

DNS-configuratie van NX-OS Base-Shell

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[DNS-configuratie van Bash-Shell](#)

[DNS-verificatie van Bash Shell](#)

[Stap 1. Controleer het gebruik van een geldig netwerk dat wordt uitgelijnd om te testen.](#)

[Stap 2. Controleer de werking van de DNS-resolutie met de naam van de Test Host.](#)

[/etc/resolv.conf bestandsindeling](#)

[Voorbeelden](#)

[Gerelateerde informatie](#)

Inleiding

In dit document worden de stappen beschreven die zijn gebruikt om DNS-servers in Bash te configureren, zodat de DNS-hostnamen op IP-adressen kunnen worden resolutie.

Cisco Nexus 3000 en 9000 Series apparaten maken toegang tot het onderliggende Linux-systeem van NX-OS mogelijk via Bash (Bourne-alweer Sell). Bash maakt systeembeheer en -bewaking mogelijk door een Linux-omgeving. Raadpleeg voor meer informatie over BaseT op NX-OS het [Baskische hoofdstuk van de Cisco Nexus 9000 Series NX-OS Programmakeuze](#).

Het kan nodig zijn om humaan-vriendelijke domeinnamen in numerieke IP-adressen te vertalen terwijl u normale taken in Bash shell uitvoert. Zulke taken omvatten het gebruik van de `curl`- of `wget` hulpprogramma's om toegang te krijgen tot resources van een webserver of het downloaden van Docker-afbeeldingen met de `docker pull`-opdracht.

Voorwaarden

Vereisten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Opmerking: De schaal van het Bash moet op uw apparaat van Cisco Nexus worden geactiveerd. Raadpleeg het gedeelte "Toegang tot basis" van het hoofdstuk in het [Cisco Nexus 9000 Series NX-OS](#) programmeerbaarheidsgids voor instructies om het veld Bash in te schakelen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Nexus 9000 platform vanaf NX-OS release 6.1(2)I2(1)
- Nexus 3000 platform vanaf NX-OS release 6.0(2)U4(1)

De informatie in dit document is gemaakt van apparatuur in een specifieke labomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

DNS-configuratie van Bash-Shell

De Linux-omgeving die door de schaal van Bash wordt benaderd, gebruikt het `/etc/resolv.conf`-bestand om DNS-configuratie op te slaan, net als de meeste andere Unix-achtige besturingssystemen.

1. Meld u aan bij de Bash shell als de basisgebruiker door de `bash sudo su -` opdracht.

```
Nexus# run bash sudo su -
root@Nexus#whoami
root
```

2. Bekijk de huidige inhoud van het `/etc/resolv.conf`-bestand. In dit voorbeeld, is het bestand leeg.

```
root@Nexus#cat /etc/resolv.conf
root@Nexus#
```

3. Open het `/etc/resolv.conf`-bestand voor het bewerken met de `vi`-teksteditor.

```
root@Nexus#vi /etc/resolv.conf
```

4. Druk op de `i`-toets om de INSERT-modus in te voeren en voer vervolgens de gewenste configuratie in. Raadpleeg het gedeelte `/etc/resolv.conf` File Format van dit document voor meer informatie over de configuratie van het `/etc/resolv.conf`-bestand.

5. Nadat het bestand is gewijzigd, drukt u op de `ESC`-toets om de INSERT-modus te verlaten en voert u vervolgens `:x in` om alle wijzigingen in het bestand op te slaan en te sluiten.

DNS-verificatie van Bash Shell

Zodra de wijzigingen worden aangebracht in de DNS-configuratie van de schaal van Bash, controleer of de wijzigingen resulteren in een succesvolle resolutie over de domeinnaam. De eenvoudigste methode om de resolutie van de domeinnaam te testen is door het gebruiken van de `ping` nutsvoorziening met een domeinhostname als doel. Dit document toont aan hoe de geldige DNS-configuratie moet worden geverifieerd met behulp van een testhost van `test.cisco.com` en DNS-servers van `192.168.2.1` en `192.168.2.2`.

Stap 1. Controleer het gebruik van een geldig netwerk dat wordt uitgelijnd om te testen.

Standaard gebruikt de Bash shell de **standaard** netwerk naamruimte tenzij anders geïnstrueerd. De netwerknaamruimtes zijn logisch gelijkwaardig aan NX-OS VRFs, en de `ip netwerken` de opdracht geven een lijst weer van namen die beschikbaar zijn in de schaal van het Bash, zoals hieronder wordt aangetoond:

```
root@Nexus#ip netns
EXAMPLE-VRF (id: 2)
management (id: 1)
default (id: 0)
```

Een geldig netwerk naamruimte om met te testen is één die IP connectiviteit heeft met de DNS nameservers in het `/etc/resolv.conf` bestand ingesteld, evenals IP connectiviteit met het IP adres waar uw testhost zich aan ontbindt.

Men kan de `ip netwerken` `exec {naamruimte} {gewenst-bevel}` gebruiken om een opdracht `{gewenst-bevel}` in de naamruimte `{naamruimte}` uit te voeren. In plaats hiervan kan men ook de schaal van de Bash binnen de context van een specifieke naamruimte met de `ip netten` behalve `{naamruimte}` `bash` opdracht uitvoeren. De voormalige methodologie wordt in het voorbeeld gebruikt, wordt geverifieerd dat het **beheer**-naamruimte IP-connectiviteit heeft met het IP-adres dat eigendom is van de host van `test.cisco.com` (192.168.2.100) en beide DNS-servers (192.168.2.2) .

```
root@Nexus#ip netns exec management ping 192.168.2.100 -c 5
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
64 bytes from 192.168.2.100: icmp_seq=1 ttl=59 time=0.277 ms
64 bytes from 192.168.2.100: icmp_seq=2 ttl=59 time=0.284 ms
64 bytes from 192.168.2.100: icmp_seq=3 ttl=59 time=0.280 ms
64 bytes from 192.168.2.100: icmp_seq=4 ttl=59 time=0.274 ms
64 bytes from 192.168.2.100: icmp_seq=5 ttl=59 time=0.297 ms

--- 192.168.2.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.274/0.282/0.297/0.017 ms
```

```
root@Nexus#ip netns exec management ping 192.168.2.1 -c 5
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=59 time=0.277 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=59 time=0.284 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=59 time=0.280 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=59 time=0.274 ms
64 bytes from 192.168.2.1: icmp_seq=5 ttl=59 time=0.297 ms

--- 192.168.2.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.274/0.282/0.297/0.017 ms
```

```
root@Nexus#ip netns exec management ping 192.168.2.2 -c 5
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=59 time=0.277 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=59 time=0.284 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=59 time=0.280 ms
64 bytes from 192.168.2.2: icmp_seq=4 ttl=59 time=0.274 ms
64 bytes from 192.168.2.2: icmp_seq=5 ttl=59 time=0.297 ms

--- 192.168.2.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.274/0.282/0.297/0.017 ms
```

Stap 2. Controleer de werking van de DNS-resolutie met de naam van de Test Host.

Gebruik de `ping` voorziening met een doel van de hostname van de testhost. Als de antwoorden van ICMP van de testgastheer worden ontvangen, en het IP adres in de antwoorden van ICMP is het IP adres dat wij van de hostname verwachten te beantwoorden en, dan wordt de DNS resolutie bevestigd binnen het shell van het Bash te werken.

Dit voorbeeld toont aan hoe het `ping` nutsbedrijf binnen **beheer** naamruimte wordt gebruikt om de correcte DNS resolutie te verifiëren. Merk op hoe het domein hostname van `test.cisco.com` oplost tot `192.168.2.100`, wat het IP adres is dat we verwachten dat de hostname zal oplossen.

```
root@Nexus#ip netns exec management ping test.cisco.com -c 5
PING test.cisco.com (192.168.2.100) 56(84) bytes of data.
64 bytes from test.cisco.com (192.168.2.100): icmp_seq=1 ttl=59 time=0.617 ms
64 bytes from test.cisco.com (192.168.2.100): icmp_seq=2 ttl=59 time=0.341 ms
64 bytes from test.cisco.com (192.168.2.100): icmp_seq=3 ttl=59 time=0.310 ms
64 bytes from test.cisco.com (192.168.2.100): icmp_seq=4 ttl=59 time=0.379 ms
64 bytes from test.cisco.com (192.168.2.100): icmp_seq=5 ttl=59 time=0.296 ms

--- test.cisco.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 0.296/0.388/0.617/0.119 ms
```

Als de naamruimte die wordt gebruikt om de DNS-resolutie te testen IP-connectiviteit op het internet heeft, kan men `cisco.com` ping `ping` pingen om te verifiëren dat externe domeinnamen naast interne domeinnamen kunnen worden opgelost. Dit is met name belangrijk als we gebruik moeten maken van voorzieningen zoals `krullen` en `wget` tegen openbare web servers. Het voorbeeld hier toont aan hoe het `ping` nutsbedrijf binnen het **beheer** naamruimte (dat IP connectiviteit op het Internet heeft) kan worden gebruikt om de juiste externe DNS resolutie te verifiëren.

```
root@Nexus#ip netns exec management ping cisco.com -c 5
PING cisco.com (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=239 time=29.2 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=239 time=29.2 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=239 time=29.3 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=239 time=29.2 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=5 ttl=239 time=29.2 ms

--- cisco.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 29.261/29.283/29.335/0.111 ms
```

`/etc/resolv.conf` bestandsindeling

Sommige gebruikelijke configuratieparameters worden hier uitgelegd. Zorg ervoor dat u alle configuratieparameters aan uw omgeving aanpast.

- **domein {domeinnaam.tld}** - definieert een standaard domeinnaam `{domein-name.tld}` om aan hostnamen toe te voegen die niet met een periode eindigen. Er kan slechts één domeinvoer in het `/etc/resolv.conf`-bestand zijn.
- **zoek {domeinnaam-1.tld} [domein-naam-2.tld...]** - definieert een ruimte-afgebakende lijst van domeinnamen (`{domeinnaam-1.tld}` en, optioneel, `[domeinnaam-2.tld]`) om aan hostnamen toe te voegen.

Opmerking: De indelingen voor het domein en de zoekopdrachten sluiten elkaar uit - er kan maar één tegelijk in gebruik zijn. Als beide items in het `/etc/resolv.conf`-bestand zijn opgenomen, wordt de ingang die het laatst in het bestand voorkomt gebruikt.

- **nameserver {adres-1}** - definieert een IP adres {adres-1} voor een DNS server waar de verzoeken om DNS resolutie naar worden doorgestuurd. Meervoudige `nameserver`-items zijn toegestaan binnen één bestand, tot maximaal drie.

Voorbeelden

Dit voorbeeld toont de inhoud van het `/etc/resolv.conf`-bestand waarin het standaarddomein van de omgeving `cisco.com` is en DNS-servers in de omgeving IP-adressen hebben van `192.168.2.1` en `192.168.2.2`. In dit scenario, als de Bash shell het IP-adres van een apparaat met een hostnaam van `foo` moet oplossen, voegt `cisco.com` toe aan het eind van de hostname zodat de Full Qualified Domain Name (FDQN) van de host `foo.cisco.com` is.

```
domain cisco.com
nameserver 192.168.2.1
nameserver 192.168.2.2
```

Het volgende voorbeeld toont de inhoud van het `/etc/resolv.conf`-bestand waarin of de `cisco.com`- of de `bar.com`-domeinnamen kunnen worden gebruikt om DNS-hostnamen op te lossen. DNS-servers in de omgeving hebben IP-adressen van `192.168.2.1` en `192.168.2.2`. In dit scenario, als de Bash-shell het IP-adres van een apparaat met een hostnaam `foo` moet oplossen, probeert deze `foo.cisco.com` eerst op te lossen `foo.foo`. Als de resolutie voor `foo.cisco.com` mislukt.

```
search cisco.com bar.com
nameserver 192.168.2.1
nameserver 192.168.2.2
```

Gerelateerde informatie

- [Cisco Nexus 9000 Series NX-OS programmeerbaarheidsgids, release 9.x](#)
- [Cisco Nexus 9000 Series NX-OS programmeerbaarheidsgids, release 7.x](#)
- [Cisco Nexus 9000 Series NX-OS programmeerbaarheidsgids, release 6.x](#)
- [Cisco Nexus 3000 Series netwerkmodule voor NX-OS programmeerbaarheid, release 9.x](#)
- [Cisco Nexus 3000 Series netwerkmodule voor NX-OS programmeerbaarheid, release 7.x](#)
- [Cisco Nexus 3000 Series netwerkmodule voor NX-OS programmeerbaarheid, release 6.x](#)
- [Cisco Nexus 3500 Series netwerkmodule voor NX-OS programmeerbaarheid, release 9.x](#)
- [Cisco Nexus 3500 Series netwerkmodule voor NX-OS programmeerbaarheid, release 7.x](#)
- [Cisco Nexus 3500 Series netwerkmodule voor NX-OS programmeerbaarheid, release 6.x](#)
- [Cisco Nexus 3600 Series netwerkmodule voor NX-OS programmeerbaarheid, release 9.x](#)
- [Cisco Nexus 3600 Series NX-OS programmeerbaarheidsgids, release 7.x](#)
- [Programmeerbaarheid en automatisering met Cisco Open NX-OS](#)