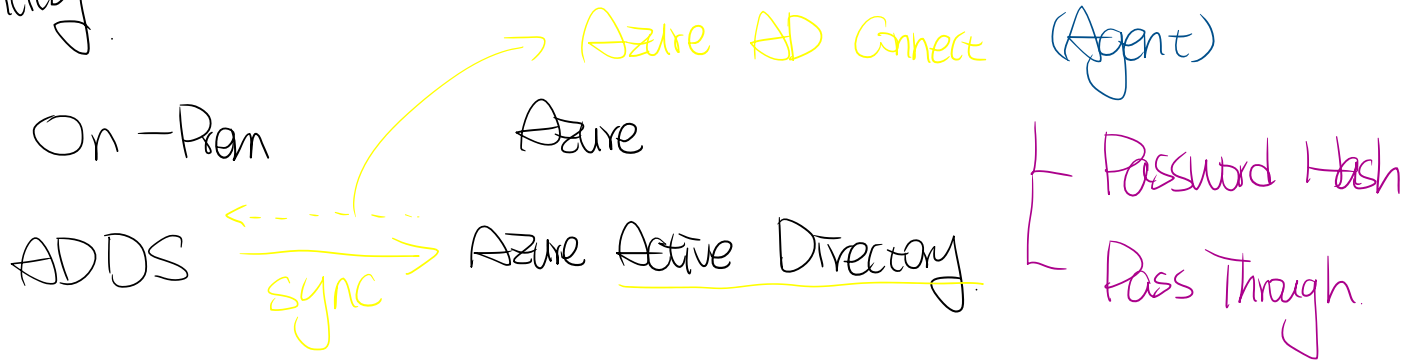


Identity



NTLM
LDAP
Kerberos

HTTPS - OAuth
X OU OpenID
X GPO WS Fed.



AAD

Join vs. Registered
Company Device BYOD
In Tune Limited Access



SSPR

VM

Azure

LDAP

Kerberos

NtLm

密码重置 | 身份验证方法

Test_Test_Contoso - Azure Active Directory

诊断并解决问题

管理

属性

身份验证方法

注册

通知

自定义

本地集成

管理员策略

活动

审核日志

使用情况见解

疑难解答和支持

新建支持请求

保存 放弃

重置所需的方法数

1 2

用户可以使用的方法

☐ 移动应用通知

☐ 移动应用代码

☒ 电子邮件

☒ 移动电话

☐ 办公室电话

☒ 安全问题

注册所需的问题数

3 4 5

重置所需的问题数

3 4 5

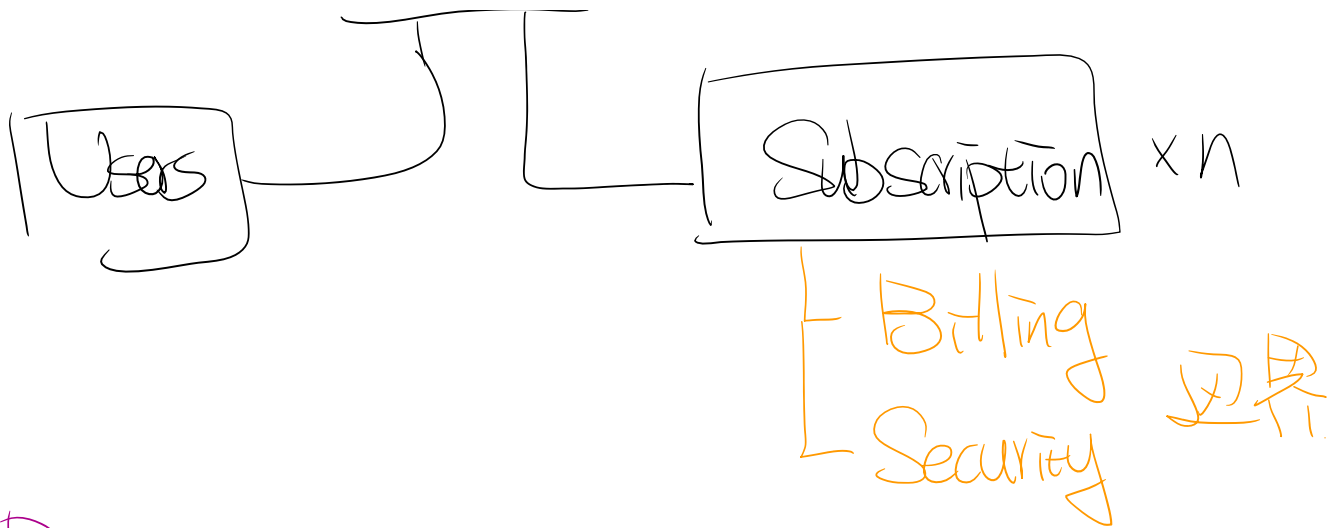
选择安全问题

AAD Global Admin

!= User Admin

X Azure Global Admin

Tenant



Region

BTOL - Hybrid Benefits

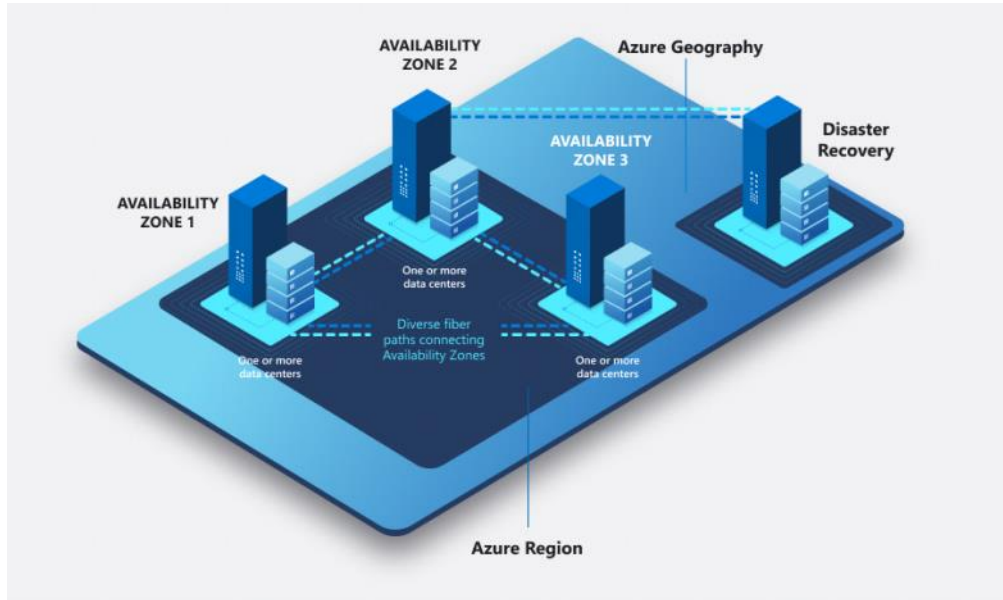
Reserved Instance $\rightarrow$ 72% off
28 \$/h

Region $\perp$ = DataCenter



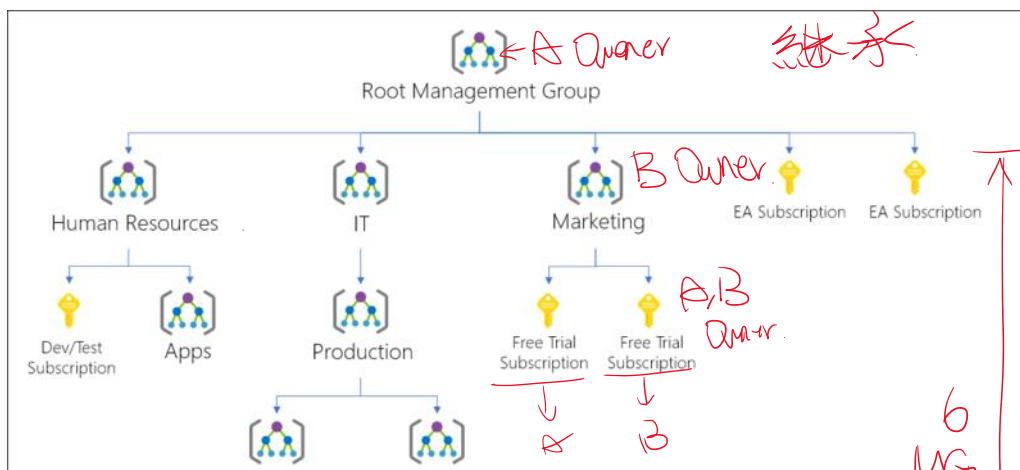
▲ Datacenter Cooling Event - Southeast Asia

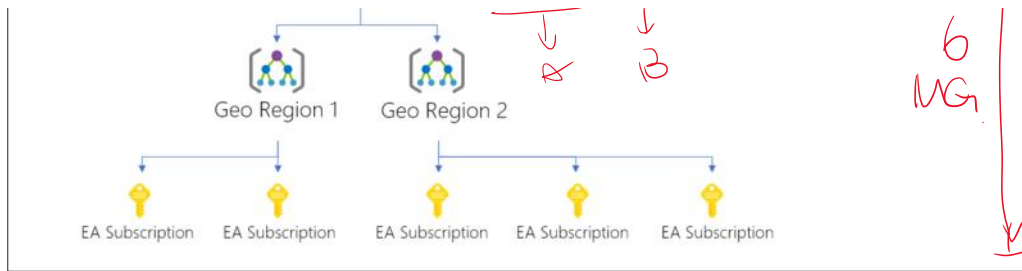
Issue Summary: Starting around 20:19 UTC on 7 February 2023, a utility power surge in the Southeast Asia region tripped all of the chiller units for one datacenter offline. While working to restore the chiller units, temperatures in the datacenter increase so we are proactively powering down compute, 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



Region Pair.

Management Group.





Tag → Metadata.

Same Policy → 規則

1. Check.

2. " + 強制

Policy [Built-in] JSON
[Custom] Import.

Initiative - Policy's Folder.

Assignment [MG
Sub ...
RG.

RBAC

Security (Service)

Principle.

Rde = 1 ~ n Permission

← Assignment →

JSON.

Owner.

Administrator

Action " * " , " * "
Not Action " Authorize / * "

Owner
Contributor

Delegation

Not ..

Assignable Scope

Administration

ARM - Azure Resource Manager

Azure Portal, - Azure Cloud Shell

Azure PowerShell - PowerShell's Module

命令式 Syntax

Cross Platform

Cmdlet v. - n.

Azure CLI - Bash

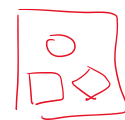
az group subgroup action

az vm create

声明式 Syntax

IaC

幂等性



ARM Template

- JSON

Parameter

- Deploy 部署

Variable

Azure DevOps - ..

Azure Bicep - Bicep → Variable
Resource — DependOn
Function — UDF
Output — PDF

Blank + VS Code Ext.
Export
Template Gallery

Networking

Virtual Network (VNET) - Addr Space - CIDR
 (SDN)
 L Independent
 L Overlapping
 L Subnet $\times n$

10.10.0.0/16

10.20.1.0/24

10.10.1.0/24, .0, .1, .2, .3, .255 $\rightarrow 256-5 \Rightarrow 251$
 10.10.2.0/28, 11 IP

↓
16

Region $\rightarrow$ *

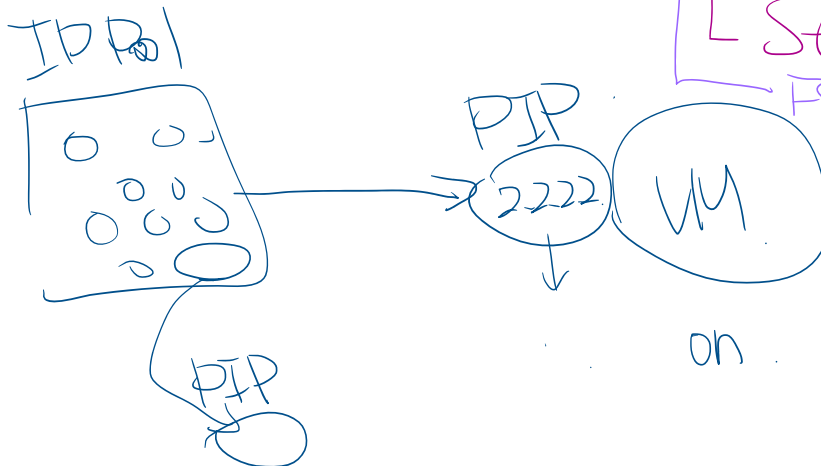
IP Private IP - Dynamic / Static

Public IP - Azure Resource

Basic Dynamic

Standard (AZ) Static

FQDN



NSG (Network Security Group)

L Network

Layer 4 FW (TCP/IP)

++ ++ ++ ++ ++

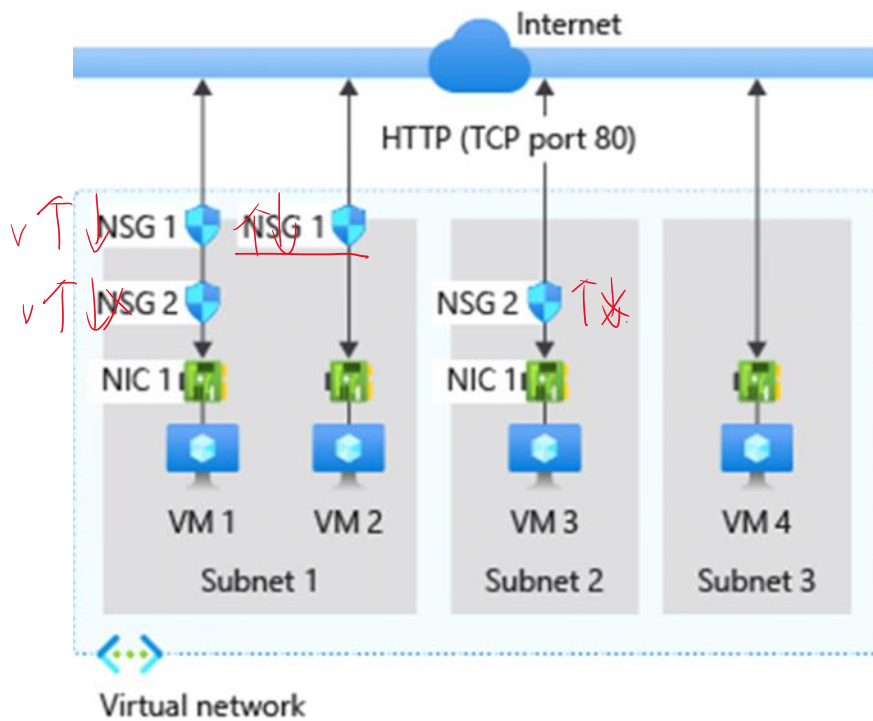
Layer 7 FW (L7/H)

- Appliance
- Subnet
- Inbound
- Outbound
- Rules x n, Priority (int) 100 ~ 4096

越小越优先

Rule 1 v RDP 450

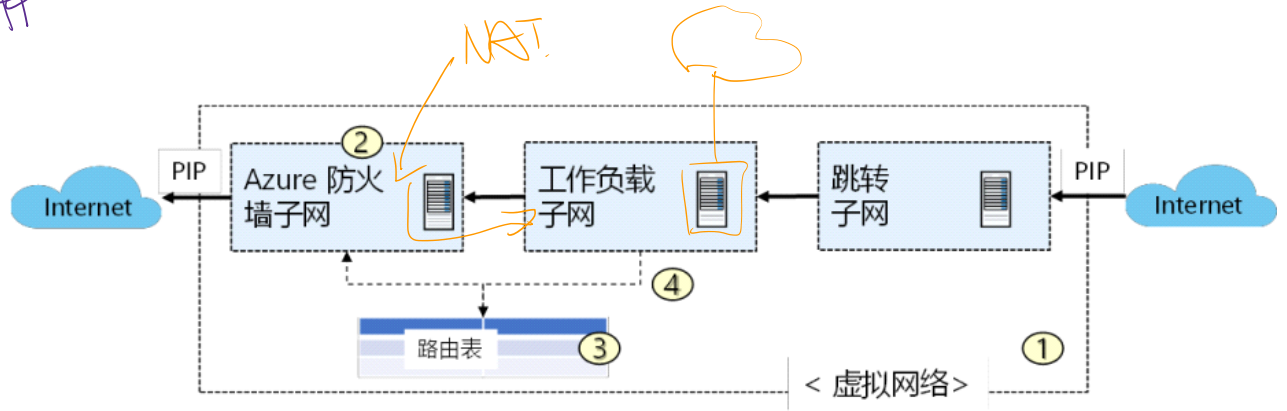
Rule 2 x RDP 300



Azure Firewall (FaaS)

- NAT
- Network
- Application
- HA
- Scale
- Layer 7 - (VM)
- Dedicated Subnet

L Application



Route — System Route ← Azure Managed

— User Define Route (UDR)

— Route Table — Route x n

— Associate to Subnet x n

Azure DNS (PaaS) < HA Scale

— Public DNS Zone dav.com

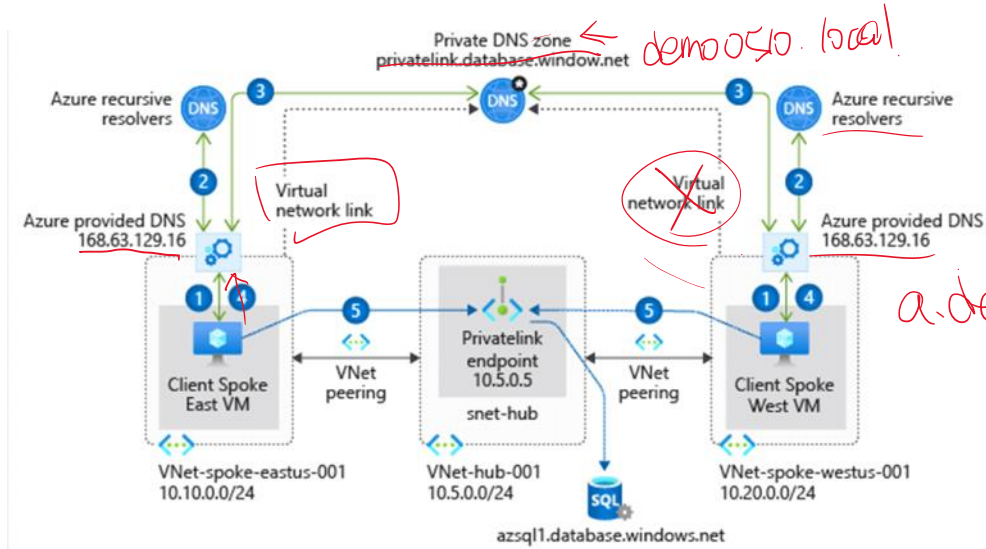
— Child Zone (Resource) .it.dav.com

↓
RBAC hr.dav.com

— Private DNS Zone — Any Name

— Link vnet x n

TV Auto Registration (Discovery)
 ↳ Auto Register Record



InterSite Connectivity

VNET ↔ VNET — Peering (对等)

VNET ↔ Other (On-Prem)
 (Other Cloud)

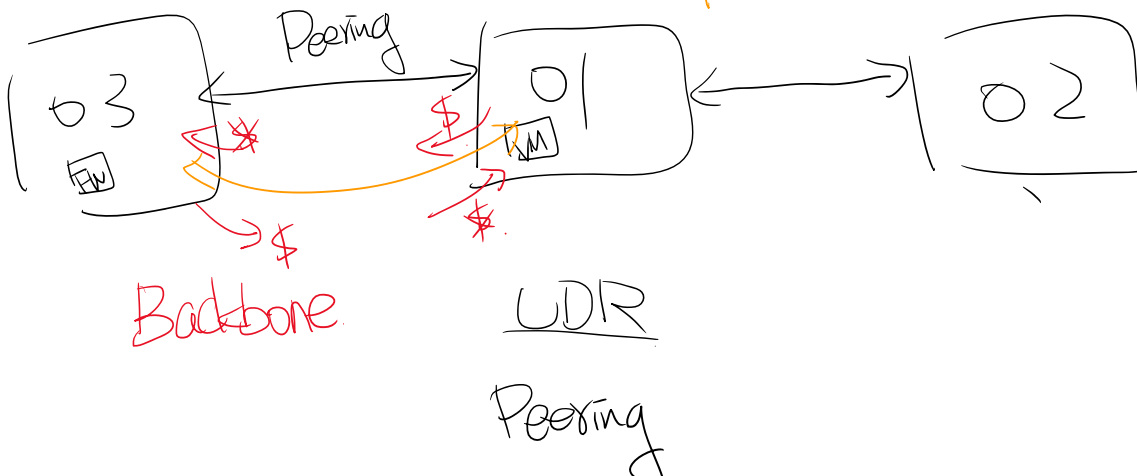
(VPN)

— 同 Region

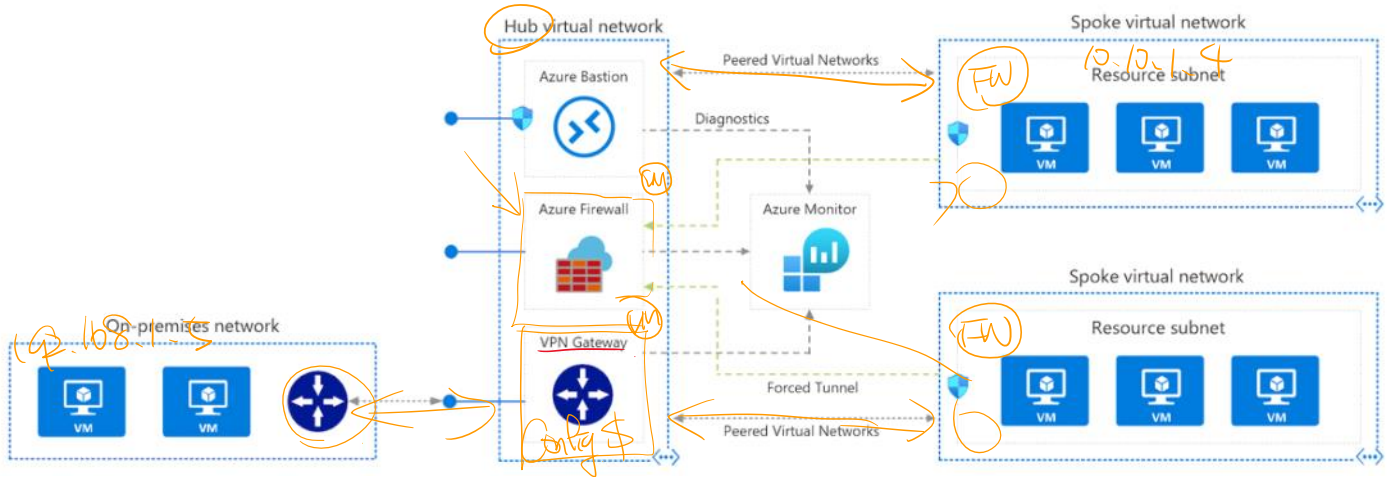
跨 Region

跨 Subs..

Hub - Spoke



Peering
V WAN



Virtual Network Gateway (VNET / VPN Gateway) (PaaS)

VPN | P2S
| S2S

HA
SKU

Express Route - ISP ↔ Azure

HA

Active - Standby

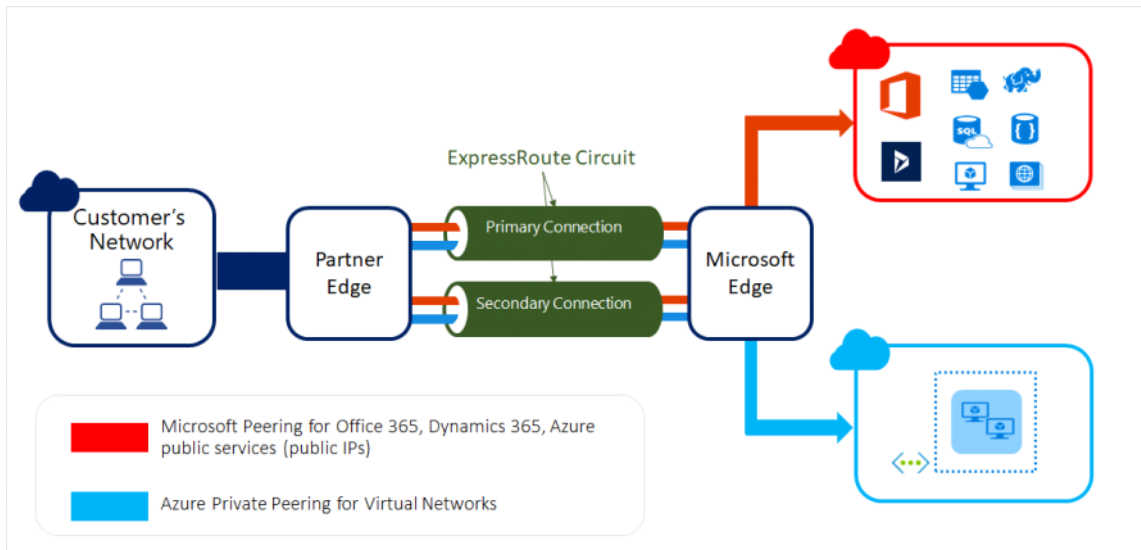
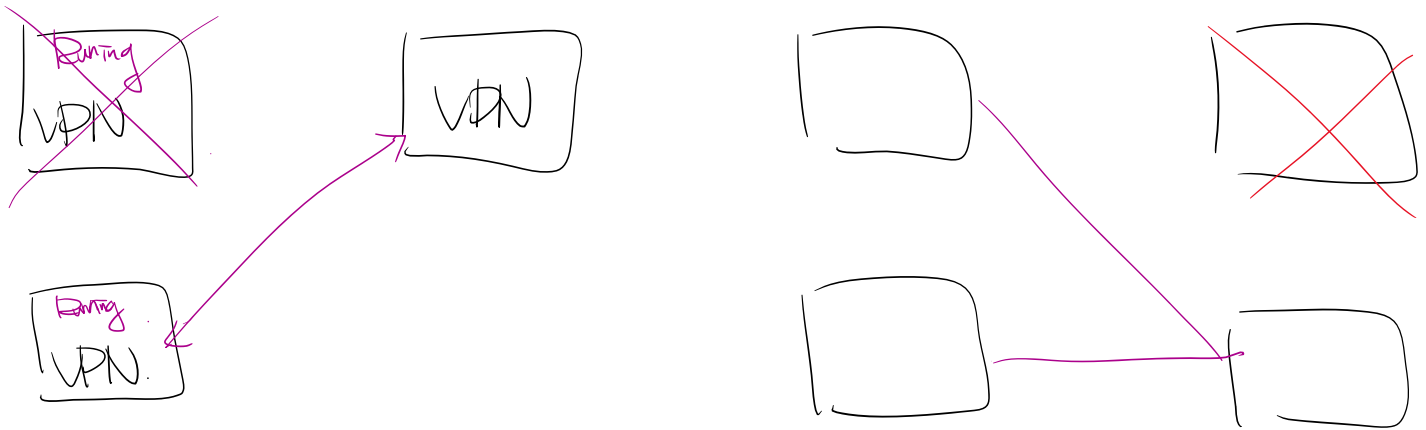
Active - Active

Azure

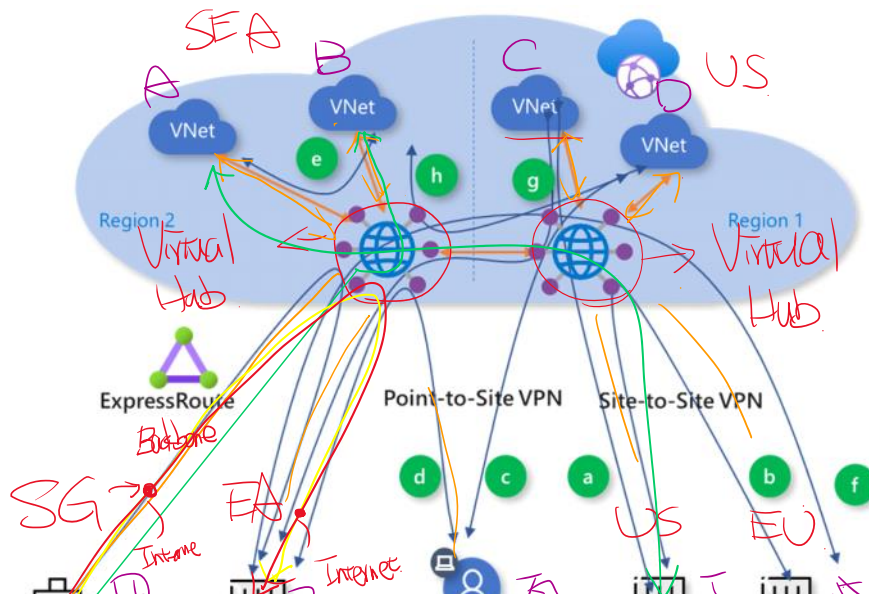
Remote

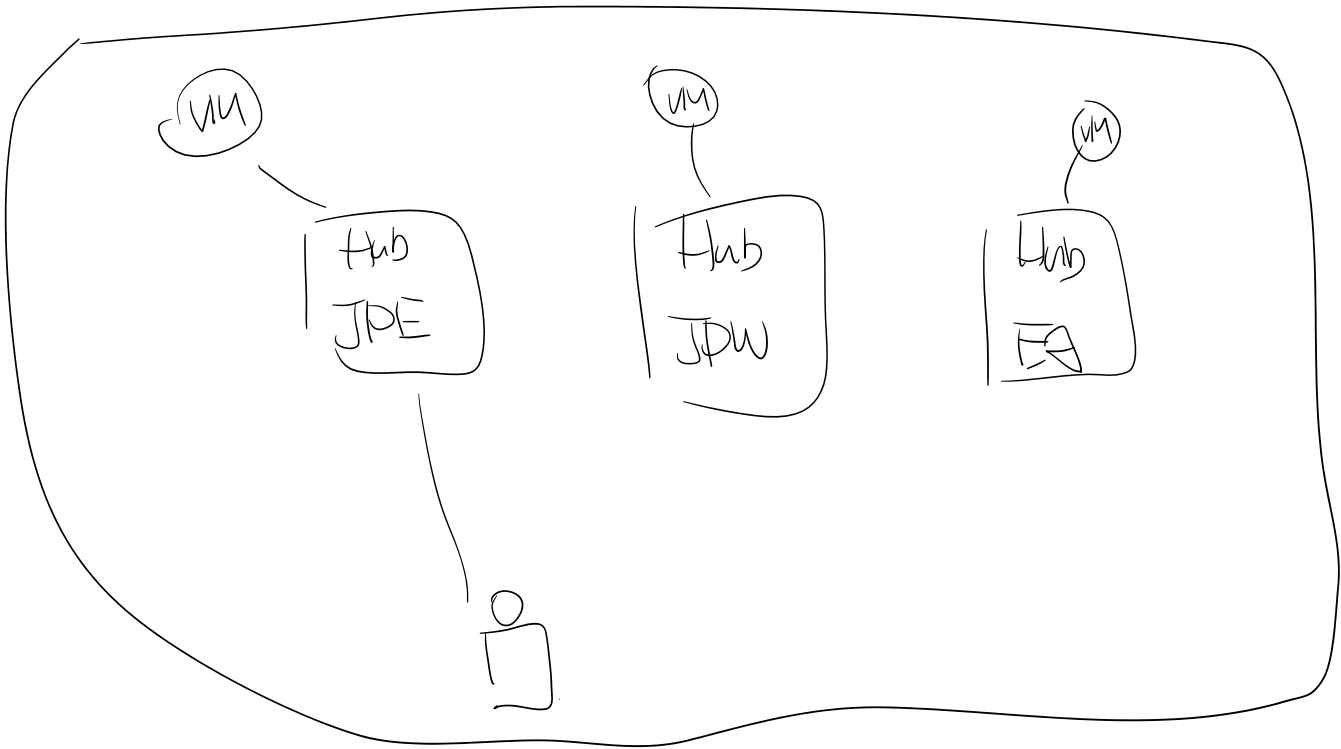
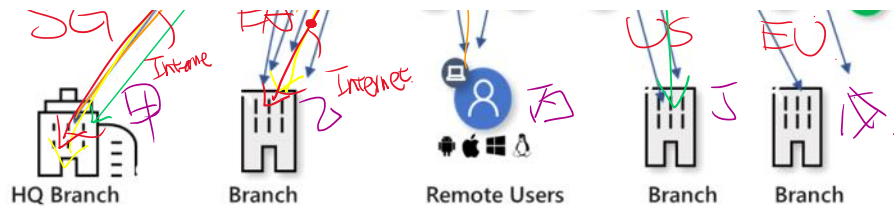
Azure

Remote



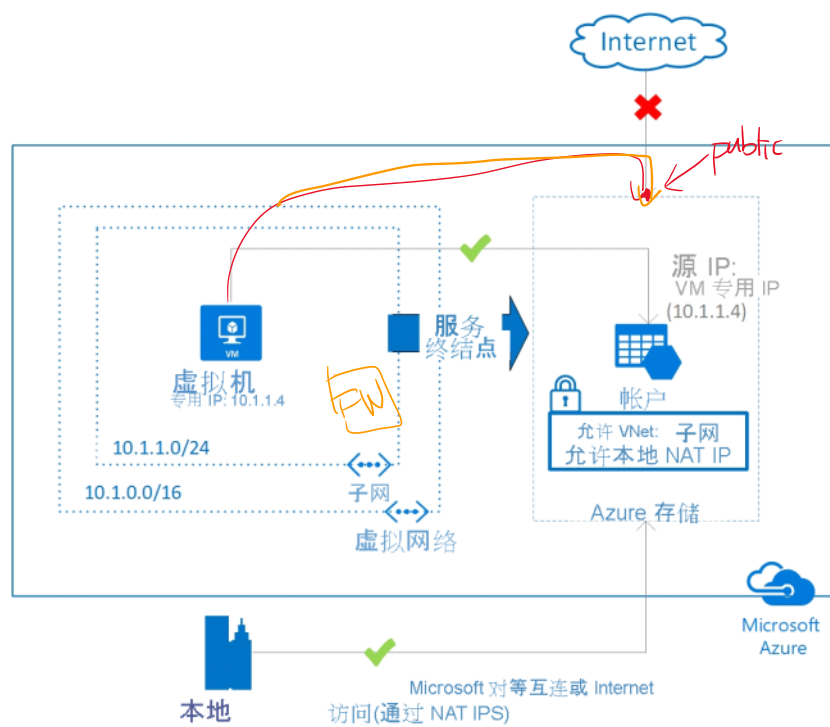
Virtual WAN

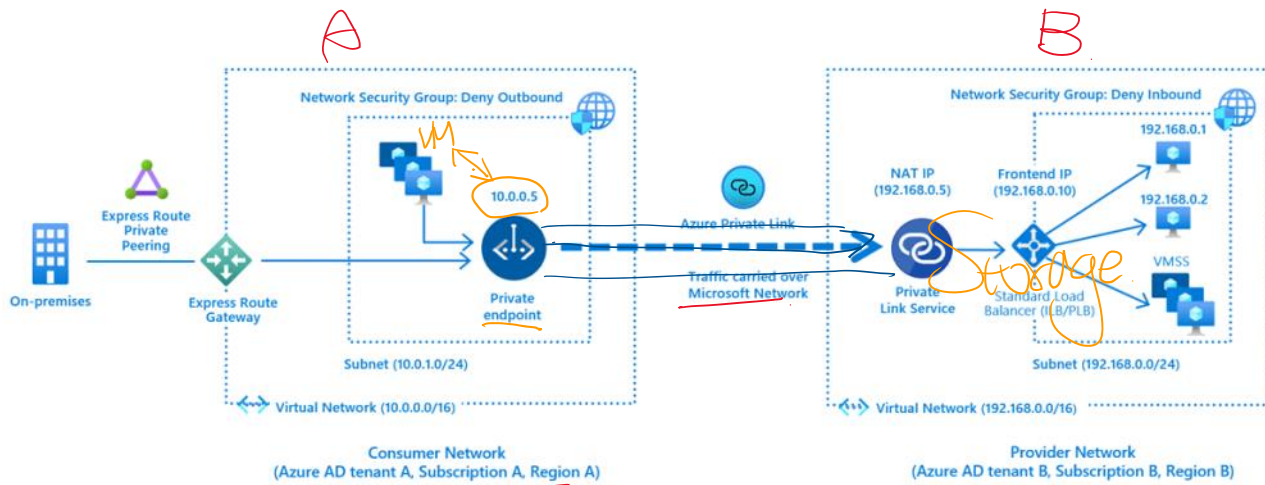




Service Endpoint

Private Endpoint / Link.





Load Balance.

Layer 7

Layer 7

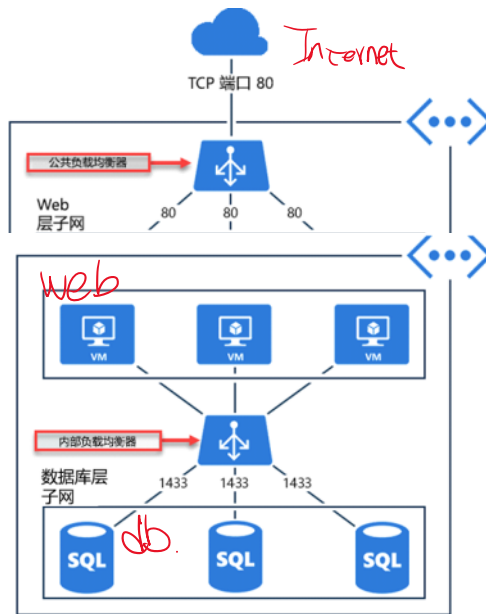
L4

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
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	

Azure LB

└ Public LB - Public IP
└ Private LB - Private IP



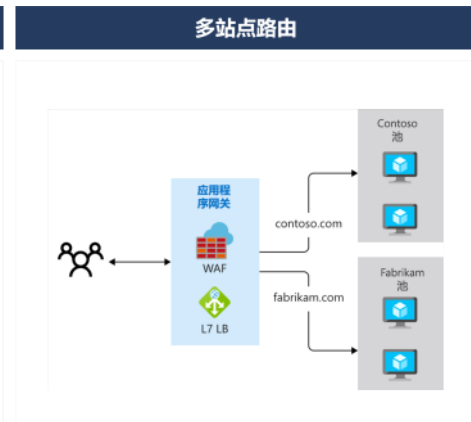
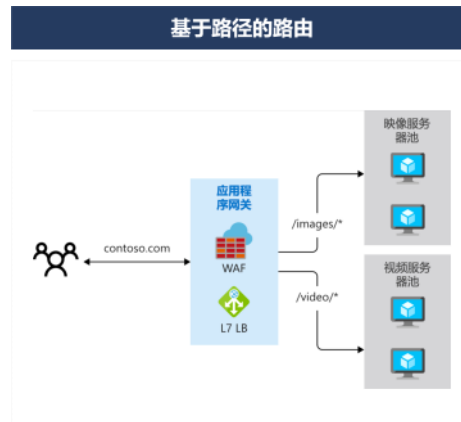
Frontend IP x n.

Backend Pool x n

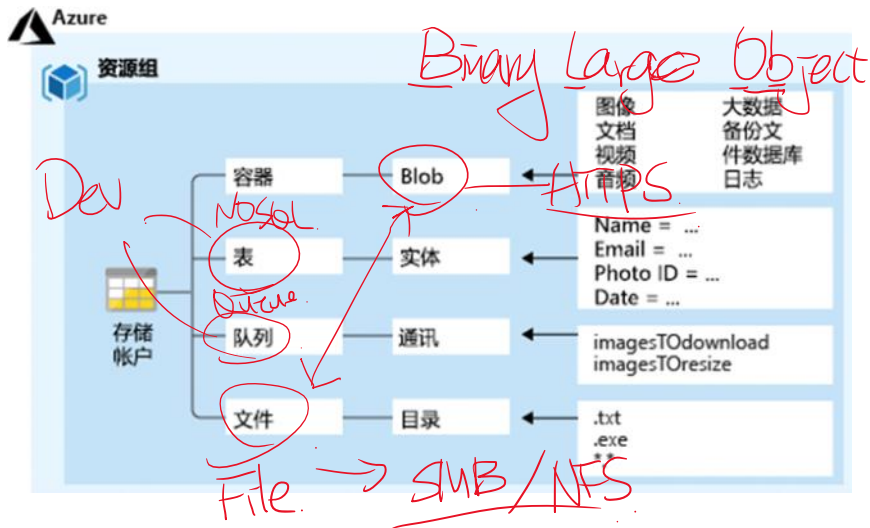
└ VM. (LB) (AG)
└ IP/FQDN (AG)

Rule.

└ Probe



Storage



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

By Mathieu Rosemain, Raphael Satter

3 MIN READ



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 - 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.

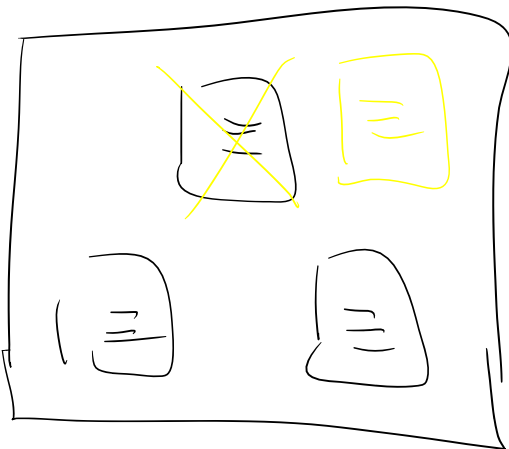
We will continue to provide updates as we have further progress towards service restoration. We will share our next update in 2 hours or as events warrant.

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

Redundancy 3 ~ 6 apps

LRS (Local)

1 Region, 1 AZ
3 apps
Zone



99.9-99%
" "

ZRS (Zone)

1 Region, 3 AZ
3 apps
Zone 1



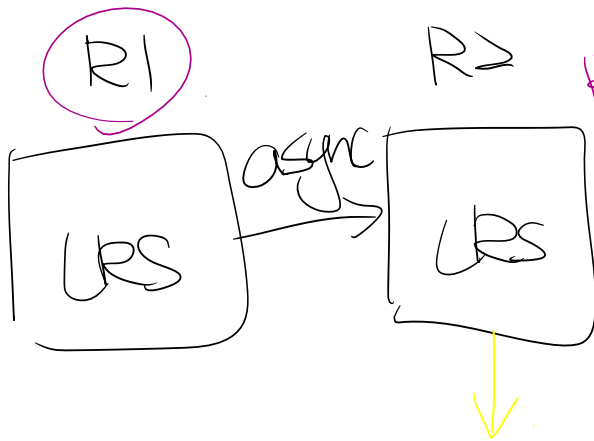
GRS (Geo) 6 apps
2x Region, 3 AZ

GZRS (Geo-Zone)

2x Region, 3 + 1 Zone

2x Region, < AZ

~ 10

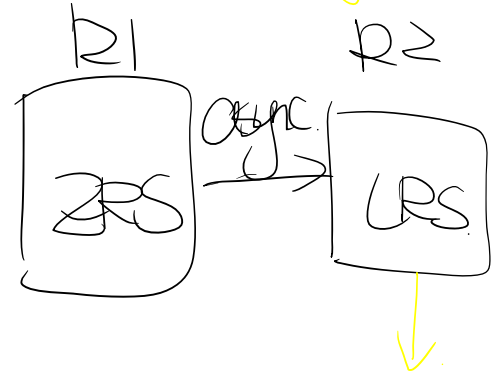


Region Pair

RA - GRS

+RA

2x Region, 3+1 Zone
60 days



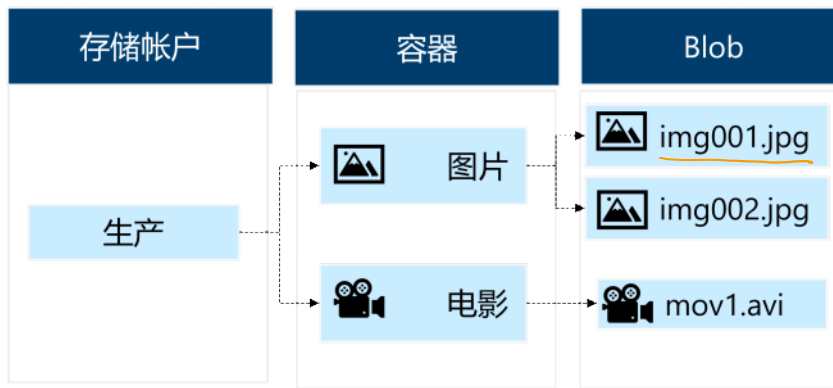
RA - GRS

Pricing = Space
Transaction

Access Tier = Hot
By Blob Cool
Archive

Default Tier = Hot, Cool
Lifecycle Management
↳ Rule x n → JSON
↳ Cooler

Container



Single Layer: 2023/01.jpg File/Name

↳ Private Access

Blob

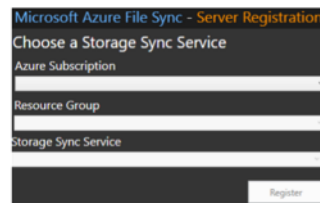
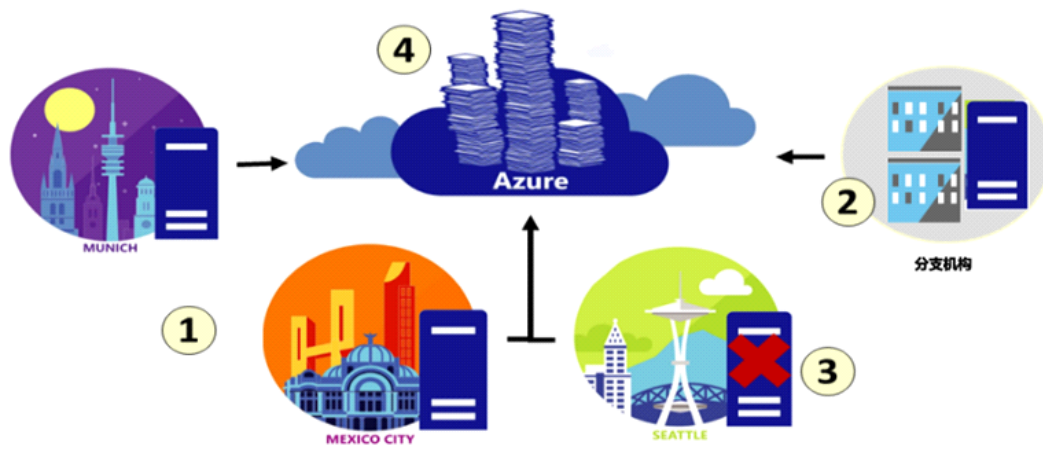
Container

<https://demo0511stor.blob.core.windows.net/images/2023/紅の豚.jpg?sp=raw&st=2023-05-08T05:51:24Z&se=2023-05-12T13:51:24Z&spr=https&sv=2022-11-02&sr=b&sig=96tFp4OPbufnUdBoaK2k7l3Oux%2FVt1iriuoWgm8y2wU%3D>

Annotations: +key 1 points to the path '2023/紅の豚.jpg'; 'Blob' points to the file name; 'Container' points to the path 'images/2023/'.

<https://demo0511stor.blob.core.windows.net/images/%E7%8C%AB%E3%81%AE%E6%81%A9%E8%BF%94%E3%81%97.jpg?si=demo0511-sas-policy&spr=https&sv=2022-11-02&sr=b&sig=HuKiuybDgCKvkxrTRuGNfl0q%2BgATNQxwWe6VhCMiNjk%3D>

+key 2 points to the path 'images/'



VM (IaaS)

- Computing
 - Shut down != Deallocated
 - Type - Series - Size
- Storage
 - Managed Disk → Azure Resource
 - UnManaged Disk, VHD → Storage Page Blob

10 VHD * 5000 IOPS

⇒ 50,000 IOPS.

VM's HA

Availability Set
(10 - AZ)

AZ ⇒ 升级

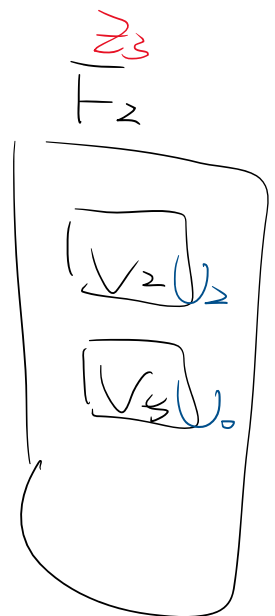
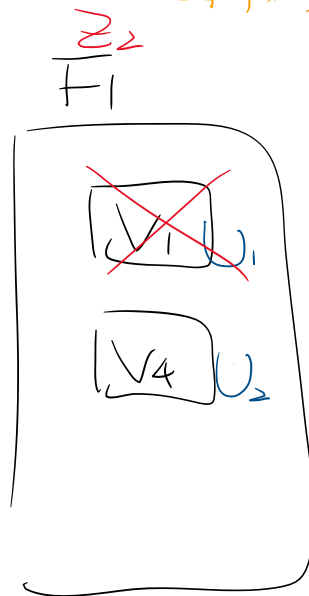
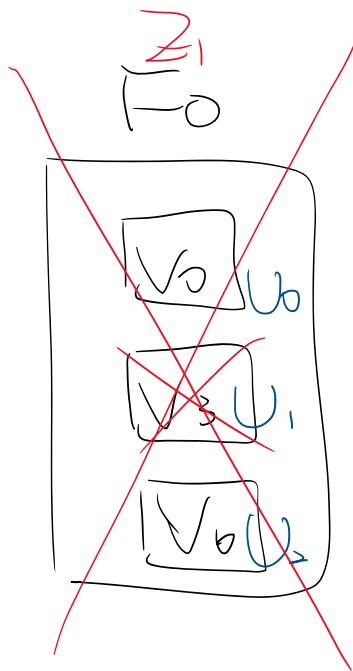
Azure Resource ← VM × n

X 1 ~ 3

Fault Domain - Hardware
容错域

x 1 ~ 20

Update Domain - Update
更新域



VM Scale Set D ~ 1000

+ HA Archi - -

+ Management

+ Scale - Manual
L Auto Scale.

Azure App Service (Web App) (PaaS)

└ App Service Plan (VMSS) ┌ HA
└ LB

└ Web App
(Sandbox Env)

Pricing / Feature

ACU - Azure Compute Unit

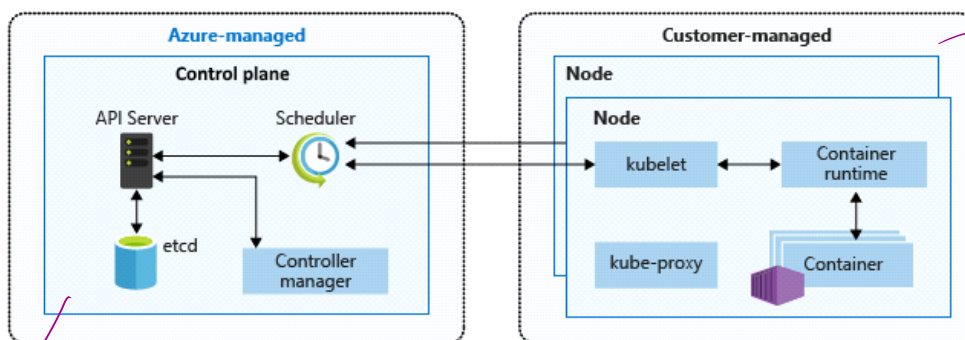
Container

└ VM
└ Web App for Container

Azure Container Registry
└ Docker Registry 2.0

└ Azure Container Instance (Simplest) ┌ Private
└ Public

└ Azure K8S Service (AKS) (PaaS)



→ $n \times \text{Resource}$

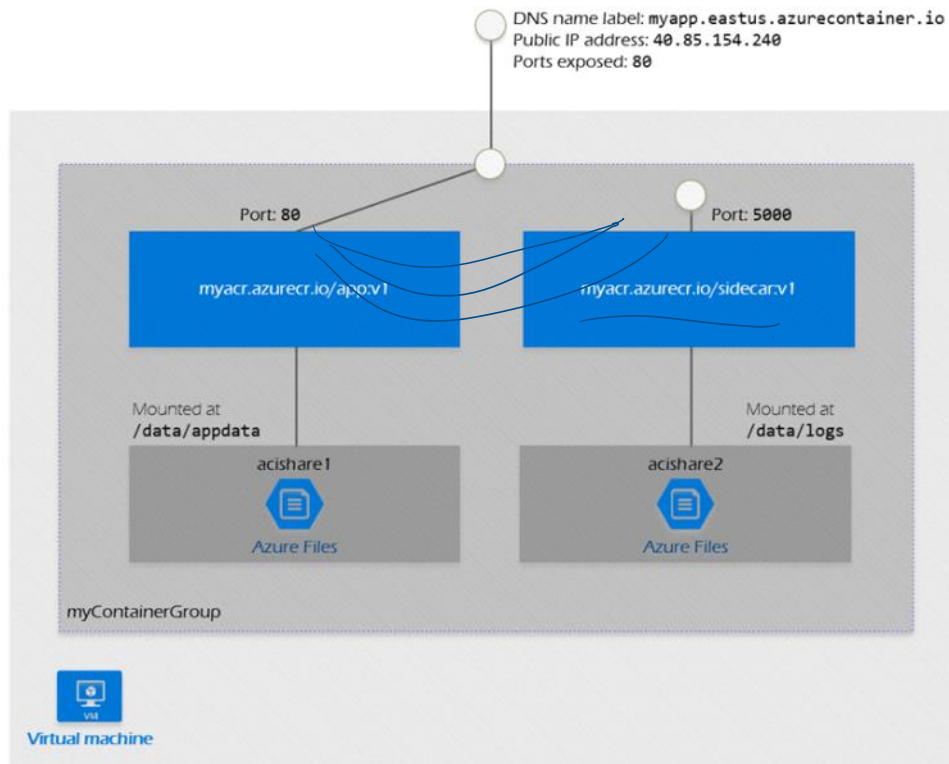
↓
Cost
(VMSS)

Pod = 1 ~ n Container

Resource

Azure Container App (KaaS)

Azure Container App (KaaS)



Backup

Azure Backup

Recovery Service Vault

DR

- 基于 Azure 的服务，用于备份和还原 Microsoft 云中的数据
- 自动存储管理
- 多种存储选项
- 无限制的数据传输
- 数据加密
- 应用程序一致性备份
- 长期保留

组件	优点	限制	保护	备份存储
Azure 备份 (MARS) 代理	• 备份物理或虚拟 Windows OS 上的文件和文件夹 • 无需单独的备份服务器	• 每天备份三次 • 非应用程序感知 • 仅限文件、文件夹和卷级还原 • 不支持 Linux	• 文件 • 文件夹	• 恢复服务保管库
Azure 备份服务器 (MABS)	• 应用感知快照 • 备份时间完全灵活 • 恢复粒度 • Hyper-V 和 VMware VM 对 Linux 的支持 • 备份和还原 VMware VM • 无需 System Center 许可证	• 无法备份 Oracle 工作负载 • 始终需要实时 Azure 订阅 • 不支持磁带备份	• 文件 • 文件夹 • 卷 • VM • 应用程序 • 工作负载	• 恢复服务保管库 • 本地附加磁盘

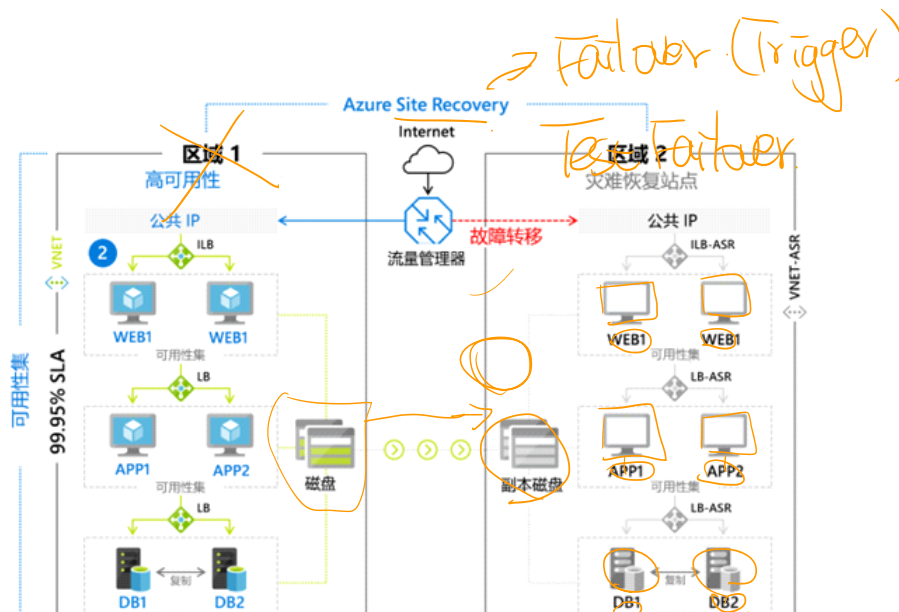
实现 Azure Site Recovery

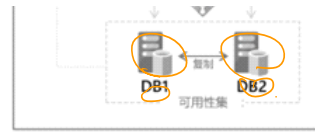
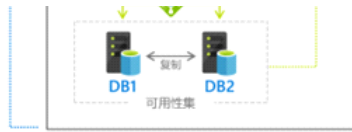
将 Azure VM 从一个 Azure 区域复制到另一个 Azure 区域

将本地 VMware VM、Hyper-V VM、物理服务器 (Windows 和 Linux)、Azure Stack VM 复制到 Azure

将 AWS Windows 实例复制到 Azure

将本地 VMware VM、System Center VMM 管理的 Hyper-V VM 和物理服务器复制到辅助站点





Azure Monitor. — Service

Azure Log Analytics workspace

↳ Resource

↳ Built-in

7~35天 - 90天

↳ LTR → Export

[Metric] Tables
[Log]

KQL (Kusto)

↳ SQL like logic