

Firepower FDMでのSNMPの設定およびトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[SNMP v3](#)

[SNMP v2c](#)

[SNMP設定の削除](#)

[確認](#)

[SNMP v3の確認](#)

[SNMP v2cの検証](#)

[トラブルシューティング](#)

[Q&A](#)

[関連情報](#)

はじめに

このドキュメントでは、REST APIを使用してバージョン6.7のFirepowerデバイス管理(FMC)で簡易ネットワーク管理プロトコル(SNMP)を有効にする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- バージョン6.7のFirepower Device Management(FDM)で管理されるFirepower Threat Defense(FTD)
- REST APIの知識
- SNMPの知識

使用するコンポーネント

Firepower Threat Defense(FTD)は、バージョン6.7のFirepower Device Management(FDM)で管理されます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。


背景説明

6.7の新機能

FTD Device REST APIは、SNMPサーバ、ユーザ、ホスト、およびホストグループの設定と管理をサポートします。FP 6.7でSNMP FTD Device REST APIがサポートされている場合：

- ユーザはFTD Device REST APIを使用してSNMPを設定し、ネットワークを管理できます
- SNMPサーバ、ユーザ、およびホスト/ホストグループは、FTD Device REST APIを使用して追加/更新または管理できます。

このドキュメントに含まれる例では、FDM APIエクスプローラで実行される構成手順について説明します。

 注:FTDがバージョン6.7を実行し、FDMによって管理されている場合、SNMPはREST API経由でのみ設定できます

機能の概要：SNMP FTD Device REST APIのサポート

- この機能は、SNMPに固有の新しいFDM URLエンドポイントを追加します。
- これらの新しいAPIを使用して、システムを監視するためのポーリングおよびトラップ用にSNMPを設定できます。
- APIを介したSNMP設定後、FirepowerデバイスのManagement Information Base (MIB ; 管理情報ベース) は、NMS/SNMPクライアントでのポーリングまたはトラップ通知に使用できます。

SNMP API/URLエンドポイント

URL	方式	モデル
/devicesettings/default/snmpservers	GET	SNMPサーバ
/devicesettings/default/snmpservers/{objId}	PUT、GET	SNMPサーバ
/object/snmphosts	投稿、取得	SNMPHost
/object/snmphosts/{objId}	PUT、DELETE、GET	SNMPHost

/object/snmpusergroups	投稿、取得	SNMPUserGroup (トンネルグループ)
/object/snmpusergroups/{objId}	PUT、DELETE、GET	SNMPUserGroup (トンネルグループ)
/object/snmpusers	投稿、取得	SNMPUser
/object/snmpusers/{objId}	PUT、DELETE、GET	SNMPUser

設定

- SNMPホストには3つのプライマリバージョンがあります

- SNMP V1

- SNMP V2C

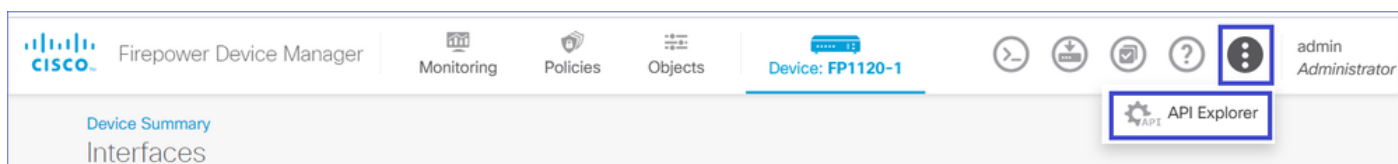
- SNMP V3

- これらはそれぞれ、「securityConfiguration」に固有の形式を持ちます。
- V1およびV2Cの場合：設定をV1またはV2Cとして識別する「コミュニティストリング」および「タイプ」フィールドが含まれます。
- SNMP V3の場合：有効なSNMP V3ユーザと、設定をV3として識別する「type」フィールドが含まれます。

SNMP v3

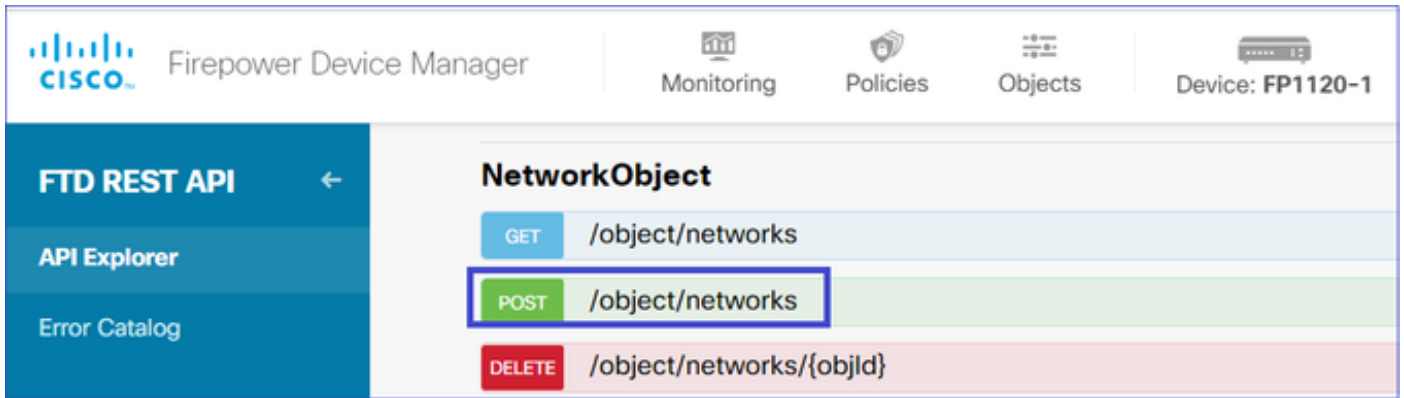
1. FDM APIエクスプローラにアクセスします

FDM GUIからFDM REST APIエクスプローラにアクセスするには、3つのドットを選択してから、APIエクスプローラを選択します。または、URL https://FDM_IP/#/api-explorer:



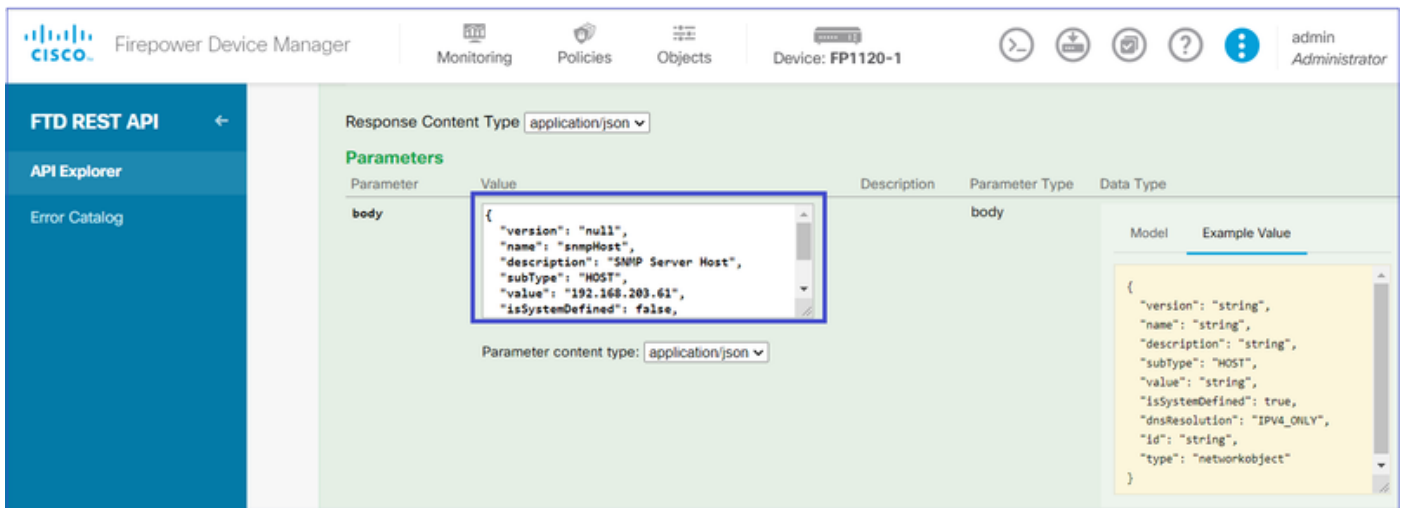
2. ネットワークオブジェクトの設定

SNMPホストの新しいネットワーク・オブジェクトを作成します。FDM APIエクスプローラで「NetworkObject」を選択し、次に「/object/networks」を選択します。



SNMPホストのJSON形式は次のとおりです。このJSONを本文セクションに貼り付け、「value」のIPアドレスをSNMPホストのIPアドレスに一致するように変更します。

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



下にスクロールしてTRY IT OUT! ボタンを選択し、API呼び出しを実行します。コールが成功すると、応答コード200が返されます。

TRY IT OUT!

レスポンス本文のJSONデータをメモ帳にコピーします。後で、SNMPホストに関する情報を入力する必要があります。



The screenshot shows the FTD REST API Explorer interface. The left sidebar contains the following menu items: "FTD REST API" (with a back arrow), "API Explorer", and "Error Catalog". The main content area displays the following information:

- URL:** `https://10.62.148.231/api/fdm/v6/object/networks`
- Response Body:** A JSON object representing a network object:

```
{  "version": "bsha3bhghu3vm",  "name": "snmpHost",  "description": "SNMP Server Host",  "subType": "HOST",  "value": "192.168.203.61",  "isSystemDefined": false,  "dnsResolution": "IPV4_ONLY",  "id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",  "type": "networkobject",  "links": {    "self": "https://10.62.148.231/api/fdm/v6/object/networks/1d10ce6d-49de-11eb-a432-e320cd56d5af"  }}
```
- Response Code:** 200

3.新しいSNMPv3ユーザを作成する

FDM APIエクスプローラで「SNMP」を選択し、次に「POST /object/snmpusers」を選択します

Firepower Device Manager

Monitoring Policies Objects Device: FP1120-1

FTD REST API ←

- API Explorer
- Error Catalog

SNMP

- GET /devicesettings/default/snmpservers
- GET /devicesettings/default/snmpservers/{objId}
- PUT /devicesettings/default/snmpservers/{objId}
- GET /object/snmpusers
- POST /object/snmpusers**

このJSONデータをメモ帳にコピーし、目的のセクションを変更します（たとえば、「authenticationPassword」、「encryptionPassword」、またはアルゴリズム）。

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

⚠ 注意：この例で使用されているパスワードは、デモ用です。実稼働環境では、強力なパスワードを使用してください

変更されたJSONデータをbodyセクションにコピーします。

Firepower Device Manager

Monitoring Policies Objects Device: FP1120-1 admin Administrator

FTD REST API ←

- API Explorer
- Error Catalog

Response Content Type: application/json

Parameters

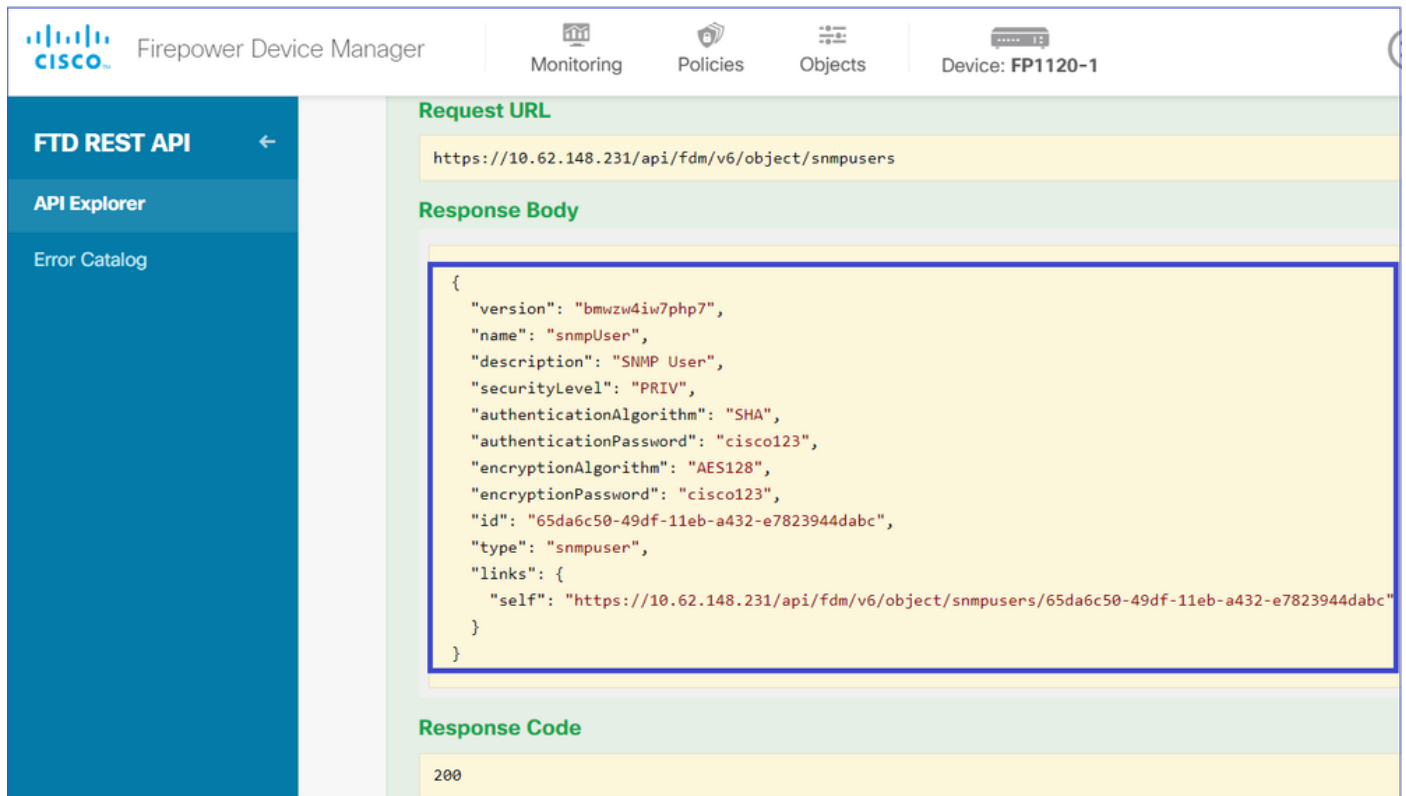
Parameter	Value	Description	Parameter Type	Data Type
body	<pre>{ "version": null, "name": "snmpUser", "description": "SNMP User", "securityLevel": "PRIV", "authenticationAlgorithm": "SHA", "authenticationPassword": "cisco123", }</pre>		body	

Parameter content type: application/json

Model Example Value

```
{
"version": "string",
"name": "string",
"description": "string",
"securityLevel": "AUTH",
"authenticationAlgorithm": "SHA",
"authenticationPassword": "string",
"encryptionAlgorithm": "AES128",
"encryptionPassword": "string",
"id": "string",
"type": "snmpuser"
}
```

下にスクロールしてTRY IT OUT!ボタンを選択し、APIコールを実行します。コールが成功すると、応答コード200が返されます。レスポンス本文のJSONデータをメモ帳にコピーします。後で、SNMPユーザに関する情報を入力する必要があります。

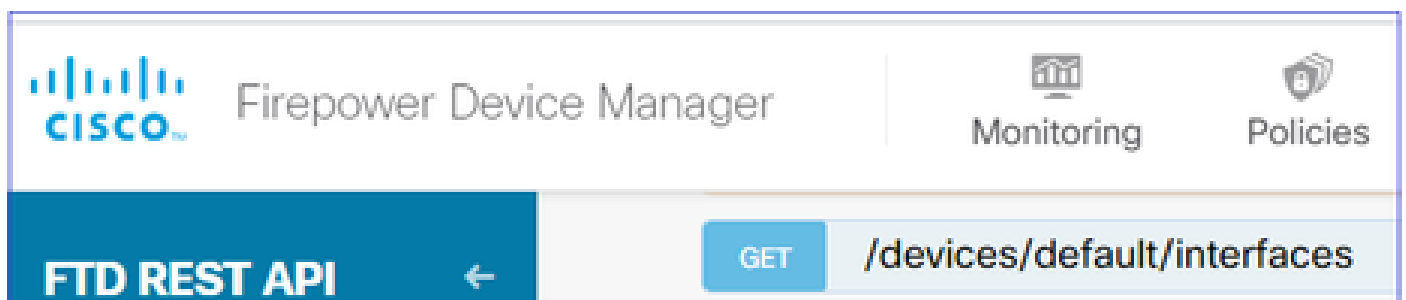


The screenshot shows the Firepower Device Manager interface. The top navigation bar includes the Cisco logo, the text "Firepower Device Manager", and icons for "Monitoring", "Policies", "Objects", and "Device: FP1120-1". On the left, a sidebar menu has "FTD REST API" selected, with sub-items "API Explorer" and "Error Catalog". The main content area displays the results of an API call:

- Request URL:** `https://10.62.148.231/api/fdm/v6/object/snmpusers`
- Response Body:** A JSON object containing details for an SNMP user, including version, name, description, security level, authentication and encryption algorithms and passwords, ID, type, and a self-link.
- Response Code:** 200

4. インターフェイス情報の取得

FDM APIエクスプローラで、「インタフェース」を選択し、次に「/devices/default/interfaces」を選択します。SNMPサーバに接続するインタフェースから情報を収集する必要があります。



The screenshot shows the Firepower Device Manager API Explorer interface. The top navigation bar includes the Cisco logo, the text "Firepower Device Manager", and icons for "Monitoring" and "Policies". The left sidebar menu has "FTD REST API" selected. The main content area shows a "GET" button and the API endpoint path: `/devices/default/interfaces`.

下にスクロールしてTRY IT OUT!ボタンを選択し、APIコールを実行します。コールが成功すると、応答コード200が返されます。レスポンス本文のJSONデータをメモ帳にコピーします。後で、インタフェースに関する情報を入力する必要があります。

The screenshot shows an API Explorer interface. On the left, there is a sidebar with the following items: "FTD REST API" (with a back arrow), "API Explorer", and "Error Catalog". The main area displays the URL "https://10.62.148.231/api/fdm/v6/devices/default/interfaces". Below the URL, the "Response Body" is shown as a JSON object, which is highlighted with a blue border. The JSON data is as follows:

```
{
  "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,

```

Below the response body, the "Response Code" is shown as "200".

JSONデータのインターフェイス「version」、「name」、「id」、および「type」をメモします。
。インターフェイス内部のJSONデータの例：

<#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",

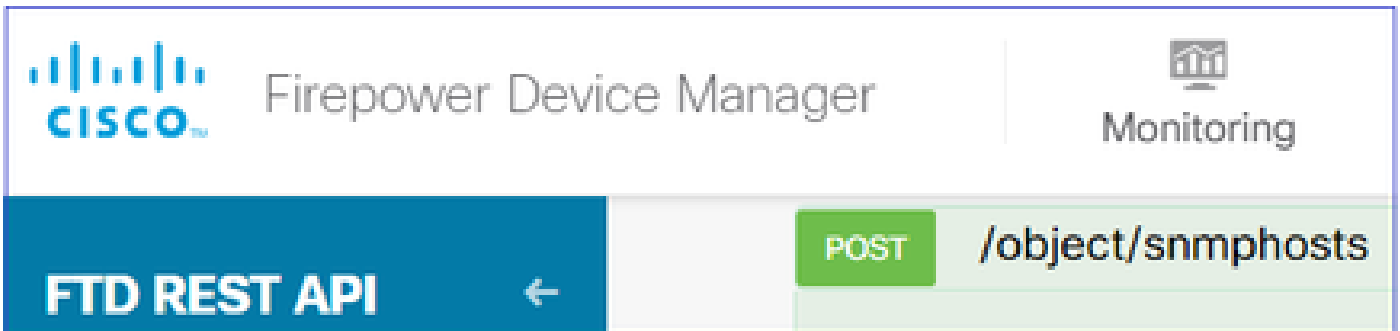
"links": {
  "self": "https://10.62.148.231/api/fdm/v6/devices/default/interfaces/fc3d07d4-49d2-11eb-85a8-65aec636a0fc"
}
},
```

JSONデータから、インターフェイス「inside」にSNMPサーバと関連付ける必要のある次のデータがあることがわかります。

- "バージョン": "kkpkibjlu6qro"
- "名前": "内部",
- "id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
- "type": "physicalinterface",

5.新しいSNMPv3ホストを作成する

FDM APIエクスプローラで「SNMP」を選択し、SNMPで/object/snmphosts/を入力します



このJSONをテンプレートとして使用します。前の手順のデータをコピーし、それに応じてテンプレートに貼り付けます。

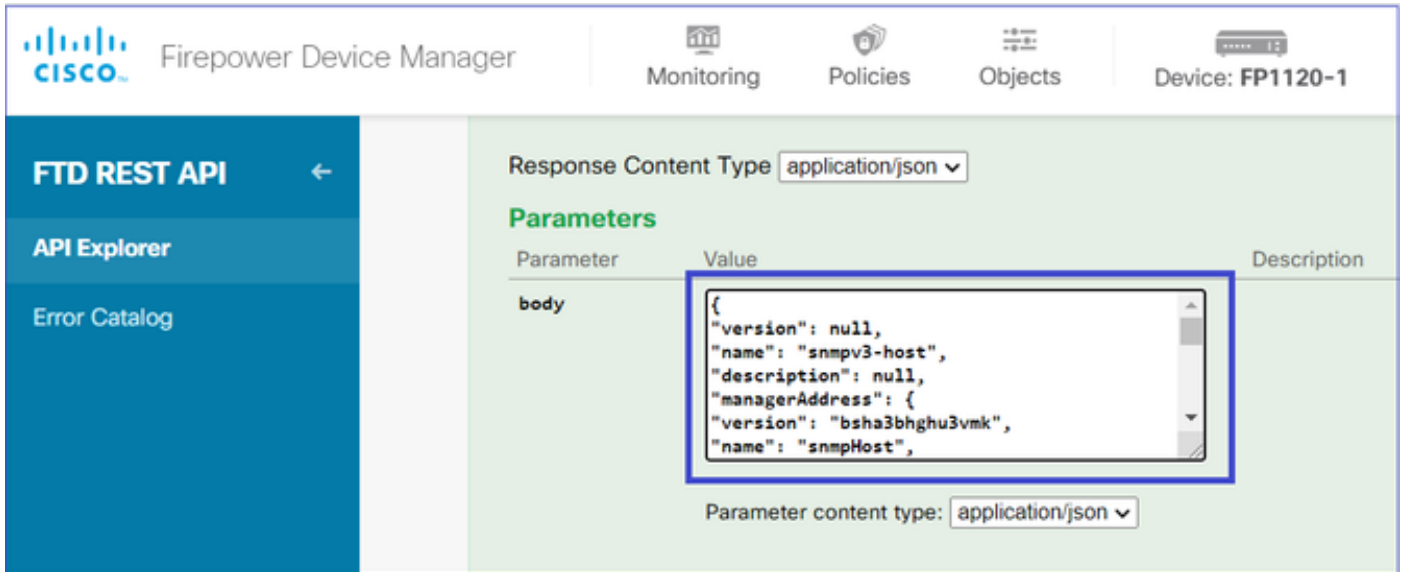
```
{
  "version": null,
  "name": "snmpv3-host",
  "description": null,
  "managerAddress": {
    "version": "bsha3bhghu3vmk",
    "name": "snmpHost",
    "id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
    "type": "networkobject"
  },
  "pollEnabled": true,
  "trapEnabled": true,
  "securityConfiguration": {
    "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：

- managerAddress id、type、version、およびnameの値を、手順1で取得した情報で置き換えます
- authenticationの値を、ステップ2で取得した情報で置き換えます

- interfaceの値を、手順3で取得したデータで置き換えます
- SNMP2の場合、認証はなく、タイプはsnmpv3securityconfigurationではなくsnmpv2csecurityconfigurationです

変更されたJSONデータを本文セクションにコピーします



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 shows 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main content area is titled 'Parameters' and shows a table with columns for 'Parameter', 'Value', and 'Description'. The 'body' parameter is highlighted with a blue box, and its value is a JSON object:

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

Below the table, the 'Parameter content type' is set to 'application/json'.

下にスクロールしてTRY IT OUT!ボタンを選択し、APIコールを実行します。コールが成功すると、応答コード200が返されます。

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": "bmwzw4iw7php7",
      "name": "snmpUser",
      "id": "65da6c50-49df-11eb-a432-e7823944dabc",
      "type": "snmpuser"
    }
  },
}
```

Response Code

```
200
```

FDM GUIに移動し、変更を配置します。SNMP設定の大部分を確認できます。

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

v2cの場合、ユーザを作成する必要はありませんが、次の操作を実行する必要があります。

1. ネットワークオブジェクト構成の作成 (「SNMPv3」セクションの説明と同じ)
2. インターフェイス情報の取得 (「SNMPv3」セクションでの説明と同じ)
3. 新しいSNMPv2cホストオブジェクトの作成

次に、SNMPv2cオブジェクトを作成するJSONペイロードの例を示します。

```
{
  "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": "snmpghost"
}

```

POSTメソッドを使用して、JSONペイロードを配置します。

The screenshot shows the Cisco Firepower Device Manager (FDM) interface. The left sidebar contains 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main area is titled 'Response Content Type' and is set to 'application/json'. Below this, the 'Parameters' section is visible, with a table containing one parameter: 'body'. The value for 'body' is a JSON object:


```

{
  "version": null,
  "name": "snmpv2-Host",
  "description": null,
  "managerAddress": {
    "version": "bsha3bhghu3vmk",
    "name": "snmpv4hostgrp",
  }
}

```

 The 'Parameter content type' is also set to 'application/json'.

下にスクロールしてTRY IT OUT！ボタンを選択し、API呼び出しを実行します。コールが成功すると、応答コード200が返されます。

The screenshot shows the results of an API call in the FDM interface. The 'Request URL' is 'https://10.62.148.231/api/fdm/v6/object/snmpghosts'. The 'Response Body' is a JSON object:


```

{
  "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": "1bfbdf0-4ac6-11eb-a432-e76cd376bca7",
  "type": "snmpghost",
  "links": {
    "self": "https://10.62.148.231/api/fdm/v6/object/snmpghosts/1bfbdf0-4ac6-11eb-a432-e76cd376bca7"
  }
}

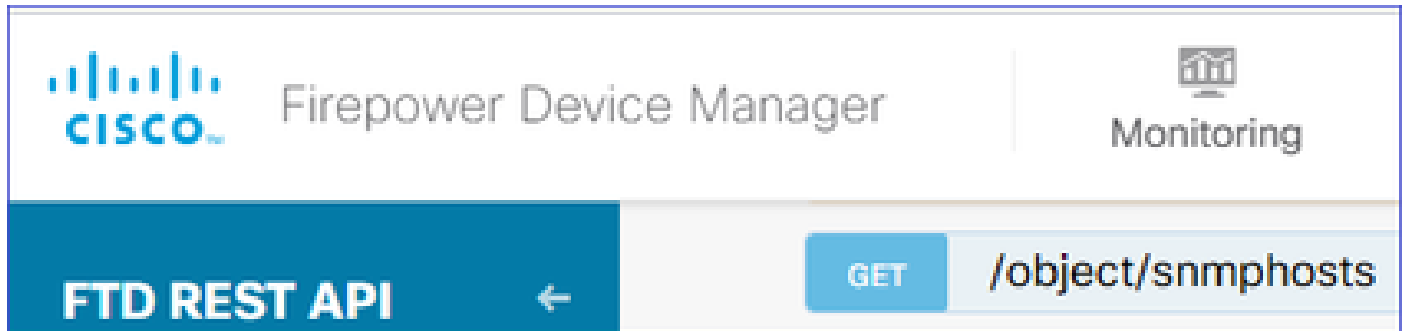
```

 The 'Response Code' is '200'.

SNMP設定の削除

ステップ 1 :

SNMPホスト情報を取得します(SNMP > /object/snmphosts)。



下にスクロールしてTRY IT OUT ! ボタンを選択し、API呼び出しを実行します。コールが成功すると、応答コード200が返されます。

オブジェクトのリストが表示されます。削除するsnmpHostオブジェクトのidをメモします。

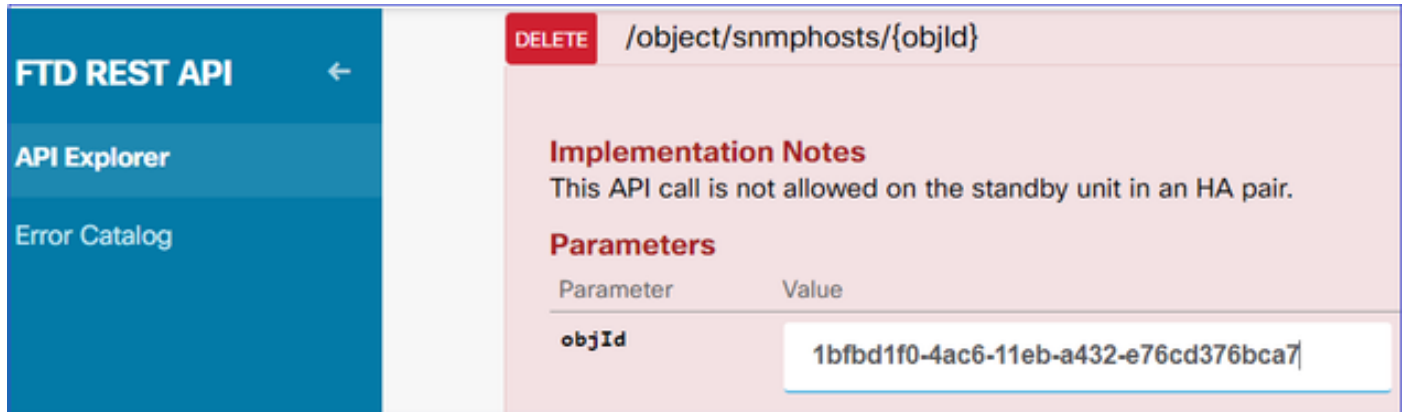
<#root>

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

```
}  
},
```

ステップ 2 :

SNMP > /object/snmphosts{objId}でDELETEオプションを選択します。手順1で収集したIDを貼り付けます。



The screenshot shows the FTD REST API interface. On the left is a navigation menu with 'API Explorer' and 'Error Catalog'. The main area displays the endpoint `/object/snmphosts/{objId}` with a 'DELETE' method. Under 'Implementation Notes', it states: 'This API call is not allowed on the standby unit in an HA pair.' Under 'Parameters', there is a table with one entry: 'objId' with a value of '1bfd1f0-4ac6-11eb-a432-e76cd376bca7'.

Parameter	Value
objId	1bfd1f0-4ac6-11eb-a432-e76cd376bca7

下にスクロールしてTRY IT OUT ! ボタンを選択し、API呼び出しを実行します。コールは応答コード400を返します。

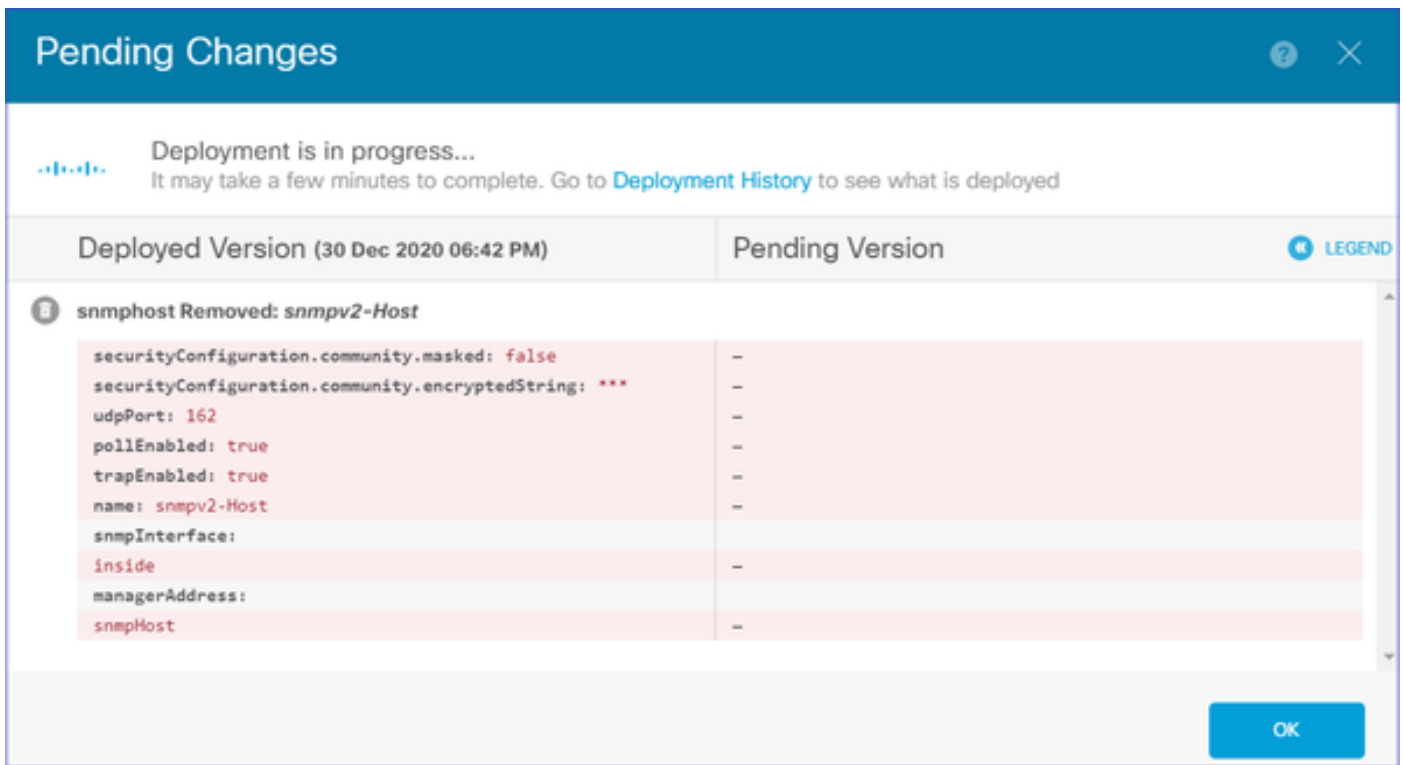


The screenshot shows the response details for the API call. The 'Response Code' is 400. The 'Response Headers' are listed in a JSON object:

```
{  
  "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"  
}
```

ステップ 3 :

変更を展開します。



展開によってホスト情報が削除されます。

```
<#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のsnmpwalkが失敗します。

```
<#root>
```

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

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

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

v3では、この順序でオブジェクトを削除する必要があります。

1. SNMPホスト (成功したリターンコードは204)

2. SNMPユーザ (成功したリターンコードは204)

オブジェクトを誤った順序で削除しようとする、次のエラーが発生します。

```
<#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": ""
      }
    ]
  }
}
```

確認

SNMP v3の確認

展開後、FTD CLIに移動してSNMP設定を確認します。engineID値は自動生成されることに注意してください。

```
<#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テスト

```
<#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の検証

```
<#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の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
```

トラブルシュート

ファイアウォールでトレースによるキャプチャを有効にします。

```
<#root>
```

```
FP1120-1#
```

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

snmpwalkツールを使用して、パケットが表示されることを確認します。

```
<#root>
```

FP1120-1#

show capture

capture CAPI type raw-data trace interface inside

[Capturing - 3137 bytes]

match udp any any eq snmp

キャプチャの内容 :

<#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

SNMPサーバの統計情報カウンタにSNMP GetまたはGet-nextの要求と応答が表示されることを確認します。

<#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

入力パケットをトレースします。パケットは内部NLPインターフェイスに対してUN-NATです。

<#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ルールは、SNMP設定の一部として自動的に展開されます。

```
<#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
```

バックエンドポートで、UDP 4161はSNMPトラフィックをリッスンします。

<#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 :::*

設定が正しくない、または不完全な場合、UN-NATフェーズがないため、入力SNMPパケットはドロップされます。

<#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 syslogは、入力パケットが廃棄されたことを示しています。

<#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.

Q&A

Q. FTD管理インターフェイスを使用してSNMPメッセージを送信できますか。

いいえ。現在はサポートされていません。

関連する機能拡張の不具合:<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu48012>

関連情報

- [Cisco Firepower Threat Defense バージョン 6.7 コンフィギュレーション ガイド \(Firepower Device Manager 用 \)](#)
- [Cisco Firepower Threat Defense REST APIガイド](#)
- [Cisco Firepowerリリースノート、バージョン6.7.0](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。