# Describe cloud concepts

# Summary

- ✓ **Cloud Computing**: Services through the internet
- ✓ **Benefits of the cloud:**

### High Availability

Continuous functioning of services

### Scalability

Ability to handle increased load

### Security

Architected to handle security

### Manageability

Ability to manage cloud resources

### Reliability

Ability of a system to recover from failures and continue to function

### Predictability

Predictable cost and performance

### Governance

Support of Governance and Compliance

# Summary

✓ **CapEx:** Upfront cost & own infrastructure

**OpEx:** No upfront cost & "pay-as-you-go"

✓ **Public Cloud:** Shared hardware, services from the internet

**Private Cloud:** Own private data center, absolute control (can be connected to internet)

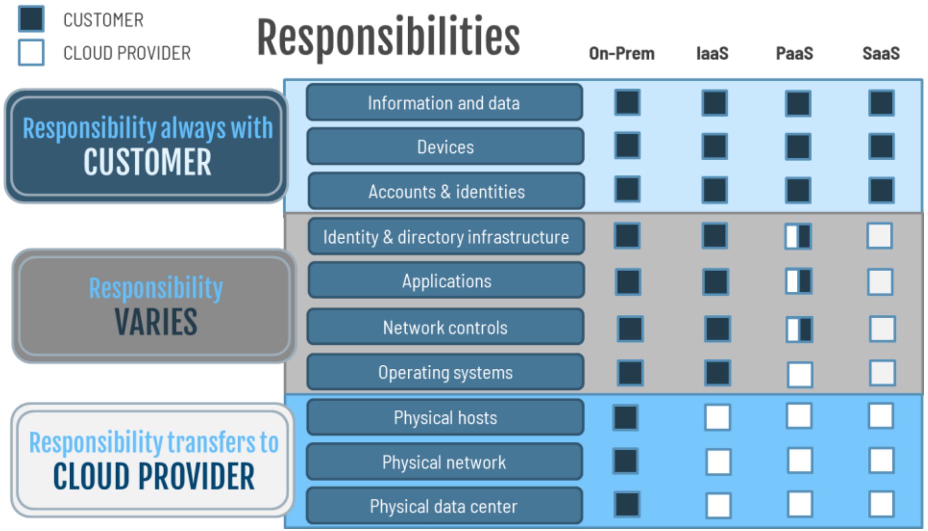
**Hybrid Cloud:** Combination of both, can come from public & private

✓ **IaaS:** Most control, VMs, Storage, Networking like VNets

**PaaS:** Mostly managed, less administrational effort, Databases, App Service

**SaaS:** Use only the end product, no installation, only configuring, email provider, Office 365 etc.

# Summary



■ CUSTOMER
□ CLOUD PROVIDER

## Responsibilities

| | Responsibilities | On-Prem | IaaS | PaaS | SaaS |
|---|---|---|---|---|---|
| Responsibility always with CUSTOMER | Information and data | ■ | ■ | ■ | ■ |
| | Devices | ■ | ■ | ■ | ■ |
| | Accounts & identities | ■ | ■ | ■ | ■ |
| Responsibility VARIES | Identity & directory infrastructure | ■ | ■ | ◨ | □ |
| | Applications | ■ | ■ | ◨ | □ |
| | Network controls | ■ | ■ | ◨ | □ |
| | Operating systems | ■ | ■ | □ | □ |
| Responsibility transfers to CLOUD PROVIDER | Physical hosts | ■ | □ | □ | □ |
| | Physical network | ■ | □ | □ | □ |
| | Physical data center | ■ | □ | □ | □ |

✓ **Consumption-based model:** No upfront cost, pay only for what you use

# Architectural components

# Summary

**Geography**

Area in the world, at least one region, define own market, data residency and compliance boundaries preserved

**Region pairs**

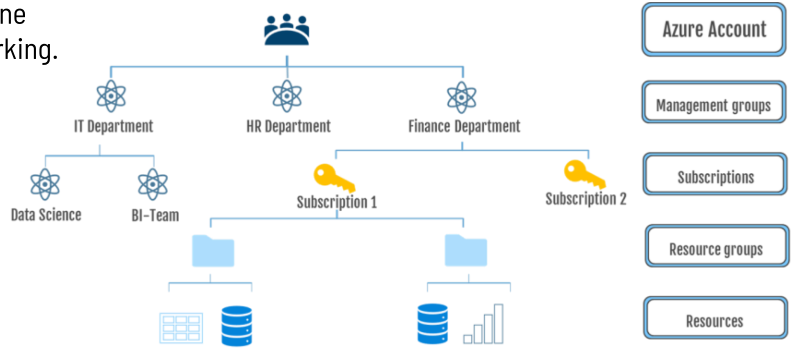
Two regions from the same geography

**Region**

Multiple data centers are connected within a radius via a dedicated regional network with low latency/latency.

**Availability Zone**

Physical locations within a region consisting of at least one data center with independent power, cooling, and networking.



# Summary

## Resources

e.g. databases, virtual machines, blob storage etc.

Can be moved to other subscriptions

## Resource groups

Management of resources

## Subscriptions

Account can have multiple subscriptions

This is where billing takes place

Cannot be merged

## Management groups

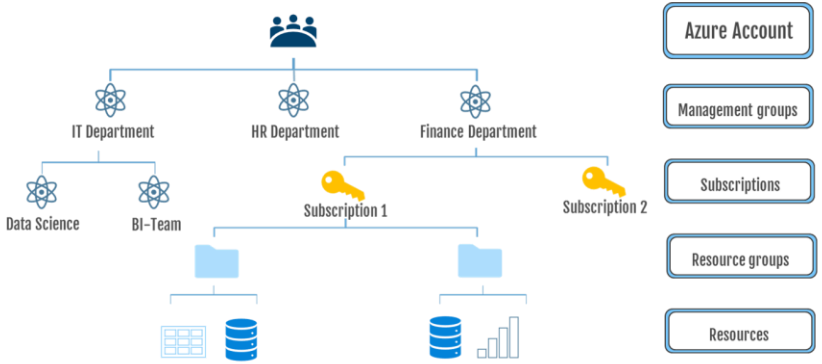
Management of subscriptions & policies

Can be nested

Environment: Test, Dev, Prod

Organizational structure

Billing purposes



# Compute Service

# Summary

## Virtual Machines

Virtualization of physical server/computer

Infrastructure-as-a-service

All software + OS is fully customizable

Fully responsible to maintain all software

## DevTest Labs

Enables users to easily create pre-defined VMs for development and testing

## VM Scale Sets

Set of auto-scaling, load balanced, identical VMs

## Availability Sets

Group VMs inside a single data center
into Fault & Update Domains

Protection against failure within data center (rack wide failure)

## Azure Virtual Desktop

Desktop and app virtualization – accessible through a browser

Virtualization of different operating systems are possible

Operating system, apps and data are separated from your local hardware

Allows multiple concurrent user-sessions

# Summary

## App Service

Platform-as-a-service

Deploy and host web applications

Managed security & autoscaling

## Azure Kubernetes Services

Orchestration service to deploy, manage, and scale containers at scale

## Azure Container Instances

Platform-as-a-service

Containers package software for deployment

Fast and simple way to upload & run containers

No need to manage a virtual machine

# Serverless

# Serverless

Serverless

- ✓ Server is invisible to the users
- ✓ They completely focus on the code
- ✓ No worry about scaling
- ✓ Focus on event-driven code
- ✓ Events or triggers
- ✓ Microbilling

# Azure Functions

**Serverless compute**: Azure manages server infrastructure and allocates resources

Scaling is automated

**Azure Functions:**
Executes code when triggered (platform, infrastructure irrelevant)

Simple functions in response to an event or a trigger

e.g. *HTTP request*

Pay only for time spent running the code

Can be stateful or stateless

# Use cases

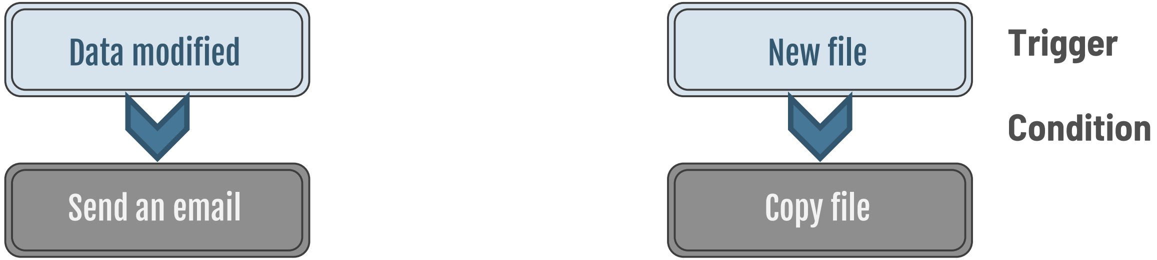
- ✓ Run code when a file is uploaded or changed
- ✓ Run scheduled small tasks

*Build event-driven systems*

*Many programming languages available*

# Azure Logic App

Used to schedule, automate and orchestrate tasks, business process and workflows.



Design a business **workflow** in a graphical way.

Send an email as a response to a trigger.

# Use cases

- ✓ Run code when a file is uploaded or changed
- ✓ Run scheduled small tasks

*Build event-driven systems*

*Many programming languages available*

# Networking

# Summary

## Virtual Networks

Emulates a physical network

Traffic is isolated and segmented

Secure communication of resources

Cloud resources + local resources

## Virtual Subnet

Further segmentation

Public subnet CAN be reached from the public internet

Private subnet CANNOT be reached from the public internet

Public subnet CAN access Privat Subnet

## VPN Gateway

Connects an Azure virtual network with an on-premise device or network (Site-to-Site)

Use an encrypted tunnel to connect two or more networks over an untrusted network (public internet)

Cost-effective solution

## ExpressRoute

Extends on-premises networks into the Microsoft cloud.

Over a private connection with the help of a connectivity provider.

More bandwidth, more secure, and more reliable

# Summary

## Private Endpoint

Uses private IP address from your virtual network
to bring PaaS services into your virtual network

Delivered via Azure Private Link

Private connection to Azure PaaS services

## Azure DNS

Provides domain name resolution
by using Microsoft infrastructure

## Content delivery network (CND)

Global network of servers that efficiently
delivers web content to users

# Storage services

# Summary

## Storage Account

Cloud solution for storing data

Account that offeres different storage services

## Redundancy options

| | |
|---|---|
| Locally redundant storage (LRS) | Zone-redundant storage (ZRS) |
| Geo-redundant storage (GRS) | Geo-zone-redundant storage (GZRS) |

## Access Tier

| | | |
|---|---|---|
| Hot | Cool | Archive |

## Blob Storage

Solution to store massive amounts of unstructured data

Any type of data: Images, documents, backups, videos

## Queue Storage

Storing large numbers of messages

## Azure Files

Managed file shares in the cloud

Can be mounted by cloud or on-premise

Replace or supplement on-premises file servers

## Azure Sync

Sync data from on-premises to Azure Files

## Azure Tables

Inexpensive NoSQL database service

Basic structured data

# Summary

## Disk storage

Storage for virtual machines
Still pay for storage
Containers (Blob Storage) used

## AzCopy

Command-line tool to copy data to and from storage accounts

## Storage Explorer

Convenient tool to manage storage resources from Desktop

## Azure Migrate

Centralized platform that with tools for planning migrations

## Data Box

Device to transfer TBs of data in and out of Azure

## Azure Marketplace

Trusted third-party companies offer additional applications

# Identity, access, and security

# Summary

## Authentication

Proving that you are who you say

## Authorization

Granting permission to an authenticated party to do something

## Multi-factor Authentication

Additional method of authentication

Biometrics or trusted device

## Azure AD

Manged service for identity and access management (Azure & O365)

Azure AD Connect: Sync on-premise Active directory & Azure AD

Free plan and premium plans (99.9% availability)

Authentication & Authorization

Distinct from other resources & services

Invite exernal users (guest users)

## Single sign-on

One set of credentionals to sign in to multiple systems

## Passwordless

Secure + convenient

Windows Hello for Business

Microsoft authenticator app

FIDO2 Security Key

# Summary

## Conditional access

Including intelligent signals in access control decisions

E.g. Administrator needs to use MFA

## Role-based access control (RBAC)

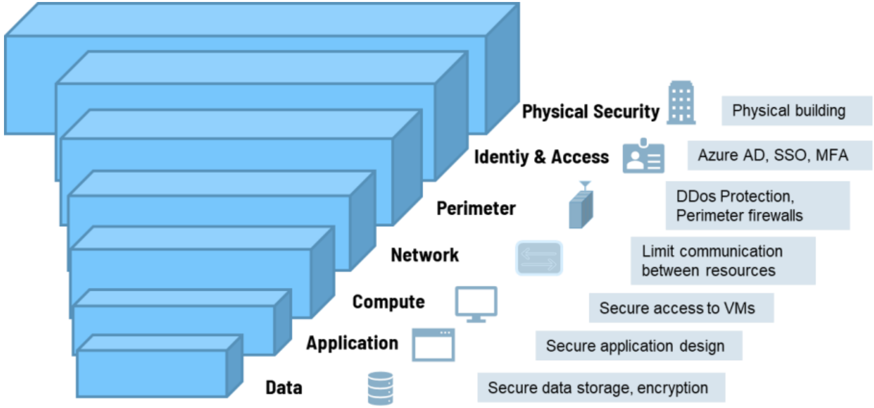
**Authorization**: Configure access for users and groups to resources

Allow one user to manage all SQL databases in a resource group

## Zero Trust

**Security principals**: Assume breach, never trust, always verify!

## Defense in depth


Physical Security
Physical building
Identiy & Access
Azure AD, SSO, MFA
Perimeter
DDos Protection, Perimeter firewalls
Network
Limit communication between resources
Compute
Secure access to VMs
Application
Secure application design
Data
Secure data storage, encryption

## Microsoft Defender for cloud

Security tools for cloud (Azure + multicloud) and on-premises

Security score, security recommendations and alerts

# Cost management

# Summary

## Cost factors

Subscription type, resource type, configuration, usage metrics, region, reserved capacity, license discounts, bandwidth

bandwidth: inbound & within region free
outbound & inter-region not free

## Cost saving options

Reserved instances

Hybrid benefit (license from on-premises)

Spot pricing

Delete unused resources, deallocate (stop) VMs

Migrate from IaaS to PaaS

## Pricing calculator

Cost estimation tool to estimate cost for resources

## TOC calculator

Calculates the total cost of ownership & cost savings when migrating to the Azure cloud

## Tags

Labels to categorize resources

Important for cost and billing

Will not be inherited

Can be enforced by Policies

# Compliance and governance

# Summary

## Policies

Enforce standards that can be applied to
Management groups, subscriptions or resource groups

Important to comply with regulations and standards

Initiative: Group of policies

## Locks

Prevent accidental deletion or modification

Delete or Read-only

Multiple locks can be applied

Will be inherited

## Blueprints

Define a package of artifacts that can be reused at large scale

Quickly build new environments with consistency
and set standards

Applied to subscription level

## Service Trust Portal

Website that contains documentation and certifications about
how Microsoft complies with the relevant regulations

Privacy statement: How Microsoft collects and uses personal data

# Managing resources

# Summary

## Azure Portal

Web-based graphical interface

Very easy to learn and navigate

Every device with a browsers

Mobile App: Convenient but limited functionality

## Azure CLI + PowerShell

Cross-platform command-line tools

Azure CLI scripting similar to Bash (az command)

Bulk deployment and repeatable tasks

## Azure Cloud Shell

Accessible through Azure Portal

Access PowerShell and Azure CLI conveniently

## Azure Arc

Managing hybrid and multi-cloud

Centralized platform for consistent management, governance and security

## Azure Resource Manager

Management layer to create, update, and deploy resources

ARM templates: Re-deployment, bulk-deployment, and define dependencies

# Monitoring tools

# Summary

## Azure Advisor

Personalized and actionable recommendations

Free guide to best practises

## Azure Monitor

Monitor performance, availability and usage of services and applications

Activity log, alerts, and application insights

## Azure Service Health

Azure Status: Global view

Service Health: Personalized view on health of used services

Resource Health: Health of your resources