AZ-900

Azure is a cloud service

We expect a few principles from a cloud:

- agility → ability to change as my needs change
- consumption based → connected to agility
- availability (HA) → there are mechanisms in place to give me high availability (e.g. distribution across racks, datacenters)
- disaster recovery → connected to availability
- scalability → there are always enough resources to meet my needs

TYPES OF CLOUD

Public cloud → externally hosted by a provider; it's multi-tenant, i.e. not exclusively dedicated to me. it's accessed over the internet; it's consumption based; it's distributed in many locations. Azure is an example.

Private cloud → using my own on premise infrastructure

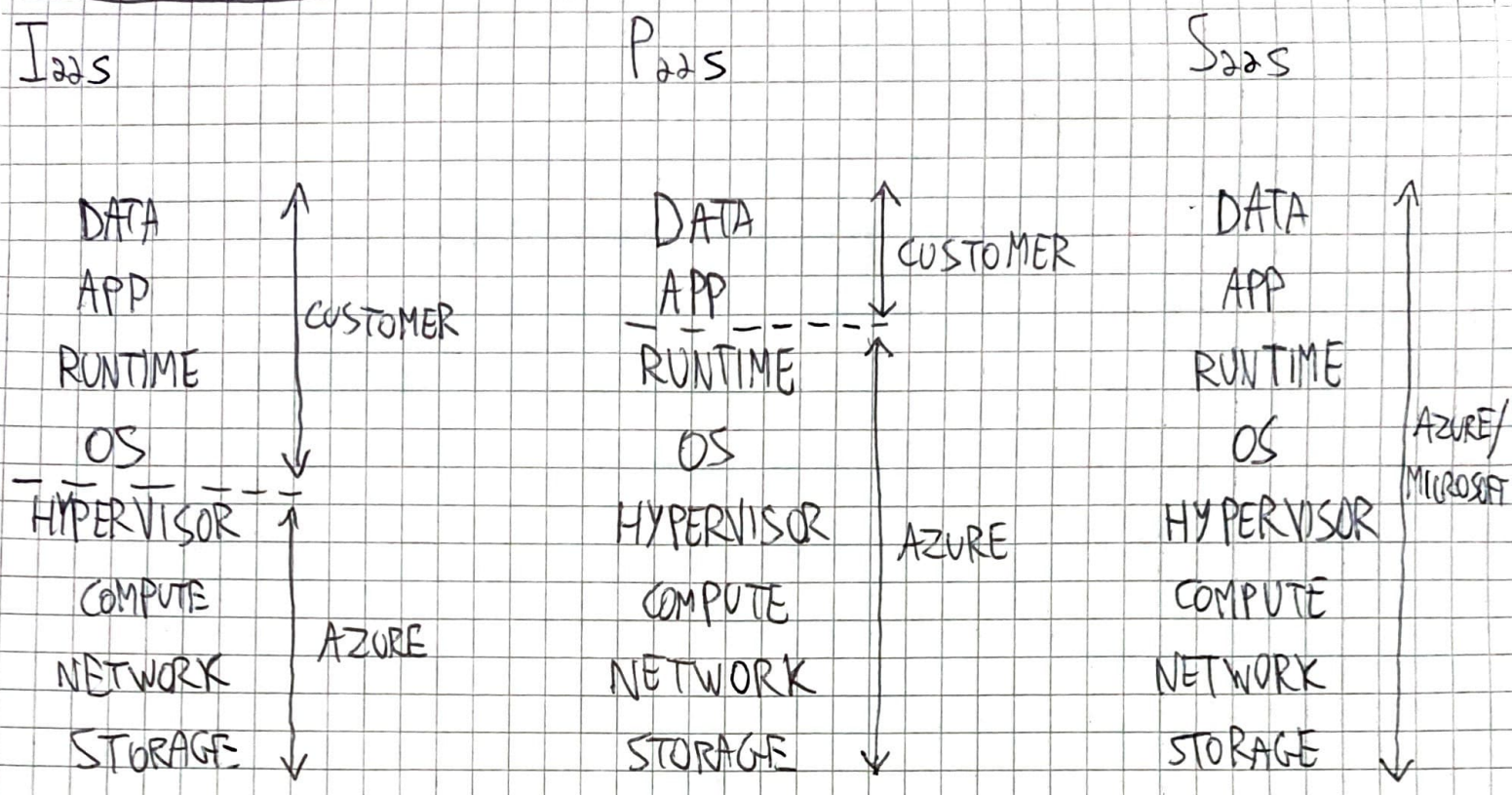
Hybrid cloud → I have both available

Anything on premises is CAP-EX (capital expenditure), i.e. I have to pay upfront. That can be painful.

Anything in the public cloud is OP-EX (operational expenditure), i.e. I pay as I go

SHARED RESPONSIBILITY

SHARED RESPONSIBILITY



REGIONS

A region is essentially a bunch of datacenters that are physically close to each other. An example might be East US.
They are important because some applications might need to meet data sovereignity requirements.
They're also important because I might want to have DR (Disaster recovery)

ENVIRONMENTS

- US gov.
- China
- Commercial (this is the one you're going to use usually)

Each environment has its own set of regions, different physical buildings etc. They're completely separated.

AVAILABILITY ZONES

Availability zones are basically each of the different datacenters that make up a region.

AZURE AD

Azure AD is an identity provider. It has a very "cloud" approach, in that it supports various protocols:

- OIDC
- SAML
- WS-FED

→ AUTHENTICATION (WHO I AM)

- OAuth 2.0 → AUTHORIZATION (WHAT I CAN DO)

I do authentication by proving:

- I know something (password)
- I have something (token, PC)
- I am someone (biometric)

These days MFA is very in vogue, and Azure supports that.

SCOPES

Management groups

Under my Azure AD I have a thing called the root management group.

Under that, I can create a hierarchy of other management groups.

Management groups get assigned RBAC, policy and budget. These things get inherited by the descendant groups underneath as well.

Subscriptions

Under management groups I can create subscriptions.

Just like management groups, I can apply RBAC, policy and budget to subscriptions

Resource groups

Resource groups get created inside of subscriptions. Here too I can apply RBAC, policy and budget.

Resource groups are NOT a boundary of connectivity. Resources in a resource group can connect to resources in different resource groups.

AZURE RESOURCE MANAGER

I have different ways to speak with the Azure Resource Manager:

- web portal (good for looking around)
- mobile app
- PowerShell az module (good for automation)
- az CLI (alternative to the PS module with different syntax)
- arm.json (good for creating)

RESOURCE LOCKS

Resource locks are a constraint on what I can delete or change. There are 2 types of locks:

- can not delete
- readonly (can't delete and can't modify)

Resource locks can be applied at different levels: subscriptions, resource groups and resources. They are inherited.

TAGS

Tags are metadata. They're basically key-value pairs.

Like resource locks, they can be applied to subscriptions, resource groups and resources.

Unlike resource locks, they do NOT inherit by default.

BLUEPRINTS

A blueprint is similar to a function in a programming language.

It contains instructions like create this tag, create a resource group, create these resources. Once the blueprint is assigned to a subscription, the function "runs"

TYPES OF RESOURCES

VMs

SKUs are basically identifiers for VMs. They indicate things like the generation of the processors, the number of processors, the amount of memory and any "special" capabilities.

If I don't want to share the physical server with other people's VMs, I can buy an Azure Dedicated Host. Like VMs, different kinds of hosts have different SKUs.

Isolated VMs are also a thing. It's basically the same thing as a dedicated host, except that a single giant VM occupies the entire host.

CONTAINERS

The most basic Azure service for containers is Azure Container Instances (ACIs). Azure Container Instances run by default on their own host, but I can have several ACIs share the same host by assigning them to a container group.

If you want a richer set of features and configuration capabilities, you're going to have to use AKS.

APP SERVICES

App Services are usually for workloads like web apps or web APIs. Azure manages the runtime (e.g. .NET). It can also run containers.

SERVERLESS SERVICES

Traditional cloud offerings are VM-based, essentially you rent a unit of a VM.

In serverless offerings, instead, you pay for the unit of work done.

Serverless services are usually event driven.

Azure Functions

Azure Functions are essentially a shippet of code that runs when some event happens. They are usually stateless and short lived.

Azure Logic Apps

It's a low code alternative to Azure Functions.

AZURE VIRTUAL DESKTOP

It's a desktop environment session or an app session (basically I only have access to one window)

AZURE KEY VAULT

It can store secrets, keys, certificates and supports RBAC and policy.

NETWORKING

A virtual network cannot span regions or subscriptions.

A virtual network needs to have 1 or more IPv4 ranges. It's common to use RFC1918 (ranges that will never route to the internet).

Within a virtual network I can have virtual subnets.

Networks span availability zones, as long as they're in the same region.

You can peer different vnets and have them communicate through Azure's backbone.

We can also connect vnets to our own on premise network through a VPN tunnel.

DDoS

Azure has both basic and standard DDoS protection.
Basic is the free offering and it protects only against "massive" attacks. Standard has a more advanced kind of protection.

STORAGE ACCOUNTS

A storage account lives in a region.

When I create a storage account I can choose what kind of resiliency I want:

- LRS: 3 copies of the data that all live within the same datacenter (availability zone)
- ZRS: 3 copies spread across different availability zones within the same region.
- GRS: 6 copies, 3 of them are in a different (paired) region
- GZRS: 6 copies, 3 in paired region, the other 3 spread across different availability zones

The redundancy type affects performance. In fact, in a "premium" storage account GRS and GZRS aren't available at all.

We have different types of storage accounts:

- blob (block, page or append)
- files (basically you can connect with SMB)
- queue
- tables (Key-value schemaless)

DATABASES

SQL

Azure SQL Database

It's a fully managed PaaS solution.

Azure SQL Managed Instance

Supports many features that aren't supported in Azure SQL Database.

Useful if you're migrating an on-prem database to the cloud and you depend on those features.

AZURE COSMOS DB

Cloud-native database. It's multi-model: I can store JSON documents, I could have column based data, I could have key-value pairs, I could have graphs.

AZURE STACK

Azure Stack is a service offered by Azure that allows you to run an Azure-like platform on-prem. It's essentially a form of private cloud.

HORIZONTAL AND VERTICAL SCALING

Horizontal scaling is when you have a VM and create multiple identical VMs to share the workload

Vertical scaling is when you have a VM and upgrade to one with more CPUs and memory.

AI SERVICES

Azure Machine Learning

Azure service for building and training models.

Azure Cognitive Services

Azure service that provides pre-trained models for a variety of use cases.

Azure Bot Services

Azure service for building bots that can interact with people.

COSTS AND OPTIMIZATION

Things that are going to affect the cost of a resource are:

- Type of resource (e.g. VM, storage account)
- SKU
- Tier (e.g. hot, cool)
- location

There are various strategies you can adopt to optimize costs:

- lifecycle management: Azure will automatically move your data from hot to cool tier and viceversa as needed
- autoscale: Azure will automatically delete and create resources as needed to handle the workload
- Azure reservations: you commit to using and paying for a certain amount of compute over a period of time (say 1 year); in exchange, you get a big discount.

Azure's <u>Pricing Calculator</u> can help you estimate your costs before you buy resources.

The <u>Total Cost of Ownership Calculator</u> can help you compare the costs of your on-prem infrastructure to what you would pay on Azure.

AZURE MONITOR

Azure Monitor is a sort of time series database where resource metrics and logs get sent to.

Metrics get sent by default, logs are opt-in. I have to enable them in the diagnostic settings.

I can create alert rules in Azure Monitor. If something meets the rule, an alert will be visible in Azure's portal.
Optionally I can also have actionables: for example, I can send an email or run an Azure Function when the rule is met.

RBAC

A role is essentially a set of actions.

When you assign a role, you assign it to a certain user AND in a certain scope (subscription, management group, resource group, resource)

Roles get inherited: if I have a role assigned to me in a management group, I also have that role in the subscriptions, resource groups and resources descended from it.

AZURE POLICY

Azure Policy allows you to define the requirements that have to be enforced. Some reasons for the requirements might be the law or internal company rules.

Policies can be applied to any scope (management group, subscription, resource group, resource). They get inherited.

A group of policies is called an initiative.

Policies can function in a number of modes (effects):

- audit → I don't want to enforce the policy, I just want to see what breaks which rules
- deny → enforce the policy
- append/modify → automatically adds or modifies tags on the resource

AGILITY AND ELASTICITY

Agility is about the ability to allocate and deallocate resources as my needs change

Elasticity is about Azure's ability to automatically scale resources, for example during peak activity hours.