

# Configuración del Equilibrio de Carga del Cliente VPN con Ordenamiento Cíclico DNS en ASA

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Paso 1. Configuración de VPN Anyconnect en ASA](#)

[Paso 2. Configuración de DNS de ordenamiento cíclico en el servidor DNS](#)

[Verificación](#)

[Troubleshoot](#)

---

## Introducción

Este documento describe cómo configurar el equilibrio de carga del cliente anyconnect vpn con ordenamiento cíclico DNS en ASA.

## Prerequisites

### Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Ha asignado direcciones IP en sus ASA y ha configurado el gateway predeterminado.
- Anyconnect VPN está configurado en los ASA.
- Los usuarios de VPN pueden conectarse a todos los ASA con el uso de su dirección IP asignada individualmente.
- El servidor DNS de los usuarios de VPN es compatible con ordenamiento cíclico.

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Configurar

### Diagrama de la red

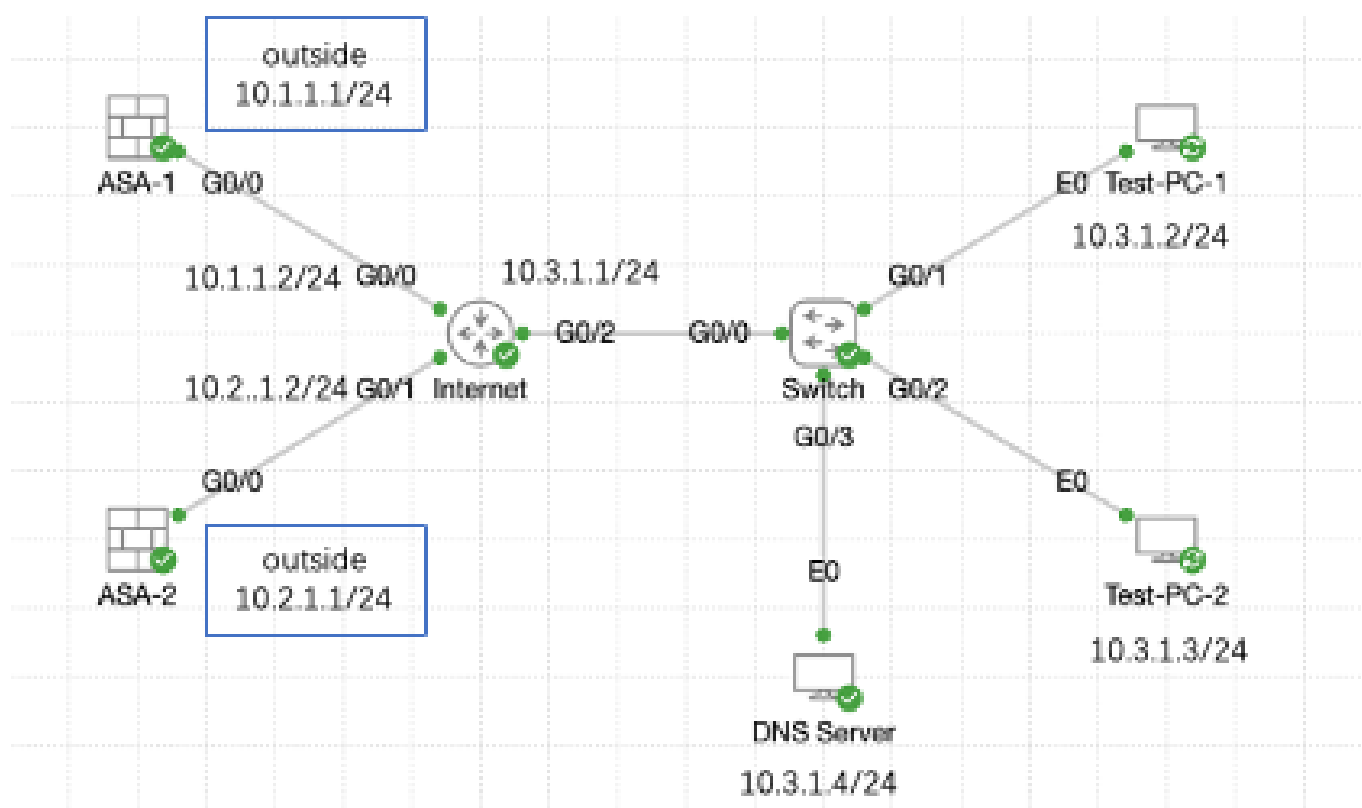


Diagrama de la red

## Configuraciones

### Paso 1. Configuración de VPN Anyconnect en ASA

Para obtener información sobre cómo configurar AnyConnect VPN en ASA, consulte este documento:

- [ASA 8.x: Ejemplo de Configuración de Acceso VPN con AnyConnect VPN Client Usando Certificado Autofirmado](#)

Esta es la configuración de ambos ASA en este ejemplo:

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
```

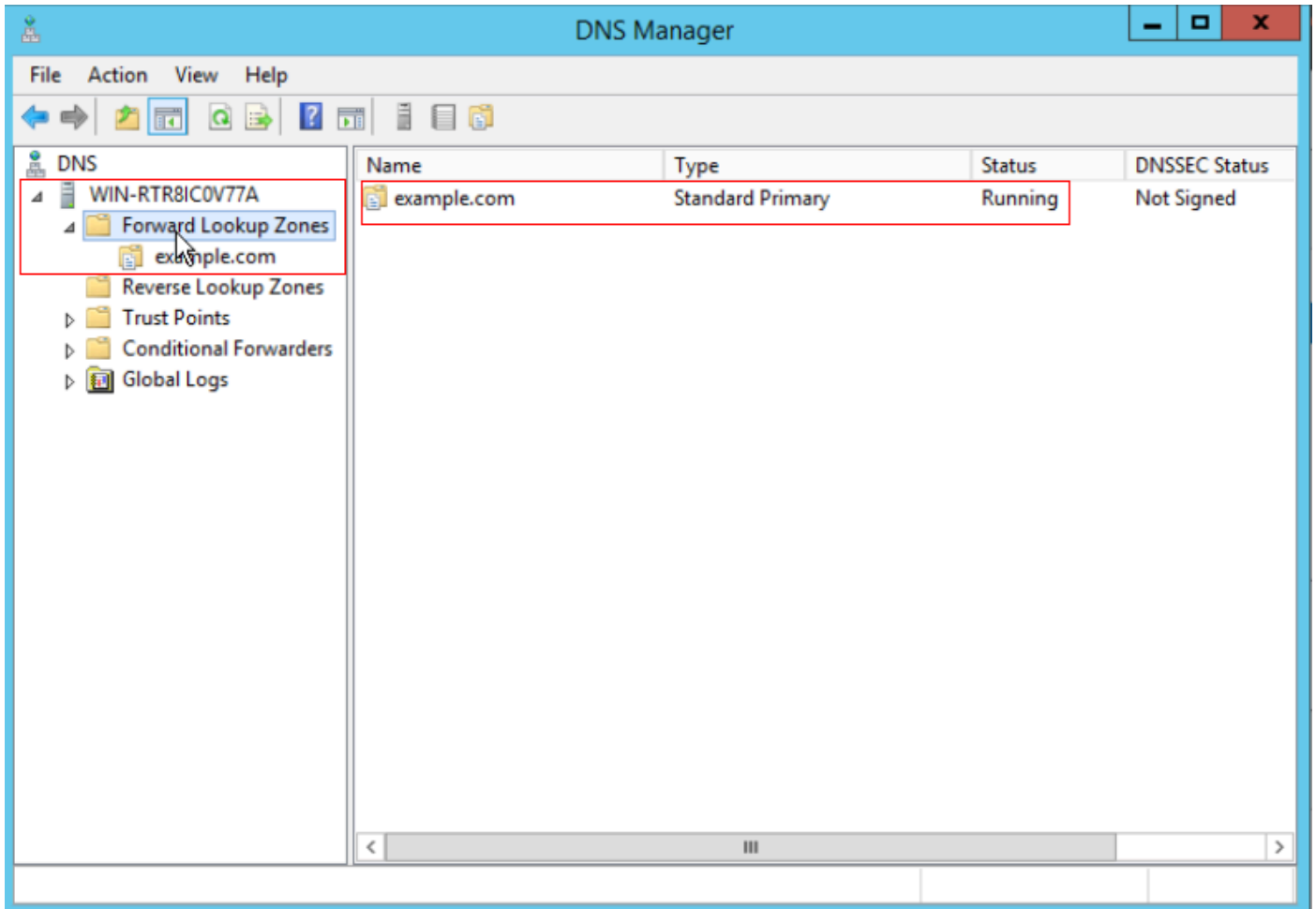
Debe poder conectarse a ambos ASA mediante su dirección IP asignada individualmente antes de pasar al paso 2.

## Paso 2. Configuración de DNS de ordenamiento cíclico en el servidor DNS

Puede utilizar cualquier servidor DNS compatible con ordenamiento cíclico; en este ejemplo, se utiliza el servidor DNS en Windows Server 2019. Para obtener información sobre cómo instalar y configurar el servidor DNS en el servidor Windows, consulte este documento:

- [Instalar y configurar el servidor DNS en Windows Server](#)

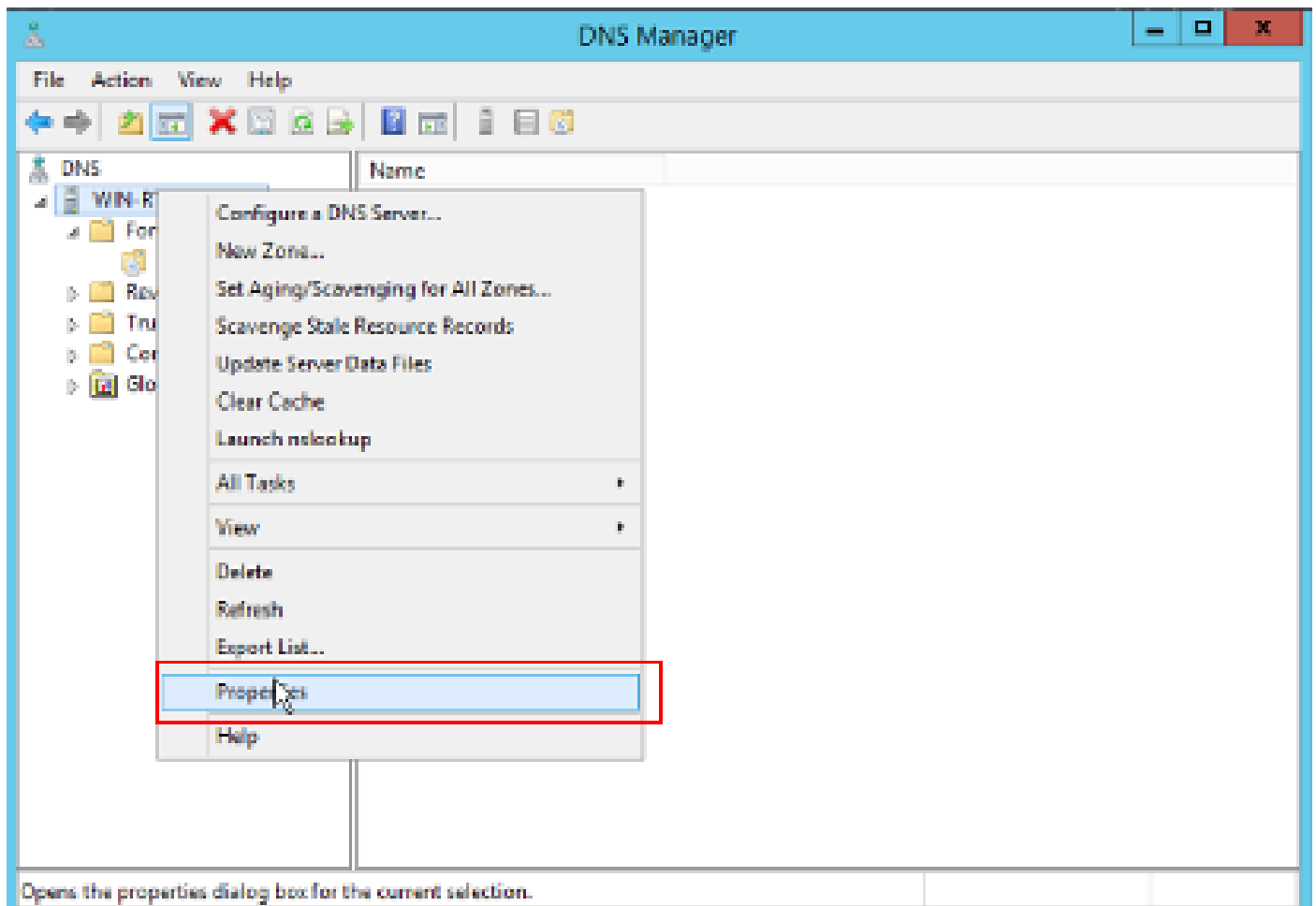
En este ejemplo, 10.3.1.4 es el servidor de Windows con el servidor DNS habilitado para el dominio example.com.



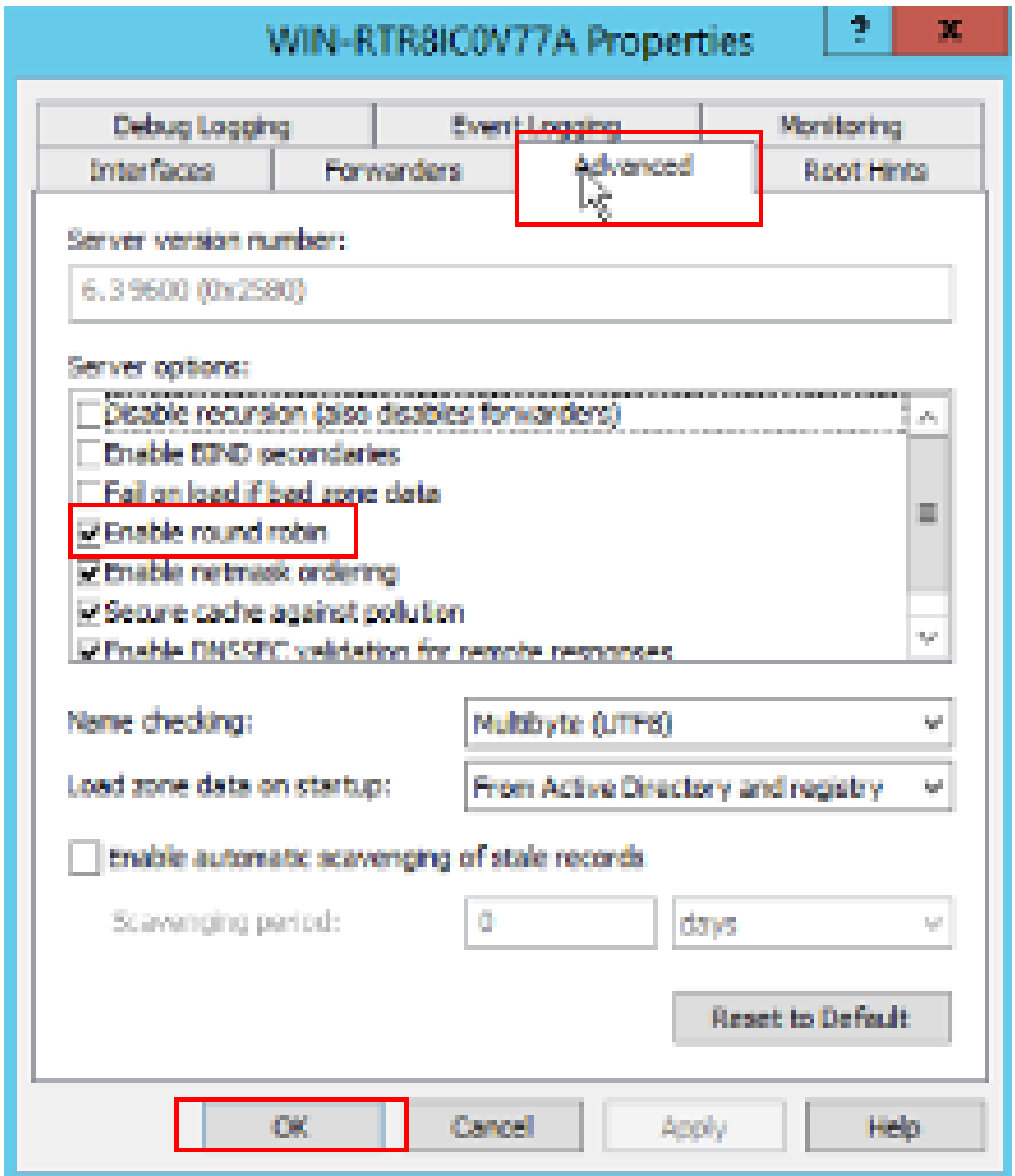
Servidor DNS

Asegúrese de que el ordenamiento cíclico está habilitado para el servidor DNS:

1. En el escritorio de Windows, abra el menú Inicio y seleccione Herramientas administrativas > DNS.
2. En el árbol de la consola, seleccione el servidor DNS que desea gestionar, haga clic con el botón derecho y, a continuación, seleccione Propiedades.
3. En la pestaña Advanced, asegúrese de que la opción Enable round robin esté marcada.



Turno rotativo 1



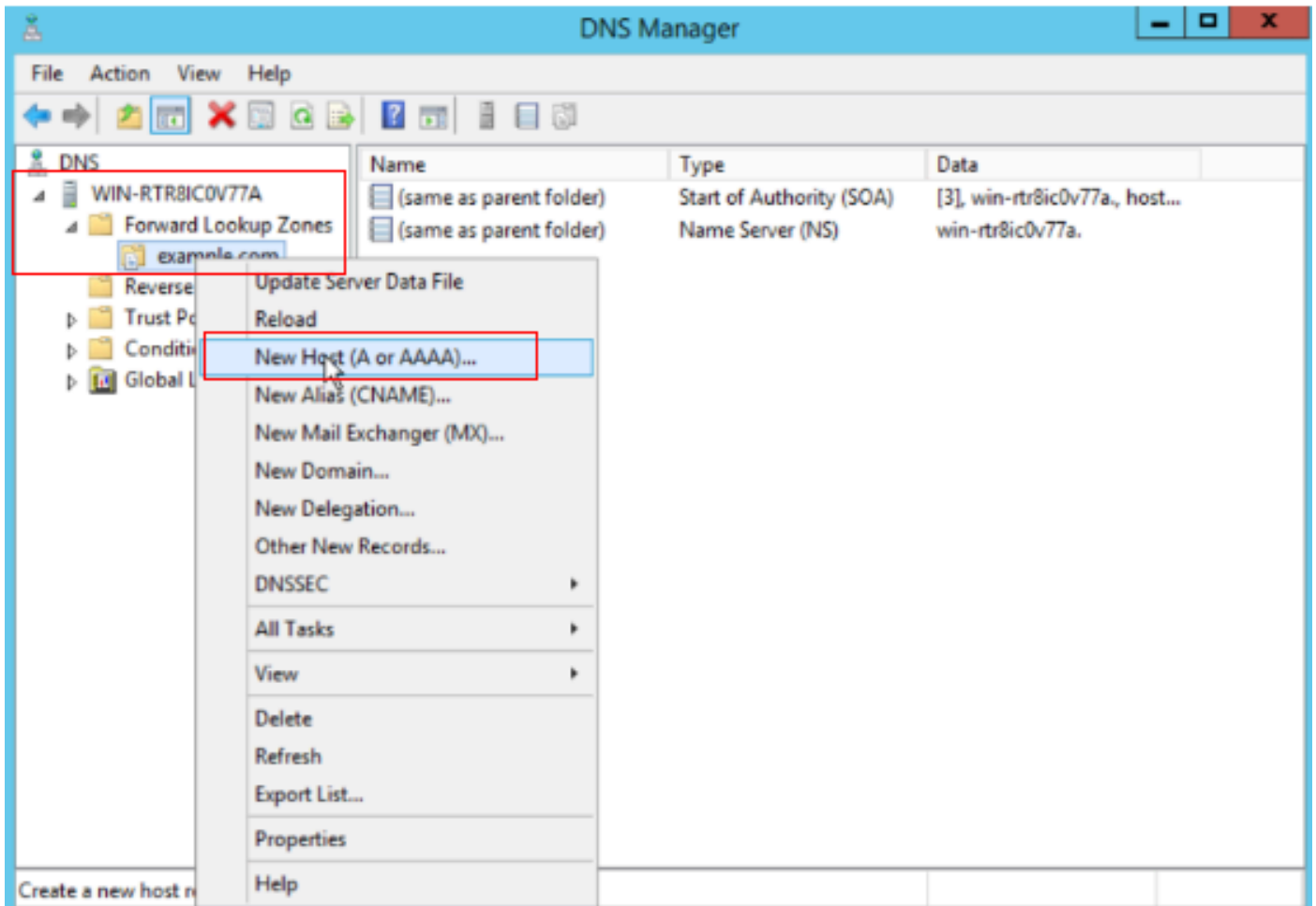
Turno rotativo 2

Cree dos registros de host para servidores VPN ASA:

1. En el escritorio de Windows, abra el menú Inicio y seleccione Herramientas administrativas > DNS.
2. En el árbol de la consola, conéctese al servidor DNS que desea administrar, expanda el servidor DNS, expanda la zona de búsqueda directa, haga clic con el botón derecho y

seleccione Nuevo host (A o AAAA).

3. En la pantalla New Host, especifique el nombre y la dirección IP del registro de host. En este ejemplo, vpn y 10.1.1.1.
4. Seleccione Add Host para crear el registro.



Crear nuevo host




## 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 1

Repita pasos similares para crear otro registro de host y asegúrese de que Name es el mismo; en este ejemplo, Name es vpn, IP address es 10.2.1.1.

## New Host X

Name (uses parent domain name if blank):

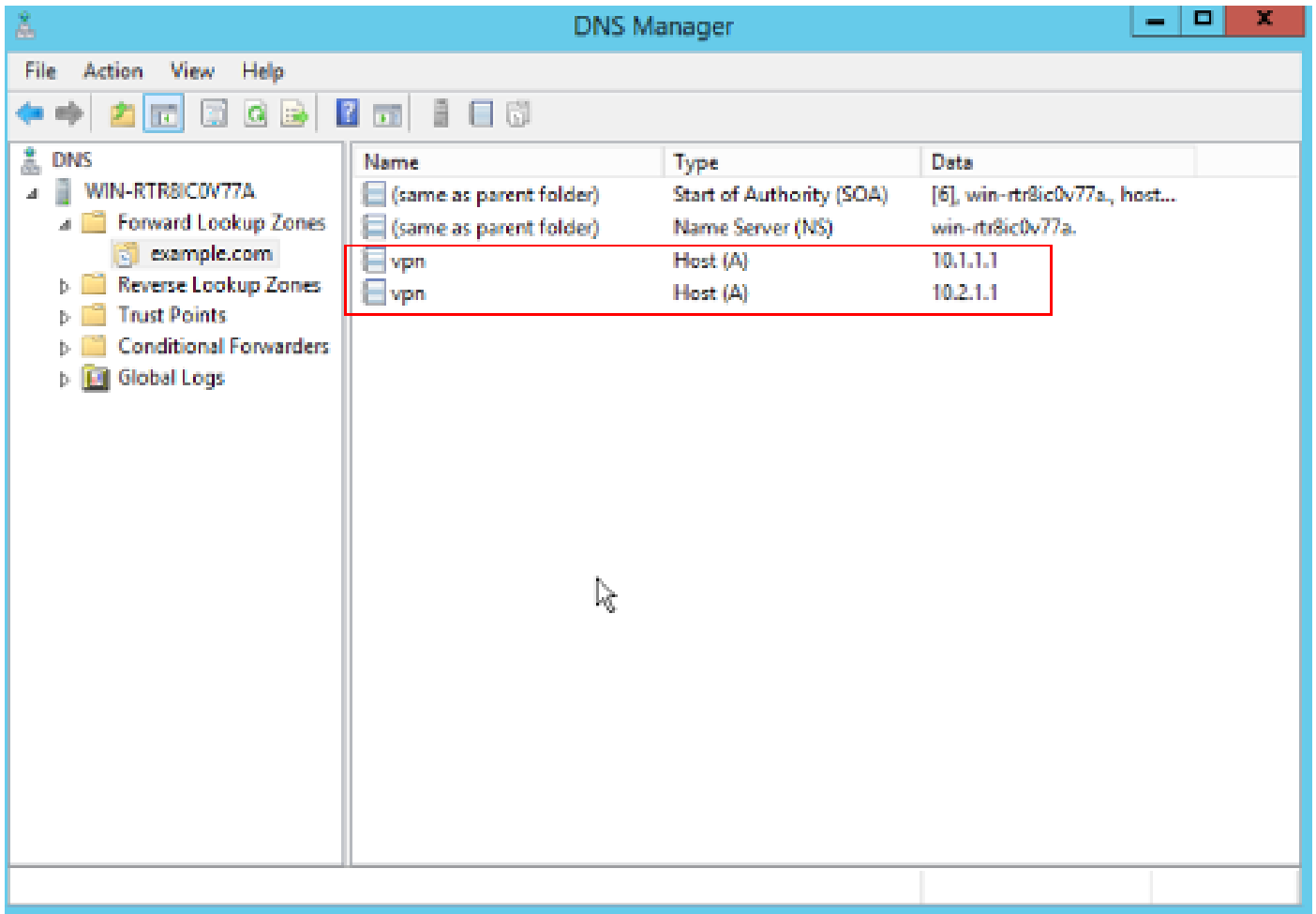
Fully qualified domain name (FQDN):

IP address:

Create associated pointer (PTR) record

Registro de host 2

Puede encontrar que hay dos hosts 10.1.1.1 y 10.2.1.1 asociados al mismo registro vpn.example.com.



Dos registros de host

## Verificación

Vaya al equipo cliente donde está instalado el cliente Cisco AnyConnect Secure Mobility; en este ejemplo, Test-PC-1, compruebe que el servidor DNS es 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



Nota: Dado que se está utilizando un certificado autofirmado para que la puerta de enlace se identifique a sí misma, pueden aparecer varias advertencias de certificado durante el intento de conexión. Se esperan y deben aceptarse para que la conexión continúe. Para evitar estas advertencias de certificado, el certificado autofirmado que se presenta debe estar instalado en el almacén de certificados de confianza del equipo cliente o, si se está utilizando un certificado de terceros, el certificado de la Autoridad de certificación debe estar en el almacén de certificados de confianza.

---

Conéctese a la cabecera de VPN [vpn.example.com](https://vpn.example.com) e introduzca el nombre de usuario y las credenciales.



**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...

---

: En ASA, puede establecer varios niveles de depuración; de forma predeterminada, se utiliza el nivel 1. Si cambia el nivel de depuración, aumenta el nivel de detalle de las depuraciones. Hágalo con precaución, especialmente en entornos de producción.

---

Puede habilitar debug para diagnosticar la conexión VPN en ASA.

- `debug webvpn anyconnect` - Muestra mensajes de depuración sobre las conexiones a los clientes VPN de Anyconnect.

Consulte [este](#) documento para resolver problemas comunes encontrados en el lado del cliente.

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).