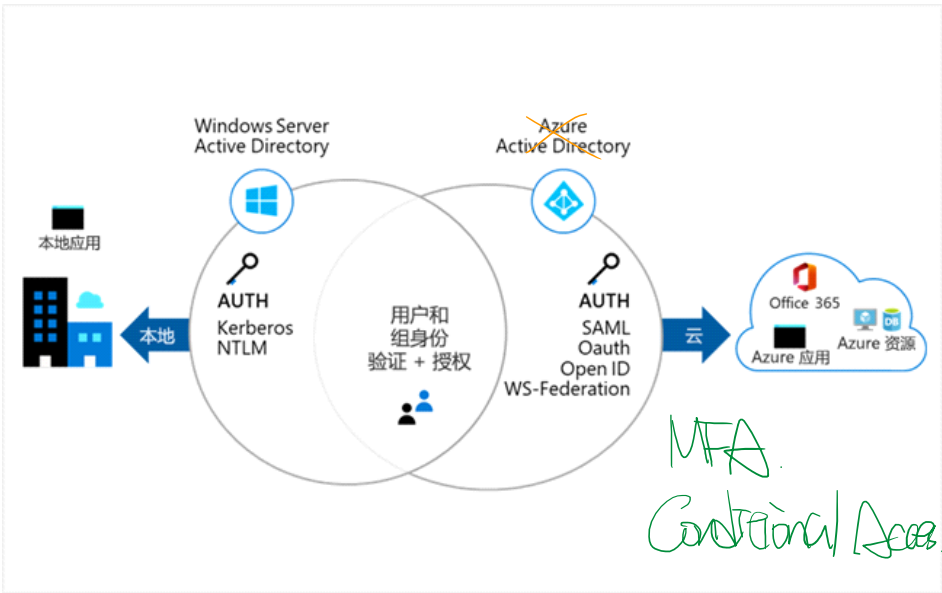
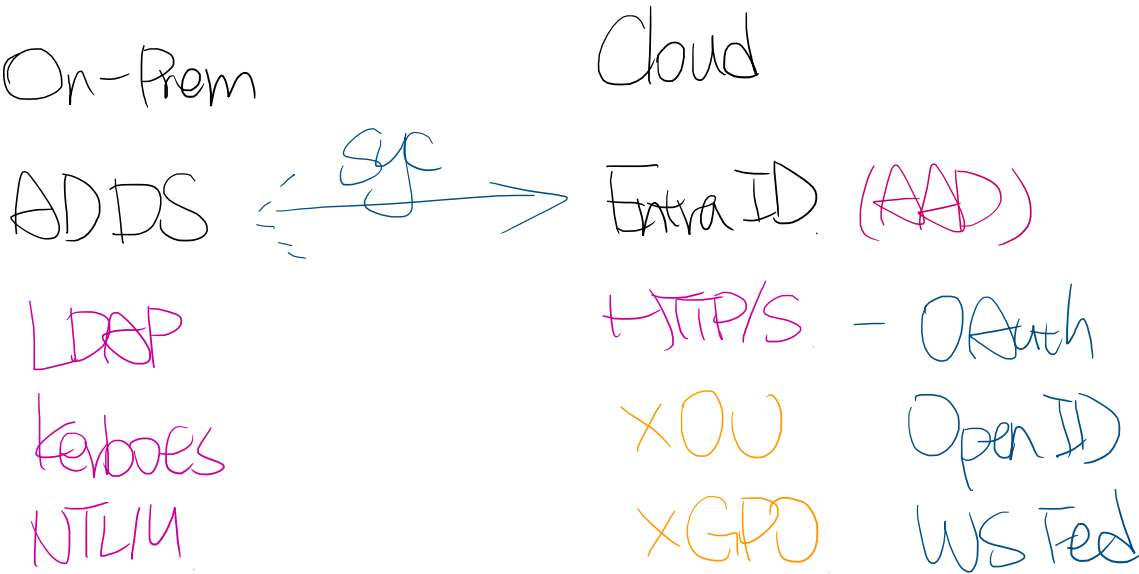


Identity



License

功能	免费	P1	P2	调控
单一登录 (无限制)	✓	✓	✓	
云和联合身份验证	✓	✓	✓	

高级组管理		✓	✓	
自助式帐户管理门户	✓	✓	✓	
多重身份验证 (MFA)	✓	✓	✓	
条件访问		✓	✓	
基于风险的条件访问 (登录风险、用户风险)			✓	
自动进行的到应用的用户和组预配		✓	✓	✓
Privileged Identity Management (PIM)			✓	✓

User / Group

Global Admin
 Entra ID User Admin

Azure User Admin

Tenant
 User Member a@c.com
 Guest b@c.org
 c@c.dev
 d@msn.com

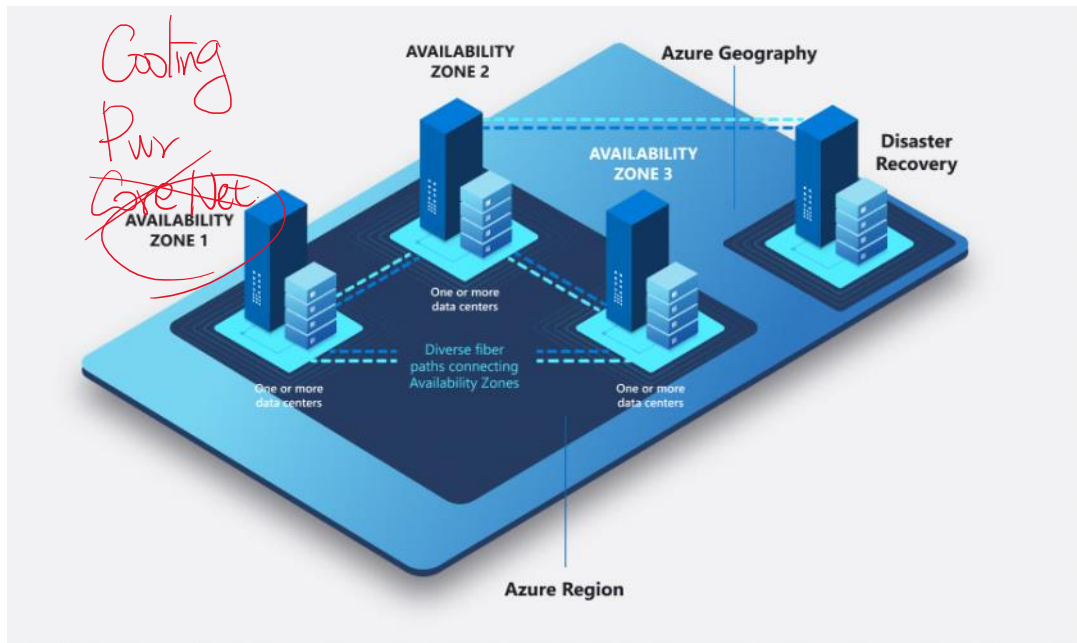
C ⇒ C.com
 C.org

Group [Security Group
IMBGS Group

Assign [Manual
Dynamic

Governance & Compliance

Region $\leftrightarrow$ ~~by~~ # $\leftrightarrow$ Data Center
3x





3F ? $\Rightarrow$ Latency

Billing

Compliance

HA

Region Pair

Subscription

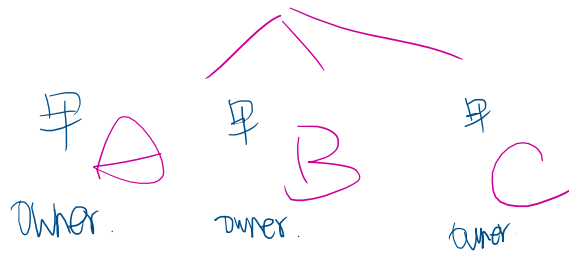
↳ Resource Group

Billing

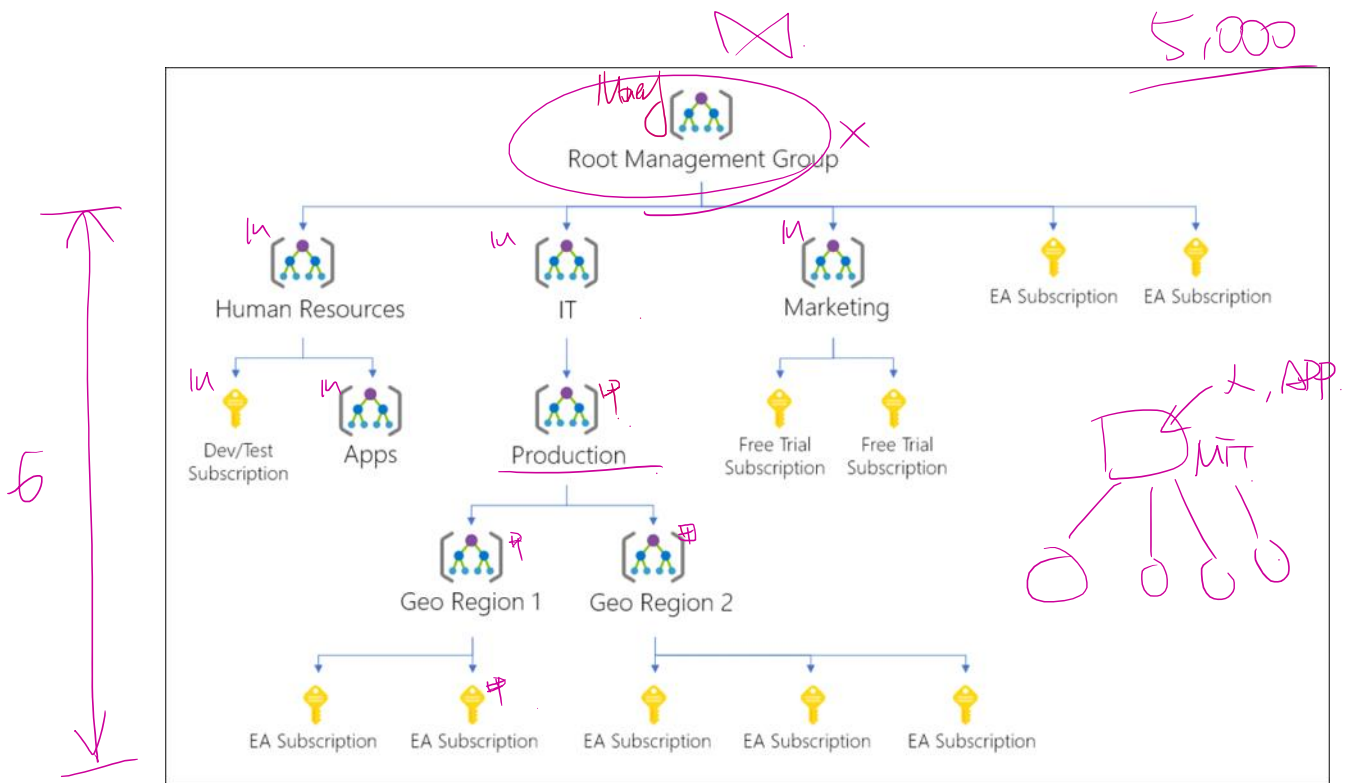
Security

HA

HA



Management Group



Tags — Metadata

RG
Resource

Re Live

en AZ104-085

Azure Policy → 規則

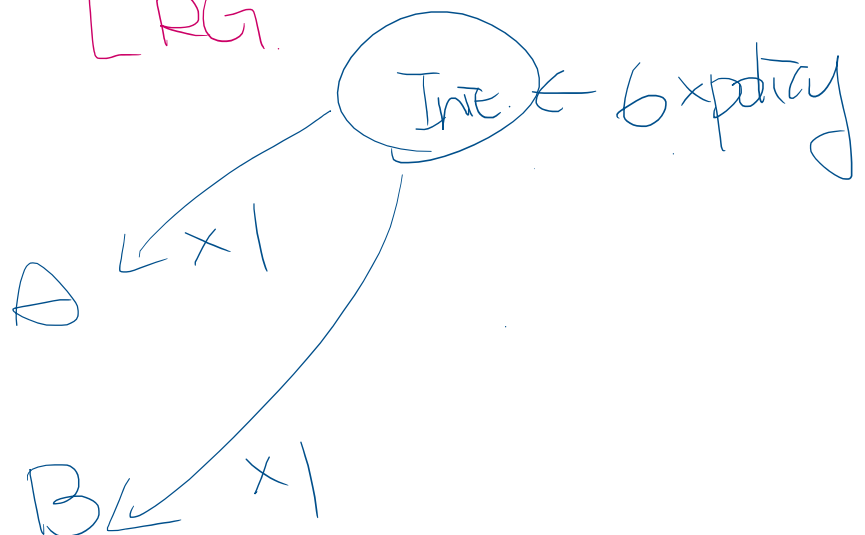
[Check
" + Enforcement.

ISO 27001

[MS - Report
User.

Definition [Policy [Built-in
Custom] - JSON
Initiative. (Policy's Folder)

Assignment [IUG
Sub
RG.



Role based Access Control (RBAC)

Role = 1 ~ n Permission

└ Built-in

└ Custom

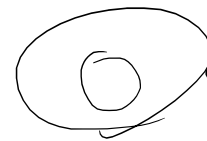
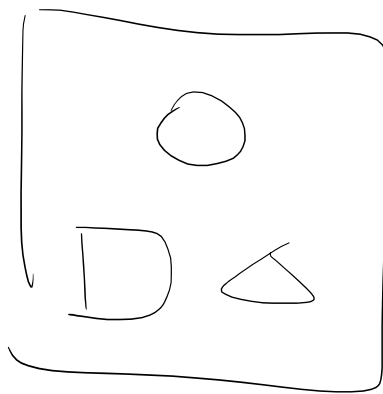
└ JSOU

Action/Not

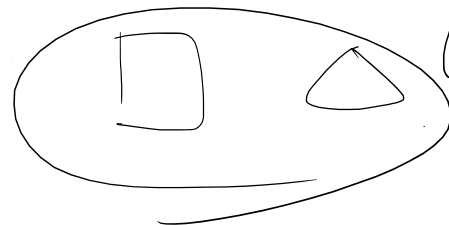
DataAction/Not

Assignable Scope

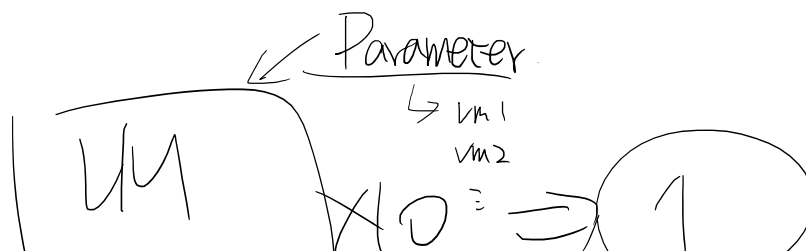
→ Check



Modify



Create



$$\begin{array}{c}
 | \quad | \quad | \\
 \hline
 \end{array}
 \quad
 \begin{array}{c}
 \text{v m z} \\
 \text{v m p} \\
 \downarrow \\
 10
 \end{array}
 \Rightarrow (1)$$

Networking

SDN

CIDR

Virtual Network (VNET)

Independent

Addr Space

32-16

10.10.0.0/16

$2^{16} \Rightarrow 65536$

Subnet x n

$2^8 \Rightarrow 256$

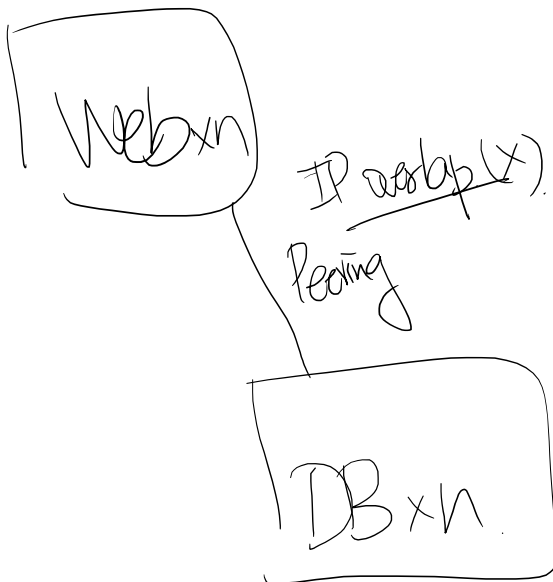
10.10.1.0/24

Reserved IP

$\Rightarrow 256 - 5 = 251$

10.10.2.0/29

$\Rightarrow 8 - 5 = 3$



IP — Private IP

Public IP

IPv4/v6

— Azure Resource

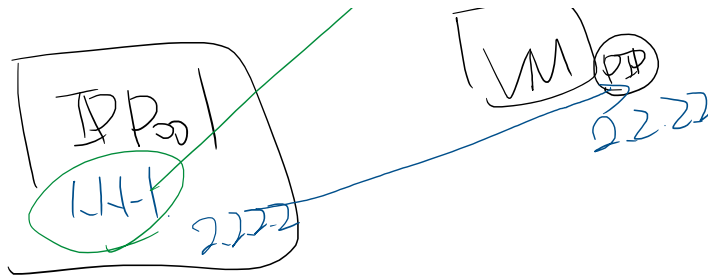
Basic

X Dynamic/Static

Standard

AZ Static





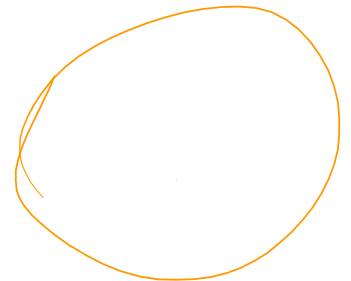
NSG (Network Security Group) Layer4 FW Stateless

Rules [InBand (Free)]
[OutBand] - priority (line)
100 ~ 4096

V RDP (3389) 200

X RDP (3389) 150

⊗ ←



Service Tag

NIC.] Associate
Subnet

Route — System Route
 — User Define Route.

└ Route Table

└ Route x N
└ link subnet.

Azure DNS Zone (PaaS)

└ (Public) DNS Zone
└ Private DNS Zone

demo.com
hr.demo.com
it . .

└ link VNET.

dev corp
dev. xxx

InterSite Connectivity.

VNET ↔ VNET

Region
└

Peering ⇒ VPN.

VNET1 $\leftrightarrow$ VNET

Region

Sub

Subscription

Peering $\Rightarrow$ VPN

VNET $\leftrightarrow$ Other

On-Prem

Other Cloud

Azure



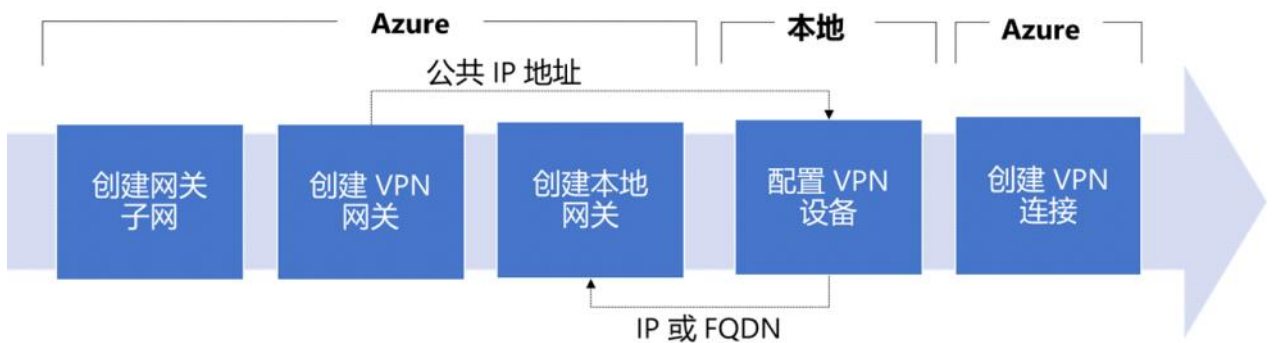
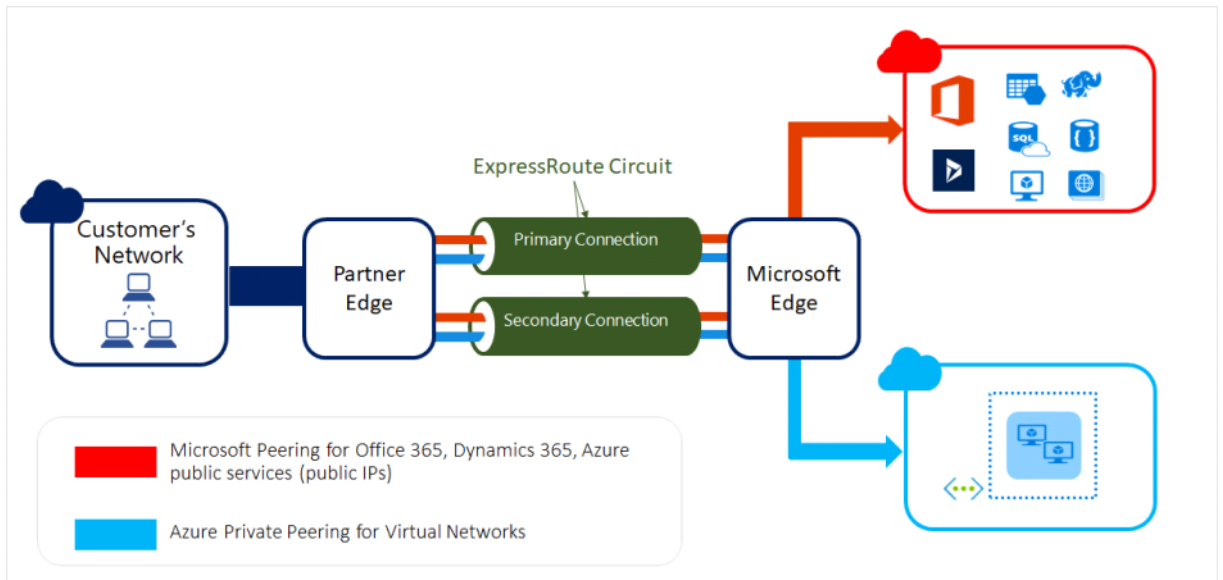
VNET Gateway
(VPN)

(VPN device)

Pass $\rightarrow$ HA (VM)
Scale

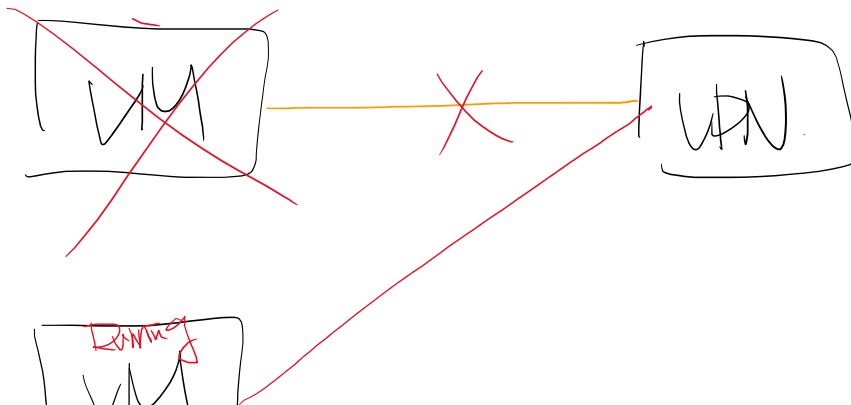
VPN { D2S
LS2S

Express Route



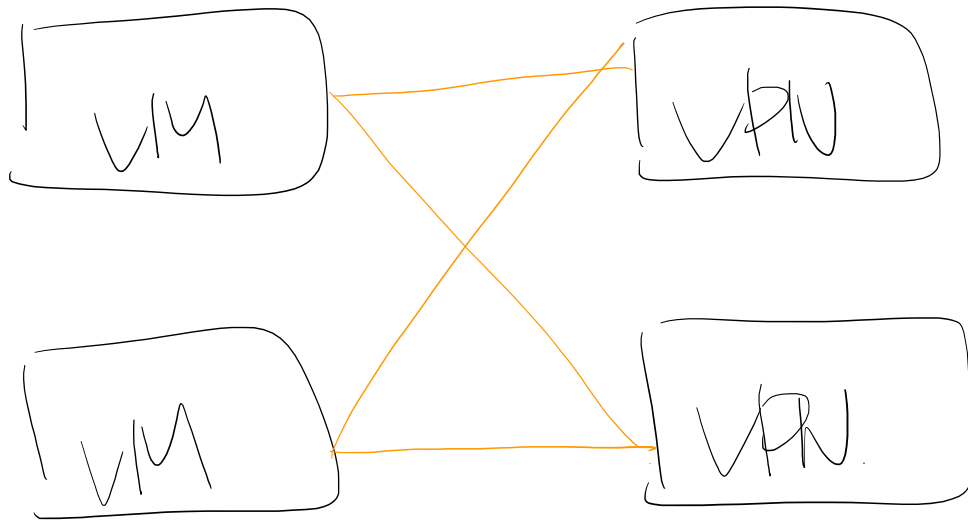
VPN HA

Active - Standby

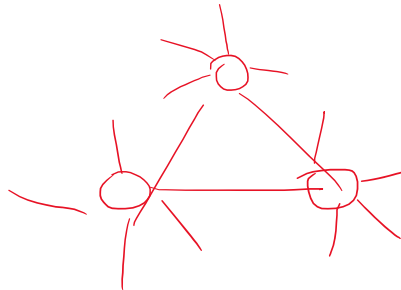
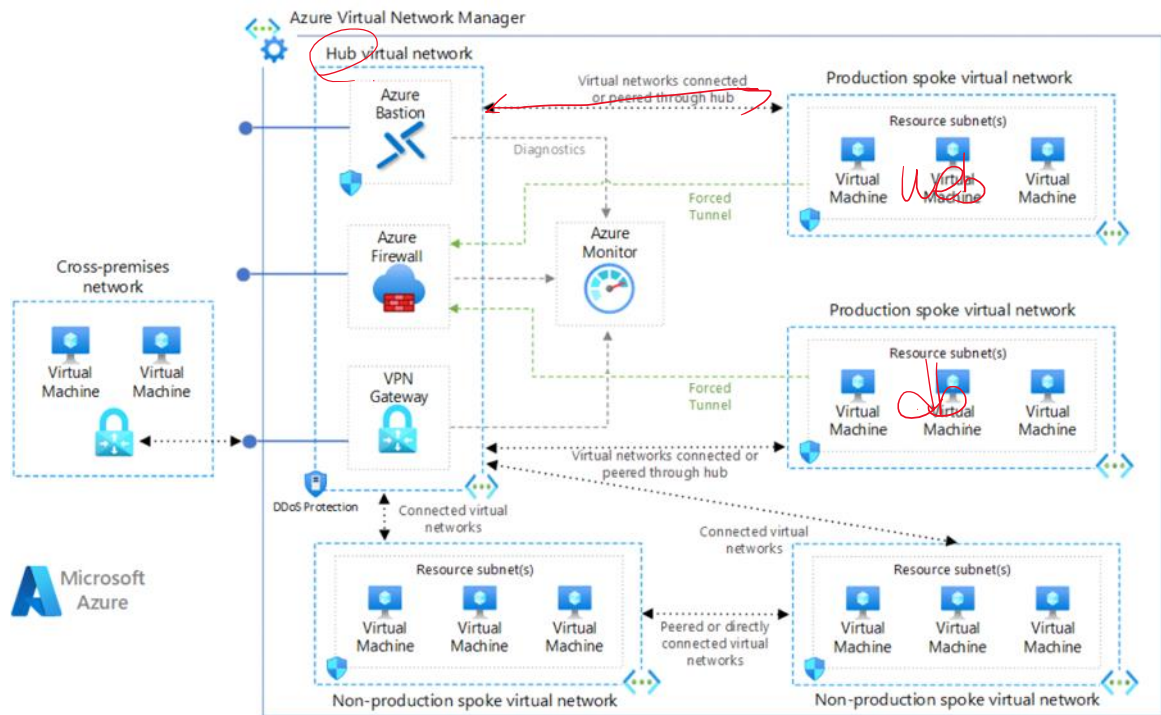




Active - Active



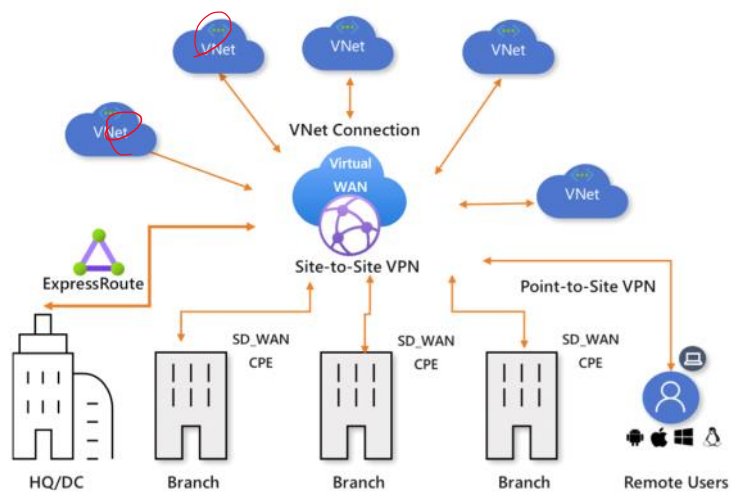
Hub - Spoke



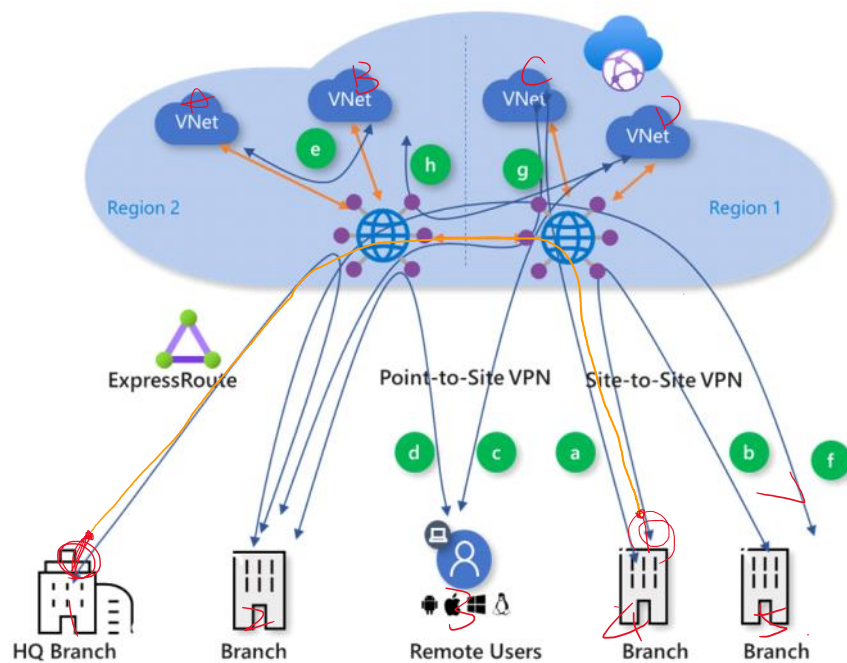
Virtual WAN

Virtual Hub (VNET)

VNET

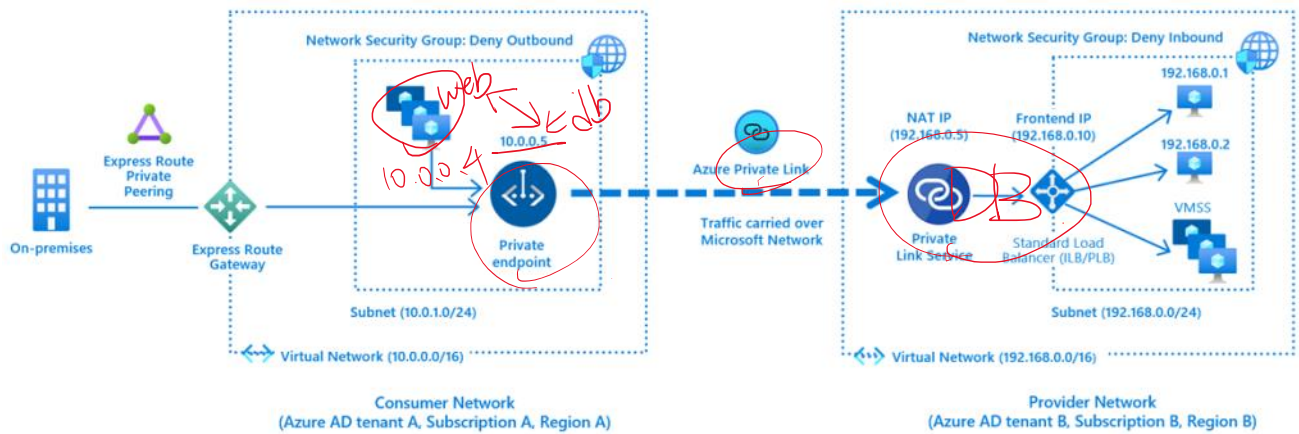
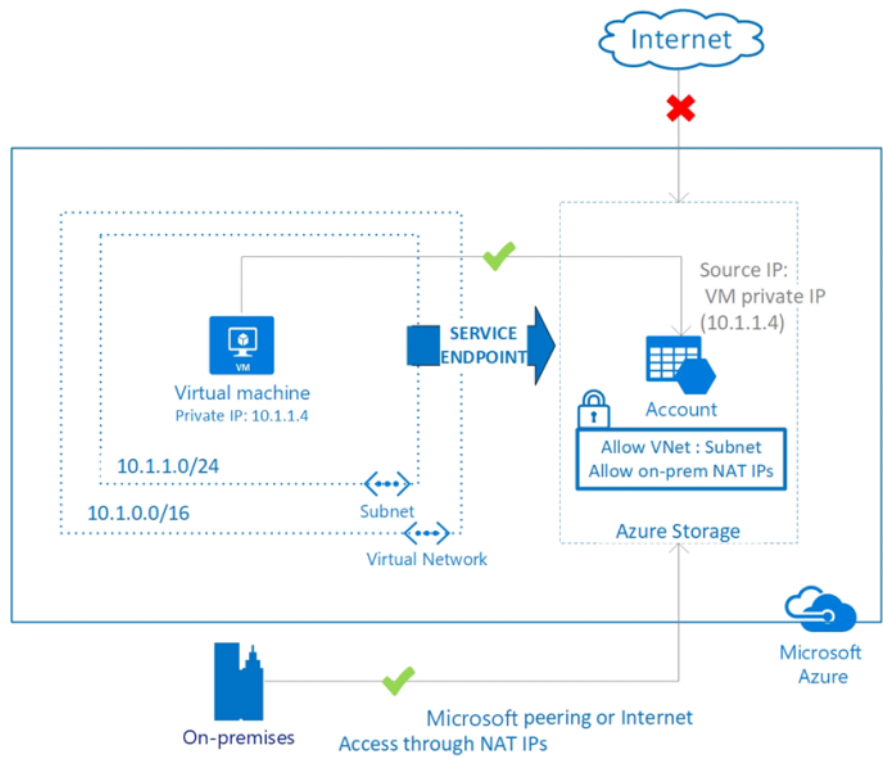


Branch 2



Service endpoint (Public endpoint)

Private Endpoint / Link



PaaS

Layer 1

Layer 2

Layer 4

DNS

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	
全局		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	



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

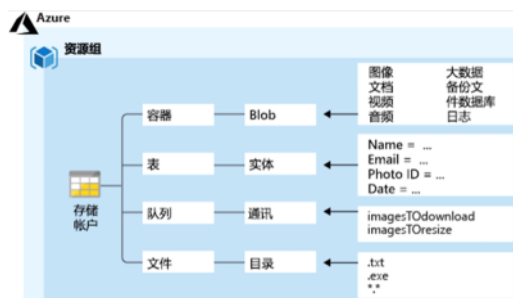
Azure 表：最适合存储结构化非关系型数据

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

Blob

HTTPS, FTPS



Azure 文件存储: 适用于云或本地部署的托管文件共享

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。

IOPS / Latency

Menu Search

TECHMONITOR

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.

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

By Mathieu Rosemain, Raphael Satter

3 MIN READ



©Microsoft Corporation

Source

Redundancy

4+2

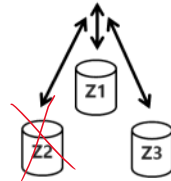
单区域



LRS

- 三个副本，一个区域，1 Zone
- 防止磁盘、节点、机架故障
- 在提交所有副本后确认写入
- 优于双奇偶校验 RAID

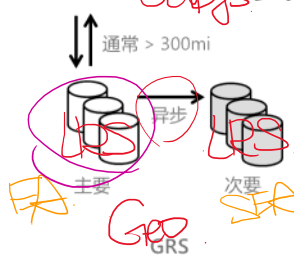
99.9%



ZRS

- 三个副本，三个区，一个区域
- 防止磁盘、节点、机架和区域故障
- 同步写入全部三个区域

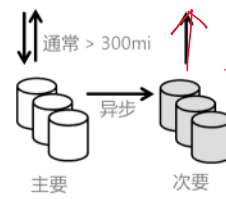
6000s 多个区域



GRS

- 六个副本，两个区域（每个区域三个）
- 防范重大区域性灾难
- 异步复制到次要对象

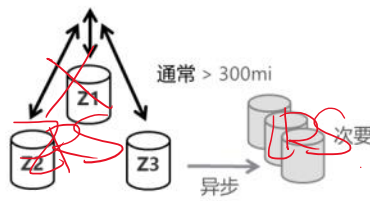
Region Pair



RA-GRS

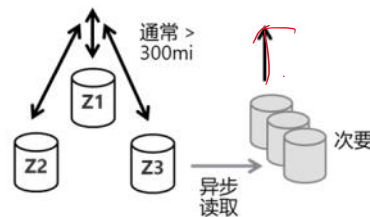
- GRS + 对次要对象的读取权限
- 单独的次要终结点
- 次要对象的恢复点目标 (RPO) 延迟可查询

多个区域



GZRS

- 六个副本，3+1 个区，两个区域
- 防止发生磁盘、节点、机架、区和区域故障
- 同步写入全部三个区并异步复制到次要对象



RA-GZRS

- GZRS + 对辅助数据的读取访问权限
- 单独的次要终结点
- 可以查询到次要对象的 RPO 延迟

⚠️ 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

Priority [Space
Transaction.

Access Tier - Hot
(By Blob) Cool
Gold
Archive

Lifecycle Management
↳ JSON
↳ Codes.

[2024/img1.jpg]
Blob Name

Shared Access Signature (SAS)

Target [Storage
Service
Container
Blob

(Access key)

+ Key

Duration

Permission

Token

<https://demo0807stor.blob.core.windows.net/images/2024/IKEA.jpg?sp=rwd&st=2024-08-07T02:56:26Z&se=2024-08-07T10:56:26Z&spr=https&sv=2022-11-02&sr=b&sig=FtXdGgfsIzEnXOejSzprws7K0q4RcpMjzSm4Cg%2F3UE%3D>

Key

Access Policy ← By Container

<https://demo0807stor.blob.core.windows.net/images/2024/IKEA.jpg?si=demo0807policy&spr=https&sv=2022-11-02&sr=b&sig=zMjBbd%2BAxS3sppKnmYzvKP%2Fge5cwTFvcwJxV4OGVRgl%3D>

VM (IaaS)

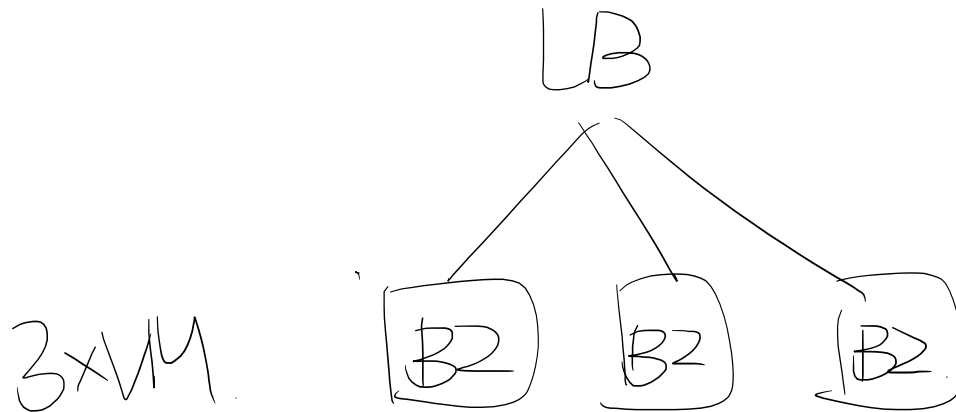
Feature

Computing ⇒ Type x 6 ⇒ Series ⇒ Size

Storage T Managed Disk → Azure Resource

L Storage
 Managed Disk $\rightarrow$ Azure Resource
 UnManaged Disk $\rightarrow$ VHD - Storage
 Page
 Blob

1 VHD $\times$ 5000 IOPS $\Rightarrow$ 50,000



VM HA

① Create AS
 ② new vm $\uparrow$
 1 ~ 3

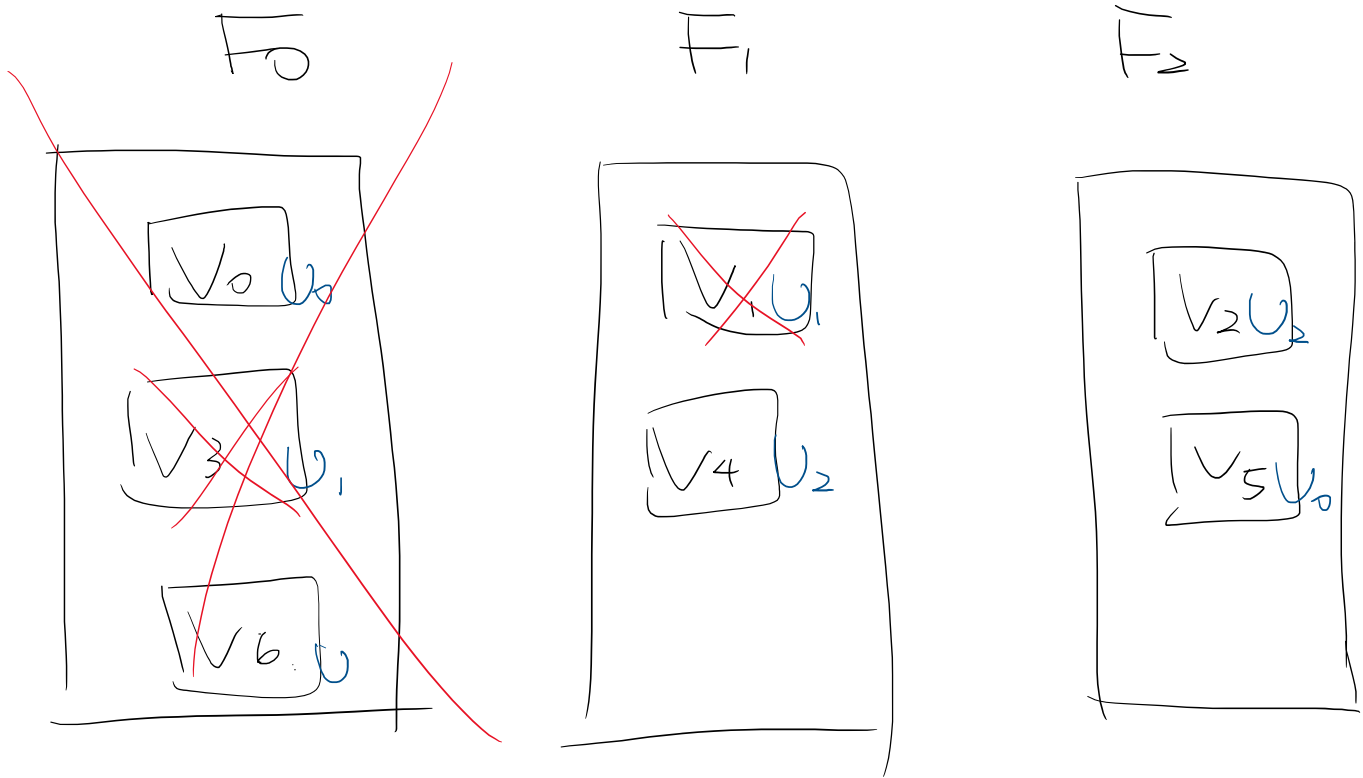
Availability Set

Fault Domain - Hardware

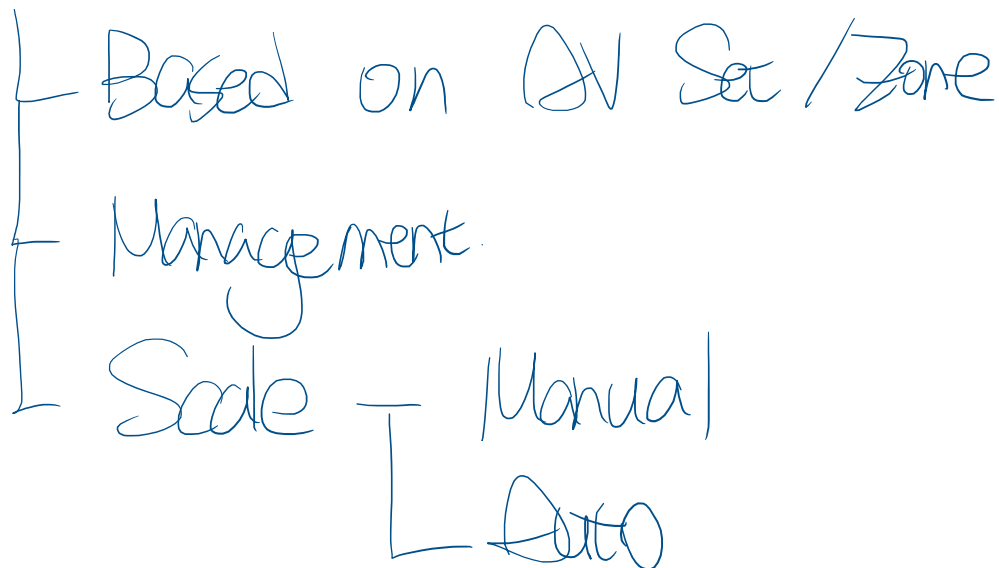
Availability Zone

1 ~ 20
 1 Update Domain - Update

L Update Domain - Update



VMSS (Scale Set)



L Loto

PaaS

Azure App Service (Web App)

L App Service Plan (VMSS)

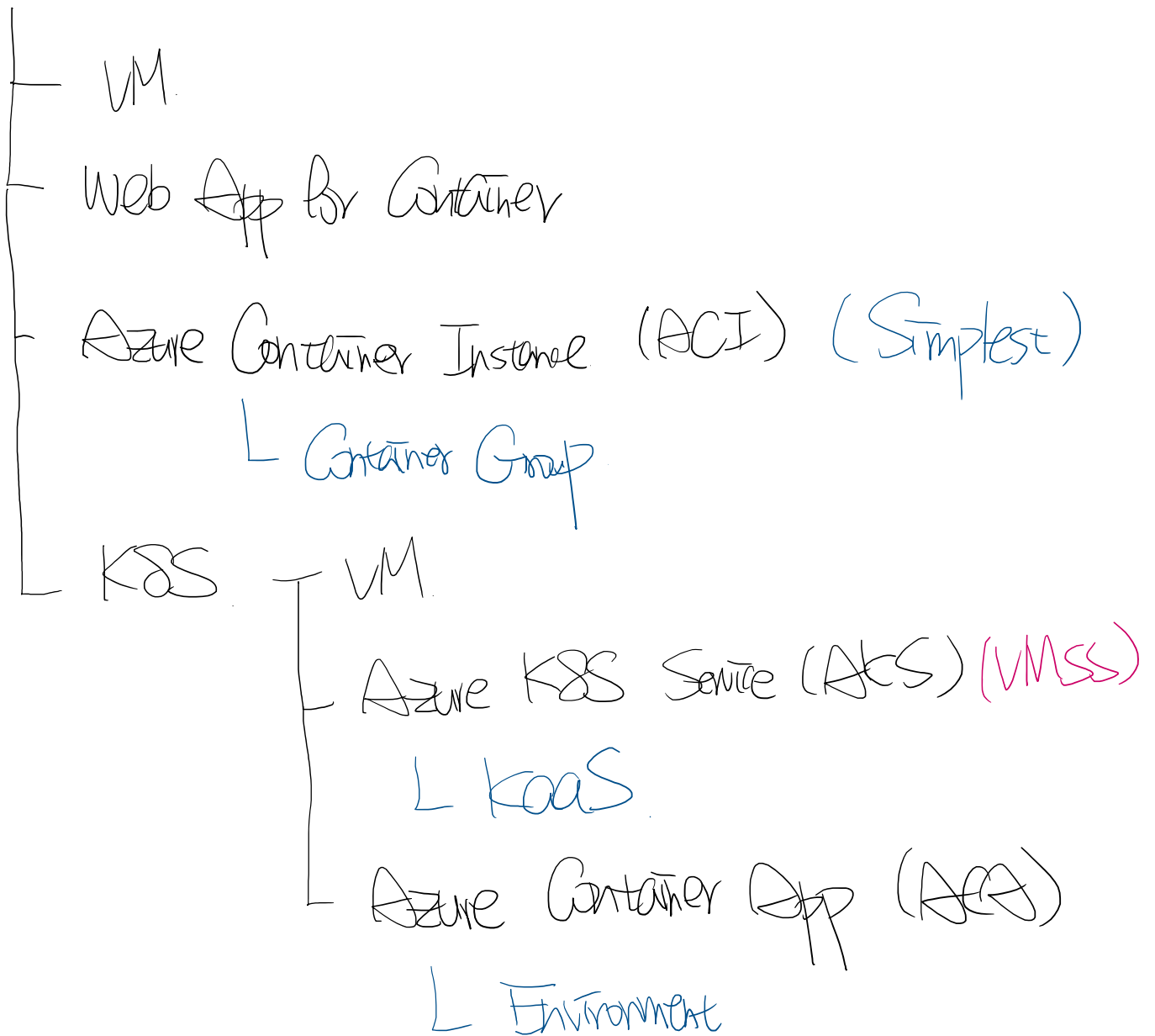
L WebApp x n

Computing
Feature / Pricing

Plan A $\Rightarrow$ 10 App

Plan B $\Rightarrow$ 5 App

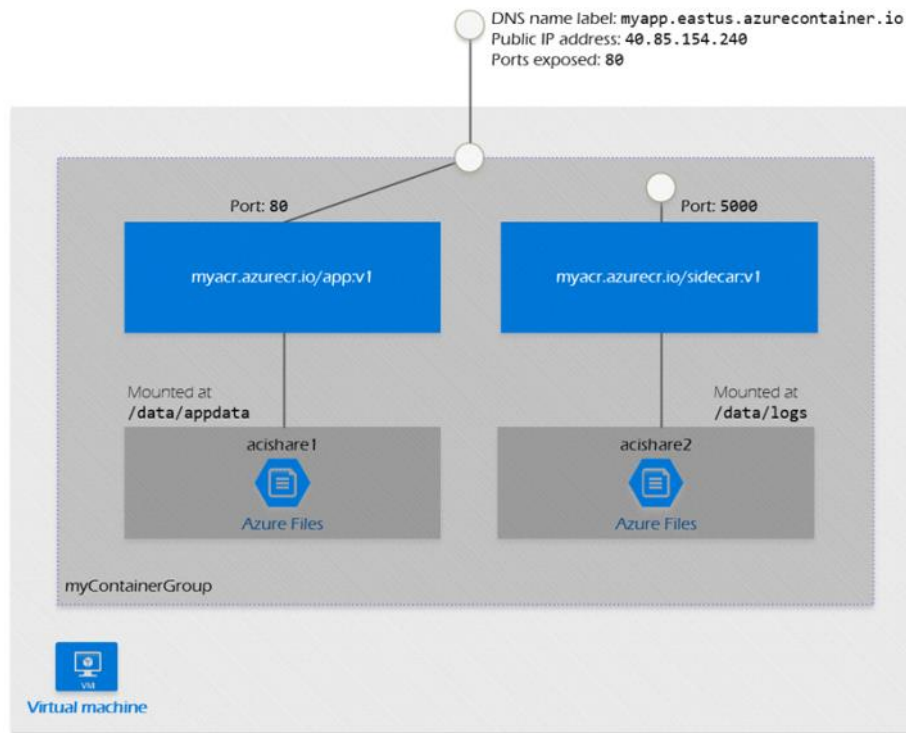
Container



Azure Container Registry (ACR)

- └ based on Docker Registry 2.0
- └ Private

Private
Public



Backup

Backup Center

Recovery Service Vault - Built-In Storage

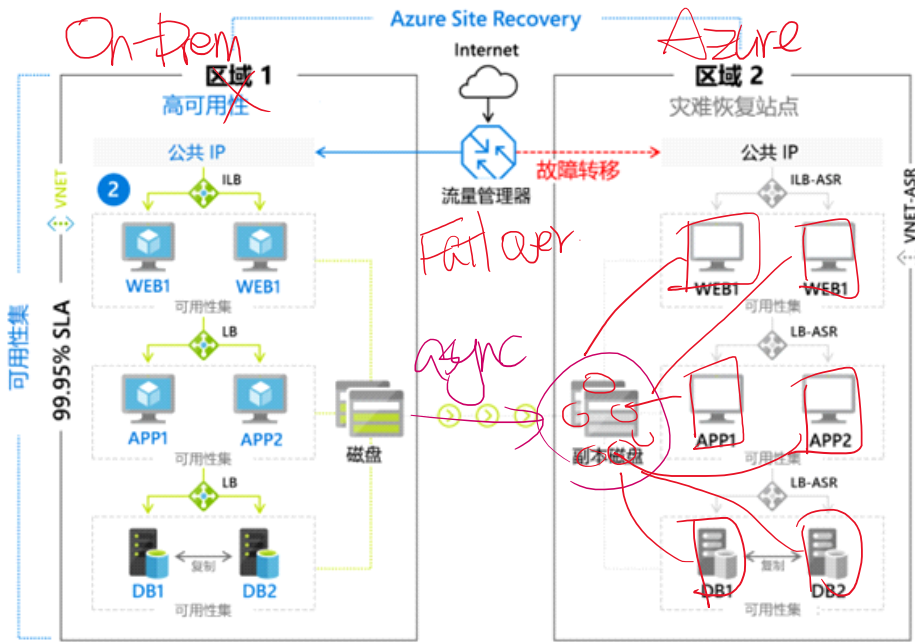
LI-Fix

- Files
- VM
- Migration.

On-Prem

- Files → MARS (Agent)
3x / day (Schedule)
- VM → ABS (Server)

- Explore
- Selection
- Backup



Monitor

└ Azure Monitor

Azure Log analytics workspace Resource x n

Table

- └ Metric, log
- └ Azure / Non Azure
- └ Built-in Storage
- └ Time
- └ Interactive
- └ Archiving

(KQL)

Kusto Query Language

Kusto Query Language

└ Archive

↳ SQL like logic

Azure ADAL

└ Target — Subscription
MG
Resource (S)

Condition └ GUI ☐
└ KQL

Action Group (Resource)

└ Notification — Email
SMS
Ann

App Phone

Action - Azure Automation

Azure Function

Webhook

etc. - - -