在ASA上配置使用DNS輪詢的VPN客戶端負載均衡

目錄

簡介

本文檔介紹如何使用ASA上的DNS輪詢來配置anyconnect vpn客戶端負載均衡。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 您已在ASA上分配了IP地址並配置了預設網關。
- ASA上配置了Anyconnect VPN。
- VPN使用者可以使用其單獨分配的IP地址連線到所有ASA。
- VPN使用者的DNS伺服器支援輪詢功能。

採用元件

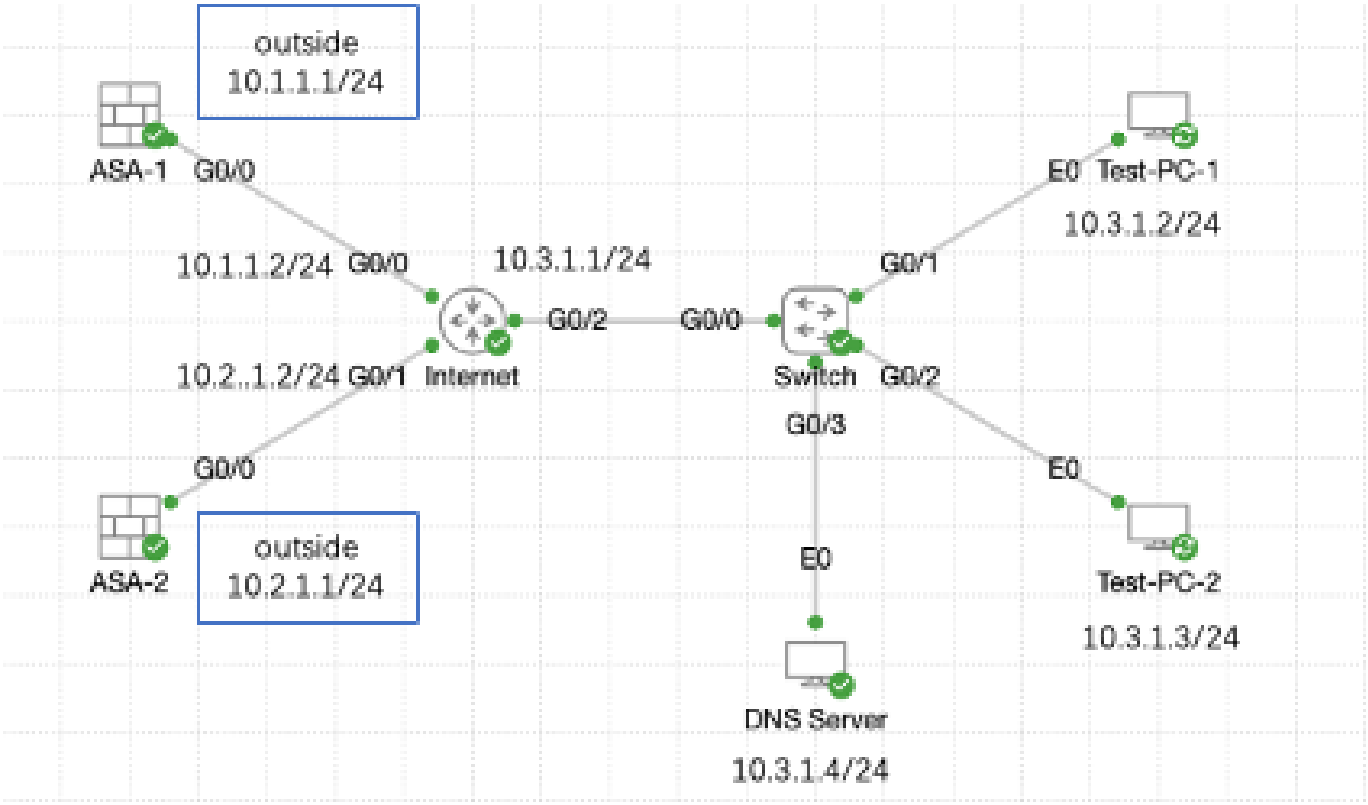
本文中的資訊係根據以下軟體和硬體版本：

- Anyconnect VPN客戶端軟體版本4.10.08025
- 思科ASA軟體版本9.18.2
- Window伺服器2019

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表



網路圖表

組態

步驟 1.在ASA上配置Anyconnect VPN

有關如何在ASA上配置anyconnect VPN，請參閱以下文檔：

- ASA 8.x：使用自簽名證書透過AnyConnect VPN客戶端進行VPN訪問的配置示例

以下是此示例中兩個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
```

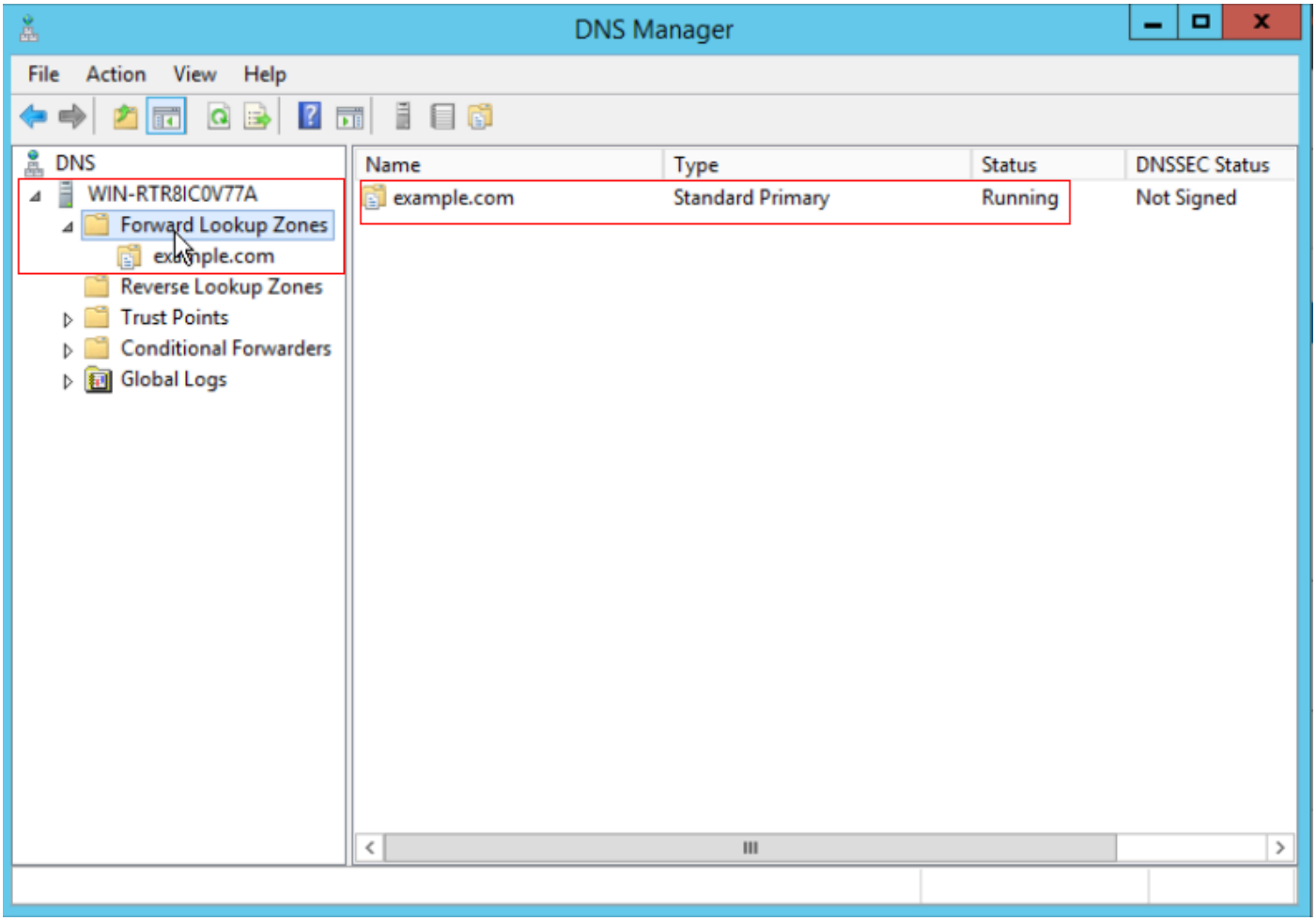
在進入第2步之前，您必須能夠使用單獨分配的IP地址連線到兩個ASA。

步驟 2.在DNS伺服器上配置輪詢DNS

您可以使用任何輪詢功能DNS伺服器，在本例中，使用Windows Server 2019上的DNS伺服器。有關如何在Windows伺服器上安裝和配置DNS伺服器，請參閱以下文檔：

- 在Windows Server上安裝並配置DNS伺服器

在本示例中，10.3.1.4是啟用了DNS伺服器供域example.com使用的windows伺服器。

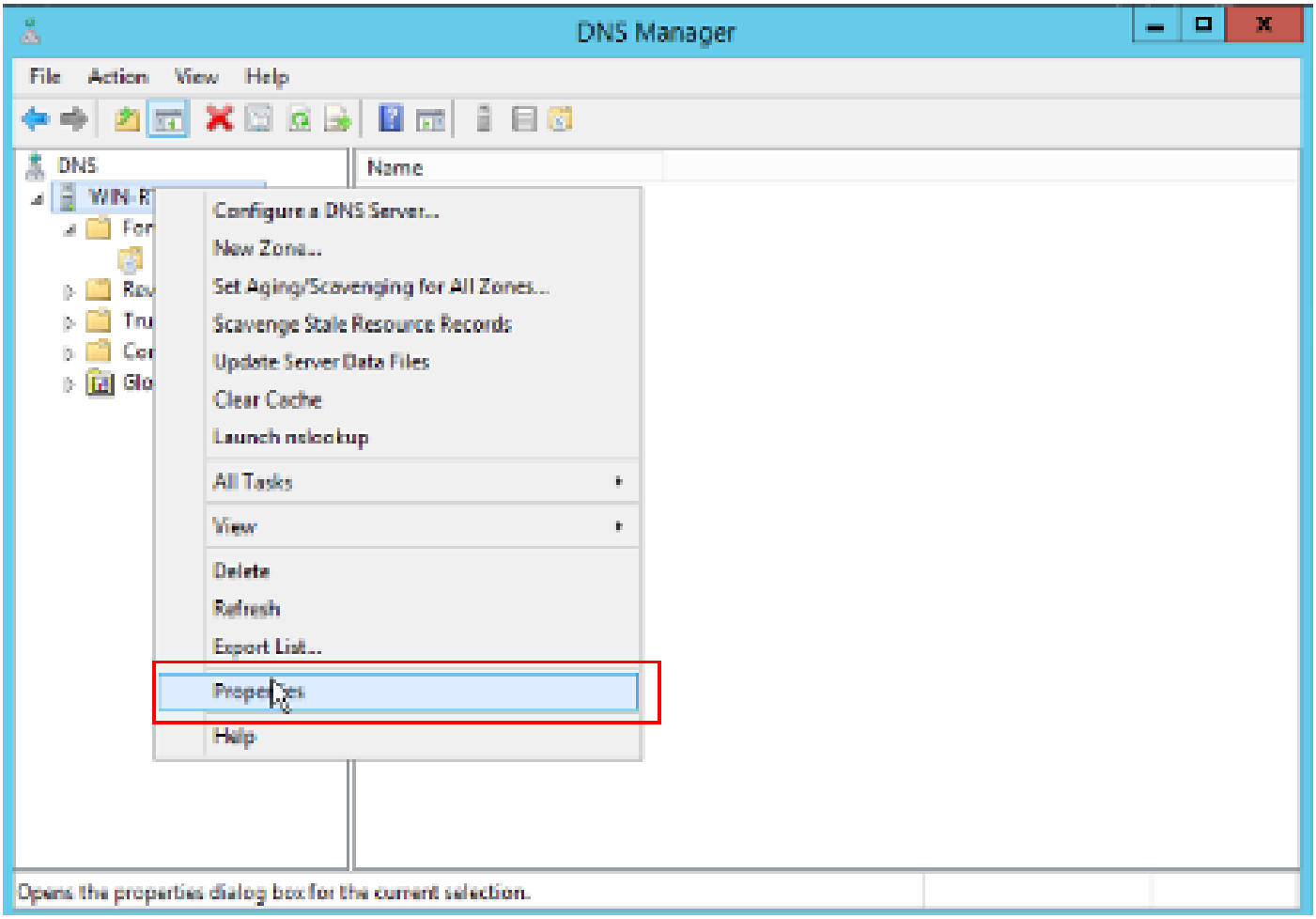


DNS伺服器

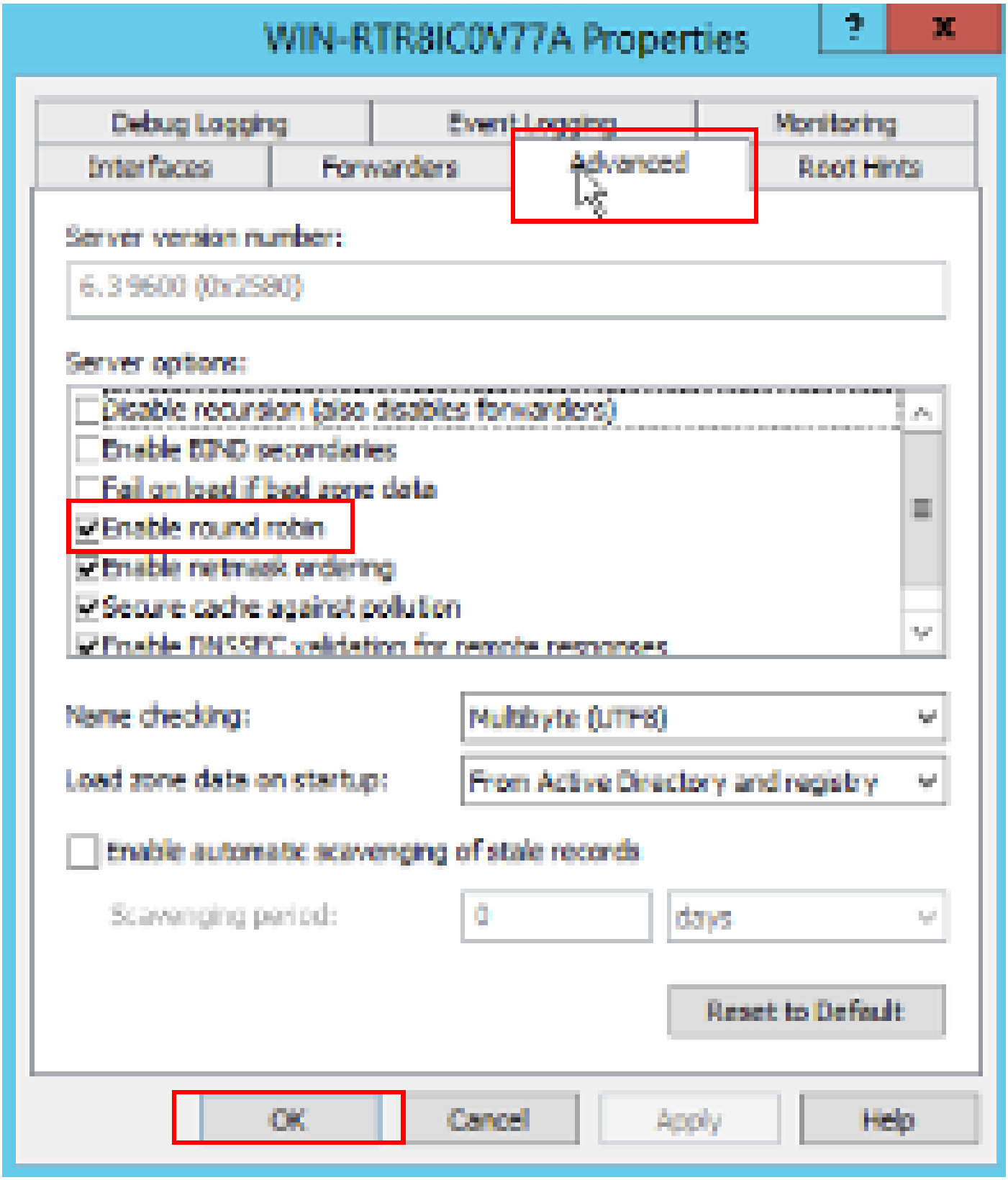
確保您的DNS伺服器已啟用輪詢：

1. 從Windows案頭打開開始選單，選擇管理工具 > DNS。
2. 在控制檯樹中，選擇要管理的DNS伺服器，按一下右鍵，然後選擇屬性。

3. 在Advanced 頁籤下，確保選中了Enable round robin。



循環配置資源1

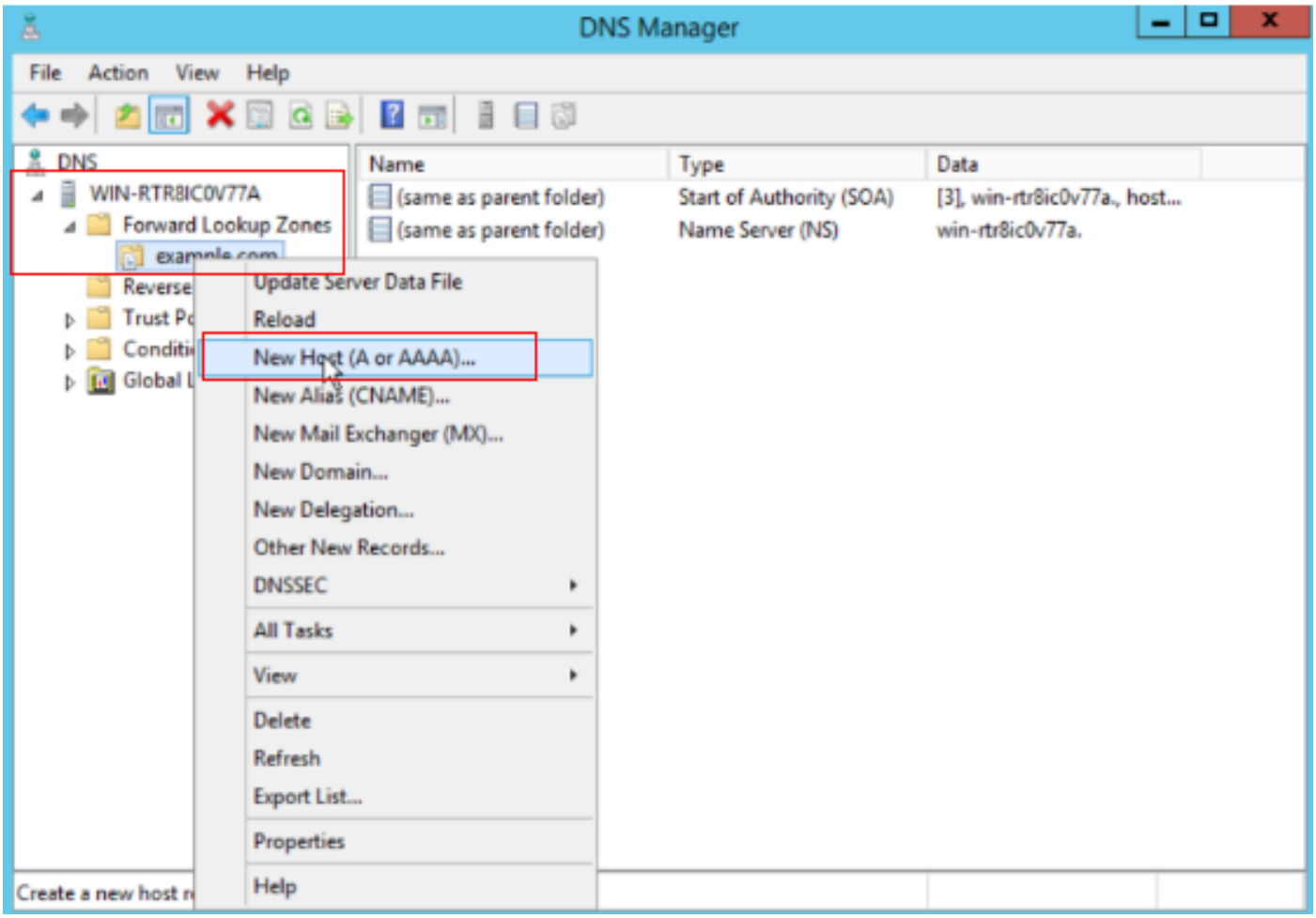


循環配置資源2

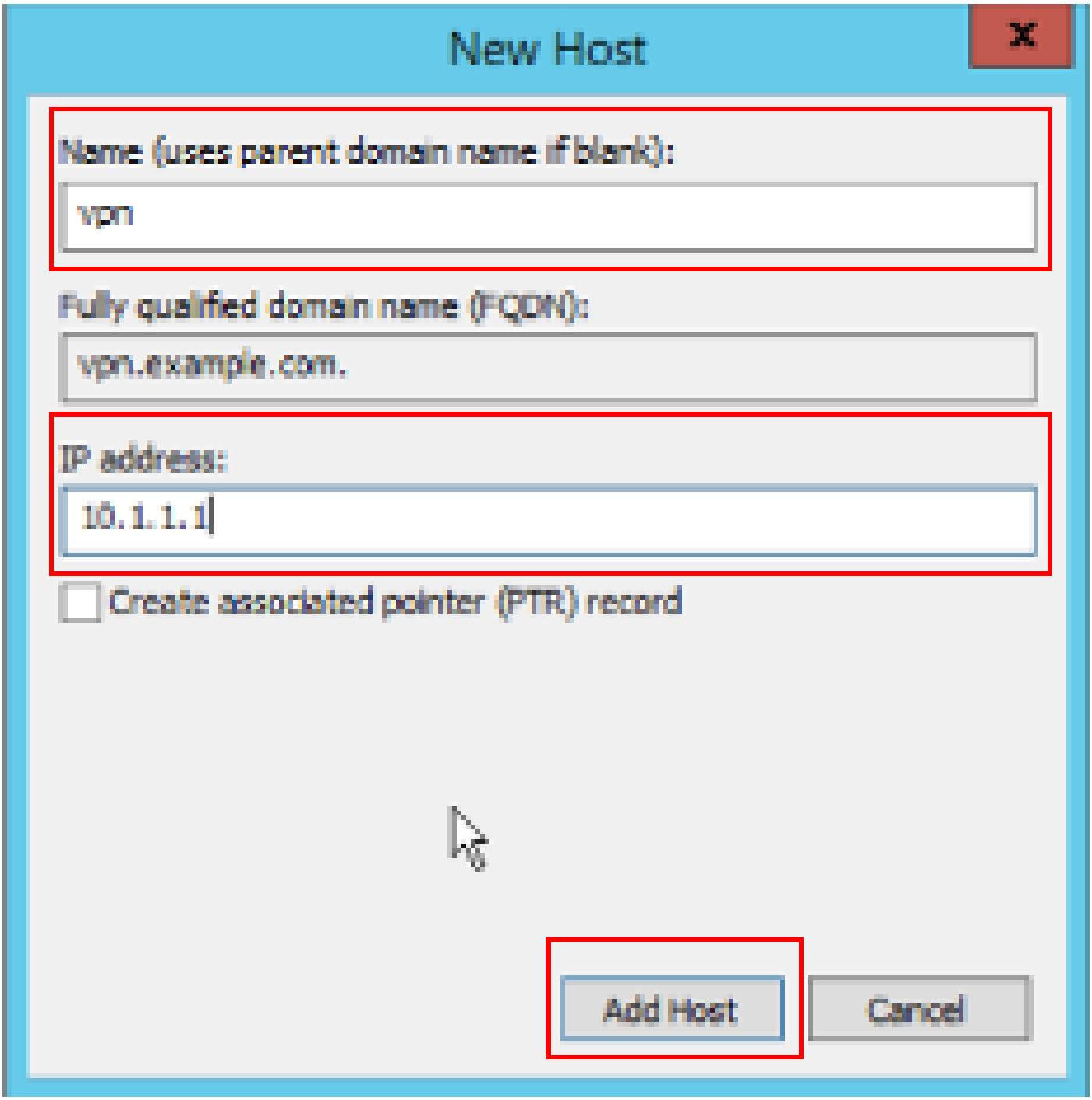
為ASA VPN伺服器建立兩個主機記錄：

1. 從Windows案頭打開開始選單，選擇管理工具 > DNS。
2. 在控制檯樹中，連線到要管理的DNS伺服器，展開DNS伺服器，展開正向查詢區域，按一下右鍵，然後選擇新建主機（A或AAAA）。
3. 在New Host螢幕上，指定主機記錄的Name和IP address。在本示例中，為vpn和10.1.1.1。

4. 選擇Add Host建立記錄。

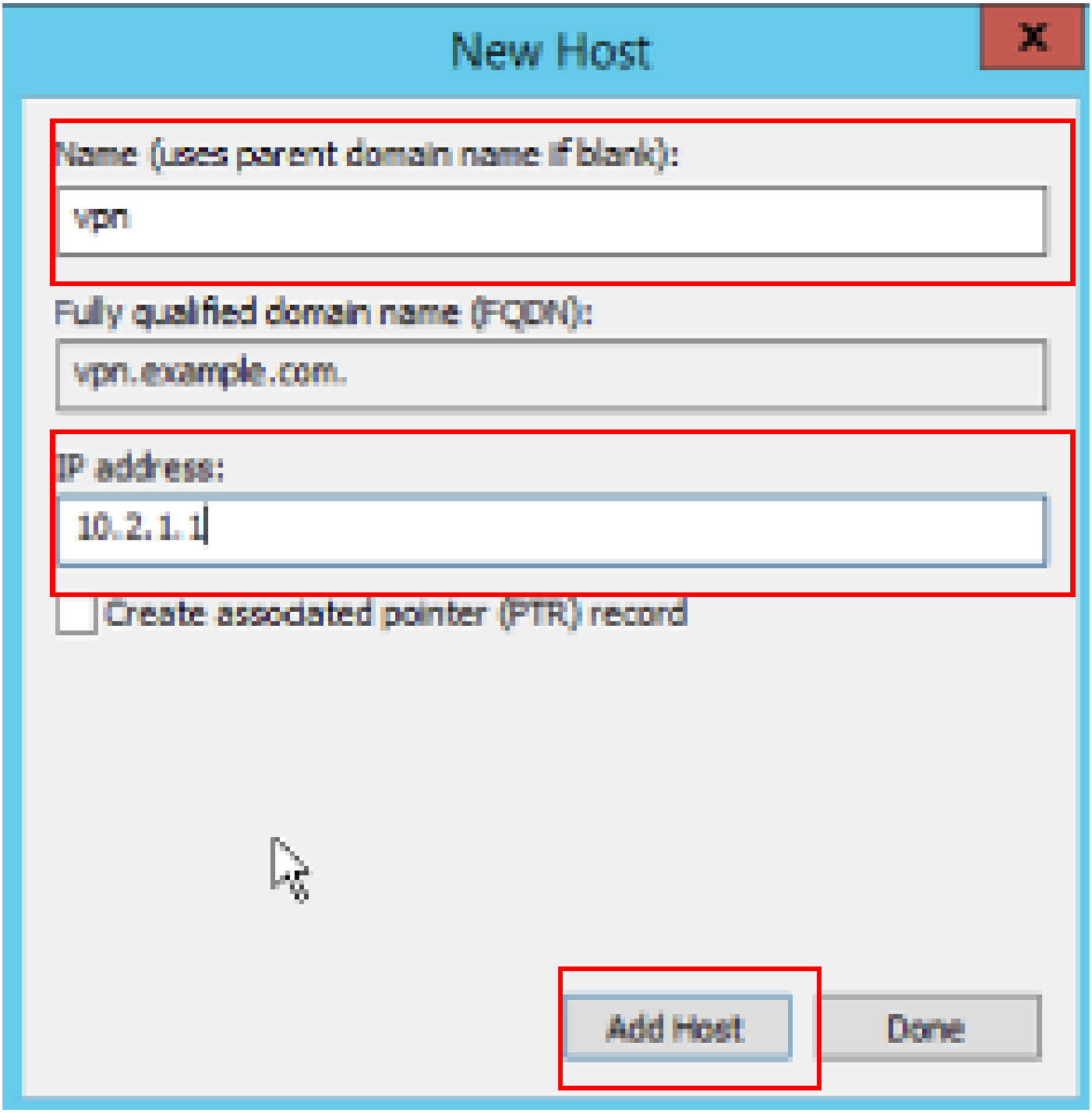


建立新主機



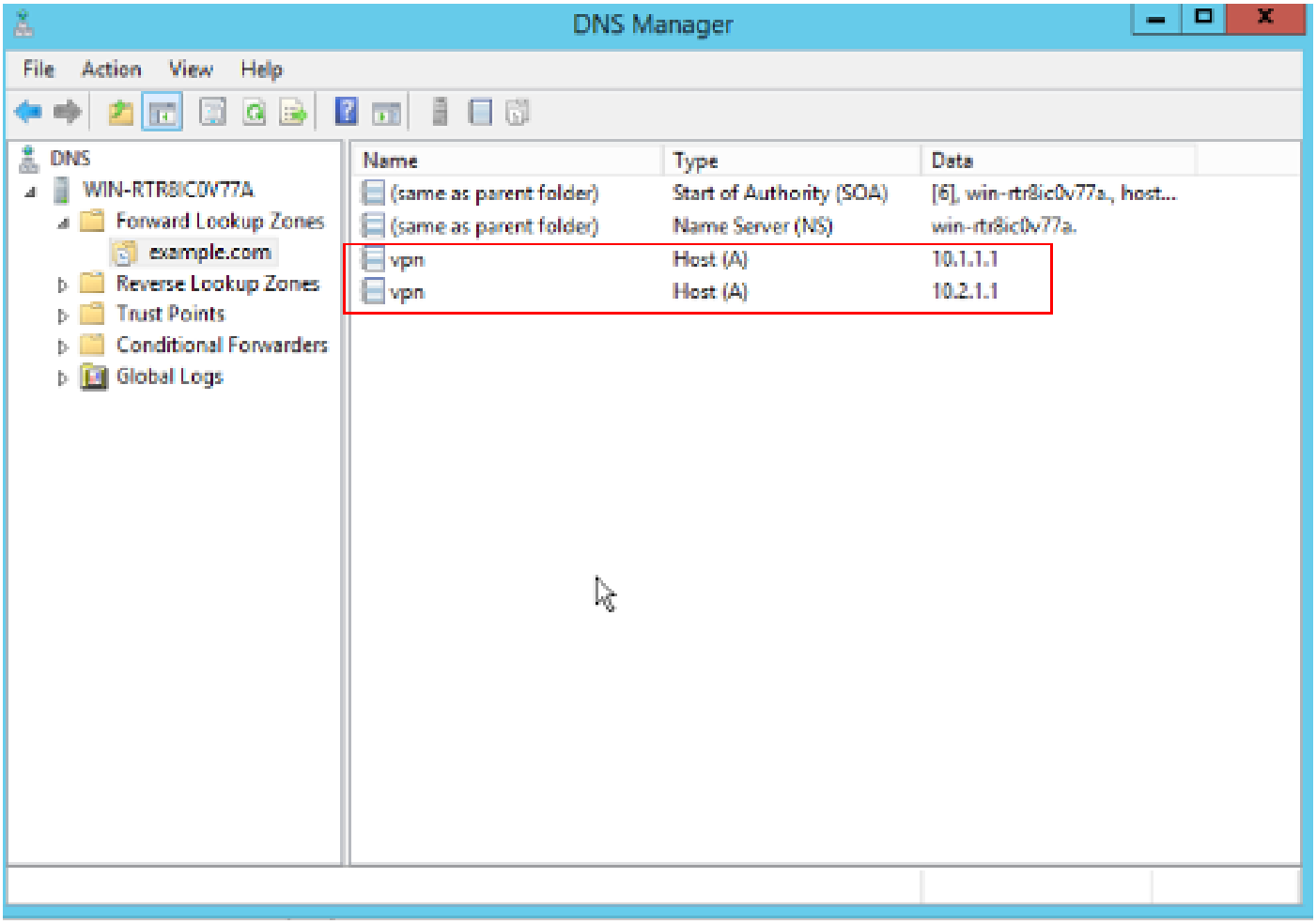
主機記錄1

重複類似步驟建立另一主機記錄，並確保Name相同，在本示例中，Name為vpn，IP address為10.2.1.1。



主機記錄2

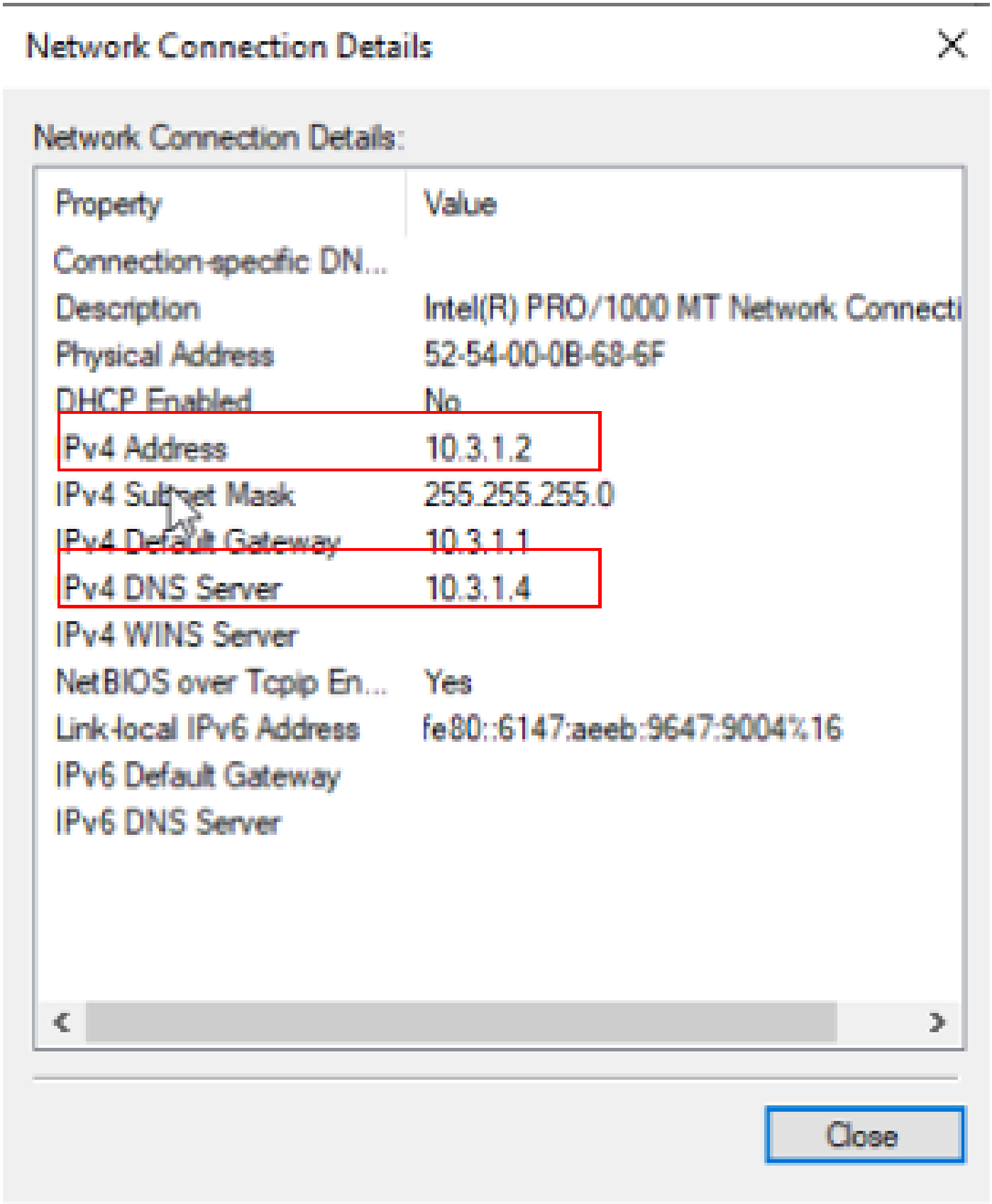
您可以發現，有兩個主機10.1.1.1和10.2.1.1與同一記錄vpn.example.com關聯。



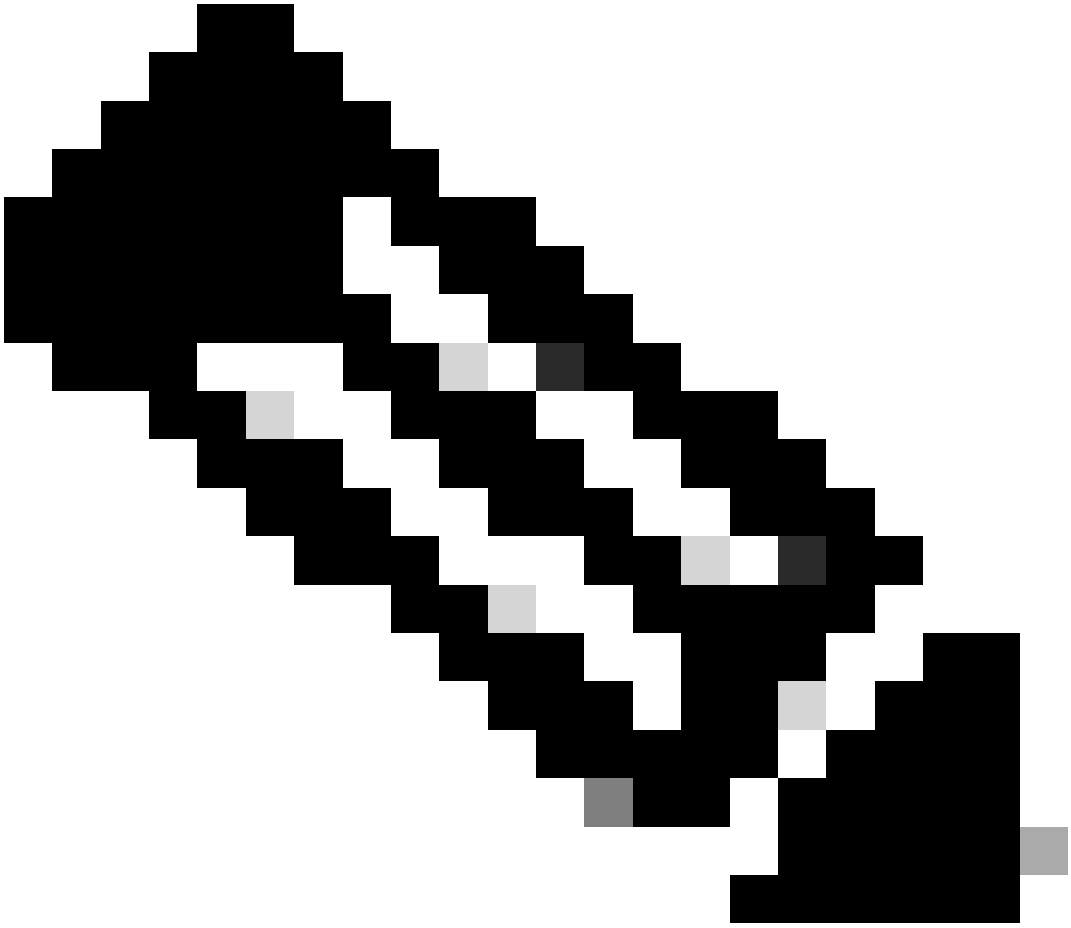
兩個主機記錄

驗證

導航到安裝了Cisco AnyConnect安全移動客戶端的客戶端電腦，在本示例中為Test-PC-1，驗證您的DNS伺服器是否為10.3.1.4。

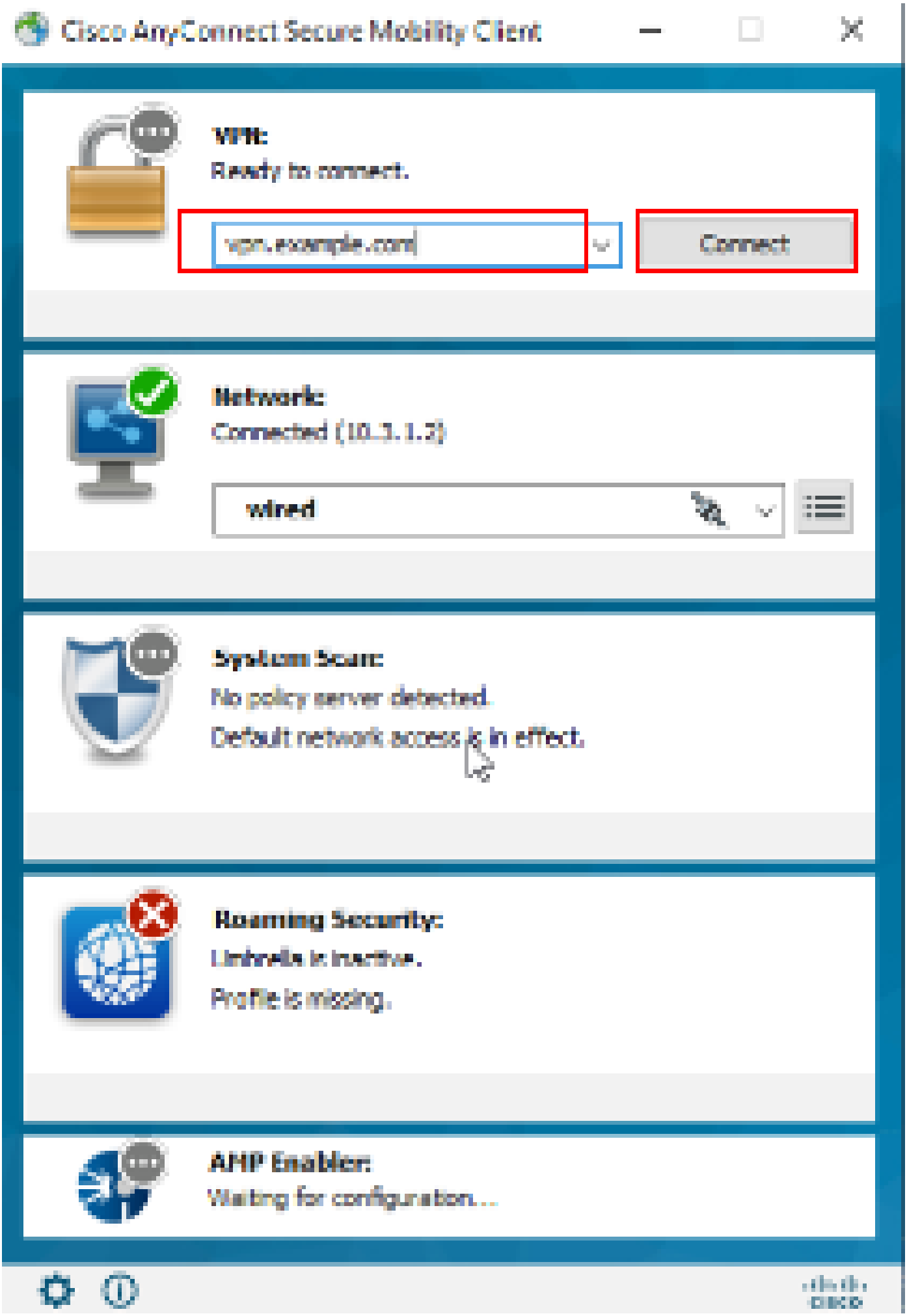

Network Connection Details
Network Connection Details:
Property
Value
Connection-specific DN...
Description
Intel(R) PRO/1000 MT Network Connecti
Physical Address
52-54-00-0B-68-6F
DHCP Enabled
No
Pv4 Address
10.3.1.2
IPv4 Subnet Mask
255.255.255.0
IPv4 Default Gateway
10.3.1.1
Pv4 DNS Server
10.3.1.4
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

PC1的IP地址



注意：由於網關使用自簽名證書來標識自己，因此連線嘗試期間可能會出現多個證書警告。這些是預期的，必須接受，連線才能繼續。為了避免這些證書警告，顯示的自簽名證書必須安裝在客戶端電腦的受信任證書儲存中，或者如果使用第三方證書，則證書頒發機構證書必須位於受信任的證書儲存中。

連線到您的VPN頭端vpn.example.com並輸入使用者名稱和憑證。



PC1 Anyconnect VPN

上，您可以設定各種調試級別；預設情況下，使用級別1。如果更改調試級別，調試的冗長會增加。請謹慎執行此操作，尤其是在生產環境中。

您可以啟用debug以診斷ASA上的VPN連線。

- debug webvpn anyconnect - 顯示關於與Anyconnect VPN客戶端連線的調試消息。

要對客戶端上的常見問題進行故障排除，請參閱此文檔。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。