

# VPN-taakverdeling voor client configureren met DNS Round Robin op ASA

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Stap 1. AnyConnect VPN configureren op ASA](#)

[Stap 2. Round Robin DNS op DNS-server configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

---

## Inleiding

Dit document beschrijft hoe u een taakverdeling voor de VPN-client kunt configureren met DNS-round robin op ASA.

## Voorwaarden

### Vereisten

Voordat u deze configuratie uitvoert, moet aan de volgende vereisten worden voldaan:

- U hebt IP-adressen aan uw ASA's toegewezen en de standaardgateway geconfigureerd.
- AnyConnect VPN is geconfigureerd op de ASA's.
- VPN-gebruikers kunnen verbinding maken met alle ASA's met behulp van hun individueel toegewezen IP-adres.
- DNS server van VPN-gebruikers is ronde robin geschikt.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

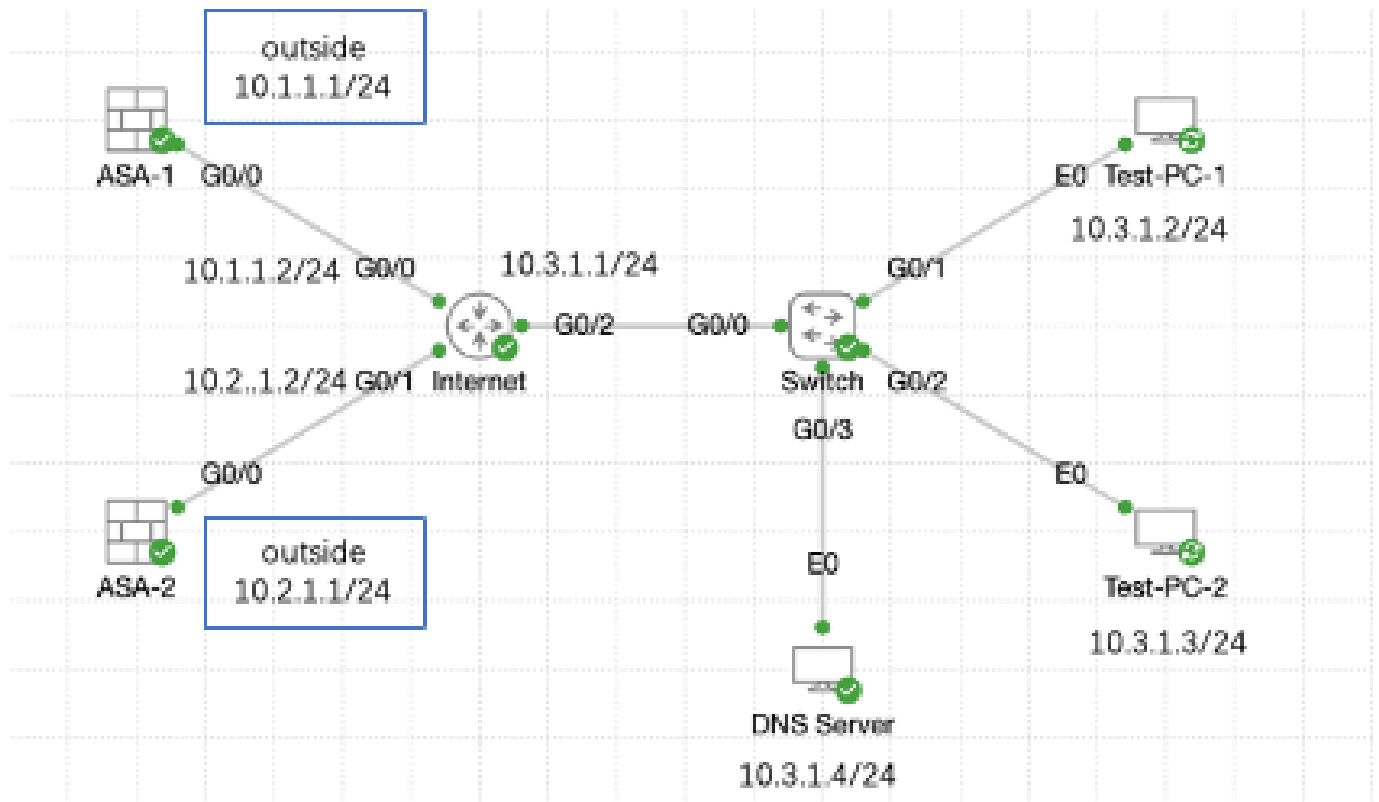
- AnyConnect VPN-clientsoftwarereleases 4.10.08025
- Cisco ASA-softwarereleases 9.18.2
- Windows Server 2019

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Configureren

### Netwerkdigram



Netwerkdigram

### Configuraties

#### Stap 1. AnyConnect VPN configureren op ASA

Raadpleeg dit document voor het configureren van een verbinding met VPN via ASA:

- [ASA 8.x: VPN-toegang met de AnyConnect VPN-client met behulp van zelf-ondertekend configuratievoorbeeld van certificaat](#)

Hier is de configuratie van beide ASA's in dit voorbeeld:

ASA1:

```
ip local pool anyconnect 10.4.0.100-10.4.0.200 mask 255.255.255.0
```

```
interface GigabitEthernet0/0
```

```
nameif outside
security-level 0
ip address 10.1.1.1 255.255.255.0

interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0

route outside 0.0.0.0 0.0.0.0 10.1.1.2 1

webvpn
enable outside
anyconnect enable
tunnel-group-list enable

group-policy anyconnect internal
group-policy anyconnect attributes
dns-server value 192.168.1.99
vpn-tunnel-protocol ssl-client
default-domain value example.com

username example1 password *****
username example1 attributes
vpn-group-policy anyconnect
service-type remote-access

tunnel-group anyconnect-tunnel-group type remote-access
tunnel-group anyconnect-tunnel-group general-attributes
address-pool anyconnect
default-group-policy anyconnect
tunnel-group anyconnect-tunnel-group webvpn-attributes
group-alias example enable
```

## ASA2:

```
ip local pool anyconnect 10.4.0.100-10.4.0.200 mask 255.255.255.0

interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.2.1.1 255.255.255.0

interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0

route outside 0.0.0.0 0.0.0.0 10.2.1.2 1

webvpn
enable outside
anyconnect enable
tunnel-group-list enable

group-policy anyconnect internal
group-policy anyconnect attributes
dns-server value 192.168.1.99
```

```
vpn-tunnel-protocol ssl-client
default-domain value example.com
```

```
username example1 password *****
username example1 attributes
vpn-group-policy anyconnect
service-type remote-access
```

```
tunnel-group anyconnect-tunnel-group type remote-access
tunnel-group anyconnect-tunnel-group general-attributes
address-pool anyconnect
default-group-policy anyconnect
tunnel-group anyconnect-tunnel-group webvpn-attributes
group-alias example enable
```

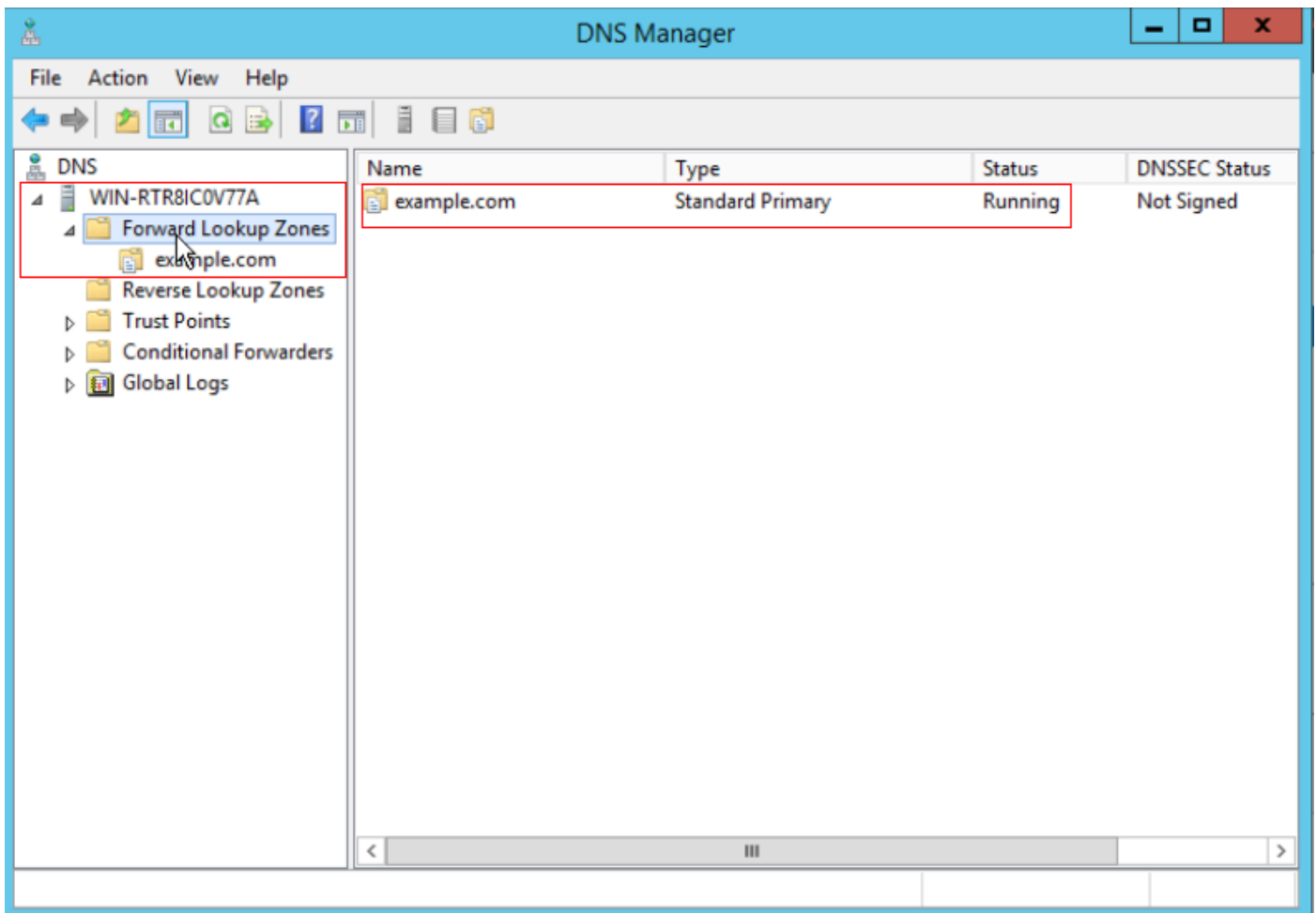
U moet met beide ASA's verbinding kunnen maken met het gebruik van hun individueel toegewezen IP-adres voordat u naar stap 2 gaat.

## Stap 2. Round Robin DNS op DNS-server configureren

U kunt elke ronde robin capble DNS-server gebruiken, in dit voorbeeld wordt DNS-server op Windows-server 2019 gebruikt. Raadpleeg dit document voor het installeren en configureren van DNS-server op Windows-server:

- [DNS-server op Windows-server installeren en configureren](#)

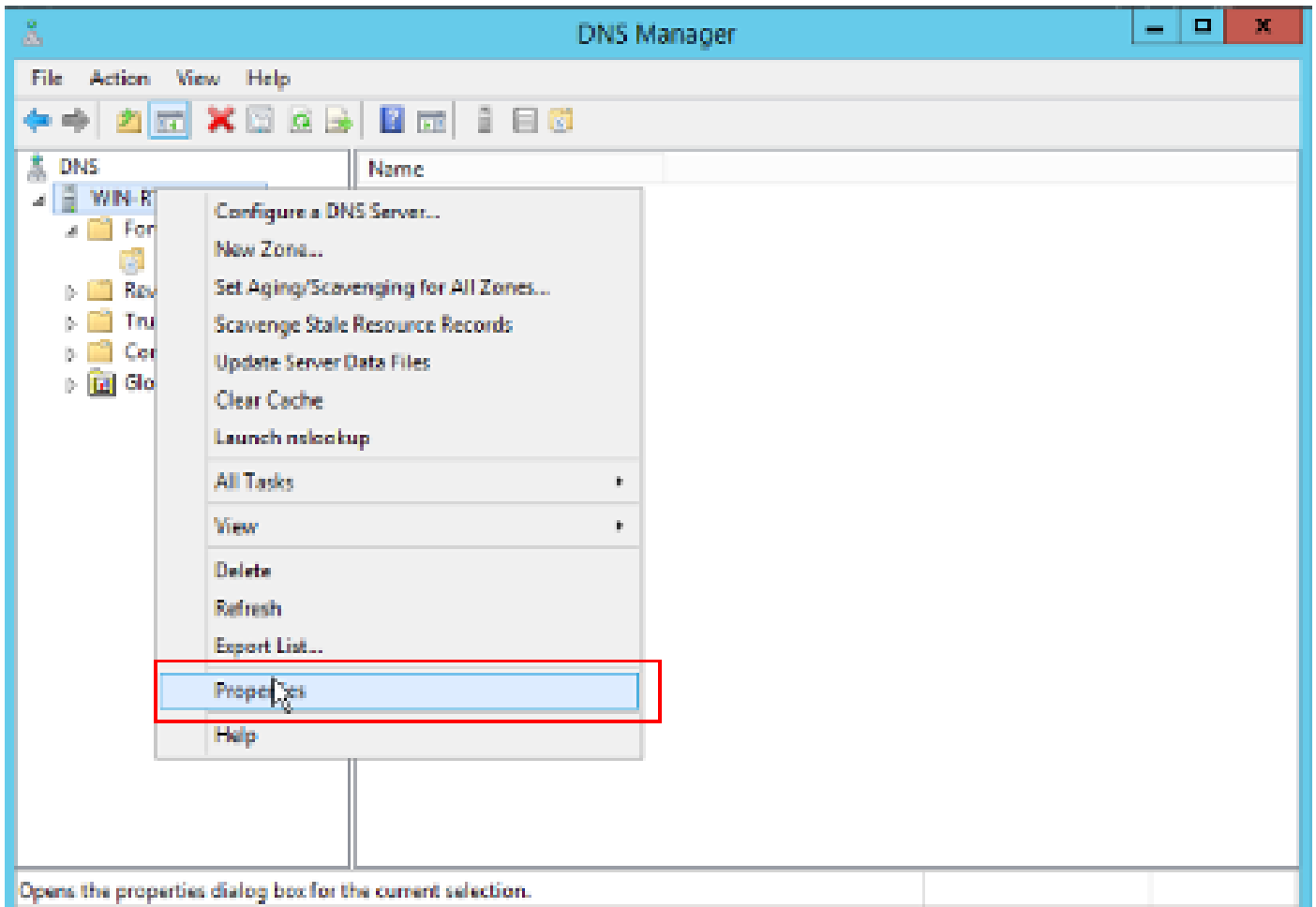
In dit voorbeeld, 10.3.1.4 is de Windows server met DNS server toelaten voor domein example.com.

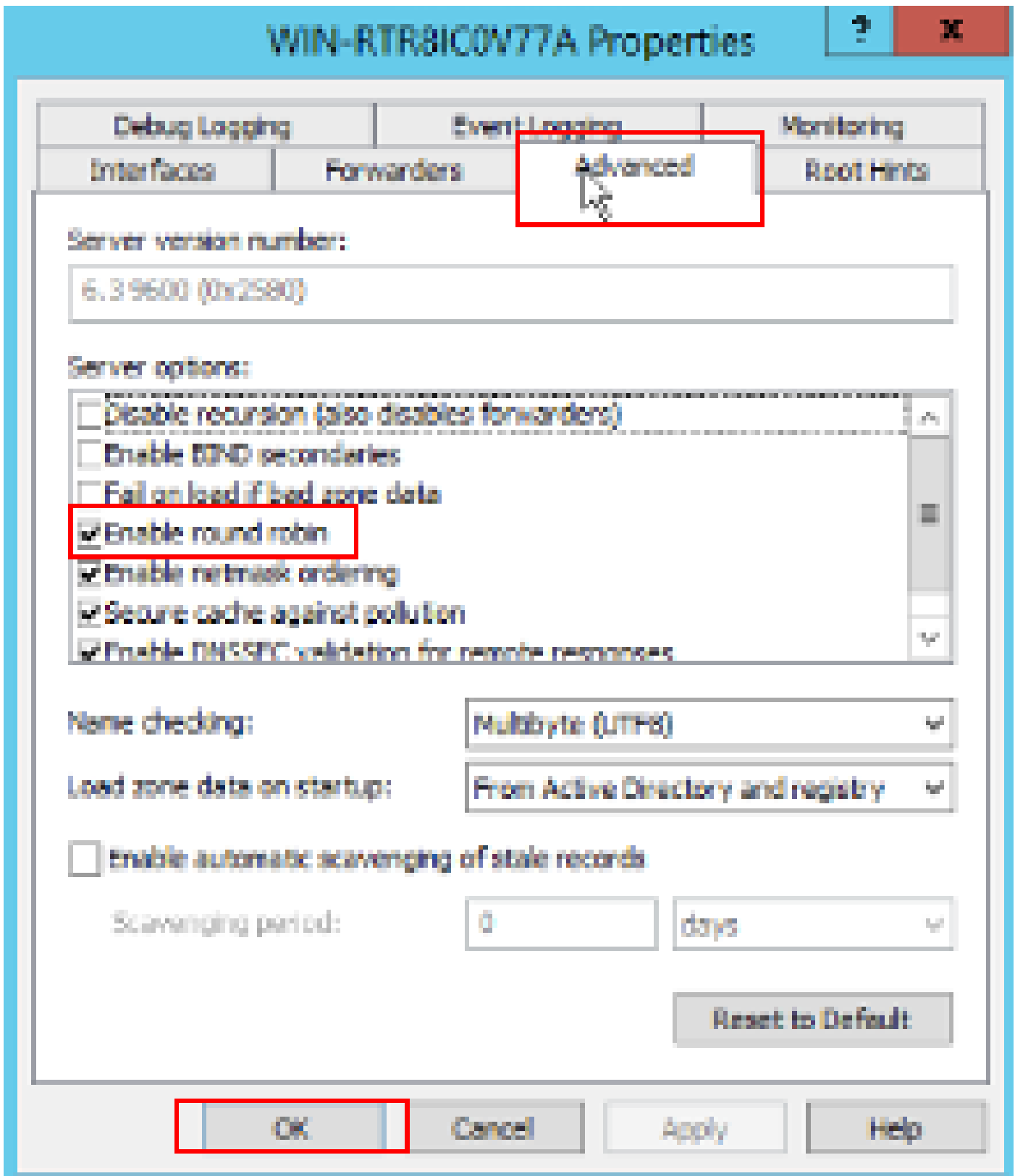


DNS-server

Zorg ervoor dat round robin is ingeschakeld voor uw DNS-server:

1. Open vanuit het bureaublad van Windows het menu Start en selecteer Beheertools > DNS.
2. Kies in de consolestructuur de DNS-server die u wilt beheren, klik met de rechtermuisknop en kies vervolgens Eigenschappen.
3. Zorg ervoor dat onder het tabblad Advanced het vakje Enable round robin is ingeschakeld.





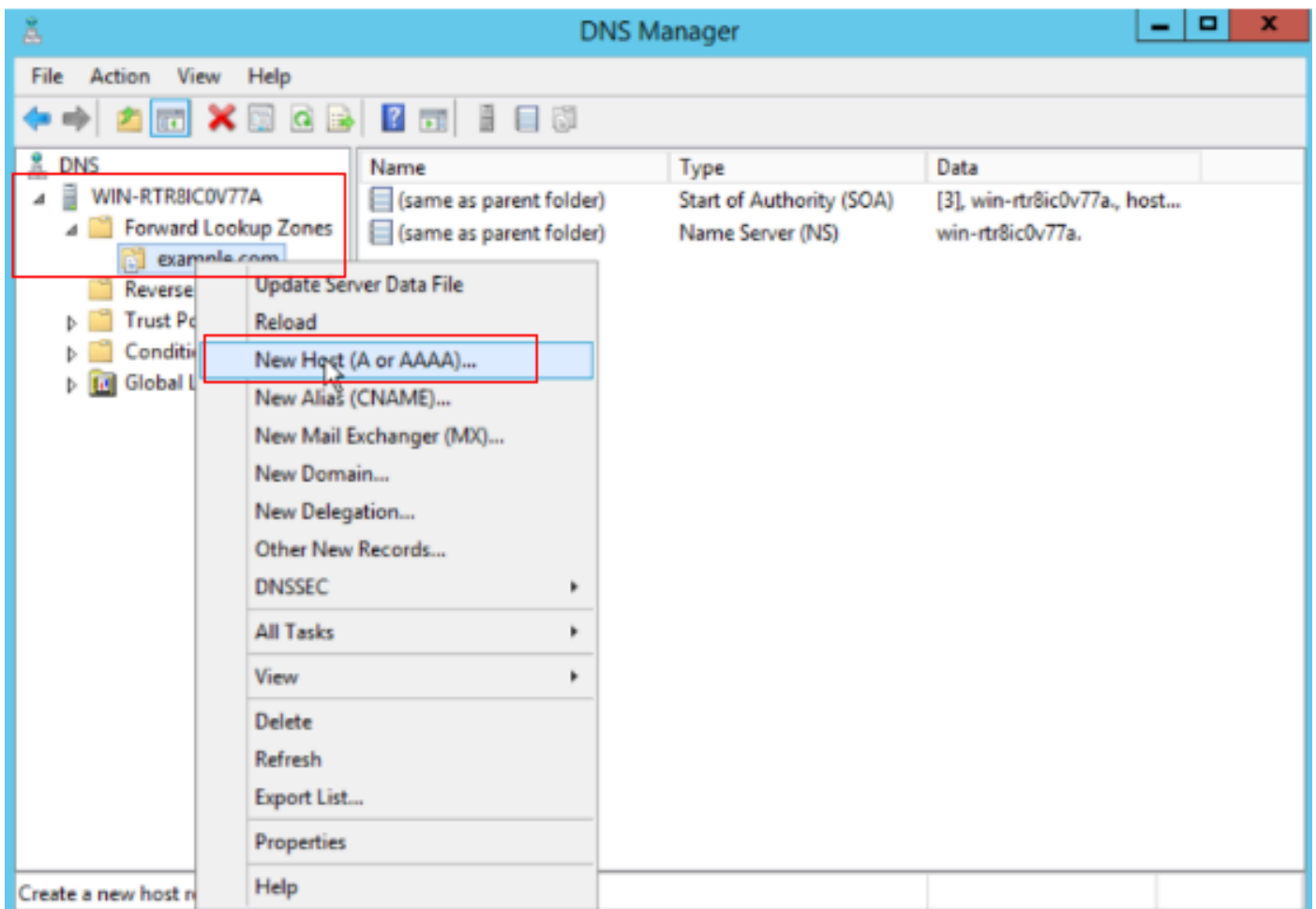
Ronde Robin 2

Maak twee hostrecords voor ASA VPN-servers:

1. Open vanuit het bureaublad van Windows het menu Start en selecteer Gereedschappen > DNS.
2. In de consoleboom, verbind met de DNS server u wenst te beheren, breid de DNS server uit, breid uw Voorwaartse Raadplegingszone uit, klik met de rechtermuisknop, dan selecteer

Nieuwe Gastheer (A of AAAA).

3. Specificeer in het scherm Nieuwe host de naam en het IP-adres van de hostrecord. In dit voorbeeld, vpn en 10.1.1.1.
4. Selecteer Add Host om de record te maken.



Nieuwe host maken




## New Host X

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

IP address:

Create associated pointer (PTR) record



Host Record 1

Herhaal vergelijkbare stappen om een andere host record te maken en zorg ervoor dat Naam hetzelfde is, in dit voorbeeld is Naam VPN, IP-adres is 10.2.1.1.

## New Host X

Name (uses parent domain name if blank):

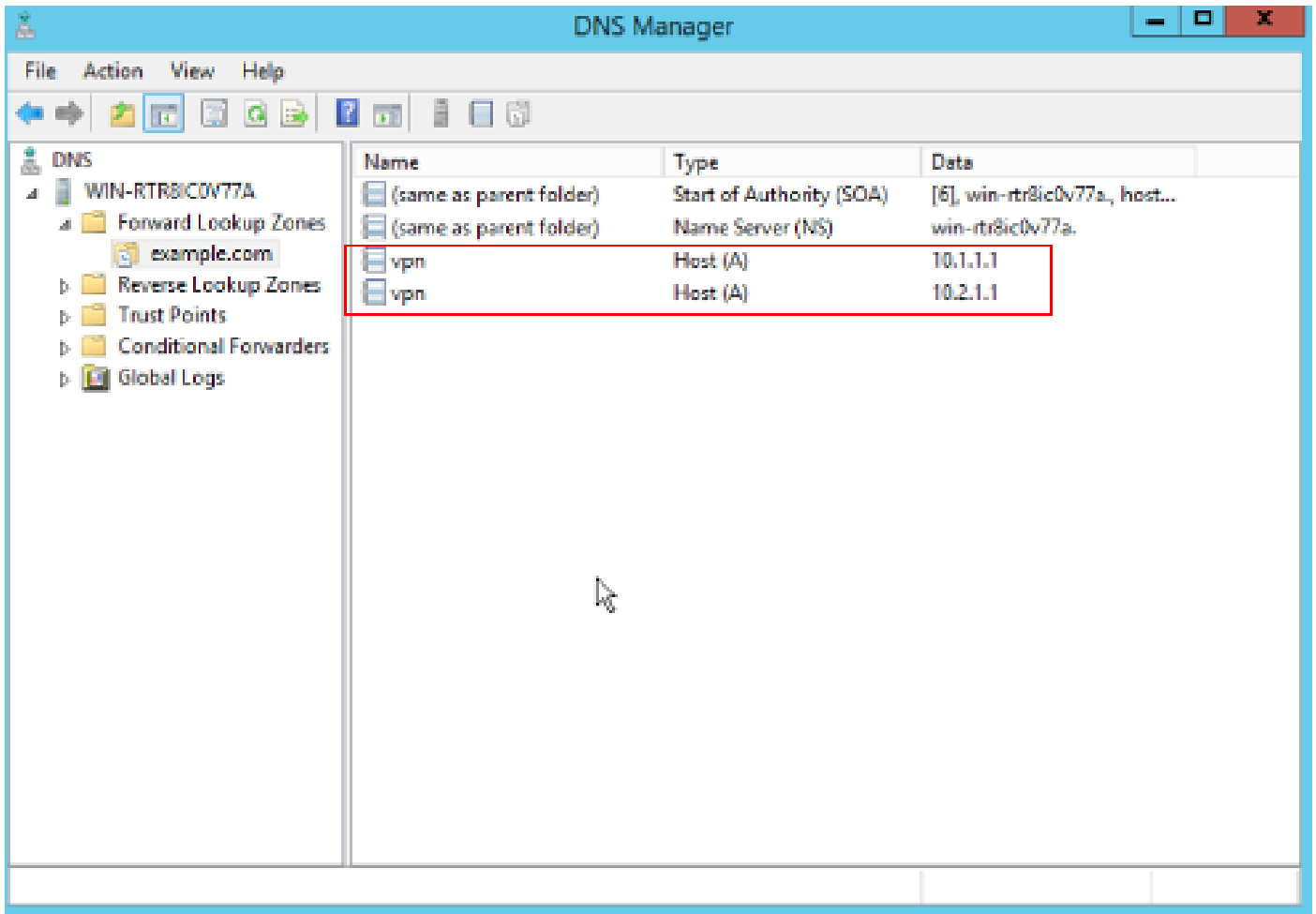
Fully qualified domain name (FQDN):

IP address:

Create associated pointer (PTR) record

Host Record 2

U kunt vinden er twee hosts 10.1.1.1 en 10.2.1.1 associëren met dezelfde record vpn.example.com.



Twee hostrecords

## Verifiëren

Navigeer naar uw clientcomputer waarop de Cisco AnyConnect Secure Mobility-client is geïnstalleerd. Controleer in dit voorbeeld Test-PC-1 of uw DNS-server 10.3.1.4 is.

## Network Connection Details



### Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Intel(R) PRO/1000 MT Network Connecti
Physical Address	52-54-00-0B-68-6F
DHCP Enabled	No
Pv4 Address	10.3.1.2
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	10.3.1.1
Pv4 DNS Server	10.3.1.4
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::6147:aeeb:9647:9004%16
IPv6 Default Gateway	
IPv6 DNS Server	

Close



Opmerking: aangezien een zelfondertekend certificaat wordt gebruikt voor de gateway om zichzelf te identificeren, kunnen er meerdere certificaatwaarschuwingen verschijnen tijdens de verbindingsooging. Deze worden verwacht en moeten worden geaccepteerd om de verbinding te kunnen voortzetten. Om deze certificaatwaarschuwingen te voorkomen, moet het zelfondertekende certificaat dat wordt overgelegd, worden geïnstalleerd in het vertrouwde certificaatarchief van de clientmachine of moet, als een certificaat van een derde wordt gebruikt, het certificaat van de certificeringsinstantie worden opgeslagen in het vertrouwde certificaatarchief.

---

Maak verbinding met uw VPN-head-end `vpn.example.com` en voer de gebruikersnaam en referenties in.



**VPN:**  
Ready to connect.



**Network:**  
Connected (10.3.1.3)



**System Scan:**  
No policy server detected.  
Default network access is in effect.



**Roaming Security:**  
Limits is inactive.  
Profile is missing.



**AMP Enabler:**  
Waiting for configuration...

---

: op de ASA kunt u verschillende debug-niveaus instellen; standaard wordt niveau 1 gebruikt. Als u het debug-niveau wijzigt, neemt de breedheid van de debugs toe. Wees hier voorzichtig mee, vooral in productieomgevingen.

---

U kunt debug in diagnostische VPN-verbinding via ASA inschakelen.

- debug webvpn anyconnect - Hier worden debug-berichten weergegeven over verbindingen met AnyConnect VPN-clients.

Raadpleeg [dit](#) document om gebruikelijke problemen op te lossen die u aan de clientzijde vindt.

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.