DevOps and Cloud Technologies

29.10.2025

BOSCH

About Me

Vladimir Nikolov

- Lead DevOps Engineer @Bosch ECS
- 15+ years of experience as Network Engineer, System Integrator, Deployment Engineer, DevOps and DevOps Lead
- Hobbies: Football, Swimming, Motorcycles...

BOSCH

Agenda

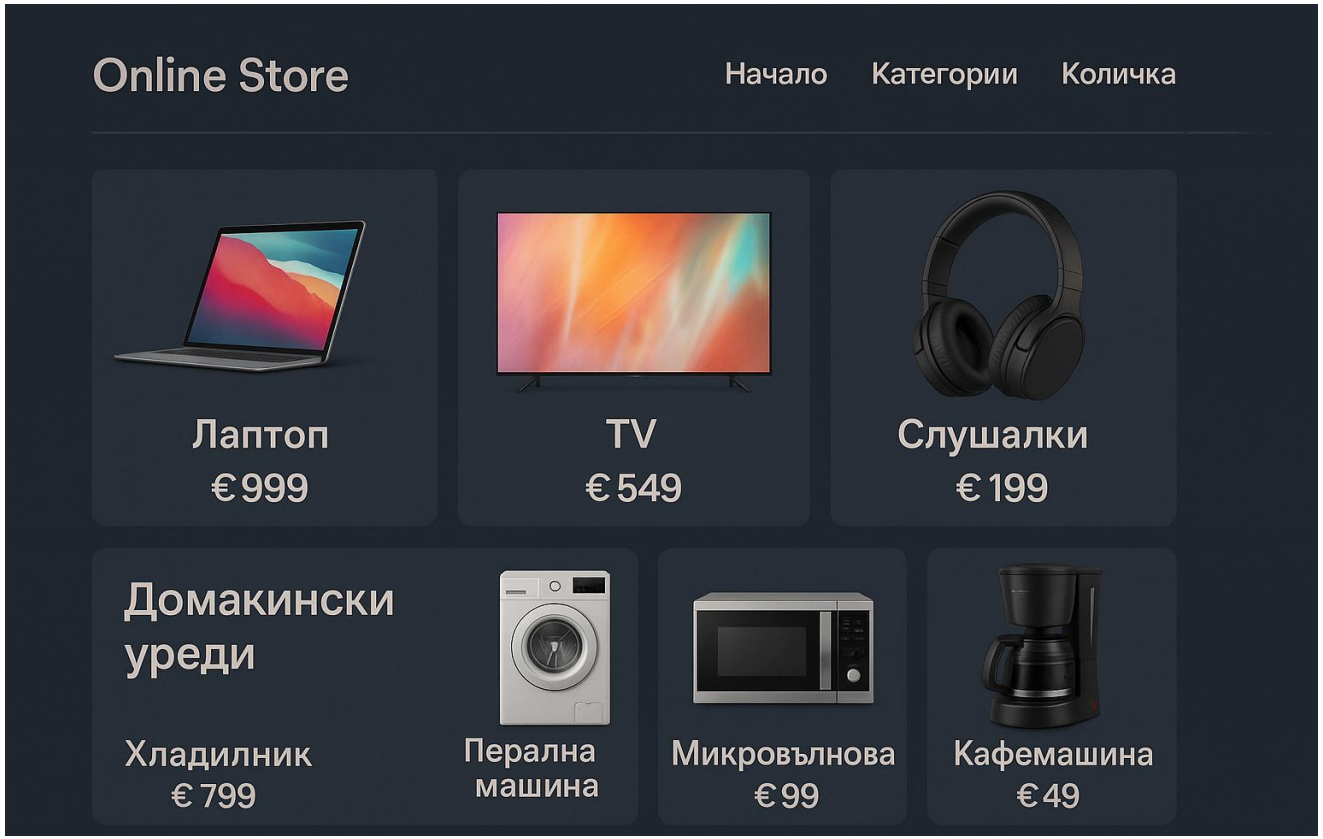
- Introduction To Cloud
- Introduction To Azure
- Azure Basic Concepts
- Azure Networks
- Azure AD
- Demo

BOSCH

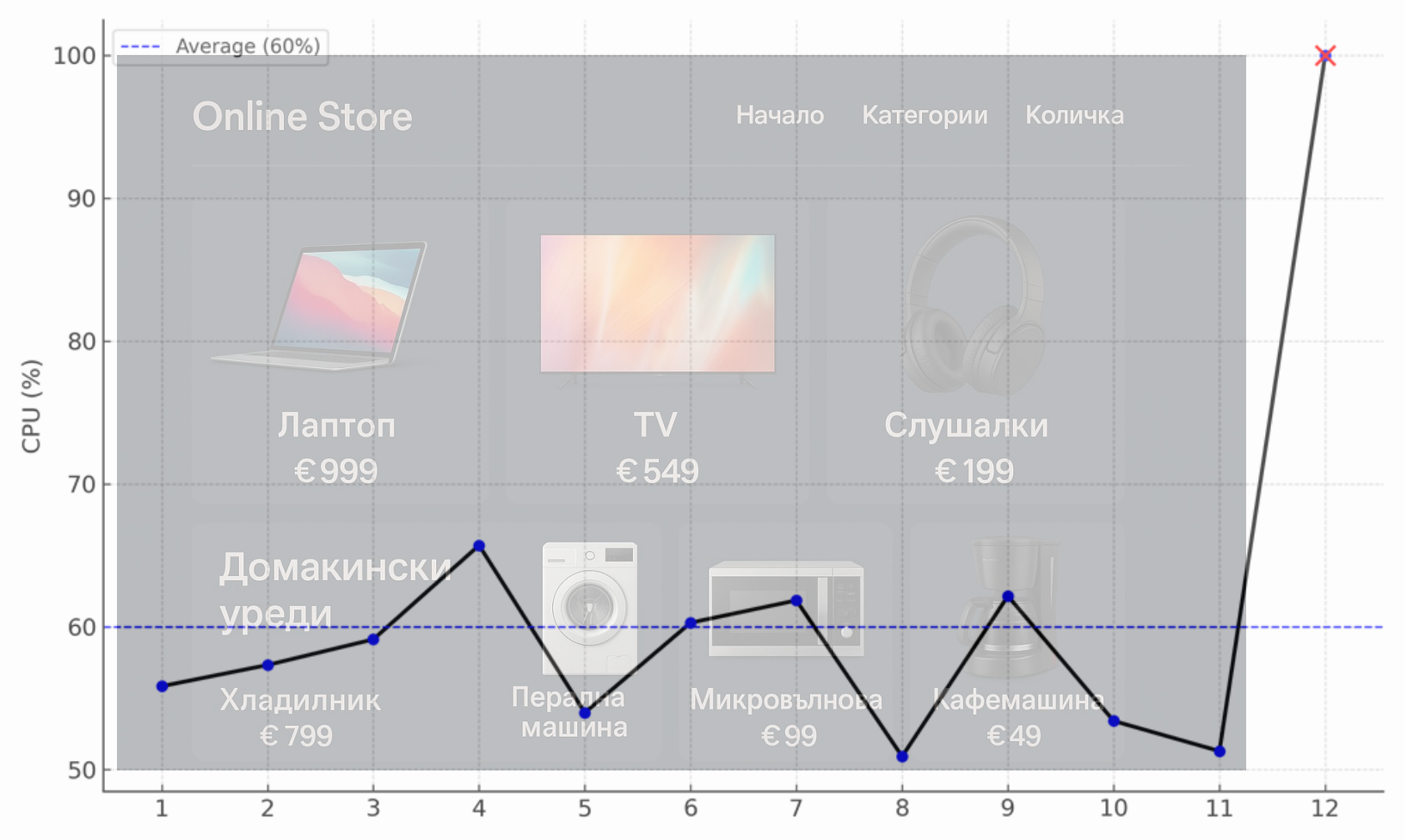
Introduction To Cloud

BOSCH

What If There's No Cloud?

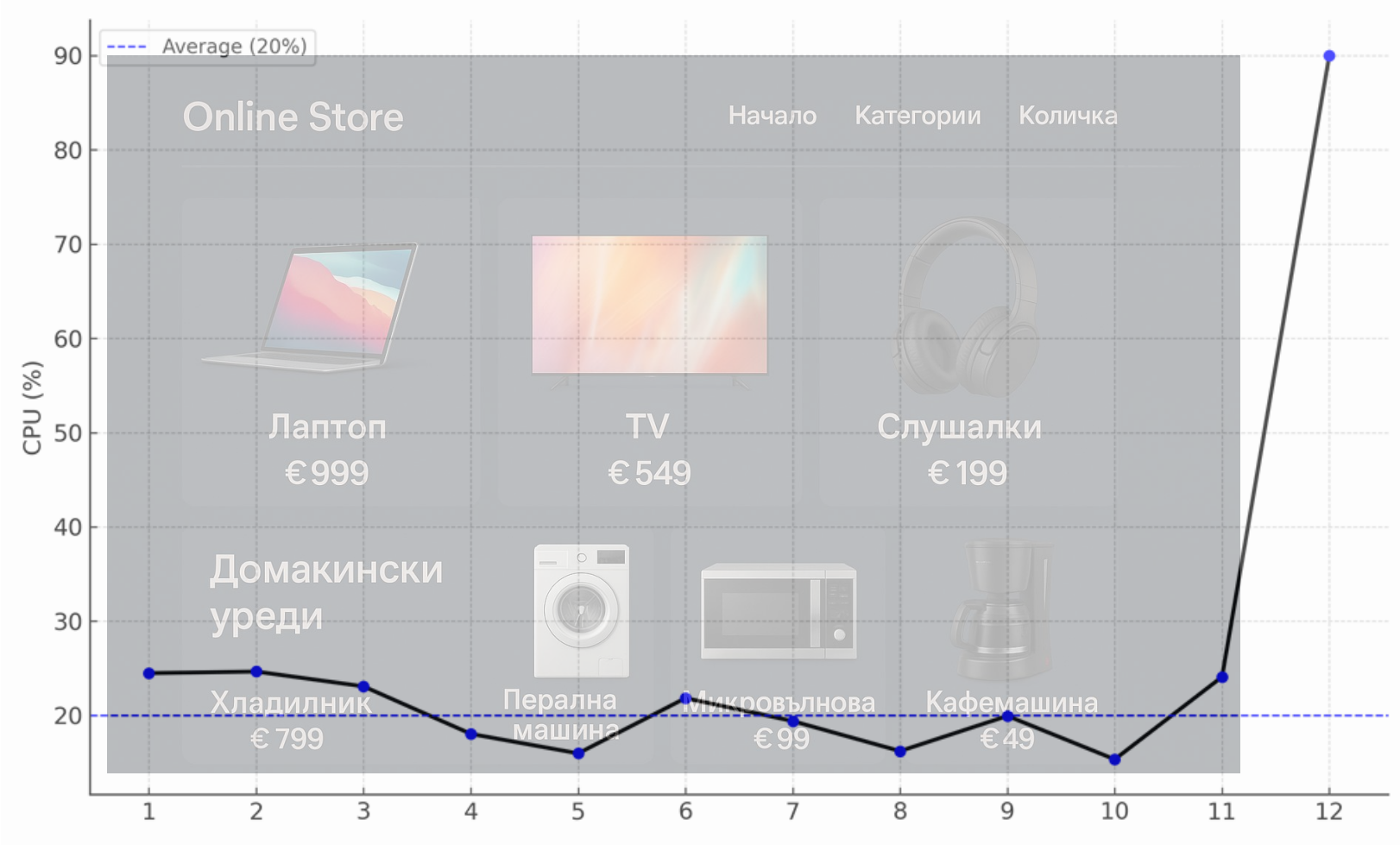


What If There's No Cloud?



BOSCH

What If There's No Cloud?



BOSCH

What is Cloud?

The NIST Definition of Cloud Computing:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

BOSCH

What is Cloud?

The NIST Definition of Cloud Computing:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Or

Cloud is compute, network, storage, apps and similar services managed by SOMEBODY ELSE

* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Essential Cloud Characteristics

1. On-Demand Self-Service:
A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

2. Broad network access:
Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g.,mobile phones, tablets, laptops, and workstations).

3. Resource Pooling:
The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

4. Rapid Elasticity:
Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

5. Measured Service:
Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Essential Cloud Characteristics

On-Demand Self-Service:

- Self service provisioning of resources, with no human or 3rd party company interaction
- Easy provisioning of resources
- It can be done any time – 24/7, 365 days in the year
- Just us and our credit card!

* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Essential Cloud Characteristics

Broad Network Access:

- Resources can be accessed and managed from everywhere
- No physical access is needed… even it's not allowed
- High speed connection available

Essential Cloud Characteristics

Resource Pooling:

- The provider’s compute resources are shared between customers in a multi-tenant model
- Cloud provider decides which physical resource to allocate for consumer’s virtual resources
- Examples of resources include storage, CPU, memory, and network bandwidth

Essential Cloud Characteristics

Rapid Elasticity :

- Resources can easily scale up and down, automatically based on demand
- Great for handling (unexpected) peaks in processing

Essential Cloud Characteristics

Measured Service:

- Consumer pays for resources he actually used
- Relatively granular approach in service measurement
  - Server uptime
  - DB Storage
  - Function calls
  - Message Broker – consumer pays for the instance and traffic
  - Kubernetes cluster – control plane and worker nodes

Cloud Service Models

Infrastructure-as-a-Service (IaaS):

- Cloud provides underlaying infrastructure (hardware), like machines, networking, storage
- Consumer responsible for installing virtual machines, OS, software, patches, maintenance

Cloud Service Models

Platform-as-a-Service (PaaS):

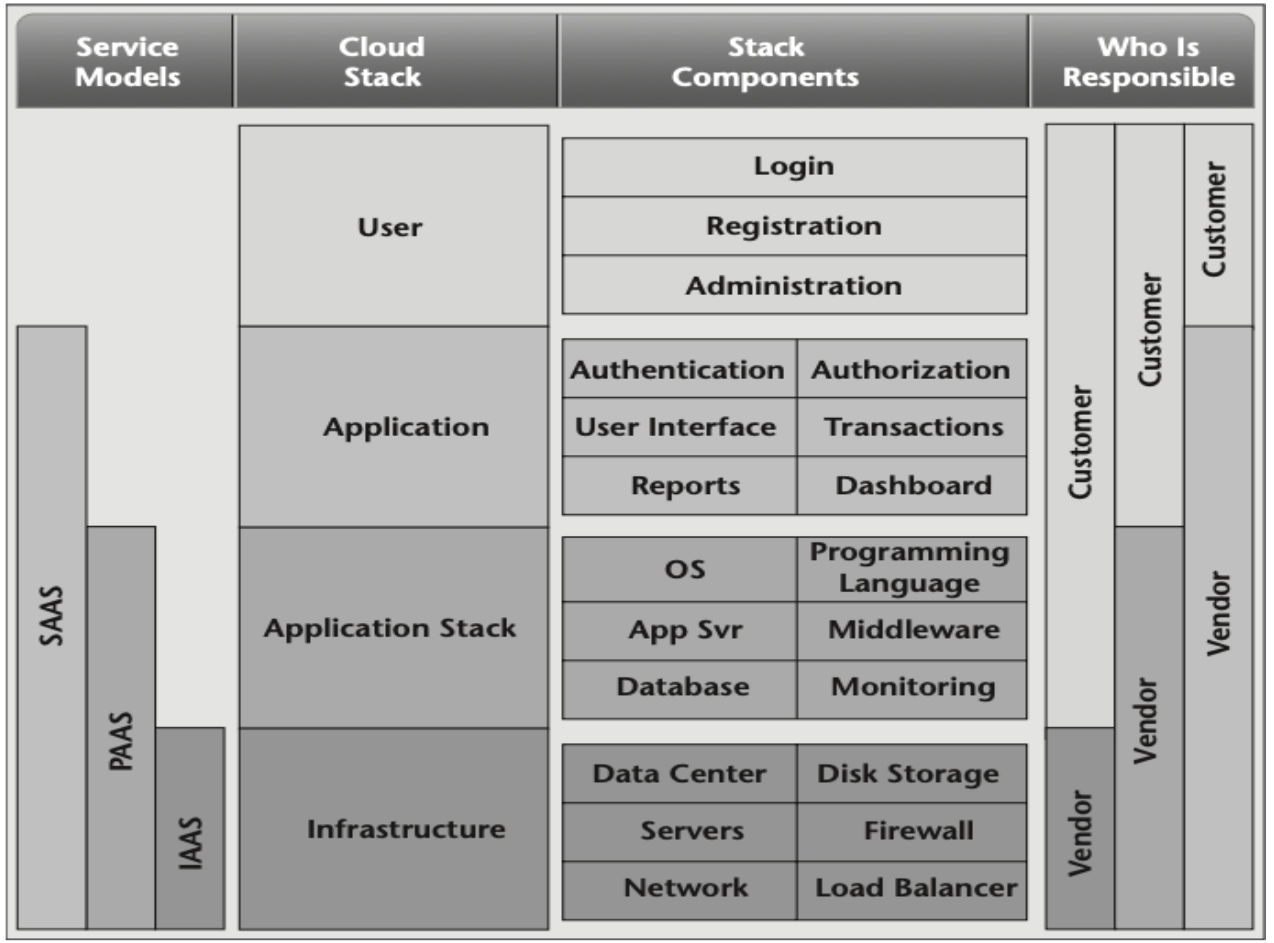
- What IaaS is to infrastructure, PaaS is to the applications
- On top of IAAS, Cloud provides also middleware, OS, security updates, database, runtime
- Consumer responsible for installing the application on top of them and runs it

Cloud Service Models

Software-as-a-Service (SaaS):

- Software provided completely from the cloud provider
- Cloud provider is responsible for everything – infrastructure, middleware, support, updates, redundancy, etc.
- The consumer is just an user
- Example – Office365

Cloud Service Models



* from “Architecting The Cloud” by Michael J. Kavis

BOSCH

Types of Cloud

Private cloud:
The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Examples:
- OpenShift
- OpenStack
- VMWARE Cloud
- Azure Stack

* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Types of Cloud

Public cloud:
The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Examples:
- AWS
- Azure
- GCP

* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Types of Cloud

Hybrid cloud:
The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Introduction To Azure

BOSCH

What the Clouds Are Made Of

BOSCH

Regions

- A geographical area that contains one or multiple datacenters, networked together with a low-latency network

Regions

- A geographical area that contains one or multiple datacenters, networked together with a low-latency network
- Upon creation, most of Azure services (resources) must be located in a region

BOSCH

Regions

- A geographical area that contains one or multiple datacenters, networked together with a low-latency network
- Upon creation, most of Azure services (resources) must be located in a region
- Some services or features are available in certain regions only, such as specific VM sizes or storage types

Regions

- A geographical area that contains one or multiple datacenters, networked together with a low-latency network
- Upon creation, most of Azure services (resources) must be located in a region
- Some services or features are available in certain regions only, such as specific VM sizes or storage types
- There could be a difference in prices depending on the region

Regions

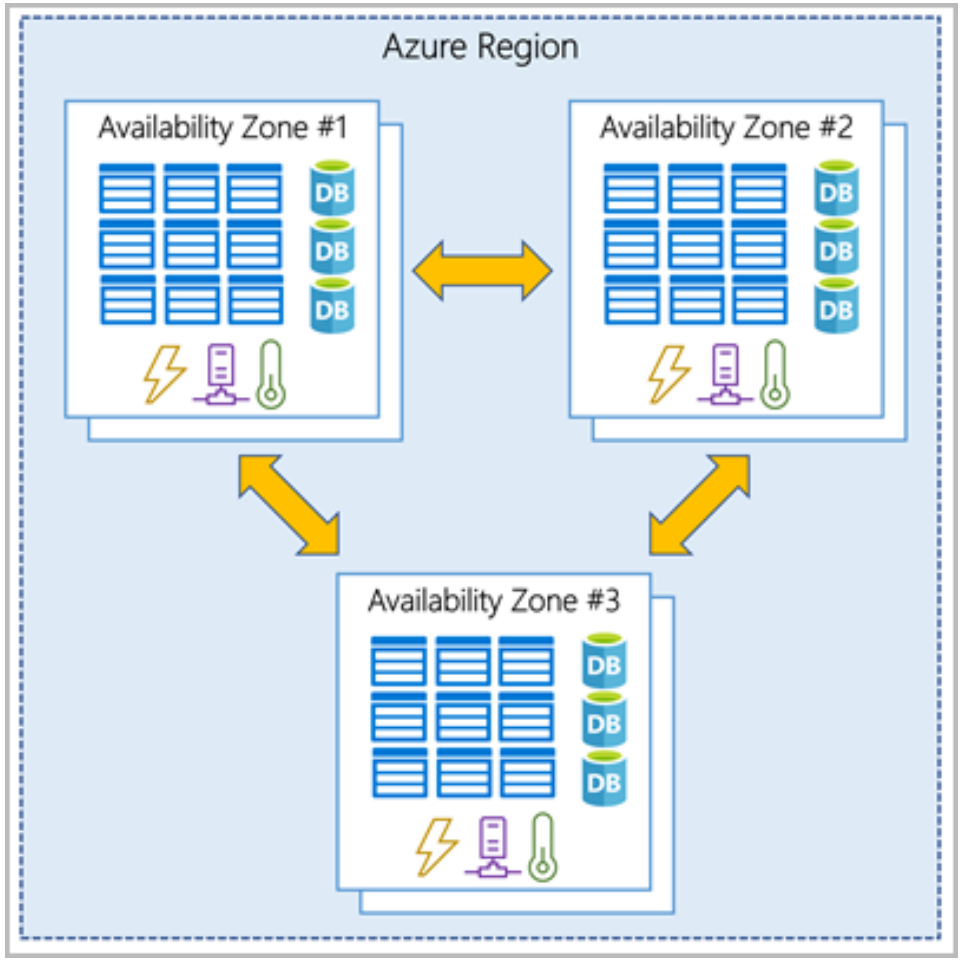
- A geographical area that contains one or multiple datacenters, networked together with a low-latency network
- Upon creation, most of Azure services (resources) must be located in a region
- Some services or features are available in certain regions only, such as specific VM sizes or storage types
- There could be a difference in prices depending on the region
- Some global Azure services do not require a region setup, such as Azure AD, Azure DNS

Regions

- A geographical area that contains one or multiple datacenters, networked together with a low-latency network
- Upon creation, most of Azure services (resources) must be located in a region
- Some services or features are available in certain regions only, such as specific VM sizes or storage types
- There could be a difference in prices depending on the region
- Some global Azure services do not require a region setup, such as Azure AD, Azure DNS
- Select Region based on:
  - Geographical proximity to systems' users
  - Service availability
  - Service Pricing
  - Availability needed
  - Compliance

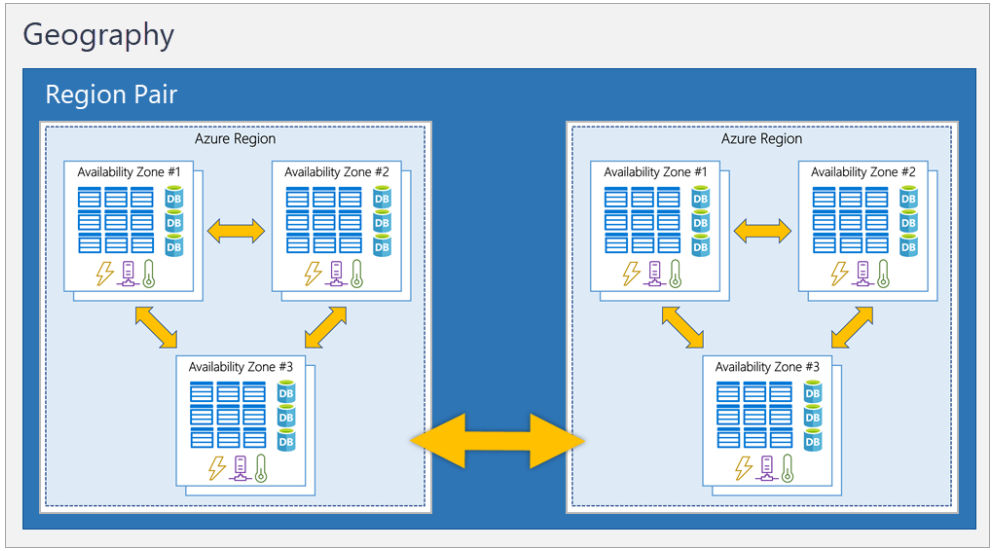
Zones

- Each Datacenter is considered a Zone
- When a region has more than one Datacenter is considered an Availability Zone
- Each Availability Zone is equipped with independent power, cooling and networking
- An Availability Zone is set up to be an isolation boundary - If one zone goes down, the other continues working
- Some cloud services benefit from Availability Zones



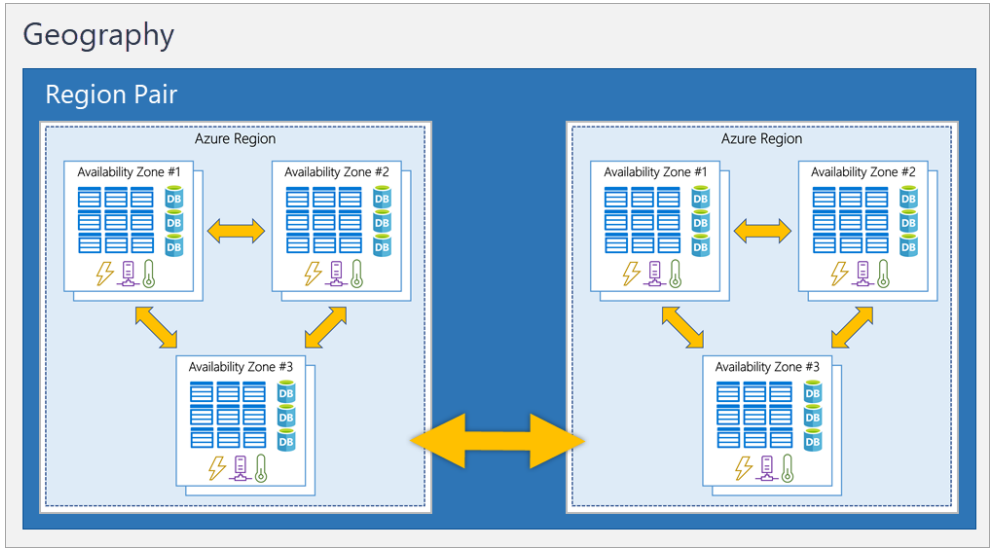
Region pairs

- If an extensive Azure outage occurs, one region out of every pair is prioritized to make sure at least one is restored as quickly as possible for applications hosted in that region pair.
- Planned Azure updates are rolled out to paired regions one region at a time to minimize downtime and risk of application outage.
- Data continues to reside within the same geography as its pair (except for Brazil South) for tax- and law-enforcement jurisdiction purposes.



Region pairs

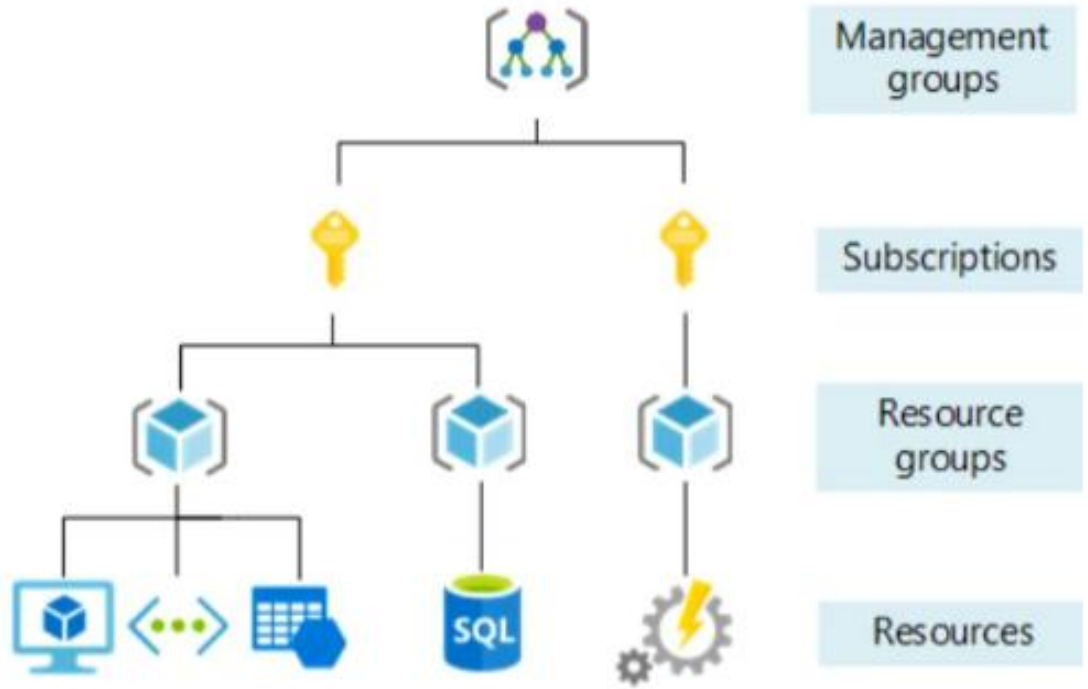
- Most Azure regions are paired with another region within the same geography (such as US, Europe, or Asia) at least 300 miles away
- This approach allows for the replication of resources across a geography that helps reduce the likelihood of interruptions because of events such as natural disasters, civil unrest, power outages, etc.
- if a region in a pair was affected by a natural disaster, services would automatically fail over to the other region in its region pair.



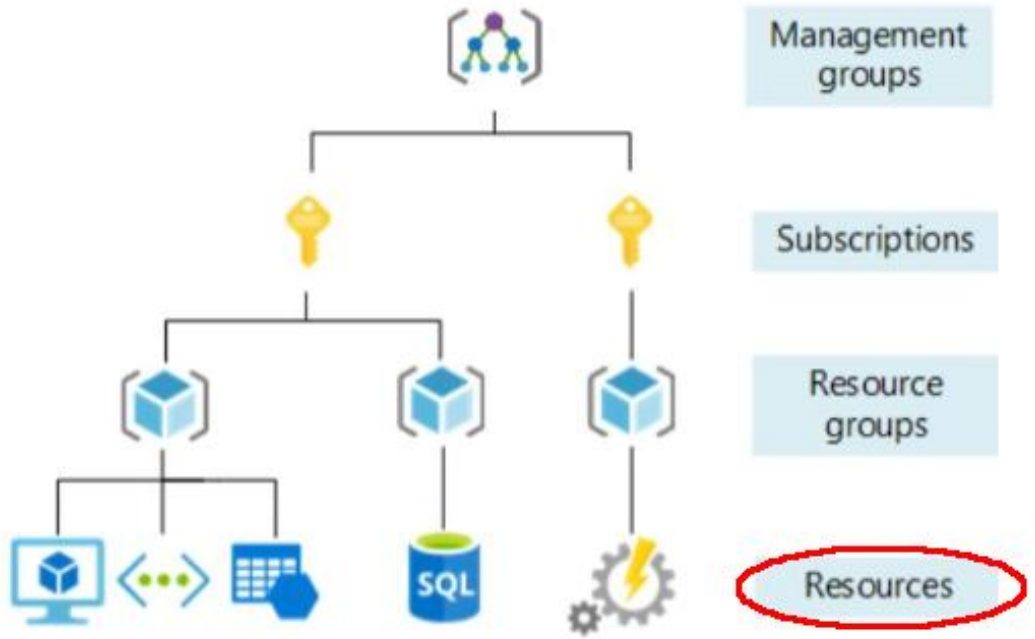
Azure Basic Concepts

BOSCH

Resource Organization

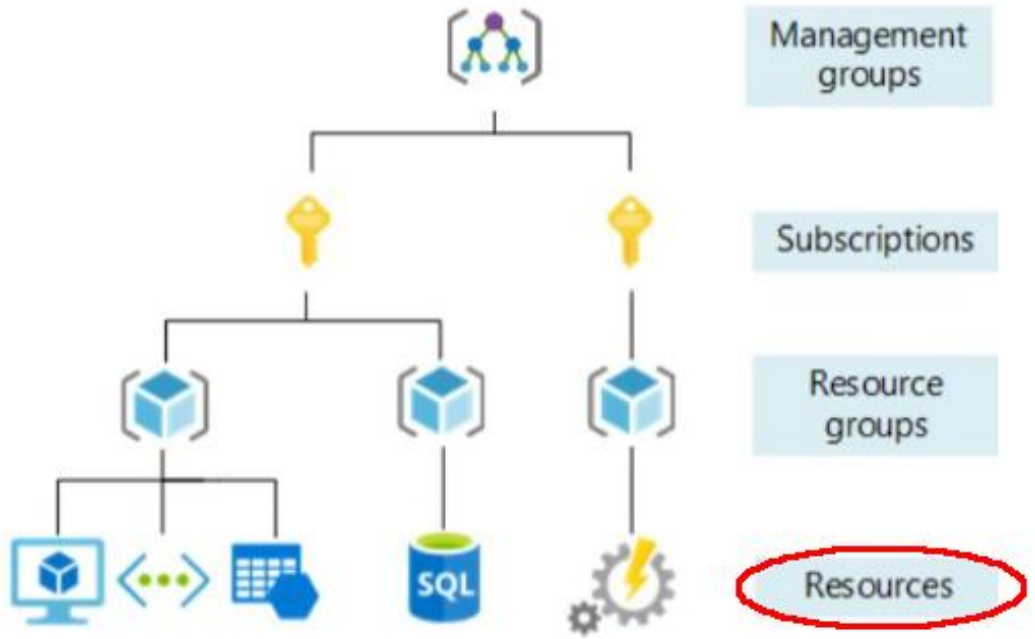


Resource Organization



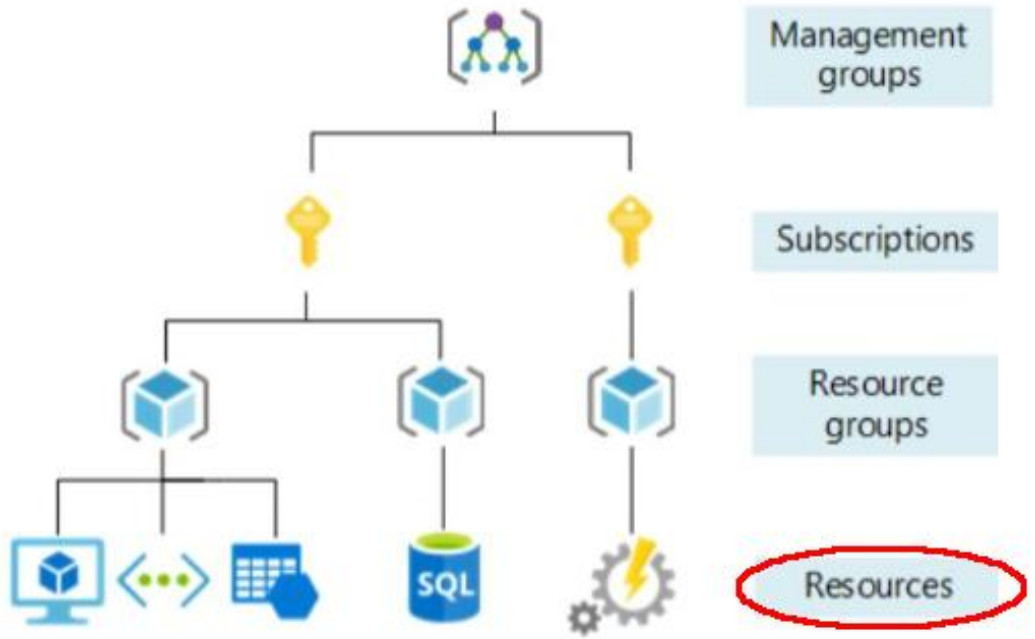
- Basic building blocks in Azure

Resource Organization



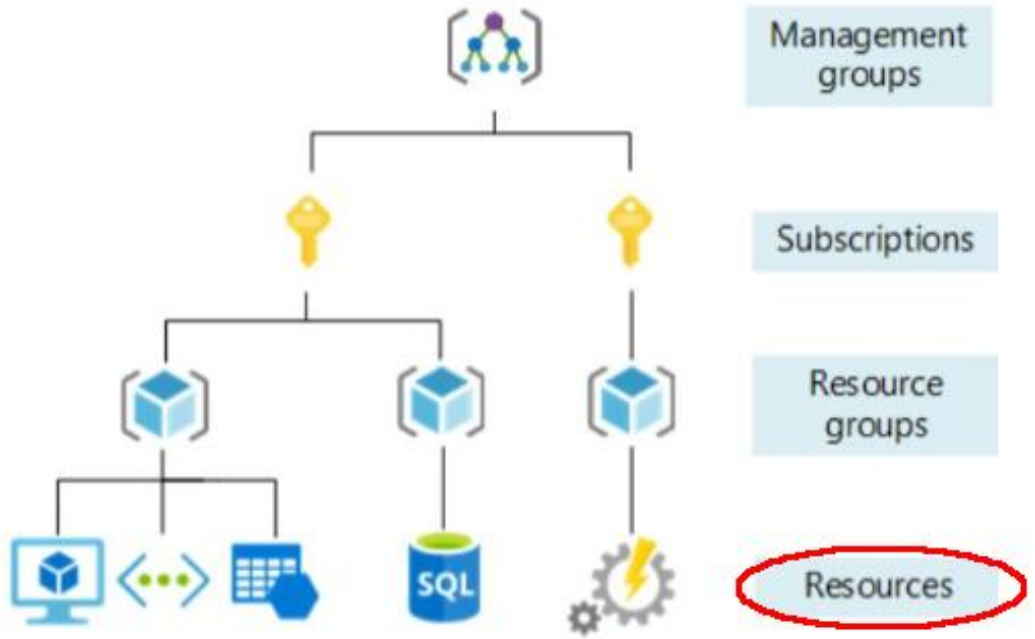
- Basic building blocks in Azure
- Everything is a resource - VMs, Virtual Networks, Databases, Kubernetes cluster, Functions, Managed IDs, etc.

Resource Organization



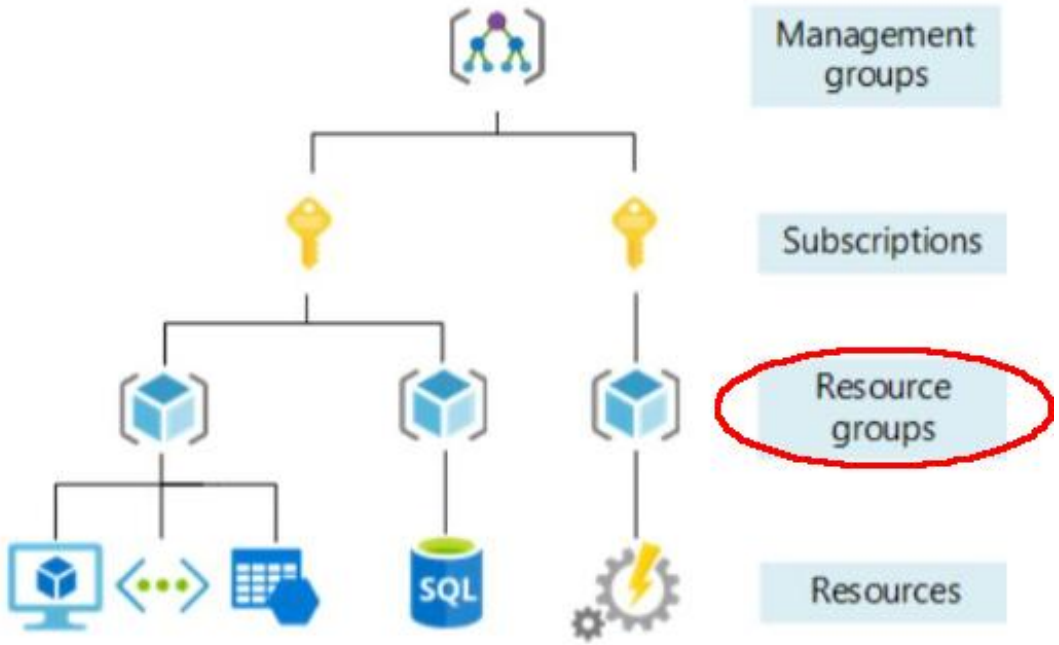
- Basic building blocks in Azure
- Everything is a resource - VMs, Virtual Networks, Databases, Kubernetes cluster, Functions, Managed IDs, etc.
- Every resource must reside into a single resource group

Resource Organization



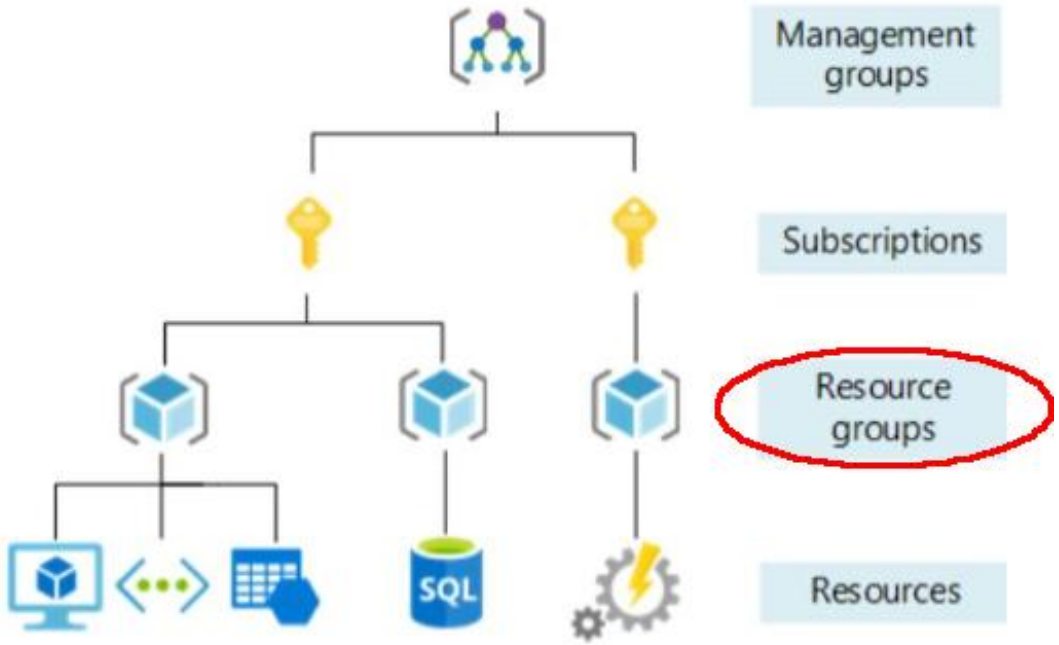
- Basic building blocks in Azure
- Everything is a resource - VMs, Virtual Networks, Databases, Kubernetes cluster, Functions, Managed IDs, etc.
- Every resource must reside into a single resource group
- Must be in the same region as the resource group they belong to

Resource Organization



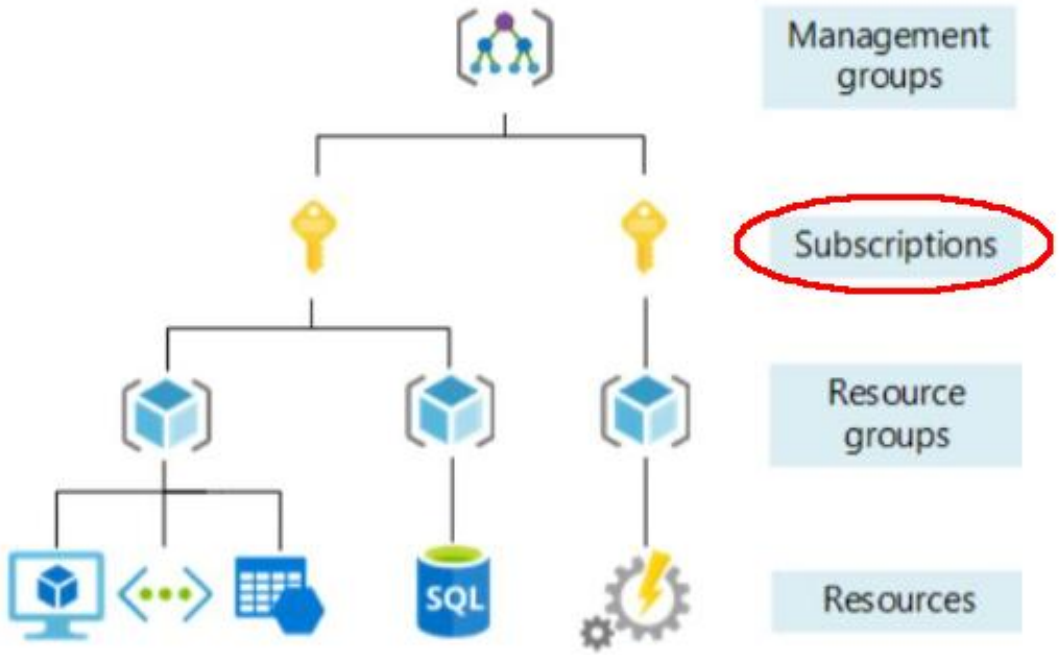
- Logical container of resources

Resource Organization



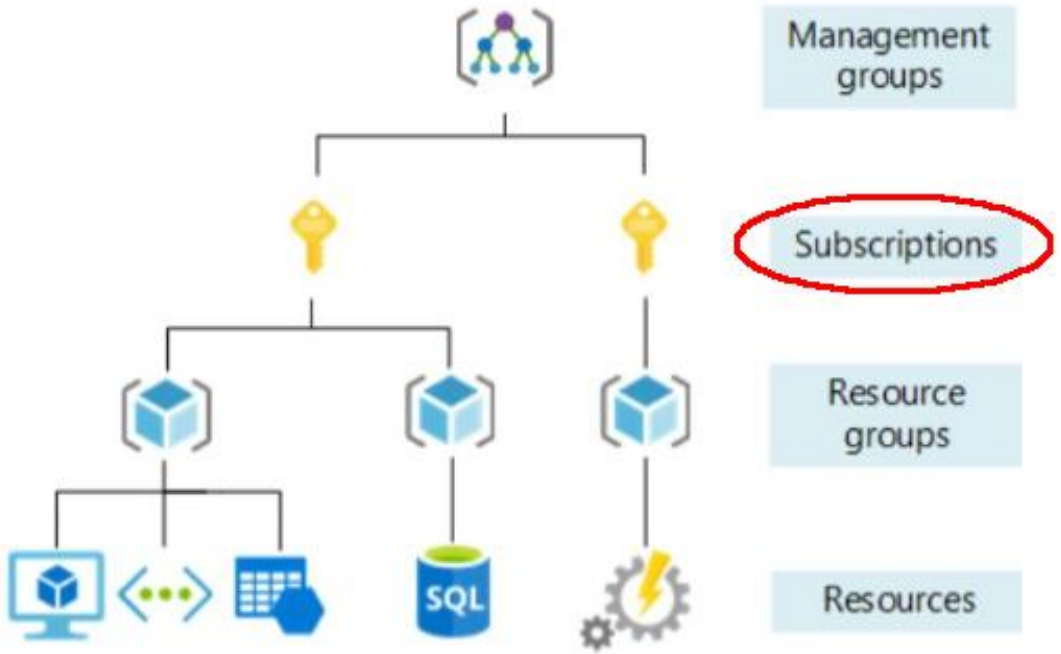
- Logical container of resources
- All resources within a resource group automatically inherit conditions applied to it

Resource Organization



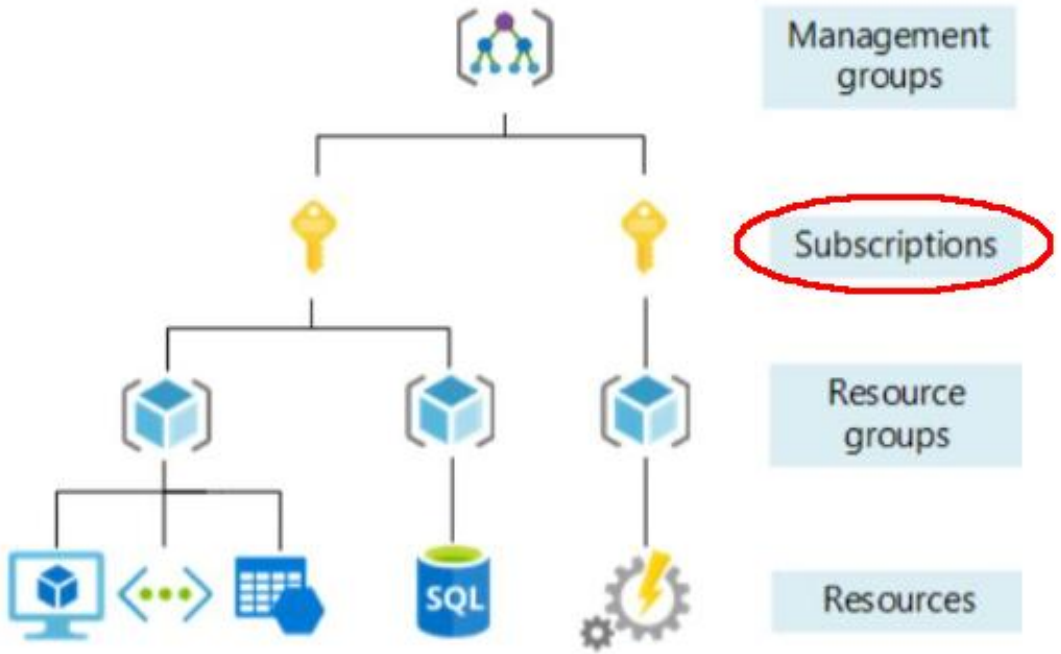
- Associated with account and cost center

Resource Organization



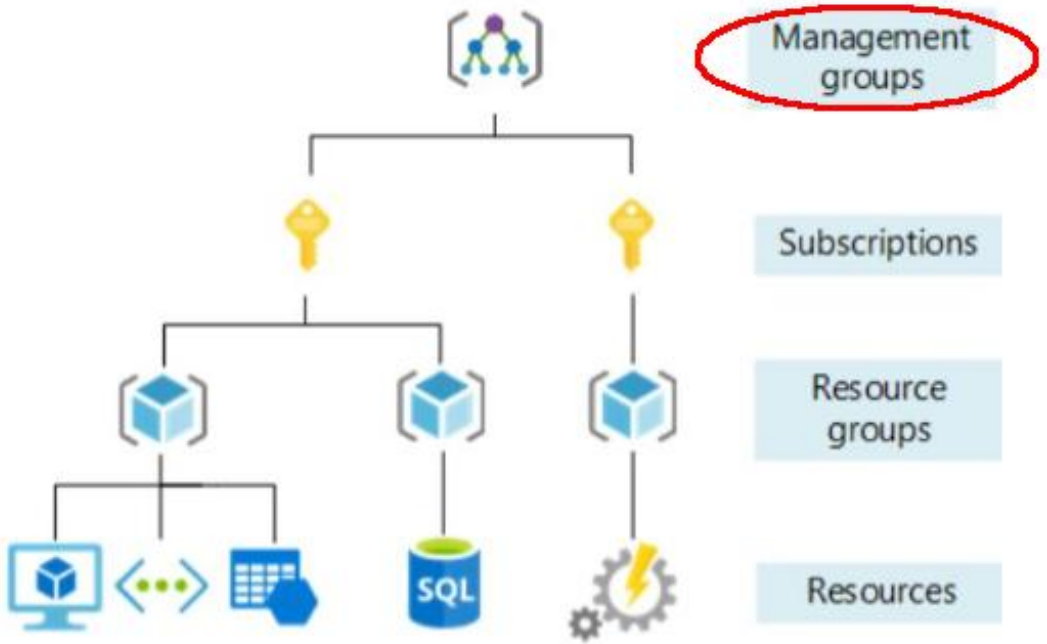
- Associated with account and cost center
- All resource groups within a subscription automatically inherit conditions applied to that subscription

Resource Organization



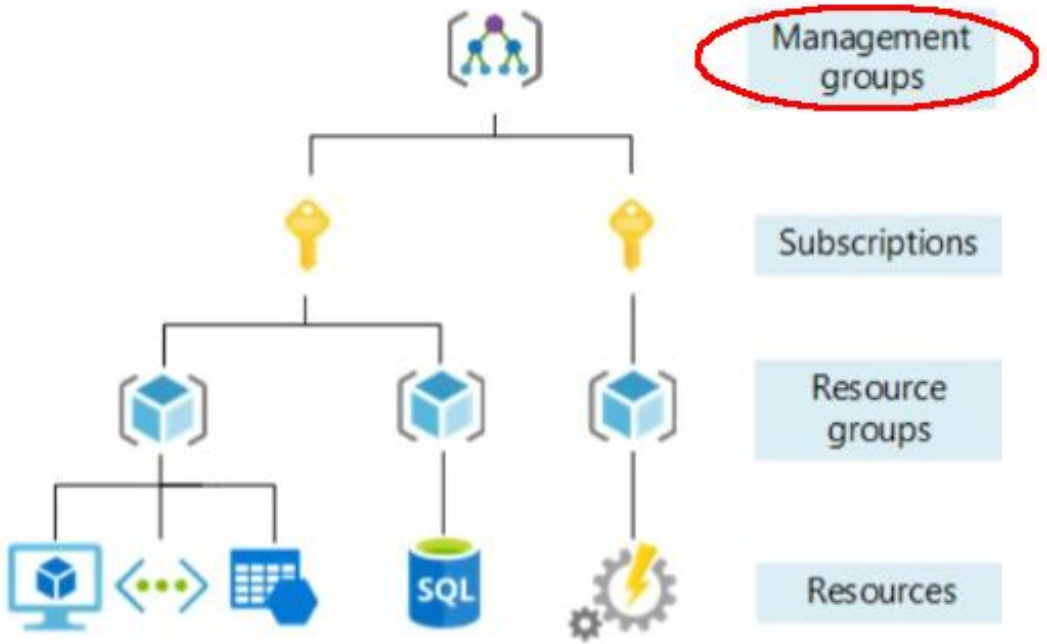
- Associated with account and cost center
- All resource groups within a subscription automatically inherit conditions applied to that subscription
- It's not an account

Resource Organization



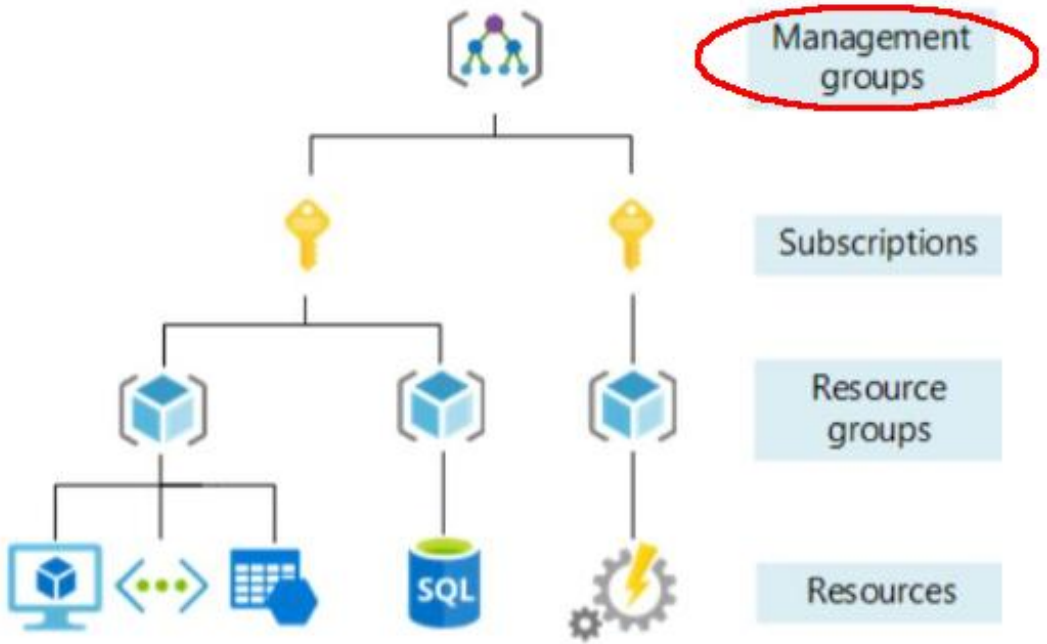
- Provides level of scope and control above subscription level

Resource Organization



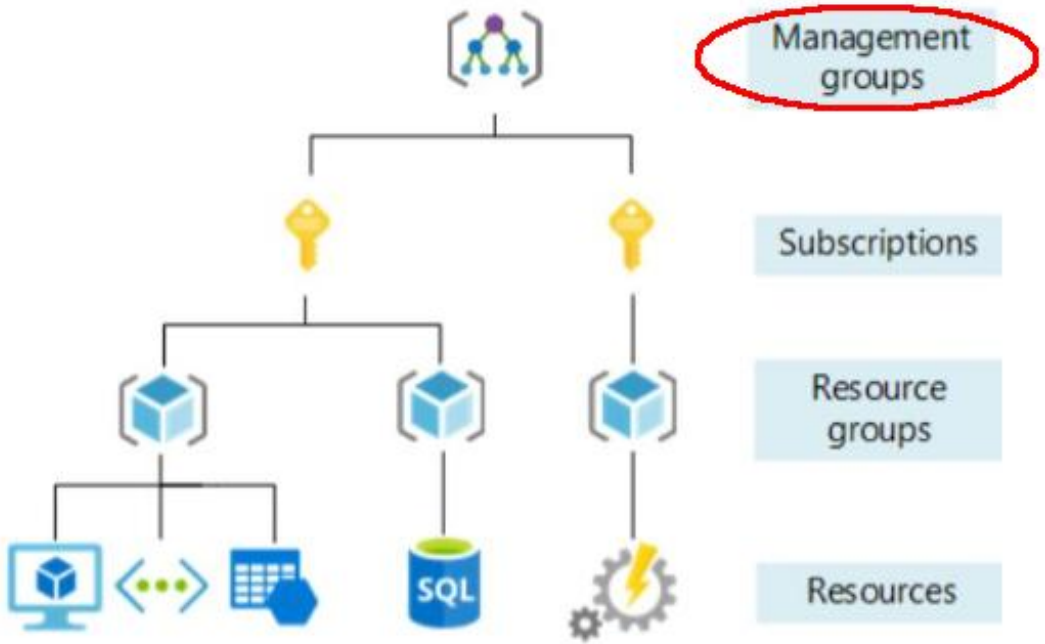
- Provides level of scope and control above subscription level
- Typically used as containers to manage access, policy and compliance for multiple subscriptions

Resource Organization



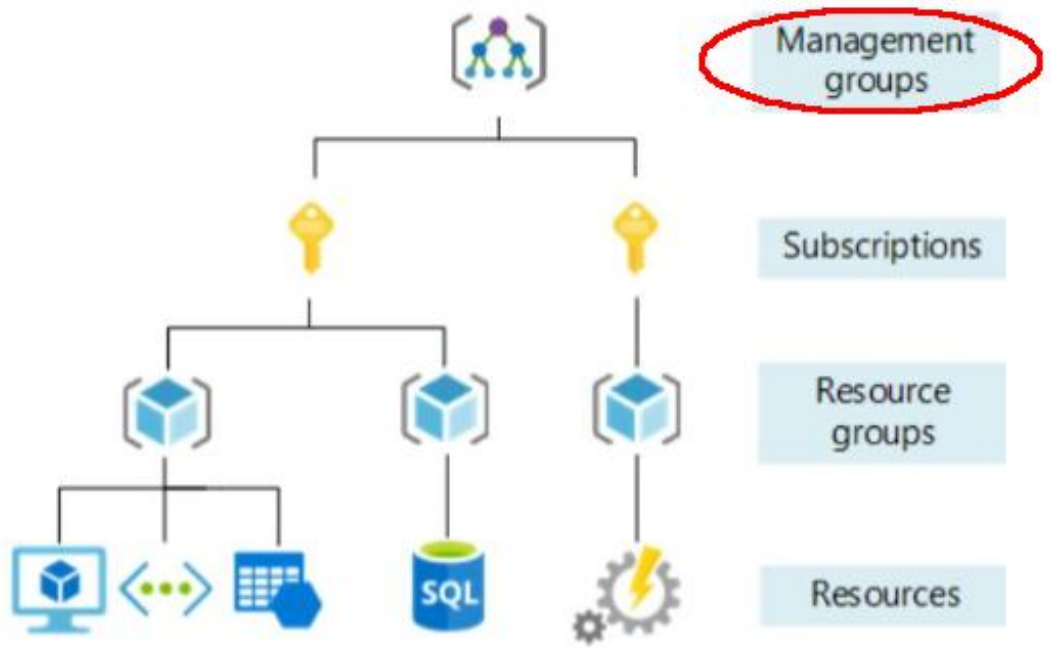
- Provides level of scope and control above subscription level
- Typically used as containers to manage access, policy and compliance for multiple subscriptions
- All new subscriptions are placed under the top-level management group (root group) by default

Resource Organization



- Provides level of scope and control above subscription level
- Typically used as containers to manage access, policy and compliance for multiple subscriptions
- All new subscriptions are placed under the top-level management group (root group) by default
- All subscriptions within a management group automatically inherit conditions applied to management group

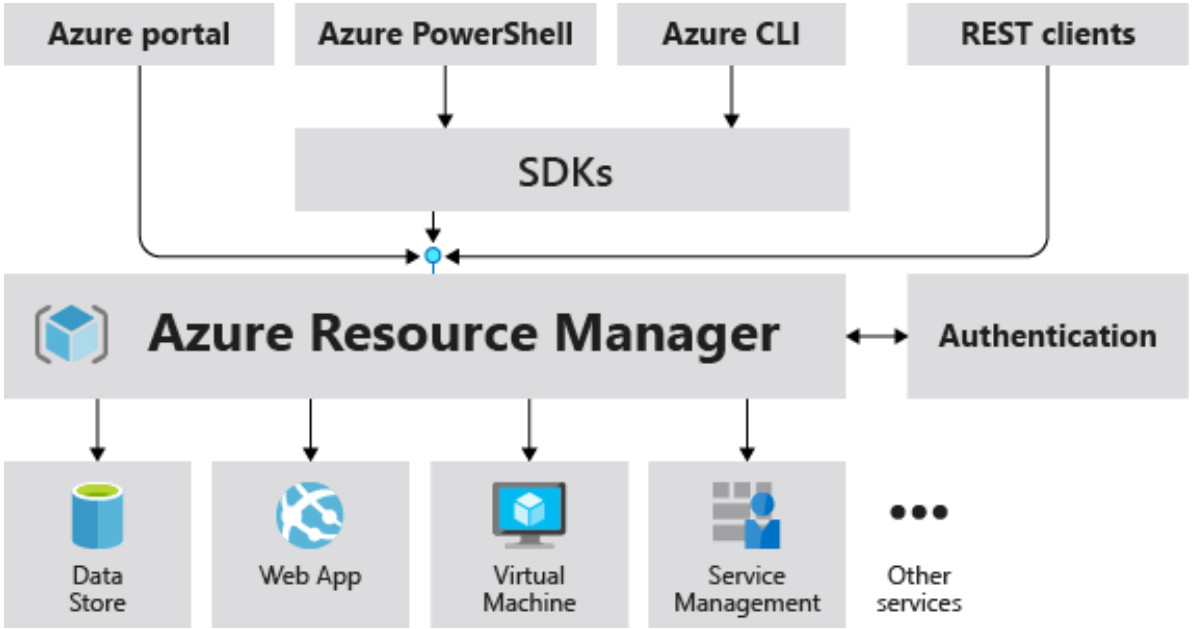
Resource Organization



- Provides level of scope and control above subscription level
- Typically used as containers to manage access, policy and compliance for multiple subscriptions
- All new subscriptions are placed under the top-level management group (root group) by default
- All subscriptions within a management group automatically inherit conditions applied to management group
- Management group tree supports up to 6 levels of depth

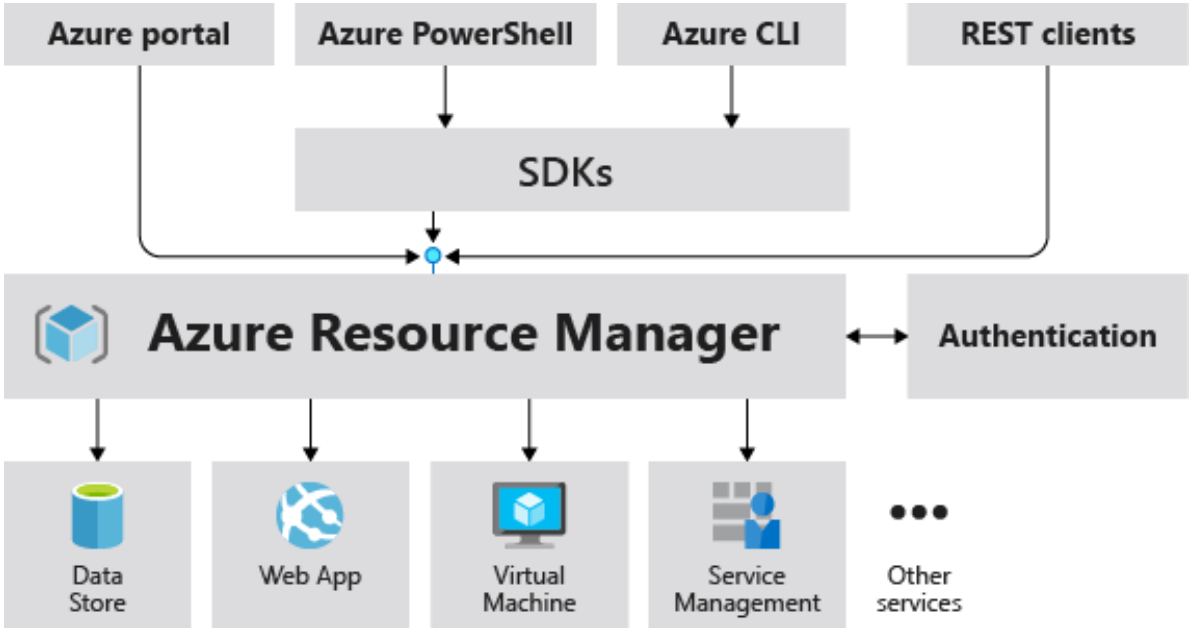
BOSCH

Azure Resource Manager



- Consumer creates, delete and manages resources through ARM

Azure Resource Manager



- Consumer creates, delete and manages resources through ARM
- Azure UI, Azure CLI, IaC tools like Terraform actually communicate to ARM

Azure Networks

BOSCH

Virtual Network

- Basically it’s a private network

Virtual Network

- Basically it’s a private network
- Based on physical network but logically separated from the other virtual networks

Virtual Network

- Basically it’s a private network
- Based on physical network but logically separated from the other virtual networks
- Free of charge

Virtual Network

- Basically it’s a private network
- Based on physical network but logically separated from the other virtual networks
- Free of charge
- Resources inside a VNet could communicate with each other by default

Virtual Network

- Basically it’s a private network
- Based on physical network but logically separated from the other virtual networks
- Free of charge
- Resources inside a VNet could communicate with each other by default
- However they can’t communicate with resources from other Vnet

Virtual Network

- Basically it’s a private network
- Based on physical network but logically separated from the other virtual networks
- Free of charge
- Resources inside a VNet could communicate with each other by default
- However they can’t communicate with resources from other Vnet
- In order to enable that we have to use peering between Vnets

Virtual Network

- Basically it’s a private network
- Based on physical network but logically separated from the other virtual networks
- Free of charge
- Resources inside a VNet could communicate with each other by default
- However they can’t communicate with resources from other Vnet
- In order to enable that we have to use peering between Vnets
- Scoped to a single region

Virtual Network

- Basically it’s a private network
- Based on physical network but logically separated from the other virtual networks
- Free of charge
- Resources inside a VNet could communicate with each other by default
- However they can’t communicate with resources from other Vnet
- In order to enable that we have to use peering between Vnets
- Scoped to a single region
- …and a single subscription

Virtual Network

- Basically it’s a private network
- Based on physical network but logically separated from the other virtual networks
- Free of charge
- Resources inside a VNet could communicate with each other by default
- However they can’t communicate with resources from other Vnet
- In order to enable that we have to use peering between Vnets
- Scoped to a single region
- …and a single subscription
- Segmented via subnets

Virtual Network

- Basically it’s a private network
- Based on physical network but logically separated from the other virtual networks
- Free of charge
- Resources inside a VNet could communicate with each other by default
- However they can’t communicate with resources from other Vnet
- In order to enable that we have to use peering between Vnets
- Scoped to a single region
- …and a single subscription
- Segmented via subnets
- Each Vnet has its own address range

Virtual Network

- Basically it's a private network
- Based on physical network but logically separated from the other virtual networks
- Free of charge
- Resources inside a VNet could communicate with each other by default
- However they can't communicate with resources from other Vnet
- In order to enable that we have to use peering between Vnets
- Scoped to a single region
- …and a single subscription
- Segmented via subnets
- Each Vnet has its own address range
- All network nodes inside a VNet must be in the same address range

Virtual Network

- Basically it's a private network
- Based on physical network but logically separated from the other virtual networks
- Free of charge
- Resources inside a VNet could communicate with each other by default
- However they can't communicate with resources from other Vnet
- In order to enable that we have to use peering between Vnets
- Scoped to a single region
- …and a single subscription
- Segmented via subnets
- Each Vnet has its own address range
- All network nodes inside a VNet must be in the same address range
- CIDR Notation, e.g. 192.168.0.0/24 (no subnet mask ;))

BOSCH

Virtual Network

- Basically it's a private network
- Based on physical network but logically separated from the other virtual networks
- Free of charge
- Resources inside a VNet could communicate with each other by default
- However they can't communicate with resources from other Vnet
- In order to enable that we have to use peering between Vnets
- Scoped to a single region
- …and a single subscription
- Segmented via subnets
- Each Vnet has its own address range
- All network nodes inside a VNet must be in the same address range
- CIDR Notation, e.g. 192.168.0.0/24 (no subnet mask ;))
- However Azure usually show the whole range, e.g. 192.168.0.0 - 192.168.255.255

BOSCH

Subnet

- Logical segment of a Virtual Network

Subnet

- Logical segment of a Virtual Network
- Hence it shares a subset of VNets' address range

Subnet

- Logical segment of a Virtual Network
- Hence it shares a subset of VNets' address range
- Free of charge

Subnet

- Logical segment of a Virtual Network
- Hence it shares a subset of VNets' address range
- Free of charge
- Resources from Subnets in the same VNet could communicate with each other by default

Subnet

- Logical segment of a Virtual Network
- Hence it shares a subset of VNets' address range
- Free of charge
- Resources from Subnets in the same VNet could communicate with each other by default
- Address schema must be carefully planned in advance as it's very hard to be changed later

Subnet

- Logical segment of a Virtual Network
- Hence it shares a subset of VNets' address range
- Free of charge
- Resources from Subnets in the same VNet could communicate with each other by default
- Address schema must be carefully planned in advance as it's very hard to be changed later
- Bad practice to use the full address range of a VNet with a single Subnet

Subnet

- Logical segment of a Virtual Network
- Hence it shares a subset of VNets' address range
- Free of charge
- Resources from Subnets in the same VNet could communicate with each other by default
- Address schema must be carefully planned in advance as it's very hard to be changed later
- Bad practice to use the full address range of a VNet with a single Subnet
- Up to 3000 Subnets per VNet

Network Security Group

- Basically it’s an ACL

Network Security Group

- Basically it’s an ACL
- Filters network traffic between resources in a VNet

Network Security Group

- Basically it’s an ACL
- Filters network traffic between resources in a VNet
- It filters network traffic based on:
  - source, source port
  - destination, destination port
  - protocol (TCP, UDP)

Network Security Group

- Basically it’s an ACL
- Filters network traffic between resources in a VNet
- It filters network traffic based on:
  - source, source port
  - destination, destination port
  - protocol (TCP, UDP)
- An NSG contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.

Network Security Group

- Basically it’s an ACL
- Filters network traffic between resources in a VNet
- It filters network traffic based on:
  - source, source port
  - destination, destination port
  - protocol (TCP, UDP)
- An NSG contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.
- Each security rule is assigned a number – rules are applied one after another based on those numbers.

Network Security Group

- Basically it’s an ACL
- Filters network traffic between resources in a VNet
- It filters network traffic based on:
  - source, source port
  - destination, destination port
  - protocol (TCP, UDP)
- An NSG contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.
- Each security rule is assigned a number – rules are applied one after another based on those numbers.
- Free of charge

Virtual Network Peering

- It’s used to connect two Virtual Networks

Virtual Network Peering

- It’s used to connect two Virtual Networks
- Once connected, from consumer point of view, those appear as a single Vnet

Virtual Network Peering

- It’s used to connect two Virtual Networks
- Once connected, from consumer point of view, those appear as a single Vnet
- Be careful of network address overlapping

BOSCH

Virtual Network Peering

- It’s used to connect two Virtual Networks
- Once connected, from consumer point of view, those appear as a single Vnet
- Be careful of network address overlapping
- Can work across regions

Virtual Network Peering

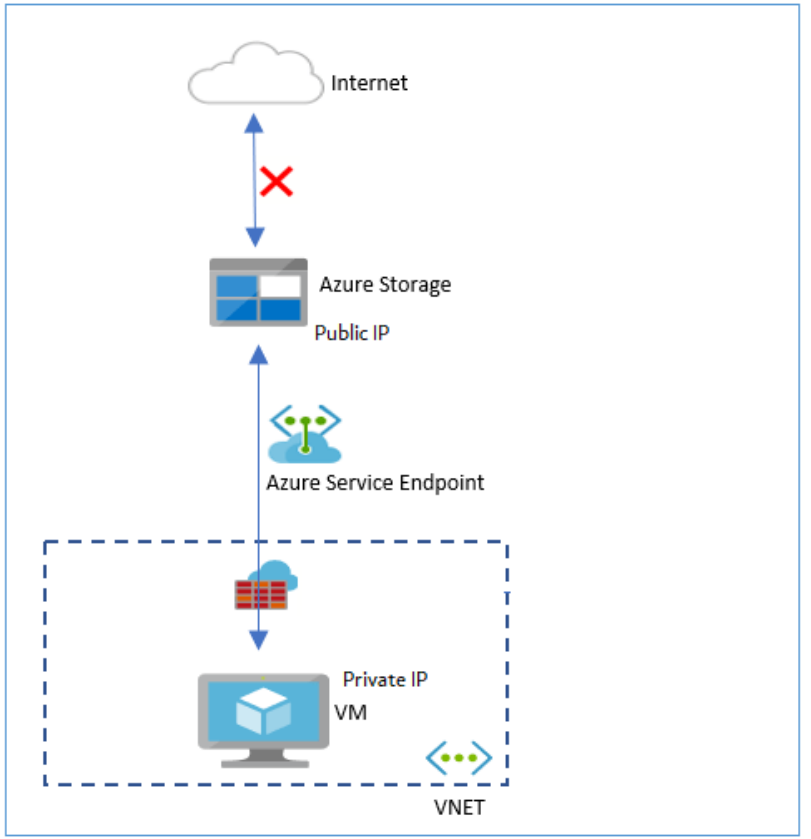
- It’s used to connect two Virtual Networks
- Once connected, from consumer point of view, those appear as a single Vnet
- Be careful of network address overlapping
- Can work across regions
- Not free of charge – billed inbound/outbound data transfer

Bastion Host

- Enables secure connection to a VM
- No open ports is needed
- Web-based connection or from terminal
- Not free of charge – ~130eur/month

Service Endpoint

- Creates a route from a VNet to a managed service (resource)
- Traffic never leaves Azure backbone
- Access from internet can be blocked
- Free of charge



Private Link

- Extends the managed service to a VNet
- From consumer perspective traffic never leaves the VNet
- Access from internet can be blocked
- Can be used from on-prem networks
- Not free of charge

BOSCH

Azure AD (Entra ID)

BOSCH

Azure AD

- Central identity and access management cloud service

Azure AD

- Central identity and access management cloud service
- Controls access to Azure resources

Azure AD

- Central identity and access management cloud service
- Controls access to Azure resources
- It uses RBAC (Users, Groups and Roles)

BOSCH

Azure AD

- Central identity and access management cloud service
- Controls access to Azure resources
- It uses RBAC (Users, Groups and Roles)
- We may add authentication to our apps using Azure AD

BOSCH

Azure AD

- Central identity and access management cloud service
- Controls access to Azure resources
- It uses RBAC (Users, Groups and Roles)
- We may add authentication to our apps using Azure AD
- Used to manage access to thousands of apps

BOSCH

Tenant

- A specific instance of Azure AD (Directory in AD)

Tenant

- A specific instance of Azure AD (Directory in AD)
- A Directory containing accounts and groups

BOSCH

Tenant

- A specific instance of Azure AD (Directory in AD)
- A Directory containing accounts and groups
- It’s not part of the subscription hierarchy

BOSCH

Tenant

- A specific instance of Azure AD (Directory in AD)
- A Directory containing accounts and groups
- It’s not part of the subscription hierarchy
- A tenant can be assigned to multiple subscriptions

Tenant

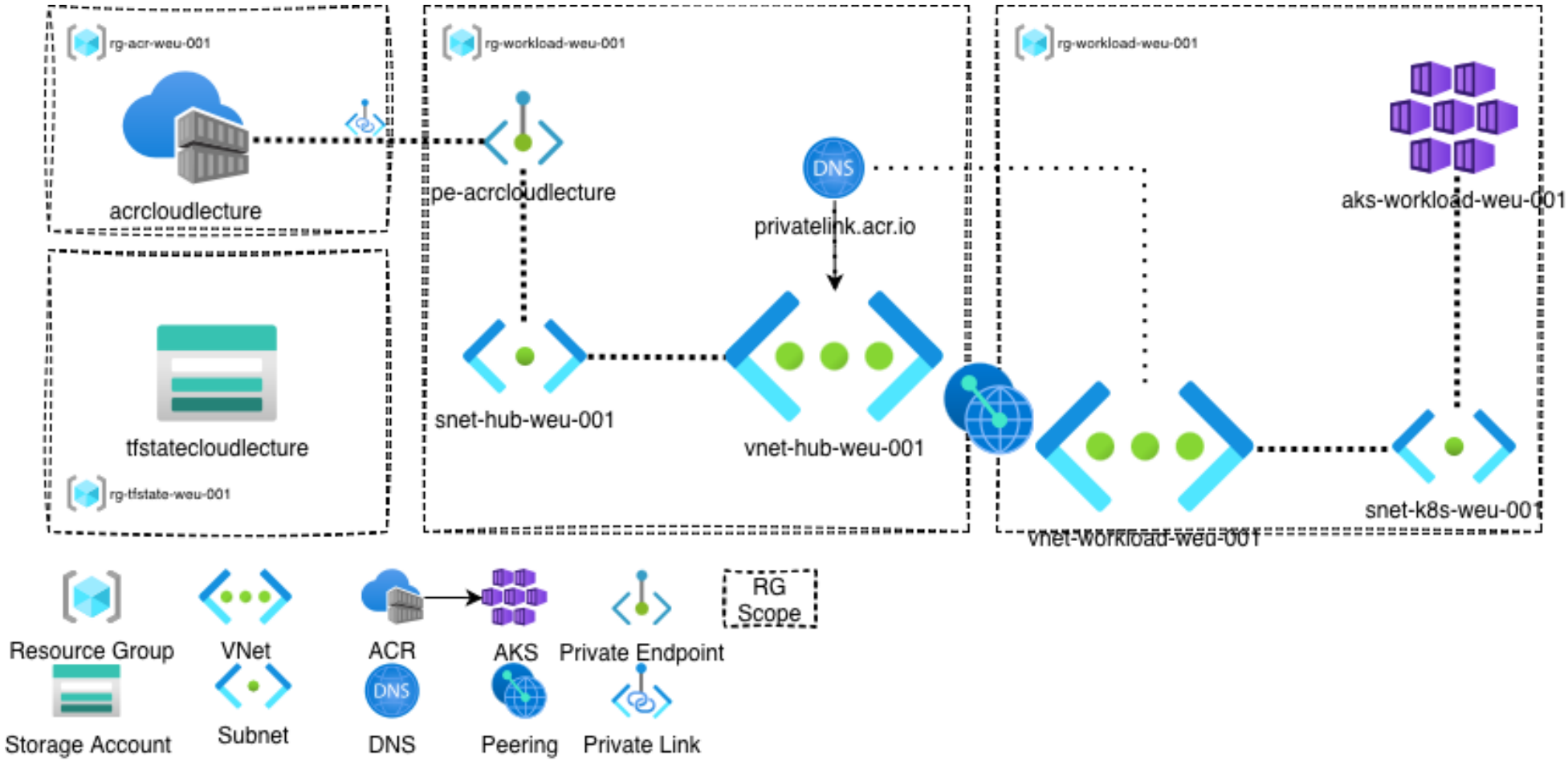
- A specific instance of Azure AD (Directory in AD)
- A Directory containing accounts and groups
- It’s not part of the subscription hierarchy
- A tenant can be assigned to multiple subscriptions
- An account can be part to multiple tenants
- A tenant is create automatically when a subscription is created

Managed Identities

- Azure AD Identity for Azure resources
- Thus Azure resource could connect or manage other resources using this ID
- No need of additional credentials
- Two types of managed identities:
  - System Assigned: Managed by Azure. Tied to resource lifecycle
  - User Assigned: Managed by User. Can be assigned to multiple resources

Demo

BOSCH



Thank you!