

在FMC中配置管理和診斷介面的合併

目錄

[簡介](#)

[必要條件](#)

[背景資訊](#)

[採用元件](#)

[設定](#)

[FTD內部架構圖表](#)

[收斂過程](#)

[驗證](#)

[疑難排解 — 研究案例](#)

[收斂配置之前](#)

[收斂配置之後](#)

簡介

本檔案介紹設定FTD 7.4.0版本新增的管理介面和診斷介面合併功能的步驟。

必要條件

思科建議您瞭解以下主題：

- 思科安全防火牆威脅防禦(FTD)
- 思科安全防火牆管理員中心(FMC)

背景資訊

在7.3及更早版本中，實體管理介面會在診斷邏輯介面(Lina)和管理邏輯介面(Linux)之間共用。

在7.4及更高版本中，診斷介面與管理相合併，從而簡化使用者體驗。

對於使用7.4及更高版本的新裝置，不能使用舊版診斷介面。只有合併的管理介面可用。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

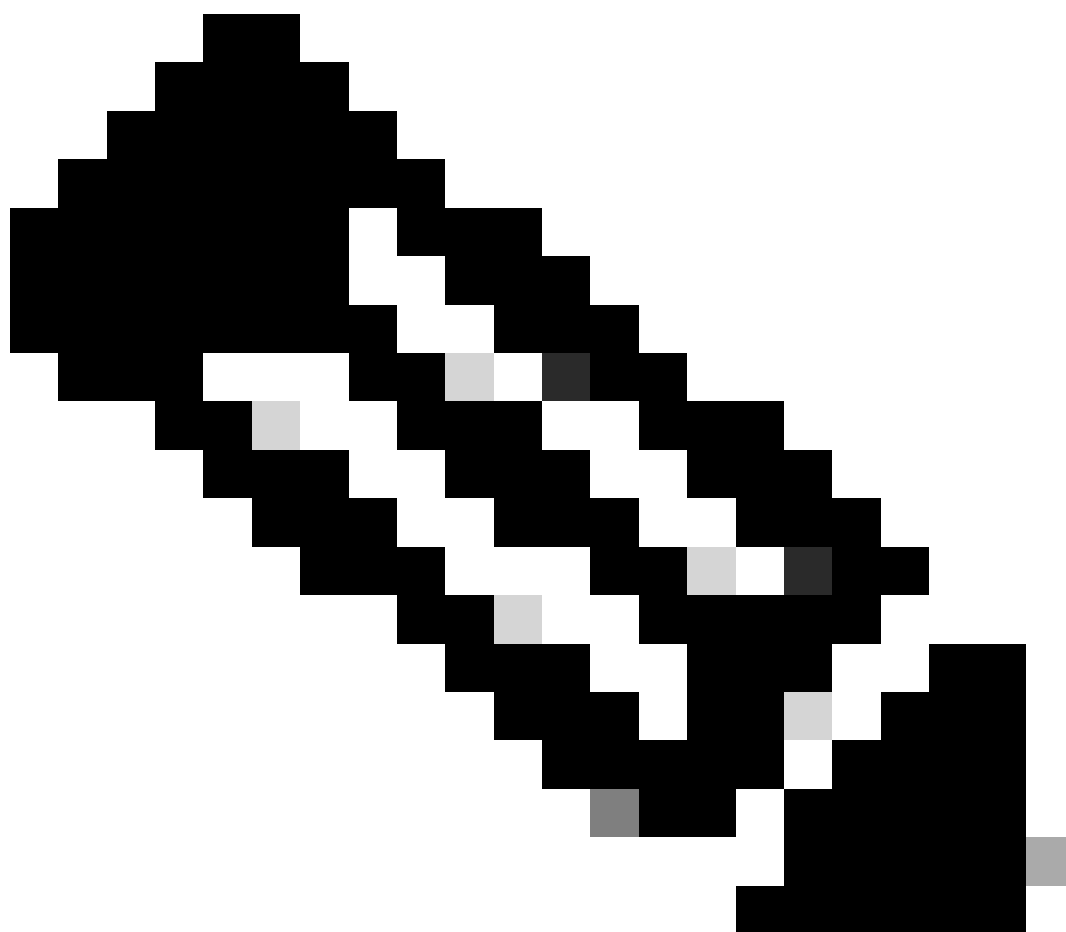
- 虛擬思科安全防火牆威脅防禦(FTD)版本7.4.2
- 虛擬思科安全防火牆管理器中心(FMC)版本7.4.2

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。

設定

如果升級到7.4或更高版本，並且您擁有診斷介面的配置，則可以選擇手動合併介面，也可以繼續使用單獨的診斷介面。

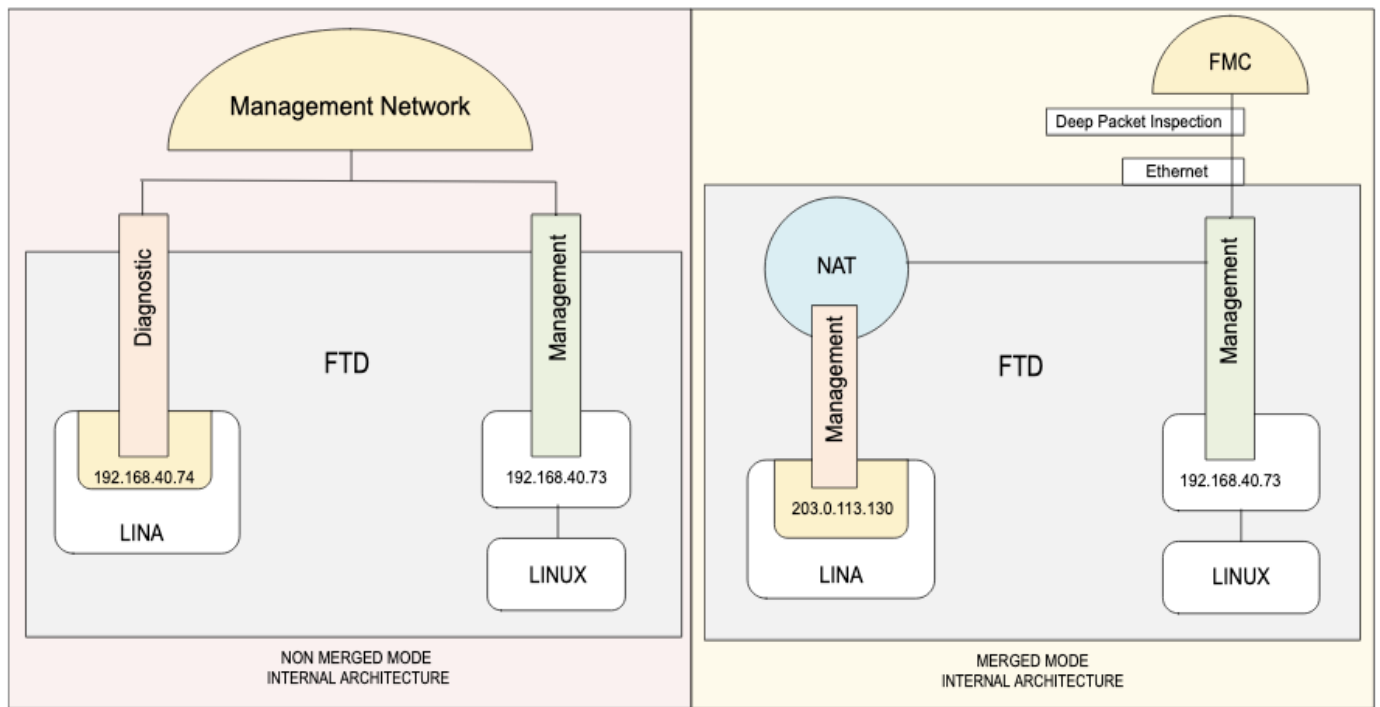
如果您沒有診斷介面的任何配置，則介面合併將自動完成。



附註：在以後的版本中將取消對診斷介面的支援，因此計畫儘快合併介面。

FTD內部架構圖表

融合管理介面概述



融合管理介面前後內部架構概述

在左側，診斷邏輯介面(Lina)和管理邏輯介面(Linux)的內部體系結構。 7.3及更低版本。

在右側，為單個管理介面提供內部架構。Lina對管理網路的訪問使用NAT服務。

收斂過程

如果診斷介面中存在配置，則升級後不會自動合併介面，您需要執行收斂過程。

此過程要求您確認配置更改，並在某些情況下手動修復配置。

要檢視裝置的當前模式，請在FTD CLI螢幕中輸入show management-interface convergence命令

```
> show management-interface convergence
no management-interface convergence
```

該結果顯示管理介面未合併。

步驟 1.

在FMC UI上，導覽至Devices > Device Management，然後選擇要編輯的FTD。它會直接開啟到Interfaces頁籤。

Firewall Management Center
Devices / Secure Firewall Interfaces

OverviewAnalysisPolicies**Devices**ObjectsIntegration

Deploy 🔍 10 ⚙️ ? admin ✓

Tac_test

SaveCancel

Cisco Firepower Threat Defense for VMware

Device**Interfaces**Inline SetsRoutingDHCPVTEP

Management Interface action needed.
Merge the Management and Diagnostic interfaces on the [Management Interface Merge](#) dialog box, or merge them later by clicking the ➤ icon for Diagnostic interface in the table below.
Merging the interface will cause some downtime. [Learn more](#)

All InterfacesVirtual Tunnels

🔍 Search by name Sync Device Add Interfaces ▾

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Diagnostic0/0	diagnostic	Physical			192.168.40.74/255.255.255.0(Stat...	Disabled	Global	➤
GigabitEthernet0/0		Physical				Disabled		
GigabitEthernet0/1		Physical				Disabled		
GigabitEthernet0/2		Physical				Disabled		

裝置升級到軟體版本7.4.2後合併診斷和管理介面所需的操作

步驟 2.

刪除Diagnostic介面上的所有配置。診斷介面必須沒有任何配置才能繼續合併。

例如，在此診斷介面中存在：IP地址和靜態路由。

Firewall Management Center
Devices / Secure Firewall Interfaces

OverviewAnalysisPolicies**Devices**ObjectsIntegration

Deploy 🔍 10 ⚙️ ? admin ✓

Tac_test

SaveCancel

Cisco Firepower Threat Defense for VM

Device**Interfaces**Inline Set

Management Interface action
Merge the Management and Diagnostic
Merging the interface will cause some d

All InterfacesVirtual Tunnels

🔍 Search by name Sync Device Add Interfaces ▾

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Diagnostic0/0	diagnostic	Physical			192.168.40.74/255.255.255.0(Stat...	Disabled	Global	➤
GigabitEthernet0/0		Physical				Disabled		
GigabitEthernet0/1		Physical				Disabled		
GigabitEthernet0/2		Physical				Disabled		

Edit Physical Interface

General**IPv4**IPv6Path MonitoringHardware ConfigurationManager AccessAdvanced

IP Type:
Use Static IP

IP Address:
192.168.40.74/255.255.255.0
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

CancelOK

刪除診斷介面IP地址

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ⓘ admin ▾ CISCO SECURE

Tac_test

Cisco Firepower Threat Defense for VMware

Device Interfaces **Inline Sets** **Routing** DHCP VTEP

Manage Virtual Routers
Global ▾
Virtual Router Properties
ECMP
BFD
OSPF
OSPFv3
EIGRP
RIP
Policy Based Routing
BGP ▾
 IPv4
 IPv6
Static Route
Multicast Routing

Network ▲

Interface

Leaked from Virtual Router

Gateway

Tunneled

Metric

Tracked

▼ IPv4 Routes

DNS diagnostic Global 192.168.40.254 false 1  

▼ IPv6 Routes

+ Add Route

在診斷介面上配置靜態路由

步驟 3.

按一下Management Interface Merge action needed區域，或按一下「診斷」(Diagnostic)介面上「編輯」(Edit)圖示（鉛筆）旁邊的Merge圖示。

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ⓘ admin ▾ CISCO SECURE

Tac_test

Cisco Firepower Threat Defense for VMware

Device **Interfaces** Inline Sets Routing DHCP

Management Interface action needed.
Merge the Management and Diagnostic interfaces on the Management Interface. Merging the interface will cause some downtime. [Learn more](#)

All Interfaces Virtual Tunnels

Interface	Logical Name
Diagnostic0/0	diagnostic
 GigabitEthernet0/0	
 GigabitEthernet0/1	
 GigabitEthernet0/2	

Management Interface Merge ⓘ

- 1. The management interface merge will be synced to the standby/data unit. The IP addresses shown in the "Review Uses" section shows the active unit's active address.
- 2. After you click Proceed, IP address changes will be saved, and you cannot revert the management interface merge, even if you discard the deployment.
- 3. Diagnostic interface static routing is no longer supported; you must delete the route before you can proceed. [Learn more](#)
- 4. HA monitoring for diagnostic interface is not supported.

In this release, you can merge the Management and Diagnostic interfaces to use the single IP instead of two IP addresses. The merged interface will be called Management and use the current management IP address. You will need to update all external services that communicate with Diagnostic IP address. [Learn more](#)

Proceed Cancel

Path Monitoring Virtual Router

Disabled Global  

Disabled 

Disabled 

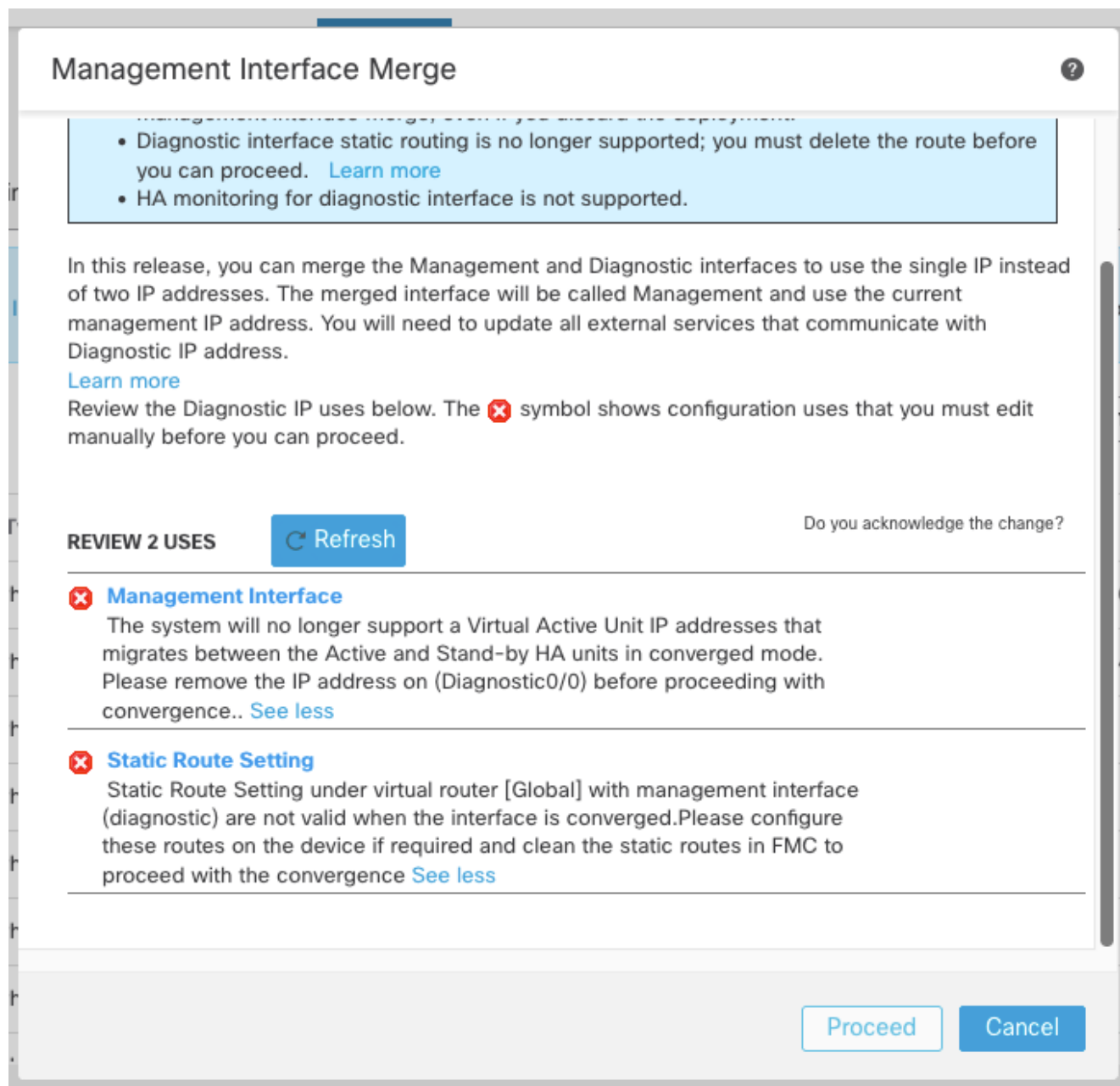
Disabled 

管理介面合併資訊，然後繼續



附註：對於高可用性對和群集，請在主用/控制單元上執行此任務。合併的配置將自動複製到備用/資料單元。

-
- 對於需要手動更改或移除的任何發生情況，都可能會出現警告圖示。



有關合併前需要刪除的配置的警告示例

如果情況如此：取消對話方塊，繼續刪除配置或重新配置，然後重新開啟Management Interface Merge對話方塊。

- 將在裝置上工作的平台設定標有警告圖示並要求確認。

Management Interface Merge

? x

- The management interface merge will be synced to the standby unit. The IP addresses shown in the "Review Uses" section shows the active unit's active address.
- After you click Proceed, IP address changes will be saved, and you cannot revert the management interface merge, even if you discard the deployment.
- Diagnostic interface static routing is no longer supported; you must delete the route before you can proceed. [Learn more](#)
- HA monitoring for diagnostic interface is not supported.

In this release, you can merge the Management and Diagnostic interfaces to use the single IP instead of two IP addresses. The merged interface will be called Management and use the current management IP address. You will need to update all external services that communicate with Diagnostic IP address.

[Learn more](#)

Review the Diagnostic IP uses below. The  symbol shows configuration uses that you must edit manually before you can proceed.

REVIEW 2 USES

 Refresh

Do you acknowledge the change?

HTTP Access

Management interface (management) is used in (HTTP Access) of PF... [See more](#)



ICMP Access

Management interface (management) is used in (ICMP Access) of PF... [See more](#)



Cancel

Proceed

必須編輯的平台設定配置警告示例

- 按一下Do you acknowledge the change中的框。列，然後按一下Proceed。

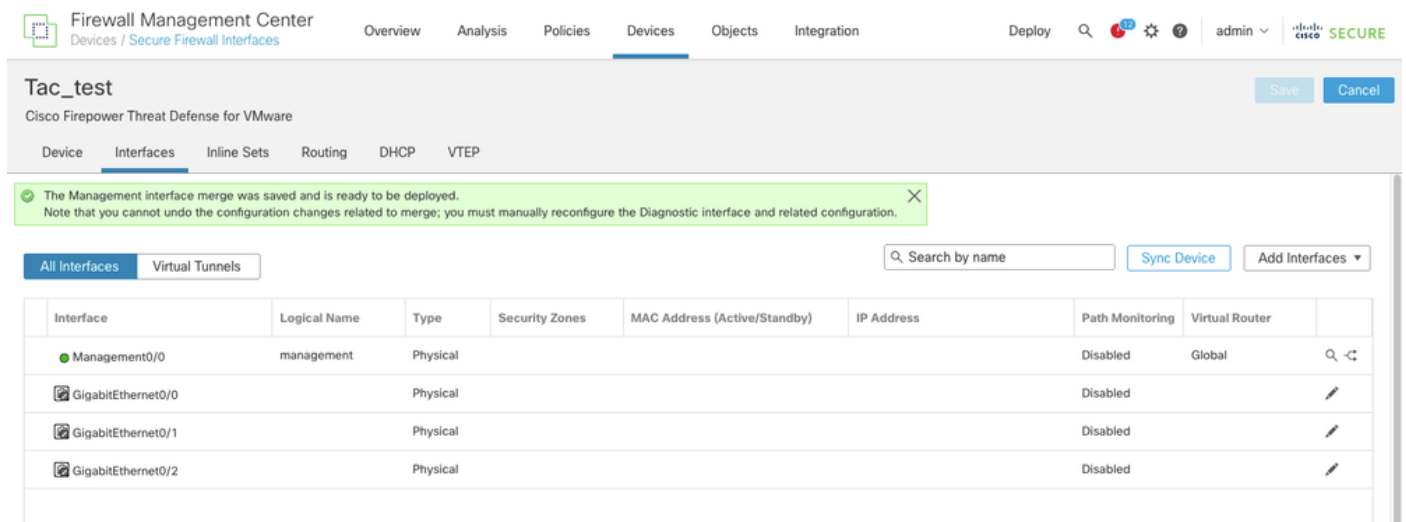
步驟 4.

合併組態後，會顯示成功的標語：

「管理介面合併已儲存並準備部署。

請注意，無法撤消與合併相關的配置更改；您必須手動重新配置診斷介面和相關配置。"

部署新的合併配置。



管理介面合併已儲存並準備部署

管理介面顯示在Interfaces頁面上，但它是只讀的。

部署後，管理介面上的收斂過程完成。

步驟5. 可選

如果您有任何外部服務與診斷介面通訊，則需要更改其配置以使用管理介面IP地址，因為在融合模式下已刪除管理路由回退。

舉例來說：

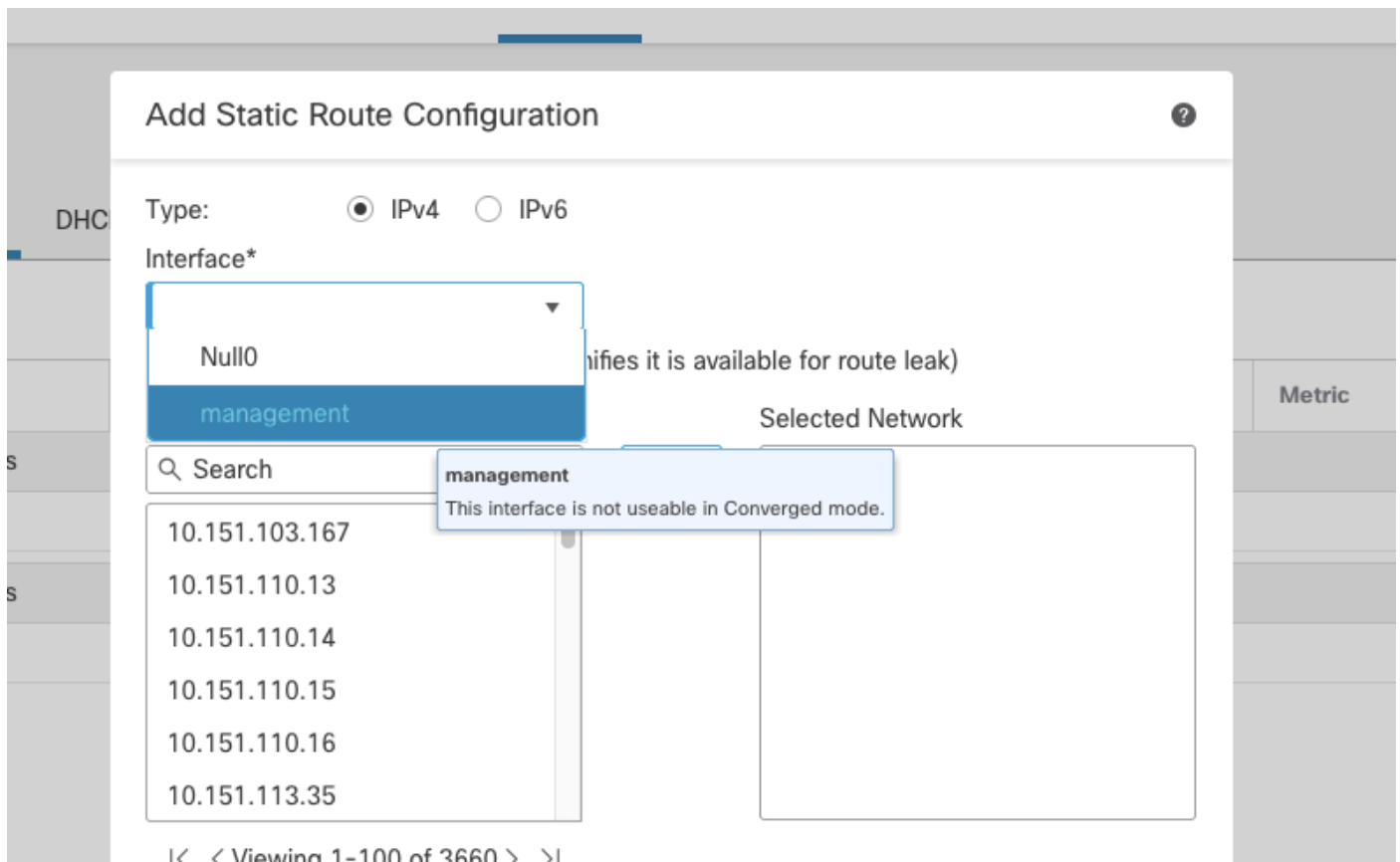
- SNMP使用者端
- RADIUS伺服器
- 要通過管理網路訪問DNS伺服器，使用者必須明確選擇「Enable DNS Lookup via diagnostic/Management Interface also」（通過診斷/管理介面啟用DNS查詢）。在Platform Settings > DNS configuration上，DNS查詢和ICMP（ping和traceroute）設定為異常：在這些情況下，威脅防禦會使用資料，如果沒有找到路由，則自動回退到管理。

管理介面使用靜態路由只能通過FTD CLI類(Linux)進行配置

Lina管理埠預設路由將所有幀傳送到Linux模組。

```
> configure network static-routes ipv4 add management ?  
IP address AAA.BBB.CCC.DDD where each part is in the range 0-255 destination address
```

在FMC UI上，管理介面呈灰色顯示，以供選擇。



合併完成後，無法在靜態路由上選擇管理介面。

驗證

在管理介面上合併後預期的更改

- 通過執行命令驗證FTD CLI關閉的收斂模式

```
> show management-interface convergence
management-interface convergence
```

- 在FMC UI上，介面名稱更改為Management0/0，邏輯名稱更改為management。

Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 12 ⚙️ ⓘ admin ▾ **SECURE**

Tac_test Save Cancel

Cisco Firepower Threat Defense for VMware

Device **Interfaces** Inline Sets Routing DHCP VTEP

All Interfaces Virtual Tunnels 🔍 Search by name Sync Device Add Interfaces ▾

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Management0/0	management	Physical				Disabled	Global	🔍 ↺
GigabitEthernet0/0		Physical				Disabled		✎
GigabitEthernet0/1		Physical				Disabled		✎
GigabitEthernet0/2		Physical				Disabled		✎

管理介面名稱和邏輯名稱合併確認

- 在FTD CLI Clish上，新的IP位址會自動在Lina上設定為管理介面。
NAT用作內部實現：內部私有IPv4地址203.0.113.130和IPv6地址fd00:0:1:1::2是已分配地址（兩者都可能更改）。
這些IP通過NAT連線到公共Linux核心FTD IPv4和IPv6地址，因此不再需要Lina上的公共IP。

在專家模式下，「ifconfig」顯示Linux的內部IPv4(203.0.113.129)和IPv6(fd00:0:1:1::1)地址。

FTD CLI Clish:

```
> show interface management
Interface Management0/0 "management", is up, line protocol is up
  Hardware is en_vtun rev00, DLY 10 usec
    Input flow control is unsupported, output flow control is unsupported
    MAC address 0050.56b3.f75d, MTU 1500
    IP address 203.0.113.130, subnet mask 255.255.255.248
```

Expert mode on Linux:

```
root@ftd01:/home/admin# ifconfig
```

```
...
```

```
tap5: flags=4419
```

```
    mtu 1500
    inet 203.0.113.129 netmask 255.255.255.248 broadcast 203.0.113.135
    inet6 fe80::8403:9ff:febf:6d16 prefixlen 64 scopeid 0x20
```

```
    inet6 fd00:0:1:1::1 prefixlen 123 scopeid 0x0
```

疑難排解 — 研究案例

在本研究案例中，在升級到7.4.2之前，虛擬FTD上的診斷介面已設定一個單獨的IP位址，用於連線到DNS查詢的外部服務。

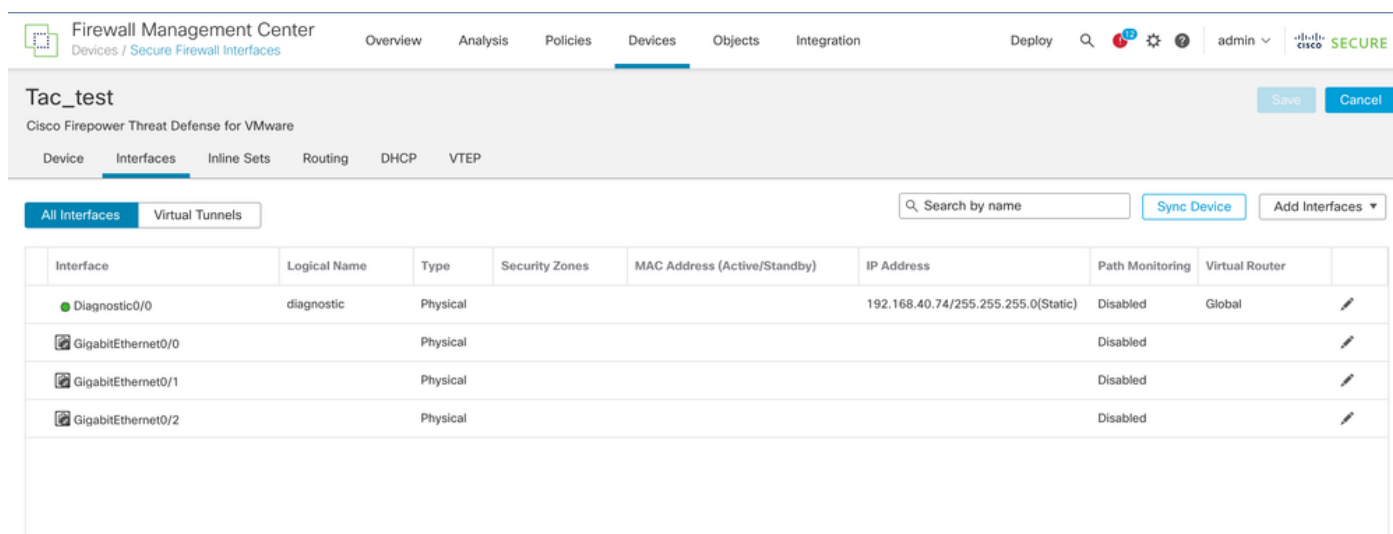
升級到7.4.2後，需要進行融合，這就是合併前後FMC UI、FTD CLI Lina和Linux中的配置方式。

FTD CLI Lina和Linux上也有流量擷取，以顯示使用邏輯診斷介面移動來使用管理介面的流量。

收斂配置之前

診斷介面具有單獨的IP和用於DNS查詢的靜態路由，因此在FTD中，它同時使用從Lina到Linux的邏輯介面。

FMC UI配置



Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 12 ⚙️ ⓘ admin ▾ CISCO SECURE

Tac_test Save Cancel

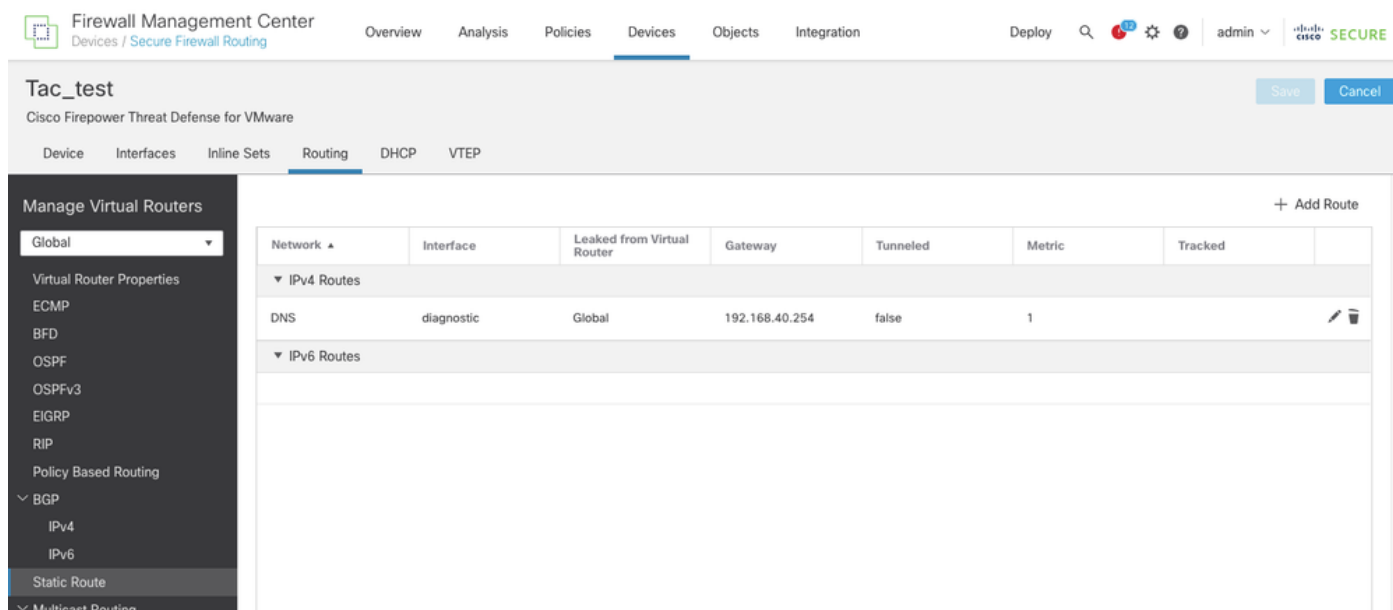
Cisco Firepower Threat Defense for VMware

Device **Interfaces** Inline Sets Routing DHCP VTEP

All Interfaces Virtual Tunnels 🔍 Search by name Sync Device Add Interfaces ▾

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Diagnostic0/0	diagnostic	Physical			192.168.40.74/255.255.255.0(Static)	Disabled	Global	
GigabitEthernet0/0		Physical				Disabled		
GigabitEthernet0/1		Physical				Disabled		
GigabitEthernet0/2		Physical				Disabled		

合併前診斷介面配置



Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 12 ⚙️ ⓘ admin ▾ CISCO SECURE

Tac_test Save Cancel

Cisco Firepower Threat Defense for VMware

Device **Interfaces** Inline Sets **Routing** DHCP VTEP

Manage Virtual Routers + Add Route

Global ▾

Virtual Router Properties

- ECMP
- BFD
- OSPF
- OSPFv3
- EIGRP
- RIP
- Policy Based Routing
- ▼ BGP
 - IPv4
 - IPv6
- Static Route**
- ▼ Multicast Routing

Network ▲	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked	
▼ IPv4 Routes							
DNS	diagnostic	Global	192.168.40.254	false	1		
▼ IPv6 Routes							

在診斷介面上配置的靜態路由

DNS配置通過

Devices > Platform Settings，選擇策略，然後選擇DNS選項卡。

Firewall Management Center

Devices / Platform Settings Editor

Overview

Analysis

Policies

Devices

Objects

Integration

FQDN_Test_PlatformSettings

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

DNS Settings

Trusted DNS Servers

DNS Resolution Settings

Specify DNS servers group and device interfaces to reach them.

Enable DNS name resolution by device

DNS Server Groups

Add

DNS_Server_lab (Default)

any

Expiry Entry Timer:

1

Range: 1-65535 minutes

Poll Timer:

240

Range: 1-65535 minutes

平台設定中的DNS配置

FQDN_Test_PlatformSettings

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

Empty Entry Name

1

Range: 1-65535 minutes

Poll Timer:

240

Range: 1-65535 minutes

Interface Objects

Devices will use specified interface objects for connecting with DNS Servers.

Available Interface Objects

Q Search

Selected Interface Objects

Add

☒ Enable DNS Lookup via diagnostic/Management interface also.

P

選中「通過診斷/管理介面啟用DNS查詢」覈取方塊

透過FTD Lina設定的診斷介面

```
interface Management0/0
management-only
nameif diagnostic
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.40.74 255.255.255.0
```

ftd01# sh ip

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
Management0/0	diagnostic	192.168.40.74	255.255.255.0	manual

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
Management0/0	diagnostic	192.168.40.74	255.255.255.0	manual

```
ftd01# sh route management-only
Routing Table: mgmt-only
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is not set

```
S      10.10.10.10 255.255.255.255 [1/0] via 192.168.40.254, diagnostic
C      192.168.40.0 255.255.255.0 is directly connected, diagnostic
L      192.168.40.74 255.255.255.255 is directly connected, diagnostic
```

FTD CLI Lina上的DNS組態

```
ftd01# sh run dns
dns domain-lookup diagnostic
DNS server-group DNS_Server_lab
    retries 5
    timeout 15
    name-server 10.10.10.10 diagnostic
    domain-name test.lab
DNS server-group DefaultDNS
dns-group DNS_Server_lab
```

在診斷介面上擷取前往DNS伺服器10.10.10.10的DNS流量

```
ftd01# sh cap
capture diag type raw-data trace detail interface diagnostic [Capturing - 340 bytes]
    match udp any host 10.10.10.10 eq domain
```

```
ftd01# sh cap diag
```

5 packets captured

1: 00:15:39.660442	192.168.40.74.59939 > 10.10.10.10.53: udp 27
2: 00:15:54.661953	192.168.40.74.59939 > 10.10.10.10.53: udp 27
3: 00:16:09.661739	192.168.40.74.59939 > 10.10.10.10.53: udp 27
4: 00:16:24.667674	192.168.40.74.59939 > 10.10.10.10.53: udp 27
5: 00:16:39.684946	192.168.40.74.59939 > 10.10.10.10.53: udp 27

5 packets shown

```
ftd01#
```

在Linux專家模式下捕獲，以確認管理介面上來自診斷介面的DNS查詢流量的正確流動

```
root@ftd01:/home/admin# tcpdump -i br1 port 53
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on br1, link-type EN10MB (Ethernet), capture size 262144 bytes
04:58:14.648941 IP 192.168.40.74.49171 > 10.10.10.10.domain: 5655+ AAAA? cisco.com. (27)
04:58:29.656317 IP 192.168.40.74.11606 > 10.10.10.10.domain: 26905+ A? cisco.com. (27)
04:58:44.686568 IP 192.168.40.74.11606 > 10.10.10.10.domain: 24324+ A? cisco.com. (27)
04:58:59.704586 IP 192.168.40.74.11606 > 10.10.10.10.domain: 35592+ A? cisco.com. (27)
04:59:14.742685 IP 192.168.40.74.11606 > 10.10.10.10.domain: 40993+ A? cisco.com. (27)
04:59:29.763690 IP 192.168.40.74.11606 > 10.10.10.10.domain: 62225+ A? cisco.com. (27)
04:59:44.796484 IP 192.168.40.74.11606 > 10.10.10.10.domain: 25350+ A? cisco.com. (27)
```

收斂配置之後

如收斂過程所述，為了進行合併，必須刪除診斷介面上的所有配置。

合併完成後，FMC和FTD CLI上的資訊如下。

使用FMC UI的管理介面配置

Devices > Device Management，選擇FTD。它會直接開啟到Interfaces頁籤。

The screenshot shows the FMC interface for a device named 'Tac_test'. The 'Interfaces' tab is selected, displaying a table of interfaces. The table has columns for Interface, Logical Name, Type, Security Zones, MAC Address (Active/Standby), IP Address, Path Monitoring, and Virtual Router. The interfaces listed are Management0/0, GigabitEthernet0/0, GigabitEthernet0/1, and GigabitEthernet0/2. All interfaces are of type 'Physical' and have 'Path Monitoring' set to 'Disabled'.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0		Physical				Disabled	
GigabitEthernet0/1		Physical				Disabled	
GigabitEthernet0/2		Physical				Disabled	

合併後的管理介面

The screenshot shows the FMC interface for a device named 'Tac_test'. The 'Routing' tab is selected, displaying a table of routes. The table has columns for Network, Interface, Leaked from Virtual Router, Gateway, Tunneled, Metric, and Tracked. The routes are categorized into IPv4 Routes and IPv6 Routes. A sidebar on the left shows the 'Manage Virtual Routers' menu with options like Global, Virtual Router Properties, ECMP, BFD, OSPF, OSPFv3, EIGRP, RIP, Policy Based Routing, BGP, IPv4, IPv6, Static Route, and Multicast Routing.

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
IPv6 Routes						

未新增到DNS伺服器的靜態路由

DNS配置必須在「平台設定」上保持相同。

Devices > Platform Settings，選擇策略，然後選擇DNS選項卡。

為了在不新增靜態路由的情況下繼續將DNS查詢傳送到管理介面，「同時通過診斷/管理介面啟用DNS查詢」。必須保持選中狀態。

 Firewall Management Center
Devices / Platform Settings Editor

OverviewAnalysisPoliciesDevicesObjectsIntegration

FQDN_Test_PlatformSettings
Enter Description

ARP InspectionBannerDNSExternal AuthenticationFragment SettingsHTTP AccessICMP AccessNetFlowSSH AccessSMTP ServerSNMPSSLSyslogTimeoutsTime SynchronizationTime ZoneUCAPL/CC CompliancePerformance Profile

DNS SettingsTrusted DNS Servers

DNS Resolution Settings

Specify DNS servers group and device interfaces to reach them.

☒ Enable DNS name resolution by device

DNS Server GroupsAdd

DNS_Server_lab (Default)
any

Expiry Entry Timer:

1

Range: 1-65535 minutes

Poll Timer:

240

Range: 1-65535 minutes

平台設定上的DNS配置

FQDN_Test_PlatformSettings

Enter Description

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

1

Range: 1-65535 minutes

Poll Timer:

240

Range: 1-65535 minutes

Interface Objects

Devices will use specified interface objects for connecting with DNS Servers.

Available Interface Objects

Q Search

Selected Interface Objects

Add



Enable DNS Lookup via diagnostic/Management interface also.

通過診斷/管理介面啟用DNS查詢的選項也必須保持相同

FTD CLI上的組態

```
> show interface management
```

```
Interface Management0/0 "management", is up, line protocol is up
```

```
Hardware is en_vtun rev00, DLY 10 usec
```

```
Input flow control is unsupported, output flow control is unsupported
```

```
MAC address 0050.56b3.f75d, MTU 1500
```

```
IP address 203.0.113.130, subnet mask 255.255.255.248
```

```
> show interface ip brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	administratively down	up
GigabitEthernet0/1	unassigned	YES	unset	administratively down	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	up
Internal-Control0/0	127.0.1.1	YES	unset	up	up
Internal-Control0/1	unassigned	YES	unset	up	up
Internal-Data0/0	unassigned	YES	unset	down	up
Internal-Data0/0	unassigned	YES	unset	up	up
Internal-Data0/1	169.254.1.1	YES	unset	up	up
Internal-Data0/2	unassigned	YES	unset	up	up
Management0/0	203.0.113.130	YES	unset	up	up

```
ftd01# sh route management-only
```

Routing Table: mgmt-only

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF

Gateway of last resort is not set

LINA端的FTD CLI上的DNS組態

```
ftd01# sh run dns
dns domain-lookup management
DNS server-group DNS_Server_lab
    retries 5
    timeout 15
    name-server 10.10.10.10 management
    domain-name test.lab
DNS server-group DefaultDNS
dns-group DNS_Server_lab
```

在Linux專家模式下捕獲，以確認DNS查詢流量在管理介面上的正確流動。

```
root@ftd01:/home/admin# tcpdump -i br1 port 53
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on br1, link-type EN10MB (Ethernet), capture size 262144 bytes
20:20:33.623146 IP ftd01.60310 > 10.10.10.10.domain: 61954+ A? cisco.com. (27)
20:20:33.623533 IP ftd01.33417 > umbrella.domain: 20595+ PTR? 10.10.10.10.in-addr.arpa. (42)
20:20:48.660172 IP ftd01.60310 > 10.10.10.10.domain: 41252+ A? cisco.com. (27)
20:20:52.638426 IP ftd01.39304 > umbrella.domain: 20595+ PTR? 10.10.10.10.in-addr.arpa. (42)
20:21:09.669133 IP ftd01.47150 > umbrella.domain: 39343+ AAAA? ftd01. (23)
20:21:09.669305 IP ftd01.50173 > umbrella.domain: 57694+ AAAA? ftd01. (23)
20:21:11.659352 IP ftd01.48092 > umbrella.domain: 46478+ PTR?.opendns.in-addr.arpa. (45)
20:21:14.673992 IP ftd01.58547 > umbrella.domain: 57694+ AAAA? ftd01. (23)
20:21:18.673371 IP ftd01.47607 > umbrella.domain: 39343+ AAAA? ftd01. (23)
20:21:18.695507 IP ftd01.60310 > 10.10.10.10.domain: 29973+ A? cisco.com. (27)
```

根據此證據，可以確認DNS查詢即使沒有通過Linux在管理介面上新增靜態路由也仍然有效。

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）。