# KOENIG

step forward

# Cloud Computing

# Cloud Computing

- Cloud computing
  - What is cloud computing
  - Shared responsibility
  - Cloud models
  - Capital vs operational costing
- Cloud benefits
  - Benefits of the cloud
- Cloud service types
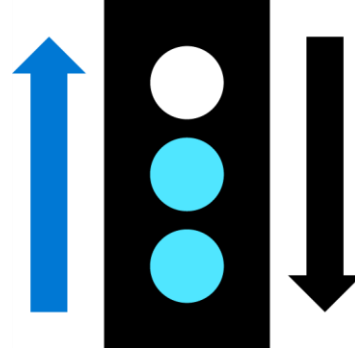  - IaaS, PaaS, and SaaS

# What is cloud computing?

- Cloud computing is the delivery of computing services over the internet, enabling faster innovation, flexible resources, and economies of scale.
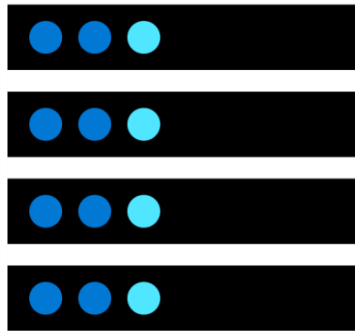
Compute        Networking        Storage

# Cloud models : private, public, and hybrid.

- Private cloud
  - Organizations create a cloud environment in their datacenter.
  - Organizations are responsible for operating the services they provide.
  - Does not provide access to users outside of the organization.
- Public cloud
  - Owned by cloud services or hosting provider.
  - Provides resources and services to multiple organizations and users.
  - Accessed via secure network connection (typically over the internet).

# Cloud models : private, public, and hybrid.

- Hybrid cloud
  - Combines public and private clouds to allow applications to run in the most appropriate location.
  - Hybrid cloud models have the following characteristics:
    - **Resource location.** Specific resources are run or used in a public cloud—others are run or used in a private cloud.
    - **Cost and efficiency.** Hybrid cloud models allow an organization to leverage some of the benefits of cost, efficiency, and scale that are available with a public cloud model.
    - **Control.** Organizations retain management control in private clouds.
    - **Skills.** Technical skills are still required to maintain the private cloud and ensure both cloud models can operate together.

# Cloud models : private, public, and hybrid.

- Cloud model comparison

| Public cloud | Private cloud | Hybrid cloud |
|---|---|---|
| • No capital expenditures to scale up.<br>• Applications can be quickly provisioned and deprovisioned.<br>• Organizations pay only for what they use. | • Hardware must be purchased for start-up and maintenance.<br><br>• Organizations have complete control over resources and security.<br><br>• Organizations are responsible for hardware maintenance and updates. | • Provides the most flexibility.<br><br>• Organizations determine where to run their applications.<br><br>• Organizations control security, compliance, or legal requirements. |

# Compare CapEx vs. OpEx

- Capital expenditure (CapEx)
  - Spend on physical infrastructure upfront.
  - Deduct the expense from your tax bill.
  - High upfront cost, but the value of your investment reduces over time.
- Operational expenditure (OpEx)
  - Spend on services or products as needed.
  - Get billed immediately.
  - Deduct the expense from your tax bill in the same year.
  - No upfront cost, pay-as-you-use.

# Consumption-based model

- Cloud service providers operate on a consumption-based model, which means that end users only pay for the resources that they use.
  - Better cost prediction.
  - Prices for individual resources and services are provided.
  - Billing is based on actual usage.

# Cloud benefits

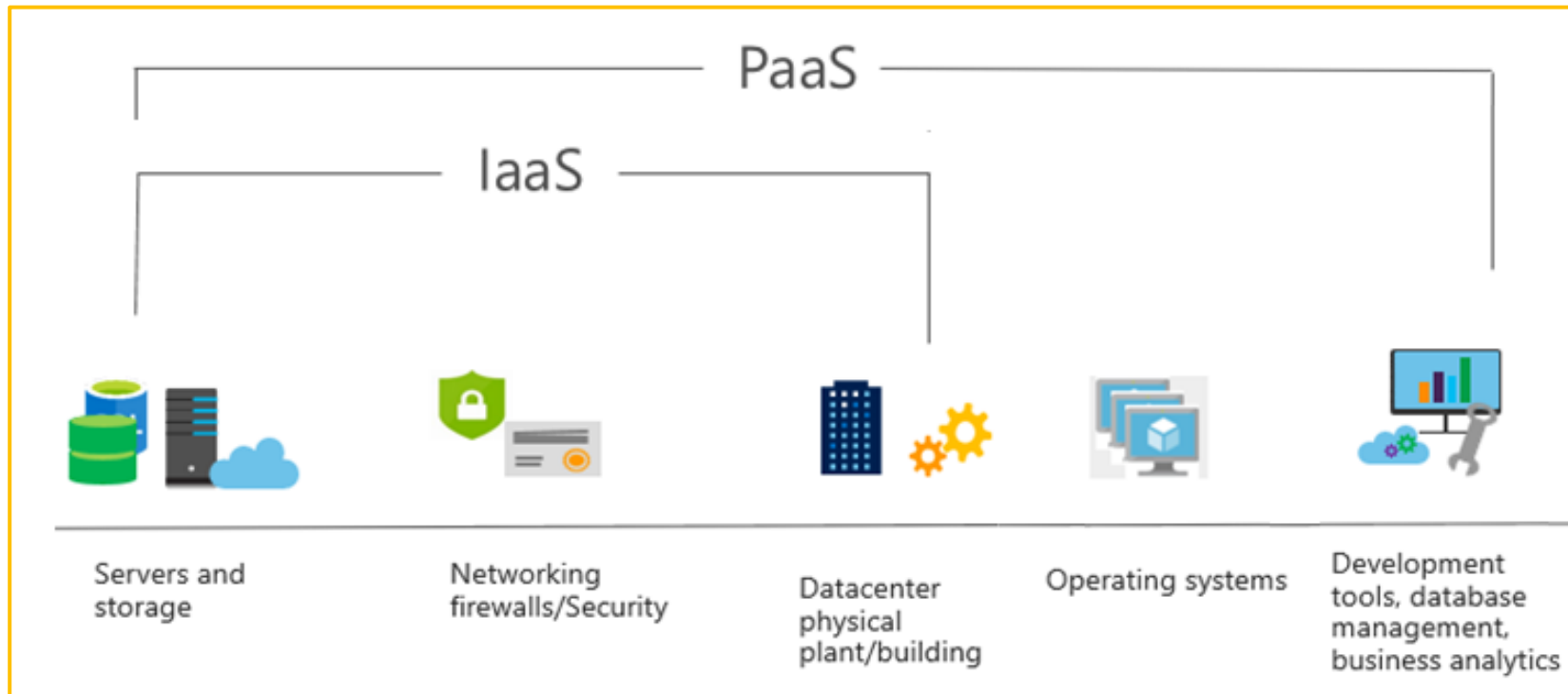| | |
|---|---|
| High availability | Elasticity |
| Scalability | Reliability |
| Predictability | Security |
| Governance | Manageability |

# Infrastructure as a service (IaaS)

- Build pay-as-you-go IT infrastructure by renting servers, virtual machines, storage, networks, and operating systems from a cloud provider.
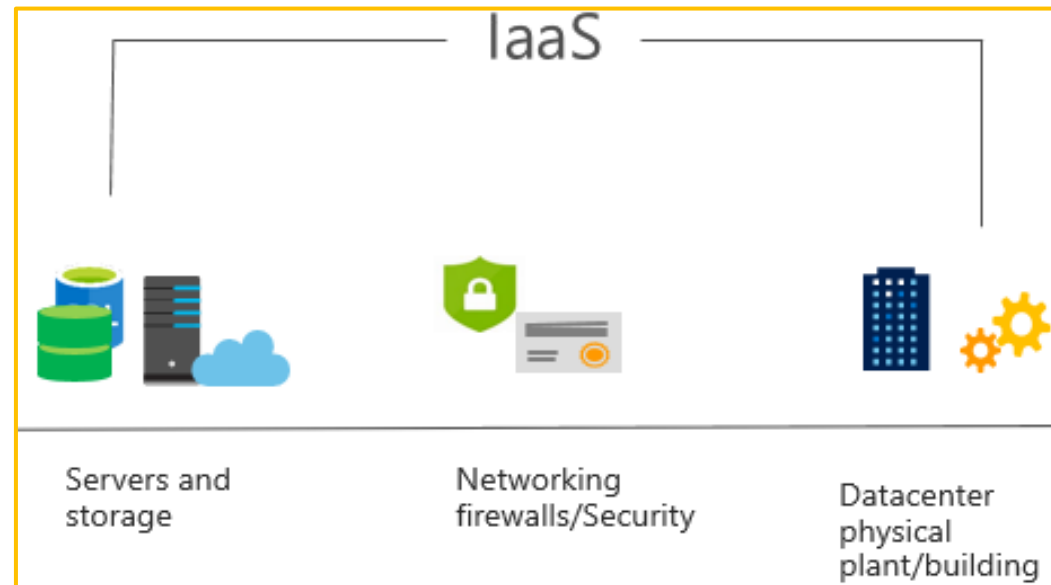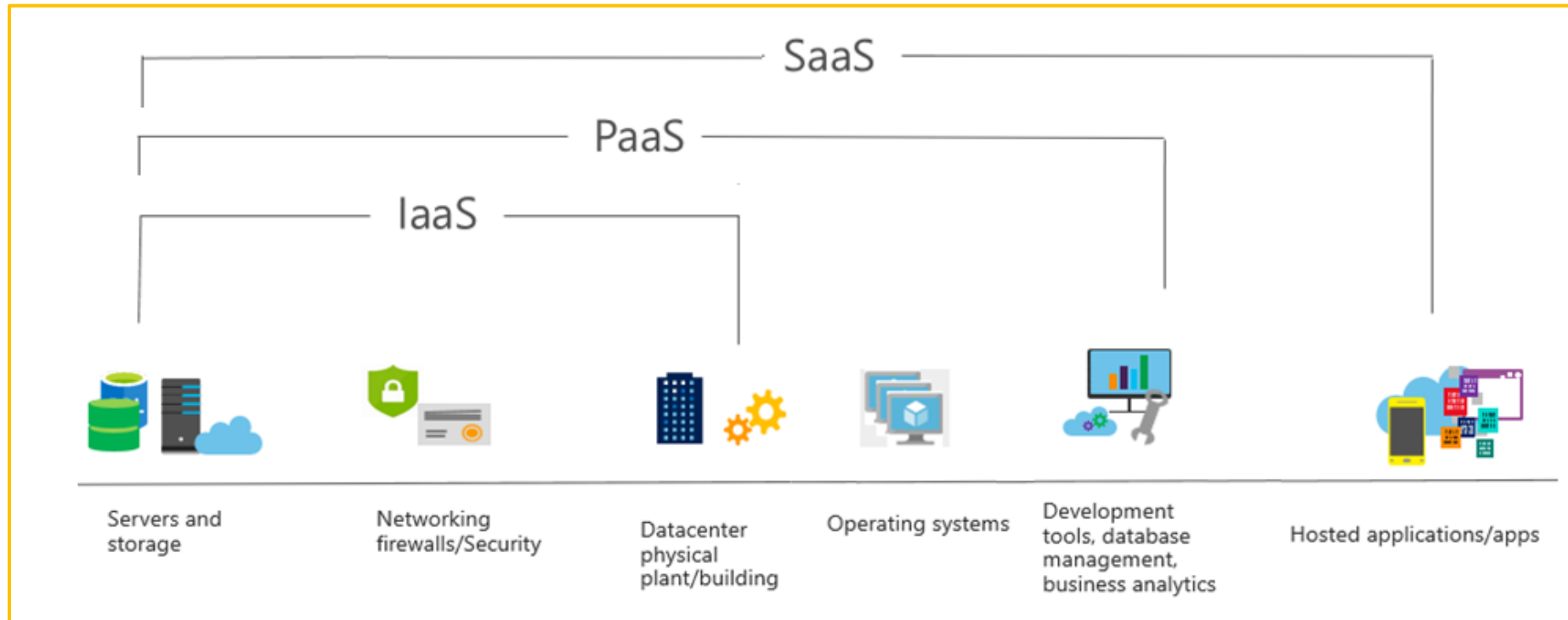
# Platform as a service (PaaS)

- Provides an environment for building, testing, and deploying software applications; without focusing on managing underlying infrastructure.



PaaS

IaaS

| Servers and storage | Networking firewalls/Security | Datacenter physical plant/building | Operating systems | Development tools, database management, business analytics |

# Software as a service (SaaS)

- Users connect to and use cloud-based apps over the internet: for example, Microsoft Office 365, email, and calendars.



SaaS

PaaS

IaaS

Servers and storage | Networking firewalls/Security | Datacenter physical plant/building | Operating systems | Development tools, database management, business analytics | Hosted applications/apps

# Cloud service comparison

## IaaS

- The most flexible cloud service.

- You configure and manage the hardware for your application.

## PaaS

- Focus on application development.

- Platform management is handled by the cloud provider.

## SaaS

- Pay-as-you-go pricing model.

- Users pay for the software they use on a subscription model.

# Infrastructure

# Infrastructure

- Compute and networking
  - Compute types
  - Application hosting
  - Virtual networking

- Storage
  - Storage services
  - Redundancy options
  - File management and migration

# Azure compute services

- Azure compute is an on-demand service that provides computing resources such as disks, processors, memory, networking, and operating systems.
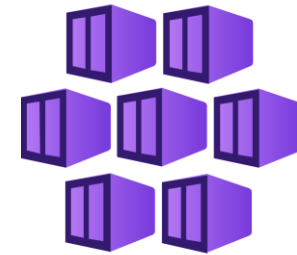
Virtual
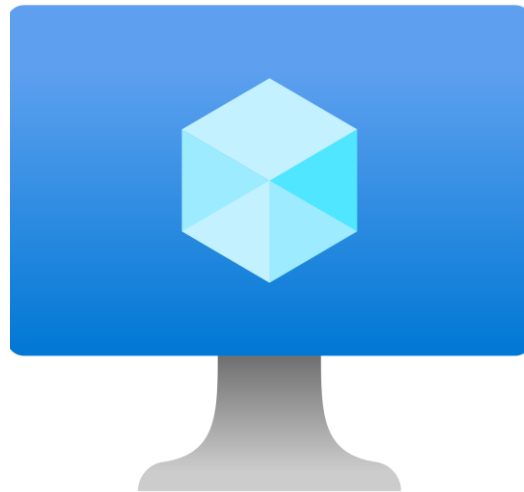Machines

App
Services
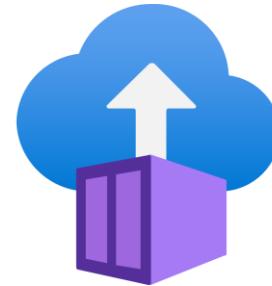
Container
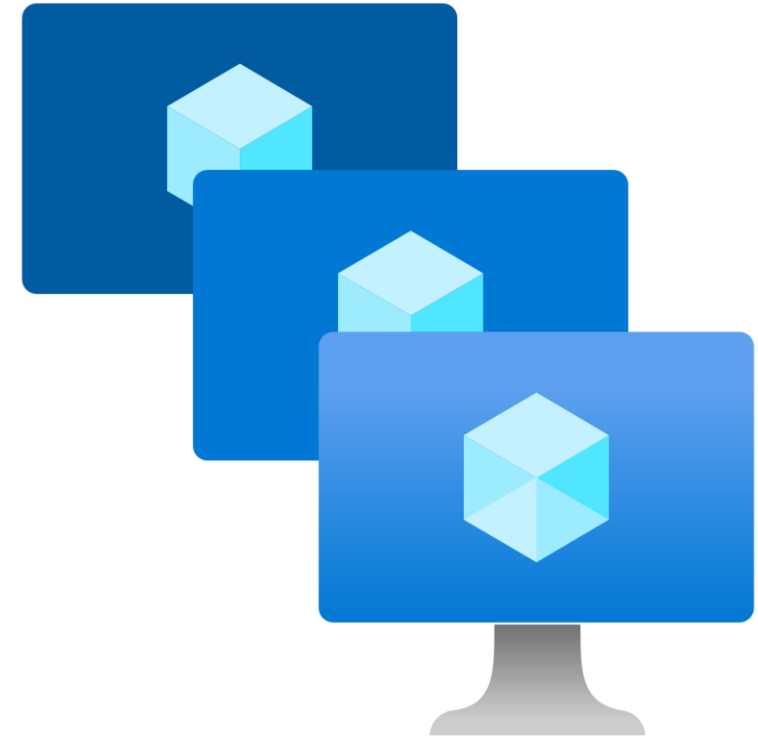Instances

Azure Kubernetes
Services (AKS)

# Azure virtual machines

- Azure virtual machines (VMs) are software emulations of physical computers.
    - Includes virtual processor, memory, storage, and networking.
    - IaaS offering that provides total control and customization.

# VM scale sets

- Scale sets provide a load-balanced opportunity to automatically scale resources.
  - Scale out when resource needs increase.
  - Scale in when resource needs are lower.

# Azure container services

- Azure containers provide a lightweight, virtualized environment that does not require operating system management, and can respond to changes on demand.

**Azure Container Instances**: A PaaS offering that runs a container or pod of containers in Azure.

**Azure Container Apps**: A PaaS offering, like container instances, that can load balance and scale.

**Azure Kubernetes Service**: An orchestration service for containers with distributed architectures and large volumes of containers.

# Comparing Azure compute options

## Virtual machines

- Cloud-based server that supports either Windows or Linux environments.

- Useful for lift-and-shift migrations to the cloud.

- Complete operating system package, including the host operating system.

## Containers

- Lightweight, miniature environment well suited for running microservices.

- Designed for scalability and resiliency through orchestration.

- Applications and services are packaged in a container that sits on top of the host operating system. Multiple containers can sit on one host OS.

# Azure App Services

- Azure App Services is a fully managed platform to build, deploy, and scale web apps and APIs quickly.
  - Works with .NET, .NET Core, Node.js, Java, Python, or php.
  - PaaS offering with enterprise-grade performance, security, and compliance requirements.

# Azure networking services

- Azure Virtual Network (VNet) enables Azure resources to communicate with each other, the internet, and on-premises networks.
  - Public endpoints, accessible from anywhere on the internet.
  - Private endpoints, accessible only from within your network.
  - Virtual subnets segment your network to suit your needs.
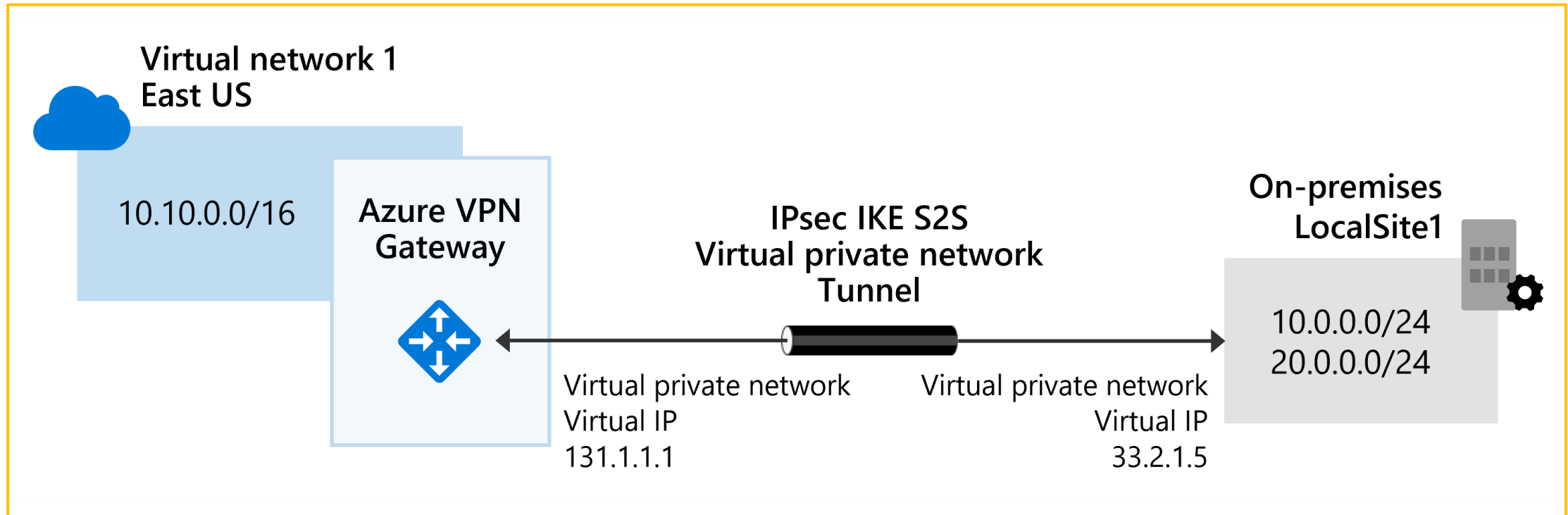  - Network peering connects your private networks directly together.
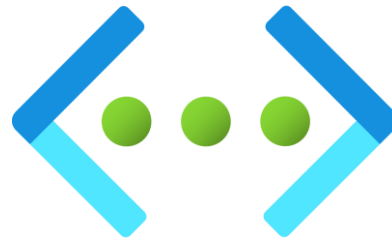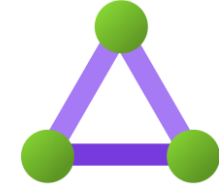
# Azure networking services: VPN Gateway

- VPN Gateway is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public internet.

**Virtual network 1**
**East US**

10.10.0.0/16

**Azure VPN Gateway**

**IPsec IKE S2S**
**Virtual private network**
**Tunnel**

**On-premises LocalSite1**

10.0.0.0/24
20.0.0.0/24

Virtual private network
Virtual IP
131.1.1.1

Virtual private network
Virtual IP
33.2.1.5

# Azure DNS

- Reliability and performance by leveraging a global network of DNS name servers using Anycast networking.

- Azure DNS security is based on Azure resource manager, enabling role-based access control and monitoring and logging.

- Ease of use for managing your Azure and external resources with a single DNS service.

- Customizable virtual networks allow you to use private, fully customized domain names in your private virtual networks.

- Alias records support alias record sets to point directly to an Azure resource.

# Storage

# Storage

- Must have a globally unique name.

- Provide over-the-internet access worldwide.

- Determine storage services and redundancy options.
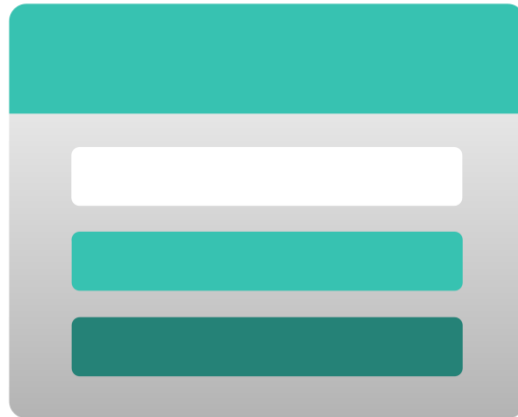
# Azure storage services

**Azure Blob:** Optimized for storing massive amounts of unstructured data, such as text or binary data.

**Azure Disk:** Provides disks for virtual machines, applications, and other services to access and use.

**Azure Files:** Sets up a highly available network file share that can be accessed by using the Server Message Block protocol.

**Azure Tables:** Provides a key/attribute option for structured nonrelational data storage with a schema-less design.

# Storage service public endpoints

| Storage service | Public endpoint |
|---|---|
| Blob Storage | https://<storage-account-name>.blob.core.windows.net |
| Data Lake Storage Gen2 | https://<storage-account-name>.dfs.core.windows.net |
| Azure Files | https://<storage-account-name>.file.core.windows.net |
| Queue Storage | https://<storage-account-name>.queue.core.windows.net |
| Table Storage | https://<storage-account-name>.table.core.windows.net |

# Azure storage access tiers

| Hot | Cool | Cold | Archive |
|-----|------|------|---------|
| Optimized for storing data that is accessed frequently. | Optimized for storing data that is infrequently accessed and stored for at least 30 days. | Optimized for storing data that is infrequently accessed and stored for at least 90 days. | Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements. |

# Cloud Security Fundamentals

# Cloud Security Fundamentals

- Microsoft Entra ID
- Compare authentication and authorization
- Multifactor authentication
- Conditional Access
- Role-based access control
- Zero Trust
- Defense in depth
- Microsoft Defender for Cloud

# Microsoft Entra ID

- Microsoft Entra ID is Microsoft Azure's cloud-based identity and access management service.
    - Authentication (employees sign in to access resources).
    - Single sign-on (SSO).
    - Application management.
    - Business to Business (B2B).
    - Device management.

# Microsoft Entra Domain Services

- Gain the benefit of cloud-based domain services without managing domain controllers.

- Run legacy applications (that can't use modern auth standards) in the cloud.

- Automatically sync from Microsoft Entra ID.

Sync users, groups, passwords, SIDs to ID

Microsoft Entra Connect Sync

Automatic background sync to your managed domain

*Virtual network*

Managed domain

Microsoft Entra ID tenant

On-premises AD
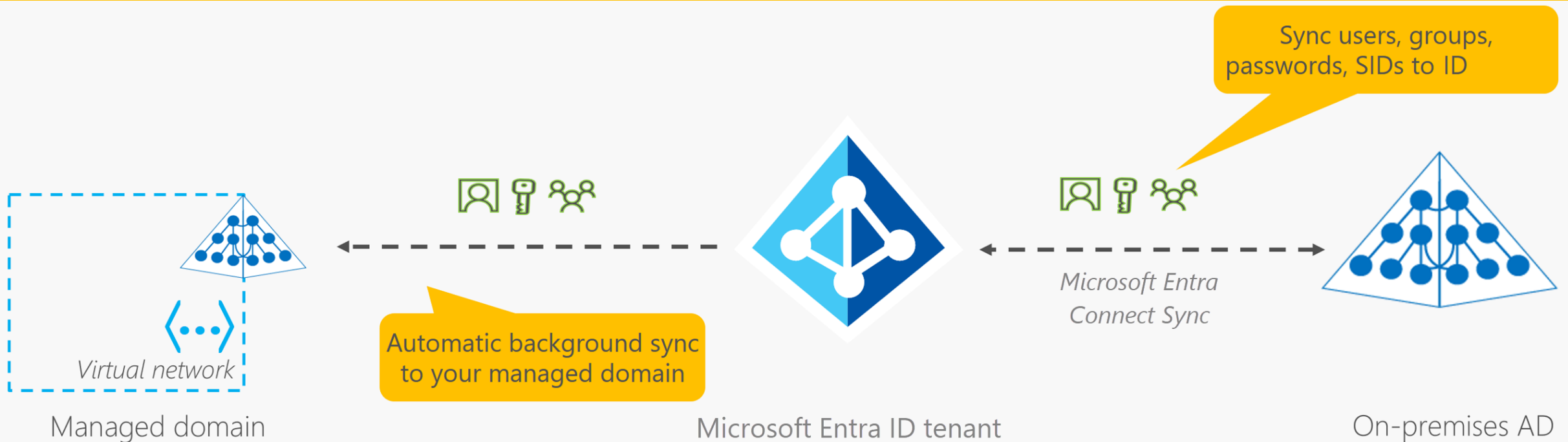
# Compare authentication and authorization

## Authentication

- Identifies the person or service seeking access to a resource.

- Requests legitimate access credentials.

- Basis for creating secure identity and access control principles.

## Authorization

- Determines an authenticated person's or service's level of access.

- Defines which data they can access, and what they can do with it.
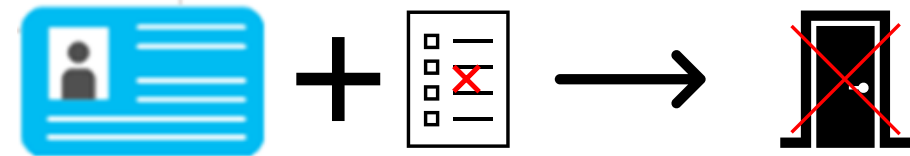
# Multifactor authentication

- Provides additional security for your identities by requiring two or more elements for full authentication.
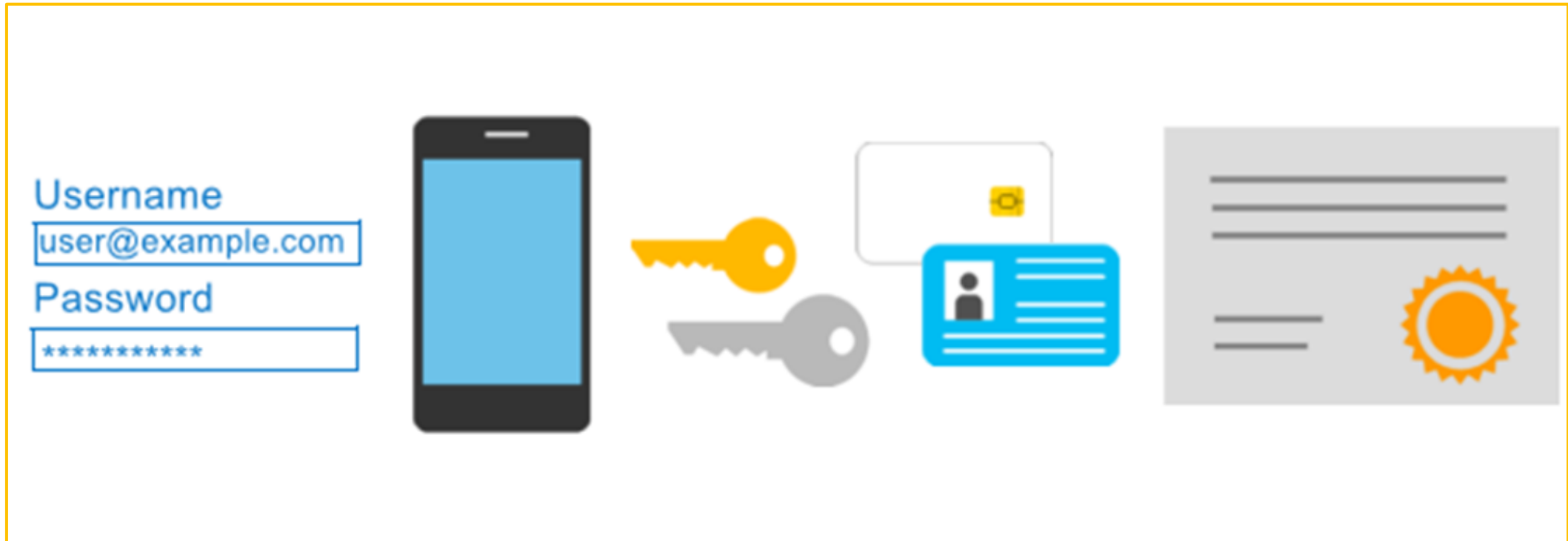
# Conditional Access

- Conditional Access is used to bring signals together, to make decisions, and enforce organizational policies.
  - User or group membership
  - IP location
  - Device
  - Application
  - Risk detection
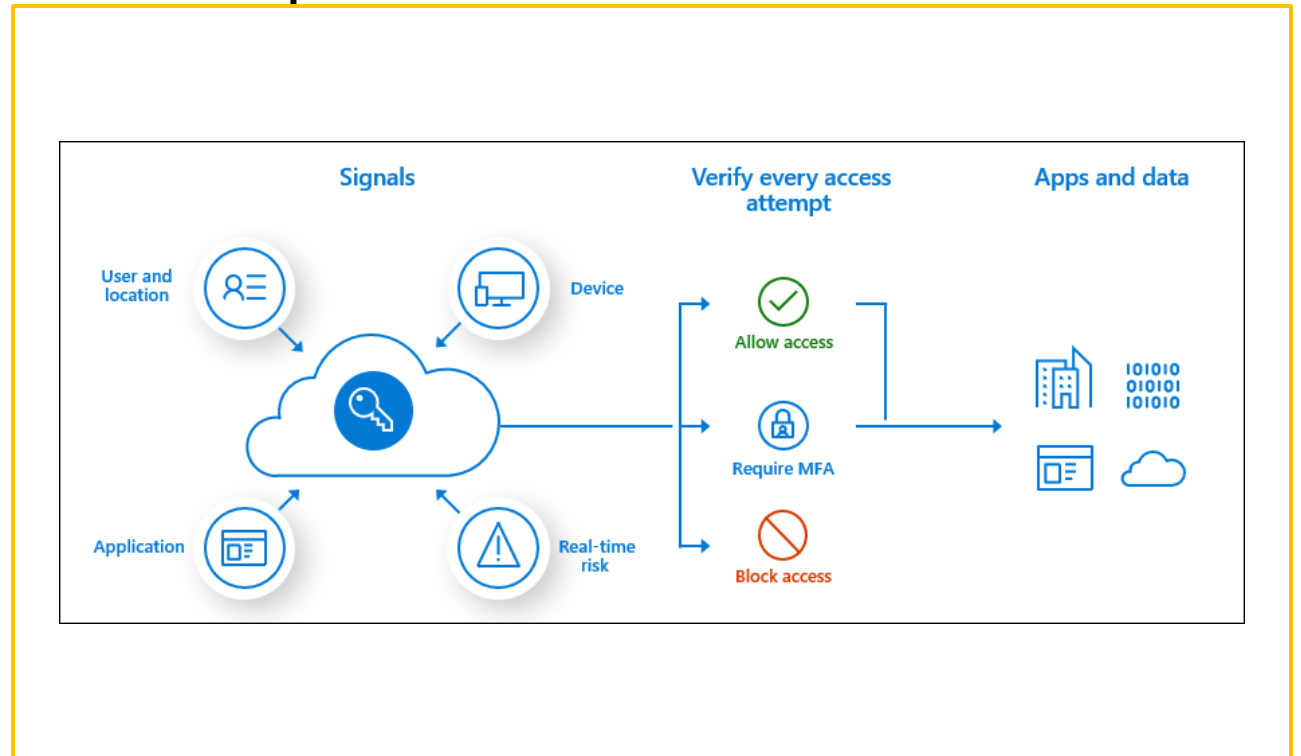
# Role-based access control

- Fine-grained access management.
- Segregate duties within the team and grant only the amount of access to users that they need to perform their jobs.
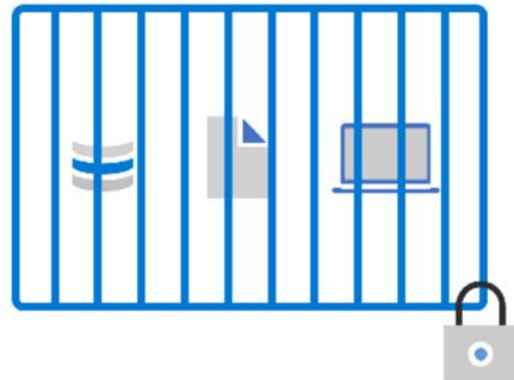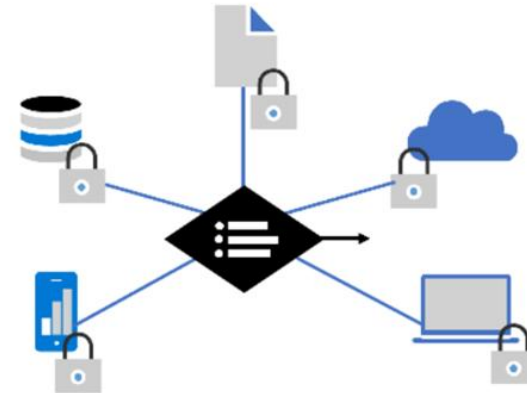- Enables access to the Azure portal and controlling access to resources.

Microsoft Entra ID

User    Apps    User groups

Azure

Azure subscription

Resource group

Resource group
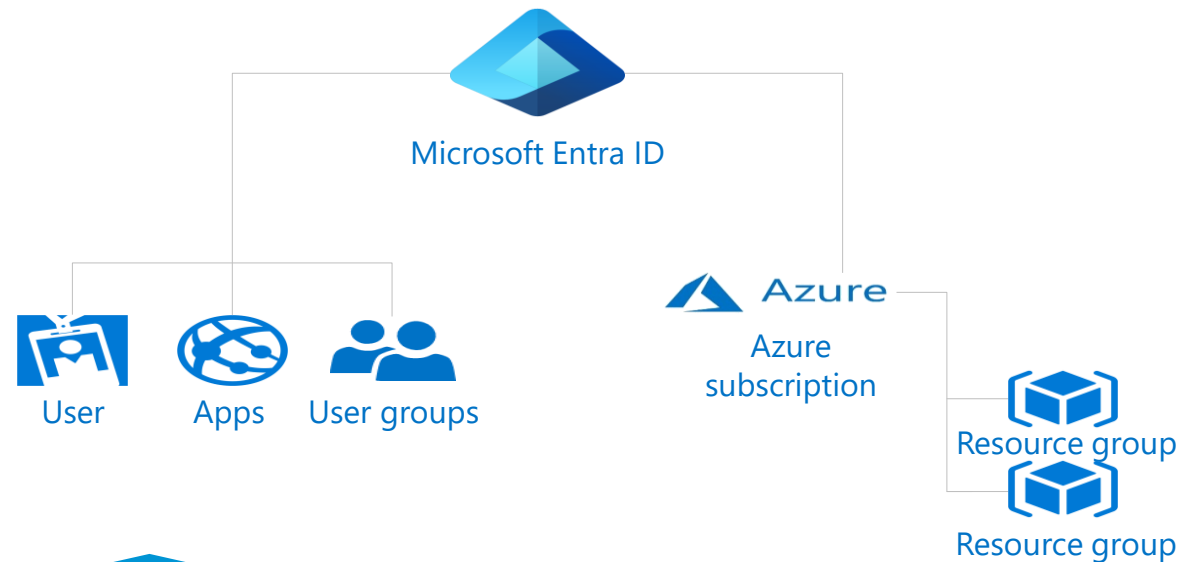
# Zero Trust



Secure assets where they are with Zero Trust

Simplify security and make it more effective

**Classic Approach**
Restrict everything to a 'secure' network

**Zero Trust**
Protect assets anywhere with central policy

# Defense in depth

- A layered approach to securing computer systems.

- Provides multiple levels of protection.

- Attacks against one layer are isolated from subsequent layers.



Physical security
Identity and access
Perimeter
Network
Compute
Application
Data
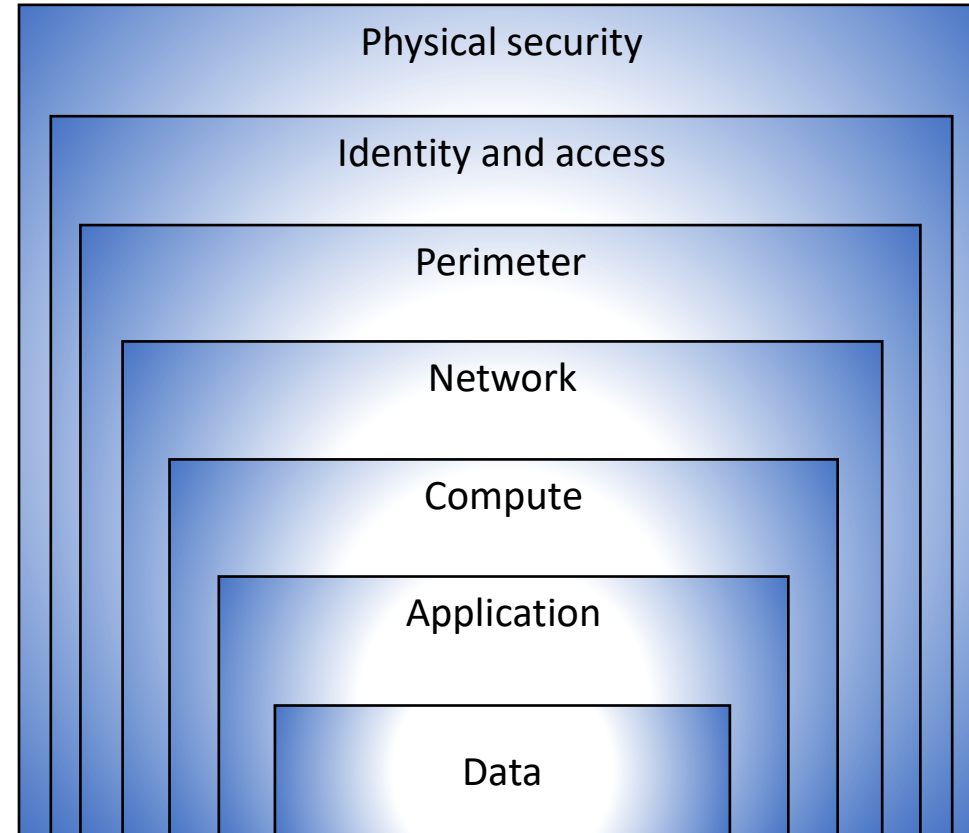
# Microsoft Defender for Cloud

- Microsoft Defender for Cloud is a monitoring service that provides threat protection across both Azure and on-premises datacenters.
  - Provides security recommendations.
  - Detect and block malware.
  - Analyze and identify potential attacks.
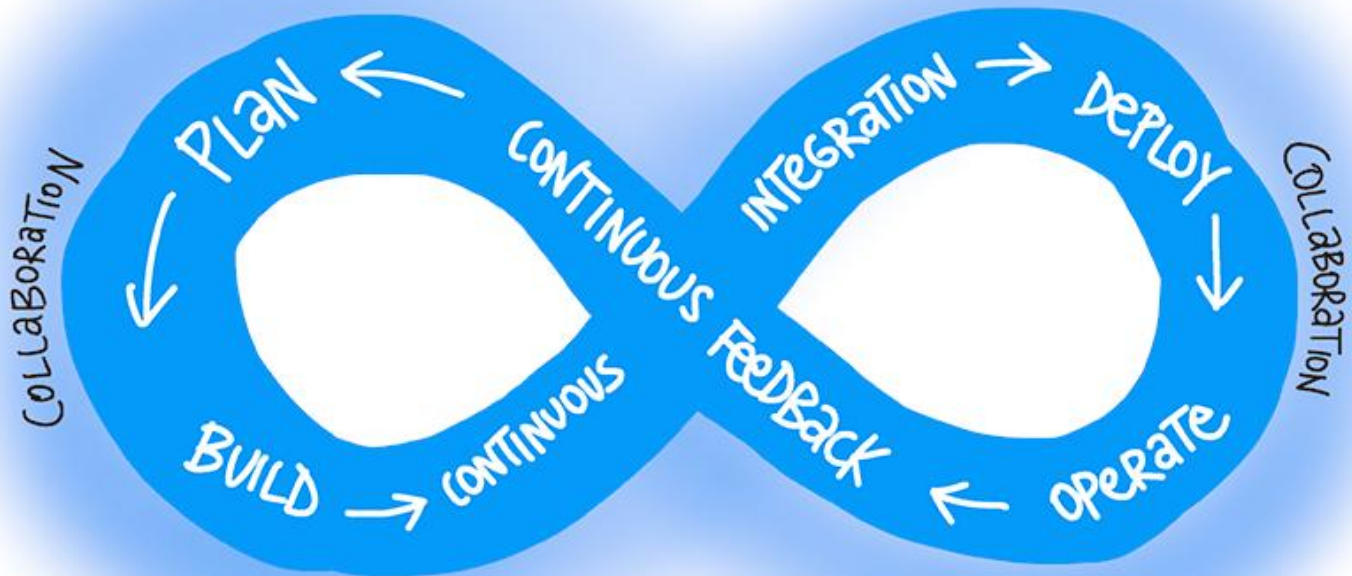  - Just-in-time access control for ports.

# DevOps

# What is DevOps?

"DevOps is the union of people, process, and products to enable continuous delivery of value to end users."
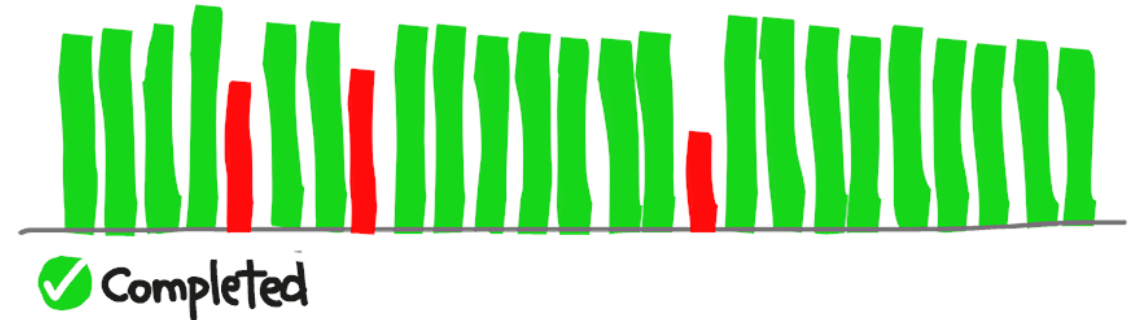
— Donovan Brown,
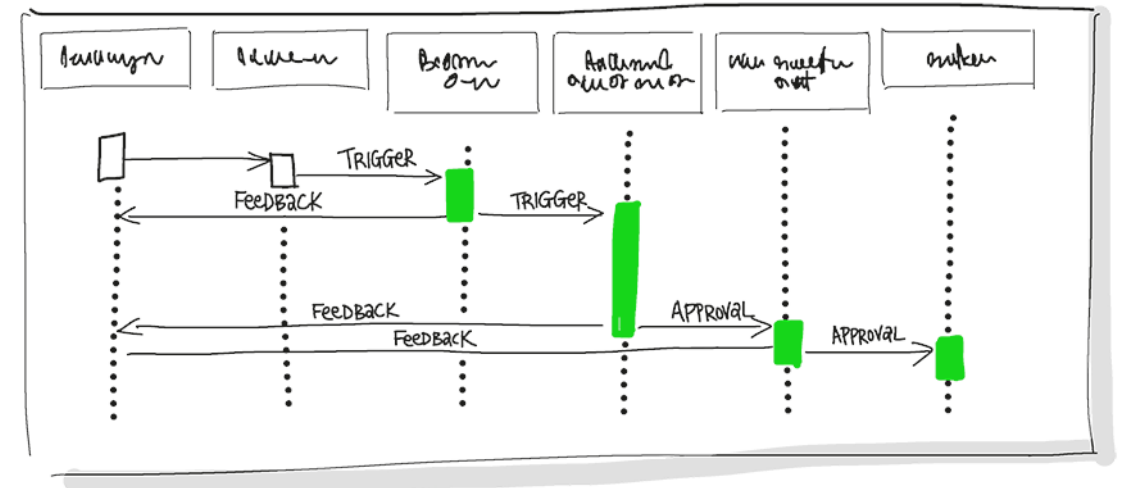
# Explore the DevOps journey

## Continuous Integration

- Continuous Integration drives the ongoing merging and testing of code, which leads to finding defects early.

## Continuous Delivery

- Continuous Delivery of software solutions to production and testing environments helps organizations quickly fix bugs and respond to ever-changing business requirements.
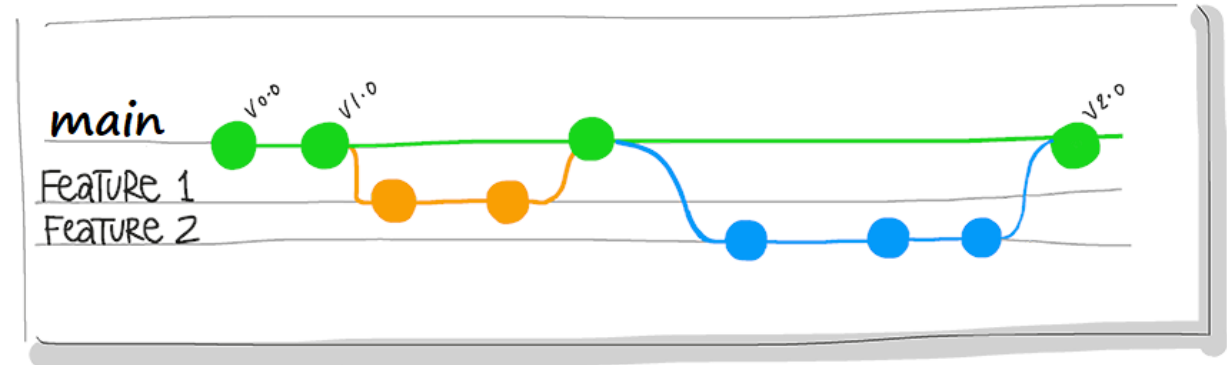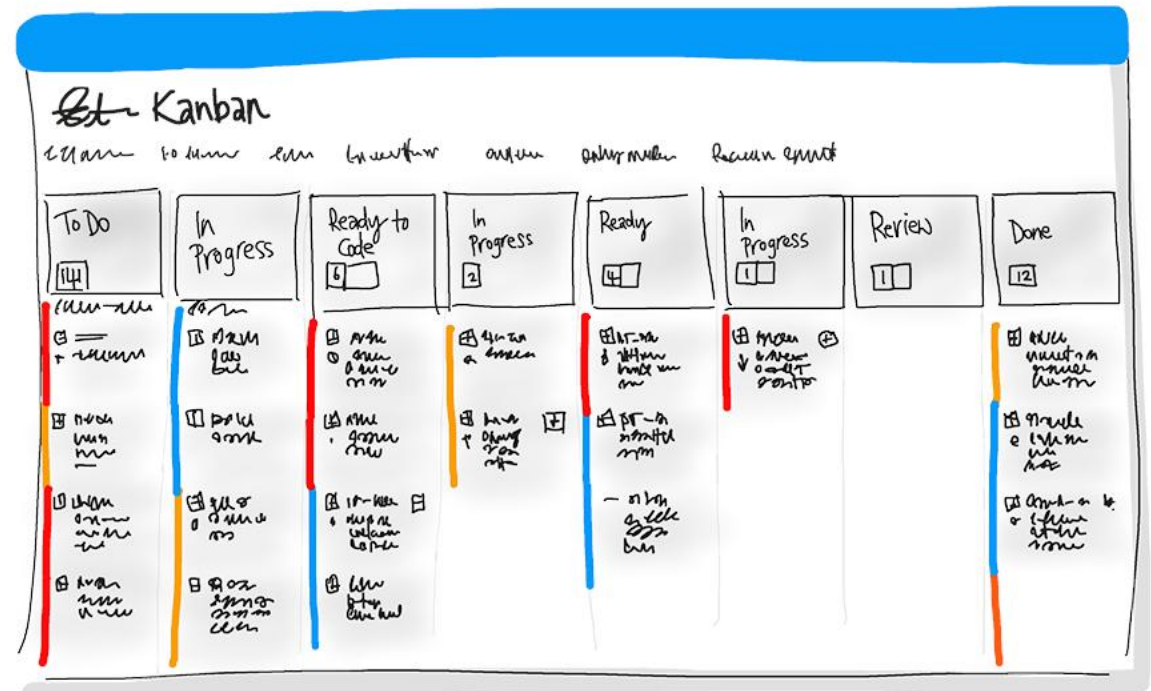
# Explore the DevOps journey

## Version Control

- Version Control, usually with a Git-based Repository, enables teams located anywhere in the world to communicate effectively during daily development activities.

## Agile/lean

- Plan and isolate work into sprints.

- Manage team capacity and help teams quickly adapt to changing business needs.

- A DevOps Definition of Done is working software collecting telemetry against the intended business goals.
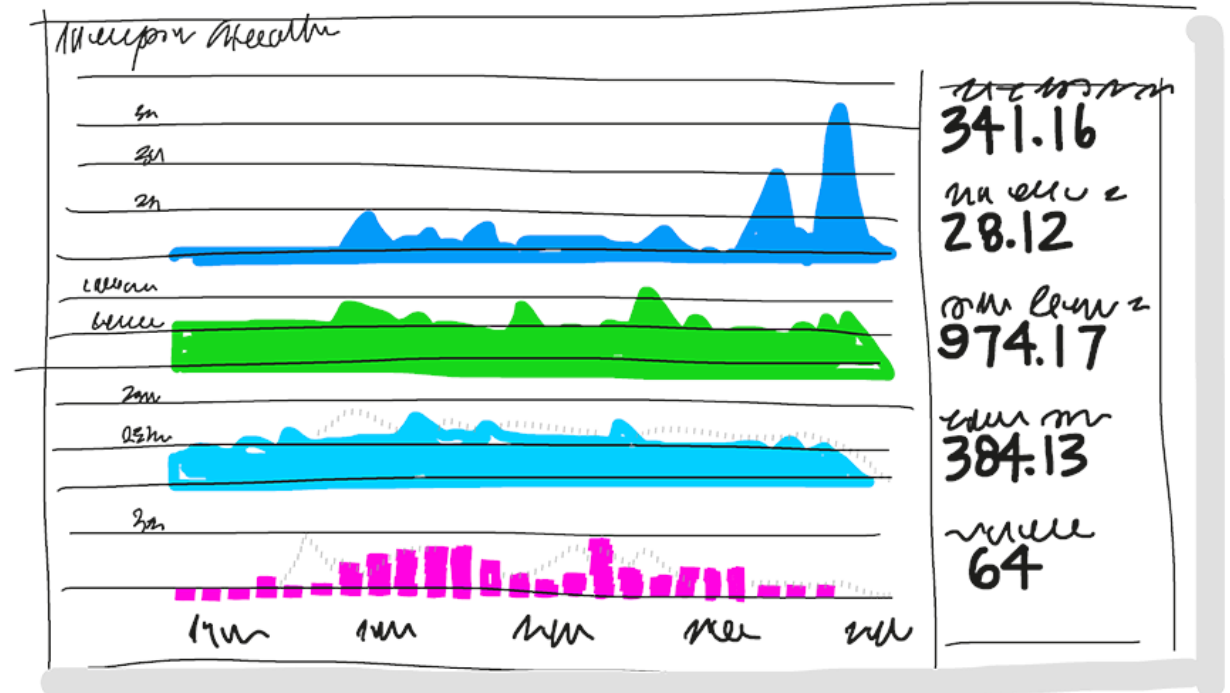
# Explore the DevOps journey

## Monitoring and logging

- Monitoring and Logging of running applications.

## Cloud

- Public and Hybrid Clouds have made the impossible easy.
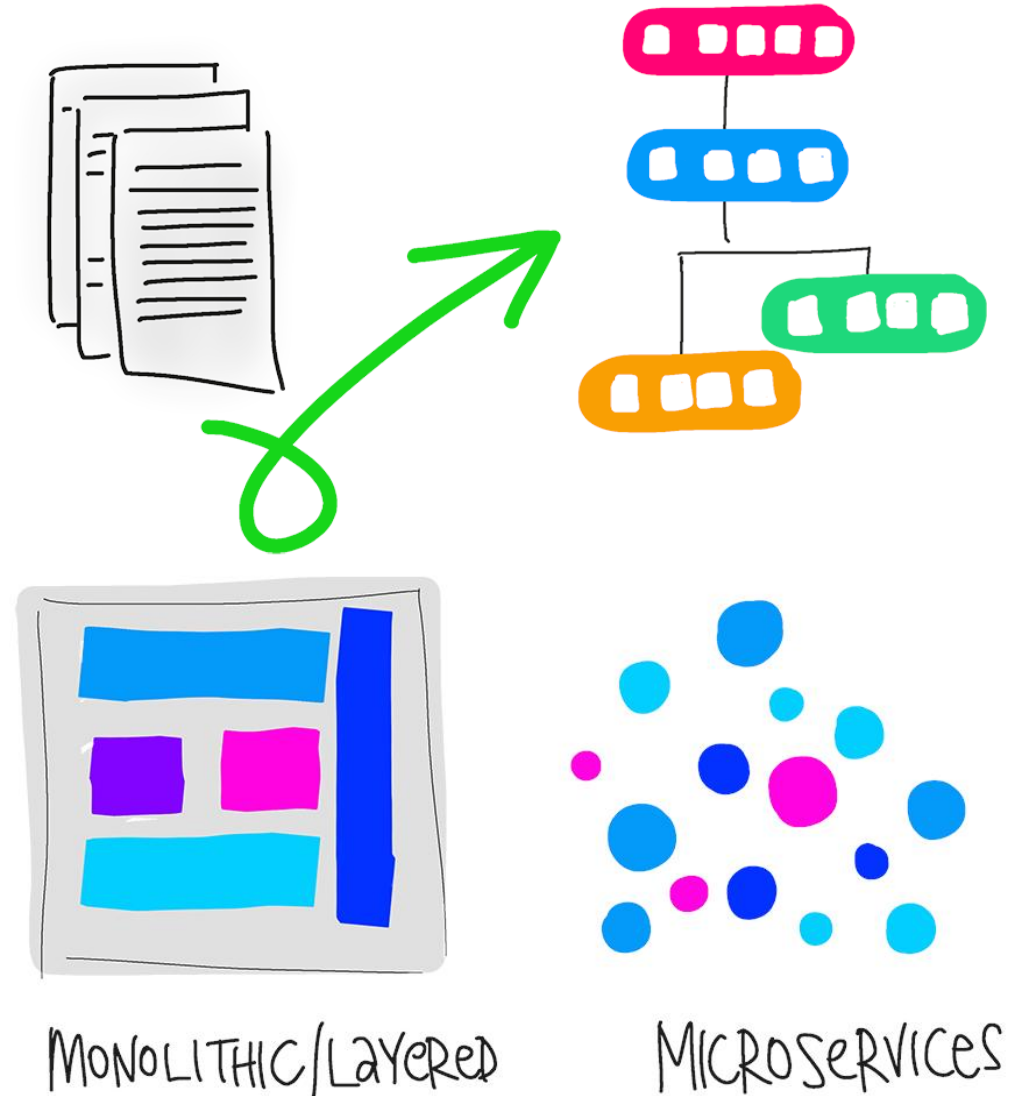
# Explore the DevOps journey

## Infrastructure as Code (IaC)

- Enables the automation and validation of the creation and teardown of environments to help with delivering secure and stable application hosting platforms.

## Microservices

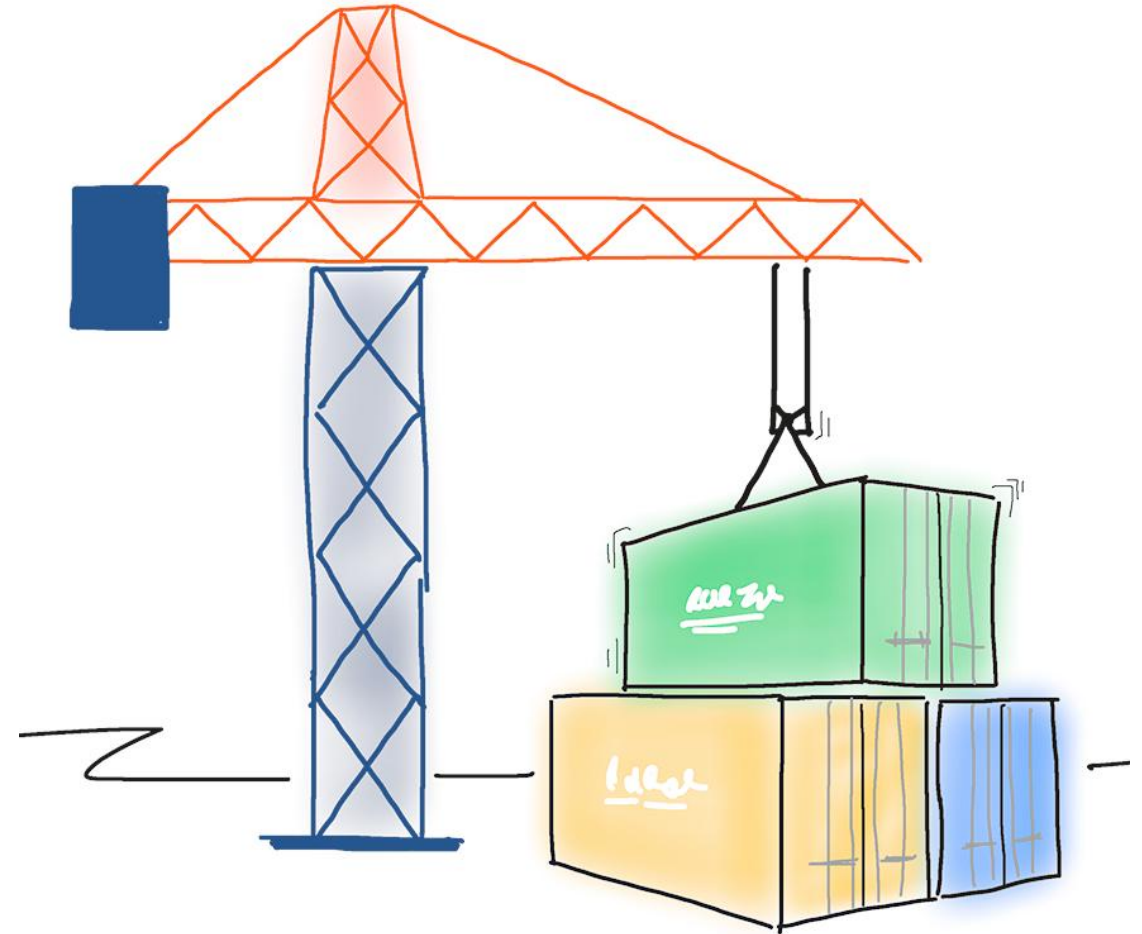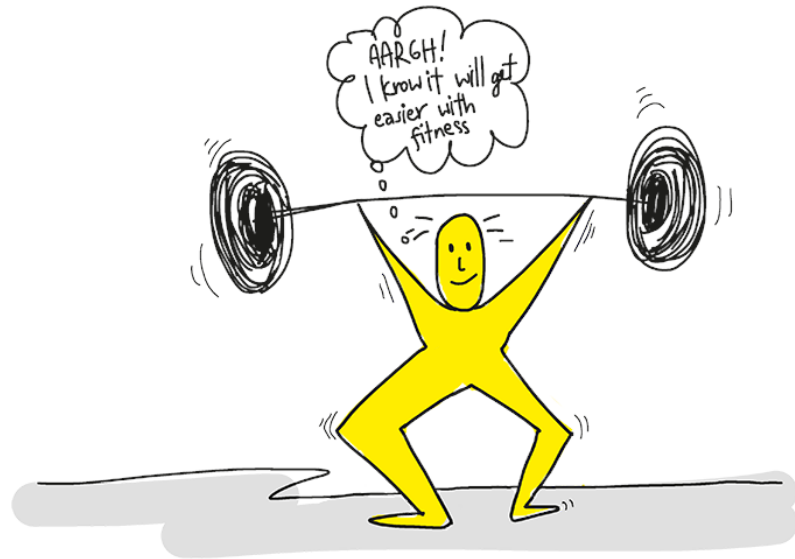- Isolate business use cases into small reusable services that communicate via interface contracts.

MONOLITHIC/LAYERED

MICROSERVICES

# Explore the DevOps journey

## Containers

- Containers are the next evolution in virtualization.

DevOps may hurt at first

# Explore agile development practices

Waterfall approach:

- Define, analyze, build and test, and deliver

- Hard to accurately define requirements, which can change over time, including during development

- Requires change requests and additional cost after delivery

Agile approach:

- Emphasizes constantly adaptive planning, and early delivery with continual improvement

- Development methods are based on releases and iterations

- At the end of each iteration, should have tested working code

- Is focused on shorter-term outcomes

# Explore principles of agile development

**1** Satisfy the customer through early and continuous delivery of valuable software

**2** Welcome changing requirements

**3** Deliver working software frequently

**4** Work together throughout the project

**5** Build projects around motivated individuals

**6** Use face-to-face conversation

**7** Measure progress through working software

**8** Agile processes promote sustainable development

**9** Continuous attention to technical excellence and good design

**10** Simplicity – The art of maximizing the amount of work not done

**11** Use self-organizing teams

**12** Reflect on how to become more effective

Happy Learning :)