

Identity

Entra ID

Entra ID Connect

Password Hash
Pass Through.

On-Prem

Azure

ADDS

sync

Entra ID (AAD)

LDAP

HTTP/S - OAuth

NTLM

x OU

OpenID

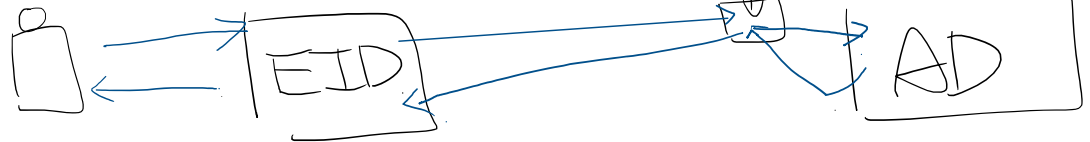
Kerberos

x GPO

WS Fed

SSPR

- User / Group
- Azure
- Prove
- Reset



Hybrid

On-Prem

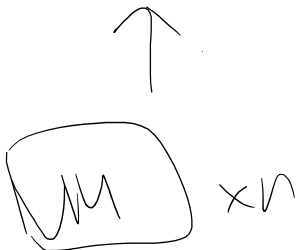
Azure

ADDS

sync

Entra ID

Entra ID DS



Entra ID

(Device)

Entra ID license

Entra ID (Device)

Entra ID license

Join (Org)

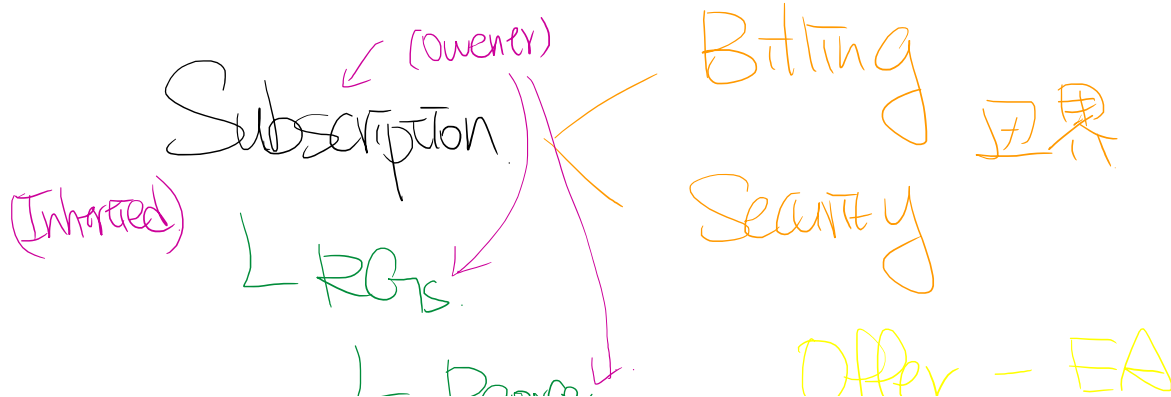
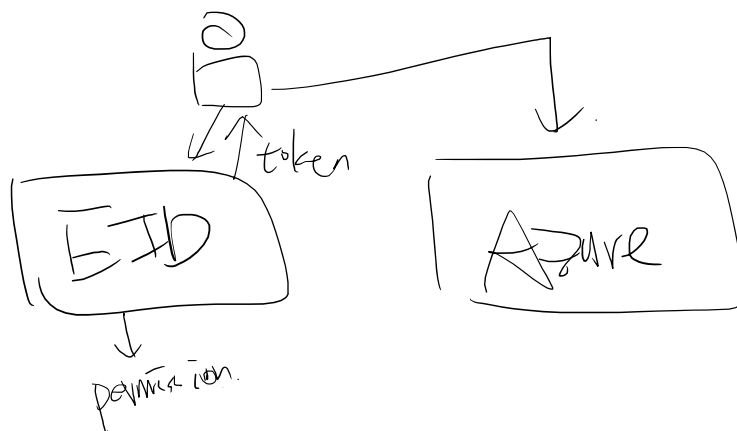
Register (BToD)

Hybrid Join (Entra + AD)

Entra ID Global Administrator

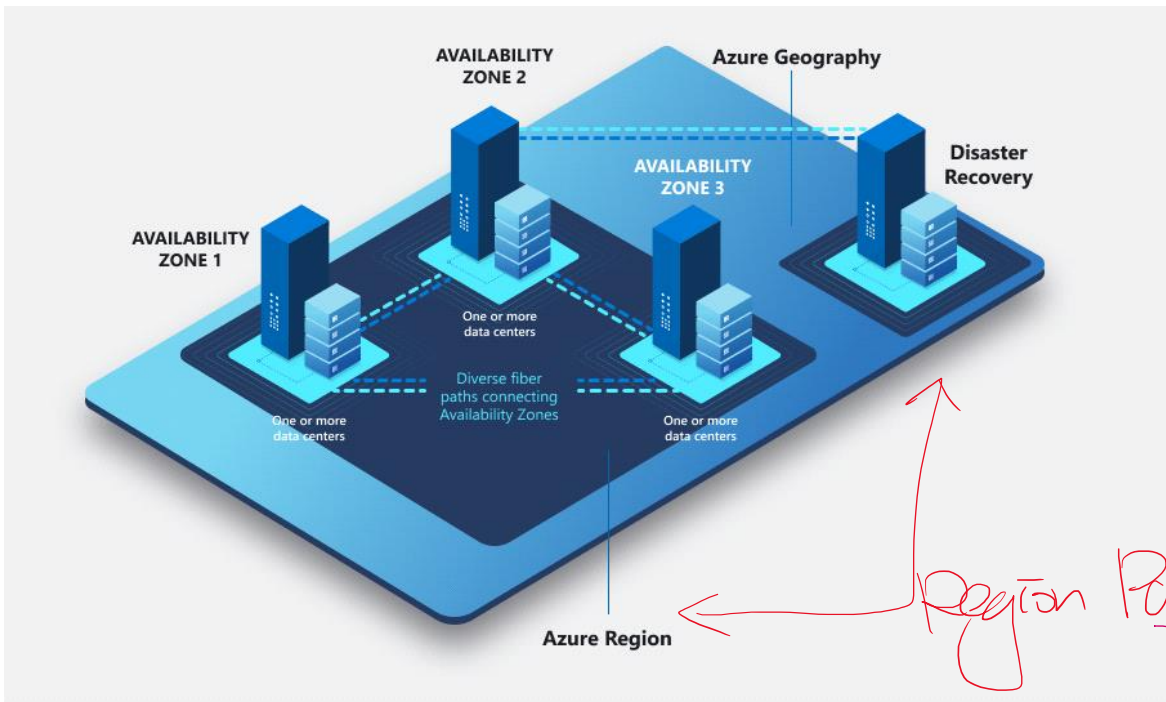
User ..

Azure Sub Global Administrator (X)



Resources
Offer - EA
CSP
PATG
Free trial.
Region 1 = Data Center
3x AZ
EIAE
Pwr, Cooling, Core Net.





- FI (latency) (RTT)
 - Geo
 - Pricing

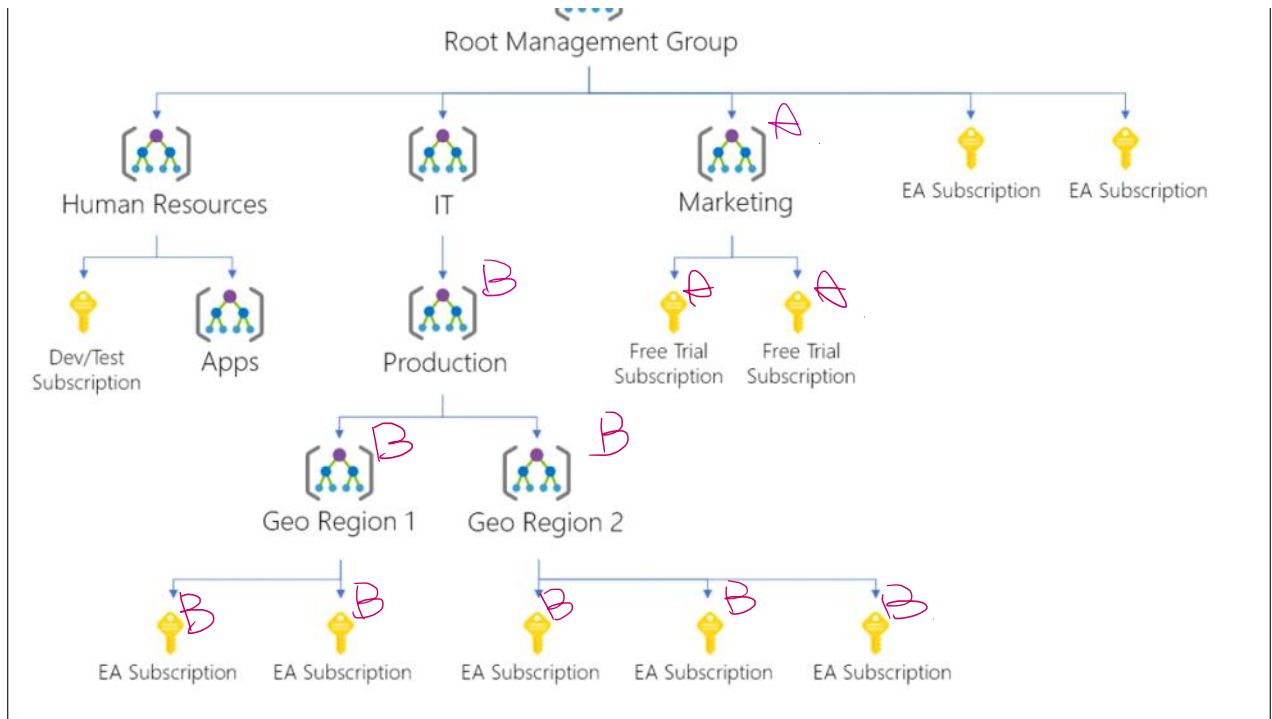
Storage - GPS
 EA - SEA
 EJP - WJP
 SEA - EQ

Management Group

→ P/S Sub

↳ Security, Billing





Cost Management

Resource vs Service
 ↓ Create ↓ Use

Tag = Metadata (key-value)

Cost Center =

Owner =

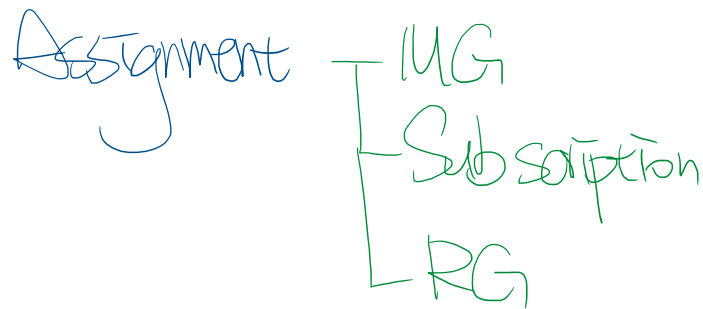
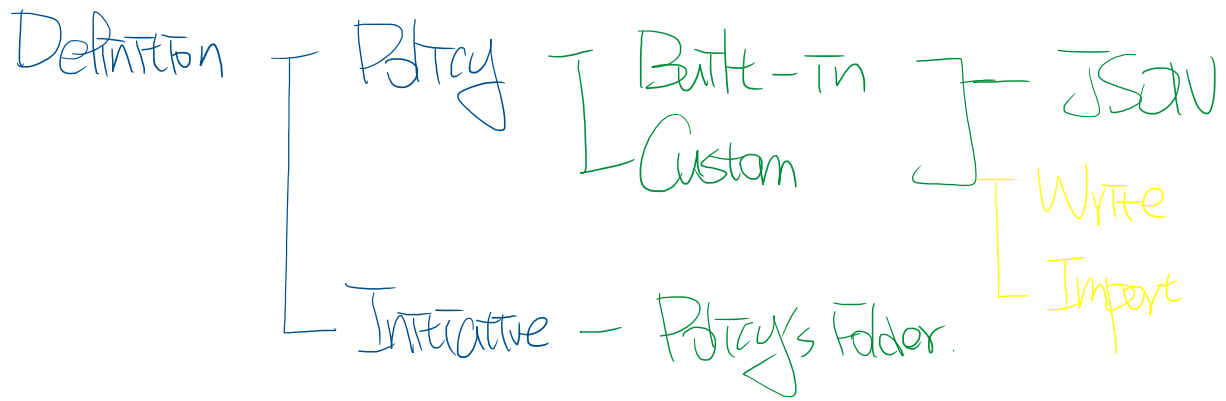
Azure Policy → Rules

- └ Check
- └ Check & enforcement

Initiative ←

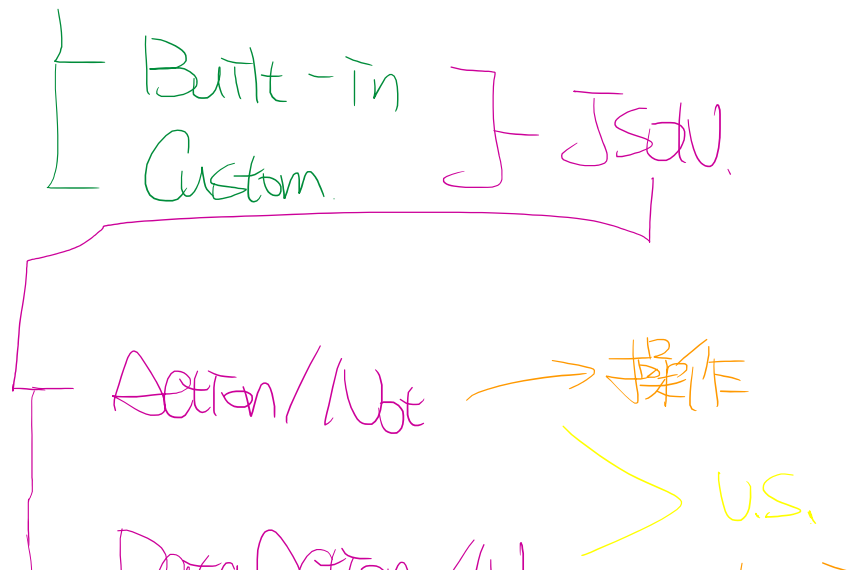
65 Policy → 1 Sub
 ↳ x\$

1x\$ ⇒ 5
 5x\$ ⇒ 25
 ↳ 5Sub



RBAC (Role based Access Control)

Role = 1 ~ n Permission



{ DataAction / Not → U.S. 数据
 Assignable Scope (Must)
 ↳ 能用在哪儿?
 MG, Sub, RG

Administration

ARM - Azure Resource Manager - Management Layer
 ↳ RG

Azure Portal - Azure Cloud Shell - Tools SDK

Azure PowerShell
 命令式
 Azure CLI
 Module, Cross Platform, Cmdlet
 Standalone, .., Bash

ARM Template - JSON - Parameter Variable
 Syntax 声明式
 Blank Gallery

Syntax 声明式

Azure Bicep - Bicep

Variable └

Resource

Function └ Pre Define

Output └ User Define

Config
Galaxy
Export

Networking

Virtual Network (VNET) - ^{SDN}Addr Space - ^{CIDR}私立

10.10.0.0/16

192.168.100.0/24

Subnet

Reserve IP

Sub1 = 10.10.1.0/24 $\Rightarrow$ ~~256~~

$\Rightarrow$ 251

Sub2 = 192.168.100.0/27 $\Rightarrow$ ~~256~~

.0 ~ .31

$\Rightarrow$ 27

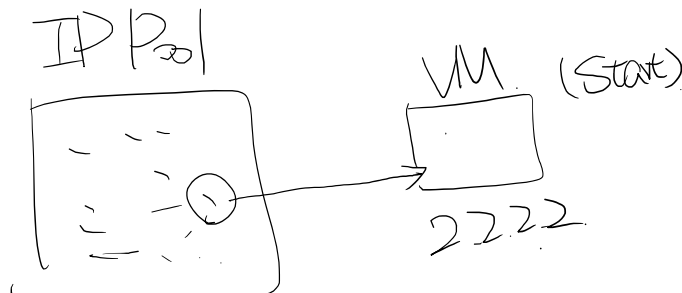
IP - Private IP - Dynamic / Static

Public IP (PIP) - ^{$\hookrightarrow$ Azure}Azure Resource

Basic X ^(IPv4 / IPv6)Static Dynamic

Standard AZ Static ..

Blitz



Network Security Group (NSG) Layer4 Stateless FW

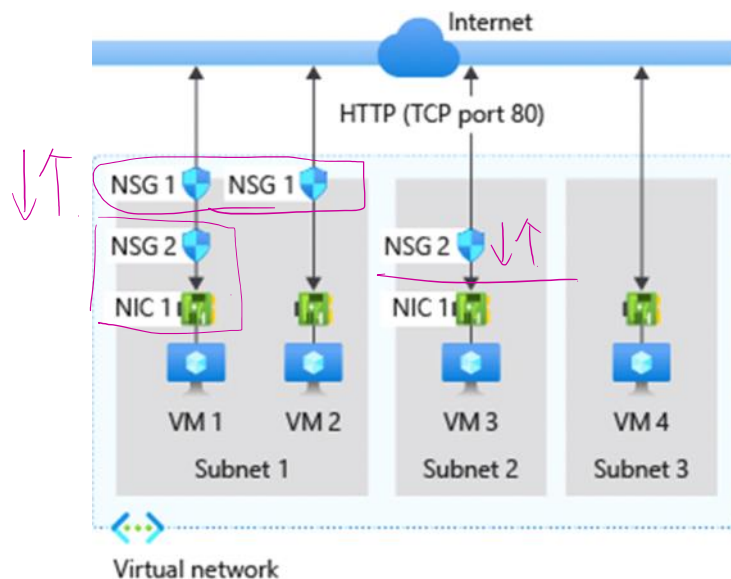
L InBand - Rule x n. - Priority (int) 100 ~ 4096
 OutBand 越小越优先

x 3389 200

v 3389 180

Default Rules $\Rightarrow$ x Edit x Delete

Association | Appliance $\leftarrow$ NSG1
 | Subnet $\leftarrow$ NSG2



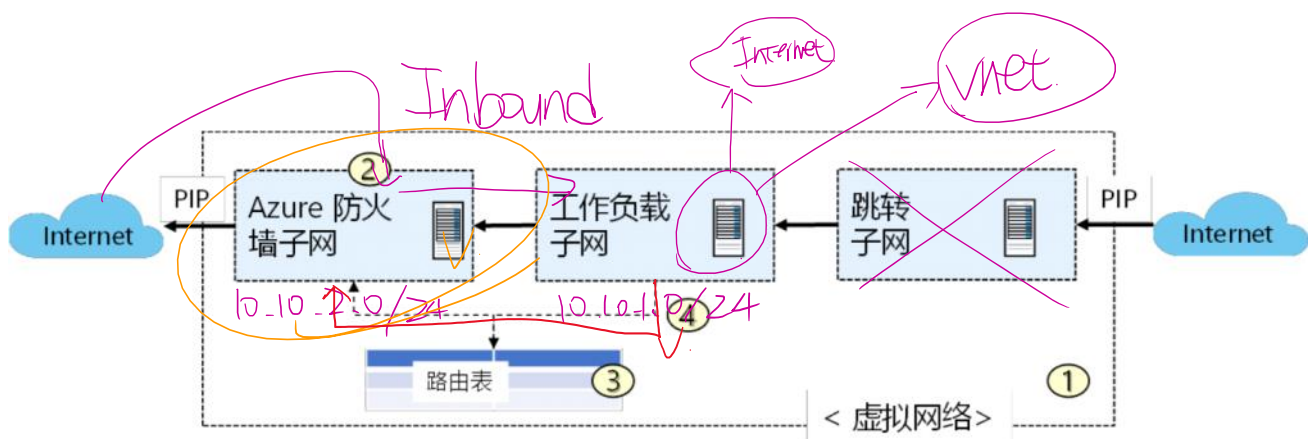
Azure Firewall

Layer7 Stateful FW

... ..

{ NAT
 { Network
 { Application

PaaS (FaaS) - (VM)
 { Dedicated Subnet

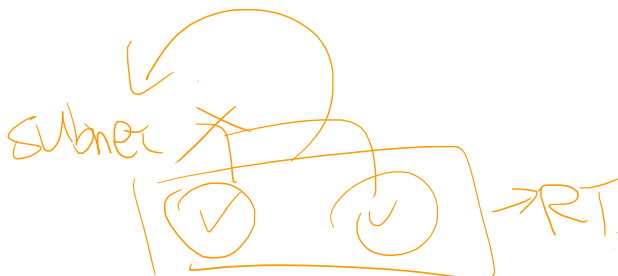


Route - System Route < Azure Managed

{ User Define Route (UDR)

{ Route Table - Route x n

{ Associate to Subnet (x n)



Azure DNS Zone (PaaS) (DNS Server)

└ (Public) DNS Zone → Internet

yu money

└ Private DNS Zone → Internal

money.local

↳ link vnet

InterSite Connectivity

VNET ↔ VNET

VNET ↔ Other

————— (VPN)
Peering (対等)

On-Prem
Other Cloud

Azure

— To Region
跨 Region
Sub

V3 ↔ V1 ↔ V2

Virtual Network Gateway (VPN Gateway)

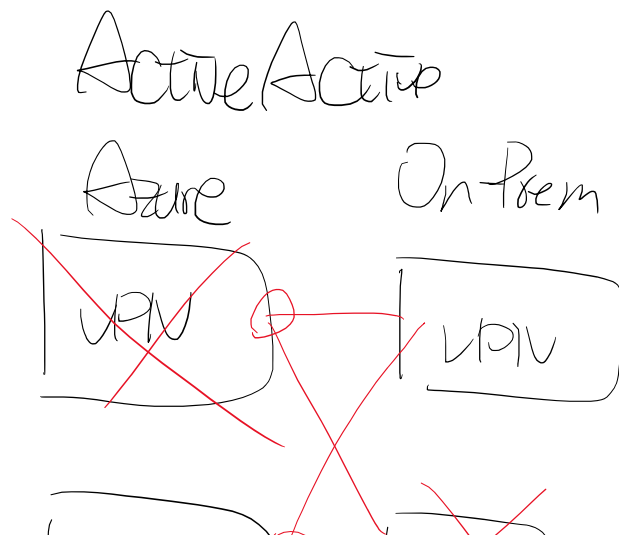
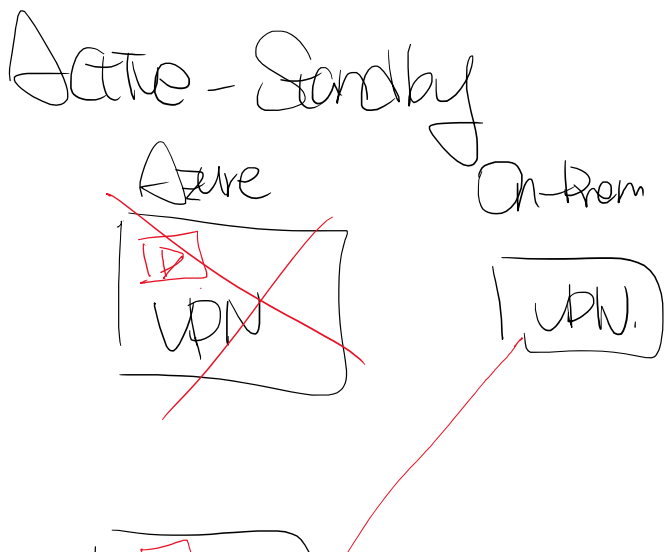
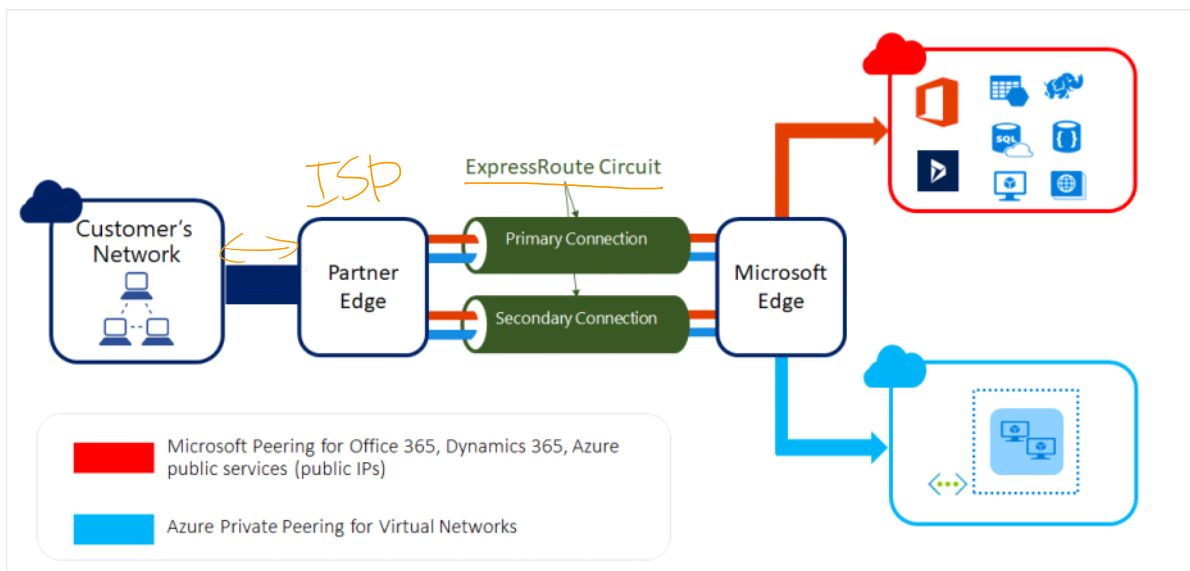
| P2S | | On-Prem | | / |

VPIN { P2S
S2S
Express Route

Resource - Pricing - SKU
(PaaS) (VMxn) - HA

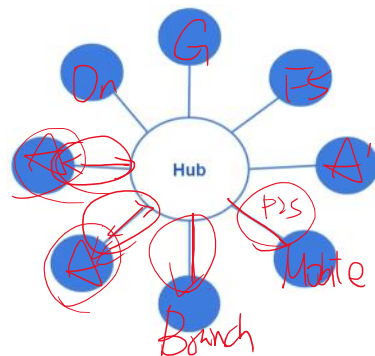
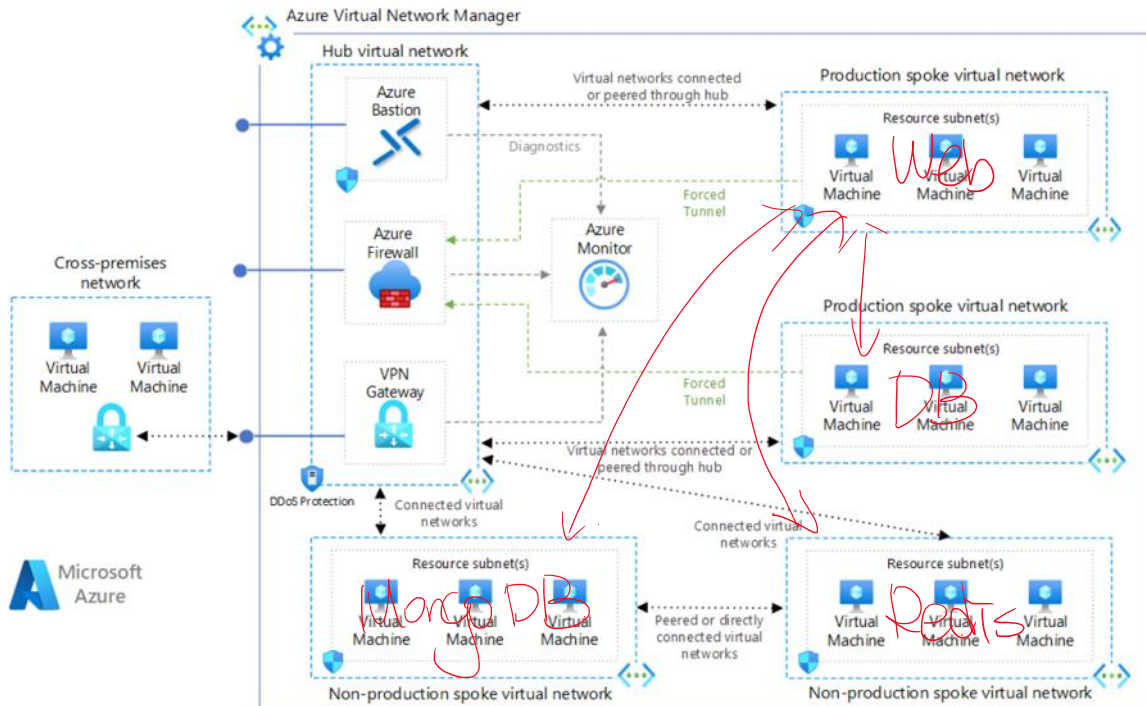
→ Gateway subnet

Active
Standby
ActiveX2

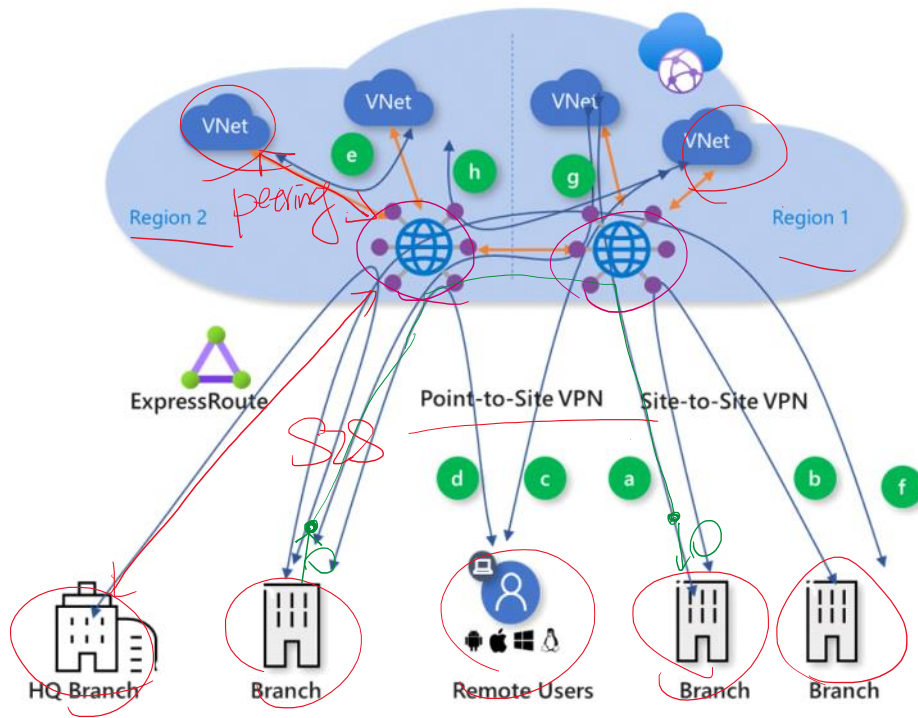


VPN

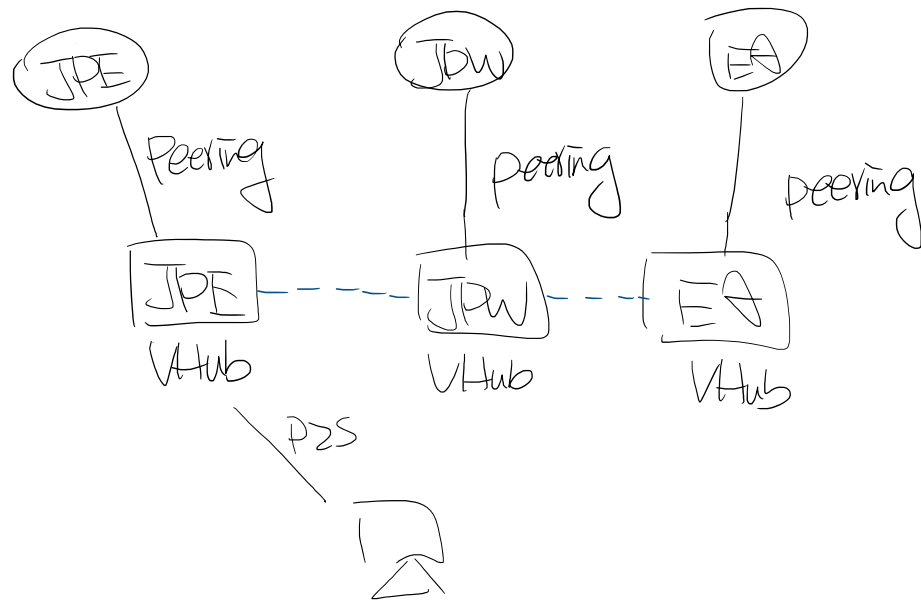
VPN



Virtual Wan.



Virtual Hub
 ↳ VNET
 ↳ Firewall
 VPN GW
 Azure Bastion

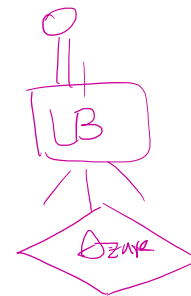


PaaS

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
区域	是	是	是	是
全局	是	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	

Domain
Path
WAF

Priority
Latency
Geo



Site Recovery

Azure Storage (IaaS)

Azure 容器: 适用于文本和二进制数据的可大规模缩放的对象存储

Azure 表: 最适合存储结构化非关系型数据

Azure 队列: 用于在应用程序组件之间进行可靠消息传送的消息传送存储

Azure 文件存储: 适用于云或本地部署的托管文件共享

资源组

存储帐户

容器 → Blob

表 → 实体

队列 → 通讯

文件 → 目录

图像、文档、视频、音频、大数据、备份文件、数据库、日志

Name = ...
Email = ...
Photo ID = ...
Date = ...

imagesToDownload
imagesToResize

.txt
.exe
...

HTTP, FTP, SMB, NFS

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。

Service

Latency, IOPS

Technology / Cloud

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.

⚠ Datacenter Cooling Event - Southeast Asia

Issue Summary: Starting around 20:19 UTC on 7 February 2023, a utility power surge in the Southeast Asia region tripped all of the chiller units for one datacenter offline. While working to restore the chiller units, temperatures in the datacenter increase so we are proactively powering down compute, storage and networking resources to avoid damage to hardware. All impacted infrastructure is in the same datacenter, within one of the region's three Availability Zones (AZs). Downstream services that have been identified as impacted include Azure App Services, Azure Backup, Azure Cosmos DB, Azure Database for MySQL & flexible server, Azure Database for PostgreSQL & flexible server, Azure Log Analytics, Azure Red Hat OpenShift, Azure Search, Azure SQL Database, and Azure Virtual Machines (VMs).

This message was last updated at 02:25 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

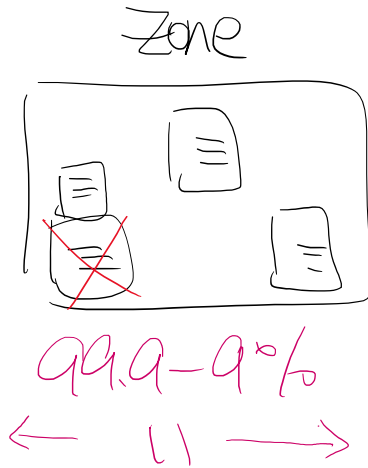
Azure

Redundancy

4+2 机制 $\Rightarrow$ 3 ~ 6 cpy's

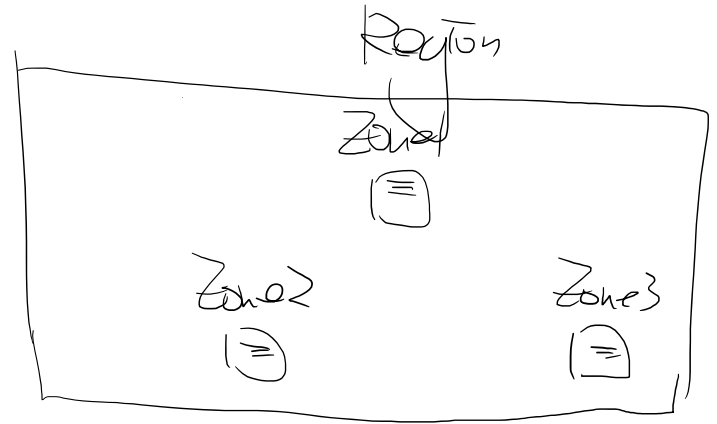
LRS (Local)

1 Region, 1 AZ 3 copys



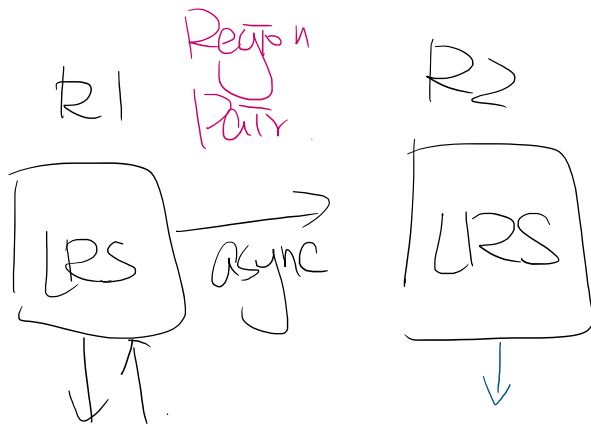
3 copys ZRS (Zone)

1 Region, 3 AZ



GRS (Geo)

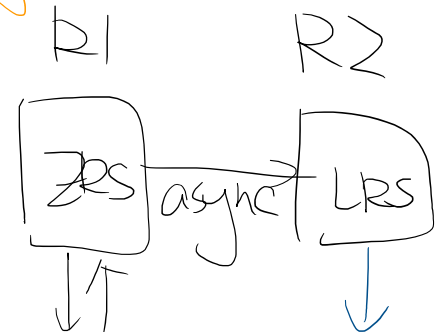
2 Region $\Rightarrow$ 2 LRS 6 copys



RA-GRS

GZRS

2 Region $\Rightarrow$ ZRS + LRS 6 copys



RA-GZRS

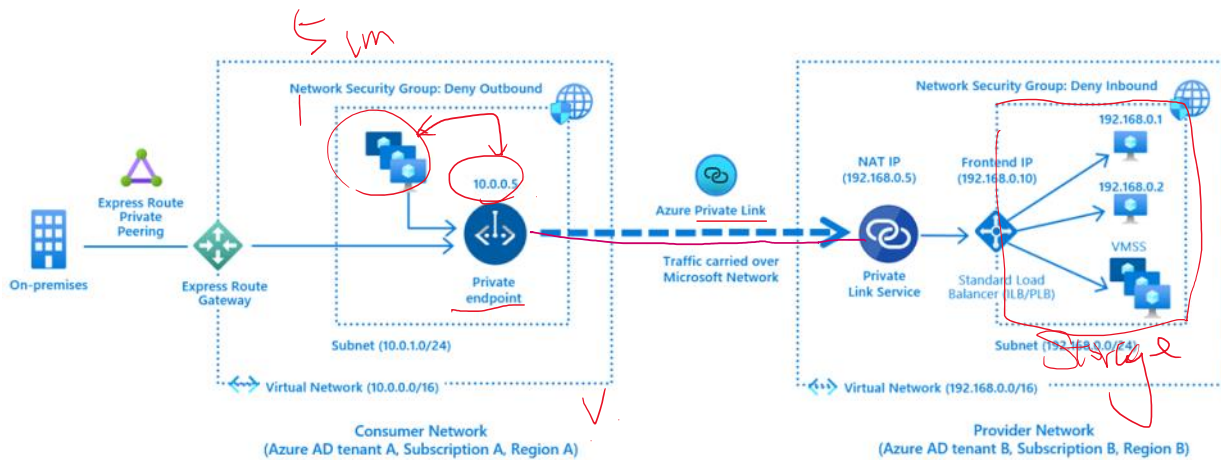
Strong Space Transaction

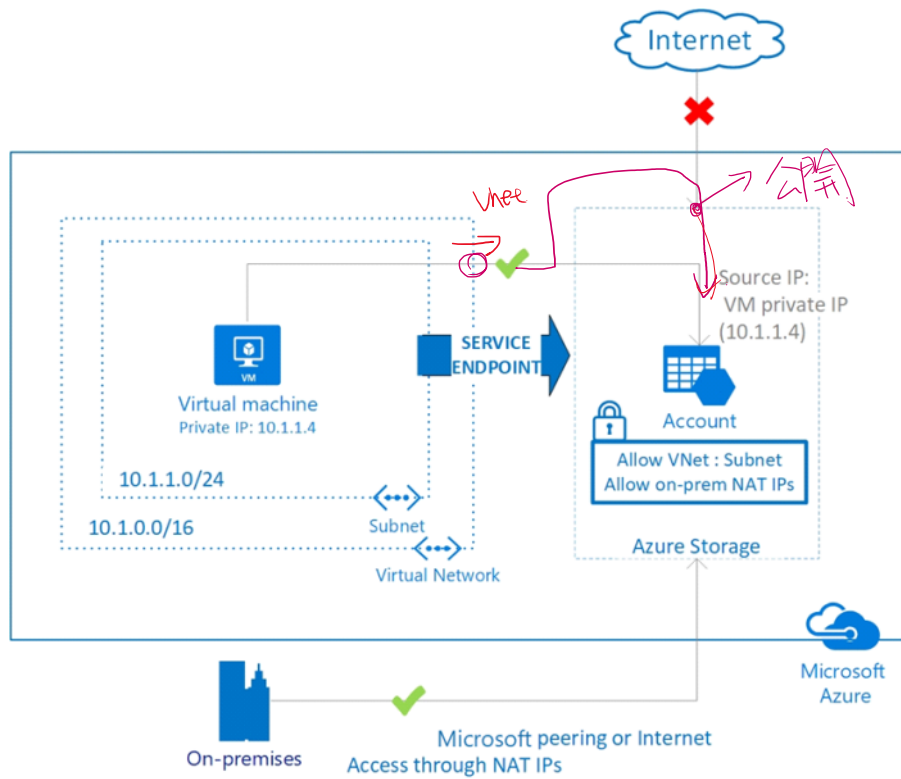
Access Tier - Hot
Cool
Cold
Archive

By Blob

Lifecycle Management
↳ Rule → Cooler

18





Snapshot vs Backup

Difference

images/ img1.jpg

[2024/img1.jpg]

Blob Name

Shared Access Signature

↳ Target + Account

✓
 ↳ Target

- Account
- Service
- Container
- Blob

Time - Start / End

Permission

<https://demo0710stor.blob.core.windows.net/images/2024/IKEA.jpg?sp=r&st=2024-07-10T03:32:31Z&se=2024-07-10T11:32:31Z&spr=https&sv=2022-11-02&sr=b&sig=XUBf9EovlStwMOKsCRkCrBW3yVhTLOrWQnqC09YU0c4%3D>

↳ (Key 1) → Key

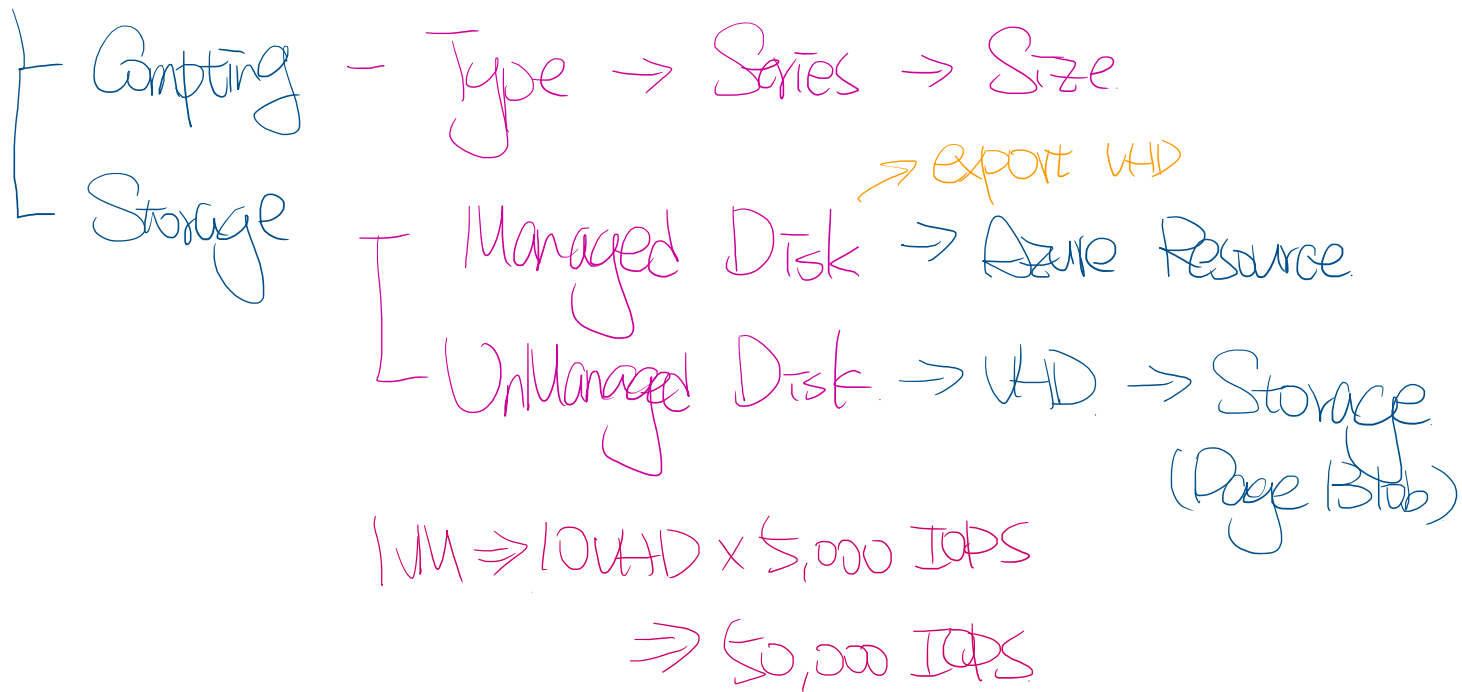
Access Policy

- Pre Config
- Part of SAS Token

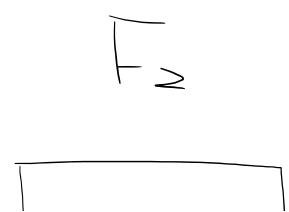
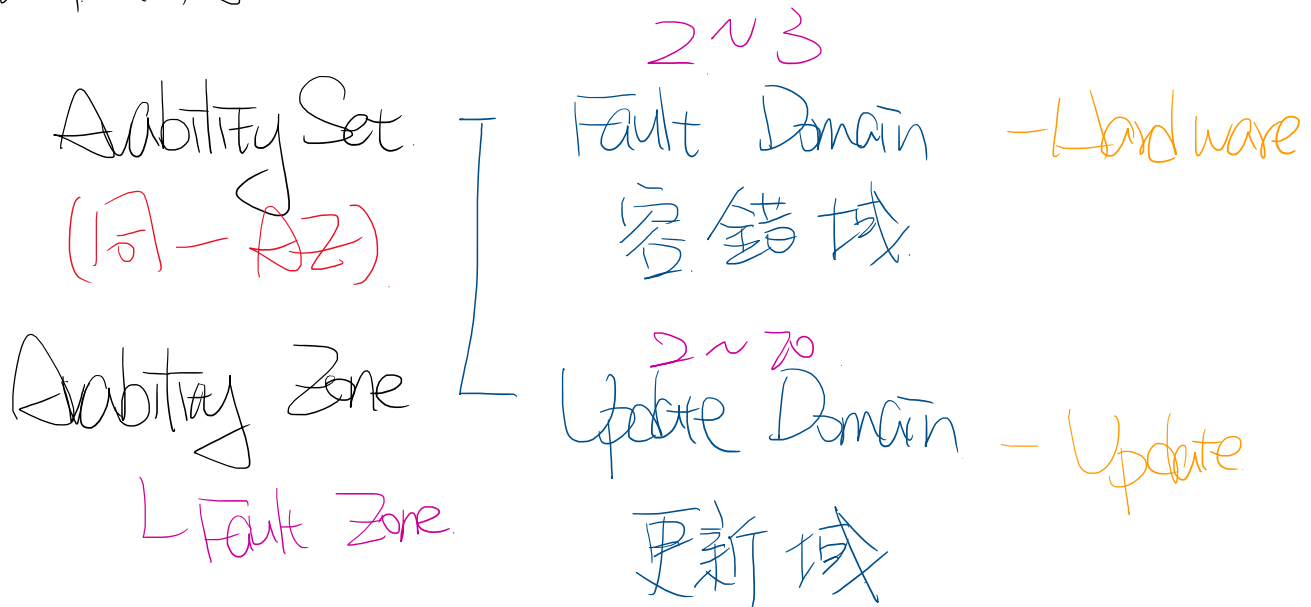
<https://demo0710stor.blob.core.windows.net/images/2024/IKEA.jpg?si=Demo0710AccessPolicy&spr=https&sv=2022-11-02&sr=b&sig=7vHaT3rxvXD23xiAzAgJBVmDe6h8pXLzicQDOo2R%2BuU%3D>

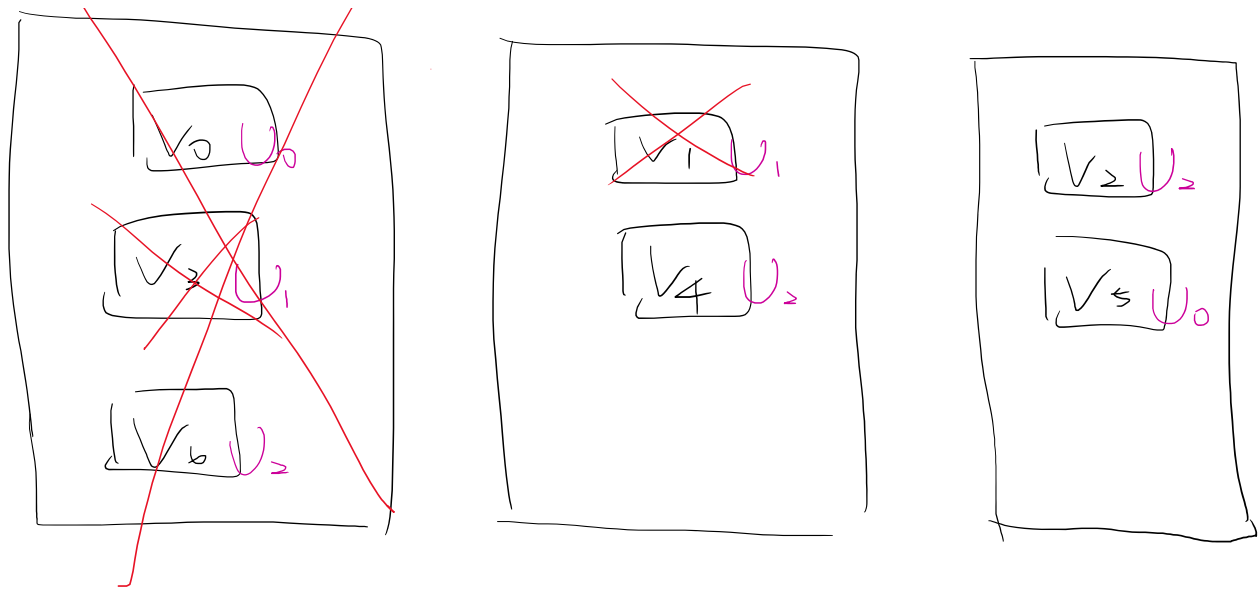
→ Key

VM (IaaS)

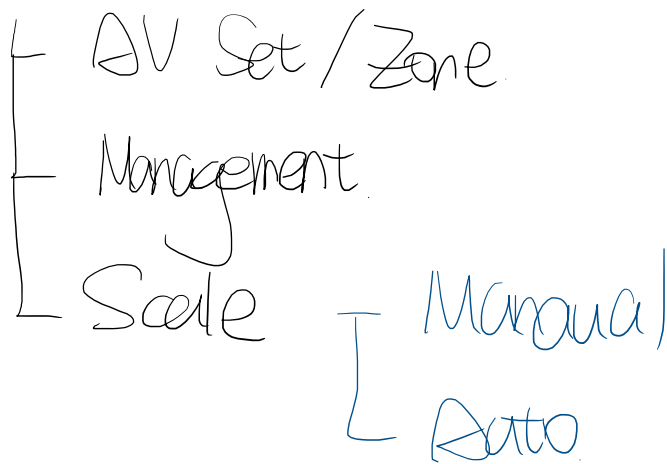


VM HA



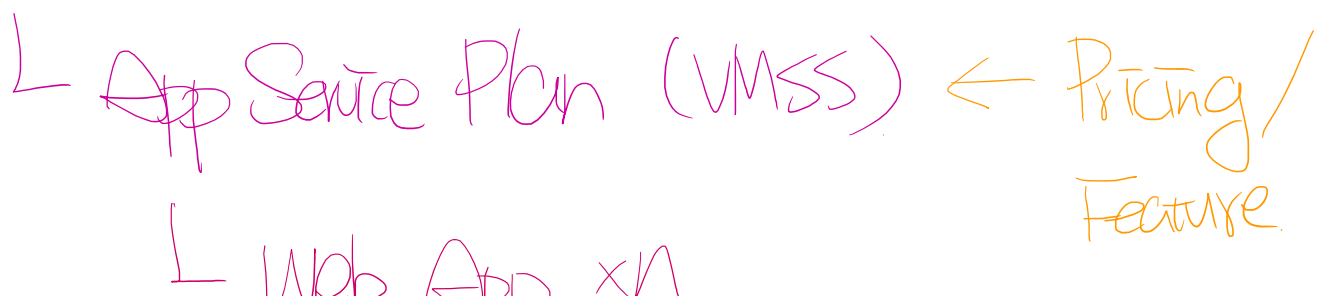


VMSS (Azure Resource) max 1,000



Paas

Azure App Service (Web Hosting)



L Web App xN.

Feature.

1 x Web $\Rightarrow$ 10 USD

10 x Web $\Rightarrow$ 10 USD

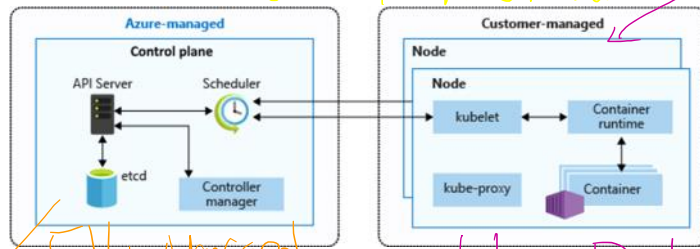
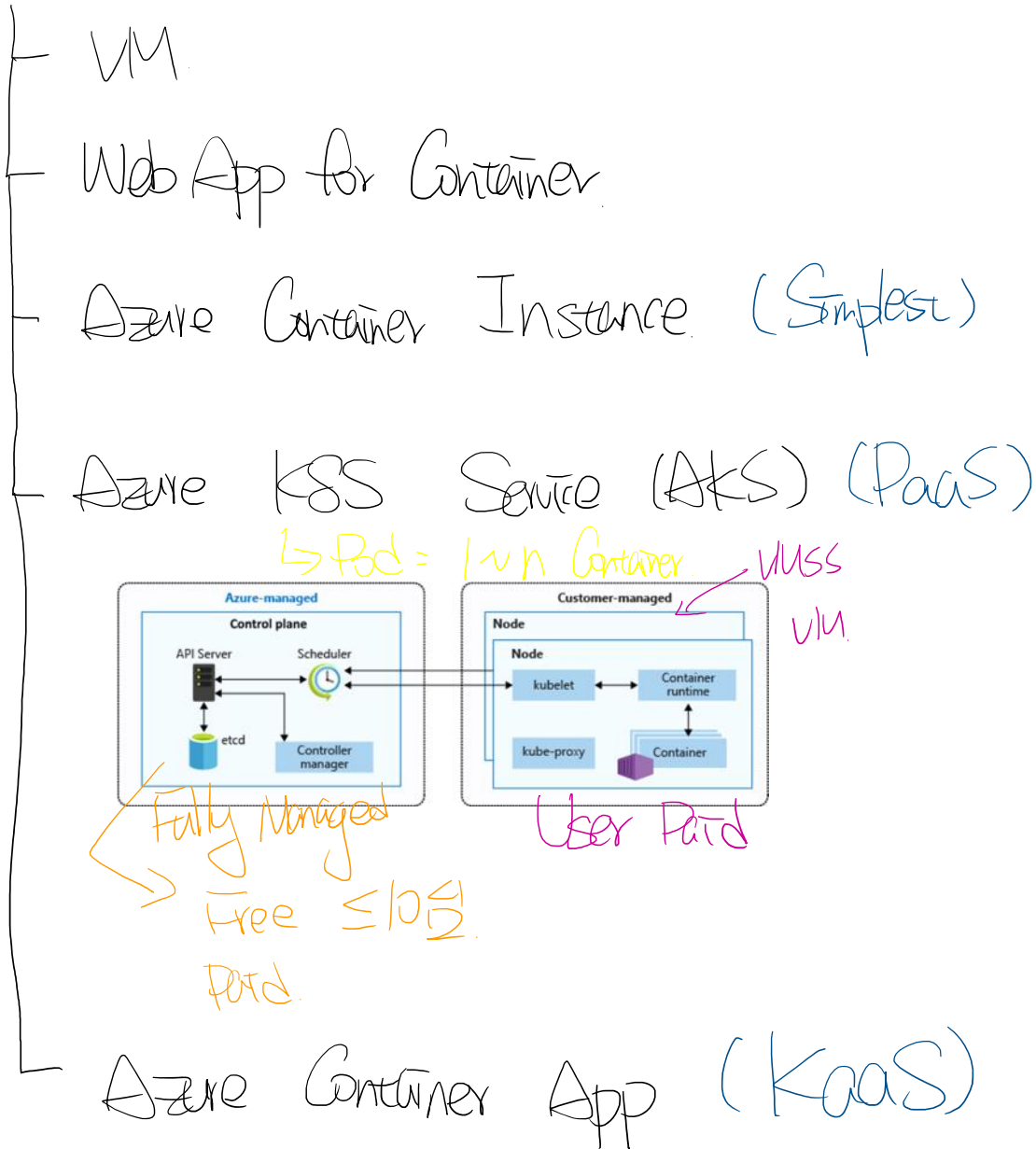
50

100

- NET, Python, PHP, Java
, Go, , JS

Docker

Container



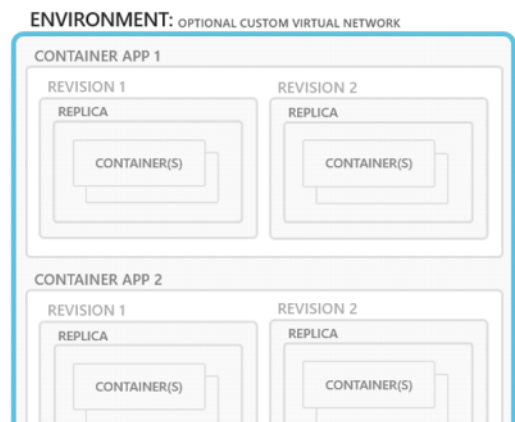
Fully Managed
 Free ≤ 10\$
 Paid

User Paid

Environment
 Container App



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

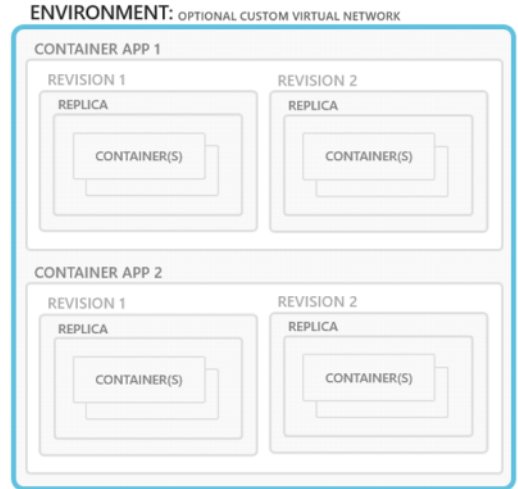


└ Environment

└ Container App.



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



Azure Container Registry
⇒ Docker Registry 2.0

└ Private
└ Public

Backup

└ Backup Center (Service)

Recovery Service Vault.

└ File / Volume - Win
└ VM - On-Prem
Azure
Other

- Built-in Storage

└ Soft-delete

MARS (Agent)

└ 自本系

└ Policy (3次/dy)

└ 手動

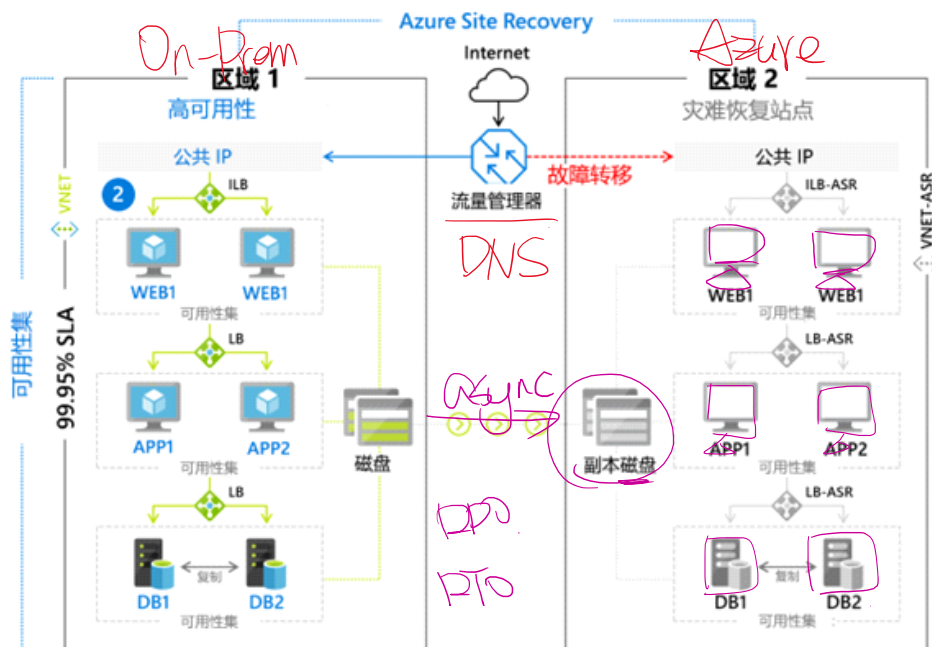
DR - Site - Live Migration

On-Prem VM

MABS (Azure Backup Server)

Disaster Recovery

Site Recovery Migration
DR



Failover
Manual
Auto

Monitor

Log Analytics Workspace

└ Built-In Storage

└ Interactive
└ Archive

└ Metric
└ Log
└ Tables



Export

Kusto Query Language (KQL)

└ SQL like logic