

Configurazione del bilanciamento del carico del client VPN con Round Robin DNS su ASA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Passaggio 1. Configurazione di Anyconnect VPN su ASA](#)

[Passaggio 2. Configurare il DNS Round Robin nel server DNS](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare il bilanciamento del carico del client vpn anyconnect con round robin DNS su un'appliance ASA.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Gli indirizzi IP sono stati assegnati alle appliance ASA e il gateway predefinito è stato configurato.
- Anyconnect VPN è configurata sulle appliance ASA.
- Gli utenti VPN sono in grado di connettersi a tutte le appliance ASA con l'uso dell'indirizzo IP assegnato singolarmente.
- Il server DNS degli utenti VPN supporta la funzionalità round robin.

Componenti usati

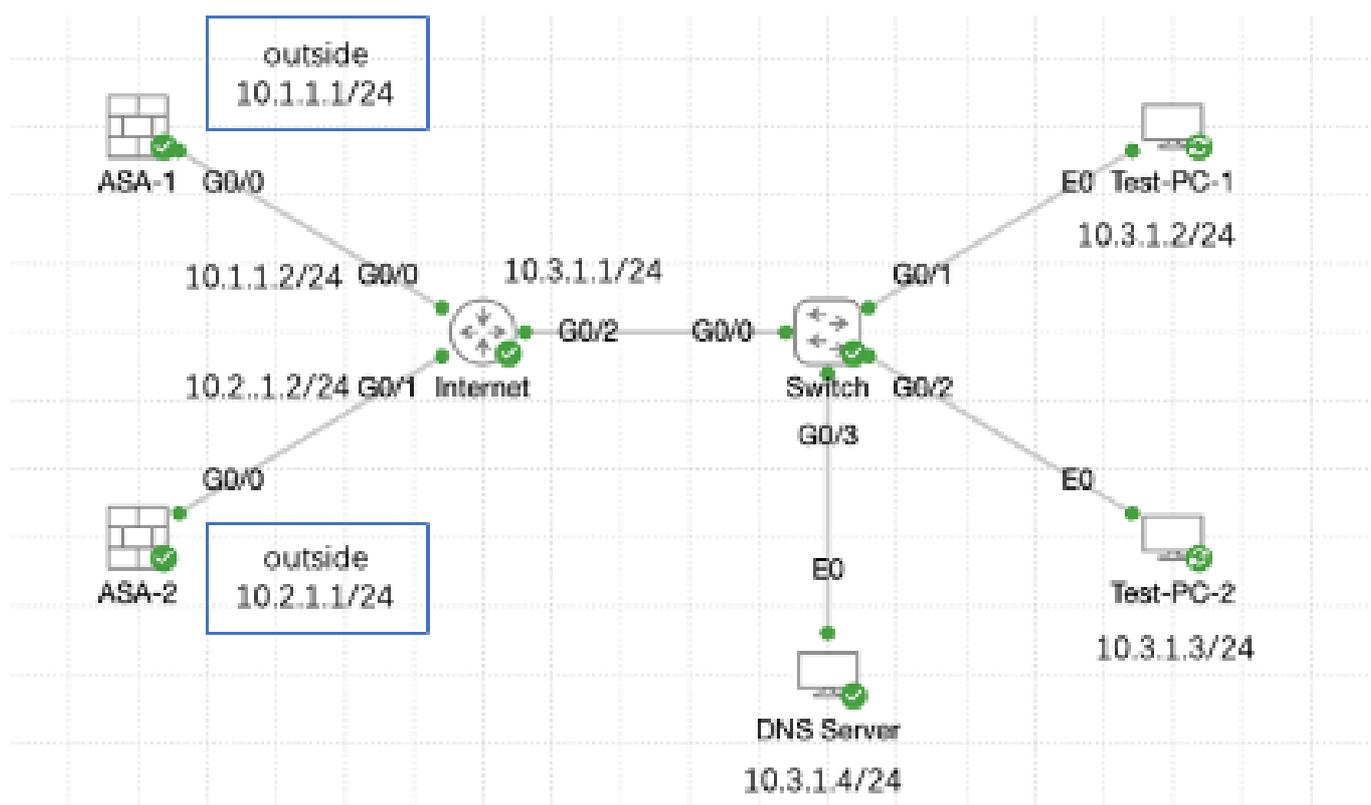
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Esempio di rete

Configurazioni

Passaggio 1. Configurazione di Anyconnect VPN su ASA

Per informazioni su come configurare anyconnect VPN su ASA, fare riferimento a questo documento:

- [ASA 8.x: esempio di configurazione del certificato autofirmato per l'accesso VPN con il client VPN AnyConnect](#)

Di seguito è riportata la configurazione di entrambe le appliance ASA nell'esempio:

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
```

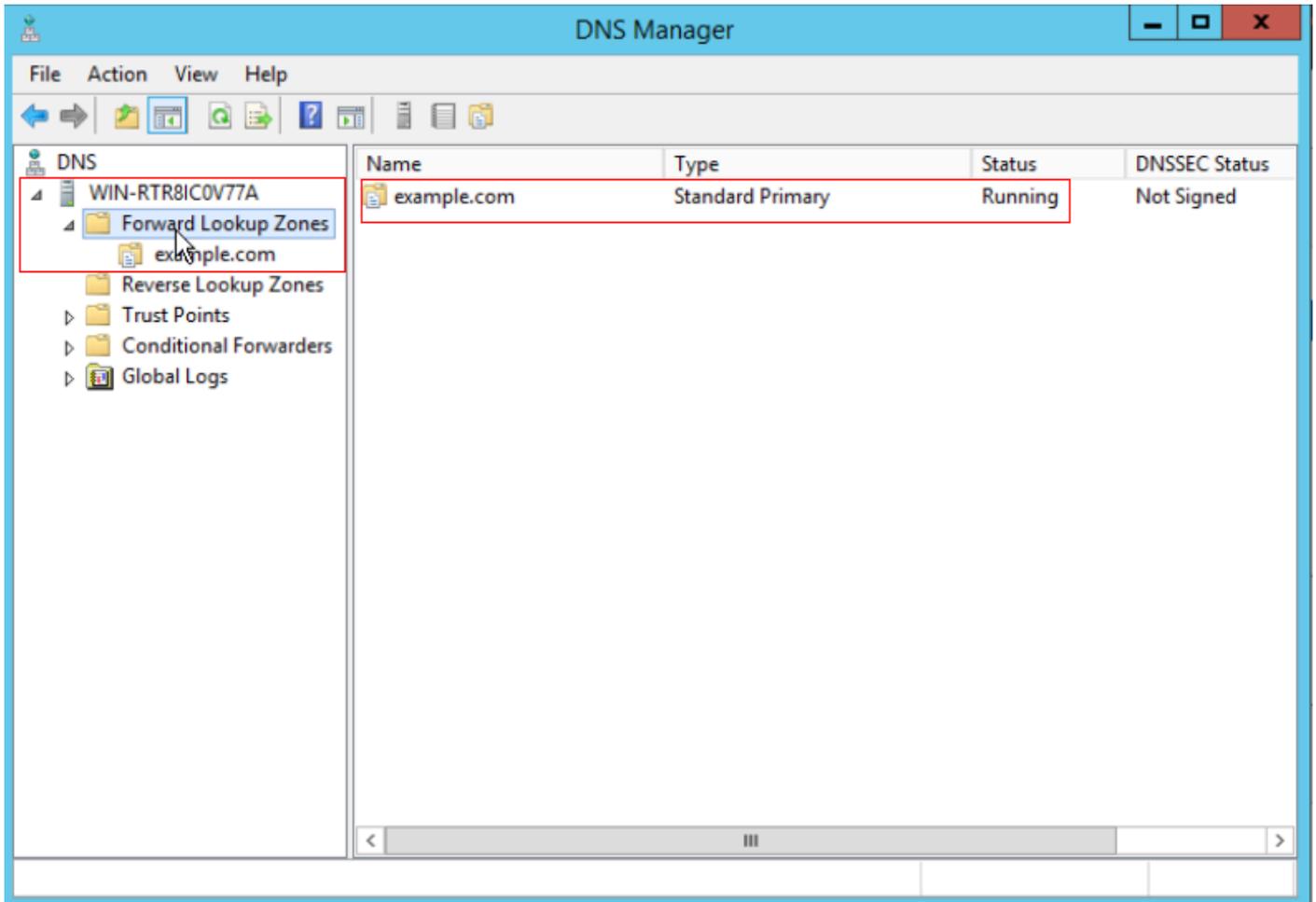
Prima di passare al punto 2, è necessario poter connettersi a entrambe le appliance ASA usando l'indirizzo IP assegnato singolarmente.

Passaggio 2. Configurare il DNS Round Robin nel server DNS

È possibile utilizzare qualsiasi server DNS round robin, in questo esempio viene utilizzato il server DNS in Windows Server 2019. Per informazioni su come installare e configurare il server DNS nel server Windows, fare riferimento a questo documento:

- [Installare e configurare il server DNS in Windows Server](#)

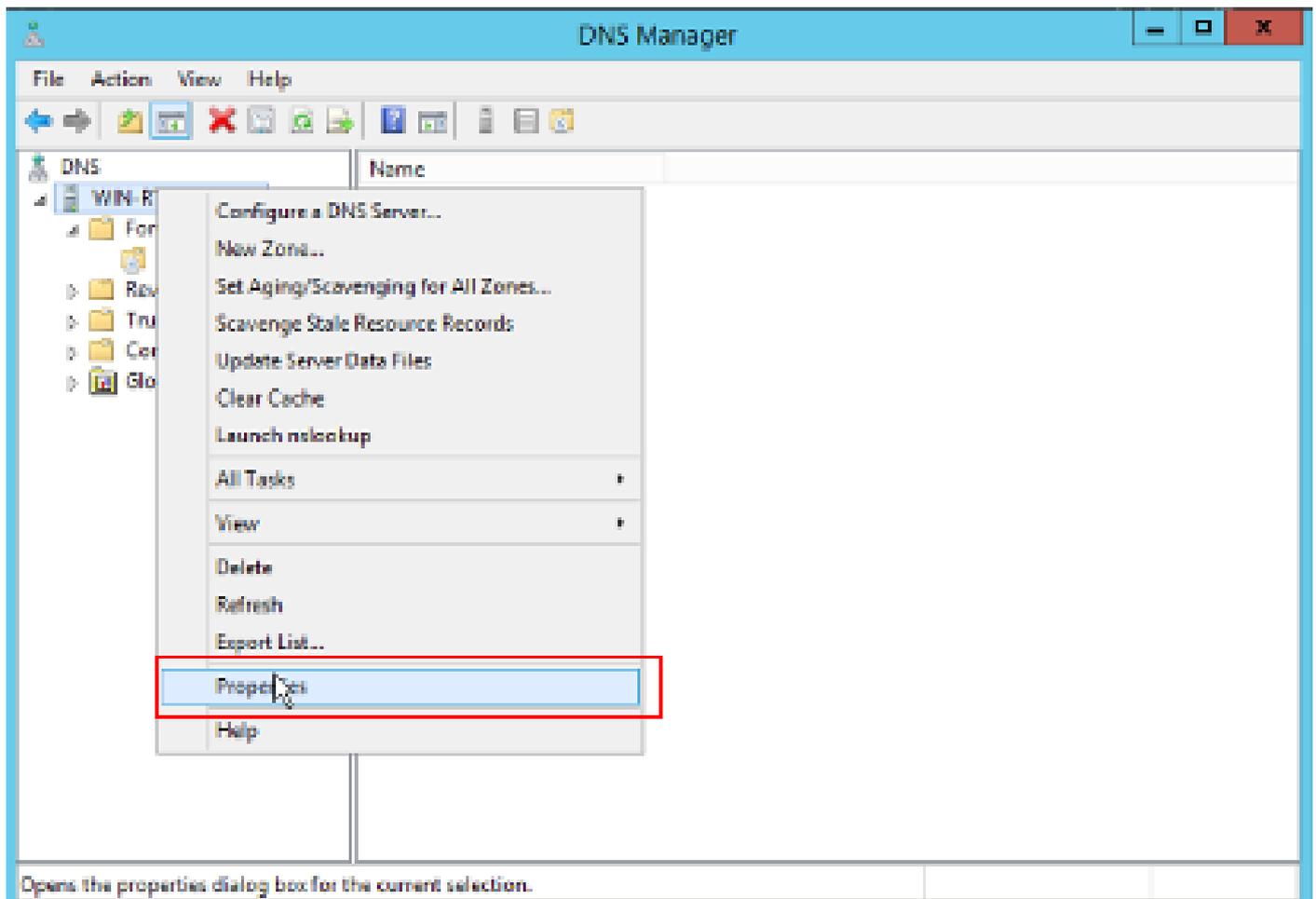
In questo esempio, 10.3.1.4 è il server Windows con il server DNS abilitato per il dominio example.com.



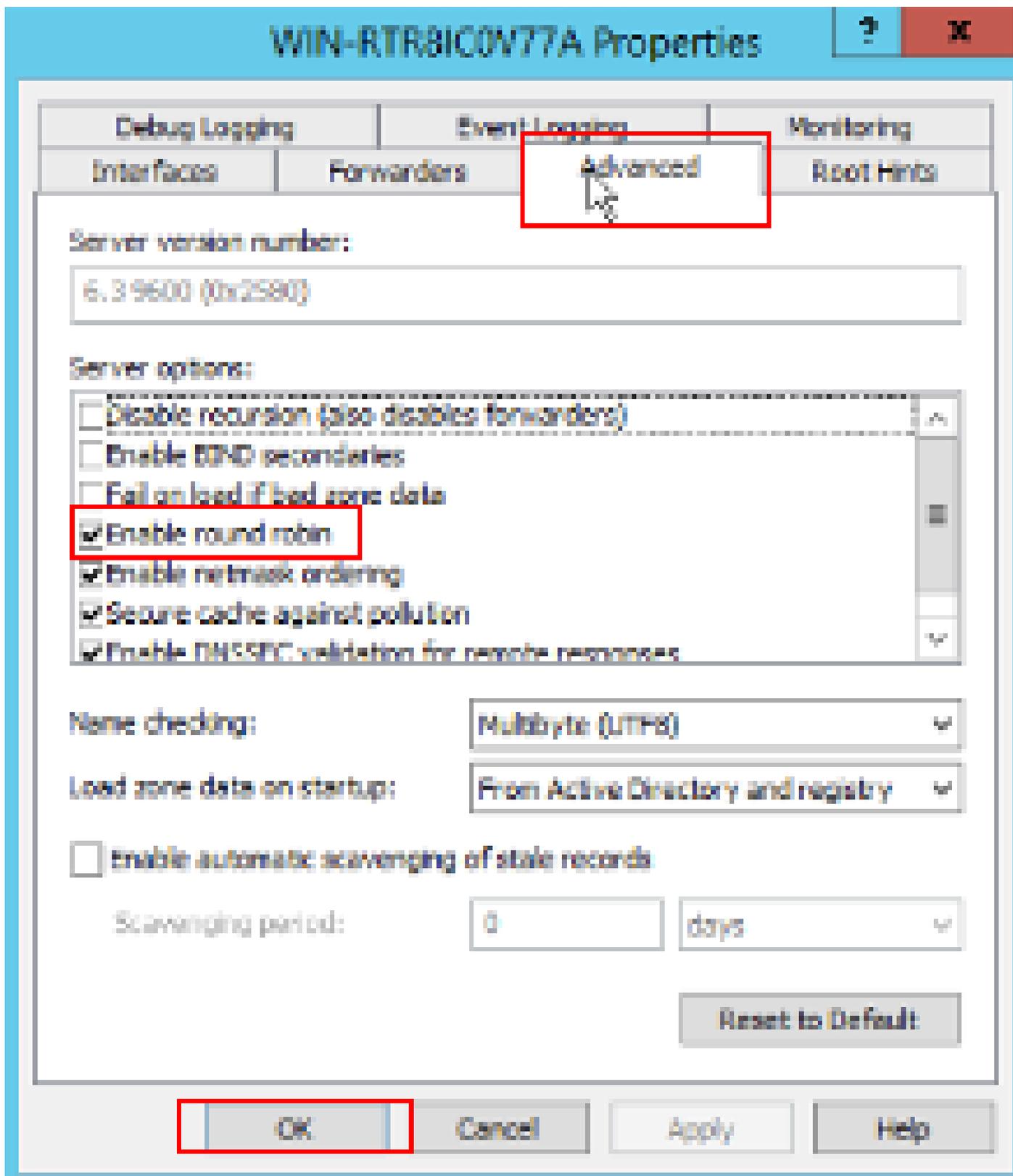
Server DNS

Verificare che round robin sia abilitato per il server DNS:

1. Dal desktop di Windows, aprire il menu Start, selezionare Strumenti di amministrazione > DNS.
2. Nell'albero della console scegliere il server DNS che si desidera gestire, fare clic con il pulsante destro del mouse e quindi scegliere Proprietà.
3. Nella scheda Avanzate, assicuratevi che l'opzione Attiva round robin (Enable round robin) sia selezionata.



Round Robin 1



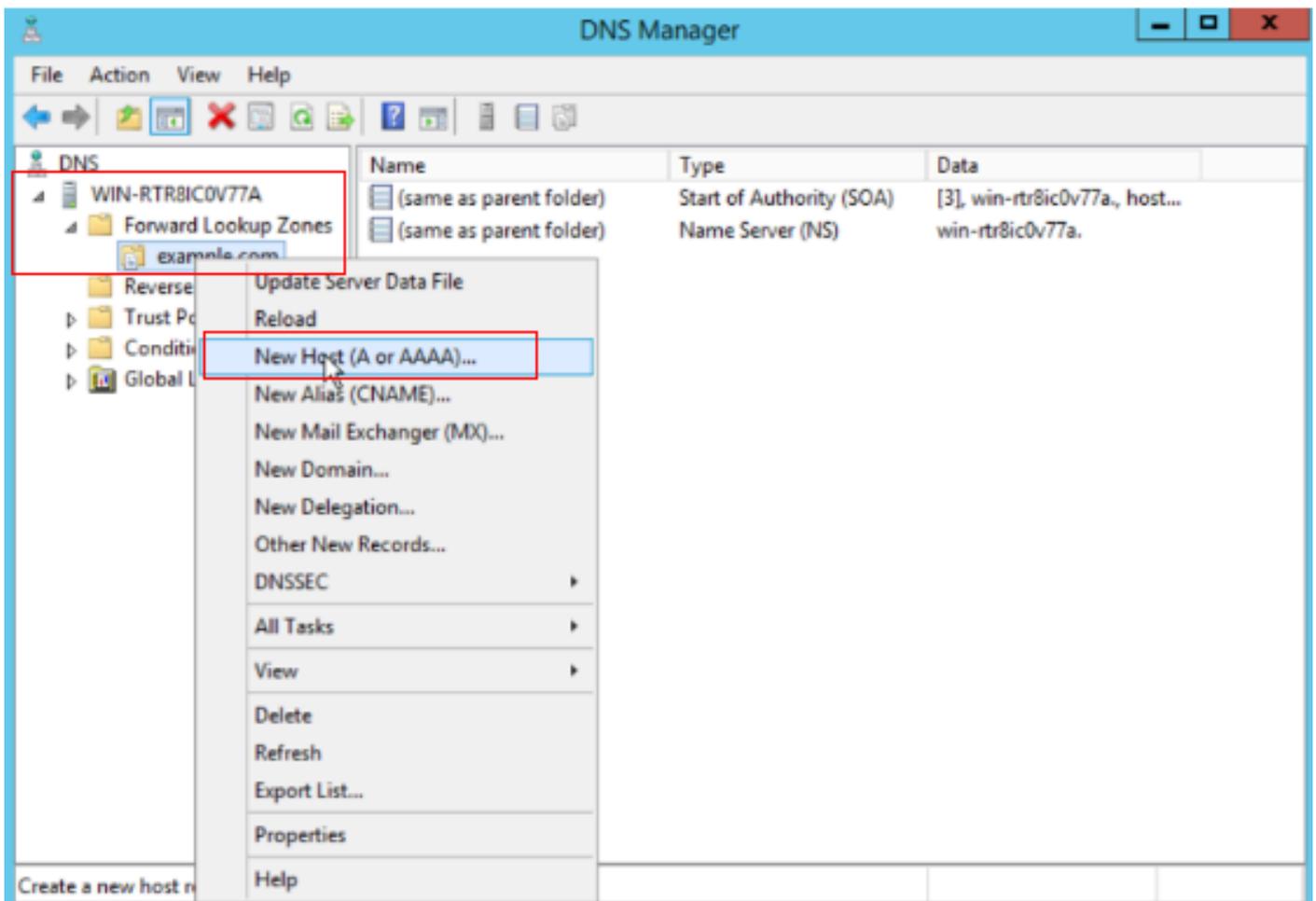
Round Robin 2

Creare due record host per i server VPN ASA:

1. Dal desktop di Windows, aprire il menu Start, selezionare Strumenti di amministrazione > DNS.
2. Nell'albero della console connettersi al server DNS che si desidera gestire, espandere il server DNS, espandere la zona di ricerca diretta, fare clic con il pulsante destro del mouse,

quindi selezionare Nuovo host (A o AAAA).

3. Nella schermata Nuovo host, specificare il nome e l'indirizzo IP del record dell'host.
Nell'esempio, vpn e 10.1.1.1.
4. Selezionare Aggiungi host per creare il record.



Crea nuovo host

New Host X

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

IP address:

Create associated pointer (PTR) record



Record host 1

Ripetere passaggi simili per creare un altro record host e assicurarsi che Nome sia lo stesso, in questo esempio Nome è vpn, Indirizzo IP è 10.2.1.1.

New Host X

Name (uses parent domain name if blank):

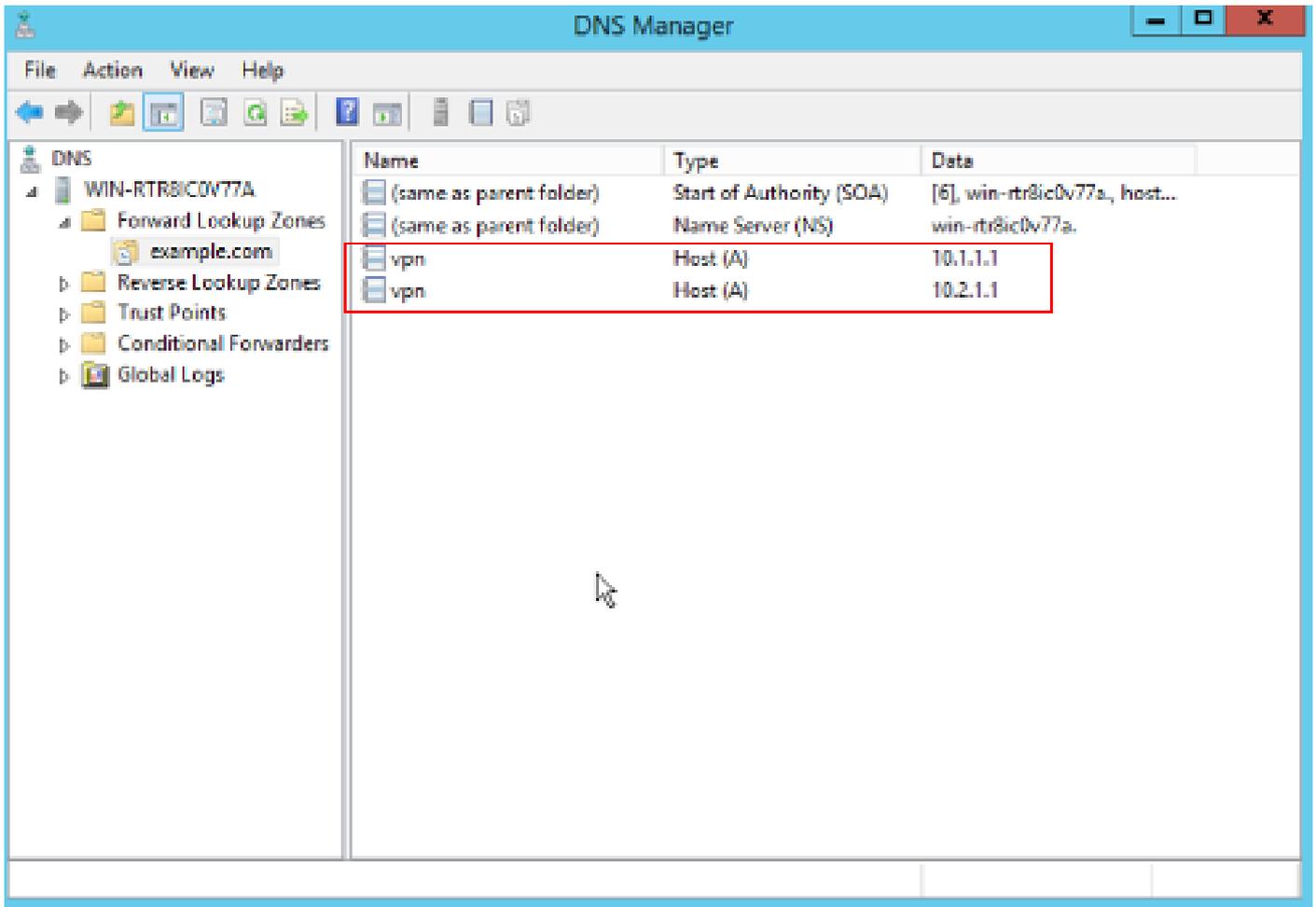
Fully qualified domain name (FQDN):

IP address:

Create associated pointer (PTR) record

Record host 2

Sono disponibili due host 10.1.1.1 e 10.2.1.1 associati allo stesso record vpn.example.com.



Due record host

Verifica

Passare al computer client in cui è installato il client Cisco AnyConnect Secure Mobility. Nell'esempio Test-PC-1 verificare che il server DNS sia 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: poiché per l'identificazione del gateway viene utilizzato un certificato autofirmato, è possibile che durante il tentativo di connessione vengano visualizzati più avvisi relativi al certificato. Questi elementi sono previsti e devono essere accettati affinché la connessione possa continuare. Per evitare la visualizzazione di questi avvisi relativi ai certificati, è necessario che il certificato autofirmato presentato sia installato nell'archivio certificati attendibile del computer client oppure, se viene utilizzato un certificato di terze parti, il certificato dell'autorità di certificazione deve trovarsi nell'archivio certificati attendibile.

Connettersi all'headend VPN `vpn.example.com` e immettere il nome utente e le credenziali.



VPN:
Ready to connect.

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...

: sull'appliance ASA, è possibile impostare vari livelli di debug; per impostazione predefinita, viene utilizzato il livello 1. Se si modifica il livello di debug, il livello di dettaglio dei debug aumenta. Procedere con cautela, soprattutto negli ambienti di produzione.

È possibile abilitare il debug sulla connessione VPN di diagnostica sull'appliance ASA.

- debug webvpn anyconnect - Visualizza i messaggi di debug sulle connessioni ai client VPN Anyconnect.

Fare riferimento a [questo](#) documento per la risoluzione dei problemi più comuni rilevati sul lato client.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).