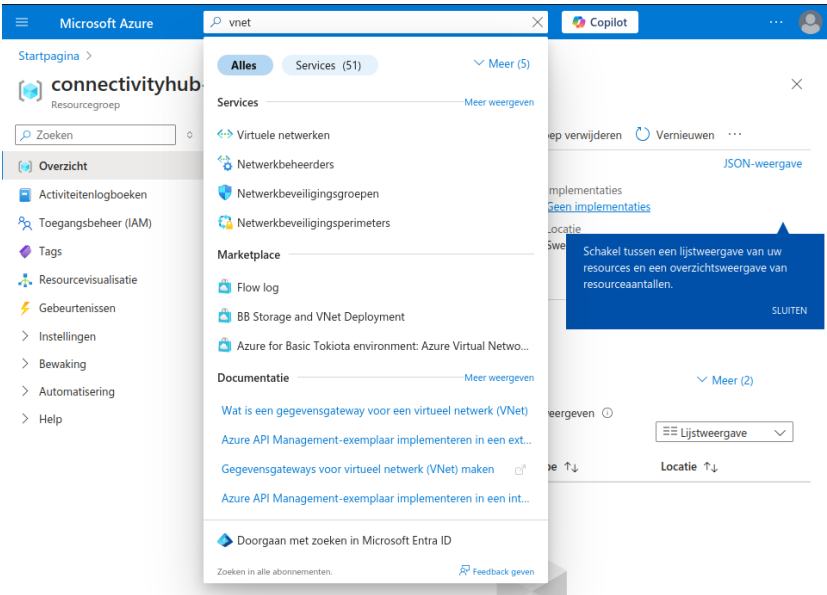


Azure VPN Gateway LAB-Guide

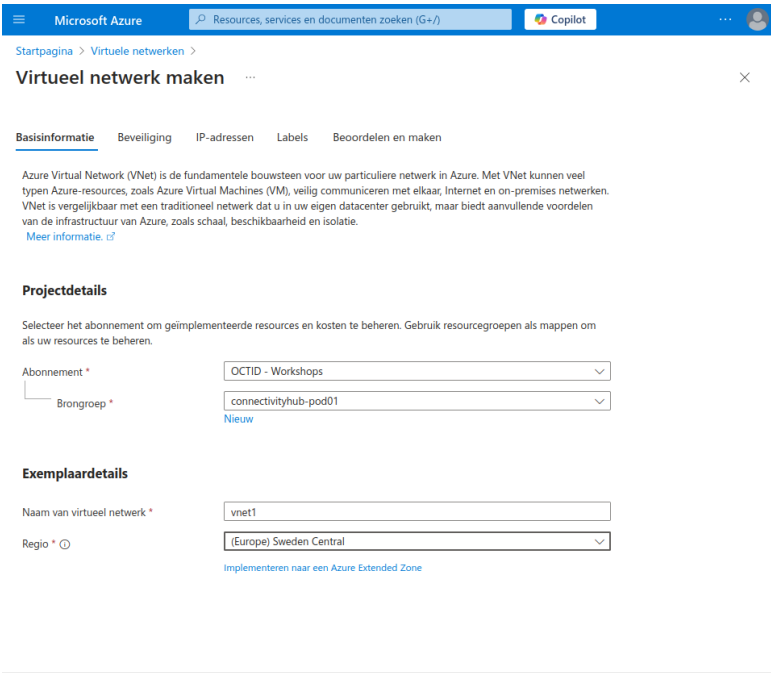
In dit lab ga je de volgende onderdelen maken in Azure:

- VNET
- Subnet
- Virtual Network Gateway
- Local Network Gateway
- Windows server om de connectivity te valideren

VNET & Subnet



Klik op 'Virtuele netwerken' en maak het object 'vnet1' aan in locatie 'Sweden Central'



Klik op ‘Volgende’

Microsoft Azure

Resources, services en documenten zoeken (G+/)

Copilot

Startpagina > Virtuele netwerken >

Virtueel netwerk maken

...

×

Basisinformatie

Beveiliging

IP-adressen

Labels

Beoordelen en maken

Configureer de adresruimte van uw virtuele netwerk met de IPv4- en IPv6-adressen en -subnetten die u nodig hebt. [Meer informatie](#)

Definieer de adresruimte van uw virtuele netwerk met een of meer IPv4- of IPv6-adresbereiken. Maak subnetten om de adresruimte van het virtuele netwerk te segmenteren in kleinere bereiken voor gebruik door uw toepassingen. Wanneer u resources implementeert in een subnet, wijst Azure aan de resource een IP-adres toe vanuit het subnet. [Meer informatie](#)

+ Een subnet toevoegen

10.31.0.0/23

10.31.0.0

/23

10.31.0.0 - 10.31.1.255

512 adressen

Adresruimte verwijderen

Subnetten	IP-adresbereik	Grootte	NAT Gateway
default	10.31.0.0 - 10.31.0.255	/24 (256 adressen)	-

IPv4-adresruimte toevoegen

Subnet verwijderen

Vorige

Volgende

Beoordelen en maken

Feedback geven

Kies hier de adresruimte die past bij je pod; 10.xx.0.0/23

xx = 30 + Pod nummer (pod01 = 31; pod10 = 40)

Verwijder het voorgestelde subnet ‘default’ die maken we zo zelf aan.

Klik de resource open en ga naar de subnetten:

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure', a search bar, and a 'Copilot' button. Below the navigation bar, the breadcrumb trail reads 'Startpagina > vnet1-1730821953922 | Overzicht > vnet1'. The main heading is 'vnet1 | Subnetten' with a star icon and a close button. Below the heading, there's a search bar labeled 'Zoeken' and a list of actions: '+ Subnet', 'Vernieuwen', 'Gebruikers beheren', and 'Verwijderen'. A descriptive text states: 'Maak subnetten om de adresruimte van het virtuele netwerk te segmenteren in kleinere bereiken voor gebruik door uw toepassingen. Wanneer u resources implementeert in een subnet, wijst Azure aan de resource een IP-adres toe vanuit het subnet.' Below this is another search bar labeled 'Subnetten zoeken'. On the left side, there's a sidebar with a search bar and a list of navigation items: 'Overzicht', 'Activiteitenlogboeken', 'Toegangsbeheer (IAM)', 'Tags', 'Problemen vaststellen en oplossen', 'Instellingen' (expanded), 'Adresruimte', 'Aangesloten apparaten', 'Subnetten' (selected), 'Bastion', 'DDoS-bescherming', 'Firewall', 'Microsoft Defender voor Cloud', 'Netwerkbeheerder', and 'DNS Services'.

Maak hier een nieuw subnet aan van het type 'Virtual Network Gateway'

The screenshot shows the 'Een subnet toevoegen' (Add a subnet) form in the Microsoft Azure portal. The form is titled 'Een subnet toevoegen' and has a close button. Below the title, there's a descriptive text: 'Selecteer een adresruimte en configureer uw subnet. U kunt een standaardsubnet aanpassen of kiezen uit subnetsjablonen als u van plan bent om bepaalde services later toe te voegen. [Meer informatie](#)'. The form contains several fields: 'Subnetdoel' (Virtual Network Gateway), 'Naam' (GatewaySubnet), 'IPv4' section with 'Een IPv4-adresruimte opnemen' (checked), 'IPv4-adresbereik' (10.31.0.0/23), 'Beginadres' (10.31.0.0), 'Grootte' (/26 (64 adressen)), and 'Adresbereik van subnet' (10.31.0.0 - 10.31.0.63). There's also an 'IPv6' section with 'Een IPv6-adresruimte opnemen' (unchecked) and a note 'Dit virtuele netwerk heeft geen IPv6-adresbereiken.' Below this is a 'Privatesubnet' section with 'Privatesubnetten verhogen de beveiliging door geen standaard uitgaande toegang te bieden. Als u uitgaande connectiviteit wilt inschakelen voor virtuele machines om toegang te krijgen tot internet, moet u expliciet uitgaande toegang verlenen. Een NAT-gateway is de aanbevolen manier om uitgaande connectiviteit te bieden voor virtuele machines in het subnet. [Meer informatie](#)'. There's a checkbox for 'Privatesubnet inschakelen (geen standaard uitgaande toegang)' which is unchecked. At the bottom, there's a 'Beveiliging' section with a note 'Vereenvoudig de internettoegang voor virtuele machines met behulp van een Network Address Translation-gateway. Filter subnetverkeer met'. At the bottom of the form, there are 'Toevoegen' and 'Annuleren' buttons, and a 'Feedback geven' link.

Dit is een /26 netwerk. Hierin komt de VPN gateway straks te draaien.

Vervolgens maken we nog een extra subnet aan voor de resources in Azure die we via de VPN gateway willen ontsluiten naar ons on-prem netwerk:

Een subnet toevoegen



Selecteer een adresruimte en configureer uw subnet. U kunt een standaardsubnet aanpassen of kiezen uit subnetsjablonen als u van plan bent om bepaalde services later toe te voegen. [Meer informatie](#)

Subnetdoel ⓘ	Default
Naam * ⓘ	default
IPv4	
Een IPv4-adresruimte opnemen	<input checked="" type="checkbox"/>
IPv4-adresbereik * ⓘ	10.31.0.0/23 10.31.0.0 - 10.31.1.255
Beginadres * ⓘ	10.31.1.0
Grootte ⓘ	/24 (256 adressen)
Adresbereik van subnet ⓘ	10.31.1.0 - 10.31.1.255

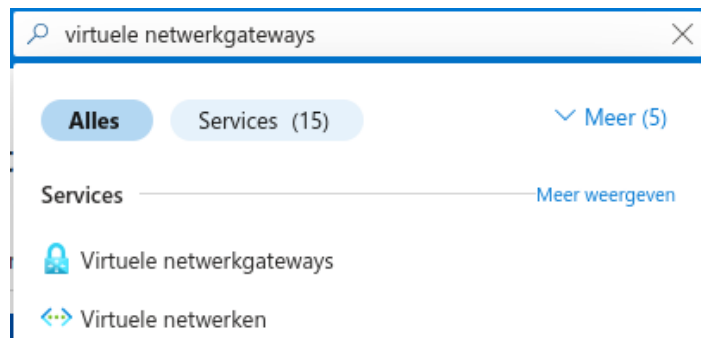
Hier kunnen

we de defaults accepteren.

Dan gaan we verder met het aanmaken van de Virtuele Netwerkgateway

Virtuele netwerkgateway

We gaan in de portal naar het onderdeel VPN gateways en klikken op 'Maken'



Hier kiezen we de volgende opties en dan maken we deze aan.

- Naam: VPNgw1
- Regio: Sweden Central
- GatewayType: VPN
- SKU: VpnGw1
- Generatie: Generation1
- Virtueel Netwerk: vnet1
- Subnet (automatisch geselecteerd): GatewaySubnet
- Openbaar IP-adres: Nieuwe maken
- Openbare IP-adresnaam: pip01
- Modus actief-actief inschakelen: Uitgeschakeld
- BGP configureren: Uitgeschakeld
- Toegang tot Key Vault inschakelen: Uitgeschakeld

[Startpagina](#) > [Virtuele netwerkgateways](#) >

Virtuele netwerkgateway maken

✔ Validatie voltooid

Basisinformatie

Labels

Beoordelen en maken

Basisinformatie

Abonnement	OCTID - Workshops
Resourcegroep	connectivityhub-pod01
Naam	VPNgw01
Regio	Sweden Central
SKU	VpnGw1
Generatie	Generation1
Virtueel netwerk	vnet1
Subnet	GatewaySubnet (10.31.0.0/26)
Gatewaytype	Vpn
VPN-type	RouteBased
Modus actief-actief inschakelen	Uitgeschakeld
BGP configureren	Uitgeschakeld
Openbaar IP-adres	pip01

Labels

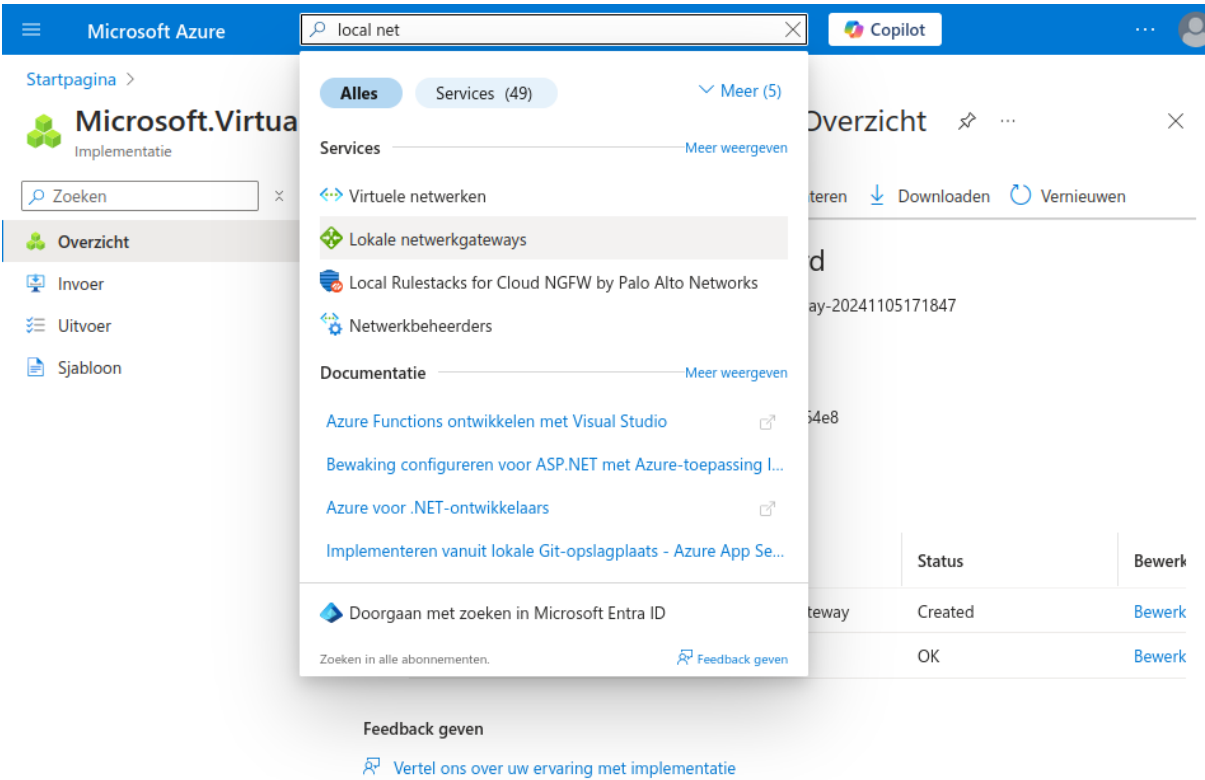
Geen

Het maken van deze VPN Gateway kan een ~10-50 minuten duren.

Ondertussen kunnen we de andere resources maken.

Local Network Gateway

In dit deel geven we het public IP op van onze on-prem IPSEC oplossing. Tevens wordt hier het subnet opgegeven welke achter de on-prem gateway bereikbaar is.



Hier maken

we een nieuw object met de volgende eigenschappen:

Basisinformatie

Geavanceerd

Beoordelen en maken

Een lokale netwerkgateway is een specifiek object dat een on-premises locatie (de site) vertegenwoordigt voor routeringsdoeleinden. [Meer informatie](#)

Projectgegevens

Abonnement *

Resourcegroep *

Exemplaar details

Regio *

Naam *

Eindpunt ⓘ

IP-adres * ⓘ

Adresruimte(n) ⓘ

OCTID - Workshops

connectivityhub-pod01

Nieuw

Sweden Central

Ingw01

IP-adres

89.37.98.241

10.10.0.0/16

Aanvullend adresbereik toevoegen

Het IP adres is hier 89.37.98.[240 + pod nummer]

Connection van de VPN Gateway

Hier stellen we de pre-shared-key in voor de site-to-site tunnel. Deze optie komt pas beschikbaar als de VPN gateway is aangemaakt.

Startpagina > VPNgw01

VPNgw01 | Verbindingen ✨ ☆ ...

Virtuele netwerkgateway

Zoeken ◊ << + Toevoegen ↻ Vernieuwen

Overzicht

Activiteitenlogboeken

Toegangsbeheer (IAM)

Tags

Problemen vaststellen en oplossen

Instellingen

Configuratie

Verbindingen

Punt-naar-site-configuratie

Onderhoud

Eigenschappen

Vergrendelingen

Bewaking

Automatisering

Help

Verbindingen zoeken

Naam	↑↓	Status	↑↓	Verbindingstype	↑↓	Peer
Geen resultaten						

Maak een nieuwe verbinding aan met de opties:

- Verbindingstype: site-naar-site (IPsec)
- Naam: con01
- Virtuele netwerkgateway: VPNgw1
- Lokale netwerkgateway: lngw01
- Verificatiemethode: Gedeelde sleutel (PSK)
- Gedeelde sleutel (PSK): podXX-4-v3ry-53cr37-1p53c-5h4r3d-k3y (XX is pod nummer)
- IKE-protocol: IKEv2

 Validatie voltooidBasisinformatie Instellingen Labels Beoordelen en maken**Basic**

Abonnement	OCTID - Workshops
Resourcegroep	connectivityhub-pod01
Regio	Sweden Central
Verbindingstype	Site-naar-site (IPsec)
Verbindingsnaam	con01

Instellingen

Virtuele netwerkgateway	VPNgw01
Lokale netwerkgateway	Ingw01
IKE-protocol	IKEv2
IPsec/IKE-beleid	Standaard
Op beleid gebaseerde verkeerskiezer gebruiken	Uitschakelen
DPD-out in seconden	45
Verbindingsmodus	Default
Gedeelde sleutel (PSK)	pod01-4-v3ry-53cr37-1p53c-5h4r3d-k3y

Remote resources

Tenslotte willen we dan nog een resource in Azure die we kunnen benaderen vanuit on-prem of vice-versa.

Klik bijvoorbeeld een windows server 2022 aan met een eigen public IP (poort 3389 voor RDP open).

Zorg ervoor dat deze in het bestaande vnet1 komt in het 'default' subnet dat we hiervoor hebben gemaakt.

VPN tunnel activeren

Indien de VPN Gateway succesvol is ingericht kan je het public IP hiervan doorgeven aan mij en zal ik de fysieke router instellen zodat de tunnel online kan komen. Het zou daarna mogelijk moeten zijn om de on-prem raspberry pi te kunnen benaderen op:

<http://10.10.10.10/>

Alles verwijderen

Indien je tot hier bent gekomen kan je alle resources **onder** je resourcegroep verwijderen.

Indien je eerder bent afgehaakt is dit ook belangrijk voor je de volgende stap gaat zetten.

Nadat je alles onder je resource-group hebt gewist gaat de presentatie hier verder.

DevOps

Op <http://tiny.cc/n3ptzz> kan je de pipeline aftrappen die hoort bij je pod; hiermee worden alle resources door terraform opnieuw aangemaakt.

Zoek in de azure portal het public IP op van de VPN gateway en geef deze door aan mij.

Vervolgens is het weer mogelijk om vanuit de Windows VM via RDP de on-prem resources te benaderen.