

在Firepower FDM上配置SNMP并对其进行故障排除

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[SNMP v3](#)

[SNMP v2c](#)

[SNMP配置删除](#)

[验证](#)

[SNMP v3验证](#)

[SNMP v2c验证](#)

[故障排除](#)

[问题解答](#)

[相关信息](#)

简介

本文档介绍如何使用REST API在6.7版的Firepower设备管理上启用简单网络管理协议(SNMP)。

先决条件

要求

Cisco 建议您了解以下主题：

- Firepower威胁防御(FTD)，由6.7版的Firepower设备管理(FDM)管理
- REST API知识
- SNMP知识

使用的组件

Firepower威胁防御(FTD)，由Firepower设备管理(FDM)管理，版本6.7。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

6.7的新增功能

FTD设备REST API支持SNMP服务器、用户、主机和主机组的配置和管理。通过FP 6.7中的SNMP FTD设备REST API支持：

- 用户可以通过FTD设备REST API配置SNMP来管理网络
- SNMP服务器、用户和主机/主机组可以通过FTD Device REST API添加/更新或管理。

文档中包含的示例描述了FDM API资源管理器采取的配置步骤。



注：当FTD运行版本6.7并由FDM管理时，只能通过REST API配置SNMP

功能概述 — SNMP FTD设备REST API支持

- 此功能添加特定于SNMP的新FDM URL终端。
- 这些新的API可用于为轮询和陷阱配置SNMP以监控系统。
- 通过API(Firepower设备上的管理信息库(MIB))进行SNMP配置后，可轮询或进行NMS/SNMP客户端上的陷阱通知。

SNMP API/URL终端

URL	方法	型号
/devicesettings/default/snmpservers	GET	SNMP服务器
/devicesettings/default/snmpservers/{objId}	PUT、GET	SNMP服务器
/object/snmphosts	POST，获取	SNMPHost
/object/snmphosts/{objId}	PUT、DELETE、GET	SNMPHost
/object/snmpusergroups	POST，获取	SNMPUserGroup
/object/snmpusergroups/{objId}	PUT、DELETE、GET	SNMPUserGroup
/object/snmpusers	POST，获取	SNMPUser

/object/snmpusers/{objId}	PUT、DELETE、GET	SNMPUser
---------------------------	----------------	----------

配置

- SNMP主机有3个主要版本

- SNMP V1

- SNMP V2C

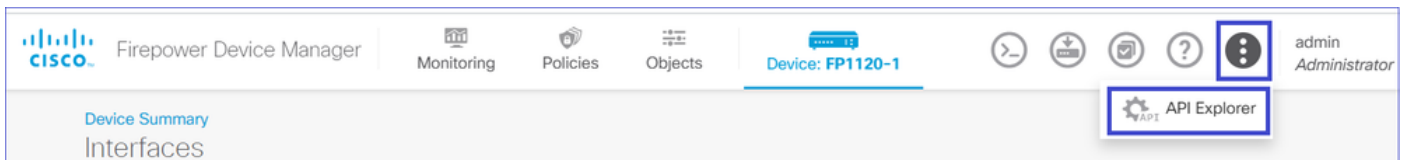
- SNMP V3

- 其中每个选项都有特定的“securityConfiguration”格式。
- 对于V1和V2C：它包含“社区字符串”和“类型”字段，该字段将配置标识为V1或V2C。
- 对于SNMP V3：它包含有效的SNMP V3用户和标识配置为V3的“类型”字段。

SNMP v3

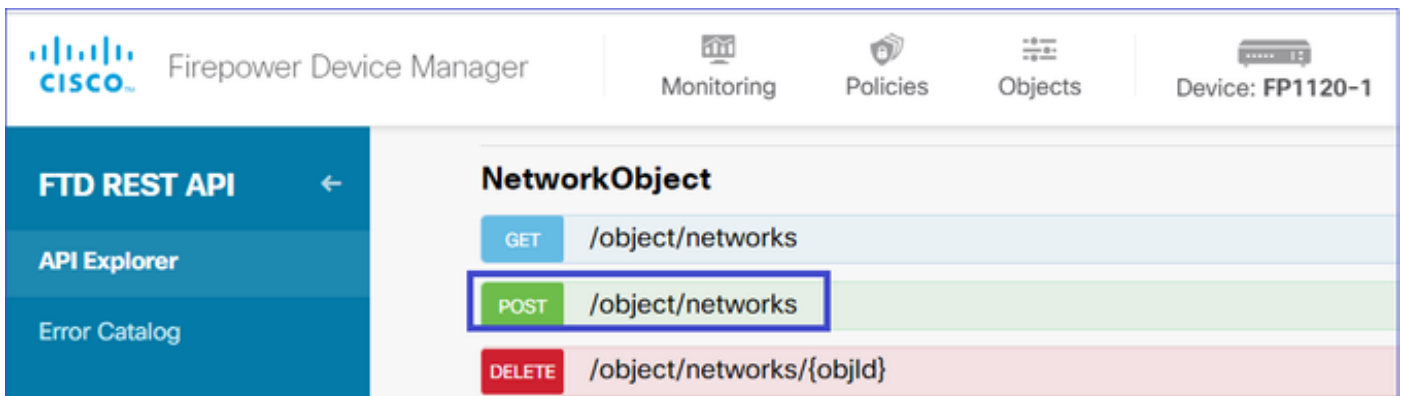
1. 访问FDM API资源管理器

要从FDM GUI访问FDM REST API资源管理器，请选择三个点，然后选择API资源管理器。或者，导航至URL https://FDM_IP/#/api-explorer。



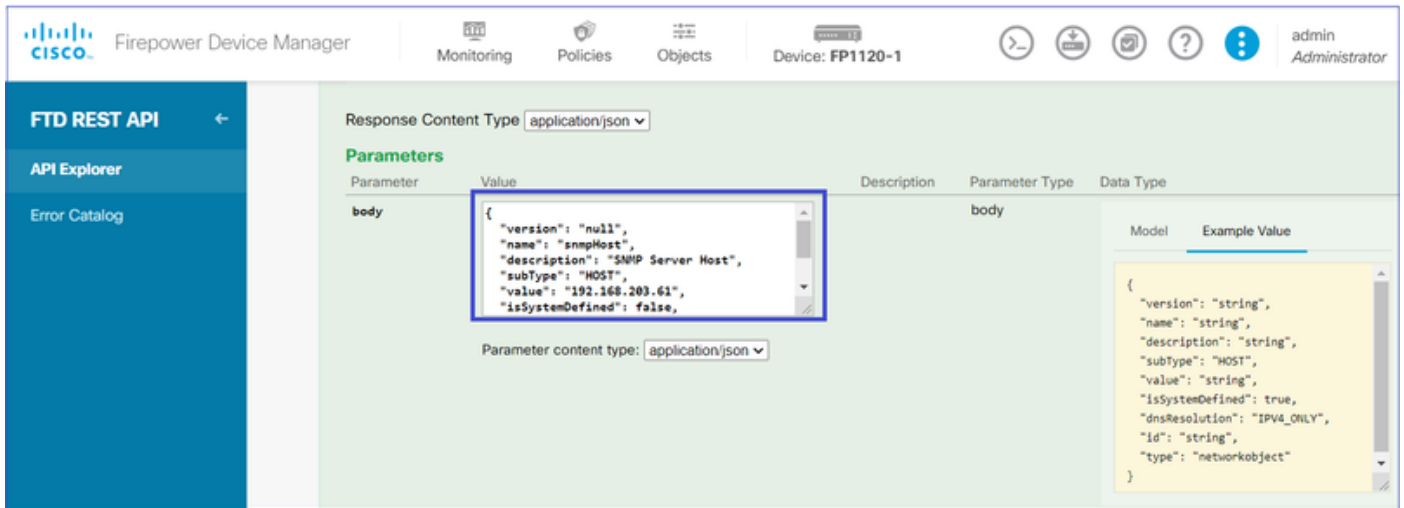
2. 网络对象配置

为SNMP主机创建新的网络对象：在FDM API资源管理器上，依次选择NetworkObject和POST /object/networks:



SNMP主机JSON格式如下。将此JSON粘贴到body部分并更改“value”上的IP地址以匹配SNMP主机IP地址：

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



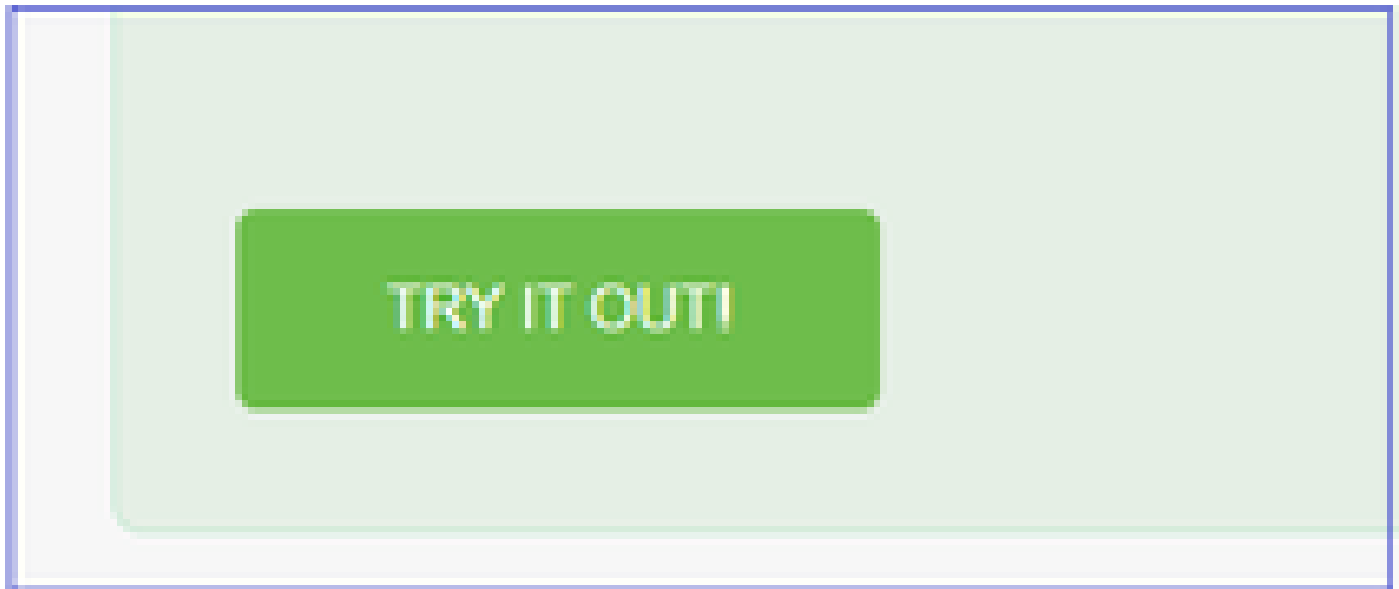
The screenshot shows the Cisco Firepower Device Manager (FDM) interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: FP1120-1'. The left sidebar has 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main area is titled 'Parameters' and shows a table with columns: Parameter, Value, Description, Parameter Type, and Data Type. A parameter named 'body' is highlighted, with its value field containing a JSON object:

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

 The 'Parameter content type' is set to 'application/json'. To the right, a 'Model' section shows an 'Example Value' with a JSON schema:

```
{
"version": "string",
"name": "string",
"description": "string",
"subType": "HOST",
"value": "string",
"isSystemDefined": true,
"dnsResolution": "IPV4_ONLY",
"id": "string",
"type": "networkobject"
}
```

向下滚动并选择TRY IT OUT！按钮以执行API调用。成功的调用返回响应代码200。

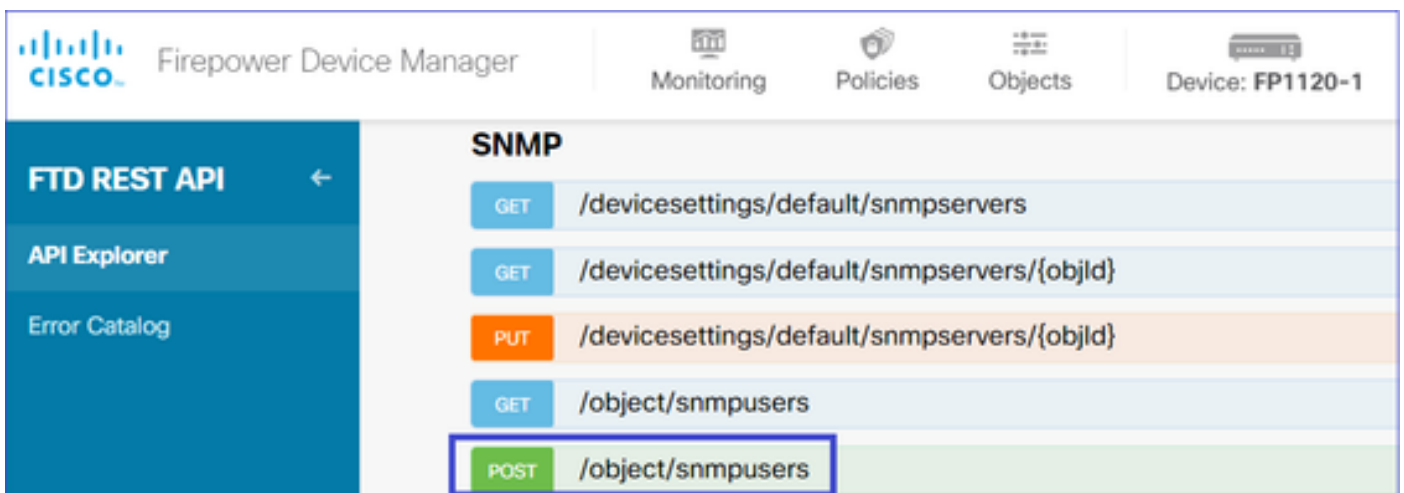


将JSON数据从响应正文复制到记事本。稍后，您需要填写有关SNMP主机的信息。




3. 创建新的SNMPv3用户

在FDM API资源管理器上，依次选择SNMP和POST/object/snmpusers

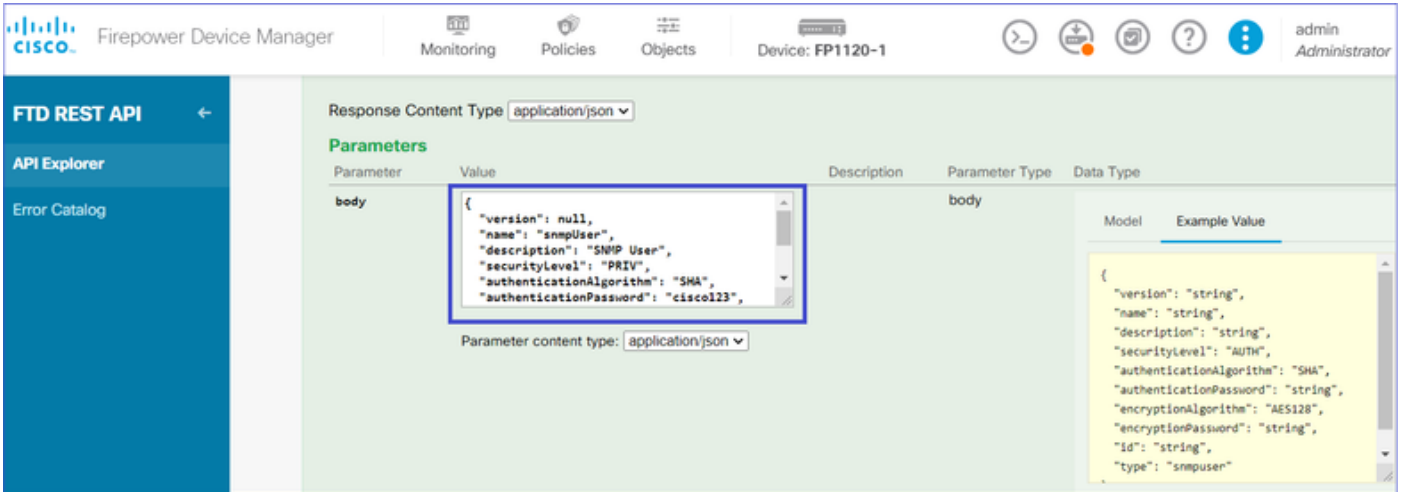


将此JSON数据复制到记事本并修改您感兴趣的部分（例如，“authenticationPassword”、“encryptionPassword”或算法）：

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

 注意：示例中使用的密码仅用于演示目的。在生产环境中，请确保使用强密码

将修改的JSON数据复制到正文部分：

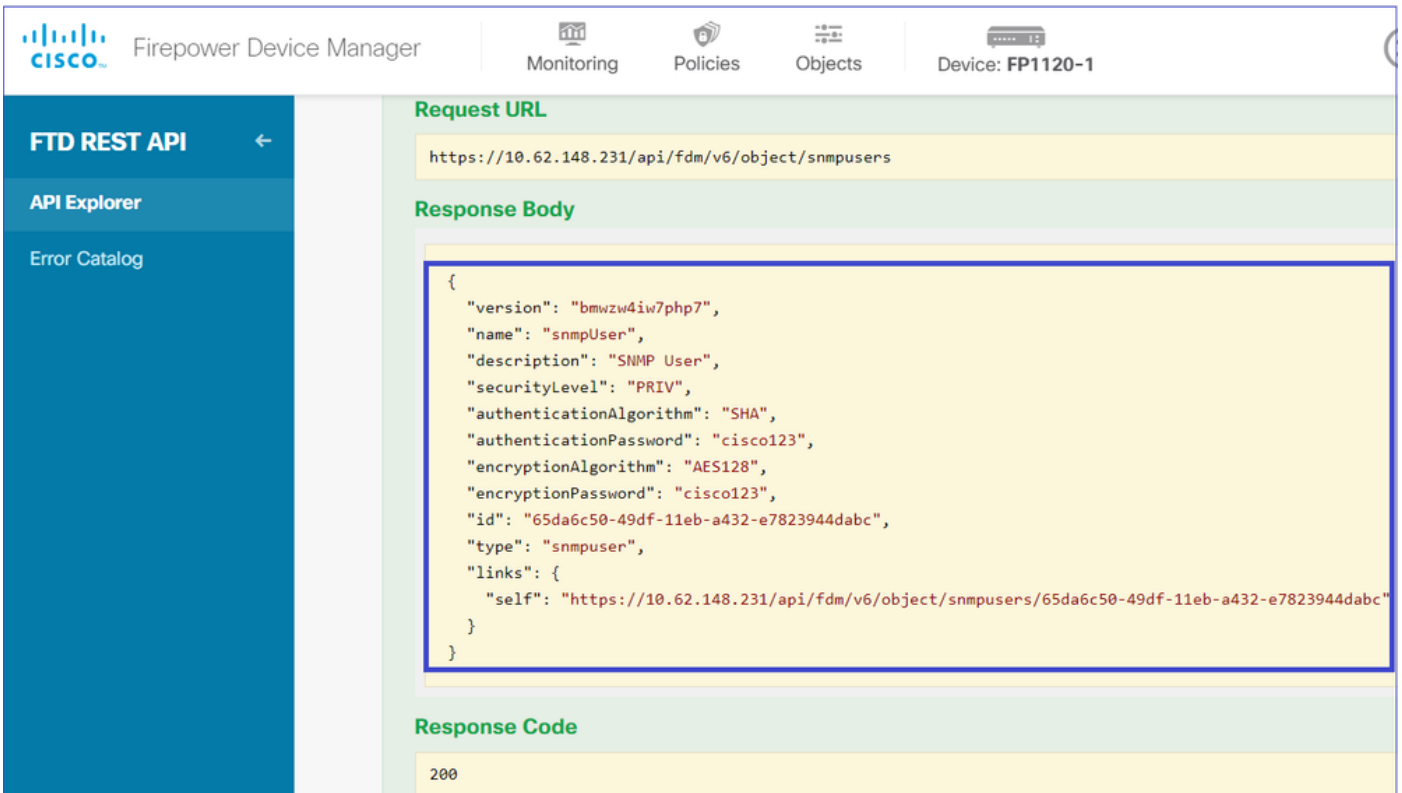


The screenshot shows the Firepower Device Manager interface for configuring an SNMP user. The 'Parameters' section is expanded, showing a 'body' parameter with a JSON value. The JSON value is highlighted with a blue box:

```
{
  "version": null,
  "name": "snmpUser",
  "description": "SNMP User",
  "securityLevel": "PRIV",
  "authenticationAlgorithm": "SHA",
  "authenticationPassword": "cisco123",
}
```

The 'Parameter content type' is set to 'application/json'. To the right, an 'Example Value' section shows a more detailed JSON structure with fields like 'version', 'name', 'description', 'securityLevel', 'authenticationAlgorithm', 'authenticationPassword', 'encryptionAlgorithm', 'encryptionPassword', 'id', and 'type'.

向下滚动并选择TRY IT OUT!按钮以执行API调用。成功的调用返回响应代码200。将JSON数据从响应正文复制到记事本。稍后，您需要填写有关SNMP用户的信息。



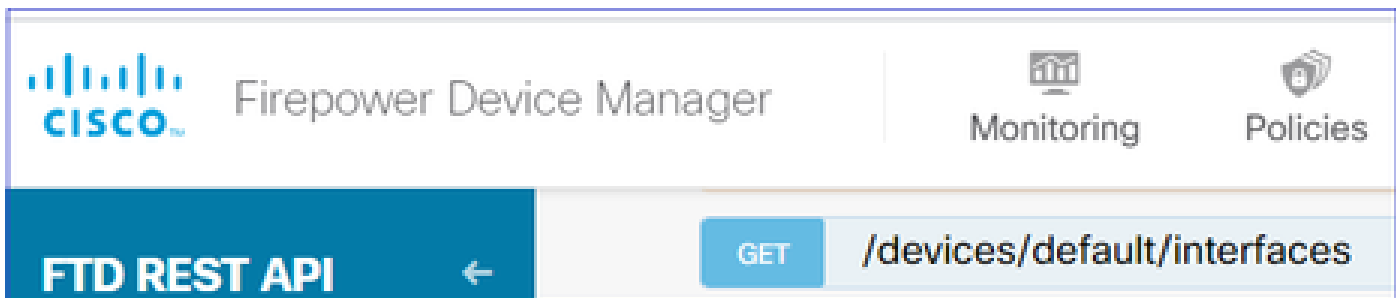
The screenshot shows the Firepower Device Manager interface displaying the response for an API call. The 'Request URL' is 'https://10.62.148.231/api/fdm/v6/object/snmpusers'. The 'Response Body' is highlighted with a blue box and contains the following JSON:

```
{
  "version": "bmwzw4iw7php7",
  "name": "snmpUser",
  "description": "SNMP User",
  "securityLevel": "PRIV",
  "authenticationAlgorithm": "SHA",
  "authenticationPassword": "cisco123",
  "encryptionAlgorithm": "AES128",
  "encryptionPassword": "cisco123",
  "id": "65da6c50-49df-11eb-a432-e7823944dabc",
  "type": "snmpuser",
  "links": {
    "self": "https://10.62.148.231/api/fdm/v6/object/snmpusers/65da6c50-49df-11eb-a432-e7823944dabc"
  }
}
```

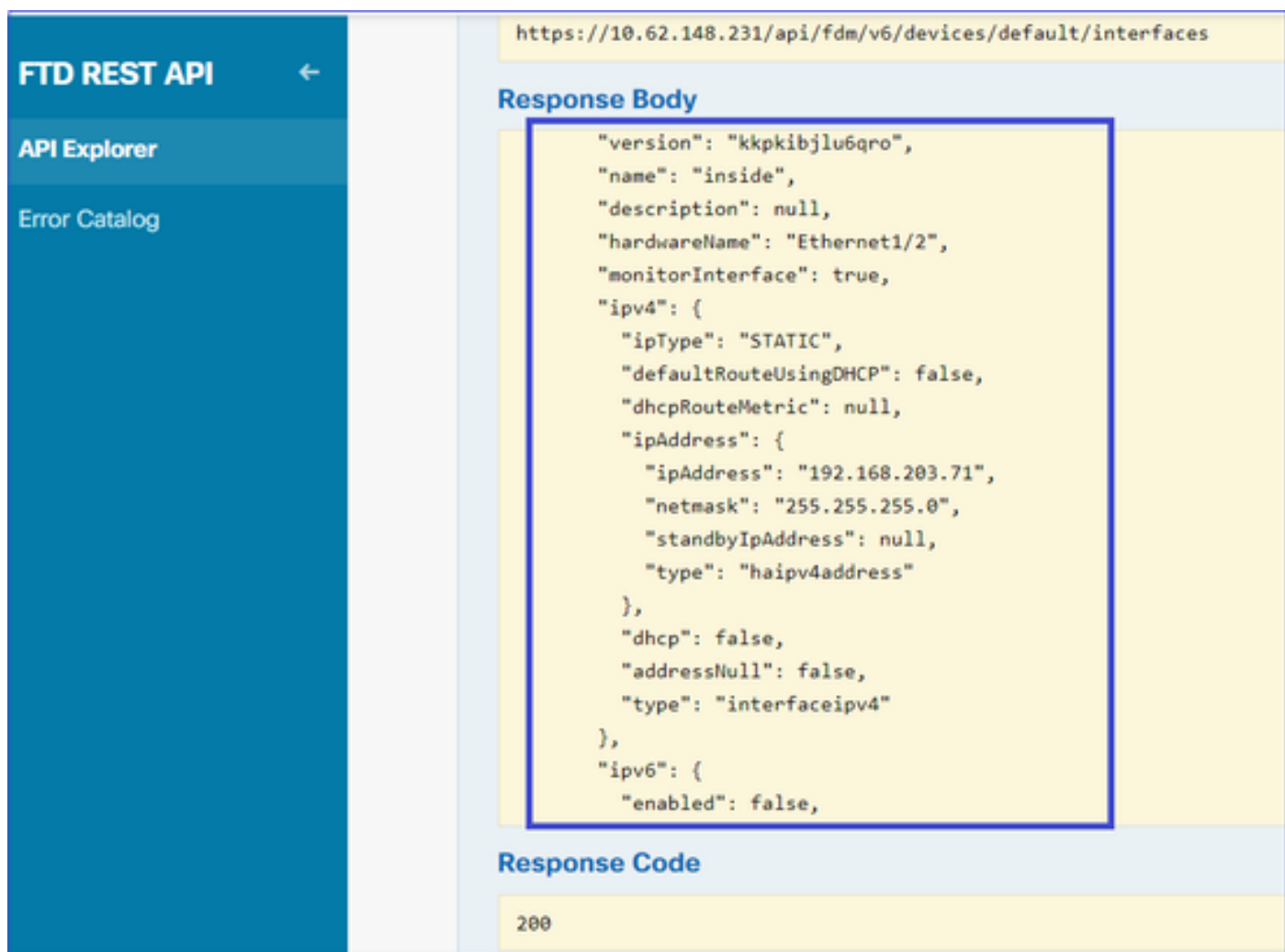
The 'Response Code' is 200.

4. 获取接口信息

在FDM API资源管理器上，依次选择Interface和GET/devices/default/interfaces。您需要从连接到SNMP服务器的接口收集信息。



向下滚动并选择TRY IT OUT!按钮以执行API调用。成功的调用返回响应代码200。将JSON数据从响应正文复制到记事本。稍后，您需要填写有关该接口的信息。



记下JSON数据中的接口“version”、“name”、“id”和“type”。来自内部接口的JSON数据示例：

<#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",

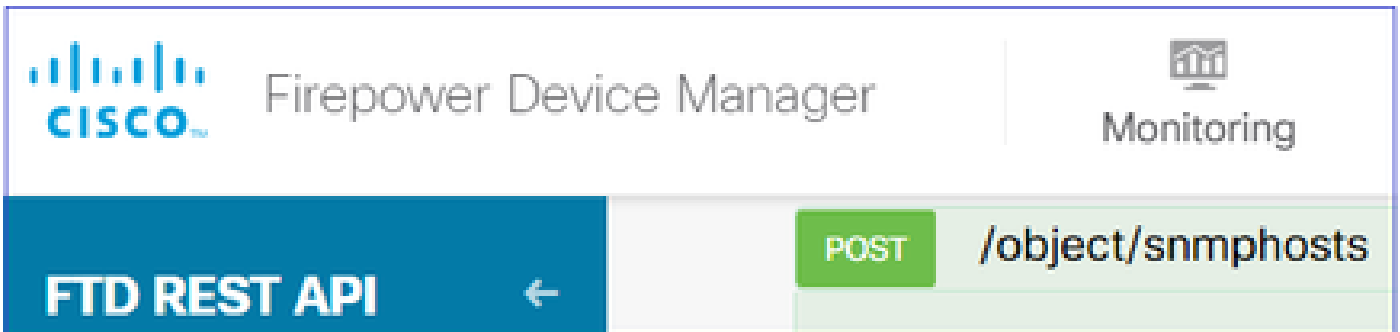
"links": {
"self": "https://10.62.148.231/api/fdm/v6/devices/default/interfaces/fc3d07d4-49d2-11eb-85a8-65aec636a0"
}
},
```


从JSON数据中，您可以看到接口“inside”包含需要与SNMP服务器关联的数据：

- "版本": "kkpkibjlu6qro"
- "名称": "内部",
- "id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
- "类型": "物理接口",

5. 创建新的SNMPv3主机

在FDM API资源管理器上，选择SNMP，然后在SNMP下选择POST/object/snmphosts/s



使用此JSON作为模板。将之前步骤中的数据复制并粘贴到模板中，如下所示：

```
{
"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"
}
```

注意：

- 用从步骤1接收的信息替换managerAddress id、type、version和name中的值
- 使用从步骤2接收的信息替换身份验证中的值
- 使用从步骤3接收的数据替换接口中的值
- 对于SNMP2，没有身份验证，类型为snmpv2csecurityconfiguration，而不是snmpv3securityconfiguration

将修改的JSON数据复制到正文部分

The screenshot shows the Cisco Firepower Device Manager (FDM) REST API configuration page for device FP1120-1. The page is titled "FTD REST API" and has a sidebar with "API Explorer" and "Error Catalog". The main content area is titled "Parameters" and shows a table with columns "Parameter", "Value", and "Description". The "body" parameter is highlighted with a blue box and contains the following JSON object:

```
{
  "version": null,
  "name": "snmpv3-host",
  "description": null,
  "managerAddress": {
    "version": "bsha3bhghu3vmk",
    "name": "snmpHost",
  }
}
```

The "Response Content Type" dropdown is set to "application/json" and the "Parameter content type" dropdown is also set to "application/json".

向下滚动并选择TRY IT OUT!按钮以执行API调用。成功的调用返回响应代码200。

FTD REST API ←

API Explorer

Error Catalog

Request URL

https://10.62.148.231/api/fdm/v6/object/snmphosts

Response Body

```
{
  "version": "gneswdadd3isp",
  "name": "snmpv3-host",
  "description": null,
  "managerAddress": {
    "version": "bsha3bhghu3vm",
    "name": "snmpHost",
    "id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
    "type": "networkobject"
  },
  "udpPort": 162,
  "pollEnabled": true,
  "trapEnabled": true,
  "securityConfiguration": {
    "authentication": {
      "version": "bmwz4iw7php7",
      "name": "snmpUser",
      "id": "65da6c50-49df-11eb-a432-e7823944dabc",
      "type": "snmpuser"
    }
  },
}
```

Response Code

200

导航到FDM GUI并部署更改。您可以看到大部分SNMP配置：

Pending Changes ? ×

✓ **Last Deployment Completed Successfully**
29 Dec 2020 02:32 PM. [See Deployment History](#)

Deployed Version (29 Dec 2020 02:32 PM)	Pending Version LEGEND																				
<p>Network Object Added: snmpHost</p> <table border="1"> <tr><td>-</td><td>subType: Host</td></tr> <tr><td>-</td><td>value: 192.168.203.61</td></tr> <tr><td>-</td><td>isSystemDefined: false</td></tr> <tr><td>-</td><td>dnsResolution: IPV4_ONLY</td></tr> <tr><td>-</td><td>description: SNMP Server Host</td></tr> <tr><td>-</td><td>name: snmpHost</td></tr> </table>		-	subType: Host	-	value: 192.168.203.61	-	isSystemDefined: false	-	dnsResolution: IPV4_ONLY	-	description: SNMP Server Host	-	name: snmpHost								
-	subType: Host																				
-	value: 192.168.203.61																				
-	isSystemDefined: false																				
-	dnsResolution: IPV4_ONLY																				
-	description: SNMP Server Host																				
-	name: snmpHost																				
<p>snmpHost Added: snmpv3-host</p> <table border="1"> <tr><td>-</td><td>udpPort: 162</td></tr> <tr><td>-</td><td>pollEnabled: true</td></tr> <tr><td>-</td><td>trapEnabled: true</td></tr> <tr><td>-</td><td>name: snmpv3-host</td></tr> <tr><td colspan="2">snmpInterface:</td></tr> <tr><td>-</td><td>inside</td></tr> <tr><td colspan="2">managerAddress:</td></tr> <tr><td>-</td><td>snmpHost</td></tr> <tr><td colspan="2">securityConfiguration.authentication:</td></tr> <tr><td>-</td><td>snmpUser</td></tr> </table>		-	udpPort: 162	-	pollEnabled: true	-	trapEnabled: true	-	name: snmpv3-host	snmpInterface:		-	inside	managerAddress:		-	snmpHost	securityConfiguration.authentication:		-	snmpUser
-	udpPort: 162																				
-	pollEnabled: true																				
-	trapEnabled: true																				
-	name: snmpv3-host																				
snmpInterface:																					
-	inside																				
managerAddress:																					
-	snmpHost																				
securityConfiguration.authentication:																					
-	snmpUser																				

MORE ACTIONS ▼ CANCEL DEPLOY NOW ▼

SNMP v2c

对于v2c，您不需要创建用户，但您仍需要：

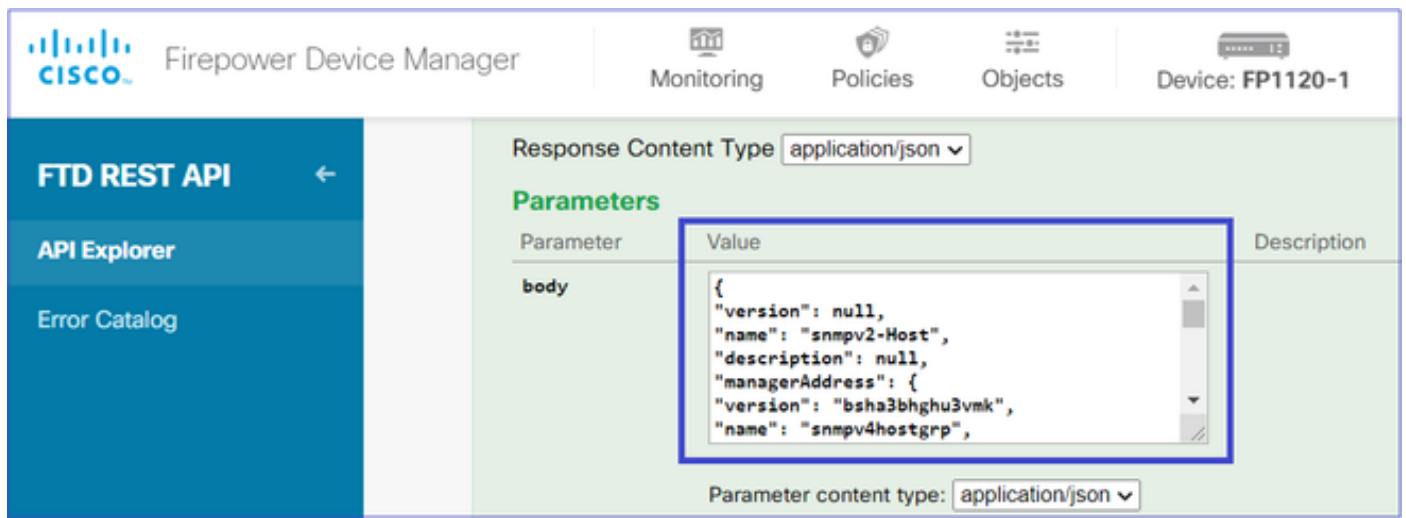
1. 创建网络对象配置（与SNMPv3部分中所述相同）
2. 获取接口信息（与SNMPv3部分中所述相同）
3. 创建新的SNMPv2c主机对象

以下是创建SNMPv2c对象的JSON负载示例：

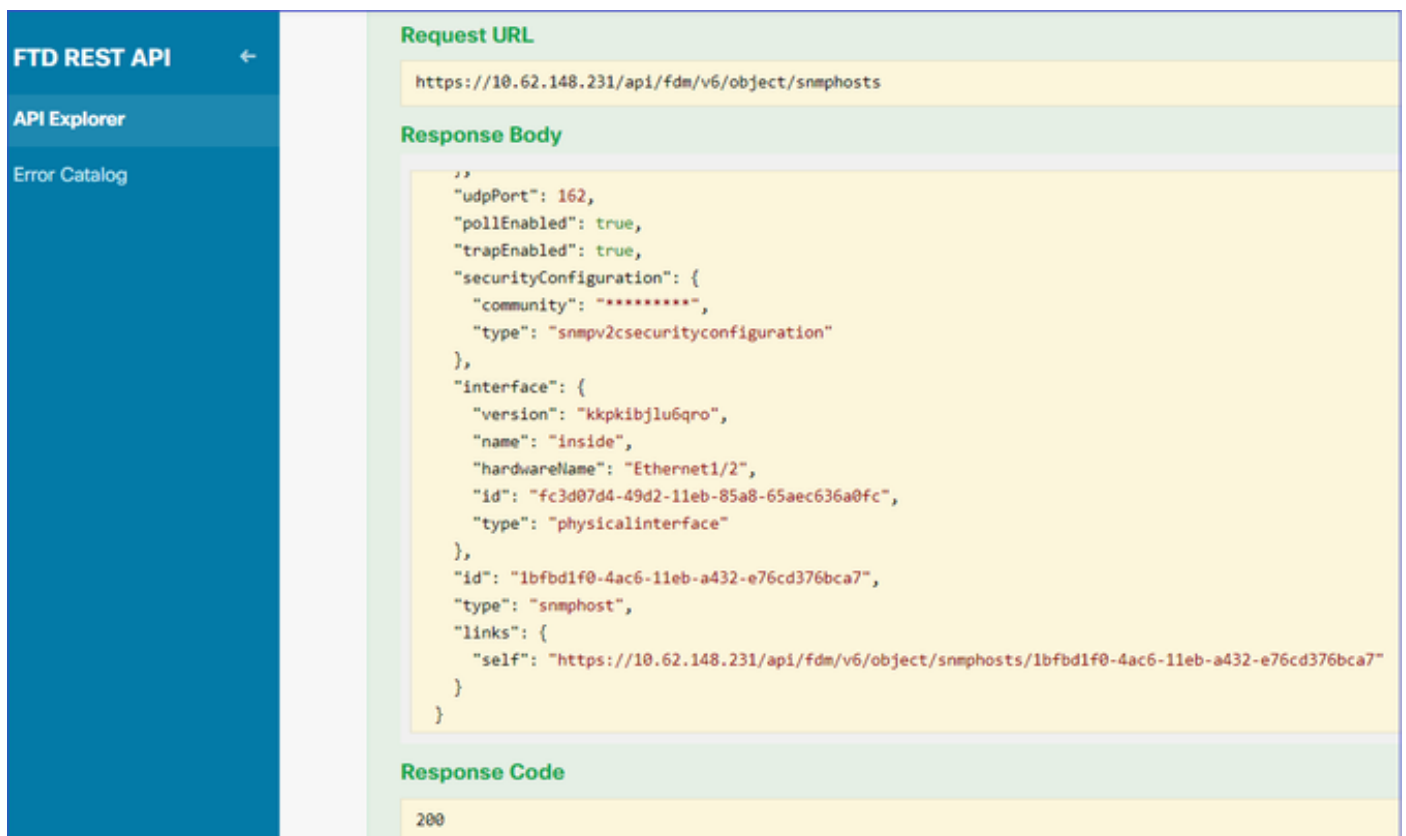
```
{
  "version": null,
  "name": "snmpv2-Host",
  "description": null,
  "managerAddress": {
    "version": "bsha3bhghu3vmk",
    "name": "snmpv4hostgrp",
    "id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
    "type": "networkobject"
  },
  "pollEnabled": true,
  "trapEnabled": true,
  "securityConfiguration": {
    "community": "cisco123",
    "type": "snmpv2csecurityconfiguration"
  }
}
```

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

使用POST方法部署JSON负载：



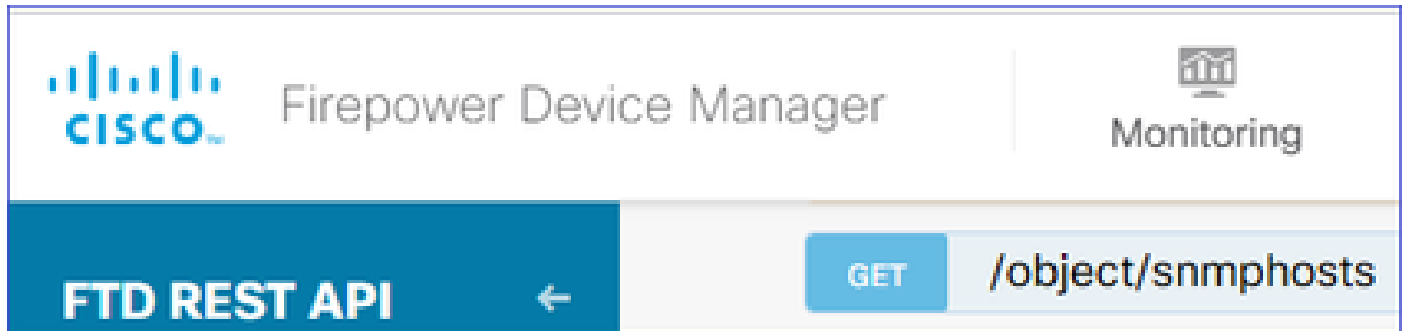
向下滚动并选择TRY IT OUT！按钮以执行API调用。成功的调用返回响应代码200。



SNMP配置删除

步骤1:

获取SNMP主机信息(SNMP > /object/snmphosts):



向下滚动并选择TRY IT OUT ! 按钮以执行API调用。成功的调用返回响应代码200。

您将获得一个对象列表。记下要删除的snmpHost对象的id:

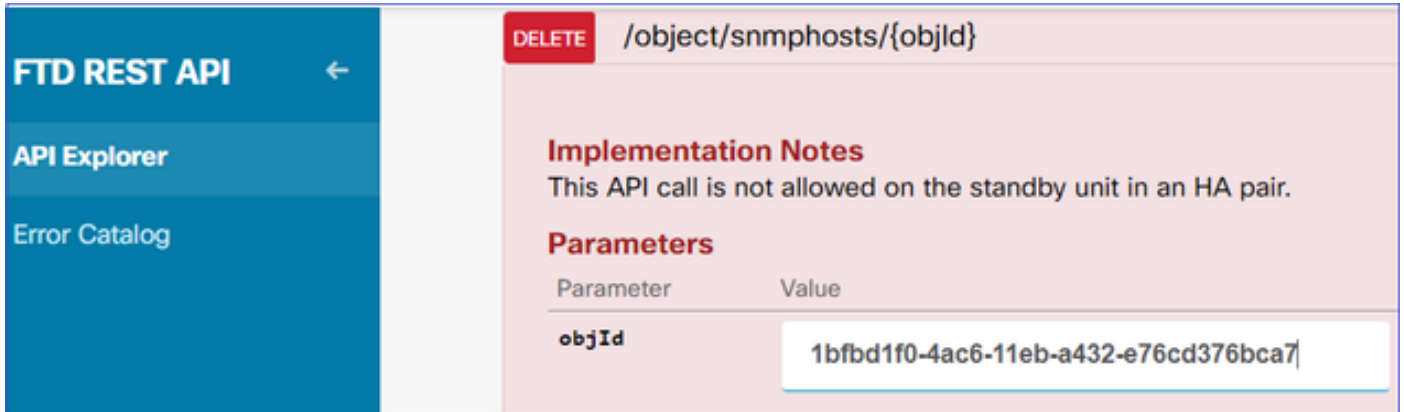
```
<#root>
```

```
{
  "items": [
    {
      "version": "ofaasthu26u1x",
      "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": "
1bfb1f0-4ac6-11eb-a432-e76cd376bca7
",
      "type": "snmpHost",
      "links": {
        "self": "https://10.62.148.231/api/fdm/v6/object/snmpHosts/1bfb1f0-4ac6-11eb-a432-e76cd376bca7"
      }
    }
  ]
}
```

},

第二步：

在SNMP >/object/snmphosts{objId}中选择DELETE选项。粘贴您在第1步中收集的ID:



The screenshot shows the FTD REST API interface. On the left is a sidebar with 'FTD REST API' and navigation options like 'API Explorer' and 'Error Catalog'. The main area displays the endpoint `/object/snmphosts/{objId}` with a 'DELETE' button. Below this, there are sections for 'Implementation Notes' (stating the call is not allowed on the standby unit in an HA pair) and 'Parameters'. A table lists the parameter `objId` with its value `1bfbd1f0-4ac6-11eb-a432-e76cd376bca7` entered in a text box.

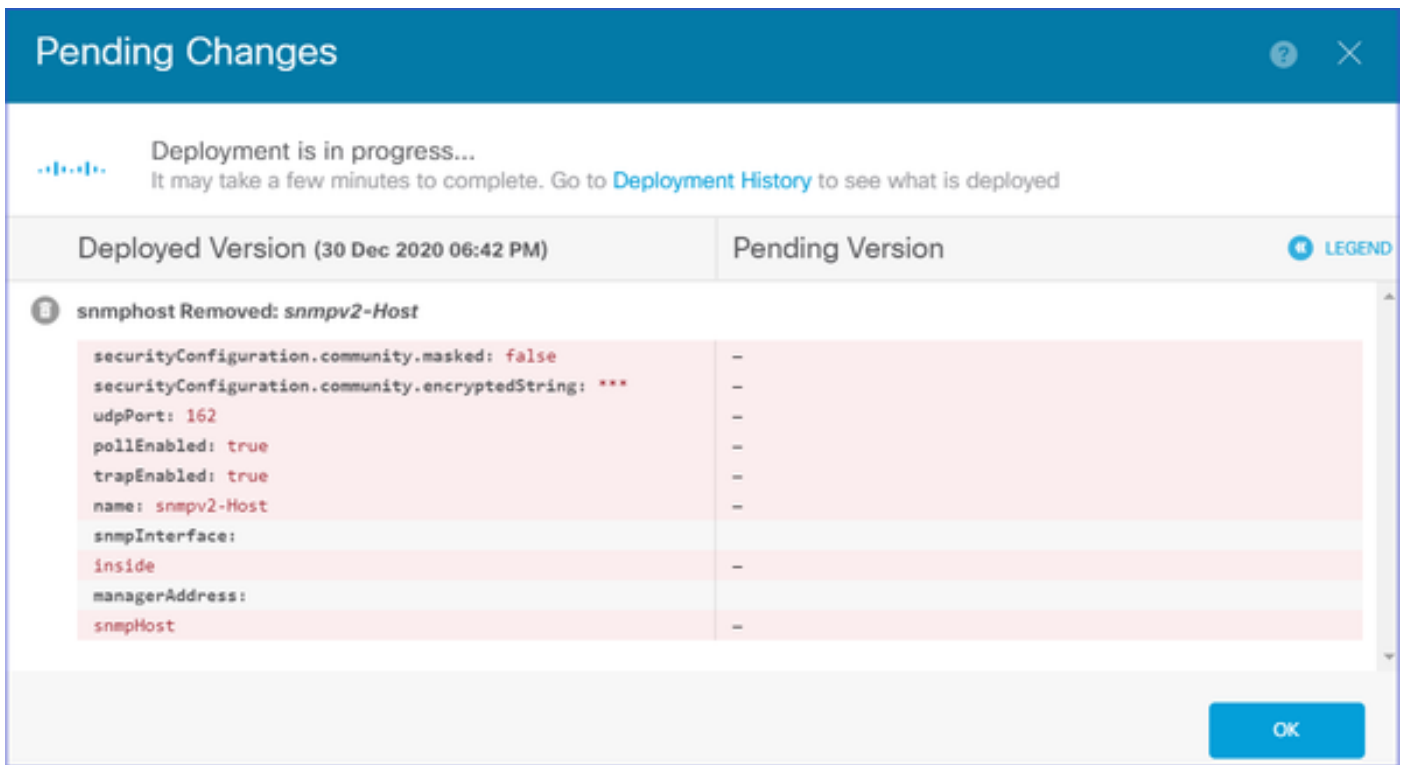
向下滚动并选择TRY IT OUT！按钮以执行API调用。该调用返回响应代码400。



The screenshot shows the response details for the API call. It includes a 'Response Code' section with the value `400`. Below that is a 'Response Headers' section containing a JSON object with various headers like `accept-ranges`, `cache-control`, `connection`, `content-type`, `date`, `expires`, `pragma`, `server`, `strict-transport-security`, `transfer-encoding`, `x-content-type-options`, `x-frame-options`, and `x-xss-protection`.

第三步：

部署更改：



部署会删除主机信息：

```
<#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 *****
```

v2c的snmpwalk失败：

```
<#root>
```

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

```
snmpwalk -v2c -c cisco123 -Os 192.168.203.71
```

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

对于v3，必须按此顺序删除对象。

1. SNMP主机 (成功的返回代码为204)

2. SNMP用户 (成功的返回代码为204)

如果尝试以错误的顺序删除对象，则会出现以下错误：

```
<#root>
{
  "error": {
    "severity": "ERROR",
    "key": "Validation",
    "messages": [
      {
        "description": "You cannot delete the object because it contains SNMPHost: snmpv3-host2, SNMPHost: snmpv3-host1.
        You must remove the object from all parts of the configuration before you can delete it.",
        "code": "deleteObjWithRel",
        "location": ""
      }
    ]
  }
}
```

验证

SNMP v3验证

部署后，导航至FTD CLI以验证SNMP配置。请注意，engineID值是自动生成的。

```
<#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:f3:62:b1:63:7e:92:34:92:b3:cf:54:86:f9:8e:2a:4c:fd

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-supply-failure
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
```

snmpwalk测试

```
<#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 9.8(2)K8"
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验证

```
<#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 *****
```

v2c的snmpwalk:

```
<#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.
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
```

故障排除

在防火墙上启用带跟踪的捕获：

```
<#root>
```

```
FP1120-1#
```

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

使用snmpwalk工具并验证您是否可以看到数据包：

```
<#root>
```

FP1120-1#

show capture

capture CAPI type raw-data trace interface inside

[Capturing - 3137 bytes]

match udp any any eq snmp

捕获内容：

<#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

验证SNMP服务器统计信息计数器是否显示SNMP Get或Get-next请求和响应：

<#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

跟踪入口数据包。数据包通过UN-NAT发送到内部NLP接口：

<#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

NAT规则作为SNMP配置的一部分自动部署：

<#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

在后端端口UDP 4161中侦听SNMP流量：

```
<#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 :::*
```

在配置不正确/不完整的情况下，会丢弃入口SNMP数据包，因为没有UN-NAT阶段：

```
<#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系统日志显示入口数据包被丢弃：

<#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.

问题解答

问：是否可以使用FTD管理接口发送SNMP消息？

否，当前不支持此功能。

相关增强缺陷：<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu48012>

相关信息

- [适用于Firepower设备管理器的思科Firepower威胁防御配置指南，版本6.7](#)
- [思科Firepower威胁防御REST API指南](#)
- [思科Firepower版本说明，版本6.7.0](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。