



# Secure Cloud Workloads!

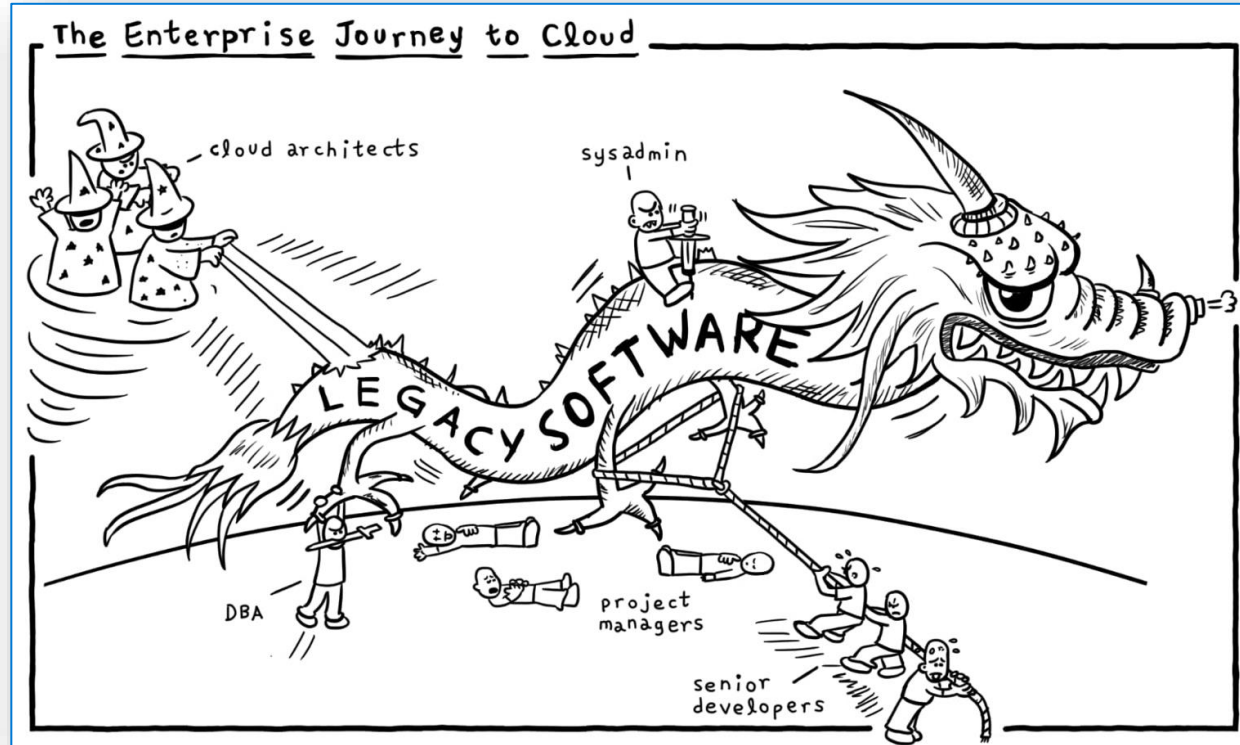
A Developer's Guide to Cloud Network Security



# 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
  - 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?

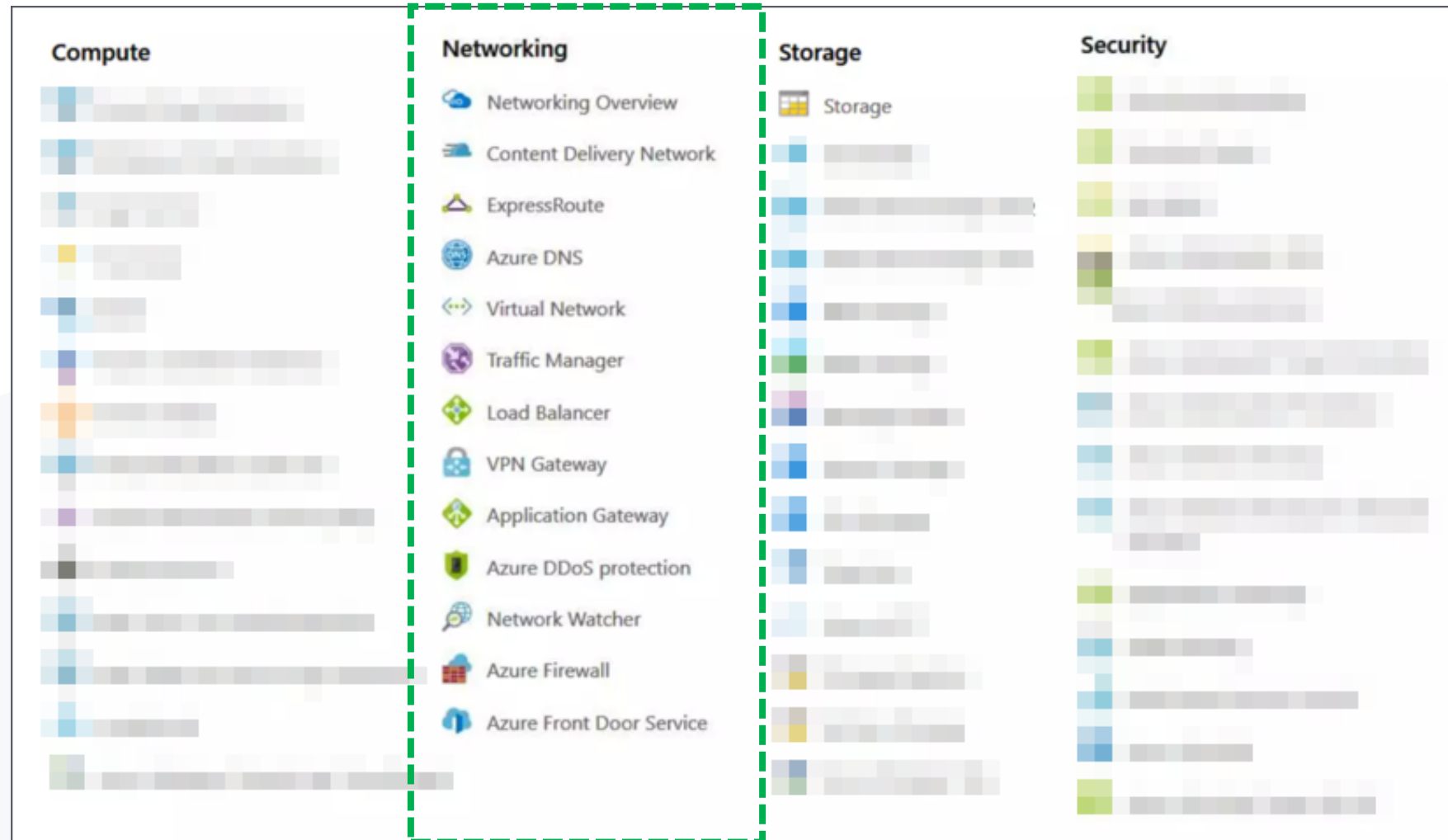
## Overview Azure Network Services





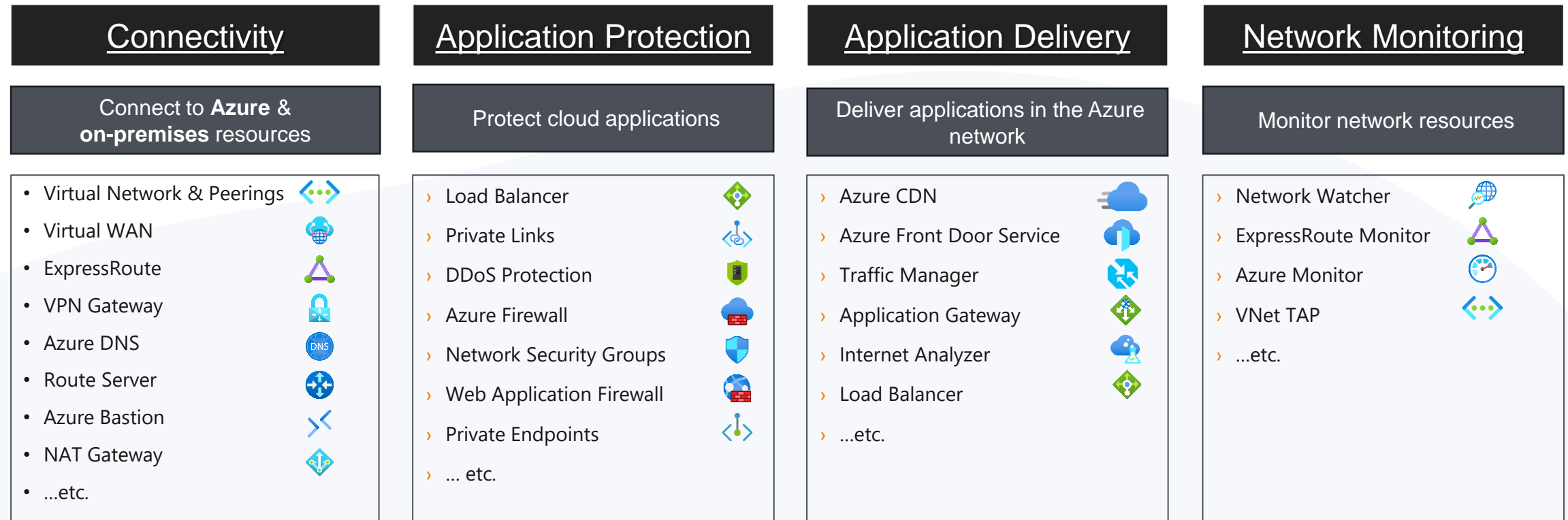
# Azure Network Services

Examples of Azure Network Services



# Azure Networking Services – Overview

Networking Capabilities to secure Azure Services



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



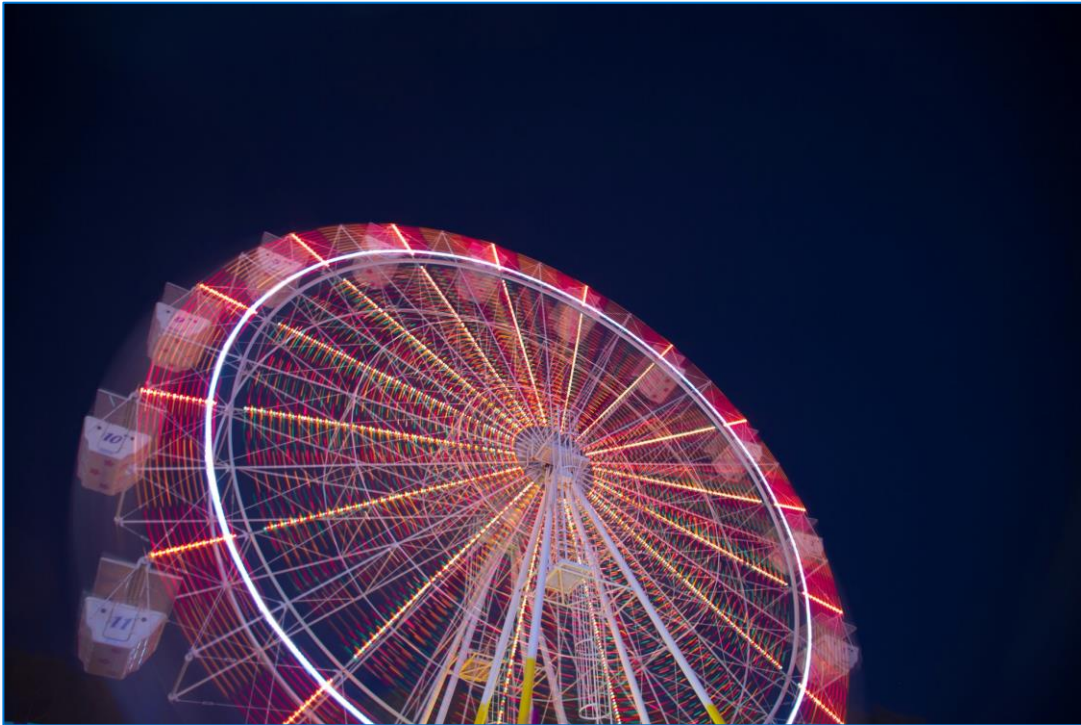
Azure Virtual Network (VNet) is the fundamental building block for the private network in Azure.

## Azure Virtual Network

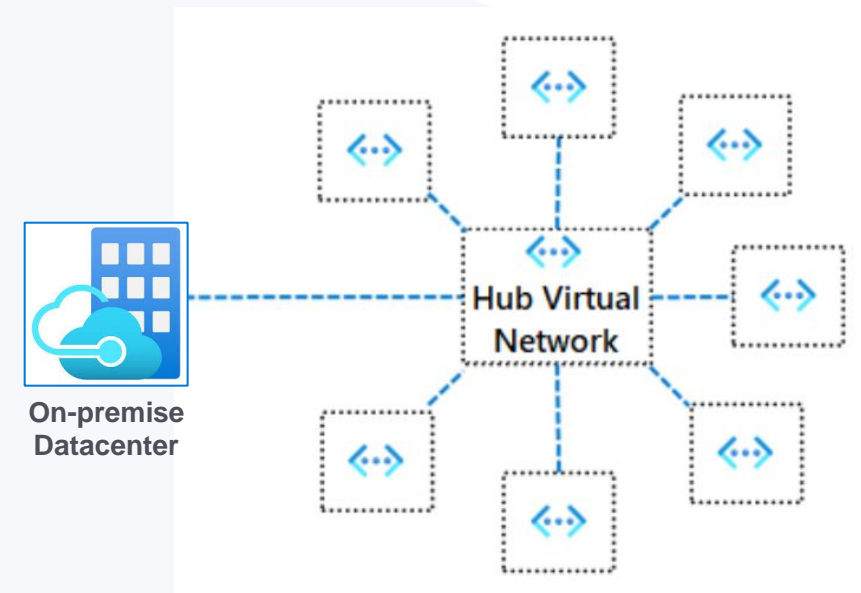


# “Hub & Spoke” Architecture

- **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>

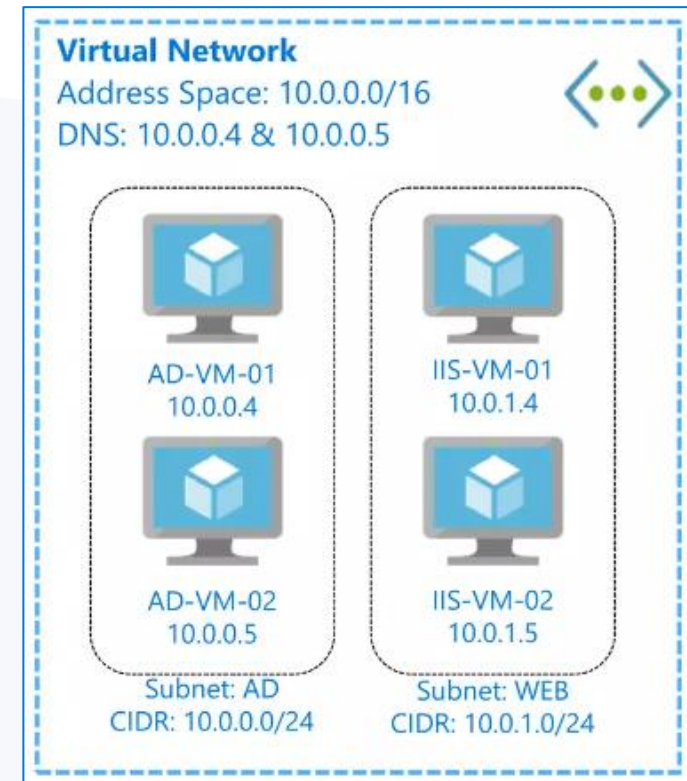




# Microsoft Azure VNets

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**



# Network Segmentation

Isolating resources in the network from each other

- Azure VNet → **/22**

([Subnet Calculator](#))

- 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>	/26 /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	<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>	/26 /26 /25 /24 /23 /22
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>	/26 /26 /25 /24 /23 /22
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>	/26 /26 /25 /24 /23 /22
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>	

## Create virtual network ...

Basics Security **IP addresses** Tags Review + create

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](#)

Add IPv4 address space | v

10.100.4.0/22 [Delete address space](#)

10.100.4.0 /22 (1,024 addresses) v

10.100.4.0 - 10.100.7.255 (1024 addresses)

+ Add a subnet

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**, not a product or a service!
- Its an approach in designing and implementing **security principles**.
- Affect 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 NSG 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**.

The screenshot displays the Azure portal interface for a Network Security Group (NSG) named 'vm-msix-nsg'. The left sidebar shows the navigation menu with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Inbound security rules, Outbound security rules, Network interfaces, Subnets, Properties, Locks, Monitoring, Alerts, and Diagnostic settings. The main content area shows the 'Essentials' tab with details about the NSG, including its location (West Europe), subscription ID, and associated resources. 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	AllowAzureLoadBalanc...	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





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

## Azure Service Endpoints

# Azure 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.
- Enables private IP addresses in the 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.



ServiceTags\_Public\_20230925.json

saexmrsvprodwe01 | Networking

Storage account

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

# Azure Service Endpoints

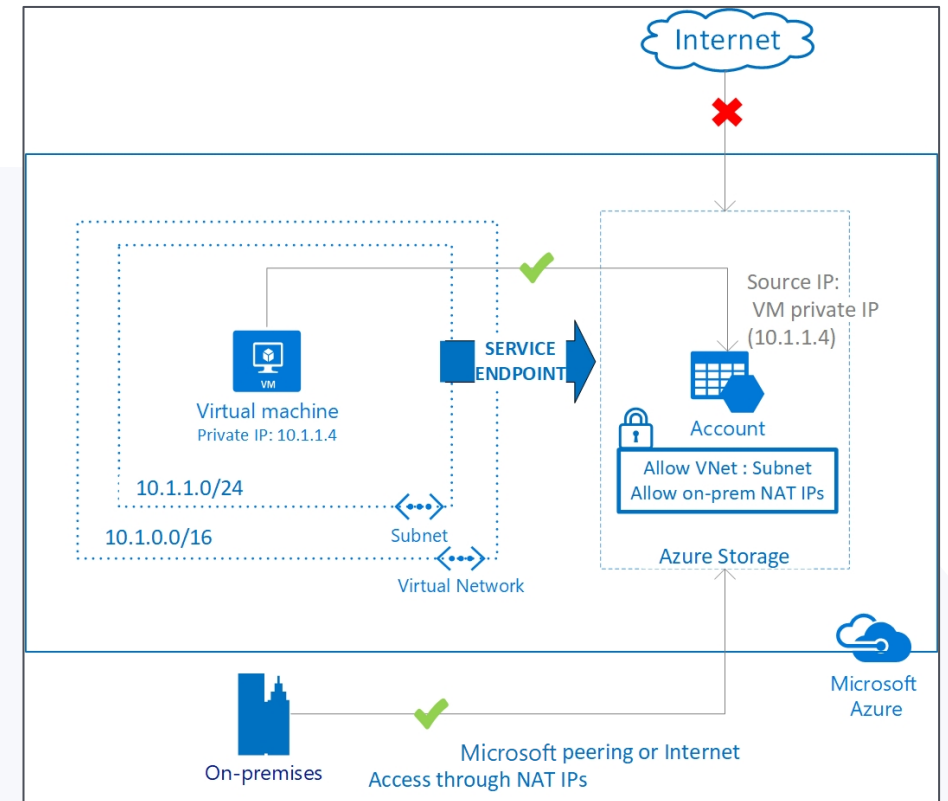
What are the main **benefits** & **limitations** of Azure Service Endpoints?

- **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:**

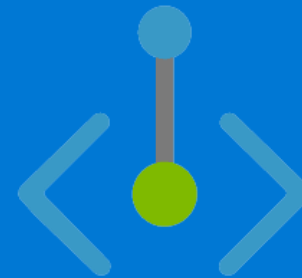
- Only available for **certain** Azure Services & Regions → [List](#)
- Cannot be used for traffic from **on-premises** to Azure.
- Allow public (NAT) **client IP** addresses from on-premises.
- Azure service using Azure **public IP** addresses will stop working.
- Certain Azure services can be allowed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





Provide a secure connectivity to Azure services using **Private** Endpoints on Azure.

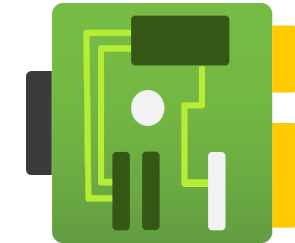
## Azure Private Endpoints








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

Data processed

Outbound data processed

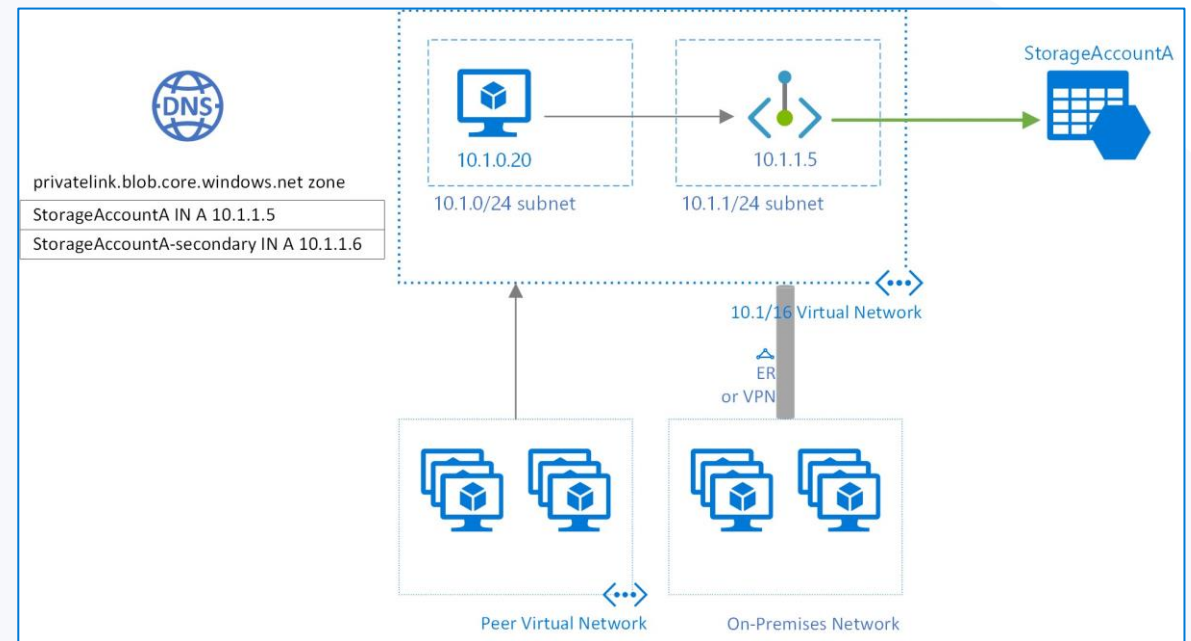
1	TB	=	€9.74
---	----	---	-------

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



# 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
<div>▼</div> <div> pep-example-01-nic</div>		
<div>▼</div>	10.100.4.4	
		saexmrsvprodwe01.blob.core.windows.net

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

privatelink.blob.core.windows.net					
Private DNS zone					
Search << + Record set → Move ▾ Delete zone Refresh					
Overview					
Essentials					
Resource group (move) rg-dns-prod-weu-01					
Subscription (move) Microsoft Azure Sponsorship 01					
Subscription ID 5da66fb4-999a-4a4a-ab9c-cc7ed4820a02					
Tags (edit)					
Owner :					
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.





What are the essential takeaways of the session?

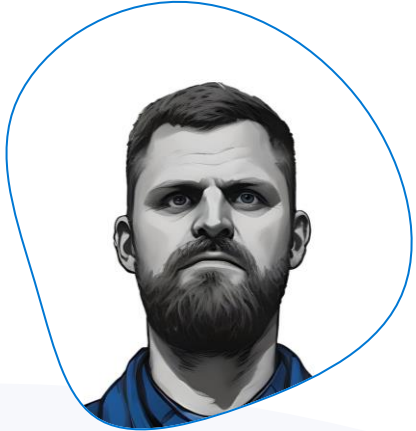
## Key Takeaways

# 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)*

Xpirit Germany GmbH

**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