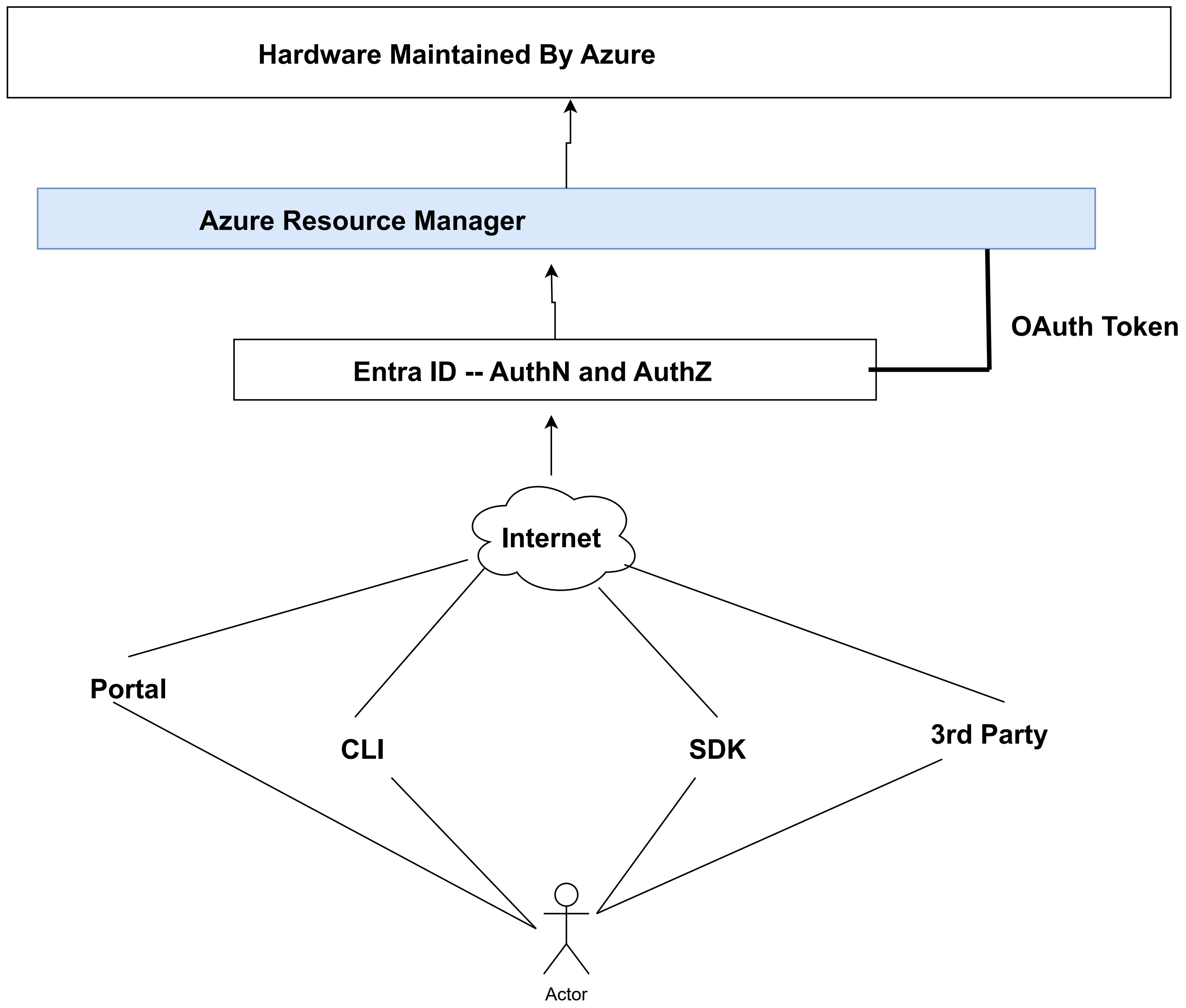


Hardware Maintained By Azure

Azure Resource Manager

OAuth Token

Entra ID -- AuthN and AuthZ

Internet

Portal

CLI

SDK

3rd Party

Actor

Cloud: Getting On-Demand Configurable resources available on demand
generally Pay AS GO Model

API ==> JSON

Azure Resource Manager: control Plane of Azure
All API Calls and Responses

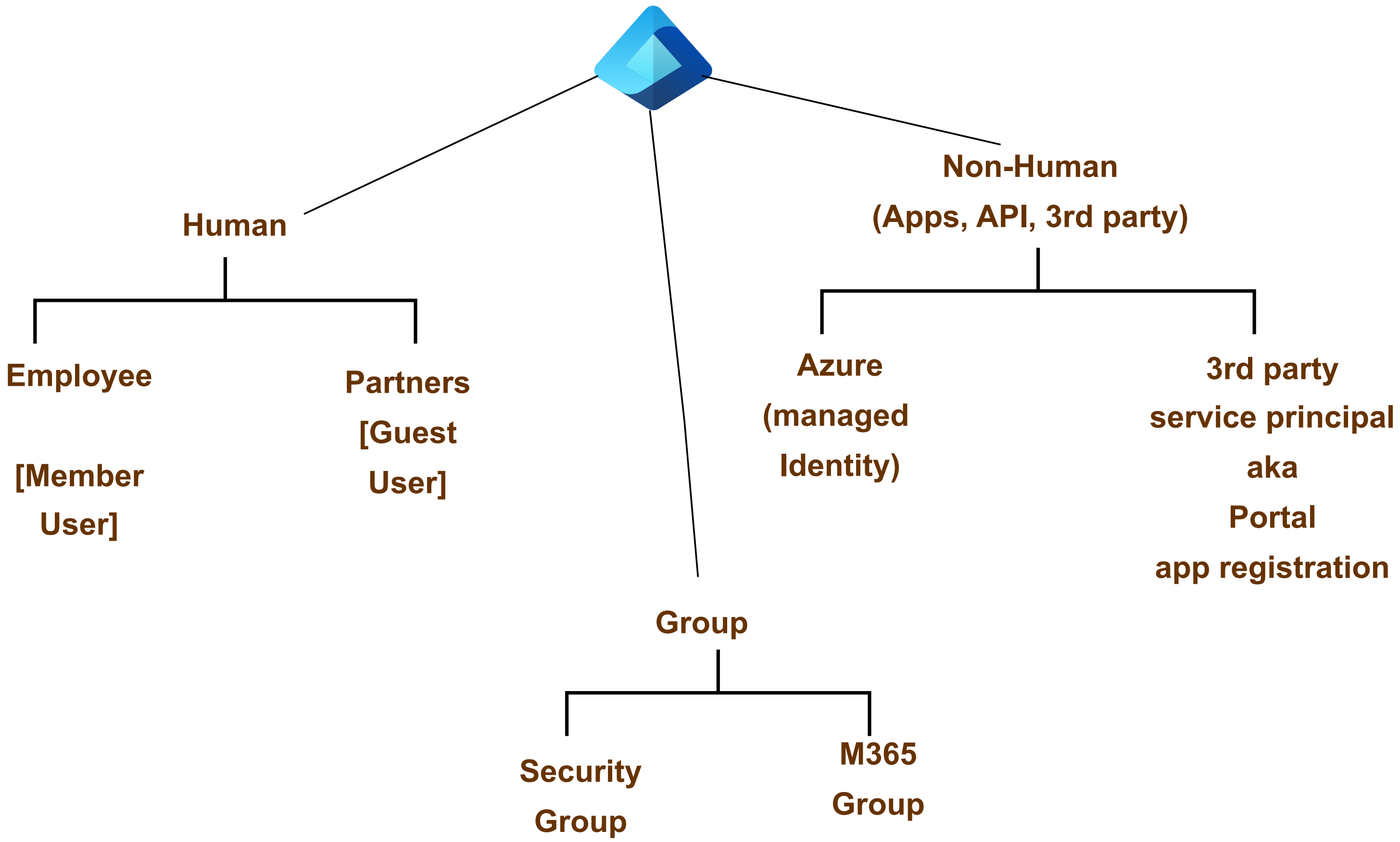
ARM Template (JSON) ==> Raise Request to ARM

ARM

Resource Provider => VM,
Storage,

Entra ID : Cloud Based IAM service
No Backup, BCDR done by customers
- Free Version also available

Identity = Any object that needs permission



Human

Employee

[Member
User]

Partners
[Guest
User]

Group

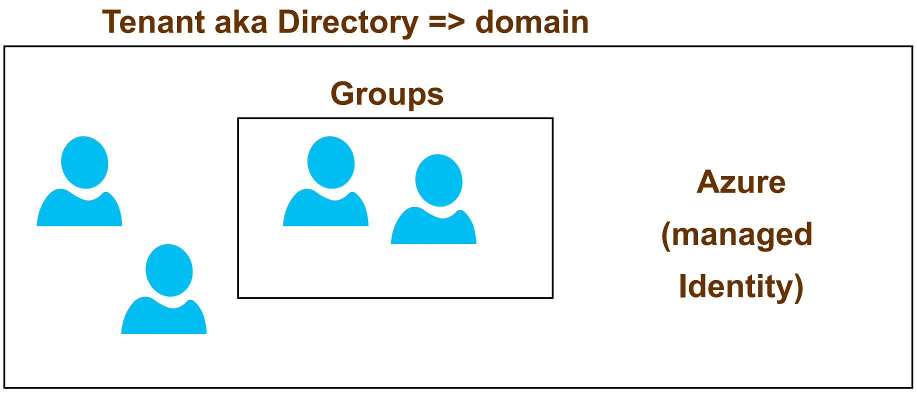
Security
Group

M365
Group

Non-Human
(Apps, API, 3rd party)

Azure
(managed
Identity)

3rd party
service principal
aka
Portal
app registration



Tenant aka Directory => domain

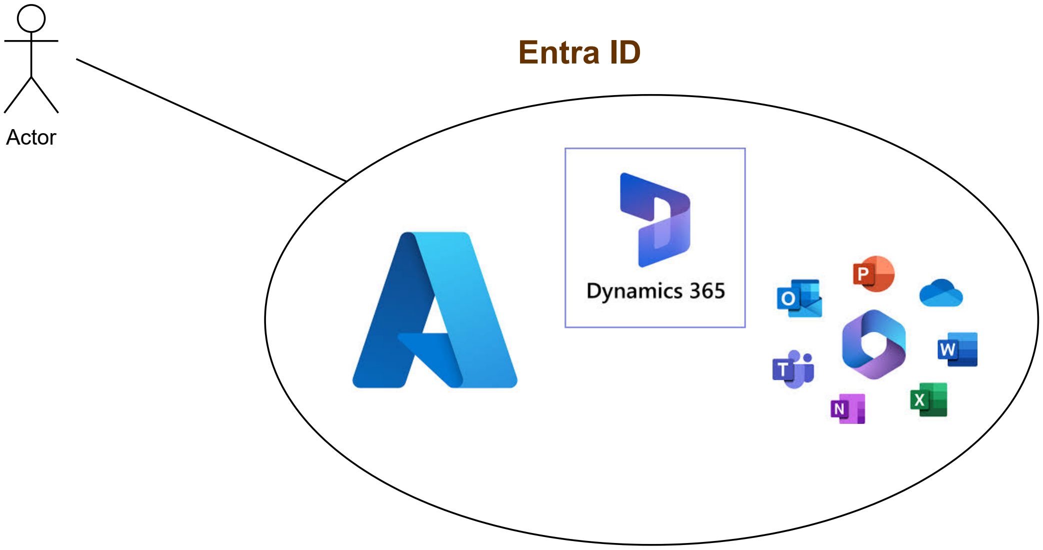
Groups

Azure (managed Identity)

LOB -1 = tenant-1

LOB -2 = tenant-2

Global Administrator: Only 2 [Recommended]



Entra ID

Azure Hierarchy :

Credit Card = Subscription = Billing and access boundary

1 subscription = 1 bill

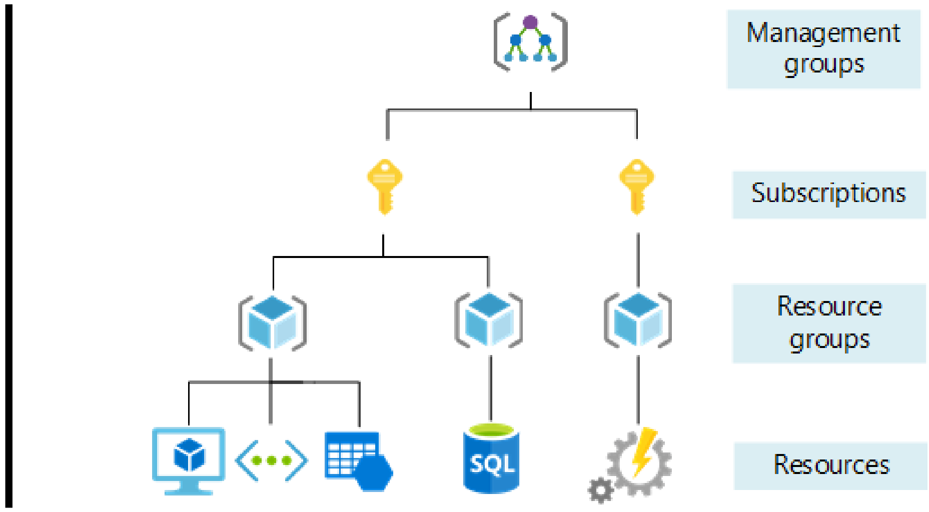
3 subscription :

Dev ———————— Separate billing

QA Avoid API limit

Prod

Policy, access inherited

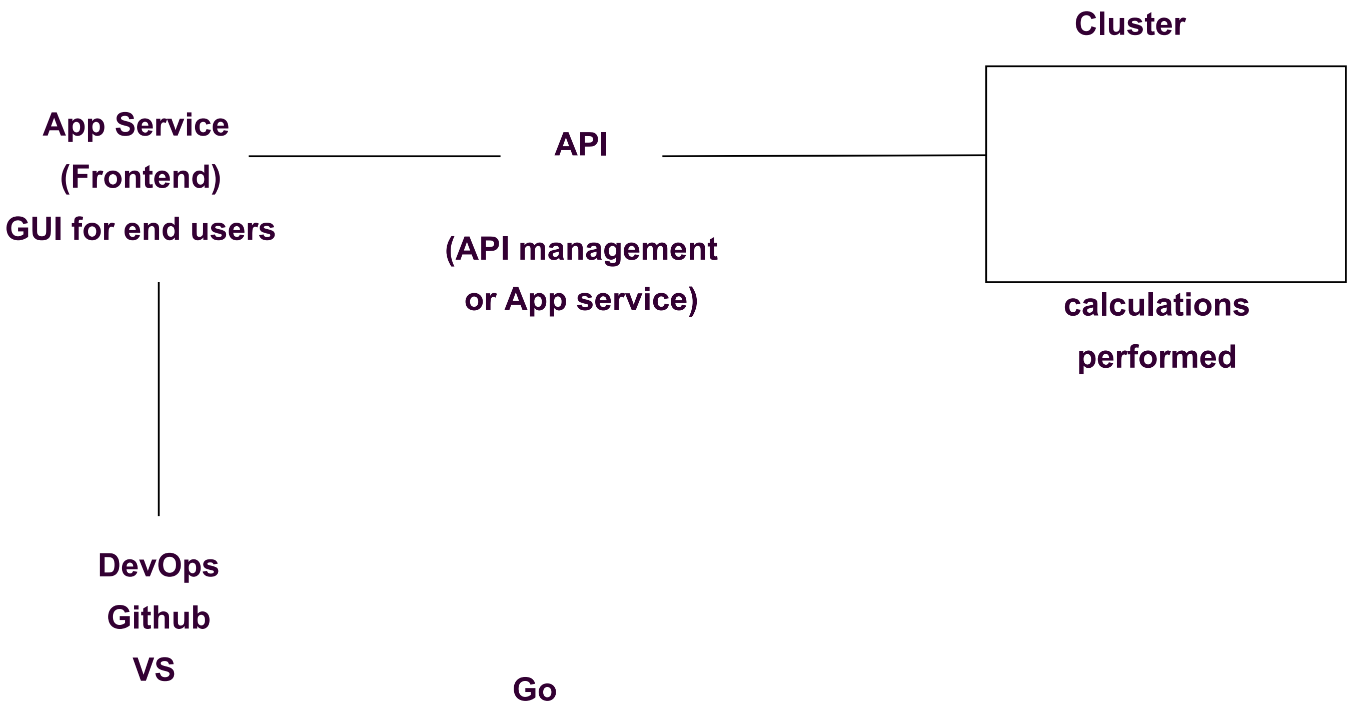


Management groups help you manage access, policy, and compliance for multiple subscriptions. All subscriptions in a management group automatically inherit the conditions that are applied to the management group.

Resource groups are logical containers where you can deploy and manage Azure resources like virtual machines, web apps, databases, and storage accounts.

Resources are instances of services that you can create in a resource group, such as virtual machines, storage, and SQL databases.

Azure App Service enables you to build and host web apps, mobile back ends, and RESTful APIs in the programming language of your choice without managing infrastructure



Cluster

App Service
(Frontend)
GUI for end users

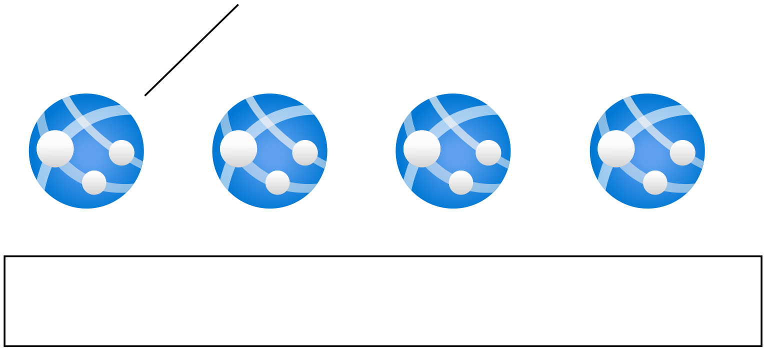
API

(API management
or App service)

calculations
performed

DevOps
Github
VS

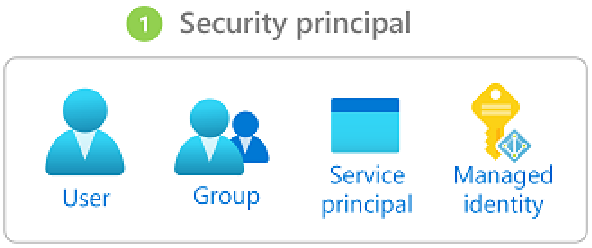
Go



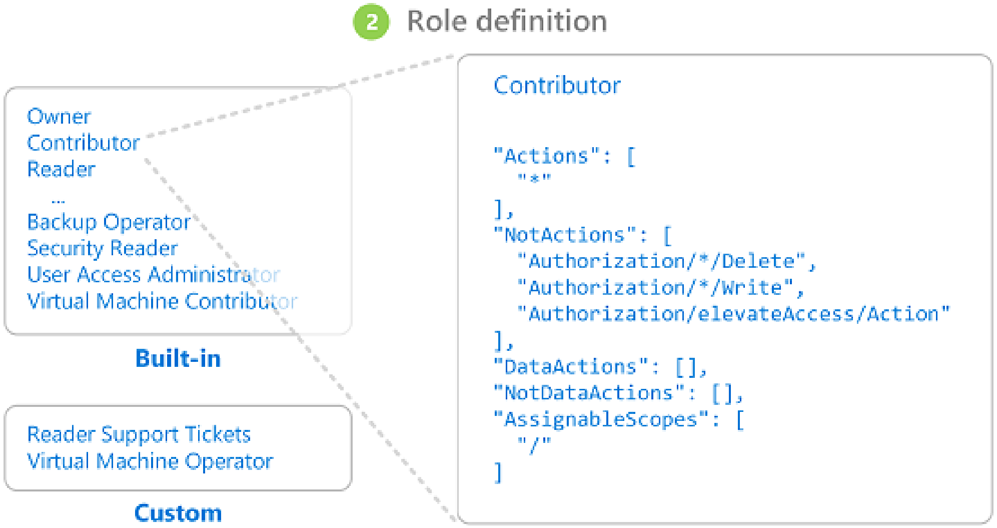
Azure App Service Plan - Hardware, Feature
(Kernel- linux, windows)

Plan - Linux
Plan2 - windows

up can upgarded and Downgrade app plan



To give Permissions in Azure ==> Use RBAC



2 Role definition

Owner
Contributor
Reader
...
Backup Operator
Security Reader
User Access Administrator
Virtual Machine Contributor

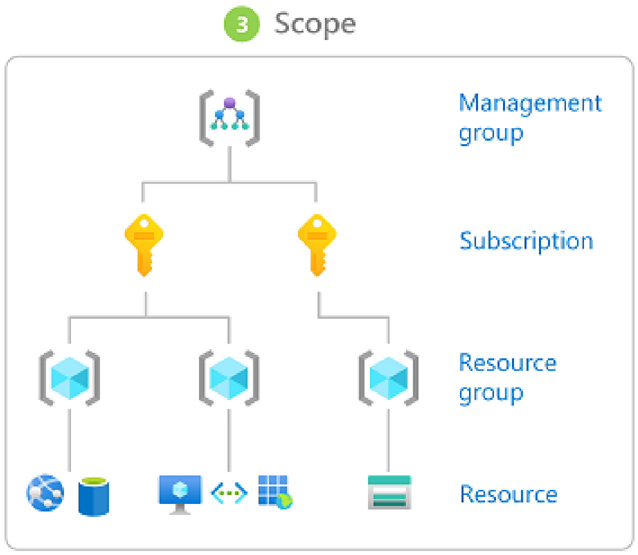
Built-in

Reader Support Tickets
Virtual Machine Operator

Custom

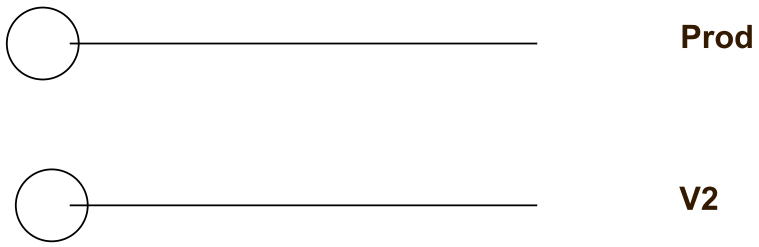
Contributor

```
"Actions": [
  "*"
],
"NotActions": [
  "Authorization/*/Delete",
  "Authorization/*/Write",
  "Authorization/elevateAccess/Action"
],
"DataActions": [],
"NotDataActions": [],
"AssignableScopes": [
  "/"
]
```



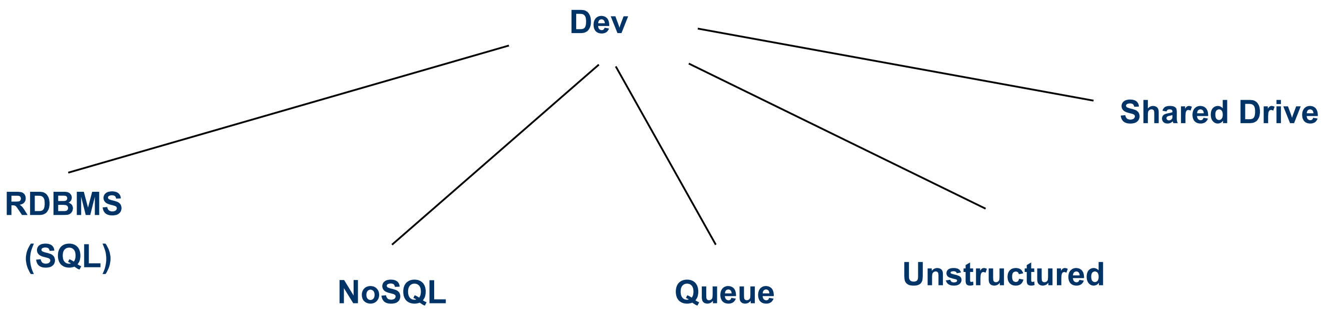
You should not deploy things directly to prod :)

Deployment Slots:



Deployment slots are live apps with their own hostnames. App content and configurations elements can be swapped between two deployment slots, including the production slot

Key Vault => Secret management
Else
Env vars



Storage Account: Infinitely Scaleable highly available Cloud Storage
- region ($)

Performance: Standard (Default)
Premium tier ($$$$)

High Availability: Pay => Cross Region replication

Pay Less => Distributes 3 different in Datacenter

Unstructured / Blob Storage: Parquet, PPT, Audio, video

- stream over browser
- backup and Restore, DR, Archiving

- HTTP/ HTTPS

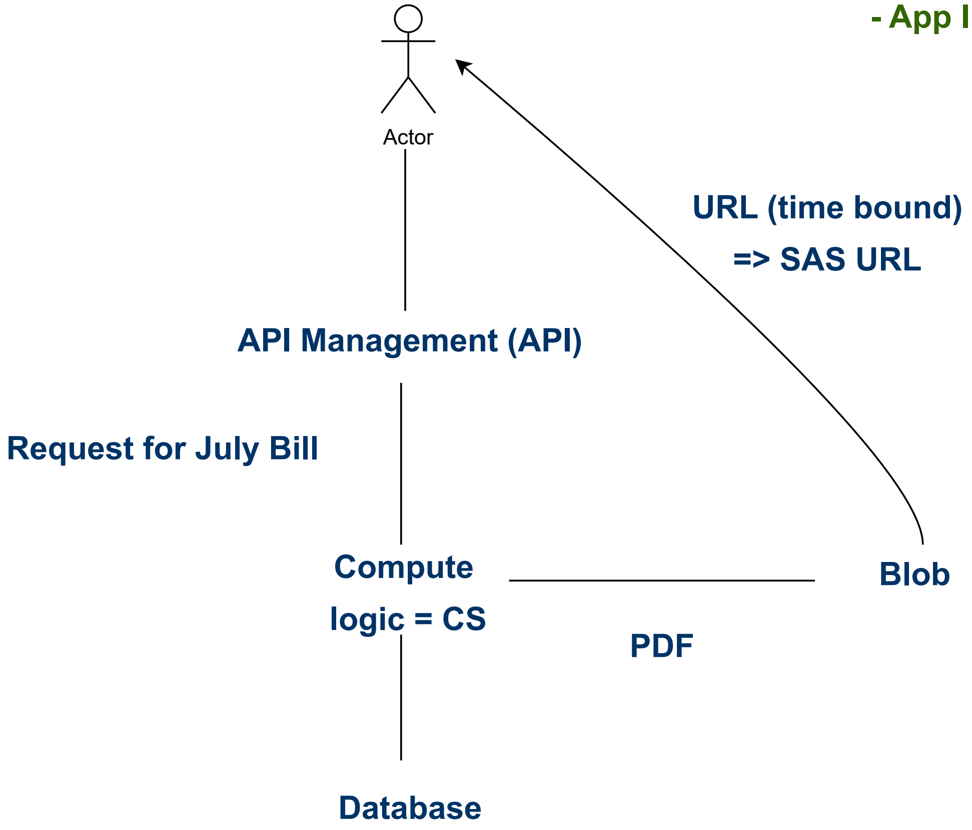
Cloud storage bucket = containers in azure

Anonymous access to this container is being blocked because anonymous access is disabled on this storage account.

SDK = Go, Python,

Why Use SDK ?

- App Intercats in the languauge



Actor

URL (time bound)

=> SAS URL

API Management (API)

Request for July Bill

Compute logic = CS

Blob

PDF

Database

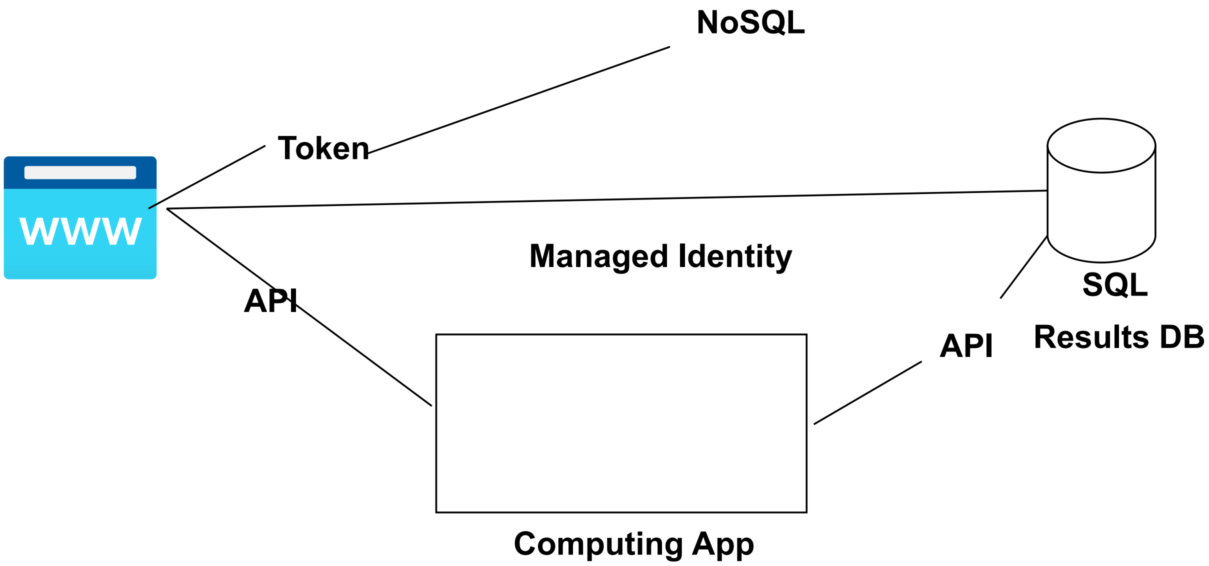
Common Methods to AuthN =

1. az cli
(az login into machine)

2. Creds at App Level
- Env Vars Pass Tokens
- Key vault to fetch and share creds
- (if it's Azure Service) ==> Managed Identity

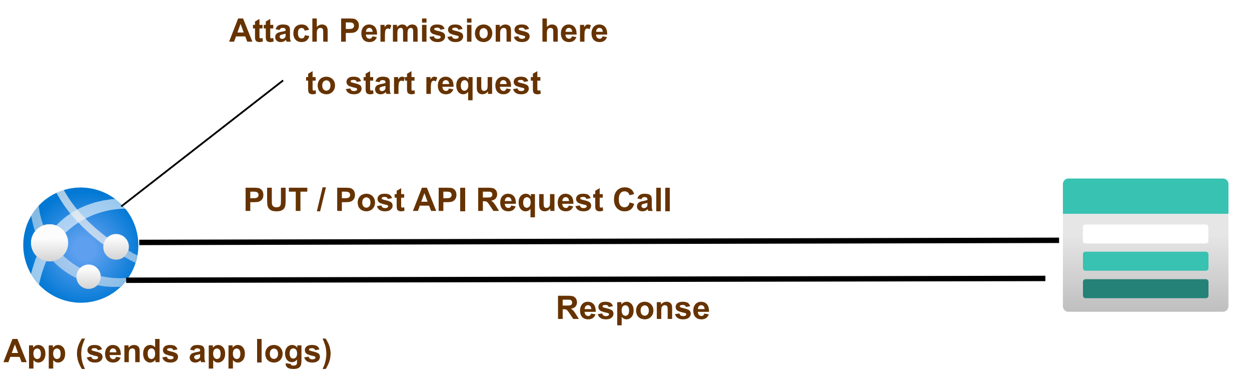
3. Service Specific Auth Methods -
SQL : User, Password
Blob = Storage Account key
SAS Token

How to AuthN
to SDK?



Grant limited access to Azure Storage resources using shared access signatures (SAS)

- Storage Account
- Container
- Blob



Attach Permissions here
to start request

PUT / Post API Request Call

Response

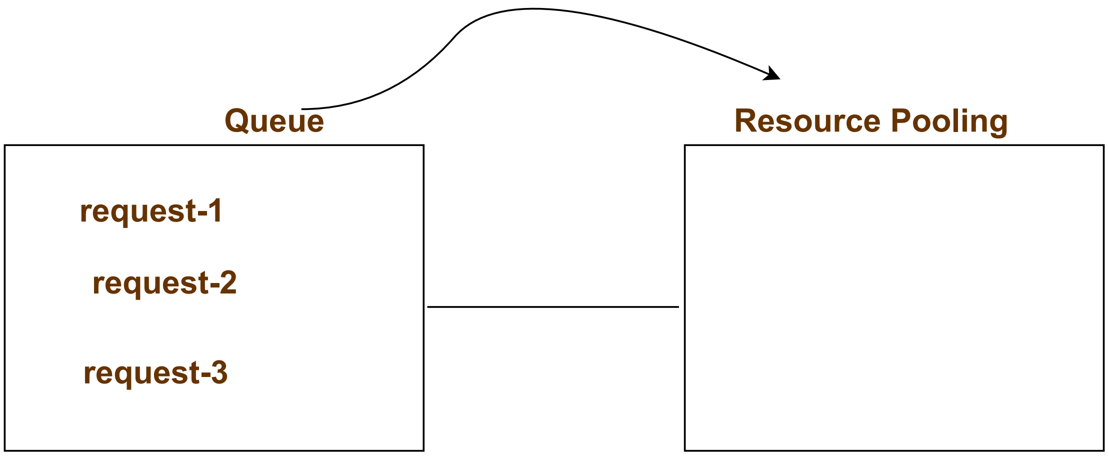
App (sends app logs)

Hybrid Connection -

ExpresRoute -

VPN - Hourly $ + Data Processing $

Databox - for offline data transfer to azure



Queue

request-1

request-2

request-3

Resource Pooling

serverless vs PaaS

similarity

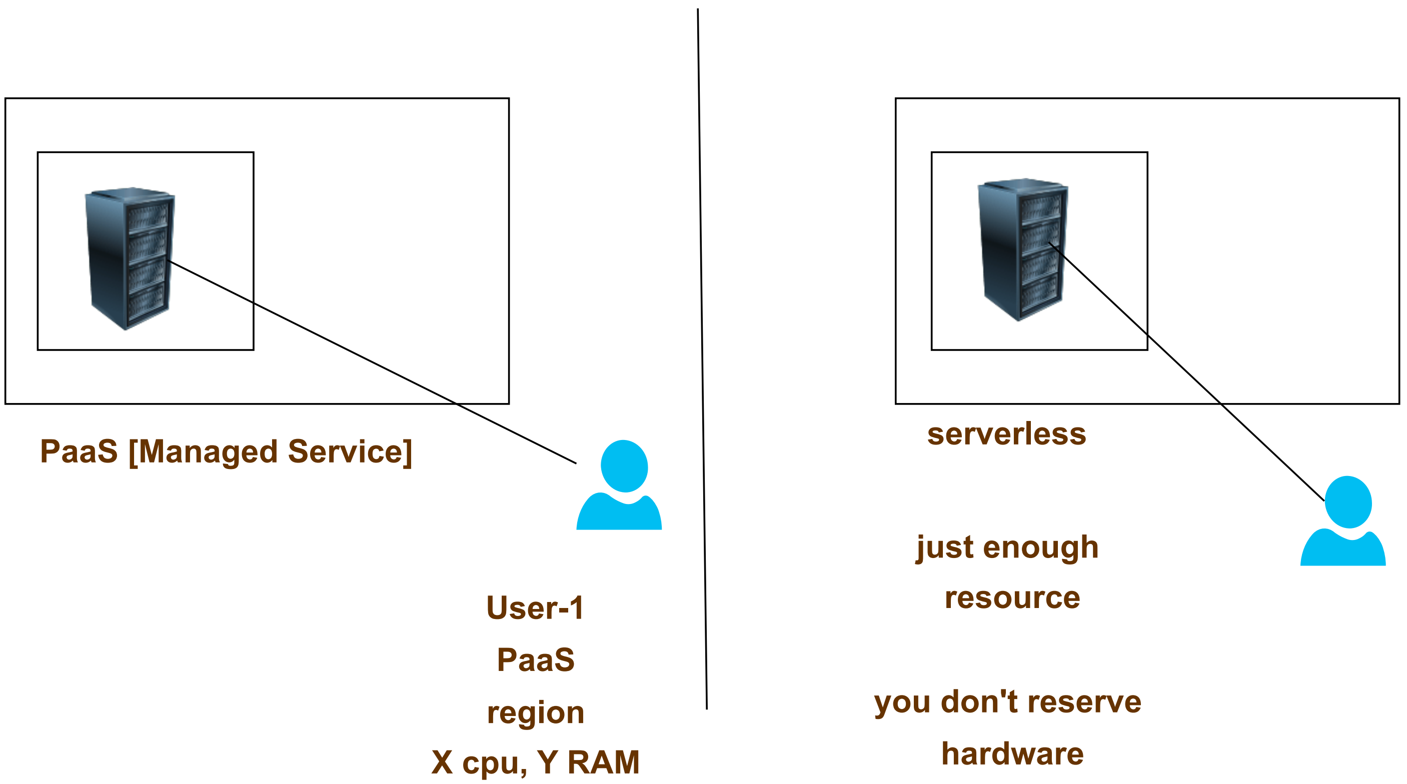
- backups, DR, scaling, updates

- OS level

Different

PaaS - You are charged
for hardware

serverless - per second billing / ececutions



PaaS [Managed Service]

User-1
PaaS
region
X cpu, Y RAM

serverless

just enough
resource

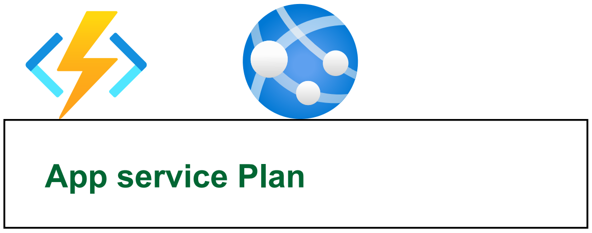
you don't reserve
hardware

AER App

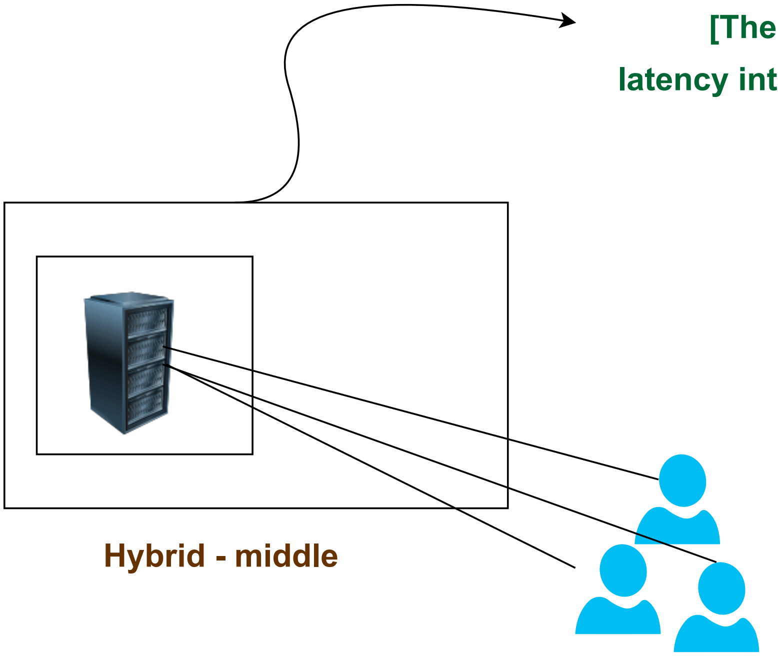
Prog Lang - C#, Python, Java

3 Hosting Types for Azure function:

1. serverless (consumption based) -
2. K8s
3. App service Plan



App service Plan



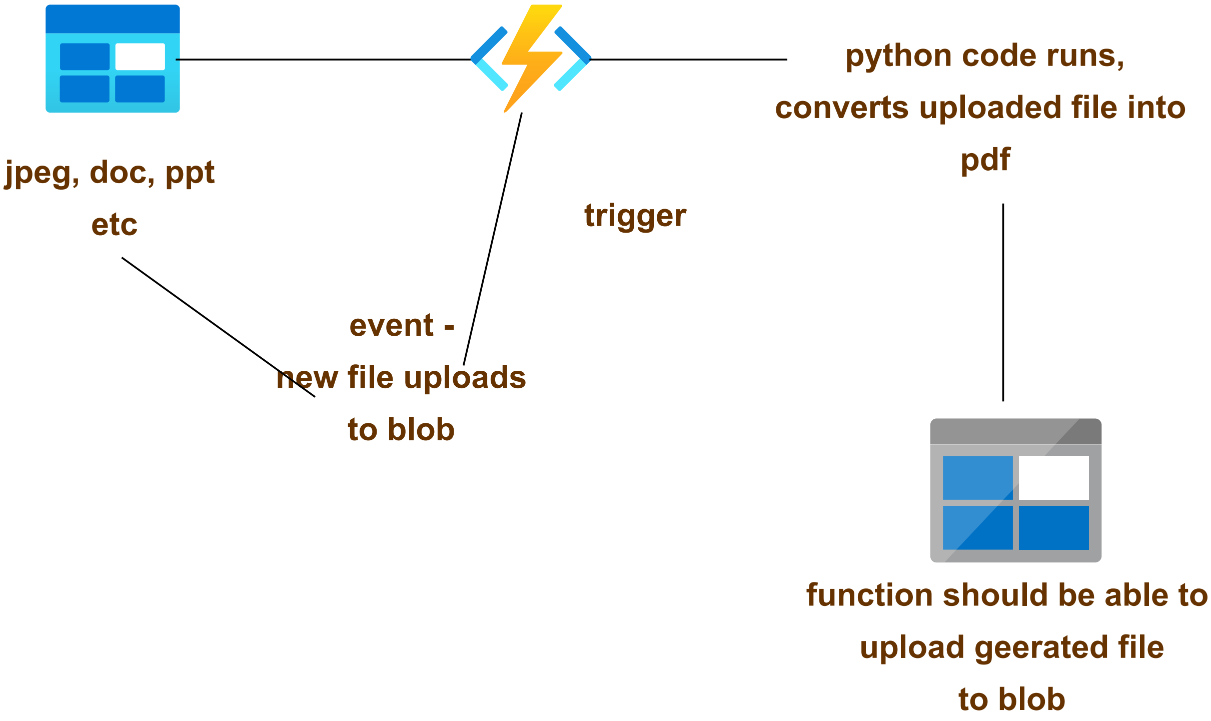
[Theoretical Term] Cold Start -

latency introduced by hardware not found

Hybrid - middle

Function - event driven - only respond

Hybrid - middle



jpeg, doc, ppt

etc

trigger

event -

new file uploads

to blob

python code runs,

converts uploaded file into

pdf

function should be able to

upload geerated file

to blob

event hub (here specify schedule) ———————— **trigger azure functions**

trigger azure functions

trigger azure functions

SQL on Azure VM - on demand compute
(OS, Size, Config)

- Full control (IaaS)
- backup, scaling, BCDR, networking
- Bring Your Own License (BYOL)
- migration

SQL Database
PaaS
Managements task - upgrading, backups, monitoring by azure

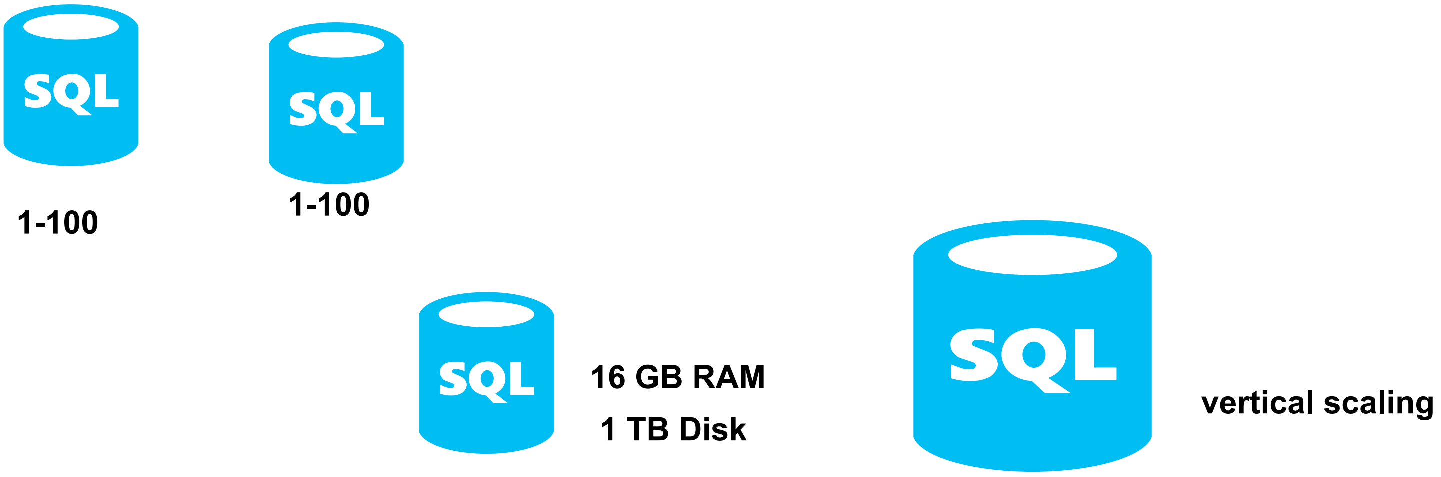
Virtual core (vCore)-based purchasing model (recommended).

dedicated - 20 vcore

https://learn.microsoft.com/en-us/azure/azure-sql/database/media/purchasing-models/pricing-model.png?view=azuresql

Managed Instance : PaaS but with dedicated rack

define shards



1-100

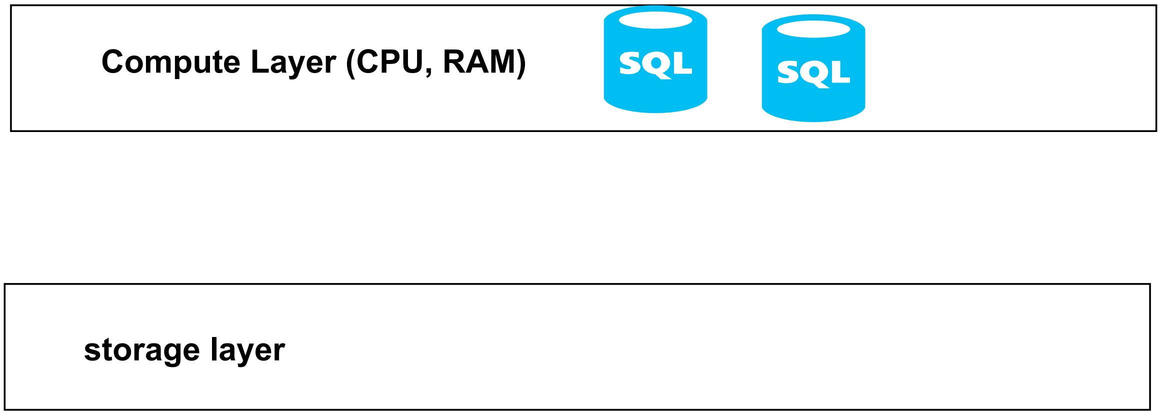
1-100

16 GB RAM

1 TB Disk

vertical scaling

Elastic Pool:

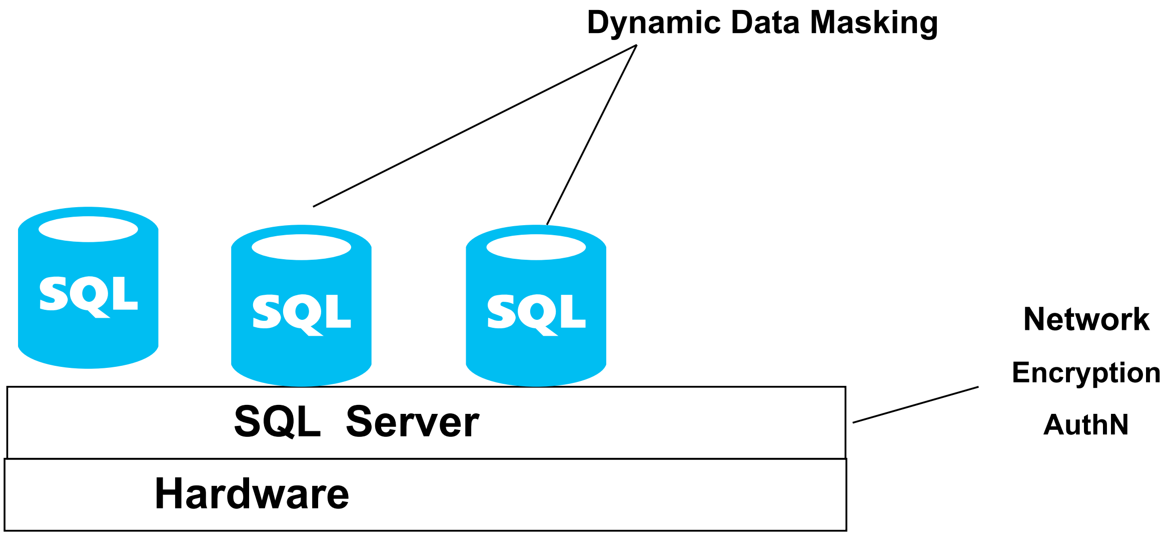


Compute Layer (CPU, RAM)

storage layer

Hyper Scale: Single DB

rapidly scale up + read only replica



Dynamic Data Masking

SQL Server

Hardware

Network

Encryption

AuthN

Entra ID = Conditional Access

PIM

No-SQL : Flexible schema

NO Rows and Columns

Modern Apps - Bank fraud detection,

Fake news (Originator,)

- Data deduplication, performance Scale

NO-SQL Types:

1. Graph Database: Neo4j, Apache gremlin

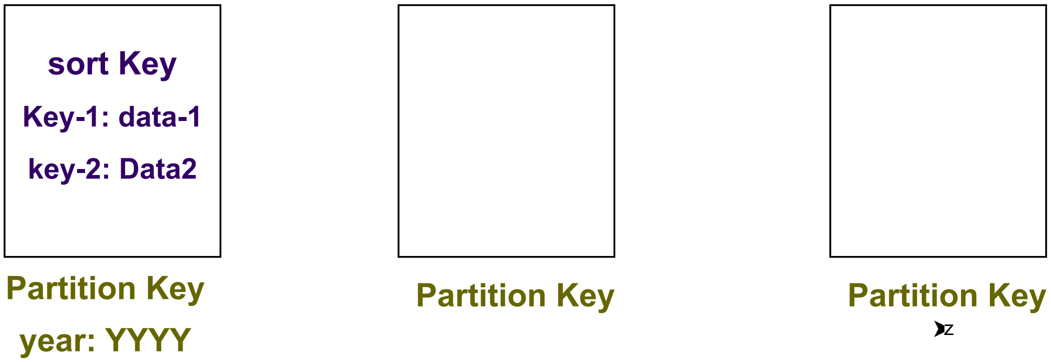
2. Document Database: MongoDB

JSON str

3. Redis - Store in-memory
milliseconds
session tokens

Key -Value Database: Ad TECH
horizontally

4. search databases:
designed indexing, aggregating results



sort Key
Key-1: data-1
key-2: Data2

Partition Key
year: YYYY

Partition Key

Partition Key

ID => 34 :: William USA
ID => 54 :: William UK

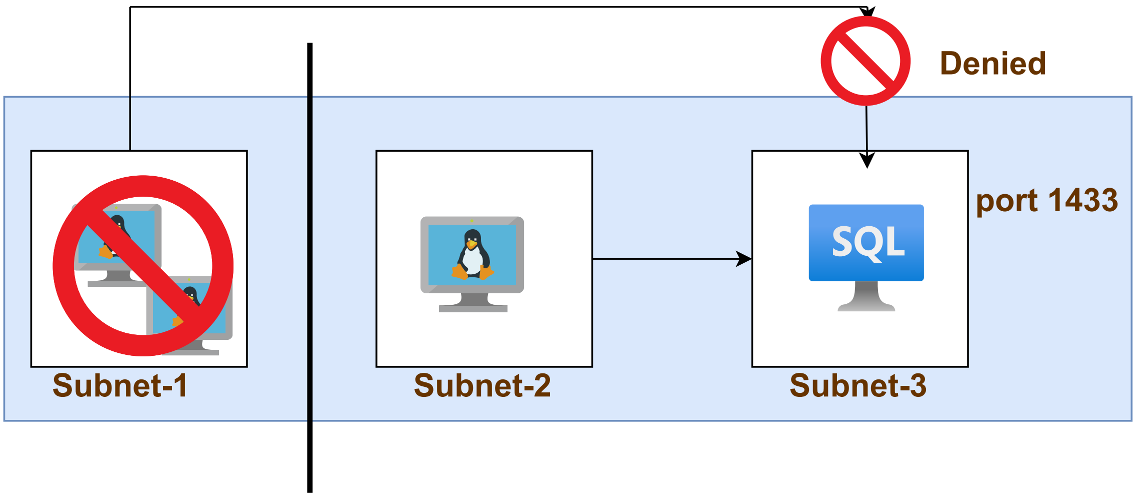
Partition Key: Any common Value

SQL => Primary Key

Key Value: Partition Key + Sort Key

Network => Facilities communication

country = Network



Denied

port 1433

Subnet-1

Subnet-2

Subnet-3

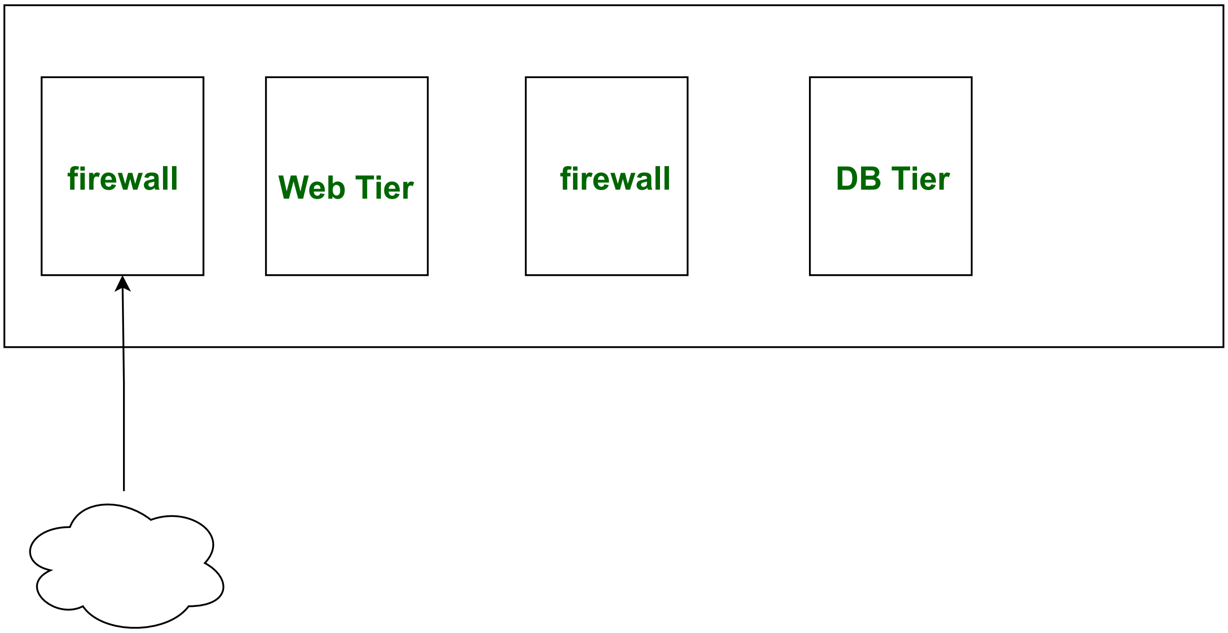
Protected Network - Firewall, WAF, IDPS, DDoS

1. Security
2. Managemnet

Subnet = Part of a Network

- machine are deployed

By convention = 1 subnet = 1 functional Requirement



firewall

Web Tier

firewall

DB Tier

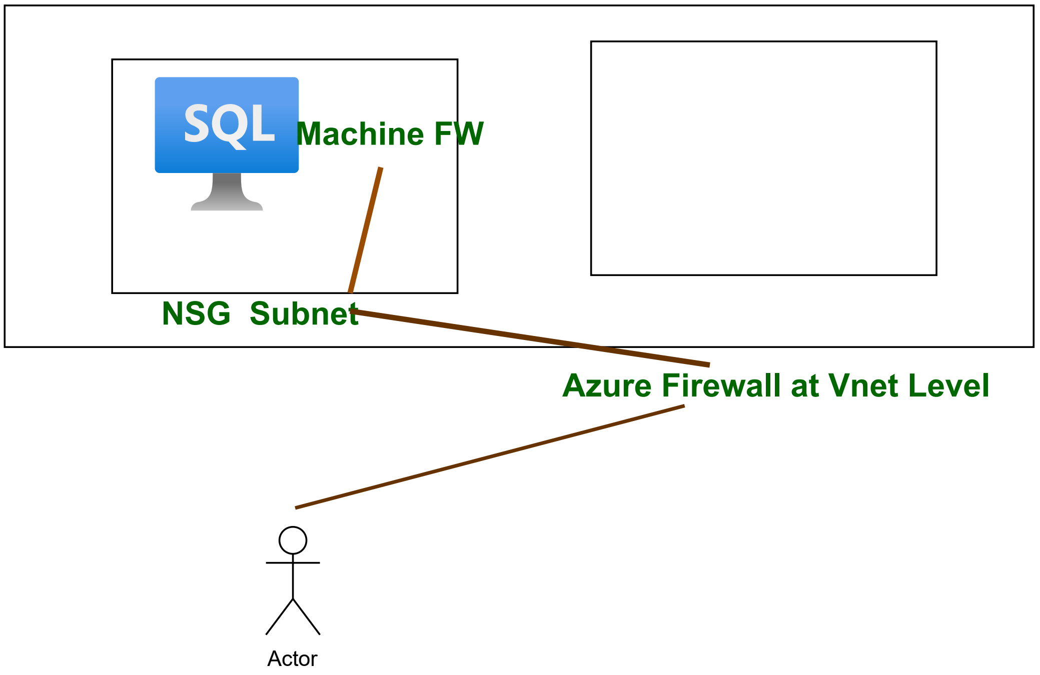
Machine => Private IP (ID) ==> Internal Network

Machine => Public IP [Optional] ==> Internet Network

PaaS - App Service, SQL, CosmosDB

- Connect PaaS via Virtual Network

1. Security
2. Cost Benefits
2. Speed



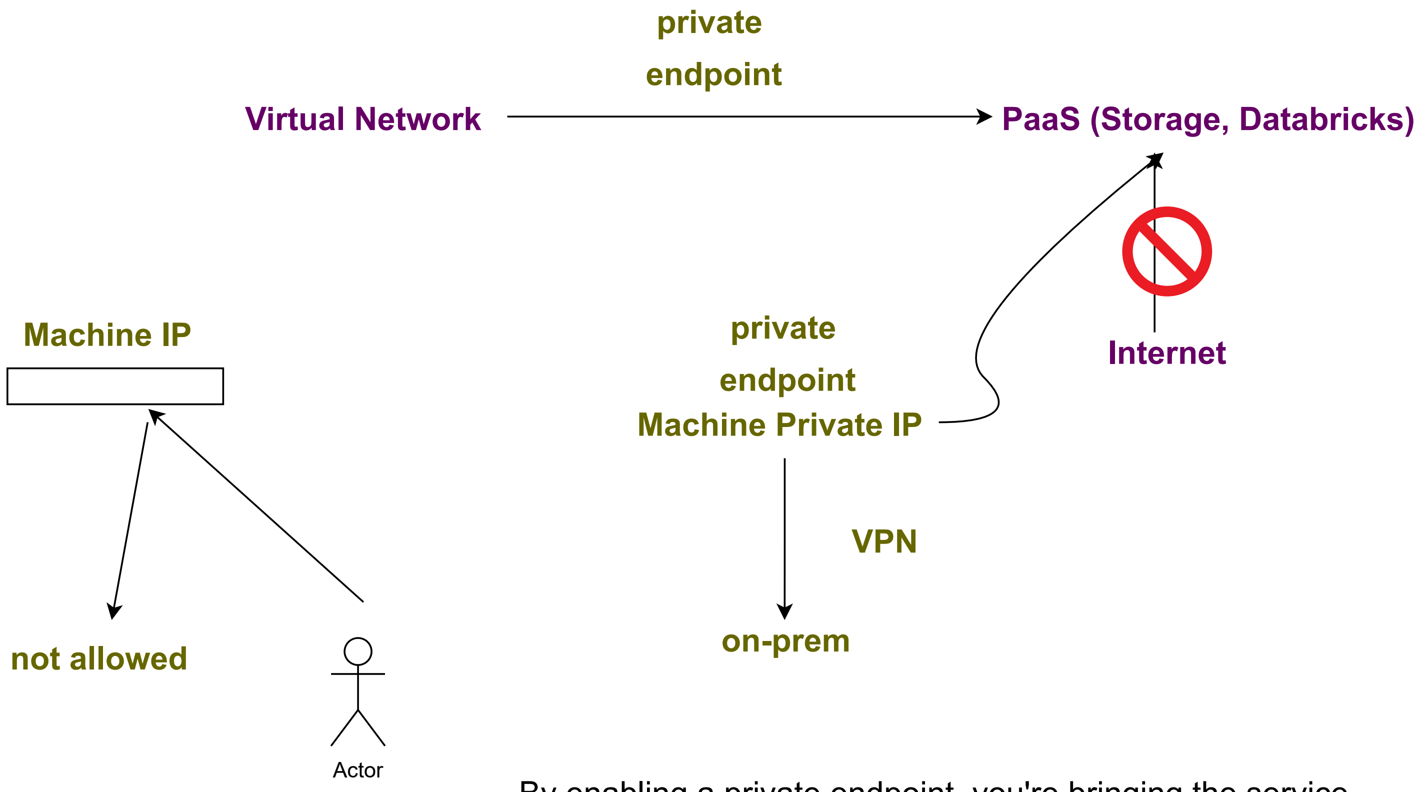
SQL

Machine FW

NSG Subnet

Azure Firewall at Vnet Level

Actor



private

endpoint

Virtual Network

PaaS (Storage, Databricks)

Internet

Machine IP

not allowed

Actor

private

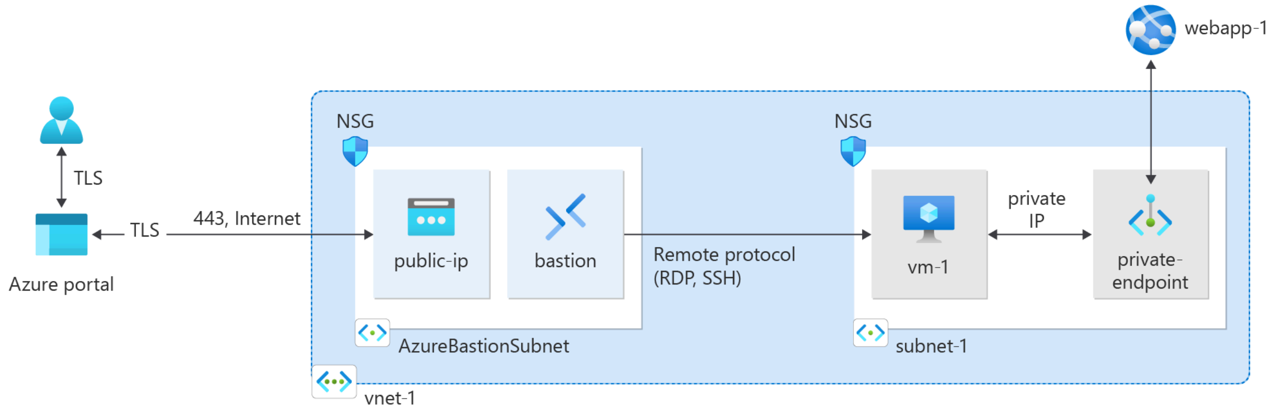
endpoint

Machine Private IP

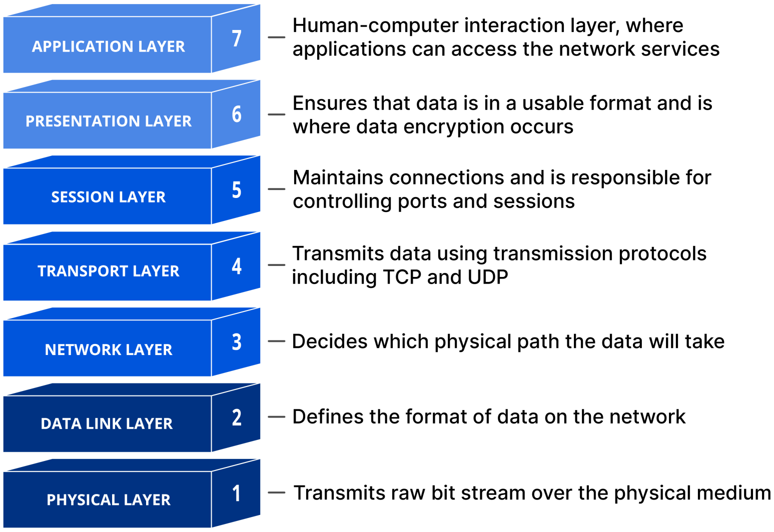
VPN

on-prem

By enabling a private endpoint, you're bringing the service into your virtual network.



OSI Model:



APPLICATION LAYER 7 — Human-computer interaction layer, where applications can access the network services

PRESENTATION LAYER 6 — Ensures that data is in a usable format and is where data encryption occurs

SESSION LAYER 5 — Maintains connections and is responsible for controlling ports and sessions

TRANSPORT LAYER 4 — Transmits data using transmission protocols including TCP and UDP

NETWORK LAYER 3 — Decides which physical path the data will take

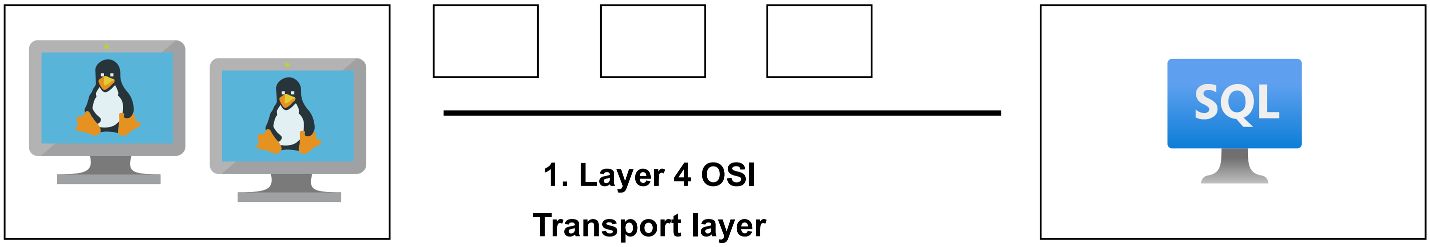
DATA LINK LAYER 2 — Defines the format of data on the network

PHYSICAL LAYER 1 — Transmits raw bit stream over the physical medium

Sender

2. HTTP Header

Reciever



1. Layer 4 OSI

Transport layer

Protocol = TCP / UDP

Ports =

Sender - Your Browser
Port = 443
protocol = tcp

Reciever = web server
https://

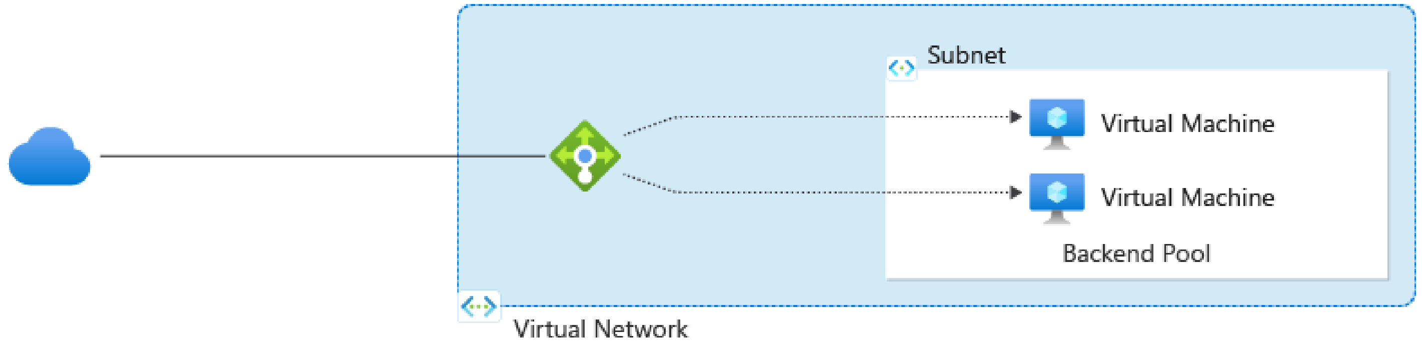
Thief's port for entry in your house = any window
Guest = main door

NOte: House address is same (IP adddress)

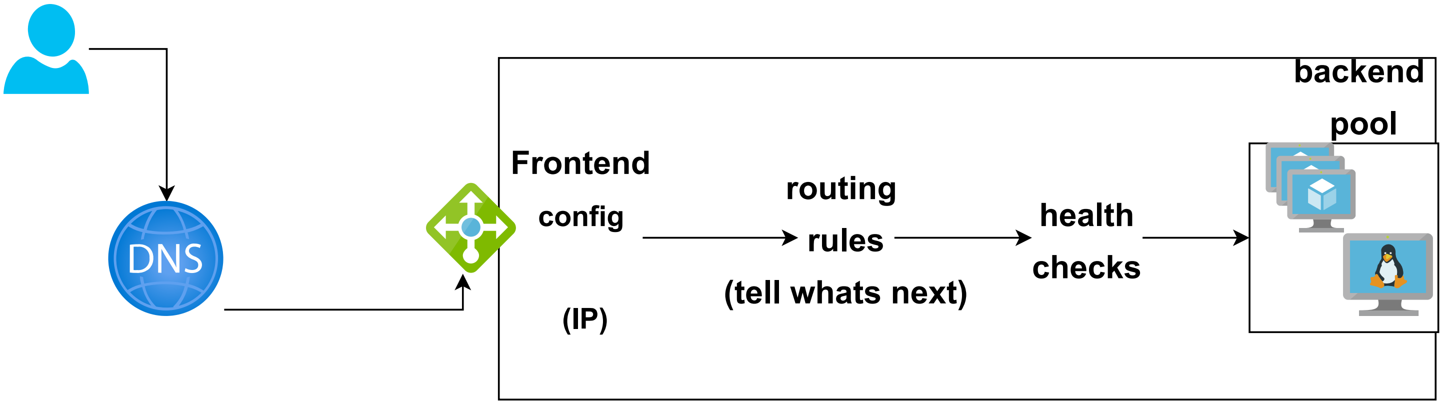
HTTP / HTTPS = Layer 7 of OSI

	Layer 7	Layer 4
regional	Application Gateway	Azure Load Balancer
Global	Front Door	Traffic Manager

Azure Load Balancer: Azure Load Balancer operates at layer 4
- single point of contact for clients
- These flows are according to configured load-balancing rules and health probes.
- Azure Virtual Machines or instances in a Virtual Machine Scale Set as backend



Azure Virtual Machine Scale Sets
let you create and manage a group of load balanced VMs.
The number of VM instances can automatically
increase or decrease in response to demand or a defined schedule.



Frontend config

(IP)

routing rules

(tell whats next)

health checks

backend pool

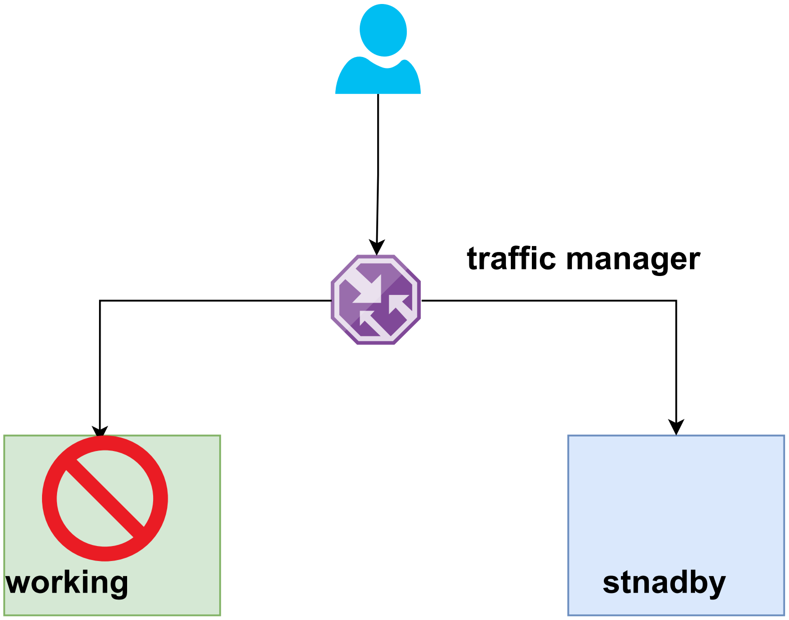
Azure Load Balancer

(all components in selected Vnet)

request-1,3 ==> vm1
request-2 => vm2 → round robin routing

Azure Traffic Manager is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness.

Comapny.com ==> IP



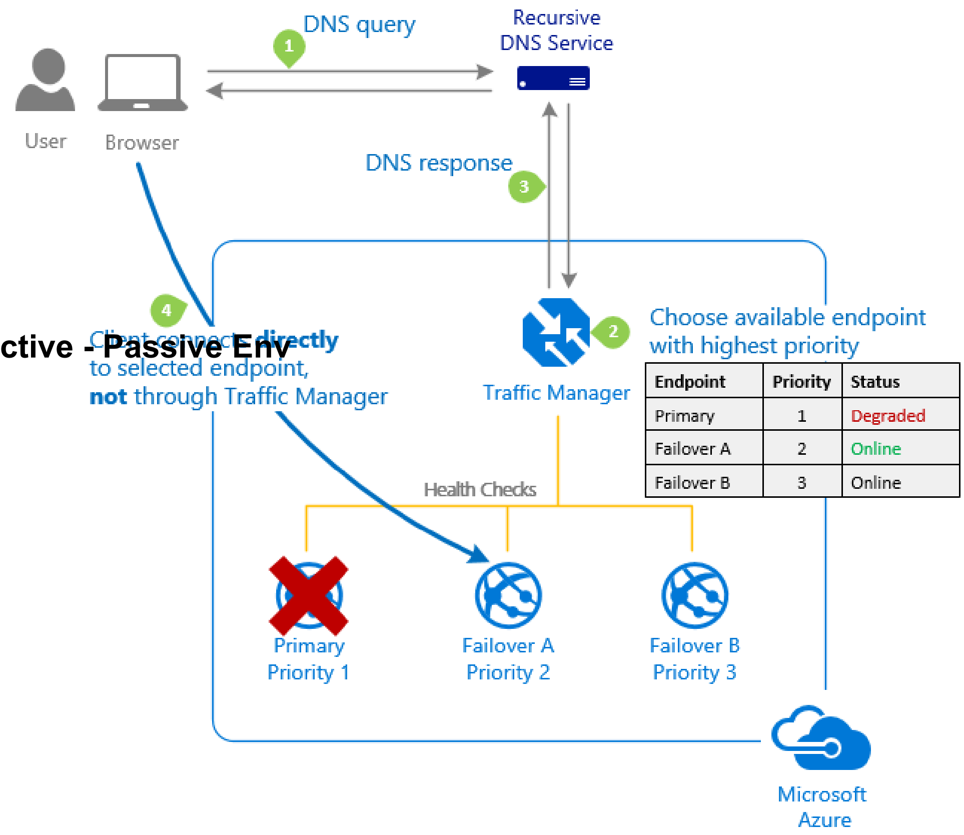
traffic manager

working

stnadby

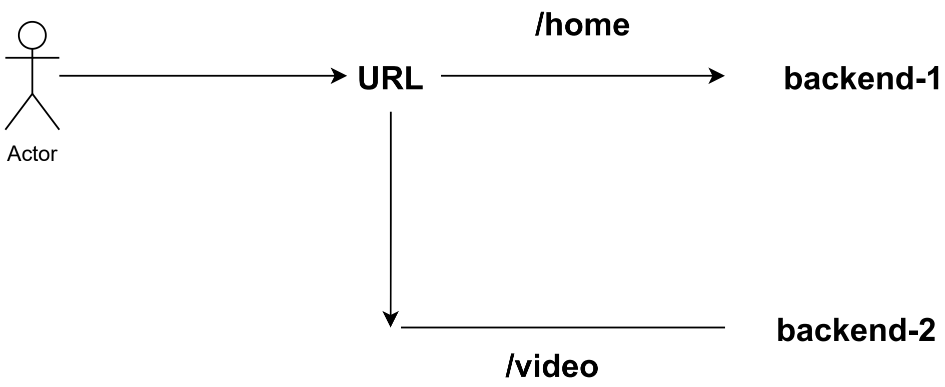
Active - Passive Env

Active - Passive Env



Endpoint	Priority	Status
Primary	1	Degraded
Failover A	2	Online
Failover B	3	Online

Layer 7 :

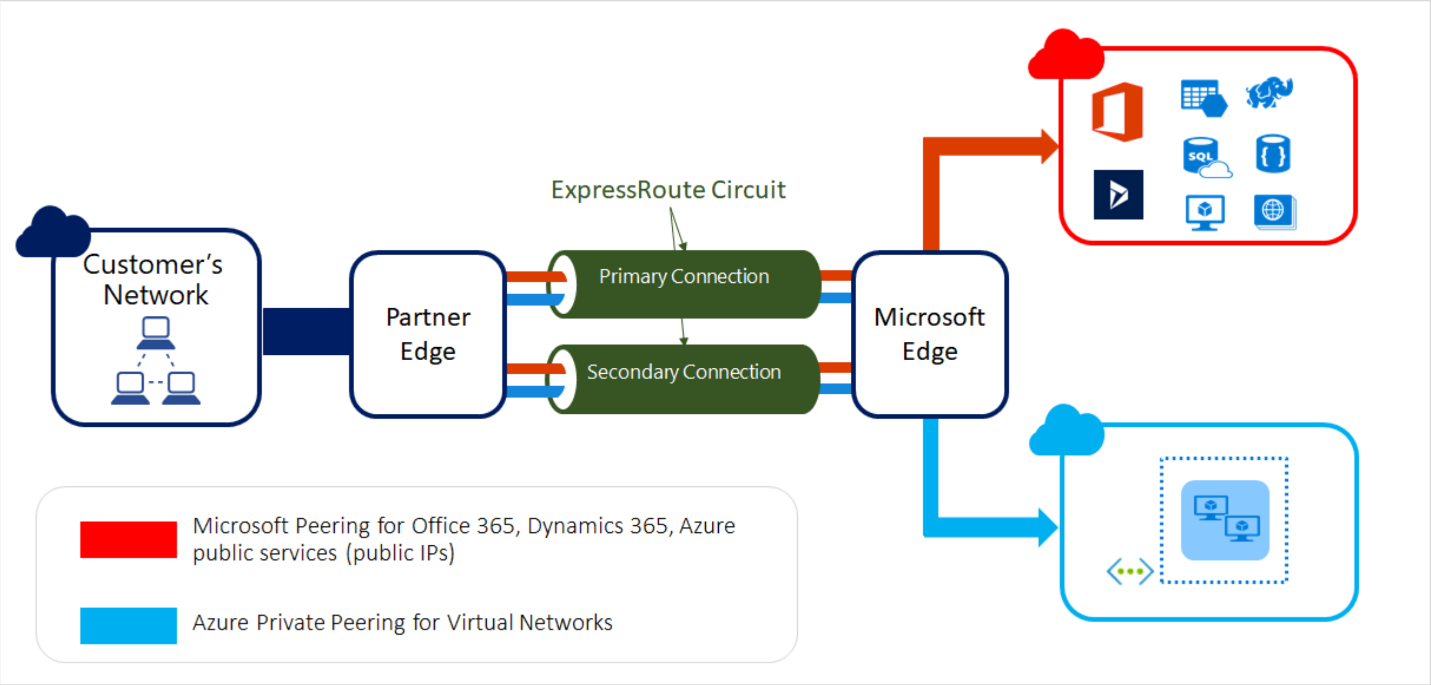


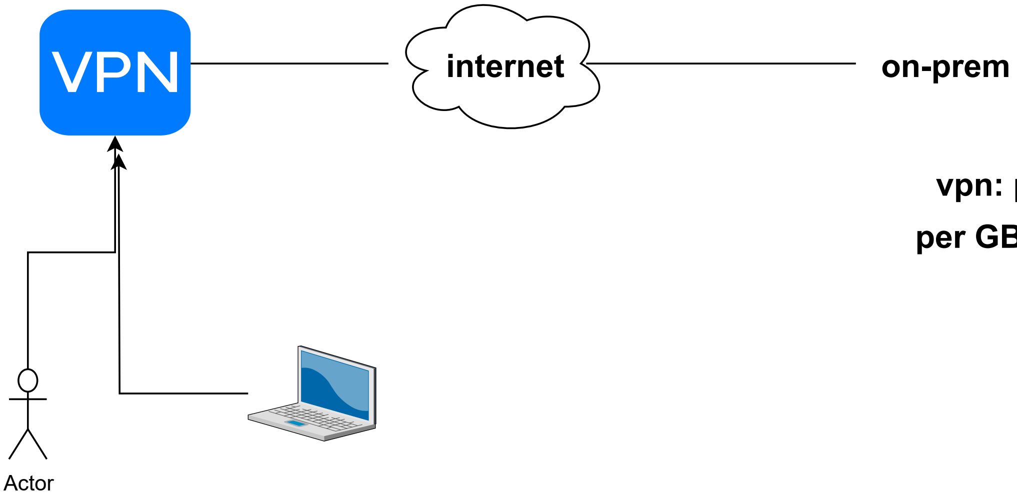
expressroute :

Physical Cable connection

[Hybrid Cloud]

offline [Private]


ExpressRoute Circuit
Customer's Network
Partner Edge
Primary Connection
Secondary Connection
Microsoft Edge
🟥 Microsoft Peering for Office 365, Dynamics 365, Azure public services (public IPs)
🟦 Azure Private Peering for Virtual Networks



vpn: per hour

per GB data cost

Defender for Cloud

Get continuous assessment and prioritized security recommendations with secure score, and verify compliance with regulatory standards

Secure Score - More Score
more Security

Azure, GCP, AWS

Key Vault - Secret Keeper
IAM :
Key vault admin = R/W to secrets
Key vult secret users = read access