Microsoft Azure Introduction

Table of Contents

What is Azure?

Microsoft calls their cloud service provider (**CSP**) Microsoft Azure Commonly referred to just **Azure**.

Cloud Concepts

Total Cost of Ownership (TCO)

- **CAPEX**: CAPEX means Capital Expenditure. It implies **spending money upfront** on physical infrastructure and deducting that expense from your tax bill over time.
    - Implies:
        - On-premise;
        - Software licenses fees;
        - Implementation;
        - Configuration;
        - Physical security;
        - Hardware;
        - IT peronnel;
        - Maintenance.

      With Capital Expenses you have to guess upfront what you plan to spend!
- **OPEX**: OPEX means Operational Expenditure. It is the costs associated with an on-premises datacenter that has shifted the cost to the service provider. The customer only has to be concerned with non-physical costs.
  Of course, with OPEX you can try a product or service without investing in equipment
    - Implies:
        - Azure;
        - Subscription fees;
        - Implementation;
        - Configuration;
        - Training.

      Moving from on-prem to the Cloud could bring up to 75% savings.

Azure Technology Overview

Azure Computing Services

- **Azure Virtual Machines** (**VMs**): Windows or Linux virtual machines (VMs) are the most common type of compute. You choose your OS, Memory, CPU, Storage and share hardware with other customers;
- **Azure Container Instances**: Docker as a Service Run containerized apps on Azure without provisioning servers or VMs;
- **Azure Kubernetes Service** (**AKS**): Kubernetes as a Service. Easy to deploy, manage and scale containerized applications. It uses the open source Kubernetes (K8) software;
- **Azure Service Fabric**: Tier-1 Enterprise Containers as a Service Distributed systems platform. Runs in Azure or on-premises. Easy to package, deploy, and manage scalable and reliable **microservices**.
- **Azure Functions**:
  - Event-driven, serverless compute (functions) run code without without provisioning or managing servers.
  - You pay only for the compute time you consume.
- **Azure Batch**:
  - Plans, schedules and executes your batch computer workloads across running 100+ jobs (i.e., the code that you want to run) in parallel.
  - Use Spot VMs to save money (previously used Low-priority VMs to save on compute).

Azure Storage Services

- **Azure Blob Storage**:
  - Object Serverless Storage. Store very large files and large amounts of unstructured files.
  - Pay only for what you store, unlimited storage, no-resizing volumes, filesystem protocols -> this is why it is called **serverless** storage.
- **Azure Disk Storage**:
  - A virtual volume. Choose SSD or HDD, encryption by default, attach volume to VMs.
  - Basically an hard drive in the cloud.
- **Azure File Storage**:
  - A shared volume that you can access and manage like a file server (e.g., throught the SMB protocol).
- **Azure Queue Storage**:

    - Listed here just because it has the word "storage" in their name, but it is actually for **messaging queue**.
        - A data store for queuing and reliably delivering messages between applications.
- **Azure Table Storage**:
    - This one, instead, should stay among DBs since it is a **Wide-Column NoSQL Database**.
        - A NoSQL store that hosts unstructured data independent of any schema.
- **Azure Data Box** (and its upgraded version **Azure Databox Heavy**):
    - A rugged briefcase computer and storage designed to move terabytes or petabytes of data.
- **Azure Archive Storage**:
    - Long term cold storage for when you need to hold onto files for years on the cheapest storage options.
- **Azure Data Lake Storage**:
    - A centralized repository that allows you to store all your structured and unstructured data at any scale.

Azure Database Services

- **Azure Cosmos DB**:
    - A fully managed NoSQL databases. Designed for scale with guarantee of 99.999% availability.
    - Azure's flagship database service.
- **Azure SQL Database**:
    - For the MS SQL Engine.
    - It is a fully managed MS SQL database with auto-scale, integral intelligence, and robust security.
- **Azure Database for MySQL / PSQL / MariaDB**
    - Fully managed and scalable MySQL / PostgreSQL / MariaDB database with high availability and security.
- **SQL Server on VMs**:
    - Again, for the MS SQL Engine.
    - Host enterprise SQL Server apps in the cloud. Lift-and-shift MS SQL servers from on-premise to Azure Cloud.
- **Azure Synapse Analytics** (Azure SQL Data Warehouse):
    - Fully managed data warehouse with integral security at every level of scale at no extra cost.
- **Azure Database Migration Service**:
    - To migrate your databases to the cloud with no application code changes.
- **Azure Cache for Redis**:
    - Caches frequently used and static data to reduce data and application latency.

- **Azure Table Storage**:
    - Already listed in the Storage Services section, but it is actually a DB.
    - Wide-Column NoSQL Database A NoSQL store that hosts unstructured data independent of any schema.

Azure Application Integration Services

Application Integration are services designed to help apps or services talk to each other.

- **Azure Notifications Hub**:
    - It uses a Pubblisher/Sububscription technology to send push notifications to any platform from any back end.
- **Azure API Apps**:
    - API Gateway:
        - Quickly build and consume APIs in the cloud. Route APIs to Azure Services.
- **Azure Service Bus**:
    - **Service Bus**:
        - Reliable cloud messaging as a service (Maas) and simple hybrid integration.
- **Azure Stream Analytics**:
    - Serverless **real-time** analytics, from the cloud to the edge
- **Azure Logic Apps**:
    - To schedule, automate and orchestrate tasks, businesses processes and workflows.
    - Integration with Enterprise SaaS and Enterprise applications.
- **Azure API Management**:
    - Hybrid, multi-cloud management platform for APIs across all environments. I.e., it puts in-front of existing APIs to add additional functionality.
- **Azure Queue Storage**:
    - Already listed in the Storage Services section, but it an Application Integration service.
    - **Messaging Queue**: a data store for queuing and reliably delivering messages between applications.

Developer and Mobile Tools

- **Azure Signal Service**:
    - **Real-Time Messaging** service: easily add real-time web functionality to applications.
    - Not to be confused with Azure Notification service.
    - Think of it like the Pusher for Azure.
- **Azure App Service**:

    - Easy to use service for deploying and scaling web-applications with .Net, Node.js Java, Python and PHP.
    - It is for developers focus on building their web-apps, and not worry about the underlying infrastructure. Think of it like **Heroku** for Azure.
- **Visual Studio**:
    - Code Editor: the IDE designed for creating powerful, scalable applications for Azure.
- **Xamarin**:
    - Mobile-App Framework to create powerful and scalable native mobile apps with .NET and Azure.

Azure DevOps Services

- **Azure DevOps**: plan smarter, collaborate, and ship faster with a set of modern dev services.
    - **Azure Boards**:
        - **Kanban board** to deliver value to your users faster using proven agile tools to plan, track, and discuss work across your teams.
    - **Azure Pipelines**:
        - Build, test, and deploy with CI/CD that works with any language, platform, and cloud.
        - Connect to GitHub or any other Git provider and deploy continuously.
    - **Azure Repos**:
        - Get unlimited, cloud-hosted private **Git repos** and collaborate to build better code with pull requests and advanced file management.
    - **Azure Test Plans**:
        - Test and ship with confidence using **manual and exploratory testing tools**.
    - **Azure Artifacts**:
        - Create, host, and share packages with your team, and add artifacts to CI/CD pipelines with a single click.
    - **Azure DeTest Labs**:
        - Fast, easy, and lean dev-test environments.

Azure Resource Manager

What is Infrastructure as code (IaC)? The process of managing and provisioning computer data centers through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools.
It means that we use scripts to set-up services like VM, DBs, Storage, etc. instead of doing it manually.

The IaC service in Azure is called **Azure Resource Manager**. It allows you to programmatically create Azure resources via a JSON template. For example, to launch a VM:

```
{
    "$schema": "https: //schema.management.azure.com/schemas/2019-04-01/deploymentTempla
    "resources": [{
        "type": "Microsoft.Compute/virtualMachines",
        "name": "MyServer",
        "properties": {
            "hardwareProfile": {
                "vmSize": "Standard_A4",
            }
        }
    }]
}
```

Azure QuickStart Templates

Azure QuickStart is a library of a **pre-made Azure Resource Manager (ARM) templates** provided by the community and partners to help you quickly launch new projects for a variety of stack scenarios:

- You can go to the Azure QuickStart Templates to find a template to deploy a Django app on Azure.
- You can deploy Ubuntu with Docker Engine.
- You can deploy a CI/CD & Containerized App Deploy Docker Enterpise & Jenkins.

Azure Virtual Network (vNet) and Subnets

Virtual Network (Net) is a logically isolated section of the Azure Network where you launch your Azure resources.
When you create a vNet, you choose a range of IPs using **CIDR Range**. A Subnet is a logical partition of an IP network into multiple smaller network segments.

- You breaks up your IP range for vNet into smaller networks.
- Subnets need to have a smaller CIDR range than to the vNet represent their portion.
- A **public subnet** is one that can reach the internet. E.g., good for a web app.
- A **private subnet** is one that cannot reach the internet. E.g., good for a DB.

Cloud-Native Networking Services

- **Azure DNS**: provides **ultra-fast** DNS responses and ultra-high domain availability.

- **Azure Virtual Network (NET)**: a logical isolated section of the Azure network for customers to launch Azure resources within.
- **Azure Load Balancer**: OSI Level 4 (Transport) Load Balancer for TCP and UDP traffic.
- **Azure Application Gateway**: OSI Level 7 (HTTP) Load Balancer, can apply a Web Application .Firewall.
- **Network Security Groups**: a virtual firewall at the subnet level.

Enterprise/Hybrid Networking Services

This is when you are using networking that is going to bridge on-prem to the cloud.

- **Azure Front Door**: a scalable and secure entry point for fast delivery of your global applications, i.e., a secure entry point into Azure from outside.
- **Azure Express Route**: a connection between your on-premise to Azure cloud from 50 Mbps to 10 Gbps.
- **Virtual WAN**: a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface.
- **Azure Connection**: a VPN connection securely connects two Azure local network via (**IPsec**).
- **Virtual Network Gateway**: a site-to-site VPN connection between an Azure virtual network and your local network.

Azure Traffic Manager

This service operates at the **DNS layer** to quickly and efficiently direct incoming DNS requests based on the **routing method of your choice**.

- Route traffic to servers the geographically near by to reduce latency.
- Fail-over to redundant systems in-case primary systems become unhealthy.
- Route to random VM to simulate A/B testing.

For example: a company has a production Server and a beta Server and it just want that 20% of the users use the beta server, e.g., using a **weighted** routing method.

Azure DNS

Azure DNS allows you to host your domains names on Azure. You can create **DNS Zones** and manage your **DNS records**.
Note that Azure DNS does not allow you to purchase domains, only the ability to manage DNS records.

Azure Load Balancer

Azure Load Balancer is used for evenly distributing incoming network traffic across a group of backend resources or servers. It operates on **OSI Layer 4** (Transport).
You can create a:

- Public Load Balancer incoming traffic from the internet to public-facing servers (Public IPs);
- Internal (Private) Load Balancer incoming internal network traffic to private-facing servers (Private IPs);

Scale Sets

It allows you group together identical Virtual Machines (VMs) and automatically increase or decrease the amount of servers based on:

- Change in CPU, memory, disk, and network performance;
- On a predefined schedule;

-> Elasticity!

IoT Services

- **IoT Central**: connects your IoT devices to the cloud.
- **IoT Hub**: enables highly secure and reliable communication between your IoT application and the devices it manage.
- **IoT Edge**: a fully managed service built on Azure IoT Hub. It allows data processing and analysis nearest the IoT devices. Edge computing is when you offload compute from the cloud to local computing hardware such as IoT devices, phones or home computers.
- **Windows 10 IOT Core Services**: a cloud services subscription that provides the essential services needed to commercialize a device on Windows 10 IoT Core. Long-term OS support and services to manage device updates and assess device health.

Big Data and Analytics Services

- **Azure Synapse Analytics** (*formally known as SQL Data Warehouse*): enterprise data warehousing and Big Data analytics. Intended to run SQL queries against large databases for things such as **reporting**.
- **HDInsight**: run **open-source analytics software** such as Hadoop, Kafka and Spark.
- **Azure Databricks**: an Apache Spark-based analytics platform optimized for the Microsoft Azure cloud services platform. Third-Party Databricks cloud services supported within Azure.

- **Data Lake Analytics**: an on-demand analytics job service that simplifies big data.
  - A **data lake** is a storage repository that holds a vast amount of **raw data** in its native format until it is needed.

AI ML Services Introduction

- **Background**:
  - Artificial Intelligence (**AI**): machines that perform jobs that mimic human behavior.
  - Machine Learning (**ML**): machines that get better at a task without explicit programming.
  - Deep Learning (**DL**): machines that have an artificial neural network inspired by the human brain to solve complex problems.
- **Azure Machine Learning Service**: a service for that simplifies running AI/ML related workloads allowing you to build flexible Pipelines to automate workflow. Use Python an R, Run DL workloads such as Tensorflow.
- **Azure Machine Learning Studio** (legacy): an older service that manages AI/ML workloads. Does not have a pipeline and other limitations. Workloads are not easily transferable to from classic to the new service.
  - Avoid it.

AI ML Services

- **Personalizer**: deliver rich, personalised experiences for every user.
- **Translator**: add real-time, multi-language text translation to your apps, website and tools.
- **Anomaly**: detector Detect anomalies in data to quickly identify and troubleshoot issues.
- **Azure Bot Service**: intelligent, serverless bot service that scales on demand.
- **Form Recogniser**: automate the extraction of text, key/value pairs and tables from your documents.
- **Computer Vision**: easily customise computer vision models for your unique use case.
- **Language Understanding**: build natural language understanding into apps, bots and IoT devices.
- **QnA Maker**: create a conversational question-and-answer bot from your existing content.
- **Text Analytics**: extract information such as sentiment, key phrases, named entities and language from your text.
- **Content moderator**: moderate text and images to provide a safer, more positive user experience.
- **Face**: detect and identify people and emotions in images.
- **Ink Recogniser**: recognise digital ink content, such as handwriting, shapes and document layout.

Serverless Services

Serverless means that the underlying servers, infrastructure and OS is taken care of by the Cloud Service Provider (CSP) It will generally be highly available, scalable and cost-effective.

- **Event driven**: serverless is **event-driven at scale**, i.e., a serverless function can be triggered or trigger other events allowing you to compose complex applications and its just scales.
- **Abstraction of Servers**: servers are abstracted away. Your code is described as functions. These functions can be running on different compute instances.
- **Micro-Billing**: Serverless compute could run for a fraction of a second. Billing into micro-seconds will save you money!

Services:

- **Azure Functions**: run small amounts of code known as serverless functions in your favorite language: C#, Java, JavaScript, Python and PowerShell.
- **Blog Storage**: Serverless Object Storage. Just upload files, don't think about the underlying file-systems, resizing.
- **LogicApps**: allows you to build serverless workflows composed of Azure Functions. Building a state machines for serverless compute.
- **Event Grid**: uses Pub/Sub messaging system to allow you react to events and trigger other Azure cloud services such as Azure Functions.

Management Tools

Azure Portal

The Azure portal is a web-based, unified console that provides an alternative to command-line tools. You can manage your Azure subscription with the Azure portal. Build, manage, and monitor everything from simple web apps to complex cloud deployments.

- **Azure Preview Portal**: in here, you can utilize new features that are in: preview, beta, other pre-release. Hence, If you want to test preview features should use preview.portal.azure.com, if you want to use stable-release and production-ready features you should you use portal.azure.com

Azure PowerShell

PowerShell is a task automation and configuration management framework. But also, a command-line shell and a scripting language.

Unlike most shells, which accept and return text, PowerShell is built on top of the .NET Common Language Runtime (CLR), and **accepts and returns NET objects** useful to automate scripting.

On Azure PowerShell, there is a set of `cmdlets` for managing Azure resources directly from the PowerShell command line.

Visual Studio Code

Azure has a service called **Visual Studio Workspaces** that allows you to spin up developer environments in using VScode right in the cloud.

Azure Cloud Shell

Azure Cloud Shell is an interactive, authenticated, browser-accessible shell for managing Azure resources. It provides the flexibility of choosing the shell experience that best suits the way you work, either **Bash** (🥺) or PowerShell.

Azure CLI

A Command Line Interface (CLI) processes commands to a computer program in the form of lines of text. Operating systems implement a command-line interface in a shell or terminal.
The Azure CLI can be installed on Windows, Mac and Linux. Once installed, you can type `az` followed by other commands to create, update, delete, view and manage Azure resources.

```
#!/bin/bash
# Create a resource group.
a group create --name myResourceGroup --location westeurope
# Create a new virtual machine, this creates SSH keys if not present.
az vm create - -resource-group myResourceGroup --name myVM - - image UbuntuLTS --genera
```

Messing with Azure

Create a Resource Group

1. Find and open **Resource Group** in the Azure Portal;
2. Click on **Add**;
3. Fill the form:
    - **Subscription**: Free Trial;
    - **Resource group**: `myResourceGroup` ;

   - **Region**: West Europe;
4. **Review + create**;
5. **Create**;
6. Wait for the deployment to complete and refresh after a while.

Create a vNet

1. Find and open **Virtual networks** in the Azure Portal;
2. Click the **Add** button;
3. Fill the form in the **Basics** tab:
   - **Subscription**: Free Trial;
   - **Resource group**: `myResourceGroup` ;
   - **Name**: `myVNet` ;
   - **Region**: West Europe;
4. Take a look to the **IP Addresses** tab:
   - **IPv4 address space**: the `/16` default range is fine;
   - The deafult `/24` range for the **Subnet** will be fine;
5. Adding stuff from the **Security** tab is not necessary for now and it will cost money (💸);
6. **Review + create**;
7. **Create**;
8. Wait for the deployment to complete;
9. **Go to resource**: a bunch of information about the subnet will be displayed and could be edited if necessary.

Launching a Server

1. Find and open **Virtual machines** in the Azure Portal;
2. Choose a **Resource group**;
3. Call the VM **myVM**;
4. Choose a **Region**;
5. Pick **No infrastructure redundancy required** as availability options;
6. Pick an **Ubuntu Server** image;
7. Pick a **Standard B1s** size, since it is just an example and it does cost real money (💸);
8. The **Authentication type** should be **SSH**, but it need some configuration, hence just pick **Password**;
9. Set the **Username** and **Password**;
10. No need to add **Inbound ports**;

11. On the **Disks** tab, **Premium SSD** is ok and even the defaul **Encryption type** should be fine;
12. Check the **Networking** tab and set:
    - **Virtual network**: `myVNet` ;
    - **Subnet**: `default` ;
    - **Public IP**: `myVM-ip` ;
    - **NIC network security group**: `Basic` ;
13. **Management** tab should be fine;
14. **Advanced** tab should be fine;
15. **Review + create**;
16. **Create**;

Once the deployment is complete, you can click to **Go to resource** and see the VM details.
Once we are sure the VM is running and the configuration is correct, since we successfully saw how to launch a VM, we can now delete it to avoid unnecessary costs (💸).
To be sure it was deleted, we can also check the **Virtual machines** section in the Azure Portal.

Creating a Azure Serverles Functions

1. Find and open **Function App** in the Azure Portal;
2. **Add**;
3. In the **Basics** tab:
    - **Subscription**: Free Trial;
    - **Resource group**: `myResourceGroup` ;
    - **Function App name**: `myFunctionApp` ;
    - **Publish**: Code;
    - **Runtime stack**: Node.js;
    - **Version**: 16;
    - **Region**: West Europe;
4. After a little bit of wandering among tabs: **Review + create**;
5. After the deployment is complete, **Go to resource**;
6. We can now create a function going to the **Functions** section on the left;
7. We select **HTTP trigger** and call it **myFunction**;
8. We can now write some code in the **index.js** file and perform some tests;
9. Lastly, we can delete the function app.

Storing files in Blob Storage

We said that Blob Storage is a serverless storage, hence we can store files without worrying about the underlying file-systems, resizing, etc.

1. Find and open **Storage accounts** in the Azure Portal;
2. **Add**;
3. In the **Basics** tab:
   - **Subscription**: Free Trial;
   - **Resource group**: `myResourceGroup` ;
   - **Storage account name**: `myBlogStorage` ;
   - **Performance**: Standard;
   - **Account kind**: BlobStorage;
   - **Region**: West Europe;
4. **Review + create**;
5. **Create**;
6. **Go to resource**;
7. We can now create a **Container** to store our files going to the **Blob service** section on the left and then **Containers**;
8. **+ Container**, we call it **myContainer** and set the **Public access level** to **Private**;
9. Now we can click on that container and, once insede, we can upload some files and see them in the **Blobs** section;
10. We can now delete the storage.

Exploring Azure Cloud Shell

Cloud Shell is accessible from anywhere inside the Azure Portal, it is among the icons on the top right.
It can be a **Bash** or a **PowerShell** shell. Once created the shell, e.g., a PowerShell we can type some commands:

```
PS Azure:\> clear
PS Azure:\> az account list
```

That's it, we can now turn off the shell.

Security

Azure Trust Center

It is a public-facing website portal providing easy access to **privacy** and **security** and **regulatory compliance** information.
Whatever the organization need to know about Azure security, privacy, and compliance, it is all in here, no login required:

- https://www.microsoft.com/en-us/trust-center/product-overview
- e.g., How GDPR is applied to Azure
- Of course, the most important part is the **Compliance** section.

Compliance Programs

Enterprise Companies WILL NOT BUY your software solutions unless its secure.
The compliances they looking for are:

- NIST 800-53;
- PIPEDA Compliant;
- HIPPA Compliant;
- FIPS-140-2 Compliant;

Some of the compliance programs are:

- **Criminal Justice Information Services (CJIS)**: any US state or local agency that wants to access the FBI's CJIS database is required to adhere to the CJIS Security Policy.
- **Cloud Security Alliance (CSA) STAR Certification**: independent third-party assessment of a cloud provider's security posture.
- **General Data Protection Regulation (GDPR)**: a European privacy law. Imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents.
- **EU Model Clauses**: contractual guarantees around transfers of personal data outside of the EU.
- **Health Insurance Portability and Accountability Act (HIPAA)**: US federal law that regulates patient Protected Health Information.
- **International Organization for Standardization (ISO) and and the International Electrotechnical Commission (IC) 27018**: code of practice, covering the processing of personal information by cloud service providers.

- **Multi-Tier Cloud Security (MTCS) Singapore**: Operational Singapore security management Standard. A common standard that cloud service providers (CSPs) can apply to address customer concerns about the security and confidentiality of data in the cloud, and the impact on businesses of using cloud services.
- **Service Organization Controls (SOC) 1, 2, and 3**: independent third-party examination reports that demonstrate how the company achieves key compliance controls and objectives.
- **National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)**: Voluntary Framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risks.
- **UK Government G-Cloud**: cloud computing certification for services used by government entities in the United Kingdom.
- **Federal Information Processing Standard (FIPS) 140-2**: US and Canadian government standard that specifies the security requirements for cryptographic modules that protect sensitive information.

Azure Active Directory

Azure Active Directory (Azure AD) is Microsoft's **cloud-based identity and access management service**, which helps your employees sign in and access resources.
It will work with external resources, such as:

- Microsoft Office 365;
- Azure Portal;
- SaaS Applications;

As well as with internal resources, such as:

- Applications within your intranet;
- Access to workstations on-premise;

Azure AD can implement **Single-Sign On** (**SSO**). With this property, a user logs in with a single ID and password to gain access to any of several related systems.

Azure AD comes in four editions:

- **Free**: MFA, SSO, Basic Security and Usage Reports, User Management;
- **Office 365 Apps**: Company Branding, SLA, Two-Sync between On-Premise and Cloud;
- **Premium 1**: Hybrid Architecture, Advanced Group Access, Conditional Access;
- **Premium 2**: Identity Protection, Identity Governance.

MFA

Multi-Factor Authentication (**MFA**) is a security control where after you fill in your username/email and password **you have to use a second device**, such as a phone, to confirm that its you logging in.
It protects against people who have stolen your password, and it is an option in most cloud providers.

Azure Security Center

Azure Security Center is a unified infrastructure security management system. It strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud.

Key Vault

Azure Key Vault helps you safeguard cryptographic keys and other secrets used by cloud apps and services.
It has many functionalities:

- **Secrets Management**: securely store and control access to tokens, passwords, certificates, API keys, and other secrets;
- **Key Management**: create and control encryption keys used to encrypt your data;
- **Certificate Management**: provision, manage, and deploy your public and private SSL certificates for use with Azure and internal connected resources;
- **Hardware Security Module**: secrets and keys can be protected either by software or FIPS 140-2 Level 2 validated HSMs.
    - An HSM is a Hardware Security Module, i.e., a piece of hardware designed to store encryption keys securely in the memory (volatile) and not on the disk, such that if a HSM is shut down the keys are lost;
    - HSMs that are multi-tenant are FIPS 140-2 Compliant (multiple customers virtually isolated on an HSM).
    - HSMs that are single-tenant are FIPS 140-3 Compliant (single customer on a dedicated HSM).

Azure DDoS Protection

Azure offers two tiers of DDoS Protection:

- **DDoS Protection Basic**:

  - Free;
  - Already turned on protect Azure's global network;
- **DDoS Protection Standard**:
  - Starting at $2,994/month;
  - Metrics, Alerts, Reporting;
  - DDoS Expert Support;
  - Application and Cost Protection SLAs.

Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. Basically, it is a vNet that decides which traffic to allow and which to deny to the other vNets

Its features are:

- Centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks;
- Uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network;
- High availability is built in, no additional load balancers are required;
- Can configure during deployment to span multiple AZ for increased availability;
- There's no additional cost for a firewall deployed in an Availability Zone (AZ);
- There are additional costs for inbound and outbound data transfers associated with AZs.

Azure Information Protection (AIP)

AIP protects sensitive information such as emails and documents with encryption, restricts access and rights, and integrates security in **Office apps**.

Application Gateway

Application Gateway is a **web-traffic load balancer** (Application Layer 7 HTTP) that re-route traffic based on a set of rules. A Web Application Firewall (WAF) can be attached for additional protection on OSI Layer 7.

Advanced Threat Protection (ATP)

The difference between an Intrusion Detection System (IDS) and an Intrusion Protection System (IPS) is that the IDS will only detect an attack, while the IPS will detect and block it.

Azure Advanced Threat Protection (**ATP**) is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Microsoft Security Development Lifecycle (SDL)

Microsoft Security Development Lifecycle (SDL) is an industry-leading software security assurance process. It is a Microsoft-wide initiative and a mandatory policy since 2004, the SDL has played a critical role in embedding security and privacy in Microsoft software and culture.

Building security into each SDL phase of the development lifecycle helps you catch issues early, and it helps you reduce your development costs.

Azure Security Policies

Azure Policy is a service you can use to create, assign, and manage policies of resources. A policy allows you to enforce or control the properties of a resource.

Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules. These business rules, described in `JSON` format, are known as **Policy Definitions**.

Role Based Access Control (RBAC)

It is a concept of how all the components of gaining access resources works.
Azure role-based access control (Azure RBAC) helps you manage **who has access to Azure resources**, what they can do with those resources, and what areas they have access to.
A Role Assignments is the way you control access to resources and consists of these three elements:

1. **Security Principal**: represents the identities requesting access to an Azure resource such as:
   - **User**: an individual who has a profile in Azure Active Directory;
   - **Group**: a set of users created in Azure Active Directory;
   - **Service Principal**: a security identity used by applications or services to access specific Azure resources;
   - **Managed identity**: an identity in Azure Active Directory that is automatically managed by Azure.
2. **Role Definition**: collection of **permissions**. A role definition lists the operations that can be performed, such as read, write, and delete. Roles can be high-level, like owner, or specific, like virtual machine reader.

Azure has built-in roles and you can define custom roles (not free).
These are the four fundamental built-in role:

	Read	Grant	Create, Update, Delete
Owner	X	X	X
Contributor	X	-	X
Reader	-	X	-
User Access Administrator	X	-	-

3. **Scope**: is the set of resources that access for the Role Assignment applies to. Scope performs Access Controls at the *Management* (management of a bunch of accounts), *Subscription* (individual accounts) or *Resource Group* (group of resources) level.

Lock resources

As an *admin*, you may need to lock a subscription, resource group, or resource to prevent other users from accidentally deleting or modifying critical resources.
In the Azure Portal you can set the following lock levels:

- `CanNotDelete` (**Delete** in the Azure Portal): authorized users can still read and modify a resource, but they can't delete the resource;
- `ReadOnly` (**Read-only** in the Azure Portal): authorized users can read a resource, but they can't delete or update the resource.

Management Groups

It is a way of managing multiple subscriptions (accounts) into a hierarchal structure.

- Each directory is given a single top-level management group called the "Root" management group.
- All subscriptions within a management group automatically inherit the conditions applied to the management group.

Azure Monitor

Azure Monitor comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments.
With AZ Monitor you can:

- Create visual dashboards to visualize the health of your resources;
- Create Smart Alerts;
- Create Automated Actions;
- Collect logs through Log Monitoring.

Service Health

Information about current and upcoming issues such as:

- Service impacting events;
- Planned maintenance;
- Other kind of changes that may affect your availability.

In particular:

1. Azure Status informs you of service outages in Azure;
2. Azure service health a personalized view of the health of the Azure services and regions you're using;
3. Azure resource health information about the health of your individual cloud resources, e.g., VMs.

Azure Advisor

Azure Advisor is a personalized **cloud consultant** that helps you follow best practices to optimize your Azure deployments. The Advisor dashboard displays personalized recommendations for all your subscriptions for the following 5 categories:

1. **High Availability**: improve the reliability of your applications;
2. **Security**: improve the security of your applications;
3. **Performance**: improve the performance of your applications;
4. **Cost**: optimize and reduce your overall Azure spend;
5. **Operational Excellence**: improve the management of your Azure resources.

Billing and Pricing

Service Level Agreements (SLAs)

Service Level Agreement (SLA) describes Azure's commitments for uptime and connectivity, e.g., 99.9999% uptime on one year base. Unfortunately, Azure SLAs are individualized per Azure Service, i.e., there is no an overall SLA for all the Azure Services.

Uptime and connectivity is described as **Performance Targets**, and a Performance Target is represented as a percentage %.

- 99% (two nines);
- 99.9% (three nines);
- 99.999% (five nines);
- 99.9999999% (nine nines).

The more the nines, the more expensive and reliable the service is. On this regard, Azure does not provide SLAs for the **Free Tier** or the shared tiers.

SLAs can be checked here.

Service Credits

Customers may have a discount applied to their Azure bill, as **compensation** for an under-performing Azure product or service based on the SLA.

For example, the Azure Virtual Machine Service Credi calculation is:

Montly Uptime Percentage	Service Credit Percentage
< 99.9%	10%
< 99%	25%
< 95%	100%

Composite SLAs

We said that Azure SLAs are individualized per Azure Service. A Composite SLA is the resulting SLA when you combine different service offerings.

For example, there is a Web App having a SLA of 99.95% and a SQL Database having a SLA of 99.99%. The Composite SLA is calculated as follows:

```
99.95% * 99.99% = 99.94%
```

Hence, the Composite SLA is 99.94%.
To improve the Composite SLA, you can use for example a queue havig a SLA of 99.9% to save the transaction requests done to the Web App when the DB is down and then process them later, when the Web App is up and running again. This bring the Composite SLA to:

```
Web App * (DB or Queue) = 99.95% * (99.99% + 99.9%) = 99.95% * 99.99999% = ~99.95%
```

Hence, the Composite SLA in this case is ~99.95%.

Total Cost of Ownership (TCO) Calculator

The TCO represents a way to estimate the cost savings you can realize by migrating your workloads to Azure. This is done through the TCP Calculator, which generates out a detailed report that can be exported as a PDF to send to decision makers.

- Resource: https://azure.microsoft.com/pricing/tco/calculator/

Azure Marketplace

Azure Marketplace are apps and services made available by third-party publishers to quickly get started. The available apps and services can be Free, Free-Trial, Pay-As-You-Go, Bring-Your-Own-License (BYOL).

The Azure Marketplace can be accessed from the Azure Portal.

Azure Support

Azure has four Support Plans:

- **Basic**: $0/month.
    - It is included in the Free Trial and gives email support only for billing and account management;
    - Azure Advisor, Azure Health Status, Community Support, Azure Documentation.
- **Developer**:
    - $29/month;
    - Email technical support during business hours;
    - Third party software support;
    - Minimal business impact (Sev C) < 8 hours;
    - Azure Advisor, Azure Health Status, Community Support, Azure Documentation.
- **Standard**:
    - $100/month;
    - Email support during business hour;
    - Phone technical support 24/7;
    - Third party software support;
    - Minimal business impact (Sev C) < 8 hours;

  - Moderate (Sev B) < 4 hours;
  - Critical business impact (Sev C) < 1 hour;
  - Azure Advisor, Azure Health Status, Community Support, Azure Documentation;
- **Professional Direct**:
  - $1000/month;
  - Email support during business hour;
  - Phone technical support 24/7;
  - Third party software support;
  - Minimal business impact (Sev C) < 4 hours;
  - Moderate (Sev B) < 2 hours;
  - Critical business impact (Sev C) < 1 hour;
  - Azure Advisor, Azure Health Status, Community Support, Azure Documentation;
  - Webinars and expertise support;
- **Enterprise**:
  - N/A data;
- Resources: https://azure.microsoft.com/en-us/support/plans/

Azure Licensing

- **Azure Hybrid Benefit**: allows companies to use their on-premise Windows Server licenses with Software Assurance to run Windows Server virtual machines on Azure at a reduced cost.
- Resources: https://azure.microsoft.com/en-gb/pricing/hybrid-benefit/#why-azure-hybrid-benefit

Azure Subscriptions

An Azure Subscription is the same as saying our Azure Account. There are four tiers of Azure Subscriptions:

- **Free Subscription**:
  - $0/month;
  - 12 months of some free services;
  - 200$ credit to spend in the first 30 days;
- **Pay-As-You-Go Subscription**:
  - Credit card required;
  - Charged at the end of the month for what you used;
- **Enterprise Agreement Subscription**:
  - An Enterprise and Azure agree on receive discounted price for licenses and cloud services;
- **Student Subscription**:
  - No Credit Card Required;

  - $100 USD credits for 12 months;
  - Requires valid student email.

Pricing Calculator

Configure and estimate the costs for Azure products. No Sign-in require. Download an Excel spreadsheet and share with your boss.

- Resources: https://azure.microsoft.com/pricing/calculator

Azure Cost Management

This service permits to:

- Perform **cost-analysis**, visualize the spending of your Azure cloud resources;
- Create **budgets**, set a budget threshold be alerted when approaching or exceeded.