

Firepower چمانرب تارادصا نم ققحتلا

تايوتحمل

[قمدقملا](#)

[قيساسالا تابلطتملا](#)

[تابلطتملا](#)

[قمدختسملا تانوكملا](#)

[چماربلا تارادصا نم ققحتلا](#)

[FMC چمانرب رادصا](#)

[FMC مدختسم قهچاو](#)

[FMC رماوأل رطس قهچاو](#)

[FMC REST-API](#)

[اهجالصاو FMC ءاطخأ فاشكتسا فلم](#)

[FTD و Firepower Module CLI](#)

[اهجالصاو FirePOWER و FTD قيطمنلا ءدجولا ءاطخأ فاشكتسا فلم](#)

[FDM چمانرب رادصا](#)

[FDM مدختسم قهچاو](#)

[FDM REST API](#)

[FTD في رماوأل رطس قهچاو](#)

[FTD SNMP](#)

[FTD Trouble Hot فلم](#)

[FXOS چمانرب رادصا](#)

[FCM مدختسم قهچاو](#)

[FxoS نم \(CLI\) رماوأل رطس قهچاو](#)

[FXOS REST-API](#)

[FXOS -ب صاخلا SNMP لوكوتورب](#)

[FXOS Chassis Show-tech فلم](#)

[FTD چمانرب رادصا](#)

[FTD في رماوأل رطس قهچاو](#)

[FTD SNMP](#)

[FMC مدختسم قهچاو](#)

[FMC REST API](#)

[FDM مدختسم قهچاو](#)

[FDM REST-API](#)

[اهجالصاو FTD ءاطخأ فاشكتسا فلم](#)

[FCM مدختسم قهچاو](#)

[FxoS نم \(CLI\) رماوأل رطس قهچاو](#)

[FXOS REST-API](#)

[FXOS Chassis Show-tech فلم](#)

[ASA چمانرب رادصا](#)

[ASA رماوأل رطس قهچاو](#)

[ASA SNMP](#)

[ASA Show-tech فلم](#)

[FCM مدختسم ةهجاو](#)

[Fxos نم \(CLI\) رماوأل رطس ةهجاو](#)

[FXOS REST-API](#)

[FXOS Chassis Show-tech فلم](#)

[ةيظمنلا Firepower ةدحو جم انرب رادصا](#)

[FMC مدختسم ةهجاو](#)

[FMC REST-API](#)

[Firepower ةيظمنلا ةدحولل \(CLI\) رماوأل رطس ةهجاو](#)

[اهحالص او ةيظمنلا Firepower ةدحو ءاطخأ فاشكتسا فلم](#)

[ASA رماوأل رطس ةهجاو](#)

[ASA Show-tech فلم](#)

[SRU و VDB و جم انرب ل اارادصا نم ققحتلا](#)

[\(SNORT\) قي م علا مزحل ا صحف كرحم رادصا](#)

[FMC مدختسم ةهجاو](#)

[FMC REST-API](#)

[FDM مدختسم ةهجاو](#)

[FDM REST API](#)

[FTD او Firepower CLI](#)

[اهحالص او FirePOWER او FTD ةيظمنلا ةدحول ا ءاطخأ فاشكتسا فلم](#)

[\(VDB\) تارغللا تانايب ةدعاق رادصا](#)

[FMC مدختسم ةهجاو](#)

[FMC رماوأل رطس ةهجاو](#)

[FMC REST-API](#)

[اهحالص او FMC ءاطخأ فاشكتسا فلم](#)

[FDM مدختسم ةهجاو](#)

[FDM REST API](#)

[FTD او Firepower Module CLI](#)

[اهحالص او FirePOWER او FTD ةيظمنلا ةدحول ا ءاطخأ فاشكتسا فلم](#)

[ل فطتلا ةدعاق ثي دحت اارادصا](#)

[FMC مدختسم ةهجاو](#)

[FMC رماوأل رطس ةهجاو](#)

[FMC REST-API](#)

[اهحالص او FMC ءاطخأ فاشكتسا فلم](#)

[FDM مدختسم ةهجاو](#)

[FDM REST API](#)

[FTD او Firepower Module CLI](#)

[اهحالص او FirePOWER او FTD ةيظمنلا ةدحول ا ءاطخأ فاشكتسا فلم](#)

[ة فورعم تالكشم](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

ةغيص ةيجمرب FirePOWER نم ققحتلا ةقيثوا اذه فص ي.

ةيساسأل اابلطتملا

تاب لطلت مالا

REST-API و SNMP و ةيساس الال جت نمل ال ةفر عم

ةمدخت سمال تانوك مالا

ةصاخ ةيل م عم ةئيب يف ةدوجوم ال ةزهجال نم دنن سمال اذ ه يف ةدراول تامول عمل ال ءاشن ان م ت تناك اذا (يفضار ت ف). حوس مم نيوك ت ب دنن سمال اذ ه يف ةمدخت سمال ةزهجال ال عيم ج ت ادب رما ي ال لم ت حم ال ري ثا تلل كم ه ف نم دكا ت ف ، لي غ ش ت ال دي ق ك ت ك ب ش

ةيل ال ال ةيل م ال تانوك م ال او ج م ارب ال تاراد صا ال دنن سمال اذ ه يف ةدراول تامول عمل ال دنن س ت

- Firepower 11xx
- Firepower 21xx
- Firepower 31xx
- Firepower 41xx
- Firepower (FMC) ةرادا زكرم 7.1.x راد صا ال
- Firepower (FXOS) 2.11.1.x ةع س وت لل لباق ال لي غ ش ت ال ما ظن
- Firepower (FDM) 7.1.x زا ه ر ي دم
- Firepower 7.1.x دي ه ت دض عاف دل ا ج م ان رب
- ASA 9.17.x

ج م ارب ال تاراد صا نم ققحت ال

FMC ج م ان رب راد صا

ةيل ال ال تاراي خ ال مادخت س اب FMC ج م ان رب راد صا نم ققحت ال نكم ي

- FMC م دخت سم ةه جاو
- FMC رم او ا رطس ةه جاو
- REST تاق ي ب ط ت ةج م رب ةه جاو ب ل ط
- اهال ص او FMC ءاط خ ا فاش ك ت س ا ف ل م
- Firepower Module CLI او FTD
- اهال ص او Firepower او FTD ةي ط م ن ال ةد ح و ل ا ءاط خ ا فاش ك ت س ا ف ل م

FMC م دخت سم ةه جاو

FMC م دخت سم ةه جاو ال ع FMC ج م ان رب راد صا نم ققحت ال ال ةيل ال ال تاراد صا ال ع ب ت ا

ل: و ح > تام ي ل ع ت ر ت خ ا 1.

Name	admin	No	No	🔍 ✎ 🗑️
Access Controlled User Statistics Provides traffic and intrusion event statistics by user				
Application Statistics Provides traffic and intrusion event statistics by application				
Application Statistics (7.1.0) Provides application statistics	admin	No	No	🔍 ✎ 🗑️
Connection Summary Provides tables and charts of the activity on your monitored network segment organized by different criteria	admin	No	No	🔍 ✎ 🗑️
Detailed Dashboard Provides a detailed view of activity on the appliance	admin	No	No	🔍 ✎ 🗑️
Detailed Dashboard (7.0.0) Provides a detailed view of activity on the appliance	admin	No	No	🔍 ✎ 🗑️
Files Dashboard Provides an overview of Malware and File Events	admin	No	No	🔍 ✎ 🗑️
Security Intelligence Statistics Provides Security Intelligence statistics	admin	No	No	🔍 ✎ 🗑️
Summary Dashboard Provides a summary of activity on the appliance	admin	No	Yes	🔍 ✎ 🗑️

2. جمانربلا رادصا نم ققحتلا:

Model	Cisco Firepower Management Center 4600
Serial Number	001234
Software Version	7.1.0 (build 90)
OS	Cisco Firepower Extensible Operating System (FX-OS) 2.11.1 (build154)
Snort Version	2.9.19 (Build 92)
Snort3 Version	3.1.7.1 (Build 108)
Rule Update Version	2022-05-02-003-vrt
Rulepack Version	2703
Module Pack Version	3070
LSP Version	lsp-rel-20220502-1613
Geolocation Update Version	2022-04-25-002
VDB Version	build 354 (2022-04-27 19:39:56)
Hostname	FMC-4600-2

FMC رماو رطس ةهجاو

FMC ل (CLI) رماوأل رطس ةهجاو ىلع FMC جمانرب رادصا نم ققحتلا تاوطخلا هذه عبتا.

جمانربلا رادصا راعشلا ضرعي. مكنحتلا ءدحو لاصتا و SSH ربع FMC ىلى لوصولا.

Cisco Firepower Extensible Operating System (FX-OS) v2.11.0 (build 154)
Cisco Secure Firewall Management Center 4600 v7.1.0 (build 90)

2. CLI ىلع **show version** رمالا ليغشتب مق:

> **show version**

```
-----[ FMC-4600-2.cisco.com ]-----
Model                : Cisco Firepower Management Center 4600 (66) Version 7.1.0 (Build 90)
UUID                 : a10ed34e-d127-11e8-b440-728439d95305
Rules update version : 2022-05-02-003-vrt
LSP version          : lsp-rel-20220502-1613
VDB version          : 354
-----
```

FMC REST-API

مدخستسأ FMC REST-API ب ل ط ل ل الخ نم FMC جم ان رب رادصا نم ق قحتل ل تاوطلخ ال هذه عبتا
curl: مادختسإ متي ، لاثم ال اذه يف . جم ان رب ال رادصا نم ق قحتل ل REST-API لي مع

1. زيمم ةقداصم زمر ب ل ط .

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H  
'Authentication: Basic' -u 'admin:Cisco123' | grep -i X-auth-access-token  
<X-auth-access-token: 9408fe38-c25c-4472-b7e6-3571bb4e2b8d
```

2. م ال عتس ال اذه يف X-auth-access ل زيمم ال ل وصولا زمر مدختسأ .

```
# curl -k -X GET 'https://192.0.2.1/api/fmc_platform/v1/info/serverversion' -H 'X-auth-access-  
token: 9408fe38-c25c-4472-b7e6-3571bb4e2b8d' | python -m json.tool  
{  
  "links": {  
    "self": "https://192.0.2.1/api/fmc_platform/v1/info/serverversion?offset=0&limit=25"  
  },  
  "items": [  
    {  
      "serverVersion": "7.1.0 (build 90)",  
      "geoVersion": "2022-04-25-002",  
      "vdbVersion": "build 354 ( 2022-04-27 19:39:56 )",  
      "sruVersion": "2022-05-04-001-vrt",  
      "lspVersion": "lsp-rel-20220504-1121",  
      "type": "ServerVersion"  
    }  
  ],  
  "paging": {  
    "offset": 0,  
    "limit": 25,  
    "count": 1,  
    "pages": 1  
  }  
}
```

جارخ ال ا قيس ننتل رم اوأ ال ةلس لس نم "python -m json.tool | عزج ال مادختسإ متي : ةطلخ الم
ي راي تخإ وهو JSON طم نب

اه حالص او FMC ءاطخأ فاشكتسأ فلم

اه حالص او ءاطخأ ال فاشكتسأ فلم يف FMC جم ان رب رادصا نم ق قحتل ل تاوطلخ ال هذه عبتا:

1. دل جم ال ال ل ل ق ت ناو اه حالص او ءاطخأ ال فاشكتسأ فلم حت فا .
<filename>.tar/results-
<date>—xxxxx/dir-archive/etc/sf/
2. swversion و swbuild حيت افم ال ال ع يوتحت يتل رطس ال نع ثح باو ims.conf فلم ال حت فا .

```
# pwd  
/var/tmp/results-05-06-2022--199172/dir-archives/etc/sf/  
# cat ims.conf | grep -E "SWVERSION|SWBUILD"  
SWVERSION=7.1.0  
SWBUILD=90
```

FTD أو Firepower Module CLI

أو FTD نم (رم اوأ ال رطس ةه جاو) CLI ال ع FMC جم ان رب رادصا نم ق قحتل ل تاوطلخ ال هذه عبتا
FirePOWER: ةدح و ة صاخ ال (CLI) رم اوأ ال رطس ةه جاو

1. FirePOWER دحو ةلاح ي ف .مكحتلا ةدحو لاصتا و SSH لال خ نم FTD لى لوصولا .
 (CLI) رم اوأل رطس ةهجاو نم و SSH، ربع ةيظمنلا ةدحو لى لوصولاب مق ،ةيظمنلا
 session sfr رمأل ربع ASA ب ةصاخلا
 expert رمأل ليغشتب مق .

```
> expert
admin@fpr2k-1:~$
```

3. نم لقا و FTD لى لى `/ngfw/var/sf/detection_engines/<uuid>/ngfw.rules` لقا رمأل ليغشتب مق .
 فص صحفو FirePOWER ةيظمنلا ةدحو لى لى `/var/sf/detection_engines/<uuid>/ngfw.rules`
 رادصا DC:

```
admin@fpr2k-1:~$ less /ngfw/var/sf/detection_engines/65455e3a-c879-11ec-869a-
900514578f9f/ngfw.rules
##### ngfw.rules ##### #
# AC Name : FTD-ACP-1652807562 # Policy Exported : Tue May 17 17:29:43 2022 (UTC) # File Written
: Tue May 17 17:31:10 2022 (UTC) # # DC Version : 7.1.0-90 OS: 90
# SRU : 2022-05-11-001-vrt
# VDB : 354
#
#####
...
```

اهحالص او FirePOWER و FTD ةيظمنلا ةدحو لى لى فاشكتسا فلم

ةدحو ةاطخا فاشكتسا فلم و FTD ي ف FMC جم انرب رادصا نم ققحتلل تاوطخلا هذه عبتا
 اهحالص او ةيظمنلا FirePOWER:

1. فاشكتسا <filename> دلجملا لى لى لقتنا و اهحالص او ةاطخا لى فاشكتسا فلم حتفا .
 مت اذا `.tar/results-<date>—xxxx/file-contents/ngfw/var/sf/detection-engines/<UUID>/` ةاطخا
 دلجملا لى لى لقتنا ، FirePOWER ةيظمنلا ةدحو لى لى فاشكتسا .
`<filename>-troubleshooting .tar/results-<date>—xxxx/file-contents/var/sf/detection-
 engines/<UUID>/`
 2. DC رادصا فص دحو `ngfw.rules` فلم حتفا .

```
# pwd
/var/tmp/results-05-06-2022--163203/file-contents/ngfw/var/sf/detection_engines/5e9fa23a-5429-
11ec-891e-b19e407404d5
# cat ngfw.rules
##### ngfw.rules ##### #
# AC Name : FTD-ACP-1652807562
# Policy Exported : Tue May 17 17:29:43 2022 (UTC)
# File Written : Tue May 17 17:31:10 2022 (UTC)
#
# DC Version : 7.1.0-90 OS: 90
# SRU : 2022-05-11-001-vrt
# VDB : 354
#
#####
...
```

FDM جم انرب رادصا


```

"refresh_token" :
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoImGU0NGIYzQtZDI0Mi0xMWVjLTK4ZWmtYTl1OTlkZGMWn2Y0IiwibmVjaWkiOiJjb2t1b1R5cGUlOiJKV1RFUmVmcVzaCI6InVzZXJvdWlkIjoiYTU3ZGVmMjgtY2M3MzIiwic2VzYmFtZSI6ImFkbWluIn0.AvgA0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw" ,
"token_type": "Bearer"
}

```

2. مثال عتسالا اذ ف لوصل ل زي مالا زملا ة مي ق مدخت سا :

```

# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoImGU0NGIYzQtZDI0Mi0xMWVjLTK4ZWmtNDd1ZTQwODkwMDVjIiwibmVjaWkiOiJjb2t1b1R5cGUlOiJKV1RFUmVmcVzaCI6InVzZXJvdWlkIjoiYTU3ZGVmMjgtY2M3MzIiwic2VzYmFtZSI6ImFkbWluIn0.1JLmHddJ2jaVRmpdXF6gg48qdBcyRuit94DLobCJ9LI' | grep -i software
"softwareVersion" : "7.1.0-90",
"softwareVersion" : "7.1.0-90",

```

FTD ف رم اوألا رطس ة هجاو

م س ق ل ا ف ة دراوال تاوطلخا ع بتا

FTD SNMP

م س ق ل ا ف ة دراوال تاوطلخا ع بتا

FTD Trouble Hot فلم

م س ق ل ا ف ة دراوال تاوطلخا ع بتا

FCM مدختسم ة هجاو

م س ق ل ا ف ة دراوال تاوطلخا ع بتا. Firepower 4100 و Firepower 9300 Series ل ع ف C M رفوت ي

Fxos نم (CLI) رم اوألا رطس ة هجاو

م س ق ل ا ف ة دراوال تاوطلخا ع بتا

FXOS REST-API

م س ق ل ا ف ة دراوال تاوطلخا ع بتا

FXOS Chassis Show-tech فلم

م س ق ل ا ف ة دراوال تاوطلخا ع بتا

FXOS جم ان رب رادصا

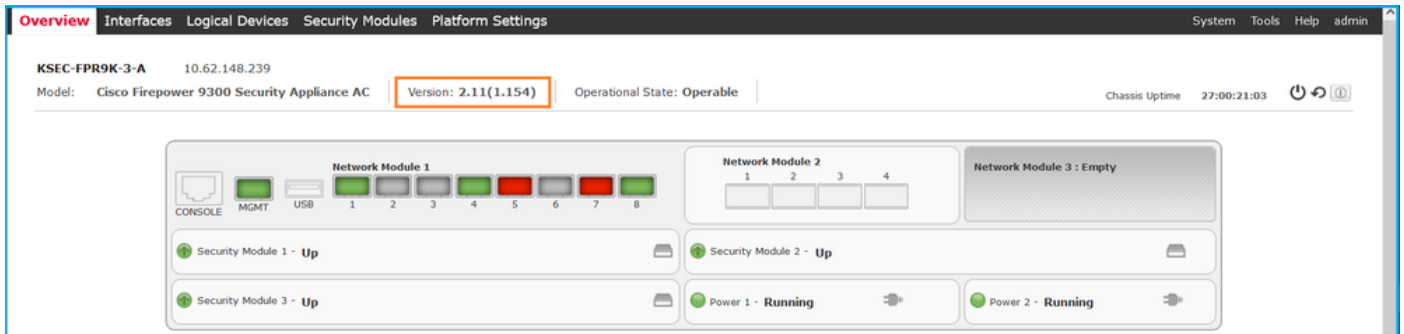
ة: لال تارايل ل مادختساب FXOS جم ان رب رادصا نم ق قحتلال نكم ي

- (طوق ف C M (Firepower 4100/9300 مدختسم ة هجاو

- رماوأل رطس ةهجاو (CLI) نم Fxos
- FXOS REST API
- FXOS ل SNMP عالطتسا
- FXOS chassis show-tech فلم.

FCM مدختسم ةهجاو

ةيسئزللا ةحفصلا لىل ع FCM UI صحف رادصا لىل ع FXOS جم انرب رادصا نم ققحتلل



FXOS رماوأل رطس ةهجاو (CLI) نم

Firepower 4100/9300

FXOS رماوأل رطس ةهجاو لىل ع FXOS جم انرب رادصا نم ققحتلل ةيلال تاوطخل عبتا

1. لك يهل اب SSH وا مكحت ةدحو لاصتا عاشن اب مق.
2. show firmware monitor رمال ليغشتب مقو قاطنلا ماظن لىل ليديتلاب مق.

```
firepower # scope system
firepower /system # show firmware monitor
FPRM:
```

```
Package-Vers: 2.11(1.154)
Upgrade-Status: Ready
```

Fabric Interconnect A:

```
Package-Vers: 2.11(1.154)
Upgrade-Status: Ready
```

Chassis 1:

Server 1:

```
Package-Vers: 2.11(1.154)
Upgrade-Status: Ready
```

Server 2:

```
Package-Vers: 2.11(1.154)
Upgrade-Status: Ready
```

Server 3:

```
Package-Vers: 2.11(1.154)
Upgrade-Status: Ready
```

FTD عم Firepower 1000/2100/3100

FXOS رماوأل رطس ةهجاو لىل ع FXOS جم انرب رادصا نم ققحتلل ةيلال تاوطخل عبتا

1. FTD ب SSH لاصتا وا لك يهل اب مكحت ةدحو لاصتا عاشن اب مق.
- FTD رطس ةهجاو لىل ع connect fxos رمال ليغشتب مق، FTD ب SSH لاصتا ةلاح يف

> connect fxos

2. رمألا لغشو قاطنلا ماظن لإ لق تنا: show firmware detail:

```
firepower # scope system
firepower /system # show firmware detail
Version: 7.1.0-90
Startup-Vers: 7.1.0-90
MANAGER:
  Boot Loader:
    Firmware-Vers: 1012.0200.0213
    Rommon-Vers: 1.0.12
    Fpga-Vers: 2.0.00
    Fpga-Golden-Vers:
    Power-Sequencer-Vers: 2.13
    Firmware-Status: OK
    SSD-Fw-Vers: 0147
  System:
    Running-Vers: 2.11(1.154)
    Platform-Vers: 2.11.1.154
    Package-Vers: 7.1.0-90
    Startup-Vers: 2.11(1.154)
  NPU:
    Running-Vers: 2.11(1.154)
    Platform-Vers: 2.11.1.154
    Package-Vers: 7.1.0-90
    Startup-Vers: 2.11(1.154)
  Service Manager:
    Running-Vers: 2.11(1.154)
    Platform-Vers: 2.11.1.154
    Package-Vers: 7.1.0-90
    Startup-Vers: 2.11(1.154)
```

زاهجلا عضو يف ASA عم FirePOWER 2100 و ASA عم Firepower 1000/3100

FXOS: رمأوالا رطس ةهجاو لإ لع FXOS جم ان رب رادصا نم ققحت لل ةيالاتا تاوطلخا لع بتا

1. ب ASA ب Telnet/SSH لاصتا وأ لك يهلاب مكحت ةدحو لاصتا عاشناب مق.
2. ASA CLI لع connect fxos رمألا ليغشت ب مق، ب ASA ب Telnet/SSH لاصتا ةلاحي يف

asa# connect fxos

2. رمألا ليغشت ب مقو قاطنلا ماظن لإ لي دب تلاب مق: show firmware detail:

```
firepower # scope system
firepower /system # show firmware detail
Version: 9.17.1
Startup-Vers: 9.17.1
MANAGER:
  Boot Loader:
    Firmware-Vers: 1012.0200.0213
    Rommon-Vers: 1.0.12
    Fpga-Vers: 2.0.00
    Fpga-Golden-Vers:
    Power-Sequencer-Vers: 2.13
    Firmware-Status: OK
    SSD-Fw-Vers: 0147
  System:
    Running-Vers: 2.11(1.154)
```

```
Platform-Vers: 2.11.1.154
Package-Vers: 9.17.1
Startup-Vers: 2.11(1.154)
NPU:
  Running-Vers: 2.11(1.154)
Platform-Vers: 2.11.1.154
Package-Vers: 9.17.1
Startup-Vers: 2.11(1.154)
Service Manager:
  Running-Vers: 2.11(1.154)
Platform-Vers: 2.11.1.154
Package-Vers: 9.17.1
Startup-Vers: 2.11(1.154)
```

يساسألماظنللاعضويف ASA عم Firepower 2100

FXOS رماوألارطسةهجاوعلع FXOS جمانربرادصانمققحتلللةياتللاواوطلالعبتا

1. ب ASA ب Telnet/SSH لاصتا وأ لكيلهلاب مكحتلال دحو وأ SSH لاصتا عاشناب مق.
ASA CLI علع connect fxos رمالا ليعغشتب مق، ب ASA ب Telnet/SSH لاصتا للاح يف

```
asa# connect fxos
```

2. رمالا ليعغشتب مقوقاطنللاماظنللا ليدبتلاب مق. **show firmware detail:**

```
firepower # scope system
firepower /system # show firmware detail
Version: 9.17.1
Startup-Vers: 9.17.1
MANAGER:
  Boot Loader:
    Firmware-Vers: 1012.0200.0213
    Rommon-Vers: 1.0.12
    Fpga-Vers: 2.0.00
    Fpga-Golden-Vers:
    Power-Sequencer-Vers: 2.13
    Firmware-Status: OK
    SSD-Fw-Vers: 0147
  System:
    Running-Vers: 2.11(1.154)
    Platform-Vers: 2.11.1.154
    Package-Vers: 9.17.1
    Startup-Vers: 2.11(1.154)
  NPU:
    Running-Vers: 2.11(1.154)
    Platform-Vers: 2.11.1.154
    Package-Vers: 9.17.1
    Startup-Vers: 2.11(1.154)
  Service Manager:
    Running-Vers: 2.11(1.154)
    Platform-Vers: 2.11.1.154
    Package-Vers: 9.17.1
    Startup-Vers: 2.11(1.154)
```

FXOS REST-API

معد متي FXOS REST-API علع FirePOWER 4100/9300 Series.

Firepower 4100/9300

مدخستسأ FXOS. نم REST-API بلط ربع FXOS جم انرب رادصا نم ققحتلل تاوطخل هذه عبتا
curl تلمعتسا، لاثم اذه يف. جم انرب رادصا نم ققحتلل REST-API ليمع

1. زي ممة قداصم زمرب بلط:

```
# curl -k -X POST -H 'USERNAME: admin' -H 'PASSWORD: Cisco123' 'https://192.0.2.100/api/login'
{
  "refreshPeriod": "0",
  "token": "1206f6a3032e7bdbeac07cfdd9d5add5cdd948e4e5f4511535a959aed7e1e2f5"
}
```

2. مالتسالا اذه يف زي ممل زمربا مدخستسأ:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
1206f6a3032e7bdbeac07cfdd9d5add5cdd948e4e5f4511535a959aed7e1e2f5'
'https://192.0.2.100/api/sys/firmware/install-platform-fw' | grep -i platformBundle
  "platformBundleName": "fxos-k9.2.11.1.154.SPA",
  "platformBundleVersion": "2.11(1.154)",
```

FXOS ب صاخال SNMP لوكوتورب

يساسالا ماظنلا عضو يف ASA عم FirePOWER 2100 لىل FXOS لىل SNMP نيوكت معد متي
و Firepower 4100/9300.

Firepower 4100/9300

SNMP ربع FXOS جم انرب رادصا نم ققحتلل لىلاتا تاوطخل عبتا:

1. [FirePOWER NGFW قزهجا لىل SNMP نيوكت](#) لىل عجرا. FXOS لىل SNMP نيوكت نم دكات.
نيوكتلا تاوطخل.
2. Cisco-Firepower-Firmware-MIB: أو 1.3.6.1.4.1.9.826.1.30.47.1.6. عاصقتسالا.
CFPRfirmwareRunningPackageVersion:

```
# snmpwalk -On -v2c -c cisco 192.0.2.100 .1.3.6.1.4.1.9.826.1.30.47.1.6
.1.3.6.1.4.1.9.826.1.30.47.1.6.20823 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.826.1.30.47.1.6.25326 = ""
.1.3.6.1.4.1.9.826.1.30.47.1.6.25331 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.826.1.30.47.1.6.30266 = STRING: "1.0.18"
.1.3.6.1.4.1.9.826.1.30.47.1.6.30269 = STRING: "1.0.18"
.1.3.6.1.4.1.9.826.1.30.47.1.6.30779 = ""
.1.3.6.1.4.1.9.826.1.30.47.1.6.30780 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.826.1.30.47.1.6.30781 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.826.1.30.47.1.6.32615 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.826.1.30.47.1.6.48820 = STRING: "0.0"
```

يساسالا ماظنلا عضو يف ASA عم Firepower 2100

SNMP ربع FXOS جم انرب رادصا نم ققحتلل لىلاتا تاوطخل عبتا:

1. [FirePOWER NGFW قزهجا لىل SNMP نيوكت](#) لىل عجرا. FXOS لىل SNMP نيوكت نم دكات.
نيوكتلا تاوطخل.
2. SNMPv2-MIB::sysDescr.0: أو 1.3.6.1.2.1.1.0. عاصقتسالا.

```
# snmpwalk -On -v2c -c cisco 192.0.2.101 SNMPv2-MIB::sysDescr.0
.1.3.6.1.2.1.1.0 = STRING: Cisco FirePOWER FPR-2140 Security Appliance, System Version
```

2.11(1.146)

```
# snmpwalk -On -v2c -c cisco 192.0.2.101 .1.3.6.1.2.1.1.1.0
.1.3.6.1.2.1.1.1.0 = STRING: Cisco FirePOWER FPR-2140 Security Appliance, System Version
2.11(1.146)
```

فلم FXOS Chassis Show-tech

Firepower 4100/9300

لكيهب صاخلا show-tech فلم يي FXOS جم انرب رادصا نم ققحتلل ةيلال تاوطلال عبتا FXOS:

1. فف sam_techsupportinfo فلم حتفا ،ثدحألا تارادصإلاو FXOS 2.7 تارادصإلا ةبسنلاب
<name>_bc1_all.tar/ FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar
فف sam_techsupportinfo فلم حتفا ،مدقألا تارادصإلا ةبسنلاب
FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar.

2. 'show firmware monitor' رمألا جارخا نم ققحت:

```
# pwd
/var/tmp/20220313201802_F241-01-11-FPR-2_BC1_all/FPRM_A_TechSupport/
# cat sam_techsupportinfo
...
`show firmware monitor`
```

FPRM:

```
Package-Vers: 2.11(1.154)
Upgrade-Status: Ready
```

Fabric Interconnect A:

```
Package-Vers: 2.11(1.154)
Upgrade-Status: Ready
```

Chassis 1:

```
Server 1:
Package-Vers: 2.11(1.154)
Upgrade-Status: Ready
Server 2:
Package-Vers: 2.11(1.154)
Upgrade-Status: Ready
Server 3:
Package-Vers: 2.11(1.154)
Upgrade-Status: Ready
...
```

Firepower 1000/2100/3100

1. فف tech_support_brief فلم حتفا <name>_fprm.tar.gz/<name>_FPRM.tar
2. 'show firmware detail' رمألا جارخا نم ققحت:

```
# pwd
/var/tmp/fp2k-1_FPRM/
# cat tech_support_brief
...
`show firmware detail`
Version: 7.1.0-90
Startup-Vers: 7.1.0-90
```

MANAGER:

Boot Loader:

Firmware-Vers: 1012.0200.0213
Rommon-Vers: 1.0.12
Fpga-Vers: 2.0.00
Fpga-Golden-Vers:
Power-Sequencer-Vers: 2.13
Firmware-Status: OK
SSD-Fw-Vers: 0147

System:

Running-Vers: 2.11(1.154)
Platform-Vers: 2.11.1.154
Package-Vers: 7.1.0-90
Startup-Vers: 2.11(1.154)

NPU:

Running-Vers: 2.11(1.154)
Platform-Vers: 2.11.1.154
Package-Vers: 7.1.0-90
Startup-Vers: 2.11(1.154)

Service Manager:

Running-Vers: 2.11(1.154)
Platform-Vers: 2.11.1.154
Package-Vers: 7.1.0-90
Startup-Vers: 2.11(1.154)

...

FTD جمانرب رادصا

ةةيلاتل تارايلال مادختساب FTD جمانرب رادصا نم ققحتل نكمي:

- FTD يف رماوالا رطس ةهجاو
- FTD SNMP عالطتسا
- اهجالصاو FTD ءاطخا فاشكتسا فلم
- FMC مدختسم ةهجاو
- FMC REST API
- FDM مدختسم ةهجاو
- FDM REST API
- FCM مدختسم ةهجاو
- Fxos نم (CLI) رماوالا رطس ةهجاو
- FXOS REST API
- FXOS Chassis Show-tech فلم

FTD يف رماوالا رطس ةهجاو

FTD يف (CLI) رماوالا رطس ةهجاو لعل FTD جمانرب رادصا نم ققحتل لةيلاتل تاوطخل عبتا

قفاوتي امب FTD ب ةصاخلا (CLI) رماوالا رطس ةهجاو لعل لوصولل تارايلال هذه مدختسا 1.
رشنللا عوضو يسااسالا ماظنلا عم

- ةيسااسالا ةمظنالا عيمج - FTD لعل رشاومل SSH لوصولو
- نم (Firepower 1000/2100/3100) FXOS مكحت ةدحول (CLI) رماوالا رطس ةهجاو نم لوصولو
ftd رمالا لصتالا لالخ
- (Firepower) رماوالا ربع FXOS لعل شتلا ماظن (CLI) رماوالا رطس ةهجاو نم لوصولو
4100/9300):

نمو، ذفنملا فرعم x لثمي شح، [telnet]مكحتللا ةدحول <x> ةيسااسالا ةدحول لعل لصوتب مق

مث

تالېثم لاددعتم رشنلل طقف ةلص اذ لېثم لانوئي ثي ح، `ftd [instance]` ب لصلتا

- رشابم لالوصولانكمي، ةيضا رتفالال (FTD) ةعرسلال قئاف لالسالال ةمظنال ةبس نلاب
جمانرب نم مكحتلال ةدحو لوصولو وأ (FTD) ةعرسلال قئاف لالسالال جمانرب لال SSH لال
ةباحسلال مدختسم ةهجاو وأ hypervisor

2. CLI لال `show version` رمألال ليلغشتب مق:

```
> show version
```

```
-----[ firepower ]-----  
Model : Cisco Firepower 2120 Threat Defense (77) Version 7.1.0 (Build 90)  
UUID : 1b324aaa-670e-11ec-ac2b-e000f0bd3ca1  
LSP version : lsp-rel-20220328-1342  
VDB version : 353  
-----
```

FTD SNMP

SNMP ربع FTD جمانرب رادصل نم ققحتلل ةيلتال تاوطلال عبتا

1. لال عجرا، FDM نم رادملال FTD جمانرب لال ةمظنلال. هنكمتو SNMP نيوكت نم دكات. [تاوطلال لال ةمظنلال FirePOWER FDM لال ةمظنلال فاشكتسا او SNMP نيوكت](#)
لال عجرا، FMC ةطساوب رادملال FTD جمانرب لال ةمظنلال. [نيوكت لال FirePOWER NGFW ةزهجا](#)
2. `OID .1.3.6.1.2.1.1.0.` وأ `SNMPv2-MIB::sysDescr.0` ءاصقتسالال `OID`:

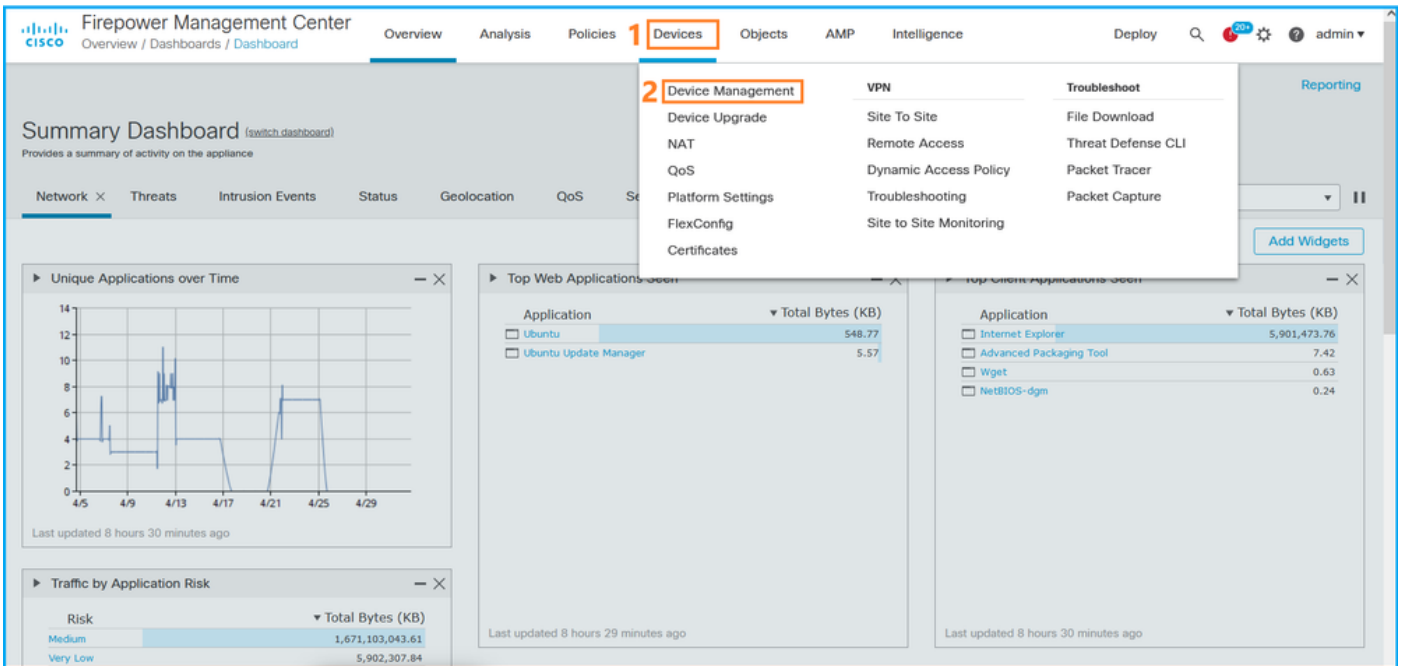
```
# snmpwalk -v2c -c cisco123 192.0.2.2 SNMPv2-MIB::sysDescr.0  
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 7.1.0 (Build 90), ASA  
Version 9.17(1)
```

```
# snmpwalk -v2c -c cisco123 192.0.2.2 SNMPv2-MIB::sysDescr.0 .1.3.6.1.2.1.1.1.0  
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Firepower Threat Defense, Version 7.1.0 (Build 90), ASA  
Version 9.17(1)
```

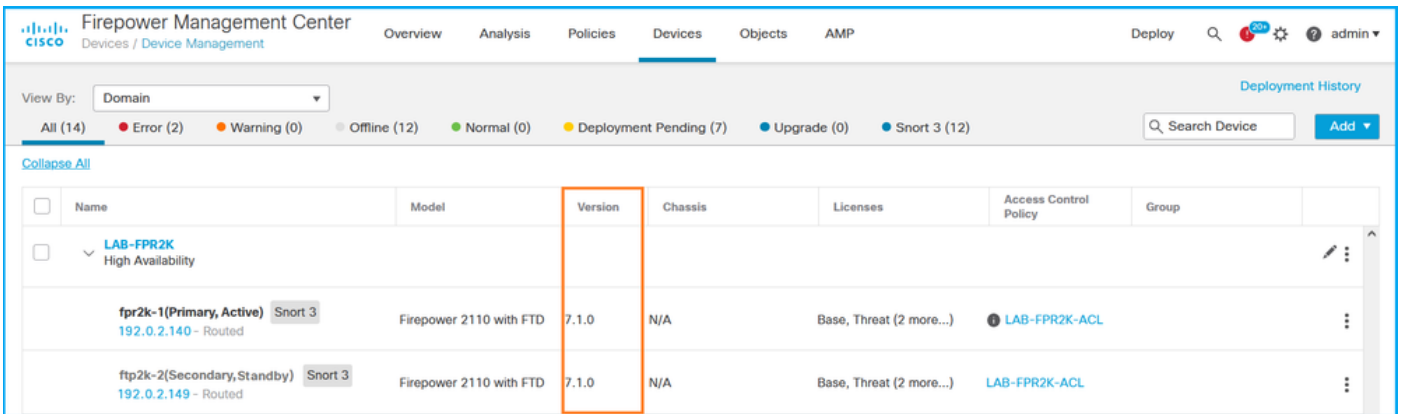
FMC مدختسم ةهجاو

FMC مدختسم ةهجاو لال FTD جمانرب رادصل نم ققحتلل ةيلتال تاوطلال عبتا

1. ةزهجالا ةرادل > ةزهجا رتخأ:



2. رادصالا دوم نم ققحت:



FMC REST API

REST-API ليمع مدختسا. FMC REST-API ربع فTD جمانرب رادصالا نم ققحتلل تاوطخل هذه عبتا curl مادختسا متي، لاثملا اذه في. جمانربلا رادصالا نم ققحتلل

1. زيمم ةقداصم زمر بلط:

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H
'Authentication: Basic' -u 'admin:Cisco123' | grep -i X-auth-access-token
<X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb
```

2. لاجملا ةملعم نوكت، REST API تامالعتسا ةبلاغ في. زاهاللا لعل يوتحي يذلا لاجملا دح. ةمئاق دادرتسال مالعتسال اذه في X ةقداصم لىل لوصولل زيمملا زمرلا مدختسا. ةيمازللا تالاجملا:

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept:
application/json' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
json.tool
```

```
{
  "items": [
```



```

{
  "name": "Global",
  "type": "Domain",
  "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
},
{
  "name": "Global/domain1",
  "type": "Domain",
  "uuid": "ef0cf3e9-bb07-8f66-5c4e-000000000001"
},
{
  "name": "Global/domain2",
  "type": "Domain",
  "uuid": "341a8f03-f831-c364-b751-000000000001"
}
],
"links": {
  "self": "https://192.0.2.1/api/fmc_platform/v1/info/domain?offset=0&limit=25"
},
"paging": {
  "count": 3,
  "limit": 25,
  "offset": 0,
  "pages": 1
}
}

```

3. ن ع م ا ل ع ت س ا ل ل ل ا ج م ل ل UUI D م د خ ت س ا :

```

# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devices/devicerecords' -H 'accept: application/json' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool

```

```

{
  "items": [
    {
      "id": "a4752f3c-86cc-11e9-8c9a-a3c958bed664",
      "links": {
        "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devices/devicerecords/a4752f3c-86cc-11e9-8c9a-a3c958bed664"
      },
      "name": "fw1.lab.local",
      "type": "Device"
    },
    {
      "id": "05e9799c-94fc-11ea-ad33-a0032ddb0251",
      "links": {
        "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devices/devicerecords/05e9799c-94fc-11ea-ad33-a0032ddb0251"
      },
      "name": "fw2.lab.local",
      "type": "Device"
    },
    {
      "id": "c8bef462-49f7-11e8-b2fb-ad9838c6ed90",
      "links": {
        "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devices/devicerecords/c8bef462-49f7-11e8-b2fb-ad9838c6ed90"
      },
      "name": "fw3.lab.local",
      "type": "Device"
    }
  ],
}

```

```

{
  "id": "3c41913a-b27b-11eb-b131-d2e2ce2a368d",
  "links": {
    "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devices/devicerecords/3c41913a-b27b-11eb-b131-d2e2ce2a368d"
  },
  "name": "fw4.lab.local",
  "type": "Device"
},
{
  "id": "48f7f37c-8cf0-11e9-bf41-fb2d7b740db7",
  "links": {
    "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devices/devicerecords/48f7f37c-8cf0-11e9-bf41-fb2d7b740db7"
  },
  "name": "fw5.lab.local",
  "type": "Device"
},
{
  "id": "0b1a9c94-8ba8-11ec-b2fd-93263934908d",
  "links": {
    "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devices/devicerecords/0b1a9c94-8ba8-11ec-b2fd-93263934908d"
  },
  "name": "fpr2k-1",
  "type": "Device"
},
},

```

4. أةواحل/زاهحل اب صاخل ا UUID و لاجل اب صاخل ا UUID مدخت سا:

```

# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/devices/devicerecords/0b1a9c94-8ba8-11ec-b2fd-93263934908d/operational/commands?offset=0&limit=25&command=show%20version' -H 'X-auth-access-token: f3233164-6ab8-4e33-90cc-2612c19571be' | python -m json.tool
{
  "items": [
    {
      "commandInput": "show version",
      "commandOutput": "-----[ fpr2k-1 ]-----\nModel
: Cisco Firepower 2110 Threat Defense (77) Version 7.1.0 (Build 90)\nUUID
0b1a9c94-8ba8-11ec-b2fd-93263934908d\nLSP version
: lsp-rel-20220502-1613\nVDB
version
: 353\n-----\n\nCisco
Adaptive Security Appliance Software Version 9.17(1) \nSSP Operating System Version
2.11(1.154)\n\nCompiled on Tue 30-Nov-21 19:37 GMT by builders\nSystem image file is
\"disk0:/mnt/boot/installables/switch/fxos-k8-fp2k-npu.2.11.1.154.SPA\"\n\nConfig file at boot was
\"startup-config\"\n\nfpr2k-1 up 10 days 4 hours\nfailover cluster up 57 days 17 hours\nStart-up
time 37 secs\n\nHardware: FPR-2110, 6588 MB RAM, CPU MIPS 1200 MHz, 1 CPU (6 cores)\n\n\n 1:
Int: Internal-Data0/1 : address is 000f.b748.4801, irq 0\n 3: Ext: Management1/1 :
address is 707d.b9e2.836d, irq 0\n 4: Int: Internal-Datal/1 : address is 0000.0100.0001, irq
0\n 5: Int: Internal-Datal/2 : address is 0000.0300.0001, irq 0\n 6: Int: Internal-Controll1/1
: address is 0000.0001.0001, irq 0\n\nSerial Number: JAD213508B6\nConfiguration last modified by
enable_1 at 04:12:18.743 UTC Wed May 4 2022\n",
      "type": "command"
    }
  ],
  "links": {
    "self": "https://192.0.2.1/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/devices/devicerecords/0b1a9c94-8ba8-11ec-b2fd-93263934908d/operational/commands?offset=0&limit=25&command=show version"
  },
  "paging": {

```

```
"count": 1,  
"limit": 25,  
"offset": 0,  
"pages": 1  
}
```

FDM مدخستسم ةهجاو

مسقلا يف ةدراولا تاوطخلا عبتا

FDM REST-API

مسقلا يف ةدراولا تاوطخلا عبتا

اهحالصإو FTD ءاطخأ فاشكتسأ فلم

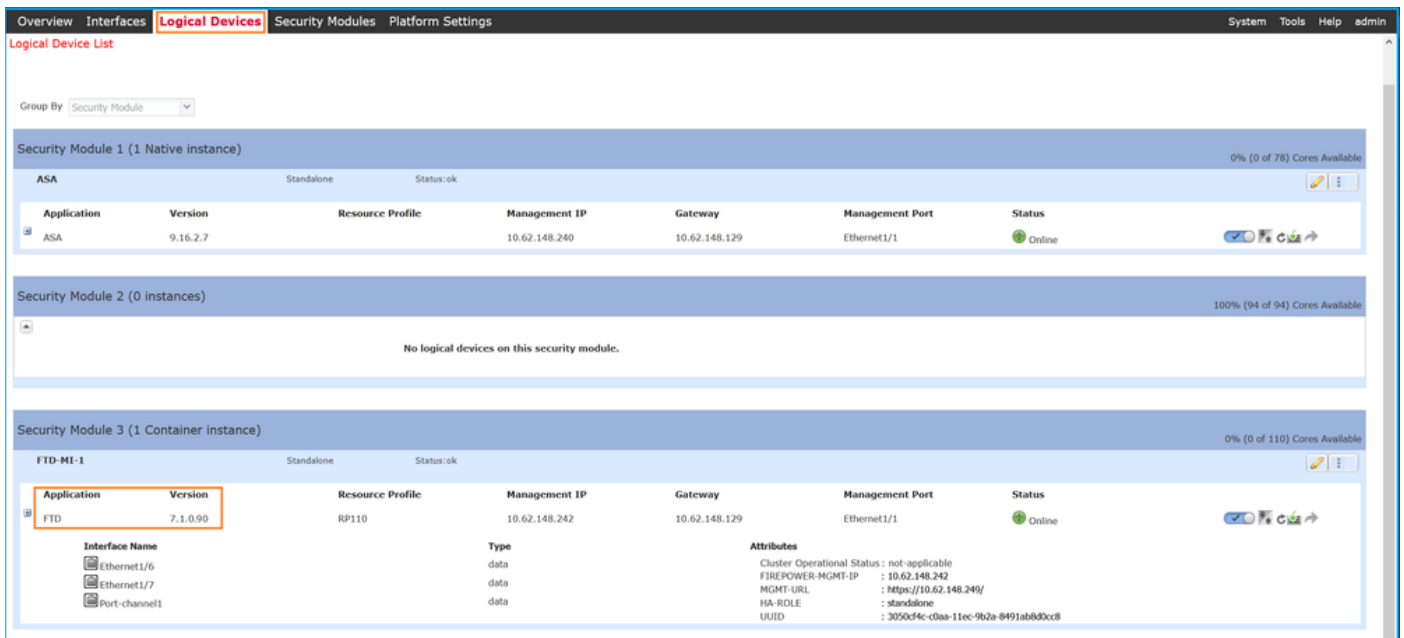
اهحالصإو FTD ءاطخأ فاشكتسأ فلم يف FTD جم انرب رادصإ نم ققحتلل تاوطخلا هذه عبتا

1. دلجملا لىل لقتناو اھحالصإو ءاطخأ الفاشكتسأ فلم حتفا .
`<filename>-troubleshooting.tar/results-<date>—xxxxx/command-output/`
2. مادختساب طخلا نع ثحبأو `usr-local-sf-bin-sfcli.pl show version.output` فلملا حتفا .
جذومنلا:

```
# pwd  
/var/tmp/results-05-06-2022--199172/dir-archives/etc/sf/  
# cat "usr-local-sf-bin-sfcli.pl show version.output"  
-----[ fpr2k-1 ]----- Model : Cisco Firepower 2110 Threat Defense  
(77) Version 7.1.0 (Build 90)  
UUID : 0b1a9c94-8ba8-11ec-b2fd-93263934908d  
LSP version : lsp-rel-20220510-1044  
VDB version : 354  
-----
```

FCM مدخستسم ةهجاو

ةمالع يف رادصإلا ددحو FCM مدخستسأ، FirePOWER 4100/9300 لىل ع FTD لىل ةبسنلاب
ةقطنملا ةزهجالا بىوبتلا:



رم اوألا رطس ةهجاو (CLI) نم Fxos

FTD لىل Firepower 4100/9300

ماظنل (CLI) رم اوألا رطس ةهجاو لىل FTD جم انرب رادصا نم ققحتلل ةيلال تاوطخل اعبتا لىل فغشتلا FXOS:

1. لكهلاب SSH وأ مكحت ةدحو لاصتا عاشناب مق.
2. رمألا لىل فغشتب مق و ssa قاطن لىل لىل دبتلاب مق.

```
firepower# scope ssa
firepower /ssa # show app-instance
App Name Identifier Slot ID Admin State Oper State Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State Cluster Role
-----
asa ASA 1 Enabled Online 9.16.2.7 9.16.2.7
Native No Not Applicable None
ftd FTD-MI-1 3 Enabled Online 7.1.0.90 7.1.0.90
Container No RP110 Not Applicable None
```

FTD لىل FirePOWER 1000/2100/3100 جم انرب

ماظنل (CLI) رم اوألا رطس ةهجاو لىل FTD جم انرب رادصا نم ققحتلل ةيلال تاوطخل اعبتا لىل فغشتلا FXOS:

1. SSH لاصتا وأ لكهلاب مكحت ةدحو لاصتا عاشناب.
2. FTD رطس ةهجاو لىل connect fxos رمألا لىل فغشتب مق، FTD ب SSH لاصتا ةلاح يف

```
> connect fxos
```

2. show app-instance رمألا لىل فغشتب مق و SSA قاطن لىل لىل دبتلاب مق.

```
firepower# scope ssa
firepower /ssa # show app-instance
```

Application Name	Slot ID	Admin State	Operational State	Running Version	Startup
Version Deploy Type	Profile Name	Cluster Oper	State Cluster Role		
ftd	1	Enabled	Online	7.1.0.90	7.1.0.90
Native	Not Applicable		None		

FXOS REST-API

ل FXOS REST-API لال خ نم FTD جم ان رب رادصل نم ققحت لل ة لالتا تا وطلخال عبتا

1. زيمم ة قداصم زمر بل ط:

```
# curl -s -k -X POST -H 'USERNAME: admin' -H 'PASSWORD: cisco' 'https://192.0.2.100/api/login'
{
  "refreshPeriod": "0",
  "token": "28821660bc74e418f3fadc443619df0387d69e7b150e035f688bed9d347b4838"
}
```

2. تي بثت م تي شيح ة تحت لال فرعم ديحت نم دكأت و مالعت سالا اذه في زيمم لال زمر لال مدخت سا:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
28821660bc74e418f3fadc443619df0387d69e7b150e035f688bed9d347b4838'
'https://192.0.2.100/api/slot/3/app-inst' | grep -Ei "identifier|version"
  "identifier": "FTD-MI-1",
  "runningVersion": "7.1.0.90",
  "hwCryptoVersion": "2",
  "startupVersion": "7.0.1.84",
  "versionIncompatibleErrorMgr": ""
```

FXOS Chassis Show-tech فلم

ل كيهب صاخ لال show-tech فلم في FTD جم ان رب رادصل نم ققحت لل ة لالتا تا وطلخال عبتا
FXOS:

FTD لى Firepower 4100/9300

1. في `sam_techsupportinfo` فلم تحت فا، ثدأل ا تارادصل او FXOS 2.7 تارادصل ا ة بس نلاب
<name>_bc1_all.tar/ FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar

في `sam_techsupportinfo` فلم تحت فا، م دقأ ل ا تارادصل ا ة بس نلاب
FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar.

2. 'show slot expand detail': نم ض ة تحت ف لك ل عطقم لال نم ققحت:

```
# pwd
/var/tmp/20220313201802_F241-01-11-FPR-2_BC1_all/FPRM_A_TechSupport/
# cat sam_techsupportinfo
...
`show slot expand detail`
Slot: Slot ID: 3 Log Level: Info Admin State: Ok Oper State: Online Disk Format State: Ok Disk
```

Format Status: 100% Clear Log Data: Available Error Msg: Application Instance: App Name: ftd

Identifier: FTD-MI-1

Admin State: Enabled

Oper State: Online

Running Version: 7.1.0.90

Startup Version: 7.1.0.90

Deploy Type: Container

...

جمع انرب FirePOWER 1000/2100/3100

1. في <name>_fprm.tar.gz/<name>_FPRM.tar فلم حت ف
2. 'show slot' و 'scope ssa' ماسق أل نم قق حت:

```
# pwd
```

```
/var/tmp/fp2k-1_FPRM/
```

```
# cat tech_support_brief
```

```
...
```

```
`scope ssa` `show slot`
```

```
Slot:
```

Slot ID	Log Level	Admin State	Operational State
1	Info	Ok	Online

```
`show app`
```

```
Application:
```

Name	Version	Description	Author	Deploy Type	CSP Type	Is Default App
ftd	7.1.0.90	N/A	cisco	Native	Application	Yes

```
`show app-instance detail`
```

```
Application Name: ftd
```

```
Slot ID: 1
```

```
Admin State: Enabled
```

```
Operational State: Online
```

```
Running Version: 7.1.0.90
```

```
Startup Version: 7.1.0.90
```

```
...
```

ASA جمع انرب رادصا

ةة لال تاراخي ل م ادخت ساب ASA جمع انرب رادصا نم قق حت ل نكمي:

- ASA رم اوأل رطس ةه جاو
- ASA SNMP عا ل طت سا
- ASA Show-tech فلم
- FCM مدخت سم ةه جاو
- Fxos نم (CLI) رم اوأل رطس ةه جاو
- FXOS REST API
- FXOS Chassis Show-tech فلم

ASA رم اوأل رطس ةه جاو

ASA CLI ع ل ASA جمع انرب رادصا نم قق حت ل لة لال تاو طخ ل ع بتا

ع ضوو ي سا سأل ما ظن ل عم ق فاوتي امب ASA CLI ل لوصول ل تاراخي ل هذه مدخت سا أ. رشن ل:

- في Firepower 2100 و FirePOWER 1000/3100 على ASA إلى رشابم ال Telnet/SSH لوصول و زاهج ال عضو
- عضو في FirePOWER 2100 على FXOS م كحت ة دحول (CLI) رم أوأا ل رطس ة هجاو نم لوصول ال
- **connect asa** رم أا ل ال خ نم ASA ب لاصت ال او يساس أا ل ماظن ال
- (Firepower 4100/9300) رم أوأا ل ربع FXOS CLI نم لوصول ال:

مق م ث ، ة ح ت ف ل ل فر ع م x ل ث م ي ث ي ح ، [telnet] م ك ح ت ل ل ة د ح و [x] ة ي ط م ن ل ل ة د ح و ل ل ي ص و ت ب م ق asa ل ي ص و ت ب

- ة د ح و ل و ص و و أا ل ASA إلى رشابم ال SSH لوصول و ، ي ره اظ ل ال ASA ص ا ر ق أ ك ر ح م ل ة ب س ن ل ل ا ب
- ة ب ا ح س ل ل م د خ ت س م ة ه ج ا و و أا ل hypervisor ج م ا ن ر ب ن م م ك ح ت ل ل

2. م ق م ا ل ل ي غ ش ت ب م ق : **show version:** رم أا ل

```
ciscoasa# show version
Cisco Adaptive Security Appliance Software Version 9.17(1)
SSP Operating System Version 2.11(1.154)
Device Manager Version 7.17(1)

Compiled on Tue 30-Nov-21 19:37 GMT by builders
System image file is "disk0:/mnt/boot/installables/switch/fxos-k8-fp2k-npu.2.11.1.154.SPA"
Config file at boot was "startup-config"
```

```
ciscoasa up 4 hours 40 mins
Start-up time 1 sec
```

ASA SNMP

SNMP: ربع ASA ج م ا ن ر ب ر ا د ص ل ن م ق ق ح ت ل ل ة ي ل ل ت ال ا و ط خ ل ل ا ع ب ت ا

1. ه ن ي ك م ت و SNMP ن ي و ك ت ن م د ك أ ت .
2. **OID SNMPv2-MIB::sysDescr.0** و **OID .1.3.6.1.2.1.1.1.0:** ع ا ل ط ت س ا ل SNMP ل ي م ع م ا د خ ت س ا .

```
# snmpwalk -v2c -c cisco123 192.0.2.2 SNMPv2-MIB::sysDescr.0
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Adaptive Security Appliance Version 9.17(1)

# snmpwalk -v2c -c cisco123 192.0.2.2 SNMPv2-MIB::sysDescr.0 .1.3.6.1.2.1.1.1.0
SNMPv2-MIB::sysDescr.0 = Cisco Adaptive Security Appliance Version 9.17(1)
```

ASA Show-tech فلم

Cisco Adaptive Security Appliance ج م ا ن ر ب ر ا د ص ل ل س ل س م ا د خ ت س ا ب ر ط س ل ل ن ع ث ح ب ل ا Software:

```
Cisco Adaptive Security Appliance Software Version 9.17(1)
SSP Operating System Version 2.11(1.154)
Device Manager Version 7.17(1)
...
```

FCM م د خ ت س م ة ه ج ا و

م س ق ل ل ي ف ة د ر ا و ل ل ا و ط خ ل ل ا ع ب ت ا .

Fxos نم (CLI) رم أوأا ل رطس ة هجاو

مس قلا يف ة دراوالا تاوطلال عبتا

FXOS REST-API

مس قلا يف ة دراوالا تاوطلال عبتا

فلم FXOS Chassis Show-tech

مس قلا يف ة دراوالا تاوطلال عبتا

ةي طمنللا Firepower ة دحو جم انرب رادصا

وأ مدقألا ةي طمنللا Sourcefire تادحول دي دجلال مسالا يف ه ASA لىل ع Firepower ةي طمنللا ة دحولال SFR.

تارايخلال هذو مادختساب هب صاخالال جم انربال رادصا نم ققحتلال نكمي

- مدختسم ةهجاو FMC
- FMC REST-API
- ةي طمنللا Firepower ة دحول CLI
- اهجال صاوا ةي طمنللا Firepower ة دحو ءاطخا فاشكتسا فلم
- رماوالا رطس ةهجاو ASA
- فم ASA Show-tech

فم مدختسم ةهجاو FMC

مس قلا يف ة دراوالا تاوطلال عبتا

FMC REST-API

مس قلا يف ة دراوالا تاوطلال عبتا

Firepower ةي طمنللا ة دحولل (CLI) رماوالا رطس ةهجاو

رطس ةهجاو لىل ع ةي طمنللا FirePOWER ة دحو جم انرب رادصا نم ققحتلال تاوطلال هذو عبتا ةي طمنللا ة دحولل (CLI) رماوالا:

1. ربع ASA ب ة صاخالال (CLI) رماوالا رطس ةهجاو نم وأ SSH ربع ةي طمنللا ة دحولاب لاصتالاب مق. `session sfr` رمالا
2. رمالا لي غشتب مق. `show version`:

```
> show version
-----[ sfr1 ]-----
Model                : ASA5516 (72) Version 7.1.0 (Build 90)
UUID                 : c049dad8-c42e-11e9-986d-bdeff3ce399e
Rules update version : 2022-05-10-001-vrt
VDB version          : 354
```


اهال صا و ةي طمن ال Firepower ةدحو ااطخأ فاشك تسأ فلم

فاشك تسأ فلم ي ةي طمن ال FirePOWER ةدحو جم ان رب رادصا نم ققحت لل تاوطخ ال هذ ع بت ا
اهال صا و ةي طمن ال ةدحو ال ااطخأ:

1. دلجم ال ال لقت ناو اهال صا و ااطخأ ال فاشك تسأ فلم حت فا .
`<filename>-troubleshooting.tar/results-<date>—xxxxx/command-output/`
2. مادخت ساب طخ ال نع ثح ب أو `usr-local-sf-bin-sfcli.pl show version.output` فلم ال حت فا .
جذوم ال:

```
# pwd
/var/tmp/results-05-12-2022--199172/command-outputs
# cat "usr-local-sf-bin-sfcli.pl show version.output"
-----[ sfr1 ]----- Model : ASA5516 (72) Version 7.1.0 (Build 90)
UUID : c049dad8-c42e-11e9-986d-bdeff3ce399e
LSP version : 2022-05-10-001-vrt
VDB version : 354
-----
```

رم او ال رطس ةه او

ةغص ةي جم ر ب ال تصح ف و ASA CLI ال ال ع رم ل ل ص ف ت sfr ةي طمن ةدحو ضرع ال تضك ر:

```
asa# show module sfr details
Getting details from the Service Module, please wait...

Card Type: FirePOWER Services Software Module
Model: ASA5516
Hardware version: N/A
Serial Number: JAD222103XA
Firmware version: N/A
Software version: 7.1.0-90
MAC Address Range: 7872.5dce.b3b2 to 7872.5dce.b3b2
App. name: ASA FirePOWER
App. Status: Up
App. Status Desc: Normal Operation
App. version: 7.1.0-90
Data Plane Status: Up
Console session: Ready
Status: Up
DC addr: No DC Configured
Mgmt IP addr: 192.168.45.45
Mgmt Network mask: 255.255.255.0
Mgmt Gateway: 0.0.0.0
Mgmt web ports: 443
Mgmt TLS enabled: true
```

فلم ASA Show-tech

sfr: ةي طمن ال ضرع ال ةدحو ل ل ص ف ت ةل س لس مادخت ساب رطس ال نع ثح ب ا:

```
----- show module sfr detail -----  
Getting details from the Service Module, please wait...
```

```
Card Type:          FirePOWER Services Software Module  
Model:             ASA5516  
Hardware version:  N/A  
Serial Number:     JAD222103XA  
Firmware version:  N/A  
Software version:  7.1.0-90  
MAC Address Range: 7872.5dce.b3b2 to 7872.5dce.b3b2  
App. name:         ASA FirePOWER  
App. Status:       Up  
App. Status Desc:  Normal Operation  
App. version:      7.1.0-90  
Data Plane Status: Up  
Console session:   Ready  
Status:            Up  
DC addr:           No DC Configured  
Mgmt IP addr:      192.168.45.45  
Mgmt Network mask: 255.255.255.0  
Mgmt Gateway:      0.0.0.0  
Mgmt web ports:    443  
Mgmt TLS enabled:  true
```

SRU و VDB و جمان ربل ا تارادصا نم ققحتا

(SNORT) قيمعلا مزحلا صحف كرحم رادصا

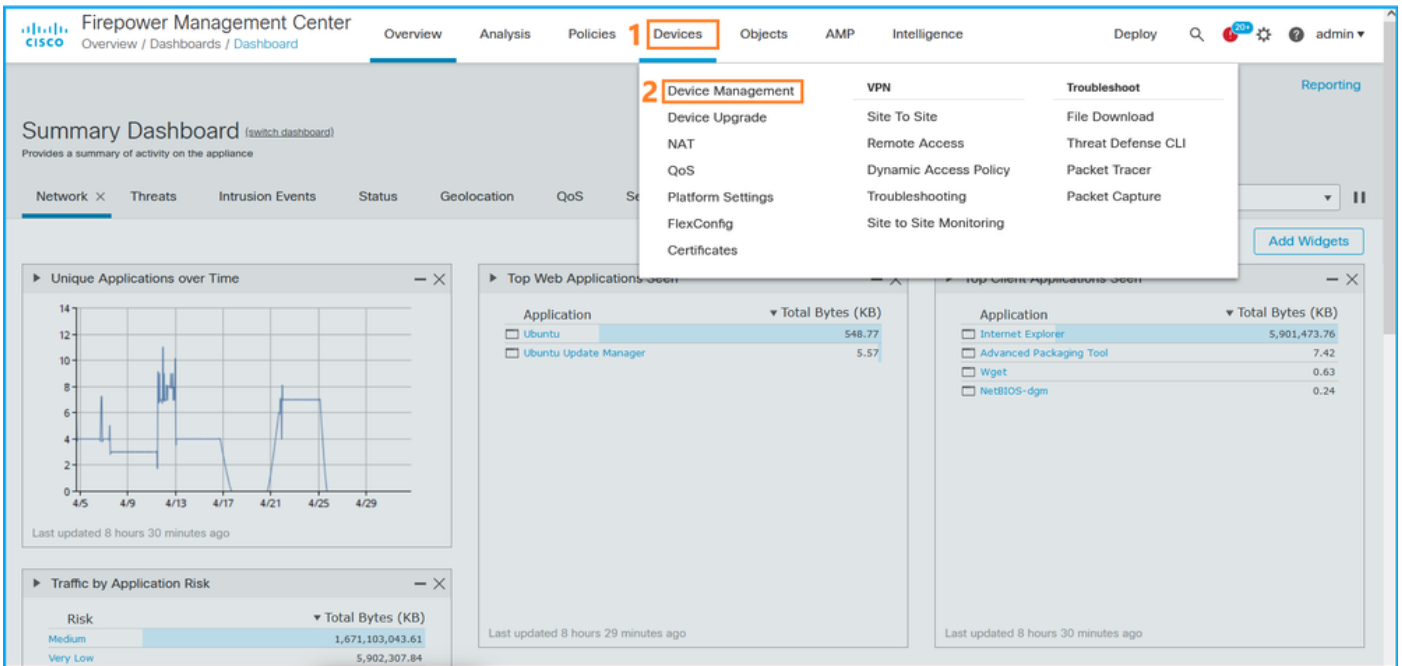
ةيالات ا تاراخيلا مادختساب snort رادصا نم ققحتا نكمي:

- مدختسم ةهجاو FMC
- FMC REST-API
- مدختسم ةهجاو FDM
- FDM REST API
- FTD و Firepower Module CLI
- اهالصا و Firepower و FTD ةيظمنلا ةدحولا ءاطخا فاشكتسا فلم

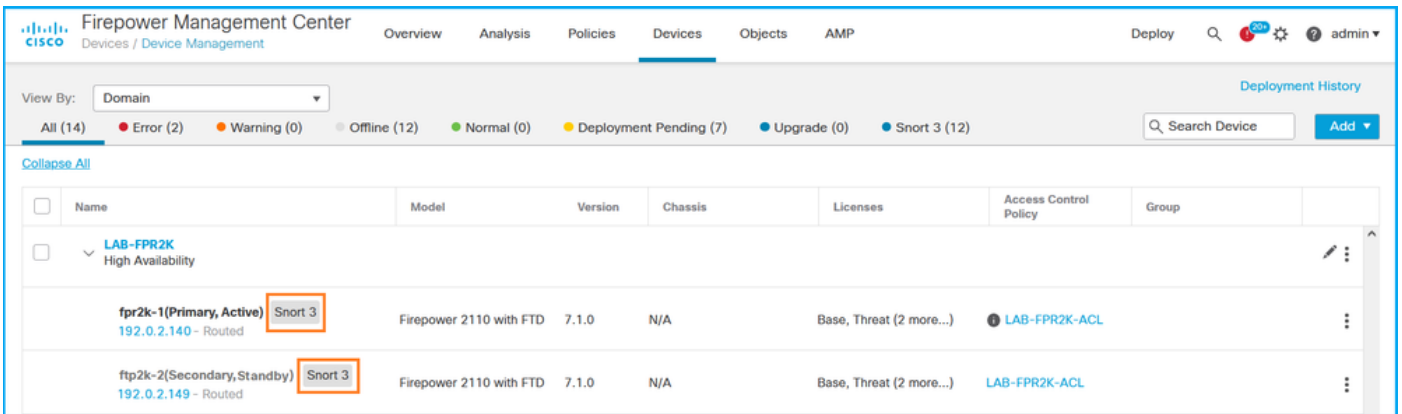
FMC مدختسم ةهجاو

FMC مدختسم ةهجاو يلع FTD جمان ربل ا تارادصا نم ققحتا لةيالاتا تاوطخلا عبتا

1. ةزهجالا ةرادا > ةزهجالا رتخا:



2. snort: سياسة نم ق قحت



FMC REST-API

لايجمع مدخست API REST مع ftd snort جمانرب رادصا نم ق قحت لل تاوطل هذه عبتا curl تلمعتسا، لاثم اذه في جمانربال رادصا نم ق قحت لل REST-API:

1. زي مة ق داصم زمرب ل ط:

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H
'Authentication: Basic' -u 'admin:Cisco123' | grep -i X-auth-access-token
<X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb
```

2. لاجملا مةلمع نوكت، REST API تامالعتسا اية بلاغ في. زا هال ال ع يوتحي يذلا لاجملا دح. مةئاق دادرتسال مالعتسال اذه في X ق داصم ال لوصولل زي مة ل زمرال مدخستسا. مةمازلل تالاجملا:

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept:
application/json' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
json.tool
```

```
{
  "items": [
```

```

    {
      "name": "Global",
      "type": "Domain",
      "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
    },
    {
      "name": "Global/domain1",
      "type": "Domain",
      "uuid": "ef0cf3e9-bb07-8f66-5c4e-000000000001"
    },
    {
      "name": "Global/domain2",
      "type": "Domain",
      "uuid": "341a8f03-f831-c364-b751-000000000001"
    }
  ],
  "links": {
    "self": "https://192.0.2.1/api/fmc_platform/v1/info/domain?offset=0&limit=25"
  },
  "paging": {
    "count": 3,
    "limit": 25,
    "offset": 0,
    "pages": 1
  }
}

```

3. DeviceRecords: ن ع م ا ل ع ت س ا ل ل ل ا ج م ل ل UUIID م د خ ت س ا

```

# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devices/devicerecords' -H 'accept: application/json' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool

```

```

{
  "items": [
    {
      "id": "a4752f3c-86cc-11e9-8c9a-a3c958bed664",
      "links": {
        "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devices/devicerecords/a4752f3c-86cc-11e9-8c9a-a3c958bed664"
      },
      "name": "fw1.lab.local",
      "type": "Device"
    },
    {
      "id": "05e9799c-94fc-11ea-ad33-a0032ddb0251",
      "links": {
        "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devices/devicerecords/05e9799c-94fc-11ea-ad33-a0032ddb0251"
      },
      "name": "fw2.lab.local",
      "type": "Device"
    },
    {
      "id": "c8bef462-49f7-11e8-b2fb-ad9838c6ed90",
      "links": {
        "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devices/devicerecords/c8bef462-49f7-11e8-b2fb-ad9838c6ed90"
      },
      "name": "fw3.lab.local",
      "type": "Device"
    }
  ]
}

```

```

    },
    {
      "id": "3c41913a-b27b-11eb-b131-d2e2ce2a368d",
      "links": {
        "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devices/devicerecords/3c41913a-b27b-11eb-b131-d2e2ce2a368d"
      },
      "name": "fw4.lab.local",
      "type": "Device"
    },
    {
      "id": "48f7f37c-8cf0-11e9-bf41-fb2d7b740db7",
      "links": {
        "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devices/devicerecords/48f7f37c-8cf0-11e9-bf41-fb2d7b740db7"
      },
      "name": "fw5.lab.local",
      "type": "Device"
    },
    {
      "id": "0b1a9c94-8ba8-11ec-b2fd-93263934908d",
      "links": {
        "self": "https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devices/devicerecords/0b1a9c94-8ba8-11ec-b2fd-93263934908d"
      },
      "name": "fpr2k-1",
      "type": "Device"
    },
  },
}

```

4. بطل اذة في واحة/زاحة لاب صاخلا UUID و لاجم لاب صاخلا UUID مدختسا:

```

# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-000000000001/devices/devicerecords/0b1a9c94-8ba8-11ec-b2fd-93263934908d' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool | grep -i snort

```

```

"snortVersion": "3.1.7.1-108",
"snortEngine": "SNORT3",

```

FDM مدختسم ةهجاو

FDM مدختسم ةهجاو لىل ع FTD جم انرب رادصا نم ققحتلل ةيالاتل تاوطخلا عبتا

1. اثايدحتلا ةحفص لىل لاقنتالا:

- احوال صا و FMC ءاطخأ فاشكتسأ فلم
- FDM مدختسم ءهجاو
- FDM REST API
- FTD ف رماوأل رطس ءهجاو
- احوال صا و Firepower و FTD ءي طمنلا ءدحو لا ءاطخأ فاشكتسأ فلم

FMC مدختسم ءهجاو

FMC مدختسم ءهجاو لىل ء VDB رادصا نم ققحتلل ءيلا تال تاوطلال ءب ت

1. لوح > تاميلعت رتخأ:

The screenshot shows the Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The main content area is titled 'About' and contains a table of available dashboards. A dropdown menu is open, showing options like 'Page-level Help', 'How-Tos', 'Documentation on Cisco.com', 'What's New in This Release', 'Software Download', 'Secure Firewall YouTube', 'Secure Firewall on Cisco.com', 'Firepower Migration Tool', 'Partner Ecosystem', 'Ask a Question', and 'TAC Support Cases'. The 'About' option is highlighted in the dropdown menu.

Name	admin	No	No	
Access Controlled User Statistics Provides traffic and intrusion event statistics by user				
Application Statistics Provides traffic and intrusion event statistics by application				
Application Statistics (7.1.0) Provides application statistics	admin	No	No	
Connection Summary Provides tables and charts of the activity on your monitored network segment organized by different criteria	admin	No	No	
Detailed Dashboard Provides a detailed view of activity on the appliance	admin	No	No	
Detailed Dashboard (7.0.0) Provides a detailed view of activity on the appliance	admin	No	No	
Files Dashboard Provides an overview of Malware and File Events	admin	No	No	
Security Intelligence Statistics Provides Security Intelligence statistics	admin	No	No	
Summary Dashboard Provides a summary of activity on the appliance	admin	No	Yes	

2. رادصا ءجار:

The screenshot shows the Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The main content area is titled 'About' and contains a table of system information. The 'VDB Version' is highlighted in the table.

Model	Cisco Firepower Management Center 4600
Serial Number	001234
Software Version	7.1.0 (build 90)
OS	Cisco Firepower Extensible Operating System (FX-OS) 2.11.1 (build154)
Snort Version	2.9.19 (Build 92)
Snort3 Version	3.1.7.1 (Build 108)
Rule Update Version	2022-05-02-003-vrt
Rulepack Version	2703
Module Pack Version	3070
LSP Version	lsp-rel-20220502-1613
Geolocation Update Version	2022-04-25-002
VDB Version	build 354 (2022-04-27 19:39:56)
Hostname	FMC-4600-2

FMC رماوأل رطس ءهجاو

FMC ل (CLI) رماوأل رطس ءهجاو لىل ء VDB رادصا نم ققحتلل ءيلا تال تاوطلال ءب ت

1. م كحتلا ءدحو لاصتا و SSH ربح FMC لىل لوصولا.
2. show version رماوأل ليغشتب مق.

> show version

```
-----[ FMC-4600-2.cisco.com ]-----  
Model : Cisco Firepower Management Center 4600 (66) Version 7.1.0 (Build 90)  
UUID : a10ed34e-d127-11e8-b440-728439d95305  
Rules update version : 2022-05-02-003-vrt  
LSP version : lsp-rel-20220502-1613  
VDB version : 354  
-----
```

FMC REST-API

REST-API ليمع مدخستسأ FMC REST-API لال خ نم VDB رادصإ نم ققحتلل تاوطخل هذه عبتا curl تلمعتسا، لاثم اذه يف جمانربال رادصإ نم ققحتلل

1. زي ممة قداصم زمربلط:

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H  
'Authentication: Basic' -u 'admin:Cisco123' | grep -i X-auth-access-token  
<X-auth-access-token: 7acdb34c-ea85-47bf-83fe-d77b63f012da
```

2. لاجملا مةلمع نوكت REST API تامالعتسا ةبلاغ يف زاهال لىع يوتحي يذلا لاجملا دح. ةمئاق دادرتسال مالعستالا اذه يف X قداصم لىل لوصولل زي ممل زمربال مدخستسأ. ةمزالل تالاجملا:

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_platform/v1/info/serverversion' -H 'X-auth-  
access-token: 7acdb34c-ea85-47bf-83fe-d77b63f012da' | python -m json.tool  
{  
  "items": [  
    {  
      "geoVersion": "2022-05-09-001",  
      "lspVersion": "lsp-rel-20220510-1044",  
      "serverVersion": "7.1.0 (build 90)",  
      "sruVersion": "2022-05-10-001-vrt",  
      "type": "ServerVersion",  
      "vdbVersion": "build 354 ( 2022-04-27 19:39:56 )"  
    }  
  ],  
  "links": {  
    "self": "https://10.62.184.21/api/fmc_platform/v1/info/serverversion?offset=0&limit=25"  
  },  
  "paging": {  
    "count": 1,  
    "limit": 25,  
    "offset": 0,  
    "pages": 1  
  }  
}
```

اهال صإو FMC ءاطخأ فاشكتسأ فلم

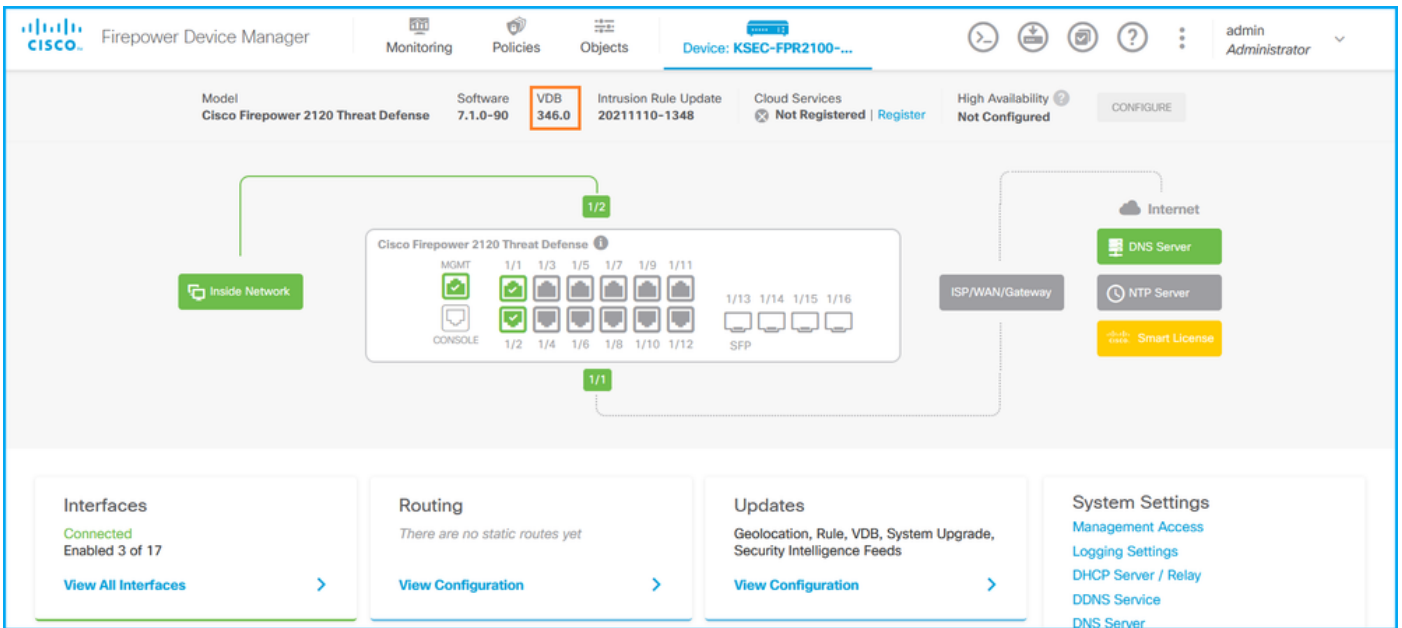
دربم ىرحتي FMC لال يف ةغيص VDB لال ققدي نأ steps اذه تعبت

1. دلجملا لىل لقتناو اهال صإو ءاطخأ فاشكتسأ فلم حتفا <filename>-troubleshooting.tar/results-<date>—xxxxx/dir-archive/etc/sf/.versiondb
2. current_build حاتفملا عم طخل دجوأو vdb.conf فلملا حتفا:

```
# pwd
/var/tmp/results-05-06-2022--199172/dir-archives/etc/sf/.versiondb
# cat vdb.conf
CURRENT_VERSION=4.5.0
CURRENT_BUILD=344
CURRENT_APPID_VER=82
CURRENT_NAVL_VER=106
```

FDM مدمتسم ةهءاو

VDB: قيقءء ةيسيسئرلا ةءفصلا يف



FDM REST API

REST-API ليمع مءءءسأ. FDM REST-API بلط ربع VDB راءصإ نم ققءءلل ءاوءءلل هءه ءبءا
curl: ءلمءءسا، لءءم اءه يف .ءمءربل راءصإ نم ققءءلل

1. زيمم ةقءاصم زمربل ط:

```
# curl -k -X POST --header 'Content-Type: application/json' --header 'Accept: application/json'
-d '{"grant_type": "password", "username": "admin", "password": "Admin#1324" }'
'https://192.0.2.2/api/fdm/latest/fdm/token'
{
  "access_token":
  "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlN2NTYjNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoiaWVhbnRlIiwiaWF0IjoiMjAyMi01-06-05T21:05:00Z",
  "expires_in": 1800,
  "refresh_expires_in": 2400,
  "refresh_token":
  "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlN2NTYjNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoiaWVhbnRlIiwiaWF0IjoiMjAyMi-06-05T21:05:00Z",
  "token_type": "Bearer"
}
```

}
2. مالع ت س ا ل ا اذ ه ي ف `access_token` ة م ي ق م د خ ت س ا .

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlNDU3ODksInN1YiI6ImFkbWluIiwianRpIjoIM2U1Njg0YjYtZDZiYS0xMwVjLTk4ZWMtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LmVzcyIsInVzZXJvdWlkIjoiyTU3ZGVmMjgtY2M3MC0xMwVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXN1clJvbGUioiJST0xFTU0Iiwib3JpZ2luIjoicGFzc3dvcmluIiwiaWF0IjoiYmFtZSI6ImFkbWluIn0.kXtsUu3_WWtOWu9w0mSdfJjwcyiVca5dgyzNjCGnlF4' | grep -i vdb
"vdbVersion" : {
  "lastSuccessVDBDate" : "2022-05-05 12:44:09Z",
  "vdbCurrentVersion" : "346",
  "vdbCurrentBuild" : "0",
  "vdbReleaseDate" : "2021-08-24 21:48:15",
  "type" : "vdbversion"
```

FTD أو Firepower Module CLI

رطس ة ه ج ا و ي ل ع و ا FTD ن م ر م ا و ا ل رطس ة ه ج ا و ي ل ع VDB ر ا د ص ا ن م ق ق ح ت ل ل ت ا و ط خ ل ا ه ذ ه ع ب ت ا ل رطس ة ه ج ا و ي ل ع ن م R م a و a l FirePOWER module (SFR):

1. FirePOWER ة د ح و ل ا ح ي ف . م ك ح ت ل ا ة د ح و ل ا ص ت ا و ا SSH ل ل ا ل خ ن م FTD ي ل ل ا ل و ص و ل ا . (CLI) ر م ا و a l رطس ة ه ج ا و ن م و ا SSH، ر ب ع ة ي ط م ن ل ا ة د ح و ل ا ي ل ل ا ل و ص و ل ا ب م ق ، ة ي ط م ن ل ا `session sfr` ر م ا ل ر ب ع ASA ب ة ص ا خ ل ا .
2. CLI ي ل ع `show version` ر م a l ل ي غ ش ت ب م ق :

```
> show version
-----[ fpr2k-1 ]-----
Model                   : Cisco Firepower 2110 Threat Defense (77) Version 7.1.0 (Build 90)
UUID                    : 0b1a9c94-8ba8-11ec-b2fd-93263934908d
LSP version             : lsp-rel-20220510-1044
VDB version             : 354
```

```
> show version
-----[ sfr1 ]-----
Model                   : ASA5516 (72) Version 7.1.0 (Build 90)
UUID                    : c049dad8-c42e-11e9-986d-bdeff3ce399e
Rules update version    : 2022-05-10-001-vrt
VDB version             : 354
```

ا ه ا ل ص ا و FirePOWER او FTD ة ي ط م ن ل ا ة د ح و ل ا ء ا ط ا خ ا ف ا ش ك ت س ا ف ل م

:د ر ب م ي ر ح ت ي ة ي ط م ن ة د ح و firepower ل ا و ا FTD ل ا ي ف ة ي ط م ن VDB ل ا ق ق و د ي ن ا steps ا ذ ه ت ع ب ت

1. <filename>- `troubleshooting.tar/results-<date>—xxxxx/command-output/` د ل ج م ل ا ي ل ل ا ل ق ت ن ا و ا ه ا ل ص ا و ء ا ط ا خ ا ل ا ف ا ش ك ت س ا ف ل م ح ت ف ا .
2. م ا د خ ت س ا ب رطس ل ا ن ع ث ح ب ا و `usr-local-sf-bin-sfcli.pl show version.output` ف ل م ل ا ح ت ف ا .
VDB ر ا د ص ا :

```
# pwd
/var/tmp/results-05-06-2022--163203/command-outputs/
```

```
# cat "usr-local-sf-bin-sfcli.pl show version.output"
-----[ fpr2k-1 ]-----
Model                : Cisco Firepower 2110 Threat Defense (77) Version 7.1.0 (Build 90)
UUID                 : 0b1a9c94-8ba8-11ec-b2fd-93263934908d
LSP version          : lsp-rel-20220510-1044
VDB version           : 354
-----

# pwd
/var/tmp/results-05-12-2022--199172/command-outputs
# cat "usr-local-sf-bin-sfcli.pl show version.output"
-----[ sfr1 ]----- Model : ASA5516 (72) Version 7.1.0 (Build 90) UUID :
c049dad8-c42e-11e9-986d-bdeff3ce399e Rules update version : 2022-05-10-001-vrt VDB version : 354
-----
```

لفطتلا ةدعاق ثي دحت تارادصا

جلا عمل لبق ام دعاوقو ةثدح مل او ةدي دجال ل فطتلا دعاوق ل فطتلا ةدعاق تا ثي دحت رفوت
ةلدعمل ةيضا رتفالا ل فطتلا جهن تاداعوا ةتبت مل دعاوق لل ةلدعمل تالاحل او

ةمزح تا ثي دحت قبطنت امك ، Snort نم 2 رادصا لىل ع (SRU) ةنم آل ةدعاق ل تا ثي دحت قبطنت
Snort نم 3 رادصا لىل ع (LSP) Lightweight ةضول ي ف نام آل

ةيلا ل تارا يخل مادختساب SRU/LSP جم انرب رادصا نم ققحت ل نكم ي

- فم دختسم ةهجاو FMC
- FMC REST-API
- اهال صا و FMC ءاطخأ فاشكتسأ فلم
- فم دختسم ةهجاو FDM
- FDM REST API
- FTD أو Firepower Module CLI
- اهال صا و Firepower أو FTD ةي طمنل ةدحول ءاطخأ فاشكتسأ فلم

فم دختسم ةهجاو

FMC: فم دختسم ةهجاو لىل ع SRU/LSP تارادصا نم ققحت ل ةيلا ل تا و طخل اعبت

ل: > تامي لعت رتخأ 1.

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and a search icon. A user profile 'admin' is visible in the top right. A help menu is open, listing various resources like 'Page-level Help', 'How-Tos', 'Documentation on Cisco.com', 'What's New in This Release', 'Software Download', 'Secure Firewall YouTube', 'Secure Firewall on Cisco.com', 'Firepower Migration Tool', 'Partner Ecosystem', 'Ask a Question', and 'TAC Support Cases'. The 'About' option is highlighted with a red box. Below the help menu, a table lists various dashboards:

Name	admin	No	No	🔍 ✎ 🗑️
Access Controlled User Statistics Provides traffic and intrusion event statistics by user				
Application Statistics Provides traffic and intrusion event statistics by application				
Application Statistics (7.1.0) Provides application statistics	admin	No	No	🔍 ✎ 🗑️
Connection Summary Provides tables and charts of the activity on your monitored network segment organized by different criteria	admin	No	No	🔍 ✎ 🗑️
Detailed Dashboard Provides a detailed view of activity on the appliance	admin	No	No	🔍 ✎ 🗑️
Detailed Dashboard (7.0.0) Provides a detailed view of activity on the appliance	admin	No	No	🔍 ✎ 🗑️
Files Dashboard Provides an overview of Malware and File Events	admin	No	No	🔍 ✎ 🗑️
Security Intelligence Statistics Provides Security Intelligence statistics	admin	No	No	🔍 ✎ 🗑️
Summary Dashboard Provides a summary of activity on the appliance	admin	No	Yes	🔍 ✎ 🗑️

2. LSP رادص او دة اقل ا شيدحت رادص | نم ققحت ال:

The screenshot shows the 'Help / About' page in the Cisco Firepower Management Center. It displays system information for a Cisco Firepower Management Center 4600. The 'Rule Update Version' and 'LSP Version' are highlighted with red boxes.

Model	Cisco Firepower Management Center 4600
Serial Number	001234
Software Version	7.1.0 (build 90)
OS	Cisco Firepower Extensible Operating System (FX-OS) 2.11.1 (build154)
Snort Version	2.9.19 (Build 92)
Snort3 Version	3.1.7.1 (Build 108)
Rule Update Version	2022-05-02-003-vrt
Rulepack Version	2703
Module Pack Version	3070
LSP Version	lsp-rel-20220502-1613
Geolocation Update Version	2022-04-25-002
VDB Version	build 354 (2022-04-27 19:39:56)
Hostname	FMC-4600-2

For technical/system questions, e-mail tac@cisco.com or call us at 1-800-553-2447 or 1-408-526-7209
Copyright 2004-2021, Cisco and/or its affiliates. All rights reserved.

FMC رم او رطس ةه او

ةدحول (CLI) رم او ال رطس ةه او يلع SRU/LSP تارادص | نم ققحت ال ةيل ال تاوطل ال عبت ال FMC م كحت ال:

1. م كحت ال ةدحو لاصتا و SSH ربع FMC يلى لوصول ال.
2. يلى CLI **show version** رم ال ليغشتب مق:

> **show version**

-----[FMC-4600-2.cisco.com]-----

```
Model : Cisco Firepower Management Center 4600 (66) Version 7.1.0 (Build 90)
UUID : a10ed34e-d127-11e8-b440-728439d95305
Rules update version : 2022-05-02-003-vrt
LSP version : lsp-rel-20220502-1613
VDB version : 354
-----
```

FMC REST-API

REST-API ليمع مدختس ا. REST-API بلط ربع جم ان ربل رادص | نم ققحت ال تاوطل ال هذه عبتا

curl: مداخلتسا متي، لاثملا اذه في جمانربلا رادصا نم ققحتلل

1. زي مة قداصم زمربل ط:

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H
'Authentication: Basic' -u 'admin:Cisco123' | grep -i X-auth-access-token

< X-auth-access-token: 9408fe38-c25c-4472-b7e6-3571bb4e2b8d
```

2. مالع تسالا اذه في X قداصم يلا لوصولل زي ممل زمربلا مداخلتسا:

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_platform/v1/info/serverversion' -H 'X-auth-
access-token: 7acdb34c-ea85-47bf-83fe-d77b63f012da' | python -m json.tool
{
  "items": [
    {
      "geoVersion": "2022-05-09-001",
      "lspVersion": "lsp-rel-20220510-1044",
      "serverVersion": "7.1.0 (build 90)",
      "sruVersion": "2022-05-10-001-vrt",
      "type": "ServerVersion",
      "vdbVersion": "build 354 ( 2022-04-27 19:39:56 )"
    }
  ],
  "links": {
    "self": "https://10.62.184.21/api/fmc_platform/v1/info/serverversion?offset=0&limit=25"
  },
  "paging": {
    "count": 1,
    "limit": 25,
    "offset": 0,
    "pages": 1
  }
}
```

اهحالصا و FMC اءاطخا فاشكتسا فلم

اهحالصا و FMC اءاطخا فاشكتسا فلم في SRU رادصا نم ققحتلل ةيالاتا تاوطخلا عبتا

1. فلم حتفا <filename>.tar/results-
<date>—xxxxx/dir-archive/etc/sf/
2. حيتا فلملا يلع يوتحت يتلا رطسالا نع شحبا و sru_versions.conf فلملا حتفا
intrusion_rules_update:

```
# pwd
/var/tmp/results-05-06-2022--199172/dir-archives/etc/sf/
# cat sru_versions.conf
Intrusion_Rules_Update=2022-04-25-003-vrt
Rule_Pack=2699
Sourcefire_Decoder_Rule_Pack=2088
Sourcefire_Policy_Pack=2763
Module_Pack=3066
snort=2.9.16-4022
```

اهحالصا و FMC اءاطخا فاشكتسا فلم في LSP رادصا نم ققحتلل ةيالاتا تاوطخلا عبتا

1. ادخل ملف `<filename>.tar/results-
<date>—xxxxx/command-output`

2. مداخلت سبب رطس لال نم ققحت و `find var-sf-lsp -maxDepth 2 -ls.output` و `/var/sf/lsp/active-lsp`

```
# pwd
```

```
/var/tmp/results-05-06-2022--199172/command-outputs
```

```
# cat "find var-sf-lsp -maxdepth 2 -ls.output"
```

```
...
```

```
Output of find /var/sf/lsp -maxdepth 2 -ls:
```

```
19138123      4 drwxrwxr-x   3 www      root      4096 May 11 04:01 /var/sf/lsp
19142268      0 lrwxrwxrwx   1 root     root      33 May 11 04:00 /var/sf/lsp/installed-
lsp -> /var/sf/lsp/lsp-rel-20220510-1044
19138299      4 drwxrwxr-x   5 www      root      4096 May 11 04:01 /var/sf/lsp/lsp-rel-
20220510-1044
19142266     600 -rwxrwxr-x   1 www      root     614400 May 10 14:55 /var/sf/lsp/lsp-rel-
20220510-1044/lsp.icdb.RELEASE.tar
19142234      4 drwxrwxr-x   5 www      root      4096 May 11 04:00 /var/sf/lsp/lsp-rel-
20220510-1044/ntd_metadata
19268898      4 drwxrwxr-x   2 www      root      4096 May 10 14:55 /var/sf/lsp/lsp-rel-
20220510-1044/icdb
19138303      4 drwxrwxr-x   6 www      root      4096 May 10 14:51 /var/sf/lsp/lsp-rel-
20220510-1044/talos_content
19142269   46640 -rw-r--r--   1 root     root    47759360 May 11 04:01 /var/sf/lsp/lsp-rel-
20220510-1044/lsp-rel-20220510-1044.tar.xz.REL.tar
19142267      4 -rwxrwxr-x   1 www      root       238 May 11 04:00 /var/sf/lsp/lsp-rel-
20220510-1044/.snort-versions
19142265      4 -rwxrwxr-x   1 www      root       26 May 10 14:51 /var/sf/lsp/lsp-rel-
20220510-1044/lspd_ver.properties
19139198     260 -rw-r--r--   1 root     root    264403 Feb 12 03:32 /var/sf/lsp/pigtail-
all-1644636642.log
19142270      0 lrwxrwxrwx   1 root     root       33 May 11 04:01 /var/sf/lsp/active-lsp
-> /var/sf/lsp/lsp-rel-20220510-1044
```

مداخلت سم ةهجاو

للفطال ةدعاق شيدحت نم ققحت ةيسئزل ةحفصلال ي:

FDM REST API

REST-API ليمع مدخستسأ FDM REST-API بلط ربع VDB رادصإ نم ققحتلل تاوطخلال هذه عبتا **curl** مادخستسإ متي، لاثملا اذه في. جمانربال رادصإ نم ققحتلل

1. زيمم ةقداصم زمر بلط 1:

```
# curl -k -X POST --header 'Content-Type: application/json' --header 'Accept: application/json'
-d '{ "grant_type": "password", "username": "admin", "password": "Admin#1324" }'
'https://192.0.2.2/api/fdm/latest/fdm/token'
{
  "access_token":
  "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoibmRjNjAtZDBmMi0xMWVjLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2hUb2t1bkV4cGlyZXNbdCI6MTY1MjI1MjM1NzQ1NywidG9rZW5UeXB1IjoiaSldUX0FjY2VzcyIsInVzZXJvdWlkIjoiyTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWlwiwidXNlclJvbGUiOiJST0xFOX0FETU1OIiwib3JpZ2luIjoicGFzc3dvcmlCJ1c2VybmFtZSI6ImFkbWluIn0.1JLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI",
  "expires_in": 1800,
  "refresh_expires_in": 2400,
  "refresh_token":
  "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoimGU0NGIxYzQtZDI0Mi0xMWVjLTk4ZWMtYTllOTlkZGMwN2Y0IiwibmJmIjoxNjUyMzQ5OTU3LCJleHAiOjE2NTIyOTY1NjksImFjY2VzclRva2VuRXhwaXJlc0F0IjoxNjUyMzQ5OTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWlwiwidXNlclJvbGUiOiJST0xFOX0FETU1OIiwib3JpZ2luIjoicGFzc3dvcmlCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
  "token_type": "Bearer"
}
```

2. مالعستسالا اذه في **access_token** ةمي ق مدخستسأ:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTI0NDU3ODksInN1YiI6ImFkbWluIiwianRpIjoim2U1Njg0YjYtZDJiYS0xMWVjLTk4ZWMtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LCJleHAiOjE2NTI0NDc1ODksInJlZnJlc2hUb2t1bkV4cGlyZXNbdCI6MTY1MjQ0ODE4OTMyNSwidG9rZW5UeXB1IjoiaSldUX0FjY2VzcyIsInVzZXJvdWlkIjoiyTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWlwiwidXNlclJvbGUiOiJST0xFOX0FETU1OIiwib3JpZ2luIjoicGFzc3dvcmlCJ1c2VybmFtZSI6ImFkbWluIn0.kXtsUu3_WWtOWu9w0mSdfJjwcyiVca5dgyzNjCGn1F4'
'https://10.62.148.181/api/fdm/v6/operational/systeminfo/default' | grep -Ei "sru|lsp"
"sruVersion" : {
  "sruVersion" : "20211110-1348",
  "lastSuccessSRUDate" : "2022-05-12 18:29:00Z",
  "lspVersions" : [ "20211110-1348" ],
  "type" : "sruversion"
```

FTD أو Firepower Module CLI

ةهجاو وأ FTD نم (CLI) رم اوأل رطس ةهجاو لىل SRU/LSP رادصإ نم ققحتلل تاوطخلال هذه عبتا FirePOWER: ةحوب ةصاخلا (CLI) رم اوأل رطس

1. FirePOWER ةحوب ةلاحي في. مكحتلا ةحوب لاصتا وأ SSH لالخي نم FTD لىل لوصولا (CLI) رم اوأل رطس ةهجاو نم وأ SSH، ربع ةيطم نلا ةحوب لىل لوصولاب مق، ةيطم نلا **session sfr** رم أل ربع ASA ب ةصاخلا
2. CLI لىل **show version** رم أل ليغشتب مق.

```
> show version
-----[ FIREPOWER1.cisco.com ]-----
Model          : Cisco Firepower 2120 Threat Defense (77) Version 7.1.0 (Build 90)
UUID           : 1cbe9952-cc6f-11ec-b63a-ae4636e42209
```



```
LSP version          : lsp-rel-20211110-1348
VDB version          : 346
```

or

```
> show version
```

```
-----[ FIREPOWER1.cisco.com ]-----
Model                : Cisco Firepower 2120 Threat Defense (77) Version 7.1.0 (Build 90)
UUID                 : 1cbe9952-cc6f-11ec-b63a-ae4636e42209
Rules update version : 2022-05-11-001-vrt
VDB version          : 346
```

```
> show version
```

```
-----[ sfr1 ]-----
Model                : ASA5516 (72) Version 7.1.0 (Build 90)
UUID                 : c049dad8-c42e-11e9-986d-bdeff3ce399e
Rules update version : 2022-05-10-001-vrt
VDB version          : 354
```

ةبسننلاب Snort 2 مادختسا مت اذا SRU شي دحت رادصا "show version" رمألا رهظي :ةظحالم
رادصاإل ضرع متي ،LSP Snort 3 لي

اهالصلإو FirePOWER أو FTD ةيظمنلا ةدحولأ ءاطخأ فاشكتسا فلم

يذل FirePOWER module أو FTD فلم يي SRU/LSP تارادصا نم ققحتلل تاوطخلا هذه عبتا
اهالصلإو ءاطخأ فاشكتسا متي

1. <filename>-
troubleshooting.tar/results-<date>—xxxxx/command-output/
مادختساب رطسلا نع ثحبا مت show version.output usr-local-sf-bin-sfcli.pl فلمال حتفا.
2. رادصا SRU/LSP:

```
# pwd
```

```
/var/tmp/results-05-06-2022--163203/command-outputs/  
# cat "usr-local-sf-bin-sfcli.pl show version.output"
```

```
-----[ FIREPOWER1.cisco.com ]-----
Model                : Cisco Firepower 2120 Threat Defense (77) Version 7.1.0 (Build 90)
UUID                 : 1cbe9952-cc6f-11ec-b63a-ae4636e42209
LSP version          : lsp-rel-20211110-1348
VDB version          : 346
```

or

```
# pwd
```

```
/var/tmp/results-05-06-2022--163203/command-outputs/  
# cat "usr-local-sf-bin-sfcli.pl show version.output"
```

```
-----[ FIREPOWER1.cisco.com ]-----
Model                : Cisco Firepower 2120 Threat Defense (77) Version 7.1.0 (Build 90)
UUID                 : 70727d06-8ba7-11ec-bfcc-999f61f27102
Rules update version : 2022-05-11-001-vrt
VDB version          : 346
```

```
# pwd
/var/tmp/results-05-12-2022--199172/command-outputs
# cat "usr-local-sf-bin-sfcli.pl show version.output"
-----[ sfr1 ]----- Model : ASA5516 (72) Version 7.1.0 (Build 90) UUID :
c049dad8-c42e-11e9-986d-bdeff3ce399e Rules update version : 2022-05-10-001-vrt
VDB version : 354
-----
```

ةفورعم تالكشم

show manager" رمألا جارخا يف FMC رادصا ضرع : [CSCwb34098](#) ENH: Cisco نم اطاخألا حيصت فرعم

ةطبترملا (OID) ةزهجالا تافرعم نيكمت : [CSCve13470](#) ENH: Cisco نم اطاخألا حيصت فرعم
FirePOWER 6.x لعل جماربلا

show version" رمأ جارخا نيمضت : [CSCwb85969](#) ENH: Cisco نم اطاخألا حيصت فرعم
اهالصال اطاخألا فاشكتسا فلم يف

تارادصا عالطتسال SNMP OIDs ممد : [CSCvu15709](#) ENH: Cisco نم اطاخألا حيصت فرعم
FirePOWER تاصنم لعل SRU/VDB/GEO عقاوم

ةلص تاذا تامولعم

- [7.1 رادصالا، Secure Firewall Management Center REST API، ل عيرسالا ادبلا ليلد](#)
- [FirePOWER NGFW ةزهجالا لعل SNMP نيوكت](#)
- [Cisco Firepower ديدهت نع عافدلا تاقيبطت ةجرمب ةهجالا ليلد](#)
- [Cisco نم FXOS REST تاقيبطتلا ةجرمب ةهجالا عجرم](#)
- [Cisco ASA عم قفاوتلا](#)
- [FXOS و 3100 ASA نمألا ةيامحلا رادجو Firepower 1000/2100 ةمزح تارادصا](#)
- [ةنمضم تانوكم](#)
- [اهالصال او Firepower اطاخأ فاشكتسال فلملا عاشنا تاءارجا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئى. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىلإ أمئاد عوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصلأل يزي لچنل دن تسمل