

Configuration et dépannage du protocole SNMP sur Firepower FDM

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[SNMP v3](#)

[SNMP v2c](#)

[Suppression de la configuration SNMP](#)

[Vérifier](#)

[Vérification SNMP v3](#)

[Vérification de SNMP v2c](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment activer le protocole SNMP (Simple Network Management Protocol) sur Firepower Device Management sur la version 6.7 avec l'API REST.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Threat Defense (FTD) géré par Firepower Device Management (FDM) sur la version 6.7
- Connaissance de l'API REST
- Connaissance du protocole SNMP

Composants utilisés

Firepower Threat Defense (FTD) géré par Firepower Device Management (FDM) sur la version 6.7.

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.


Informations générales

Nouveautés de la version 6.7

L'API REST du périphérique FTD prend en charge la configuration et la gestion du serveur, des utilisateurs, de l'hôte et des groupes d'hôtes SNMP. Avec la prise en charge de l'API REST du périphérique FTD SNMP dans FP 6.7 :

- Un utilisateur peut configurer SNMP via l'API REST du périphérique FTD pour gérer le réseau
- Le serveur SNMP, les utilisateurs et les groupes d'hôtes/hôtes peuvent être ajoutés/mis à jour ou gérés via l'API REST du périphérique FTD.

Les exemples inclus dans le document décrivent les étapes de configuration effectuées par l'Explorateur d'API FDM.

 Remarque : SNMP ne peut être configuré via l'API REST que lorsque FTD exécute la version 6.7 et est géré par FDM

Présentation des fonctionnalités - Prise en charge de l'API REST du périphérique SNMP FTD

- Cette fonctionnalité ajoute de nouveaux points de terminaison d'URL FDM spécifiques au protocole SNMP.
- Ces nouvelles API peuvent être utilisées pour configurer SNMP pour les interrogations et les dérouterments afin de surveiller les systèmes.
- La post-configuration SNMP via les API, les bases d'informations de gestion (MIB) sur les périphériques Firepower, sont disponibles pour les interrogations ou pour la notification de dérouterment sur le client NMS/SNMP.

Terminaux d'API/URL SNMP

| URL | Méthodes | Modèles |
|---|-----------|--------------|
| /devicesettings/default/snmpservers | GET | Serveur SNMP |
| /devicesettings/default/snmpservers/{objId} | PUT, GET | Serveur SNMP |
| /object/snmphosts | POST, GET | Hôte SNMP |
| /object/snmphosts/{objId} | METTRE, | Hôte SNMP |

| | | |
|--------------------------------|----------------------------------|-------------------------|
| | SUPPRIMER, OBTENIR | |
| /object/snmpusergroups | POST, GET | GroupeUtilisateursSNMPU |
| /object/snmpusergroups/{objId} | METTRE, SUPPRIMER, OBTENIR | GroupeUtilisateursSNMPU |
| /object/snmpusers | POST, GET | SNMPUser |
| /object/snmpusers/{objId} | METTRE, SUPPRIMER, OBTENIR | SNMPUser |

Configurer

- L'hôte SNMP dispose de 3 versions principales

- SNMP V1

- SNMP V2C

- SNMP V3

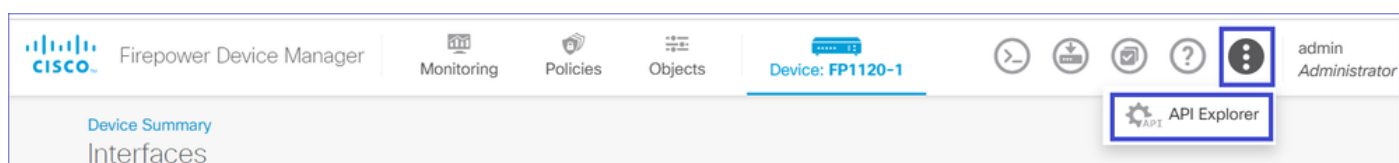
- Chacun d'entre eux a un format spécifique pour « securityConfiguration ».
- Pour V1 et V2C : contient une « chaîne de communauté » et un champ « type » qui identifie la configuration comme V1 ou V2C.
- Pour SNMP V3 : contient un utilisateur SNMP V3 valide et un champ « type » qui identifie la configuration comme étant V3.

SNMP v3

1. Accédez à l'Explorateur d'API FDM

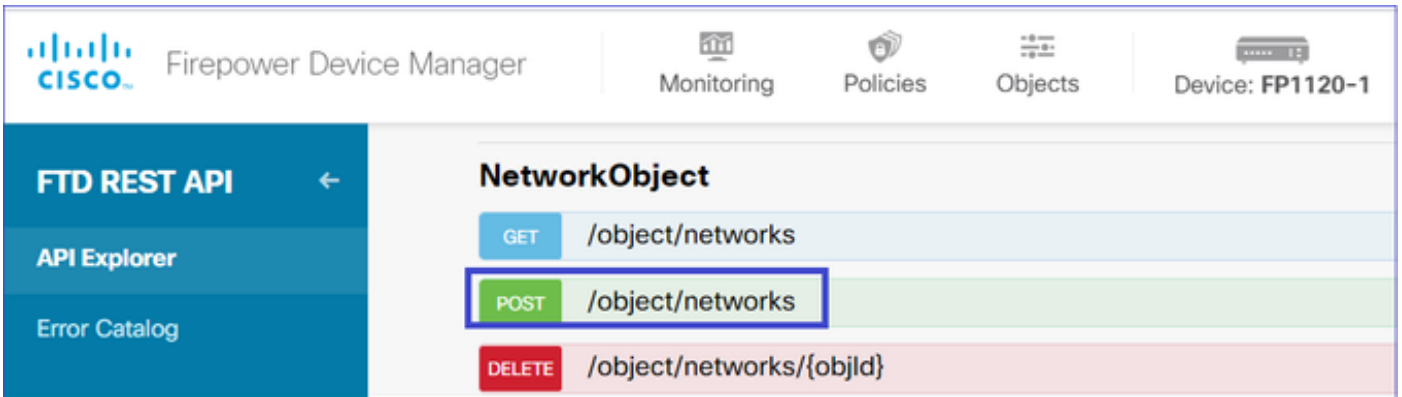
Pour accéder à l'explorateur d'API FDM REST à partir de l'interface utilisateur graphique FDM, sélectionnez les 3 points, puis API Explorer. Vous pouvez également accéder à l'URL

[https://FDM_IP/#!/api-explorer:](https://FDM_IP/#!/api-explorer)



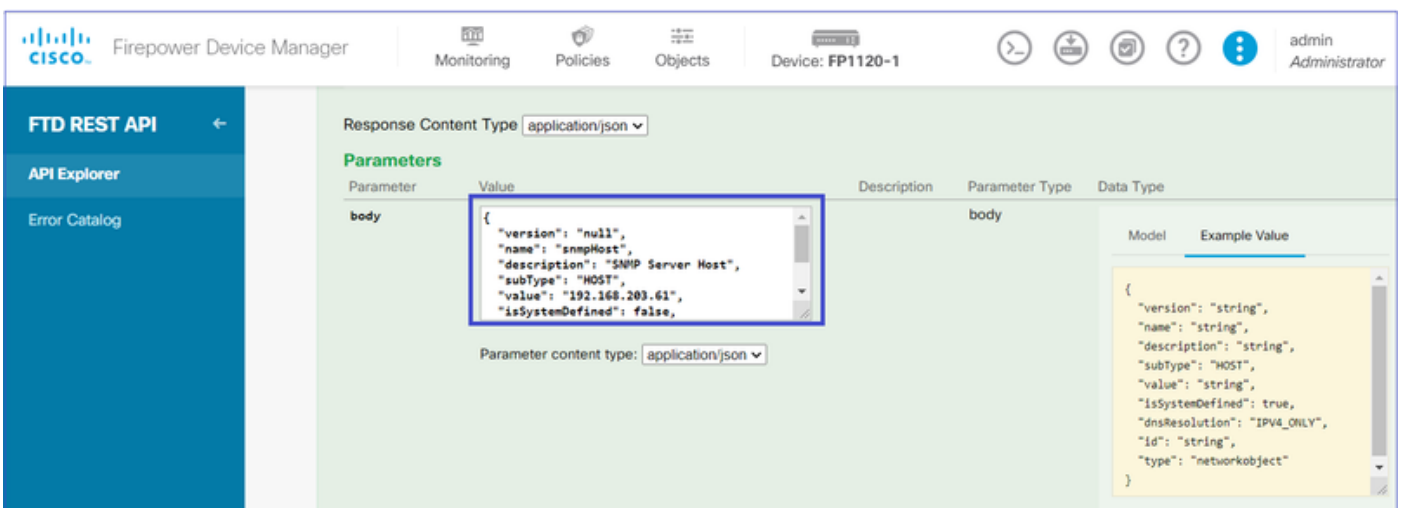
2. Configuration des objets réseau

Créez un nouvel objet réseau pour l'hôte SNMP : dans l'Explorateur d'API FDM, sélectionnez NetworkObject, puis POST /object/networks :



Le format JSON de l'hôte SNMP est le suivant. Collez ce JSON dans la section body et modifiez l'adresse IP sur « value » pour qu'elle corresponde à l'adresse IP de l'hôte SNMP :

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



Faites défiler l'affichage vers le bas et sélectionnez le bouton TRY IT OUT ! pour exécuter l'appel API. Un appel réussi renvoie le code de réponse 200.

TRY IT OUT!

Copiez les données JSON du corps de la réponse vers un bloc-notes. Par la suite, vous devrez compléter les informations relatives à l'hôte SNMP.



The screenshot displays the FTDM REST API Explorer interface. On the left, a sidebar contains the following menu items: "FTD REST API" (with a back arrow), "API Explorer", and "Error Catalog". The main area shows a REST client view for the endpoint `https://10.62.148.231/api/fdm/v6/object/networks`. The "Response Body" section contains the following JSON data:

```
{
  "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"
  }
}
```

The "Response Code" section shows a status of 200.

3. Créez un nouvel utilisateur SNMPv3

Dans l'explorateur d'API FDM, sélectionnez SNMP, puis POST /object/snmpusers

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**

Copiez ces données JSON dans un bloc-notes et modifiez les sections qui vous intéressent (par exemple, « authenticationPassword », « encryptionPassword » ou les algorithmes) :

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

⚠ Attention : les mots de passe utilisés dans les exemples sont uniquement utilisés à des fins de démonstration. Dans un environnement de production, assurez-vous d'utiliser des mots de passe forts

Copiez les données JSON modifiées dans la section body :

Firepower Device Manager

Monitoring Policies Objects Device: FP1120-1 admin Administrator

FTD REST API ←

- API Explorer
- Error Catalog

Response Content Type: application/json

Parameters

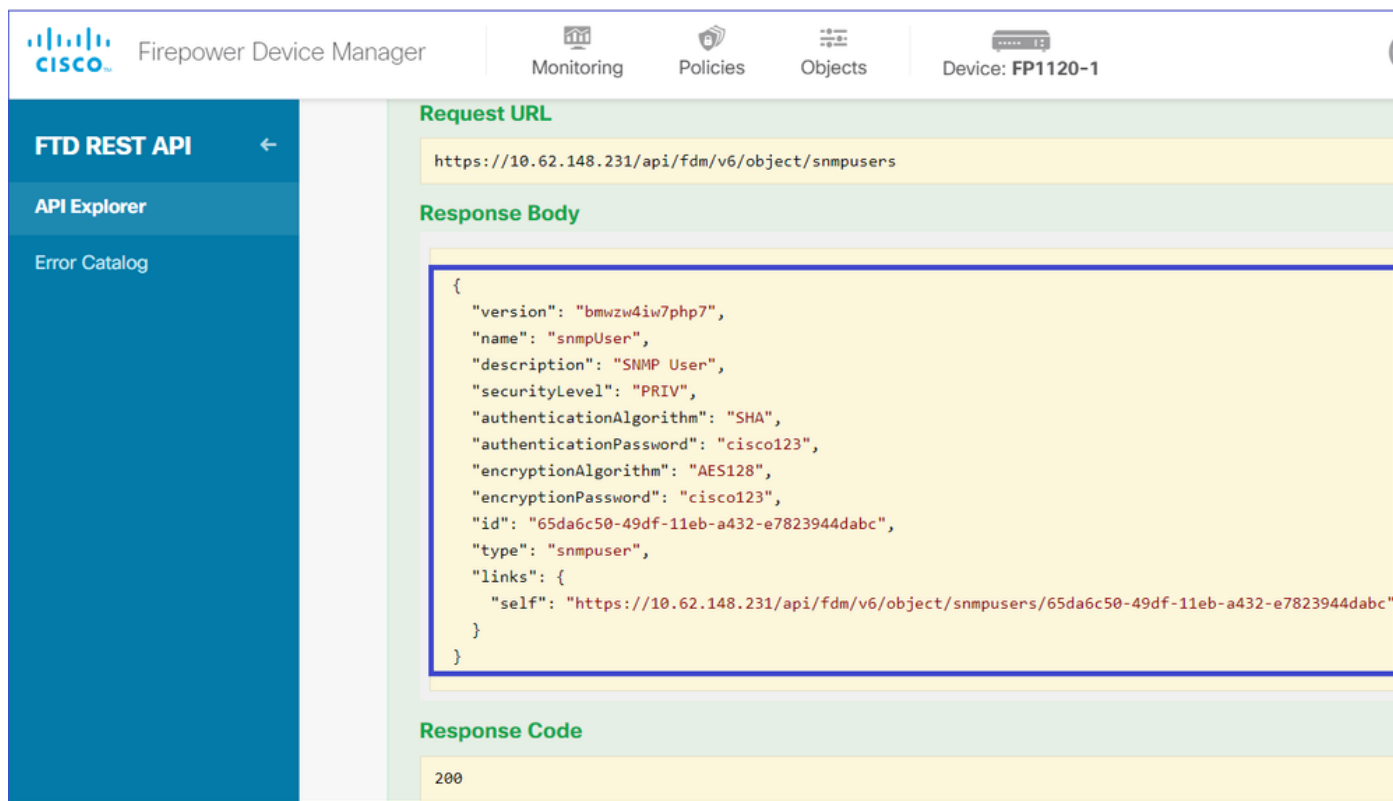
| Parameter | Value | Description | Parameter Type | Data Type |
|-----------|--|-------------|----------------|-----------|
| body | <pre>{ "version": null, "name": "snmpUser", "description": "SNMP User", "securityLevel": "PRIV", "authenticationAlgorithm": "SHA", "authenticationPassword": "cisco123",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

Faites défiler l'écran vers le bas et sélectionnez le bouton TRY IT OUT! pour exécuter l'appel API. Un appel réussi renvoie le code de réponse 200. Copiez les données JSON du corps de la réponse vers un bloc-notes. Par la suite, vous devrez compléter les informations relatives à l'utilisateur SNMP.

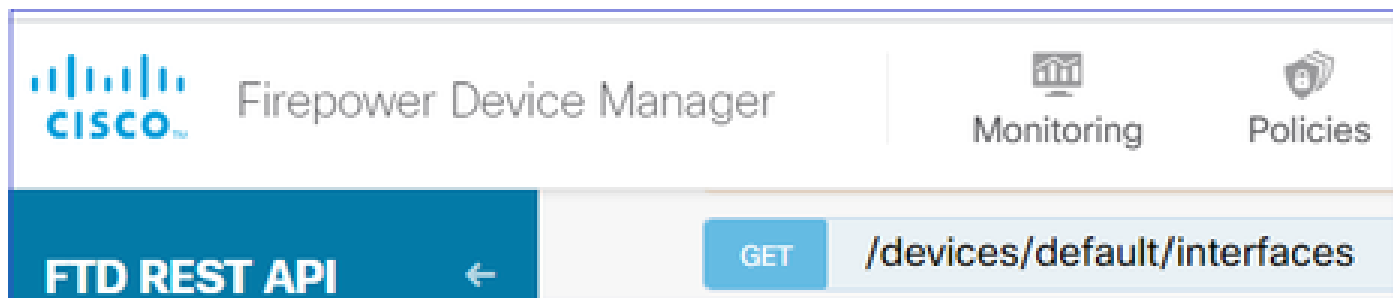


The screenshot shows the Firepower Device Manager REST API interface. The top navigation bar includes the Cisco logo, the text "Firepower Device Manager", and icons for "Monitoring", "Policies", and "Objects". The device name "Device: FP1120-1" is displayed on the right. The left sidebar contains "FTD REST API" (selected), "API Explorer", and "Error Catalog". The main content area is divided into three sections: "Request URL" with the value "https://10.62.148.231/api/fdm/v6/object/snmpusers", "Response Body" containing a JSON object, and "Response Code" with the value "200".

```
{
  "version": "bmwz4iw7php7",
  "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"
  }
}
```

4. Obtenir les informations d'interface

Dans l'Explorateur d'API FDM, sélectionnez Interface, puis GET /devices/default/interfaces. Vous devez collecter des informations à partir de l'interface qui se connecte au serveur SNMP.



The screenshot shows the Firepower Device Manager REST API interface. The top navigation bar includes the Cisco logo, the text "Firepower Device Manager", and icons for "Monitoring" and "Policies". The left sidebar contains "FTD REST API" (selected). The main content area shows the endpoint "/devices/default/interfaces" with a "GET" button next to it.

Faites défiler l'écran vers le bas et sélectionnez le bouton TRY IT OUT! pour exécuter l'appel API. Un appel réussi renvoie le code de réponse 200. Copiez les données JSON du corps de la réponse vers un bloc-notes. Par la suite, vous devrez fournir des informations sur l'interface.

FTD REST API ←

API Explorer

Error Catalog

https://10.62.148.231/api/fdm/v6/devices/default/interfaces

Response Body

```

"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,

```

Response Code

200

Notez la version, le nom, l'ID et le type de l'interface à partir des données JSON. Exemple de données JSON provenant de l'interface interne :

<#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
}
},

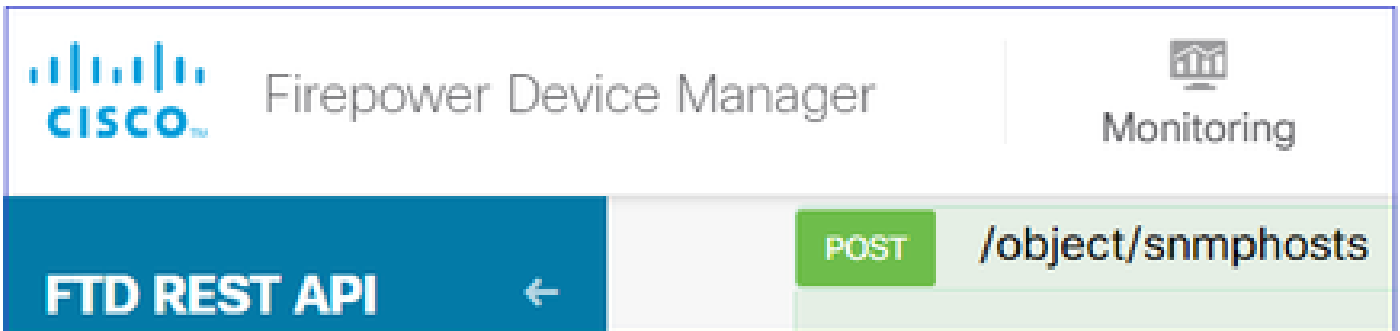
```

À partir des données JSON, vous pouvez voir que l'interface « inside » a ces données qui doivent être associées au serveur SNMP :

- "version" : "kkpkibjlu6qro"
- "name" : "inside",
- "id" : "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
- "type" : "interface physique",

5. Créez un nouvel hôte SNMPv3

Dans FDM API Explorer, sélectionnez SNMP, puis POST /object/snmphosts/ sous SNMP



Utilisez ce fichier JSON comme modèle. Copiez et collez les données des étapes précédentes dans le modèle en conséquence :

```
{
  "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"
}
```

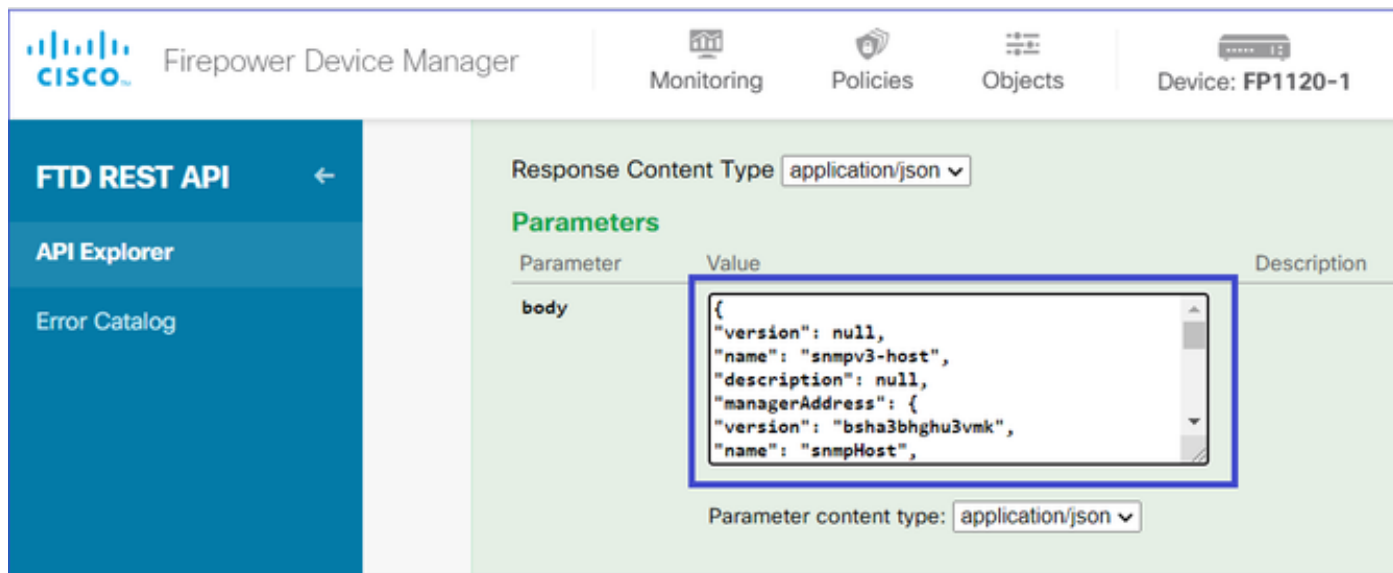
Remarque :

- Remplacez la valeur dans managerAddress id, type, version et name par les informations que vous avez reçues de l'étape 1
- Remplacez la valeur de l'authentification par les informations que vous avez reçues à l'étape

2

- Remplacez la valeur de l'interface par les données que vous avez reçues à l'étape 3
- Pour SNMP2, il n'existe aucune authentification et le type est snmpv2csecurityconfiguration au lieu de snmpv3securityconfiguration

Copier les données JSON modifiées dans la section body



The screenshot shows the Cisco Firepower Device Manager REST API interface. The left sidebar contains 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main area shows 'Response Content Type' set to 'application/json'. Below this is a 'Parameters' table with columns 'Parameter', 'Value', and 'Description'. The 'body' parameter is highlighted with a blue box and contains the following JSON:

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

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

Faites défiler l'écran vers le bas et sélectionnez le bouton TRY IT OUT! pour exécuter l'appel API. Un appel réussi renvoie le code de réponse 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": "bmwzw4iw7php7",
      "name": "snmpUser",
      "id": "65da6c50-49df-11eb-a432-e7823944dabc",
      "type": "snmpuser"
    }
  }
},
```

Response Code

200

Accédez à l'interface utilisateur graphique de FDM et déployez les modifications. Vous pouvez voir la plupart des configurations SNMP :

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 |
|--|---|
| + Network Object Added: <i>snmpHost</i> | |
| - | subType: Host |
| - | value: 192.168.203.61 |
| - | isSystemDefined: false |
| - | dnsResolution: IPV4_ONLY |
| - | description: SNMP Server Host |
| - | name: snmpHost |
| + snmpHost Added: <i>snmpv3-host</i> | |
| - | udpPort: 162 |
| - | pollEnabled: true |
| - | trapEnabled: true |
| - | name: snmpv3-host |
| snmpInterface: | inside |
| managerAddress: | snmpHost |
| - | snmpHost |
| securityConfiguration.authentication: | snmpUser |
| - | snmpUser |

MORE ACTIONS ▾
CANCEL
DEPLOY NOW ▾

SNMP v2c

Pour v2c, vous n'avez pas besoin de créer un utilisateur, mais vous devez tout de même :

1. Créer une configuration d'objet réseau (comme décrit dans la section SNMPv3)
2. Obtenir les informations d'interface (comme décrit dans la section SNMPv3)
3. Créer un nouvel objet hôte SNMPv2c

Voici un exemple de charge utile JSON qui crée un objet 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": "snmpghost"
}

```

Utilisez la méthode POST pour déployer la charge utile JSON :

The screenshot shows the Cisco Firepower Device Manager interface. The left sidebar contains 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main area is titled 'FTD REST API' and shows a configuration for a REST API call. The 'Response Content Type' is set to 'application/json'. Under 'Parameters', there is a table with one row: 'body' with a value of a JSON object. The JSON object is:


```

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

```

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

Faites défiler l'affichage vers le bas et sélectionnez le bouton TRY IT OUT ! pour exécuter l'appel API. Un appel réussi renvoie le code de réponse 200.

The screenshot shows the results of the REST API call. The left sidebar is the same as in the previous screenshot. The main area shows the 'Request URL' as 'https://10.62.148.231/api/fdm/v6/object/snmpghosts'. Below that, the 'Response Body' is displayed as 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": "1bfbdf1f0-4ac6-11eb-a432-e76cd376bca7",
  "type": "snmpghost",
  "links": {
    "self": "https://10.62.148.231/api/fdm/v6/object/snmpghosts/1bfbdf1f0-4ac6-11eb-a432-e76cd376bca7"
  }
}

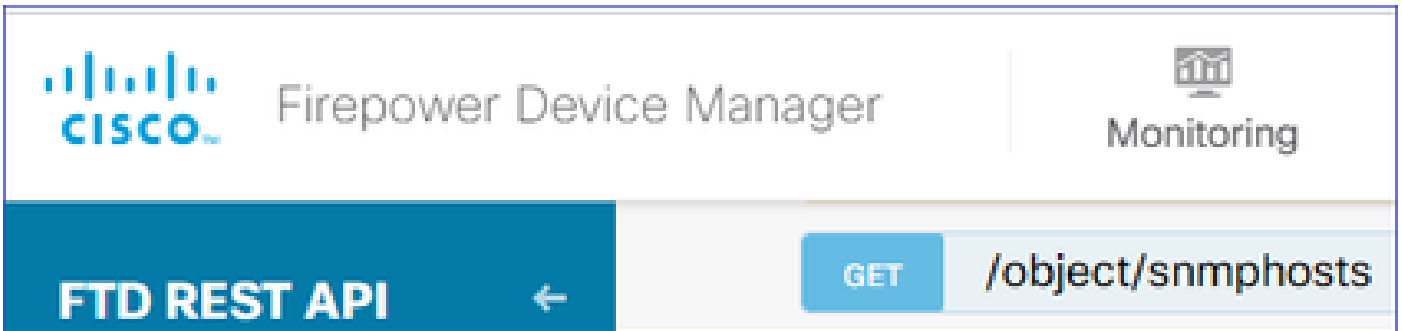
```

 At the bottom, the 'Response Code' is shown as '200'.

Suppression de la configuration SNMP

Étape 1.

Obtenez les informations sur l'hôte SNMP (SNMP > /object/snmphosts) :



Faites défiler l'affichage vers le bas et sélectionnez le bouton TRY IT OUT ! pour exécuter l'appel API. Un appel réussi renvoie le code de réponse 200.

Vous obtenez une liste d'objets. Notez l'ID de l'objet snmpHost que vous souhaitez supprimer :

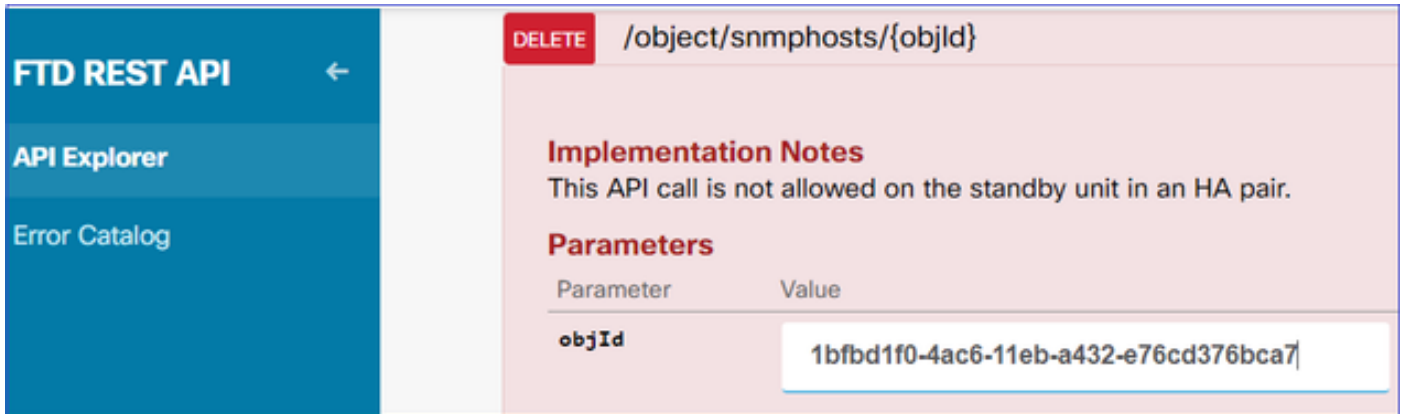
```
<#root>
```

```
{
  "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"
```

```
}  
},
```

Étape 2.

Choisissez l'option DELETE dans SNMP > /object/snmphosts{objId}. Collez l'ID que vous avez collecté à l'étape 1 :



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 red '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.

| Parameter | Value |
|--------------------|---|
| <code>objId</code> | <code>1bfbd1f0-4ac6-11eb-a432-e76cd376bca7</code> |

Faites défiler l'affichage vers le bas et sélectionnez le bouton TRY IT OUT ! pour exécuter l'appel API. L'appel renvoie le code de réponse 400.

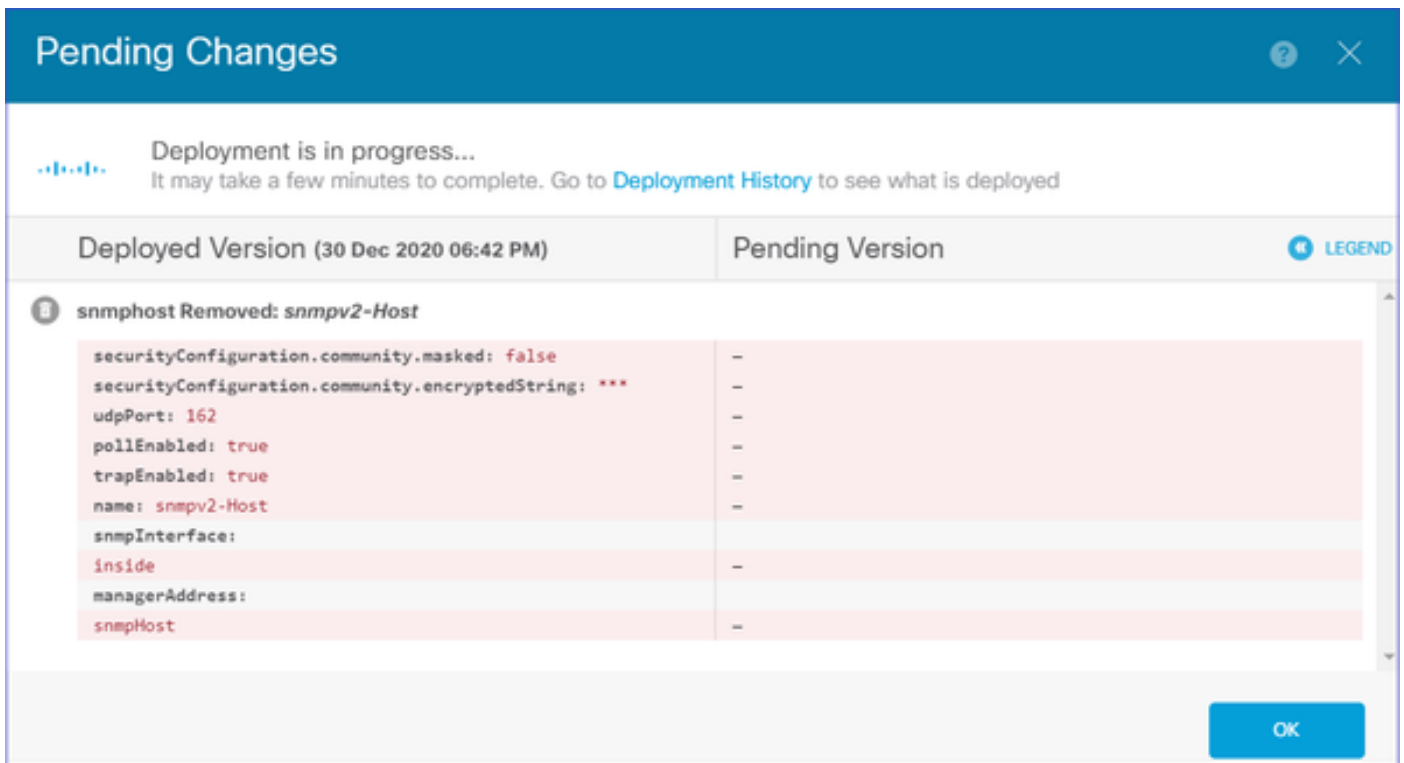


The screenshot shows the response details for the API call. It displays a 'Response Code' of 400 and a list of 'Response Headers' in JSON format.

```
{  
  "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"  
}
```

Étape 3.

Déployez la modification :



Le déploiement supprime les informations d'hôte :

```
<#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 pour v2c échoue :

```
<#root>
```

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

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

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

Pour v3, vous devez supprimer les objets dans cet ordre.

1. Hôte SNMP (le code de retour réussi est 204)


```
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-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
```

test de snmpwalk

```
<#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)K9"
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
...
```

Vérification de SNMP v2c

```
<#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 pour 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.
```

```
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
```

Dépannage

Activez la capture avec trace sur le pare-feu :

```
<#root>
```

```
FP1120-1#
```

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

Utilisez l'outil snmpwalk et vérifiez que vous pouvez voir les paquets :

```
<#root>
```

FP1120-1#

show capture

capture CAPI type raw-data trace interface inside

[Capturing - 3137 bytes]

match udp any any eq snmp

Le contenu de la capture :

<#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 |

Vérifiez que les compteurs de statistiques du serveur SNMP affichent les requêtes et réponses Get ou Get-next SNMP :

<#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

Suivre un paquet entrant. Le paquet est UN-NAT vers l'interface NLP interne :

<#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

La règle NAT est déployée automatiquement dans le cadre de la configuration 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

Sur le port principal, UDP 4161 écoute le trafic 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 :::*

En cas de configuration incorrecte ou incomplète, le paquet SNMP entrant est abandonné car il n'y a pas de phase UN-NAT :

<#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

Les syslog FTD LINA indiquent que le paquet entrant est rejeté :

<#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.

Informations connexes

- [Guide de configuration de Cisco Firepower Threat Defense pour Firepower Device Manager, version 6.7](#)
- [Guide de l'API REST de Cisco Firepower Threat Defense](#)
- [Notes de version de Cisco Firepower, version 6.7.0](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.