çžè§£Firepowerå¨ï¿½è„…é˜²ç¦¦ï¼ˆFMCè¨—ç®¡ï¼‰

ç›®éŒ„

ç°¡ä»‹
å¿…è¦ï¿½æ¢ä»¶
éœ€æ±‚
æŽ¡ç”¨å…ƒä»¶
èƒŒæ™¯è³‡è¨Š
åŠŸèƒ½ï¼æ¦‚è¿°
6.3ä¹‹å‰ç‰ˆæœ¬çš„ç‰¹æœ¬å‘ï¼Ÿ
è¨å®š
ç¶²è·¯åœ–
æž¶æ§‹ â€” è¦ï¿½é»ž
é…ï¿½ç½®æ¥é©Ÿ
é©—è‰
ç–‘é›£æŽ’è§£
æ”¶é›†FMCæ•…éšœæŽ’é™¤æª”æ¡ˆ
å¸¸è¦‹å•ï¿½é¡Œ/éŒ¯èª¤æ¶ˆæ¯
éƒ¨ç½²å¤±æ•—
å»ºè°ç„¡æ•…éšœæŽ’é™¤
æ²’æœ‰å•Ÿç”¨çš„FQDN
å•ï¿½ç″

ç°¡ä»‹

æœ¬æª”æ¡ˆå°‡èªªæ˜Žçˆ¹Firepowerç®¡ç�†ä¸å¿ƒ(FMC)å’ŒFirepowerå¨ï¿½è„…é˜²ç¦¦(FTD)çš„FQDNåŠŸèƒ½ï¼ˆè‡

å¿…è¦ï¿½æ¢ä»¶

éœ€æ±‚

æ€ï¿½ç§‘å»ºè°®æ¨¨çžè§£ä»¥ä¸‹é¡Œï¼š

- Firepowerç®¡ç�†ä¸å¿ƒ

æŽ¡ç”¨å…ƒä»¶

本文件中的資訊是根據以下軟體和硬體版本：

- æ€ï¿½ç§‘Firepowerå¨ï¿½è„…é˜²ç¦¦(FTD)è™›æ“¬ï¼Œéï¿½ç¨è»Ÿé«”ç‰ˆæœ¬6.3.0
- Firepowerç®¡ç�†ä¸å¿ƒè™›æ“¬(vFMC)ï¼Œéï¿½ç¨è»Ÿé«”ç‰ˆæœ¬6.3.0

本文件中的資訊是根據特定實驗室環境內的裝置所建立。本文件中使用的所有裝置皆已清除（預設）組態。如果您的網路正在運作，請確保您瞭解任何指令可能造成的影響。

èƒŒæ™¯è³‡è¨Š

æœ¬æª”æ¡ˆä»‹ç´¹è»Ÿé«”ç‰ˆæœ¬6.3.0å¼•å…¥å°Firepowerç®¡ç�†ä¸å¿ƒ(FMC)å'ŒFirepowerå¨ è„…é˜²ç¦¦(

æ¤åŠŸèƒ½å˜åœ¨æ–¼æ€�ç§'èª¿é©©åž‹å®‰å…¨è£ç½®(ASA)ä¸¼Œä½†ä¸¦ä¸ä¸€åœ¨FTDçš„å^ç•«è»Ÿé

åœ¨é…ç½®FQDNå°ç±»ä¹‹å‰ï¼Œè«‹ç¢ºä¿æ»¿è¶³ä»¥ä¸‹è¦æ±‚ï¼š

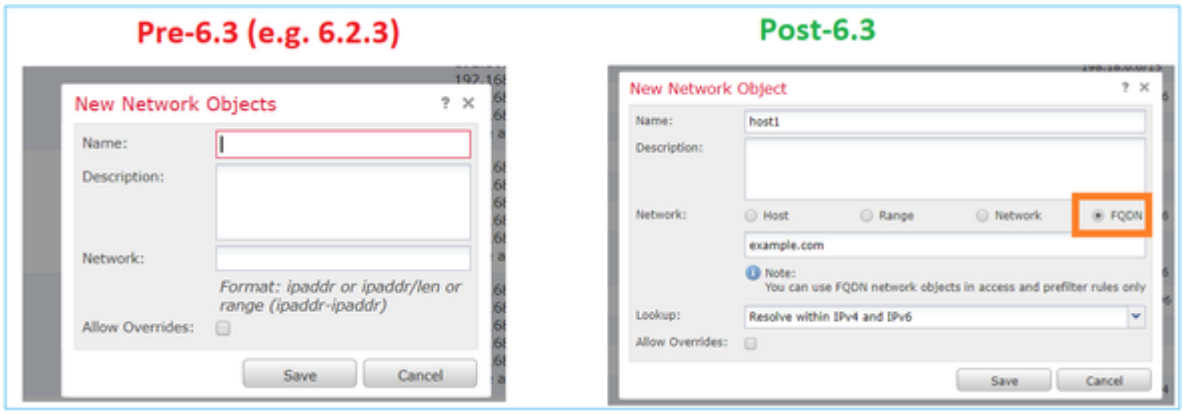
- Firepowerç®¡ç†ä¸å¿åå…é ˆé‹è¡Œ6.3.0ç‰ˆæ––æ›´é«˜ç‰ˆæœ¬ã€‚å¯¯ä»¥æ˜¯ç‰©ç†çš„ï¼
- Firepowerå¨ è„…é˜²ç¦¦å¿…é ˆé¡è¡Œ6.3.0ç‰ˆæ––æ›´é«˜ç‰ˆæœ¬ã€‚å¯¯ä»¥æ˜¯ç‰©ç†çš„ï¼

åŠŸèƒ½æ¦‚è¿°

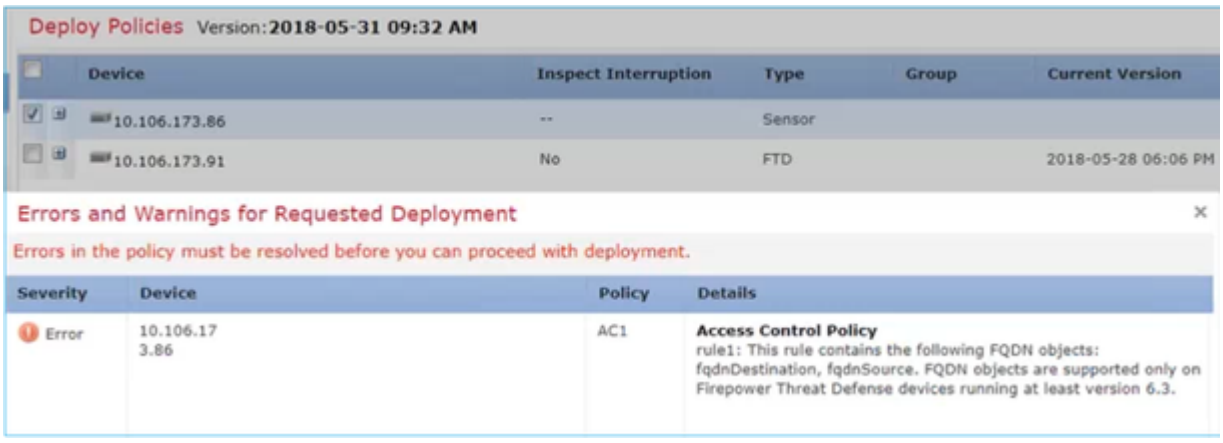
æ¤åŠŸèƒ½å°‡FQDNè§£æž�ç,ºIPåœ°å€ï¼Œä¸¦åœ¨è¨ªå••æŽ§åˆ¶è¦‡å‰‡ä¸ä½¿ç”¨è©²IPåœ°å€ã€‚

6.3ä¹‹å‰ç‰ˆæœ¬å'Œï¼Ÿ

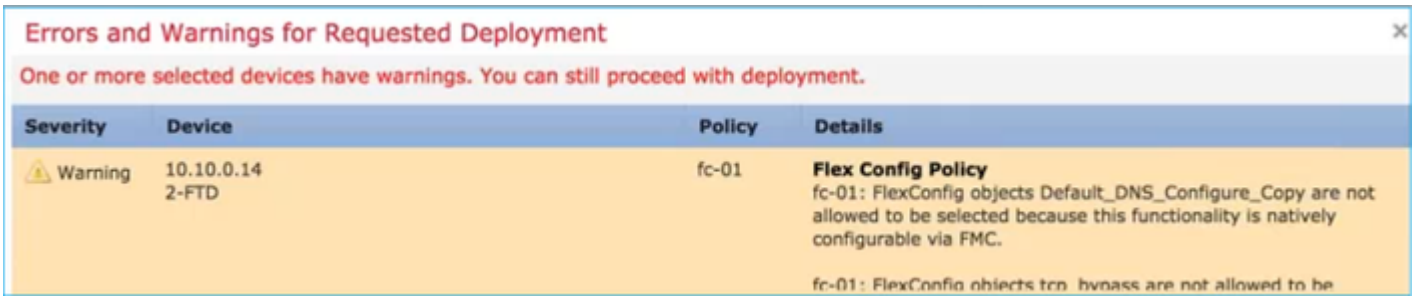
- é�‹è¡Œ6.3.0ä¹‹å‰ç‰ˆæœ¬çš„FMCå'ŒFTDç„¡æ³•é…ç½®FQDNå°ç±»ã€‚



- å¦‚æžœFMCé�‹è¡Œç‰ˆæœ¬6.3æ^–æ›´é«˜ç‰ˆæœ¬ï¼Œä½†FTDé�‹è¡Œç‰ˆæœ¬ä½Žæ–¼6.3ï¼Œ

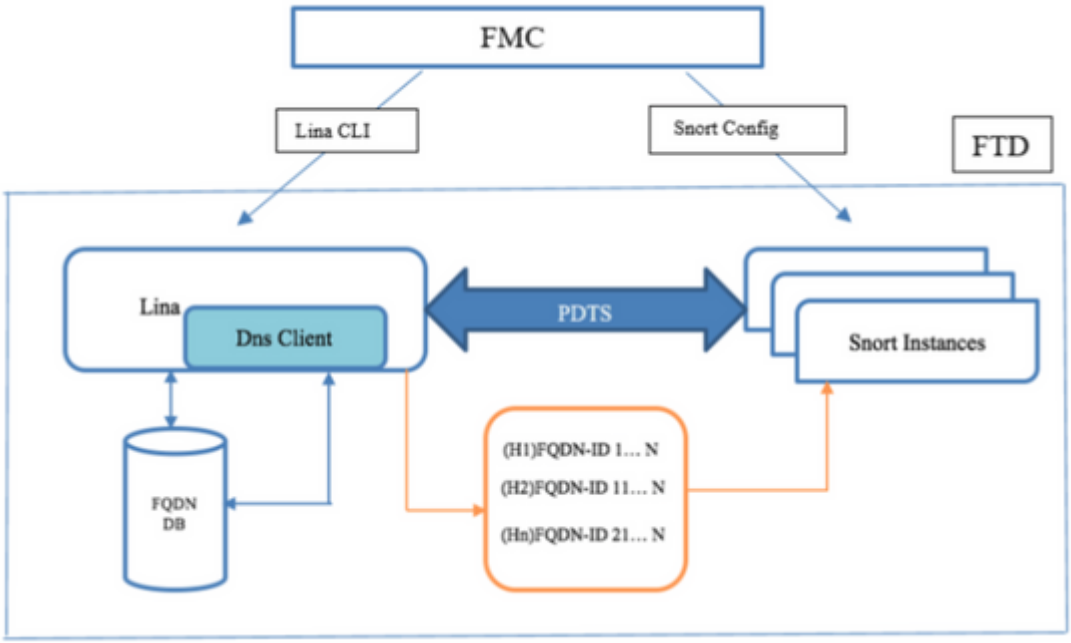


- æ¤å¤–ï¼Œå¦‚æžœé€�é�ŽFlexConfigè¨ å®šDNSç‰©ä»¶ï¼Œå'Šï¼š



è¨å®š

ç¶²è·¯åœ–è¡¨



æž¶æ§‹ â€” è¦�é»ž

- DNSè§£æž�ï¼ˆDNSå°ºIPï¼‰åœ¨LINAä¸ç™¼ç”Ÿ
- LINAå°‡å°�æ˜ å„²å˜åœ¨å…¶è³‡æ–™å°«ä¸
- å°�æ–¼æ¯�å€‹é€£ç·šï¼Œæ¤å°�æ˜ å¾žLINAå,³é€�åˆ°snort
- FQDNçš„è§£æž�ç¸¾æ–¼ç««æ–¼é«˜å�¯ç”¨æ€§æ–¹æ¡ˆé›†é……ç½®

é……ç½®æ¥é©Ÿ

æ¥é©Ÿ1.é……ç½®ã€ŒDNSä¼°æœ›å™¨çµ„å°�è±¡ã€�

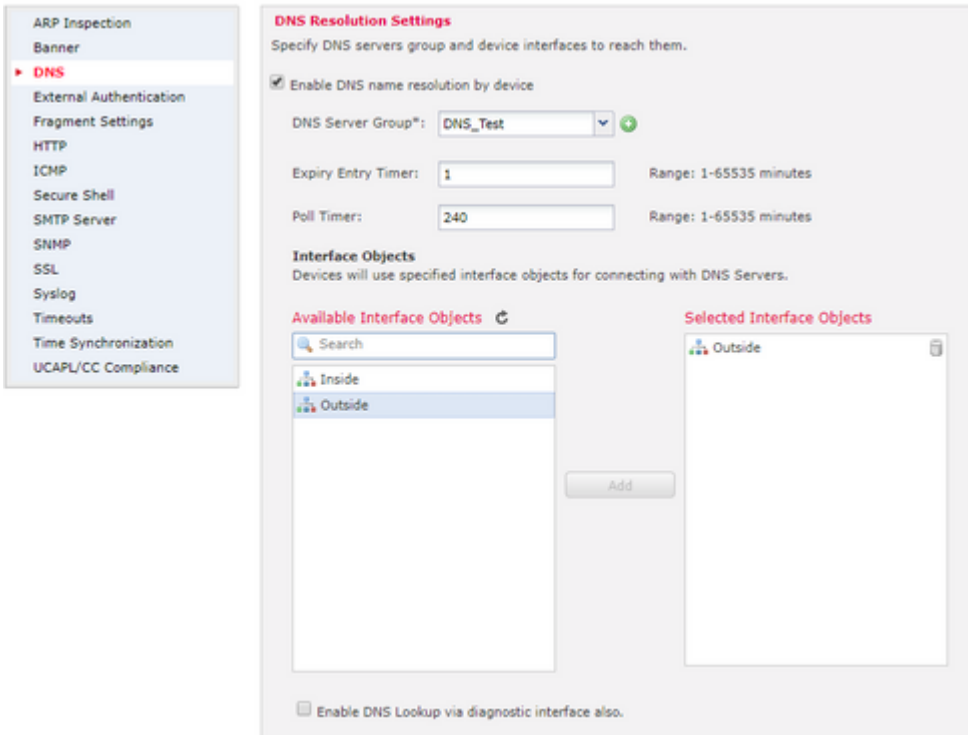
â€ƒ

- DNSä¼ æœ�å™¨çµ„å��ç¨±ä¸�èƒ½è¶…é�Ž63å€‹å—å…ƒ
- åœ¨åšŸÝéƒ¨ç½²ä¸¼Œå°�è±¡å��ç¨±åœ¨åŒŸå±¤æ¬¡çµ„ä¸å¿…é ˆæ˜¯å”¯ä¸€çš„ã€‚ç³»çµ±å
- é ˆè¨åŸŸï¼ˆå¯¯é¸ï¼‰ç”¨æ–¼éŒ„å Š å^°é�žå®Œå…¨é™�å®šçš„ä¸»æ©Ÿå��
- é ˆè¨çš„Retriesâ’ŒTimeoutå€¼æ˜¯é ¡å¡«å……çš„ã€‚

  - Retries â€”
    ç³»çµ±æœªæ”¶åˆ°éŸ¿æ‡‰æ™‚ï¼Œé‡�è©¦DNSä¼ æœ�å™¨æ¸…å–®çš„æ¬¡æ•¸ï¼ˆå¾ž0å^°10ï¼‰
  - Timeout â€”
    å¯¦ä¸€å€‹ä¼ æœ�å™¨å˜—è©¦é€£çºŒå^°ä¸‹ä¸€å€‹DNSä¼ æœ�å™¨ä¹‹å‰ï¼Œç‰¹æ•¸ï¼Œ

- è¼¸å…¥è¦åŠ å…¥æ¤çµ„çš„DNSä¼ æœ�å™¨ã€‚å®ƒå¯¯ä»¥æ˜¯é€—è™Ÿå†éš”å€¼çš„IPv4æ^–I
- DNSä¼ æœ�å™¨çµ„ç”¨æ–¼è§£æž�åœ¨ã€Œå¹²å¯°è¨å®šã€ä¸é…ç½®çš„ä¸€å€‹æ^–å¤šå€‹ä
- æ”¯æ´ç”¨æ–¼DNSä¼ æœ�å™¨çµ„å°�è±¡CRUDçš„REST API

æ¥é©Ÿ2.é…ç½®DNSï¼ˆå¯¯é¸ï¼‰



- ï¼ˆå¯¯é¸‰ä¿®æ”¹å^°æœŸæ¢ç›®è¨ˆæ™‚å™¨å’Œè¼ªè©¢è¨ˆæ™‚å™¨å€¼ï¼ˆä»¥å^†é˜ç,°

å^°æœŸæ¢ç›®è¨^æ™‚å™¨é¸é …æŒ‡å®šæœ¨å…¶ç”Ÿå˜æ™‚é–“(TTL)é¸ŽæœŸå¾Œå¾žDNSæŸ¥è©¢

è¼ªè©¢è¨^æ™‚å™¨é¸é …æŒ‡å®šæ™‚é–“é™¤ŒèœŠé…é¸Žæ¤æ™‚é–“é™¤å^¶ï¼Œè£ç½®å°‡æŸ¥è©¢

- ï¼^å¯¯é¸ï¼‰å¾žå¯¯ç”¨æ¸…å–®ä¸é¸æ“‡æ‰€éœ€çš„ä»»é¸å°ç›±ï¼Œä¸¦å°‡å…¶æ–°å¢žåˆ°æ‰€é¸æ¸…å–®ä¸

å°ææ–¼Firepowerå¨ è¨„é¸é¸ç¨¦ç¦¦6.3.0è£ç½®ï¼Œæžœæœªé¸æ“‡ä»»é¸ç›±ï¼Œä¸”ç¦ç”¨è¨ºæ–·ä»»å‹™ï¼Œæ‰€æœ‰DNSæŸ¥è©¢ï¼‰ lookup anyï¼‰ã€‚

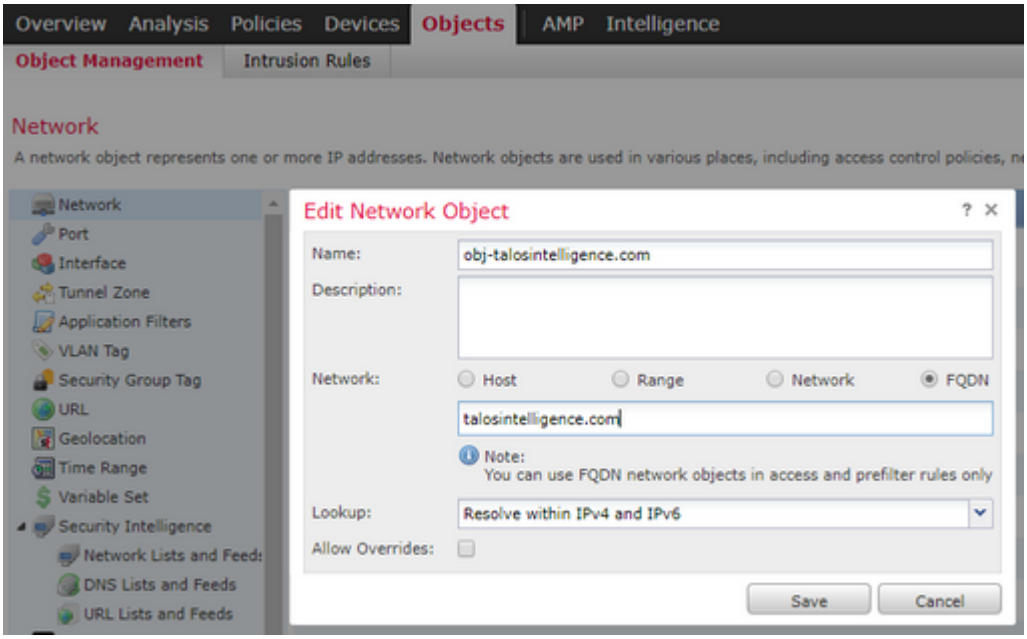
å¦‚æœæ²’有指定任何介面，或者指定的介面沒有IPv4或IPv6地址，則將使用管理介面查詢DNSæŸ¥è©¢ï¼‰

- ï¼^å¯¯é¸ï¼‰é¸ä¸Enable DNS Lookup via the diagnostic interface alsoè¦^å¯¯æ–¹å¼

å¦‚果啟ŸçŽ°è©²åŠŸèƒ½ï¼Œæ‰€é¸ç¦¦æœƒå°‡æŸ¥è¯¢é€æ–™™ä»»é¸å’Œè¨ºæ–·ä»»é
> Device Management > edit device >
Interfacesé ¢é¸ä¸Šç‚ºè¨ºæ–·ä»»é¸é…ç½®IPåœ°å€ã€‚

æ¥é©Ÿ3. é…ç½®å°è±¡ç¶²è·¯FQDN

å°Žèˆªå^°å°è±¡(Objects)>å°è±¡ç®¡ç†(Object Management)ï¼Œåœ¨ç¶²è·¯å°è±¡é¸§æŒ‡å®šé¸é …ã€‚

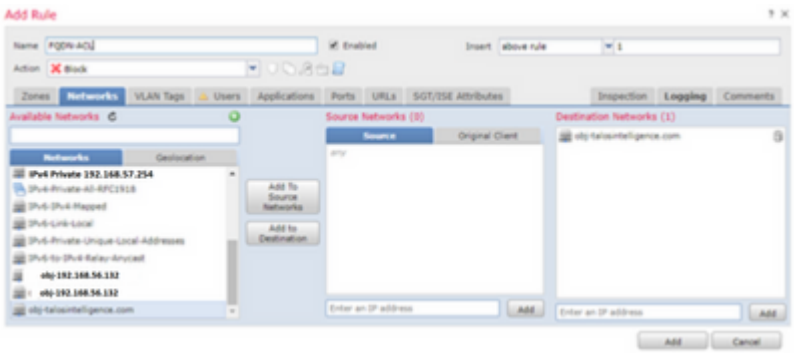


- ç•¶ä½¿ç”¨è€…å»ºç«‹FQDNå°è±¡æ™‚ï¼Œæ^32ä½å”¯ä¸€ID
- æ¤IDå¾žFMCæŽ¨é€å^°LINAå’ŒSnort
- åœ¨LINAä¸ï¼Œæ¤IDèˆ‡ç‰©ä»¶ä¸—è¯
- åœ¨snortä¸ï¼Œæ¤IDèˆ‡åŒ…å«è©²å°è±¡ç§„è¨ªå••æŽ§å^¶è¦‡ç››è¯

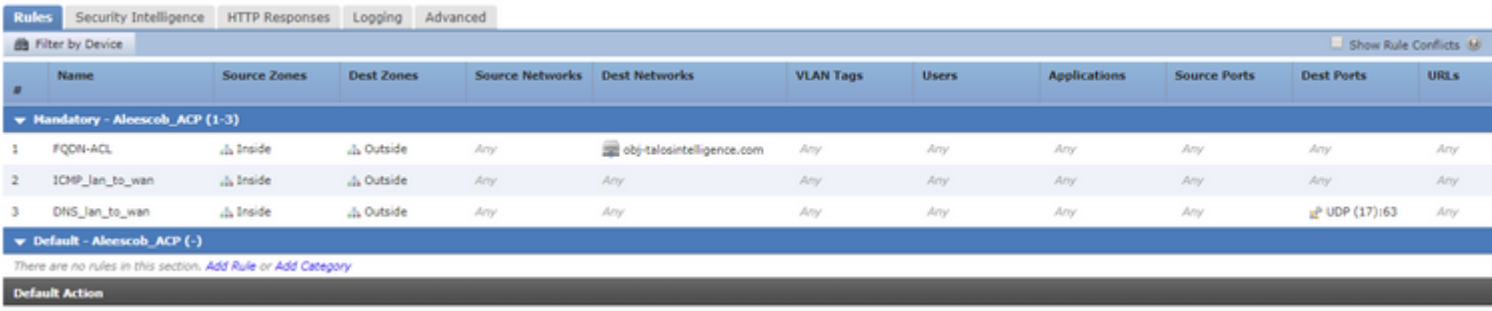
æ¥é©Ÿ4.å»ºç«‹å••æŽ§å^¶è¦‡

ä½¿ç”¨ä»¥

ç‰„FQDNå°è±¡ä»¤ç«‹è¦‰ä¸éƒ¨ç½²ç–•ï¼š



â€ƒ



æ³¨æ„ï¼šåœ¨è¨ªå••æŽ§åˆ¶ç–•ä¸éƒ¨ç½²FQDNå°è±¡æ™‚ï¼Œå°‡ç™¼ŸFQDNè§£æž•ç„¡ç¬¬ä¸€

é©—è‰

ä½¿ç”¨æœ¬ç¯€å…§å®¹ä¾†é©—æ‰€éœ€çš„組態是否正常運作。

- é€™æ˜¯åœ¨éƒ¨ç½²FQDNä¹‹å‰çš„FTDåˆ°åŸ·è¡Œï¼š

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

- é€™æ˜¯FQDNéƒ¨ç½²å¾Œçš„é…ç½®ï¼š

```
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
```

- ä»¥ä¸‹æ˜¯FQDNå°

ï¿½è±¡åœ¨LINAä¸çš„é¡¯ç¤ºæ–¹å¼ï¿½ï¼š

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

- å¦‚果å·²éƒ¨ç½²FQDNï¼Œå‰€€™æ˜¯FQDNå˜å––æ¸…å–®åœ¨LINAä¸çš„é¡¯ç¤ºæ–¹å¼ï¿½ï¼š

```
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
```

- ä»¥ä¸‹æ˜¯Snort(ngfw.rules)ä¸çš„å¤–è§€ï¼š

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

æ³¨æ„ï¼šåœ¨æ¤æ–¹æ³•ä¸ï¼Œç”±æ–¼FQDNå°è±¡ç”¨æ–¼ç›®æ¨™ï¼Œæ¤å› æ¤å®ƒè¢«åˆ—ç‚ºdstfqdnã

- å¦‚果æªœæŸ¥show dnsåŒshow fqdnå‘½ä»¤ï¼Œåœ¨å¯¯ä»¥æ³¨æ„到分é–‹å§‹è§£æž tallosintelligenceçš„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:DB
```

- å¦‚æžœæ‚¨åœ¨LINAä¸‹é¢‘show access-listï¼Œå°±æœƒæ³¨æ„åˆ°æ¯”å€‹è§£æžå°¦å’Œä¸æ¬¡æ•¸çš„å±•é–‹å°ˆæ¡ˆï¼š

```
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
```

- å¦‚æ–‰æ‰€çº¤ï¼Œå°†talosintelligence.comåŸ·è¡Œpingæ“ä½œå¤±æ•—ï¼Œç„¶è¨ªå•æ¸…å–®æ¸…æ¥šåœ°è¡¨æ˜Žï¼Œè¿™äº›æ•°æ®åŒ…æ˜¯ç”±è®¿é—®åˆ—è¡¨ä¸¢å¼ƒçš„ã€‚

â€f

- ä¹‹å‰ï¿½å,³é€ï¿½çš„ICMPè³‡æ–™åŒ…å¾žLINAçš„å‘½ä¸¦è¨ˆæ•¸ï¼š

```
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
```

- åœ¨è¼¸å…¥ä»¤é¢ä¸å––ICMPè¦�æ±,ä¸¦é¡¯ç¤ºç‹ºæ¯ æ£„ï¼š

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 icmp:echo request 3 8:04:12.479162 172.31.4.161 > 192.168.56.132 icmp:echo reply 4: 18:04:13.309966 192.168.56.132 > 172.31.4.161 icmp:echo request 5: 18:04:13.462149 172.31.4.161 > 192.168.5 6.132 icmpï¼šå›žæ‡‰åŽè¦†6: 18:04:14.308425 192.168.56.132 > 172.31.4.161 icmpï¼šå›žæ‡‰è«‹æ±,7: 18:04:14.475424 172.31.4.161> 192.168.56.132 icmpï¼šå›žæ‡‰åŽè¦†8: 18:04:15.306823 192.168.56 32 > 172.31.4.161 icmpï¼šå›žæ‡‰è«‹æ±,9: 18:04:15.463339 172.31.4.161 > 192.168.56.132 icmpï¼šå›žæ‡‰åŽè¦†10: 18:04:25.713662 192.168.56.132 > 192.168.27.54 icmpï¼šå›žæ‡‰è«‹æ±,1: 18:04:3 .704232 192.168.56.132 > 192.168.27.54 icmpï¼šå›žæ‡‰è«‹æ±,12: 18:04:35.711480 192.168.56.132 > 192.168.27.54 icmpï¼šå›žæ‡‰è«‹æ±,13: 18:04:40.707528 192.168.56.132 > 168 27.54 icmp:echo request aleescob# sho cap asp | in 192.168.27.54 162: 18:04:25.713799 192.168.56.132 > 192.168.27.54 icmpï¼šå›žæ‡‰è«‹æ±,165: 18:04:30.704355 192.168.56.132 > 192.168.27.54 icmpï¼šå›žæ‡‰è«‹æ±,168: 18 4:35.711556 192.168.56.132 > 192.168.27.54 icmpï¼šå›žæ‡‰è«‹æ±,176: 18:04:40.707589 192.168.56.132 > 192.168.27.54 icmpï¼šå›žæ‡‰è«‹æ±,

- ä»¥ä¸‹æ˜¯è¿½è¹¤è»Œè·¡å°‹æ‰¾å…¶ä¸€å€‹ICMPå°�åŒ…çš„æ–¯å¼�ï¼š

```
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
```

- å¦‚æžœè¨ªå••æŽ§åˆ¶è¦å‰‡æ“ä½œç‚ºAllowï¼Œå‰‡æ¤ç‚ºçµ±æ”¯æ´firewall-engine-debugçš„è¼¸å‡ºç¤ºä¾‹

```
> 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
```

- å°‡FQDNéƒ¨ç½²ç‚ºé »é©Žæ¿¾å™¨(Fastpath)çš„ä¸€éƒ¨å^†æ™‚ï¼Œé€™æ˜¯ngfwä¸çš„å¤–è§€ã€ru

```
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.
```

- åœ¨LINAçš„è§’åº¦èˆ‡è¿½è¹¤å°�åŒ…æ¯”è¼ƒï¼š

```
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:
```

ç–‘é›£æŽ’è§£

1. å¾žFMCé…�ç½®

- é©—è‰ç•¥åŒ…æ¨¡å¼šæ˜¯å¦¦é…ç½®æ£ç¢º
- é©—è‰éƒ¨ç½²æ˜¯å¦¦æˆ�åŠŸ

2. åœ¨FTDä¸Šéƒ¨ç½²æªæ–Ÿ¥

- é�‹è¡Œshow dnsåŒshow access-listä»¥æªæ¢è¦–FQDNæ˜¯å¦¦å·²è§£æž�ä»¥å�ŠACè¦�å‰‡æ˜¯å¦¦å·²å±•é–‹
- é�‹è¡Œshow run object networkï¼Œè¨˜ä¸‹è¦†ç›—è¯¯çš„IDï¼ˆä¾‹å¦‚ï¼Œï¼Œï¼Xä»£è¡¨ï¼‰
- é�‹è¡Œshow fqdn id Xä»¥æªæ¢æŸ¥FQDNæ˜¯å¦¦æ£ç¢ºè§£æž�å^°æº�IP
- é©—è‰ngfw.rulesæªæ¡ˆæ˜¯å¦¦å…·æœ‰ä»¥FQDN ID Xä½œç‚ºæº�çš„ACè¦�å‰‡
- é�‹è¡Œç³»çµ±æ”¯æ�´firewall-engine-debugä¸¦æªæ¢æŸ¥Snortå^¤å®šçµ�果

æ”¶é›†FMCæ•…éšœæŽ’é™¤æªæ¡ˆ

æ‰€éœ€çš„æ‰€æœ‰æ—¥å¿—æ—¶æ—¶é—´èŒƒå´ç½®é€šé�ŽFMCæ•…éšœæŽ’é™¤æ”¶é›†ã€‚è¦†ç›–æ‰€æœ‰
GUIé�‹è¡Œæ•…éšœæŽ’é™¤ã€‚å¦¦å‰‡ï¼Œåœ¨FMC
Linuxæ��ç¤ºç¬¦ä¸‹é�‹è¡Œsf_troubleshoot.plã€‚å¦¦æžœæ¨¡ç™¼ç¾¾å••é¡Œï¼Œè«‹å•’æ€•ç§

FMCæ—¥èªŒ

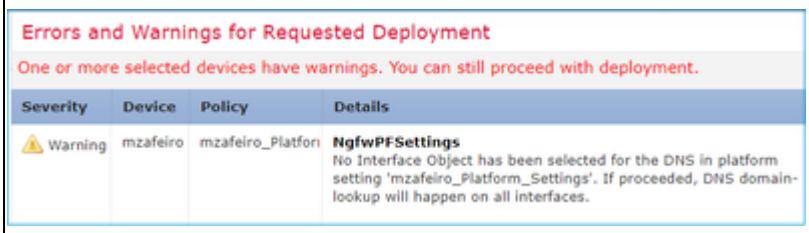
æ—¥èªŒæ”¯å��ç¨±/ä½�ç½®	ç›®çš„
/opt/CSCOpx/MDC/log/operation/vmssharedsvcs.log	æ‰€æœ‰APIå‘¼å�«
/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log	æ‰€æœ‰APIå‘¼å�«
/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log	CLIç”Ÿæˆ�æ—¥èªŒ
/opt/CSCOpx/MDC/tomcat/logs/stdout.log	Tomcatæ—¥èªŒ
/var/log/mojo.log	Mojoæ—¥èªŒ
/var/log/CSMAgent.log	CSMå’ŒDCä¹‹é–“çš„RESTå‘¼å�«
/var/log/action_queue.log	DCçš„æ“�作éšŠåˆ—æ—¥èªŒ

å¸¸è¦‹å•�é¡Œ/éŒ¯èª¤æ¶ˆæ�¯

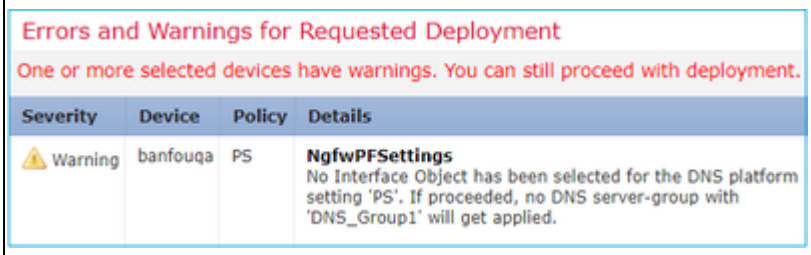
ä»¥ä¸‹æ˜¯FQDNå’ŒDNSä¼¼æœ�å™¨çµ„å°�è±¡å’ŒDNSè¨å®šçš„UIä¸é¡¯ç¤ºçš„éŒ¯èª¤/è¦å‘Šï¼š

éŒ¯èª¤/è¦å‘Š
Name contains invalid characters. Name should be start with either alphabet or underscore and follow with either alphanumeric or special characters (-, _ ,+,.)
å��ç¨±åŒ…å�«ç„¡æ•ˆå—å…ƒã€‚å��ç¨±å¿…é ˆä»¥å—æ¯�æˆ–ä¸‹åˆ’ç·šé–‹é ¼Œç„¶å¾Œæ˜¯å—æ

é ¯è¨åŸŸå€¼ç„¡æ•ˆ



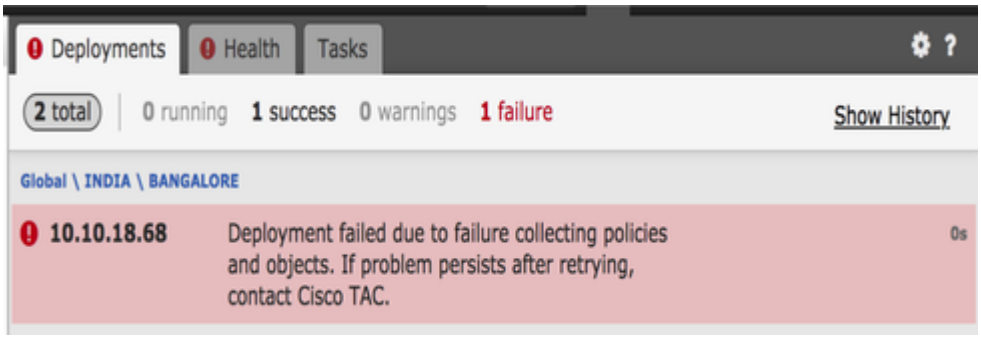
åœ¨å¹³å°è¨å®šã€Œmzafeiro_Platform_Settingsã€ä¸æœªç‚ºDNSé¸æ“‡ä»»é¢ç°å°è±¡ã€å¦‚æœ



åœ¨å¹³å°è¨å®šã€Œmzafeiro_Platform_Settingsã€ä¸æœªç‚ºDNSé¸æ“‡ä»»é¢ç°å°è±¡ã€å¦‚æœ

éƒ¨ç½²å¤±æ•—

åœ¨é™¤ACç–•ç•¥é éé˜ç–•ç»¥å¤–çš„ç–•ç»ä½¿ç”¨FQDNæ™‚ï¼Œå¯¦éƒ¨ç½²ç”Ÿæˆ
UIä¸é¡¯ç¤ºï¼š



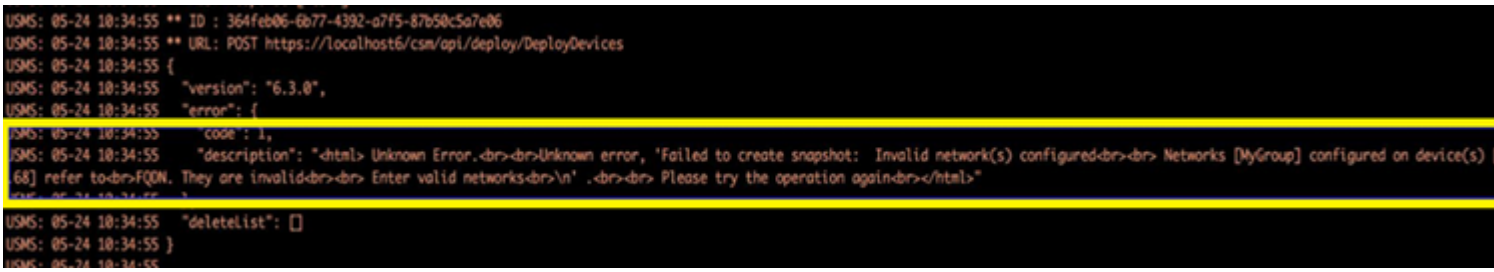
å»ºè°çš„æ•…éšœæŽ’é™¤æ¥é©Ÿ

1)é–‹å•Ÿæ—¥èªŒæ”¡ï¼šï¼/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

2)æ³¢ŸÝ¥é©—è‰å ±æ–‡ï¼Œé¡žä¼¼æ–¼ï¼š

"é…ç½®çš„ç¶²è·¯ç„¡æ•ˆã€åœ¨è£ç½®[DeviceNames]ä¸Šé…ç½®çš„ç¶²è·¯[NetworksContaining

â€ƒ



â€ƒ

3)å»ºè°çš„è¡Œï¼š

é©—è‰æ˜¯å¦·²ä½¿ç”¨åŒ…å«FQDNå°è±¡çš„FQDNæ˜–çµ„é…ç½®ä»¥ä¸‹å€‹æ˜–å¤šå€‹ç–ç•¥

a)è°«ä»½ç–ç•¥

b)åŒ…å«æ‡‰ç”¨æ–¼ACç–ç•¥çš„FQDNçš„è®Šæ•¸é›†

æ²’有å•Ÿç”¨çš„FQDN

ç³»çµå¯¯ä»¥é€éžFTD CLIé¡¯ç¤ºä¸€å€‹å°ˆæ¡ˆï¼š

> show dns INFOï¼šæ²’有å•Ÿç”¨çš„FQDN

åœ¨æ‡‰ç”¨…·œ‰å®šç¾©fqdnçš„å°è±¡ä¹‹å‰ï¼Œä¸Šæœƒå•Ÿç”¨DNSã€‚æ‡‰ç”¨å°è±¡ï¼Œ

å•ç”

å•ï¼šä½¿ç”¨FQDNçš„Packet Traceræ˜¯å¦¦æ˜¯å°å•é¡Œé€è¡Œæ•…éšœæŽ’é™¤çš„有æ•ˆæ¸¬è©¦ï¼Ÿ
ç”¨æ˜¯ï¼Œæ¨å¯¯ä»¥å°‡fqdnéž„é …è‡³Packet Traceräº€èµ·ä½¿ç”¨ã€‚

å•ï¼šFQDNè¦å‰‡æ›´æ–°ä¼šæœå™¨IPåœ°å€çš„é »çŽ‡å¦‚ä½•ï¼Ÿ
ç”¨å¯¯æ–°ï¼DNSéŸ¿æ‡‰çš„TTLå€¼ã€‚TTLå€¼é€ŽæœŸå¾Œï¼Œå°‡ä½¿ç”¨æ–°çš„DNSæŸ¥è©¢ç
é€™ä¹Ÿå¯¯æ–°ï¼DNSä¼ºæœå™¨é…ç½®ä¸çš„Poll Timerå±¬æ€§ã€‚¶è¼ªè©¢DNSè¨ˆæ™‚å™¨é€ŽæœŸæ–°è§£æžçš„IPæ¢ç›®çš„TTLé€ŽæœŸæ™‚,ï

å•ï¼šé€™å°ç¶²è©¢DNSæ˜¯å¦¦æœ‰ï¼Ÿ
ç”¨è¼ªè©¢DNSå¯¯ä»¥ç„¡«é‹è¡Œï¼Œ ç,ºæ¤åŠŸèƒ½åœ¨FMC/FTDä¸Šä½¿ç”¨DNSå®¢æˆ¶ç«¯ï¼Œè

å•ï¼šæ˜¯å¦¦å°ä½ŽTTL DNSå€¼æœ‰é™åˆ¶ï¼Ÿ
ç”¼å¦¦,æžœDNSéŸ¿æ‡‰å…·æœ‰0
TTLï¼ŒFTDè£ç½®æœƒå¢žåŠ 60ç§’ã€‚åœ¨é€™ç¨®æƒ…æ³ä‹ï¼ŒTTLå€¼è‡³å°ç,º60ç§’ã€‚

å•ï¼šå› æ¤ï¼Œé è¨æƒ…æ³ä‹FTDæœƒä¿ç•™é è¨å€¼60ç§ï¼Ÿ
ç”¼ä½¿ç”¨è€…å§‹ç¼å¯¯ä»¥åœ¨DNSä¼ºæœå™¨ä¸Šä½¿ç”¨é€ŽæœŸæ¢ç›®è¨ˆæ™‚å¨å®šè¦†

å•ï¼šå®ƒå¦¦ä½•è‡ªå‹•æ‘DNSéŸ¿æ‡‰ä¸çš„å¤šå€‹IPåœ°å€ï¼Œï¼ŒDNSä¼ºæœå™¨å¯¯åœ¨å¤šå€‹IPåœ°å€ä¹‹é–“è‡ªå‹•æ‡‰ç”¨è¼ªè©¢ï¼Œä»¥å¹³è¡¡æµé‡ã€‚FTDæœƒä¿ç•™DNSéŸ¿æ‡‰çš„åŽŸå§‹é †åºï¼Œä¸¦ä¾è³´æ¼”ç®—æ³•åœ¨å¤šå€‹IPåœ°å€ä¹‹é–“è¼ªè©¢ã€‚
ç”¼ä½¿ç”¨è€…å§‹ç¼å¯¯ä»¥åœ¨DNSä¼ºæœå™¨ä¸Šä½¿ç”¨é€ŽæœŸæ¢ç›®è¨ˆæ™‚å¨å®šè¦†

å•ï¼šæ˜¯å¦¦è¨^ç•«åŒ…å«é ¦½é¸é …ï¼Œé¯¯ç¤ºä»»ä½•é–‹ç™¼æ›´æ”¹ä¹‹å‰‍åˆ›å»ºæŽ¨é
ç”ï¼šé€™æ˜¯éšéŽFlexé…ç½®æ��ä¾›ç„**Preview**
configé¸é …çš„ä€éƒ¨å^†ã€‚é ¦½å·²ç¶“å˜åœ¨ï¼Œä½†æ˜¯å®ƒéš±è—�åœ¨Flex Configç–ç•¥ä¸‚æ^'å€'è¨^ç•«å°‡ï¼Œä½¿å…¶ç”¨æ^�ç,ºé€šç”¨ç”¢å“"ã€‚

å•ï¼šFTDä¸Šçš„å“ªå€‹ä»‹é¢¢ç”¨æ–¼å¥·è¡ŒDNSæŸ¥è©¢ï¼Ÿ
ç”ï¼šå¯¯ä»¥é…ç½®ã€‚¦‚æžœæ²'有覆盖è¨®å®šä»‹é¢¢ï¼Œå‰‡FTDä¸Šçš„æ‰€æœ‰å“

**å•ï¼šå¦³ä½¿å°‘æ•…障排除æ‰€éœ€çš„æ‰€è¨—ç®¡çš„NGFWæ‡‰ç”¨ç¨‹åº
IPè½‰æ›ï¼Ÿ**
ç”ï¼šæ˜¯ã€‚

**å•ï¼šæ˜¯å¦¦å¯¯ä»¥æ¸…é™¤DNSå¿«å–ï¼Œä¾¿å°‘FQDN
ACLé€²è¡Œæ•…éšœæŽ'é™¤ï¼Ÿ**
ç”ï¼šæ˜¯çš„ï¼Œæ¨å¯¯ä»¥åœ¨è£ç½®ä¸Šè¡Œ**clear dns**å'Œ**clear dns-hosts cache** å‘½ä»¤ã€‚

å•ï¼šä½•æ™‚è§¸ç™¼FQDNè§£æž�ï¼Ÿ
Aï¼šåœ¨ACç–•ä¸éç½²FQDNå°�è±¡æ™‚ï¼Œæœ€é€²è¡ŒFQDNè§£æž�ã€‚

å•ï¼šæ˜¯å¦¦å¯ªè§£æž…é™¤å–®å€‹ç«™žçš„å¿«å––ï¼Ÿ
ç”ï¼šæ˜¯ã€‚å¦¨æœæ,¨çŸ¥é"åŸŸå��æ^–IPåœ°å€ï¼Œå‰ä»¥æ¸…é™¤å®fï¼Œä½†æ ¹æ“šACLçš
dns host
agni.tejas.comå‘½ä»¤ï¼Œä¼¿ç”¨è€…é—œé—hosté€€å€‹ä¸»æ©Ÿæ¸…ä¸Šçš„å¿«å––ï¼Œå
host agni.tejas.comæ‰€ç¤ºã€‚

å•ï¼šæ˜¯å¦¦å¯¯ä»¥ä½¿ç”¨è¨¬ç”¨å—…fï¼Œ*.microsoft.com?
ç”ï¼šå¦¦ã€‚FQDNå¿…é ˆä»¥æ•¸å—æ^–å—æ¯”é–‹å§‹å'Œçµæ尾ã€‚å…§éƒ¨å—…å…få¯ªè§£æž¯æ¯”æ

**å•ï¼šå¦¦ä¸±è§£æž¯æ¯”å¦¦åœ¨ACç·¨è¯æ™‚,åŸ·è¡Œï¼Œè€Œä¸‚æ¯”åœ¨ç¬¬ä¸€æ¬¡å¾Œ
ç”ï¼šéƒ¨ACç–•ç•¥å¾«æ^–å¾æ¯”é€²è¡Œå¯¯ç¨±è§£æž¯ã€‚æ ¹æ“šTTLæ™‚é–“å^°æœŸï¼Œç°Œè¨,æœƒç¶**

å•ï¼šæ˜¯å¦¦è¨^ç•«èƒ½å¤ è™•ç†Microsoft Office 365é›²IPåœ°å€(XML)æ„…å–®ï¼Ÿ
ç”ï¼šç›®å‰‍ä¸‚æ”¯æ´æ¤œä½œã€‚

å•ï¼šSSLç–•ç•¥ä¸æ˜¯å¦¦æ��ä¾›FQDN?
ç”ï¼šæš«æ™‚ä¸‚å¯¯è¨¯ï¼ˆè»Ÿé«"ç‰ˆæœ¬6.3.0ï¼‰ã€‚åƒ…ACç–•ç•¥çš„æ°‘ç¶²è·¯å'Œç›®æ¨™ç¶²è·¯æ

**å•ï¼šæ˜¯å¦¦æœ‰ä»»ä½•å¯¯ä¾›æ��ä¾›æœ‰æœ‰é—œå·²è§£æž¯FQDNè³‡è¨Šçš„æ·²å²æ—
ç”ï¼šè‹¥è¦'å®ç‰¹å®šç›®çš„FQDNé€²è¡Œæ•…éšœæŽ'é™¤ï¼Œå¯¯ä½¿ç”¨ **system support trace**å‘½ä»¤ã€‚è·Ÿè¹¤é¡¯ç¤ºè³‡æ–™åŒ…çš„FQDN
IDã€‚æ¨å¯¯ä»¥æ¯"è¼ƒè©²IDé€²è¡Œæ•…éšœæŽ'é™¤ã€‚é„„å¯¯ä»¥å•Ÿç"¨ç³»çµ±æ—¥èªŒæ¶ˆæ¯74
dnsè§£æž¯æ´»å‹•ã€‚

å•ï¼šè£ç½®æ˜¯å¦¦åœ¨ä½¿ç”¨å·²è§£æž¯IPçš„é€£ç·šè¡ä¸¨éŒ„FQDN?
ç”ï¼šè‹¥è¦'å®ç‰¹å®šç›®çš„FQDNé€²è¡Œæ•…éšœæŽ'é™¤ï¼Œå¯¯ä½¿ç”¨ **system support trace**å‘½ä»¤ã€‚è·Ÿè¹¤é¡¯ç¤ºè³‡æ–™åŒ…çš„FQDN
IDã€‚æ¨å¯¯ä»¥æ¯"è¼ƒè©²IDé€²è¡Œæ•…éšœæŽ'é™¤ã€‚ä»¥å¾Œè¨^ç•«åœ¨FMCä¸Šçš„ä°‹ä»¶è¦–å¯

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）。