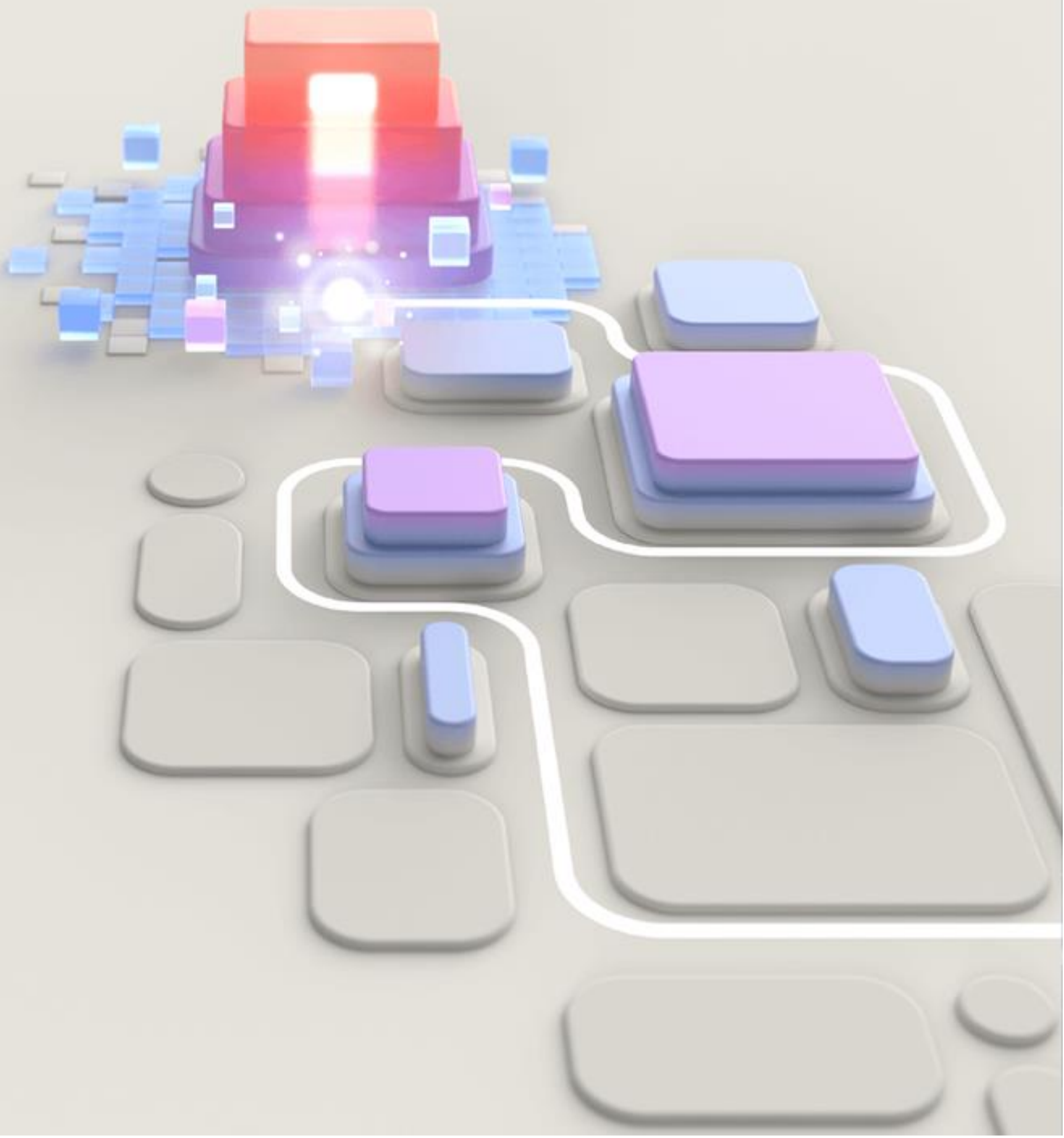
Microsoft

# AZ-700

# Designing and Implementing Azure Networking Solutions

Guten Morgen!



# Thomas Jäkel

brainymotion

Lead Trainer Cloud Infrastructure

Microsoft Certified Trainer since 1999

github.com/www42/az-700

Heidelberg

Physik

NT 4.0

AD

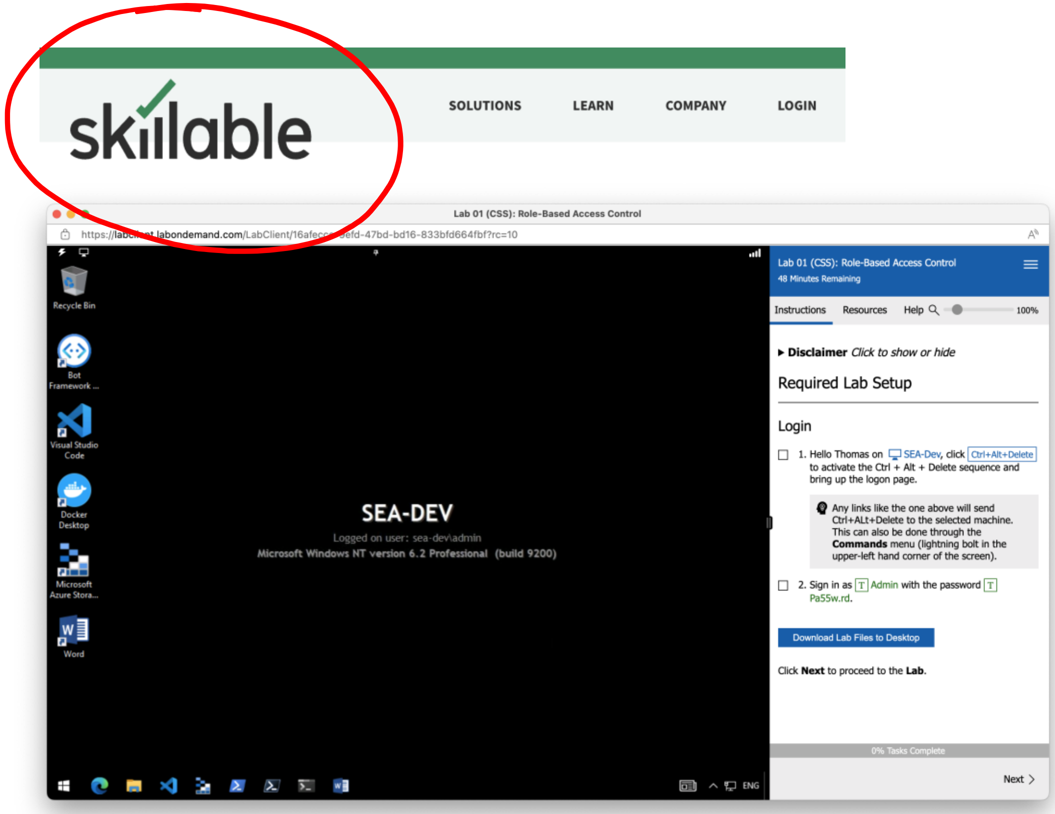
Exch

2011 Windows Azure

2013 ARM Azure

# AZ-700 Labs

- Login with Training Key
- Azure Subscription paid by Skillable
- SEA-DEV + Instructions
- 180 Days 10 x



Lab 01 (CSS): Role-Based Access Control

https://labclient.labondemand.com/LabClient/16afecc[illegible]efd-47bd-bd16-833bfd664fbf?rc=10

SEA-DEV

Logged on user: sea-dev\admin

Microsoft Windows NT version 6.2 Professional (build 9200)

Lab 01 (CSS): Role-Based Access Control

48 Minutes Remaining

▸ **Disclaimer** *Click to show or hide*

Required Lab Setup

Login

□ 1. Hello Thomas on SEA-Dev, click Ctrl+Alt+Delete to activate the Ctrl + Alt + Delete sequence and bring up the logon page.

Any links like the one above will send Ctrl+ALt+Delete to the selected machine. This can also be done through the **Commands** menu (lightning bolt in the upper-left hand corner of the screen).

□ 2. Sign in as T Admin with the password T Pa55w.rd.

Click **Next** to proceed to the **Lab**.

# AZ-700 Agenda

$9^{00} - 17^{00}$

$12^{00} - 13^{00}$

Module 01: Introduction to Azure Virtual Networks IPv6

Module 02: Designing and Implementing Hybrid Networking virtual GW vWAN

Module 03: Designing and Implementing Azure ExpressRoute

Module 04: Load balance non-HTTP(S) traffic in Azure ~~Basic~~ Standard LB

Module 05: Load balance HTTP(S) traffic in Azure App GW WAF FrontDoor

Lab 6 Module 06: Design and Implement Network Security Pa55w.rd1234

Lab 7 Module 07: Design and Implement private access to Azure Services EP

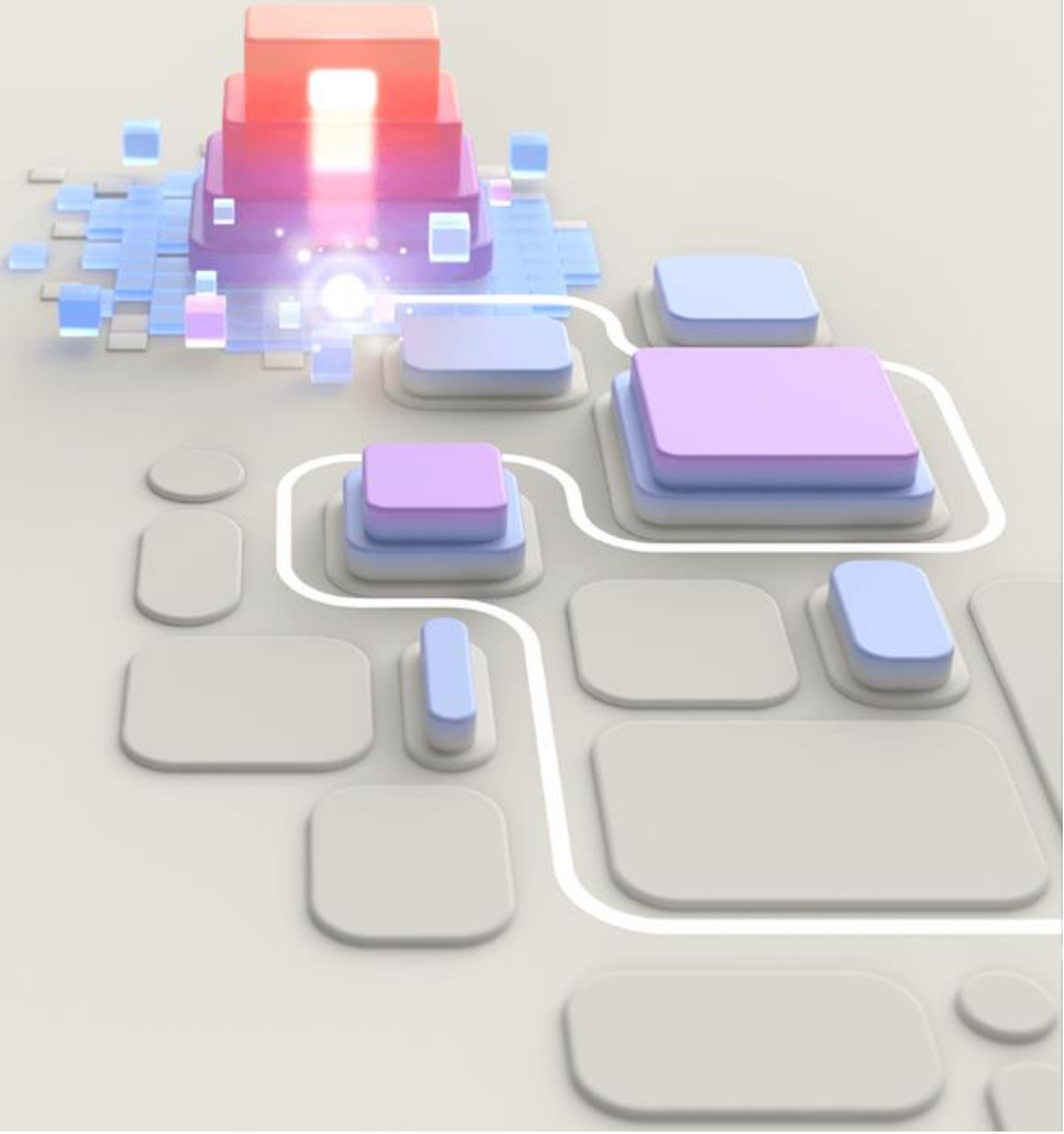
Lab 8 Module 08: Design and Implement Network Monitoring Network Watcher

LA KQL Lang

Microsoft

Mod 7

# AZ-700T00A
# Design and implement private access to Azure Services



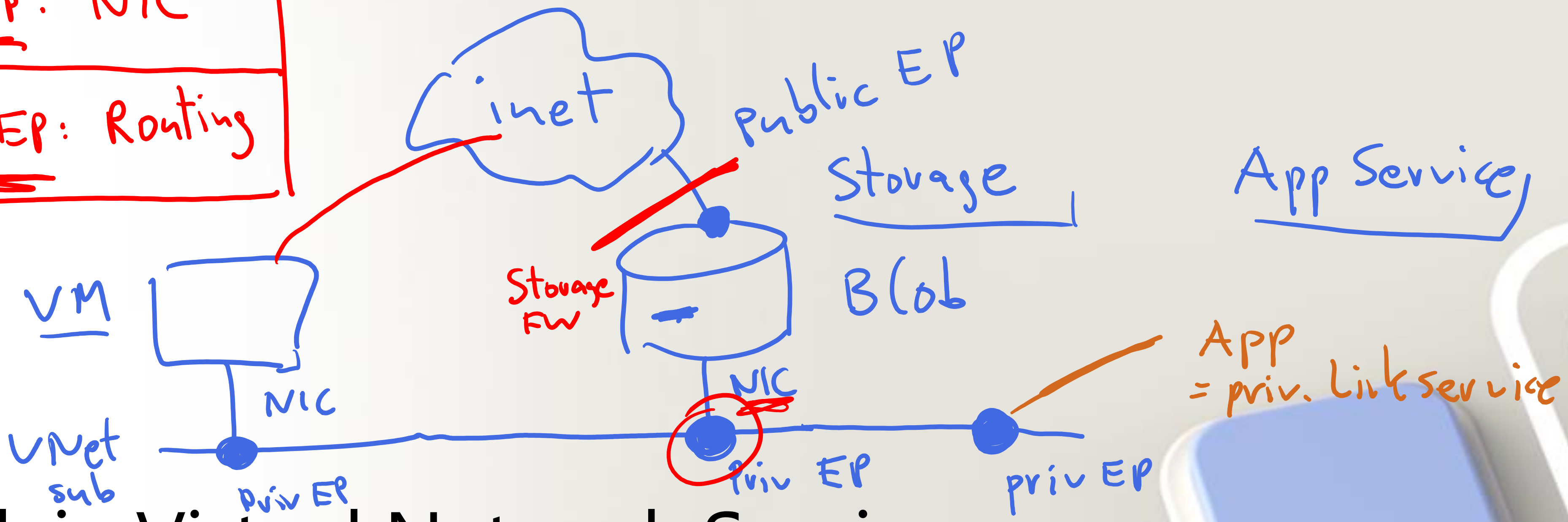
# Design and Implement Private Access to Azure Services

- Explain Virtual Network Service Endpoints
- Define Private Link Services and Private Endpoints
- Integrate Private Endpoint with DNS
- Exercise – Restrict network access to PaaS resources with virtual network service endpoints
- Exercise – Create an Azure Private Endpoint using Azure PowerShell

Lab

2. Private EP: NIC

1. Service EP: Routing



# Explain Virtual Network Service Endpoints

Azure Policies
eff

RBAC Owner Perm. Manament
perm. Data
eff

* NO

Network watcher

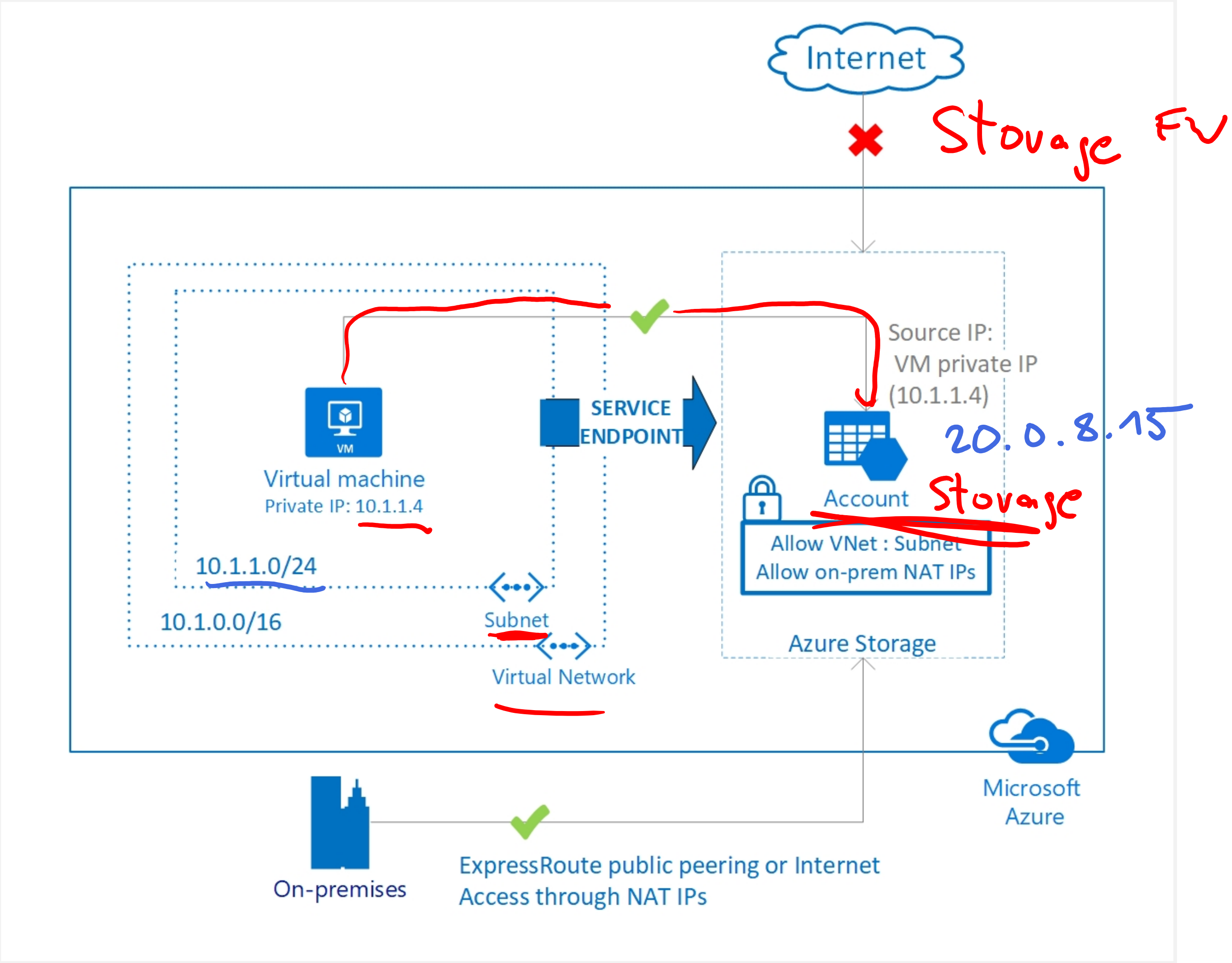
# Learning Objectives – Virtual Network Service Endpoints

- What is a Service Endpoint?
- Add Service Endpoints to a subnet
- Demonstration
- Learning Recap

# What is Service Endpoint?

Secure and direct connectivity to Azure services over an optimized route over the Azure backbone network Routing

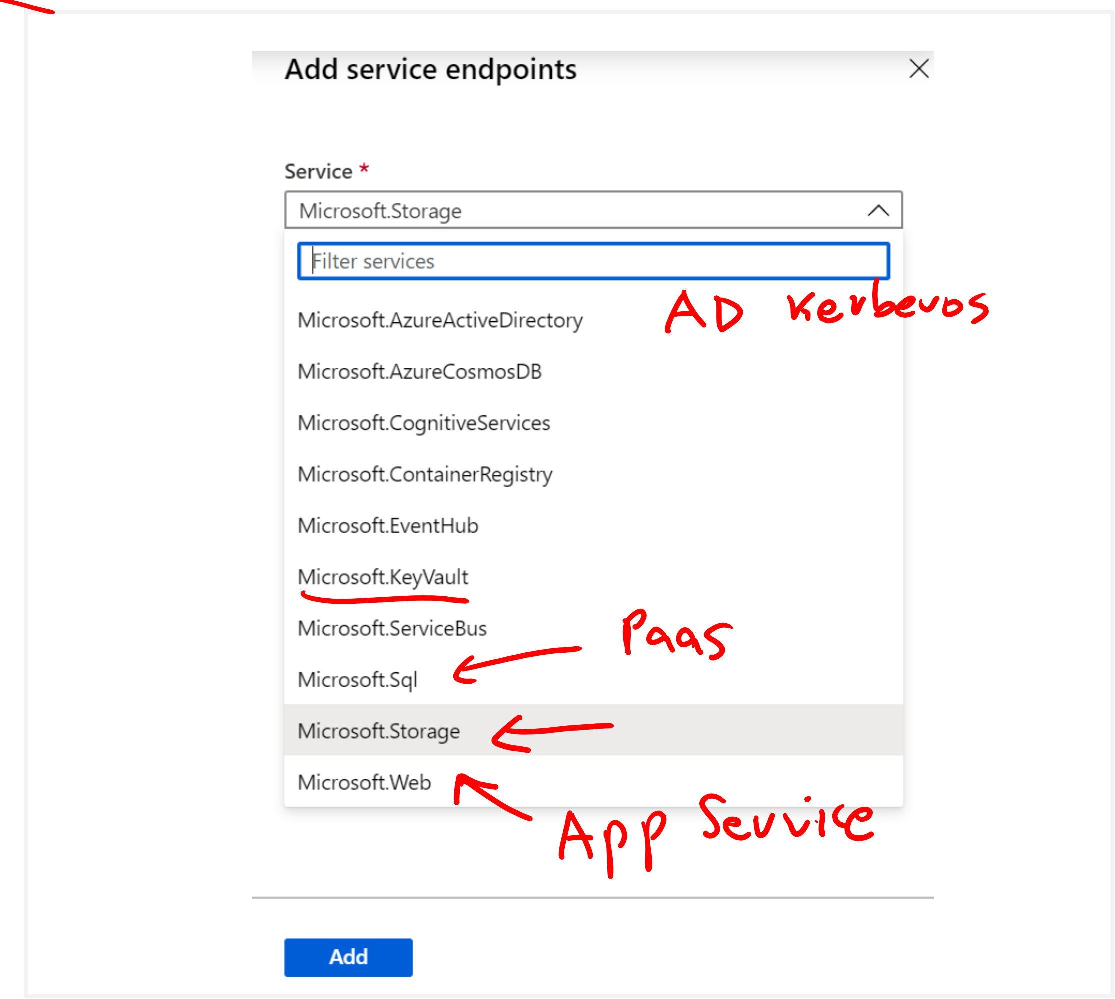
Optimal routing for Azure service traffic from your virtual network



# Add Service Endpoints to a subnet

There are many services that support endpoints

Adding service endpoints can take up to 15 minutes to complete



Add service endpoints

Service *

Microsoft.Storage

- Microsoft.AzureActiveDirectory
- Microsoft.AzureCosmosDB
- Microsoft.CognitiveServices
- Microsoft.ContainerRegistry
- Microsoft.EventHub
- Microsoft.KeyVault
- Microsoft.ServiceBus
- Microsoft.Sql
- Microsoft.Storage
- Microsoft.Web

AD kerberos

Paas

App Service

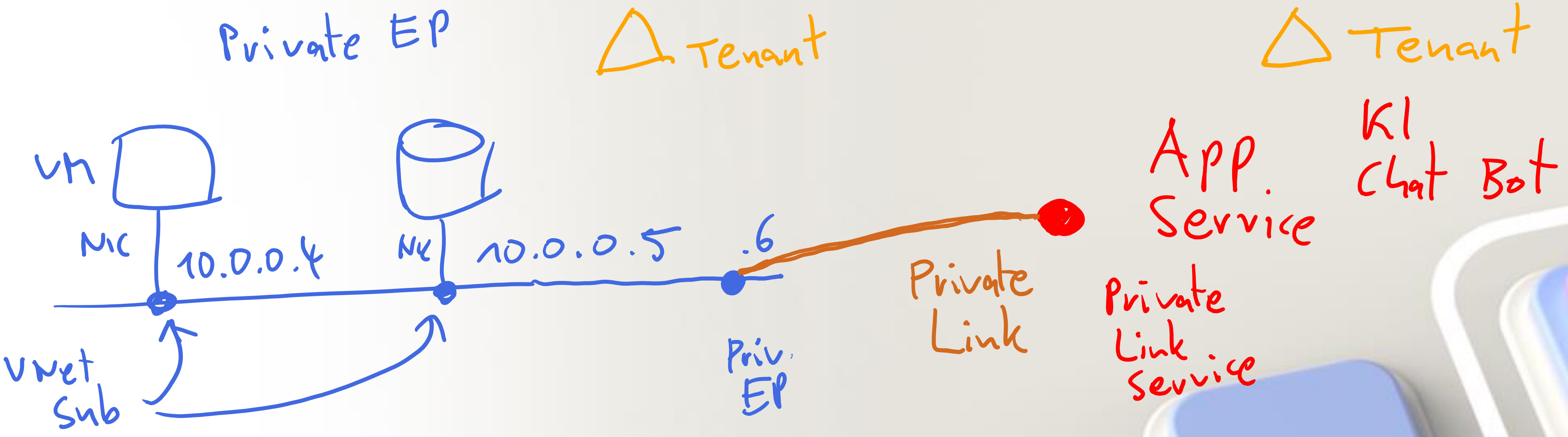
# Demonstration - Create a Service Endpoint service

- Create a virtual network with one subnet
- Add a subnet and enable a service endpoint
- Create an Azure resource and allow network access to it from only a subnet
- Deploy a virtual machine (VM) to each subnet
- Confirm access to a resource from a subnet
- Confirm access is denied to a resource from a subnet and the internet

# Learning Recap – Explain virtual network Service endpoints

Check your knowledge questions and additional study

Azure virtual network service endpoints | Microsoft Docs



# Define Private Link Services and Private Endpoints

# Learning Objectives – Private Link Services and Private Endpoints

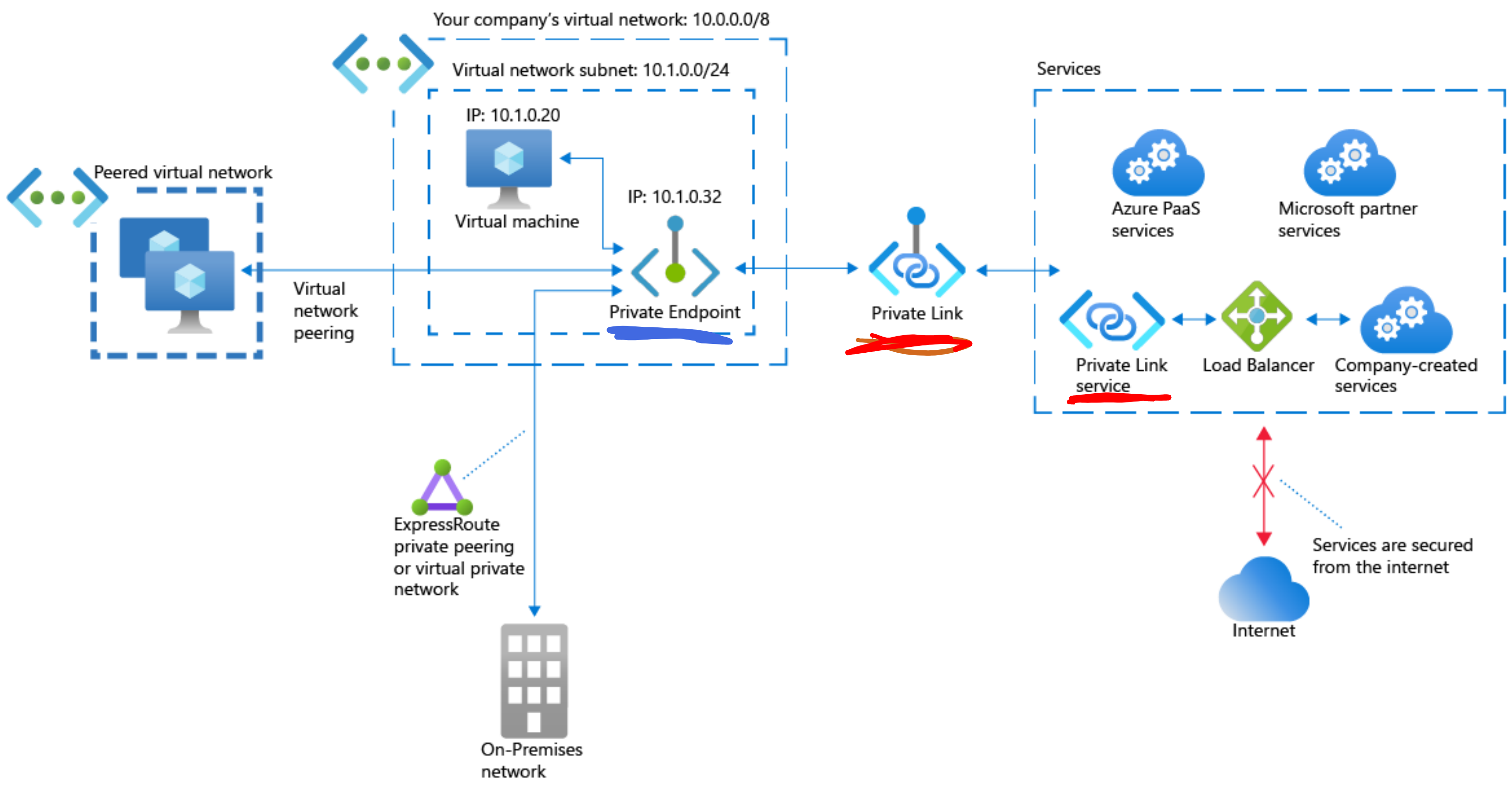
- What is Azure Private Link?
- What is Azure Private endpoint?
- What is Azure private Link service?
- Private Link service workflow
- Private endpoint properties
- Demonstration
- Learning Recap

# What is Azure Private Link ?

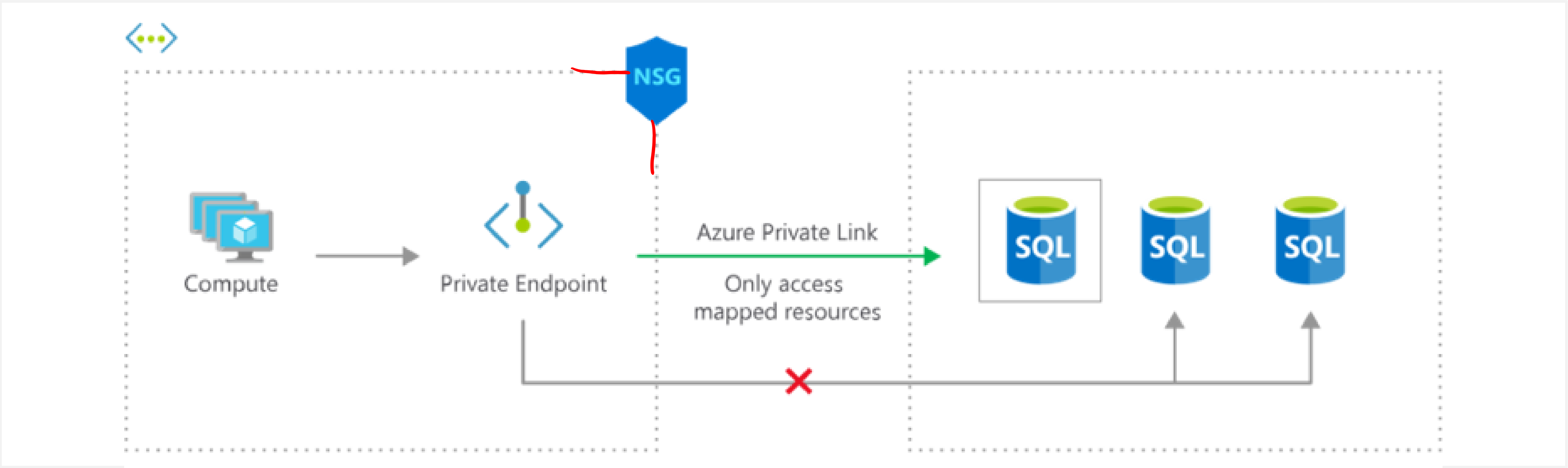
Integration with on-premises and peered networks

In the event of a security incident within your network, only the mapped resource would be accessible

Private connectivity to services on Azure. Traffic remains on the Microsoft network, with no public internet access



# What is Azure Private Endpoint ? = Network Interface

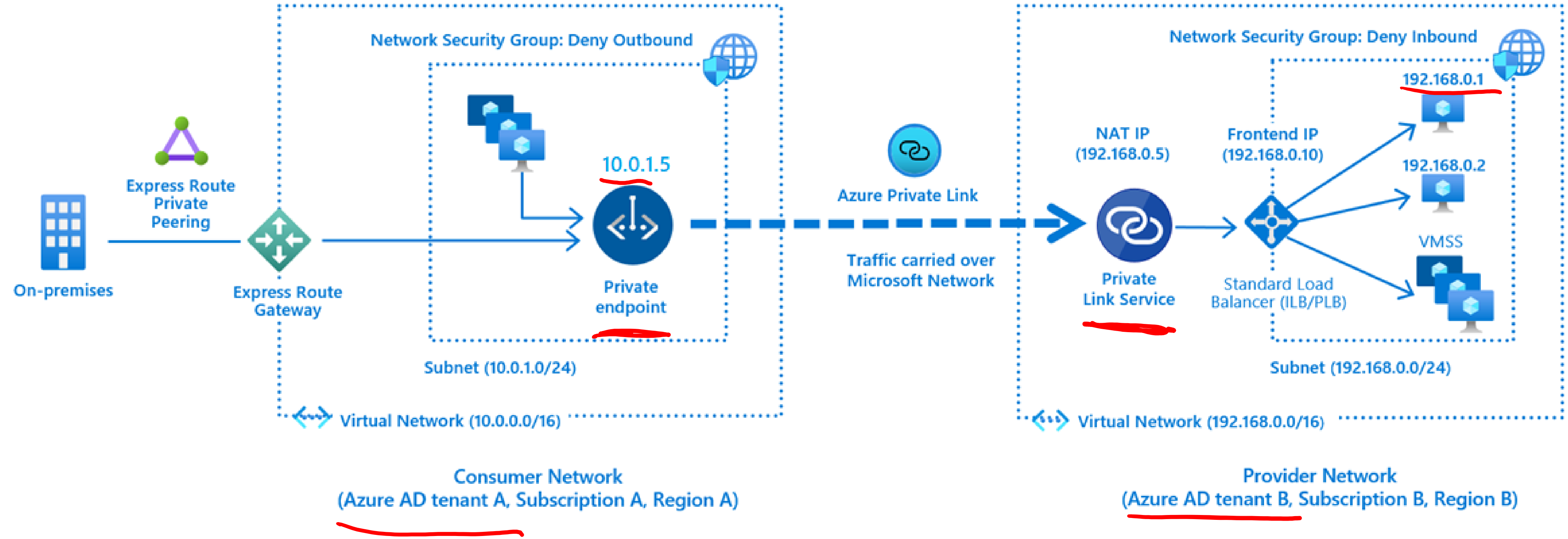


The Azure resource becomes, in a sense, a part of your virtual network.

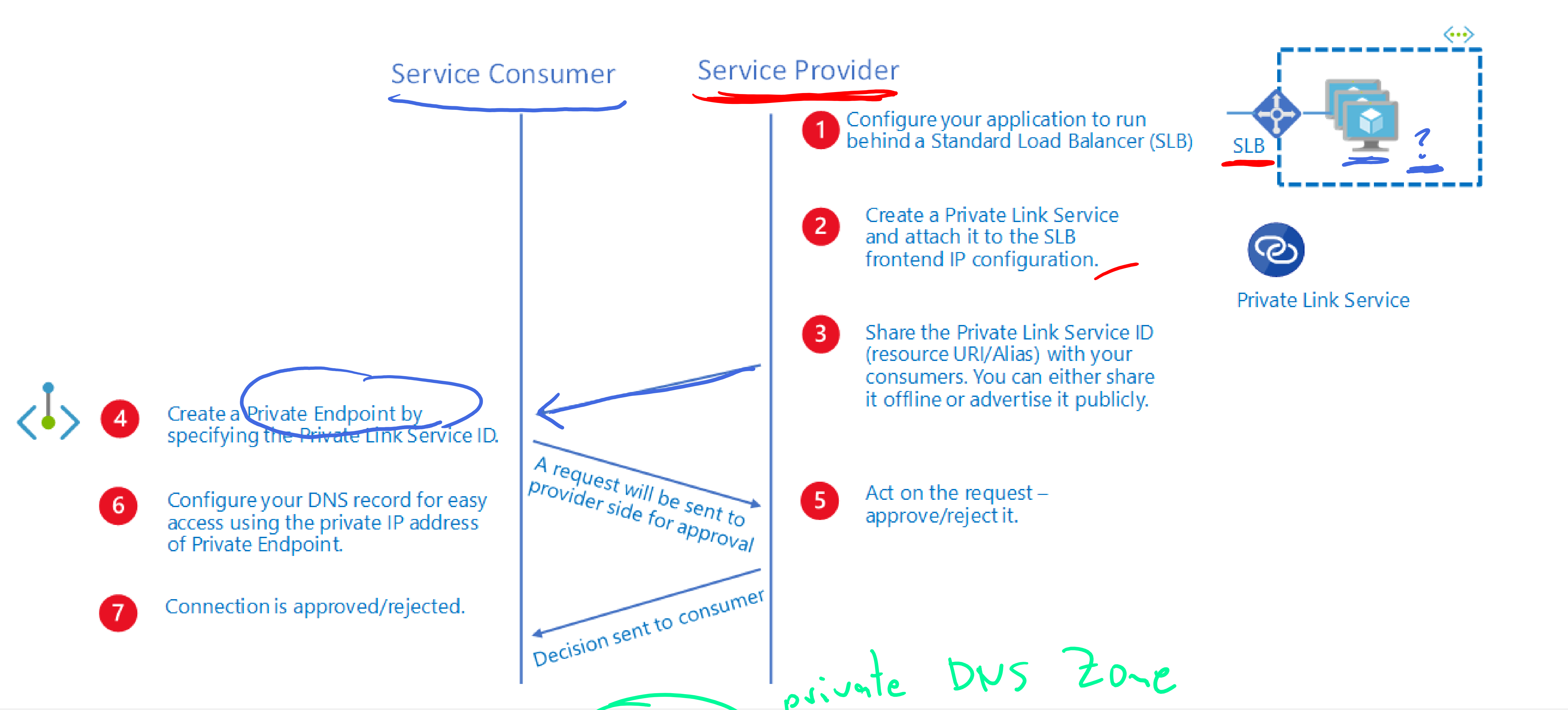
The connection to the resource now uses the Microsoft Azure backbone network instead of the public internet

Configure the Azure resource to no longer expose its public IP address, which eliminates that potential security risk.

# What is Azure Private Link service?


Network Security Group: Deny Outbound
10.0.1.5
Express Route Private Peering
On-premises
Express Route Gateway
Private endpoint
Subnet (10.0.1.0/24)
Virtual Network (10.0.0.0/16)
Consumer Network
(Azure AD tenant A, Subscription A, Region A)
Azure Private Link
Traffic carried over Microsoft Network
Network Security Group: Deny Inbound
192.168.0.1
NAT IP
(192.168.0.5)
Frontend IP
(192.168.0.10)
192.168.0.2
VMSS
Private Link Service
Standard Load Balancer (ILB/PLB)
Subnet (192.168.0.0/24)
Virtual Network (192.168.0.0/16)
Provider Network
(Azure AD tenant B, Subscription B, Region B)

# Private Link service workflow



Service Consumer

Service Provider

1 Configure your application to run behind a Standard Load Balancer (SLB)

2 Create a Private Link Service and attach it to the SLB frontend IP configuration.

3 Share the Private Link Service ID (resource URI/Alias) with your consumers. You can either share it offline or advertise it publicly.

4 Create a Private Endpoint by specifying the Private Link Service ID.

A request will be sent to provider side for approval

5 Act on the request – approve/reject it.

Decision sent to consumer

6 Configure your DNS record for easy access using the private IP address of Private Endpoint.

7 Connection is approved/rejected.

private DNS Zone

# Private Endpoint properties

| Property | Description |
|---|---|
| **Name** | A unique name within the resource group. |
| **Subnet** | The subnet to deploy and allocate private IP addresses from a virtual network |
| **Private Link Resource** | The private link resource to connect using resource ID or alias, from the list of available types. A unique network identifier will be generated for all traffic sent to this resource. |
| **Target subresource** | The subresource to connect. Each private link resource type has different options to select based on preference. |
| **Connection approval method** | Automatic or manual. Based on Azure role-based access control (Azure RBAC) permissions, your private endpoint can be approved automatically. If you try to connect to a private link resource without Azure RBAC, use the manual method to allow the owner of the resource to approve the connection. |
| **Request Message** | You can specify a message for requested connections to be approved manually. This message can be used to identify a specific request. |
| **Connection status** | A read-only property that specifies if the private endpoint is active. Only private endpoints in an approved state can be used to send traffic. Additional states available:<br>**Approved:** Connection was automatically or manually approved and is ready to be used.<br>**Pending**: Connection was created manually and is pending approval by the private link resource owner.<br>**Rejected**: Connection was rejected by the private link resource owner.<br>**Disconnected:** Connection was removed by the private link resource owner. The private endpoint becomes informative and should be deleted for cleanup. |

# Demonstration – Create a Private Link service

- Create a Private Link service that refers to your service
- Give Private Link access to your service or resource deployed behind an Azure Standard Load Balancer
- Users of your service have private access from their virtual network

# Learning Recap – Private Link and Private Endpoint

Check your knowledge questions and additional study

[What is Azure Private Link? | Microsoft Docs]

[What is an Azure Private Endpoint? | Microsoft Docs]

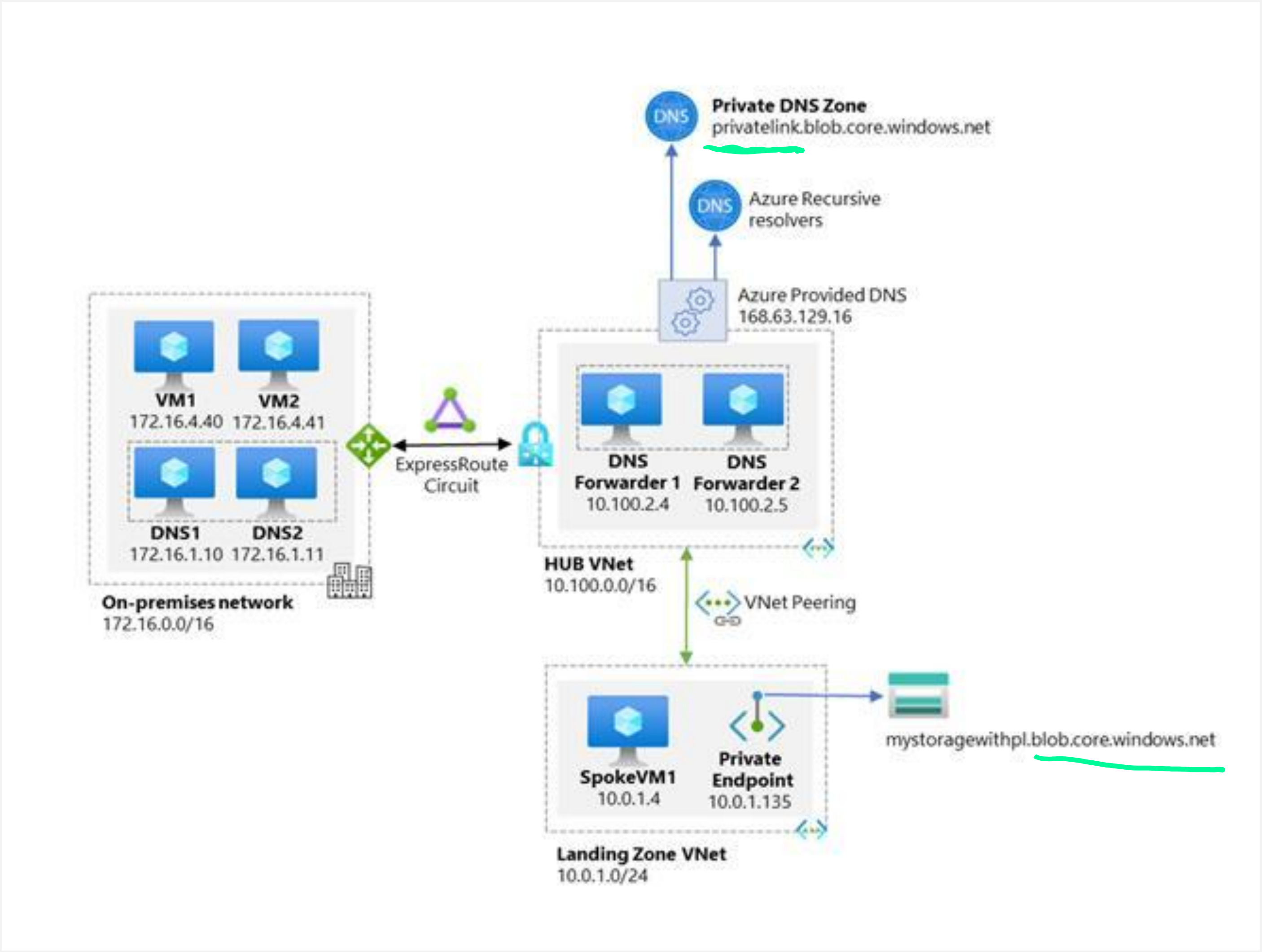
# Integrate Private Endpoint with DNS

# Learning Objectives – Integrate Private endpoint with DNS

- Azure Private Endpoint DNS configuration
- Azure services Private DNS zone configuration examples
- Virtual network workloads without custom DNS server
- On-premises workloads using Azure DNS Private Resolver
- Virtual network and on-premises workloads using a DNS forwarder
- Learning Recap

# Azure Private Endpoint DNS configuration

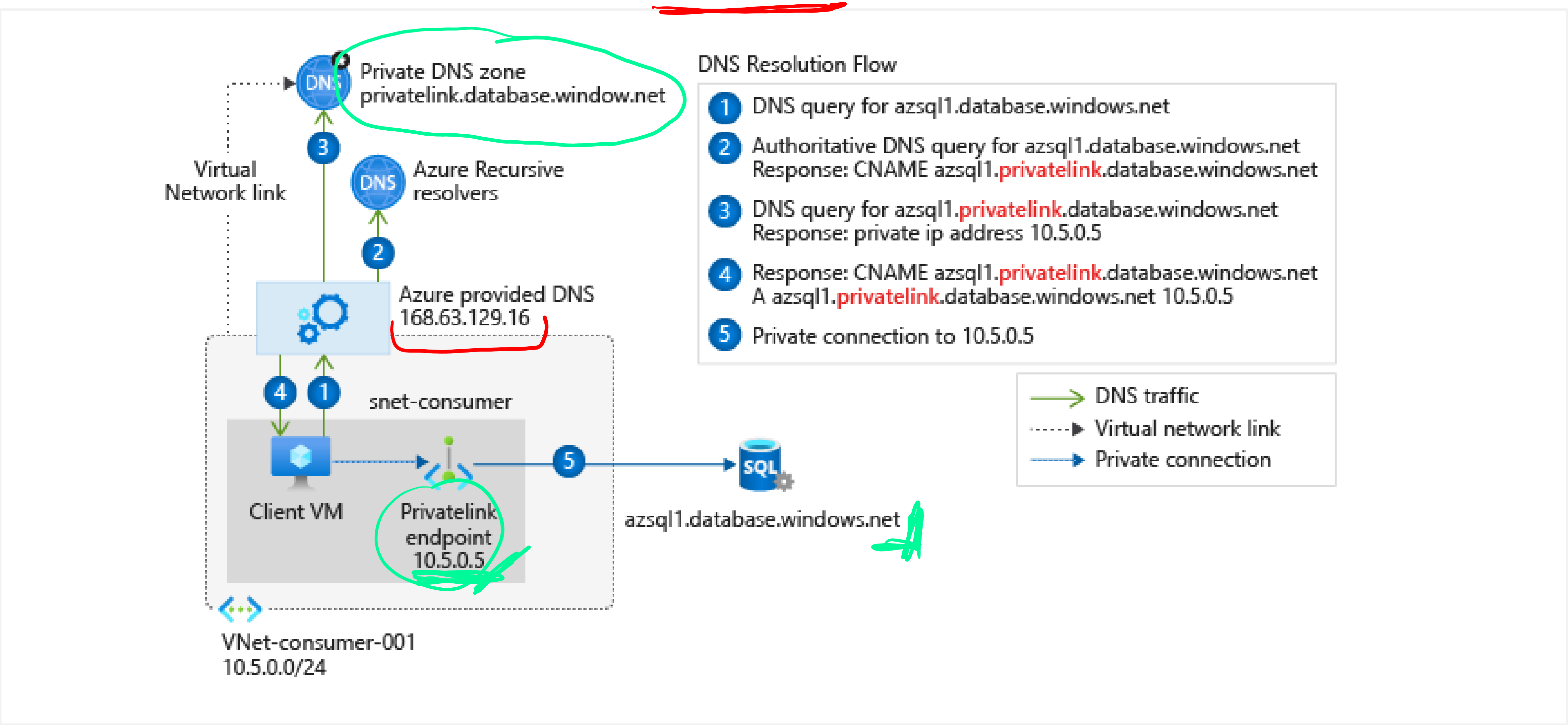
High-level architecture for enterprise environments with central DNS resolution and where name resolution for Private Endpoint resources is done via Azure Private DNS



# Azure services Private DNS zone configuration examples

| Private Link resource type / Subresource | Private DNS zone name |
|---|---|
| **Azure Automation / (Microsoft.Automation/automationAccounts) / Webhook, DSCAndHybridWorker** | privatelink.Azure-automation.net |
| **Azure SQL Database (Microsoft.Sql/servers) / sqlServer** | privatelink.database.windows.net |
| **Azure Synapse Analytics (Microsoft.Sql/servers) / sqlServer** | privatelink.database.windows.net |
| **Azure Synapse Analytics (Microsoft.Synapse/workspaces) / Sql** | privatelink.sql.Azuresynapse.net |
| **Storage account (Microsoft.Storage/storageAccounts) / Blob (blob, blob_secondary)** | privatelink.[Service].core.windows.net |

# Virtual network workloads without custom DNS server

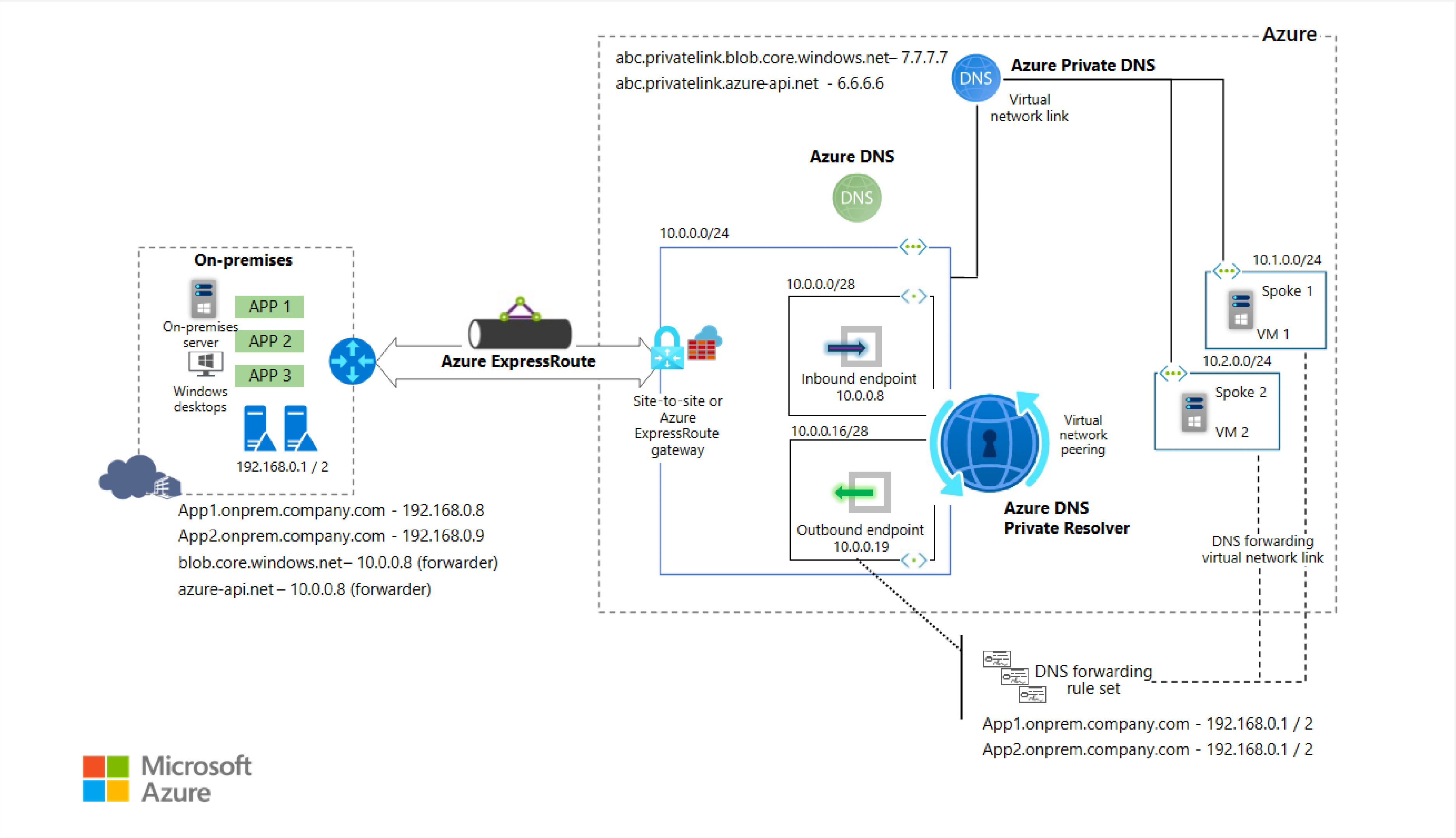


DNS Resolution Flow

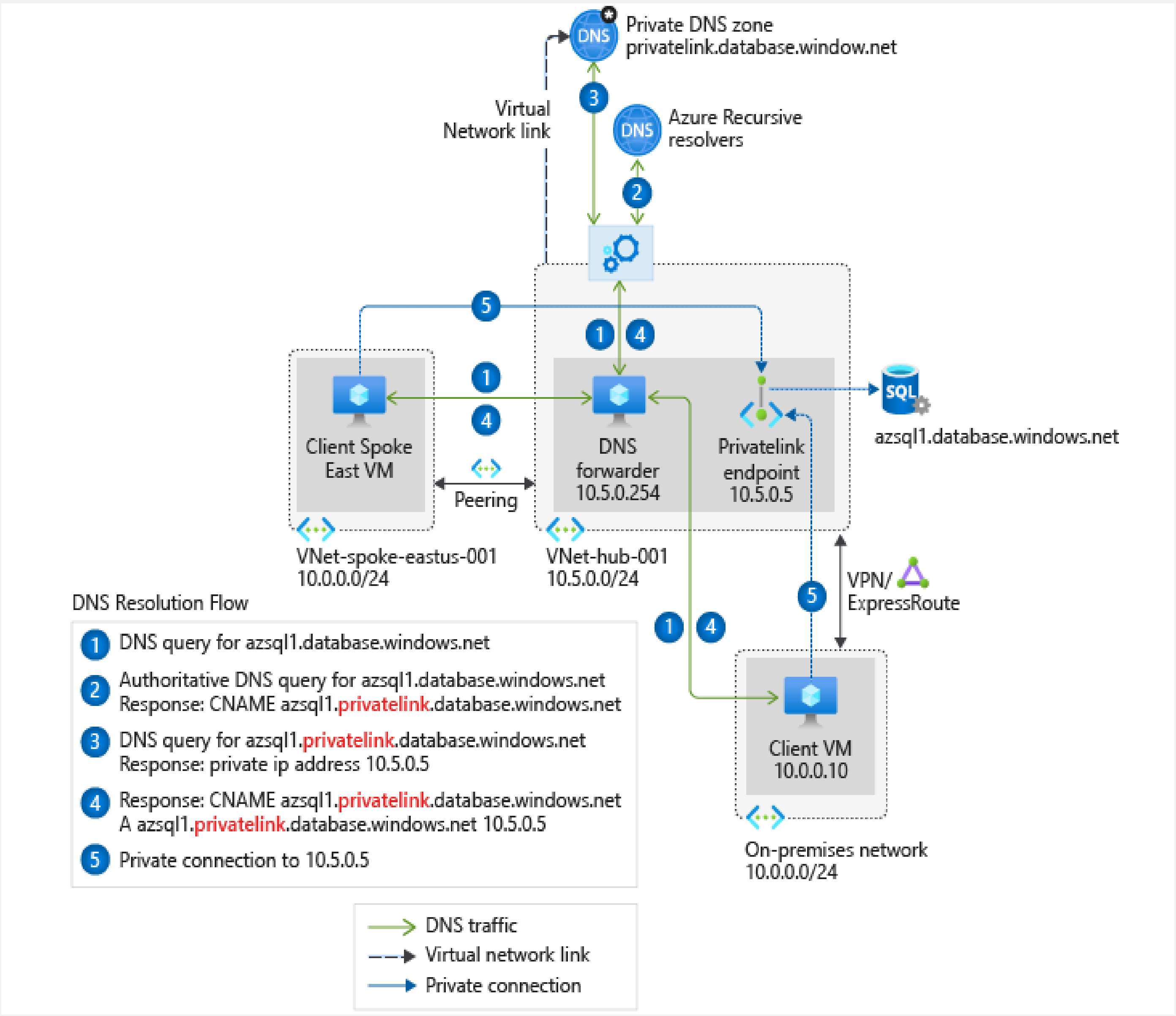
1. DNS query for azsql1.database.windows.net
2. Authoritative DNS query for azsql1.database.windows.net
   Response: CNAME azsql1.privatelink.database.windows.net
3. DNS query for azsql1.privatelink.database.windows.net
   Response: private ip address 10.5.0.5
4. Response: CNAME azsql1.privatelink.database.windows.net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

→ DNS traffic
······▶ Virtual network link
--▶ Private connection

# On-premises workloads using Azure DNS Private Resolver


Azure
abc.privatelink.blob.core.windows.net– 7.7.7.7
abc.privatelink.azure-api.net - 6.6.6.6
DNS
Azure Private DNS
Virtual network link
Azure DNS
DNS
10.0.0.0/24
10.0.0.0/28
Inbound endpoint 10.0.0.8
10.0.0.16/28
Outbound endpoint 10.0.0.19
Azure DNS Private Resolver
Virtual network peering
10.1.0.0/24
Spoke 1
VM 1
10.2.0.0/24
Spoke 2
VM 2
DNS forwarding virtual network link
On-premises
On-premises server
APP 1
APP 2
APP 3
Windows desktops
192.168.0.1 / 2
Azure ExpressRoute
Site-to-site or Azure ExpressRoute gateway
App1.onprem.company.com - 192.168.0.8
App2.onprem.company.com - 192.168.0.9
blob.core.windows.net– 10.0.0.8 (forwarder)
azure-api.net – 10.0.0.8 (forwarder)
DNS forwarding rule set
App1.onprem.company.com - 192.168.0.1 / 2
App2.onprem.company.com - 192.168.0.1 / 2
Microsoft Azure

# Virtual network and on-premises workloads using a DNS forwarder



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

# Learning Recap – Integrate Private Endpoint with DNS

Check your knowledge questions and additional study

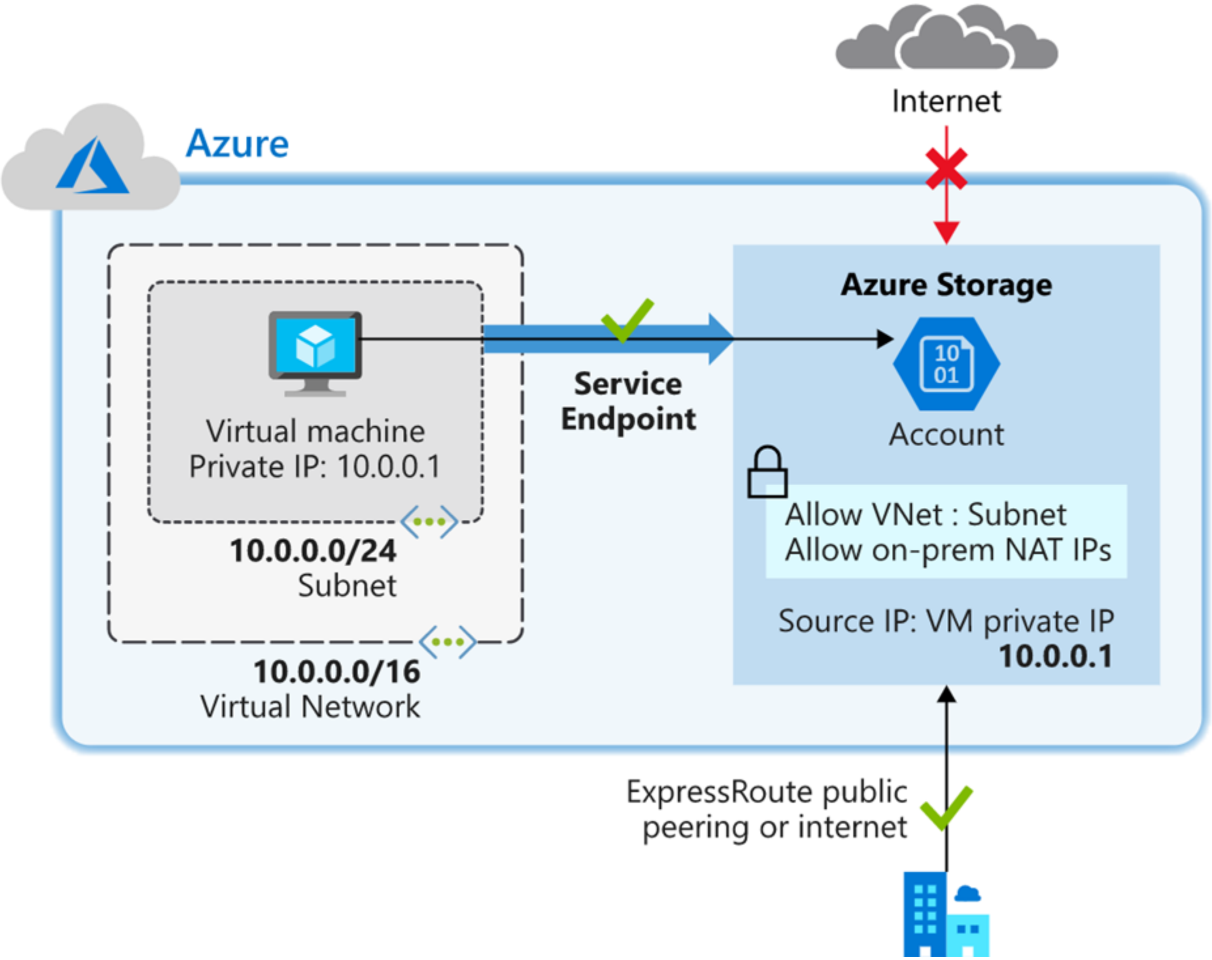
[Azure Private Endpoint DNS configuration | Microsoft Docs]

# Exercise - Restrict network access to PaaS resources with virtual network service endpoints

Lab 7 Teil 1

# Restrict network access to PaaS resources with virtual network service endpoints

- Create a virtual network
- Enable a service endpoint
- Restrict network access for a subnet
- Add additional outbound rules
- Allow access for RDP connections
- Restrict network access to a resource
- Create a file share in the storage account
- Restrict network access to a subnet
- Create virtual machines
- Confirm access to storage account
- Clean up resources



# Learning Recap – virtual network service endpoints

Check your knowledge questions and additional study

Azure virtual network service endpoints | Microsoft Docs

# Exercise - Create an Azure Private Endpoint using Azure PowerShell

Lab 7 Teil 2

# Create an Azure Private Endpoint using Azure PowerShell 7

Cloud Shell

module Az.* ✓

Task 1: Create a resource group

Task 2: Create a virtual network and bastion host

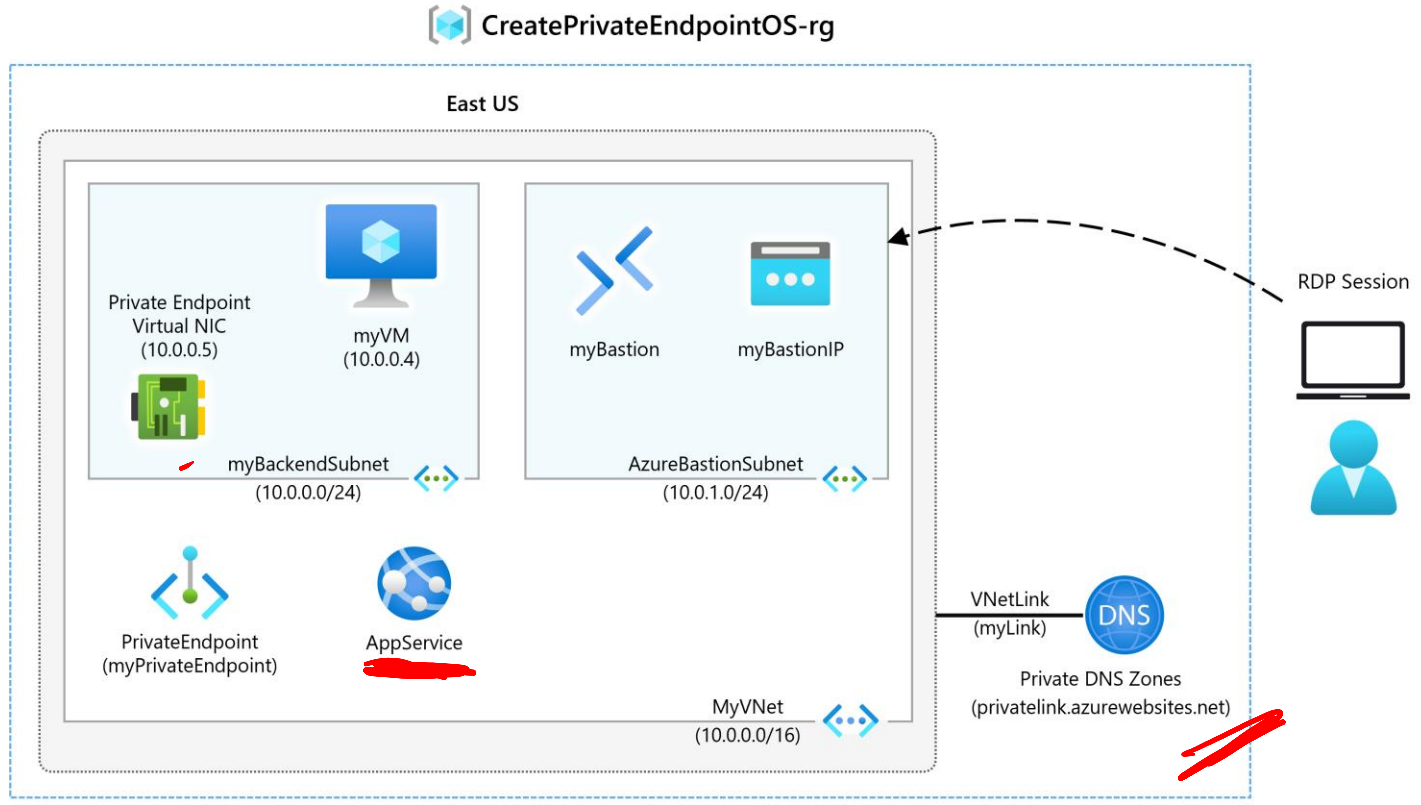
Task 3: Create a test virtual machine

Task 4: Create a Private Endpoint

Task 5: Configure the private DNS zone

Task 6: Test connectivity to the Private Endpoint

Task 7: Clean up resources



# Learning Recap - Create an Azure Private Endpoint

Check your knowledge questions and additional study

Quickstart - Create a Private Endpoint using the Azure portal | Microsoft Docs

# End of presentation