Notes for AZ-900 Fundamentals

This document describes definitions covered in the learning material for AZ-900. The aim of this document is to help with learning Azure Fundamentals in a way I can understand it. To do this I use quotes directly from the documentation from Microsoft, which I try to shorten (take out only the essentials). In addition, if I think the documentation is too verbose or not essential I write my own short summary of the covered material.

Note: beware of name changes to any of the described Azure Services. There seems to be a tendency towards renaming things from Azure X to Microsoft X.[[1]](#footnote-1)

Contents

[Cloud computing concepts 4](#_Toc107389616)

[Categories of services on Azure: 5](#_Toc107389617)

[Types of Cloud Deployment Models 6](#_Toc107389618)

[Public cloud 6](#_Toc107389619)

[Private cloud 6](#_Toc107389620)

[Hybrid cloud 6](#_Toc107389621)

[Advantages of cloud computing (disaster recovery, elasticity…) 6](#_Toc107389622)

[Deciding which Azure Services to use 7](#_Toc107389623)

[Virtual Machines 7](#_Toc107389624)

[App Service 7](#_Toc107389625)

[Containers, Kubernetes, Microservices 7](#_Toc107389626)

[Function & Logic Apps (Serverless) 7](#_Toc107389627)

[Virtual Desktop 8](#_Toc107389628)

[Azure Virtual Network (advanced) 8](#_Toc107389629)

[Communications with on-premises devices: 8](#_Toc107389630)

[Point-to-site virtual private networks 8](#_Toc107389631)

[Site-to-site virtual private networks 8](#_Toc107389632)

[Azure ExpressRoute 8](#_Toc107389633)

[VPN Gateways 9](#_Toc107389634)

[ExpressRoute 9](#_Toc107389635)

[Azure Storage 9](#_Toc107389636)

[Disk storage 10](#_Toc107389637)

[Blob storage 10](#_Toc107389638)

[File storage 11](#_Toc107389639)

[Access tiers 12](#_Toc107389640)

[Databases on Azure 12](#_Toc107389641)

[Azure Cosmos DB 12](#_Toc107389642)

[Azure SQL Database 12](#_Toc107389643)

[Azure SQL Managed Instance 12](#_Toc107389644)

[Analysis of big data 13](#_Toc107389645)

[Choosing Artificial Intelligence (AI) Tools 14](#_Toc107389646)

[Machine Learning 14](#_Toc107389647)

[Cognitive Services 14](#_Toc107389648)

[Bot Services 15](#_Toc107389649)

[Choosing IoT (Internet of Things) Tools 15](#_Toc107389650)

[Choosing Serverless Tools 15](#_Toc107389651)

[Azure DevOps 15](#_Toc107389652)

[Tools for Managing Azure Itself 16](#_Toc107389653)

[Azure Portal 16](#_Toc107389654)

[Azure Mobile App 16](#_Toc107389655)

[Azure PowerShell 16](#_Toc107389656)

[Azure CLI 16](#_Toc107389657)

[ARM Templates 16](#_Toc107389658)

[Azure Monitoring Tools 17](#_Toc107389659)

[Azure Advisor 17](#_Toc107389660)

[Azure Monitor 17](#_Toc107389661)

[Azure Health Service 18](#_Toc107389662)

[Security on Azure 19](#_Toc107389663)

[Summary of Security services: 19](#_Toc107389664)

[Azure Firewall 20](#_Toc107389665)

[Miscellaneous Security 20](#_Toc107389666)

[DDoS 20](#_Toc107389667)

[NSG (internal firewall) 20](#_Toc107389668)

[Security Recommendations 20](#_Toc107389669)

[Microsoft Defender for Cloud (previously Azure Security Center) 21](#_Toc107389670)

[Security Sentinel 21](#_Toc107389671)

[Azure Key Vault 21](#_Toc107389672)

[Azure Dedicated Host 21](#_Toc107389673)

[Governance (Access Control & More) 22](#_Toc107389674)

[Azure Role-Based-Access-Control 22](#_Toc107389675)

[Resource Locks 22](#_Toc107389676)

[Organizing Resources 22](#_Toc107389677)

[Example tagging structure 23](#_Toc107389678)

[Azure Policy 23](#_Toc107389679)

[Azure Blueprints 23](#_Toc107389680)

[Cloud Adoption Framework 24](#_Toc107389681)

[Privacy & Complying to Laws 24](#_Toc107389682)

[Azure Identity Services (Azure Active Directory) 25](#_Toc107389683)

[Service Level Agreements (SLAs) 26](#_Toc107389684)

[Typical Azure SLA Parts 26](#_Toc107389685)

[Calculating an apps uptime 27](#_Toc107389686)

[Managing Costs in Azure 28](#_Toc107389687)

[Purchasing Azure Services 28](#_Toc107389688)

[Subscription types 28](#_Toc107389689)

[Purchasing services 28](#_Toc107389690)

[What affects cost? 29](#_Toc107389691)

[Minimize costs 29](#_Toc107389692)

# Cloud computing concepts

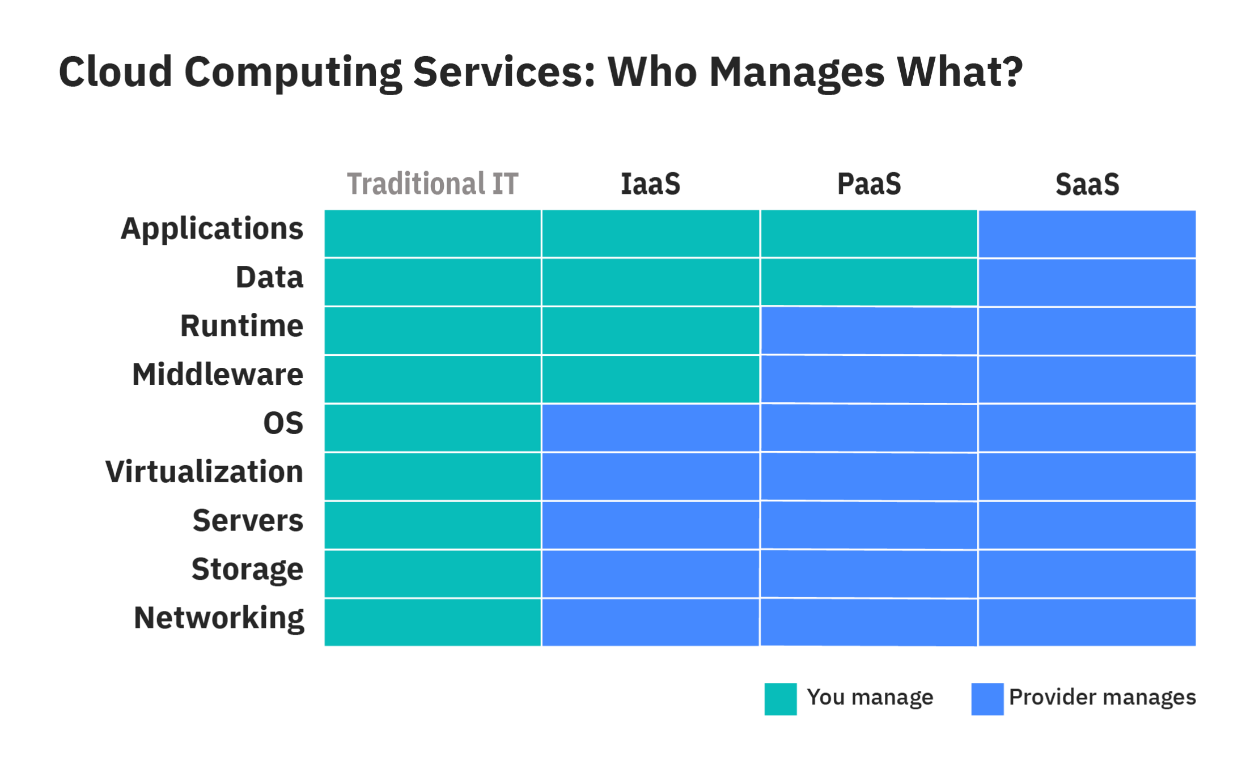
**Cloud computing**: using a 3rd party’s computing resources, so you don’t need an on-premises datacenter and the costs that come with it. Pay-as-you-go model.

**Azure:** Microsoft’s cloud computing platform. Offers a wide range of SaaS, PaaS and IaaS.

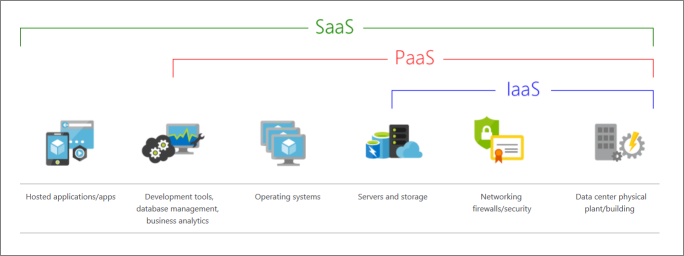
**SaaS:** Software as a Service. A fully functional service, which the receiver can use out-of-the-box.

**PaaS:** Platform as a Service. A fully functional service, such as Azure, where the user manages the applications and data themselves.

**IaaS:** Infrastructure as a Service. Largest degree of control. Virtual machine is an example of this.



Source:

  
source: <https://docs.microsoft.com/en-us/learn/azure-fundamentals/fundamental-azure-concepts/media/iaas-paas-saas-575a09e9.png>

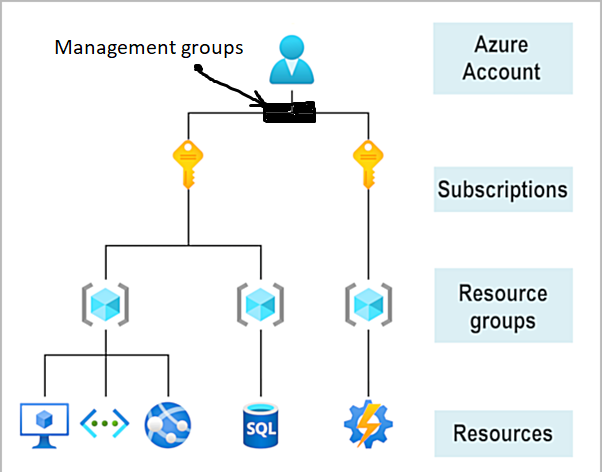
**Capital Expenditure (CapEx):** paying upfront for everything. Values decreases over time. Less flexible.

**Operational Expenditure (OpEx):** pay-as-you-go. Values remains constant. Flexible.

|  |  |  |
| --- | --- | --- |
| Context | CapEx | OpEx |
| The upfront *cost* | Significant | None |
| *Ongoing cost* | Low | Based on usage |
| *Tax Deduction* | Over-time | Same year |
| *Early Termination* | No | Anytime |
| *Maintenance* | Significant | Low |
| *Value over time* | Lowers | No change |

**Managing Resources**

A company has one Azure account. This Azure account has one or more subscriptions, which it can give to different types of employees. These subscriptions have access to some resource groups, which have resources specific to that group. A resource can be anything from a database, analytics or a web application. (All subscriptions within a [management group](https://docs.microsoft.com/en-us/learn/modules/azure-architecture-fundamentals/management-groups-subscriptions) automatically inherit the conditions applied to the management group).

****

## Categories of services on Azure:

* **Compute (most common reason for companies to use Azure)**
* Networking
* Storage
* Mobile
* Databases
* **Web**
* Internet of Things (IoT)
* Big data
* AI
* DevOps

**Virtual Machine:** a computer emulated in another computer, with their own OS.

## Types of Cloud Deployment Models

There are three deployment models for cloud computing: public cloud, private cloud, and hybrid cloud.

Public cloud: can be used by everyone (e.g. one computer can host software from multiple companies).

Private cloud: can only be used by the specific company/organization. (Hardware is bought specifically for the company)

Hybrid: a combination of the two, where data and applications can be shared between public and private cloud.

### Public cloud

* No capital expenditures to scale up.
* Applications can be quickly provisioned and deprovisioned.
* Organizations pay only for what they use.

### Private cloud

* Hardware must be purchased for start-up and maintenance.
* Organizations have complete control over resources and security.
* Organizations are responsible for hardware maintenance and updates.

### Hybrid cloud

* Provides the most flexibility.
* Organizations determine where to run their applications.
* Organizations control security, compliance, or legal requirements.

## Advantages of cloud computing (disaster recovery, elasticity…)

* **High availability**: Depending on the service-level agreement (SLA) that you choose, your cloud-based apps can provide a continuous user experience with no apparent downtime, even when things go wrong.
* **Scalability**: Apps in the cloud can scale *vertically* and *horizontally*:
  + Scale vertically to increase compute capacity by adding RAM or CPUs to a virtual machine.
  + Scaling horizontally increases compute capacity by adding instances of resources, such as adding VMs to the configuration.
* **Elasticity**: You can configure cloud-based apps to take advantage of autoscaling, so your apps always have the resources they need.
* **Agility**: Deploy and configure cloud-based resources quickly as your app requirements change.
* **Geo-distribution**: You can deploy apps and data to regional datacenters around the globe, thereby ensuring that your customers always have the best performance in their region.
* **Disaster recovery**: By taking advantage of cloud-based backup services, data replication, and geo-distribution, you can deploy your apps with the confidence that comes from knowing that your data is safe in the event of disaster. (Read about *Region Pairs, Availability Zones, Azure Regions for details*)

## Deciding which Azure Services to use

### Virtual Machines

When you want to have:

* Total control over the operating system (OS).
* The ability to run custom software.
* Custom hosting configurations.

For scaling you can use scale sets:

**Virtual machine scale sets** let you deploy and manage a set of identical virtual machines.

### App Service

Use the App Service, when you just want to deploy and not bother with anything else. You can deploy Web Apps, Mobile apps, API’s and WebJobs (scheduled or triggered) in an App Service. App Service contains a free tier for sites that are small and have low-traffic.

### Containers, Kubernetes, Microservices

Kubernetes manages pods (which can contain one or more containers), containers can contain microservices, and microservices are components of functionality (e.g., a calendar function) that could be used in an app that, together with other microservices, make up the app. If one microservice goes down, it shouldn’t affect the rest.

### Function & Logic Apps (Serverless)

[Azure Functions vs Azure Logic Apps](https://docs.microsoft.com/en-us/learn/modules/azure-compute-fundamentals/azure-functions)

Serverless computing is the abstraction of servers, infrastructure, and operating systems. Those 3 things are not your concern. Scaling and performance are handled automatically. You're billed only for the exact resources you use. There's not even a need to reserve capacity.

Azure Functions are commonly used when you need to perform work in response to an event (often via a REST request), timer, or message from another Azure service, and when that work can be completed quickly, within seconds or less. This costs less than using a Virtual Machine (which you still pay for while it’s idle).

Where functions execute code, **logic apps** execute workflows that are designed to automate business scenarios and are **built from predefined logic blocks**.

### Virtual Desktop

Virtual Desktop enables workers to connect to a virtual version of a computer, regardless of their own operating system. E.g., a worker from Japan can connect to a pc in Europe and experience less latency, when perform actions in addition to fewer issues because the software is separated from the hardware they use.

# Azure Virtual Network (advanced)

Azure Virtual Network enables communication between apps, devices, user and databases, both on-premise and on Azure. It can be thought of as an extension of an on-premise network. It is a potential way to increase security, for example when sharing data between two branches of a company at different locations.

Azure virtual networks provide the following key networking capabilities:

* Isolation and segmentation
* Internet communications
* Communicate between Azure resources
* Communicate with on-premises resources
* Route network traffic
* Filter network traffic
* Connect virtual networks

You can create and configure Azure virtual networks from the Azure portal, Azure PowerShell, Azure CLI, Azure Cloud Shell or an ARM template.

## Communications with on-premises devices:

Point-to-site virtual private networks

The typical approach to a virtual private network (VPN) connection is from a computer outside your organization, back into your corporate network. In this case, the client computer initiates an encrypted VPN connection to connect that computer to the Azure virtual network.

Site-to-site virtual private networks

A site-to-site VPN links your on-premises VPN device or gateway to the Azure VPN gateway in a virtual network. In effect, the devices in Azure can appear as being on the local network. The connection is encrypted and works over the internet.

### Azure ExpressRoute

For environments where you need greater bandwidth and even higher levels of security, Azure ExpressRoute is the best approach. ExpressRoute provides a dedicated private connectivity to Azure that doesn't travel over the internet. (You'll learn more about ExpressRoute in a separate unit later in this module.)

## [VPN Gateways](https://docs.microsoft.com/en-us/learn/modules/azure-networking-fundamentals/azure-vpn-gateway-fundamentals)

A VPN gateway is a type of virtual network gateway. Azure VPN Gateway instances are deployed in a dedicated subnet of the virtual network and enable the following connectivity:

* Connect on-premises datacenters to virtual networks through a *site-to-site* connection.
* Connect individual devices to virtual networks through a *point-to-site* connection.
* Connect virtual networks to other virtual networks through a *network-to-network* connection.

## [ExpressRoute](https://docs.microsoft.com/en-us/learn/modules/azure-networking-fundamentals/express-route-fundamentals)

Highly secure. ExpressRoute sends data over private network, not public.

# [Azure Storage](https://docs.microsoft.com/en-us/learn/modules/azure-storage-fundamentals/azure-storage-accounts)

Azure storage can be used to store data as if they were on disks on-premises (blobs, files, and disks). It can exist in 3 modes: *hot*, *cold* or *archive* depending on the frequency of use.

A storage account provides a unique namespace for your Azure Storage data, that's accessible from anywhere in the world over HTTP or HTTPS

Types of storage:

* Disk Storage
* Blob Storage
* Files Storage

A comparison between them can be seen here:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Blob Storage** | **Disk Storage** | **File Storage** |
| **Type of storage** | Object storage to store all types of data formats. | Block storage for virtual machines. | File system across multiple machines. |
| **Max Storage Size** | Same as maximum storage account capacity | 65,536 GiB for ultra disk  32,767 GiB for standard and premium drives | Scale up to 100 TiB |
| **Max File Size** | 190.7 TiB for block blob  195 GiB for append blob  8 TiB for page blob | Equivalent to the maximum size of your volumes | 4 TiB for a single file |
| **Performance (Throughput)** | 500 requests per second for a single blob | Up to 2000 MBps per disk. | 6,204 MiB/s for egress  4,136 MiB/s for ingress |
| **Data Accessing** | Objects can be accessed via HTTP/HTTPs. | A single virtual machine in a single AZ. | Share your files either on-premises or in the cloud. |
| **Encryption Methods** | Encrypt your data using Azure SSE (256-bit AES) | SSE by storage service and ADE for OS and data disks. | Encrypt your data using Azure SSE (256-bit AES) |
| **Backup and Restoration** | Versioning, snapshots and object replication | You can back up your managed disks at any point in time using snapshots. | Uses file share snapshots |
| **Pricing** | You are billed based on the stored data per month, operations performed, data transfer, and redundancy. | You pay for the disk size, snapshots, and number of transactions. | You pay for the provisioned GiB per month and the number of servers connected to the cloud endpoint. |
| **Use Cases** | Static website, media and log files, backups, analytics workloads | Boot volumes and transaction-intensive workloads | Central location of your files, monitoring logs and applications |

Source: <https://tutorialsdojo.com/azure-blob-vs-disk-vs-file-storage/>

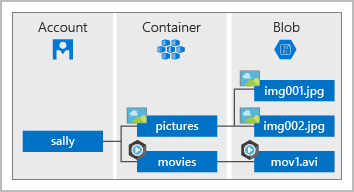
## Disk storage

## Disk Storage provides disks for Azure virtual machines. Applications and other services can access and use these disks as needed, similar to how they would in on-premises scenarios. Disk Storage allows data to be persistently stored and accessed from an attached virtual hard disk. Blob storage

Blob storage can store massive amounts of unstructured data, in the form of example text or binary. It can manage simultaneous uploads, video data, log files that won’t stop growing, etc.

Blob Storage is ideal for:

* Serving images or documents directly to a browser.
* Storing files for distributed access.
* Streaming video and audio.
* Storing data for backup and restore, disaster recovery, and archiving.
* Storing data for analysis by an on-premises or Azure-hosted service.
* Storing up to 8 TB of data for virtual machines.



Source: <https://docs.microsoft.com/en-us/learn/modules/azure-storage-fundamentals/azure-blob-container-storage>

## File storage

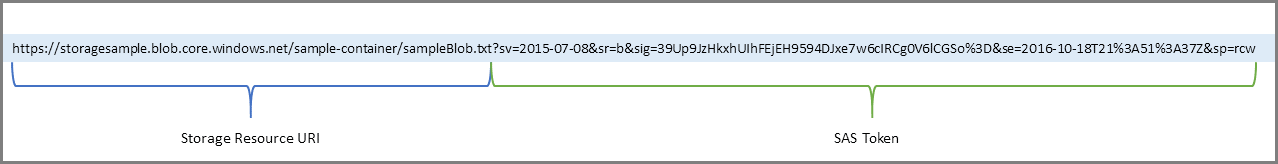
Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) and Network File System (NFS) protocols.

Typical usage scenarios would be to share files anywhere in the world, diagnostic data, or application data sharing. An example could be the sharing of a configuration file between developers.

Use Azure Files for the following situations:

* Many on-premises applications use file shares. Azure Files makes it **easier to migrate** those applications that share data to Azure. If you mount the Azure file share to the same drive letter that the on-premises application uses, the part of your application that accesses the file share should work with minimal changes, if any.
* **Store configuration files** on a file share and access them from multiple VMs. Tools and utilities used by multiple developers in a group can be stored on a file share, ensuring that everybody can find them, and that they use the same version.
* **Write data to a file share**, and process or analyze the data later. For example, you might want to do this with diagnostic logs, metrics, and crash dumps.

You can access the files from anywhere in the world, by using a URL that points to the file. You can also use Shared Access Signature (SAS) tokens to allow access to a private asset for a specific amount of time.



## Access tiers

Access tiers exist to reduce the cost, where possible, for storage.

* **Hot access tier**: Optimized for storing data that is accessed frequently (for example, images for your website).
* **Cool access tier**: Optimized for data that is infrequently accessed and stored for at least 30 days (for example, invoices for your customers).
* **Archive access tier**: Appropriate for data that is rarely accessed and stored for at least 180 days, with flexible latency requirements (for example, long-term backups).

# [Databases on Azure](https://docs.microsoft.com/en-us/learn/modules/azure-database-fundamentals/introduction)

A variety of database options exist in Azure. This section will give an overview of each.

All the databases have 99.99% uptime[[2]](#footnote-2) apart from Cosmos DB, where they didn’t make such a claim.

All the databases are kept updated with latest security, have backups and can be scaled.

The databases (at least MySql & PostgresSql) have adjustable automatic backups and point-in-time-restore for up to 35 days.

## Azure Cosmos DB

This is a multi-model database, which can use: SQL, MongoDB, Cassandra, Tables, and Gremlin.

This means you can, for example, have a relational database (schema needed) and a document based database (no schema needed).

It is flexible and fast (9ms max delay in data access[[3]](#footnote-3))

## Azure SQL Database

Azure SQL DB runs a relational Microsoft SQL Server database. Azure SQL Database is a platform as a service (PaaS) database engine. It handles most of the database management functions, such as upgrading, patching, backups, and monitoring, without user involvement.

You can migrate your existing SQL Server databases with minimal downtime by using the Azure Database Migration Service.

### Azure SQL Managed Instance

Similar to the Azure SQL DB, but have some differences. They are compared at the following link: <https://docs.microsoft.com/en-us/azure/azure-sql/database/features-comparison> . One example is that it can be setup to handle more characters (e.g. Cyrillic, a writing system used in Eastern Europe + Asia).

## [Analysis of big data](https://docs.microsoft.com/en-us/learn/modules/azure-database-fundamentals/azure-big-data-analytics)

There are 4 tools for analyzing and handling big data in Azure:

**Azure Synapse Analytics (formerly Azure SQL Data Warehouse)**

You can query data on your terms by using either *serverless* or *provisioned resources* at *scale*. You have a unified experience to ingest, prepare, manage, and serve data for immediate business intelligence and machine learning needs.

**Azure HDInsight**

[Azure HDInsight](https://azure.microsoft.com/services/hdinsight/) is a fully managed, open-source analytics service for enterprises. It's a cloud service that makes it easier, faster, and more cost-effective to process massive amounts of data. + Something about **Clusters.** Can be used with Hadoop, Spark and Kafka (open source apache software)

**Azure Databricks**

**Enables you to quickly get insight from data and build AI solutions.** Azure Databricks supports Python, Scala, R, Java, and SQL, as well as data science frameworks and libraries including TensorFlow, PyTorch, and scikit-learn.

**Azure Data Lake Analytics**

This is an on-demand analytics job service, which simplifies big data. You can just query it to transform data, instead of needing a lot of setup. Cost effective, because you can switch how much power to use on it.

# Choosing [Artificial Intelligence (AI)](https://docs.microsoft.com/en-us/learn/modules/ai-machine-learning-fundamentals/1-introduction) Tools

There exist 2 approaches to AI: *deep learning* and *machine learning*. Deep learning is to make a machine “truly” learn, like a human. Machine learning on the other hand, is to take a model and feed it a lot of data, which should improve the model’s accuracy.

On Azure there are three options for AI:

* Azure Machine Learning
* Azure Cognitive Services
* Azure Bot Service

## Machine Learning

Machine learning is for making predictions through models and data. It can be used via a web API endpoint.

With Azure Machine Learning, you can:

* Create a process that defines how to obtain data, how to handle missing or bad data, how to split the data into either a training set or test set, and deliver the data to the training process.
* Train and evaluate predictive models by using tools and programming languages familiar to data scientists.
* Create pipelines that define where and when to run the compute-intensive experiments that are required to score the algorithms based on the training and test data.
* Deploy the best-performing algorithm as an API to an endpoint so it can be consumed in real time by other applications.

Choose Azure Machine Learning when your data scientists need complete control over the design and training of an algorithm using your own data.

## Cognitive Services

Cognitive services offer prebuild machine learning models you can use. Compared to Azure Machine Learning, which requires you to make your own and train it, you can (for the most part) use Cognitive service models out-of-the-box.

Azure Cognitive Services can be divided into the following categories:

* **Language** services: Allow your apps to process natural language with prebuilt scripts, evaluate sentiment, and learn how to recognize what users want.
* **Speech** services: Convert speech into text and text into natural-sounding speech. Translate from one language to another and enable speaker verification and recognition.
* **Vision** services: Add recognition and identification capabilities when you're analyzing pictures, videos, and other visual content.
* **Decision** services: Add personalized recommendations for each user that automatically improve each time they're used, moderate content to monitor and remove offensive or risky content, and detect abnormalities in your time series data.
* For more customization you might need to use Azure Machine Learning.

## Bot Services

[Azure Bot Service](https://azure.microsoft.com/services/bot-service/) and Bot Framework are platforms for creating virtual agents that understand and reply to questions just like a human.

Bots can be used to shift simple, repetitive tasks, such as taking a dinner reservation or gathering profile information, on to automated systems that might no longer require direct human intervention. Users converse with a bot by using text, interactive cards, and speech. A bot interaction can be a quick question and answer, or it can be a sophisticated conversation that intelligently provides access to services.

# Choosing IoT (Internet of Things) Tools

IoT is a broad term, which encompasses devices connected through the internet.

Azure offers 3 options for IoT:

* Azure IoT Hub, most basic (central message hub for bidirectional communication)
* Azure IoT Central (builds on IoT Hub. Adds a prebuild, customizable dashboard, from which you can monitor, control your IoT devices)
* Azure Sphere (end-to-end secure system IoT solution, most advanced, but most setup)

# Choosing Serverless Tools

Serverless computing is a term used to describe an execution environment that's set up and managed for you. You merely specify what you want to happen by writing code or connecting and configuring components in a visual editor, and then specify the actions that trigger your functionality, such as a timer or an HTTP request. Best of all, you never have to worry about an outage, your code can scale instantly to meet demand, and you pay based only on the actual usage of your code.

Azure has **Azure Functions** and **Azure Logic Apps**, which are serverless.

Azure Functions trigger single methods to run based on a trigger of some sort. Azure Logic App executes flows based on triggers. Azure Functions can trigger Azure Logic Apps and vice-versa.

The two services are priced differently. Azure Functions pricing is based on the number of executions and the running time of each execution. Logic Apps pricing is based on the number of executions and the type of connectors that it utilizes.

# Azure DevOps

Azure offers a tool called DevOps, which can function as a Git repository, kanban board and more for you management needs. Compared to GitHub it has more *granular* access control. In addition you can have Azure DevTest Labs with which you can run your tests on Virtual Machines made for that specific purpose.

# [Tools for Managing Azure Itself](https://docs.microsoft.com/en-us/learn/modules/management-fundamentals/2-identify-product-options)

For configuring the services available on Azure you have a few options:

* Azure Portal
* Azure Mobile App
* Azure PowerShell
* Azure CLI
* ARM Templates

The following sections will give an overview of each.

## Azure Portal

This is the visual tool for Azure (accessed at [www.portal.azure.com](http://www.portal.azure.com)). It is beginner friendly, but the other tools are faster to use, once you’ve gotten to know them.

## Azure Mobile App

This provides quick access to monitoring of your resources on Azure and you have some control over them as well, such as: restarting an app, run Azure CLI cmds, run Azure PowerShell cmdlets.

Use this for remote work, when a desktop or laptop is not accessible.

## Azure PowerShell

A terminal, where developers and other IT professionals can execute commands called “cmdlets” (pronounced *command-lets*). Cmdlets call the Azure Rest API to manage anything on Azure.

They can be combined with a script file or executed independently.

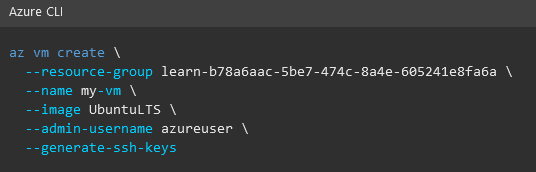
The script files can automate routine setup, teardown and maintenance or deploy infrastructure.

Azure PowerShell is cross-platform and can be used in a browser via Azure Cloud Shell.

## Azure CLI

Azure CLI is similar to Azure PowerShell, apart from the syntax used. The choice of CLI vs PowerShell is preference based.

Example that creates a virtual machine with Ubuntu installed:



(\ = continue line on next line)

## ARM Templates

ARM (in this case) stands for Azure Resource Manager.

By using Azure Resource Manager templates (ARM templates), you can describe the resources you want to use in a **declarative JSON format.** The benefit is that the entire ARM template is **verified before any code is executed** to ensure that the resources will be created and connected correctly.

To use ARM Templates, the developer defines the desired state and configuration for each resource in the template, which are **executed in parallel**. Templates can execute PowerShell and Bash scripts before or after the resource has been set up.

ARM Templates features:

* Efficient and can potentially create many resources in parallel.
* Creates all dependencies in the correct order.
* Can be used without worrying that it failed in the middle of provisioning the necessary infrastructure.

# Azure Monitoring Tools

At a high level there are three options:

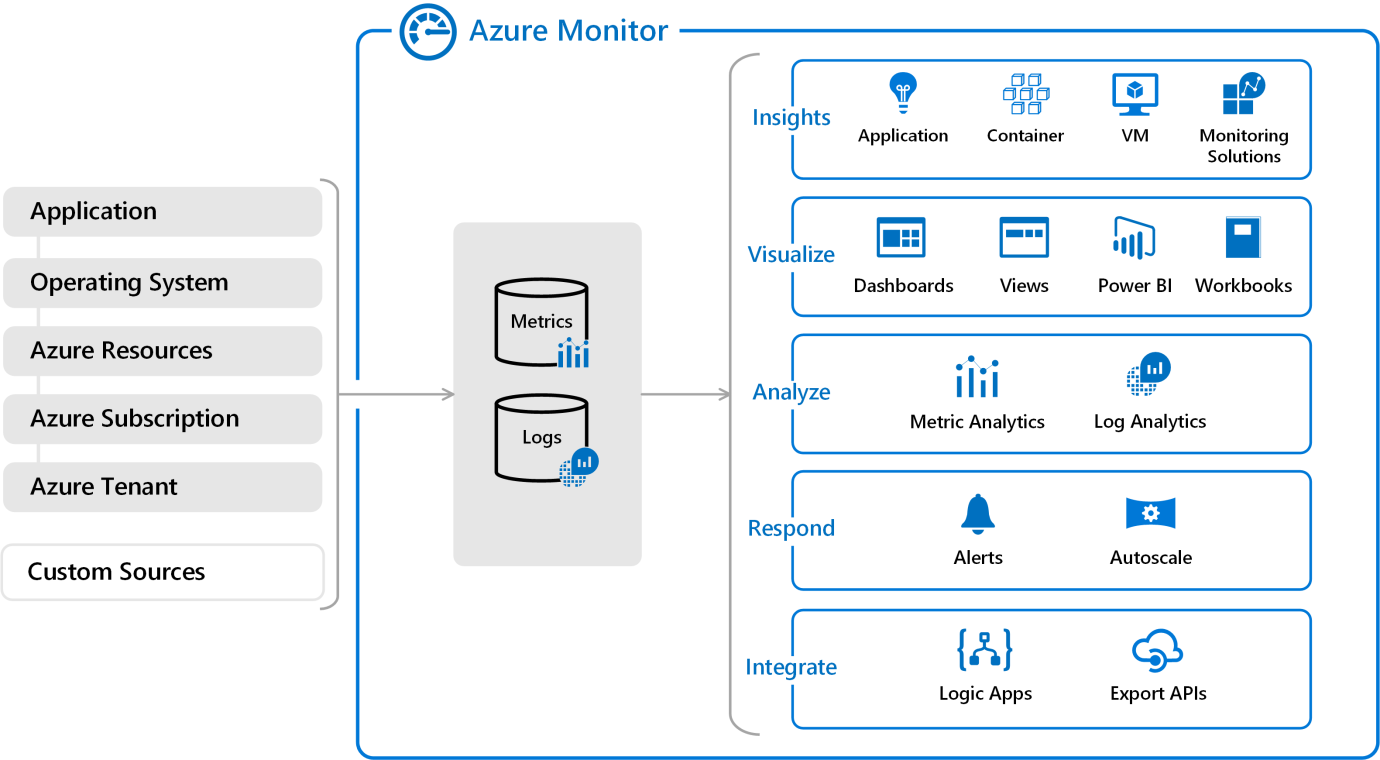
* Azure Advisor
* Azure Monitor
* Azure Service Health

## Azure Advisor

Analyses your usage and makes recommendations for increased performance, reduce cost and more.

## Azure Monitor

Azure Monitor: a platform for collecting, analyzing, visualizing, and potentially taking action based on the metric and logging data from your entire Azure and on-premises environment. Useful for pinpointing an issue.



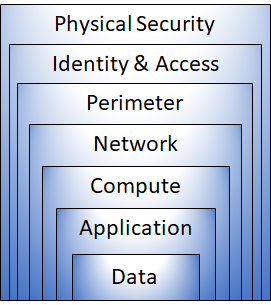
You can use the data provided by the Monitor to help you react to critical events in real time, through alerts delivered to teams via SMS, email, and so on.

## Azure Health Service

Personalized view of the health status on parts of Azure you rely on, so you can prepare for downtime or figure out if it is Azure and its services that are causing issues.

# [Security on Azure](https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/2-what-is-defense-in-depth)

To explain the security on Azure you first need to understand the layers of security in place. They are:



Here's a brief overview of the role of each layer:

* The *physical security* layer is the first line of defense to protect computing hardware in the datacenter.
* The *identity and access* layer controls access to infrastructure and change control.
* The *perimeter* layer uses distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
* The *network* layer limits communication between resources through segmentation and access controls.
* The *compute* layer secures access to virtual machines.
* The *application* layer helps ensure that applications are secure and free of security vulnerabilities.
* The *data* layer controls access to business and customer data that you need to protect

## Summary of Security services:

Microsoft Defender for Cloud provides visibility of your security posture across all of your services, both on Azure and on-premises.

Azure Sentinel aggregates security data from many different sources, and provides additional capabilities for threat detection and response.

Azure Key Vault stores your applications' secrets, such as passwords, encryption keys, and certificates, in a single, central location.

Azure Dedicated Host provides dedicated physical servers to host your Azure VMs for Windows and Linux.

## Azure Firewall

Azure firewall is a cloud-based network security service that helps protect resources in your Azure Virtual Networks. It works similarly to an on-premises firewall.

Azure Firewall provides a central location to create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.

Azure Firewall provides many features, including:

* Built-in high availability.
* Unrestricted cloud scalability.
* Inbound and outbound filtering rules.
* Inbound Destination Network Address Translation (DNAT) support.
* **Azure Monitor logging.**

## Miscellaneous Security

### DDoS

Azure provides DDoS protection to all their services. There are 2 levels, Basic (free) and Standard (additional cost).

* Basic DDoS protection protects the Azure Infrastructure and monitors traffic.
* Standard DDoS protection helps protect your Virtual Networks, and potentially your web applications, from “volumetric attacks” (traffic flooding) & “protocol attacks” (exploit vulnerability). (web apps DDoS protection requires a Web application firewall (WAF), which exists in Azure Application Gateway)

### NSG (internal firewall)

Network Security Group (NSG) enables you to filter network traffic within an Azure virtual network. A NSG can be thought of as an internal firewall.

### Security Recommendations

Perimeter layer

* Use Azure DDoS Protection to filter large-scale attacks before they can cause a denial of service for users.
* Use perimeter firewalls with Azure Firewall to identify and alert on malicious attacks against your network.

Network layer

* Limit communication between resources by segmenting your network and configuring access controls.
* Deny by default.
* Restrict inbound internet access and limit outbound where appropriate.
* Implement secure connectivity to on-premises networks.

Combine available security methods, such as NSG + Web App Firewall.

## Microsoft Defender for Cloud (previously Azure Security Center)

Microsoft Defender for Cloud can:

* Monitor security settings across on-premises and cloud workloads.
* **Automatically apply required security settings to new resources** as they come online.
* Provide security recommendations that are based on your current configurations, resources, and networks.
* Continuously **monitor your resources and perform automatic security assessments to identify potential vulnerabilities** before those vulnerabilities can be exploited.
* Use machine learning to **detect and block malware from being installed on your virtual machines (VMs) and other resources**. You can also use *adaptive application controls* to define rules that list allowed applications to ensure that only applications you allow can run.
* **Detect and analyze potential inbound attacks** and investigate threats and any post-breach activity that might have occurred.
* Provide **just-in-time access control for network ports**. Doing so reduces your attack surface by ensuring that the network only allows traffic that you require at the time that you need it to.

## Security Sentinel

* Detect undetected threats
* Collect data at scale (across apps, users, devices…)
* Respond to threats quickly with automated tasks

## [Azure Key Vault](https://docs.microsoft.com/en-us/learn/modules/protect-against-security-threats-azure/4-manage-secrets-key-vault)

Azure Key Vault can help you:

* **Manage secrets.** You can use Key Vault to securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets.
* **Manage encryption keys.** You can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys that are used to encrypt your data.
* **Manage SSL/TLS certificates.** Key Vault enables you to provision, manage, and deploy your public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for both your Azure resources and your internal resources.
* **Store secrets backed by Hardware Security Modules (HSMs).** These secrets and keys can be protected either by software or by FIPS 140-2 Level 2 validated HSMs.

## [Azure Dedicated Host](https://docs.microsoft.com/en-us/learn/modules/protect-against-security-threats-azure/6-host-virtual-machines-dedicated-hosts)

Normally you share physical hardware with others (though the VMs are isolated from each other). If you need dedicated hardware only for your organization you use Azure Dedicated Host.

# Governance (Access Control & More)

The term governance describes the general process of establishing rules and policies and ensuring that those rules and policies are enforced.

Governance is most beneficial when you have:

* Multiple engineering teams working in Azure.
* Multiple subscriptions to manage.
* Regulatory requirements that must be enforced.
* Standards that must be followed for all cloud resources.

## Azure Role-Based-Access-Control

To control access to resources Azure uses *Azure Role-based-access-control (RBAC)*. There are predefined roles, but you can make your own.

If you assign a role at subscription level, the person with that role can also access any resources made with that subscription.

Roles can be assigned to individuals or groups.

You manage access permissions on the **Access control (IAM)** pane in the Azure portal.

## Resource Locks

A [resource lock](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources) prevents resources from being accidentally deleted or changed. Think of a resource lock as a warning system that reminds you that a resource should not be deleted or changed.

You can apply locks to a subscription, a resource group, or an individual resource. You can set the lock level to **CanNotDelete** or **ReadOnly**.

* **CanNotDelete** means authorized people can still read and modify a resource, but they can't delete the resource without first removing the lock.
* **ReadOnly** means authorized people can read a resource, but they can't delete or change the resource. Applying this lock is like restricting all authorized users to the permissions granted by the **Reader** role in Azure RBAC.

Resource Locks can be combined with *Azure Blueprints*.

## Organizing Resources

One way to organize related resources is to place them in their own subscriptions. You can also use resource groups to manage related resources. Resource tags are another way to organize resources. Tags provide extra information, or metadata, about your resources. This metadata is useful for:

* **Resource management** Tags enable you to locate and act on resources that are associated with specific workloads, environments, business units, and owners.
* **Cost management and optimization** Tags enable you to group resources so that you can report on costs, allocate internal cost centers, track budgets, and forecast estimated cost.
* **Operations management** Tags enable you to group resources according to how critical their availability is to your business. This grouping helps you formulate service-level agreements (SLAs). An SLA is an uptime or performance guarantee between you and your users.
* **Security** Tags enable you to classify data by its security level, such as *public* or *confidential*.
* **Governance and regulatory compliance** Tags enable you to identify resources that align with governance or regulatory compliance requirements, such as ISO 27001. Tags can also be part of your standards enforcement efforts. For example, you might require that all resources be tagged with an owner or department name.
* **Workload optimization and automation** Tags can help you visualize all of the resources that participate in complex deployments. For example, you might tag a resource with its associated workload or application name and use software such as Azure DevOps to perform automated tasks on those resources.

### Example tagging structure

|  |  |
| --- | --- |
| Name | Value |
| AppName | The name of the application that the resource is part of. |
| CostCenter | The internal cost center code. |
| Owner | The name of the business owner who's responsible for the resource. |
| Environment | An environment name, such as "Prod," "Dev," or "Test." |
| Impact | How important the resource is to business operations, such as "Mission-critical," "High-impact," or "Low-impact." |

## Azure Policy

[Azure Policy](https://azure.microsoft.com/services/azure-policy) is a service in Azure that enables you to create, assign, and manage policies that control or audit your resources. These policies enforce different rules across all of your resource configurations so that those configurations stay compliant with corporate standards.

Implementing a policy in Azure Policy involves three tasks:

* Create a policy definition. (e.g. CORS should never allow \*)
* Assign the definition to resources. (e.g. a resource group)
* Review the evaluation results.

Azure policies can be grouped further with *Azure Policy initiatives*.

Predefined policies exist.

## Azure Blueprints

Once your organization grows beyond one subscription, you might want to use Azure Blueprints. With [Azure Blueprints](https://azure.microsoft.com/services/blueprints) you can define a **repeatable** **set** of governance tools and standard Azure resources that your organization requires, so you don’t have to configure Azure Policy for every subscription.

Azure Blueprints orchestrates the deployment of various resource templates and other artifacts, such as:

* Role assignments
* Policy assignments
* Azure Resource Manager templates
* Resource groups

Blueprints are also versioned. Versioning enables you to track and comment on changes to your blueprint.

## [Cloud Adoption Framework](https://docs.microsoft.com/en-us/learn/modules/microsoft-cloud-adoption-framework-for-azure/2-cloud-adoption-framework-overview)

The Cloud Adoption Framework helps you adapting Azure cloud services, by helping you through these steps:

* Define your strategy. What is the *measurable* business goal?
* Make a plan. Take inventory of what you have and what you need to reach the goal. Each resource should take one of the following: Re-host, refactor, re-architect, rebuild, or replace.
* Ready your organization.
* Adopt the cloud.
* Govern and manage your cloud environments.

The steps will help you decide what you need from the cloud and how to make it happen.

The three main components of the Cloud Adoption Framework (plan, ready, and adopt) can be applied to different stages for cloud adopters. They should be revisited often because cloud adoption is an ongoing journey, not a destination.

# [Privacy & Complying to Laws](https://www.microsoft.com/licensing/docs)

Find out if Azure holds up to proper standards as defined by law.

Keywords:

* **Microsoft Privacy Statement** (what, how and why personal data is stored. Exists for every service in Azure.)
* **Online Services Terms** (specifies the obligations for Microsoft and their customer about data & security)
* **Data Protection Addendum**, DPA (expands on the Online Services Terms)
* **Trust Center** (<https://www.microsoft.com/da-dk/trust-center?rtc=1>)
* Check info about security, privacy, compliance, policies, features and practices for every Microsoft product
* (holds a link to: <https://docs.microsoft.com/da-DK/compliance/>)
* [**Azure compliance documentation**](https://docs.microsoft.com/en-us/azure/compliance/) (check if Azure is following a specific standard, such as ISO-27001)
* The compliance documentation provides reference blueprints, or policy definitions, for common standards that you can apply to your Azure subscription
* **Azure Government**
* Part of azure that is specifically for the US Government.
* **Azure China 21Vianet**
* Operated by 21Vianet
* Azure offering in China. Requires less than 50% ‘foreign investments’ for locally registered companies.

# [Azure Identity Services](https://docs.microsoft.com/en-us/learn/modules/secure-access-azure-identity-services/) (Azure Active Directory)

*Azure Active Directory (Azure AD)* is Microsoft's cloud-based identity and access management service. With Azure AD, you control the identity accounts, but Microsoft ensures that the service is available globally.

**Active Directory** is related to **Azure AD**, but they have some key differences.

Microsoft introduced Active Directory in Windows 2000 to give organizations the ability to manage multiple on-premises infrastructure components and systems by using a single identity per user.

When you secure identities on-premises with Active Directory, Microsoft doesn't monitor sign-in attempts. When you connect Active Directory with Azure AD, Microsoft can help protect you by detecting suspicious sign-in attempts at no extra cost. For example, Azure AD can detect sign-in attempts from unexpected locations or unknown devices.

**Azure AD** provides services such as:

* **Authentication**

This includes verifying identity to access applications and resources. It also includes providing functionality such as self-service password reset, multifactor authentication, a custom list of banned passwords, and smart lockout services.

* **Single sign-on**

SSO enables you to remember only one username and one password to access multiple applications. A single identity is tied to a user, which simplifies the security model. As users change roles or leave an organization, access modifications are tied to that identity, which greatly reduces the effort needed to change or disable accounts.

* **Application management**

You can manage your cloud and on-premises apps by using Azure AD. Features like Application Proxy, SaaS apps, the My Apps portal (also called the access panel), and single sign-on provide a better user experience.

* **Device management**

Along with accounts for individual people, Azure AD supports the registration of devices. Registration enables devices to be managed through tools like Microsoft Intune. It also allows for device-based **Conditional Access** policies to restrict access attempts to only those coming from known devices, regardless of the requesting user account.

Azure AD can be used on both external services, such as Microsoft Office 365 or Azure Portal, and internal services, such as apps developed within your organization.

To connect Azure AD with an existing Active Directory you can use **Azure AD Connect**, which syncs user identities between Azure AD and Active Directory.

To use Conditional Access, you need an Azure AD Premium P1 or P2 license. If you have a Microsoft 365 Business Premium license, you also have access to Conditional Access features.

**KEYWORDS:**

***Multifactor Authentication:*** additional authorization checks, which can be something the user knows, something the user has, and something the user is (biometrics, SMS, etc.).

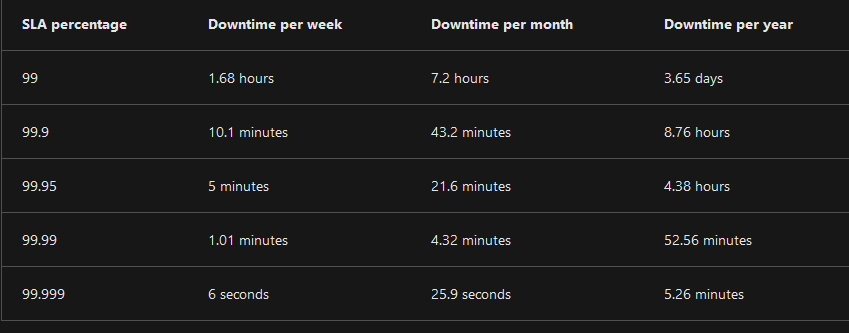
***Authentication (AuthN):*** are you who you say you are? (if yes, the user is authenticated)

***Authorization (AuthZ):*** gives the authenticated user or service some power, which determines what they have access to.

# [Service Level Agreements](https://docs.microsoft.com/en-us/learn/modules/choose-azure-services-sla-lifecycle/) (SLAs)

Service Level Agreements are a standard (not just for Microsoft and Azure), but generally in business. They can be used for both internal (e.g. between departments in a business) and external agreements (e.g. between “MyCompany” and Microsoft).

They define the guaranteed level of provider gives to the receiver and vice versa. This could, for example, be a % uptime of a service. E.g. a service has 99% uptime or 99.9% uptime.

  
Chart showing uptime in concrete numbers based on percentage.   
Source: <https://docs.microsoft.com/en-us/learn/modules/choose-azure-services-sla-lifecycle/2-what-are-service-level-agreements>

You can [see Azure’s SLA’s at this link](https://azure.microsoft.com/en-us/support/legal/sla/).   
Example service agreement: <https://azure.microsoft.com/en-us/support/legal/sla/mysql/v1_2/>

## Typical Azure SLA Parts

**Introduction**

This section explains what to expect in the SLA, including its scope and how subscription renewals can affect the terms.

**General terms**

This section contains terms that are used throughout the SLA so that both parties (you and Microsoft) have a consistent vocabulary. For example, this section might define what's meant by downtime, incidents, and error codes.

This section also defines the general terms of the agreement, including how to submit a claim, receive credit for any performance or availability issues, and limitations of the agreement.

**SLA details**

This section defines the specific guarantees for the service. Performance commitments are commonly measured as a percentage. That percentage typically ranges from 99.9 percent ("three nines") to 99.99 percent ("four nines").

The primary performance commitment typically focuses on uptime, or the percentage of time that a product or service is successfully operational. Some SLAs focus on other factors as well, including latency, or how fast the service must respond to a request.

This section also defines any additional terms that are specific to this service.

## Calculating an apps uptime

To more accurately calculate uptime for an app dependent on multiple services you do the following:

* Take each service’s SLA guaranteed uptime
* Multiply them which each other (add the uptime of a service multiple times, if the app depends on more than one)

**Example:** we have an app that uses an [App Service](https://azure.microsoft.com/en-us/support/legal/sla/app-service/v1_5/) (on a non-free tier) + a [General Purpose SQL Server Database](https://azure.microsoft.com/en-us/support/legal/sla/azure-sql-database/v1_6/) + [Azure Maps](https://azure.microsoft.com/en-us/support/legal/sla/azure-maps/v1_0/)

* The App Service has a 99.95% uptime
* The Map Service has a 99.99% uptime
* The Database Service has a 99.99% uptime

This is the calculation: 0.9995 (app) \* 0.9999 (database) \* 0.9995 (maps) = 0.9989 (99.89% uptime)

If we add a [Single Instance Virtual Machine using Standard HDD Managed Disks](https://azure.microsoft.com/en-us/support/legal/sla/virtual-machines/v1_9/) (which doesn’t seem relevant, considering that the App Service handles the infrastructure)

* The Virtual Machine has a 95% uptime

The guaranteed uptime plummets to 0.9989 \* 0.95 = 0.9489 (94.89% uptime)

# Managing Costs in Azure

Microsoft provides some tools to calculate costs for running Azure.

One of those tools is the [TCO Calculator](https://azure.microsoft.com/en-us/pricing/tco/calculator/) (Total Cost of Ownership Calculator). The TCO compares on-premises cost vs. Azure costs.

The TCO Calculator is used in 3 steps.

* Define your workloads (what are you using at your on-premises datacenter)
* Adjust assumptions (adjustments to electricity costs, IT personnel, hardware maintenance costs, etc.)
* View the report.

## Purchasing Azure Services

The following questions may arise, when you want to migrate to Azure:

* What types of Azure subscriptions are available?
* How do we purchase Azure services?
* Does location or network traffic affect cost?
* What other factors affect the final cost?
* How can we get a more detailed estimate of the cost to run on Azure?

### Subscription types

Azure offers both free and paid subscription options to fit your needs and requirements. They are:

**Free trial**

A free trial subscription provides you with 12 months of popular free services, a credit to explore any Azure service for 30 days, and more than 25 services that are always free. Your Azure services are disabled when the trial ends or when your credit expires for paid products, unless you upgrade to a paid subscription.

[Overview of free services](https://azure.microsoft.com/en-in/pricing/free-services/)

**Pay-as-you-go**

A pay-as-you-go subscription enables you to pay for what you use by attaching a credit or debit card to your account. Organizations can apply for volume discounts and prepaid invoicing.

**Member offers**

Your existing membership to certain Microsoft products and services might provide you with credits for your Azure account and reduced rates on Azure services. For example, member offers are available to **Visual Studio subscribers**, Microsoft Partner Network members, Microsoft for Startups members, and Microsoft Imagine members.

### Purchasing services

You can purchase services through 3 ways:

* An Enterprise Agreement (Large customers, a commitment of 3 years for expected services)
* Directly from the web aka Web Direct (through Azure portal with standard prices, billed monthly)
* Through a Cloud Solution Provider (CSP). A Microsoft Partner, that assists with your usage of Azure. Bills go through them.

## What affects cost?

The type of resource you use. Example: You want Storage. What type of storage? Is it SDD, is it a Blob, is it Hot, Cold or Archive? Another resource could be a Virtual Machine, which also have a lot of parameters on cost.

Determining how much a resource was used depends on multiple factors. In the case of a VM these factors are relevant:

* Overall CPU time.
* Time spent with a public IP address.
* Incoming (ingress) and outgoing (egress) network traffic of the VM.
* Disk size and amount of disk read and disk write operations.

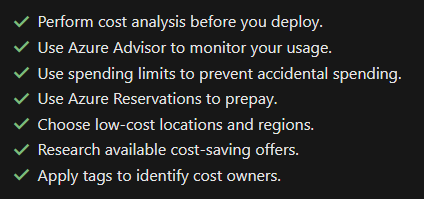
In Azure, you can delete or **deallocate** a VM. Deleting a VM means that you no longer need it. The VM is removed from your subscription, and then it's prepared for another customer.

**Deallocating a VM means that the VM is no longer running**. But the associated hard disks and data are still kept in Azure. The VM isn't assigned to a CPU or network in Azure's datacenter, so it doesn't generate the costs associated with compute time or the VM's IP address. Because the disks and data are still stored, and the resource is present in your Azure subscription, you're **still billed for disk storage**.

Another tool Microsoft provides is the [Azure Pricing](https://azure.microsoft.com/en-us/pricing/calculator/) calculator, which can be used to get an estimate of what it would cost to use Azure.

## Minimize costs

* Before you deploy, consider options carefully use the Azure Pricing & TCO Calculator.
* Make use of Azure Advisor to cut resources you don’t use
* Utilize Azure Cost Management + Billing, which can:
* Report on usage
* Categorize used resources
* Create and manage budgets
* Alert you on usage
* Provide recommendations
* De-allocate Virtual Machines during off hours (e.g. test VMs in weekends)
* Delete unused resources
* Migrate from IaaS to PaaS services
* Save on licensing – eg. Use Linux instead of Windows for hosting, when able.
* Use Azure Hybrid Benefit (make use of previously purchased licenses)



1. <https://techcommunity.microsoft.com/t5/itops-talk-blog/azure-security-product-name-changes-microsoft-ignite-november/ba-p/3004418?WT.mc_id=modinfra-48365-socuff> [↑](#footnote-ref-1)
2. <https://docs.microsoft.com/en-us/learn/modules/azure-database-fundamentals/azure-mysql-database> [↑](#footnote-ref-2)
3. <https://docs.microsoft.com/en-us/learn/modules/azure-database-fundamentals/azure-cosmos-db> [↑](#footnote-ref-3)