验证Firepower软件版本

目录

简介

本文档介绍Firepower软件版本的验证。

先决条件

要求

基本产品知识、REST-API、SNMP。

使用的组件

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

本文档中的信息基于以下软件和硬件版本：

- Firepower 11xx
- Firepower 21xx
- Firepower 31xx
- Firepower 41xx
- Firepower管理中心(FMC)版本7.1.x
- Firepower可扩展操作系统(FXOS)2.11.1.x
- Firepower设备管理器(FDM)7.1.x
- Firepower威胁防御7.1.x
- ASA 9.17.x

验证软件版本

FMC软件版本

FMC软件版本可以使用以下选项进行验证：

- FMC UI
- FMC CLI
- REST API请求
- FMC故障排除文件
- FTD或Firepower模块CLI
- FTD或Firepower模块故障排除文件

FMC UI

按照以下步骤验证FMC UI上的FMC软件版本：

1. 选择**帮助>关于**：
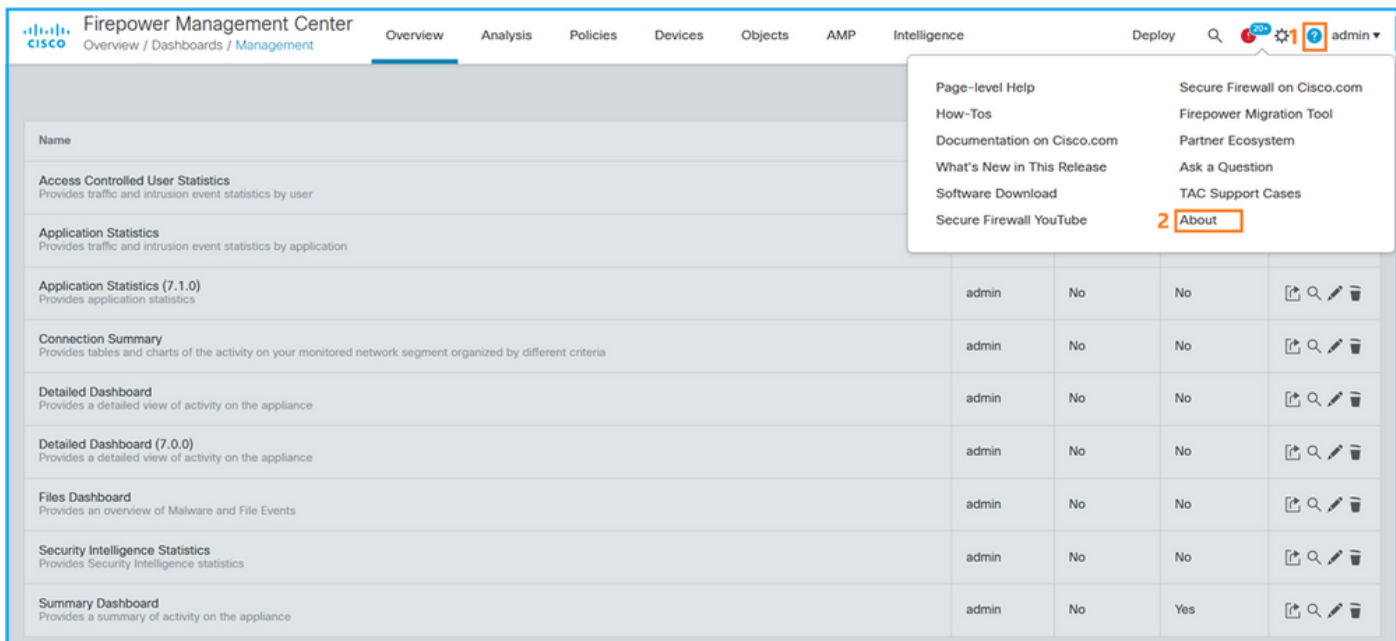
2.检查软件版本：
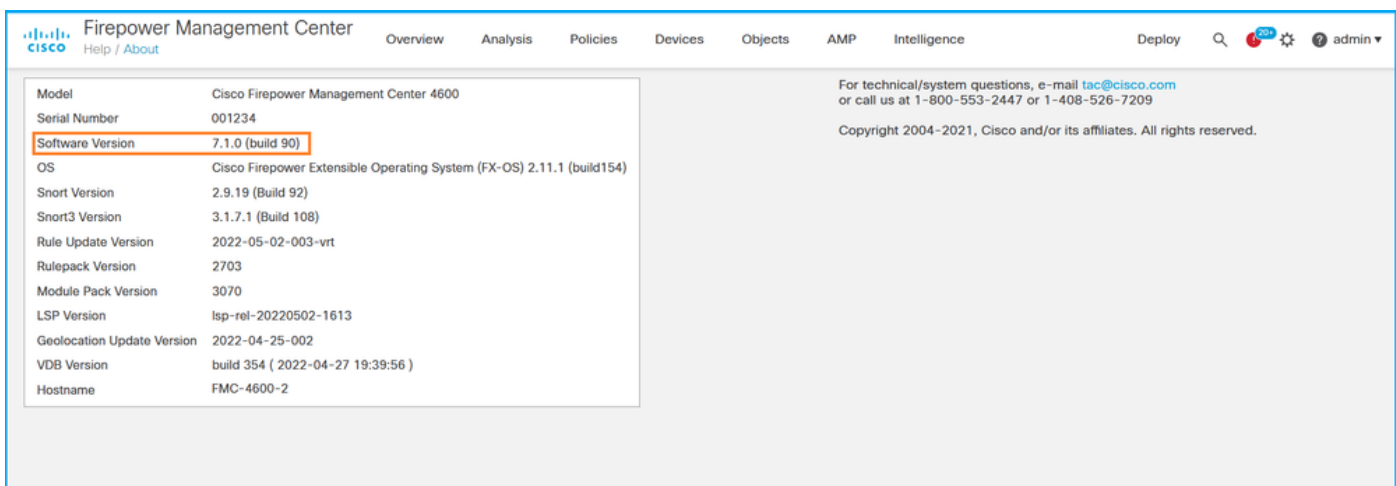
FMC CLI

按照以下步骤验证FMC CLI上的FMC软件版本。

1. 通过SSH或控制台连接访问FMC。标语显示软件版本：

```
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上运行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

按照以下步骤通过FMC REST-API请求验证FMC软件版本。使用REST-API客户端验证软件版本。在本例中，**curl**被使用：

1. 请求身份验证令牌：

```
# 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**查询中使用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
 }
}
```

> **注意**：命令字符串的"| python -m json.tool"部分用于格式化JSON样式的输出，是可选的。

FMC故障排除文件

按照以下步骤验证故障排除文件中的FMC软件版本：

1. 打开故障排除文件并导航至文件**夹<filename>.tar/results-<date>—xxxxxx/dir-archives/etc/sf/**
2. 打开文件ims.conf并找到键为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模块CLI

按照以下步骤验证FTD CLI或Firepower模块CLI上的FMC软件版本：

1. 通过SSH或控制台连接访问FTD。对于Firepower模块，请通过SSH或通过session sfr命令从ASA CLI访问**模块**。

2. 运行专家命令。

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

3.在Firepower模块上运行less /ngfw/var/sf/detection_engines/<UUID>/ngfw.rules 命令，或在
Firepower模块上运行less /var/sf/detection_engine/<UUID>/ngfw.rules 命令并检查行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模块故障排除文件

按照以下步骤验证FTD或Firepower模块故障排除文件中的FMC软件版本：

1. 如果文件是在FTD上生成的，请打开故障排除文件并导航至**文件夹<filename>-troubleshoot
.tar/results-<date>—xxxxx/file-contents/ngfw/sf/detection-engines/<UUID>/**。对于
Firepower模块，导航至文件夹**<filename>-troubleshoot .tar/results-<date>—xxxxxx/file-
contents/var/sf/detection-engines/<UUID>/**
2. 打开ngfw.**rules文件并**检查行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软件版本

可使用以下选项验证FDM软件版本：

- FDM UI
- FTD CLI
- FTD SNMP轮询

- FTD故障排除文件
- FDM REST API
- Firepower机箱管理器(FCM)用户界面
- FXOS CLI
- FXOS REST API
- FXOS机箱show-tech文件

FDM UI

要验证FDM UI上的软件版本，请在主页上选中"软件"：

FDM REST API

按照以下步骤通过FDM REST-API请求验证FDM软件版本。使用REST-API客户端验证软件版本。在本例中，使用curl:

1. 请求身份验证令牌：

```
# 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.eyJpYXQiOjE2NTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoiNDk3MmRjNjAtZDBmMi0xMW
VjLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2hUb2tlbkV4cG
lyZXNBdCI6MTY1MjI1MjM1NzQ1NywidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC
0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2
VybmFtZSI6ImFkbWluIn0.lJLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI",
"expires_in": 1800,
"refresh_expires_in": 2400,
"refresh_token":
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGU0NGIxYzQtZDI0Mi0xMW
VjLTk4ZWMtYTllOTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIzOTY1NjksImFjY2Vzc1Rva2VuRXhwaX
Jlc0F0IjoxNjUyMzk1OTY5MDcwLCJyZWZyZXNoQ291bnQiOi0xLCJ0b2tlblR5cGUiOiJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2
luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
```

```
"token_type": "Bearer"
}
```
2.在此查询中使用访问令牌值：

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoiNDk3MmRjNjAtZDBmMi0xMWV
jLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2hUb2tlbkV4cGl
yZXNBdCI6MTY1MjI1MjM1NzQ1Nywid G9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC0
xMWVjLTk4ZWMtZjk4ODExNjNjNjZlZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2V
ybmFtZSI6ImFkbWluIn0.1JLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI'
'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

按照部分中的步骤操作。

FTD SNMP

按照部分中的步骤操作。

FTD故障排除文件

按照部分中的步骤操作。

FCM用户界面

FCM在Firepower 4100和Firepower 9300系列上可用。按照部分中的步骤操作。

FXOS CLI

按照部分中的步骤操作。

FXOS REST-API

按照部分中的步骤操作。

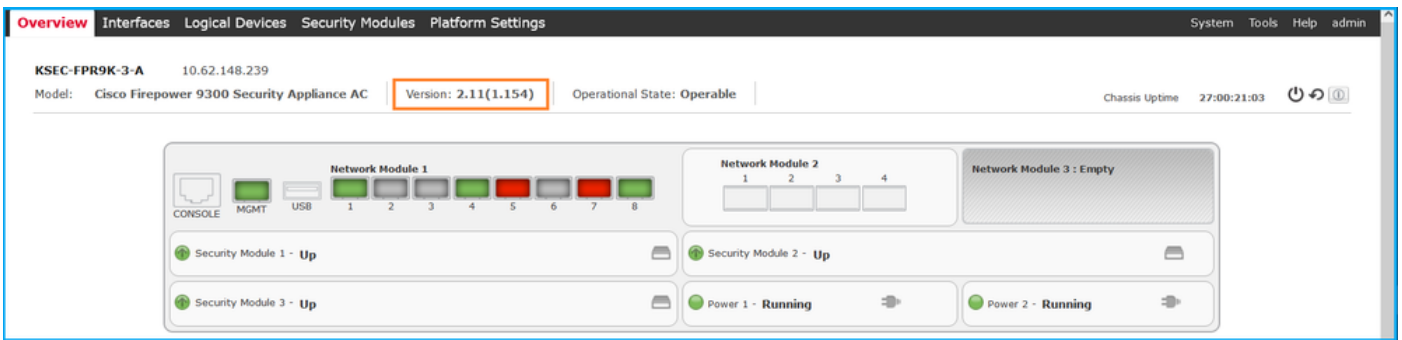## FXOS机箱show-tech文件

按照部分中的步骤操作。

FXOS软件版本

FXOS软件版本可使用以下选项进行验证：

- FCM UI（仅限Firepower 4100/9300）
- FXOS CLI
- FXOS REST API
- FXOS SNMP轮询
- FXOS机箱show-tech文件。

FCM用户界面

要验证FCM UI上的FXOS软件版本，请在主页上选中Version:

FXOS CLI

Firepower 4100/9300

按照以下步骤验证FXOS CLI上的FXOS软件版本：

1. 与机箱建立控制台或SSH连接。
2. 切换到范围系统并运行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
```

带FTD的Firepower 1000/2100/3100

按照以下步骤验证FXOS CLI上的FXOS软件版本：

1. 建立与机箱的控制台连接或与FTD的SSH连接。

如果与FTD的SSH连接，请在FTD CLISH上运行connect fxos命令：

```
> connect fxos
```

2.切换到范围系统并运行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)
```

采用ASA的Firepower 1000/3100，采用ASA的Firepower 2100在设备模式下

按照以下步骤验证FXOS CLI上的FXOS软件版本：

1. 建立与机箱的控制台连接或与ASA的telnet/SSH连接。

在与ASA建立telnet/SSH连接时，在ASA CLI上运行**connect fxos**命令。

```
asa# connect fxos
```

2. 切换到范围系统并运行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)
```

在平台模式下具有ASA的Firepower 2100

按照以下步骤验证FXOS CLI上的FXOS软件版本：

1. 建立与机箱的SSH或控制台连接，或与ASA的telnet/SSH连接。
在与ASA建立telnet/SSH连接时，在ASA CLI上运行**connect fxos**命令。

```
asa# connect fxos
```

2. 切换到范围系统并运行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系列支持FXOS REST-API。

Firepower 4100/9300

按照以下步骤通过FXOS REST-API请求验证FXOS软件版本。使用REST-API客户端验证软件版本。在本例中，使用curl:

1. 请求身份验证令牌：

```
# curl -k -X POST -H 'USERNAME: admin' -H 'PASSWORD: Cisco123' 'https://192.0.2.100/api/login'
{
   "refreshPeriod": "0",
   "token": "1206f6a3032e7bdbeac07cfdd9d5add5cdd948e4e5f4511535a959aed7e1e2f5"
}
```
2.在此查询中使用令牌：

```
# 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配置在平台模式和Firepower 4100/9300下的ASA的Firepower 2100上受支持。

Firepower 4100/9300

按照以下步骤通过SNMP验证FXOS软件版本：

1. 确保在FXOS上配置了SNMP。有关配置步骤，请参阅在Firepower NGFW设备上配置SNMP。
2. 轮询.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"
```
在平台模式下具有ASA的Firepower 2100

按照以下步骤通过SNMP验证FXOS软件版本：

1. 确保在FXOS上配置了SNMP。有关配置步骤，请参阅在Firepower NGFW设备上配置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机箱show-tech文件

Firepower 4100/9300

按照以下步骤验证FXOS机箱show-tech文件中的FXOS软件版本：

1. 对于FXOS版本2.7及更高版本，请在**<name>_BC1_all.tar/ FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar**中打开sam_techsupportinfo文件
对于早期版本，请在**FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar**中打开 sam_techsupportinfo文件。

2. 检查"show firmware monitor"**命令的**输出:

```
# 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**中打开文件tech_support_brief
2. 检查"show firmware detail"**命令的输**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软件版本

FTD软件版本可使用以下选项进行验证：

- FTD CLI
- FTD SNMP轮询
- FTD故障排除文件
- FMC UI
- FMC REST API
- FDM UI
- FDM REST API
- FCM用户界面
- FXOS CLI
- FXOS REST API
- FXOS机箱show-tech文件

FTD CLI

按照以下步骤验证FTD CLI上的FTD软件版本：

1. 根据平台和部署模式，使用以下选项访问FTD CLI:

- 直接SSH访问FTD — 所有平台
- 从FXOS控制台CLI(Firepower 1000/2100/3100)通过命令connect ftd**访问**
- 通过命令(Firepower 4100/9300)从FXOS CLI访问：
  connect module <x> [console|telnet],其中x是插槽ID，然后

  connect ftd [instance]，其中实例仅与多实例部署相关。

- 对于虚拟FTD、直接SSH访问FTD或从虚拟机监控程序或云UI进行控制台访问

2.在CLI上**运行**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

按照以下步骤通过SNMP验证FTD软件版本：

1. 确保已配置并启用SNMP。对于FDM管理的FTD，请参阅在Firepower FDM上配置SNMP并对其进行故障排除以了解配置步骤。有关FMC管理的FTD，请参阅在Firepower NGFW设备上配置SNMP以了解配置步骤。
2. 轮询OID SNMPv2-MIB::sysDescr.0或OID .1.3.6.1.2.1.1.0.:

```
# 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

按照以下步骤验证FMC UI上的FTD软件版本：

1. 选择**Devices > Device Management**:

2.检查"**版本**"列：

FMC REST API

按照以下步骤通过FMC REST-API验证FTD软件版本。使用REST-API客户端验证软件版本。在本例中，**curl**被使用：

1. 请求身份验证令牌：

```
# 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.确定包含设备的域。在大多数REST API查询中，域**参数**是必填项。在此**查询中使用X-auth-access-token**检索域列表：

```
# 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查询设备记录：

```
# 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和设备/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\"\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-Data1/1    : address is 0000.0100.0001, irq
0\n 5: Int: Internal-Data1/2    : address is 0000.0300.0001, irq 0\n 6: Int: Internal-Control1/1
: 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 UI

按照部分中的步骤操作。

FDM REST-API

按照部分中的步骤操作。

FTD故障排除文件

按照以下步骤验证FTD故障排除文件中的FTD软件版本:

1. 打开故障排除文件并导航至文件夹<filename>-troubleshoot .tar/results-
<date>—xxxxxx/command-outputs/

2. 打开文件usr-local-sf-bin-sfcli.pl show version.output，并找到带有Model的行：

```
# 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用户界面

对于Firepower 4100/9300上的FTD，请使用FCM并在"逻辑设备"选项卡中选中"版本"：

FXOS CLI

Firepower 4100/9300上的FTD

按照以下步骤验证FXOS CLI上的FTD软件版本：

1. 与机箱建立控制台或SSH连接。
2. 切换到scope ssa并运行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

按照以下步骤验证FXOS CLI上的FTD软件版本：

1. 建立到机箱的控制台连接或到FTD的SSH连接
如果与FTD的SSH连接，请在FTD CLISH上运行**connect fxos**命令：

```
> connect fxos
```

2.切换到范围**ssa**并运行**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	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

按照以下步骤通过FXOS REST-API验证FTD软件版本:

1.请求身份验证令牌：

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

2.在此查询中使用令牌，并确保指定安装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机箱show-tech文件

按照以下步骤验证FXOS机箱show-tech文件中的FTD软件版本：

Firepower 4100/9300上的FTD

1.对于FXOS 2.7及更高版本，请在**<name>_BC1_all.tar/**

FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar中打开sam_techsupportinfo文件

对于早期版本，请在FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar中打开sam_techsupportinfo文件。

2.在"show slot expand detail"下，检查每个插槽的部分：

```
# 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中打开文件tech_support_brief
2. 检查部分"scope ssa"和"show slot"：

```
# 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软件版本

可使用以下选项验证ASA软件版本：

- ASA CLI
- ASA SNMP轮询

- ASA show-tech文件
- FCM用户界面
- FXOS CLI
- FXOS REST API
- FXOS机箱show-tech文件

ASA CLI

按照以下步骤验证ASA CLI上的ASA软件版本：

1.根据平台和部署模式使用以下选项访问ASA CLI:

- 以设备模式直接telnet/SSH访问Firepower 1000/3100和Firepower 2100上的ASA
- 在平台模式下从Firepower 2100上的FXOS控制台CLI访问，并通过connect asa命令连**接到**ASA
- 通过命令(Firepower 4100/9300)从FXOS CLI访问：

连接模块<x> [console|telnet],其中x是插槽ID，然后连**接asa**

- 对于虚拟ASA，直接SSH访问ASA，或从虚拟机监控程序或云UI进行控制台访问
2.运行**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

按照以下步骤通过SNMP验证ASA软件版本：

1. 确保已配置并启用SNMP。
2. 使用SNMP客户端轮询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文件

使用Cisco自适应安全设备软**件版本字符串搜索**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用户界面

按照部分中的步骤操作。

FXOS CLI

按照部分中的步骤操作。

FXOS REST-API

按照部分中的步骤操作。

FXOS机箱show-tech文件

按照部分中的步骤操作。

Firepower模块软件版本

ASA上的Firepower模块是旧Sourcefire模块或SFR的新名称。

可使用以下选项验证其软件版本：

- FMC UI
- FMC REST-API

- Firepower模块CLI
- Firepower模块故障排除文件
- ASA CLI
- ASA show-tech文件

FMC UI

按照部分中的步骤操作。

FMC REST-API

按照部分中的步骤操作。

Firepower模块CLI

按照以下步骤验证模块CLI上的Firepower模块软件版本：

1.通过SSH或通过session sfr命令从ASA CLI连接到模块。

2.运行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模块故障排除文件

按照以下步骤验证模块故障排除文件中的Firepower模块软件版本：

1. 打开故障排除文件并导航至文件夹<filename>-troubleshoot .tar/results-<date>—xxxxxx/command-outputs/
2. 打开文件usr-local-sf-bin-sfcli.pl show version.output，并找到带有Model的行：

```
# 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上运行show module sfr details命令并检查软件版本：

```
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文件

使用show module sfr detail字符串搜索行：

```
------------------ 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
```

验证Snort、VDB和SRU版本

深度数据包检测引擎(Snort)版本

可使用以下选项验证Snort版本：

- FMC UI
- FMC REST-API
- FDM UI
- FDM REST API
- FTD或Firepower模块CLI
- FTD或Firepower模块故障排除文件

FMC UI

按照以下步骤验证FMC UI上的FTD Snort版本：

1. 选择Devices > Device Management:
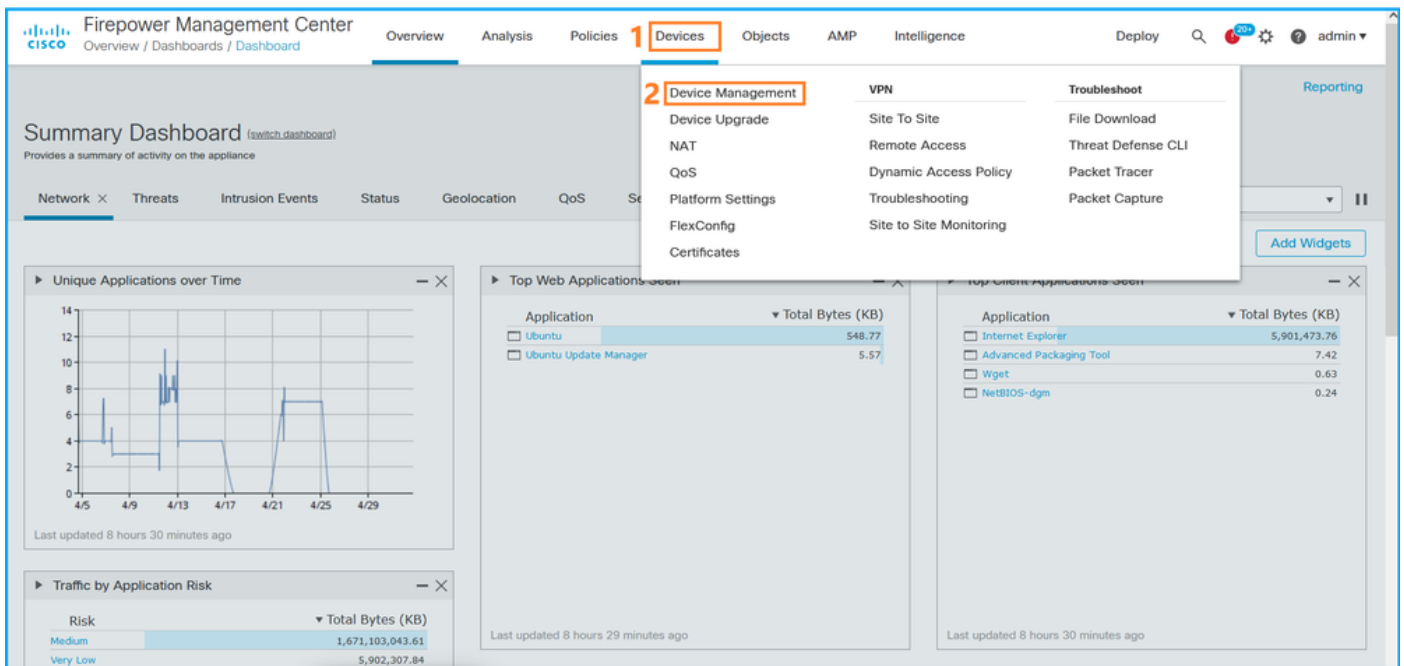
2.检查Snort标签：
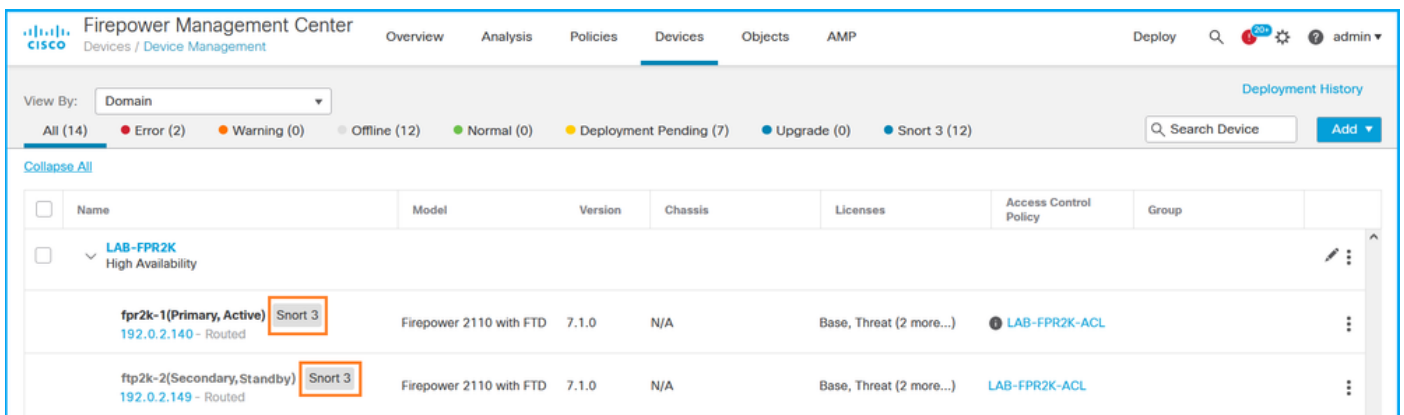
FMC REST-API

按照以下步骤通过FMC REST-API验证FTD Snort版本。使用REST-API客户端验证软件版本。在本例中，使用curl:

1. 请求身份验证令牌：

```
# 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.确定包含设备的域。在大多数REST API查询中，域参数是必填项。在此查询中使用X-auth-access-token检索域列表：

```
# 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查询设备记录:

```
# 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.在此请求中使用域UUID和设备/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

按照以下步骤验证FDM UI上的FTD Snort版本：

1. 转至"**更新**"页面:

2.检查Snort检测引擎:

FDM REST API

按照以下步骤通过FDM REST-API请求验证Snort版本。使用REST-API客户端验证软件版本。在本例中，使用curl:

1. 请求身份验证令牌：

```
# 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.eyJpYXQiOjE2NTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoiNDk3MmRjNjAtZDBmMi0xMW
VjLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnNlc2hUb2tlbkV4cG
lyZXNBdCI6MTY1MjI1MjM1NzQ1Nywid29rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC
0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2
VybmFtZSI6ImFkbWluIn0.lJLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI",
```

```
"expires_in": 1800,
"refresh_expires_in": 2400,
"refresh_token":
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGU0NGIxYzQtZDI0Mi0xMW
VjLTk4ZWMtYTllOTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIzOTY1NjksImFjY2Vzc1Rva2VuRXhwaX
Jlc0F0IjoxNjUyMzk1OTY5MDcwLCJyZWZyZXNoQ291bnQiOi0xLCJ0b2tlblR5cGUiOiJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2
luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
"token_type": "Bearer"
}
```

2.在此查询中使用access_token值：

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTI0NDU3ODksInN1YiI6ImFkbWluIiwianRpIjoiM2U1Njg0YjYtZDJiYS0xMWV
jLTk4ZWMtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LCJleHAiOjE2NTI0NDc1ODksInJlZnJlc2hUb2tlbkV4cGl
yZXNBdCI6MTY1MjQ0ODE4OTMyNSwidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC0
xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2V
ybmFtZSI6ImFkbWluIn0.kXtsUu3_WWtOWu9w0mSDfJjwcyiVCa5dgyzNjCGnlF4'
'https://10.62.148.181/api/fdm/v6/operational/systeminfo/default'  | grep -i snort

"snortVersion" : { "snortVersion" : "3.1.7.1-108",
"snortPackage" : "/ngfw/var/sf/snort-3.1.7.1-108/snort-75-3.1.7.1-108-daq14.tar.bz2",
"type" : "snortversion
```

FTD或Firepower CLI

在FTD CLI上，运行**show snort3 status**命令:

```
> show snort3 status
Currently running Snort 3
```
Firepower模块仅支持Snort 2。

FTD或Firepower模块故障排除文件

按照以下步骤验证FTD故障排除文件中的Snort版本：

1. 打开故障排除文件并导航至文**件夹<filename>-troubleshoot .tar/results-
   <date>—xxxxxx/command-outputs**
2. 打开文**件usr-local-sf-bin-sfcli.pl show snort3.output:**

```
# pwd
/var/tmp/results-05-06-2022--163203/command-outputs
# cat "usr-local-sf-bin-sfcli.pl show snort3.output"
Output of /ngfw/usr/local/sf/bin/sfcli.pl show snort3:
Currently running Snort 3
```
Firepower模块仅支持Snort 2。

漏洞数据库(VDB)版本

可使用以下选项验证VDB版本：

- FMC UI
- FMC REST-API

- FMC故障排除文件
- FDM UI
- FDM REST API
- FTD CLI
- FTD或Firepower模块故障排除文件

FMC UI

按照以下步骤验证FMC UI上的VDB版本：

1. 选择**帮助>关于**：

2.检查**VDB版本**:

FMC CLI

按照以下步骤验证FMC CLI上的VDB版本：

1. 通过SSH或控制台连接访问FMC。
2. 运行**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

按照以下步骤通过FMC REST-API验证VDB版本。使用REST-API客户端验证软件版本。在本例中，使用curl:

1. 请求身份验证令牌：

```
# 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.确定包含设备的域。在大多数REST API查询中，域参数是必填项。在此查询中使用X-auth-access-token检索域列表：

```
# 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故障排除文件

按照以下步骤验证FMC故障排除文件中的VDB版本：

1. 打开故障排除文件并导航至文件夹<filename>-troubleshoot .tar/results-<date>—xxxxx/dir-archives/etc/sf/.versiondb
2. 打开文件vdb.conf并找到键为CURRENT_BUILD的行:

```
# 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 UI

在主页上检查VDB:

FDM REST API

按照以下步骤通过FDM REST-API请求验证VDB版本。使用REST-API客户端验证软件版本。在本例中，使用curl:

1. 请求身份验证令牌：

```
# 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.eyJpYXQiOjE2NTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoiNDk3MmRjNjAtZDBmMi0xMW
VjLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2hUb2tlbnV4cG
lyZXNBdCI6MTY1MjI1MjM1NzQ1NywidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC
0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2
VybmFtZSI6ImFkbWluIn0.lJLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI",
"expires_in": 1800,
"refresh_expires_in": 2400,
"refresh_token":
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGU0NGIxYzQtZDI0Mi0xMW
VjLTk4ZWMtYTllOTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIzOTY1Njk5ImZjY2Vzc1Rva2VuRXhwaX
Jlc0F0IjoxNjUyMzk1OTY5MDcwLCJyZWZyZXNoQ291bnQiOi0xLCJ0b2tlblR5cGUiOiJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2
luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
"token_type": "Bearer"
}
```

2.在此查询中使用access_token值：

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTI0NDU3ODksInN1YiI6ImFkbWluIiwianRpIjoiM2U1Njg0YjYtZDJiYS0xMWV
jLTk4ZWMtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LCJleHAiOjE2NTI0NDc1ODksInJlZnJlc2hUb2tlbkV4cGl
yZXNBdCI6MTY1MjQ0ODE4OTMyNSwidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJJVdWlkIjoiYTU3ZGVmMjgtY2M3MC0
xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2V
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模块CLI

按照以下步骤验证FTD CLI或Firepower模块(SFR)CLI上的VDB版本：

1. 通过SSH或控制台连接访问FTD。对于Firepower模块，请通过SSH或通过session sfr命令从ASA CLI访问模块。
2. 在CLI上运行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模块故障排除文件

按照以下步骤验证FTD或Firepower模块故障排除文件中的VDB版本：

1. 打开故障排除文件并导航至文件夹<filename>-troubleshoot.tar/results-<date>—xxxxxx/command-outputs/
2. 打开文件usr-local-sf-bin-sfcli.pl show version.output，并找到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
-----------------------------------------------------
```

入侵规则更新版本

入侵规则更新提供新的和更新的入侵规则和预处理器规则、已安装规则的已修改状态以及已修改的默认入侵策略设置。

安全规则更新(SRU)适用于Snort版本2，轻量安全包(LSP)更新适用于Snort版本3。

可使用以下选项验证SRU/LSP软件版本：

- FMC UI
- FMC REST-API
- FMC故障排除文件
- FDM UI
- FDM REST API
- FTD或Firepower模块CLI
- FTD或Firepower模块故障排除文件

FMC UI

按照以下步骤验证FMC UI上的SRU/LSP版本：

1. 选择**帮助>关于**：
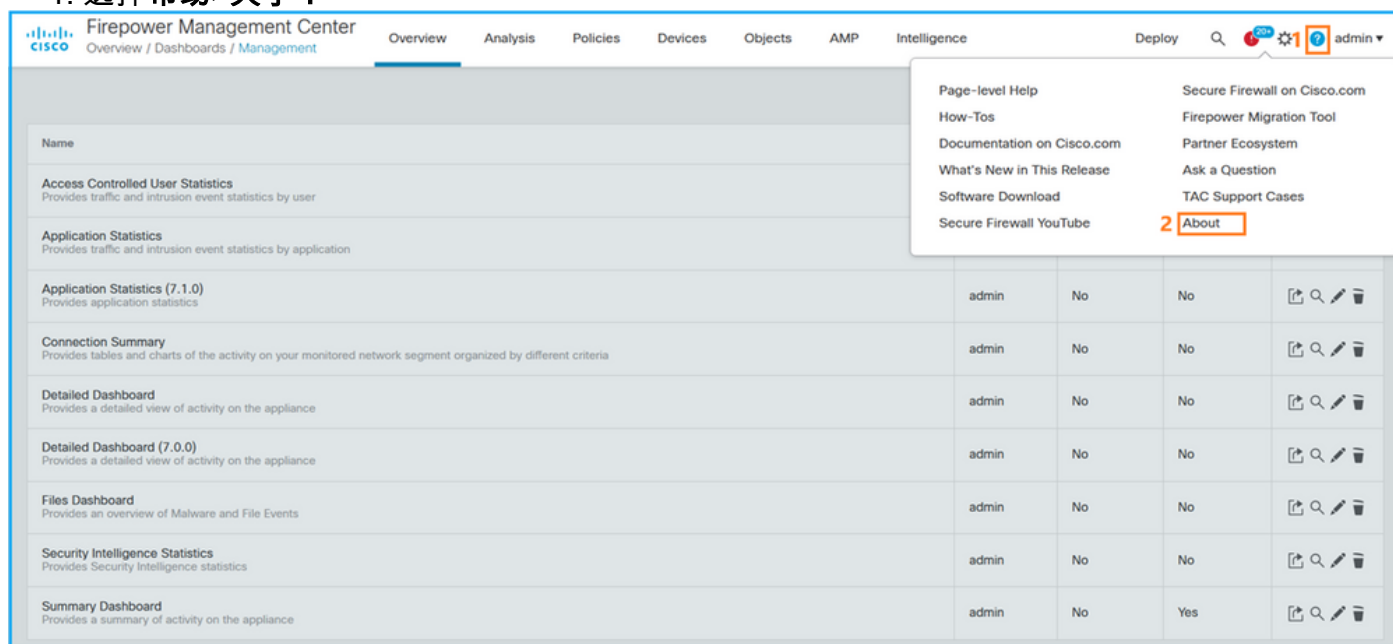
2.检查**规则更新版**本**和LSP版本**:
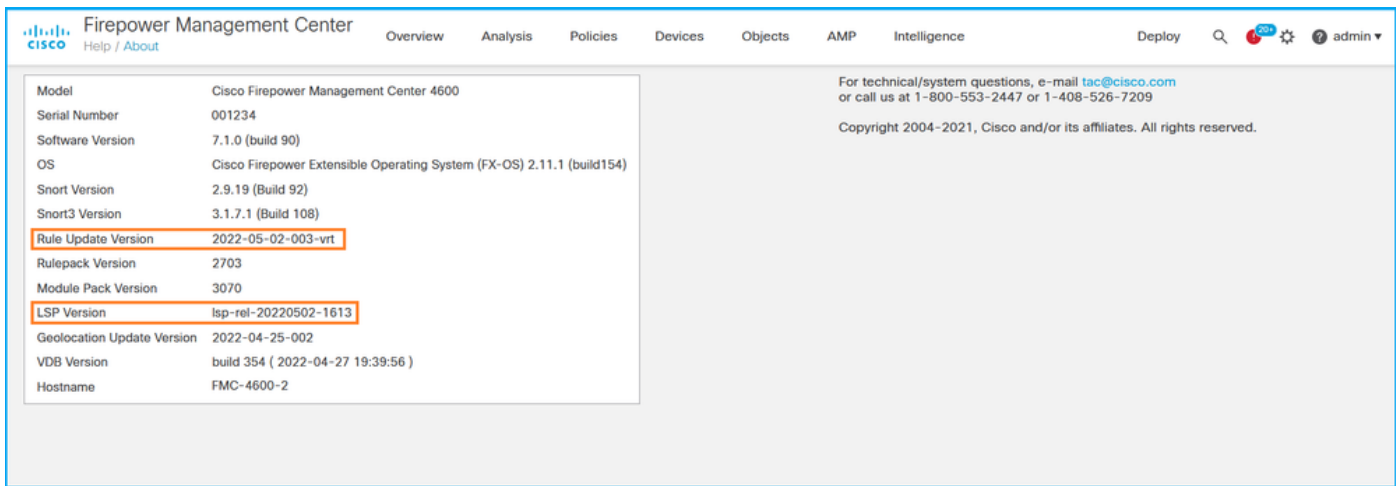
FMC CLI

按照以下步骤验证FMC CLI上的SRU/LSP版本：

1. 通过SSH或控制台连接访问FMC。
2. 在CLI上**运行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

按照以下步骤通过REST-API请求验证软件版本。使用REST-API客户端验证软件版本。在本例中，**curl**被使用：

1. 请求身份验证令牌：

```
# 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**查询中使用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故障排除文件

按照以下步骤验证FMC故障排除文件中的SRU版本：

1. 打开故障排除文件并转到文件夹<filename>.tar/results-<date>—xxxxxx/dir-archives/etc/sf/
2. 打开文件sru_versions.conf，并找到键为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
```

按照以下步骤验证FMC故障排除文件中的LSP版本：

1. 打开故障排除文件并转到文件夹<filename>.tar/results-<date>—xxxxxx/command-outputs
2. 打开文件，查找var-sf-lsp -maxdepth 2 -ls.output，并使用/var/sf/lsp/active-lsp检查该行

```
# 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
```

```
 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
```

FDM UI

在主页上，选中Intrusion Rule Update:

FDM REST API

按照以下步骤通过FDM REST-API请求验证VDB版本。使用REST-API客户端验证软件版本。在本例中，**curl**被使用：

  1. 请求身份验证令牌：

```
# 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.eyJpYXQiOjE2NTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoiNDk3MmRjNjAtZDBmMi0xMW
VjLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2hUb2tlbkV4cG
lyZXNBdCI6MTY1MjI1MjM1NzQ1Nywid2hpdGVsaXN0IjoiSldUX0ZGY2Vzcy1sYVJlZnJlc2gtLWRYVXRNTEdTbWV2ZVdlbk
0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwid2hlbGlzdCI6IjANLW5lc3NJHDm1lbkV4cGlyZXNBdCI6MTY1MjI1MjM1NzQ1N
ywid2hpdGVsaXN0IjoiSldUX0ZGY2Vzcy1sYVJlZnJlc2gtLWRYVXRNTEdTbWV2ZVdlbk0xMWVjLTk4ZWMtZjk4ODExNjNjZ
WIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2
VybmFtZSI6ImFkbWluIn0.lJLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI",
"expires_in": 1800,
"refresh_expires_in": 2400,
"refresh_token":
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGU0NGIxYzQtZDI0Mi0xMW
VjLTk4ZWMtYTllOTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIzOTY1NjksImFjY2Vzc1Rva2VuRXhwaX
Jlc0F0IjoxNjUyMzk1OTY5MDcwLCJyZWZyZXNoQ291bnQiOi0xLCJ0b2tlblR5cGUiOiJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2
luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
"token_type": "Bearer"
}
```
2.在此查询中使用access_token值：

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTI0NDU3ODksInN1YiI6ImFkbWluIiwianRpIjoiM2U1Njg0YjYtZDBiYS0xMWV
jLTk4ZWMtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LCJleHAiOjE2NTI0NDc1ODksInJlZnJlc2hUb2tlbkV4cGl
yZXNBdCI6MTY1MjQ0ODE4OTMyNSwidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC0
xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2V
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模块CLI

按照以下步骤验证FTD CLI或Firepower模块CLI上的SRU/LSP版本：

1. 通过SSH或控制台连接访问FTD。对于Firepower模块，请通过SSH或通过session sfr命令从ASA CLI访问**模块**。
2. 在CLI上**运行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
--------------------------------------------------------
```

> **注意**：如果使用Snort 2，则**show version**命令会显示SRU更新版本。图中显示了Snort 3 LSP版本。

FTD或Firepower模块故障排除文件

按照以下步骤验证FTD或Firepower模块故障排除文件中的SRU/LSP版本：

1. 打开故障排除文件并转到文**件夹<filename>-troubleshoot.tar/results-<date>—xxxxxx/command-outputs/**

2. 打开文件usr-local-sf-bin-sfcli.pl show version.output，并找到带有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
-----------------------------------------------------
```

已知问题

思科漏洞ID [CSCwb34098](#) 增强：在"show managers"命令输出中显示FMC版本

思科漏洞ID [CSCve13470](#)　增强：在FirePOWER 6.x上启用软件相关OID

思科漏洞ID [CSCwb85969](#) 增强：在故障排除文件中包含"show version" FMC CLISH命令的输出

思科漏洞ID [CSCvu15709](#)　增强：支持SNMP OID以轮询Firepower平台上的SRU/VDB/GEO位置版本

相关信息

- [安全防火墙管理中心REST API快速入门指南，版本7.1](#)
- [在Firepower NGFW设备上配置SNMP](#)
- [思科Firepower威胁防御REST API指南](#)
- [思科FXOS REST API参考](#)

- [思科ASA兼容性](#)
- [Firepower 1000/2100和安全防火墙3100 ASA和FXOS捆绑包版本](#)
- [捆绑组件](#)
- [Firepower文件生成过程故障排除](#)