

ASA에서 DNS 라운드 로빈을 사용하여 VPN 클라이언트 로드 밸런싱 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[1단계. ASA에서 Anyconnect VPN 구성](#)

[2단계. DNS 서버에서 라운드 로빈 DNS 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 ASA에서 DNS 라운드 로빈과 함께 anyconnect vpn 클라이언트 로드 밸런스를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- ASA에 IP 주소를 할당하고 기본 게이트웨이를 구성했습니다.
- Anyconnect VPN은 ASA에 구성됩니다.
- VPN 사용자는 개별적으로 할당된 IP 주소를 사용하여 모든 ASA에 연결할 수 있습니다.
- VPN 사용자의 DNS 서버는 라운드 로빈이 가능합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

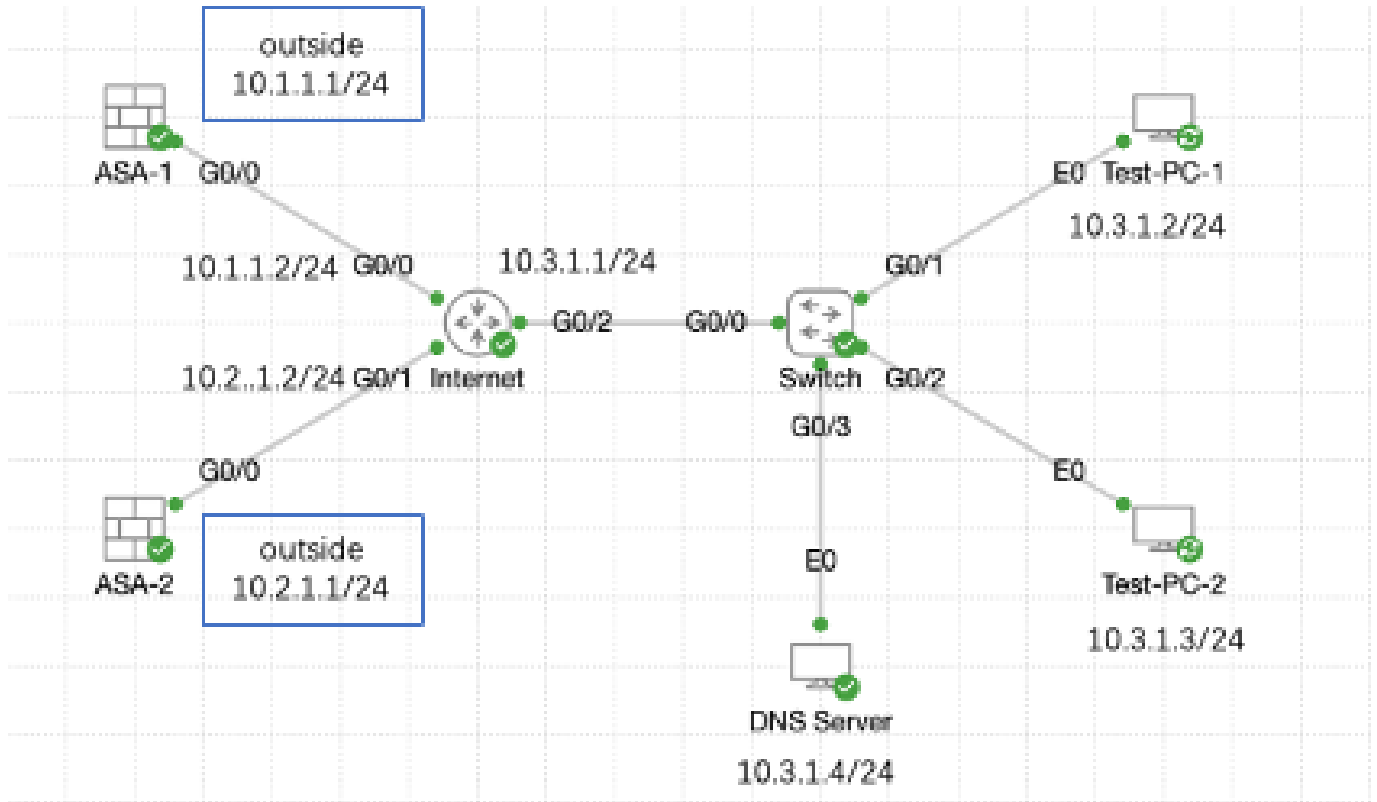
- Anyconnect VPN 클라이언트 소프트웨어 릴리스 4.10.08025
- Cisco ASA 소프트웨어 릴리스 9.18.2
- 윈도우 서버 2019

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 다이어그램



네트워크 다이어그램

설정

1단계. ASA에서 Anyconnect VPN 구성

ASA에서 anyconnect VPN을 구성하는 방법은 다음 문서를 참조하십시오.

- [ASA 8.x: 자체 서명 인증서 컨피그레이션을 사용하는 AnyConnect VPN 클라이언트를 통한 VPN 액세스 예](#)

이 예에서 두 ASA의 컨피그레이션은 다음과 같습니다.

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
```

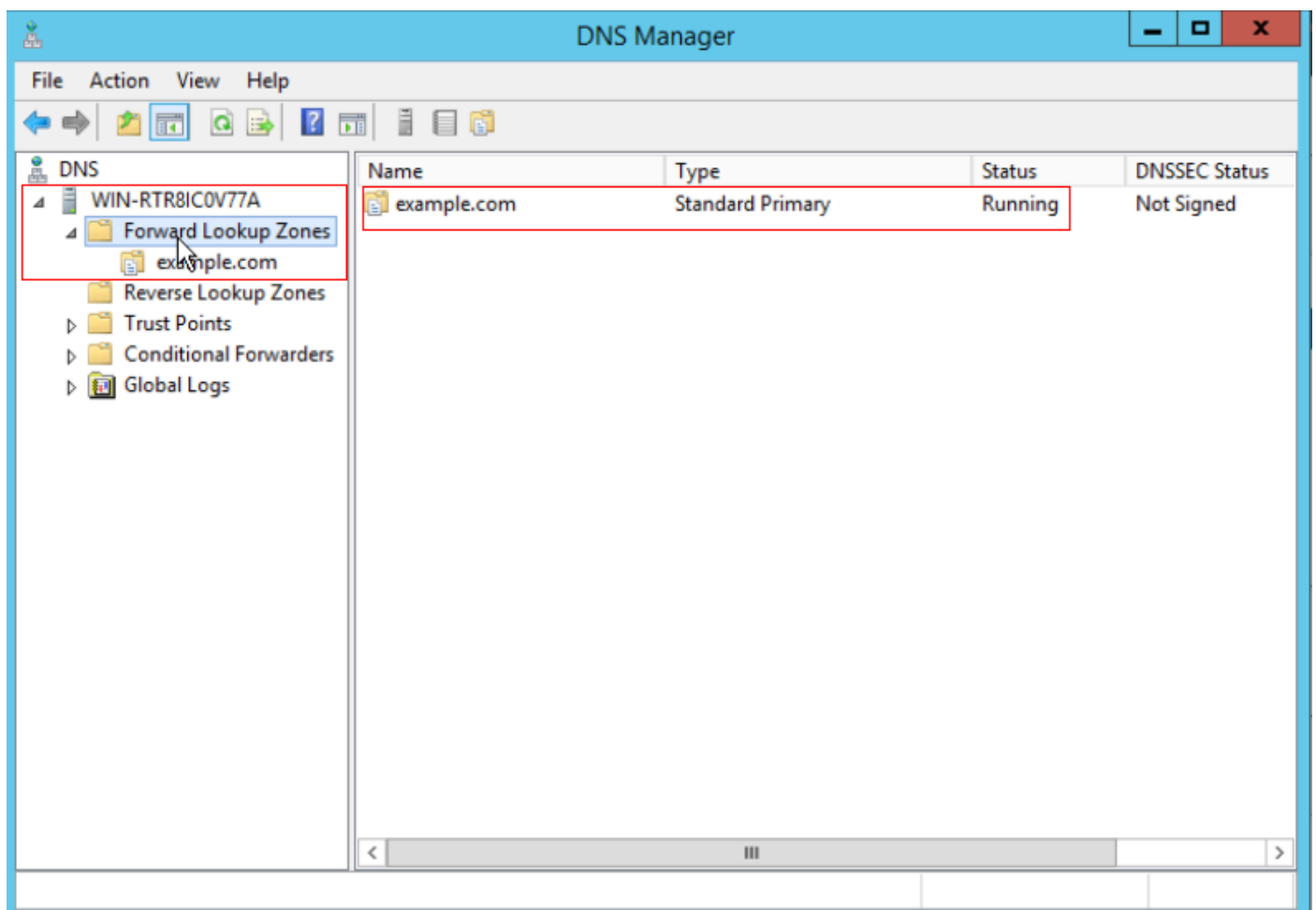
2단계로 이동하기 전에 개별적으로 할당된 IP 주소를 사용하여 두 ASA에 모두 연결할 수 있어야 합니다.

2단계. DNS 서버에서 라운드 로빈 DNS 구성

모든 라운드 로빈 가능 DNS 서버를 사용할 수 있습니다. 이 예에서는 windows server 2019의 DNS 서버가 사용됩니다. Windows 서버에 DNS 서버를 설치하고 구성하는 방법은 다음 문서를 참조하십시오.

- [Windows Server에 DNS 서버 설치 및 구성](#)

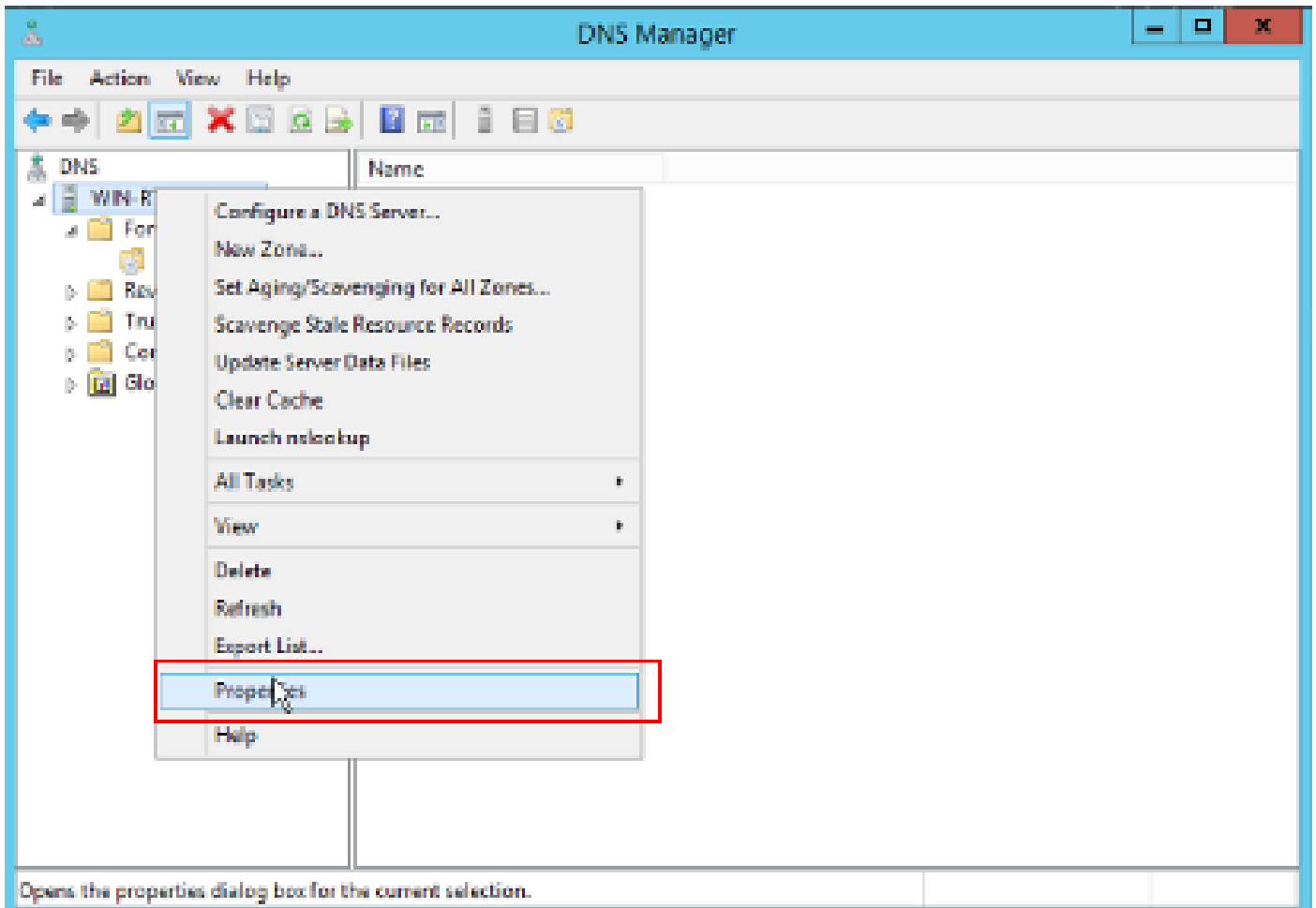
이 예에서 10.3.1.4는 도메인 example.com에 대해 DNS 서버가 활성화된 Windows 서버입니다.



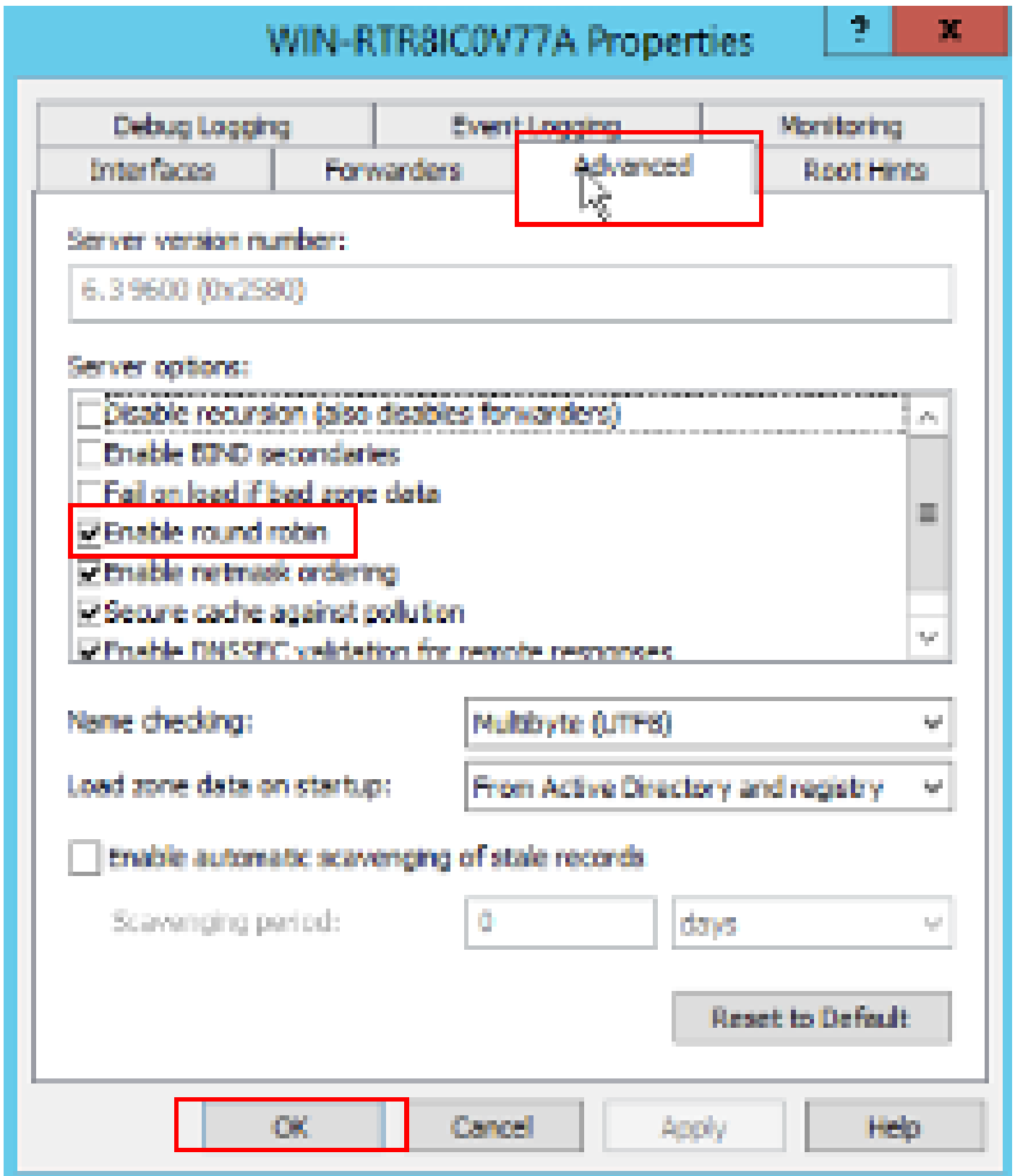
DNS 서버

DNS 서버에 대해 라운드 로빈이 활성화되어 있는지 확인합니다.

1. Windows 바탕 화면에서 시작 메뉴를 열고 관리 도구 > DNS를 선택합니다.
2. 콘솔 트리에서 관리할 DNS 서버를 선택하고 마우스 오른쪽 단추를 클릭한 다음 속성을 선택합니다.
3. Advanced(고급) 탭에서 Enable round robin(라운드 로빈 활성화)이 선택되어 있는지 확인합니다.



라운드 로빈 1



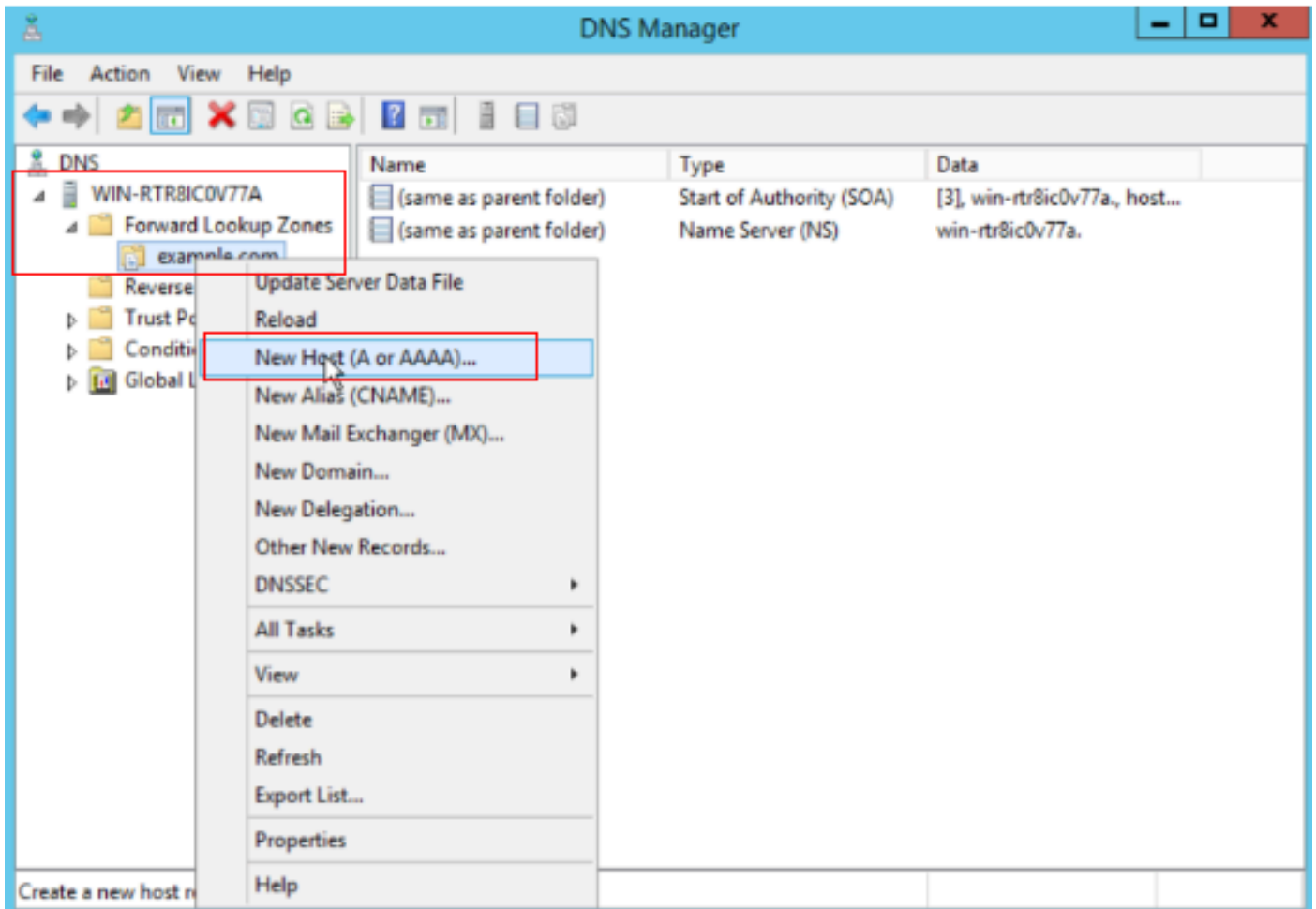
라운드 로빈 2

ASA VPN 서버에 대해 두 개의 호스트 레코드를 생성합니다.

1. Windows 바탕 화면에서 시작 메뉴를 열고 관리 도구 > DNS를 선택합니다.
2. 콘솔 트리에서 관리할 DNS 서버에 연결하고 DNS 서버를 확장한 다음 정방향 조회 영역을 확장하고 마우스 오른쪽 단추를 클릭한 다음 새 호스트(A 또는 AAAA)를 선택합니다.
3. New Host(새 호스트) 화면에서 호스트 레코드의 Name(이름)과 IP 주소를 지정합니다. 이 예

에서는 vpn 및 10.1.1.1입니다.

4. 레코드를 생성하려면 Add Host(호스트 추가)를 선택합니다.



새 호스트 생성

New Host X

Name (uses parent domain name if blank):
vpn

Fully qualified domain name (FQDN):
vpn.example.com.

IP address:
10.1.1.1

Create associated pointer (PTR) record

호스트 레코드 1

유사한 단계를 반복하여 다른 호스트 레코드를 생성하고 Name이 동일한지 확인합니다. 이 예에서 Name은 vpn, IP 주소는 10.2.1.1입니다.

New Host X

Name (uses parent domain name if blank):

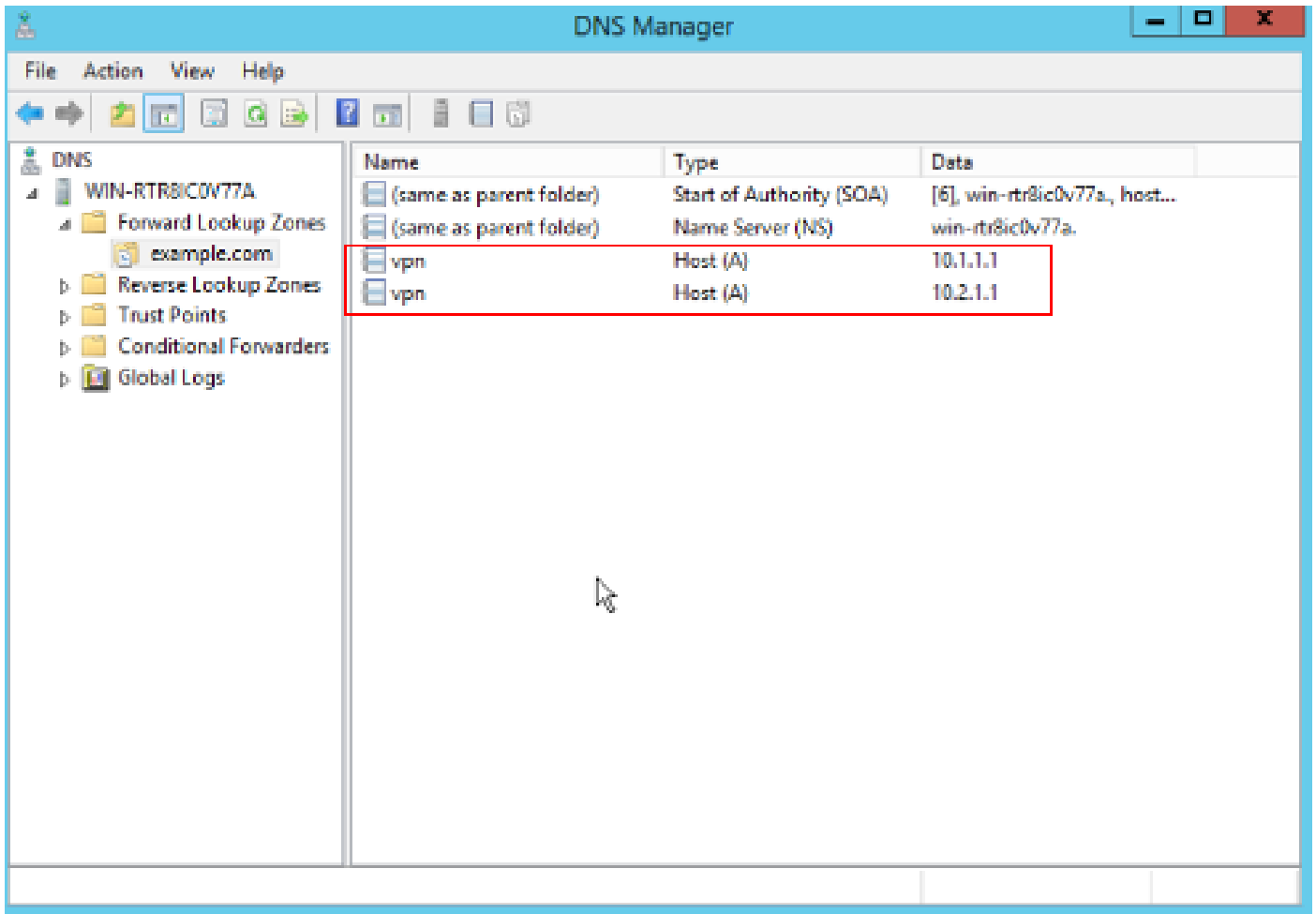
Fully qualified domain name (FQDN):

IP address:

Create associated pointer (PTR) record

호스트 레코드 2

동일한 레코드 vpn.example.com에 연결된 두 개의 호스트 10.1.1.1 및 10.2.1.1이 있습니다.



2개의 호스트 레코드

다음을 확인합니다.

Cisco AnyConnect Secure Mobility Client가 설치된 클라이언트 시스템으로 이동합니다. 이 예에서는 Test-PC-1에서 DNS 서버가 10.3.1.4인지 확인합니다.

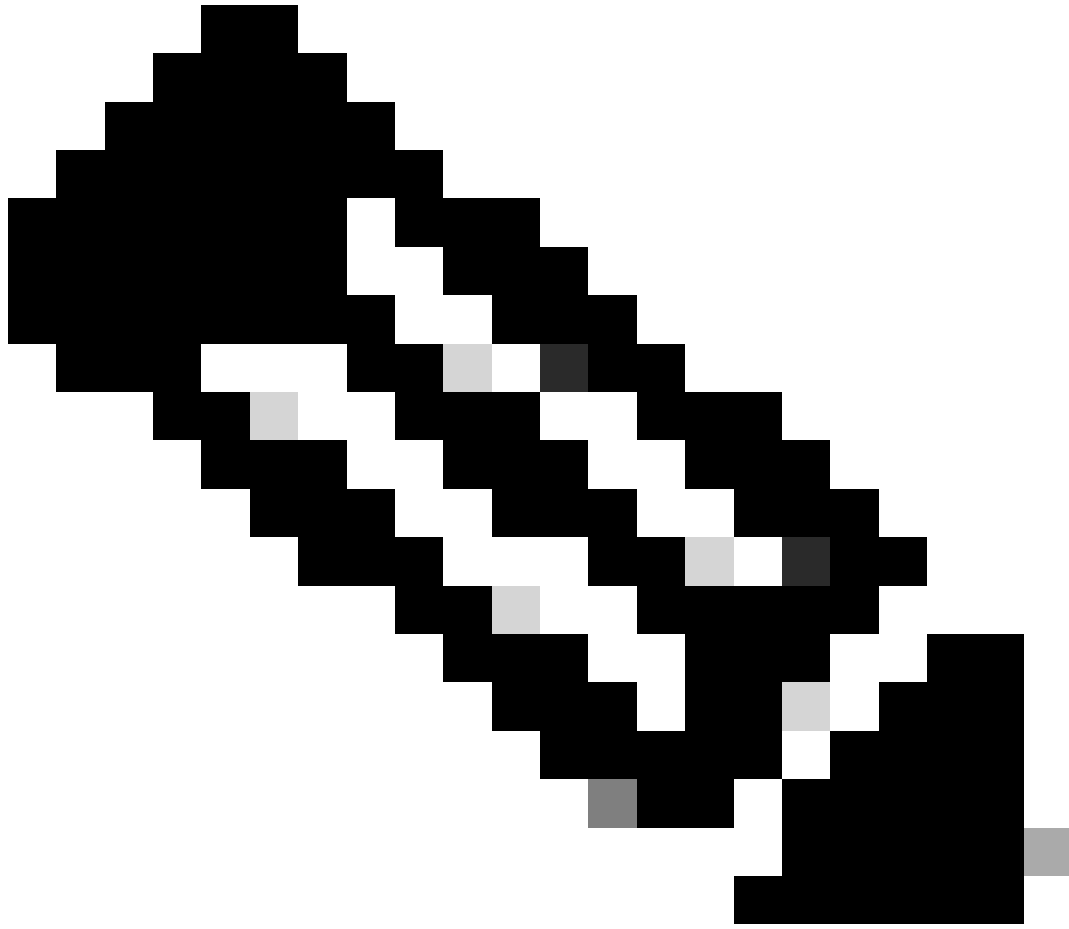
Network Connection Details



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



참고: 자체 서명 인증서는 게이트웨이가 자신을 식별하는 데 사용되므로 연결 시도 중에 여러 인증서 경고가 나타날 수 있습니다. 이러한 연결은 예상되며 연결을 계속하려면 수락해야 합니다. 이러한 인증서 경고를 방지하려면 표시되는 자체 서명 인증서를 클라이언트 시스템의 신뢰할 수 있는 인증서 저장소에 설치해야 합니다. 또는 타사 인증서가 사용 중인 경우 인증 기관 인증서는 신뢰할 수 있는 인증서 저장소에 있어야 합니다.

VPN 헤드엔드 vpn.example.com에 연결하고 사용자 이름과 자격 증명을 입력합니다.



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...

에서는 다양한 디버그 레벨을 설정할 수 있습니다. 기본적으로 레벨 1이 사용됩니다. 디버그 수준을 변경하면 디버그의 자세한 내용이 증가합니다. 특히 프로덕션 환경에서는 이 작업을 신중하게 수행해야 합니다.

ASA에서 진단 VPN 연결에 대한 디버그를 활성화할 수 있습니다.

- `debug webvpn anyconnect` - Anyconnect VPN 클라이언트 연결에 대한 디버그 메시지를 표시합니다.

클라이언트 측에서 발견되는 일반적인 문제를 트러블슈팅하려면 [이](#) 문서를 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.