

在ASA上配置使用DNS轮询的VPN客户端负载均衡

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置](#)

[步骤1:在ASA上配置Anyconnect VPN](#)

[第二步：在DNS服务器上配置轮询DNS](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何使用ASA上的DNS轮询配置anyconnect vpn客户端负载均衡。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 您已在 ASA 上分配了 IP 地址并配置了默认网关。
- Anyconnect VPN在ASA上配置。
- VPN用户可以使用其单独分配的IP地址连接到所有ASA。
- VPN用户的DNS服务器支持轮询功能。

使用的组件

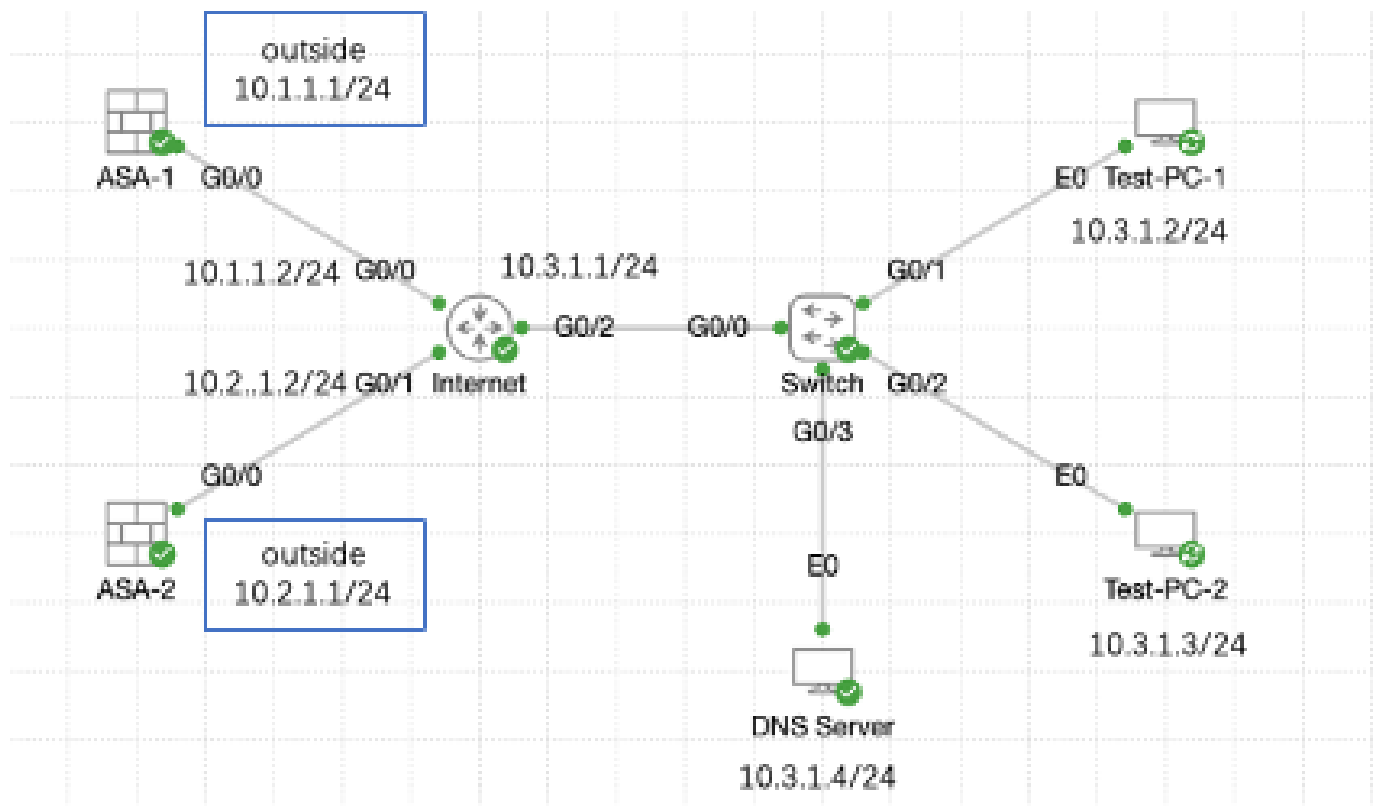
本文档中的信息基于以下软件和硬件版本：

- Anyconnect VPN客户端软件版本4.10.08025
- 思科ASA软件版本9.18.2
- Windows Server 2019

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



网络图

配置

步骤1:在ASA上配置Anyconnect VPN

有关如何在ASA上配置anyconnect VPN，请参阅以下文档：

- [ASA 8.x：使用自签名证书通过AnyConnect VPN客户端进行VPN访问的配置示例](#)

以下是该示例中两个ASA的配置：

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
```

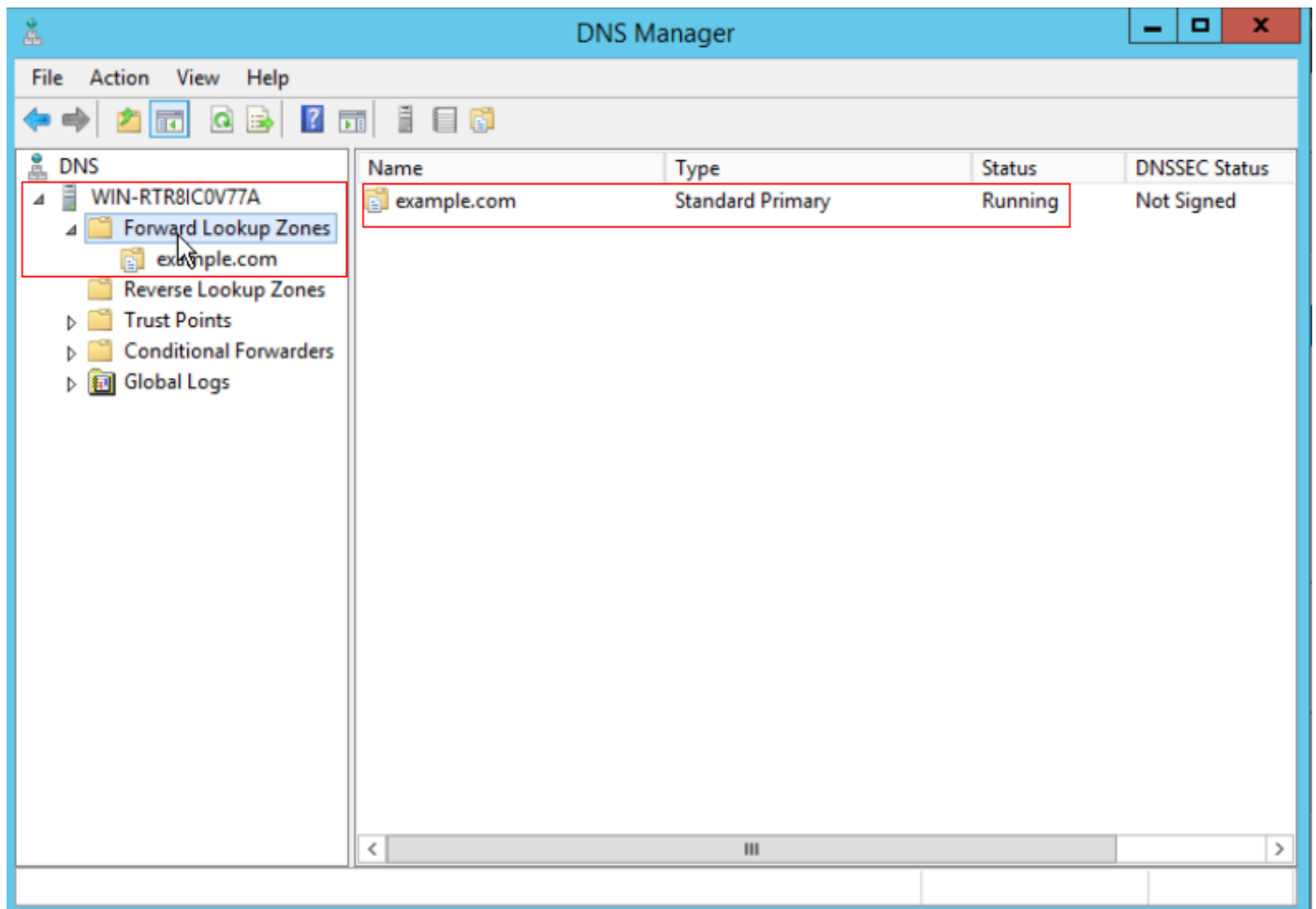
在进入第2步之前，您必须能够使用单独分配的IP地址连接到两个ASA。

第二步：在DNS服务器上配置轮询DNS

您可以使用任何能够轮询的DNS服务器，在本例中，使用windows server 2019上的DNS服务器。有关如何在Windows服务器上安装和配置DNS服务器的信息，请参阅以下文档：

- [在Windows服务器上安装和配置DNS服务器](#)

在本示例中，10.3.1.4是启用了example.com域的DNS服务器的Windows服务器。

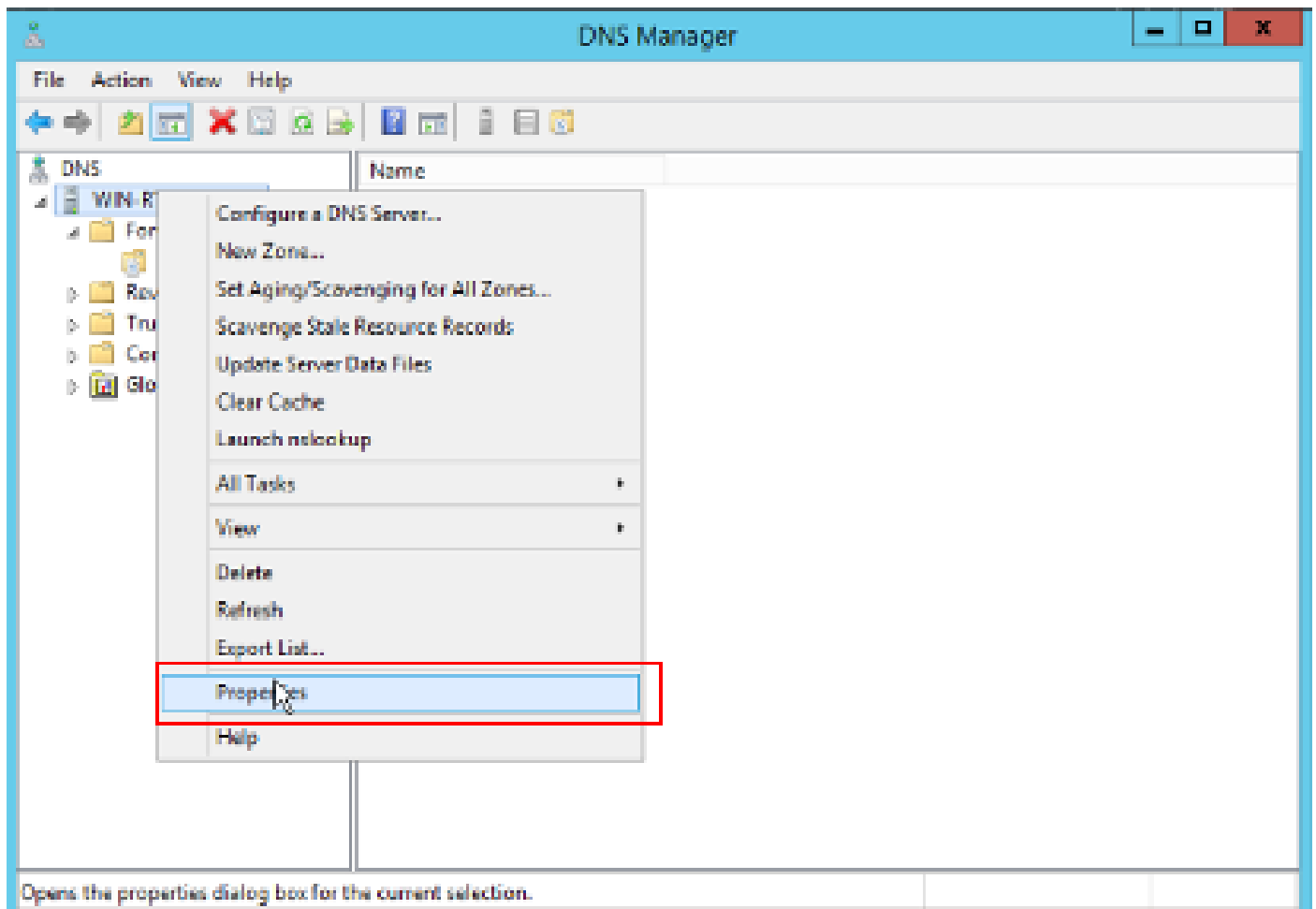


DNS 服务器

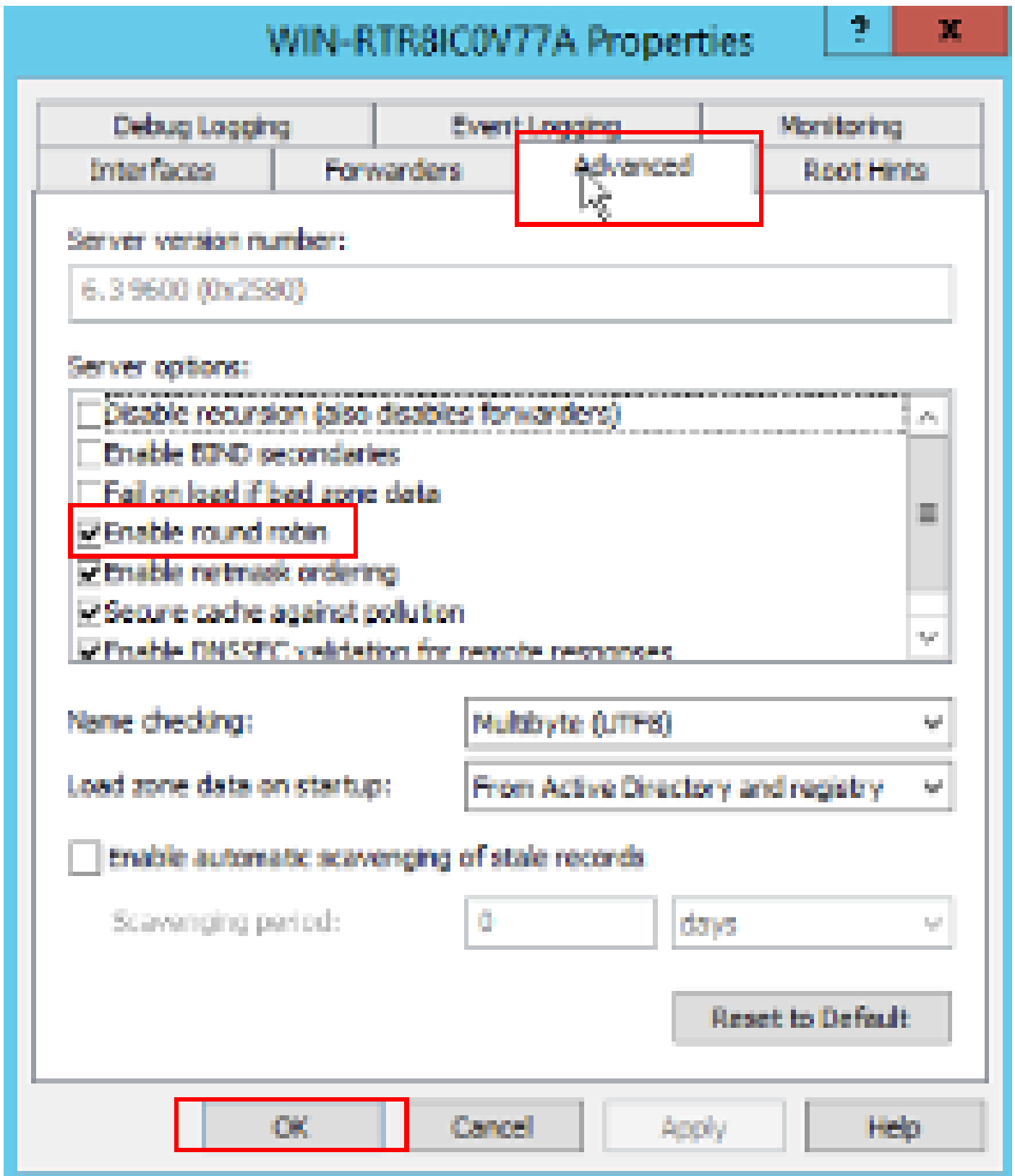
确保您的DNS服务器已启用轮询：

1. 从Windows桌面打开开始菜单，选择管理工具 > DNS。
2. 在控制台树中，选择要管理的DNS服务器，右键单击，然后选择属性。

3. 在Advanced选项卡下，确保选中Enable round robin。



循环法1

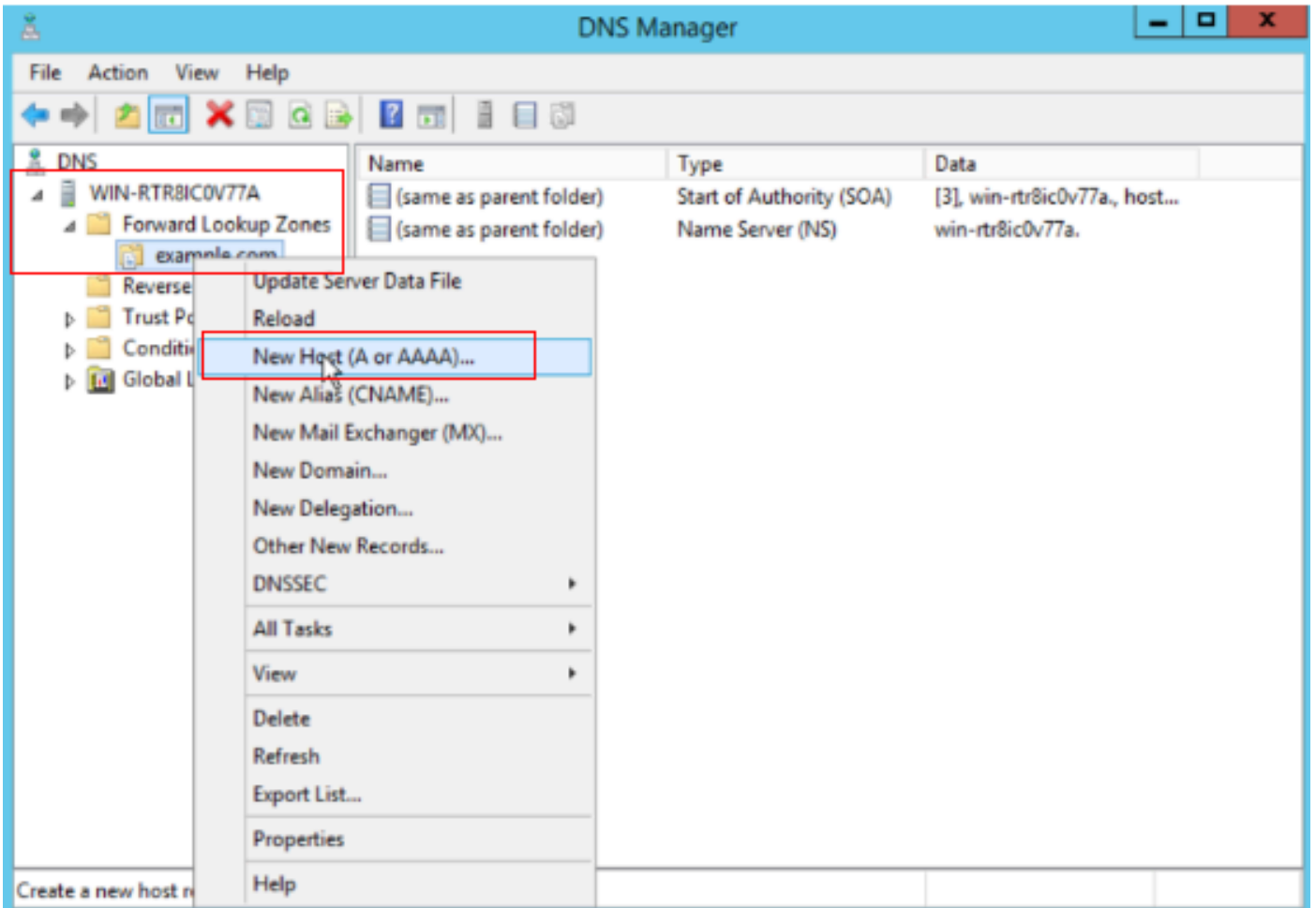


循环法2

为ASA VPN服务器创建两个主机记录：

1. 从Windows桌面打开开始菜单，选择管理工具 > DNS。
2. 在控制台树中，连接到要管理的DNS服务器，展开DNS服务器，展开正向查找区域，右键单击，然后选择新建主机（A或AAAA）。
3. 在New Host屏幕上，指定主机记录的Name和IP address。在本例中为vpn和10.1.1.1。

4. 选择Add Host创建记录。



创建新主机


New Host X

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

IP address:

Create associated pointer (PTR) record



主机记录1

重复类似步骤创建另一个主机记录，并确保Name相同，在本示例中，Name为vpn，IP address为10.2.1.1。

New Host X

Name (uses parent domain name if blank):

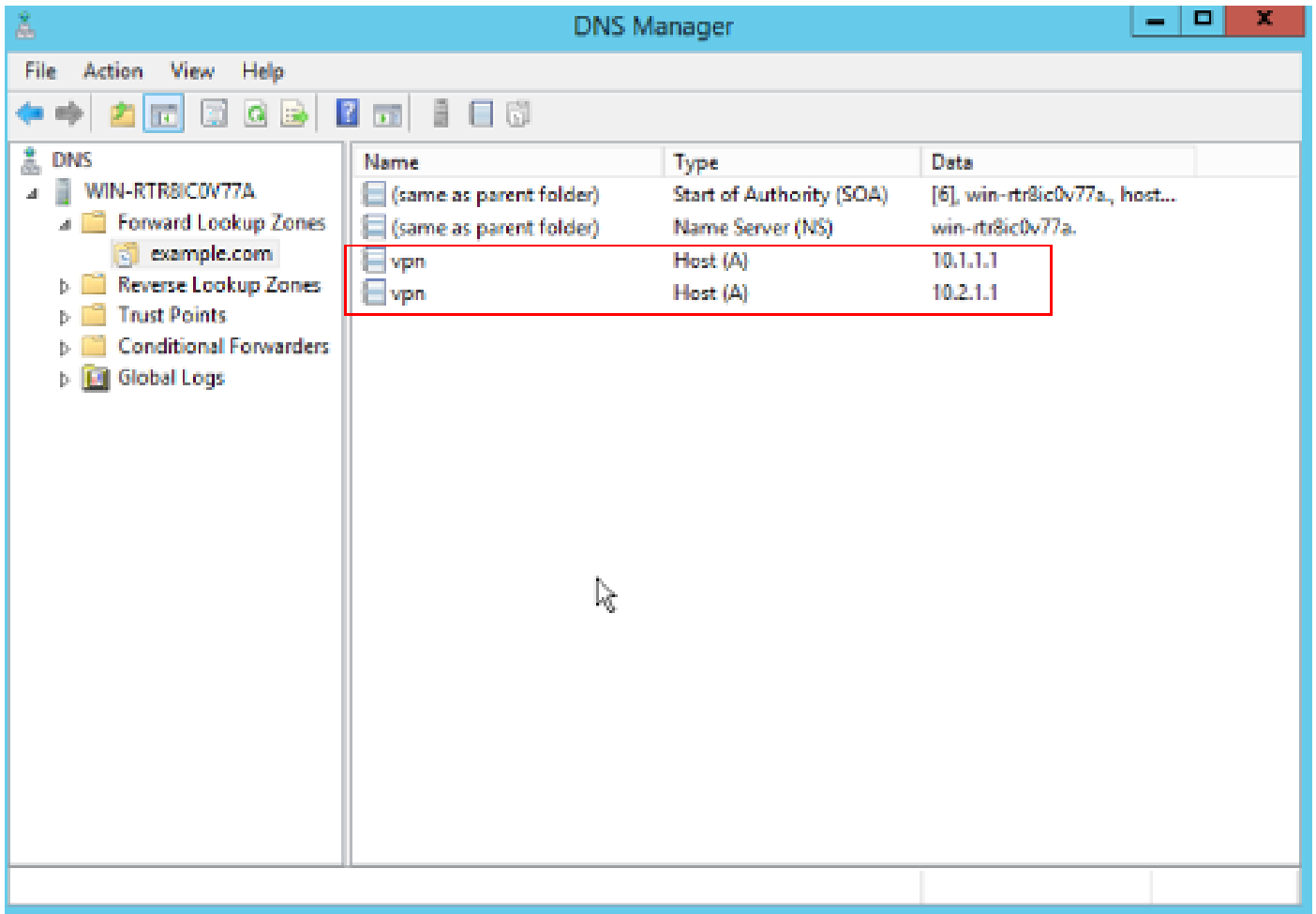
Fully qualified domain name (FQDN):

IP address:

Create associated pointer (PTR) record

主机记录2

您会发现，有两个主机10.1.1.1和10.2.1.1与同一记录vpn.example.com关联。



两个主机记录

验证

导航到安装Cisco AnyConnect安全移动客户端的客户端（在本示例中为Test-PC-1），验证DNS服务器是否为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



注意：由于自签名证书正用于网关进行自我标识，因此在尝试连接期间可能会显示多个证书警告。这些应为预期值，必须接受它们才能继续连接。为了避免这些证书警告，提供的自签名证书必须安装在客户端计算机的受信任证书库中，或者如果正在使用第三方证书，则证书颁发机构证书必须位于受信任的证书库中。

连接到您的VPN头端vpn.example.com并输入用户名和凭证。



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...

上，您可以设置各种调试级别；默认情况下，使用级别1。如果更改调试级别，调试的冗余将增加。请谨慎执行此操作，尤其是在生产环境中。

您可以启用debug以诊断ASA上的VPN连接。

- `debug webvpn anyconnect` - 显示与到Anyconnect VPN客户端的连接有关的调试消息。

要对客户端上的常见问题进行故障排除，请参阅[此](#)文档。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。