

使用FTD作為中繼代理在DHCP伺服器上啟用DHCP作用域選項

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[組態](#)

[網路圖表](#)

[配置DHCP中繼](#)

[配置DHCP中繼代理](#)

[配置外部DHCP伺服器](#)

[在外部DHCP伺服器上啟用選項43](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文說明如何在FMC管理的FTD中使用，在DHCP伺服器上啟用選項。

必要條件

需求

- Firepower技術知識
- 動態主機控制協定(DHCP)伺服器/DHCP中繼知識。

採用元件

- 本檔案中的資訊是根據虛擬思科FTD和FMC 7.4.0版
- Windows Server 2019用作DHCP伺服器

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。

背景資訊

威脅防禦裝置可以使用RFC 2132、RFC 2562和RFC 5510中指定的DHCP選項傳輸資訊。

它支援編號為1到255的所有DHCP選項，但選項1、12、50-54、58-59、61、67和82除外。

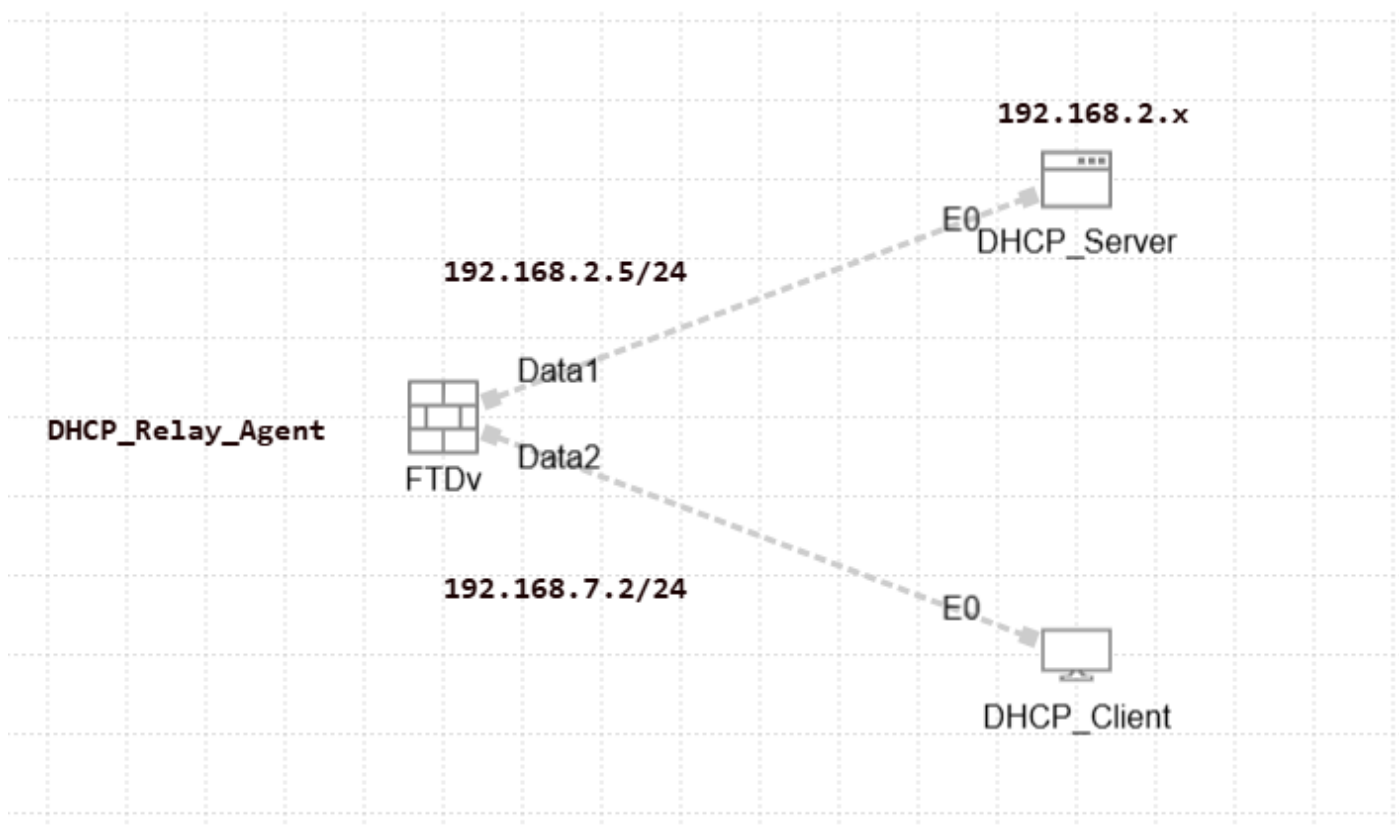
RFC 2132指定了兩個與供應商特定配置相關的DHCP選項：選項60和選項43。

本文檔提供配置示例，並說明DHCP選項43（供應商特定資訊）如何在Windows Server 2019上運行，FTD將充當DHCP中繼代理。

選項43使DHCP伺服器能夠向客戶端傳輸供應商特定的資訊，方便接入點等裝置找到並連線到其控制器，即使它們位於不同的VLAN或子網上。

組態

網路圖表



Network_Diagram

配置DHCP中繼

FTD介面充當DHCP中繼代理，促進使用者端與外部DHCP伺服器之間的通訊。

它偵聽客戶端請求並附加基本配置資料，例如DHCP伺服器向客戶端分配地址所需的客戶端鏈路資訊。

當從DHCP伺服器收到響應時，介面將應答資料包轉發回DHCP客戶端。

配置DHCP中繼包括兩個主要步驟：

- 1.設定DHCP中繼代理。
- 2.設定外部DHCP伺服器。

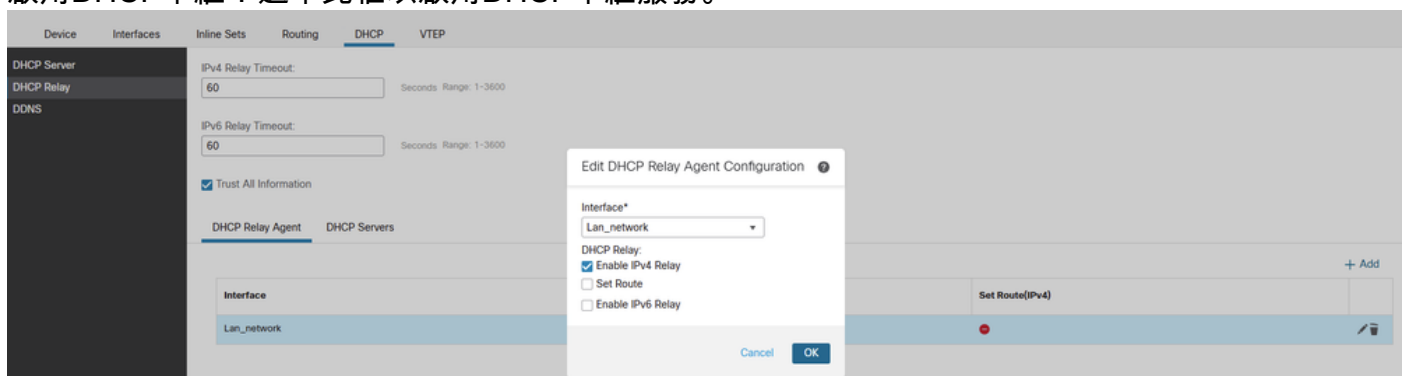
配置DHCP中繼代理

要配置DHCP中繼，請檢查以下步驟：

- 1.導航至Devices > Device Management。
- 2.按一下FTD裝置的編輯按鈕。
- 3.導航到DHCP > DHCP Relay選項。
- 4.按一下Add。

Interface:從下拉選單中選擇相應的介面。這是介面偵聽客戶端請求的位置，並且DHCP客戶端可以直接連線到此介面以處理IP地址請求。

啟用DHCP中繼：選中此框以啟用DHCP中繼服務。



DHCP_Relay_Agent_Config

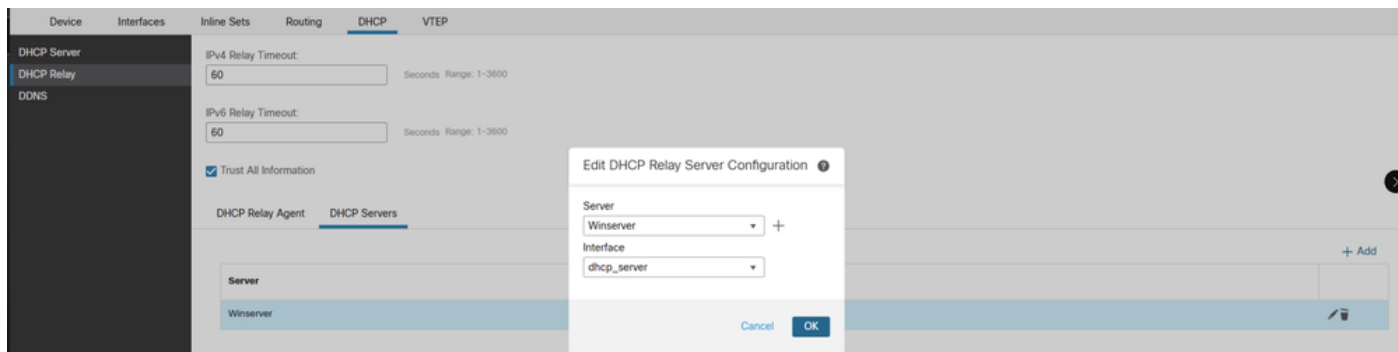
- 5.按一下OK儲存DHCP中繼代理的配置設定。

配置外部DHCP伺服器

要配置將客戶端請求轉發到的外部DHCP伺服器的IP地址，請檢查以下步驟：

導航到DHCP Server部分，然後按一下Add"

- 1.在Server欄位中，輸入DHCP伺服器的IP地址。您可以從下拉選單中選擇一個現有網路對象，也可以通過按一下加號(+)圖示建立一個新的網路對象。
- 2.在Interface欄位中，指定連線到DHCP伺服器的介面。
- 3.要儲存配置，請按一下OK。然後，按一下Save以儲存平台設定。



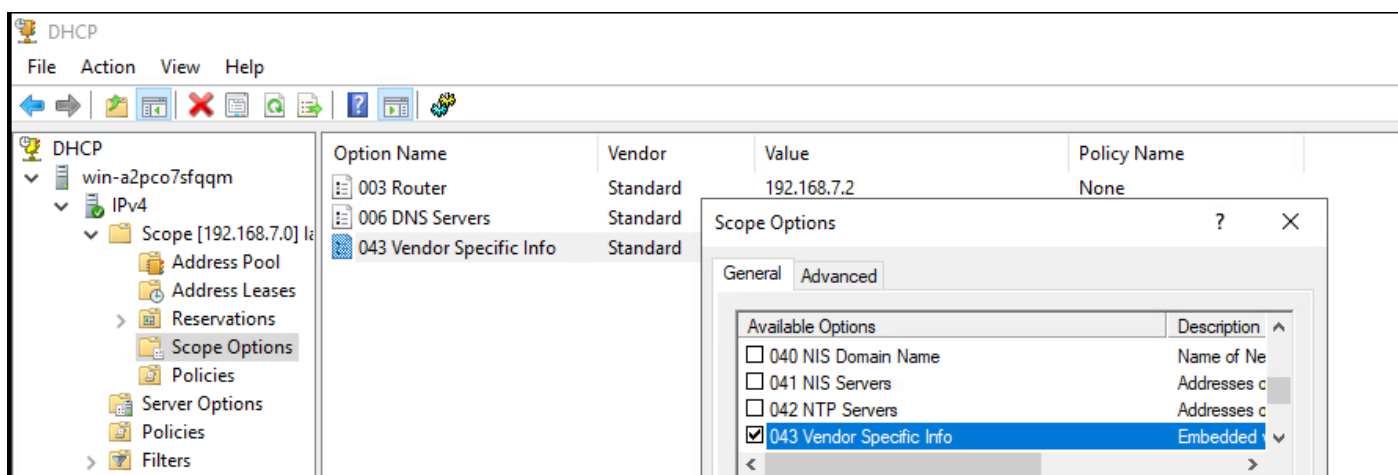
DHCP_Server_Config

4.接下來，轉到部署選項，選擇要應用更改的FTD裝置，然後按一下部署以啟動平台設定的部署。

在外部DHCP伺服器上啟用選項43

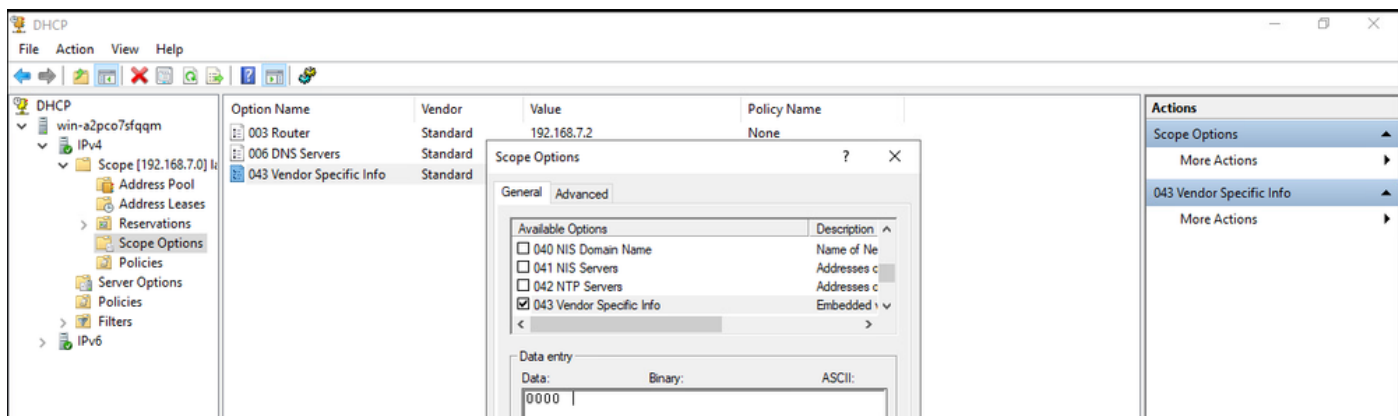
請註：根據RFC 2132，選項43的最小長度為1。

導航到DHCP伺服器設定並轉到IPv4，然後選擇Scope和Scope Options >More Actions >Configure Options並啟用選項43



Enable_Option_43_On_External_DHCP_Server

最初，預設設定會保留值為空，導致FTD捨棄封包並將其分類為格式不正確的封包。



從使用Wireshark的伺服器端，我們發現，在OFFER資料包中，當長度為0時，沒有選項43的值。

2845_	25665.243313	192.168.7.2	192.168.2.6	DHCP	344 DHCP Discover - Transaction ID 0x74376143
2845_	25665.243654	192.168.7.2	192.168.7.2	DHCP	342 DHCP Offer - Transaction ID 0x74376143
2845_	25665.243685	192.168.7.2	192.168.2.6	DHCP	370 DHCP Request - Transaction ID 0x74376143

Server host name not given	0000	00 50 56 a0 94 7c 00 50	56 a0 a8 54 08 00 45 00	PV... P V...T...E
Boot file name not given	0010	01 48 05 f3 00 00 00 11	00 00 c0 a8 02 06 c0 a8	H.....
Magic cookie: DHCP	0020	07 02 00 43 00 43 01 34	8b 9e 02 01 06 00 74 37	...C-C-4.....t7
> Option: (53) DHCP Message Type (Offer)	0030	61 43 00 00 00 00 00 00	00 00 c0 a8 07 0a c0 a8	aC...P V...Y...
> Option: (1) Subnet Mask (255.255.0)	0040	02 06 c0 a8 07 02 00 50	56 a0 2c 59 00 00 00 00	P V...Y...
> Option: (58) Renewal Time Value	0050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (59) Rebinding Time Value	0060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (51) IP Address Lease Time	0070	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (54) DHCP Server Identifier (192.168.2.6)	0080	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (3) Router	0090	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (6) Domain Name Server	00a0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (43) Vendor-Specific Information	00b0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
Length: 0	00c0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
Value: <MISSING>	00d0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
Value: <MISSING>	00e0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
	00f0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
	0100	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	

Non_Working_Server_Side_cap

Cisco Firepower威脅防禦(FTD)捨棄這些封包，因為這些封包的長度為0，且被視為格式錯誤，違反了RFC 2132。

```
<#root>
```

```
firepower#
```

```
debug dhcprelay packet
```

```
debug dhcprelay packet enabled at level 1
ftd# DHCPD/RA: Relay msg received, fip=ANY, fport=0 on Lan_network interface
DHCPD/RA: Received a BOOTREQUEST from interface 3 (size = 302)
DHCPD/RA: Binding successfully added to hash table
DHCPRA: relay binding created for client 0050.56a0.2c59.
DHCPRA: setting giaddr to 192.168.7.2.
dhcpd_forward_request: request from 0050.56a0.2c59 forwarded to 192.168.2.6.
```

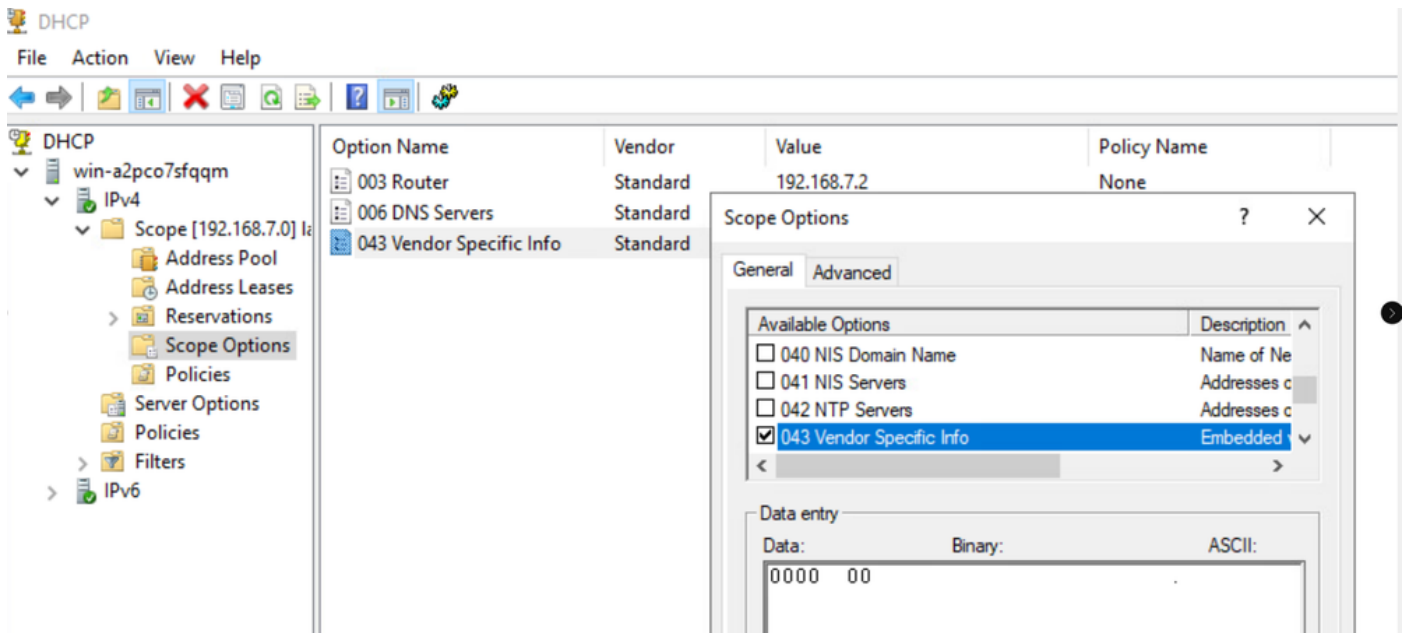
```
DHCPD/RA: option 43 is malformed.
```

```
DHCPD/RA: Unable to load workspace.
```

```
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on Lan_network interface
DHCPD/RA: Received a BOOTREQUEST from interface 3 (size = 328)
DHCPRA: relay binding found for client 0050.56a0.2c59.
DHCPRA: setting giaddr to 192.168.7.2.
DHCPRA: Server request counter 1
dhcpd_forward_request: request from 0050.56a0.2c59 forwarded to 192.168.2.6.
```

要根據RFC 2132將二進位制值調整為大於0，請按兩下043 Vendor Specific Info欄位並將值設定為00，如下圖所示。

此更改可確保IP地址成功租借給客戶端。



Changed_Binary_Value_to_

當選項43上的值設定為1時，伺服器端DORA進程

2848...	25882.406605	192.168.7.2	192.168.2.6	DHCP	344	DHCP Discover	- Transaction ID 0x9a608024
2848...	25882.406970	192.168.7.2	192.168.2.6	DHCP	342	DHCP Offer	- Transaction ID 0x9a608024
2848...	25882.409264	192.168.7.2	192.168.2.6	DHCP	370	DHCP Request	- Transaction ID 0x9a608024
2848...	25882.409833	192.168.7.2	192.168.2.6	DHCP	342	DHCP ACK	- Transaction ID 0x9a608024

Client hardware address padding: 00000000000000000000	0010	01 48 05 f4 00 00 00 11	00 00 c0 a8 02 06 c0 a8	H.....
Server host name not given	0020	07 02 00 43 00 43 01 34	8b 9e 02 01 06 00 9a 60	...C-D-4 HE.....
Boot file name not given	0030	00 24 00 00 00 00 00 00	00 00 c0 a8 07 0a c0 a8	...C-D-4 HE.....
Magic cookie: DHCP	0040	02 06 c0 a8 07 02 00 50	56 a0 2c 59 00 00 00 00	...P V,Y.....
> Option: (53) DHCP Message Type (Offer)	0050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (1) Subnet Mask (255.255.255.0)	0060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (58) Renewal Time Value	0070	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (59) Rebinding Time Value	0080	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (51) IP Address Lease Time	0090	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (54) DHCP Server Identifier (192.168.2.6)	00a0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (3) Router	00b0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (6) Domain Name Server	00c0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (43) Vendor-Specific Information	00d0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
Length: 1	00e0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
Value: 00	00f0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (255) End	0100	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
	0110	00 00 00 00 00 00 63 82	53 63 35 01 02 01 04 ff	...C- SC5.....
	0120	ff ff 00 3a 04 00 05 46	00 3b 04 00 09 3a 80 33	...F-;...:3

伺服器端_工作_pcap

當選項43上的值設定為1時，客戶端DORA會進行處理，我們可以看到客戶端是通過IP租借的。

2907...	1837526.548275	0.0.0.0	255.255.255.255	DHCP	344	128 DHCP Discover	- Transaction ID 0x9a608024
2907...	1837526.550203	192.168.2.6	192.168.7.10	DHCP	342	72 DHCP Offer	- Transaction ID 0x9a608024
2907...	1837526.551703	0.0.0.0	255.255.255.255	DHCP	370	128 DHCP Request	- Transaction ID 0x9a608024
2907...	1837526.553008	192.168.2.6	192.168.7.10	DHCP	342	72 DHCP ACK	- Transaction ID 0x9a608024

> Option: (53) DHCP Message Type (Offer)	0000	00 50 56 a0 2c 59 00 50	56 a0 48 2d 08 00 45 00	..PV,Y-P V,H...E..
> Option: (1) Subnet Mask (255.255.255.0)	0010	01 48 11 12 40 00 48 11	96 32 c0 a8 02 06 c0 a8	..H-@-H-2.....
> Option: (58) Renewal Time Value	0020	07 0a 00 43 00 44 01 34	48 45 02 01 06 00 e2 68	...C-D-4 HE.....h
> Option: (59) Rebinding Time Value	0030	3c 3f 00 00 00 00 00 00	00 00 c0 a8 07 0a c0 a8	<?.....
> Option: (51) IP Address Lease Time	0040	02 06 c0 a8 07 02 00 50	56 a0 2c 59 00 00 00 00	...P V,Y.....
> Option: (54) DHCP Server Identifier (192.168.2.6)	0050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (3) Router	0060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (6) Domain Name Server	0070	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
> Option: (43) Vendor-Specific Information	0080	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
Length: 1	0090	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
Value: 00	00a0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
	00b0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
	00c0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	

客戶端_工作端_pcap

<#root>

firepower#

debug dhcprelay packet

```
debug dhcprelay packet enabled at level 1
ftd# DHCPD/RA: Relay msg received, fip=ANY, fport=0 on Lan_network interface
DHCP: Received a BOOTREQUEST from interface 3 (size = 302)
DHCPRA: relay binding found for client 0050.56a0.2c59.
DHCPRA: setting giaddr to 192.168.7.2.
dhcpd_forward_request: request from 0050.56a0.2c59 forwarded to 192.168.2.6.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on dhcp_server interface
DHCP: Received a BOOTREPLY from relay interface 2 (size = 300, xid = 0x81f5dddc) at 06:55:25 UTC Tue Ma
DHCPRA: relay binding found for client 0050.56a0.2c59.
DHCPD/RA: creating ARP entry (192.168.7.10, 0050.56a0.2c59).
DHCPRA: forwarding reply to client 0050.56a0.2c59.
DHCPRA: Client Ip Address :192.168.7.10
DHCPRA: subnet mask in dhcp options :255.255.255.0
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on Lan_network interface
DHCP: Received a BOOTREQUEST from interface 3 (size = 328)
DHCPRA: relay binding found for client 0050.56a0.2c59.
DHCPRA: Server requested by client 192.168.2.6
DHCPRA: setting giaddr to 192.168.7.2.
DHCPRA: Server request counter 1
dhcpd_forward_request: request from 0050.56a0.2c59 forwarded to 192.168.2.6.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on dhcp_server interface
DHCP: Received a BOOTREPLY from relay interface 2 (size = 300, xid = 0x81f5dddc) at 06:55:25 UTC Tue Ma
DHCPRA: relay binding found for client 0050.56a0.2c59.
DHCPRA: exchange complete - relay binding deleted for client 0050.56a0.2c59.
DHCPD/RA: Binding successfully deactivated
dhcpd_destroy_binding() removing NP rule for client 192.168.7.2
DHCPD/RA: free ddns info and binding
DHCPD/RA: creating ARP entry (192.168.7.10, 0050.56a0.2c59).
DHCPRA: forwarding reply to client 0050.56a0.2c59.

DHCPRA: Client Ip Address :192.168.7.10

DHCPRA: subnet mask in dhcp options :255.255.255.0
```

驗證

設定DHCP伺服器或中繼之前，請確保FTD已向FMC註冊。此外，在DHCP中繼配置中驗證是否存在與DHCP伺服器的連線。

```
<#root>
```

```
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
<#root>
```

```
><Press Enter>
```

```
firepower#
```

```
ping
```

從FTD CLI驗證DHCP中繼代理配置。

```
<#root>
```

```
firepower#
```

```
show running-config dhcprelay
```

```
dhcprelay server 192.168.2.6 dhcp_server
dhcprelay enable Lan_network
dhcprelay timeout 60
dhcprelay information trust-all
```

疑難排解

若要疑難排解，請考慮以下幾點：

1. 驗證FTD和DHCP伺服器之間的路由，確保可從DHCP伺服器連線至該路由。
2. 確保DHCP伺服器具有訪問DHCP中繼代理介面的路由。
3. 若要解決使用者端無法接收IP位址的問題，您可以在FTD路由介面上執行封包擷取。

這將允許您檢查資料包捕獲中DHCP伺服器的DORA進程。

您可以使用[使用Firepower威脅防禦捕獲和Packet Tracer](#)有效地執行資料包捕獲。

要停止和刪除之前啟動的特定資料包捕獲會話，請執行以下命令。

```
no capture <capture_name>
```

4. 要檢查狀態並收集dhcprelay debug，請執行以下命令

為此，請登入FTD CLI。

```
<#root>
```

```
system support diagnostic-cli
```

```
enable
```

按Enter鍵。

```
<#root>
```

```
show dhcprelay statistic
```

```
show dhcprelay state
```

要檢查調試是否已啟用，請在以下命令執行。

```
<#root>
```

```
show debug
```

```
<#root>
```

To capture debug excute below commands

```
debug dhcprelay packet  
debug dhcprelay event
```

```
<#root>
```

To disable debug

```
undebug all
```

相關資訊

[使用FMC設定FTD上的DHCP伺服器和中繼](#)

[DHCP和DDNS](#)

[技術支援與文件 - Cisco Systems](#)

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）。