

Identity

On-Prem

✓
AD DS

LDAP
Kerberos
NTLM

Hybrid
Sync
→
←

Entra ID Connect

✓
Entra ID

HTTP/S - OAuth

XOAUTH

X GPO

→ 443
(Agent)
(Cloud)

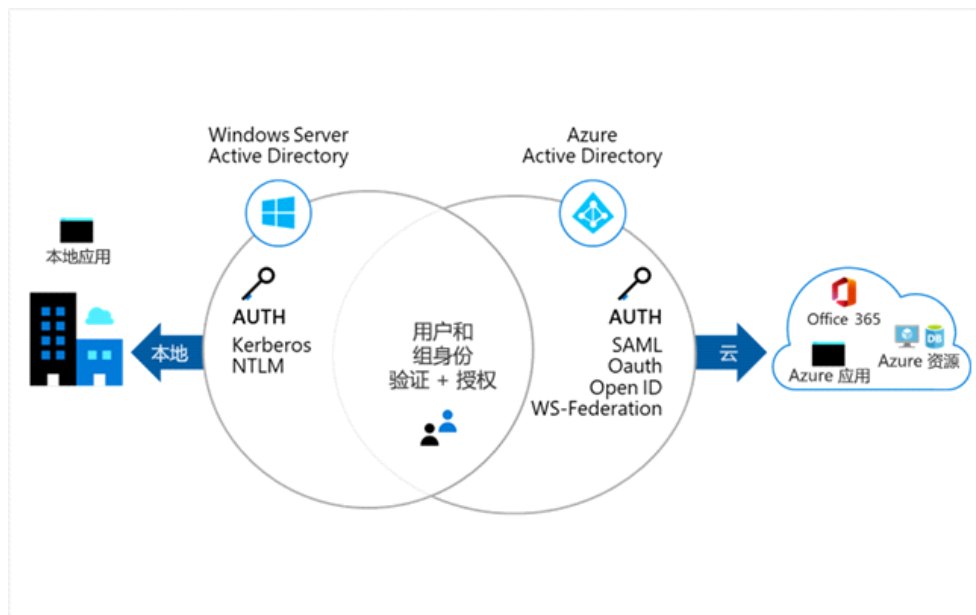
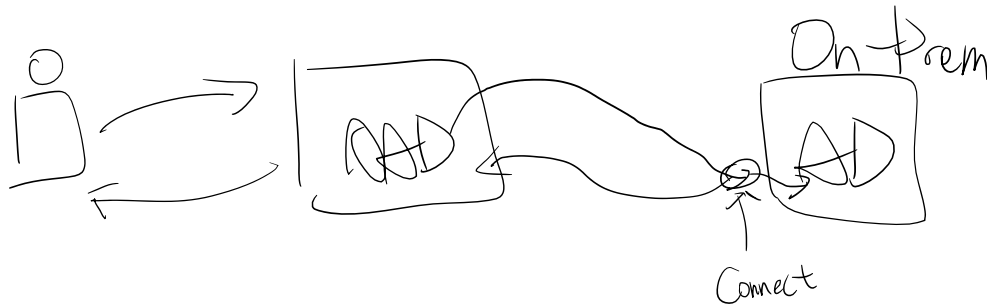
Password
Hash
PassThrough

Entra ID DS

(DSaaS)

OpenID

WSFed



Entra ID

Register → BYOD, user own device

Join → full control

Hybrid Join

Azure AD 注册设备	Azure AD 加入设备	混合 Azure AD 加入设备
• 支持自带设备办公 • 已注册的设备使用 Microsoft 帐户登录 • 附加到授予对资源的访问权限的 Azure AD 帐户 • 使用 Microsoft Intune 等移动设备管理 (MDM) 工具进行控制 • OS - Windows 10 及更高版本、iOS、Android 和 MacOS	• 面向云优先或仅使用云的组织 • 组织拥有的设备 • 仅与 Azure AD 联接 - 所需的组织帐户 • 可使用条件访问策略 • OS - Windows 10 及更高版本设备	• 已将 Win32 应用部署到这些使用 Active Directory 计算机身份验证的设备 • 你想继续使用“组策略”来管理设备 • 你想使用现有映像解决方案来部署设备 • OS - Windows 7 及更高版本设备

User / Group
RBAC (Role-based Access Control)

Entra ID Global Admin
AAD User Admin

Azure Global Admin
X User / Group

User T Member

tenant - mtt.com
mtt.org

User └ Member
└ Guest

external - mtt.com
mtt.org

a@mtt.com
b@mtt.org └ Member

c@mtt.cn
d@mtt.tw └ Guest
e@hotmail.com - Guest

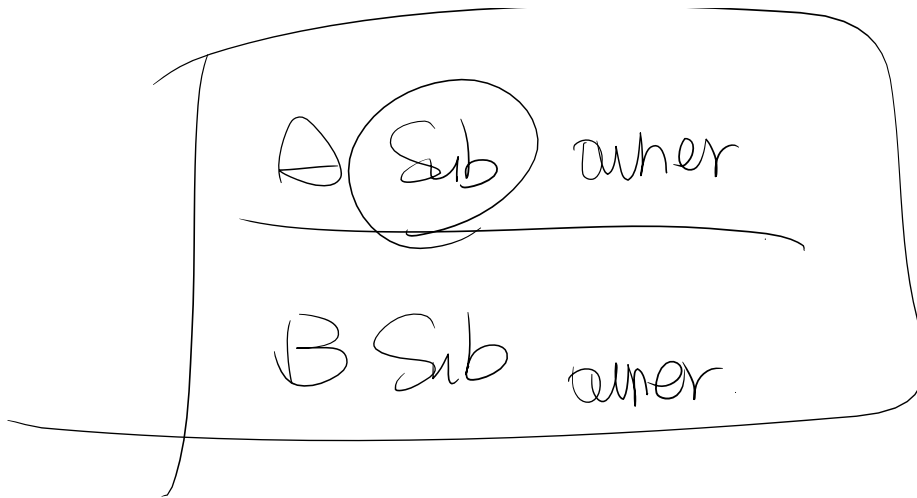
Group └ Security Group
└ M365 Group

└ Design └ Manual

└ Dynamic └ User
└ Device

Tenant

User └ └ Subscription < Billing
Security 边界



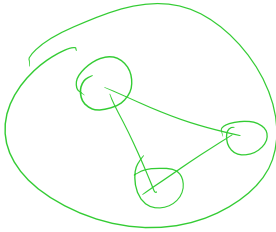
Region $\rightarrow$ $3 \times$ Availability Zone $\leftarrow n \times$ Data Center

区域

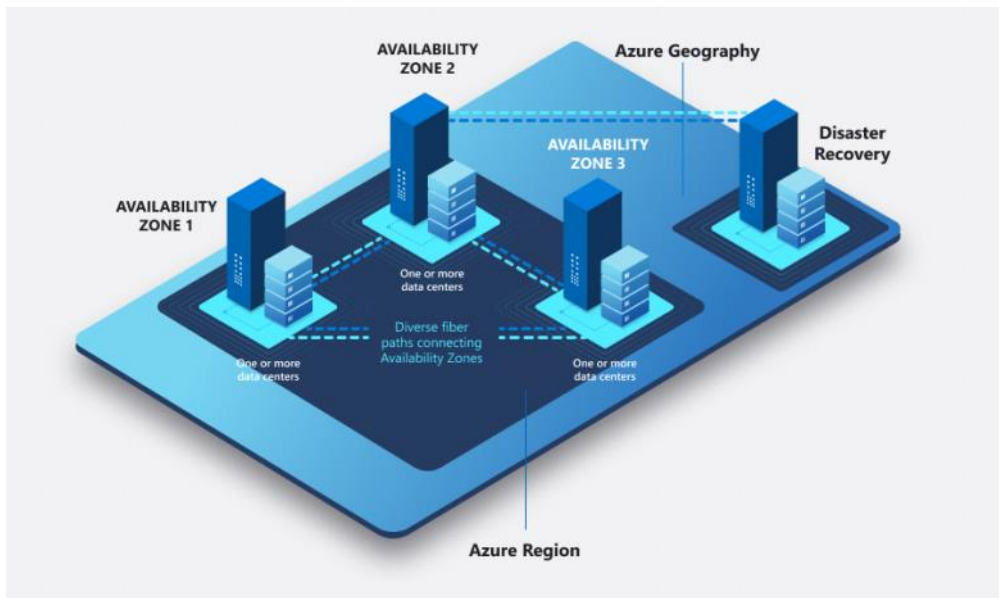
可用区(域)

数据中心

East Asia



Power, Cooling, Core/Net



Region Pair



Management Group.

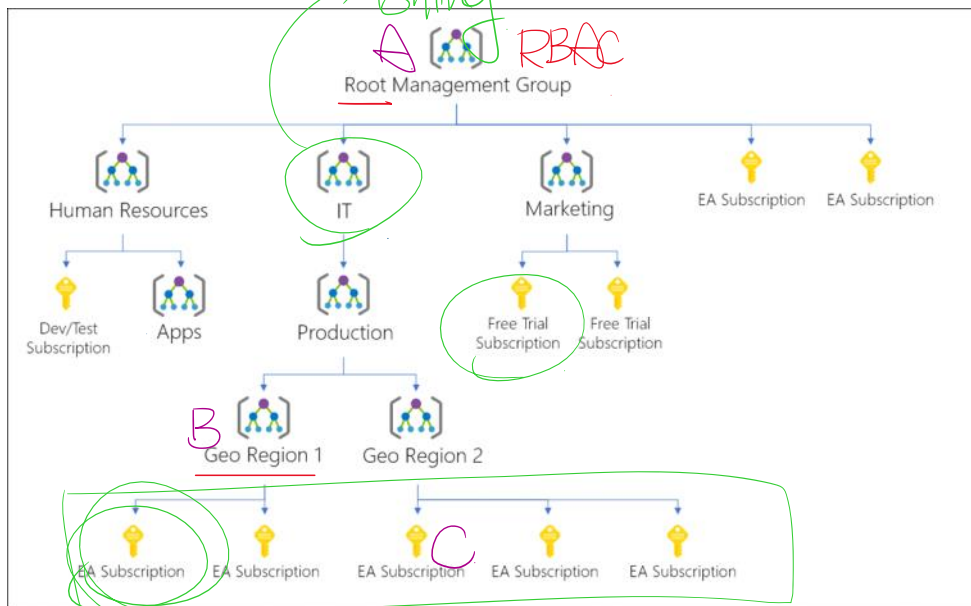
↳ Cross Sub

Tree, Inherit

Billing

A RBAC

A = All Sub



Cost Management (Service) ←

U

(Resource) ← Create 後 才 用

Tag = Metadata (key-value)

Cost Center

Owner

Azure Policy → 規則

{ Check = Non-Compliance
" + 強制 =

ISO27001

{ MS-Report
User

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

5x assign | x init
5x sub | 2 Policy

assign x 5

assign x5

x5

Assignment

- MG
- Subscription
- RG

RBAC (Role-based Access Control)

Role = 1 or more Permission

- Built-In
- Custom

→ JSDV

- Action
- Not Action
- Data Action
- Not Data Action
- Assignable Scope

Administration (Tool)

ARM - Azure Resource Manager - Management Layer

Azure Portal - Azure Cloud Shell

Azure PowerShell

PowerShell's Module

Cross Platform (PowerShell Core)

Cmdlet → V. - n.

Azure CLI

命令式

New - AzVM - - - - -

Find - Cmd - - - -

→ Shell Script

→ Installer

n.

v.

AZ [group] [subgroup] [Command]

AZ VM create

(IaC)

声明式

→ JSON

ARM Template

~

Deployment

} Syntax

Azure Bicep $\rightarrow$ Syntax
 $\rightarrow$ Bicep

Parameter $\leftarrow$ Deploy 時, 人為互動

Variable $\leftarrow$ $C = A + B$

Resource

Function $\left\{ \begin{array}{l} \text{Pre Define} \\ \text{User Define} \end{array} \right.$

Output

Networking

Virtual Network (VNET) - Addr Space - CIDR

↳ Independent

10.10.0.0/16

10.20.0.0/16

Subnet

→ .0, .1, .2, .3, .255

Reserved IP

Sub1 10.10.1.0 / 24 → ~~256~~ - 5 ⇒ 251

Sub2 10.20.5.0 / 27 → 32 - 5 ⇒ 27

IP - Private IP

↳ Public IP - Azure Resource

IPv4/v6

Basic (Static) x Dynamic
Standard AZ Static

1.1.1.1

IP Pool

VM Start FQDN
2.2.2.2

NSG (Network Security Group) Layer 4 Stateless FW

Rules - InBound - Priority (Int) Smaller has higher priority
OutBound
100 ~ 4096

L OutBound

100 ~ 4096

priority

80

110

X 3389

(IP) (Service)

120

X 8080

Service Tag

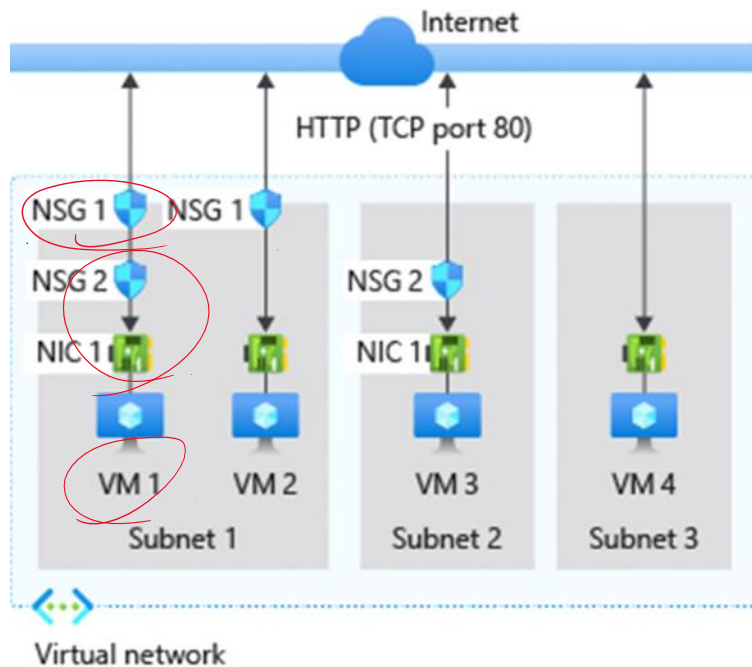
Associate

Default Rules (X Edit, X Delete)

Appliance (VM vNIC)

(Override)

Subnet



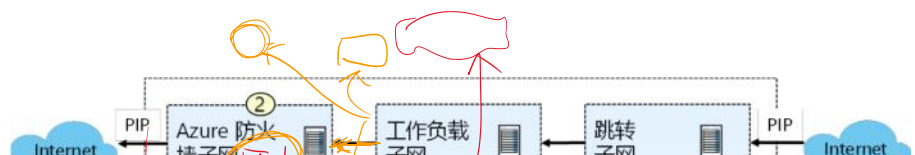
Azure Firewall (Firewall as a Service) (PaaS) - (VM)

Layer 3 Stateful FW.

LHA Scale

Subnet

NAT
Network



↳ Route Table - Ruten.

Azure DNS (PaaS DNS Service)

Xdev.com

US-Dev-Wm

Uk der Gm

Tip der.com

L Link VNET

$$VNET \leftrightarrow VNET$$

Region

$$1/\sqrt{1-\beta^2} = \gamma = 1.01005$$

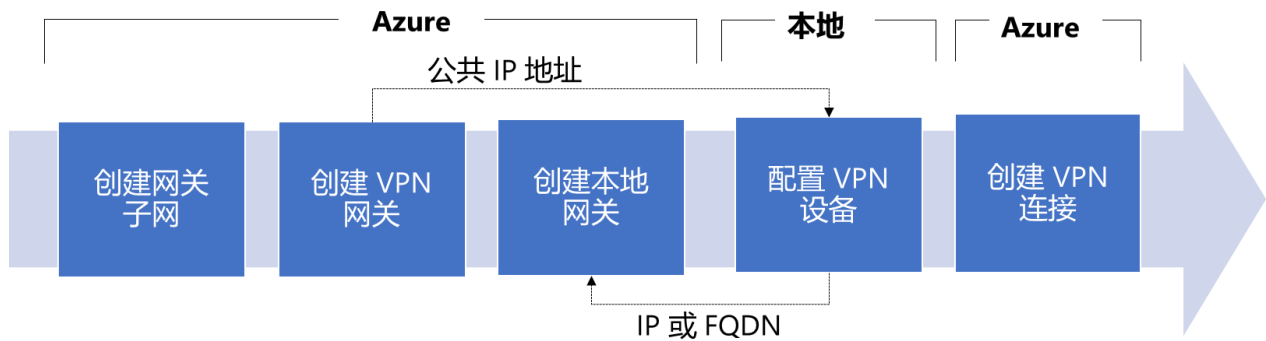
VNET $\leftrightarrow$ Other (On-Prem)

S2S
P2S VPN

Express Route

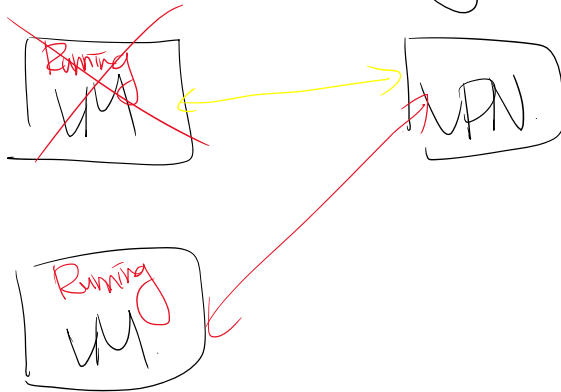
VNET Gateway

(PaaS) $\rightarrow$ Scale
 $\rightarrow$ (VM) HA

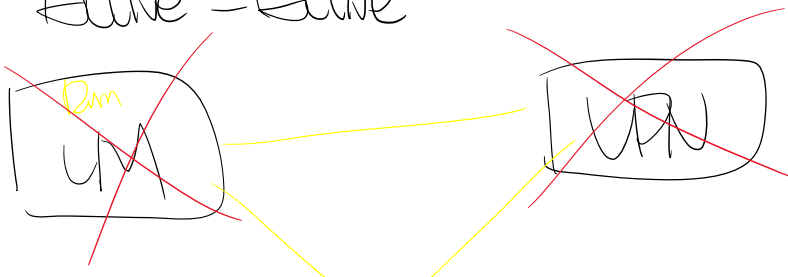


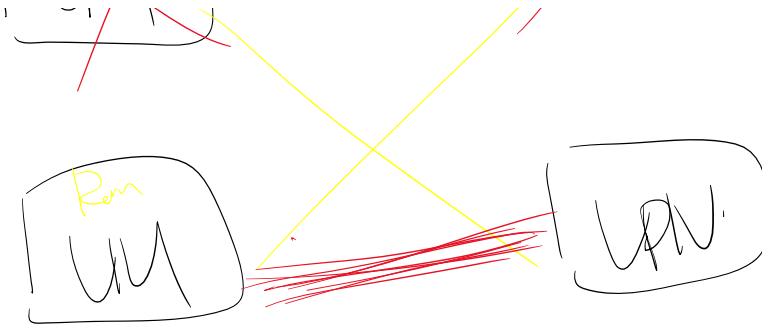
HA

Active - Standby



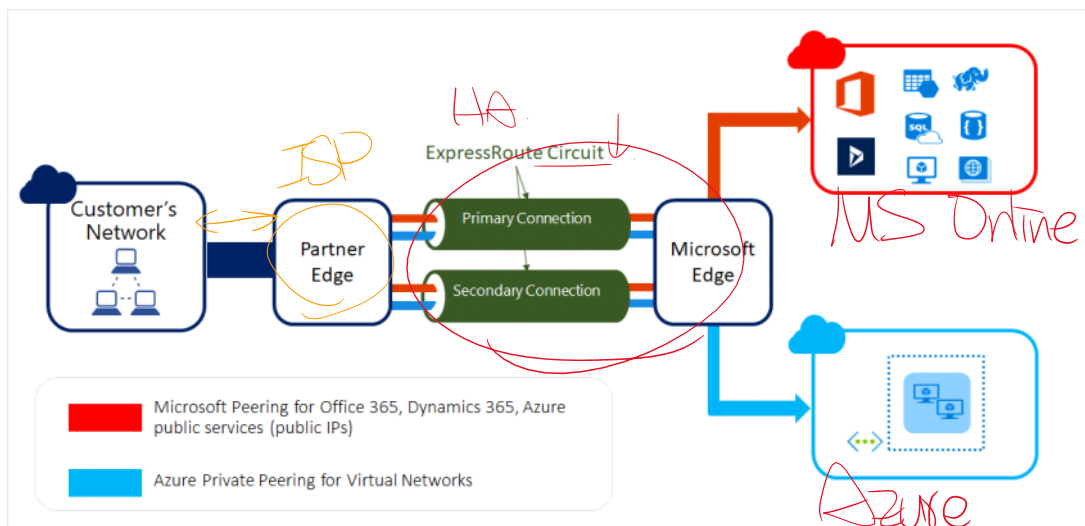
Active - Active



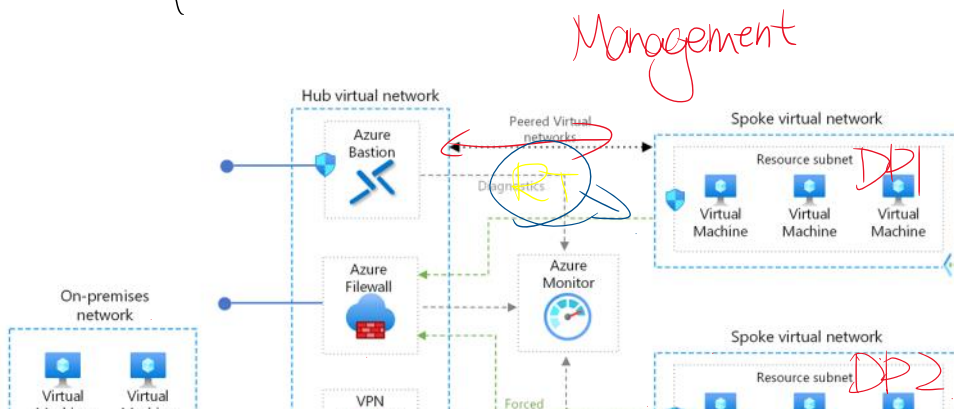


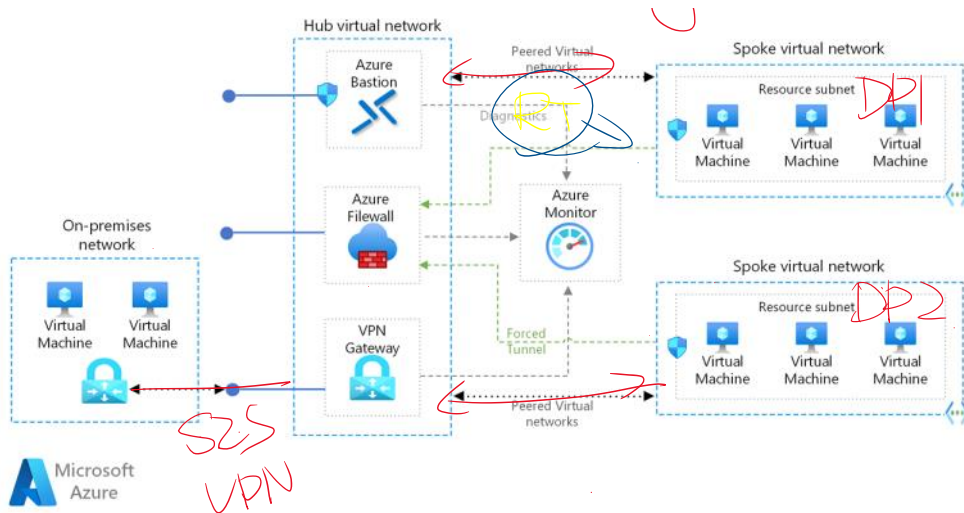
Express Route

↳ Private Connection



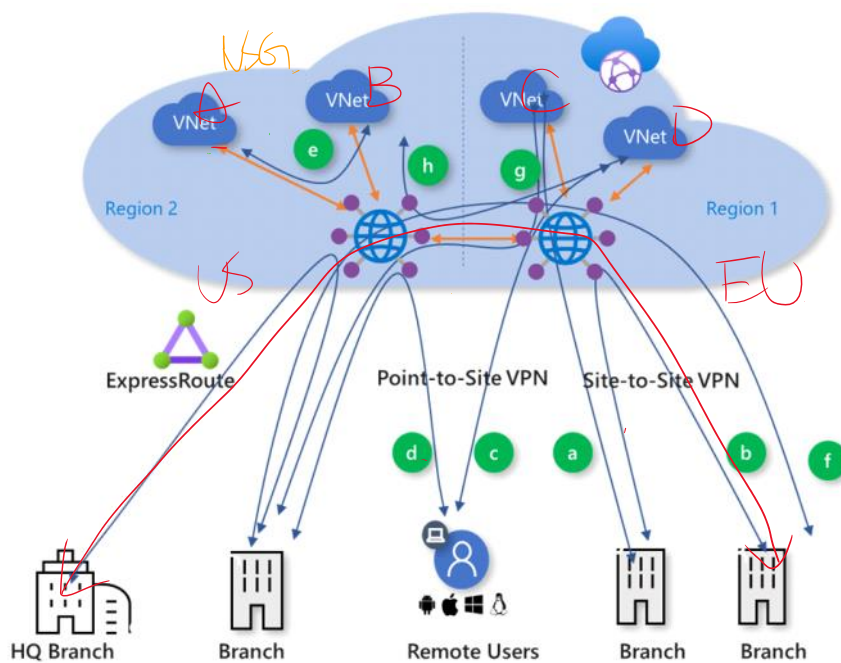
Hub - Spoke





VWAN (based-on Hub-Spoke)

↳ Remove Route Management



Virtual Hub
↳ Region

LB

Paas
Layer 7

Layer 7

Layer 4

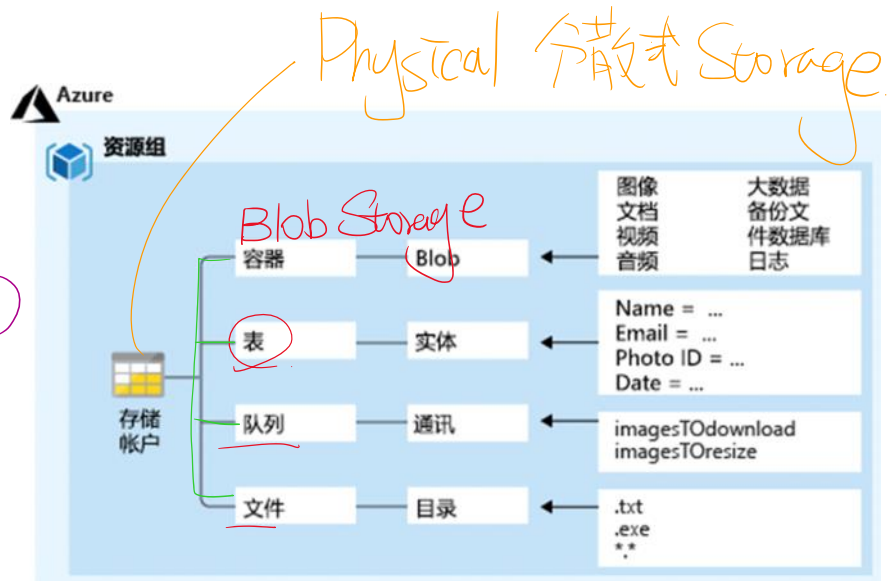
DNS

功能	应用程序网关	Front Door	负载均衡器	流量管理器
使用	使用 Web 应用程序防火墙增强应	可缩放的安全增强型交付	均衡入站和出站连接以及	在全球 Azure 区域内以最佳方式

情况	用程序安全性时，优化来自应用程序服务器场的交付。	点，适用于基于微服务的 全局 Web 应用程序。	对应用程序或服务器终结点的请求。	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

- Blob
 - HTTP/S (FTP)
 - Block - 循序
 - Page - 随机
- Files (Share)
 - SMB, NFS



Blob

File

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。

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.

⚠️ 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

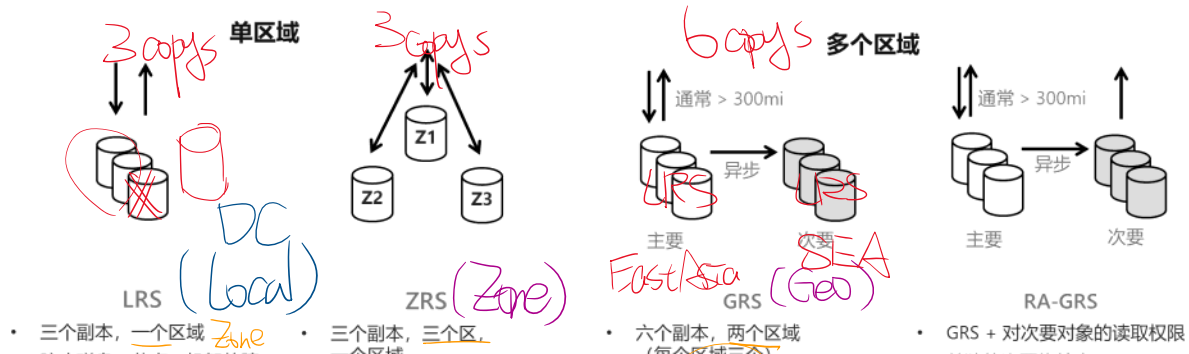
3 MIN READ



© Microsoft Corporation

Azure

Redundancy 3~6 copies



LRS (Local)

- 三个副本，一个区域 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

99.9-99.999%

ZRS (Zone)

- 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

Fast/Slow (Geo)

GRS

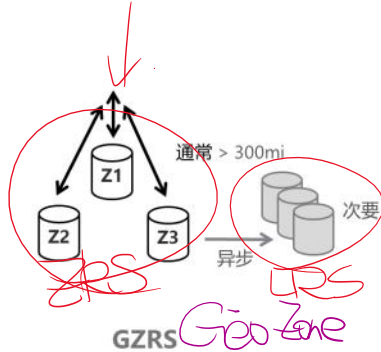
- 六个副本，两个区域（每个区域三个）
- 防范重大区域性灾难
- 异步复制到次要对象

Region Pair

RA-GRS

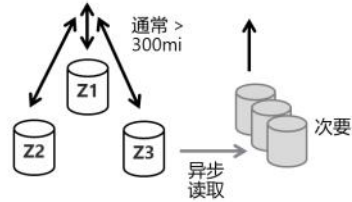
- GRS + 对次要对象的读取权限
- 单独的次要终结点
- 次要对象的恢复点目标 (RPO) 延迟可查询

Read Access



- 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

多个区域



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

Range = Space
Transaction

Access Tier - Hot
(By Blob) Cool

Cold

Archive

Lifecycle Management
Rule (JSQV)
Cooler

Shared Access Signature (SAS)

Target
Duration
Permission

← Storage
Service
Container
Blob

+ key

<https://demo0417stor.blob.core.windows.net/images/IKEA.jpg?sp=rawd&st=2024-04-17T03:00:56Z&se=2024-04-18T11:00:56Z&spr=https&sv=2022-11-02&sr=b&sig=SPbdRWwFvV7m6UTZiGAS%2FFWaQFQiCpTvZ2%2FTtsrbxXw%3D>

SAS Token

+ key

VM (IaaS)

Computing - Type - Series - Size

Storage - Managed Disk - Azure Resource

UnManaged Disk - VHD - Storage

Unmanaged I/O - storage
 10VHD x 5,000 IOPS Page Blob
 $\Rightarrow 50,000 \text{ IOPS}$

VM HA

Resource

Availability Set

1 ~ 3

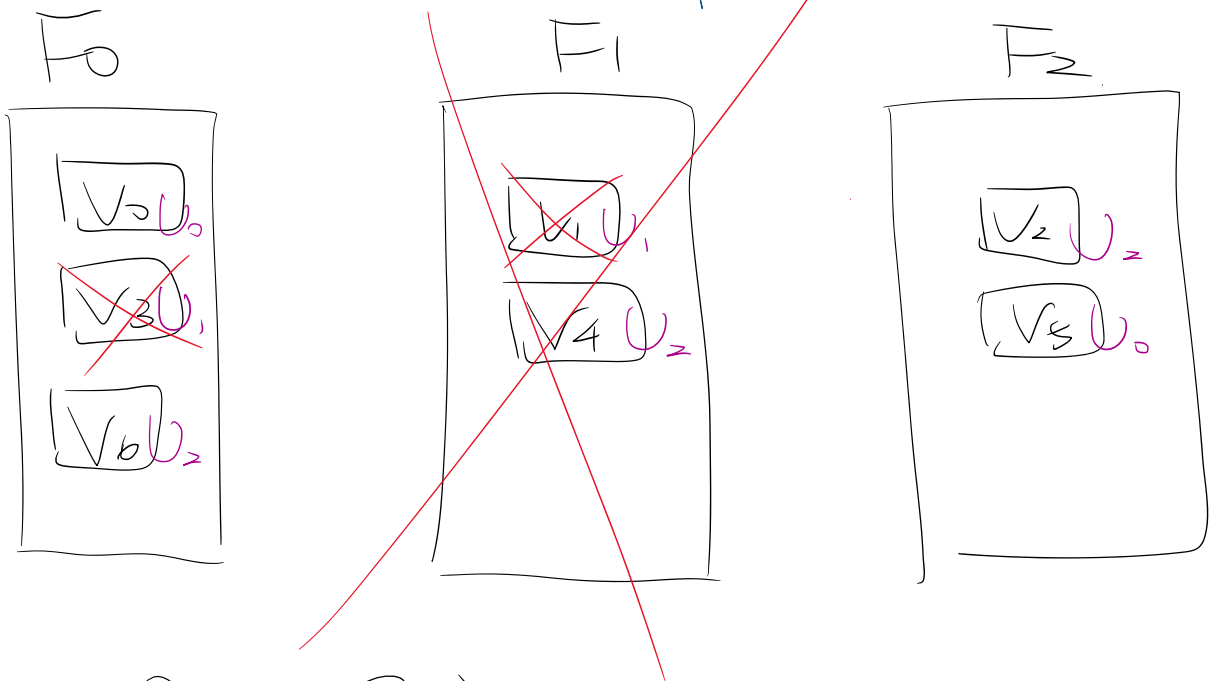
Fault Domain - Hardware

F0 - AZ

Availability Zone

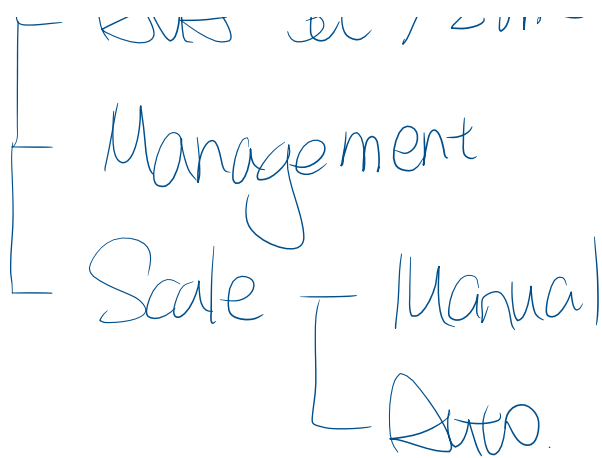
1 ~ 20

Update Domain - Software



VMSS (Scale Set)

- AVA Set / Zone



PaaS Solution (Computing)

Azure App Service

App Service Plan (VMSS) ← Pricing / Feature Performance

└ Web App x n

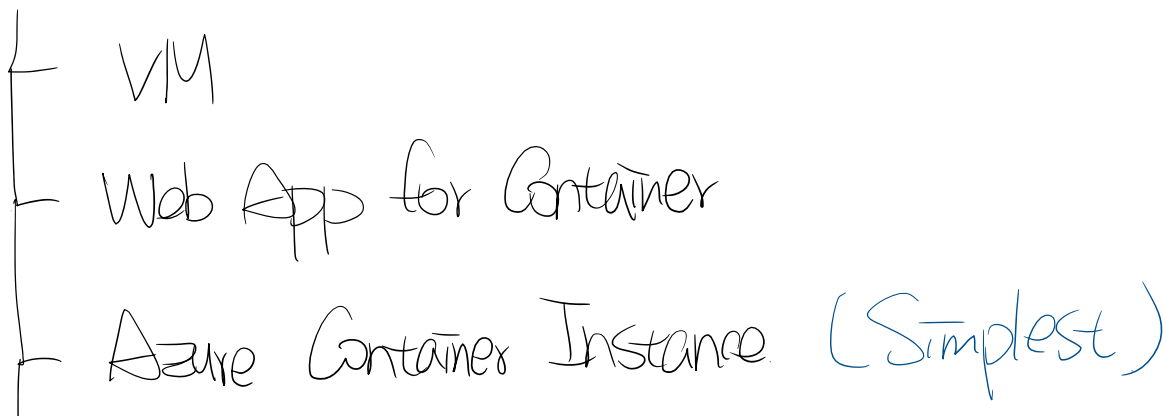
↓
 A S1 10 App
 B S1 5 App

Azure Compute Unit

vCPU

Scale

Container



[Azure Container Service (ACS)

[K8S - Azure K8S Service (AKS)
 └─ KaaS

 └─ Azure Container App (ACA)
 └─ Environment

Azure Container Registry (ACR)

└─ based on Docker Registry 2.0

└─ Private

└─ Public

04

Monday, April 15, 2024 8:37 AM