

# NX-OS Bash外殼DNS配置

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[Bash外殼DNS配置](#)

[Bash外殼DNS驗證](#)

[步驟1.檢驗是否使用了有效的網路名稱空間進行測試。](#)

[步驟2.使用測試主機的主機名檢驗DNS解析的運行情況。](#)

[/etc/resolv.conf檔案格式](#)

[範例](#)

[相關資訊](#)

## 簡介

本文檔介紹在Bash中配置DNS伺服器以允許將DNS主機名解析為IP地址的步驟。

Cisco Nexus 3000和9000系列裝置允許通過Bash(Bourne-Again SHell)訪問NX-OS的底層Linux系統。Bash支援通過Linux環境進行系統管理和監控。有關Bash on NX-OS的詳細資訊，請參閱[Cisco Nexus 9000系列NX-OS可程式設計性指南](#)的Bash一章。

在Bash shell中執行正常任務時，可能需要將人性化的域名轉換為數字IP地址。這些任務包括使用curl或wget實用程式從Web伺服器訪問資源或使用docker pull命令下載Docker映像。

## 必要條件

### 需求

本文件所述內容不限於特定軟體和硬體版本。

**附註：**將在您的Cisco Nexus裝置上啟用Bash外殼。有關啟用Bash shell的說明，請參閱[Cisco Nexus 9000系列NX-OS可程式設計性指南](#)中Bash一章的「訪問Bash」一節。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 從NX-OS版本6.1(2)I2(1)開始的Nexus 9000平台
- 從NX-OS版本6.0(2)U4(1)開始的Nexus 3000平台

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

# Bash外殼DNS配置

通過Bash外殼訪問的Linux環境利用/etc/resolv.conf檔案儲存DNS配置，類似於大多數其他類Unix作業系統。

1.以root使用者身份通過run bash sudo su -命令登入Bash shell。

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

2.檢視/etc/resolv.conf檔案的當前內容。在此示例中，檔案為空。

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

3.使用vi文本編輯器開啟/etc/resolv.conf檔案進行編輯。

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

4.按i鍵進入「插入」模式，然後輸入所需的配置。有關如何在/etc/resolv.conf檔案中設定配置格式的詳細資訊，請參閱本文檔的/etc/resolv.conf檔案格式部分。

5.修改檔案後，按ESC鍵退出「插入」模式，然後輸入:~以儲存對檔案的所有更改並關閉該檔案。

# Bash外殼DNS驗證

對Bash外殼的DNS配置進行更改後，驗證更改是否會導致域名解析成功。測試域名解析的最簡單方法是使用ping實用程式，將域主機名作為目標。本文示範了如何使用test.cisco.com的測試主機和192.168.2.1和192.168.2.2的DNS伺服器驗證有效的DNS配置。

## 步驟1.檢驗是否使用了有效的網路名稱空間進行測試。

預設情況下，Bash shell使用default網路名稱空間，除非另有說明。網路名稱空間在邏輯上等同於NX-OS VRF，命令的ip netns顯示可用於Bash shell的名稱空間清單，如下所示：

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

要測試的有效網路名稱空間是具有IP連線至/etc/resolv.conf檔案中配置的DNS名稱伺服器以及測試主機解析為IP地址的IP連線的名稱空間。

可以使用ip netns exec {namespace} {desired-command}命令在名稱空間{namespace}中執行{desired-command}。或者，可以使用ip netns exec {namespace} bash命令在特定名稱空間的上下文中執行Bash shell。此處範例中使用的是前一種方法，經驗證management名稱空間與test.cisco.com主機（即192.168.2.100）及兩台DNS伺服器（192.168.2.1和192.168.2.2）所擁有的IP位址具有IP連線。

```
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
```

## 步驟2.使用測試主機的主機名檢驗DNS解析的運行情況。

將ping實用程式用於測試主機的主機名目標。如果從測試主機收到ICMP應答，並且ICMP應答中包含的IP地址是我們預計主機名要解析的IP地址，則確認DNS解析在Bash shell中起作用。

此示例演示了如何在management名稱空間中使用ping實用程式來驗證正確的DNS解析。請注意test.cisco.com的域主機名如何解析為192.168.2.100，這是我們希望主機名解析到的IP地址。

```
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
```

如果用於測試DNS解析的名稱空間具有到Internet的IP連線，則可以對cisco.com執行ping操作，以驗證除內部域名外是否可以解析外部域名。如果需要對公共Web伺服器使用curl和wget等實用程式，這一點尤為重要。此處的示例演示了如何在management名稱空間（具有Internet的IP連線）內使

用ping實用程式來驗證正確的外部DNS解析。

```
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檔案格式

此處介紹一些常見的配置引數。確保修改所有配置引數以匹配您的環境。

- **domain {domain-name.tld}** — 定義預設域名{domain-name.tld}。/etc/resolv.conf檔案中只能有一個
- **搜尋{domain-name-1.tld} [domain-name-2.tld..]** — 定義要附加到主機名的以空格分隔的域名清單({domain-name-1.tld}和 ( 可選 ) [domain-name-2.tld])。

附註：domain和search條目是互斥的 — 一次只能使用一個條目。如果兩個條目都包含在/etc/resolv.conf檔案中，則使用檔案中最後出現的條目。

- **nameserver {address-1}** — 為轉發DNS<sub>DNS</sub>務器定義IP地址{address-1}。單個檔案內允許多個nameserver條目，最多三個條目。

## 範例

此範例顯示/etc/resolv.conf檔案的內容，其中環境的預設網域為cisco.com，且環境中的DNS伺服器的IP位址為192.168.2.1和192.168.2.2。在此案例中，如果Bash shell需要解析主機名為foo的裝置的IP位址，則會將cisco.com附加到主機名的結尾，如此一來，主機的完全限定網域名稱(FDQN)就foo.cisco.com。

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

以下示例顯示/etc/resolv.conf檔案的內容，其中cisco.com或bar.com域名可用於解析DNS主機名。環境中的DNS伺服器的IP地址為192.168.2.1和192.168.2.2。在此方案中，如果Bash外殼需要解析主機名為foo的裝置IP地址，它會先嘗試解析foo.cisco.com，如果解析foo.cisco.com失敗，則嘗試解析foo.bar.com。

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

## 相關資訊

- [Cisco Nexus 9000系列NX-OS可程式設計性指南9.x版](#)
- [Cisco Nexus 9000系列NX-OS可程式設計性指南7.x版](#)
- [Cisco Nexus 9000系列NX-OS可程式設計性指南6.x版](#)
- [Cisco Nexus 3000系列NX-OS可程式設計性指南9.x版](#)
- [Cisco Nexus 3000系列NX-OS可程式設計性指南7.x版](#)
- [Cisco Nexus 3000系列NX-OS可程式設計性指南6.x版](#)
- [Cisco Nexus 3500系列NX-OS可程式設計性指南9.x版](#)
- [Cisco Nexus 3500系列NX-OS可程式設計性指南7.x版](#)
- [Cisco Nexus 3500系列NX-OS可程式設計性指南6.x版](#)
- [Cisco Nexus 3600系列NX-OS可程式設計性指南9.x版](#)
- [Cisco Nexus 3600系列NX-OS可程式設計性指南7.x版](#)
- [Cisco Open NX-OS的可程式設計性和自動化](#)