SNMP auf FirePOWER FDM konfigurieren und Fehlerbehebung dafür durchführen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie das Simple Network Management Protocol (SNMP) für das FirePOWER-Gerätemanagement in Version 6.7 mit der REST-API aktiviert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Firepower Threat Defense (FTD) verwaltet durch Firepower Device Management (FDM) auf Version 6.7
- Kenntnisse der REST-API
- SNMP-Kenntnisse

Verwendete Komponenten

Firepower Threat Defense (FTD) verwaltet durch Firepower Device Management (FDM) auf Version 6.7.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Neuerungen bei 6.7

Die REST-API für FTD-Geräte unterstützt die Konfiguration und Verwaltung von SNMP-Servern, Benutzern, Hosts und Hostgruppen. Mit der Unterstützung der SNMP FTD Device REST API in FP 6.7:

- Ein Benutzer kann SNMP über die REST-API des FTD-Geräts konfigurieren, um das Netzwerk zu verwalten.
- SNMP-Server, Benutzer und Host-/Hostgruppen können über die REST-API für FTD-Geräte hinzugefügt, aktualisiert oder verwaltet werden.

In den im Dokument enthaltenen Beispielen werden die Konfigurationsschritte des FDM-API-Explorers beschrieben.

Hinweis: SNMP kann nur über die REST-API konfiguriert werden, wenn FTD Version 6.7 ausführt und von FDM verwaltet wird.

Funktionsübersicht - Unterstützung der REST-API für SNMP FTD-Geräte

- Mit dieser Funktion werden neue SNMP-spezifische FDM-URL-Endpunkte hinzugefügt.
- Diese neuen APIs können verwendet werden, um SNMP für Abfragen und Traps zur Überwachung von Systemen zu konfigurieren.
- Die SNMP-Konfiguration über APIs bereitstellen, stehen die Management Information Bases (MIBs) auf den FirePOWER-Geräten für Abfragen oder Trap-Benachrichtigungen auf dem NMS/SNMP-Client zur Verfügung.

SNMP-API/URL-Endpunkte

URL	**Methoden**	**Modelle**
/devicesettings/default/snmpservers	HOLEN	SNMPServer
/devicesettings/default/snmpservers/{objId}	PUT, GET	SNMPServer
/object/snmphosts	POST, LOS	SNMPHost
/object/snmphosts/{objId}	PUT, DELETE, GET	SNMPHost
/object/snmpusergroups	POST, LOS	SNMPUserGruppe
/object/snmpusergroups/{objId}	PUT, DELETE, GET	SNMPUserGruppe
/object/snmpusers	POST, LOS	SNMPUser
/object/snmpusers/{objId}	PUT, DELETE, GET	SNMPUser

Konfigurieren

- Der SNMP-Host verfügt über drei primäre Versionen

- SNMP V1

- SNMP V2C

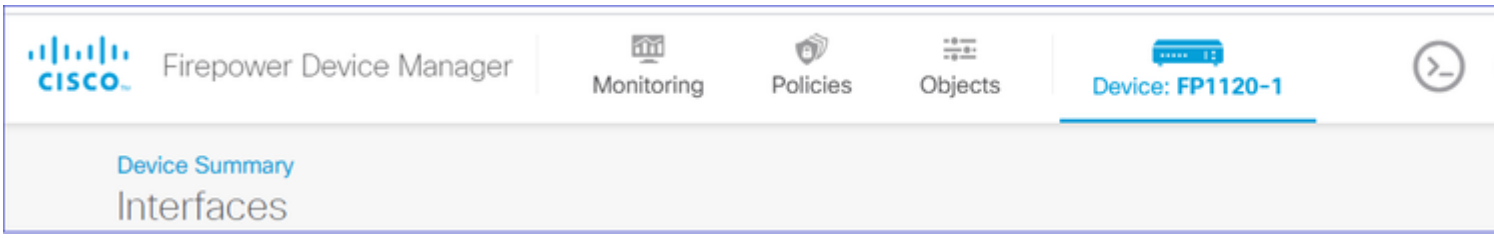
- SNMP V3

- Jede dieser Konfigurationen hat ein spezielles Format für "securityConfiguration".
- Für V1 und V2C: Es enthält ein "Community String"- und ein "type"-Feld, das die Konfiguration als V1 oder V2C identifiziert.
- Für SNMP V3: Enthält einen gültigen SNMP V3-Benutzer und ein "Typ"-Feld, das die Konfiguration als V3 identifiziert.

SNMP v3

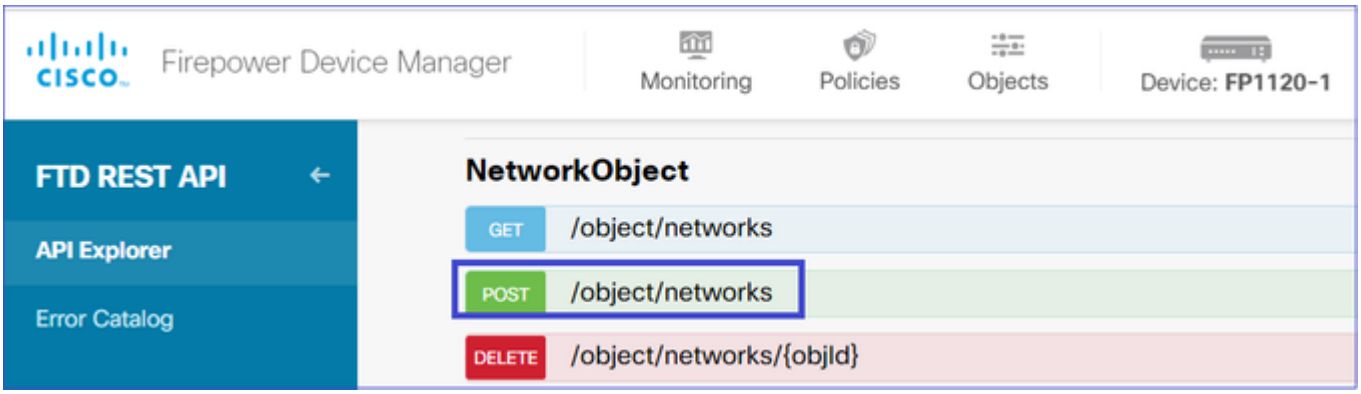
1. Zugriff auf den FDM API Explorer

Um über die FDM-GUI auf den FDM-REST-API-Explorer zuzugreifen, wählen Sie die drei Punkte und anschließend den **API-Explorer aus**. Oder navigieren Sie zur URL https://FDM_IP/#/api-explorer:



2. Konfiguration des Netzwerkobjekts

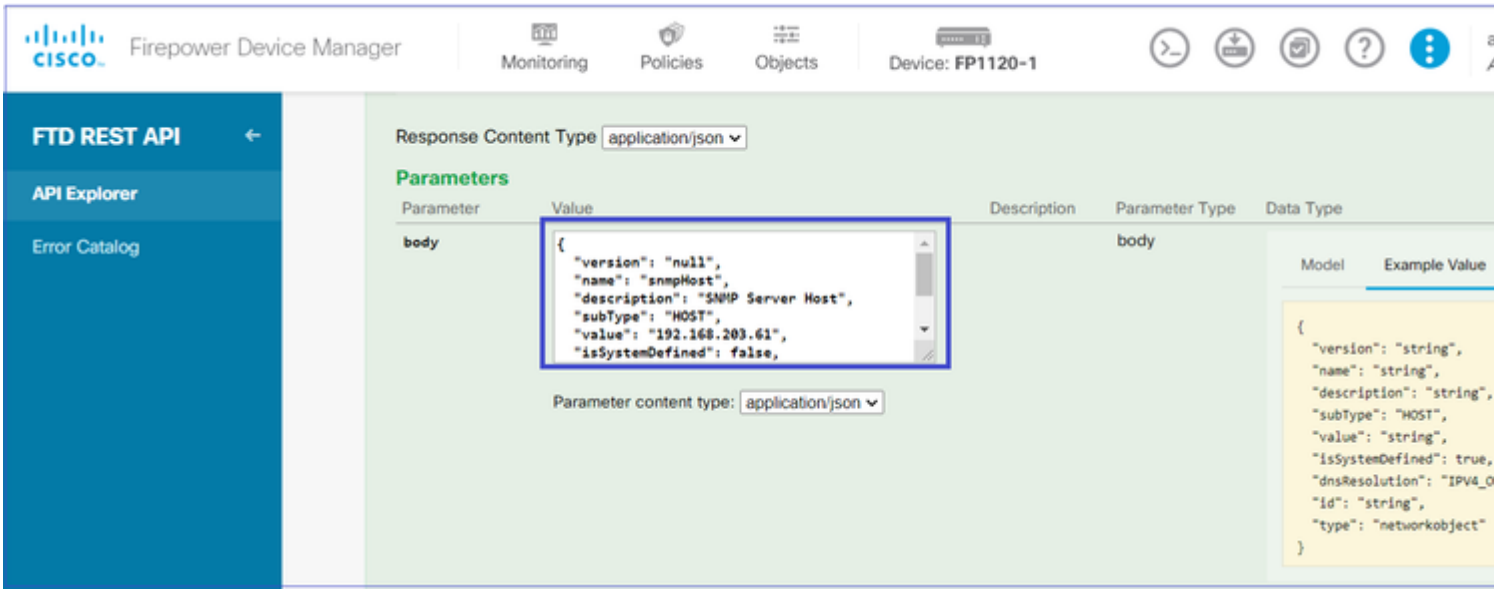
Erstellen Sie ein neues Netzwerkobjekt für den SNMP-Host: Wählen Sie im FDM-API-Explorer NetworkObject (Netzwerkobjekt) und anschließend POST/**Objekt/Netzwerke aus**:



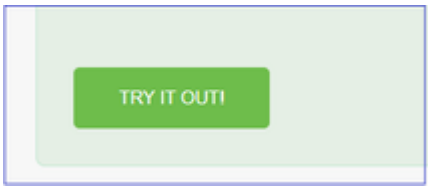
Dieses Format wird für den SNMP-Host JSON verwendet. Fügen Sie diese JSON in den Textabschnitt ein, und ändern Sie die IP-Adresse auf "Wert", damit sie mit der IP-Adresse des SNMP-Hosts übereinstimmt:

```
{
"version": "null",
"name": "snmpHost",
```

```
"description": "SNMP Server Host",
"subType": "HOST",
"value": "192.168.203.61",
"isSystemDefined": false,
"dnsResolution": "IPV4_ONLY",
"type": "networkobject"
}
```

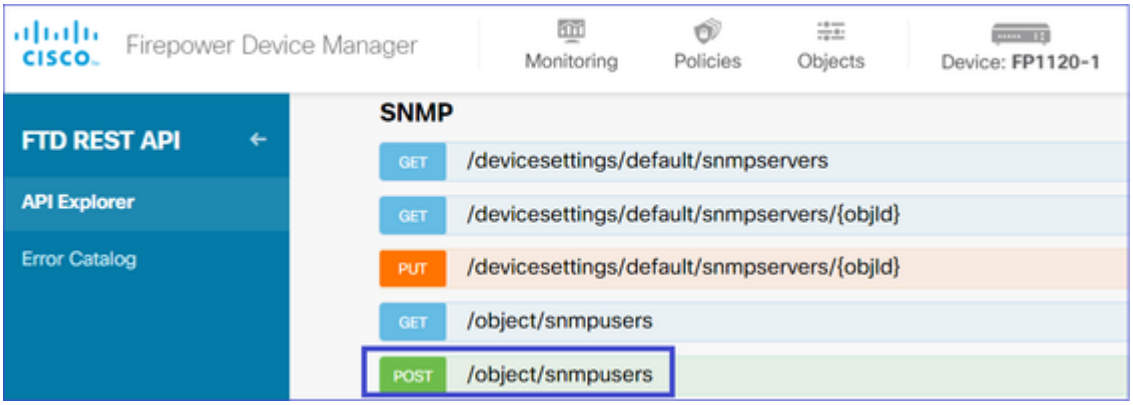
Blättern Sie nach unten, und wählen Sie die Schaltfläche TRY IT OUT! aus, um den API-Aufruf auszuführen. Bei einem erfolgreichen Aufruf wird der Antwortcode 200 zurückgegeben.



Kopieren Sie die JSON-Daten aus dem Antworttext auf ein Notizblock. Später müssen Sie die Informationen zum SNMP-Host eingeben.

3. Erstellen Sie einen neuen SNMPv3-Benutzer

Wählen Sie im FDM API Explorer SNMP und anschließend POST/**object/snmpusers aus.**



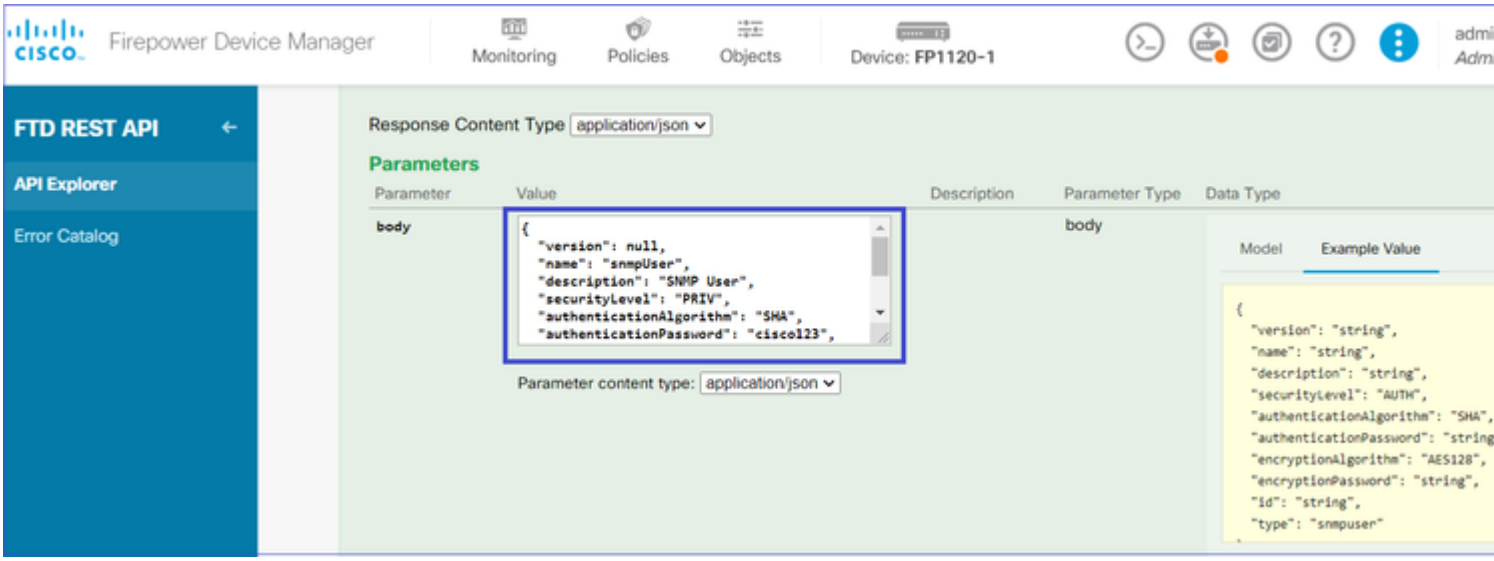
Kopieren Sie diese JSON-Daten in ein Notizblock, und ändern Sie die für Sie interessanten Abschnitte (z. B. "authenticationPassword", "encryptionPassword" oder die Algorithmen):

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

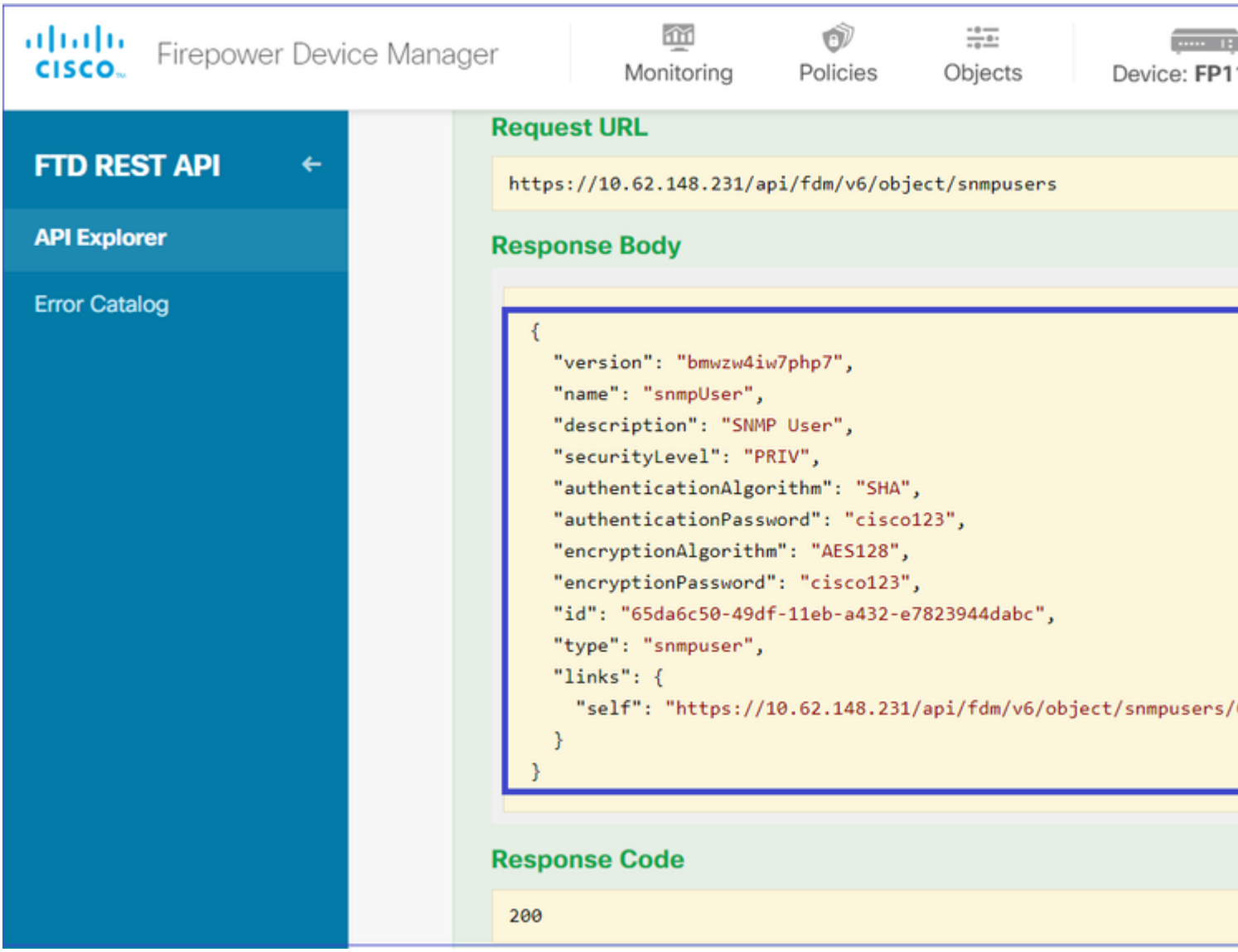
Achtung: Die in den Beispielen verwendeten Passwörter dienen nur zu Demonstrationszwecken.

Stellen Sie in einer Produktionsumgebung sicher, dass Sie sichere Kennwörter verwenden.

Kopieren Sie die geänderten JSON-Daten in den Textabschnitt:

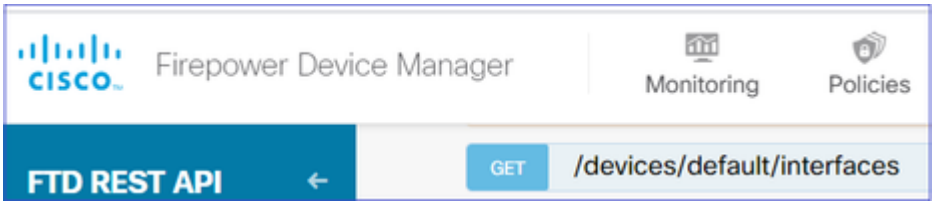


Blättern Sie nach unten, und wählen Sie die Schaltfläche **TRY IT OUT!** aus, um den API-Aufruf auszuführen. Bei einem erfolgreichen Aufruf wird der Antwortcode 200 zurückgegeben. Kopieren Sie die JSON-Daten aus dem Antworttext auf ein Notizblock. Später müssen Sie die Informationen zum SNMP-Benutzer ausfüllen.



4. Schnittstelleninformationen abrufen

Wählen Sie im FDM API Explorer Interface und dann GET **/devices/default/interfaces aus**. Sie müssen Informationen von der Schnittstelle sammeln, die mit dem SNMP-Server verbunden ist.



Blättern Sie nach unten, und wählen Sie die Schaltfläche **TRY IT OUT!** aus, um den API-Aufruf auszuführen. Bei einem erfolgreichen Aufruf wird der Antwortcode 200 zurückgegeben. Kopieren Sie die JSON-Daten aus dem Antworttext auf ein Notizblock. Später müssen Sie Informationen über die Schnittstelle ausfüllen.

Notieren Sie sich die Schnittstelle "version", "name", "id" und "type" aus den JSON-Daten. Beispiel für JSON-Daten von Schnittstelle in:

<#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",

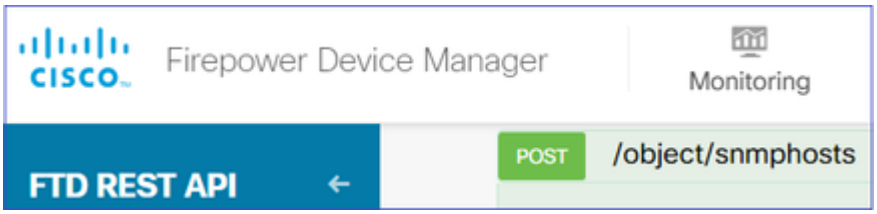

```
"links": {
"self": "https://10.62.148.231/api/fdm/v6/devices/default/interfaces/fc3d07d4-49d2-11eb-85a8-65aec636a0f
}
},
```


Aus den JSON-Daten können Sie sehen, dass die Schnittstelle "inside" diese Daten enthält, die mit dem SNMP-Server verknüpft werden müssen:

- "version": "kkpkibjlu6qro"
- "Name": "innen",
- "id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
- "Typ": "physische Schnittstelle",

5. Erstellen Sie einen neuen SNMPv3-Host.

Wählen Sie im FDM API Explorer SNMP und dann POST/**object/snmphosts/** unter SNMP aus.



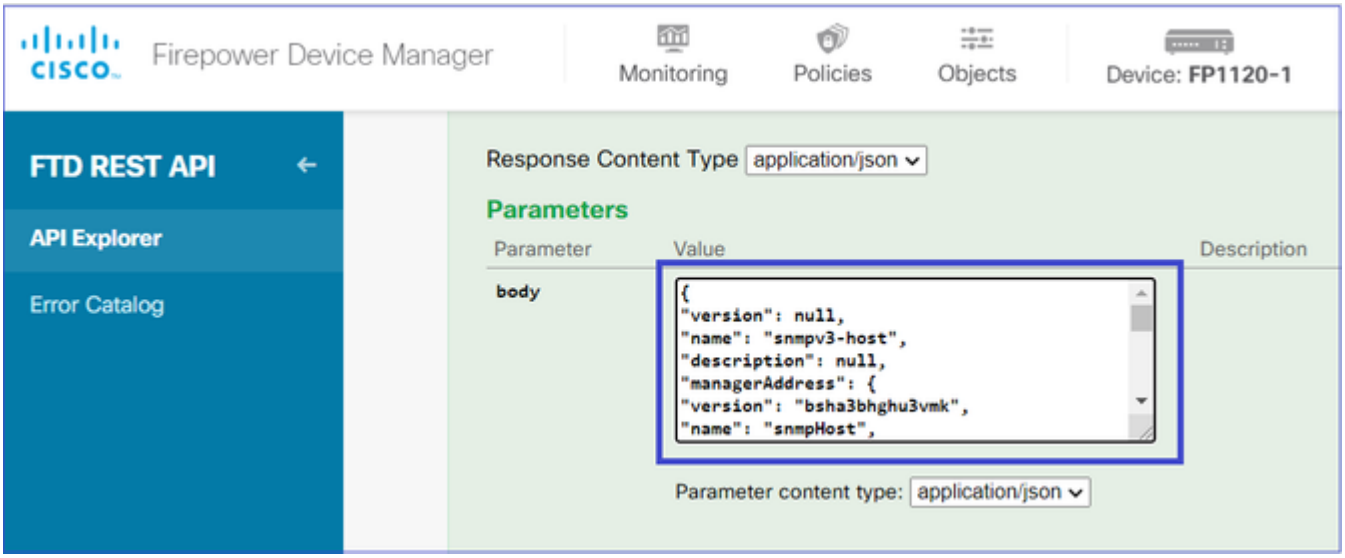
Verwenden Sie diese JSON als Vorlage. Kopieren Sie die Daten aus den vorherigen Schritten in die Vorlage, und fügen Sie sie entsprechend ein:


```
{
"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"
}
```

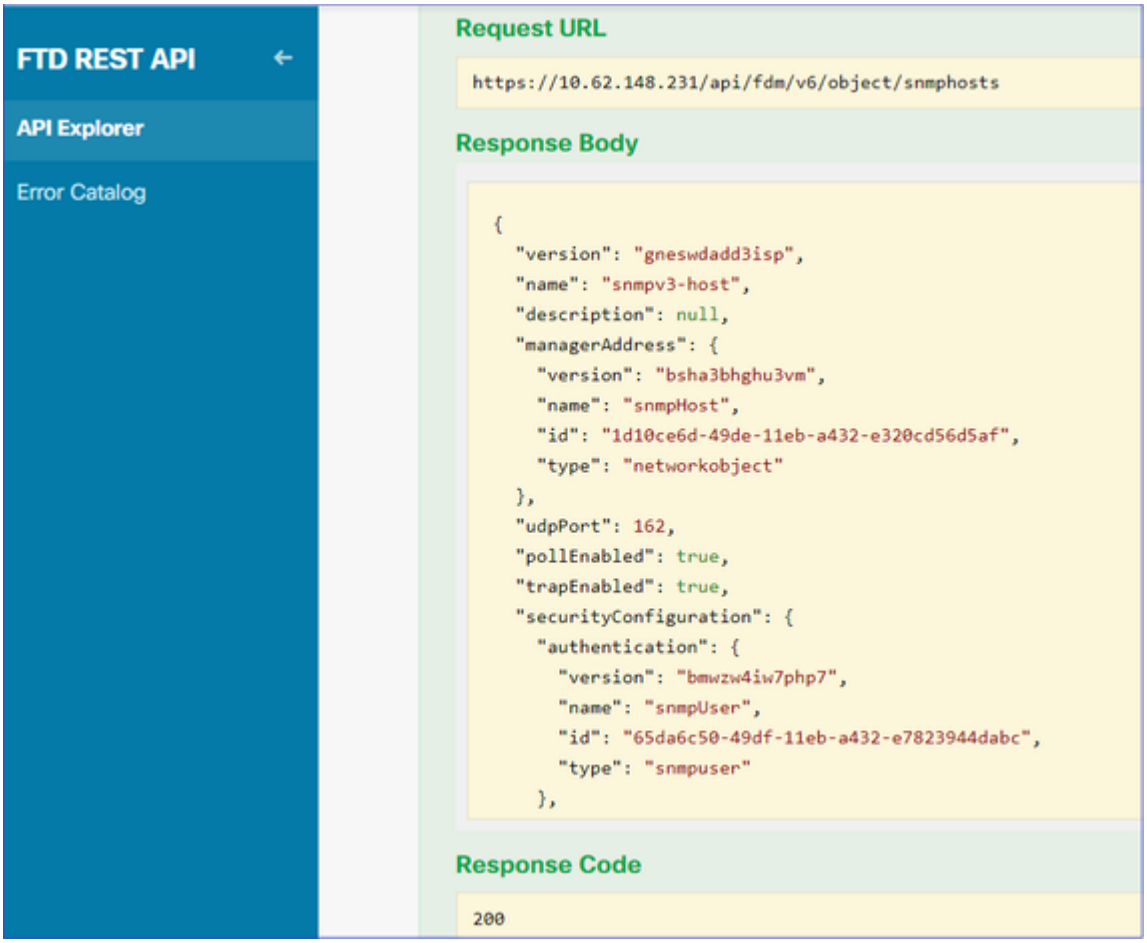

Anmerkung:

- Ersetzen Sie den Wert in managerAddress id, type, version und name durch die Informationen, die Sie aus Step1 erhalten haben.
- Ersetzen Sie den Wert in der Authentifizierung durch die Informationen, die Sie aus Schritt 2 erhalten haben.
- Ersetzen Sie den Wert in der Schnittstelle durch die Daten, die Sie aus Schritt 3 erhalten haben.
- Für SNMP2 gibt es keine Authentifizierung, und der Typ lautet snmpv2csecurityconfiguration anstelle von snmpv3securityconfiguration

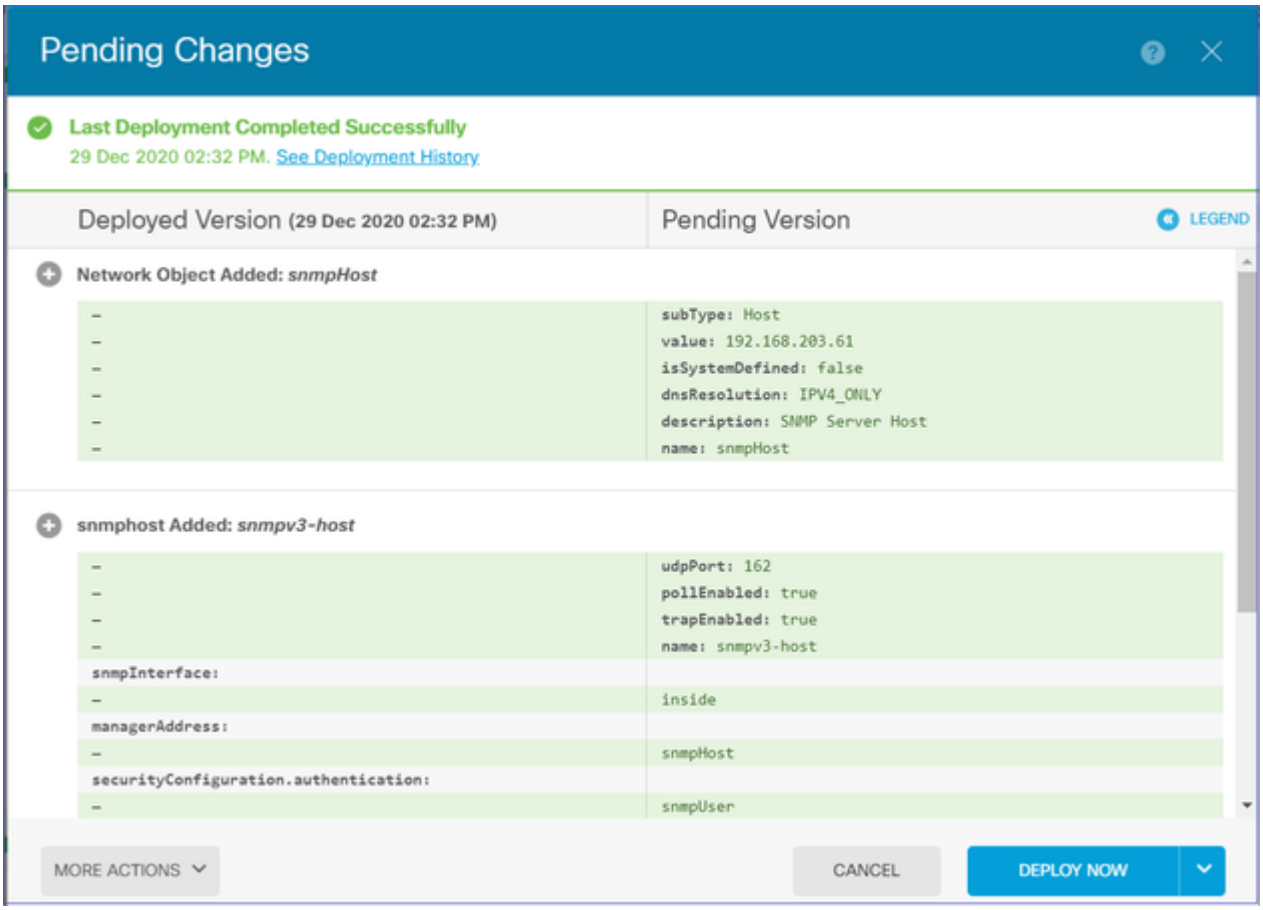
Kopieren der geänderten JSON-Daten in den Textabschnitt



Blättern Sie nach unten, und wählen Sie die Schaltfläche **TRY IT OUT!** aus, um den API-Aufruf auszuführen. Bei einem erfolgreichen Aufruf wird der Antwortcode 200 zurückgegeben.



Navigieren Sie zur FDM-GUI, und stellen Sie die Änderungen bereit. Der Großteil der SNMP-Konfiguration wird angezeigt:



SNMP v2c

Für v2c müssen Sie keinen Benutzer erstellen, aber Sie müssen trotzdem:

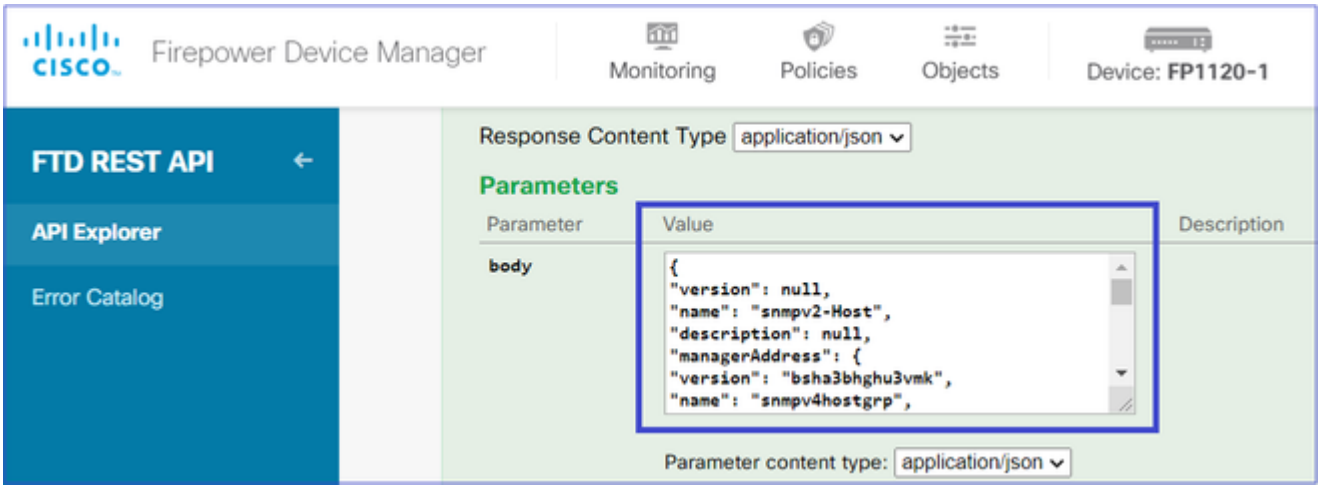
1. Erstellen einer Netzwerkobjektkonfiguration (wie im Abschnitt SNMPv3 beschrieben)
2. Schnittstelleninformationen abrufen (wie im Abschnitt SNMPv3 beschrieben)
3. Erstellen eines neuen SNMPv2c-Hostobjekts

Dies ist ein Beispiel für eine JSON-Nutzlast, die ein SNMPv2c-Objekt erstellt:

```
{
"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"
}
```

Verwenden Sie die POST-Methode, um die JSON-Nutzlast bereitzustellen:

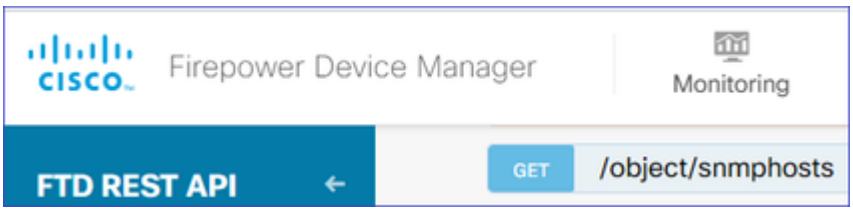


Blättern Sie nach unten, und wählen Sie die Schaltfläche TRY IT OUT! aus, um den API-Aufruf auszuführen. Bei einem erfolgreichen Aufruf wird der Antwortcode 200 zurückgegeben.

Entfernen der SNMP-Konfiguration

Schritt 1:

Abrufen der SNMP-Hostinformationen (**SNMP** > **/object/snmphosts)**:



Blättern Sie nach unten, und wählen Sie die Schaltfläche TRY IT OUT! aus, um den API-Aufruf auszuführen. Bei einem erfolgreichen Aufruf wird der Antwortcode 200 zurückgegeben.

Man bekommt eine Liste von Objekten. Notieren Sie sich die ID des snmphost-Objekts, das Sie entfernen möchten:

<#root>

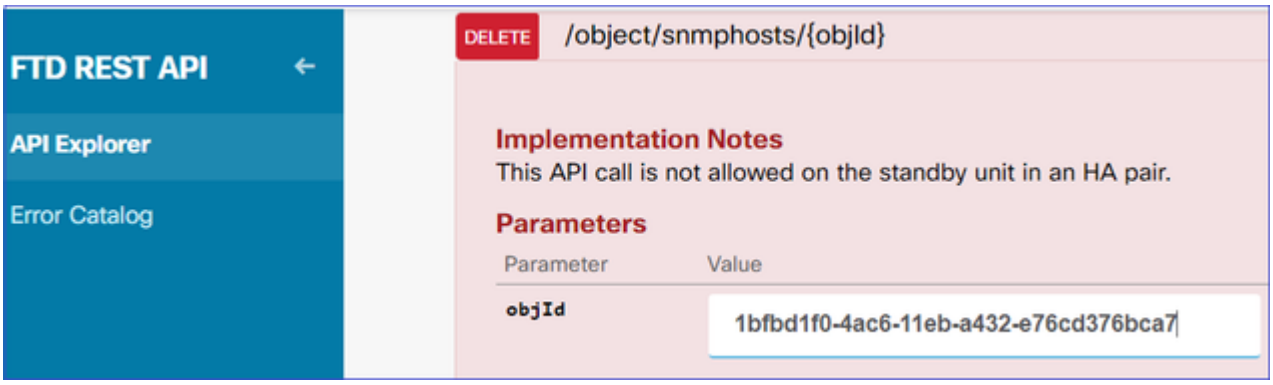

```
{
"items": [
{
"version": "ofaasthu26ulx",
"name": "snmpv2-Host",
"description": null,
"managerAddress": {
"version": "bsha3bhghu3vm",
"name": "snmpHost",
"id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
"type": "networkobject"
},
"udpPort": 162,
"pollEnabled": true,
"trapEnabled": true,
"securityConfiguration": {
"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

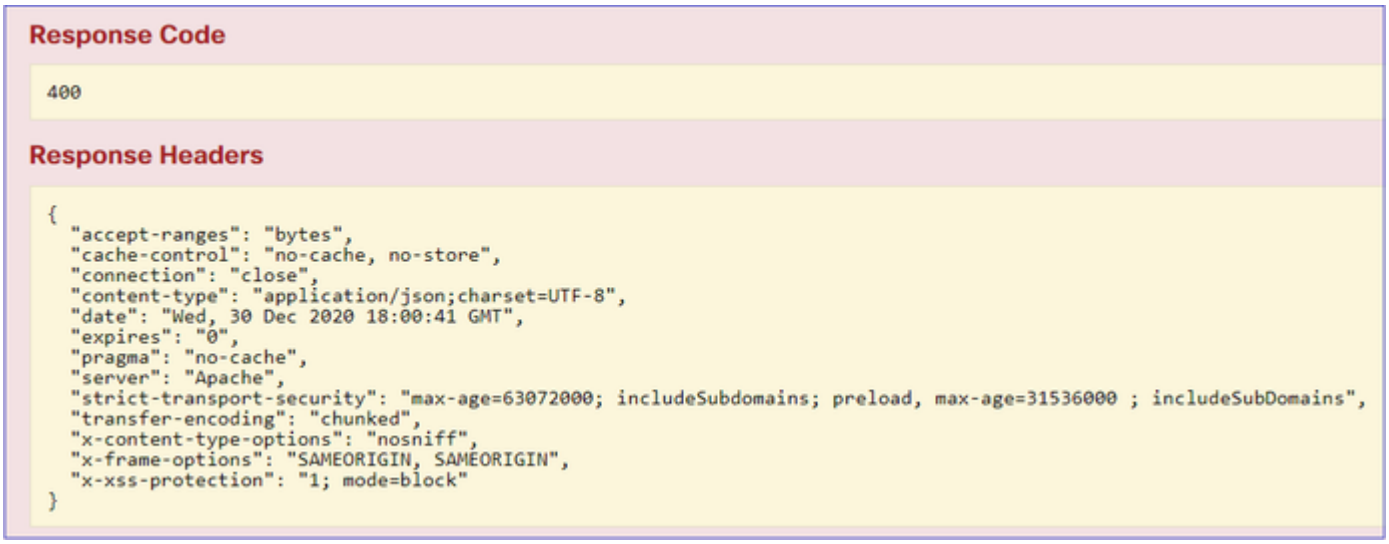

```
",
"type": "snmphost",
"links": {
"self": "https://10.62.148.231/api/fdm/v6/object/snmphosts/1bfbd1f0-4ac6-11eb-a432-e76cd376bca7"
}
},
```


Schritt 2:

Wählen Sie die Option LÖSCHEN in **SNMP** > **/object/snmphosts{objId} aus.** Fügen Sie die in Schritt 1 erfasste ID ein:

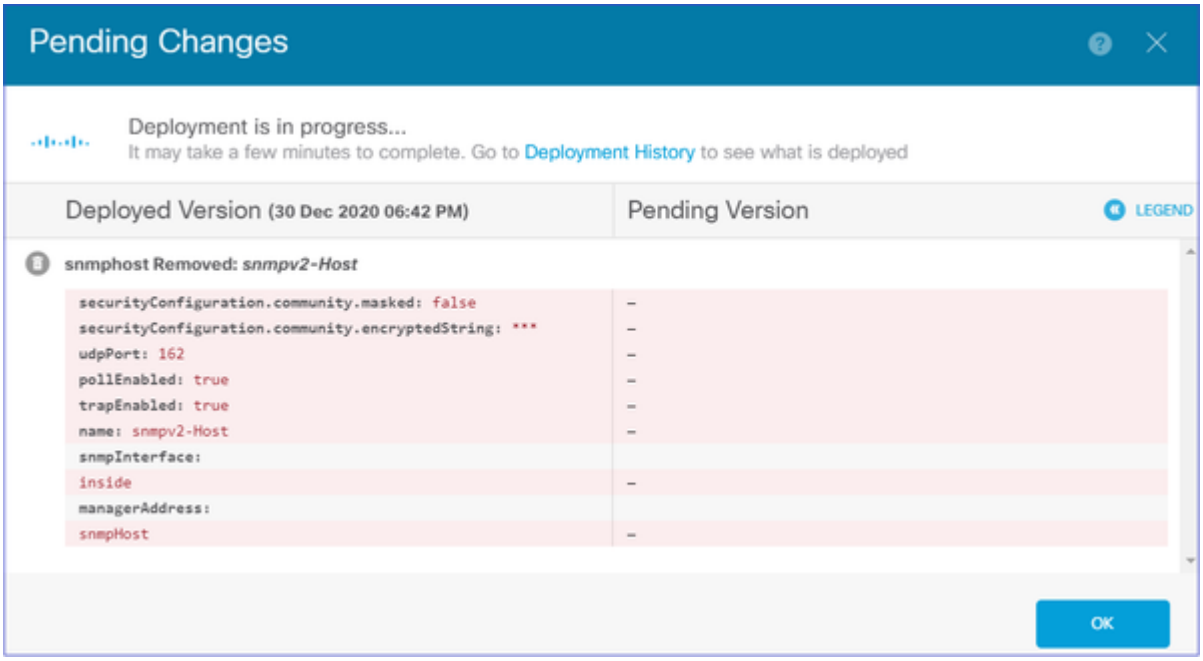


Blättern Sie nach unten, und wählen Sie die Schaltfläche TRY IT OUT! aus, um den API-Aufruf auszuführen. Der Anruf gibt den Antwortcode 400 zurück.



Schritt 3:

Bereitstellen der Änderung:



Bei der Bereitstellung werden die Hostinformationen entfernt:

<#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 *****
```

SNMPwalk für v2c schlägt fehl:

<#root>

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

snmpwalk -v2c -c cisco123 -OS 192.168.203.71

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

Für v3 müssen Sie die Objekte in dieser Reihenfolge löschen.

1. SNMP-Host (der erfolgreiche Rückgabecode ist 204)
2. SNMP-Benutzer (der erfolgreiche Rückgabecode lautet 204)

Wenn Sie versuchen, die Objekte in der falschen Reihenfolge zu löschen, erhalten Sie diesen Fehler:

<#root>

```
{
"error": {
"severity": "ERROR",
"key": "Validation",
"messages": [
{
"description": "You cannot delete the object because it contains SNMPHost: snmpv3-host2, SNMPHost: snmpv
```

You must remove the object from all parts of the configuration before you can delete it.",

```
"code": "deleteObjWithRel",
"location": ""
}
]
}
}
```

Überprüfung

SNMP v3-Überprüfung

Navigieren Sie nach der Bereitstellung zu FTD CLI, um die SNMP-Konfiguration zu überprüfen. Beachten Sie, dass der engineID-Wert automatisch generiert wird.

```
<#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 auth sha ca:1b:18:f3:62:b1:63:7e:92:34:92:b3:cf:54:86:f9:8e:2a:4c:fd priv aes 128 ca:1b:18:f3


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-su
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
```

Schnappversuch

<#root>

```
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 9.1
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
...
```

SNMP v2c-Überprüfung

<#root>

```
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 für v2c:

<#root>

```
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 9.1
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
```

Fehlerbehebung

Erfassung mit Ablaufverfolgung auf der Firewall aktivieren:

<#root>

FP1120-1#

capture CAPI trace interface inside match udp any any eq snmp

Verwenden Sie das snmpwalk-Tool, und vergewissern Sie sich, dass die Pakete angezeigt werden:

<#root>

FP1120-1#

show capture

capture CAPI type raw-data trace interface inside

[Capturing - 3137 bytes]

  match udp any any eq snmp

Inhalt der Aufzeichnung:

<#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
```

Stellen Sie sicher, dass die Zähler für die SNMP-Serverstatistiken SNMP Get- oder Get-next-Anfragen und -Antworten anzeigen:

<#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

Verfolgen eines eingehenden Pakets Das Paket wird als UN-NAT an die interne NLP-Schnittstelle gesendet:

<#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
```

Die NAT-Regel wird automatisch als Teil der SNMP-Konfiguration bereitgestellt:

<#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 stati
translate_hits = 0, untranslate_hits = 0

Auto NAT Policies (Section 2)
â€¦
```

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

translate_hits = 0, untranslate_hits = 2

Auf dem Backend-Port überwacht das UDP 4161 den SNMP-Datenverkehr:

<#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 :::*
```

Im Fall einer falschen/unvollständigen Konfiguration wird das eingehende SNMP-Paket verworfen, da keine UN-NAT-Phase vorhanden ist:

<#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
```

FTD LINA-Syslogs zeigen, dass das Eingangspaket verworfen wird:

<#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:192.168.2
Dec 30 2020 18:36:39: %FTD-7-710005: UDP request discarded from 192.168.203.61/50105 to inside:192.168.2
```

Zugehörige Informationen

- Cisco Firepower Threat Defense - Konfigurationsleitfaden für Firepower Device Manager, Version 6.7
- Cisco Firepower Threat Defense - REST-API-Leitfaden
- Cisco FirePOWER - Versionshinweise, Version 6.7.0

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.