تكوين SNMP واستكشاف أخطائه وإصلاحها على FirePOWER FDM

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

ما الجديد في 6.7

التكوين

SNMP v3

SNMP v2c

إزالة تكوين SNMP

التحقق من الصحة

التحقق من SNMP v3

التحقق من SNMP v2c

استكشاف الأخطاء وإصلاحها

أسئلة وأجوبة

معلومات ذات صلة

المقدمة

يوضح هذا المستند كيفية تكوين بروتوكول إدارة الشبكة البسيط (SNMP) على الإصدار 6.7 من إدارة جهاز FirePOWER باستخدام واجهة برمجة تطبيقات REST.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الدفاع ضد تهديد Firepower (FTD) المدار من قبل FirePOWER Device Management (FDM)، الإصدار 6.7
- معرفة REST API
- معرفة SNMP

المكونات المستخدمة

الدفاع ضد تهديد Firepower تتم إدارته بواسطة FirePOWER Device Management، الإصدار 6.7.

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

6.7 وش الجديد على

يدعم FTD Device REST API تكوين وإدارة خادم SNMP والمستخدمين والمضيفين ومجموعات الأجهزة المضيفة. مع دعم واجهة برمجة التطبيقات لجهاز SNMP FTD في FP، الإصدار 6. 7:

- يمكن للمستخدم تكوين SNMP من خلال واجهة برمجة تطبيقات FTD REST API لإدارة الشبكة.
- يمكن إضافة/تحديث أو إدارة خادم SNMP والمستخدمين ومجموعات المضيفين/المضيفين من خلال واجهة برمجة تطبيقات REST لجهاز FTD.

تصف الأمثلة المضمنة في المستند خطوات التكوين التي تم إتخاذها بواسطة مستكشف واجهة برمجة التطبيقات (API) ل FDM.

ملاحظة: لا يمكن تكوين بروتوكول SNMP إلا من خلال واجهة برمجة تطبيقات REST عندما يقوم FTD بتشغيل الإصدار 6.7 وتتم إدارته بواسطة FDM.

نظرة عامة على الميزات - دعم واجهة برمجة التطبيقات (API) لواجهة برمجة التطبيقات (REST) لجهاز SNMP FTD

- تضيف هذه الميزة نقاط نهاية عنوان URL جديد ل FDM خاصة ب SNMP.
- يمكن إستخدام واجهات برمجة التطبيقات الجديدة هذه لتكوين SNMP لاستطلاعات الرأي والفخاخ لمراقبة الأنظمة.
- يتم توفير تكوين ما بعد بروتوكول SNMP عبر واجهات برمجة التطبيقات (API)، وقواعد معلومات الإدارة (MIB) على أجهزة FirePOWER، لعمليات الاقتراع أو إلخاطار الفحص على عميل NMS/SNMP.

نقاط نهاية SNMP API/URL

الطرز	الأساليب	URL
SNMPServer	إحضار	/devicesettings/default/snmpservers
SNMPServer	خذ، ضع	/devicesettings/default/snmpservers/{objId}
SNMPHost	الحصول على، إرسال	/object/snmphosts
SNMPHost	الحصول، حذف، وضع	/object/snmphosts/{objId}

	على	
/object/snmpusergroups	إرسال، الحصول على	SNMPUserGroup
/object/snmpuserGroups/{objId}	وضع، حذف، الحصول على	SNMPUserGroup
/object/snmpusers	إرسال، الحصول على	SNMPUser
/object/snmpusers/{objId}	وضع، حذف، الحصول على	SNMPUser

التكوين

يحتوي مضيف SNMP على 3 إصدارات أساسية:

1. SNMP v1
2. SNMP v2C
3. SNMP v3

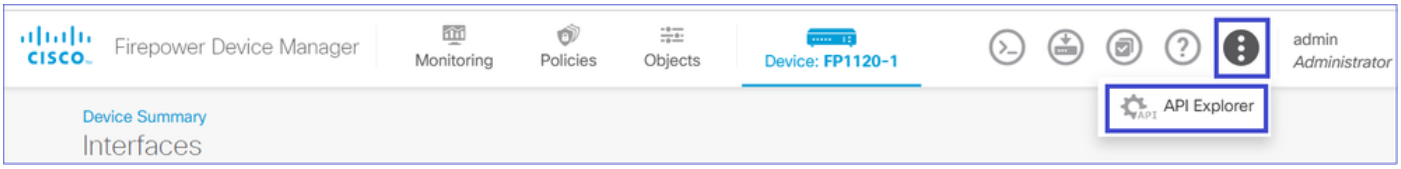
لكل واحد من هذه تنسيق خاص ل securityConfiguration. بالنسبة للإصداريين V1 و V2C: يحتوي على سلسلة مجتمع وحقل نوع يعرف التكوين بأنه V1 أو V2C.

بالنسبة ل SNMP v3: يحتوي على مستخدم SNMP v3 صالح وحقل نوع يعرف التكوين على أنه v3.

SNMP v3

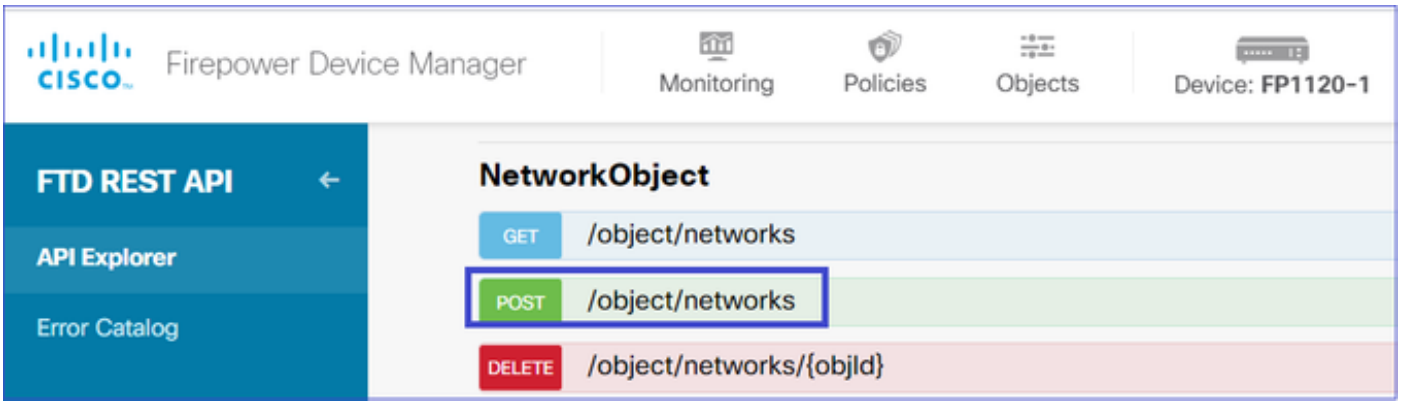
1. الوصول إلى مستكشف واجهة برمجة التطبيقات (API) ل FDM.

للوصول إلى مستكشف واجهة برمجة التطبيقات (API) ل FDM REST من واجهة المستخدم الرسومية (GUI) ل FDM، حدد النقاط الثلاث ثم مستكشف واجهة برمجة التطبيقات (API). بدلا من ذلك، انتقل إلى مستكشف واجهة برمجة تطبيقات URL.



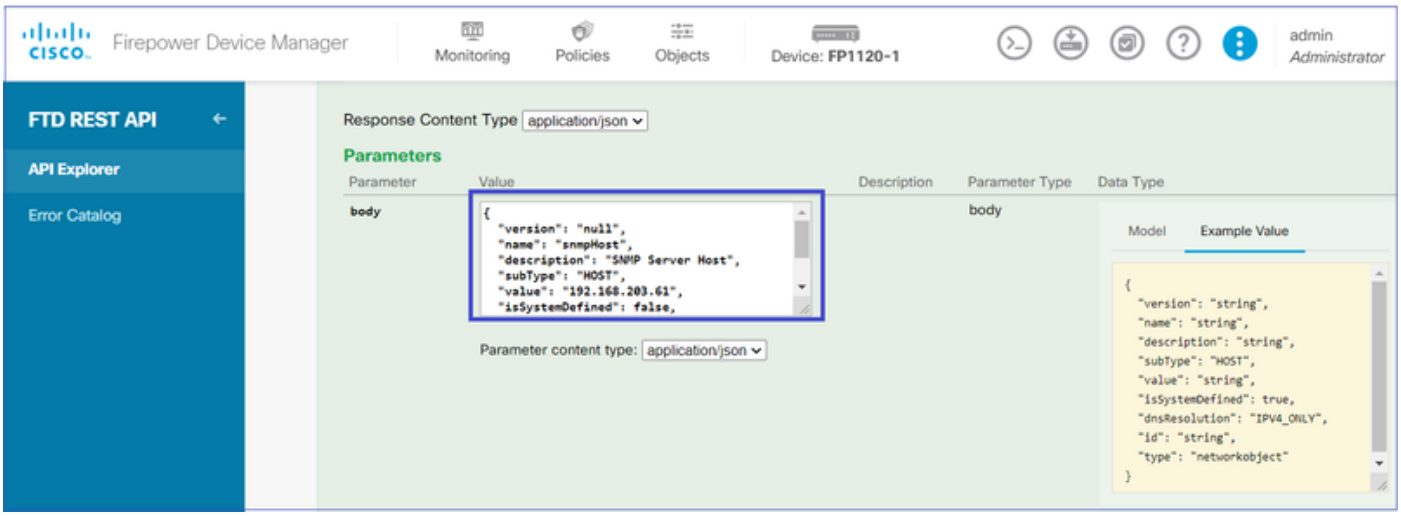
2. تكوين كائن الشبكة.

إنشاء كائن شبكة جديد لمضيف SNMP. في برنامج Explorer FDM API، حدد NetworkObject ثم قم بنشر/كائن/شبكات:



تنسيق JSON لمضيف SNMP وهو هذا. الصق JSON هذا في قسم النص الأساسي وتغيير عنوان IP على القيمة لمطابقة عنوان IP لمضيف SNMP:

```
{
"version": "null",
"name": "snmpHost",
"description": "SNMP Server Host",
"subType": "HOST",
"value": "192.168.203.61",
"isSystemDefined": false,
"dnsResolution": "IPV4_ONLY",
"type": "networkobject"
}
```

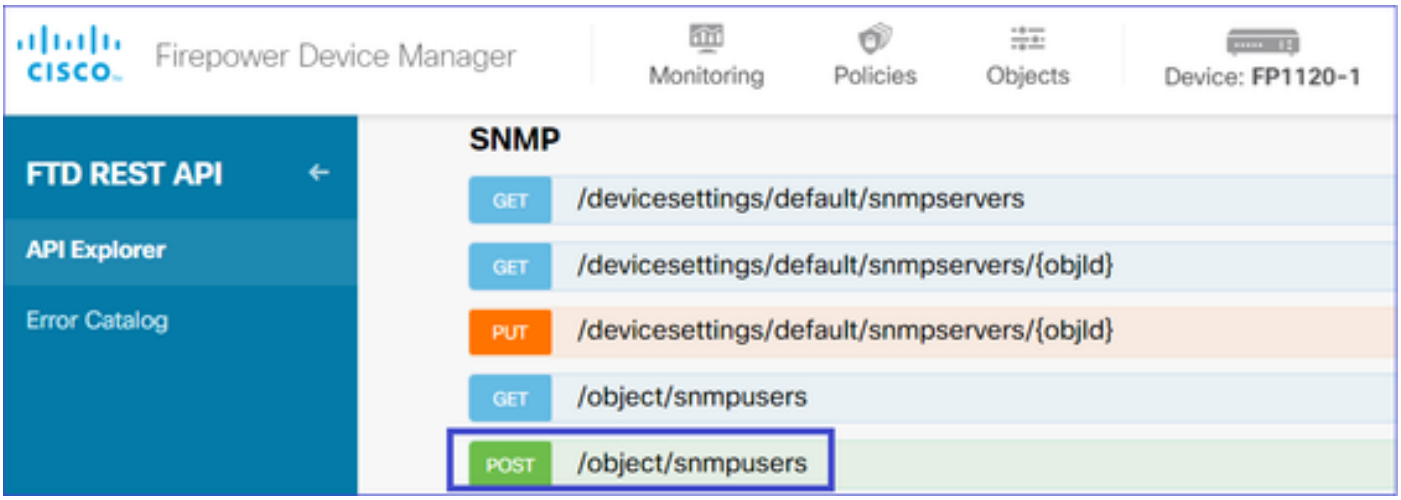


قم بالتمرير إلى أسفل وحدد الزر المحاولة! لتنفيذ إستدعاء واجهة برمجة التطبيقات (API). تقوم مكالمة ناجحة بإرجاع رمز الاستجابة 200.

انسخ بيانات JSON من جهة الاستجابة إلى دفتر ملاحظات. لاحقا، تحتاج إلى ملء المعلومات حول مضيف SNMP.

3. إنشاء مستخدم جديد للإصدار الثالث من بروتوكول إدارة الشبكة البسيط (SNMP).

في FDM API Explorer، حدد SNMP ثم قم بترحيل/كائن/snmpusers.

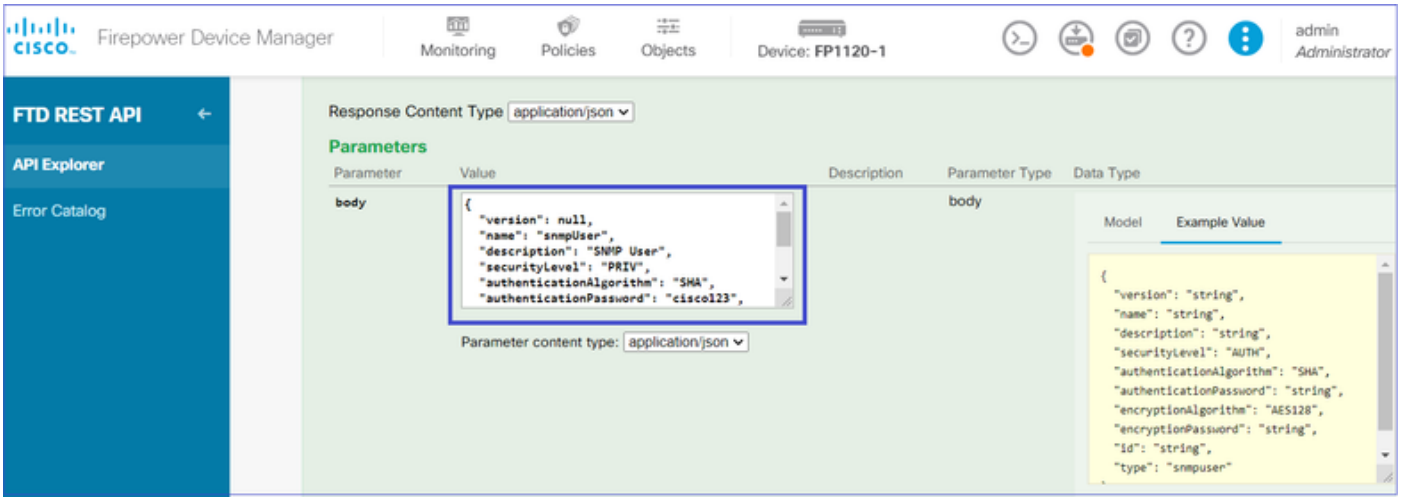


انسخ بيانات JSON هذه إلى مفكرة وقم بتعديل الأقسام التي يهمك (على سبيل المثال، authenticationPassword أو encryptionPassword أو الخوارزميات):

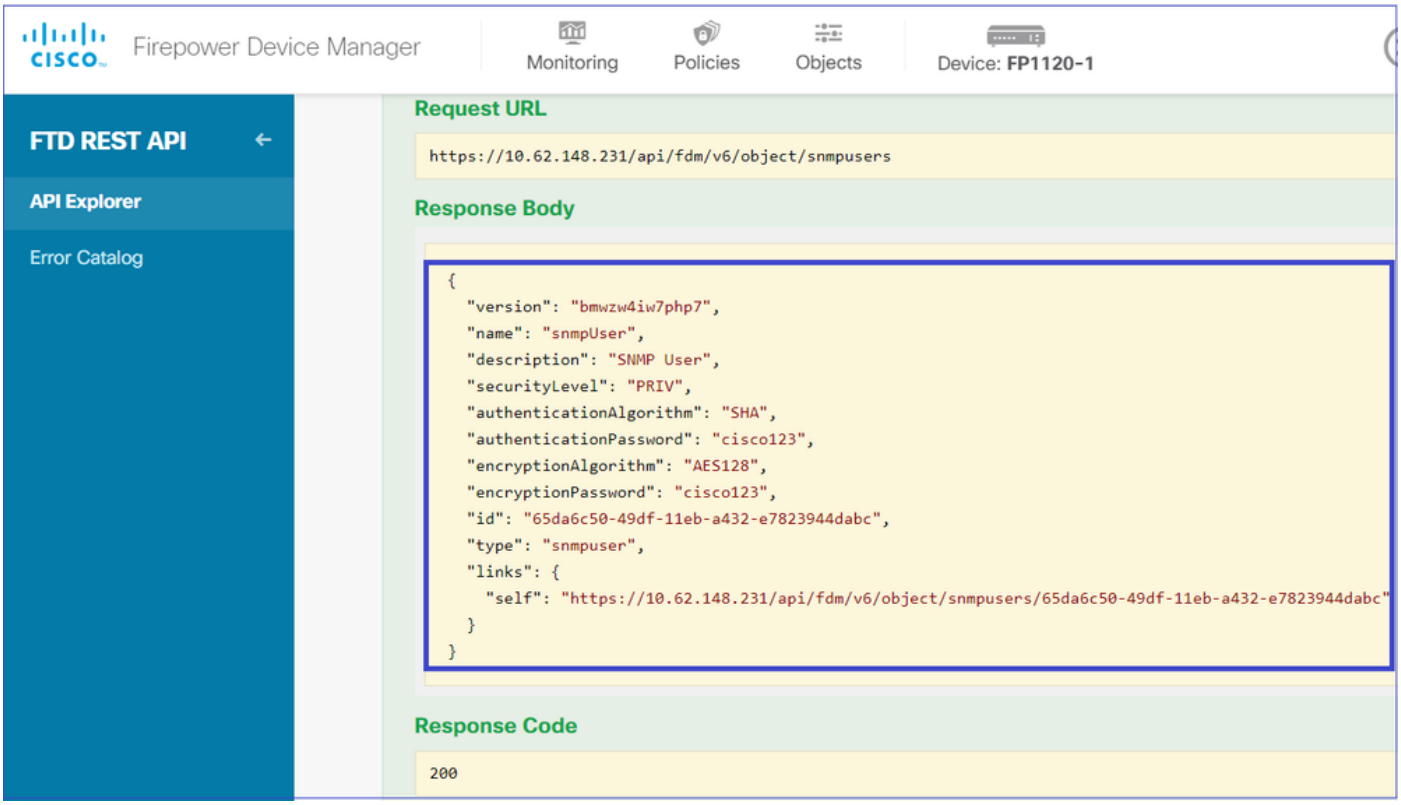
```
{
"version": null,
"name": "snmpUser",
"description": "SNMP User",
"securityLevel": "PRIV",
"authenticationAlgorithm": "SHA",
"authenticationPassword": "cisco123",
"encryptionAlgorithm": "AES128",
"encryptionPassword": "cisco123",
"id": null,
"type": "snmpuser"
}
```

⚠ تحذير: كلمات المرور المستخدمة في الأمثلة هي لأغراض العرض التوضيحي فقط. في بيئة إنتاج، تأكد من استخدام كلمات مرور قوية

انسخ بيانات JSON المعدلة إلى قسم النص الأساسي:

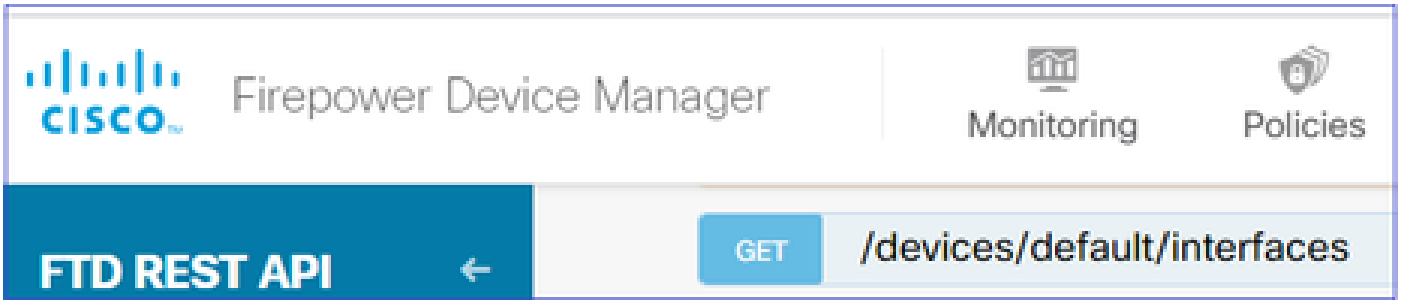


قم بالتمرير إلى أسفل وحدد الزر المحاولة! لتنفيذ استدعاء واجهة برمجة التطبيقات (API). تقوم المكالمة بإرجاع رمز الاستجابة 200. انسخ بيانات JSON من جهة الاستجابة إلى دفتر ملاحظات. لاحقا، تحتاج إلى علم المعلومات حول مستخدم SNMP.



4. احصل على معلومات الواجهة.

على مستكشف واجهة برمجة التطبيقات (API) ل FDM، حدد الواجهة ثم احصل على /الأجهزة/default/interfaces. تحتاج إلى تجميع المعلومات من الواجهة التي تتصل بخادم SNMP.



قم بالتمرير إلى أسفل وحدد الزر المحاولة! لتنفيذ استدعاء واجهة برمجة التطبيقات (API). تقوم المكالمة بإرجاع رمز الاستجابة 200. انسخ بيانات JSON من جهة الاستجابة إلى دفتر ملاحظات. لاحقا، تحتاج إلى تعبئة معلومات حول الواجهة.

تذكر إصدار الواجهة والاسم والمعرف والنوع من بيانات JSON. مثال على بيانات JSON من الواجهة الداخلية:

<#root>


```
 {
"version": "kkpkibjlu6qro",
"name": "inside",
"description": null,
"hardwareName": "Ethernet1/2",
"monitorInterface": true,
"ipv4": {
"ipType": "STATIC",
"defaultRouteUsingDHCP": false,
"dhcpRouteMetric": null,
"ipAddress": {
"ipAddress": "192.168.203.71",
"netmask": "255.255.255.0",
"standbyIpAddress": null,
"type": "haipv4address"
},
"dhcp": false,
"addressNull": false,
"type": "interfaceipv4"
},
"ipv6": {
```

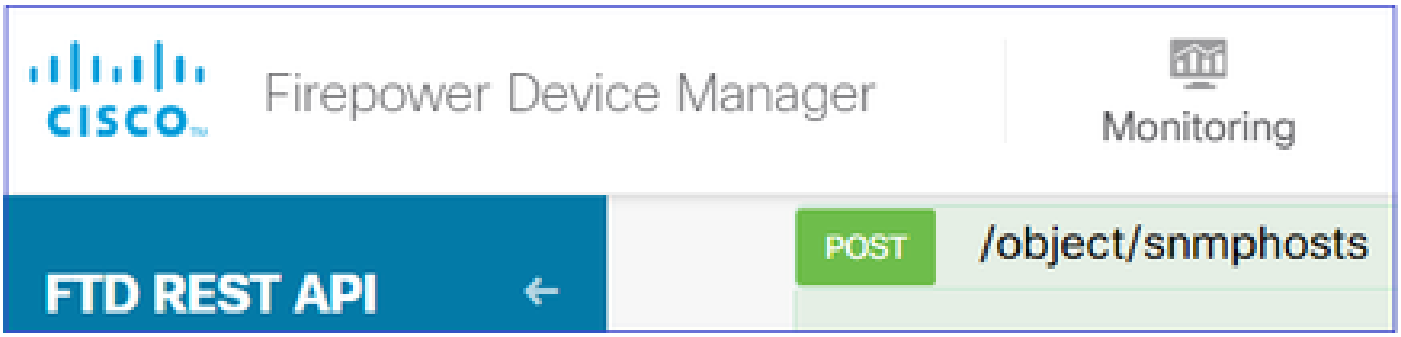
```
"enabled": false,
"autoConfig": false,
"dhcpForManagedConfig": false,
"dhcpForOtherConfig": false,
"enableRA": false,
"dadAttempts": 1,
"linkLocalAddress": {
"ipAddress": "",
"standbyIpAddress": "",
"type": "haipv6address"
},
"ipAddresses": [
{
"ipAddress": "",
"standbyIpAddress": "",
"type": "haipv6address"
}
],
"prefixes": null,
"type": "interfaceipv6"
},
"managementOnly": false,
"managementInterface": false,
"mode": "ROUTED",
"linkState": "UP",
"mtu": 1500,
"enabled": true,
"macAddress": null,
"standbyMacAddress": null,
"pppoe": null,
"speedType": "AUTO",
"duplexType": "AUTO",
"present": true,
"tenGigabitInterface": false,
"gigabitInterface": false,


"id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",




"type": "physicalinterface",


"links": {
"self": "https://10.62.148.231/api/fdm/v6/devices/default/interfaces/fc3d07d4-49d2-11eb-85a8-65aec636a0
}
},
```


من بيانات JSON، يمكنك رؤية الواجهة في الداخل تحتوي على البيانات التي يلزم اقترانها بخادم SNMP:

- الإصدار: kkpkibjlu6qro
- الاسم: داخل، iid: fc3d07d4-49d2-11eb-85a8-65aec636a0fc،
- النوع: الواجهة الفيزيائية،

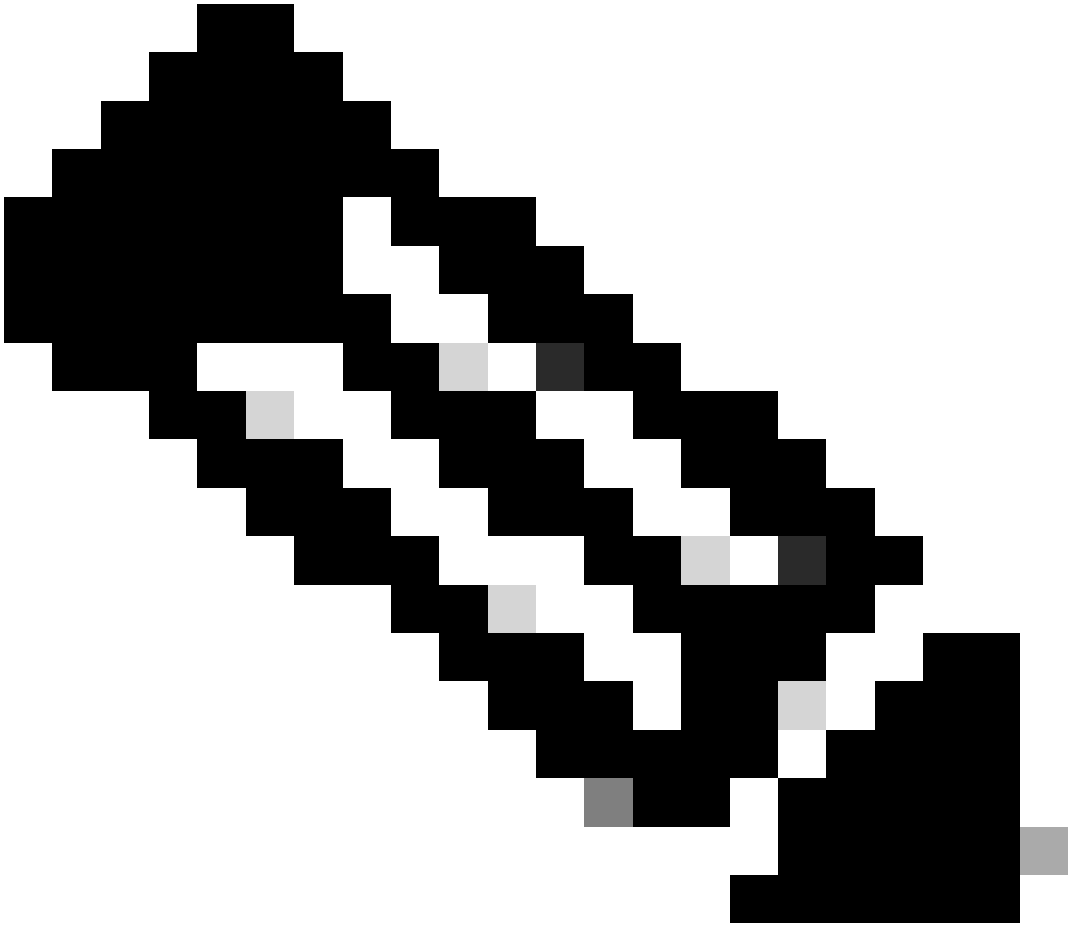
5. إنشاء مضيف SNMPv3 جديد.

في "مستكشف واجهة برمجة التطبيقات (API) ل FDM"، حدد SNMP ثم ترحيل/كائن/SNMPhosts/ أسفل SNMP.



أستخدم JSON هذا كقالب. نسخ ولصق البيانات من الخطوات السابقة إلى القالب وفقا لذلك:

```
{
"version": null,
"name": "snmpv3-host",
"description": null,
"managerAddress": {
"version": "bsha3bhghu3vmk",
"name": "snmpHost",
"id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
"type": "networkobject"
},
"pollEnabled": true,
"trapEnabled": true,
"securityConfiguration": {
"authentication": {
"version": "bmwzw4iw7php7",
"name": "snmpUser",
"id": "65da6c50-49df-11eb-a432-e7823944dabc",
"type": "snmpuser"
},
"type": "snmpv3securityconfiguration"
},
"interface": {
"version": "kkpkibjlu6qro",
"name": "inside",
"id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
"type": "physicalinterface"
},
"id": null,
"type": "snmphost"
}
```

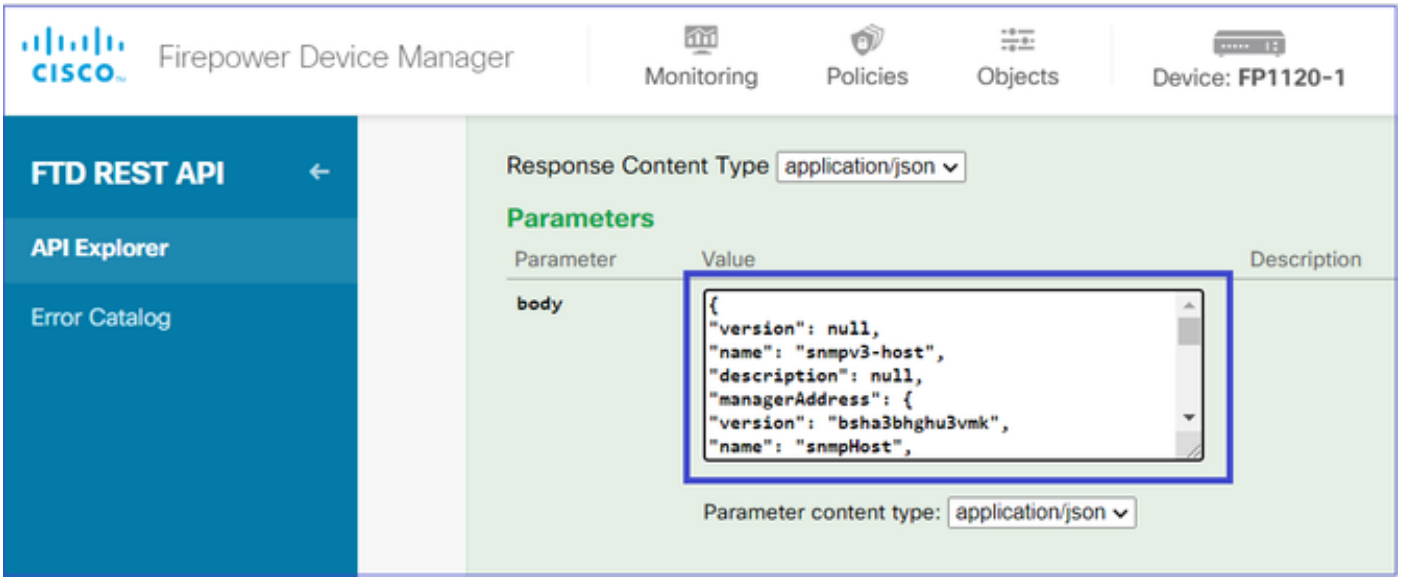


ملاحظة:

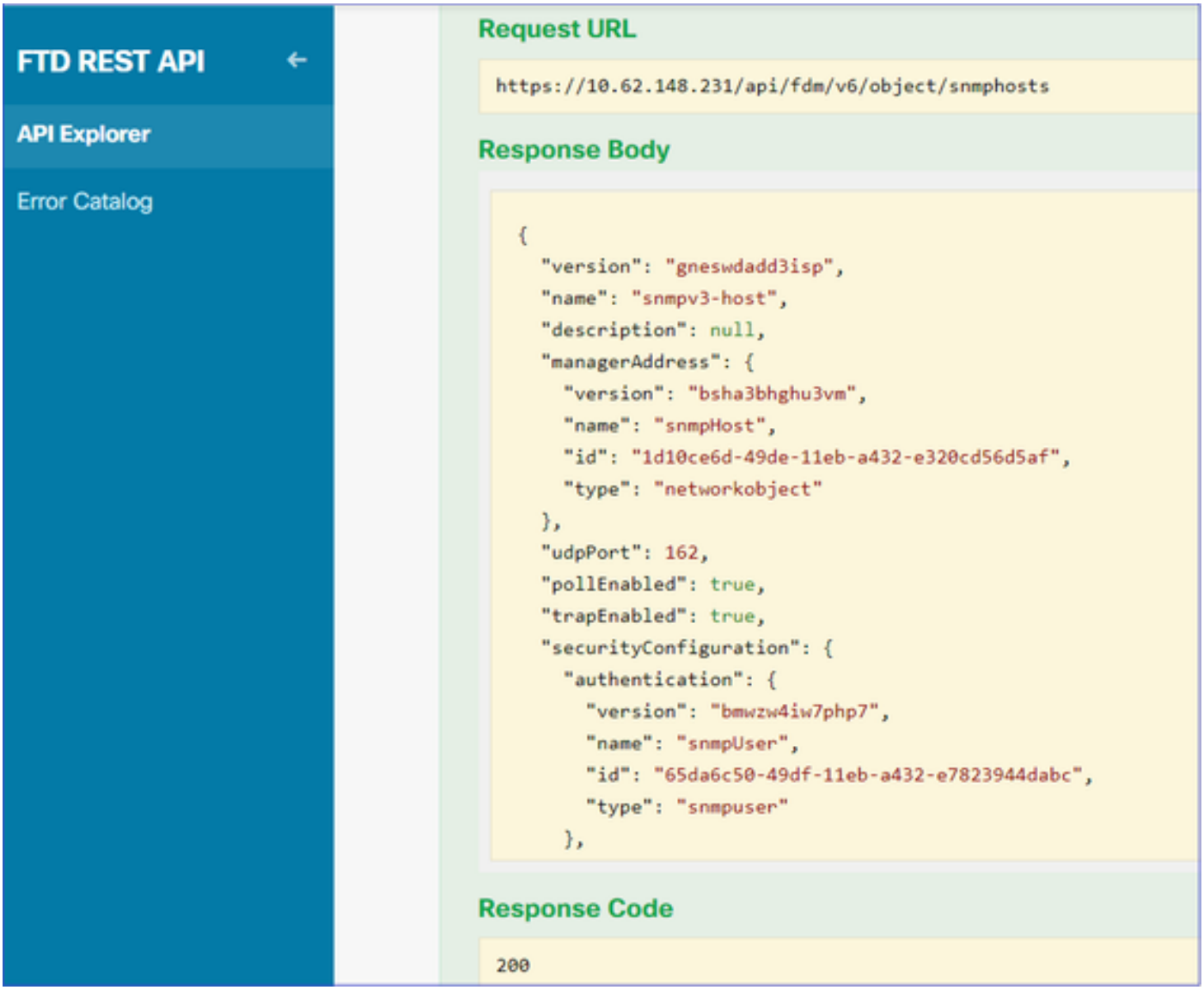
- استبدل القيمة في معرف ManagerAddress والنوع والإصدار والاسم بالمعلومات التي إستلمتها من الخطوة 1.
- استبدل القيمة في المصادقة بالمعلومات التي إستلمتها من الخطوة 2.
- استبدل القيمة في الواجهة بالبيانات التي إستلمتها من الخطوة 3.

بالنسبة لبروتوكول SNMP2، إذا لم توجد مصادقة، والنوع هو snmpV2csecurityConfiguration بدلا من snmpv3securityConfiguration.

انسخ بيانات JSON المعدلة إلى قسم النص الأساسي.

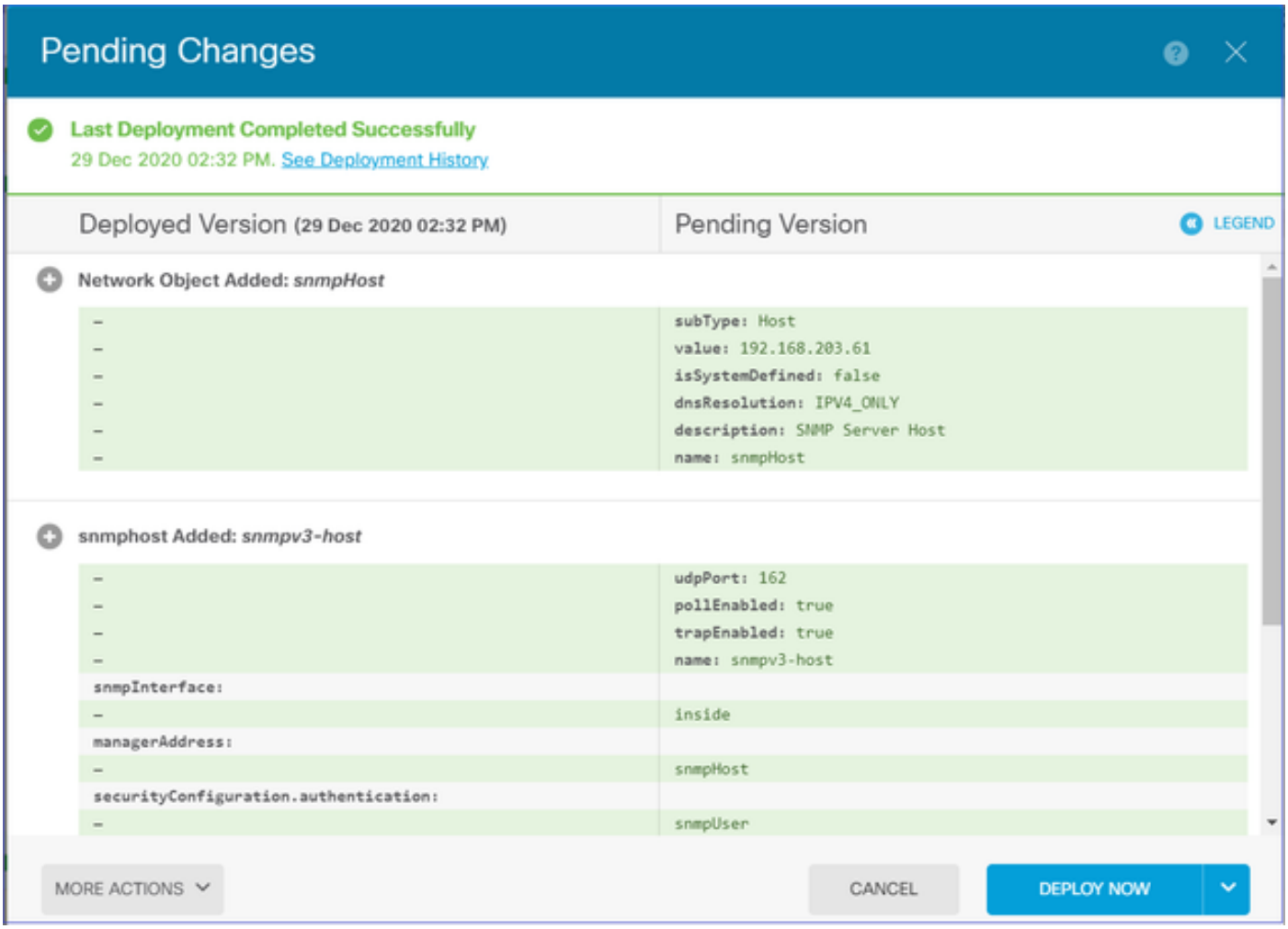


قم بالتمرير إلى أسفل وحدد الزر المحاولة! لتنفيذ إستدعاء واجهة برمجة التطبيقات (API). تقوم مكالمة ناجحة بإرجاع رمز الاستجابة 200.



انتقل إلى واجهة المستخدم الرسومية (GUI) ل FDM ونشر التغييرات. يمكنك الاطلاع على

تكوين SNMP معظم:



SNMP v2c

بالنسبة ل v2c ال تحتاج إلى إنشاء مستخدم ولكن ال تزال بحاجة إلى:

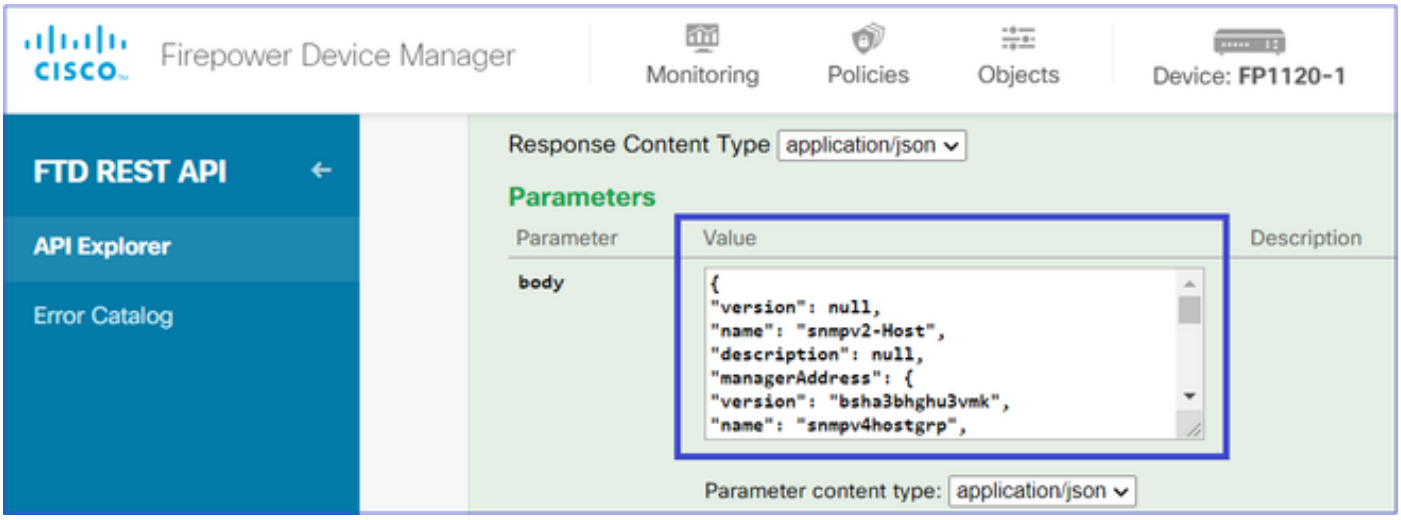
1. إنشاء تكوين كائن شبكة (مثل الموصوف في قسم SNMPv3)
2. الحصول على معلومات الواجهة (كما هو موضح في قسم SNMPv3)
3. إنشاء كائن مضيف SNMPv2c جديد

هذه عينة من حمولة JSON التي تنشئ كائن SNMPv2c:

```
{
"version": null,
"name": "snmpv2-Host",
"description": null,
"managerAddress": {
"version": "bsha3bhghu3vmk",
"name": "snmpv4hostgrp",
"id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
"type": "networkobject"
},
"pollEnabled": true,
"trapEnabled": true,
"securityConfiguration": {
```

```
"community": "cisco123",
"type": "snmpv2csecurityconfiguration"
},
"interface": {
"version": "kkpkibjlu6qro",
"name": "inside",
"id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
"type": "physicalinterface"
},
"id": null,
"type": "snmphost"
}
```

أستخدم أسلوب POST لنشر حمولة JSON:

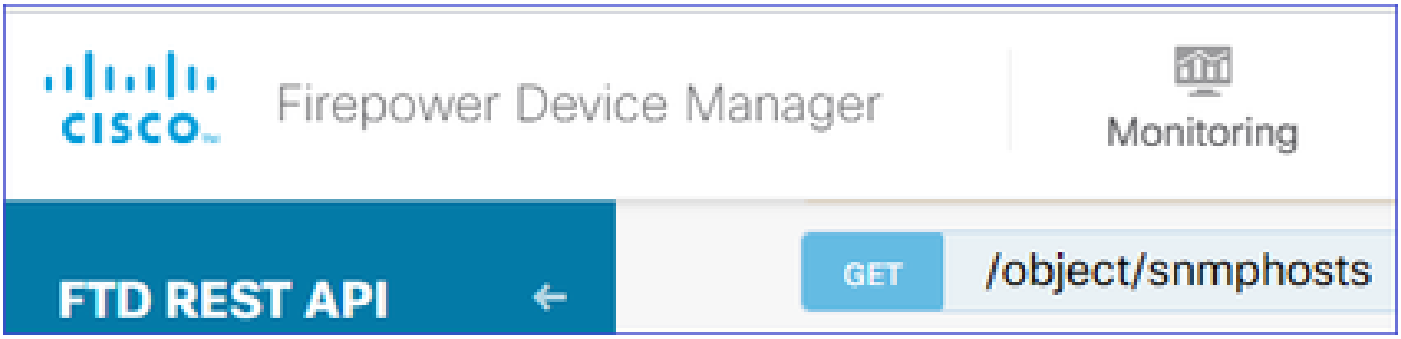


قم بالتمرير إلى أسفل وحدد الزر "تجربة الخروج"! لتنفيذ إستدعاء واجهة برمجة التطبيقات (API). تقوم مكالمة ناجحة بإرجاع رمز الاستجابة 200.

إزالة تكوين SNMP

الخطوة 1.

الحصول على معلومات مضيف SNMP (SNMP > /object/snmpHost):



قم بالتمرير إلى أسفل وحدد الزر "تجربة الخروج"! لتنفيذ إستدعاء واجهة برمجة التطبيقات (API). تقوم مكالمة ناجحة بإرجاع رمز الاستجابة 200.

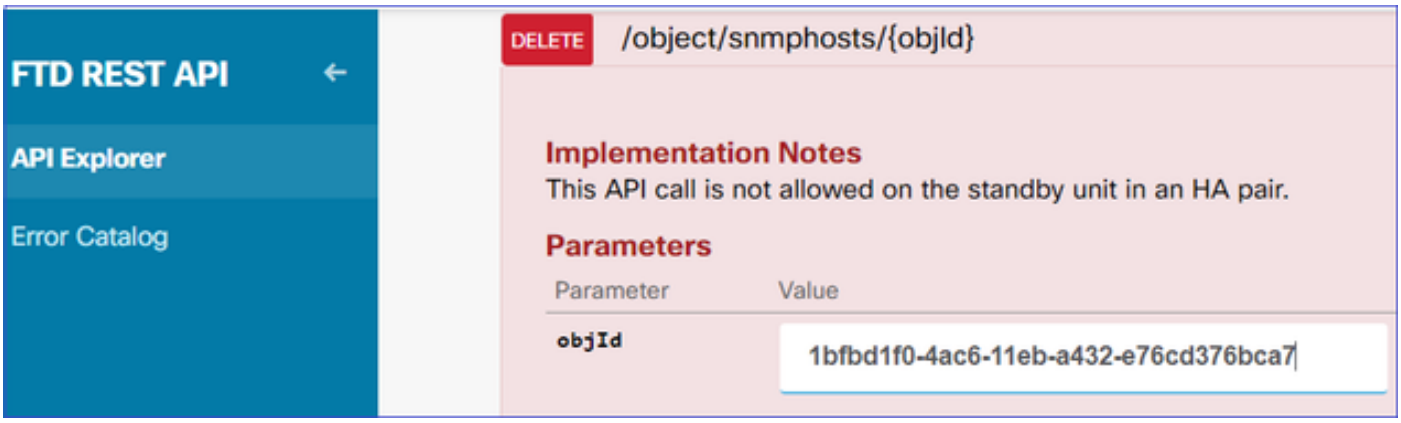
تحصل على قائمة بالكائنات. لاحظ معرف الكائن snmphost الذي تريد إزالته:

```
{
"items": [
{
"version": "ofaasthu26ulx",
"name": "snmpv2-Host",
"description": null,
"managerAddress": {
```

```
"version": "bsha3bhghu3vm",
"name": "snmpHost",
"id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
"type": "networkobject"
},
"udpPort": 162,
"pollEnabled": true,
"trapEnabled": true,
"securityConfiguration": {
"community": "**********",
"type": "snmpv2csecurityconfiguration"
},
"interface": {
"version": "kkpkibjlu6qro",¬
"name": "inside",
"hardwareName": "Ethernet1/2",
"id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
"type": "physicalinterface"
},
"id": "1bfbd1f0-4ac6-11eb-a432-e76cd376bca7",
"type": "snmphost",
"links": {
"self": "https://10.62.148.231/api/fdm/v6/object/snmphosts/1bfbd1f0-4ac6-11eb-a432-e76cd376bca7"
}
},
```


الخطوة 2.

أختر خيار الحذف في SNMP > /object/snmphost{objId}. الصق المعرف الذي جمعته في الخطوة 1:



قم بالتمرير إلى أسفل وحدد الزر "تجربة الخروج"! لتنفيذ إستدعاء واجهة برمجة التطبيقات (API). ترجع المكالمة رمز الاستجابة 400.

Response Code

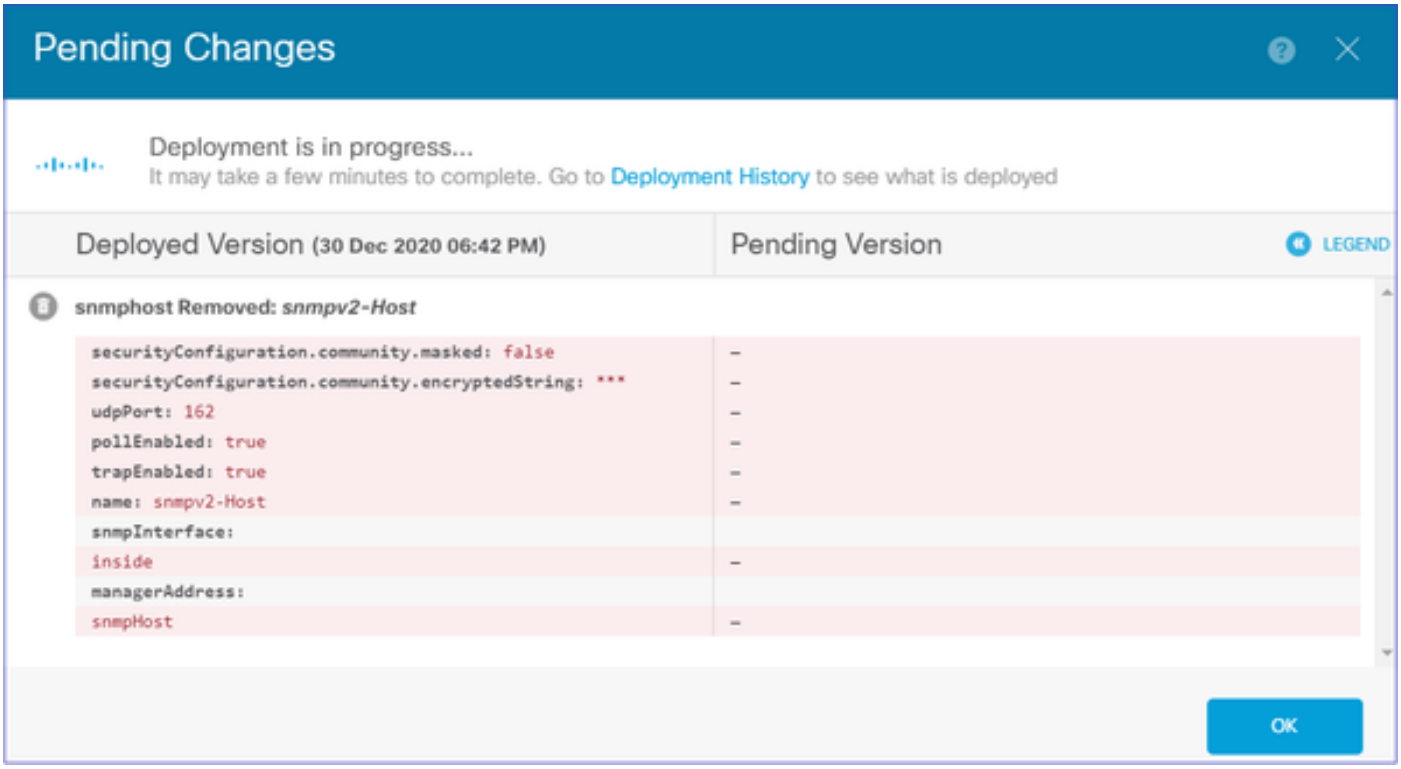
400

Response Headers


```
{
  "accept-ranges": "bytes",
  "cache-control": "no-cache, no-store",
  "connection": "close",
  "content-type": "application/json;charset=UTF-8",
  "date": "Wed, 30 Dec 2020 18:00:41 GMT",
  "expires": "0",
  "pragma": "no-cache",
  "server": "Apache",
  "strict-transport-security": "max-age=63072000; includeSubdomains; preload, max-age=31536000 ; includeSubDomains",
  "transfer-encoding": "chunked",
  "x-content-type-options": "nosniff",
  "x-frame-options": "SAMEORIGIN, SAMEORIGIN",
  "x-xss-protection": "1; mode=block"
}
```


الخطوة 3.

نشر التغيير:



يعمل النشر على إزالة معلومات المضيف:

<#root>

FP1120-1#

show run snmp-server

```
snmp-server group AUTH v3 auth
snmp-server group PRIV v3 priv
snmp-server group NOAUTH v3 noauth
snmp-server location null
```

```
snmp-server contact null
snmp-server community *****
```

فشل SNMPwalk ل v2c:

<#root>

```
root@kali2:~#
```

snmpwalk -v2c -c cisco123 -OS 192.168.203.71

```
Timeout: No Response from 192.168.203.71
```

بالنسبة للإصدار 3، يجب حذف الكائنات بهذا الترتيب.

1. مضيف SNMP (رمز الإرجاع الناجح هو 204)
2. مستخدم بروتوكول SNMP (رمز الإرجاع الناجح هو 204)

إذا حاولت حذف الكائنات بالترتيب الخاطئ، تحصل على هذا الخطأ:

```
{
"error": {
"severity": "ERROR",
"key": "Validation",
"messages": [
{
"description": "You cannot delete the object because it contains SNMPHost: snmpv3-host2, SNMPHost: snmp
You must remove the object from all parts of the configuration before you can delete it.",
"code": "deleteObjWithRel",
"location": ""
}
]
}
}
```

التحقق من الصحة

التحقق من SNMP v3

بعد النشر، انتقل إلى واجهة سطر الأوامر (CLI) الخاصة ب FTD للتحقق من تكوين SNMP.
الحظ أنه تم إنشاء قيمة engineID تلقائيا.

<#root>

```
FP1120-1#
```

```
connect ftd


>
system support diagnostic-cli


Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

FP1120-1>
enable


Password:
FP1120-1#
show run all snmp-server


snmp-server group AUTH v3 auth
snmp-server group PRIV v3 priv
snmp-server group NOAUTH v3 noauth
snmp-server user snmpUser PRIV v3 engineID 80000009febdf0129a799ef469aba2d5fcf1bfd7e86135a1f8 encrypted
snmp-server listen-port 161
snmp-server host inside 192.168.203.61 version 3 snmpUser udp-port 162
snmp-server location null
snmp-server contact null
snmp-server community *****
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
no snmp-server enable traps syslog
no snmp-server enable traps ipsec start stop
no snmp-server enable traps entity config-change fru-insert fru-remove fan-failure power-supply power-s
no snmp-server enable traps memory-threshold
no snmp-server enable traps interface-threshold
no snmp-server enable traps remote-access session-threshold-exceeded
no snmp-server enable traps connection-limit-reached
no snmp-server enable traps cpu threshold rising
no snmp-server enable traps ikev2 start stop
no snmp-server enable traps nat packet-discard
no snmp-server enable traps config
no snmp-server enable traps failover-state
no snmp-server enable traps cluster-state
snmp-server enable oid mempool
snmp-server enable
```

اختبار سير شرعي

```
root@kali2:~# snmpwalk -v3 -l authPriv -u snmpUser -a SHA -A cisco123 -x AES -X cisco123 192.168.203.71
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Firepower Threat Defense, Version 6.7.0 (Build 65), ASA Version 9.
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.2663
iso.3.6.1.2.1.1.3.0 = Timeticks: (1616700) 4:29:27.00
iso.3.6.1.2.1.1.4.0 = STRING: "null"
iso.3.6.1.2.1.1.5.0 = STRING: "FP1120-1"
iso.3.6.1.2.1.1.6.0 = STRING: "null"
iso.3.6.1.2.1.1.7.0 = INTEGER: 4
...
```

التحقق من SNMP v2c

```
FP1120-1# show run snmp-server
snmp-server host inside 192.168.203.61 community ***** version 2c
snmp-server location null
snmp-server contact null
snmp-server community *****
```

SnmpWalk ل v2c:

```
root@kali2:~# snmpwalk -v2c -c cisco123 -OS 192.168.203.71
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Firepower Threat Defense, Version 6.7.0 (Build 65), ASA Version 9.
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.2663
iso.3.6.1.2.1.1.3.0 = Timeticks: (10482200) 1 day, 5:07:02.00
iso.3.6.1.2.1.1.4.0 = STRING: "null"
iso.3.6.1.2.1.1.5.0 = STRING: "FP1120-1"
iso.3.6.1.2.1.1.6.0 = STRING: "null"
iso.3.6.1.2.1.1.7.0 = INTEGER: 4
```

استكشاف الأخطاء وإصلاحها

تمكين الالتقاط باتتبع على جدار الحماية:

```
<#root>

FP1120-1#

capture CAPI trace interface inside match udp any any eq snmp
```

أستخدم أداة التنقل البسيط وتحقق من قدرتك على رؤية الحزم:

```
<#root>

FP1120-1#

show capture

capture CAPI type raw-data trace interface inside

[Capturing - 3137 bytes]

  match udp any any eq snmp
```

محتويات الالتقاط:

```
<#root>

FP1120-1#

show capture CAPI



154 packets captured

   1: 17:04:16.720131       192.168.203.61.51308 > 192.168.203.71.161:  udp 39
   2: 17:04:16.722252       192.168.203.71.161 > 192.168.203.61.51308:  udp 119
   3: 17:04:16.722679       192.168.203.61.51308 > 192.168.203.71.161:  udp 42
   4: 17:04:16.756400       192.168.203.71.161 > 192.168.203.61.51308:  udp 51
   5: 17:04:16.756918       192.168.203.61.51308 > 192.168.203.71.161:  udp 42
```

تحقق من أن عدادات إحصائيات خادم SNMP تظهر طلبات واستجابات SNMP الحصول على طلبات واستجابات SNMP أو الحصول على تالي:

```
<#root>

FP1120-1#

show snmp-server statistics



62



SNMP packets input


0 Bad SNMP version errors
0 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors

58 Number of requested variables


0 Number of altered variables
0 Get-request PDUs

58 Get-next PDUs


0 Get-bulk PDUs
0 Set-request PDUs (Not supported)

58 SNMP packets output


0 Too big errors (Maximum packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
```

58 Response PDUs

0 Trap PDUs

تتبع حزمة مدخل. الربط un-nat إلى الداخلي NLP قارن:

<#root>

FP1120-1#

show capture CAPI packet-number 1 trace

30 packets captured

1: 17:04:16.720131 192.168.203.61.51308 > 192.168.203.71.

161

: udp 39
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: UN-NAT

Subtype: static
Result: ALLOW
Config:
Additional Information:
NAT divert to egress interface nlp_int_tap(vrfid:0)

Untranslate 192.168.203.71/161 to 169.254.1.3/4161

Phase: 4
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1078, packet dispatched to next module

Phase: 10
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:

Found next-hop 169.254.1.3 using egress ifc nlp_int_tap(vrfid:0)

Phase: 11
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
Found adjacency entry for Next-hop 169.254.1.3 on interface nlp_int_tap
Adjacency :Active
MAC address 3208.e2f2.b5f9 hits 0 reference 1

Result:

input-interface: inside(vrfid:0)

```
input-status: up
input-line-status: up
```

output-interface: nlp_int_tap(vrfid:0)

```
output-status: up
output-line-status: up
```

Action: allow

يتم نشر قاعدة NAT تلقائيا كجزء من تكوين SNMP:

<#root>

FP1120-1#

show nat

```
Manual NAT Policies (Section 1)
1 (nlp_int_tap) to (inside) source dynamic nlp_client_0_192.168.203.61_intf4 interface destination stat
translate_hits = 0, untranslate_hits = 0

Auto NAT Policies (Section 2)
…
```

2 (nlp_int_tap) to (inside) source static nlp_server_0_snmp_intf4 interface service udp 4161 snmp

translate_hits = 0, untranslate_hits = 2

في المنفذ الخلفي، يستمع UDP 4161 لحركة مرور SNMP:

<#root>

>

expert

```
admin@FP1120-1:~$
```

sudo netstat -an | grep 4161

```
Password:
udp 0 0 169.254.1.3:4161 0.0.0.0:*
udp6 0 0 fd00:0:0:1::3:4161 :::*
```

في حالة التكوين غير الصحيح/غير الكامل، يتم إسقاط حزمة SNMP الخاصة بالمدخل نظرا لعدم وجود مرحلة unnat:

<#root>

FP1120-1#

show cap CAPI packet-number 1 trace

6 packets captured

1: 18:36:35.868485 192.168.203.61.50105 > 192.168.203.71.

161

: udp 42
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: No ECMP load balancing
Result: ALLOW
Config:
Additional Information:
Destination is locally connected. No ECMP load balancing.

Found next-hop 192.168.203.71 using egress ifc identity(vrfid:0)

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5

Type: ACCESS-LIST

Subtype:

Result: DROP

Config:
Implicit Rule
Additional Information:

```
Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
Action: drop

Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x0000557415b6347d flow
```

يظهر FTD LINA syslogs أن المدخل ربط مهمل:

```
<#root>

FP1120-1#

show log | include 161


Dec 30 2020 18:36:38: %FTD-7-710005: UDP request discarded from 192.168.203.61/50105 to inside:192.168.
Dec 30 2020 18:36:39: %FTD-7-710005: UDP request discarded from 192.168.203.61/50105 to inside:192.168.
```

أسئلة وأجوبة

س. هل يمكنني إستخدام واجهة إدارة FTD لإرسال رسائل SNMP؟

ال، هذا غير مدعوم حاليا.

عيب التحسين ذو الصلة: [دعم واجهة برمجة التطبيقات (API) لبروتوكول SNMP لحركة المرور لواجهة NGFW-MGMT](#)

معلومات ذات صلة

- [دليل تكوين Firepower Threat Defense من Cisco لإدارة أجهزة Firepower، الإصدار 6.7](#)
- [دليل واجهة برمجة تطبيقات الدفاع عن تهديد Cisco Firepower](#)
- [ملاحظات إصدار Cisco Firepower، الإصدار 6.7.0](#)

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).