

驗證Firepower軟體版本

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[驗證軟體版本](#)

[FMC軟體版本](#)

[FMC UI](#)

[FMC CLI](#)

[FMC REST-API](#)

[FMC故障排除檔案](#)

[FTD或Firepower模組CLI](#)

[FTD或Firepower模組疑難排解檔案](#)

[FDM軟體版本](#)

[FDM UI](#)

[FDM REST API](#)

[FTD CLI](#)

[FTD SNMP](#)

[FTD疑難排解檔案](#)

[FXOS軟體版本](#)

[FCM UI](#)

[FXOS CLI](#)

[FXOS REST-API](#)

[FXOS SNMP](#)

[FXOS機箱show-tech檔案](#)

[FTD軟體版本](#)

[FTD CLI](#)

[FTD SNMP](#)

[FMC UI](#)

[FMC REST API](#)

[FDM UI](#)

[FDM REST-API](#)

[FTD疑難排解檔案](#)

[FCM UI](#)

[FXOS CLI](#)

[FXOS REST-API](#)

[FXOS機箱show-tech檔案](#)

[ASA軟體版本](#)

[ASA CLI](#)

[ASA SNMP](#)

[ASA show-tech檔案](#)

[FCM UI](#)

[FXOS CLI](#)

[FXOS REST-API](#)

[FXOS機箱show-tech檔案](#)

[Firepower模組軟體版本](#)

[FMC UI](#)

[FMC REST-API](#)

[Firepower模組CLI](#)

[Firepower模組故障排除檔案](#)

[ASA CLI](#)

[ASA show-tech檔案](#)

[驗證Snort、VDB和SRU版本](#)

[深度封包檢測引擎\(Snort\)版本](#)

[FMC UI](#)

[FMC REST-API](#)

[FDM UI](#)

[FDM REST API](#)

[FTD或Firepower CLI](#)

[FTD或Firepower模組疑難排解檔案](#)

[漏洞資料庫\(VDB\)版本](#)

[FMC UI](#)

[FMC CLI](#)

[FMC REST-API](#)

[FMC故障排除檔案](#)

[FDM UI](#)

[FDM REST API](#)

[FTD或Firepower模組CLI](#)

[FTD或Firepower模組疑難排解檔案](#)

[入侵規則更新版本](#)

[FMC UI](#)

[FMC CLI](#)

[FMC REST-API](#)

[FMC故障排除檔案](#)

[FDM UI](#)

[FDM REST API](#)

[FTD或Firepower模組CLI](#)

[FTD或Firepower模組疑難排解檔案](#)

[已知的問題](#)

[相關資訊](#)

簡介

本檔案將說明Firepower軟體版本的驗證。

必要條件

需求

基本產品知識、REST-API、SNMP。

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

本文中的資訊係根據以下軟體和硬體版本：

- Firepower 11xx
- Firepower 21xx
- Firepower 31xx
- Firepower 41xx
- Firepower管理中心(FMC)版本7.1.x
- Firepower可擴充作業系統(FXOS)2.11.1.x
- Firepower裝置管理器(FDM)7.1.x
- Firepower威脅防禦7.1.x
- ASA 9.17.x

驗證軟體版本

FMC軟體版本

可以使用以下選項驗證FMC軟體版本：

- FMC UI
- FMC CLI
- REST API請求
- FMC故障排除檔案
- FTD或Firepower模組CLI
- FTD或Firepower模組故障排除檔案

FMC UI

按照以下步驟驗證FMC UI上的FMC軟體版本：

1. 選擇**Help > About**:

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. 檢查軟體版本:

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 CLI

按照以下步驟驗證FMC CLI上的FMC軟體版本。

1. 通過SSH或控制檯連線訪問FMC。標語顯示軟體版本：

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

2. 在CLI上運行show version命令：

```
> 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

按照以下步驟通過FMC REST-API請求驗證FMC軟體版本。使用REST-API客戶端驗證軟體版本。
在此範例中，使用curl:

1. 請求身份驗證令牌：

```
# 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. 在此查詢中使用X-auth-access-token:

```
# 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  
  }  
}
```

附註：命令字串的「| python -m json.tool」部分用於以JSON樣式格式化輸出，該部分是可選的。

FMC故障排除檔案

按照以下步驟驗證故障排除檔案中的FMC軟體版本：

1. 開啟疑難解答檔案，導航到資料夾<filename>.tar/results-<date>—xxxxxx/dir-archives/etc/sf/
2. 開啟檔案ims.conf，並找到具有金鑰SWVERSION和SWBUILD的行：

```
# 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或Firepower模組CLI

按照以下步驟驗證FTD CLI或Firepower模組CLI上的FMC軟體版本：

1. 透過SSH或主控台連線存取FTD。對於Firepower模組，請通過SSH或通過session sfr命令從

ASA CLI訪問該模組。

2. 運行expert命令。

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

3.在FTD上執行 `less /ngfw/var/sf/detection_engine/<UUID>/ngfw.rules` 命令，或在Firepower模組上執行`less /var/sf/detection_engine/<UUID>/ngfw.rules` 命令，並檢查行DC版本：

```
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
#
#####
...
```

FTD或Firepower模組疑難排解檔案

請依照以下步驟操作，驗證FTD或Firepower模組疑難排解檔案中的FMC軟體版本：

1. 如果檔案是在FTD上產生，請開啟疑難排解檔案並導覽至<filename>-troubleshoot .tar/results-<date>—xxxxxx/file-contents/ngfw/var/sf/detection-engine/<UUID>/ 資料夾。對於Firepower模組，導航到資料夾<filename>-troubleshoot .tar/results-<date>—xxxxxx/file-contents/var/sf/detection-engine/<UUID>/
2. 開啟ngfw.rules檔案並檢查行DC版本：

```
# 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軟體版本

可以使用以下選項驗證FDM軟體版本：

- FDM UI
- FTD CLI


```
luIjoiCGFzc3dvcMqiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",  
"token_type": "Bearer"  
}
```

2.在此查詢中使用訪問令牌值：

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer  
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoibmMjMmRjNjAtZDBmMi0xMWV  
jLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjozNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2h0b2t1bWV4cG1  
yZXNbdCI6MTY1MjI1MjM1NzQ1NywidG9rZW5UeXB1IjoisIldUX0FjY2VzcyIsInVzZXJvdWlkIjoiyTU3ZGVmMjgtY2M3MC0  
xMWVjLTk4ZWMtZjk4ODExNjNjZWlwiwidXN1c1JvbGUiOiJST0xFOX0FETU1OIiwib3JpZ2luIjoicGFzc3dvcMqiLCJ1c2V  
ybmfZSI6ImFkbWluIn0.1JLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI'  
'https://192.0.2.2/api/fdm/v6/operational/systeminfo/default' | grep -i software  
"softwareVersion" : "7.1.0-90",  
"softwareVersion" : "7.1.0-90",
```

FTD CLI

請按照一節中的步驟操作。

FTD SNMP

請按照一節中的步驟操作。

FTD疑難排解檔案

請按照一節中的步驟操作。

FCM UI

FCM在Firepower 4100和Firepower 9300系列上可用。請按照一節中的步驟操作。

FXOS CLI

請按照一節中的步驟操作。

FXOS REST-API

請按照一節中的步驟操作。

FXOS機箱show-tech檔案

請按照一節中的步驟操作。

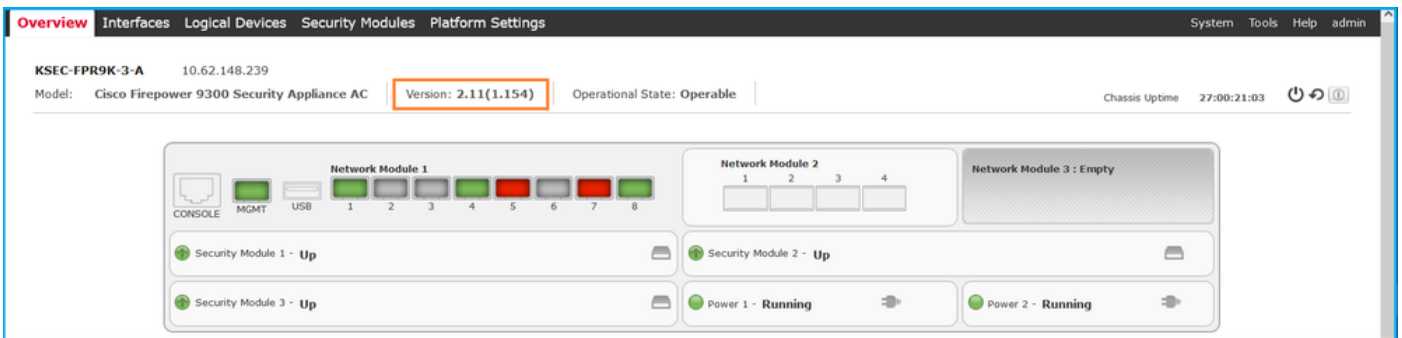
FXOS軟體版本

可以使用以下選項驗證FXOS軟體版本：

- FCM UI (僅限Firepower 4100/9300)
- FXOS CLI
- FXOS REST API
- FXOS SNMP輪詢
- FXOS機箱show-tech檔案。

FCM UI

要驗證FCM UI上的FXOS軟體版本，請選中首頁上的Version:



FXOS CLI

Firepower 4100/9300

按照以下步驟驗證FXOS CLI上的FXOS軟體版本：

1. 建立到機箱的控制檯或SSH連線。
2. 切換到scope system 並運行show firmware monitor 命令:

```
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
```

採用FTD的Firepower 1000/2100/3100

按照以下步驟驗證FXOS CLI上的FXOS軟體版本：

1. 建立到機箱的控制檯連線或到FTD的SSH連線。
若使用SSH連線到FTD，請在FTD CLISH上執行connect fxos命令：

```
> connect fxos
```

2. 切換到scope system 並運行show firmware detail 命令:

```
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)
```

具備ASA的Firepower 1000/3100和裝置模式中具有ASA的Firepower 2100

按照以下步驟驗證FXOS CLI上的FXOS軟體版本：

1. 建立到機箱的控制檯連線或到ASA的telnet/SSH連線。
如果通過telnet/SSH連線到ASA，請在ASA CLI上運行connect fxos命令。

```
asa# connect fxos
```

2. 切換到scope system並運行show firmware detail命令:

```
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)
```

在平台模式下具備ASA的Firepower 2100

按照以下步驟驗證FXOS CLI上的FXOS軟體版本：

1. 建立與機箱的SSH或控制檯連線或與ASA的telnet/SSH連線。
如果通過telnet/SSH連線到ASA，請在ASA CLI上運行**connect fxos**命令。

```
asa# connect fxos
```

2. 切換到**scope system** 並運行**show firmware detail** 命令：

```
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

Firepower 4100/9300系列支援FXOS REST-API。

Firepower 4100/9300

按照以下步驟通過FXOS REST-API請求驗證FXOS軟體版本。使用REST-API客戶端驗證軟體版本。在此範例中使用了curl:

1. 請求身份驗證令牌：

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

2.在此查詢中使用令牌：

```
# 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 SNMP

FXOS上的SNMP配置在帶有ASA的Firepower 2100平台模式和Firepower 4100/9300上受支援。

Firepower 4100/9300

按照以下步驟通過SNMP驗證FXOS軟體版本：

1. 確保在FXOS上配置了SNMP。有關配置步驟，請參閱[在Firepower NGFW裝置上配置SNMP](#)。
2. Poll `.1.3.6.1.4.1.9.9.826.1.30.47.1.6`或CISCO-FIREPOWER-FIRMWARE-MIB:`cfprFirmwareRunningPackageVersion`:

```
# snmpwalk -On -v2c -c cisco 192.0.2.100 .1.3.6.1.4.1.9.9.826.1.30.47.1.6
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.20823 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.25326 = ""
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.25331 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.30266 = STRING: "1.0.18"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.30269 = STRING: "1.0.18"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.30779 = ""
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.30780 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.30781 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.32615 = STRING: "2.11(1.154)"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.48820 = STRING: "0.0"
```

在平台模式下具備ASA的Firepower 2100

按照以下步驟通過SNMP驗證FXOS軟體版本：

1. 確保在FXOS上配置了SNMP。有關配置步驟，請參閱[在Firepower NGFW裝置上配置SNMP](#)。
2. Poll `.1.3.6.1.2.1.1.1.0`或SNMPv2-MIB::`sysDescr.0`:

```
# snmpwalk -On -v2c -c cisco 192.0.2.101 SNMPv2-MIB::sysDescr.0
.1.3.6.1.2.1.1.1.0 = 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)
```

FXOS機箱show-tech檔案

Firepower 4100/9300

按照以下步驟驗證FXOS機箱show-tech檔案中的FXOS軟體版本：

1. 對於FXOS版本2.7及更高版本，請在<name>_BC1_all.tar/
FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar中開啟檔案sam_techsupportinfo
對於早期版本，請在FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar中開啟檔案
sam_techsupportinfo。

2. 檢查「show firmware monitor」命令的輸出：

```
# 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. 在<name>_FPRM.tar.gz/<name>_FPRM.tar中開啟檔案tech_support_brief

2. 檢查「show firmware detail」命令的輸出：

```
# 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軟體版本

使用以下選項可驗證FTD軟體版本：

- FTD CLI
- FTD SNMP投票
- FTD疑難排解檔案
- FMC UI
- FMC REST API
- FDM UI
- FDM REST API
- FCM UI
- FXOS CLI
- FXOS REST API
- FXOS機箱show-tech檔案

FTD CLI

請依照以下步驟在FTD CLI上驗證FTD軟體版本：

1. 根據平台和部署模式，使用以下選項訪問FTD CLI:

- 直接通過SSH訪問FTD — 所有平台
- 通過**connect ftd**指令，從FXOS主控台CLI(Firepower 1000/2100/3100)進行存取
- 通過命令(Firepower 4100/9300)從FXOS CLI訪問：
connect module <x> [console|telnet]，其中x是插槽ID，然後

連線ftd [例項],其中例項僅與多例項部署相關。

- 對於虛擬FTD，直接通過SSH訪問FTD，或透過虛擬機器監控程式或雲使用者介面進行主控台訪問

2.在CLI上運行**show version**命令：

```
> 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

請依照以下步驟操作，透過SNMP驗證FTD軟體版本：

1. 確保已配置並啟用SNMP。有關FDM管理的FTD的資訊，請參閱[在Firepower FDM上配置SNMP並對其進行故障排除](#)。有關FMC管理的FTD的資訊，請參閱[在Firepower NGFW裝置上配置SNMP](#)以瞭解配置步驟。
2. Poll OID **SNMPv2-MIB::sysDescr.0**或OID **.1.3.6.1.2.1.1.1.0**：

```
# 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 UI

按照以下步驟驗證FMC UI上的FTD軟體版本：

1. 選擇**Devices > Device Management**:

The screenshot displays the Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', '1 Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and 'admin'. A dropdown menu is open under 'Devices', with '2 Device Management' highlighted. The main content area shows a 'Summary Dashboard' with various widgets: 'Unique Applications over Time' (line graph), 'Top Web Applications' (table), 'Top Client Applications' (table), and 'Traffic by Application Risk' (table).

Application	Total Bytes (KB)
Ubuntu	548.77
Ubuntu Update Manager	5.57

Application	Total Bytes (KB)
Internet Explorer	5,901,473.76
Advanced Packaging Tool	7.42
Wget	0.63
NetBIOS-dgm	0.24

Risk	Total Bytes (KB)
Medium	1,671,103,043.61
Very Low	5,902,307.84

2. 檢查**Version**列：

Name	Model	Version	Chassis	Licenses	Access Control Policy	Group
LAB-FPR2K High Availability						
fpr2k-1(Primary, Active) Snort 3 192.0.2.140 - Routed	Firepower 2110 with FTD	7.1.0	N/A	Base, Threat (2 more...)	LAB-FPR2K-ACL	
ftp2k-2(Secondary, Standby) Snort 3 192.0.2.149 - Routed	Firepower 2110 with FTD	7.1.0	N/A	Base, Threat (2 more...)	LAB-FPR2K-ACL	

FMC REST API

請依照以下步驟操作，透過FMC REST-API驗證FTD軟體版本。使用REST-API客戶端驗證軟體版本。在此範例中，使用curl:

1. 請求身份驗證令牌：

```
# 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. 標識包含裝置的域。在大多數REST API查詢中，domain 引數是必需的。在此查詢中使用X-auth-access-token以檢索域清單：

```
# 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. 使用域UUID查詢裝置記錄：

```
# 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.使用域UUID和裝置/容器UUID:

```
# 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\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\n1:
Int: Internal-Data0/1 : address is 000f.b748.4801, irq 0\n3: Ext: Management1/1 :
address is 707d.b9e2.836d, irq 0\n4: Int: Internal-Data1/1 : address is 0000.0100.0001, irq
0\n5: Int: Internal-Data1/2 : address is 0000.0300.0001, irq 0\n6: Int: Internal-Controll1/1
: address is 0000.0001.0001, irq 0\n\nSerial Number: JAD213508B6\n\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 UI

請按照一節中的步驟操作。

FDM REST-API

請按照一節中的步驟操作。

FTD疑難排解檔案

請依照以下步驟操作，驗證FTD疑難排解檔案中的FTD軟體版本：

1. 開啟疑難解答檔案，導航到資料夾<filename>-troubleshoot.tar/results-<date>—xxxxxx/command-outputs/

2. 開啟檔案usr-local-sf-bin-sfcli.pl show version.output , 找到Model:

```
# 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 UI

對於Firepower 4100/9300上的FTD , 請使用FCM並在「Logical devices」頁籤中選中Version:

The screenshot displays the 'Logical Devices' section of the FCM UI. It is divided into three Security Modules:

- Security Module 1 (1 Native instance):** Contains one ASA application with version 9.16.2.7. The status is 'Online'.
- Security Module 2 (0 instances):** No logical devices are present on this module.
- Security Module 3 (1 Container instance):** Contains one FTD application with version 7.1.0.90. The status is 'Online'. The application details are expanded to show:
 - Interface Name:** Ethernet1/6, Ethernet1/7, Port-channel1
 - Type:** data
 - Attributes:** Cluster Operational Status: not-applicable, FIREPOWER-MGMT-IP: 10.62.148.242, MGMT-URL: https://10.62.148.240/, HA-ROLE: standalone, UUID: 3050d4c-c0aa-11ec-9b2a-8491ab800c8

FXOS CLI

Firepower 4100/9300上的FTD

請依照以下步驟在FXOS CLI上驗證FTD軟體版本:

1. 建立到機箱的控制檯或SSH連線。
2. 切換到scope ssa , 然後運行show app-instance 命令:

```
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
```

Firepower 1000/2100/3100上的FTD

請依照以下步驟在FXOS CLI上驗證FTD軟體版本：

1. 建立到機箱的控制檯連線或到FTD的SSH連線

若使用SSH連線到FTD，請在FTD CLISH上執行**connect fxos**命令：

```
> connect fxos
```

2. 切換到scope ssa，然後運行show app-instance命令：

```
firepower# scope ssa
```

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

Application Name	Slot ID	Admin State	Operational State	Running Version	Startup Version
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

請依照以下步驟操作，透過FXOS REST-API驗證FTD軟體版本：

1. 請求身份驗證令牌：

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

2. 使用此查詢中的標籤，並確保指定安裝FTD的插槽ID：

```
# 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機箱show-tech檔案

按照以下步驟驗證FXOS機箱show-tech檔案中的FTD軟體版本：

Firepower 4100/9300上的FTD

1. 對於FXOS 2.7及更高版本，請在<name>_BC1_all.tar/

FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar中開啟檔案sam_techsupportinfo

對於早期版本，請在FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar中開啟檔案sam_techsupportinfo。

2.檢查「show slot expand detail」下每個插槽的部分：

```
# 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
...
```

Firepower 1000/2100/3100上的FTD

1. 在<name>_FPRM.tar.gz/<name>_FPRM.tar中開啟檔案tech_support_brief
2. 檢查「scope ssa」和「show slot」部分：

```
# 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軟體版本

可以使用以下選項驗證ASA軟體版本：

- ASA CLI
- ASA SNMP輪詢

- ASA show-tech檔案
- FCM UI
- FXOS CLI
- FXOS REST API
- FXOS機箱show-tech檔案

ASA CLI

按照以下步驟驗證ASA CLI上的ASA軟體版本：

1.根據平台和部署模式，使用以下選項訪問ASA CLI:

- 在裝置模式下直接通過telnet/SSH訪問Firepower 1000/3100和Firepower 2100上的ASA
- 在平台模式下從Firepower 2100上的FXOS控制檯CLI訪問，並使用**connect asa** 命令連線到ASA
- 通過命令(Firepower 4100/9300)從FXOS CLI訪問：

connect module <x> [console|telnet]，其中x是插槽ID，然後連接asa

- 對於虛擬ASA，直接通過SSH訪問ASA，或者通過虛擬機器監控程式或雲UI進行控制檯訪問

2.運行**show version**命令：

```
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

按照以下步驟通過SNMP驗證ASA軟體版本：

1. 確保已配置並啟用SNMP。
2. 使用SNMP客戶端輪詢OID **SNMPv2-MIB::sysDescr.0**或OID **.1.3.6.1.2.1.1.1.0**:

```
# 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檔案

使用Cisco Adaptive Security Appliance Software Version字串搜索行:

Cisco Adaptive Security Appliance Software Version 9.17(1)

SSP Operating System Version 2.11(1.154)

Device Manager Version 7.17(1)

...

FCM UI

請按照一節中的步驟操作。

FXOS CLI

請按照一節中的步驟操作。

FXOS REST-API

請按照一節中的步驟操作。

FXOS機箱show-tech檔案

請按照一節中的步驟操作。

Firepower模組軟體版本

ASA上的Firepower模組是舊版Sourcefire模組或SFR的新名稱。

可以使用以下選項驗證其軟體版本：

- FMC UI
- FMC REST-API

- Firepower模組CLI
- Firepower模組故障排除檔案
- ASA CLI
- ASA show-tech檔案

FMC UI

請按照一節中的步驟操作。

FMC REST-API

請按照一節中的步驟操作。

Firepower模組CLI

按照以下步驟驗證模組CLI上的Firepower模組軟體版本：

- 1.通過SSH或通過`session sfr`命令從ASA CLI連線到模組。
- 2.運行`show version`命令：

```
> 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
-----
```

Firepower模組故障排除檔案

按照以下步驟驗證模組故障排除檔案中的Firepower模組軟體版本：

1. 開啟疑難解答檔案，導航到資料夾<filename>-troubleshoot.tar/results-<date>—xxxxxx/command-outputs/
2. 開啟檔案usr-local-sf-bin-sfcli.pl show version.output，找到Model:

```
# 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
-----
```

ASA CLI

在ASA CLI上運行show module sfr details命令並檢查軟體版本：

```
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
```

ASA show-tech檔案

使用show module sfr detail字串搜尋行：

```
----- 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
```

驗證Snort、VDB和SRU版本

深度封包檢測引擎(Snort)版本

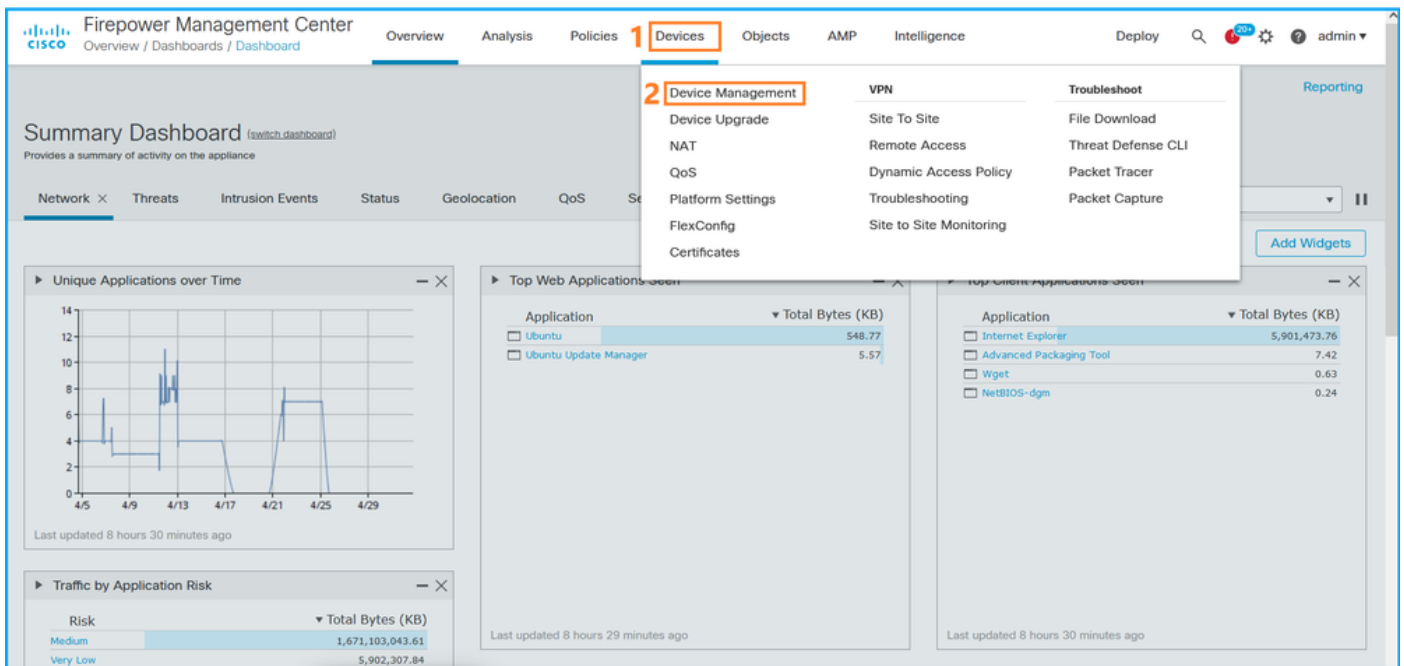
使用以下選項可以驗證Snort版本：

- FMC UI
- FMC REST-API
- FDM UI
- FDM REST API
- FTD或Firepower模組CLI
- FTD或Firepower模組故障排除檔案

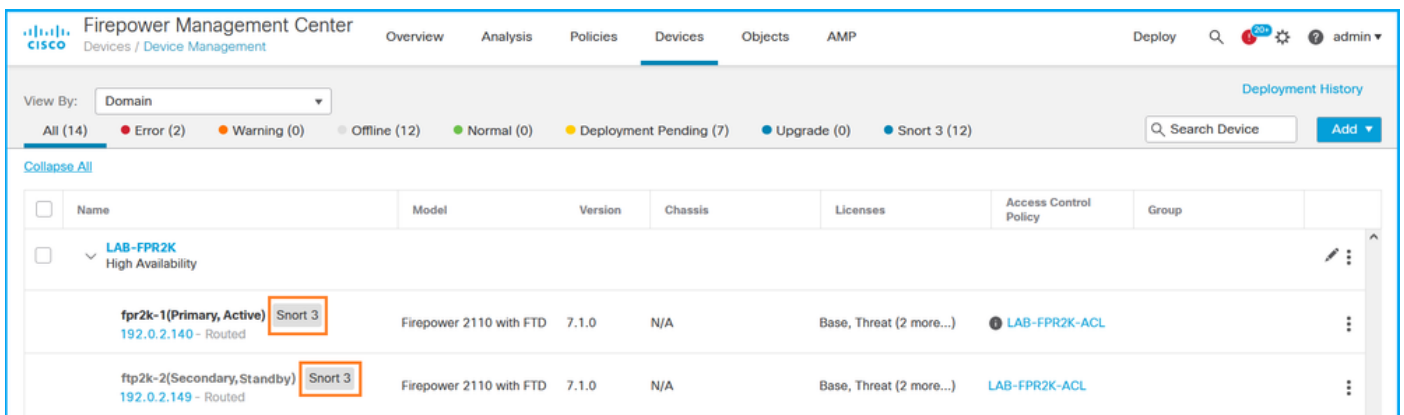
FMC UI

按照以下步驟驗證FMC UI上的FTD Snort版本：

1. 選擇Devices > Device Management:



2. 檢查Snort標籤：



FMC REST-API

請依照以下步驟操作，透過FMC REST-API驗證FTD Snort版本。使用REST-API客戶端驗證軟體版本。在此範例中使用了curl：

1. 請求身份驗證令牌：

```
# 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. 標識包含裝置的域。在大多數REST API查詢中，domain 引數是必需的。在此查詢中使用X-auth-access-token以檢索域清單：

```
# 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.使用域UUID查詢裝置記錄:

```

# 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. 在此請求中使用域UUID和裝置/容器UUID:

```

# 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 UI

按照以下步驟驗證FDM UI上的FTD Snort版本：

1. 轉到**更新**頁面:

- FMC故障排除檔案
- FDM UI
- FDM REST API
- FTD CLI
- FTD或Firepower模組故障排除檔案

FMC UI

按照以下步驟驗證FMC UI上的VDB版本：

1. 選擇Help > About:

The screenshot shows the FMC UI with the 'Help' menu open. The 'About' option is highlighted with a red box. The main content area displays a table of dashboard widgets.

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. 檢查VDB版本:

The screenshot shows the 'About' page in the FMC UI. The 'VDB Version' field is highlighted with a red box, displaying 'build 354 (2022-04-27 19:39:56)'.

Model	Cisco Firepower Management Center 4600	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.
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 CLI

按照以下步驟驗證FMC CLI上的VDB版本：

1. 通過SSH或控制檯連線訪問FMC。
2. 執行show version指令：

```
> 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

按照以下步驟通過FMC REST-API驗證VDB版本。使用REST-API客戶端驗證軟體版本。在此範例中使用了curl:

1. 請求身份驗證令牌：

```
# 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.標識包含裝置的域。在大多數REST API查詢中，domain 引數是必需的。在此查詢中使用X-auth-access-token以檢索域清單：

```
# 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
  }
}
```

FMC故障排除檔案

按照以下步驟驗證FMC故障排除檔案中的VDB版本：

1. 開啟疑難解答檔案並導航到資料夾<filename>-troubleshoot .tar/results-<date>—xxxxxx/dir-archives/etc/sf/.versiondb
2. 開啟檔案vdb.conf，找到包含項CURRENT_BUILD的行：

2.在此查詢中使用access_token值：

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlNTI0NDU3ODksInN1YiI6ImFkbWluIiwianRpIjoim2U1Njg0YjYtZDZiYS0xMWV
jLTk4ZWMtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LmFkbWluIiwiaWF0IjoiSldUX0FjY2VzcyIsInVzZXJvdWlkIjoiYTU3ZGVmMjgtY2M3MC0
xMWVjLTk4ZWMtZjk4ODExNjNjZWlwiwiwidXN1clJvbnVjIiwiaXN0IjoiST0xR0FETU10Iiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2V
ybmfTzSI6ImFkbWluIn0.kXtsUu3_WWtOWu9w0mSdfJjwcyiVca5dgyzNjCGnlF4'
'https://10.62.148.181/api/fdm/v6/operational/systeminfo/default' | 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或Firepower模組CLI

按照以下步驟在FTD CLI或Firepower模組(SFR)CLI上驗證VDB版本：

1. 透過SSH或主控台連線存取FTD。對於Firepower模組，請通過SSH或通過session sfr命令從ASA CLI訪問該模組。
2. 在CLI上運行show version命令：

```
> 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
-----
```

FTD或Firepower模組疑難排解檔案

請依照以下步驟操作，驗證FTD或Firepower模組疑難排解檔案中的VDB版本：

1. 開啟疑難解答檔案，導航到<filename>-troubleshoot.tar/results-<date>-xxxxxx/command-outputs/
2. 開啟檔案usr-local-sf-bin-sfcli.pl show version.output，然後找到具有VDB版本的行：

```
# 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
-----
```

入侵規則更新版本

入侵規則更新提供新的和更新的入侵規則和前處理器規則、已安裝規則的修改狀態以及修改的預設入侵策略設定。

安全規則更新(SRU)適用於Snort版本2，輕量安全包(LSP)更新適用於Snort版本3。

可以使用以下選項驗證SRU/LSP軟體版本：

- FMC UI
- FMC REST-API
- FMC故障排除檔案
- FDM UI
- FDM REST API
- FTD或Firepower模組CLI
- FTD或Firepower模組故障排除檔案

FMC UI

按照以下步驟驗證FMC UI上的SRU/LSP版本：

1. 選擇Help > About:

Name	Description	Actions
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 [Icons]
Connection Summary	Provides tables and charts of the activity on your monitored network segment organized by different criteria	admin No No [Icons]
Detailed Dashboard	Provides a detailed view of activity on the appliance	admin No No [Icons]
Detailed Dashboard (7.0.0)	Provides a detailed view of activity on the appliance	admin No No [Icons]
Files Dashboard	Provides an overview of Malware and File Events	admin No No [Icons]
Security Intelligence Statistics	Provides Security Intelligence statistics	admin No No [Icons]
Summary Dashboard	Provides a summary of activity on the appliance	admin No Yes [Icons]

2. 檢查規則更新版本和LSP版本:

The screenshot shows the Cisco Firepower Management Center (FMC) web interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The main content area displays system information for a Cisco Firepower Management Center 4600. The 'Rule Update Version' is 2022-05-02-003-vrt and the 'LSP Version' is lsp-rel-20220502-1613. Other information includes the 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)), Rulepack Version (2703), Module Pack Version (3070), Geolocation Update Version (2022-04-25-002), VDB Version (build 354 (2022-04-27 19:39:56)), and Hostname (FMC-4600-2). A sidebar on the right contains contact information for technical support and a copyright notice.

FMC CLI

按照以下步驟驗證FMC CLI上的SRU/LSP版本：

1. 通過SSH或控制檯連線訪問FMC。
2. 在CLI上運行**show version**命令：

```
> 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

按照以下步驟通過REST-API請求驗證軟體版本。使用REST-API客戶端驗證軟體版本。在此範例中，使用**curl**：

1. 請求身份驗證令牌：

```
# 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. 在此查詢中使用**X-auth-access-token**：

```
# 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
  }
}
}

```

FMC故障排除檔案

按照以下步驟驗證FMC故障排除檔案中的SRU版本：

1. 開啟疑難解答檔案並轉到資料夾<filename>.tar/results-<date>—xxxxxx/dir-archives/etc/sf/
2. 開啟檔案sru_versions.conf，然後找到包含金鑰Intrusion_Rules_Update的行：

```

# 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

```

按照以下步驟驗證FMC故障排除檔案中的LSP版本：

1. 開啟疑難排解檔案並前往資料夾<filename>.tar/results-<date>—xxxxxx/command-output
2. 開啟文件，查詢var-sf-lsp -maxdepth 2 -ls.output，然後使用/var/sf/lsp/active-lsp檢查該行

```

# 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

```



```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlNDU3ODksInN1YiI6ImFkbWluIiwianRpIjoim2U1Njg0YjYtZDZiYS0xMWV
jLTk4ZWmtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LCJleHAiOiJlNDU3ODksInJlZnJlc2hUb2t1bkV4cG1
yZXNBdCI6MTY1MjQ0ODE4OTMyNSwidG9rZW5UeXB1IjoislDUxOFjY2VzcyIsInVzZXJvdWlkIjoiyTU3ZGVmMjgtY2M3MC0
xMWVjLTk4ZWmtZjk4ODE4OTMyNSwidG9rZW5UeXB1IjoislDUxOFjY2VzcyIsInVzZXJvdWlkIjoiyTU3ZGVmMjgtY2M3MC0
ybmFtZSI6ImFkbWluIn0.kXtsUu3_WWtOWu9w0mSdfJjwcyiVca5dgyzNjCGnlF4'
'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或Firepower模組CLI

按照以下步驟驗證FTD CLI或Firepower模組CLI上的SRU/LSP版本：

1. 透過SSH或主控台連線存取FTD。對於Firepower模組，請通過SSH或通過session sfr命令從ASA CLI訪問該模組。
2. 在CLI上運行show version命令：

```
> 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
-----
```

附註：如果使用Snort 2,show version命令將顯示SRU更新版本。顯示Snort 3 LSP版本。

FTD或Firepower模組疑難排解檔案

按照以下步驟驗證FTD或Firepower模組故障排除檔案中的SRU/LSP版本：

1. 開啟疑難解答檔案，並轉到資料夾<filename>-troubleshoot.tar/results-<date>-xxxxxx/command-output/
2. 開啟檔案usr-local-sf-bin-sfcli.pl show version.output，然後找到帶有SRU/LSP版本的行：

```

# 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
-----

```

已知的問題

思科錯誤ID [CSCwb34098](#) ENH:在「show managers」命令輸出中顯示FMC版本

思科錯誤ID [CSCve13470](#) ENH:在FirePOWER 6.x上啟用軟體相關OID

思科錯誤ID [CSCwb85969](#) ENH:在疑難排解檔案中包括「show version」 FMC CLISH指令的輸出

思科錯誤ID [CSCvu15709](#) ENH:支援SNMP OID在Firepower平台上輪詢SRU/VDB/GEO位置版本

相關資訊

- [安全防火牆管理中心REST API快速入門手冊7.1版](#)
- [在Firepower NGFW裝置上配置SNMP](#)
- [Cisco Firepower威脅防禦REST API指南](#)
- [Cisco FXOS REST API參考](#)
- [Cisco ASA相容性](#)
- [Firepower 1000/2100和安全防火牆3100 ASA和FXOS捆綁版本](#)
- [捆綁元件](#)

- [Firepower檔案生成故障排除過程](#)