فهم ميزة FQDN على الدفاع ضد تهديد FirePOWER (الإدارة من FMC)

المحتويات

المقدمة

يصف هذا المستند تكوين ميزة FQDN (اعتبارا من V6.3.0) لمركز إدارة FirePOWER (FMC) والدفاع عن تهديد FirePOWER (FTD).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مركز إدارة Firepower

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج التالية:

- الجهاز الظاهري للدفاع ضد تهديد FirePOWER (FTD) من Cisco الذي يشغل الإصدار 6.3.0 من البرنامج
- Firepower Management Center Virtual (vFMC) الذي يشغل الإصدار 6.3.0 من البرنامج

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يصف هذا المستند تكوين ميزة "اسم المجال المؤهل بالكامل (FQDN)" التي إدخالها إصدار البرنامج 6.3.0 إلى مركز إدارة Firepower (FMC) والدفاع عن تهديد FirePOWER (FTD).

هذه الميزة موجودة في جهاز الأمان القابل للتكيف (ASA) من Cisco ولكنها لم تكن في إصدارات البرامج الأولية من FTD.

تأكد من استيفاء هذه الشروط قبل تكوين كائنات FQDN:

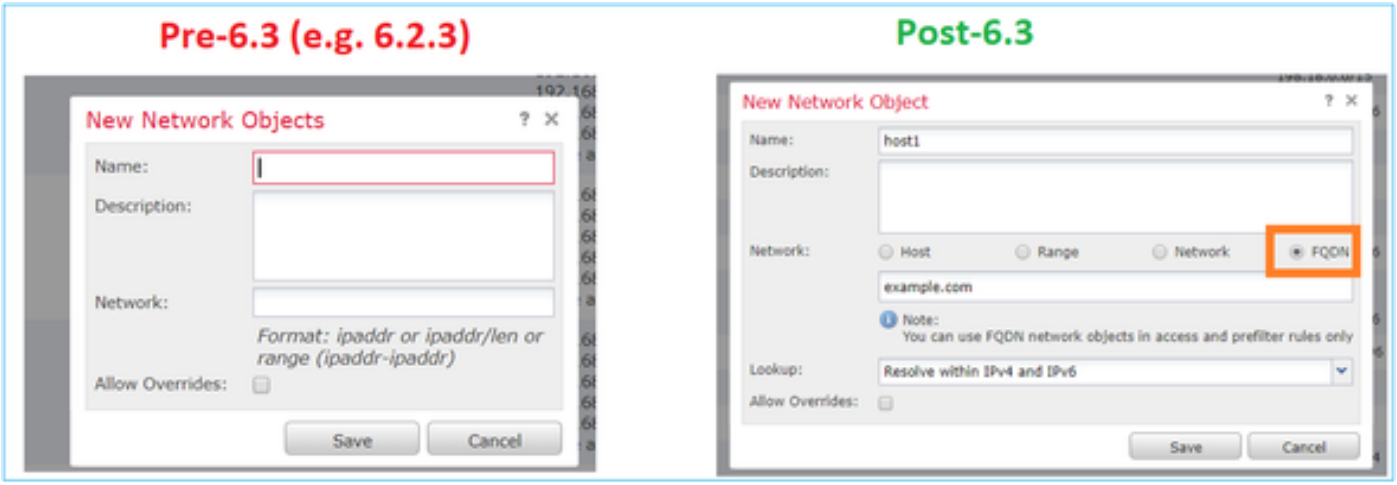
- يجب أن يقوم مركز إدارة Firepower بتشغيل الإصدار 6.3.0 أو إصدار أحدث. يمكن أن يكون مادي أو افتراضي
- يجب أن يقوم "الدفاع عن تهديد Firepower" بتشغيل الإصدار 6.3.0 أو إصدار أحدث. يمكن أن يكون مادي أو افتراضي

نظرة عامة على الميزة

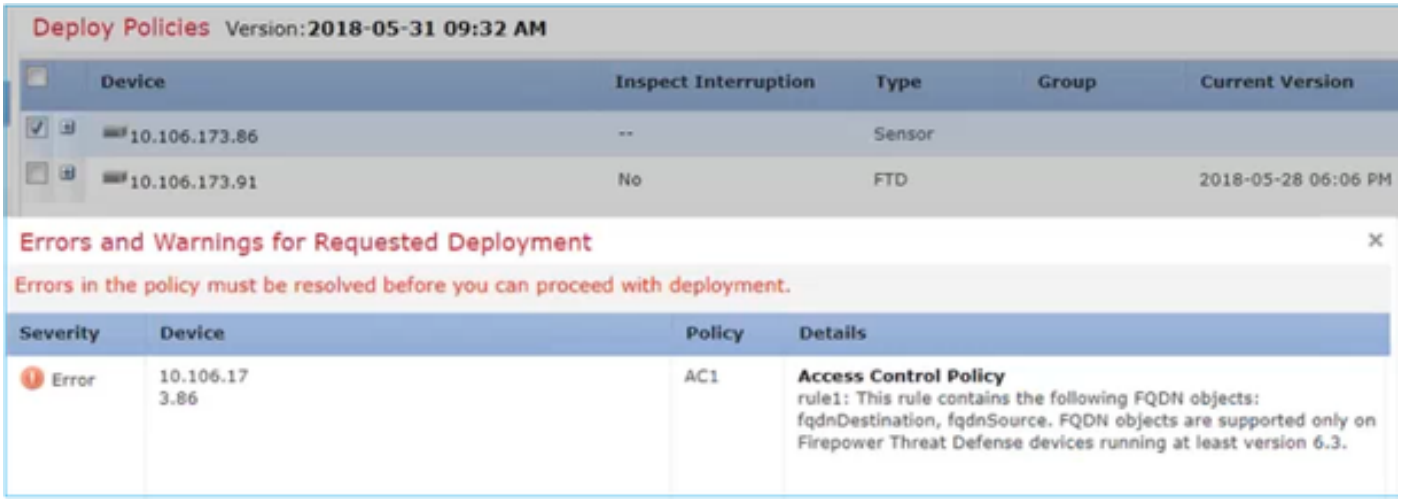
تقوم هذه الميزة بحل FQDN في عنوان IP وتستخدم هذا العنوان الأخير لتصفية حركة المرور عند الإشارة إليه بواسطة قاعدة التحكم في الوصول أو نهج التصفية المسبقة.

ماذا عن ما قبل 6.3؟

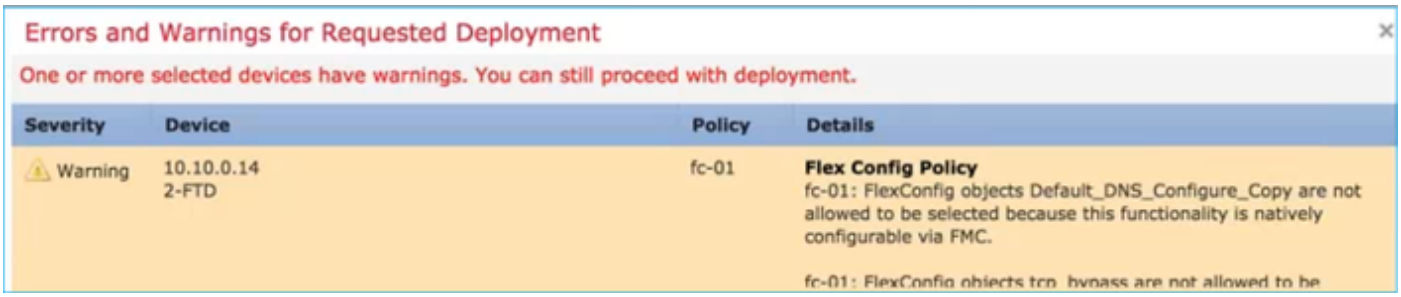
- يتعذر على FMC و FTD اللذين يشغلان إصدارا أقدم من 6.3.0 تكوين كائنات FQDN.



- في حالة تشغيل FMC الإصدار 6.3 أو إصدار أحدث ولكن FTD يشغل إصدارا أقدم من 6.3، يظهر نشر أحد السياسات هذا الخطأ:

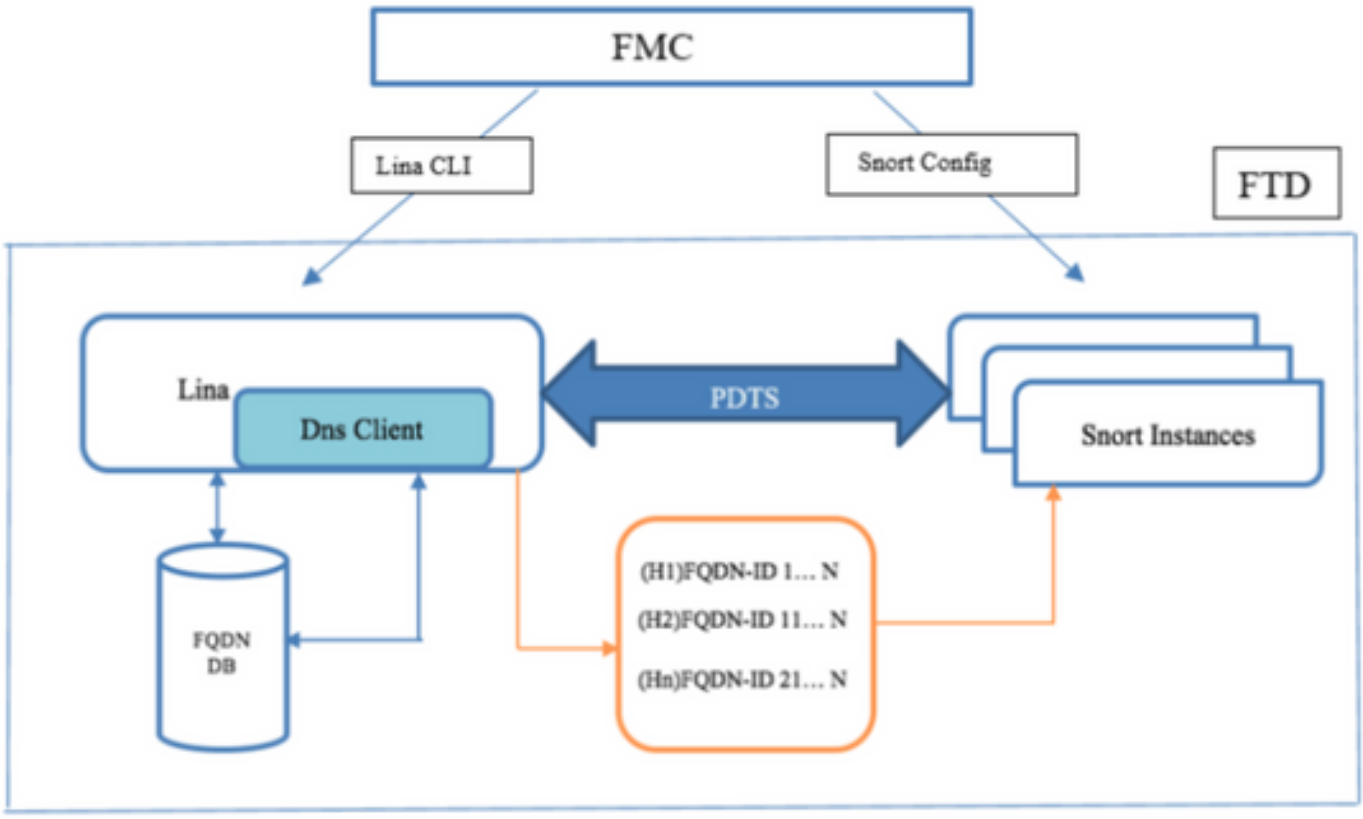


- بالإضافة إلى ذلك، إذا قمت بتكوين كائن DNS عبر FlexConfig، يظهر هذا التحذير:



التكوين

الرسم التخطيطي للشبكة

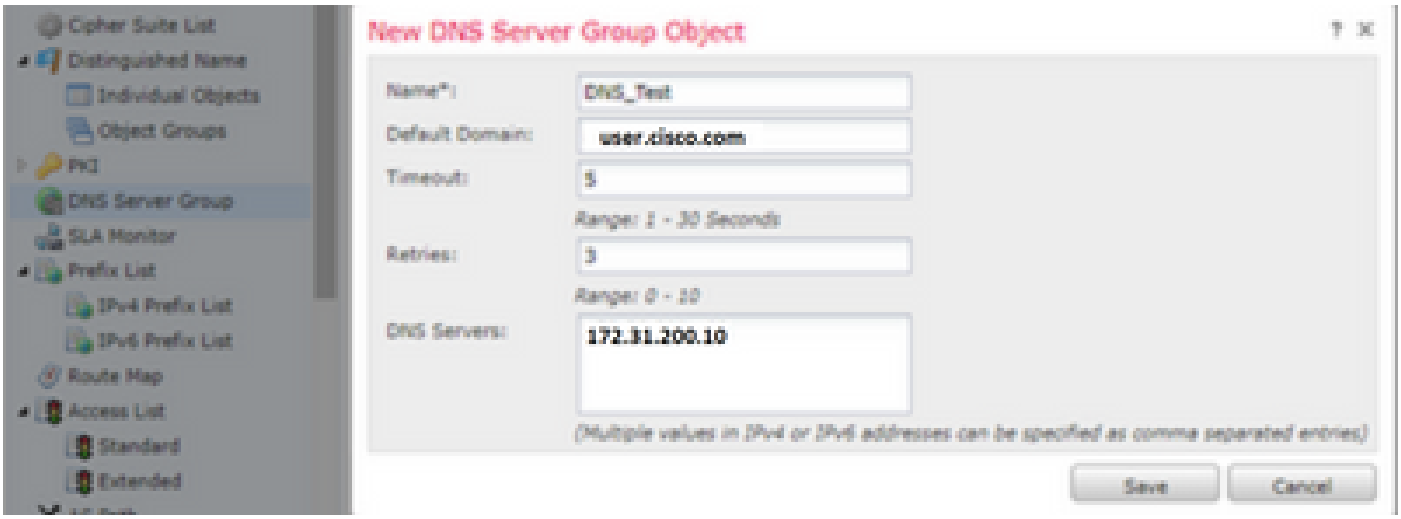


الهندسة المعمارية - النقاط البارزة

- دقة وضوح DNS (DNS إلى IP) تحدث في LINA
- يخزن LINA التعيين في قاعدة بياناته
- على أساس كل اتصال، يتم إرسال هذا التعيين من LINA إلى snort
- يتم حل FQDN بشكل مستقل عن التوفر العالي أو تكوين المجموعة

خطوات التكوين

الخطوة 1. تكوين "كائن مجموعة خوادم DNS"



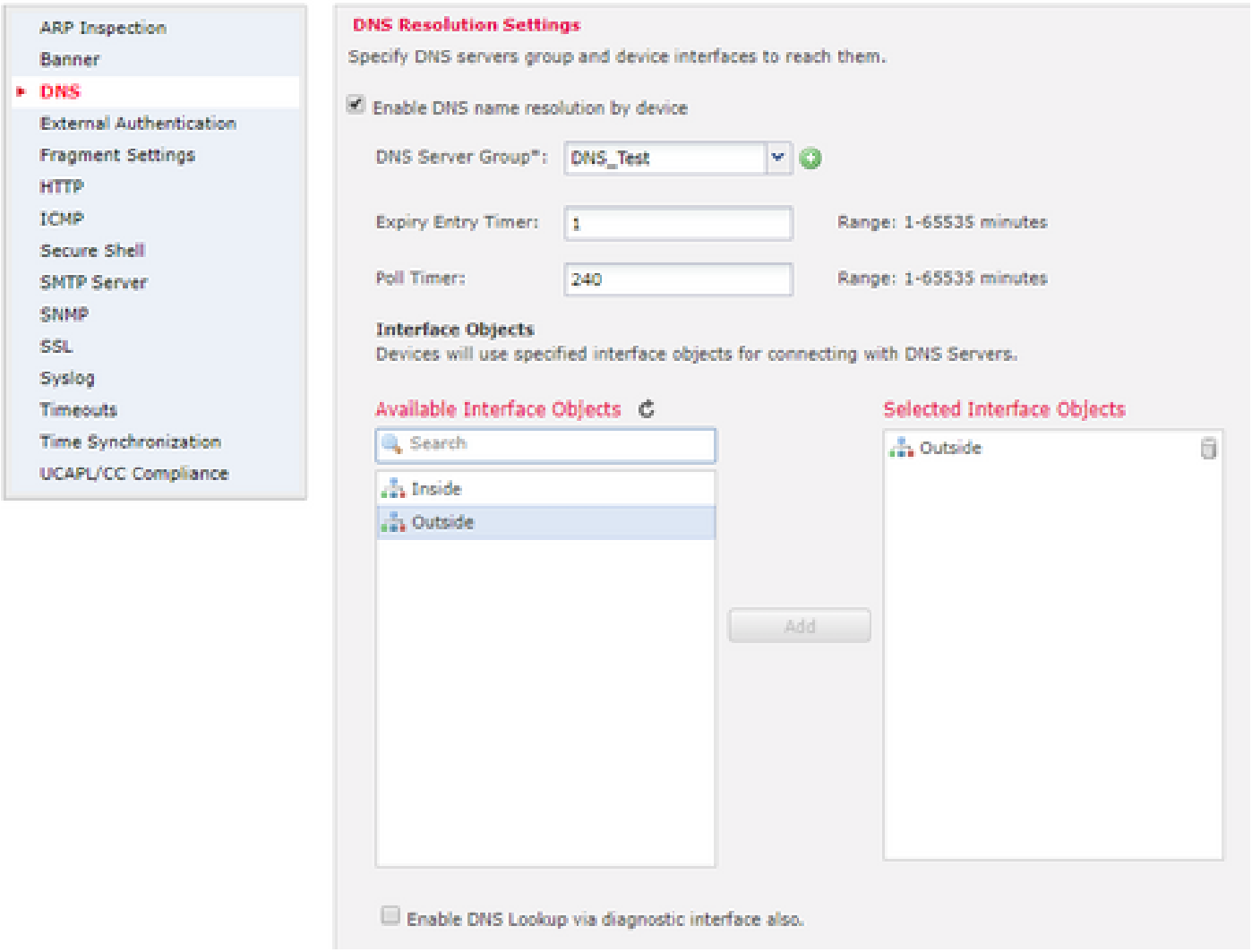
- يجب ألا يتجاوز اسم مجموعة خوادم DNS 63 حرفا
- في النشر متعدد المجالات، يجب أن تكون أسماء الكائنات فريدة ضمن التدرج الهرمي للمجال. يمكن للنظام التعرف على أي تعارض مع اسم كائن ال يمكنك عرضه في المجال الحالي لديك
- يتم إستخدام المجال الافتراضي (إختياري) لإلحاق أسماء المضيف غير المؤهلة بالكامل
- تم مسبقا علم قيم عمليات إعادة المحاولة والتوقيت الافتراضيين.

    - عمليات إعادة المحاولة- عدد المرات، من 0 إلى 10، لإعادة محاولة قائمة خوادم DNS عندما ال يتلقى النظام إستجابة. القيمة الافتراضية هي 2.

    - المهلة—عدد الثواني، من 1 إلى 30، قبل أن يحاول آخر إلى خادم DNS التالي. الافتراضي وه 2 ثانية. وفي كل مرة يقوم النظام بإعادة محاولة قائمة الخوادم، تتضاعف المهلة.

- أدخل خوادم DNS لتكون جزءا من هذه المجموعة. يمكن أن يكون هذا إما تنسيق IPv4 أو IPv6 كقيم مفصولة بفاصلة
- يتم إستخدام مجموعة خوادم DNS للحل باستخدام كائن الواجهة أو الكائنات التي تم تكوينها في إعدادات النظام الأساسي
- REST API لكائن مجموعة خوادم DNS مدعوم

الخطوة 2. تكوين DNS (إعدادات النظام الأساسي)



- (إختياري) قم بتعديل قيم مؤقت انتهاء صلاحية الإدخال ومؤقت الاستطلاع في دقائق:

يحدد خيار مؤقت إدخال انتهاء الصلاحية حد الوقت لإزالة عنوان IP الخاص ب FQDN الذي تم حله من جدول البحث عن DNS بعد انتهاء صلاحية مدة البقاء (TTL) الخاص به. تتطلب إزالة إدخال ما إعادة تحويل الجدول، بحيث يمكن لعمليات الإزالة المتكررة زيادة حمل العملية على الجهاز. يقوم هذا الإعداد بتوسيع مدة البقاء (TTL) فعليا.

يحدد خيار مؤقت الاستقصاء الحد الزمني الذي يستعلم بعده الجهاز عن خادم DNS لحل FQDN الذي تم تعريفه في مجموعة كائنات الشبكة. يتم حل FQDN بشكل دوري إما عند انتهاء صلاحية مؤقت الاستقصاء، أو عند انتهاء صلاحية مدة البقاء (TTL) لإدخال IP الذي تم حله، أيهما يحدث أولا.

- (إختياري) حدد كائنات الواجهة المطلوبة من القائمة المتاحة وأضفها إلى قائمة كائنات الواجهة المحددة وتأكد من إمكانية الوصول إلى خادم DNS من خلال الواجهة (الواجهات) المحددة:

بالنسبة لأجهزة Firepower Threat Defense 6.3.0، إذا لم يتم تحديد واجهات وتم تعطيل الواجهة التشخيصية للبحث عن DNS، يحدث تحليل DNS عبر أي واجهة تتضمن الواجهة التشخيصية (يتم تطبيق الأمر dnsdomain-lookup any).

إذا لم تقم بتحديد أي واجهات—ولم تقم بتمكين بحث DNS على الواجهة التشخيصية، فإن

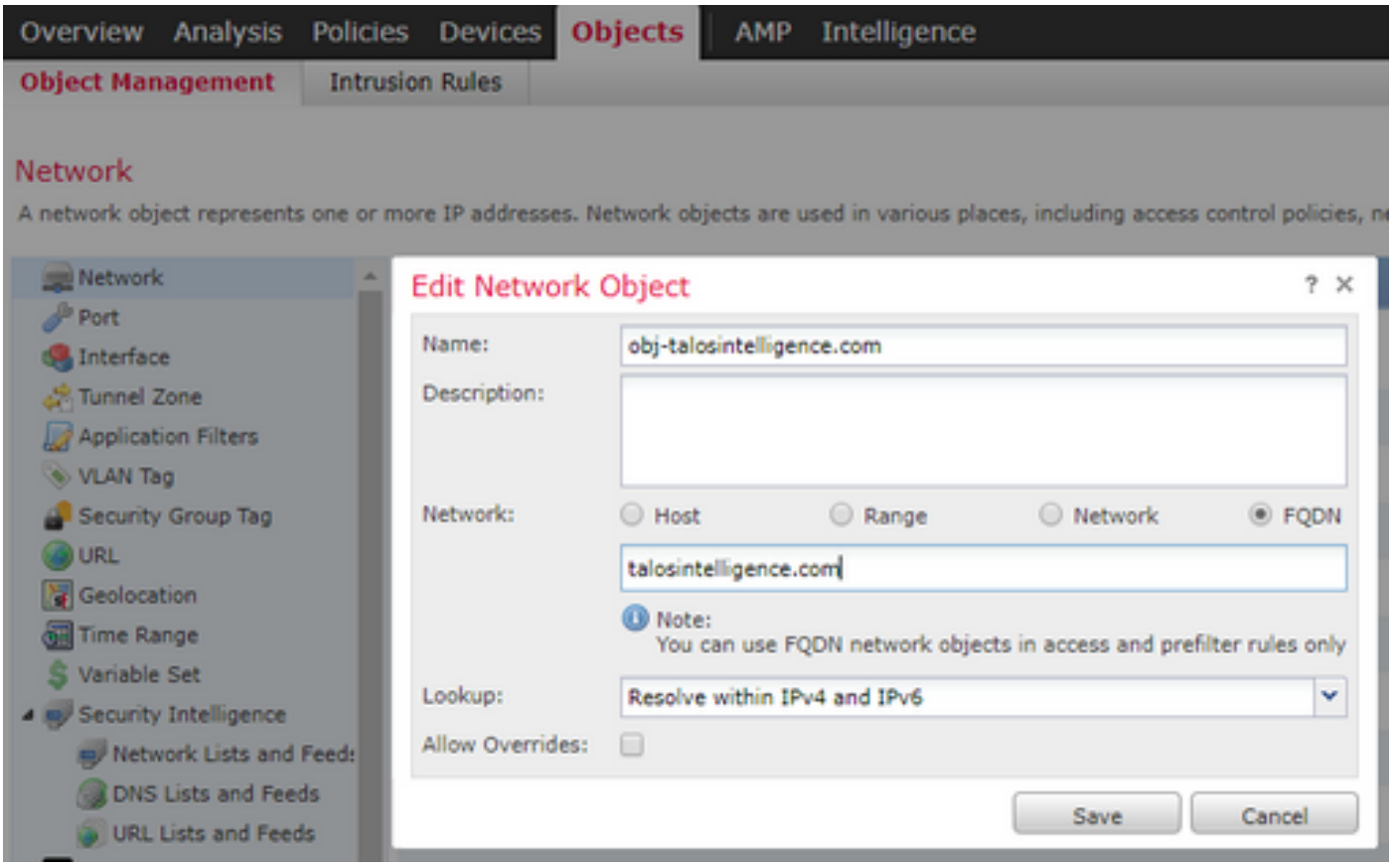
FTD يستخدم جدول توجيه البيانات لتحديد الواجهة. إذا لم يكن هناك تطابق، فإنه يستخدم جدول توجيه الإدارة.

- (إختياري) حدد تمكين بحث DNS من خلال خانة الاختيار أيضا للواجهة التشخيصية

إذا تم تمكين هذا الخيار، يستخدم "الدفاع عن تهديد FirePOWER" كل من واجهات البيانات المحددة وواجهة التشخيص لدقة DNS. تأكد من تكوين عنوان IP لواجهة التشخيص على صفحة الأجهزة > إدارة الأجهزة > تحرير الجهاز > الواجهات.

الخطوة 3. تكوين FQDN لشبكة الكائن

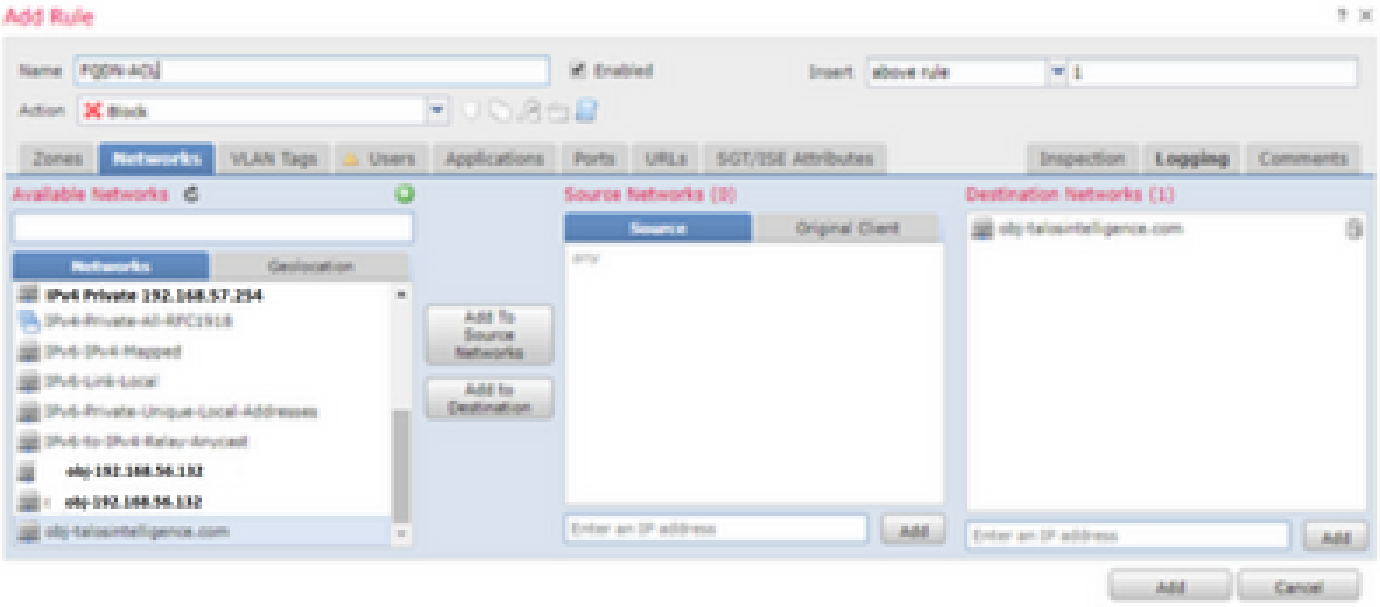
انتقل إلى كائنات > إدارة الكائن، ضمن كائن الشبكة حدد خيار FQDN.

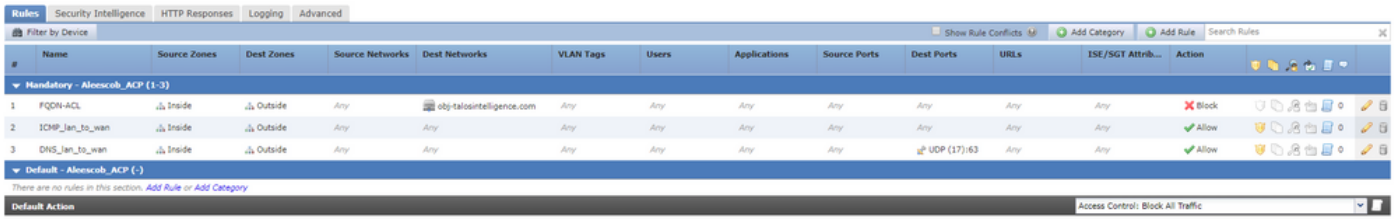


- يتم إنشاء معرف فريد 32 بت عندما يقوم المستخدم بإنشاء كائن FQDN
- يتم دفع هذا المعرف من FMC إلى كل من LINA و Snort
- في LINA، يقترن هذا المعرف بالكائن
- في الشيخير، يقترن هذا المعرف بقاعدة التحكم بالوصول التي تحمل هذا الكائن

الخطوة 4. إنشاء قاعدة تحكم بالوصول

إنشاء قاعدة باستخدام كائن FQDN السابق ونشر النهج:





ملاحظة: يحدث المثيل الأول من تحليل FQDN عند نشر كائن FQDN في نهج التحكم في الوصول

التحقق من الصحة

أستخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

- هذا هو التكوين الأولي ل FTD قبل نشر FQDN:

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

- هذا هو التكوين بعد نشر FQDN:

```
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
```

- هذه هي الطريقة التي يبدو بها كائن FQDN في LINA:

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

- عند نشره بالفعل، هكذا تبدو قائمة الوصول إلى FQDN في LINA:

```
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
```

- هذا ما تبدو عليه في 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
```

ملاحظة: في هذا السيناريو، نظرا لاستخدام كائن FQDN للوجهة، يتم إدراجه على أنه dstfqdn.

- إن يفحص أنت عرض dns وأبديت fqdn أمر، أنت يستطيع لاحظت أن المميزة بدأت أن يحل الـ IP لـ tallosintelligence:

```
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:DI
```

- اذإ تمق بفحص إظهار ةمئاق لوصولا يف LINA، كنكمي ةظحالم تالاخدإلا ةعسوملا لكل لوصولا تارم ددعو حوضو ةقد:

```
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
```

- امك وه حضوم يف الصورة، يفشل إختبار الاتصال إلى talosintelligence.com دوجول ارظن FQDN ل قباطت يف ةمئاق لوصولا. لمع ليلحت DNS ذنم رظح ةمزح ICMP ةطساوب FTD.

```
C:\Windows\system32>ping talosintelligence.com

Pinging talosintelligence.com [192.168.27.54] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.27.54
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>_
```

- عدد مرات الوصول من LINA مزجل ICMP التي تم إرسالها مسبقا:

```
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
```

- يتم التقاط طلبات ICMP وإظهارها يتم إسقاطها في واجهة الدخول:

aleescob# show cap في 13 حزمة ملتقطة 1: 18:03:41.558915 192.168.56.132>172.31.200.100 ICMP: 192.168.56.132 UDP ميناء 59396 يتعذر الوصول إليه 2: 18:04:12.3212692.166.16666.166616163>13 72.31.4.161 icmp: طلب echo 3: 18:04:12.479162 172.31.4.161>192.168.56.132 icmp: رد الارتداد 4: 18:04:13.309966.192.166.132>172.31.4.161 ICMP: طلب الارتداد: 18:0:4 3.462149 172.31.4.161>192.168.56.132 icmp: رد echo 6: 18:04:14.308425 192.168.56.132>172.31.4.161 icmp: طلب echo 7: 18:04:14.47542172.31.311.311.11.1112.11112.3.111111112.162.12.12.162222622.1262226>>>>> 192.168.56.132 icmp: رد echo 8: 18:04:15.306823 192.168.56.132>172.31.4.161 icmp: طلب echo 9: 18:04:15.463339 172.31.4.161>192.168.56.132 ICMP: رد الارتداد: 10: 8:04:25.713662 192.168.56.132 > 192.168.27.54 icmp: طلب echo 11: 18:04:30.704232 192.168.56.132>192.168.27.54 icmp: طلب echo 12: 18:04:35.71144801 2.168.56.132 > 192.168.27.54 icmp: طلب echo 13: 18:04:40.707528 192.168.56.132>192.168.27.54 icmp: طلب echo _Cob# sho cap asp | في 192.168.27.54 162: 18:04:25.713799 192.168.56.132>192.168.27.54 icmp: طلب echo 165: 18:04:30.704355192.168.56.132>192.168.27.54 طلب ICMP: 168: 18:04:35.711556 192.168.56.132 > 192.168.27.54 icmp: طلب echo 176: 18:04:40.707589 192.168.56.132 > 192.168.27.54 ICMP: طلب echo

- هذه هي الطريقة التي يبدو بها التتبع لأحد حزم ICMP هذه:

```
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
```

- إذا كان الإجراء الخاص بقاعدة التحكم في الوصول مسموحا به، فهذا مثال على إخراج دعم النظام لجدار حماية-محرك-تصحيح الأخطاء

```
> 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
```

- عند نشر FQDN كجزء من عامل تصفية مسبق (FastPath)، هذا يدب في القواعد 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.
```

- من وجهة نظر LINA مع حزمة متتبع:

```
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:
```

استكشاف الأخطاء وإصلاحها

1. التكوين من FMC

- تحقق من تكوين النهج وإعدادات خادم DNS بشكل صحيح
- التحقق من نجاح النشر

2. نشر التحقق من FTD

- قم بتشغيل show dns و show access list لحل مت اذإ ام ةفرعمل FQDN وتوسعة قواعد التيار المتردد
- قم بتشغيل العرض تشغيل شبكة الكائن ولاحظ أسفل المعرف المرتبط بالكائن (قل X للمصدر)
- قم بتشغيل show fqdn id x للتحقق من حل FQDN إلى IP المصدر بشكل صحيح
- التحقق مما إذا كان ملف ngfw.rules يحتوي على قاعدة AC بمعرف FQDN X مصدر
- قم بتشغيل تصحيح أخطاء محرك جدار الحماية الخاص معدب النظام وفحص الحكم الصادر عن التطفل

تجميع ملفات أستكشاف أخطاء FMC وإصلاحها

يتم تجميع جميع السجلات المطلوبة من أستكشاف أخطاء FMC وإصلاحها. لتجميع جميع السجلات المهمة من FMC، قم بتشغيل أستكشاف الأخطاء وإصلاحها من واجهة المستخدم الرسومية (GUI) ل FMC. وإلا من موجه FMC Linux، قم بتشغيل sf_troubleshooting.pl. إذا وجدت مشكلة، يجري إرسال أستكشاف أخطاء FMC وإصلاحها باستخدام التقرير الخاص بك إلى مركز المساعدة التقنية (TAC) من Cisco.

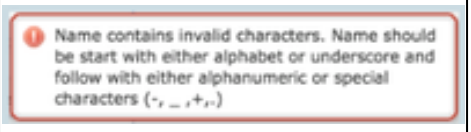
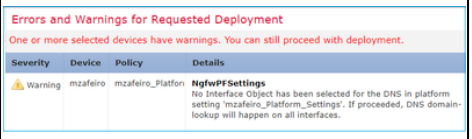
سجلات FMC

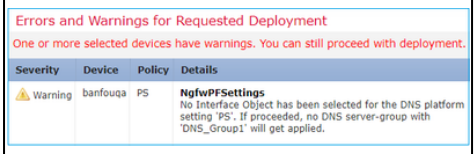
اسم ملف السجل/موقعه	الغرض
/opt/CSCOpx/MDC/log/operation/vmsshareddsvcs.log	كافة المكالمات API
/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log	كافة المكالمات API
/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log	سجلات إنشاء واجهة سطر الأوامر (CLI)
/opt/CSCOpx/MDC/tomcat/logs/stdout.log	طقل عوذج
/var/log/mojo.log	سكول وجوم

/var/log/CSMAgent.log	إجراء مكالمات الراحة بين CSM و DC
/var/log/action_queue.log	سجل قائمة انتظار إجراءات DC

المشاكل الشائعة/رسائل الخطأ

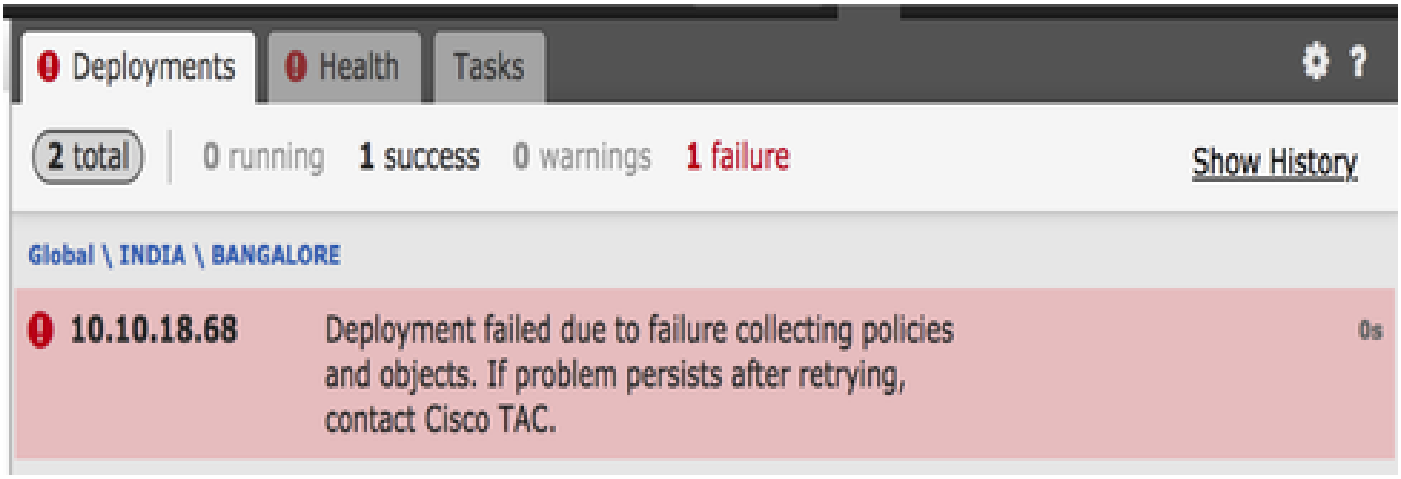
هذه هي الأخطاء/التحذيرات المعروضة في واجهة المستخدم لكائن FQDN ومجموعة خوادم DNS وإعدادات DNS:

خطأ/تحذير	السيناريو	الوصف
 يحتوي الاسم على أحرف غير صحيحة. يجب أن تبدأ الأسماء بالحروف الأبجدية أو التسطير ثم بعد ذلك إما الحروف الأبجدية الرقمية أو الحروف الخاصة. (-،_،+،.)	مستعمل تكوين اسم غير صحيح	يتم إعلام المستخدم بـ "مسموح" الحروف والحد الأقصى للنطاق.
 قيمة المجال الافتراضية غير صالحة	يقوم المستخدم بتكوين اسم مجال غير صحيح	يتم إعلام المستخدم بالحروف المسموح بها والنطاق الأقصى.
 لم يتم تحديد كائن واجهة لـ DNS في إعداد النظام الأساسي 'mzafiro_platform_settings'. في حالة المتابعة، سيتم قريبا إجراء البحث عن مجال DNS على جميع الواجهات	لم يحدد المستخدم أي واجهة للبحث عن المجال لجهاز ما بعد 6.3	تم تحذير المستخدم من أن DNS سيتم تطبيق واجهة سطر الأوامر لمجموعة الخوادم قريبا لجميع الواجهات.

 لم يتم تحديد كائن واجهة لـ DNS في إعداد النظام الأساسي 'mzafiro_platform_settings'. في حالة المتابعة، لن يتم تطبيق أي مجموعة خوادم DNS مع "DNS" قريبا	لم يحدد المستخدم أي واجهة للبحث عن المجال لجهاز 6.2.3	تم تحذير المستخدم أن DNS واجهة سطر الأوامر (CLI) الخاصة بمجموعة الخوادم ليست تم الإنشاء.

فشل النشر

عند إستخدام FQDN في النهج بخلاف نهج AC/نهج عامل التصفية المسبق، يمكن حدوث هذا الخطأ وإظهاره في واجهة مستخدم FMC:



خطوات أستكشاف الأخطاء وإصلاحها الموصى بها

1) افتح ملف السجل: /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

2) التحقق من صحة رسالة مماثلة لـ:

"تم تكوين شبكة (شبكات) غير صالحة. تشير الشبكات [NetworksContainsFQDN] التي تم تكوينها على الجهاز (الأجهزة) [DeviceName] إلى FQDN

3) الإجراء المقترح:

تحقق من تكوين نهج أو أكثر من النهج المذكورة أدناه بالفعل باستخدام FQDN أو مجموعة تحتوي على كائن (كائنات) FQDN أو عدم محاولة نشره بعد إزالة هذه الكائنات.

أ) سياسة الهوية

ب) مجموعات المتغيرات التي تحتوي على FQDN مطبقة على سياسة AC

لم يتم تنشيط FQDN

يمكن أن يعرض النظام التالي من خلال واجهة سطر الأوامر (CLI) الخاصة ب FTD:

> إظهار معلومات DNS: لا يوجد FQDN منشط

لا يتم تنشيط DNS حتى يتم تطبيق كائن ذي قيمة FQDN معرفة. بعد تطبيق كائن، يتم حل هذا.

أسئلة وأجوبة

س: هل Packet-tracer مع FQDN إختبار صالح لاستكشاف المشاكل وإصلاحها؟
أ: نعم، يمكنك إستخدام خيار fqdn مع packet-tracer.

س: كم مرة تقوم قاعدة FQDN بتحديث عنوان IP الخاص بالخادم؟
A: يعتمد على قيمة مدة البقاء (TTL) الخاصة باستجابة DNS. بمجرد انتهاء صلاحية قيمة TTL، يتم حل FQDN مرة أخرى باستخدام استعلام DNS جديد.
يعتمد هذا أيضا على سمة مؤقت الاستقصاء المعرفة في تكوين خادم DNS. يتم حل قاعدة FQDN بشكل دوري عند انتهاء صلاحية مؤقت DNS للاستطلاع أو عند انتهاء صلاحية مدة البقاء (TTL) للإدخال IP الذي تم حله، أيهما يأتي أولا.

س: هل يعمل هذا مع نظام أسماء النطاقات (DNS) الدوري؟
A: يعمل نظام أسماء النطاقات (DNS) الدوري بشكل سلس حيث تعمل هذه الميزة على FMC/FTD باستخدام عميل DNS، كما أن تكوين نظام أسماء النطاقات (DNS) الدوري يقع على جانب خادم DNS.

س: هل هناك حد لقيم DNS ذات مدة البقاء (TTL) المنخفضة؟
أ: إذا جاءت إستجابة DNS مع 0 مدة البقاء (TTL)، يضيف جهاز FTD 60 ثانية إليها. في هذه الحالة، تكون قيمة TTL 60 ثانية كحد أدنى.

س: إذا يحتفظ FTD بشكل افتراضي بالقيمة الافتراضية وهي 60 ثانية؟
A: يمكن للمستخدم دائما تجاوز مدة البقاء (TTL) من خلال إعداد مؤقت "انتهاء صلاحية الإدخال" على خادم DNS.

س: كيف تتعامل مع استجابات نظام أسماء النطاقات (DNS) المنقول؟ على سبيل المثال،

يمكن أن توفر خوادم DNS عناوين IP مختلفة استنادا إلى الموقع الجغرافي للطالبين. هل من الممكن طلب جميع عناوين IP لشبكة FQDN؟ مثل أمر الحفر على Unix؟
أ: نعم، إذا كانت شبكة FQDN قادرة على حل عناوين IP المتعددة، فسيتم دفع جميع هذه العناوين إلى الجهاز وتوسيع قاعدة AC وفقا لذلك.

س: هل هناك خطط لتضمين خيار معاينة يظهر الأوامر التي تم دفعها قبل أي تغييرات مميزة؟
أ: هذا جزء من خيار معاينة التكوين المتاح عبر Flex config. المعاينة موجودة بالفعل، ولكنها مخفية في نهج تكوين مرن. هناك خطة لنقله وجعله عاما.

س: ما هي الواجهة الموجودة على FTD التي يتم إستخدامها لإجراء البحث عن DNS؟
ج: هو قابل للتكوين. عندما لا يتم تكوين أي واجهات، يتم تمكين جميع الواجهات المسماة على FTD للبحث عن DNS.

س: هل يقوم كل NGFW بدار بأداء تحليل DNS الخاص به وترجمة IP FQDN بشكل منفصل حتى عندما تطبق نفس نهج الوصول على كل منها باستخدام كائن FQDN نفسه؟
نعم.

س: هل يمكن مسح ذاكرة التخزين المؤقت ل DNS لقواعد التحكم في الوصول ل FQDN استكشاف الأخطاء وإصلاحها؟
أ: نعم، يمكنك تنفيذ أوامر مسح DNS ومسح ذاكرة التخزين المؤقت ل DNS-host على الجهاز.

س: متى يتم تشغيل دقة FQDN بالضبط؟
A: يحدث تحليل FQDN عند نشر كائن FQDN في سياسة التي ار المتردد.

س: هل يمكن تنظيف ذاكرة التخزين المؤقت لموقع واحد فقط؟
نعم. إذا كنت تعرف اسم المجال أو عنوان IP، فيمكنك مسحه، ولكن ال يوجد أمر مثل هذا لكل منظور قائمة التحكم في الوصول (ACL). على سبيل المثال، يتوفر الأمر clear dns host agni.tejas.com لمسح ذاكرة التخزين المؤقت على المضيف حسب أساس الكلمة الأساسية المضيف كما هو الحال في مضيف DNS agni.tejas.com.

س: هل من الممكن إستخدام أحرف البدل، مثل *.microsoft.com؟
أ: يجب أن يبدأ رقم FQDN وينتهي برقم أو حرف. يسمح فقط بالحروف والأرقام والوصلات كحروف داخلية.

س: هل يتم تحليل الاسم في وقت تجميع AC وليس في وقت الطلبات الأولى أو اللاحقة؟ إذا كان مدة البقاء (TTL) منخفضة (أقل من وقت تجميع التاي المتردد أو تدفق البيانات السريع أو أي شيء آخر)، هل يمكن فقد بعض عناوين IP؟
A: يحدث حل الاسم بمجرد نشر سياسة التاي المتردد. ويتبع ذلك انتهاء صلاحية مدة البقاء (TTL).

س: هل هناك خطط للتمكن من معالجة قائمة عناوين IP للسحابة (XML) الخاصة ب Microsoft Office 365؟
أ: هذا غير مدعوم في الوقت الحالي.

س: هل FQDN متوفر في نهج SSL؟
A: ليس في الوقت الحالي (الإصدار 6.3.0 من البرنامج). كائنات FQDN مدعومة فقط في شبكة المصدر والوجهة لنهج التاي المتردد فقط.

س: هل هناك أي سجلات تاريخية يمكن أن توفر معلومات حول FQDNs التي تم حلها؟ مثل LINA syslogs، على سبيل المثال.
أ: الاستكشاف أخطاء FQDN وإصلاحها إلى وجهة معينة، يمكنك إستخدام أمر تتبع دعم النظام. تظهر المسارات معرف FQDN للحزمة. يمكنك مقارنة المعرف الاستكشاف الأخطاء وإصلاحها. يمكنك أيضا تمكين رسائل syslog 746015، 746016 لتعقب نشاط تحليل DNS ل FQDN.

س: هل يقوم الجهاز بتسجيل FQDN في جدول الاتصالات مع IP الذي تم حله؟
a: الاستكشاف أخطاء FQDN وإصلاحها إلى وجهة معينة، يمكنك إستخدام الأمر دعم النظام trace، حيث تظهر المسارات معرف FQDN الخاص بالحزمة. يمكنك مقارنة المعرف الاستكشاف الأخطاء وإصلاحها. هناك خطط للحصول على سجلات FQDN في عارض الأحداث على FMC في المستقبل.

س: ما هي أوجه القصور في ميزة قاعدة FQDN؟

أ: التي تم تغيير الميزة إذا تم إستخدام قاعدة FQDN على وجهة تقوم بتغيير عنوان IP بشكل متكرر (على سبيل المثال: خوادم الإنترنت التي انتهت صلاحية مدة البقاء (TTL) لها صفر)، ويمكن لمحطات العمل أن يتنبأ بها المطاف إلى المتالك عنوان IP جديدة لم تعد تتوافق مع ذاكرة التخزين المؤقت ل DNS ل FTD. ونتيجة لذلك، فإنها لا تطابق قاعدة ACP. بشكل افتراضي، يضيف FTD دقيقة واحدة فوق انتهاء صلاحية TTL المستلمة من إستجابة DNS والتي يمكن تعيينها على صفر. في هذه الشروط، يوصى بشدة باستخدام ميزة تصفية URL التي تعد الأفضل لحالة الاستخدام هذه.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).