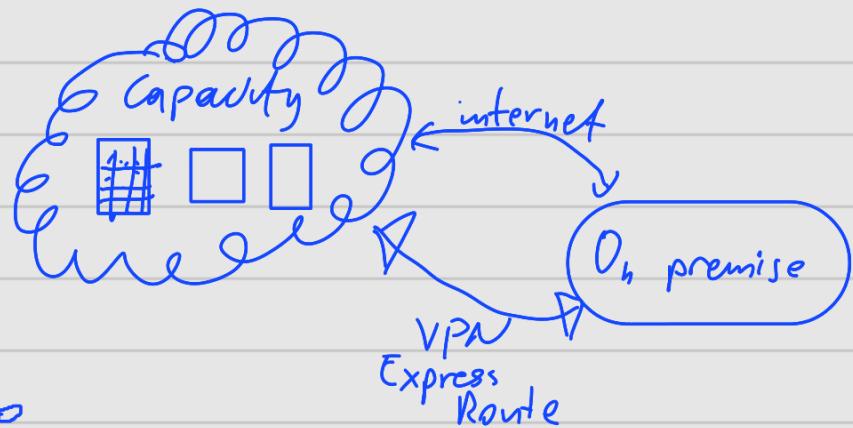
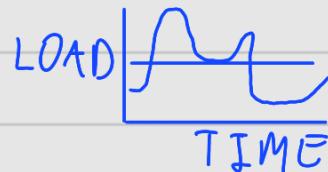


## Benefits of cloud:

Cloud :  
↓  
multitenant



- Pay as you go
- Segmentation between customers
- Access usually from the internet
  - ↳ Private connectivity possible too (ie Express Route)
- Cloud is agile
- Region agility
- High Availability
- Disaster Recovery
- Scalability



CapEx, OpEx: - Capital Expenditure (on premise, buy equipment)  
- Operating - (cloud, pay as you use)

Opex: consumption based, pay only when used  
Capex: Buy the assets

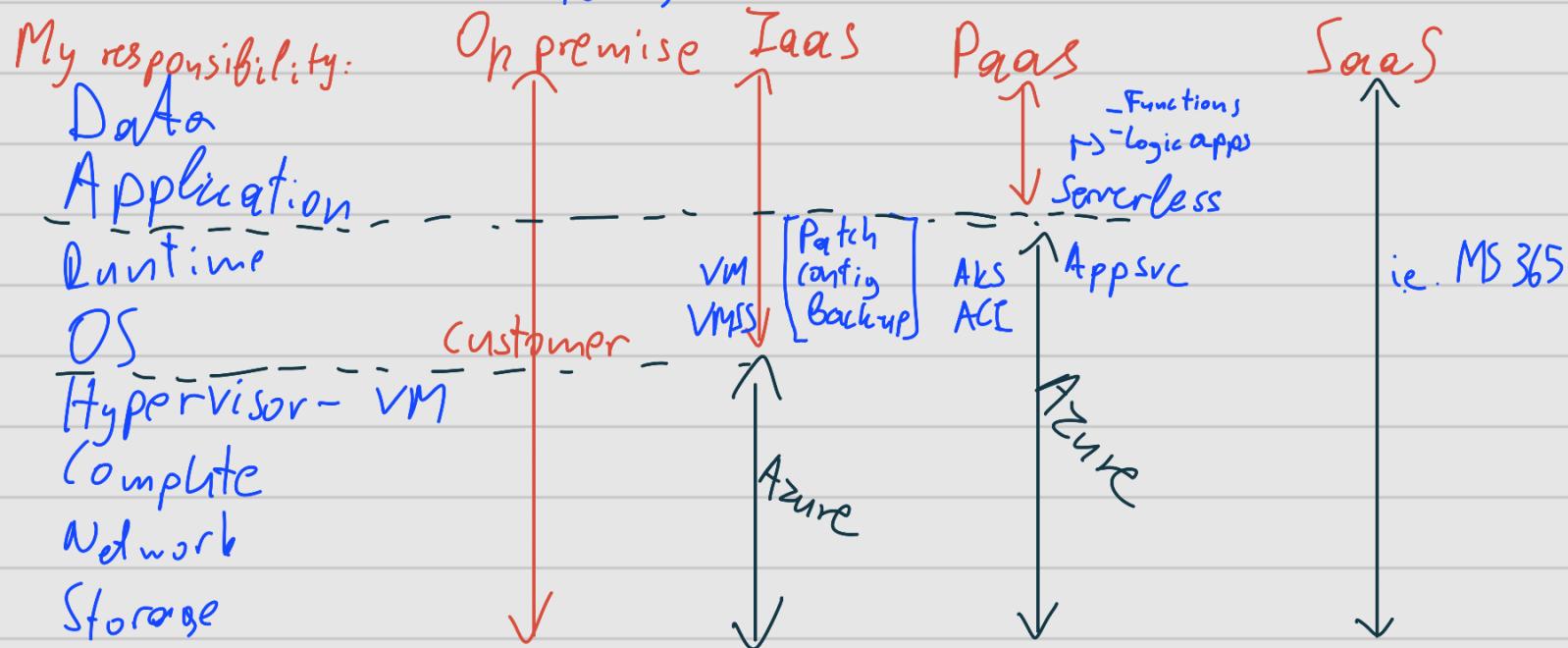


## Categories of cloud services:

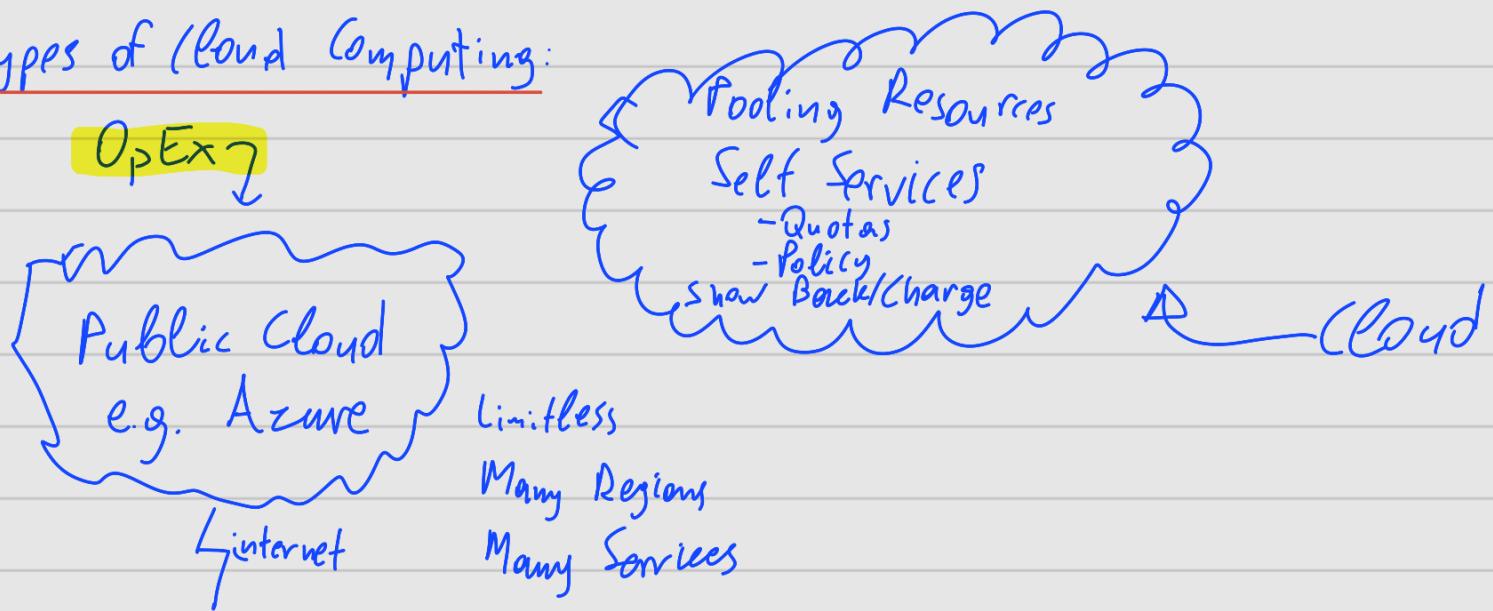
layers:

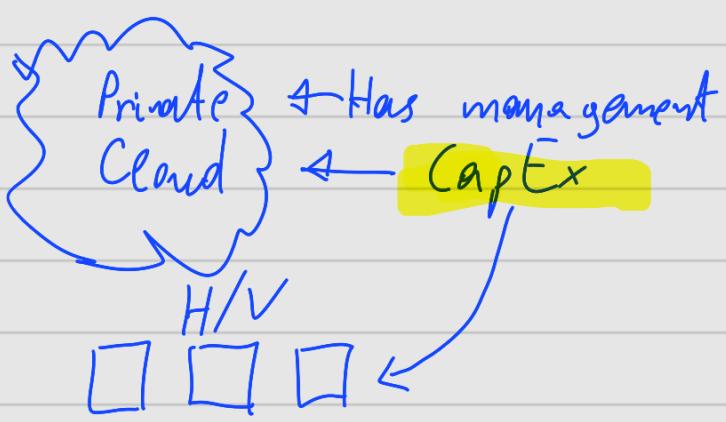
Data Application Runtime OS

Hypervisor - VM  
Complete Network  
Storage



## Types of Cloud Computing:





## Hybrid : Public + Private

### Reliability / Predictability :

#### Reliability:

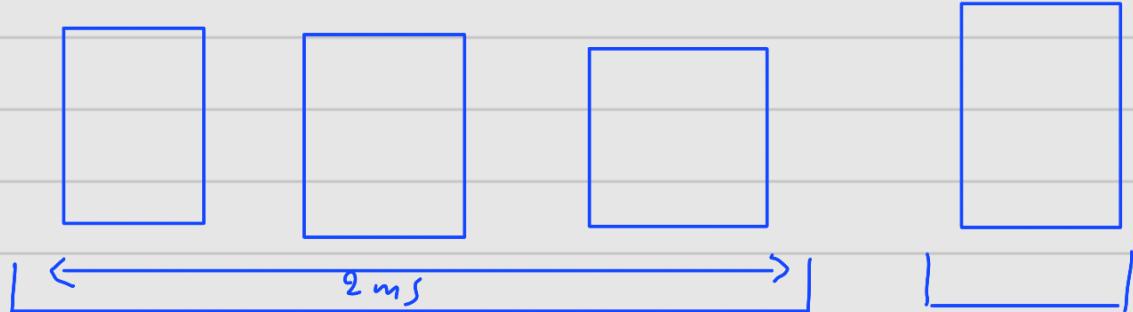
- Public cloud has auto-healing
- Storage x3
- Autoscale
- SLA
- Design for failure
- Monitor

#### Predictability:

- SKU
- ACU (Azure Compute Unit)
- Behavior
- Use Templates
  - ↳ Automation
  - ↳ Devops

### Region / Region Pairs:

Data Centers:



Region ie East US

Region West Coast

- ``Get-AzEnvironment``: Shows German Cloud, Azure, China Cloud
- ``Get-AzLocation / ff``: Shows the regions we can use

- I can pick any region I want
- Pick regions far apart for resiliency

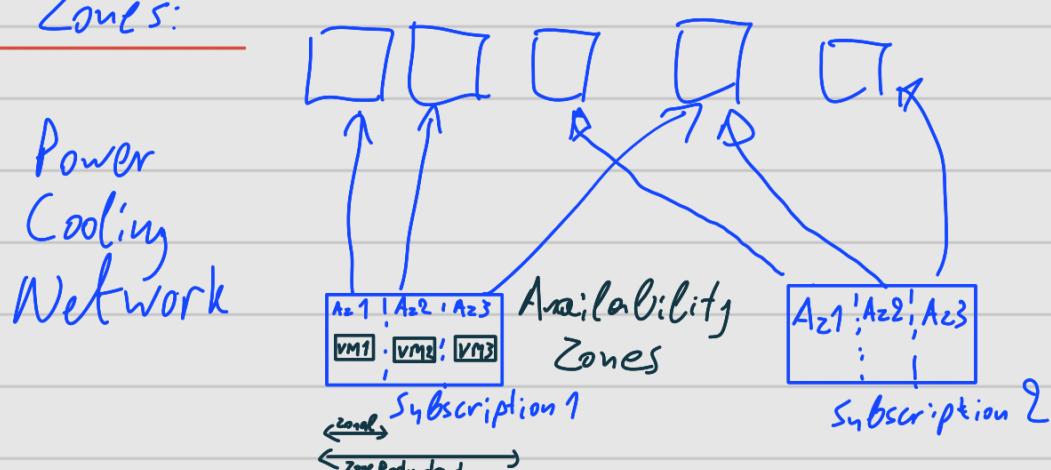
### Regions:

- Performance
- Regulatory
- Data Resiliency

Replication pairs: Same region, but far away

- Resiliency
- is used by Azure but also by us

### Availability Zones:

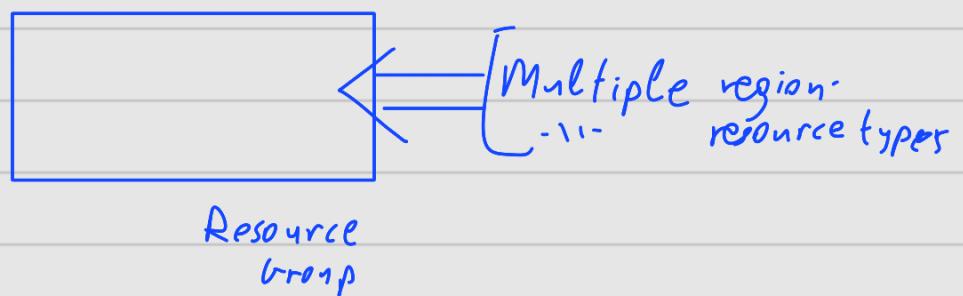


- I can select 1, 2 or 3 availability zones
- Create resiliency for a building level problem
- Can withstand platform or region going down

Zonal: 1 Availability Zone

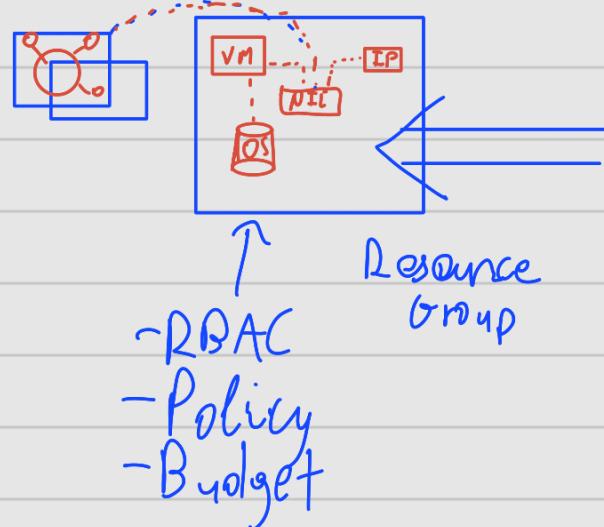
Zone Redundant: Spans 3 zones automatically

## Resource Groups:



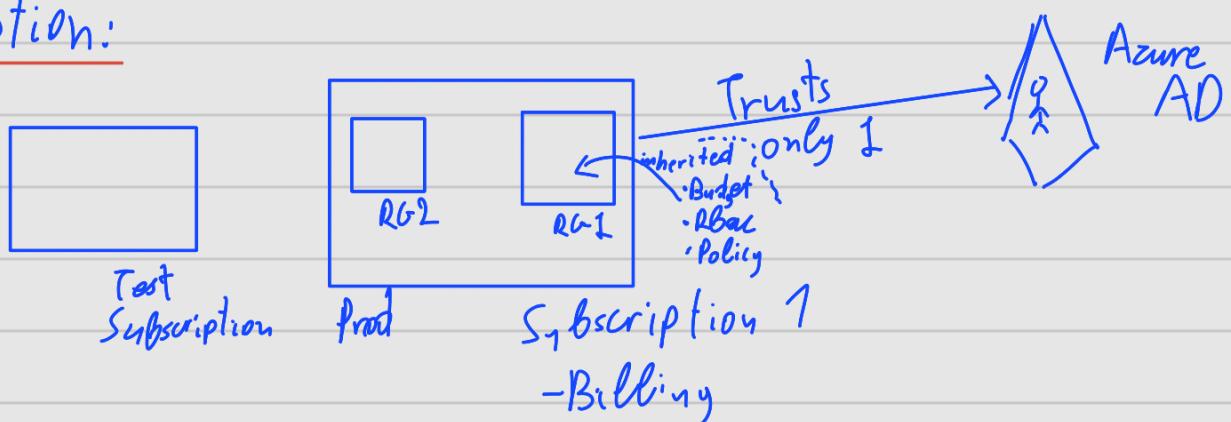
- Cannot put a resource group into a resource group

## Resource Groups:



- Multiple regions
- Multiple resource types
- Cannot have a resource group inside a resource group
- Share lifecycles
- has tags

## Subscription:



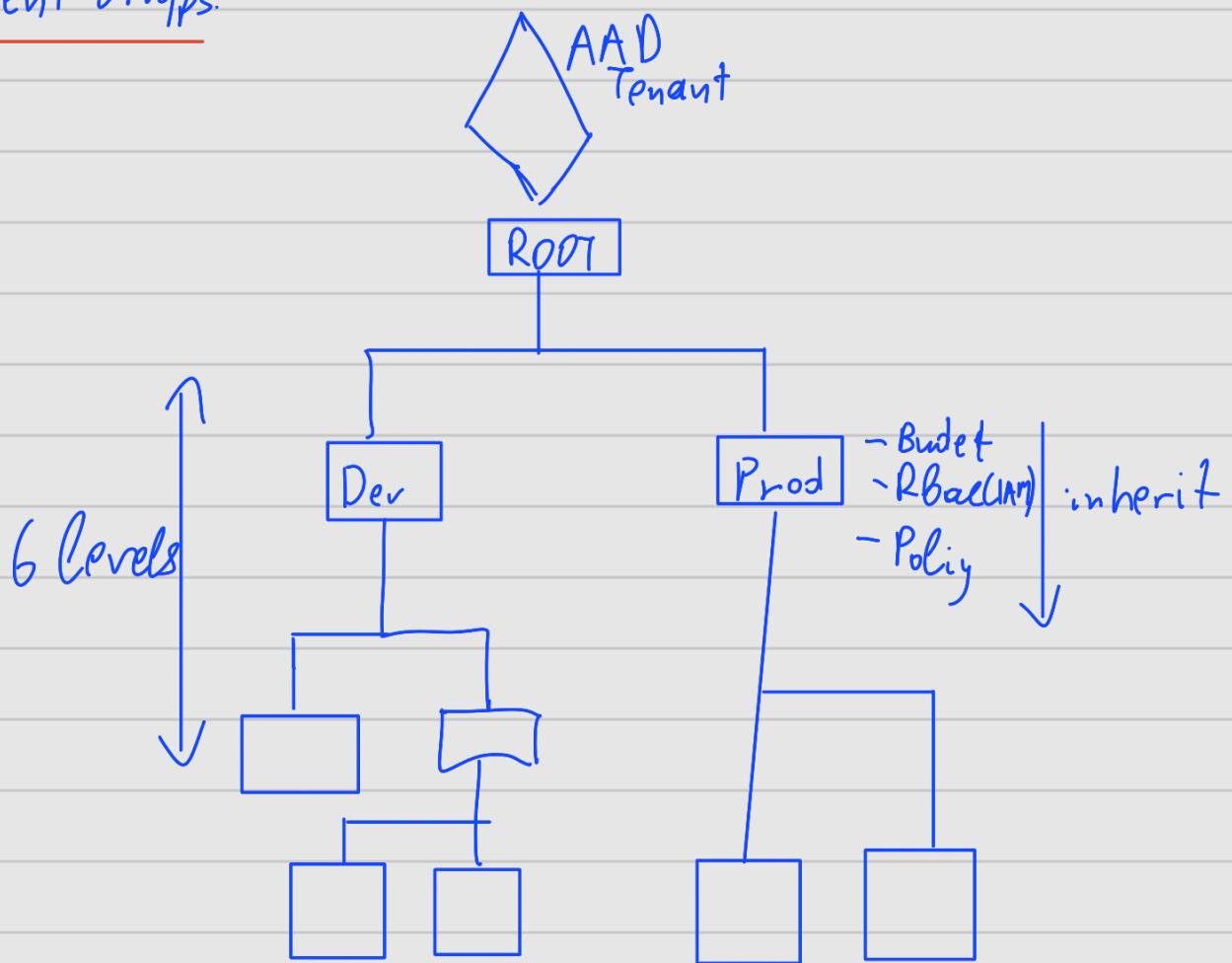
- I can apply:
  - Budget
  - RBAC
  - Policy
- Has one or more subscription groups
- Has limits

Separate Based on environments

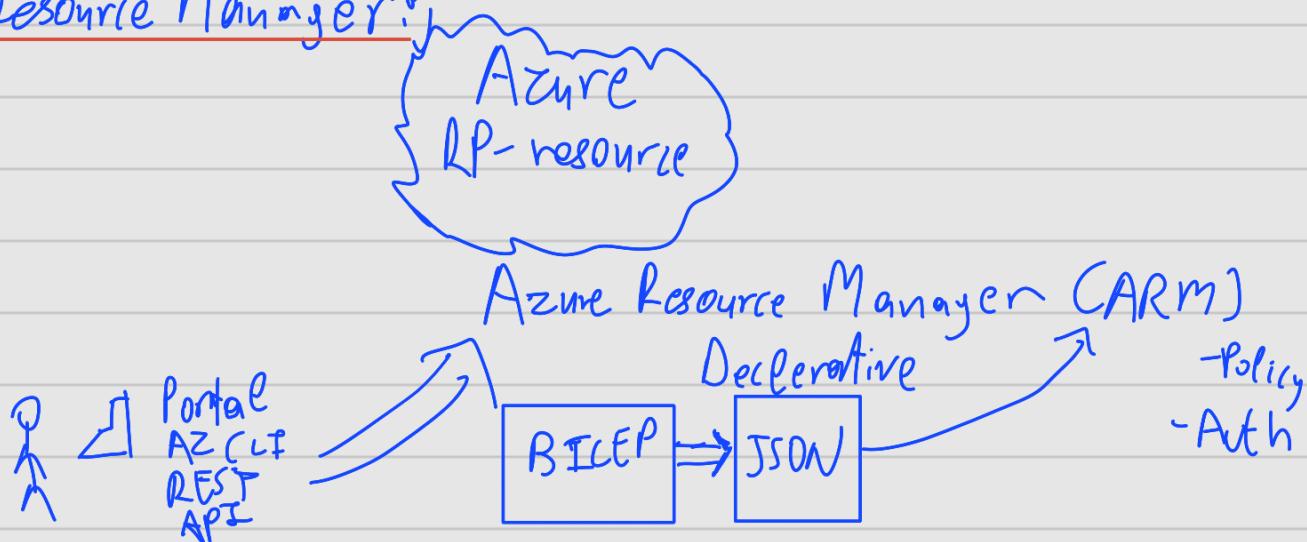
- Billing
- Units

Management Groups:

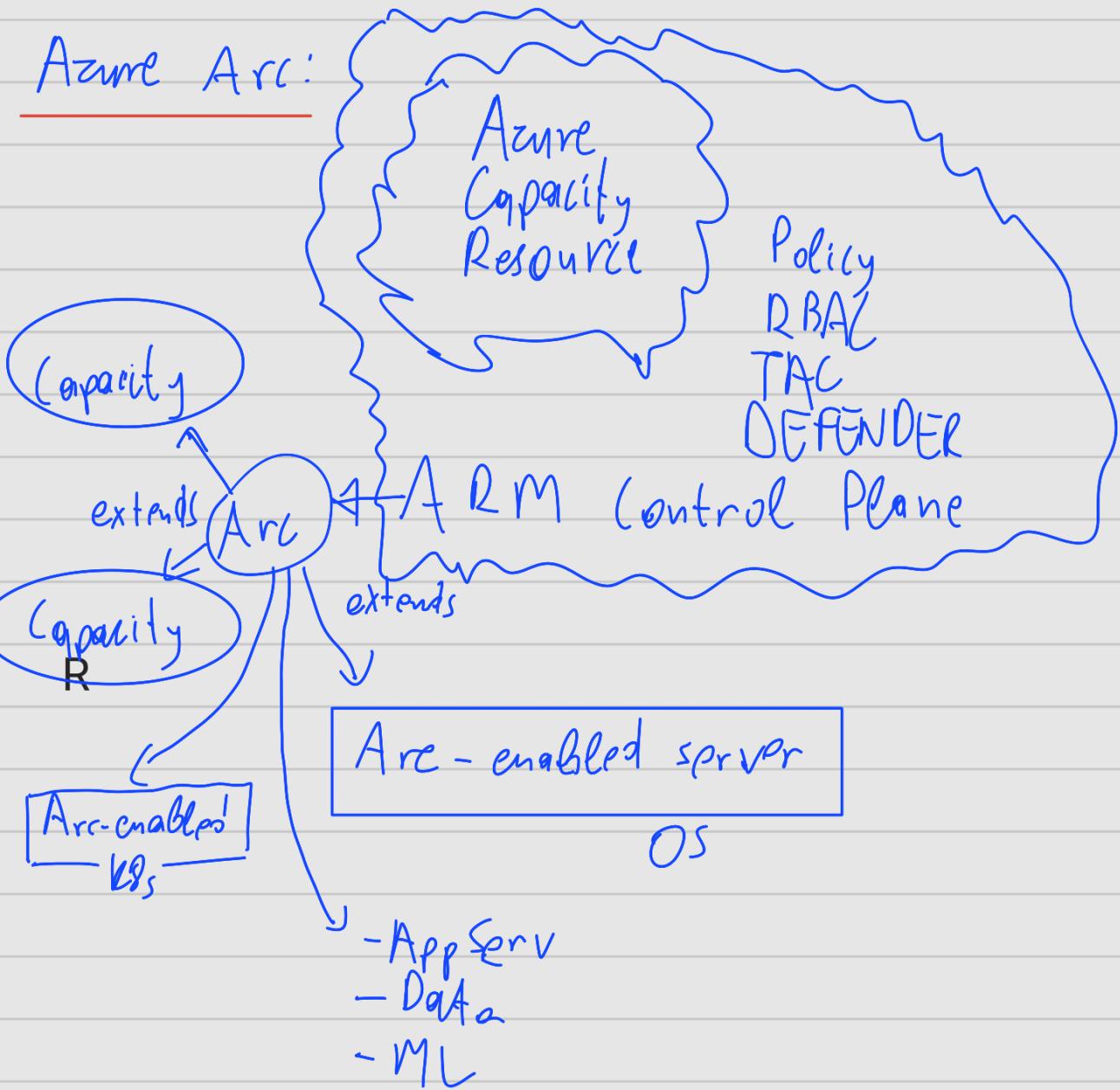
Groups :



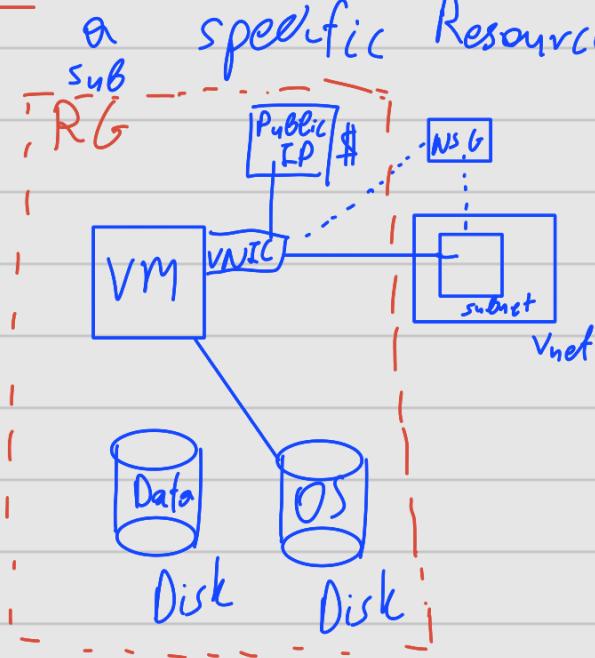
Azure Resource Manager:



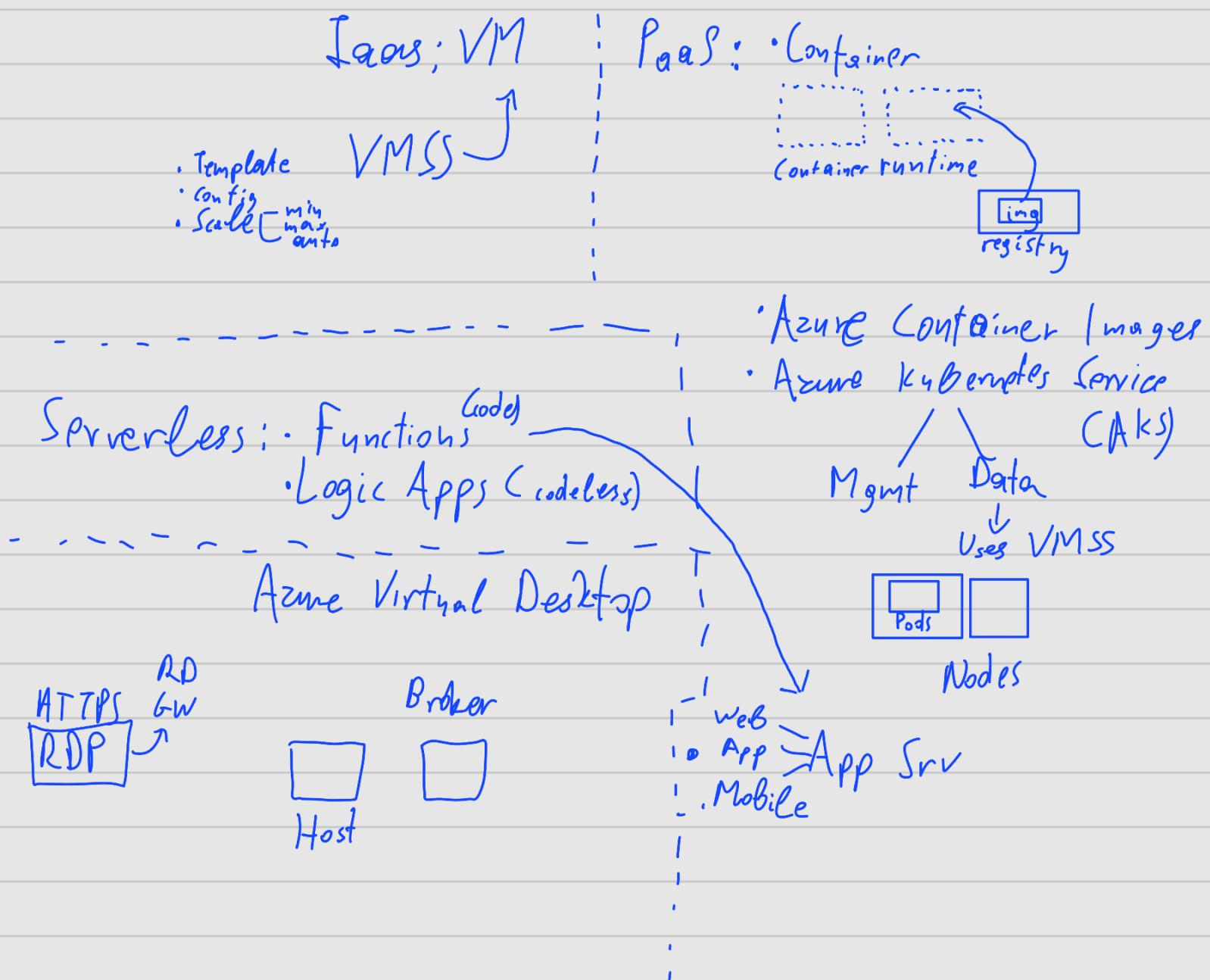
## Azure Arc:



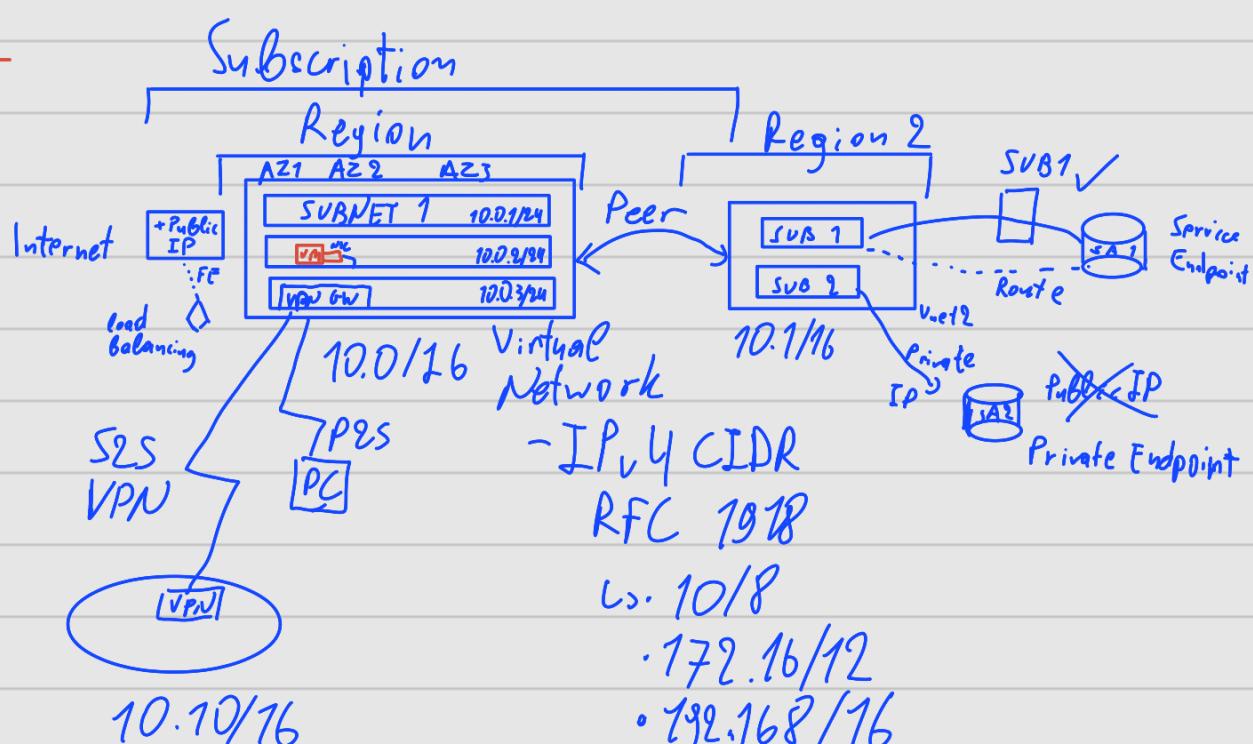
Resources for VM: - A VM lives inside a subscription, inside a specific Resource Group



## Core Compute: • Ratios for FaaS



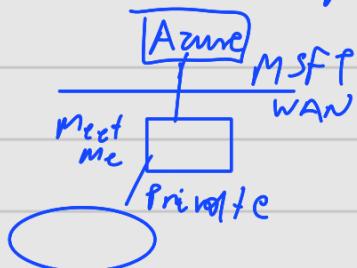
## Core Network:



## [IPv6 CIDR]

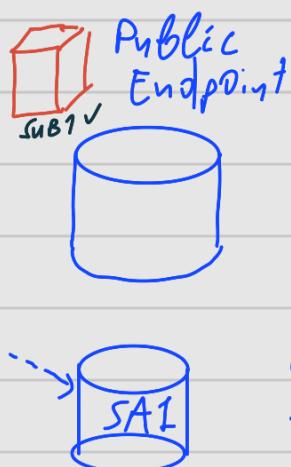
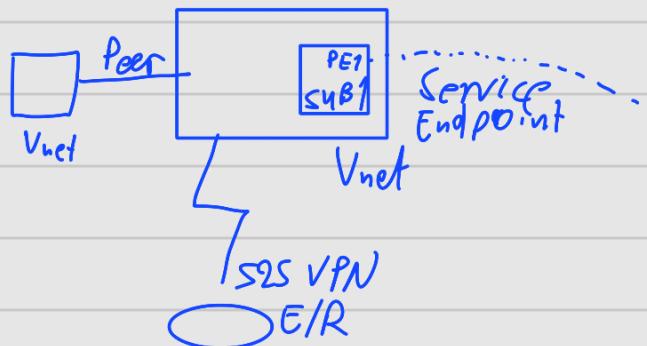
- You always loose 5 IP addresses per subnet
- We have 2 VPN GW: - Policy (static, don't use)  
- Route Based (P2S, better)
- With multiple VPN gateways:
  - Active-Active (multiple IP)
  - Active-Passive

• Express Route:



- Private Peering: Express Route Based, I have an ER GW
- Microsoft Peering
- Make sure the IP range used is unique

Public and Private Endpoints:



Can communicate from the private endpoint

Storage Account:

- Lives in a region
- Good practise: create in the same region with the other VM components

acct type:  
GPv2      STD  
                prem ] performance

acct type:  
- block blob      Files  
- Page blob

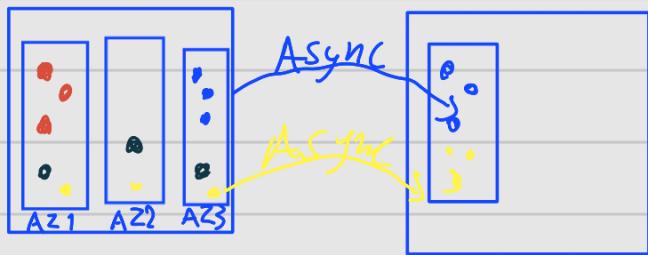
• Redundancy  
 ↘ ↘  
 LRS

LRS: 3 copies of data in the same Building

ZRS: 3 copies, 1 in each AZ

GRS: 3 copies in an AZ + async 3 in another region AZ

GZRS: 3 copies, 1 in each AZ + async 3 in another region AZ



LRS x 3

ZRS x 3

GRS 3+3

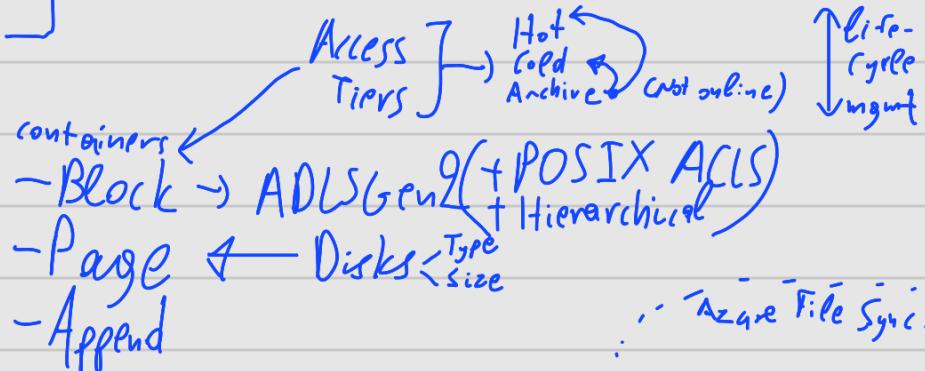
] premium available

std available

GZRS 3+3

[+RA]

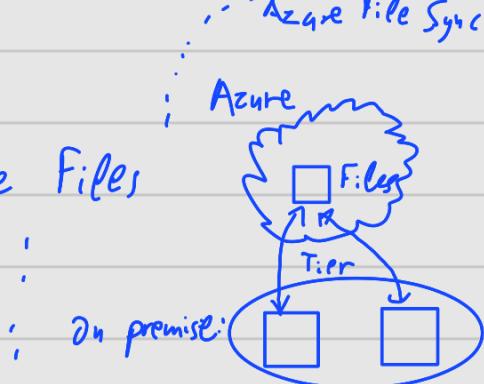
Services:



Files: - SMB / NFS Share Files

Queries: FIFO

Table: Key:Value



Databases: - SQL → SQL Server - Relational DB

- Fixed Schema  
(columns)



Offerings: - Azure SQL DB (PaaS)

- Azure SQL Managed Instance  
(In your Vnet, compatibility)

Open Source: - MySQL ] Managed  
- PostgreSQL ] Database

- Citus ↗ multi server  
X ↗ Sharding Data

- Cosmos DB

↳ Multi Model

• Multi Consistency

Document, SQL, mongo

column - Cassandra

graph - Gremlin

Movement n' Migrations:

Azure

Files → Cloud Endpoint (x 1)



↳ Sync Group



Former Endpoints  
(<10)

- Move  
- Sync ↗  
Azure  
File  
Sync

(+ Cloud Tiering)

Azure Storage Explorer: interact w/ content and file  
↳ shares  
↳ interactive

Az Copy: · Automation

· Copying

· Cloud ↔ Cloud (too)

↳ Happens in server side

Azure Migrate: ↳ VM / I/O S



Azure Data Box: · Disk

↳ importing

· Box (80 TB)

↳ import/export

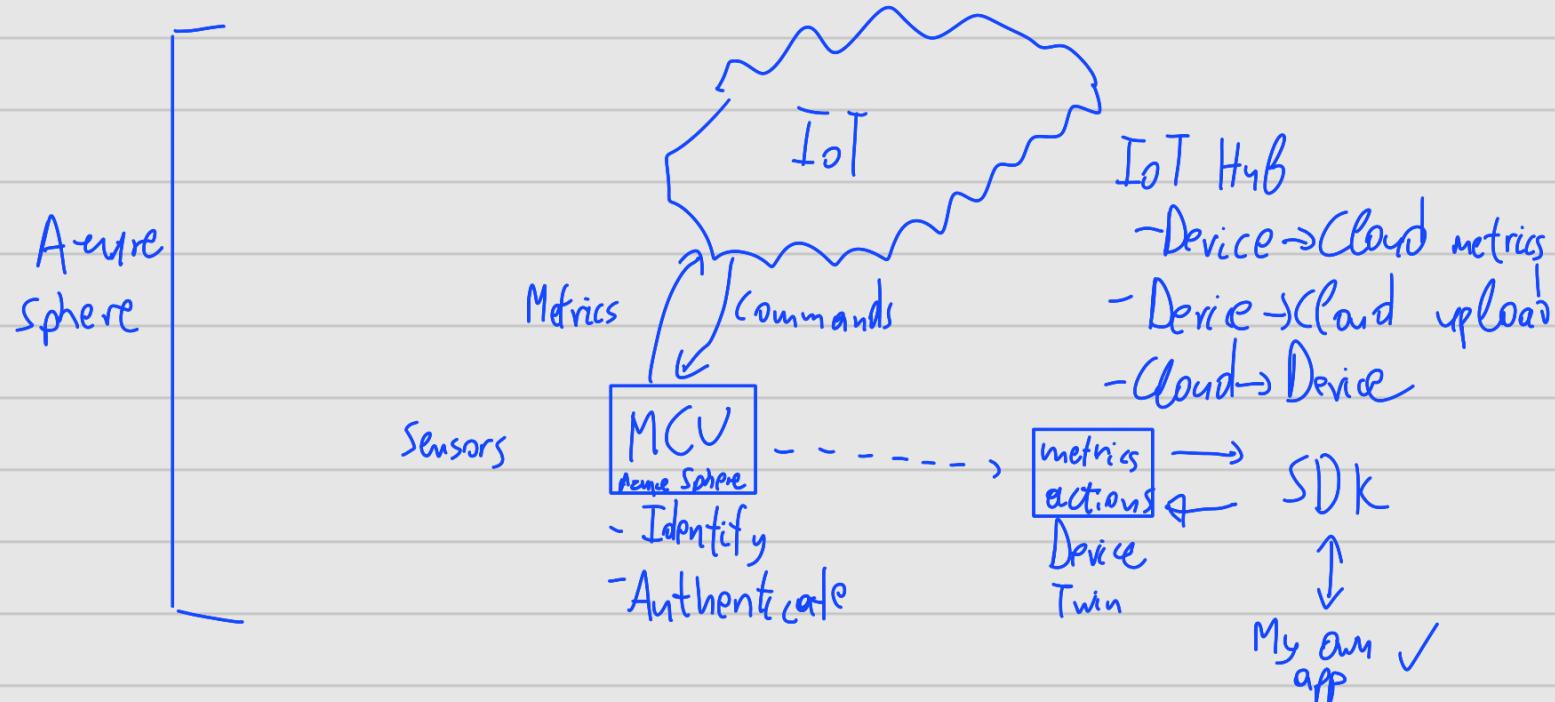
· Box Heavy (770 TB)

Market place:

· Licensing

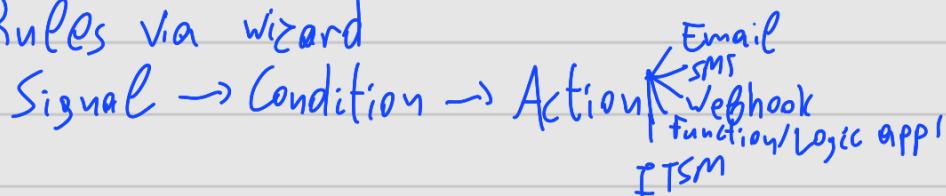
· BYO - license or buy from Azure

IoT Services:



IoT Central - - - - - <sup>uses</sup> IoT Hub (PaaS)  
(SaaS)

- Dashboards/apps
- Templates for devices + Simulated
- Common industry scenarios
- Full customize
- + Rules via wizard

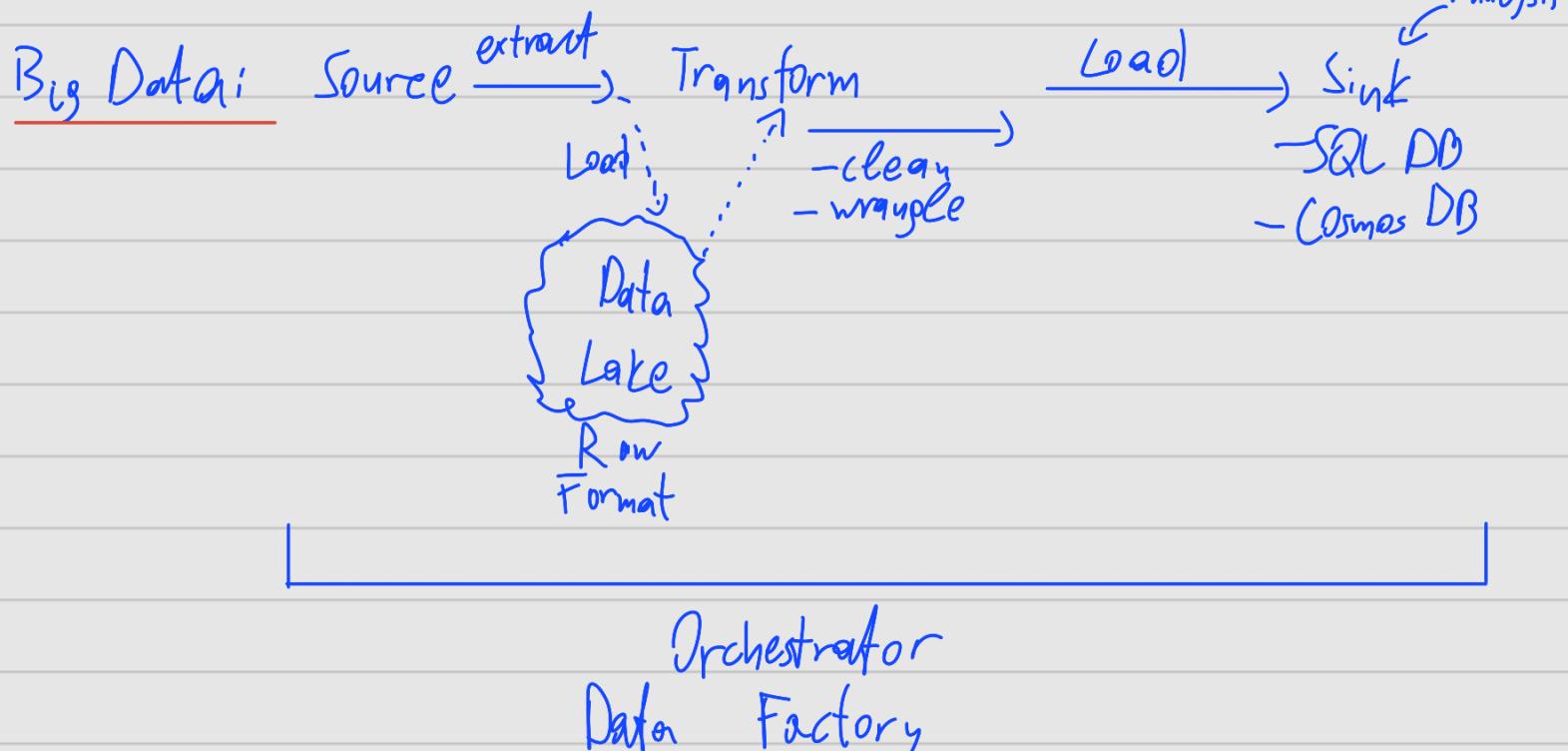


IoT Hub: write my own app

IoT Central: Out of the Box

Azure Sphere: End to End

- Azure Sphere Security Service ①
- Custom Linux OS by MS ②
- Azure Sphere on device ③
- Certificates
- Highest lvl of security



- HDInsight: Open Source Analytics Services / Frameworks

- ↳ • Hadoop
- Storm
- Spark
- Kafka
- Hive LLF

- Databricks: Spark Based analytics

- Azure Synapse Analytics: ~ Workspace

AI services :

Azure  
Machine Learning → Platform for Predictions  
Data Scientists

- Total Control
- How to get data
- Training + Eval models
- pipeline
- Deploy algorithm → API → endpoint

Azure Cognitive Services

- - Prebuilt models
- Language
- Speech
- Vision
- Decision

?  
App

Azure Bot Service → - Chat

- - Virtual Agents

↳ understand

- knowledge base

Serverless: - Consumption Based  
- Event Driven → G, E, D, rest

Azure Functions: - Code  
- Stateless  
[Durable]

Azure Logic Apps: No/Low Code

- Automating  
- Connectors: 

DevOps: - Repos

↳ Version Control  
- Git  
- TFSVC

↳ Boards

↳ Pipelines

- CI/CD

↳ Artifact

Github: - Repos

• Git

- Actions

• CI/CD + much more

• environments

- Projects

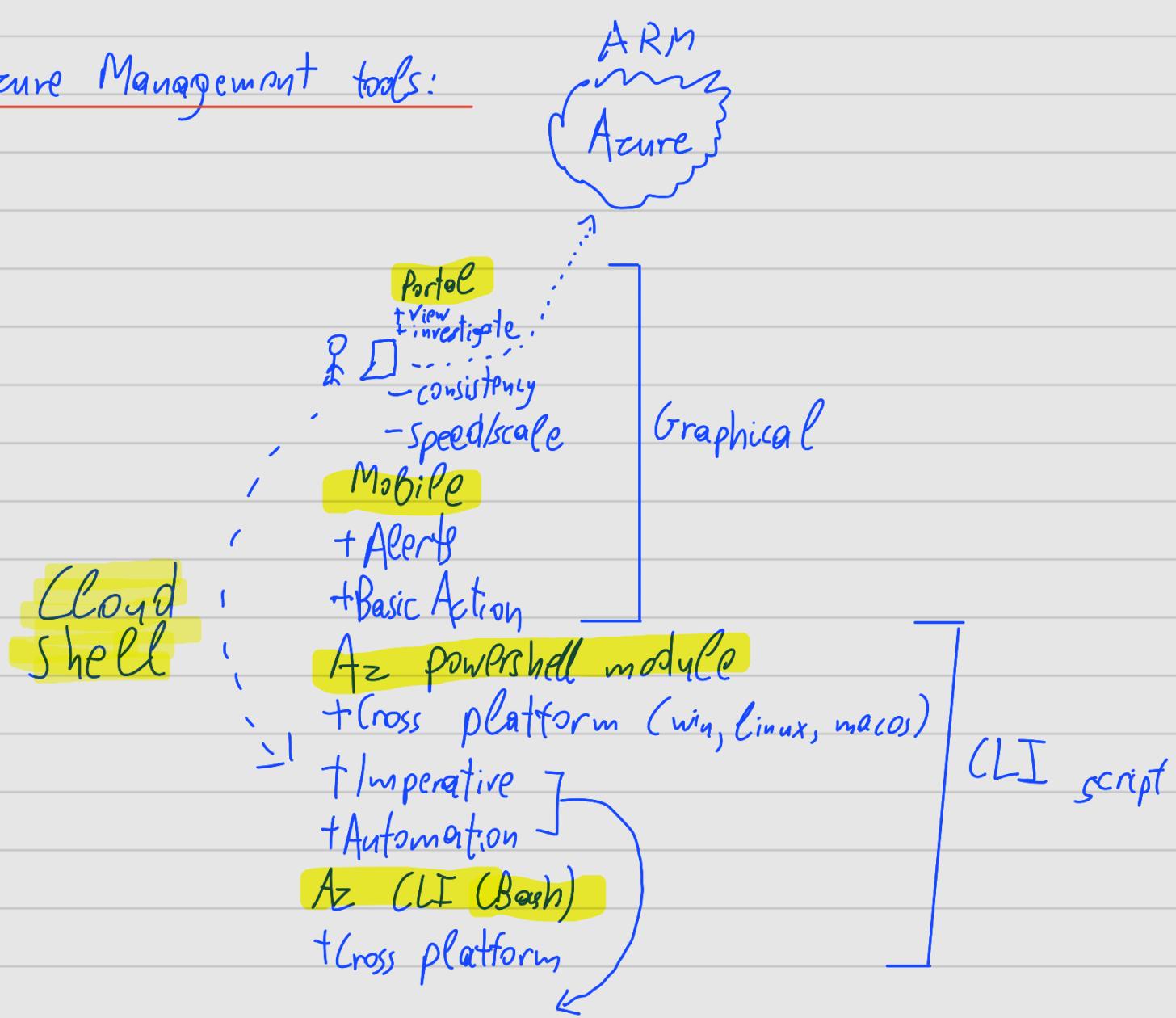
Azure DevTest Labs: → Arm Templates

• Provisioning

• Test

• Delete

## Azure Management tools:

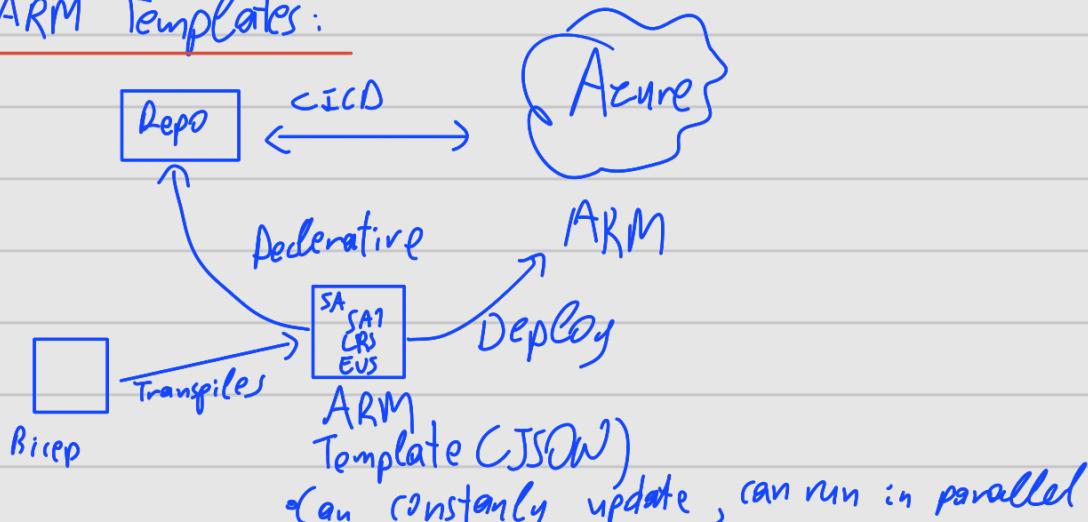


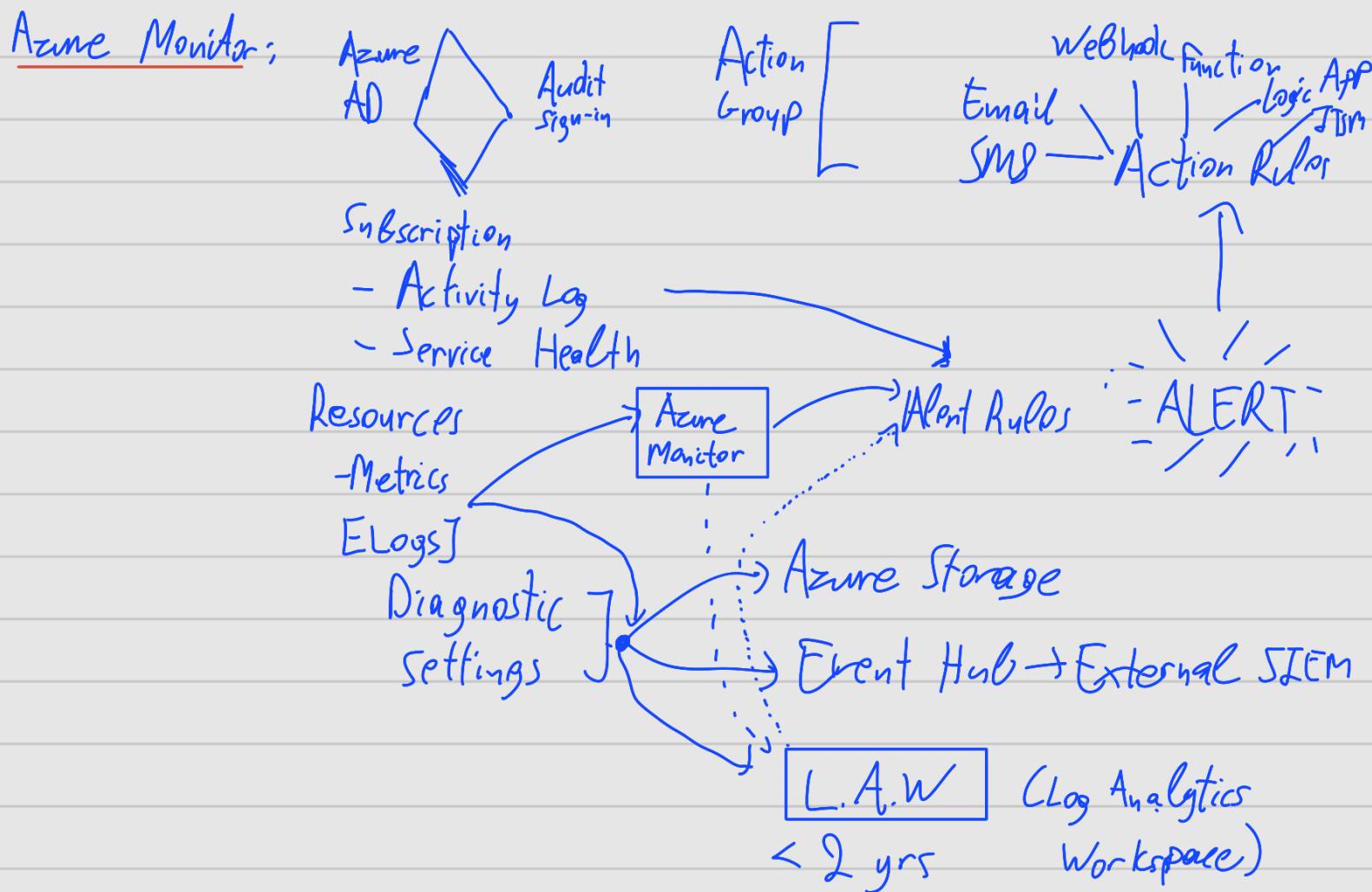
Best practise for provisioning: Azure ARM

Azure Advisor:

- recommendations
- cost optimization

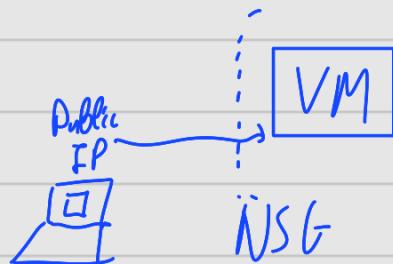
## ARM Templates:





- Service Health:
- Health history
  - Root cause
  - Notifications

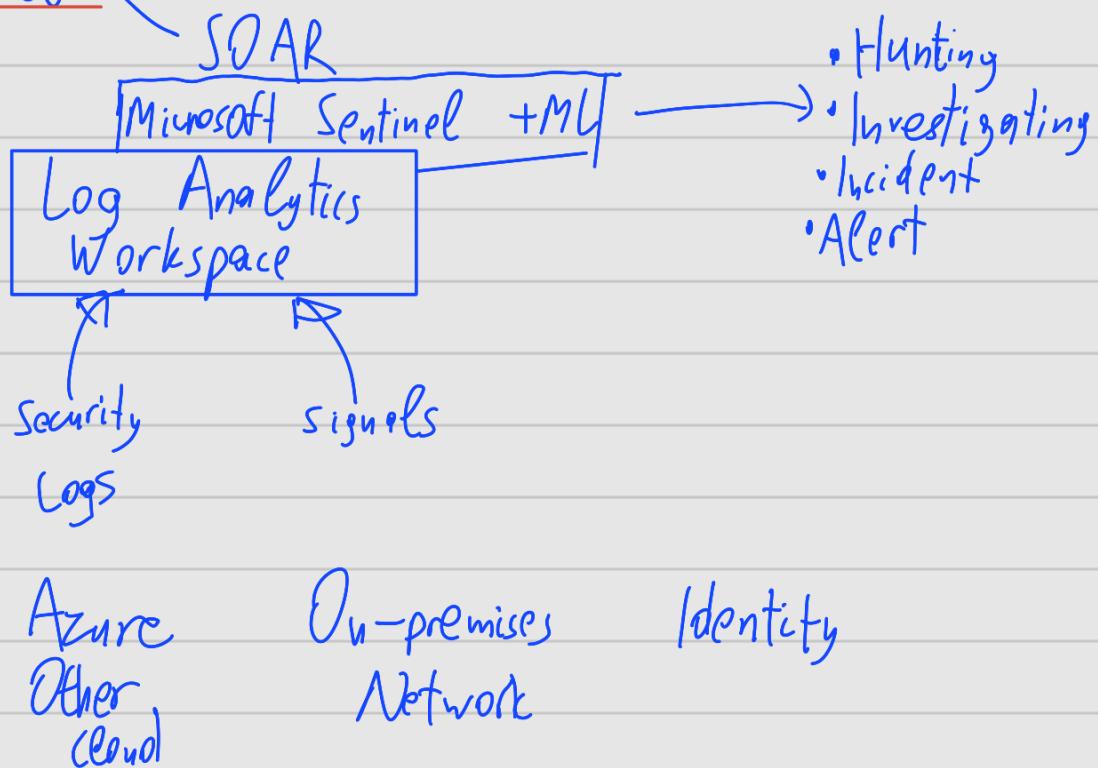
- Defender for cloud:
- has recommendations
  - can be used for compliance
  - Defender plans



## Key Vault:



## MS Sentinel:



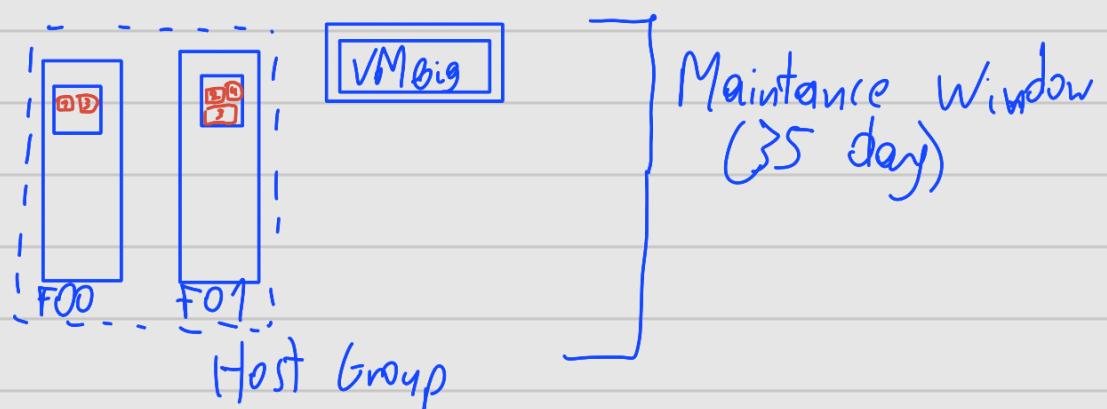
## Dedicated Hosts:

Normally:

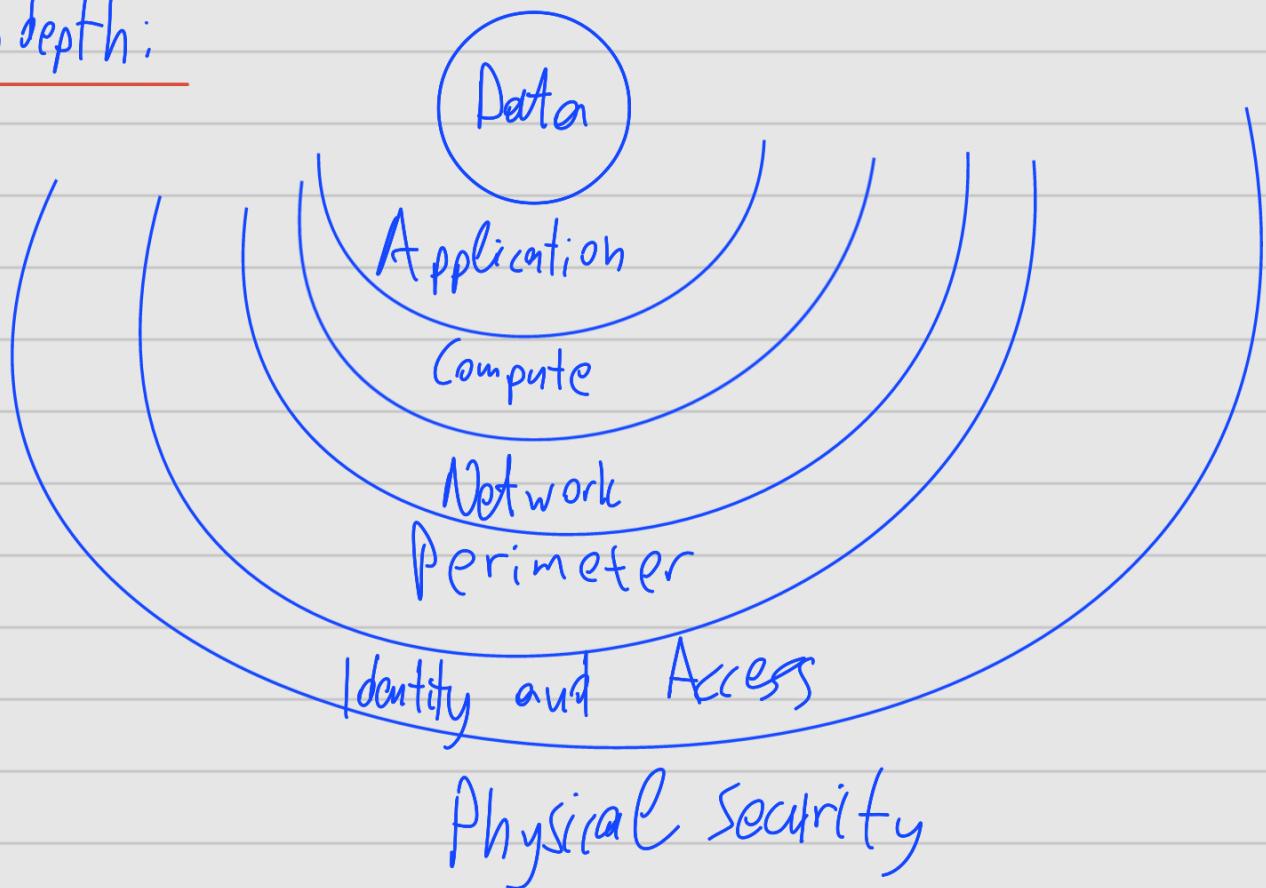


Host

Region E.U.S  
 [AZ1 AZ2 AZ3]



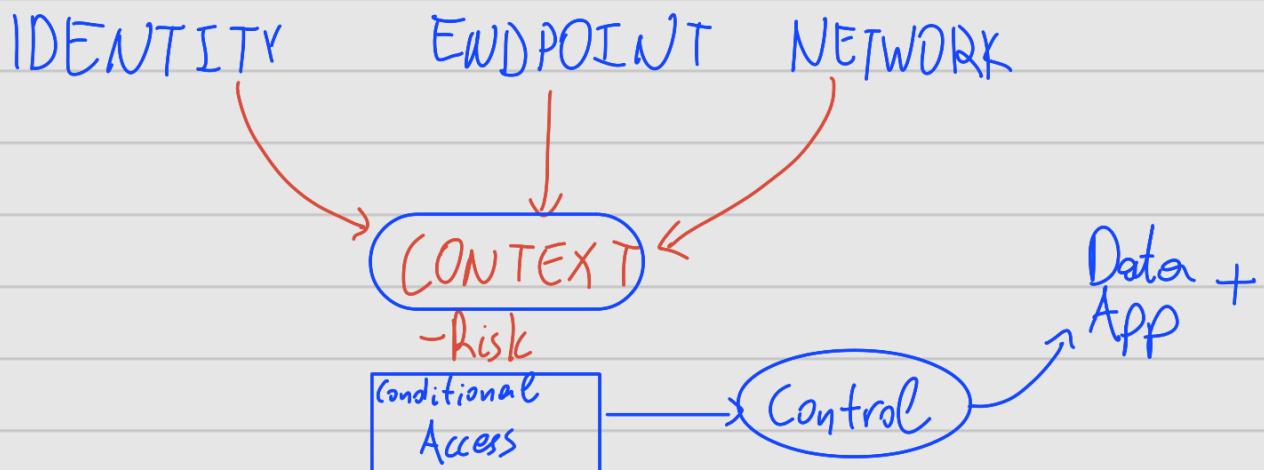
## Defense in depth:



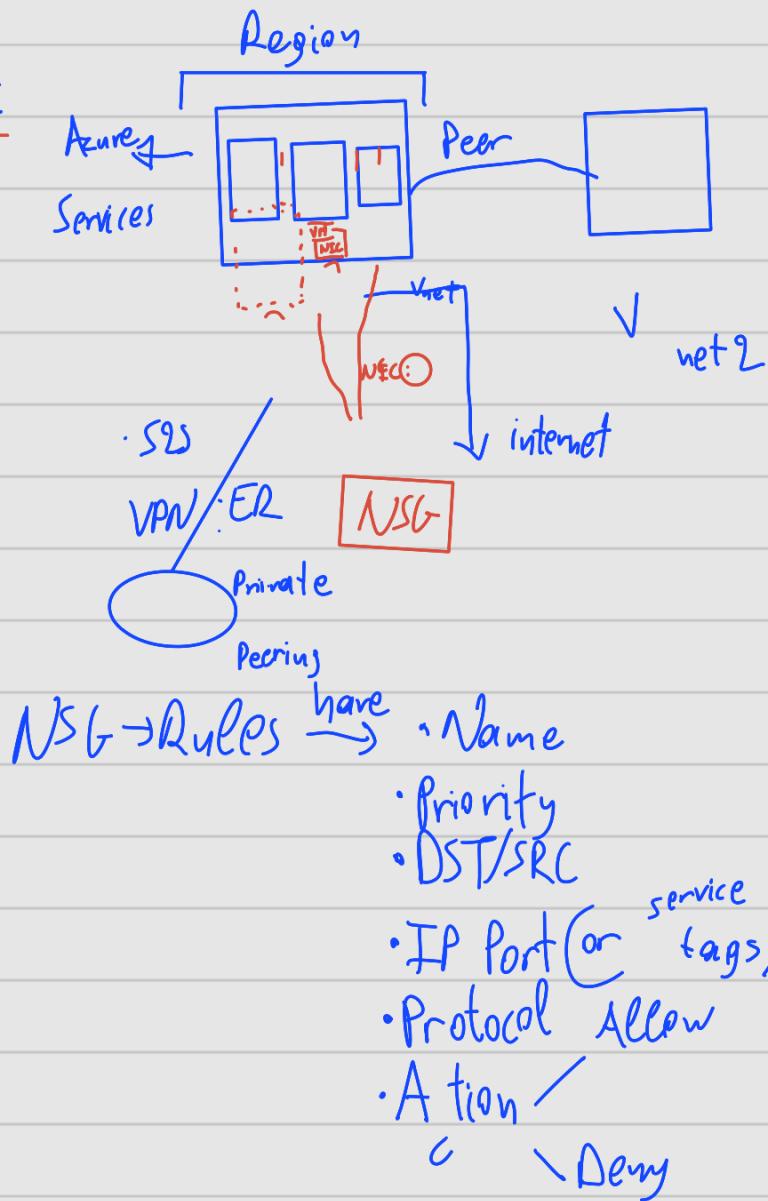
(Confidentiality  
Integrity  
Availability)

Zero Trust:

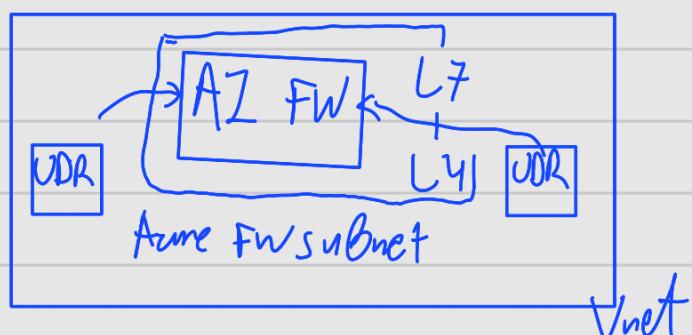
- 1) Verify Explicitly
- 2) Least privilege
- 3) Assume Breach



## NSG:



## Firewall:



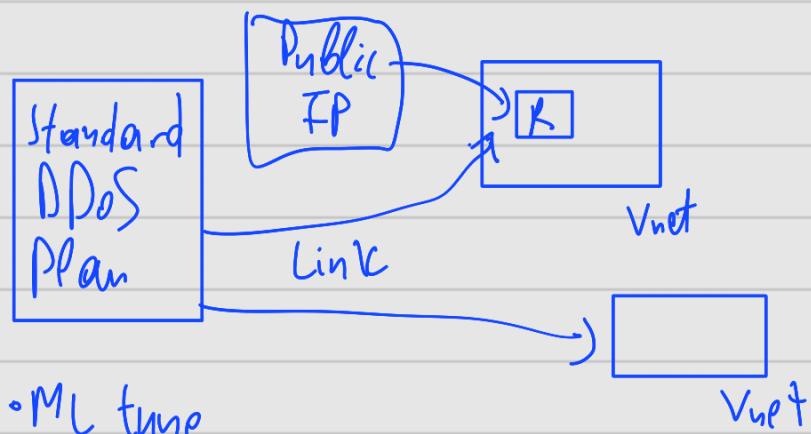
UDR: User Defined Routes

- Application Rule (URL, FQDN)
- Network Rules (IPs, Port)
- Premium TLS inspection
- DNAT w/ public IP

## DDoS Protection:

- Volumetric
  - Protocol
  - Application
- Break Availability

# Basic DDoS Protection



- ML time
- Reporting
- Metrics
- Rapid response
- Credit

1 premium plan → 100 IPs

## Authentication and Authorization:

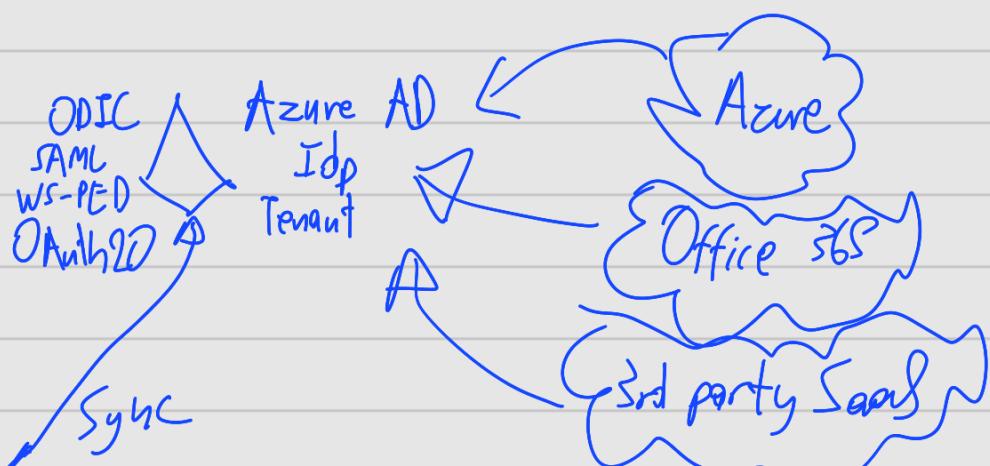
(Authn)

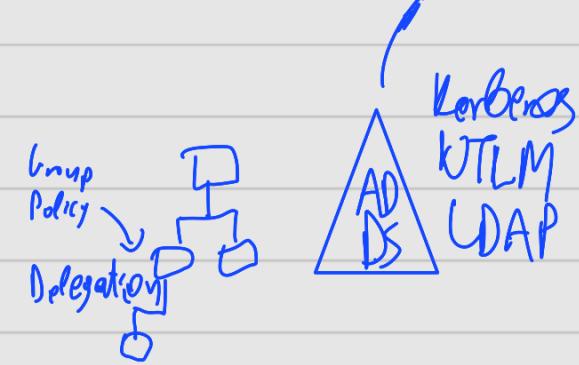
Authentication:  
(Authn)      • Validate id  
                  • Methods:  
                  - we know (password)  
                  - we are (biometric)  
                  - we have (token, pc)

Authorization:  
(Authz)      • What we can do  
                  • Method: RBAC

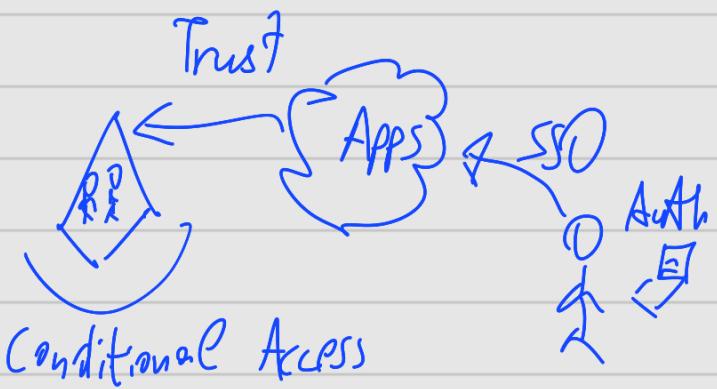
## Azure AD:

(can use  
conditional  
Access)





Conditional Access, SSO, MFA:



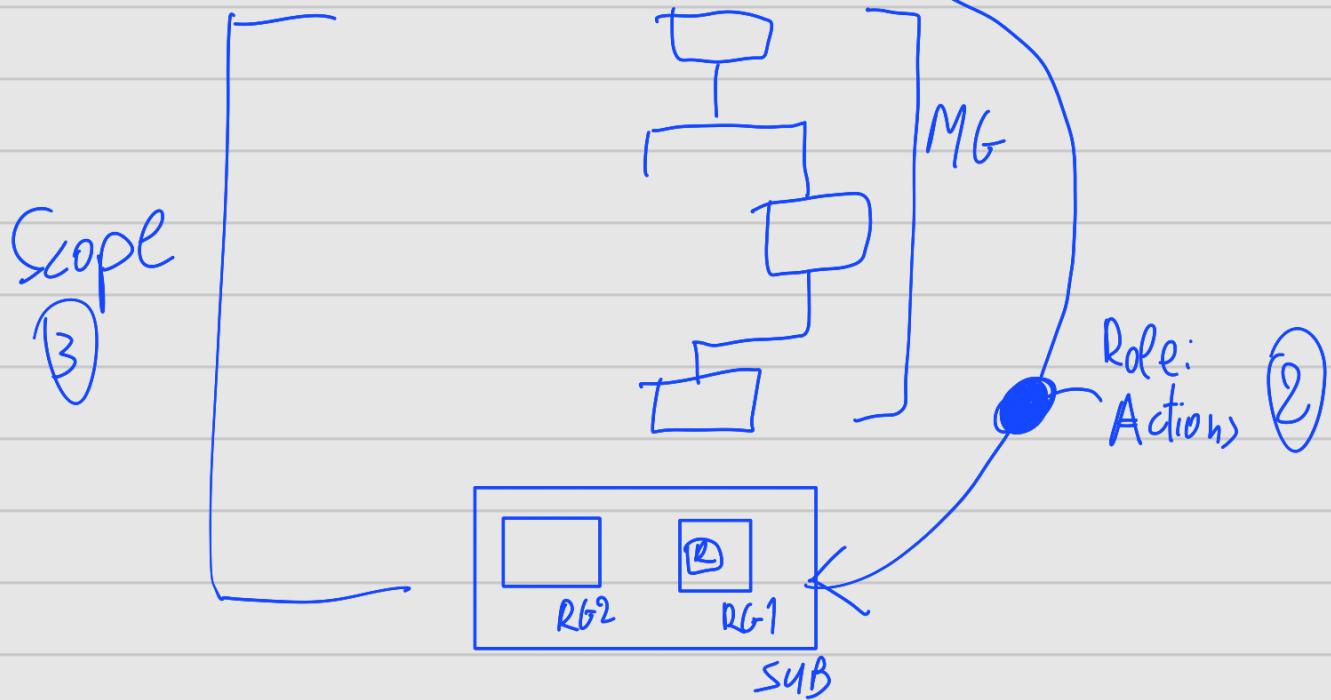
AAD P<sub>1</sub> +  
Auth app  
SMS, call  
+ Token

Device  
MFA  
Passwords know have

MFA:  
≥ 2 methods

Security defaults: MFA - Auth App (Free)

RBAC: Role Assignment



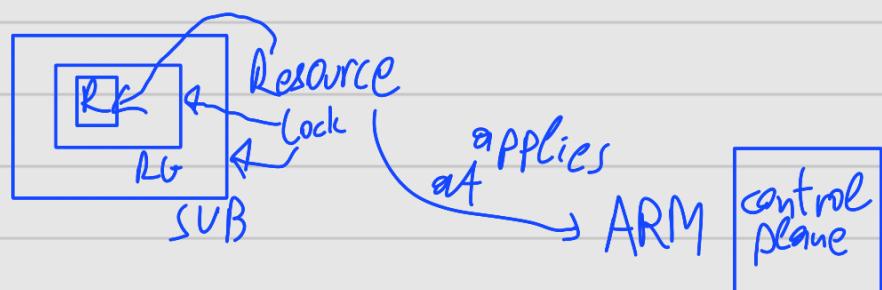
# Role Assignment



Roles: Owner, Contributor, Reader

Scopes are inherited

## Resource Locks:

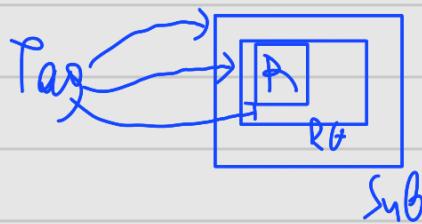


### Options:

- Delete
- Read only
- The owner can add, remove locks
- User Access Administrator can add, remove locks

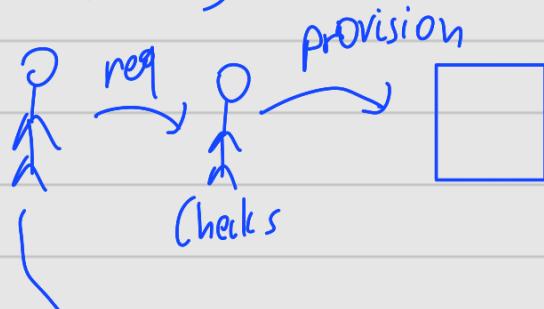
Control plane is not affected

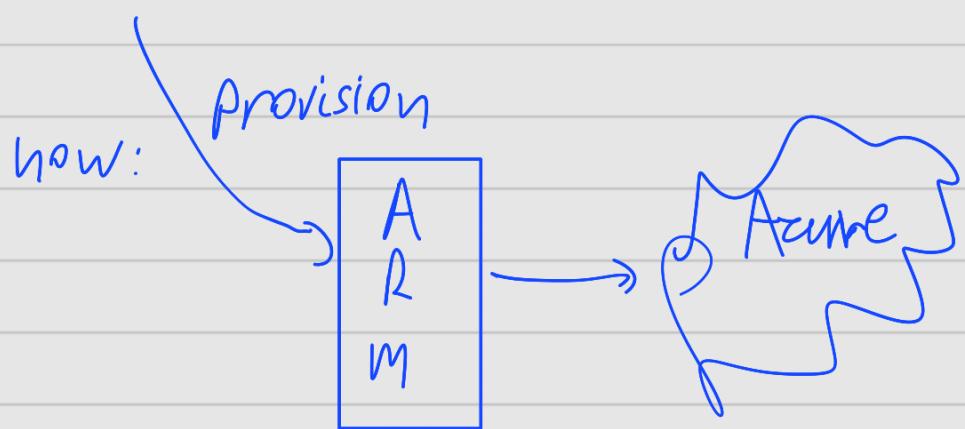
Tags : - Tag is key:value  
- Tags are not inherited (only w/ policy)



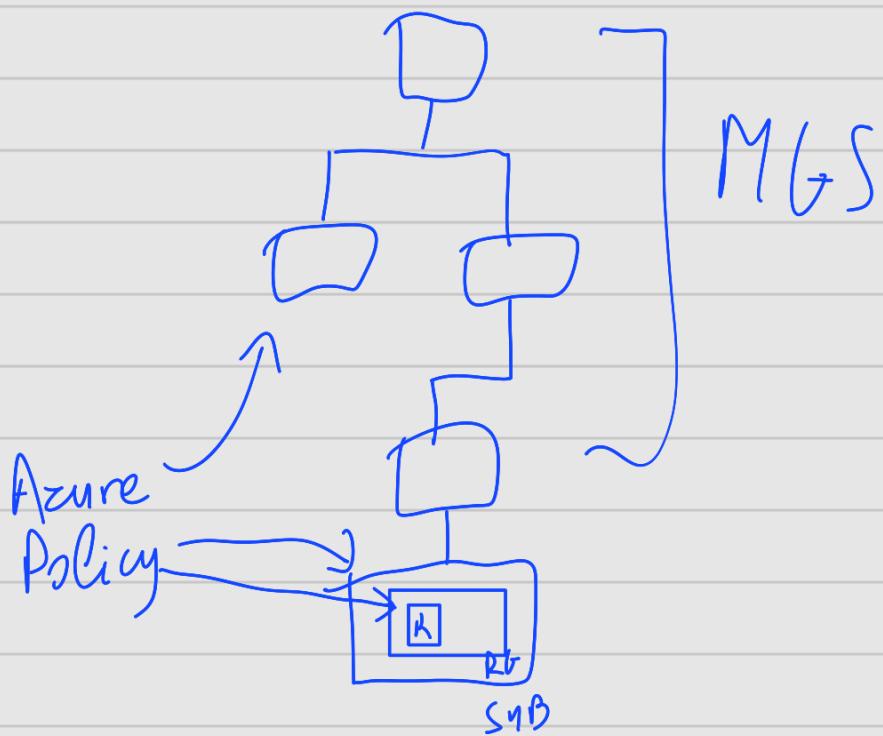
• Use AZ policy to enforce tag creation

## Azure Policy:





↳ Guardrails: Azure Policy



- Policy is „inherited“
- “Initiative”: n - number of policies
- Effect:
  - Audit
  - Deny
  - Append/Modify
  - If not exists
- (can apply definitions (compliance etc))

## Hierarchy Constraints:

- Policy
  - ↳ Rules
- Actions

inherited

- RBAC
  - ↳ Role

'Assignment  
Role(I) Scope'

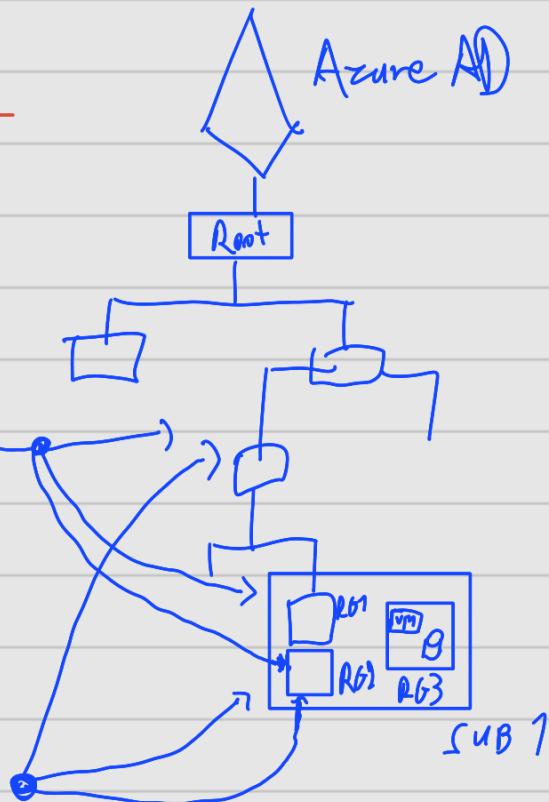
- Budget
  - ↳ \$ %
  - Actual Forecast

Azure AD

Root



≤ 6 levels of Management Groups



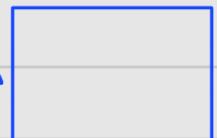
## Azure Blueprints:

- Don't Lock
- Don't Deploy
- Read Only

Assign

Blueprint: Resource Groups

- ↳ ARM Templates
  - RBAC
  - Policy



Sub

(Cloud Adoption Framework: Best practices

Define (strategy → Plan → Ready → Adopt)  
Gover, manage

MPS, OST, DPA: • Microsoft Privacy Statement

- Online Services Terms
- Data Protection Addendum

## Trust Center, Azure Compliance:

- Security  
Privacy  
Compliance
- Trust Center: Privacy, Compliance

Sovereign Regions: • Azure (Cloud, China (East), US Gov, German)  
• Separated physically and logically  
• For certifications, meet the requirements

## Factors that affect cost:

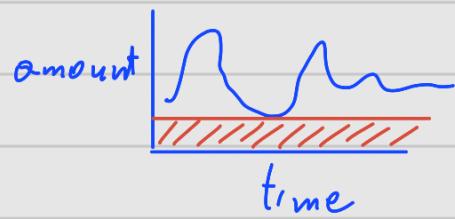


- Type
- SKU
  - Tiers
  - Size
- Location

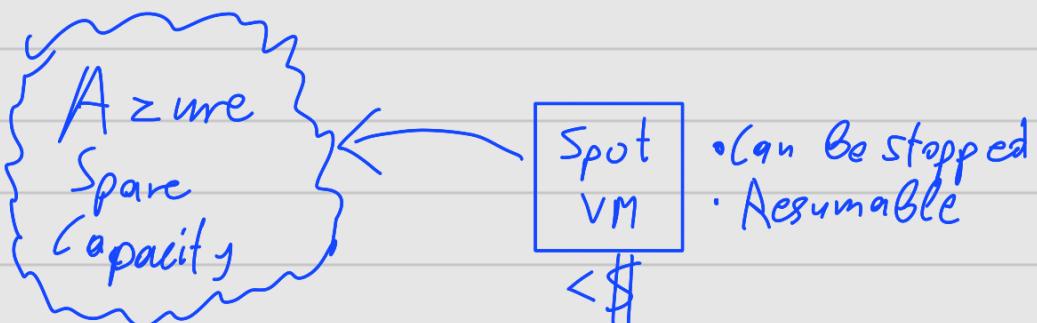
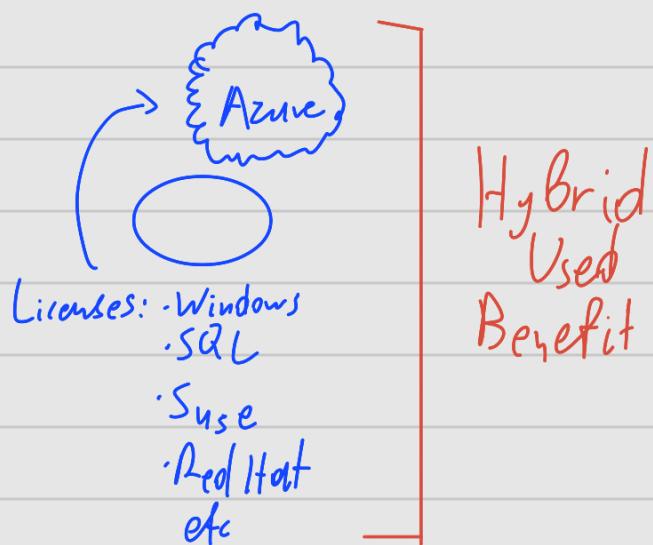
- Meter
  - Exist
  - Running
  - Instances
  - Work - Serverless
- Storage
  - Used
  - Provisioned
- Interactions
- Licensing

## Reducing Costs:

<span style="font-size: 2em;">\$</span> <span style="border: 1px solid black; padding: 2px;">R</span>	<p>Tags (identification) ←</p> <ul style="list-style-type: none"> <li>- Exist</li> <li>- Running</li> <li>- Instances</li> <li>- Work - <u>Serverless</u></li> </ul> <p>Azure Advisor</p> <ul style="list-style-type: none"> <li>- Type</li> <li>- SKU ← Ratio CPU:Mem</li> <li>• Tiers [ Hot / Cold / Archive ]</li> <li>• Size</li> <li>- Location</li> </ul>	<p>Meter</p> <ul style="list-style-type: none"> <li>- Delete when not required</li> <li>- Deallocate</li> <li>- Autoscale</li> </ul>
		<ul style="list-style-type: none"> <li>- Storage</li> <li>• Used</li> <li>• Provisioned</li> <li>- Interactions</li> <li>- Licensing</li> </ul>



Azure Reservations  
(1/3 Yrs) → Discount



Pick max price

Pricing, TCO calc:

- Add everything to get realistic quotes
- TCO: how much money you save moving to the cloud

Azure Cost management:

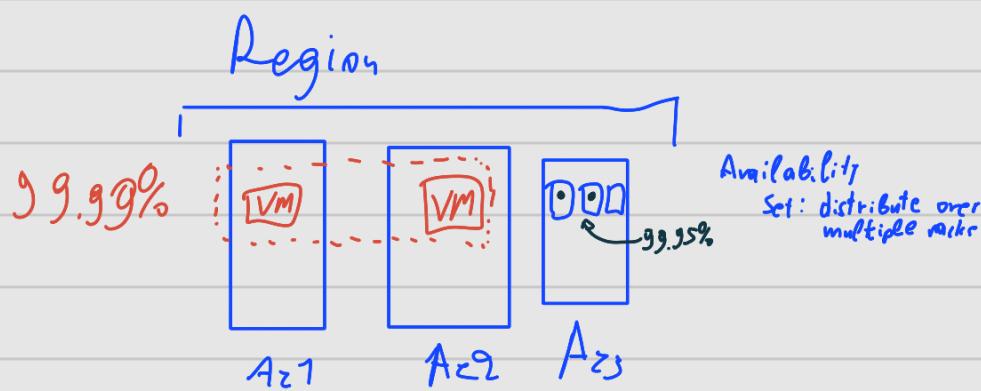
- Cost Analysis (has ML)
- Breaks down costs
- Budget: Fixes on amount

↓      ↓  
actual    Forecasted

SLAs:

- Availability

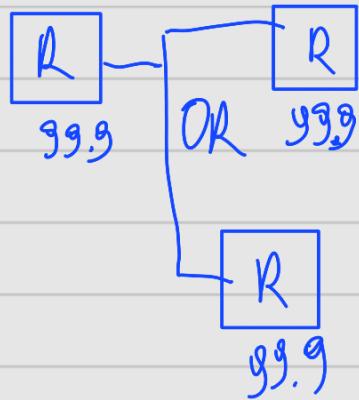
SLA	Downtime per week
99%	1.68 Hrs
99.9	10.1 min
99.95	5 min
99.99	1.01 min
99.999	6 seconds



→ Storage SLA differ

Azure Status: see if servers are ok

Compositing  
SLA:



→ Multiplied

Service Lifecycle :

