



# Network Security on Azure

## How to stay safe & secure Cloud workloads the right way?

(by Stefan Rapp, 11.12.2024, 12:00 – 12:45)

# What is Network Security all about?



imgflip.com

JAKE-CLARK.TUMBLR

Focus on...



“Network Architecture” → Groundwork



# ...Bad Results

## Network Security is suffering!

- Vulnerabilities & Potential breaches
- Network Complexity
- Operational Inefficiencies (slower)
- Scalability Issues (growth & changes)
- Compliance Risks (industry standards & regulations)
- Inconsistent Security Settings (each team)



# Table of contents

1. Prerequisites
2. Overview Network Services
3. Virtual Network (VNet)
4. Traffic Management
5. Service & Private Endpoints
6. Infrastructure as Code (IaC)
7. Key Takeaways (Q&A)





Which requirements must be fulfilled before an enterprise can successfully start with Azure workloads (modernization).

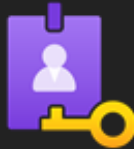
## Prerequisites of Azure Network Services

# Prerequisites Checklist

What is needed before bringing the first Workload to Azure?

## Cloud Strategy (Goal, Destination, etc.)

### Azure Governance



- Azure Billing & Cost Management
- Azure Hierarchy
- Azure RBAC
- Azure Policies
- Naming Convention
- Tag & Lock Strategy

### Azure Core Infrastructure



- General Design
- **Network Architecture & Security**
- Hybrid Connection
- Azure Firewall & Azure NVA
- Logging & Monitoring
- etc.

### Cloud Automation



- No “Click-Click-Cloud”/”ClickOps”
- Infrastructure as Code (IaC)
- Central Module Library
- Reusability
- Module Lifecycle
- CI/CD
- etc.

## Azure Security





What kind of Azure resources are relevant to bring application workloads to the cloud?























## Overview Azure Network Services



# Azure Networking Services – Overview

Networking Capabilities to secure Azure Services

- **Access & Connect** Azure resources and on-premises resources
- **Support, Protect, and Monitor** applications in the Azure network.

Connectivity	Application Protection	Application Delivery	Network Monitoring
Connect to <b>Azure &amp; on-premises</b> resources	Protect cloud applications	Deliver applications in the Azure network	Monitor network resources
<ul style="list-style-type: none"><li>• Virtual Network &amp; Peerings </li><li>• Virtual WAN </li><li>• ExpressRoute &amp; VPN </li><li>• Azure DNS </li><li>• User defined Routes </li><li>• NAT Gateway </li><li>• ...etc.</li></ul>	<ul style="list-style-type: none"><li>› Private Links </li><li>› DDoS Protection </li><li>› Azure Firewall </li><li>› Network Security Groups </li><li>› Web Application Firewall (WAF) </li><li>› Private Endpoints </li><li>› ... etc.</li></ul>	<ul style="list-style-type: none"><li>› Azure CDN </li><li>› Azure Front Door Service </li><li>› Traffic Manager </li><li>› Application Gateway </li><li>› Internet Analyzer </li><li>› Load Balancer </li><li>› ...etc.</li></ul>	<ul style="list-style-type: none"><li>› Network Watcher </li><li>› ExpressRoute Monitor </li><li>› Azure Monitor </li><li>› VNet Flow Log </li><li>› ...etc.</li></ul>

- Microsoft [CAF](#) for Azure
- Azure Well-architected Framework ([WAF](#))





Azure Virtual Network (VNet) is the fundamental building block for the private network in Azure.

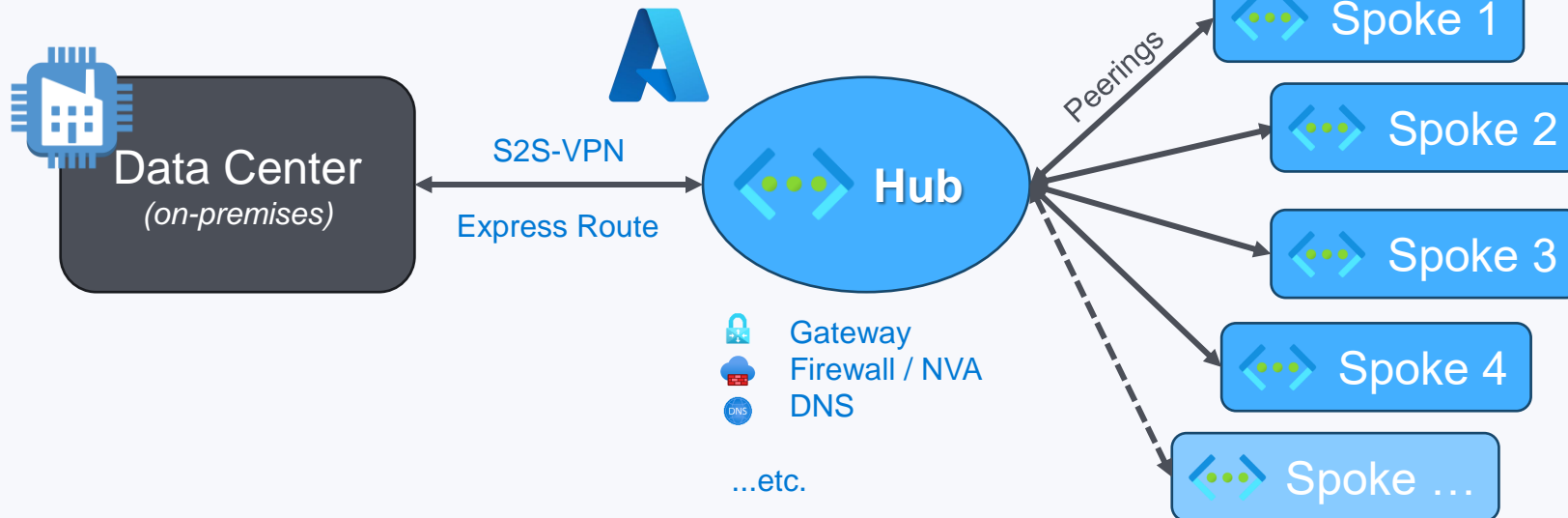
## Azure Virtual Network



# Azure Networking Services

## Azure Virtual Network

- Fundamental building block in Microsoft Azure to connect cloud resources.
- Hub & Spoke Architecture**
  - Hub Network: **Shared** Azure Services
  - Spoke Network: VNets isolated and manage app workloads **separately**
  - VNet Peering ist nicht **Transitiv!**



# Network Segmentation

Isolating resources in the network from each other

- Azure VNet → **/22**

([Visual Subnet Calculator - Split/Join](#))

- Azure Subnet → **/26** → Number of possible Subnets **16**
- Azure Subnet → **/27** → Number of possible Subnets **32**

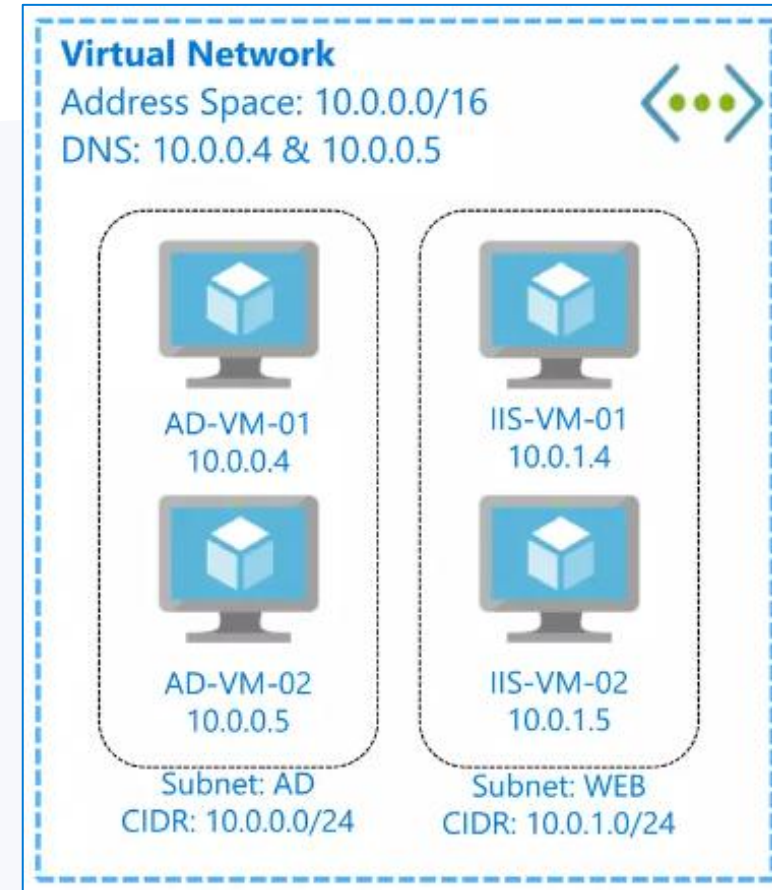
Subnet address	Range of addresses	Useable IPs	Hosts	Divide	Join
10.100.4.0/26	10.100.4.0 - 10.100.4.63	10.100.4.1 - 10.100.4.62	62	<a href="#">Divide</a>	<div> <div>/26</div> <div>/25</div> <div>/24</div> <div>/23</div> <div>/22</div> </div>
10.100.4.64/26	10.100.4.64 - 10.100.4.127	10.100.4.65 - 10.100.4.126	62	<a href="#">Divide</a>	
10.100.4.128/26	10.100.4.128 - 10.100.4.191	10.100.4.129 - 10.100.4.190	62	<a href="#">Divide</a>	
10.100.4.192/26	10.100.4.192 - 10.100.4.255	10.100.4.193 - 10.100.4.254	62	<a href="#">Divide</a>	
10.100.5.0/26	10.100.5.0 - 10.100.5.63	10.100.5.1 - 10.100.5.62	62	<a href="#">Divide</a>	
10.100.5.64/26	10.100.5.64 - 10.100.5.127	10.100.5.65 - 10.100.5.126	62	<a href="#">Divide</a>	
10.100.5.128/26	10.100.5.128 - 10.100.5.191	10.100.5.129 - 10.100.5.190	62	<a href="#">Divide</a>	
10.100.5.192/26	10.100.5.192 - 10.100.5.255	10.100.5.193 - 10.100.5.254	62	<a href="#">Divide</a>	
10.100.6.0/26	10.100.6.0 - 10.100.6.63	10.100.6.1 - 10.100.6.62	62	<a href="#">Divide</a>	
10.100.6.64/26	10.100.6.64 - 10.100.6.127	10.100.6.65 - 10.100.6.126	62	<a href="#">Divide</a>	
10.100.6.128/26	10.100.6.128 - 10.100.6.191	10.100.6.129 - 10.100.6.190	62	<a href="#">Divide</a>	
10.100.6.192/26	10.100.6.192 - 10.100.6.255	10.100.6.193 - 10.100.6.254	62	<a href="#">Divide</a>	
10.100.7.0/26	10.100.7.0 - 10.100.7.63	10.100.7.1 - 10.100.7.62	62	<a href="#">Divide</a>	
10.100.7.64/26	10.100.7.64 - 10.100.7.127	10.100.7.65 - 10.100.7.126	62	<a href="#">Divide</a>	
10.100.7.128/26	10.100.7.128 - 10.100.7.191	10.100.7.129 - 10.100.7.190	62	<a href="#">Divide</a>	
10.100.7.192/26	10.100.7.192 - 10.100.7.255	10.100.7.193 - 10.100.7.254	62	<a href="#">Divide</a>	



# Microsoft Azure VNets

What are the characteristics of an Azure VNet?

- **Logical isolation** with control over the network
- Support for IP addresses ranges (CIDR)
- **DNS** Support
- **Non-overlapping** address ranges
- Support for **static/dynamic** IPs
- **DHCP** “*out-of-the-box*” available





How to **filter** and **control** traffic?

## Network Traffic Management

# Network Security Groups (NSG)

Use NSG to filter network traffic between Azure resources in an Azure VNet.

- No extra **costs**.
- Enables subnet **segmentation** scenarios.
- Contains a list of ACL **rules** that “*Allow*” or “*Deny*” traffic from/to a VNET. (Layer 3 & 4)
- **Restrict** traffic from/to internal and external sources.
- Rules on URLs or FQDN is not **supported**.
- But “*Service Tags*” can be used for rules.
- Custom rules with **priority** between 100 and 4096.
- Can be assigned to a **NIC** or an Azure **subnet**.



The screenshot displays the Azure portal interface for a Network Security Group (NSG) named 'vm-msix-nsg'. The left sidebar shows navigation options like Overview, Activity log, Access control (IAM), Tags, and Settings. The main area shows the 'Essentials' section with details about the resource group, location, subscription, and associated subnets and network interfaces. Below this, there is a table of security rules, categorized into Inbound and Outbound rules. Each rule entry includes its priority, name, port, protocol, source, destination, and action (Allow or Deny).

Priority	Name	Port	Protocol	Source	Destination	Action
<b>Inbound Security Rules</b>						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
<b>Outbound Security Rules</b>						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

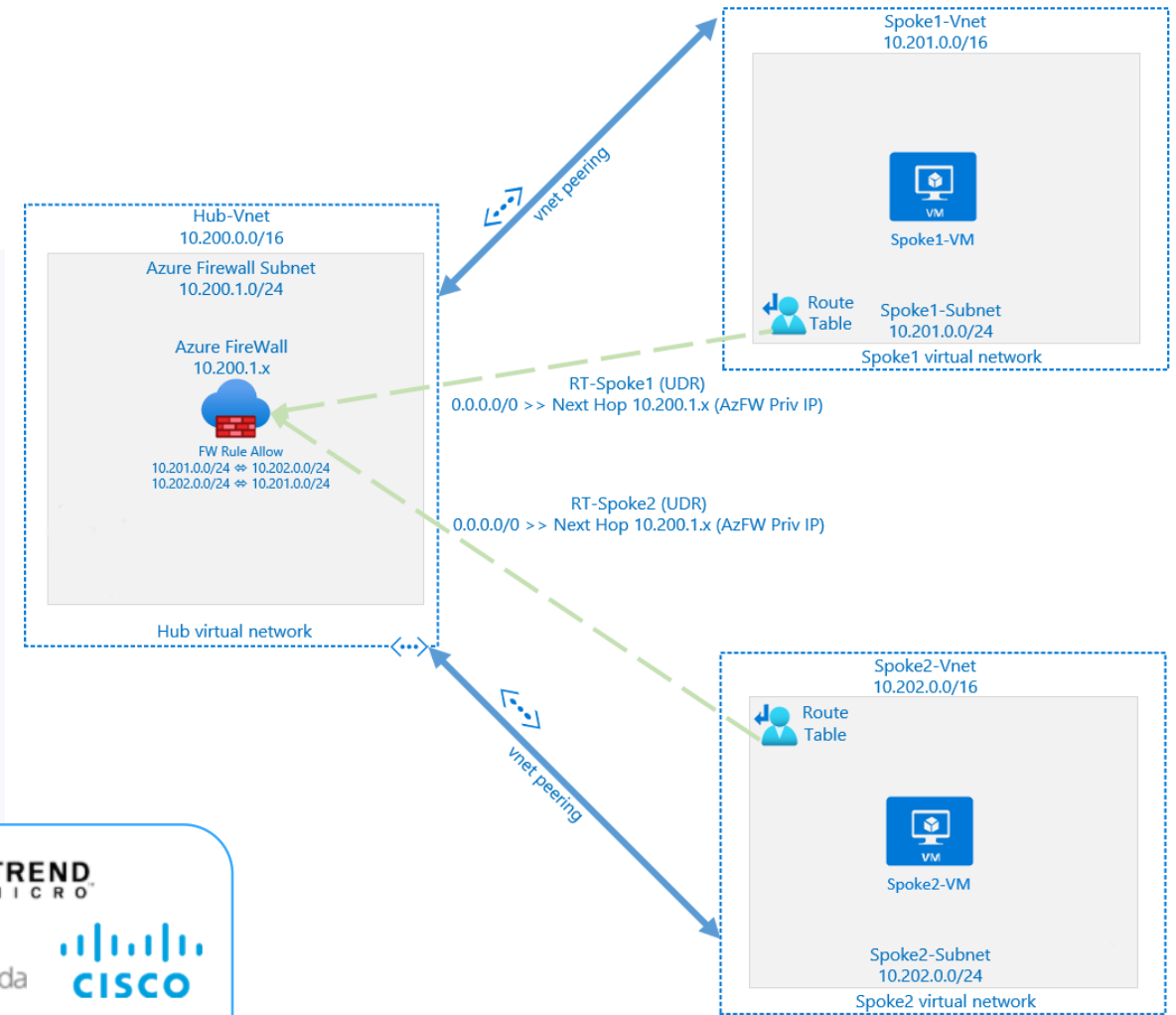


# Firewalling & Routing

- Control network traffic
- Centralized Management (SPoC)
  - East-west Traffic (within trusted boundary)
  - North-south Traffic (to external boundary)
- Key Components:
  - Azure Firewall/NVA
  - VNet Peering
  - Route Tables (UDRs)

• Azure Firewall → PaaS  (cloud-native)

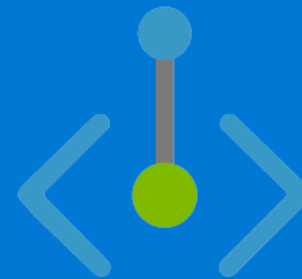
• Azure NVA → IaaS 





Provide a secure and direct connectivity to Azure services.

## Service & Private Endpoints



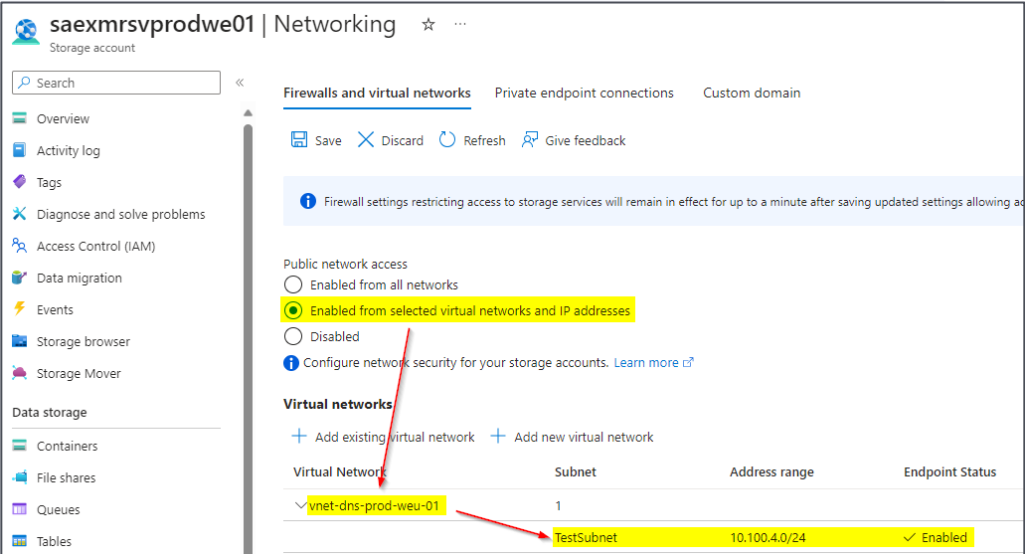
# Service Endpoints

## Overview



- Azure Services are generally **public**. → [Document \(JSON\)](#)
- Fully **removing** public internet access → Only allow traffic from your **VNet/Subnet**.
- Provide a **secure** and **direct** connectivity to Azure services.
- Enable private IP addresses in the Azure VNet to reach the endpoint of an Azure service.
- An optimized route over the **Azure Backbone** network.
- Goal: Secure your **critical** Azure service resources.
- Without needing a **public IP** address on the VNet.

 ServiceTags\_Public\_20230925.json



saexmrsvprodwe01 | Networking

Storage account

Search

Firewalls and virtual networks | Private endpoint connections | Custom domain

Save | Discard | Refresh | Give feedback

Firewall settings restricting access to storage services will remain in effect for up to a minute after saving updated settings allowing ad

Public network access

☐ Enabled from all networks

☒ Enabled from selected virtual networks and IP addresses

☐ Disabled

Configure network security for your storage accounts. [Learn more](#)

Virtual networks

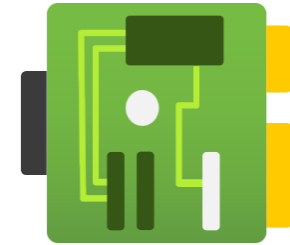
+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status
vnet-dns-prod-weu-01	1		
	TestSubnet	10.100.4.0/24	✓ Enabled



# Private Endpoint

Use Private Endpoint with a **private IP** to secure your Azure service.



- Private endpoint = **NIC** that uses a private IP address from your VNet.
- Used to bring certain services **into** your VNet.
- Connects **privately** and **securely** to a service that is powered by **Azure Private Link**.
- Private Link resource is the **destination target** of a specified private endpoint ([List](#)).
- Causes extra **costs**! 💰 💰 💰

Private Link Service

There is no charge for Private link service

Private Endpoint

1	x	730	Hours	x	€0.010	=	€6.94
Endpoints					Per unit/hour		

Data processed

Outbound data processed

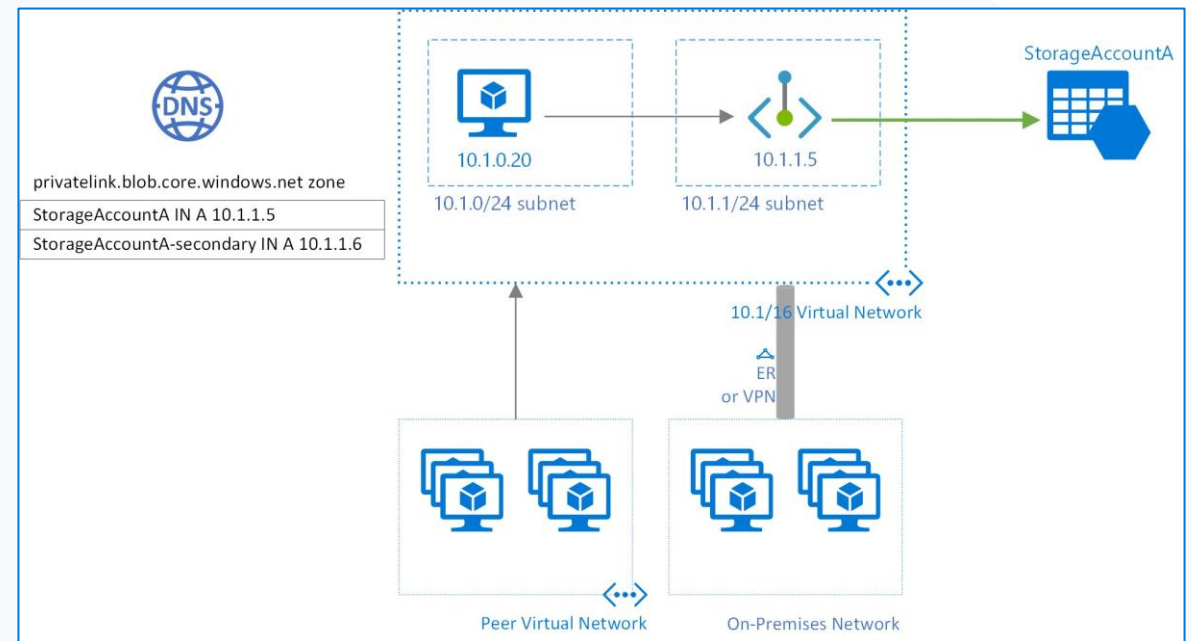
1	TB	=	€9.74
---	----	---	-------

Inbound data processed

1	TB	=	€9.74
---	----	---	-------

In addition to the Data Processed charges, **Bandwidth** charges are also applicable. [Learn more about Bandwidth pricing.](#)

Upfront cost	€0.00
Monthly cost	€26.43

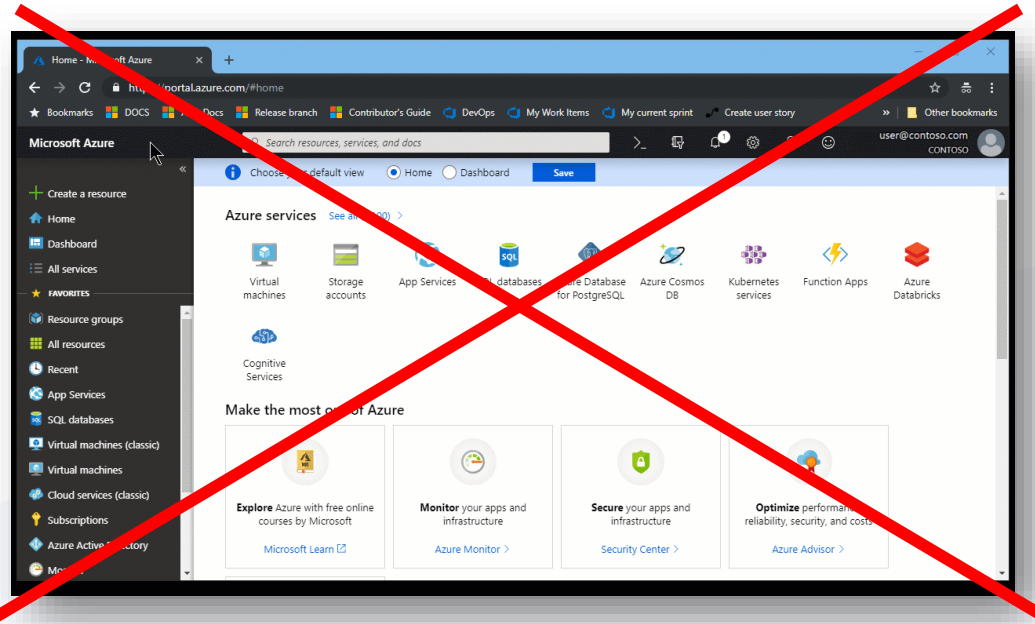




Why IaC is a real game changer?

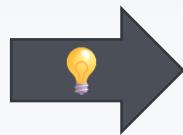
## Infrastructure as Code (IaC)

# Mind change administration interface

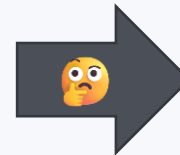


```
You, 4 weeks ago | 1 author (You)
1 resource "azurerm_resource_group" "this" {
2   count = var.create_resource_group ? 1 : 0
3   name = var.resource_group_name
4   location = var.module_location
5
6   tags = merge(
7     var.module_tags,
8     var.resource_group_tags
9   )
10 }
11
You, 4 weeks ago | 1 author (You)
12 resource "azurerm_virtual_network" "this" {
13   count = var.create_virtual_network ? 1 : 0
14   location = var.module_location
15   resource_group_name = try(azurerm_resource_group.this[0].name, var.resource_group_name)
16   name = var.virtual_network_name
17   address_space = var.virtual_network_address_space
18   bgp_community = var.virtual_network_bgp_community
19   dns_servers = var.virtual_network_dns_servers
20   edge_zone = var.virtual_network_edge_zone
21   flow_timeout_in_minutes = var.virtual_network_flow_timeout_in_minutes
22
23   You, 2 months ago | 1 author (You)
24   dynamic "ddos_protection_plan" {
25     for_each = var.virtual_network_ddos_protection_plan != null ? var.virtual_network_ddos_protection_plan : {}
26   }
27 }
```

„Click-Click-Cloud“  
„Clicky-Bunti“



„Transition 2 cloud“  
→ Shift from “static” to  
“dynamic” infrastructure



Cloud Operating  
Model ⚙️





What are the essential takeaways of the session?

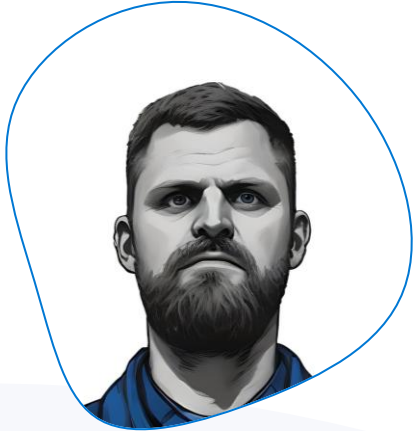
## Key Takeaways

# Key Takeaways

- ✓ Check with your Governance & Platform Team before the start!
- ✓ Start making a **plan** → Network **design** (“*But do not click!*”)
- ✓ Use Microsoft **CAF** & **Well-architected** Framework
- ✓ **Size** your application network according to your workload
  - # of possible hosts
  - # of possible subnets
  - Restrictions from Microsoft
- ✓ Think about a suitable **separation** of the application workloads
- ✓ How traffic is **controlled** in the given Azure Landing Zone
- ✓ Secure Azure Services using the “*Networking*” section
  - ✓ Service Endpoints
  - ✓ Private Endpoints
- ✓ Use **IaC** approach to do resource provisioning in the cloud



# PROFILE – Speaker



**Stefan Rapp**

*Cloud Solution Architect (CSA) & Microsoft MVP*

**Xebia**

Let's engage: <https://www.linkedin.com/in/rapster83/>

#AzureRocks 🙌👤🎸

E-Mail: [info@blog.misterazure.com](mailto:info@blog.misterazure.com)

Blog: <https://blog.misterazure.com>

GitHub: [@rapster83](https://github.com/rapster83)



**Specializations:** *(MS Consultant since 2008)*

- Identity & Access Management (IAM)
- Microsoft Infrastructure
- Azure Governance
- Azure Infrastructure
- Cloud Automation – IaC (with Terraform)
- Cloud Migrations
- Application Modernization