

# Configurar o balanceamento de carga do cliente VPN com rodízio DNS no ASA

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Etapa 1. Configurar o AnyConnect VPN no ASA](#)

[Etapa 2. Configurar o DNS de rodízio no servidor DNS](#)

[Verificar](#)

[Troubleshooting](#)

---

## Introdução

Este documento descreve como configurar o balanceamento de carga do cliente vpn anyconnect com rodízio DNS no ASA.

## Pré-requisitos

### Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Você atribuiu endereços IP em seus ASAs e configurou o gateway padrão.
- O AnyConnect VPN está configurado nos ASAs.
- Os usuários de VPN podem se conectar a todos os ASAs com o uso de seus endereços IP atribuídos individualmente.
- O servidor DNS de usuários VPN é compatível com rodízio.

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Anyconnect VPN Client versões 4.10.08025
- Software Cisco ASA versões 9.18.2
- Windows Server 2019

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

### Diagrama de Rede

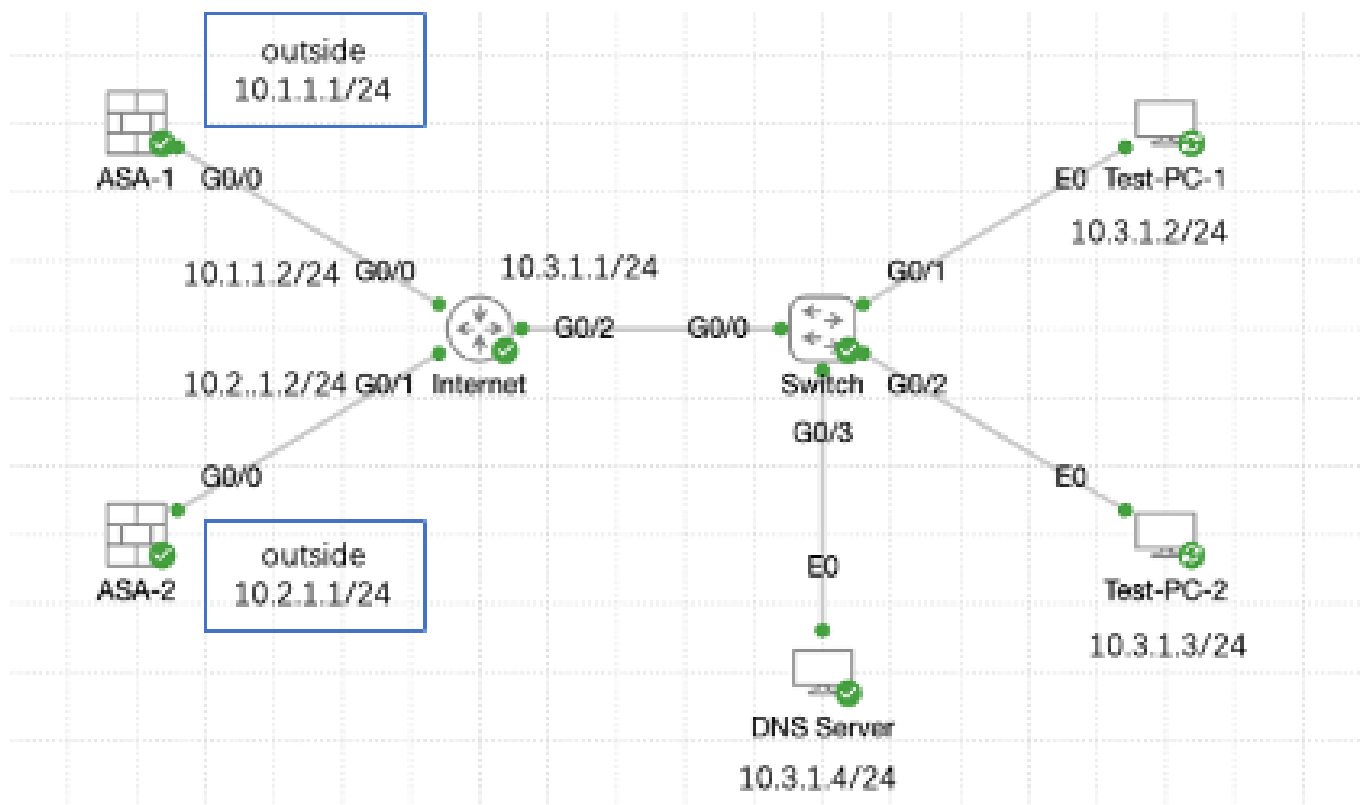


Diagrama de Rede

## Configurações

### Etapa 1. Configurar o AnyConnect VPN no ASA

Para saber como configurar o anyconnect VPN no ASA, consulte este documento:

- [ASA 8.x : Exemplo de Configuração de Acesso VPN com o AnyConnect VPN Client Usando Certificado Autoassinado](#)

Aqui está a configuração de ambos os ASAs neste exemplo:

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
```

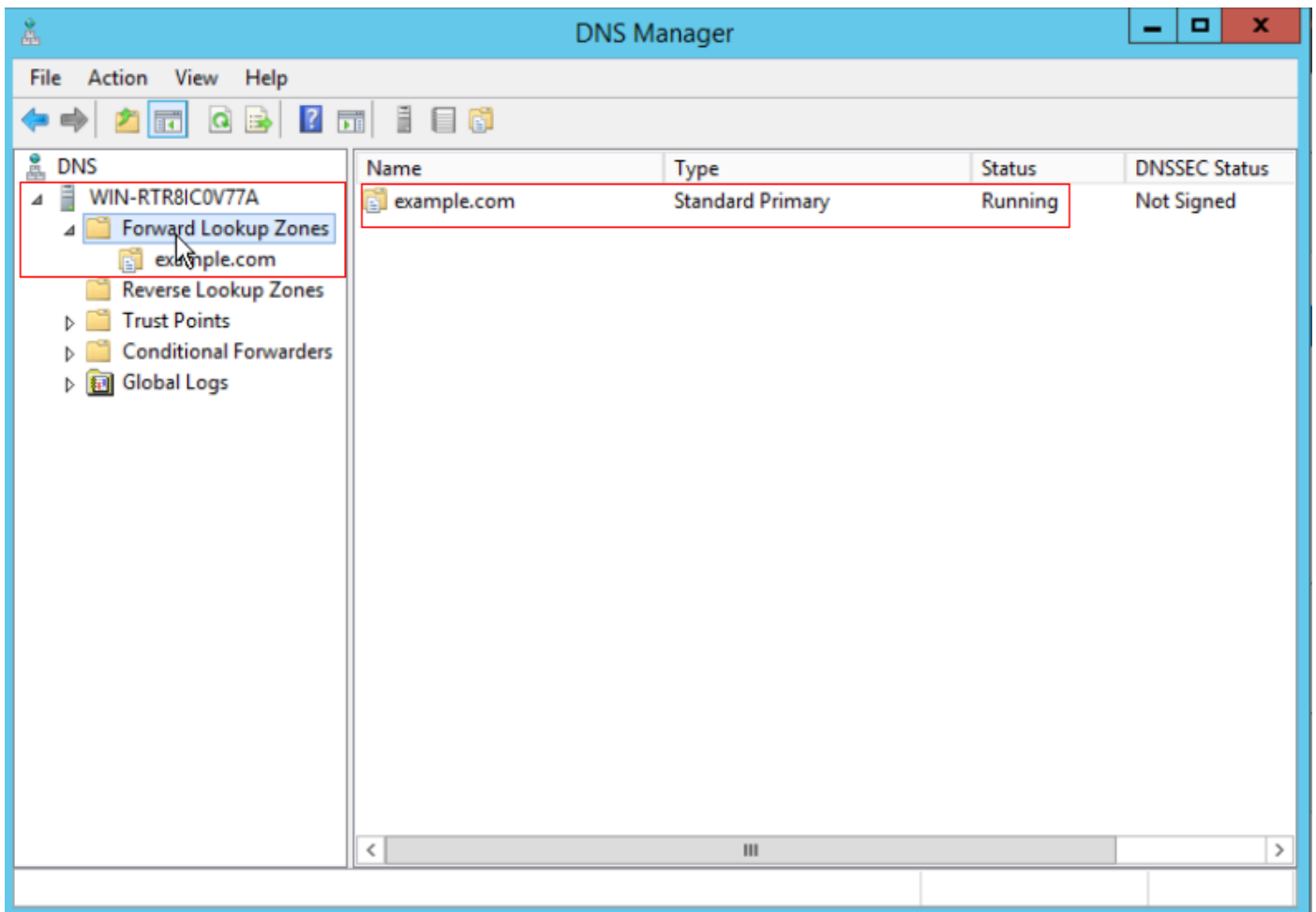
Você deve conseguir se conectar a ambos os ASAs com o uso de seus endereços IP atribuídos individualmente antes de passar para a etapa 2.

## Etapa 2. Configurar o DNS de rodízio no servidor DNS

Você pode usar qualquer servidor DNS compatível com rodízio, neste exemplo, o servidor DNS no Windows Server 2019 é usado. Para saber como instalar e configurar o servidor DNS no servidor Windows, consulte este documento:

- [Instalar e configurar o servidor DNS no Windows Server](#)

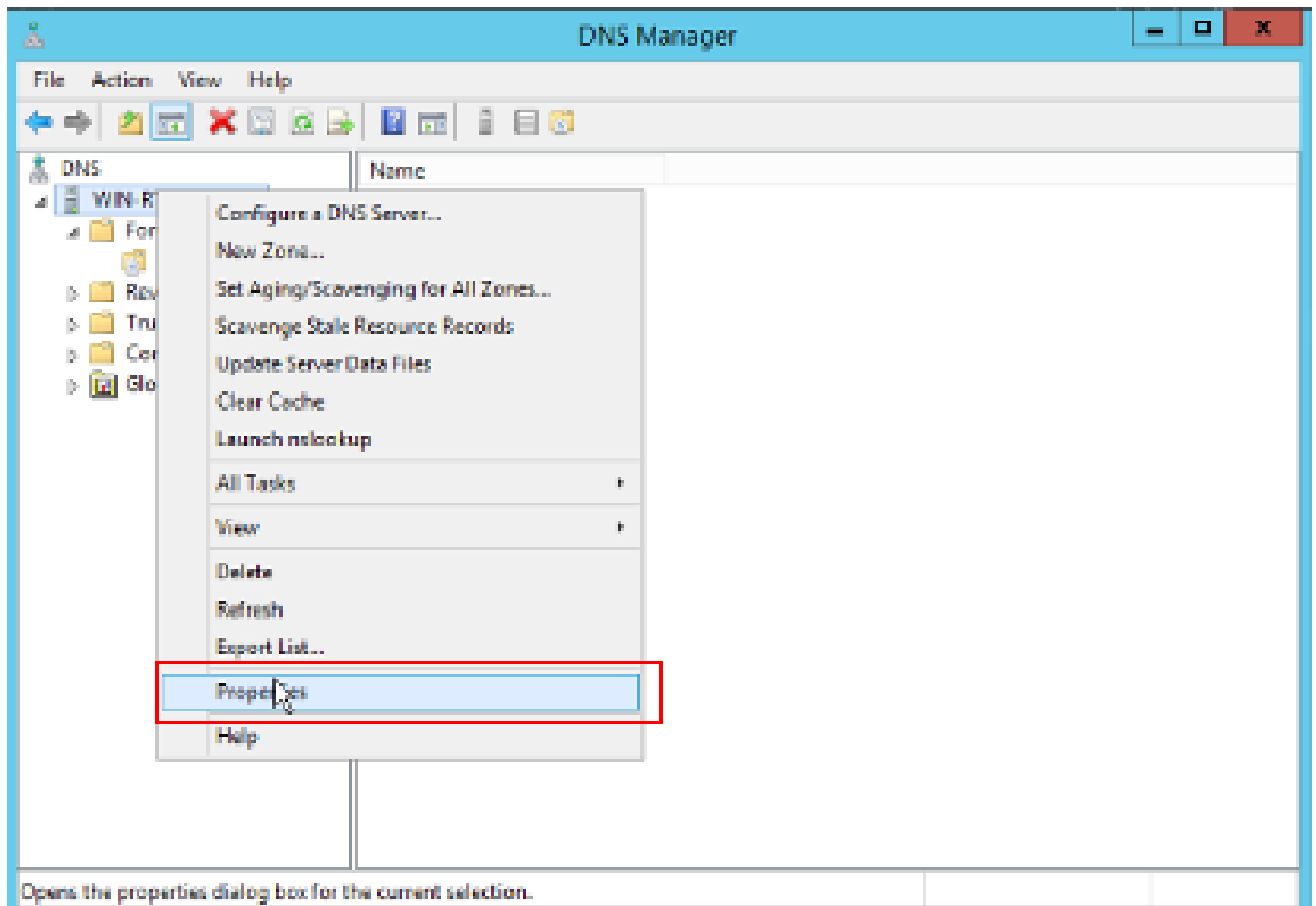
Neste exemplo, 10.3.1.4 é o servidor do Windows com o servidor DNS habilitado para o domínio example.com.



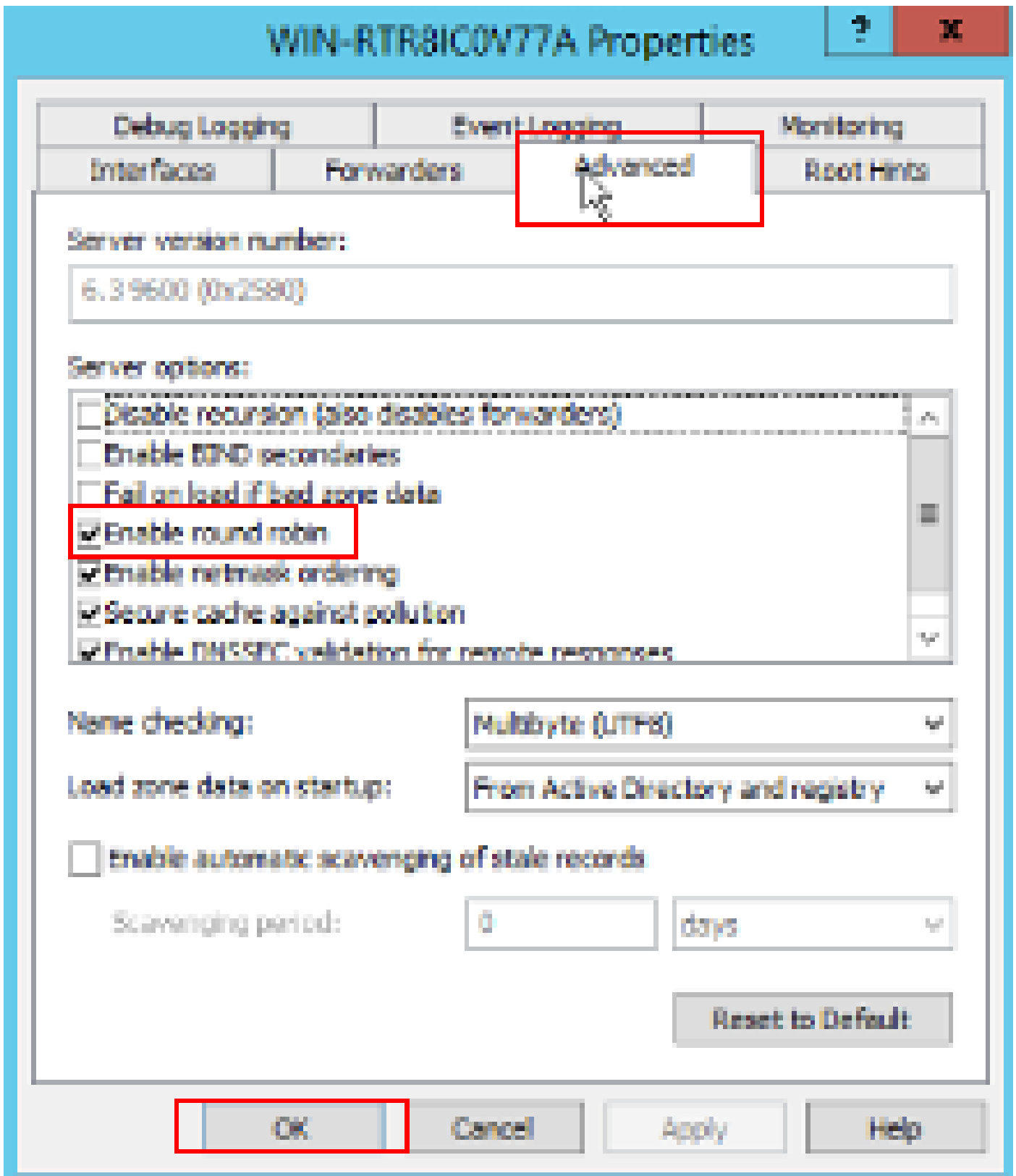
Servidor DNS

Verifique se o rodízio está habilitado para o servidor DNS:

1. Na área de trabalho do Windows, abra o menu Iniciar, selecione Ferramentas Administrativas > DNS.
2. Na árvore do console, escolha o servidor DNS que deseja gerenciar, clique com o botão direito do mouse e selecione Properties.
3. Na guia Advanced, certifique-se de que Enable round robin esteja marcado.



Rodizio 1



Rodízio 2

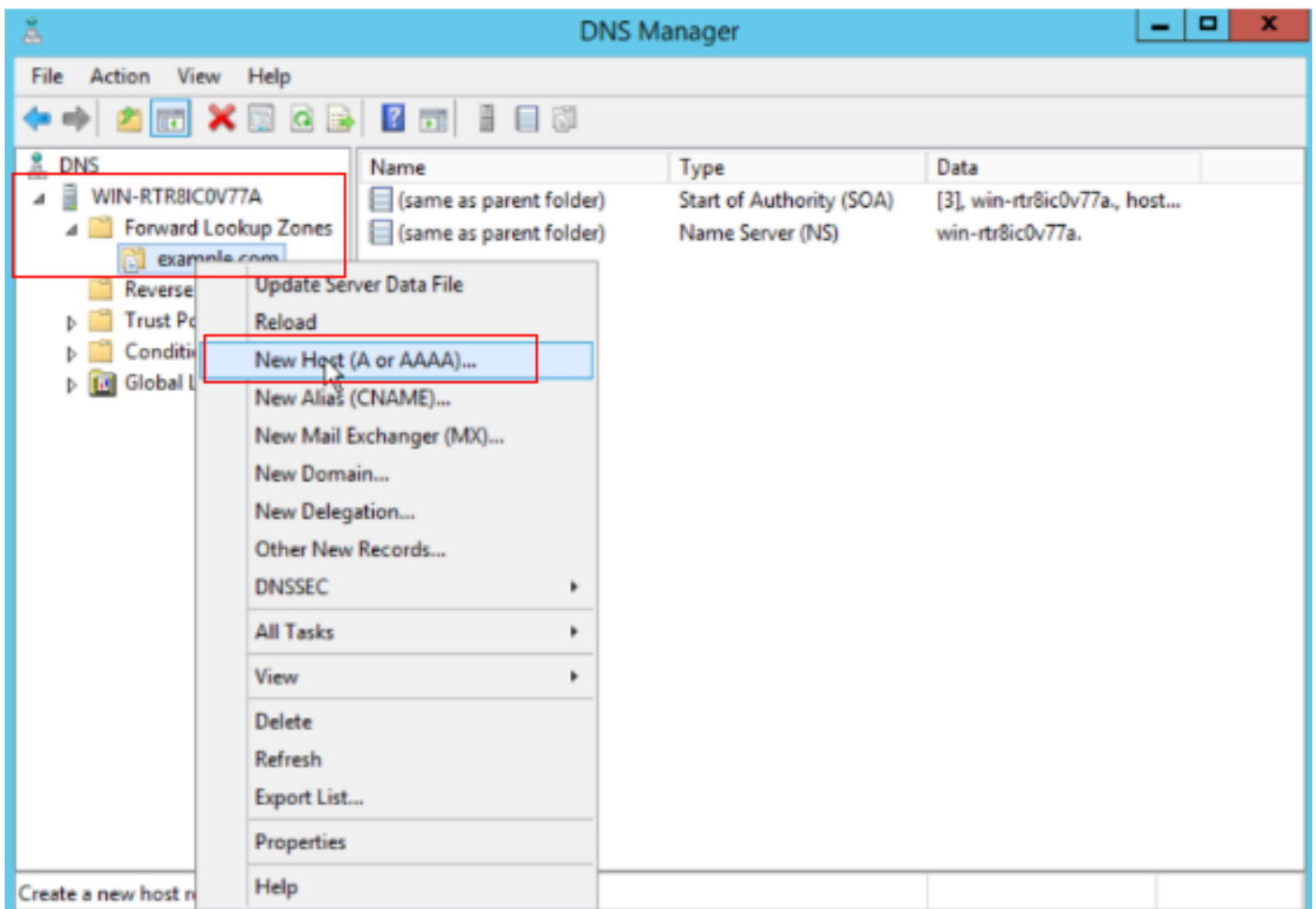
Crie dois registros de host para servidores ASA VPN:

1. Na área de trabalho do Windows, abra o menu Iniciar, selecione Ferramentas Administrativas > DNS.
2. Na árvore do console, conecte-se ao servidor DNS que deseja gerenciar, expanda o servidor DNS, expanda a Zona de pesquisa direta, clique com o botão direito do mouse e

selecione Novo host (A ou AAAA).

3. Na tela Novo host, especifique o Nome e o endereço IP do registro do host. Neste exemplo, vpn e 10.1.1.1.

4. Selecione Add Host para criar o registro.



Criar novo host




## New Host X

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

IP address:

Create associated pointer (PTR) record



Registro do host 1

Repita etapas semelhantes para criar outro registro de host e certifique-se de que o Nome seja o mesmo; neste exemplo, Nome é vpn, endereço IP é 10.2.1.1.

## New Host X

Name (uses parent domain name if blank):

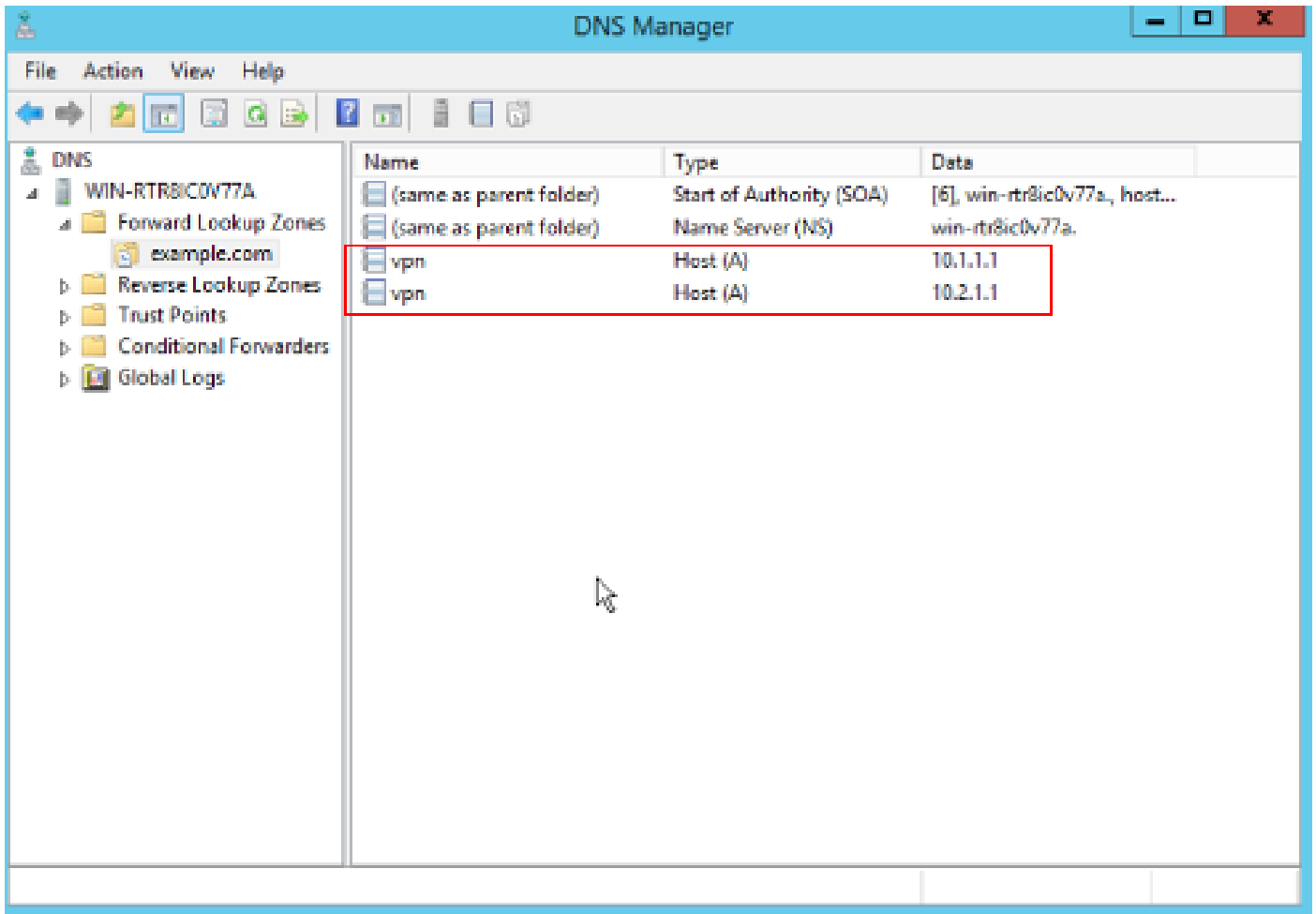
Fully qualified domain name (FQDN):

IP address:

Create associated pointer (PTR) record

Registro de host 2

Você pode encontrar dois hosts 10.1.1.1 e 10.2.1.1 associados ao mesmo registro vpn.example.com.



Dois registros de host

## Verificar

Navegue até a máquina do cliente onde o cliente Cisco AnyConnect Secure Mobility está instalado. Neste exemplo, Test-PC-1, verifique se o servidor DNS é 10.3.1.4.

## Network Connection Details

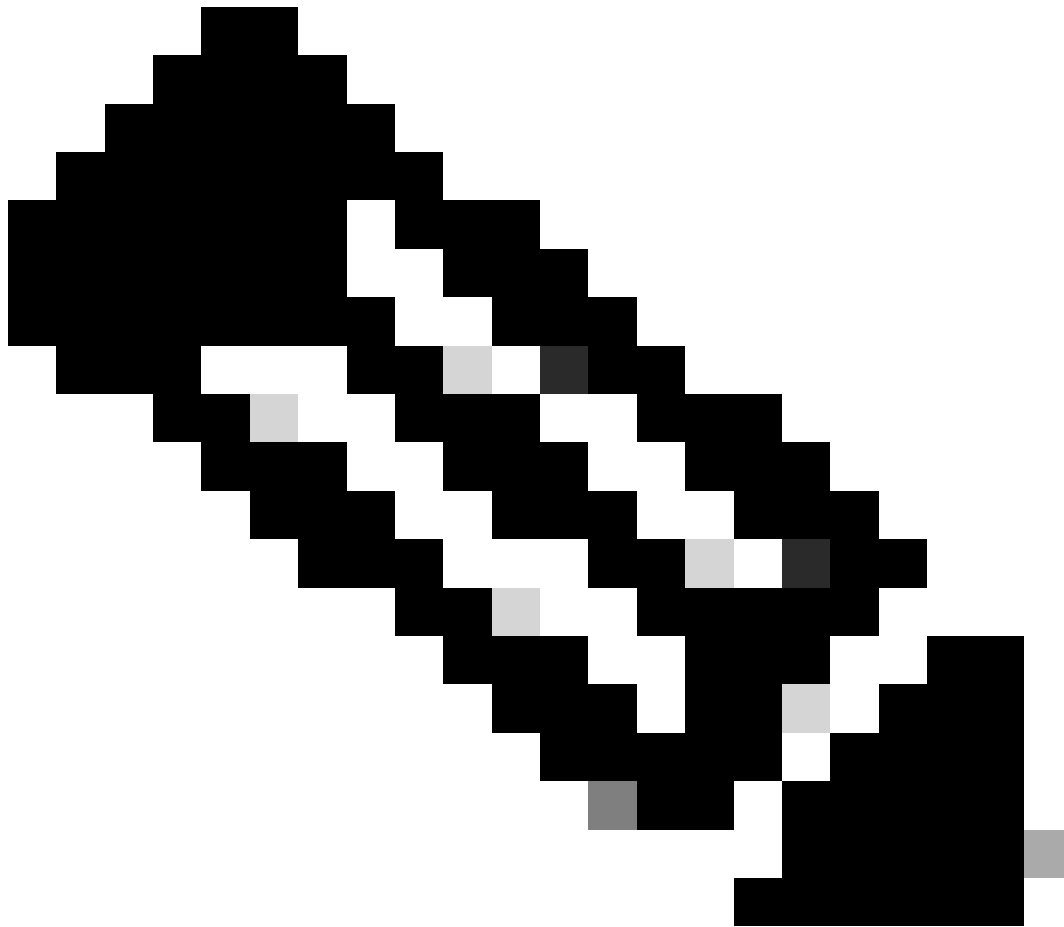


### Network Connection Details:

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

Endereço IP do PC1



Observação: como um certificado autoassinado está sendo usado para que o Gateway se identifique, vários avisos de certificado podem aparecer durante a tentativa de conexão. Eles são esperados e devem ser aceitos para que a conexão continue. Para evitar esses avisos de certificado, o certificado autoassinado apresentado deve ser instalado no repositório de certificados confiáveis da máquina cliente ou, se um certificado de terceiros estiver sendo usado, o certificado da Autoridade de Certificação deverá estar no repositório de certificados confiáveis.

---

Conecte-se ao seu headend da VPN `vpn.example.com` e insira o nome de usuário e as credenciais.



**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...

---

: no ASA, você pode definir vários níveis de depuração; por padrão, o nível 1 é usado. Se você alterar o nível de depuração, o detalhamento das depurações aumentará. Faça isso com cuidado, especialmente em ambientes de produção.

---

Você pode habilitar a depuração para diagnosticar a conexão VPN no ASA.

- `debug webvpn anyconnect` - Exibe mensagens de depuração sobre conexões com clientes AnyConnect VPN.

Consulte [este](#) documento para solucionar problemas comuns encontrados no lado do cliente.

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.