瞭解Firepower威脅防禦（FMC管理）中的FQDN功能

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

- 功能概述
- 6.3之前的版本呢？

設定

- 網路圖表
- 架構-要點
- 設定步驟

驗證

疑難排解

- 收集FMC故障排除檔案
- 常見問題/錯誤消息
- 部署失敗
- 建議的故障排除步驟
- 沒有啟用的FQDN

問答

簡介

本文檔介紹對Firepower管理中心(FMC)和Firepower威脅防禦(FTD)的FQDN功能（從6.3.0版開始）的配置。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower管理中心

採用元件

本檔案中的資訊是根據以下軟體版本：

- 運行軟體版本6.3.0的Cisco Firepower威脅防禦(FTD)虛擬
- 運行軟體版本6.3.0的Firepower管理中心虛擬(vFMC)

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

本文檔介紹由6.3.0版軟體引入的Firepower管理中心(FMC)和Firepower威脅防禦(FTD)完全限定域名(FQDN)功能的配置。

此功能存在於思科調適型安全裝置(ASA)中，但FTD的初始軟體版本中沒有。

在配置FQDN對象之前，請確保滿足以下條件：

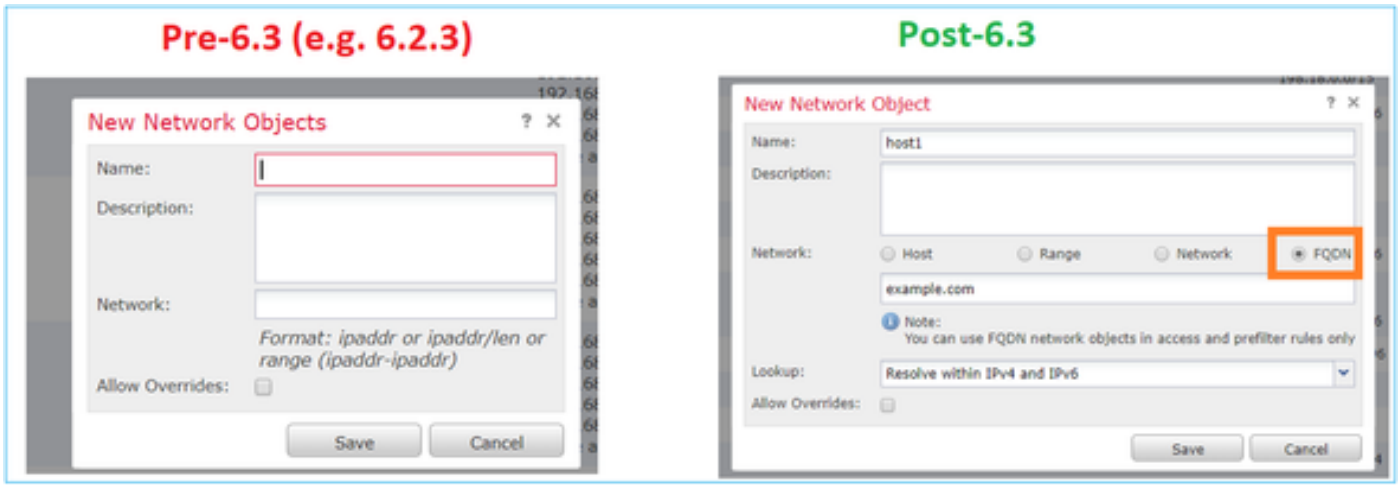
- Firepower管理中心必須運行版本6.3.0或更高版本。可以是物理或虛擬
- Firepower威脅防禦必須運行版本6.3.0或更高版本。可以是物理或虛擬

功能概述

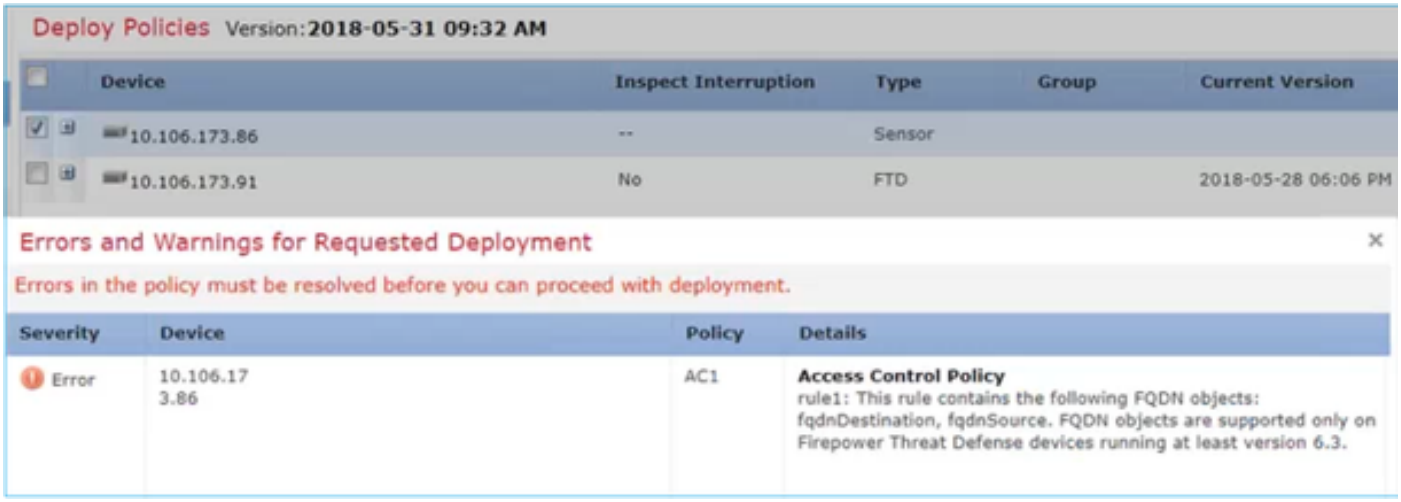
此功能將FQDN解析為IP地址，並在訪問控制規則或預過濾器策略引用後使用後者過濾流量。

6.3之前的版本呢？

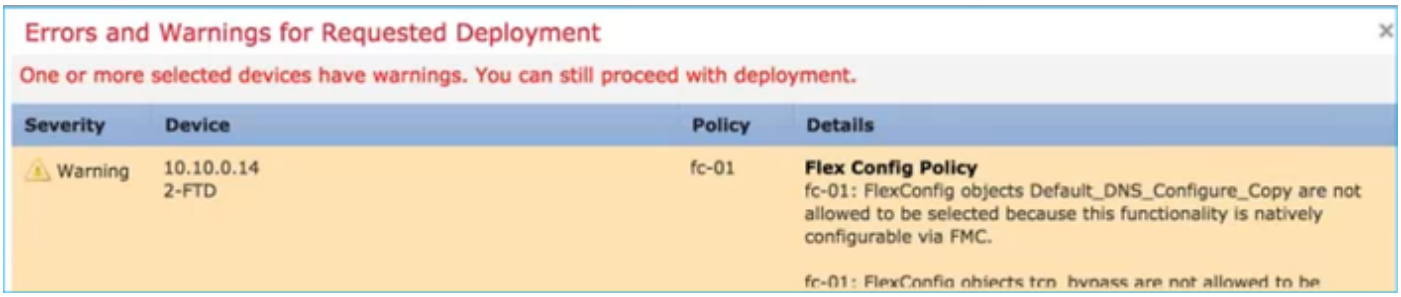
- 運行早於6.3.0版本的FMC和FTD無法配置FQDN對象。



- 如果FMC執行版本6.3或更新版本，但FTD執行版本早於6.3，則原則的部署會顯示以下錯誤：

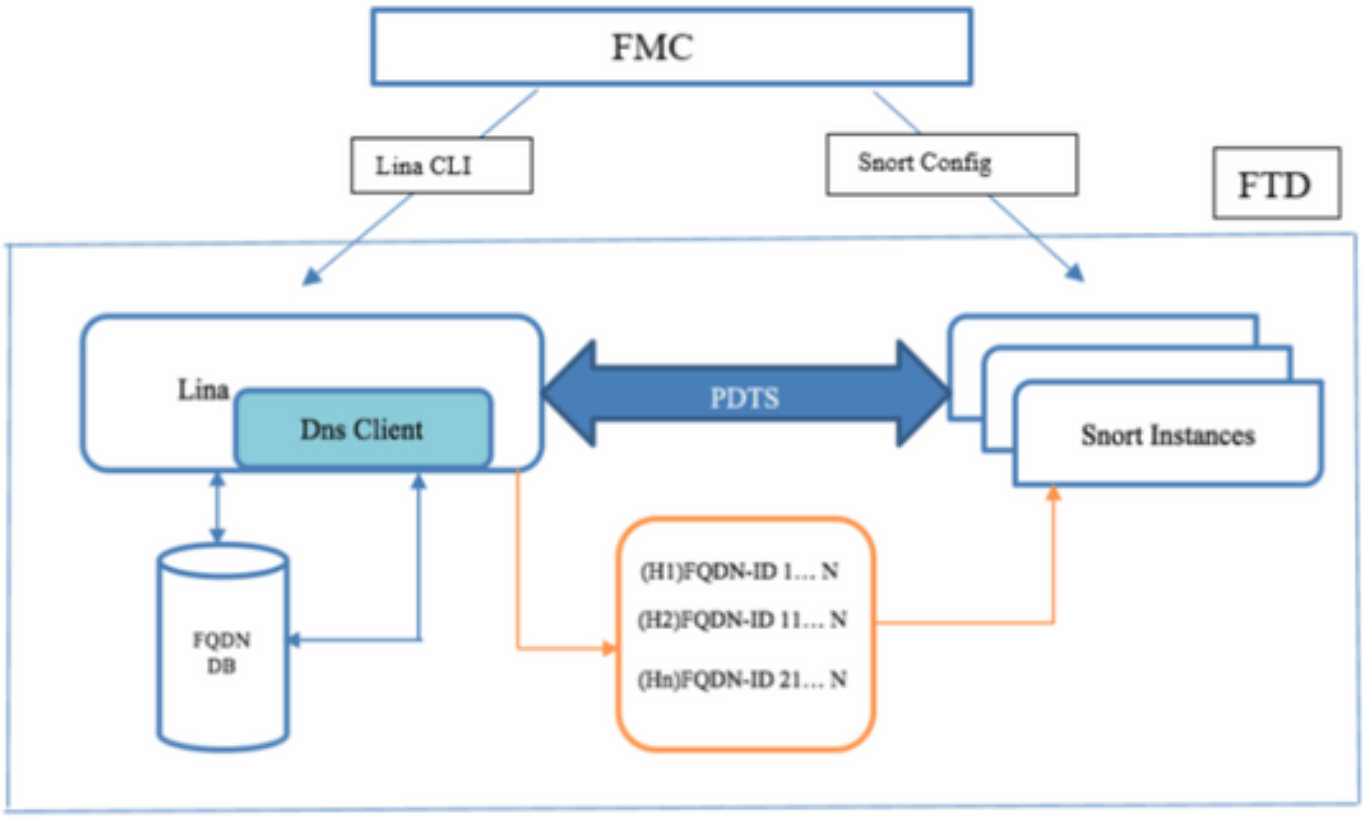


- 此外，如果透過FlexConfig配置DNS對象，則會出現以下警告：



設定

網路圖表

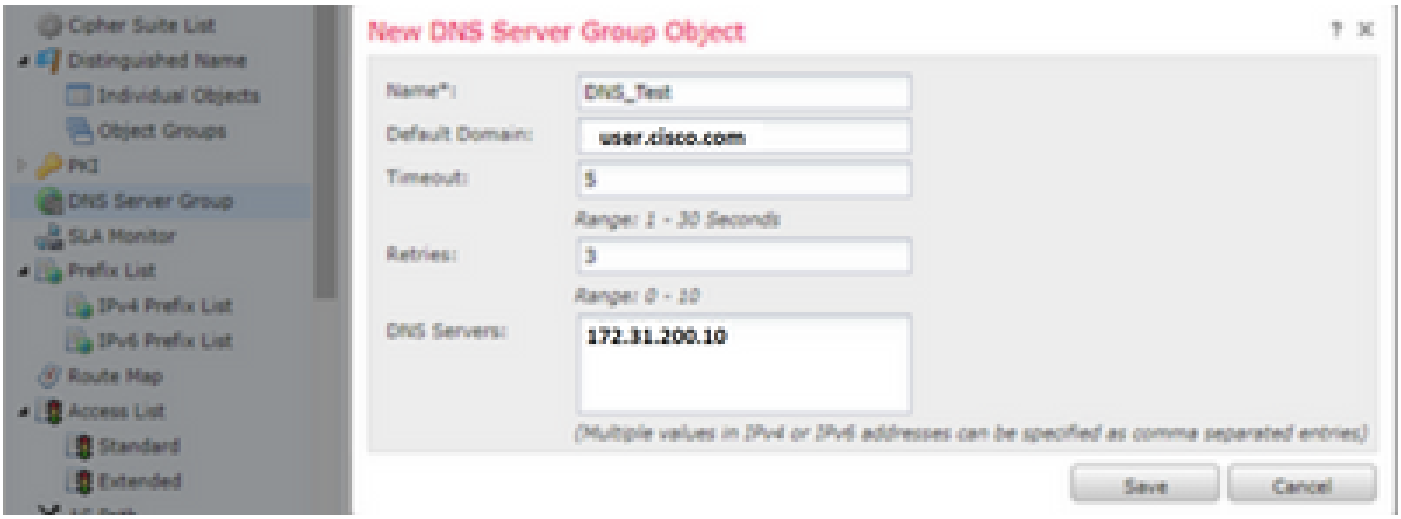


架構-要點

- DNS解析（DNS到IP）發生在LINA中
- LINA在其資料庫中儲存對映
- 根據每個連線，此對映從LINA傳送到snort
- FQDN解析獨立於高可用性或群集配置

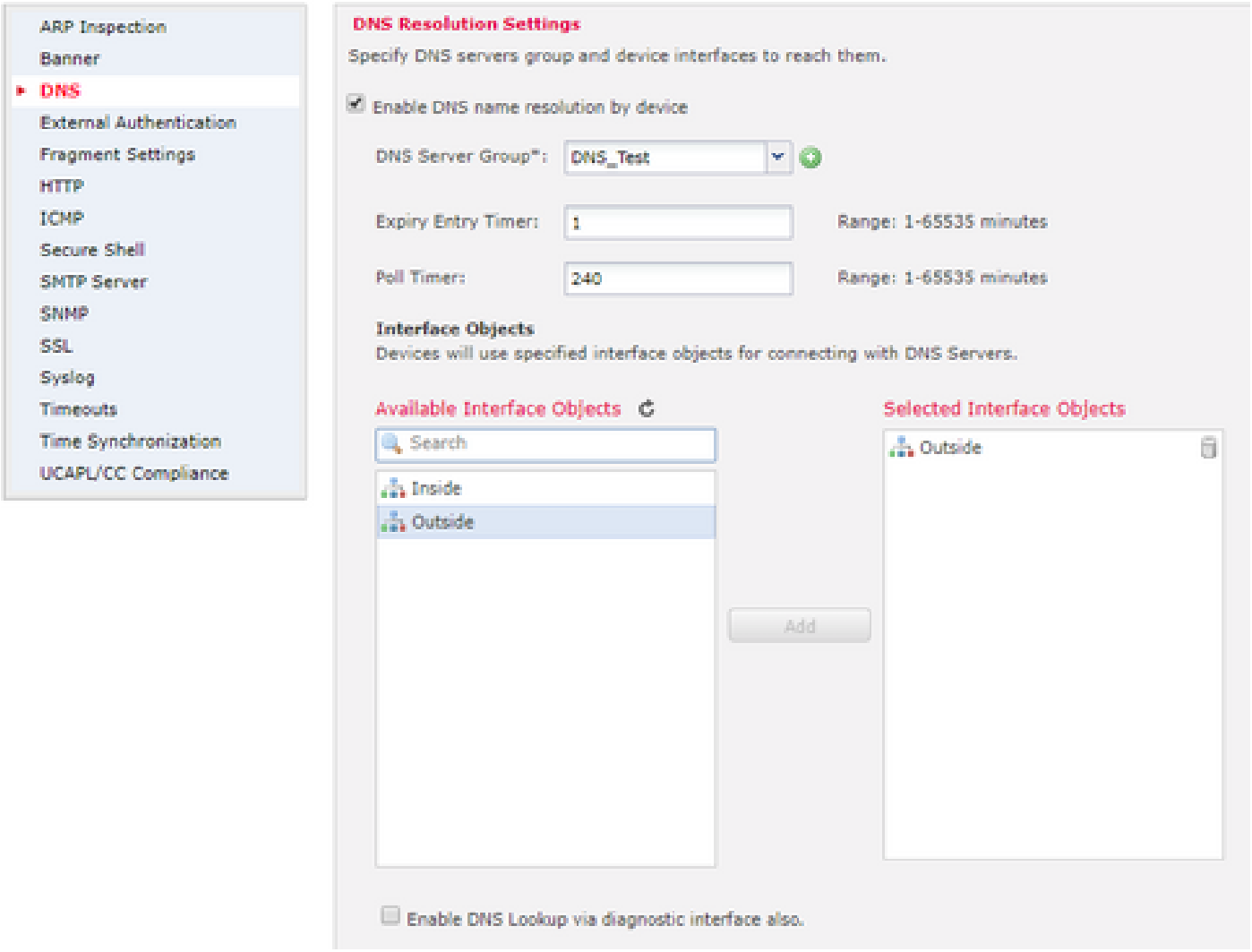
設定步驟

步驟 1.配置「DNS伺服器組對象」



- DNS伺服器組名稱不能超過63個字元
- 在多域部署中，對象名稱在域層次結構中必須是唯一的。系統可以辨識與您目前網域中無法檢視之物件名稱的衝突
- 預設域（可選）用於附加到非完全限定的主機名
- 預設的「重試」和「逾時」值會預先填入。
    - Retries -當系統未收到響應時，重試DNS伺服器清單的次數（從0到10）。預設值為2。
    - Timeout -另一個伺服器嘗試訪問下一個DNS伺服器之前經過的秒數（從1到30）。預設值為2秒。每次系統重試伺服器清單時，此逾時就會加倍。
- 輸入要加入此組的DNS伺服器。可以是逗號分隔值的IPv4或IPv6格式
- DNS伺服器組用於解析介面對象或平台設定中配置的對象
- 支援REST API for DNS Server Group object CRUD

步驟 2.配置DNS（平台設定）



- （可選）修改到期條目計時器和輪詢計時器值（以分鐘為單位）：

expiry entry timer選項指定在解析的FQDN的生存時間(TTL)過期後，從DNS查詢表中刪除其IP地址的時間限制。刪除條目需要重新編譯表，因此頻繁刪除會增加裝置上的進程負載。此設定實際上會擴充TTL。

輪詢計時器選項指定時間限制，超過此時間後，裝置將查詢DNS伺服器以解析網路對象組中定義的FQDN。輪詢計時器已過期或解析的IP條目的TTL已過期時（以先出現者為準），會定期解析FQDN。

- （可選）從可用清單中選擇所需的介面對象，並將其增加到「所選介面對象」清單中，並確保可透過所選介面訪問DNS伺服器：

對於Firepower威脅防禦6.3.0裝置，如果未選擇任何介面，並且停用診斷介面進行DNS查詢，則DNS解析將透過包括診斷介面的任何介面進行（應用命令dnsdomain-lookup any）。

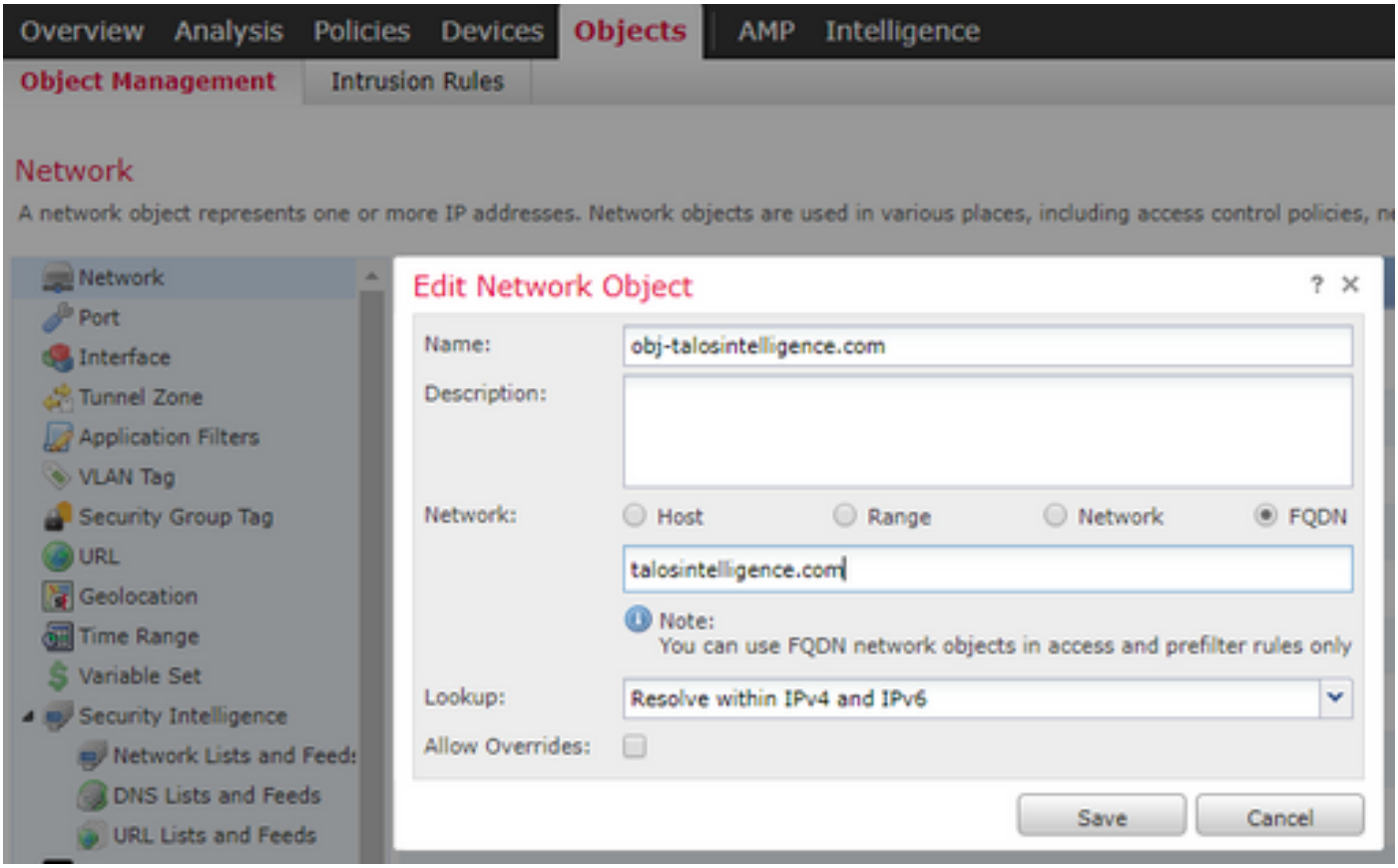
如果您未指定任何介面，且未在診斷介面上啟用DNS查閱，FTD會使用資料路由表來決定介面。如果沒有匹配項，則使用管理路由表。

- （可選）選中Enable DNS Lookup via the diagnostic interface also覈取方塊

如果啟用，Firepower威脅防禦會同時使用選定的資料介面和診斷介面進行DNS解析。請務必在Devices > Device Management > edit device > Interfaces頁面上配置診斷介面的IP地址。

步驟 3. 配置對象網路FQDN

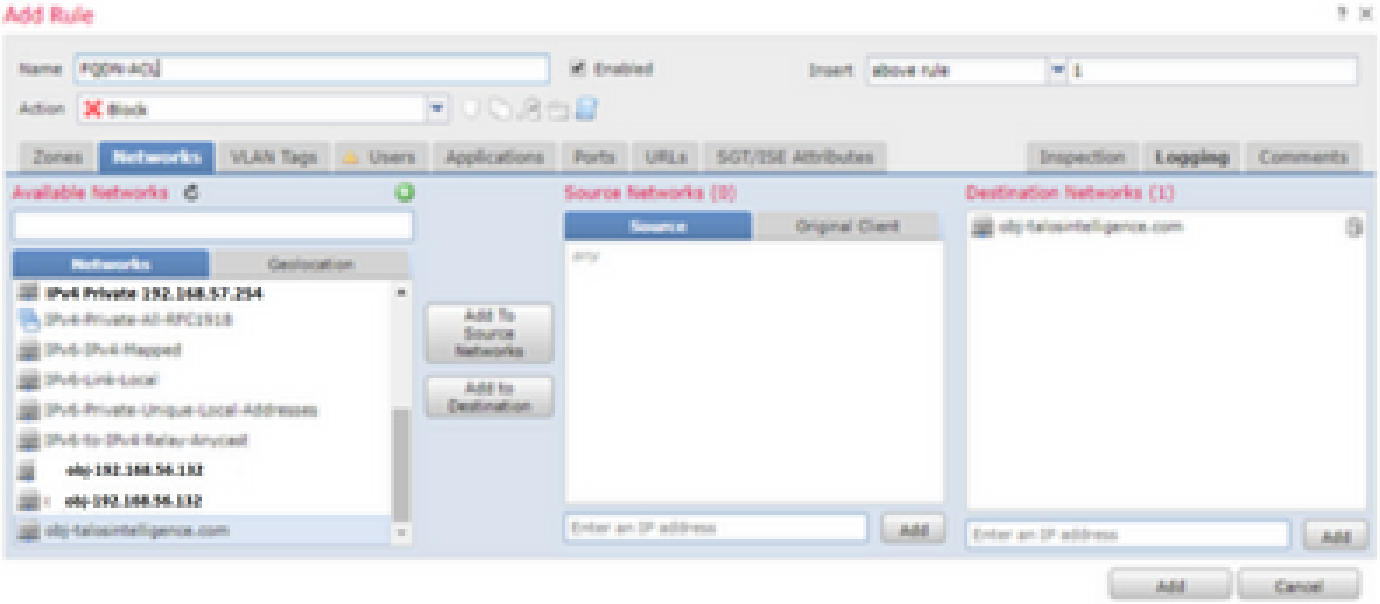
導航到「對象」>「對象管理」，在網路對象中指定選擇FQDN選項。

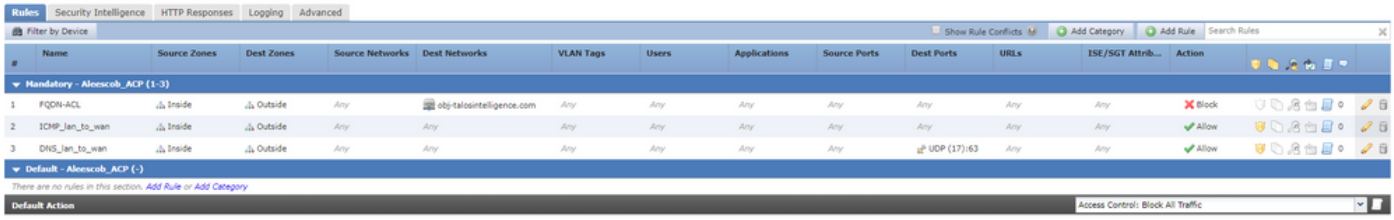


- 使用者建立FQDN對象時生成32位唯一ID
- 此ID從FMC推送到LINA和Snort
- 在LINA中，此ID與物件關聯
- 在snort中，此ID與包含該對象的訪問控制規則相關聯

步驟 4.建立存取控制規則

使用以前的FQDN對象建立規則並部署策略：





注意：在訪問控制策略中部署FQDN對象時，將發生FQDN解析的第一個例項

驗證

使用本節內容，確認您的組態是否正常運作。

- 這是部署FQDN之前的FTD初始組態：

```
aleescob# show run dns
DNS server-group DefaultDNS
```

- 這是FQDN部署後的配置：

```
aleescob# show run dns
dns domain-lookup wan_1557
DNS server-group DNS_Test
    retries 3
    timeout 5
    name-server 172.31.200.100
    domain-name aleescob.cisco.com
DNS server-group DefaultDNS
dns-group DNS_Test
```

- 以下是FQDN對象在LINA中的外觀：

```
object network obj-talosintelligence.com
 fqdn talosintelligence.com id 268434436
```

- 如果已部署，則FQDN訪問清單在LINA中的外觀如下：

```
access-list CSM_FW_ACL_ remark rule-id 268434437: ACCESS POLICY: Aleescob_ACP - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434437: L4 RULE: FQDN-ACL
access-list CSM_FW_ACL_ advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintelligence.co
```

- 以下是Snort (ngfw.rules)中的外觀：

```
# Start of AC rule.
268434437 deny 1 any  any 2 any  any any any  (log dcforward flowstart) (dstfqdn 268434436)
# End rule 268434437
```

注意：在此案例中，由於FQDN物件用於目的地，因此會列為dstfqdn。

- 如果檢查show dns和show fqdn命令，您可以注意到該功能已開始解析tallosintelligence的IP：

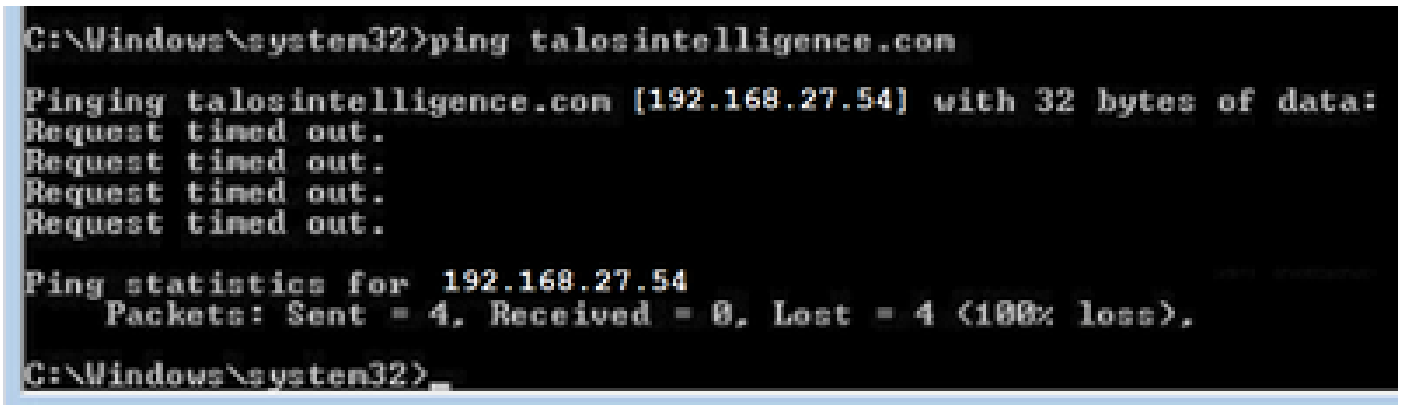
```
aleescob# show dns
Name: talosintelligence.com
  Address: 2001:DB8::6810:1b36                          TTL 00:05:43
  Address: 2001:DB8::6810:1c36                          TTL 00:05:43
  Address: 2001:DB8::6810:1d36                          TTL 00:05:43
  Address: 2001:DB8::6810:1a36                          TTL 00:05:43
  Address: 2001:DB8::6810:1936                          TTL 00:05:43
  Address: 192.168.27.54                                  TTL 00:05:43
```

```
  Address: 192.168.29.54                                  TTL 00:05:43
  Address: 192.168.28.54                                  TTL 00:05:43
  Address: 192.168.26.54                                  TTL 00:05:43
  Address: 192.168.25.54                                  TTL 00:05:43


aleescob# show fqdn
FQDN IP Table:
ip = 2001:DB8::6810:1b36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1c36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1d36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1a36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1936, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.27.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.29.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.28.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.26.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.25.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

FQDN ID Detail:
FQDN-ID = 268434436, object = obj-talosintelligence.com, domain = talosintelligence.com
        ip = 2001:DB8::6810:1b36, 2001:DB8::6810:1c36, 2001:DB8::6810:1d36, 2001:DB8::6810:1a36, 2001:D
```

- 如果您在LINA中勾選show access-list，就可能會注意到每個解析度和命中次數的展開專案：

```
firepower# show access-list
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintel
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 fqdn talosintelligenc
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.27.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.29.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.28.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.26.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.25.54 (t
```

- 如圖所示，對talosintelligence.com執行ping操作失敗，因為訪問清單中的FQDN存在匹配。由於FTD封鎖了ICMP封包，DNS解析已運作。



- 來自LINA的先前傳送的ICMP資料包的命中計數：

```
access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintelli
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 fqdn talosintelligenc
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.27.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.29.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.28.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.26.54 (t
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.25.54 (t
```

- 在入口介面中捕獲和顯示ICMP請求並將其丟棄：

aleescob# show cap in 13 packets captured 1： 18:03:41.558915 192.168.56.132 > 172.31.200.100 icmp： 192.168.56.132 udp port 59396 unreachable 2： 18:04:12.322126 192.168.56.132 > 172.31.4.161 icmp： echo request 3 8:04:12.479162 172.31.4.161 > 192.168.56.132 icmp：回應回覆4： 18:04:13.309966 192.168.56.132 > 172.31.4.161 icmp：回應請求5： 18:04:13.462149 172.31.4.161 > 192.168.5 6.132 icmp：回應應答6： 18:04:14.308425 192.168.56.132 > 172.31.4.161 icmp：回應請求7： 18:04:14.475424 172.31.4.161> 192.168.56.132 icmp：回應應答8： 18:04:15.306823 192.168.566.5 32 > 172.31.4.161 icmp：回應請求9： 18:04:15.463339 172.31.4.161 > 192.168.56.132 icmp：回應應答10： 18:04:25.713662 192.168.56.132 > 192.168.27.54 icmp：回應請求1： 18:04:3 .704232 192.168.56.132 > 192.168.27.54 icmp：回應請求12:18:04:35.711480 192.168.56.132 > 192 2.168.27.54 icmp：回應請求13:18:04:40.707528 192.168.56.132 > 192.168.27.54 icmp：回應請求aleescob# sho cap asp | 在192.168.27.54 162： 18:04:25.713799 192.168.56.132 > 192.168.27.54 icmp：回應請求165： 18:04:30.704355 192.168.56.132 > 192.168.27.54 icmp：回應請求168： 18:18:0 4:35.711556 192.168.56.132 > 192.168.27.54 icmp：回應請求176：

18:04:40.707589 192.168.56.132 > 192.168.27.54 icmp：回應請求

- 以下是trace查詢其中一個ICMP資料包的方式：

```
aleescob# sho cap in packet-number 10 trace

13 packets captured

  10: 18:04:25.713662       192.168.56.132 > 192.168.27.54 icmp: echo request
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.57.254 using egress ifc  wan_1557

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintelligence.co
access-list CSM_FW_ACL_ remark rule-id 268434437: ACCESS POLICY: Aleescob_ACP - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434437: L4 RULE: FQDN-ACL
Additional Information:

Result:
input-interface: lan_v1556
input-status: up
input-line-status: up
output-interface: wan_1557
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

- 如果訪問控制規則的操作為Allow，則這是系統支援firewall-engine-debug的輸出示例

```
> system support firewall-engine-debug

Please specify an IP protocol: icmp
Please specify a client IP address: 192.168.56.132
Please specify a server IP address:
Monitoring firewall engine debug messages

192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 new firewall session
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 DAQ returned DST FQDN ID: 268434436
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 Starting with minimum 2, 'FQDN-ACL', and SrcZone first wi
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 Match found for FQDN id: 268434436
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 match rule order 2, 'FQDN-ACL', action Allow
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 MidRecovery data sent for rule id: 268434437,rule_action:
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 allow action
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 deleting firewall session
```

- 將FQDN部署為預過濾器(Fastpath)的一部分時，它在ngfw.rules中的外觀如下：

```
iab_mode Off
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268434439 fastpath any any  any any any  any any any  (log dcforward both) (tunnel -1)
268434438 allow any any  1025-65535 any any  3544 any 17  (tunnel -1)
268434438 allow any any  3544 any any  1025-65535 any 17  (tunnel -1)
268434438 allow any any  any any any  any any 47  (tunnel -1)
268434438 allow any any  any any any  any any 41  (tunnel -1)
268434438 allow any any  any any any  any any 4  (tunnel -1)
# End of tunnel and priority rules.
```

- 從含有追蹤封包的LINA角度來看：

```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip any object obj-talosintelligence.com rule-id 268434439 event-
access-list CSM_FW_ACL_ remark rule-id 268434439: PREFILTER POLICY: Prefilter-1
access-list CSM_FW_ACL_ remark rule-id 268434439: RULE: FQDN_Prefilter
Additional Information:
```

疑難排解

1. 從FMC配置

- 驗證是否正確配置了策略和DNS伺服器設定
- 驗證部署是否成功

2. 在FTD上部署檢查

- 運行show dns和show access-list以檢視是否已解析FQDN和AC規則是否已展開
- 運行show run object network，記下與對象關聯的ID（例如，X代表源）
- 運行show fqdn id X以檢查FQDN是否已正確解析為源IP
- 驗證ngfw.rules檔案是否具有以FQDN ID X作為源的AC規則
- 運行系統支援firewall-engine-debug並檢查Snort裁決

收集FMC故障排除檔案

所需的所有日誌都從FMC故障排除中收集。要從FMC收集所有重要日誌，請從FMC GUI運行故障排除。否則，在FMC Linux提示符下，運行sf_troubleshoot.pl。如果您發現問題，請向思科技術支援中心(TAC)提交FMC故障排除和報告。

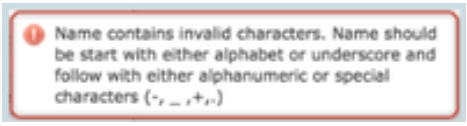
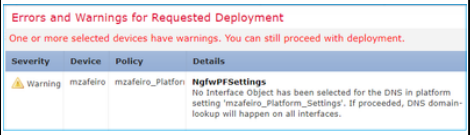
FMC日誌

記錄檔名稱/位置	目的
/opt/CSCOpx/MDC/log/operation/vmssharedsvcs.log	所有API呼叫
/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log	所有API呼叫
/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log	CLI生成日誌
/opt/CSCOpx/MDC/tomcat/logs/stdout.log	Tomcat日誌
/var/log/mojo.log	Mojo日誌
/var/log/CSMAgent.log	CSM和DC之間的REST呼叫

/var/log/action_queue.log	DC的操作隊列日誌

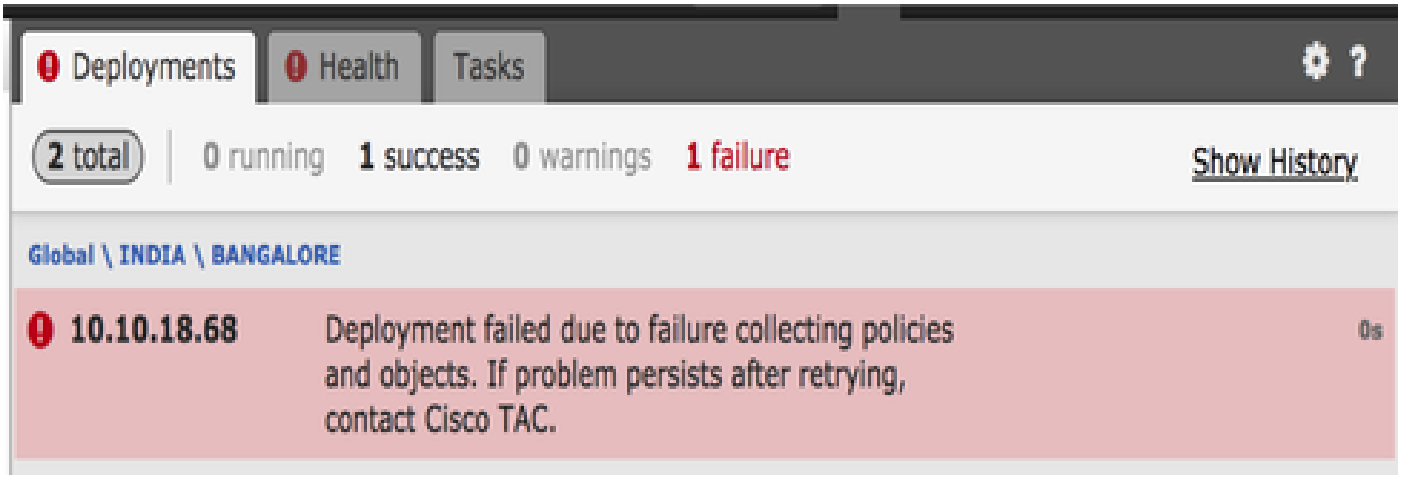
常見問題/錯誤消息

以下是FQDN和DNS伺服器組對象的UI中顯示的錯誤/警告以及DNS設定：

錯誤/警告	案例	說明
 名稱包含無效字元。名稱必須以字母或下劃線開頭，後面必須是字母數字或特殊字元。(-、_、+、.)	使用者 配置錯誤名稱	將允許的資訊通知使用者 字元和最大範圍。
 無效的預設網域值	使用者配置錯誤的域名	將允許的字元和最大範圍通知使用者。
 在平台設定「mzafeiro_Platform_Settings」中未為DNS選擇介面對象。如果繼續，DNS域名查詢將很快在所有介面上發生	使用者未選取任何介面以進行網域查閱 對於6.3後裝置	系統會警告使用者，DNS 即將應用伺服器組CLI 到所有介面。
 在平台設定「mzafeiro_Platform_Settings」中未為DNS選擇介面對象。如果繼續，則不會立即應用具有「DNS」的DNS伺服器組	使用者未選取任何介面以進行網域查閱 對於6.2.3裝置	警告使用者 DNS 伺服器群組CLI不是 已生成。

部署失敗

在除AC策略/預過濾器策略以外的策略中使用FQDN時，可能會發生此錯誤並顯示在FMC UI中：



建議的故障排除步驟

1)打開日誌檔案：/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

2)檢查驗證訊息，類似於：

「配置的網路無效。在裝置[裝置名稱]上配置的網路[NetworksContainingFQDN]是指FQDN」

3)建議的行動：

驗證是否已使用包含FQDN對象的FQDN或組配置了一個或多個下面提及的策略，並在刪除這些對象後重新嘗試部署這些策略。

a)身份策略

b)包含應用於AC策略的FQDN的變數集

沒有啟用的FQDN

系統可以透過FTD CLI顯示下一個專案：

> show dns INFO：沒有啟用的FQDN

在應用具有已定義fqdn的對象之前，不會啟用DNS。套用物件後，就會解決這個問題。

問答

問：使用FQDN的Packet Tracer是否是對問題進行故障排除的有效測試？
答：是的，您可以將fqdn選項與Packet Tracer一起使用。

問：FQDN規則多久更新一次伺服器的IP地址？
答：這取決於DNS響應的TTL值。一旦TTL值過期，將使用新的DNS查詢再次解析FQDN。這還取決於DNS伺服器配置中定義的Poll Timer屬性。當輪詢DNS計時器過期或解析的IP條目的TTL過期時（以先到者為準），會定期解析FQDN規則。

問：這對輪詢DNS是否有效？
答：輪詢DNS可順利運作，因為這項功能可在使用DNS使用者端的FMC/FTD上運作，且輪詢DNS組態位於DNS伺服器端。

問：TTL DNS值是否有限制？
答：如果DNS回應具有0 TTL，則FTD裝置會增加60秒。在這種情況下，TTL值最小60秒。

問：因此預設情況下，FTD會保留預設值60秒？
答：使用者始終可以在DNS伺服器上使用過期條目計時器設定覆蓋TTL。

問：它如何與任播DNS響應互動操作？例如，DNS伺服器可以根據地理位置為請求者提供不同的IP地址。能否為FQDN請求所有IP地址？像Unix上的dig指令嗎？
答：是的，如果FQDN能夠解析多個IP地址，則所有地址都將推送到裝置，AC規則將相應地展開。

問：是否計畫包含預覽選項，以顯示任何部署更改之前已推送的命令？
答：這是透過Flex配置提供的預覽配置選項的一部分。預覽已經存在，但在Flex Config策略中隱藏它。我們計畫將其移出，使之成為通用部件。

問：FTD上的哪個介面可用於執行DNS查詢？
答：可以配置。如果沒有設定任何介面，則會啟用FTD上所有命名介面進行DNS查閱。

問：即使對具有相同FQDN對象的所有託管的NGFW應用相同的訪問策略，每個託管的NGFW是否也分別執行自己的DNS解析和FQDN IP轉換？
答：是。

問：能否清除FQDN ACL的DNS快取以進行故障排除？
答：是的，您可以在裝置上執行clear dns和clear dns-hosts cache命令。

問：FQDN解析到底何時觸發？
答：FQDN解析在AC策略中部署FQDN對象時發生。

問：是否只能清除單個站點的快取？

答：是。如果您知道域名或IP地址，則可以將其清除，但是根據ACL的角度，沒有這樣的命令。例如，發出clear dns host agni.tejas.com命令可以用關鍵字host按主機清除主機上的快取，如dns host agni.tejas.com中所述。

問：是否可以使用萬用字元，例如*.microsoft.com？
A：否。FQDN必須以數字或字母開始和結束。只有字母、數字和連字型大小可以做為內部字元。

問：名稱解析是在AC編譯時執行，而不是在第一次或後續請求時執行？如果遇到低TTL（小於AC編譯時間、快速流量或其他因素），是否可能會丟失某些IP地址？
答：部署AC策略後立即進行名稱解析。根據TTL時間到期，續訂將繼續。

問：是否計畫處理Microsoft Office 365雲IP地址(XML)清單？
答：目前不支援此功能。

問：SSL策略中是否提供FQDN？
答：目前不需要（軟體版本6.3.0）。FQDN對象僅在源網路和目標網路中僅支援AC策略。

問：是否有任何歷史日誌可以提供已解析FQDN的相關資訊？例如，LINA系統日誌。
答：要排除FQDN到特定目標的故障，可以使用system support trace命令。跟蹤顯示資料包的FQDN ID。您可以比較ID以進行疑難排解。您還可以啟用Syslog消息746015，746016跟蹤FQDN dns解析活動。

問：裝置是否使用解析的IP在連線表中記錄FQDN？
答：要排除FQDN到特定目標的故障，可以使用system support trace命令，其中，跟蹤顯示資料包的FQDN ID。您可以比較ID以進行疑難排解。計畫將來在FMC上的事件檢視器中使用FQDN日誌。

問：FQDN規則功能有哪些缺點？

答：如果FQDN規則用於經常更改IP地址的目標（例如：TTL到期為零的網際網路伺服器），則此功能無法擴展，工作站最終可能擁有不再與FTD DNS快取匹配的新IP地址。因此，它與ACP規則不匹配。預設情況下，FTD會將DNS回應所收到的TTL到期加上1分鐘，且不能設定為零。在這些情況下，強烈建議使用最適合此使用案例的URL過濾功能。

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）。