

ASAでのDNSラウンドロビンによるVPNクライアントロードバランスの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[ステップ 1: ASAでのAnyConnect VPNの設定](#)

[ステップ 2: DNSサーバでのラウンドロビンDNSの設定](#)

[確認](#)

[トラブルシューティング](#)

はじめに

このドキュメントでは、ASAでDNSラウンドロビンを使用したAnyConnect VPNクライアント(SVC)のロードバランスを設定する方法について説明します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- ASA に IP アドレスが割り当てられていて、デフォルト ゲートウェイが設定されている。
- Anyconnect VPNがASAで設定されている。
- VPNユーザは、個別に割り当てられたIPアドレスを使用してすべてのASAに接続できます。
- VPNユーザのDNSサーバはラウンドロビン対応です。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

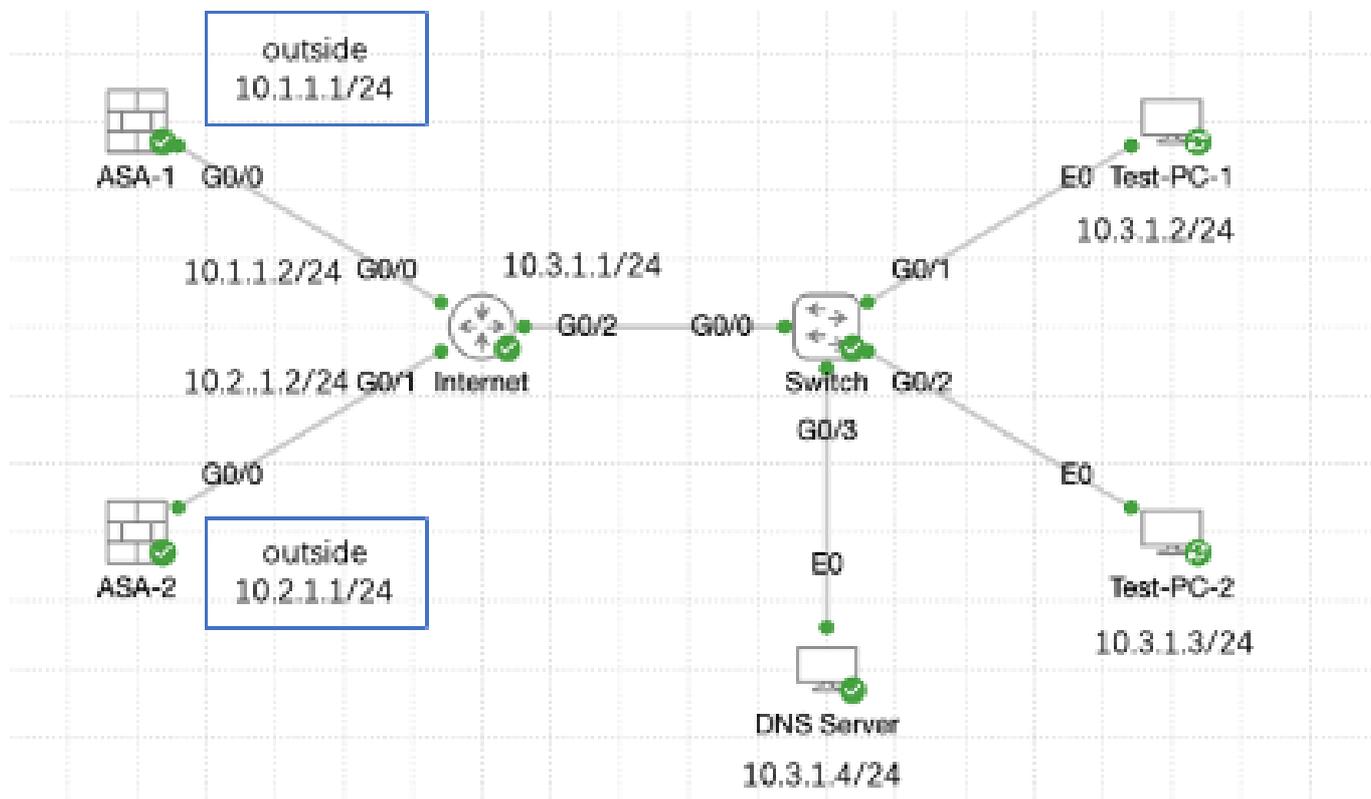
- Anyconnect VPN Clientソフトウェアリリース4.10.08025
- Cisco ASAソフトウェアリリース9.18.2
- ウィンドウサーバ2019

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図



ネットワーク図

コンフィギュレーション

ステップ 1 : ASAでのAnyConnect VPNの設定

ASAでのAnyConnect VPNの設定方法については、次のドキュメントを参照してください。

- [ASA 8.x : 自己署名証明書を使用したAnyConnect VPNクライアントによるVPNアクセスの設定例](#)

次に、この例の両方のASAの設定を示します。

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
```

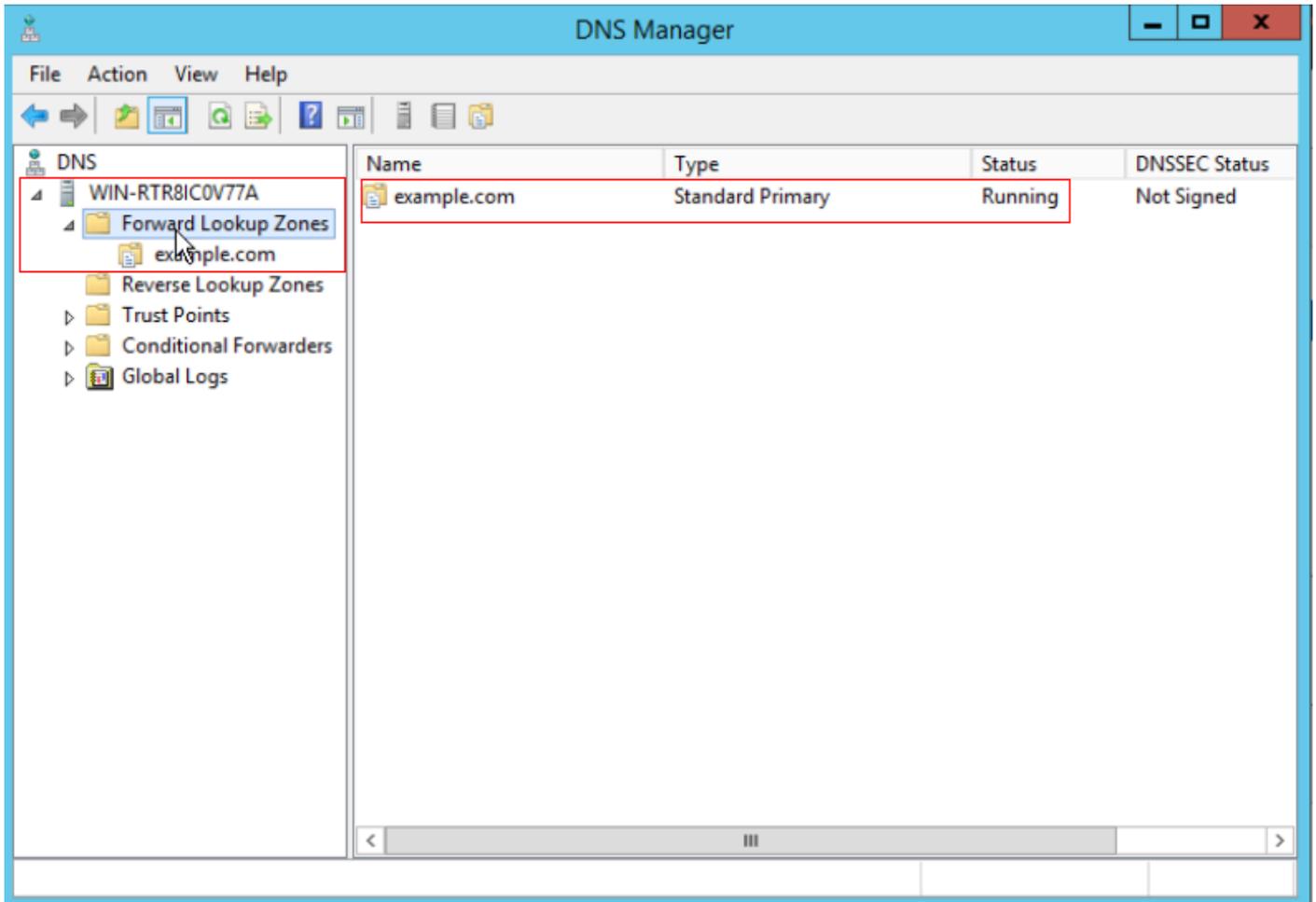
手順2に進む前に、個別に割り当てられたIPアドレスを使用して両方のASAに接続できる必要があります。

ステップ 2 : DNSサーバでのラウンドロビンDNSの設定

ラウンドロビン対応の任意のDNSサーバを使用できます。この例では、Windows Server 2019のDNSサーバが使用されています。WindowsサーバにDNSサーバをインストールして設定する方法については、次のドキュメントを参照してください。

- [Windows ServerでのDNSサーバのインストールと設定](#)

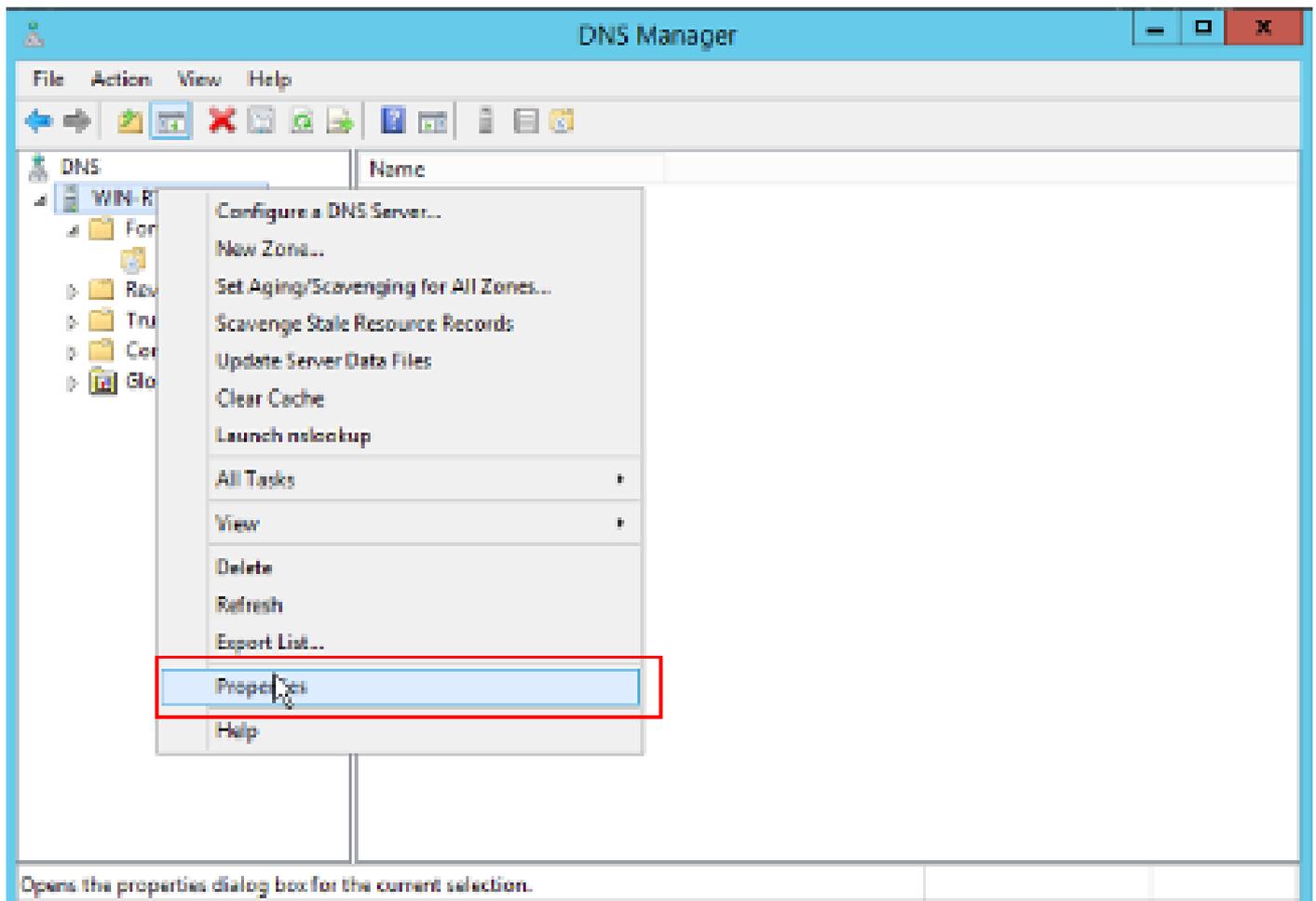
この例では、10.3.1.4はドメインexample.comに対してDNSサーバが有効になっているWindowsサーバです。



DNS サーバ

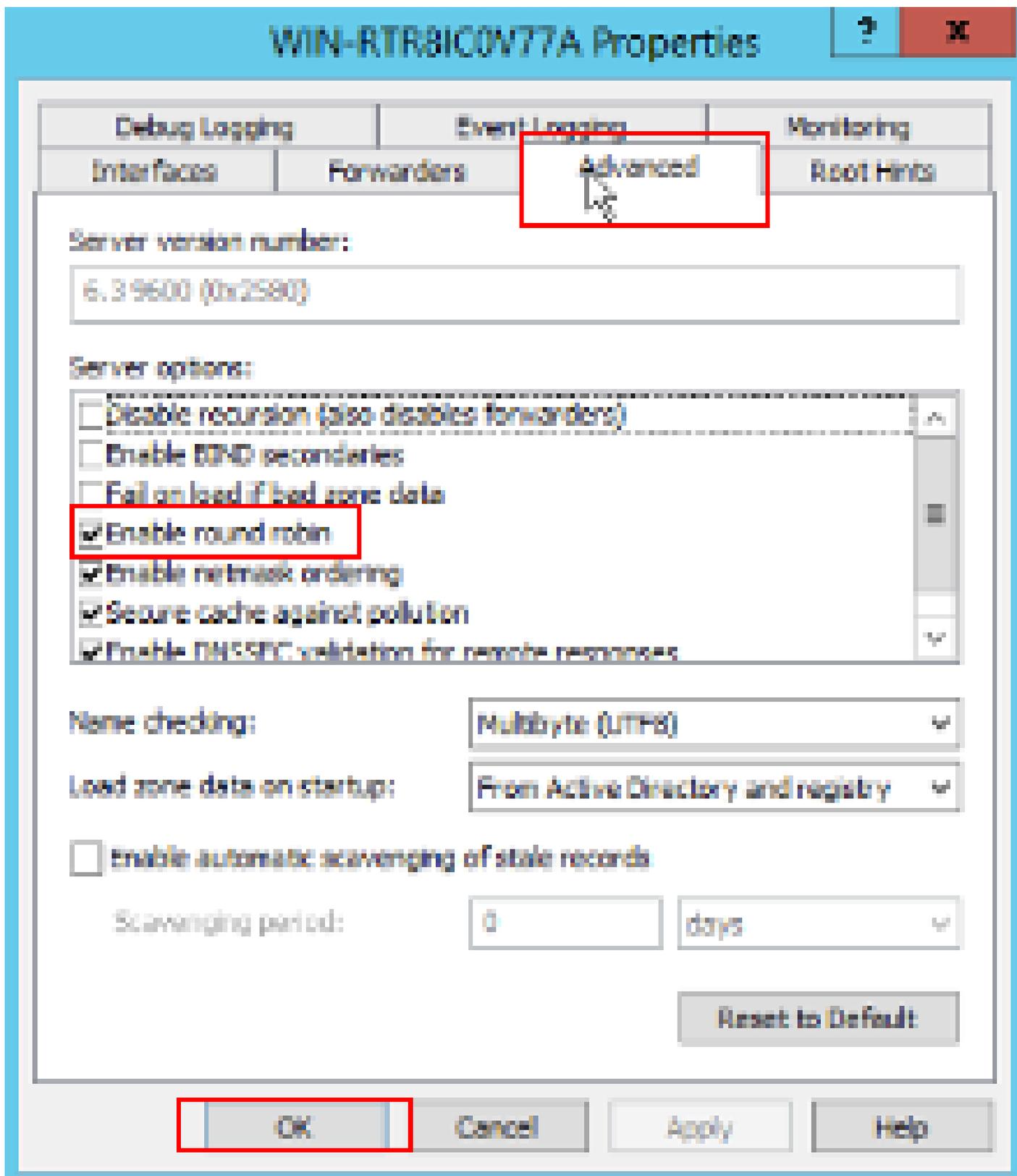
DNSサーバでラウンドロビンが有効になっていることを確認します。

1. WindowsのデスクトップでStartメニューを開き、Administrative Tools > DNSの順に選択します。
2. コンソールツリーで、管理するDNSサーバを選択し、右クリックしてPropertiesを選択します。
3. タブAdvancedで、Enable round robinにチェックマークが入っていることを確認します。



ラウンドロビン1

ラウ

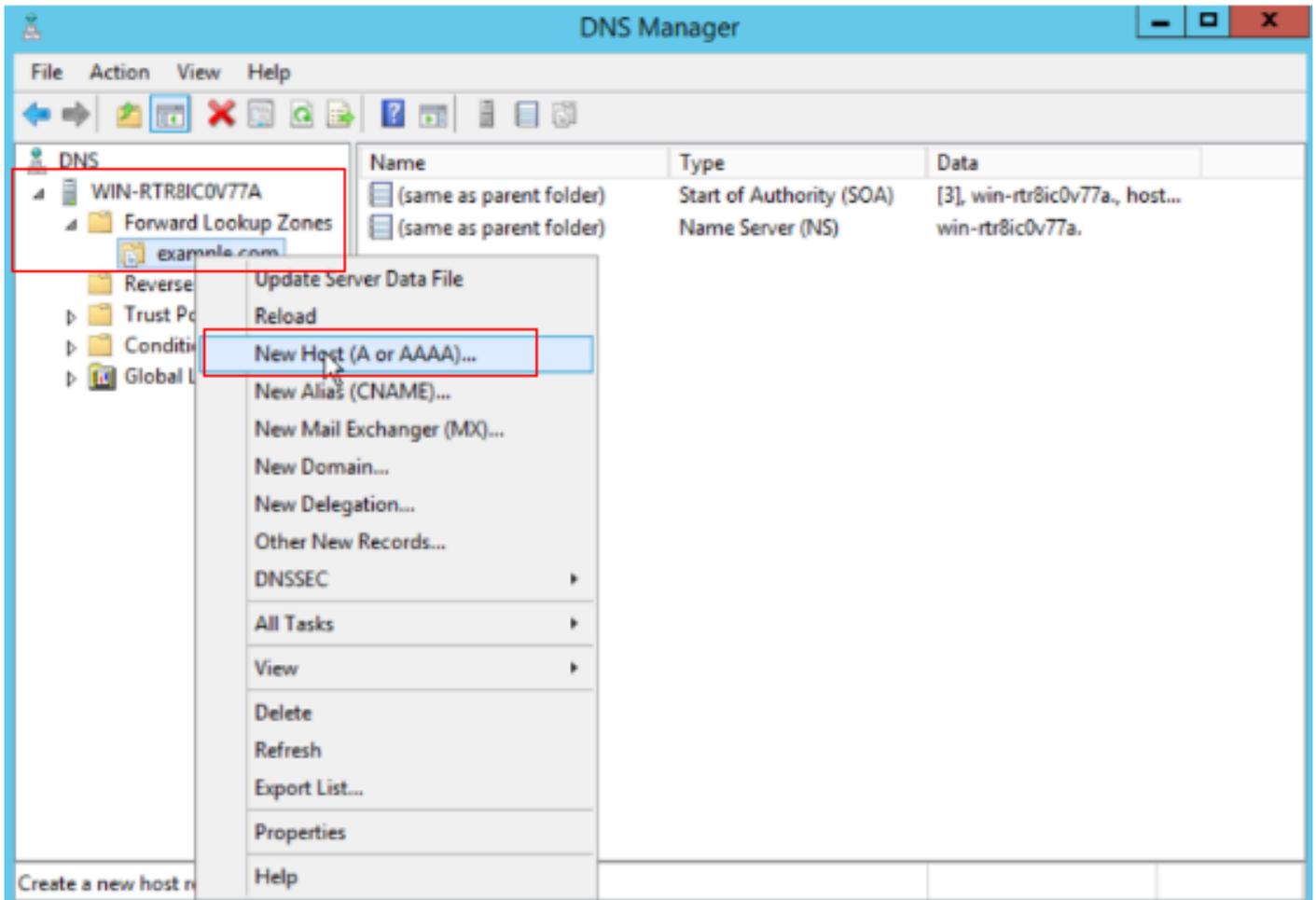


ンドロビン2

ASA VPNサーバ用に2つのホストレコードを作成します。

1. WindowsのデスクトップでStartメニューを開き、Administrative Tools > DNSの順に選択します。
2. コンソールツリーで、管理するDNSサーバに接続し、DNSサーバを展開し、前方参照ゾーンを展開します。右クリックして、New Host (A or AAAA)を選択します。

3. New Host画面で、ホストレコードのNameとIP addressを指定します。この例では、vpnと10.1.1.1です。
4. Add Hostを選択してレコードを作成します。



新しいホストの作成

New Host ✕

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

IP address:

Create associated pointer (PTR) record



ホストレコード1

同様の手順を繰り返して、別のホストレコードを作成し、Nameが同じであることを確認します。この例では、Nameがvpn、IP addressが10.2.1.1です。

New Host X

Name (uses parent domain name if blank):

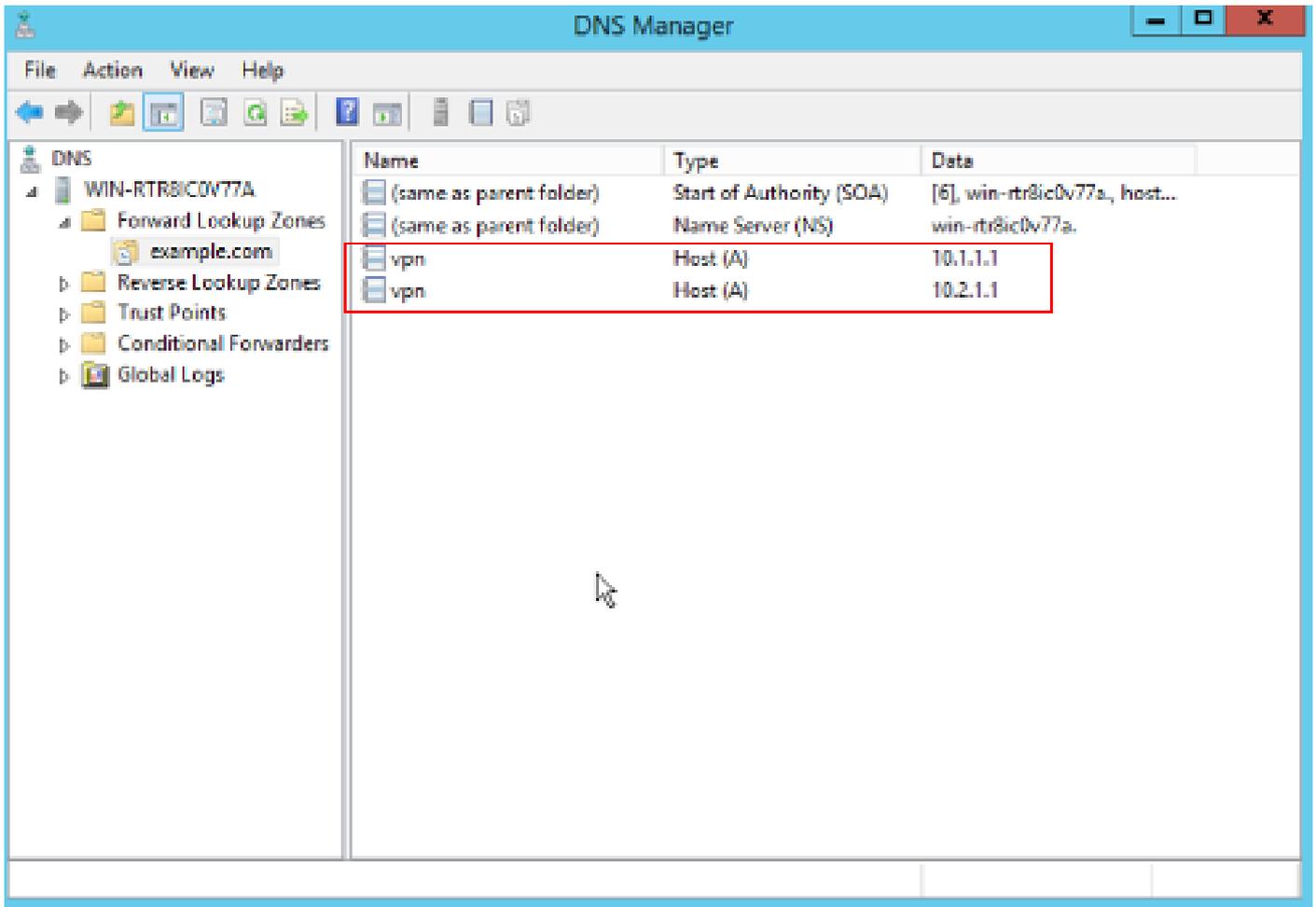
Fully qualified domain name (FQDN):

IP address:

Create associated pointer (PTR) record

ホストレコード2

2つのホスト10.1.1.1と10.2.1.1が同じレコードvpn.example.comに関連付けられていることがわかります。



2つのホストレコード

確認

Cisco AnyConnectセキュアモバイルクライアントがインストールされているクライアントマシンに移動します (この例ではTest-PC-1)。DNSサーバが10.3.1.4であることを確認します。

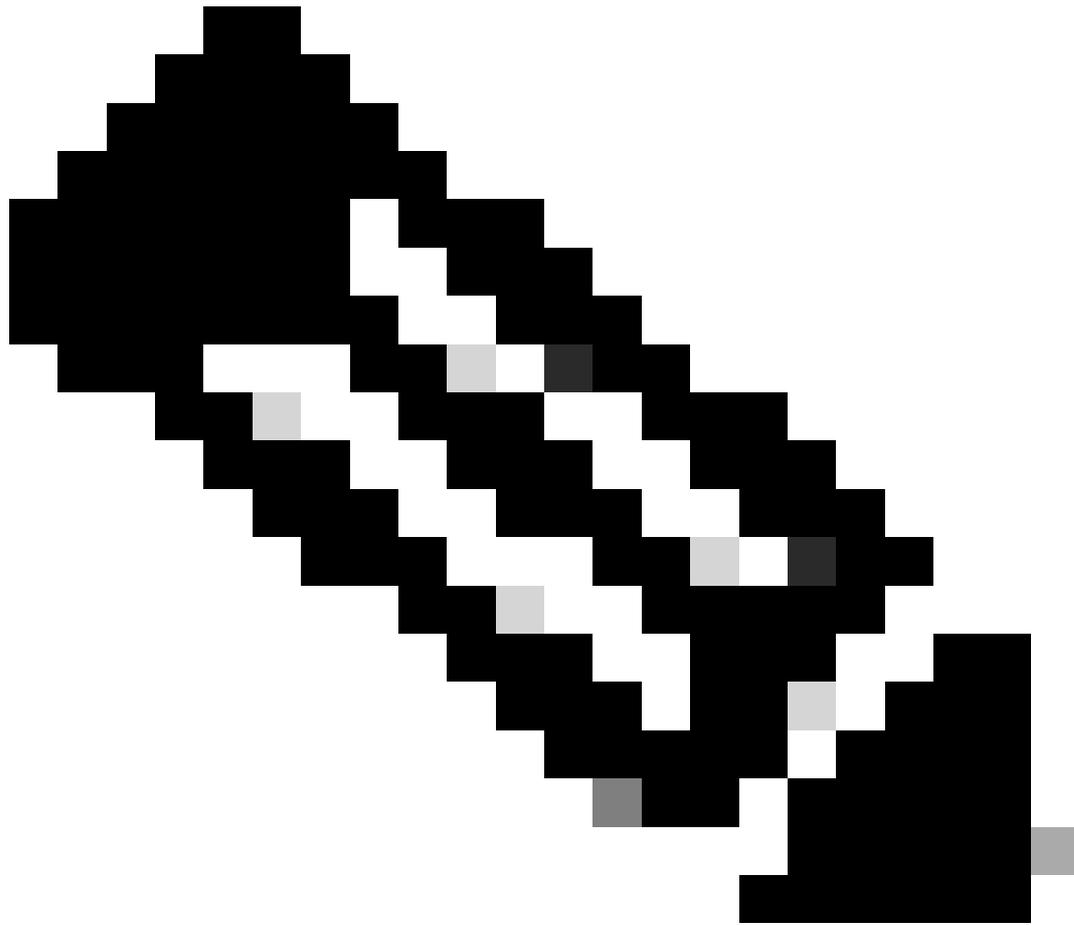
Network Connection Details



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：ゲートウェイが自身を識別するために自己署名証明書が使用されているため、接続試行中に複数の証明書の警告が表示される場合があります。これらは接続を続行するために必要であり、受け入れる必要があります。これらの証明書の警告を回避するには、提示される自己署名証明書がクライアントマシンの信頼された証明書ストアにインストールされている必要があります。サードパーティ証明書が使用されている場合は、認証局(CA)証明書が信頼された証明書ストアに存在する必要があります。

VPNヘッドエンドvpn.example.comに接続し、ユーザ名とクレデンシャルを入力します。



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...



翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。