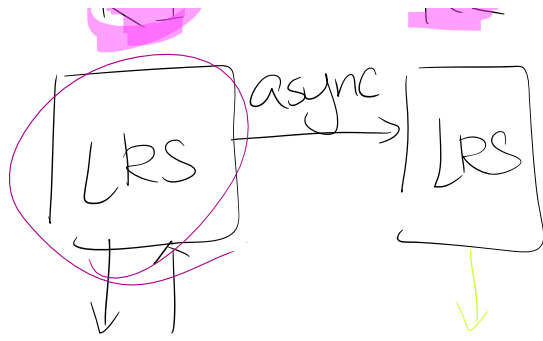
2 Region, 2 AZ 6 copies



GZRS (Geo-Zone)

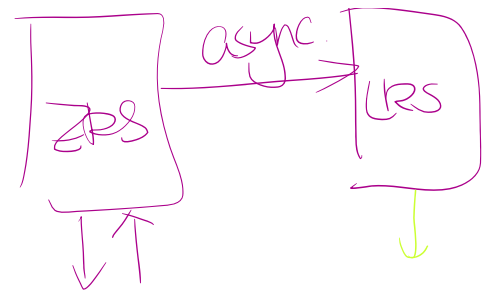
2 Region, 3+1 AZ 6 copies





RA-GRS

RA



99.999%

RA-GZRS

Pricing = Space
Transaction

Standard
Premium

Access Tier = Hot
(By Blob) Cool
Gold
Archive

Lifecycle Management
↳ Rules → JSOV
↳ Colder

Access Level { Private
Blob
Container

Access Key (Root)

Access Key (Root)

Entire ID

Shared Access Signature

BLK

<https://lab07stordog.blob.core.windows.net/images/%E7%B4%85%E3%81%AE%E8%B1%9A.jpg?sp=r&st=2023-11-22T03:19:15Z&se=2023-11-22T11:19:15Z&spr=https&sv=2022-11-02&sr=b&sig=rSSJ0Md4gwqvNXATBSt2l8a99X9dgb7eVr5iBg6NNE%3D>

Blb.

+key → Regenerate

Access Policy (By Container)

Pre Config
Part of SAS

<https://lab07stordog.blob.core.windows.net/images?si=demo1122policy&spr=https&sv=2022-11-02&sr=c&sig=ov8pZpl0v7oojh0tlEVWuIomJqyjgDl9pnaMMOqgFDo%3D>

+key

VM (IaaS)

└ Computing - Type - Series - Size.

└ Storage └ Managed Disk - Azure Resource
└ Un Managed Disk - VHD - Storage

10 VHD x 500 IOPS $\Rightarrow$ 5000 IOPS
limitation.

4 VM $\leftarrow$ [LB]

HQ?

$\leftarrow$ + VM

HQ =

Resource

Availability Set
(10 AZ)

1 ~ 3

Fault Domain - Hardware
容錯域

Availability Zone

1 ~ 20

Update Domain - Update

更新域

☑ 1 ☑ 2 ☑ 3

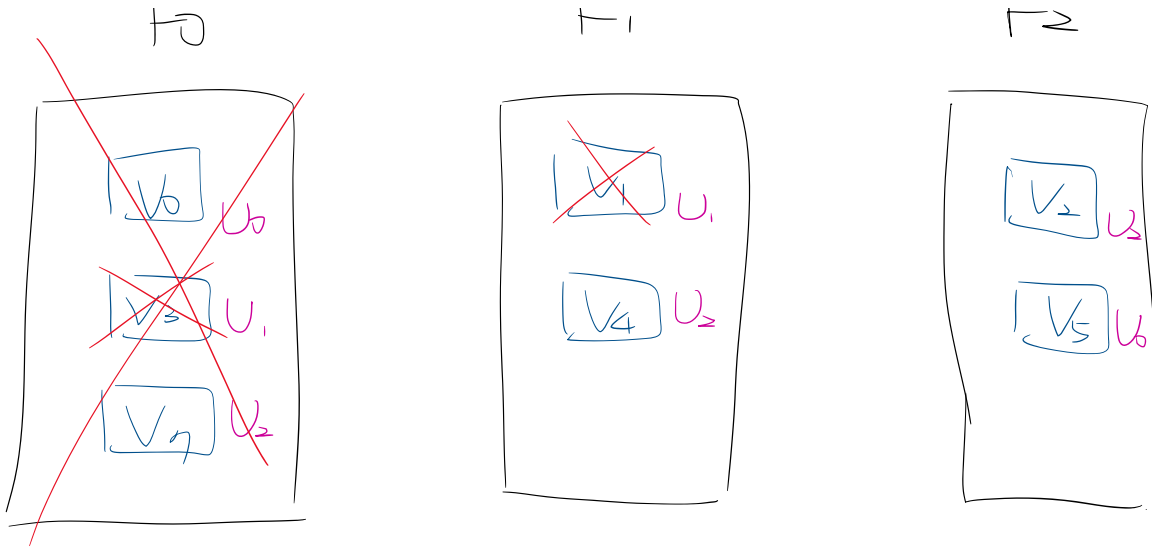
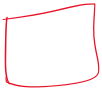
Auto
Recover

F₀

F₁

F₂

Auto
Recovery



VMSS (Scale Set)

- based on AV Set / AV Zone.
- Management
- Scale
 - Manual
 - Auto.

12/2 ($\frac{1}{16}$) $\Rightarrow ?$
 12/16 ($\frac{1}{16}$)

PaaS

Azure App Service

└ App Service Plan (VMSS)

→ Pricing
Performance
Feature

→ ...

11

↳ Azure Web App $\times n$.

120000
↳ ACU
Azure Compute
Unit

Plan A $\Rightarrow$ 10 web app

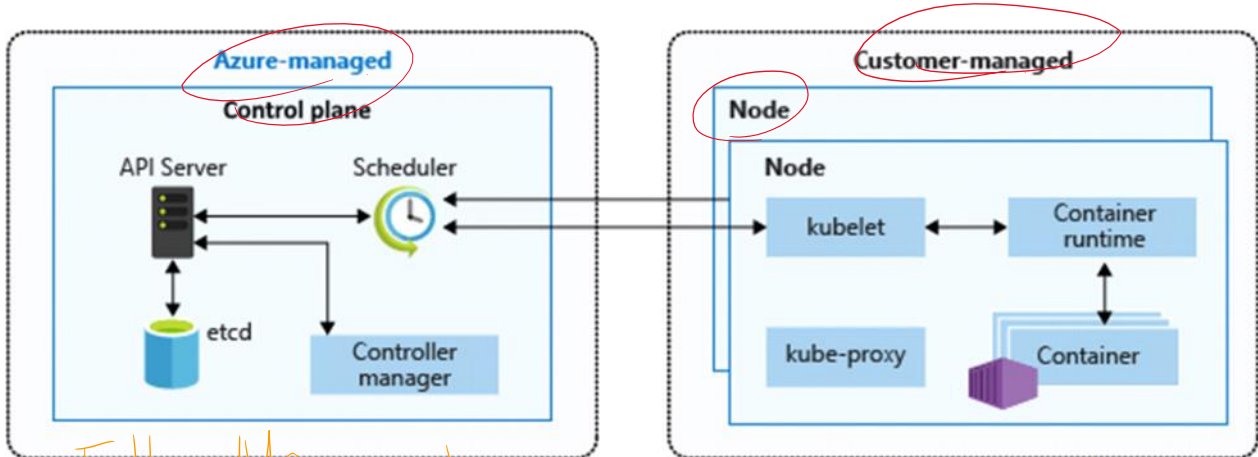
\$相等.

Plan B $\Rightarrow$ 5 web app

Container

- VM
- Web App for Container
- Azure Container Instance (PaaS) (Simplest)
- Azure K8S Service (AKS) (PaaS)
- Azure Container App (KaaS)

AKS $\rightarrow$ Pod = 1 ~ N Container.



Fully Managed

Free = ~ 10\$

Node Pool x n
VMSS

Azure Container Registry (PaaS)

Docker Registry 2.0

- Public
- Private

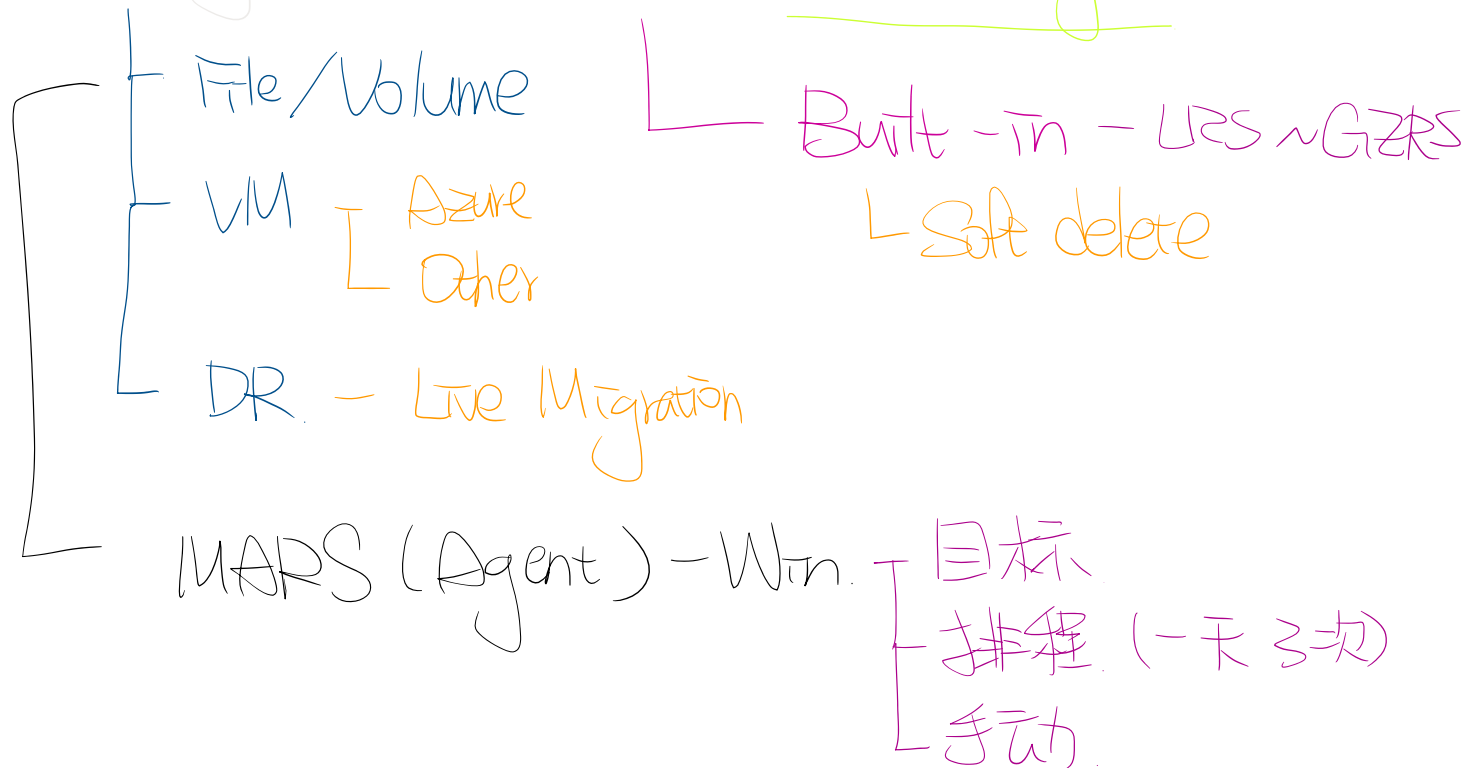
Docker Registry 2.0

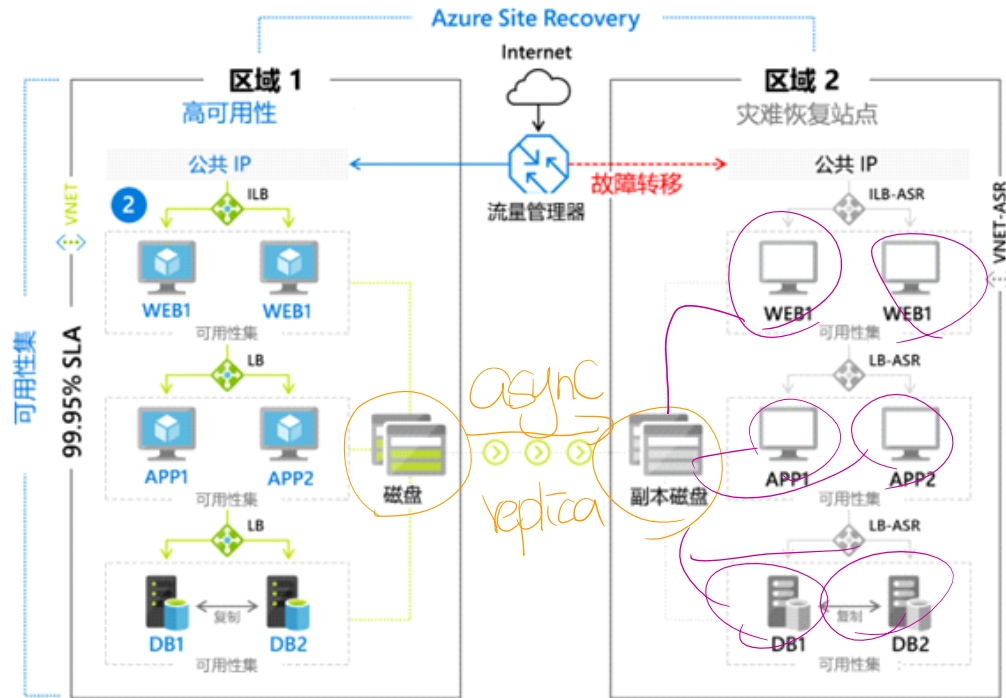
L Private

Backup

L Backup Center

Recovery Service Vault - Same Region





Test Failover
L (x)

Failover
└ Manual
└ Auto.

Monitor.

└ Azure Monitor (Service).

└ Managed Grafana
└ Prometheus

└ Log Analytics Workspace.

(Resource)

└ Built-in Storage

└ Metric } Tables
└ Log }

└ Interactive - 7 ~ 35 ~ 60 ~ ...

[Interactive - 1 ~ 35 ~ 40 ~ ...
[Executive - 10 yr.

Kusto Query Language (KQL)

↳ SQL like logic