# Kunt u FQDN-functies begrijpen bij Firepower Threat Defence (door FMC beheerd)

## Inhoud



## Inleiding

In dit document wordt de configuratie beschreven van de FQDN-functie (vanaf v6.3.0) naar Firepower Management Center (FMC) en Firepower Threat Defence (FTD).

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Management Center

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Cisco Firepower Threat Defense (FTD) Virtual-software waarop versie 6.3.0 wordt uitgevoerd
- Firepower Management Center Virtual (vFMC) waarop versie 6.3.0 wordt uitgevoerd

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Achtergrondinformatie

In dit document wordt de configuratie beschreven van de functie Volledig gekwalificeerde domeinnaam (FQDN) die door softwareversie 6.3.0 is geïntroduceerd in Firepower Management Center (FMC) en Firepower Threat Defence (FTD).

Deze optie is aanwezig in de Cisco adaptieve security applicatie (ASA), maar was niet aanwezig op de eerste softwarereleases van FTD.

Zorg ervoor dat aan deze voorwaarden is voldaan voordat u FQDN-objecten configureert:

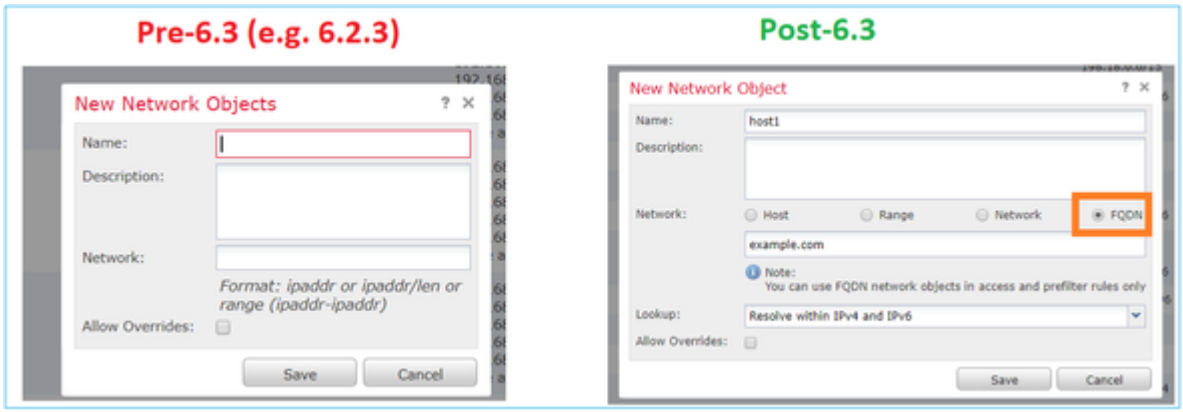
- Het Firepower Management Center moet versie 6.3.0 of hoger uitvoeren. Het kan fysiek of virtueel zijn
- De Firepower Threat Defense moet versie 6.3.0 of hoger uitvoeren. Het kan fysiek of virtueel zijn

## Overzicht van functies

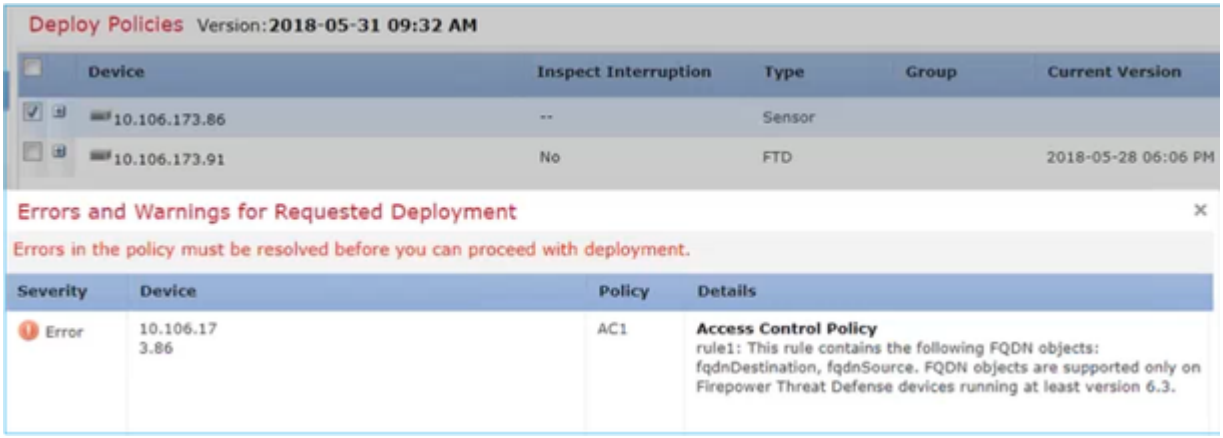
Deze eigenschap lost een FQDN in een IP adres op en gebruikt de laatstgenoemde om verkeer te filteren wanneer van verwijzingen voorzien door een Regel van het Toegangsbeheer of een Prefilterbeleid.

## Wat met pre-6.3?

- FMC en FTD die een versie eerder uitvoeren dan 6.3.0 kunnen FQDN-objecten niet configureren.

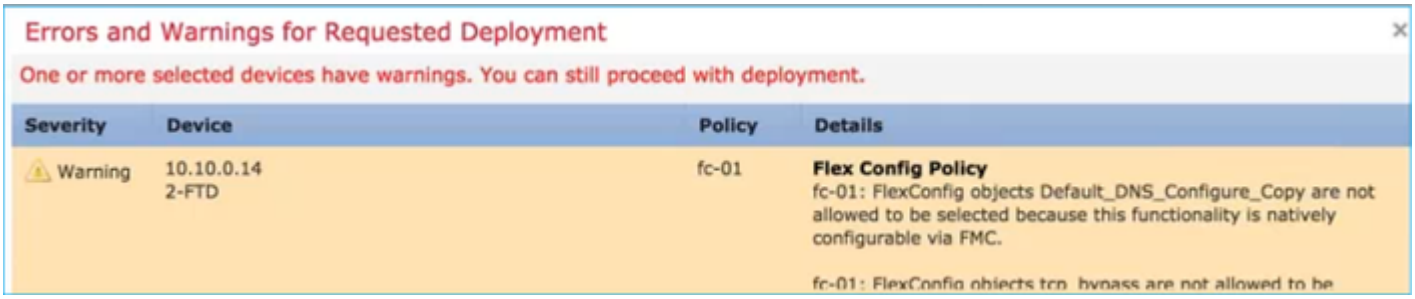



- Indien het FMC versie 6.3 of hoger uitvoert, maar het FTD een versie eerder dan 6.3 uitvoert, toont de invoering van een beleid deze fout:



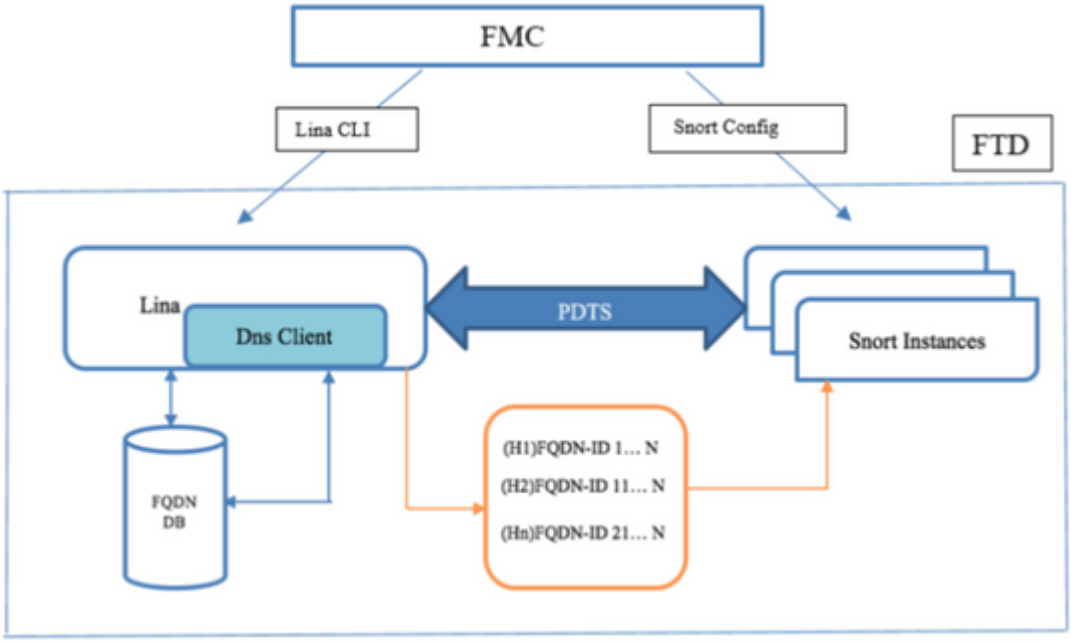

- Als u bovendien via FlexConfig een DNS-object configureert, wordt deze waarschuwing

weergegeven:




# Configureren

## Netwerkdiagram




## Architectuur - Salient points

- DNS-resolutie (DNS naar IP) gebeurt in LINA
- LINA slaat de mapping op in de database
- Deze mapping wordt per verbinding van LINA naar snort verzonden
- De resolutie van FQDN gebeurt onafhankelijk van de configuratie van hoge beschikbaarheid of cluster

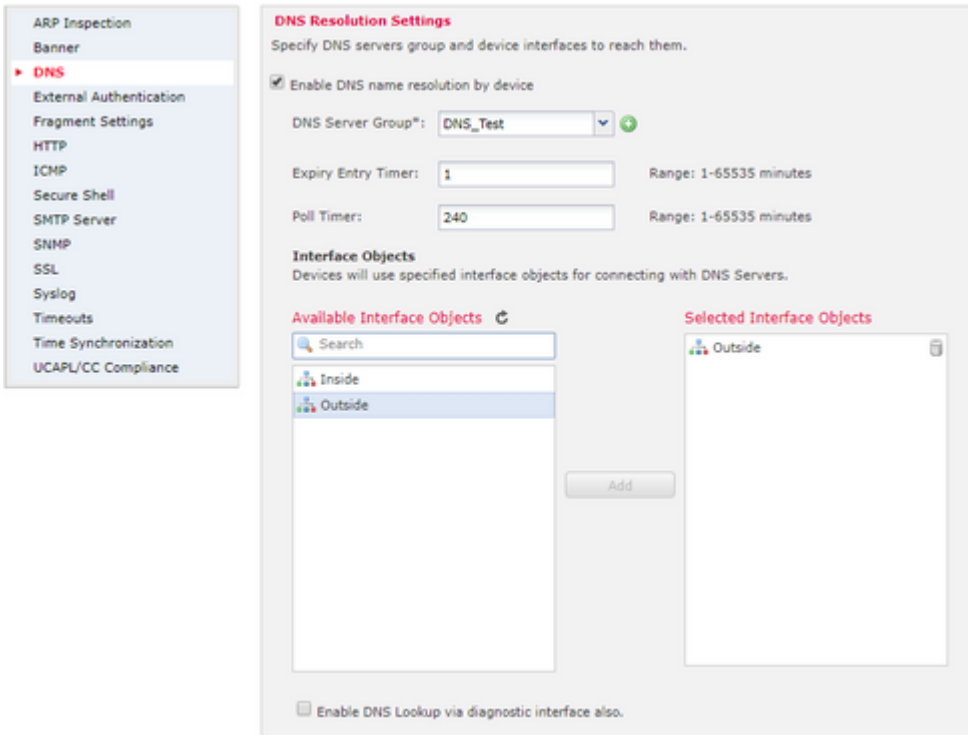
## Configuratiestappen

Stap 1. Het "DNS-servergroepobject" configureren


â€ƒ

- De naam van de DNS-servergroep mag niet langer zijn dan 63 tekens
- In een multidomeinplaatsing, moeten de objecten namen binnen de domeinhiërarchie uniek zijn. Het systeem kan een conflict identificeren met de naam van een object dat u in uw huidige domein niet kunt bekijken
- Het standaard domein (optioneel) wordt gebruikt om aan de hostnamen die niet volledig gekwalificeerd zijn toe te voegen
- De standaard waarden voor opnieuw proberen en time-out worden vooraf ingevuld.
    - Het aantal keren opnieuw proberen - van 0 tot 10 - om de lijst met DNS-servers opnieuw uit te proberen wanneer het systeem geen respons ontvangt. De standaardwaarde is 2.
    - Time-outâ€”Het aantal seconden van 1 tot 30, voordat een andere probeert naar de volgende DNS-server. De standaardinstelling is 2 seconden. Elke keer dat het systeem de lijst met servers opnieuw probeert, verdubbelt deze time-out.
- Voer de DNS-servers in die deel uitmaken van deze groep. U kunt hiervoor een IPv4- of IPv6-indeling gebruiken als waarden met kommascheiding
- De DNS-servergroep wordt gebruikt voor de resolutie met het interfaceobject of de objecten die in Platform-instellingen zijn geconfigureerd
- REST API voor DNS-servergroep object CRUD wordt ondersteund

Stap 2. DNS configureren (platforminstellingen)




- (Optioneel) Wijzig de waarden van de Timer en de timer voor poll in minuten:

De optie van de de ingangstimer van de vervaldatum specificeert de tijdslimiet om het IP adres van een opgelost FQDN uit de DNS raadplegingslijst te verwijderen nadat zijn Time-to-live (TTL) verloopt. Verwijder een ingang vereist dat de lijst opnieuw wordt samengesteld, zodat kunnen de frequente verwijderingen de proceslading op het apparaat verhogen. Deze instelling breidt de TTL vrijwel uit.

De optie poll timer geeft de tijdslimiet aan waarna het apparaat de DNS server vraagt om de FQDN die is gedefinieerd in een netwerk object groep op te lossen. Een FQDN wordt periodiek opgelost of wanneer de opiniepeiltimer is verlopen, of wanneer de TTL van de opgeloste IP-ingang is verlopen, afhankelijk van wat het eerst gebeurt.

- (Optioneel) Selecteer de gewenste interfaceobjecten in de beschikbare lijst en voeg ze toe aan de lijst Geselecteerde interfaceobjecten en controleer of de DNS-server bereikbaar is via de geselecteerde interface(s):

Voor FirePOWER Threat Defense 6.3.0-apparaten geldt dat als er geen interfaces zijn geselecteerd en de diagnostische interface is uitgeschakeld voor DNS-lookup, de DNS-resolutie gebeurt via elke interface die de diagnostische interface bevat (de opdracht dnsdomain-lookup any is van toepassing).

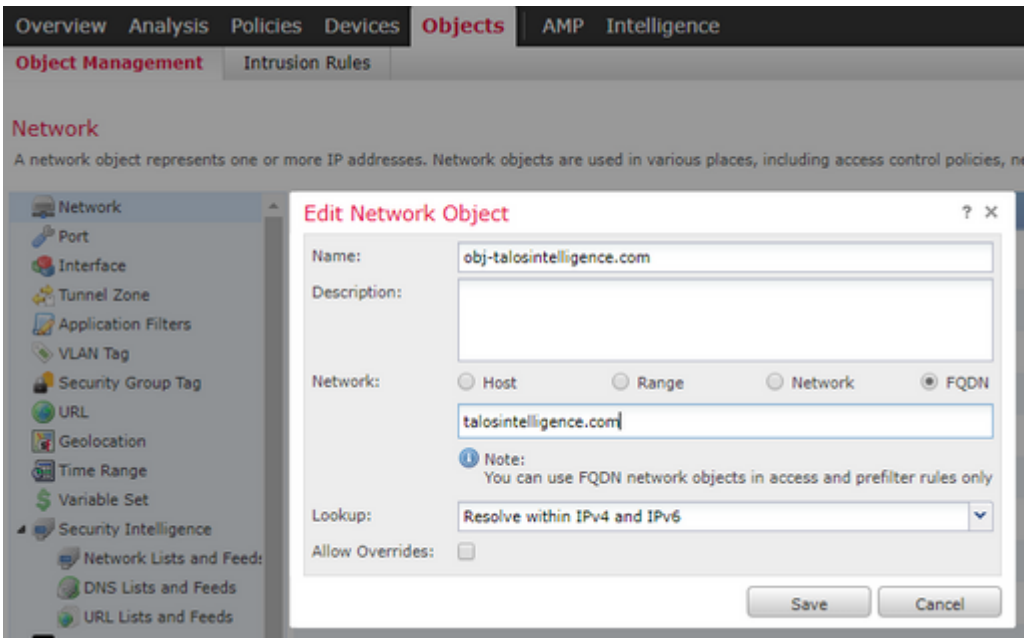
Als u geen interfaces specificeert, en DNS-raadpleging op de diagnostische interface niet inschakelt, gebruikt de FTD de tabel Data Routing om de interface te bepalen. Als er geen overeenkomst is, gebruikt het de Routing Table van het Beheer.

- (Optioneel) Selecteer ook DNS-raadpleging inschakelen via het selectievakje voor diagnostische interface

Indien ingeschakeld, gebruikt Firepower Threat Defence zowel de geselecteerde data-interfaces als de diagnostische interface voor DNS-resoluties. Zorg ervoor dat u een IP-adres configureert voor de diagnostische interface op de pagina Apparaten > Apparaatbeheer > Apparaat bewerken > Interfaces.

Stap 3. Configureer het Objectnetwerk FQDN

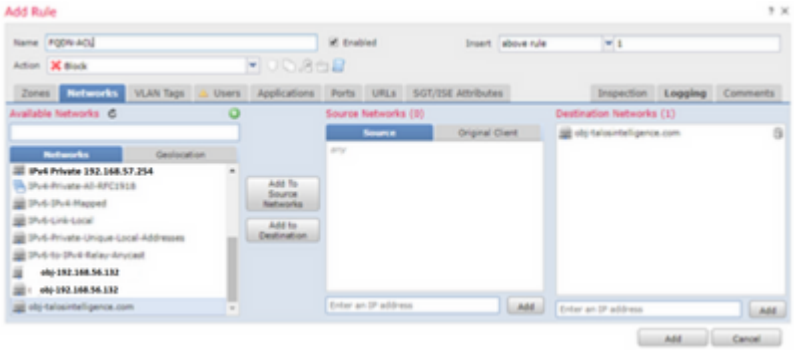
Navigeer naar Objecten > Objectbeheer, binnen een netwerkobject specificeer selecteer de optie FQDN.



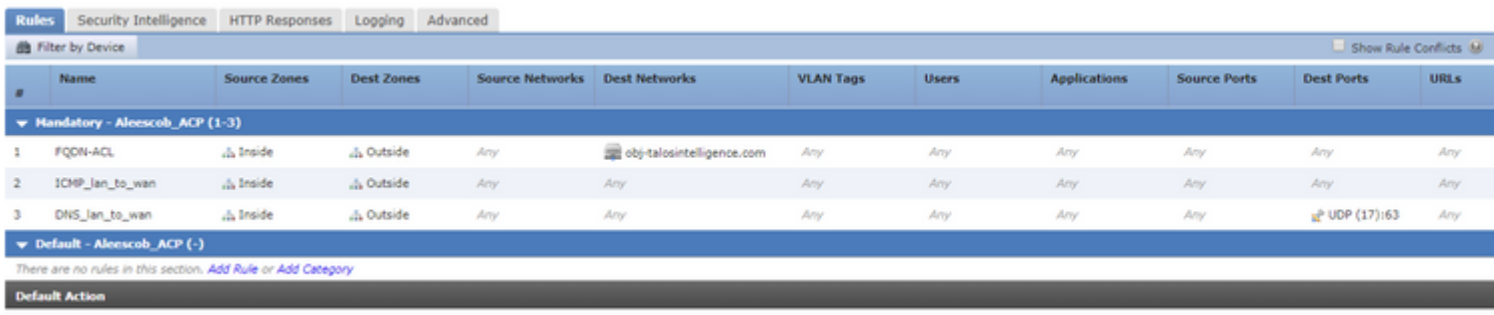

- Een 32-bits unieke ID wordt gegenereerd wanneer de gebruiker een FQDN-object maakt
- Deze ID wordt van FMC naar zowel LINA als Snort gedrukt
- In LINA wordt deze ID geassocieerd met het object
- Kortom, deze ID is gekoppeld aan de toegangscontroleregel die dat object bevat

Stap 4. Een toegangscontroleregel maken

Maak een regel met het vorige FQDN-object en implementeer het beleid:




â€ƒ




Opmerking: De eerste instantie van de FQDN-resolutie vindt plaats wanneer het FQDN-object wordt

geïmplementeerd in een toegangscontrolebeleid

# Verifiëren

Gebruik dit gedeelte om te bevestigen dat uw configuratie correct werkt.

- Dit is de eerste FTD-configuratie voordat FQDN wordt geïmplementeerd:

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

- Dit is de configuratie na FQDN-implementatie:

```
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
```

- Zo ziet het FQDN-object er in LINA uit:

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

- Wanneer het reeds wordt opgesteld, is dit hoe de FQDN toegang-lijst in LINA kijkt:

```
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.com
```

- Zo ziet het eruit in Snort (ngfw.rules):

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

Opmerking: In dit scenario, omdat het FQDN-object is gebruikt voor de bestemming, wordt het vermeld als dstfqdn.

- Als u controleert tonen dns en tonen fqdn bevelen, kunt u opmerken dat de eigenschap is begonnen om IP voor tallosintelligence op te lossen:

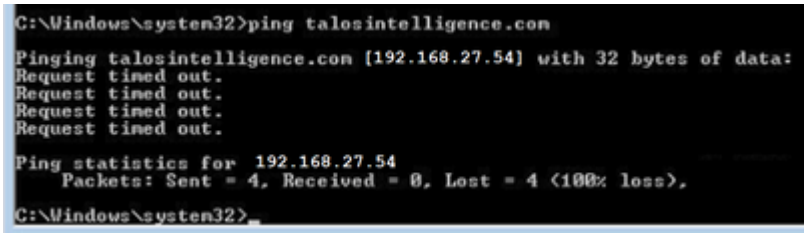
```
aleescob# show dns
Name: talosintelligence.com
  Address: 2001:DB8::6810:1b36                          TTL 00:05:43
  Address: 2001:DB8::6810:1c36                          TTL 00:05:43
  Address: 2001:DB8::6810:1d36                          TTL 00:05:43
  Address: 2001:DB8::6810:1a36            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

- Als u in LINA de toegangslijst voor tonen controleert, kunt u de uitgebreide ingangen voor elke

resolutie en klaptellingen opmerken:

```
firepower# show access-list
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintell
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 fqdn talosintelligence
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1b
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1c
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1d
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1a
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:19
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.27.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.29.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.28.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.26.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.25.54 (ta
```

- Zoals in de afbeelding wordt getoond, mislukt een ping naar talosintelligence.com omdat er een overeenkomst voor FQDN in de toegangslijst is. De DNS-resolutie werkt sinds het ICMP-pakket wordt geblokkeerd door de FTD.




â€ƒ

- Hit telt van LINA voor de eerder verzonden ICMP-pakketten:

```
access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintellig
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 fqdn talosintelligence
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1b
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1c
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1d
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1a
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:19
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.27.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.29.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.28.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.26.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.25.54 (ta
```

- ICMP-verzoeken worden opgenomen en weergegeven in de toegangsinterface:

aleescob# tonen een dop in 13 pakjes opgenomen 1: 18:03:41.558915 192.168.56.132 > 172.31.200.100 ICMP: 192.168.56.132 udp poort 59396 onbereikbaar 2: 18:04:12.322126 192.168.56.132 > 172.32 18:04:12.479162 172.31.4.161 > 192.168.56.132 icmp: echo antwoord 4: 18:04:13.309966 192.168.56.132 > 172.31.4.161 icmp: echo verzoek 5: 18:0462149:13.13 Icmp: echo-antwoord 6: 18:04:14.308425 192.168.561 > 172.31.4.161 Icmp: echo-verzoek 7: 18:04:14.475424 172.31.4.161> 192.168 26.132 icmp:

echo antwoord 8: 18:04:15.306823 192.168.56.132 > 172.31.4.161 icmp: echo verzoek 9: 18:04:15.463339 172.31.4.161 > 192.168.56.132 713662 192.168.56.132 > 192.168.27.54 icmp: echo verzoek 11: 18:04:30.704232 192.168.56.132 > 192.168.27.54 icmp: echo verzoek 12: 18:04:35.711480 192.168.56.13 > 192.168.27.54 icmp: echo verzoek 13: 18:04:40.707528 192.168.56.132 > 192.168.27.54 icmp: echo verzoek aleescob# sho cap asp | in 192.168.27.54:162:18:04:25.713799 192.168.56.132 > 192.168.27.54 icmp: echoverzoek 165:18:04:30.704355 192.168.56.132 > 192.168.27.54 echo verzoek 168: 18:04:35.711556 192.168.56.132 > 192.168.27.54 icmp: echo verzoek 176: 18:04:40.707589 192.168.56.132 > 192.168.27.54 icmp: echo verzoek

- Dit is hoe het spoor naar één van deze pakketten ICMP zoekt:

```
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.com
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
```

- Als de actie voor de toegangscontroleregel Toestaan is, is dit een voorbeeld van de output van systeem steun firewall-motor-debug

```
> 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 wit
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:2
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
```

- Wanneer de FQDN wordt geïmplementeerd als deel van een voorfilter (Fastpath), ziet dit er zo uit in ngfw.rules:

```
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.
```

- Vanuit het oogpunt van LINA met een overgetrokken pakket:

```
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-l
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:
```

# Problemen oplossen

1. Configuratie vanaf VCC

- Controleer of het beleid en de DNS-serverinstellingen goed zijn geconfigureerd
- Controleer of de implementatie succesvol is

2. Controle op FTD implementeren

- Laat show dns zien en toon access-list om te zien of FQDN is opgelost en AC regels zijn uitgebreid
- Uitvoeren laat het netwerk van uitvoerobjecten zien en noteer de id die aan het object is gekoppeld (zeg X voor bron)
- Run toont fqdn id X om te controleren of de FQDN is opgelost in de juiste IP-bronmodus
- Controleer of het bestand ngfw.rules AC-regel heeft met FQDN-id X als bron
- Start systeemondersteuning firewall-engine-debug en controleer het korte oordeel

## Verzamel FMC-bestanden voor probleemoplossing

Alle benodigde logbestanden worden verzameld via een probleemoplossing van het VCC. Om alle belangrijke logbestanden van het VCC te verzamelen, voert u een probleemoplossing uit in de VCC GUI. Anders vanuit een FMC Linux prompt, run sf_troubleshoot.pl. Als u een probleem vindt, dient u een FMC-probleemoplossing met uw rapport in bij het Cisco Technical Assistance Center (TAC).

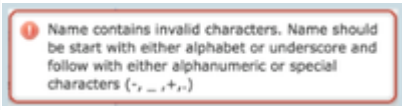
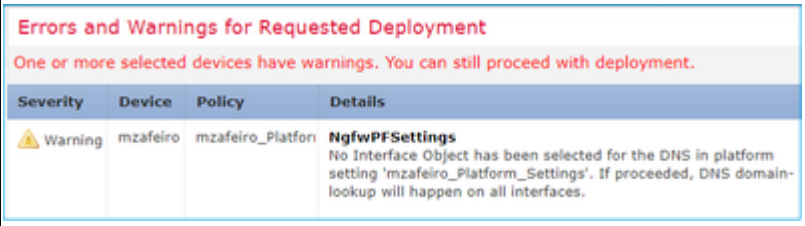
VCC-logbestanden

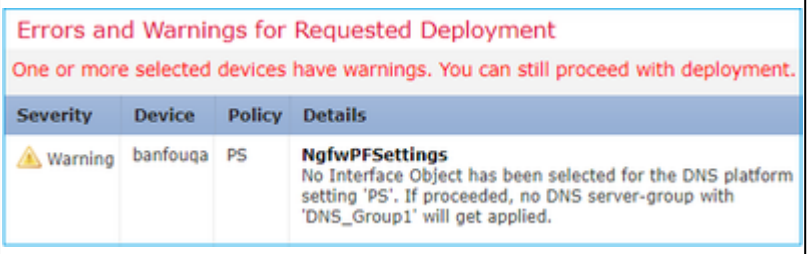
| Naam/locatie logbestand | Doel |
|---|---|
| `/opt/CSCOpx/MDC/log/operation/vmssharedsvcs.log` | Alle API-oproepen |
| `/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log` | Alle API-oproepen |
| `/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log` | CLI-generatielogboeken |
| `/opt/CSCOpx/MDC/tomcat/logs/stdout.log` | Tomcat Logs |
| `/var/log/mojo.log` | Mojo Logs |

| | |
|---|---|
| `/var/log/CSMAgent.log` | RUST-oproepen tussen CSM en DC |
| `/var/log/action_queue.log` | Logboek voor DC-actieruimte |

## Veelvoorkomende problemen/foutmeldingen

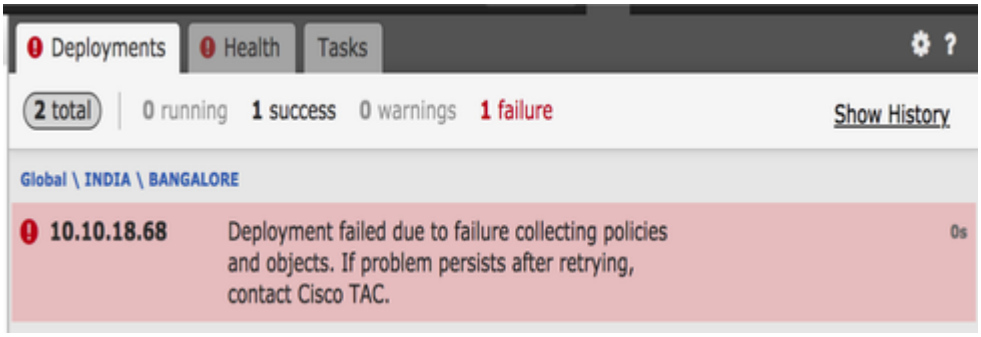
Dit zijn de fouten/waarschuwingen die in UI voor FQDN- en DNS-servergroepobject en DNS-instellingen worden getoond:

| Fout/waarschuwing | scenario | Beschrijving |
|---|---|---|
|  <br>De naam bevat ongeldige tekens. De namen moeten met of alfabet of onderstreepteken en dan of alfanumerieke of speciale karakters na beginnen. (-,_,+,.) | Gebruiker<br><br>vormt verkeerde naam | De gebruiker wordt geïnformeerd over het toegestane<br><br>tekens en maximumbereik. |
|  <br>Ongeldige standaardwaarde voor domein | Gebruiker configureert verkeerde domeinnaam | De gebruiker wordt op de hoogte gesteld van de toegestane tekens en het maximale bereik. |
|  <br>Er is geen interface-object geselecteerd voor de DNS in platforminstelling â€˜mzafeiro_Platform_Settingsâ€™. Indien dit wordt doorgezet, zal DNS-domeinraadpleging binnenkort op alle interfaces plaatsvinden | De gebruiker selecteert geen interface voor domeinraadpleging<br><br>Voor een post-6.3-apparaat | De gebruiker is gewaarschuwd dat de DNS<br><br>server groep CLI wordt binnenkort toegepast<br><br>naar alle interfaces. |

| | | |
|---|---|---|
|  <br>Er is geen interface-object geselecteerd voor de DNS in platforminstelling â€˜mzafeiro_Platform_Settingsâ€™. Als dit wordt gedaan, wordt binnenkort geen DNS-servergroep met DNS toegepast | De gebruiker selecteert geen interface voor domeinraadpleging<br><br>Voor een 6.2.3-inrichting | Gebruiker is gewaarschuwd<br><br>dat de DNS<br><br>CLI van servergroep is niet<br><br>gegenereerd. |

## Implementatiefout

Wanneer een FQDN wordt gebruikt in een ander beleid dan AC Policy/Prefilter, kan deze fout optreden en worden getoond in de FMC UI:



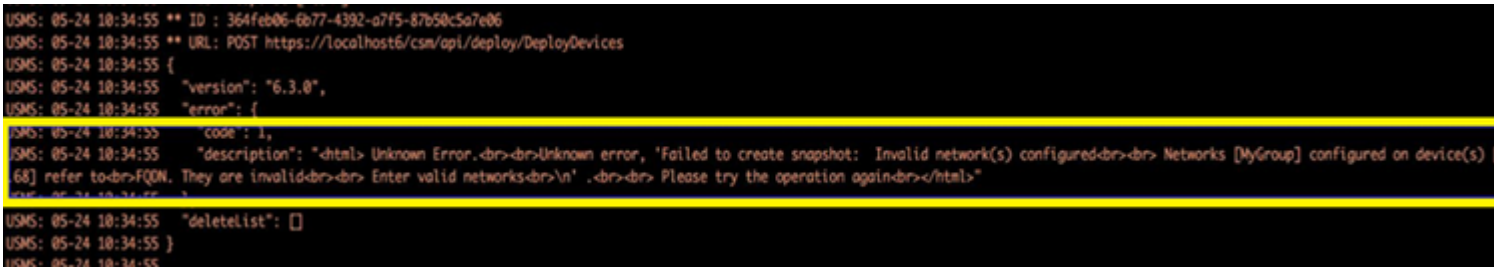

## Aanbevolen stappen voor probleemoplossing

1) Open logfile: /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

2) Controleer of het valideringsbericht vergelijkbaar is met:

"Ongeldige netwerk(en) geconfigureerd. Netwerken [NetworksContainedFQDN] die op het apparaat (de apparaten) zijn geconfigureerd [DeviceNames] verwijzen naar FQDN"

â€ƒ




â€ƒ

3) Voorgestelde actie:

Controleer of een of meer van de onderstaande beleidslijnen al zijn geconfigureerd met een FQDN of groep

die een FQDN-object(en) bevat en probeer de implementatie van hetzelfde opnieuw nadat die objecten zijn verwijderd.

a) Identiteitsbeleid

b) Variabele sets die een FQDN-toepassing op AC-beleid bevatten

### Geen geactiveerd FQDN

Het systeem kan de volgende tonen via de FTD CLI:

**> tonen dns INFO: geen geactiveerde FQDN**

DNS wordt niet geactiveerd tot een object met een gedefinieerde fqdn is toegepast. Nadat een object is toegepast, wordt dit opgelost.

# Vraag en antwoord

**Q: Is Packet-tracer met FQDN een geldige test om problemen op te lossen?**
A: Ja, u kunt fqdn optie gebruiken met packet-tracer.

**V: Hoe vaak werkt de FQDN-regel het IP-adres van de server bij?**
A: Het hangt af van de TTL-waarde van de DNS-respons. Wanneer de TTL-waarde is verlopen, wordt de FQDN opnieuw opgelost met een nieuwe DNS-query.
Dit is ook afhankelijk van het kenmerk Poll Timer gedefinieerd in de DNS-serverconfiguratie. FQDN-regel wordt periodiek opgelost wanneer de Poll DNS-timer is verlopen of wanneer de TTL van de opgeloste IP-ingang is verlopen, afhankelijk van wat het eerst komt.

**V: Werkt dit voor round-robin DNS?**
A: Round-robin DNS werkt naadloos als deze functie werkt op het FMC/FTD met het gebruik van een DNS-client en de round-robin DNS-configuratie is aan de DNS-serverkant.

**Q: Is er een beperking voor de lage TTL DNS waarden?**
A: Als een DNS-reactie met 0 TTL komt, voegt het FTD-apparaat 60 seconden toe aan het. In dit geval is de TTL-waarde minimaal 60 seconden.

**Q: Dus de FTD houdt standaard de standaardwaarde van 60 seconden?**
A: De gebruiker kan de TTL altijd met voeten treden met de instelling van de Invoertimer Verlopen op DNS-server.

**V: Hoe het interopereert met anycast DNS antwoorden? DNS-servers kunnen bijvoorbeeld verschillende IP-adressen aan aanvragers geven op basis van geolocatie. Is het mogelijk om alle IP-adressen voor een FQDN aan te vragen? Vind je het delopdracht op Unix leuk?**
A: Ja, als FQDN in staat is om meerdere IP-adressen op te lossen, worden alle naar het apparaat geduwd en de AC-regel wordt dienovereenkomstig uitgebreid.

**Q: Zijn er plannen om een voorproefoptie te omvatten die toont de bevelen vóór om het even welke depoloment verandering wordt geduwd?**
A: Dit maakt deel uit van de optie **Preview-configuratie die** beschikbaar is via Flex-configuratie. De voorbeeldweergave is al aanwezig, maar is verborgen in Flex Config-beleid. Er is een plan om het te verplaatsen en generiek te maken.

**Q: Welke interface op de FTD wordt gebruikt om de DNS raadpleging uit te voeren?**

A: Het is configureerbaar. Wanneer er geen interfaces zijn geconfigureerd, zijn alle benoemde interfaces op FTD ingeschakeld voor de DNS-lookup.

**V: Voert elke beheerde NGFW zijn eigen DNS-resolutie en FQDN IP-vertaling afzonderlijk uit, zelfs wanneer hetzelfde toegangsbeleid op al deze apparaten met hetzelfde FQDN-object wordt toegepast?**
A: Ja.

**Q: Kan het DNS geheim voorgeheugen voor FQDN ACLs worden ontruimd om problemen op te lossen?**
A: Ja, u kunt de **duidelijke dns** en **duidelijke dns-hosts cache** opdrachten op het apparaat uitvoeren.

**Q: Wanneer precies de FQDN resolutie wordt geactiveerd?**
A: FQDN-resolutie gebeurt wanneer het FQDN-object wordt geïmplementeerd in een AC-beleid.

**V: Is het mogelijk om de cache alleen voor een enkele site te verwijderen?**
A: Ja. Als u de domeinnaam of IP-adres kent, kunt u deze wissen, maar er is geen opdracht als zodanig per ACL-perspectief. De opdracht **clear dns host agni.tejas.com** is bijvoorbeeld aanwezig om de cache op host-door-host basis te wissen met de trefwoordhost zoals in **dns host agni.tejas.com**.

**V: Is het mogelijk om wildcards te gebruiken, zoals *.microsoft.com?**
A: Nee. FQDN moet beginnen en eindigen met een cijfer of letter. Alleen letters, cijfers en koppeltekens zijn toegestaan als interne tekens.

**Q: Wordt de naamresolutie uitgevoerd op AC compilatietijd en niet op het tijdstip van de eerste of verdere verzoeken? Als we een lage TTL (minder dan AC compilatietijd, fast-flux of iets anders) bereiken, kunnen dan bepaalde IP-adressen worden gemist?**
A: De resolutie van de naam gebeurt zodra het beleid van AC wordt opgesteld. Na het verstrijken van de TTL-tijd volgt de verlenging.

**V: Zijn er plannen om Microsoft Office 365 cloud IP-adressen (XML) te kunnen verwerken?**
A: Dit wordt op dit moment niet ondersteund.

**V: Is FQDN beschikbaar in SSL-beleid?**
A: Niet voor nu (softwareversie 6.3.0). FQDN-objecten worden alleen ondersteund in het bron- en doelnetwerk voor AC-beleid.

**V: Zijn er historische logboeken die informatie kunnen geven over opgeloste FQDNâ€™s? Net als bijvoorbeeld LINA-systemen.**
A: Om problemen op te lossen FQDN naar een bepaalde bestemming, kunt u de opdracht **systeemondersteuning traceren** gebruiken. De sporen tonen de FQDN-id van het pakket. U kunt de ID vergelijken om problemen op te lossen. U kunt ook Syslog-746015 inschakelen 746016 de FQDN-dns-resolutieactiviteit te volgen.

**Q: Is het apparatenlogboek FQDN in aansluitingstabel met opgelost IP?**
A: Om problemen op te lossen FQDN aan een bepaalde bestemming, kunt u het bevel van het **systeemsteun spoor** gebruiken, waar de sporen FQDN-ID van het pakket tonen. U kunt de ID vergelijken om problemen op te lossen. Er zijn plannen om in de toekomst FQDN-logbestanden in de eventviewer op FMC te hebben.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.