Azure Meetup KONSTANZ

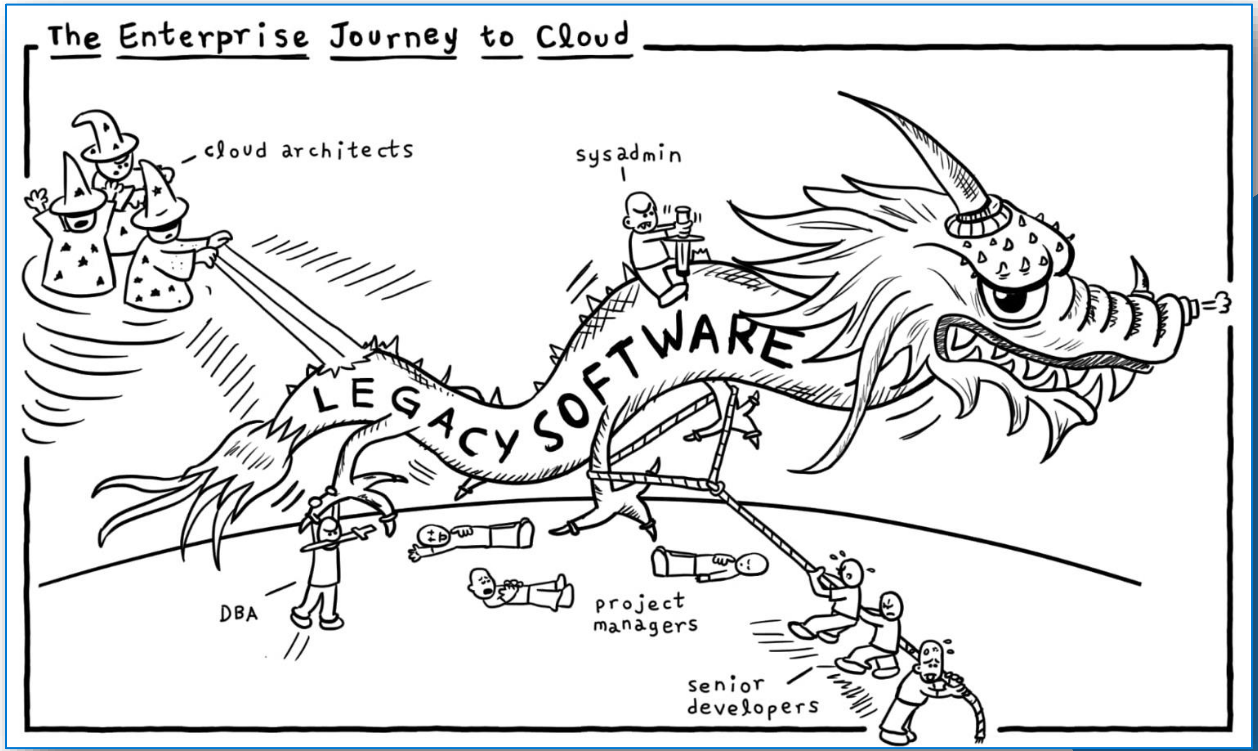
Azure Meetup STUTTGART

Secure Cloud Workloads!

A Developer's Guide to Cloud Network Security

How Cloud Projects “normally” start

How Cloud Projects “normally” run



Source: https://tanzu.vmware.com/content/blog/enterprise-journey-to-the-cloud

Table of contents

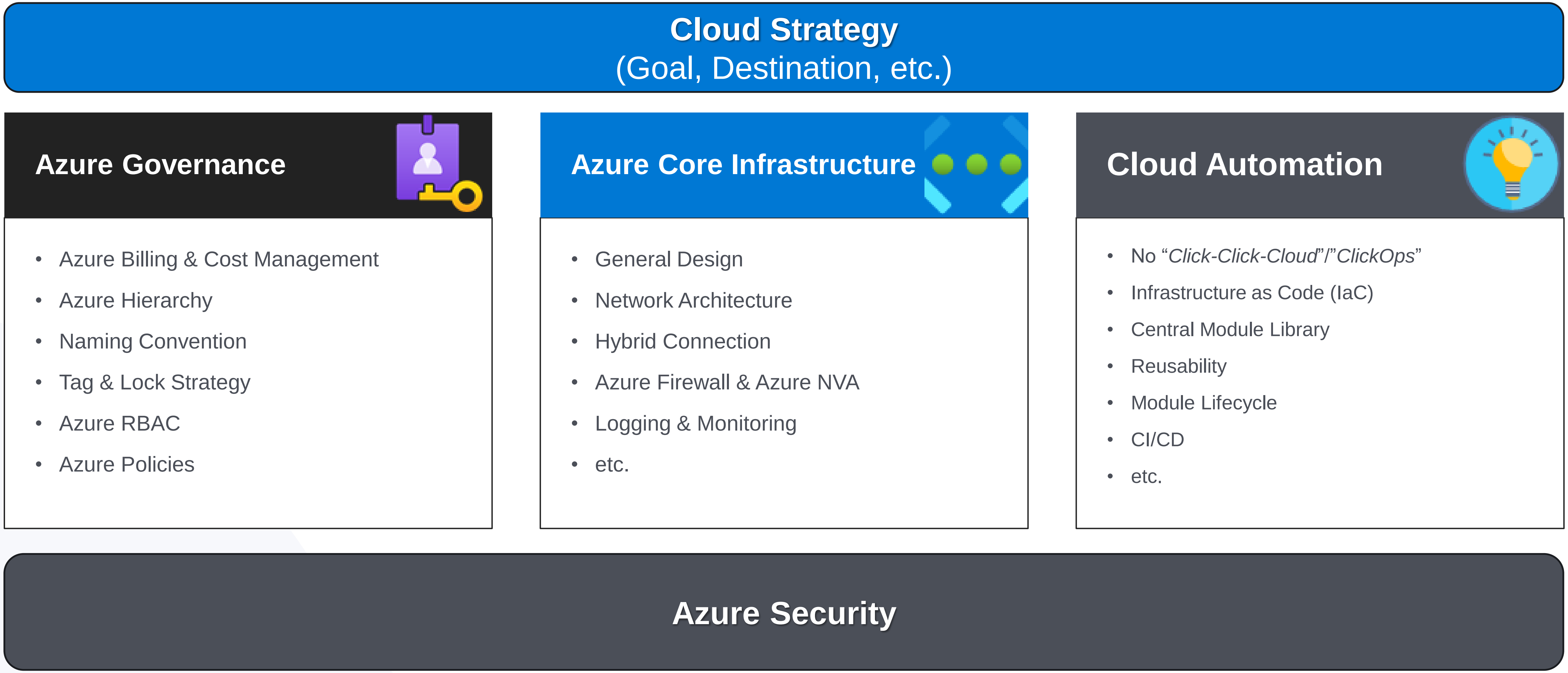
1. Prerequisites
2. Overview of Azure Network Services
3. Azure Virtual Network
4. Azure Service Endpoints
5. Azure Private Endpoint
6. General Azure Security Services
7. Key Takeaways (Q&A)

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

Prerequisites
# of Azure Network Services

Prerequisites

What is needed before bringing the first Workload to Azure?



Cloud Strategy

(Goal, Destination, etc.)

Azure Governance

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

Azure Core Infrastructure

- General Design
- Network Architecture
- 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

Why Network Security on Azure?

- Collection of Azure **best practices** to enhance the network security.
- Derived from **experience** with Azure networking in real **customer projects**.

Content:

- What is **best practice**?
- Why you want to enable that best practice?
- What might be the result if you **fail** to enable the best practice?
- Possible **alternatives** to the best practice?
- **How** can you learn to enable the best practice?

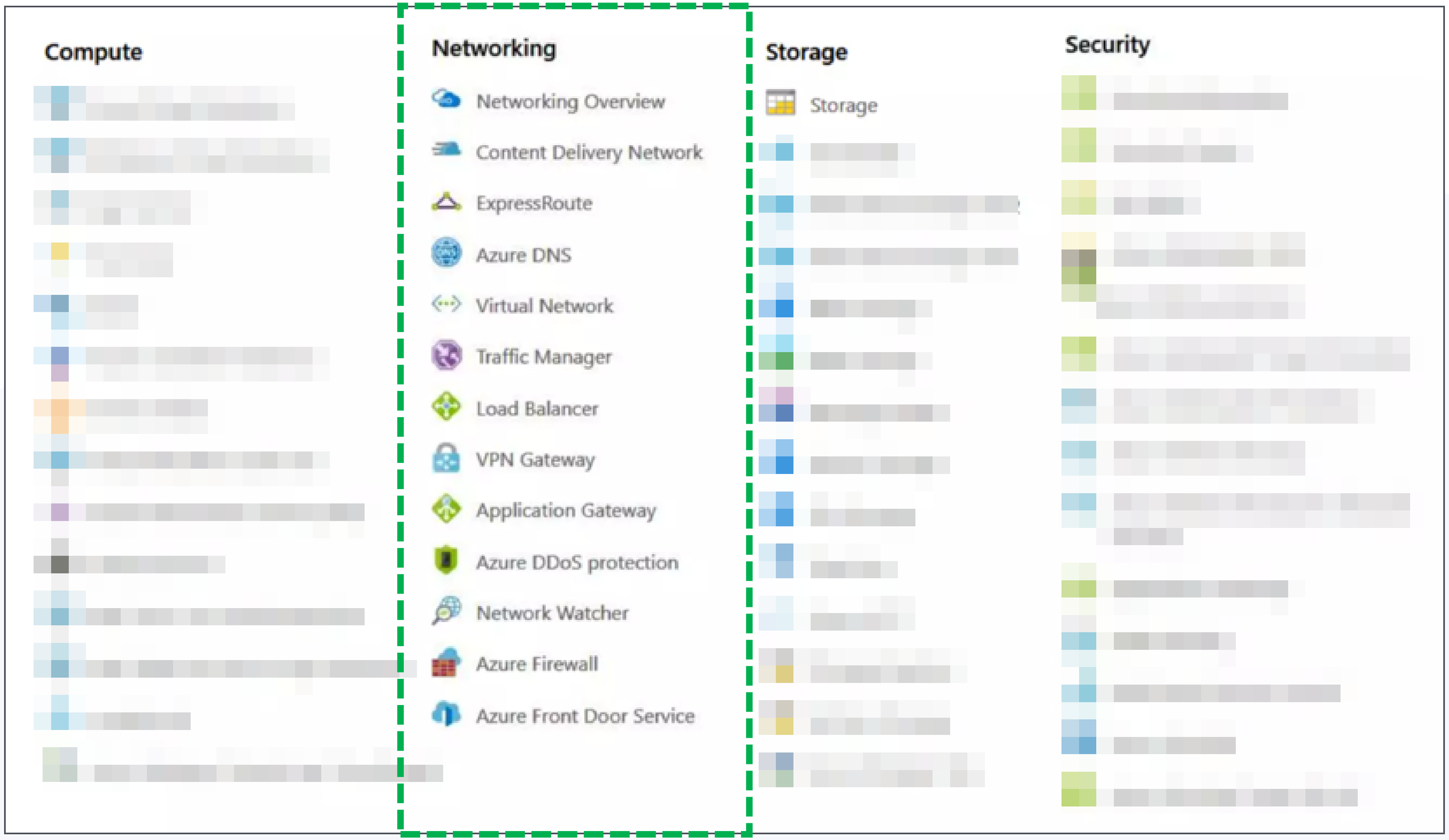
- Based on a consensus opinion. → Microsoft **CAF** & Well-architected Framework (**WAF**)
- Usage of Azure platform capabilities and feature sets.
- Stay up to date ("*Don't get left behind*").

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

Overview Azure Network Services

Azure Network Services

Examples of Azure Network Services



Compute

Networking

- Networking Overview
- Content Delivery Network
- ExpressRoute
- Azure DNS
- Virtual Network
- Traffic Manager
- Load Balancer
- VPN Gateway
- Application Gateway
- Azure DDoS protection
- Network Watcher
- Azure Firewall
- Azure Front Door Service

Storage

- Storage

Security

Azure Networking Services – Overview

Networking Capabilities to secure Azure Services

Connectivity

Connect to **Azure** & **on-premises** resources

- Virtual Network & Peerings
- Virtual WAN
- ExpressRoute
- VPN Gateway
- Azure DNS
- Route Server
- Azure Bastion
- NAT Gateway
- ...etc.

Application Protection

Protect cloud applications

- Load Balancer
- Private Links
- DDoS Protection
- Azure Firewall
- Network Security Groups
- Web Application Firewall
- Private Endpoints
- ... etc.

Application Delivery

Deliver applications in the Azure network

- Azure CDN
- Azure Front Door Service
- Traffic Manager
- Application Gateway
- Internet Analyzer
- Load Balancer
- ...etc.

Network Monitoring

Monitor network resources

- Network Watcher
- ExpressRoute Monitor
- Azure Monitor
- VNet TAP
- ...etc.

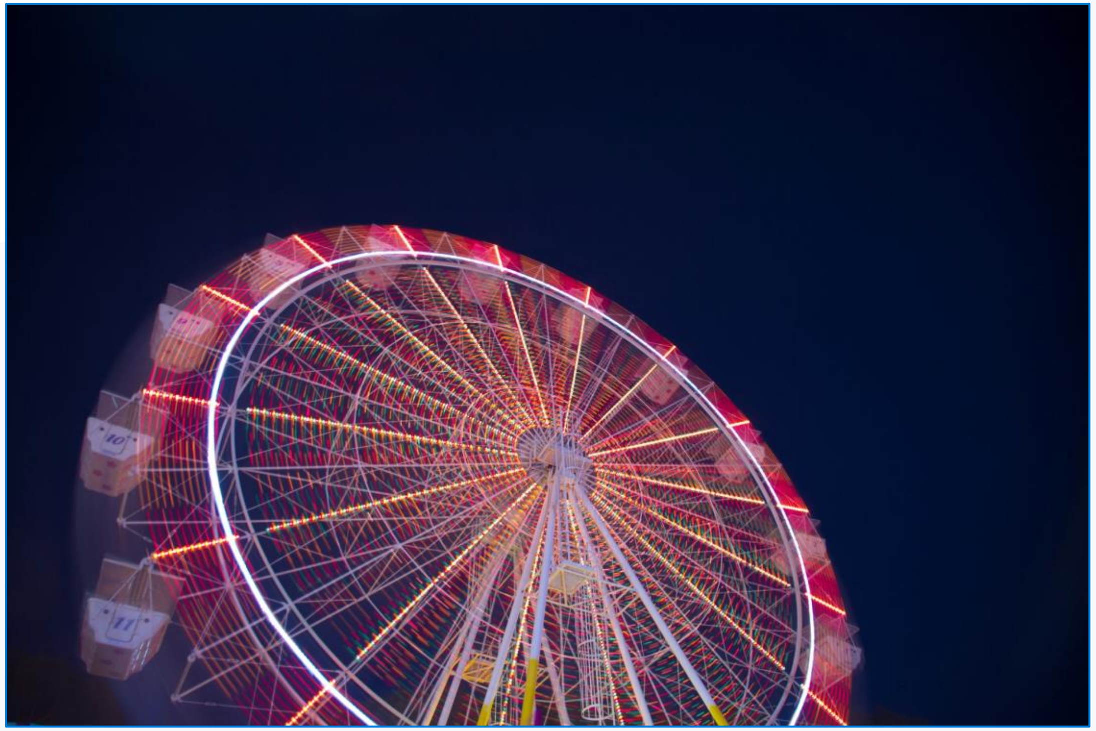
Azure networking services enable users to **access/connect** Azure resources and on-premises resources, **protect**, **deliver**, and **monitor** the applications in the Azure network.

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

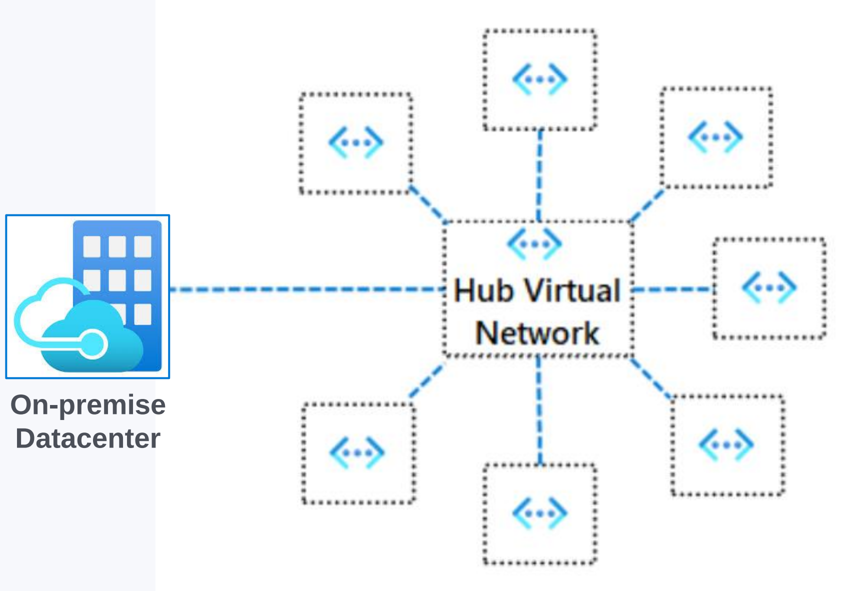
Azure Virtual Network

“Hub & Spoke” Architecture

- **Hub** = VNet hosts **shared** Azure services
- **Spoke** = VNets isolated and manage app workloads **separately**



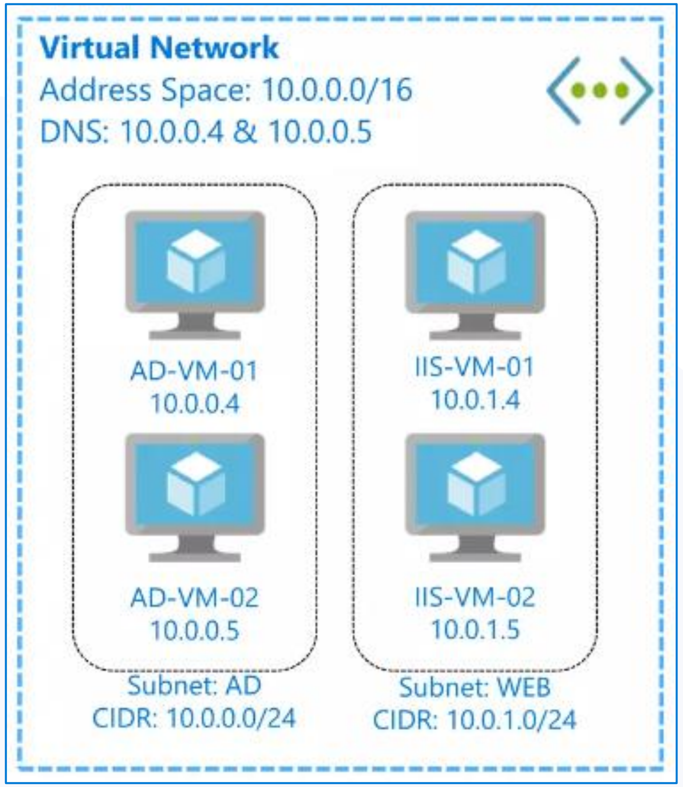
Source: https://unsplash.com/photos/timelapse-low-angle-of-white-and-red-ferris-wheel-oXyzqlcNNaU



Microsoft Azure VNets

What are the characteristics of an Azure VNet?

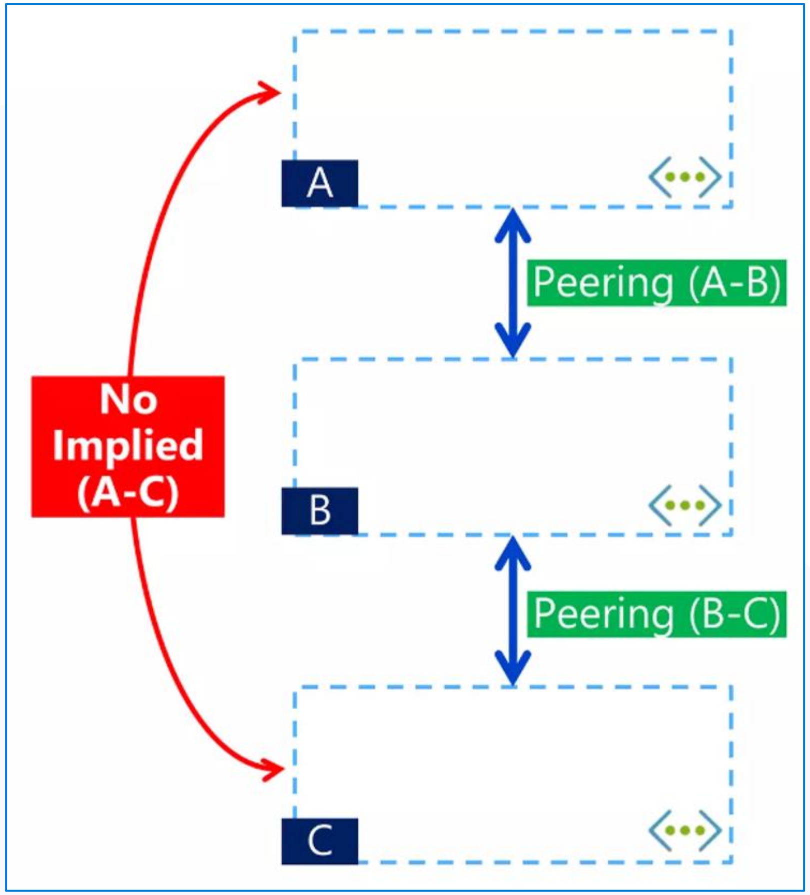
- **Logical isolation** with control over the network
- Contain **subnets** to **isolate traffic** using NSGs or FW
- Support for IP addresses ranges (CIDR)
- One or more **non-overlapping** address ranges
- Support for **static/dynamic** IPs
- **DHCP** "*out-of-the-box*" available
- **DNS** Support
- **Hybrid** Connectivity Support:
  - VPN Site-to-Site
  - VPN Point-to-Site
  - ExpressRoute
- VNet cannot span over **Azure Subscriptions**



Azure VNet Peerings

- **Connect** 2 VNets in the same/other region
- Utilizes the **Azure Backbone** network
- Appears as one network for connectivity
- Managed as separate resource

- VNet peering is between 2 Vnets
- There is no derived **transitive** relationship.
- VNet address spaces cannot **overlap**.
- Peered VNets can be in different subscriptions (linked to same tenant).
- Inter-VNet traffic is not encrypted.
- Think about name resolution (DNS).

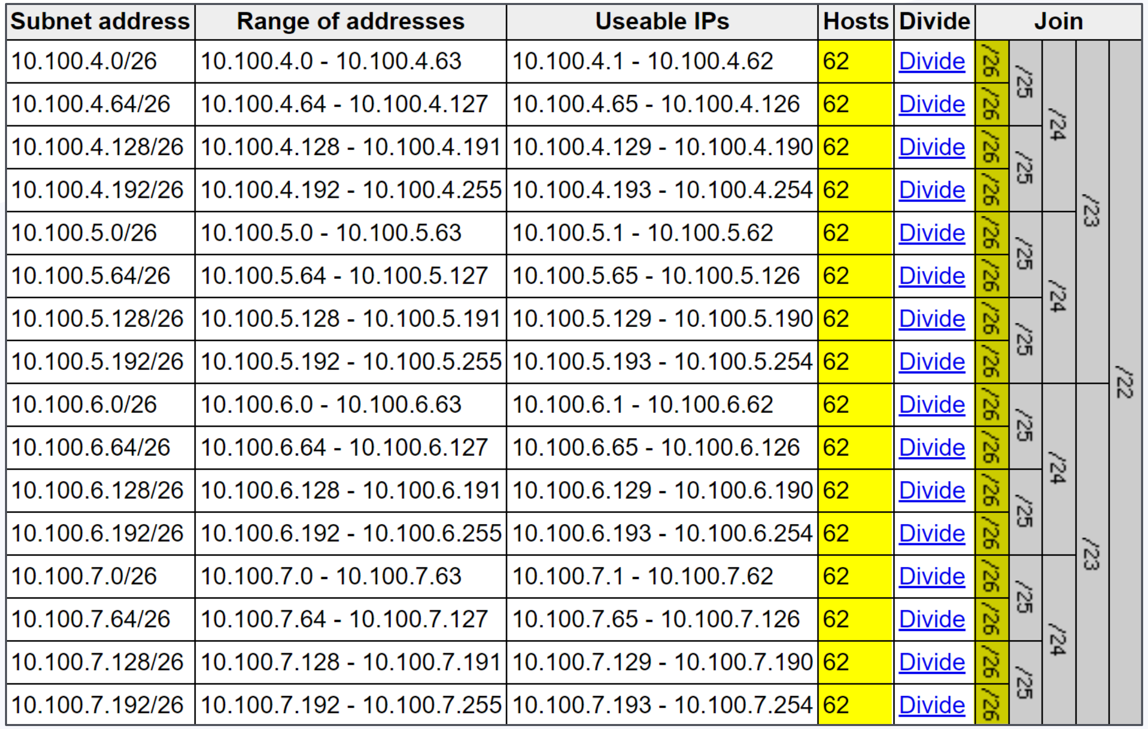


Network Segmentation

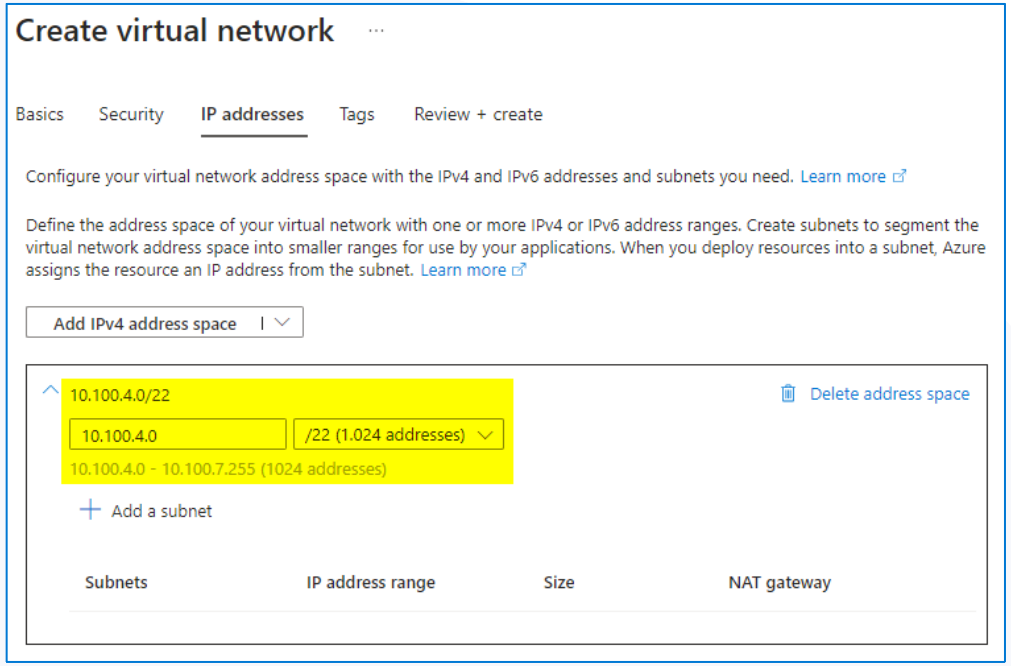
Isolating resources in the network from each other

- Azure VNet → **/22**
  - Azure Subnet → **/26** → Number of possible Subnets **16**
  - Azure Subnet → **/27** → Number of possible Subnets **32**

(Subnet Calculator)



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	Divide	/26	/25	/24	/23	/22
10.100.4.64/26	10.100.4.64 - 10.100.4.127	10.100.4.65 - 10.100.4.126	62	Divide	/26				
10.100.4.128/26	10.100.4.128 - 10.100.4.191	10.100.4.129 - 10.100.4.190	62	Divide	/26	/25			
10.100.4.192/26	10.100.4.192 - 10.100.4.255	10.100.4.193 - 10.100.4.254	62	Divide	/26				
10.100.5.0/26	10.100.5.0 - 10.100.5.63	10.100.5.1 - 10.100.5.62	62	Divide	/26	/25	/24		
10.100.5.64/26	10.100.5.64 - 10.100.5.127	10.100.5.65 - 10.100.5.126	62	Divide	/26				
10.100.5.128/26	10.100.5.128 - 10.100.5.191	10.100.5.129 - 10.100.5.190	62	Divide	/26	/25			
10.100.5.192/26	10.100.5.192 - 10.100.5.255	10.100.5.193 - 10.100.5.254	62	Divide	/26				
10.100.6.0/26	10.100.6.0 - 10.100.6.63	10.100.6.1 - 10.100.6.62	62	Divide	/26	/25	/24	/23	
10.100.6.64/26	10.100.6.64 - 10.100.6.127	10.100.6.65 - 10.100.6.126	62	Divide	/26				
10.100.6.128/26	10.100.6.128 - 10.100.6.191	10.100.6.129 - 10.100.6.190	62	Divide	/26	/25			
10.100.6.192/26	10.100.6.192 - 10.100.6.255	10.100.6.193 - 10.100.6.254	62	Divide	/26				
10.100.7.0/26	10.100.7.0 - 10.100.7.63	10.100.7.1 - 10.100.7.62	62	Divide	/26	/25	/24		
10.100.7.64/26	10.100.7.64 - 10.100.7.127	10.100.7.65 - 10.100.7.126	62	Divide	/26				
10.100.7.128/26	10.100.7.128 - 10.100.7.191	10.100.7.129 - 10.100.7.190	62	Divide	/26	/25			
10.100.7.192/26	10.100.7.192 - 10.100.7.255	10.100.7.193 - 10.100.7.254	62	Divide	/26				



Create virtual network ···

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. Learn more

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. Learn more

10.100.4.0/22

10.100.4.0 | /22 (1.024 addresses)

10.100.4.0 - 10.100.7.255 (1024 addresses)

Subnets	IP address range	Size	NAT gateway

Zero Trust Network

Ensure Zero Trust methodology in the Azure Hub & Spoke network.

- Mindset → “*assume breach, never trust, always verify*”

🔑 Verify explicitly → **Always authenticate & authorize**

🔒 Least privilege approach → **Limit user access**

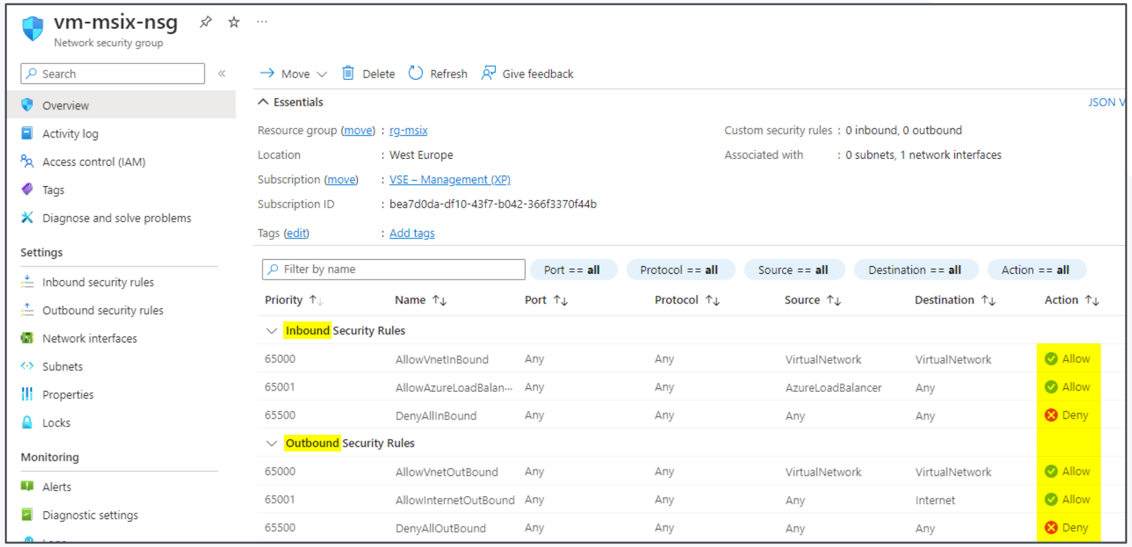
👤 Assume breach → **Min. blast radius & segment access**

- Zero Trust is a security **strategy**, <u>not</u> a product or a service!
- It’s an approach in designing and implementing **security principles**.
- Affects cloud infrastructure, deployment strategy, and implementation.

Network Security Groups (NSG) – Overview

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.
- Manage using "*Infrastructure as Code*" (IaC).
- Enforce NGS and rules with "*DeployIfNotExist*" Policy.
- 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**.



Resource group (move) : rg-msix
Location : West Europe
Subscription (move) : VSE – Management (XP)
Subscription ID : bea7d0da-df10-43f7-b042-366f3370f44b
Tags (edit) : Add tags
Custom security rules : 0 inbound, 0 outbound
Associated with : 0 subnets, 1 network interfaces

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

Provide a secure and direct connectivity to Azure services using **Service** Endpoints on Azure.

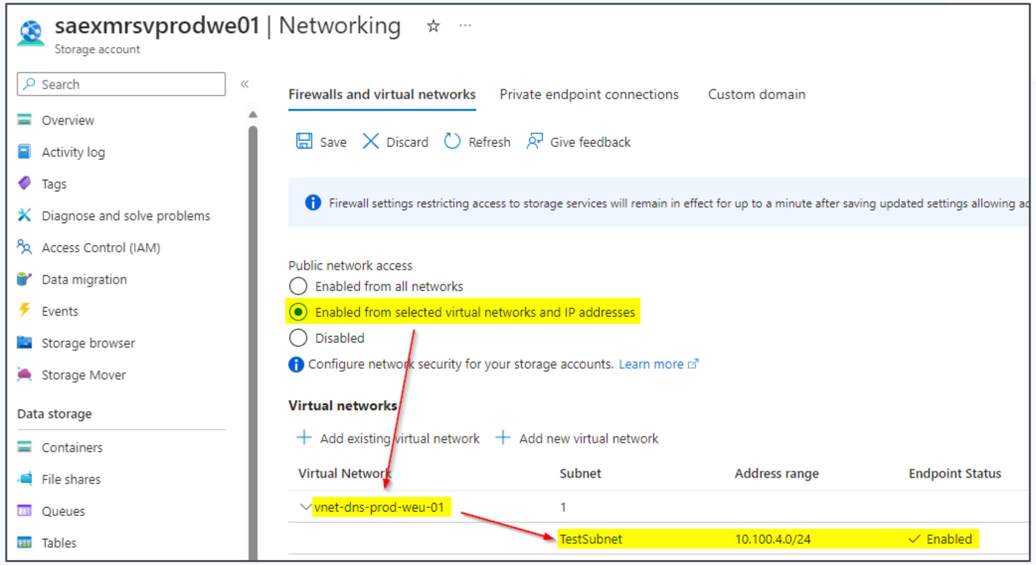
Azure Service Endpoints

Azure Service Endpoints

Overview

ServiceTags_Public_20230925.json

- 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.
- Effective Route → nextHopType = `VirtualNetworkServiceEndpoint`
- An optimized route over the **Azure Backbone** network.
- Goal: Secure your **critical** Azure service resources.
- Without needing a **public IP** address on the VNet.



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

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

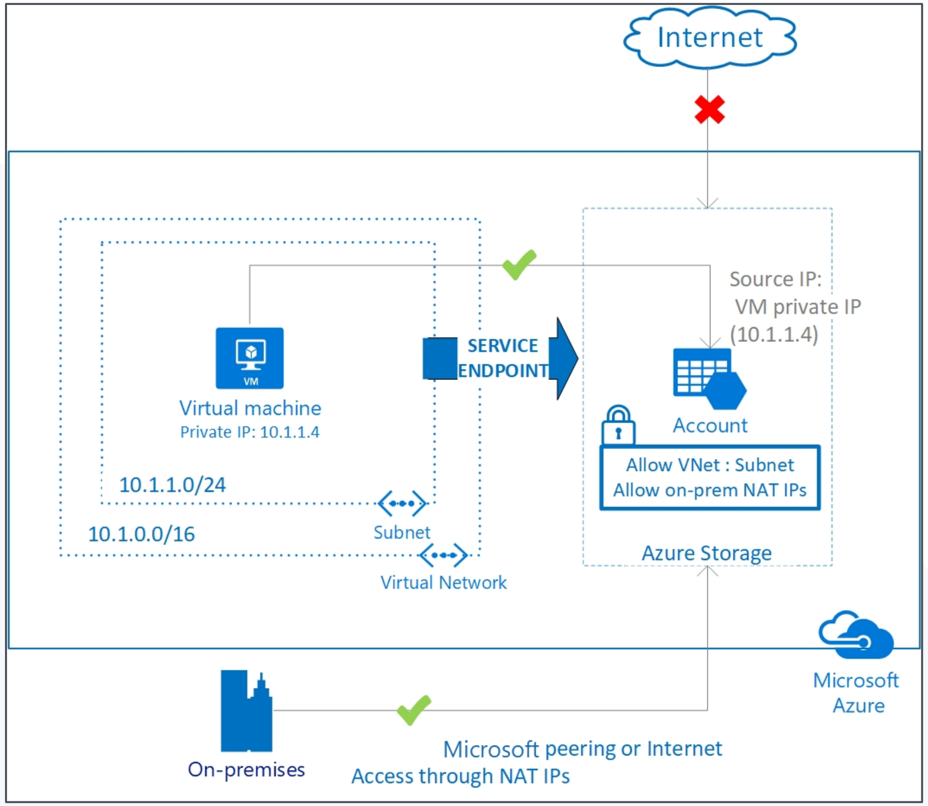
Virtual Network	Subnet	Address range	Endpoint Status
vnet-dns-prod-weu-01	1		
	TestSubnet	10.100.4.0/24	✓ Enabled

Azure Service Endpoints

What are the main **benefits** & **limitations** of Azure Service Endpoints?

- **Benefits:**
  - No extra **costs** for using service endpoints.
  - Improved **security** for your Azure service resources.
  - Optimal **routing** for Azure service traffic from your VNet.
  - Simple to **set up** with less management overhead.
  - Switches from **public** `IPv4` to **private** `IPv4` addresses.
  - **DNS entries** for Azure services remain the **same**.
  - NSGs can be used to block **outbound** traffic (*Service Tags*).

- **Limitations:**
  - Only available for **certain** Azure Services & Regions → List
  - Cannot be used for traffic from **on-premises** to Azure.
  - Allow public (NAT) **client IP** addresses from on-premises.
  - Azure service using Azure **public IP** addresses will stop **working**.
  - Certain Azure services can be allowed based on the **trusted services** list.



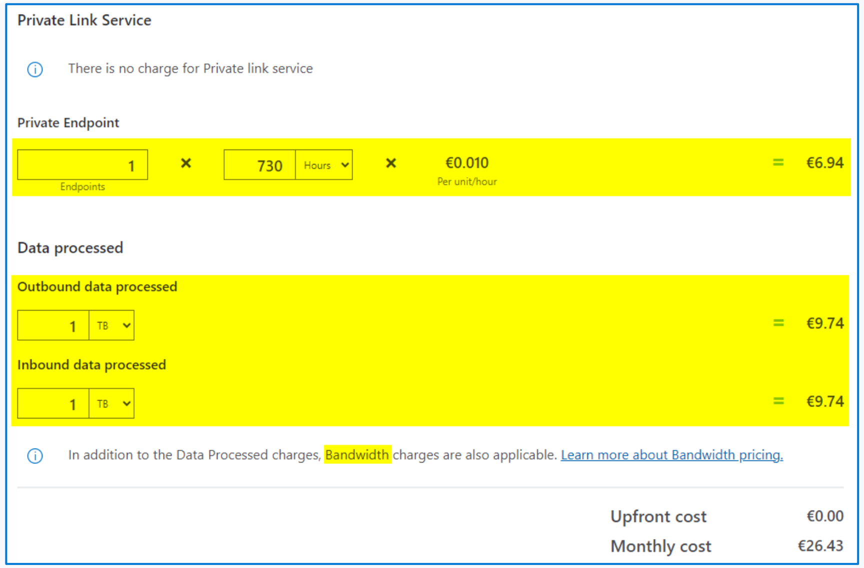
Provide a <u>secure</u> connectivity to Azure services using **<u>Private</u>** Endpoints on Azure.

Azure Private Endpoints

Azure Private Endpoint – Overview

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 Endpoints	×	730 Hours	×	€0.010 Per unit/hour	=	€6.94

Data processed

Outbound data processed

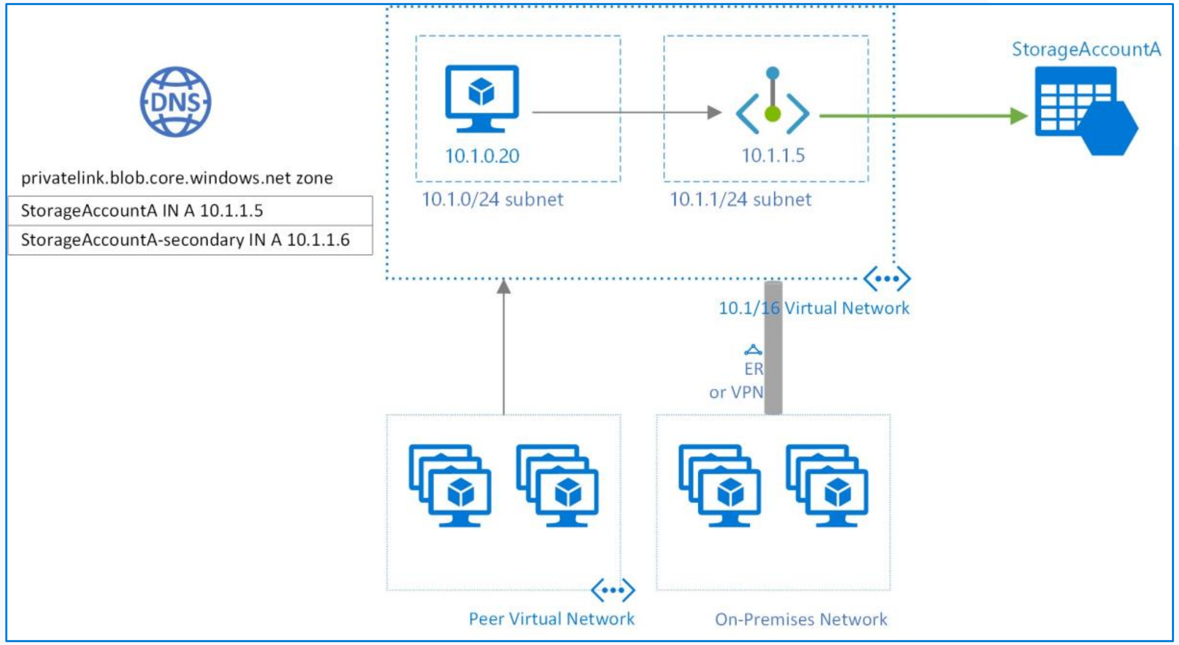
1 TB	=	€9.74

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



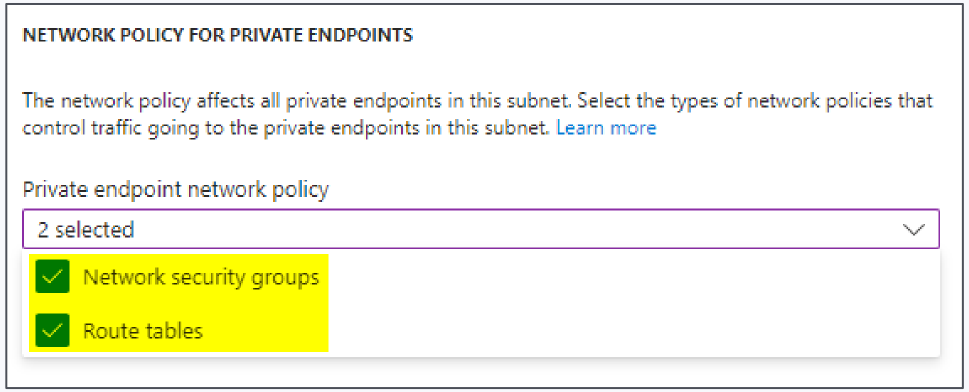
privatelink.blob.core.windows.net zone

StorageAccountA IN A 10.1.1.5
StorageAccountA-secondary IN A 10.1.1.6

Azure Private Endpoint

How to protect and secure your private endpoint?

- By default, network policies (**UDR**, **NSG**) are disabled for a subnet in a VNet.
- Network policy support must be **enabled** for the subnet.
- Once enable it affects all **private endpoints** within the subnet.
- Ensure connection requests **go through** an Azure Firewall/NVA.



NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. Select the types of network policies that control traffic going to the private endpoints in this subnet. Learn more

Private endpoint network policy

2 selected

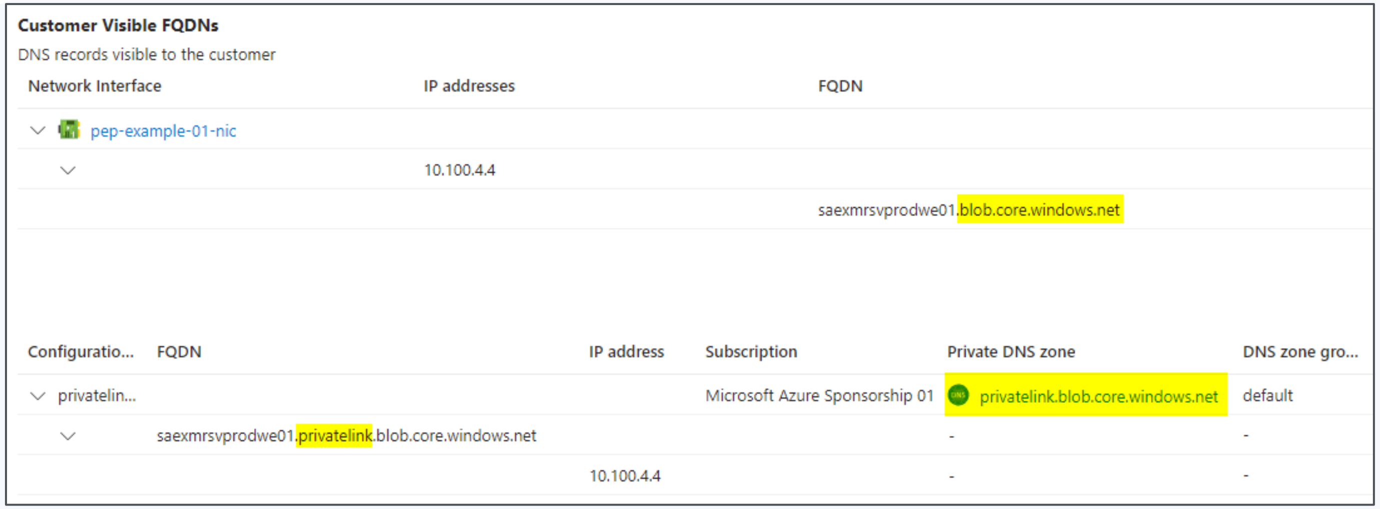
☑ Network security groups

☑ Route tables

Azure Private Endpoint – DNS

How to configure DNS if you are using private endpoints?

- Goal: Resolve the private endpoint IP address to the FQDN
- Azure Services have **already** a **DNS configuration** for a public endpoint. → Must be **overridden**!
- NIC associated contains the **information** to configure your DNS.
- NIC information includes **FQDN** and private **IP addresses** for the Azure Private Link.
- Recommend to **integrate** your private endpoint using a **private DNS zone**.

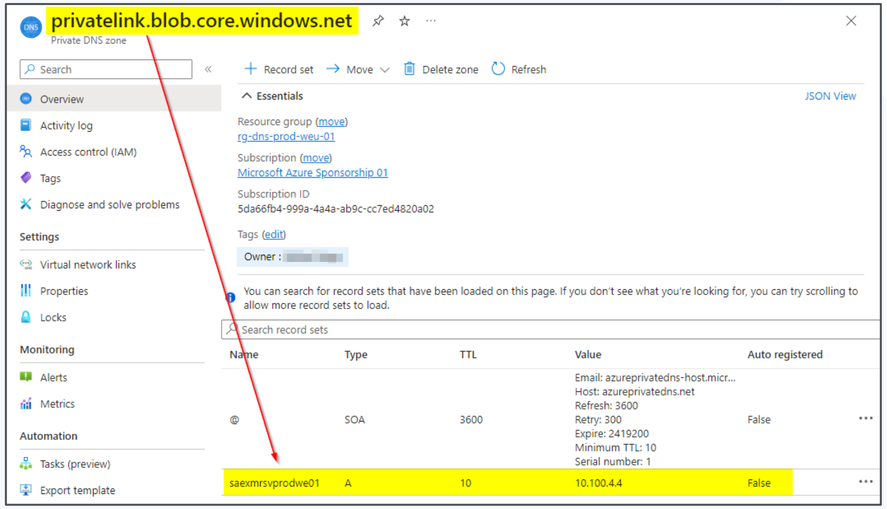


Customer Visible FQDNs

DNS records visible to the customer

Network Interface	IP addresses	FQDN
pep-example-01-nic		
	10.100.4.4	
		saexmrsvprodwe01.blob.core.windows.net

Configuratio...	FQDN	IP address	Subscription	Private DNS zone	DNS zone gro...
privatelin...			Microsoft Azure Sponsorship 01	privatelink.blob.core.windows.net	default
	saexmrsvprodwe01.privatelink.blob.core.windows.net			-	-
		10.100.4.4		-	-



privatelink.blob.core.windows.net

Private DNS zone

Resource group (move)
rg-dns-prod-weu-01

Subscription (move)
Microsoft Azure Sponsorship 01

Subscription ID
5da66fb4-999a-4a4a-ab9c-cc7ed4820a02

Tags (edit)
Owner : [redacted]

You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load.

Search record sets

Name	Type	TTL	Value	Auto registered
@	SOA	3600	Email: azureprivatedns-host.micr... Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1	False
saexmrsvprodwe01	A	10	10.100.4.4	False

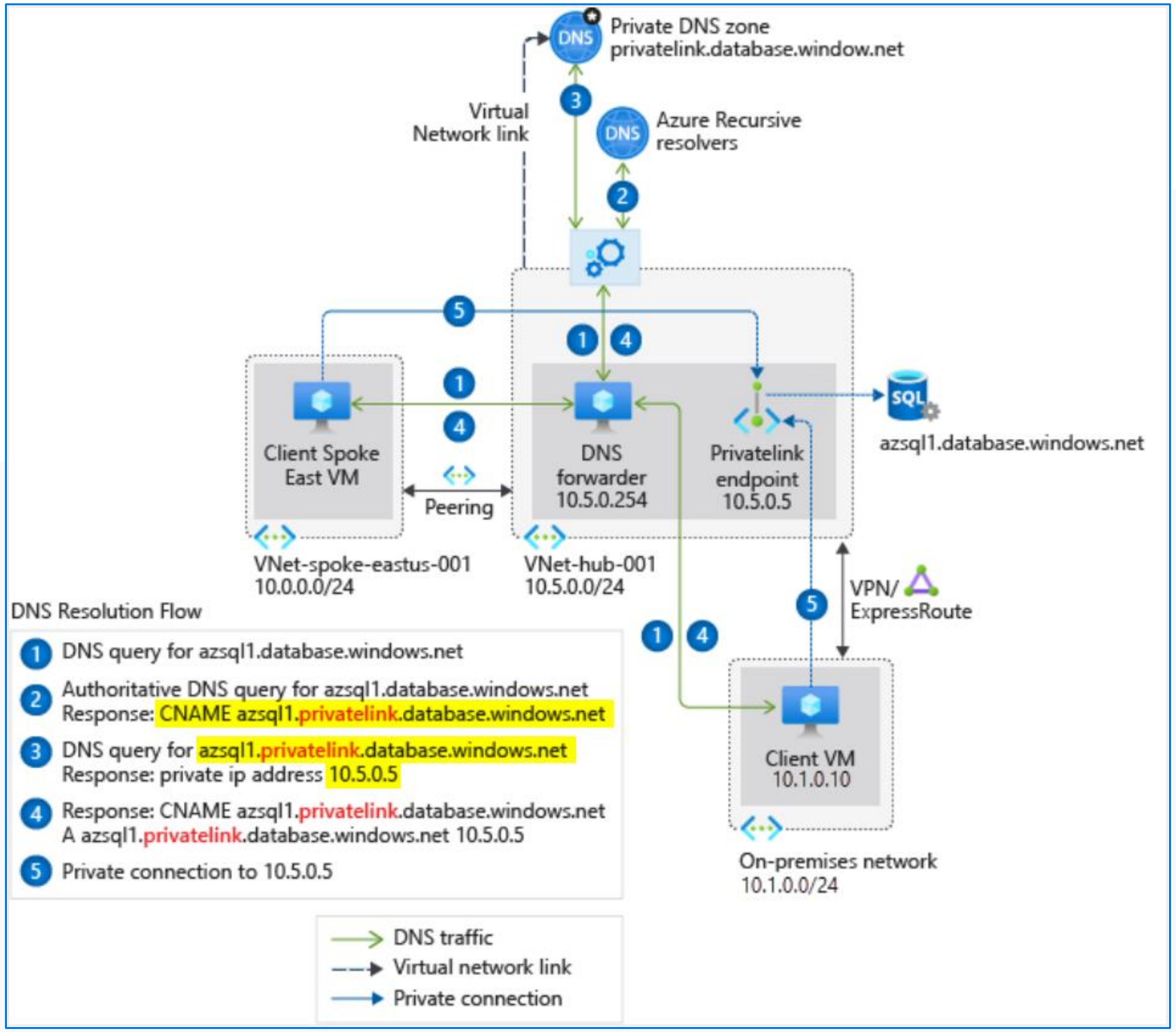
Azure Private Endpoint – Name Resolution

How does name resolution work behind the scenes?

- Options to configure your DNS settings for private endpoints:
  - Host file (only for testing)
  - Private DNS Zone
  - DNS Forwarder (DNS Server)
- Azure creates a CNAME on the **public DNS**. → Redirects the resolution to the **private domain** name.
  - A → [*name*].blob.core.windows.net
  - CNAME → [*name*].**privatelink**.blob.core.windows.net
  - IP address → 10.100.4.4
- Your applications do not need to change the **connection URL**.
- When resolving to a **DNS** service, the DNS server will **resolve** to your **private endpoints**.

Azure Private Endpoint – DNS Query Process

Scenarios of DNS resolution.



DNS Resolution Flow

1. DNS query for azsql1.database.windows.net
2. Authoritative DNS query for azsql1.database.windows.net
   Response: CNAME azsql1.privatelink.database.windows.net
3. DNS query for azsql1.privatelink.database.windows.net
   Response: private ip address 10.5.0.5
4. Response: CNAME azsql1.privatelink.database.windows.net
   A azsql1.privatelink.database.windows.net 10.5.0.5
5. Private connection to 10.5.0.5

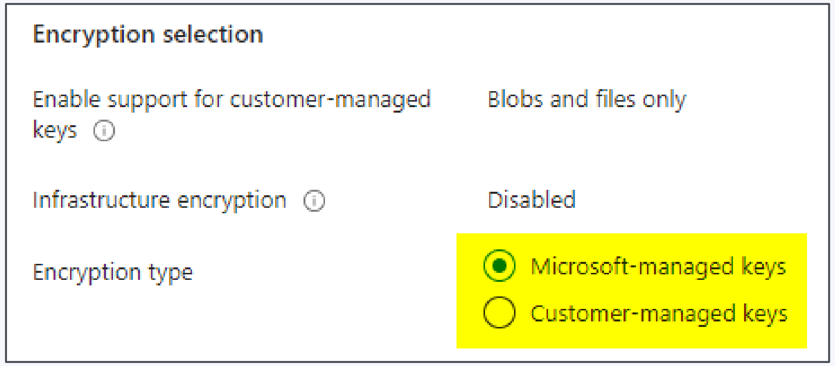
Additional services to secure your application workloads on Azure

General Azure Security Resources

Azure Key Management

Focus data protection on Azure using key management.

- Keys used for Azure Data Encryption **at rest** on certain Azure resources.
- Encryption keys can be either “*platform-managed*” (**PMK**) or “*customer-managed*” (**CMK**).
- By default, Azure encrypts storage account data at rest (managed **by Microsoft**).
- Customers do not **interact** with PMKs. → 256-bit AES (FIPS 140-2 compliant)
- CMK stored in a **key vault** with full access by the customer.
- **BYOK** scenarios are supported as well (Link) using HSM.
- Recommendation use **CMK** to protect data.



Encryption selection

Enable support for customer-managed keys ⓘ	Blobs and files only
Infrastructure encryption ⓘ	Disabled
Encryption type	● Microsoft-managed keys ○ Customer-managed keys

Azure Managed Identities

Connect to Azure resources securely without any credential management.

- Eliminate the need to manage **credentials** of the identity.
- Provide automatically an identity in Microsoft Entra ID for applications.
- Used when connecting to resources that support **Microsoft Entra authentication**.
- No need to **manage credentials**. → Credentials are not even accessible to customers.
- Can be used at no **extra cost**.
- For Azure or Arc-enabled workloads only!
- 2 types of managed identities:
  - `System-assigned` → Some Azure resources allow to enable a managed identity directly on the resource.
  - `User-assigned` → Create a managed identity as a standalone Azure resource

What are the essential takeaways of the session?

Key Takeaways

Key Takeaways

- ✓ Check with the Azure Infrastructure Team before the start!
- ✓ Use given Azure Landing Zone
- ✓ Start making a **plan** or network **design** (“*But do not Click!*”)
- ✓ **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
- ✓ Are there areas of **shared responsibilities** with other teams
- ✓ Secure Azure Services using the “*Networking*” section
  - ✓ Service Endpoints
  - ✓ Private Endpoints

PROFILE – Speaker

Stefan Rapp

Cloud Solution Architect (CSA) & Microsoft MVP

Xpirit Germany GmbH Xebia

Azure

Microsoft Most Valuable Professional

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

#AzureRocks 🤘 🧑‍🎤 🎸

E-Mail: info@blog.misterazure.com

Blog: https://blog.misterazure.com

GitHub: @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