Controleer de softwareversies

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Controleer de softwareversies **FMC-softwareversie FMC UI FMC CLI FMC REST-API** FMC-bestand voor probleemoplossing FTD of FirePOWER Module CLI FTD of FirePOWER Module-bestand voor probleemoplossing **FDM-softwareversie FDM UI FDM REST API FTD CLI FTD SNMP** FTD Troubleshot-bestand **FXOS-softwareversie** FCM UI **FXOS CLI FXOS REST-API FXOS SNMP FXOS-chassis testbestand FTD Software versie FTD CLI FTD SNMP FMC UI FMC REST API** FDM UI **FDM REST-API** FTD Problemen oplossen FCM UI **FXOS CLI FXOS REST-API FXOS-chassis testbestand ASA-softwareversie** ASA CLI ASA SNMP ASA show-tech-bestand

FCM UI **FXOS CLI FXOS REST-API FXOS-chassis testbestand** Software voor Firepower Module FMC UI **FMC REST-API Firepower Module CLI** Firepower Module-bestand voor probleemoplossing ASA CLI ASA show-tech-bestand Controleer de versies Snort, VDB en SRU Diepgaande Packet Inspection Engine (snort) versie FMC UI **FMC REST-API** FDM UI FDM REST API FTD of Firepower CLI FTD of FirePOWER Module-bestand voor probleemoplossing VDB-versie (Vulnerability Database) FMC UI FMC CLI **FMC REST-API** FMC-bestand voor probleemoplossing FDM UI **FDM REST API** FTD of FirePOWER Module CLI FTD of FirePOWER Module-bestand voor probleemoplossing Inbraakregel Update versies FMC UI FMC CLI **FMC REST-API** FMC-bestand voor probleemoplossing FDM UI **FDM REST API** FTD of FirePOWER Module CLI FTD of FirePOWER Module-bestand voor probleemoplossing Bekende problemen Gerelateerde informatie

Inleiding

In dit document wordt de verificatie van FirePOWER-softwareversies beschreven.

Voorwaarden

Vereisten

Basisproductkennis, REST-API, SNMP.

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower 11xx
- Firepower 21xx
- Firepower 31xx
- Firepower 41xx
- Firepower Management Center (FMC) versie 7.1.x
- Firepower eXtenable Operating System (FXOS) 2.11.1.x
- Firepower Apparaatbeheer (FDM) 7.1.x
- Firepower Threat Defense 7.1.x
- ASA 9.17.x

Controleer de softwareversies

FMC-softwareversie

De FMC-softwareversie kan met behulp van deze opties worden geverifieerd:

- FMC UI
- FMC CLI
- REST API-verzoek
- FMC-bestand voor probleemoplossing
- FTD of Firepower module CLI
- FTD of FirePOWER Module probleemoplossingsbestand

FMC UI

Volg deze stappen om de FMC-softwareversie op FMC UI te controleren:

1. Help kiezen > Over:

Firepower Management Center Overview / Dashboards / Management	Overview	Analysis	Policies	Devices	Objects	AMP	Intellig	ence		Deploy	۹ (🚰 🛟 👩 admin 🔻
Name Access Controlled User Statistics Provides traffic and intrusion event statistics by user Application Statistics Provides traffic and intrusion event statistics by application								Page-level Help How-Tos Documentation on What's New in Thi: Software Downloa Secure Firewall Yo	Cisco.com s Release d uTube	s F 7 2 7	Secure Fire Firepower M Partner Eco Ask a Ques FAC Suppo About	wall on Cisco.com Migration Tool system tion rt Cases
Application Statistics (7.1.0) Provides application statistics								admin	No	N	0	
Connection Summary Provides tables and charts of the activity on your monitored ne	etwork segment o	ganized by differ	ent criteria					admin	No	N	0	10 Q / 1
Detailed Dashboard Provides a detailed view of activity on the appliance								admin	No	N	0	C 9/1
Detailed Dashboard (7.0.0) Provides a detailed view of activity on the appliance								admin	No	N	0	C 9 / 7
Files Dashboard Provides an overview of Malware and File Events								admin	No	N	0	C 9/1
Security Intelligence Statistics Provides Security Intelligence statistics								admin	No	N	0	C < / 7
Summary Dashboard Provides a summary of activity on the appliance								admin	No	Y	es	C < / 1

2. Controleer softwareversie:

Firepower Management Center Overview Analysis Policies	Devices Objects AMP Intelligence Deploy Q 崎 🌣 🔞 admin 🔻
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) Snort Version 3.1.7.1 (Build 108) Rule Update Version 2022-05-02-003-vrt Rulepack Version 2703 Module Pack Version 3070 LSP Version Isp-rel-20220502-1613 Geolocation Update Version 2022-04-25-002 VOB Version build 354 (2022-04-27 19:39:56) Hostname FMC-4600-2	For technical/system questions, e-mail tac@cisco.com or call us at 1-800-553-2447 or 1-408-526-7209 Copyright 2004-2021, Cisco and/or its affiliates. All rights reserved.

FMC CLI

Volg deze stappen om de FMC-softwareversie op de FMC CLI te controleren.

1. Toegang tot FMC via SSH of console-verbinding. Op de banner wordt de softwareversie weergegeven:

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

2. Start de opdracht Versie-signaal op CLI:

> show version		
[FMC-4600-2.ci	s	o.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

Volg deze stappen om de FMC-softwareversie via een REST-API-verzoek van het FMC te controleren. Gebruik een REST-API client om de softwareversie te controleren. In dit voorbeeld wordt **curl** gebruikt:

1. Echtheidstoken aanvragen:

```
# 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</pre>
```

2. Gebruik het X-auth-access-token in deze query:

```
# 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
 }
```

Opmerking: Het gedeelte "| **python -m json.tool**" van de opdrachtstring wordt gebruikt voor het formatteren van uitvoer in JSON-stijl en is optioneel.

FMC-bestand voor probleemoplossing

Volg deze stappen om de FMC-softwareversie in het bestand van de probleemoplossing te controleren:

- 1. Opent het bestand voor probleemoplossing en navigeer naar de map

 <br/
- 2. Open het bestand ims.conf en vind de regels met de toetsen SWVERSIE en SWBUILD:

```
# 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 of FirePOWER Module CLI

Volg deze stappen om de FMC-softwareversie op de FTD CLI of de Firepower module CLI te controleren:

- 1. Toegang tot FTD via SSH of console verbinding. In het geval van de Firepower module, heb toegang tot de module via SSH, of van de ASA CLI via de **sessie sfr** opdracht.
- 2. Start de opdracht van de expert.

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

3. Start de opdracht Minder /ngfw/var/sf/detectie_engine/<UID>/ngfw.rules voor FTD of minder /var/sf/detectie_engine/<UID>/ngfw.rules voor de FirePOWER-module en controleer de rij DC-versie:

FTD of FirePOWER Module-bestand voor probleemoplossing

Volg deze stappen om de FMC-softwareversie in het FTD of het bestand voor probleemoplossing in de FirePOWER-module te controleren:

- 2. Open het bestand ngfw.regels en controleer de rij DC versie:

```
# 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-softwareversie

De FDM-softwareversie kan met het gebruik van deze opties worden geverifieerd:

- FDM UI
- FTD CLI
- FTD SNMP-stemming
- FTD Problemen oplossen
- FDM REST API
- Firepower Chassis Manager (FCM) UI
- FXOS CLI
- FXOS REST API
- FXOS chassis tovertech-bestand

FDM UI

U kunt de softwareversie op FDM UI-controle van software op de hoofdpagina controleren:

CISCO. Firepower Device Manager	Monitoring Policies Objects	Device: KSEC-FPR2100	admin · · · · · · · · · · · · · · · · · · ·
Model Cisco Firepower 2120 1	hreat Defense Software VDB Intrusion Rule U 7.1.0-90 346.0 20211110-134	Ipdate Cloud Services High Availa 8 Not Registered Register Not Config 	ability CONFIGURE
C Inside Network	1/2 Cisco Firepower 2120 Threat Defense © MGMT 1/1 1/3 1/5 1/7 1/9 1/1 © © © © © © © © © CONSOLE 1/2 1/4 1/6 1/8 1/10 1/1: 1/1	1 1/13 1/14 1/15 1/16 2 SFP	teway
Interfaces Connected Enabled 3 of 17 View All Interfaces	Routing There are no static routes yet View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server / Relay DDNS Service DNS Server

FDM REST API

Volg deze stappen om de FDM-softwareversie te controleren via een FDM REST-API-verzoek. Gebruik een REST-API client om de softwareversie te controleren. In dit voorbeeld wordt de curl gebruikt:

1. Echtheidstoken aanvragen:

```
# 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
```

```
0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXN1c1JvbGUiOiJST0xFX0FETU10Iiwib3JpZ21uIjoicGFzc3dvcmQiLCJ1c2
VybmFtZSI6ImFkbWluIn0.1JLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI",
```

```
"expires_in": 1800,
"refresh_expires_in": 2400,
"refresh_token":
"eyJhbGci0iJIUzI1NiJ9.eyJpYXQi0jE2NTIzOTQxNjksInN1Yi16ImFkbWluIiwianRpIjoiMGU0NGIxYzQtZDI0Mi0xMW
VjLTk4ZWMtYTllOTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAi0jE2NTIzOTY1NjksImFjY2VzclRva2VuRXhwaX
Jlc0F0IjoxNjUyMzk10TY5MDcwLCJyZWZyZXNoQ291bnQi0i0xLCJ0b2tlblR5cGUi0iJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk40DExNjNjZWIwIiwidXNlclJvbGUi0iJST0xFX0FETUl0Iiwib3JpZ2
luIjoicGFzc3dvcmQiLCJlc2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
"token_type": "Bearer"
}
2. Gebruik de waarde van het toegangstoken in deze zoekopdracht:
```

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoiNDk3MmRjNjAtZDBmMi0xMWV
jLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2hUb2tlbkV4cGl
yZXNBdCI6MTY1MjI1MjM1NzQ1NywidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC0
xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2V
ybmFtZSI6ImFkbWluIn0.lJLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI'
```

FTD CLI

Volg de stappen in het gedeelte.

FTD SNMP

Volg de stappen in het gedeelte.

FTD Troubleshot-bestand

Volg de stappen in het gedeelte.

FCM UI

FCM is beschikbaar op Firepower 4100 en Firepower 9300 Series. Volg de stappen in het gedeelte.

FXOS CLI

Volg de stappen in het gedeelte.

FXOS REST-API

Volg de stappen in het gedeelte.

FXOS-chassis testbestand

Volg de stappen in het gedeelte.

FXOS-softwareversie

De FXOS-softwareversie kan met het gebruik van deze opties worden geverifieerd:

- FCM UI (alleen Firepower 4100/9300)
- FXOS CLI
- FXOS REST API
- FXOS SNMP-stemming
- FXOS chassis show-tech bestand.

FCM UI

U kunt de FXOS-softwareversie controleren met behulp van de FCM UI-**selectietoetsing** op de hoofdpagina:

Overview Interface	s Logical Devices Security Modules Platform Settings	System	Tools	Help	admin
KSEC-FPR9K-3-A Model: Cisco Firepo	10.62.148.239 Operational State: Operable Chassis Uptime	27:00:21	:03	ው ቃ	0
	Network Module 1 Network Module 2 Network Module 3 : Empty CONSOLE 1 2 3 4 5 6 7 8 Network Module 3 : Empty Network Module 3 : Empty				
	🗑 Security Module 1 - Up				
	🗑 Security Module 3 - Up 🖨 Power 1 - Running 🍽 🖗 Power 2 - Running 🍽				

FXOS CLI

4100/9300

Volg deze stappen om de FXOS-softwareversie op FXOS CLI te controleren:

- 1. Maak een console of SSH-verbinding met het chassis.
- 2. Switch naar toepassingssysteem en voer de opdracht monitor-weergave uit:

```
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
Firepower 1000/2100/3100 met FTD
```

Volg deze stappen om de FXOS-softwareversie op FXOS CLI te controleren:

1. Maak een console-verbinding met het chassis of de SSH-verbinding met de FTD. Als er een SSH-verbinding naar de FTD is gemaakt, voert u de opdracht **Connect fxos** op FTD CLISH uit:

> connect fxos

2. Switch naar het scope-systeem en voer het opdracht INTELLICHTINGENDETAFELS uit:

```
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)
```

Firepower 1000/3100 met ASA, FirePOWER 2100 met ASA in wasmodus

Volg deze stappen om de FXOS-softwareversie op FXOS CLI te controleren:

Maak een console-verbinding met het chassis of telnet/SSH verbinding met ASA.
 Als het om een telnet-/SSH-verbinding met ASA gaat, voert u de connect fxo-opdracht op ASA CLI uit.

asa# connect fxos

2. Switch naar het toepassingssysteem en voer de opdracht Sourcedetails uit:

```
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)
```

Firepower 2100 met ASA in platform modus

Volg deze stappen om de FXOS-softwareversie op FXOS CLI te controleren:

1. SSH- of console-verbinding maken met de chassis- of telnet-/SSH-verbinding met ASA. Als het om een telnet-/SSH-verbinding met ASA gaat, voert u de **connect fxo-**opdracht op ASA CLI uit.

```
asa# connect fxos
2. Switch naar het toepassingssysteem en voer de opdracht Sourcedetails uit:
```

```
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

FXOS REST-API wordt ondersteund op Firepower 4100/9300 Series.

4100/9300

Volg deze stappen om de FXOS-softwareversie via een FXOS REST-API-verzoek te controleren. Gebruik een REST-API client om de softwareversie te controleren. In dit voorbeeld wordt de curl gebruikt:

1. Echtheidstoken aanvragen:

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

2. Gebruik het token in deze zoekopdracht:

FXOS SNMP

SNMP-configuratie op FXOS wordt ondersteund op Firepower 2100 met ASA in platform modus en Firepower 4100/9300.

4100/9300

Volg deze stappen om de FXOS-softwareversie via SNMP te controleren:

- Zorg ervoor dat SNMP is ingesteld op FXOS. Raadpleeg <u>SNMP</u> configureren<u>op FirePOWER</u> <u>NGFW-applicaties</u> voor configuratiestappen.
- 2. Poll .1.3.6.1.4.1.9.9.826.1.30.47.1.6 of CISCO-FIREPOWER-FIRMWARE-MIB: cFirmwareRunningPackageVersie:

```
# 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)"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.30781 = 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"
```

Firepower 2100 met ASA in platform modus

Volg deze stappen om de FXOS-softwareversie via SNMP te controleren:

- Zorg ervoor dat SNMP is ingesteld op FXOS. Raadpleeg <u>SNMP</u> configureren <u>op FirePOWER</u> <u>NGFW-applicaties</u> voor configuratiestappen.
- 2. Poll .1.3.6.1.2.1.1.1.0 of 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-chassis testbestand

4100/9300

Volg deze stappen om de FXOS-softwareversie in het FXOS-chassis-bestand te controleren:

 Voor FXOS versies 2.7 en later, open bestand sam_techsupportinfo in <name>_BC1_all.tar/FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar

Voor eerdere versies open bestand sam_techsupportinfo in FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar.

2. Controleer de uitvoer van de opdracht firmware monitor":

```
f bwg
/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. Bestand tech_support_brief in <name>_FPRM.tar.gz/<name>_FPRM.tar
- 2. Controleer de uitvoer van de opdracht 'Show firmware detail':

```
# 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 Software versie

De FTD-softwareversie kan met het gebruik van deze opties worden geverifieerd:

- FTD CLI
- FTD SNMP-stemming
- FTD Problemen oplossen
- FMC UI
- FMC REST API
- FDM UI
- FDM REST API
- FCM UI
- FXOS CLI
- FXOS REST API
- FXOS-chassis testbestand

FTD CLI

Volg deze stappen om de FTD-softwareversie op FTD CLI te controleren:

1. Gebruik deze opties om toegang te krijgen tot de FTD CLI in overeenstemming met het platform en de implementatiemodus:

- Directe SSH-toegang tot FTD alle platforms
- Toegang van de FXOS-console CLI (Firepower 1000/2100/3100) via commando verbinden met ftd
- Toegang van de FXOS CLI via opdrachten (Firepower 4100/9300): Sluit module <x> [console|telnet] aan, waar x de sleuf-ID is, en dan

verbinding met ftd [instantie], waarbij de instantie alleen relevant is voor meerkanaalsimplementatie.

- Voor virtuele FTD's, directe SSH-toegang tot FTD of console-toegang van de hypersupervisor of cloud UI
- 2. Start de opdracht Versie-signaal op CLI:

<pre>> show version</pre>	
[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

Volg deze stappen om de FTD-softwareversie via SNMP te controleren:

- Zorg ervoor dat SNMP is ingesteld en ingeschakeld. Raadpleeg voor FDM-Managed FTD <u>SNMP configureren en probleemoplossing in Firepower FDM</u> voor configuratiestappen. Raadpleeg voor FMC-beheerde FTD <u>SNMP configureren op FirePOWER NGFW-applicaties</u> voor configuratiestappen.
- 2. Poll OID SNMPv2-MIB::sysDescr.0 of 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

Volg deze stappen om de FTD-softwareversie op FMC UI te controleren:

1. Apparaten kiezen > Apparaatbeheer:



2. Controleer de kolom Versie:

altali cisco	. Fire	epower Management Center o	verview Analysis	Policies	Devices Object	s A	AMP		Deploy	Q (⁰⁰ ¢	🕜 admin	a v
View B All (iy: [(14)	Oomain	(12) • Normal (0)	Deployme	nt Pending (7) 🔹 U	pgrade	(0) • Snort 3 (12)		Q Sea	D rch Devic	eployme :e	nt History Add	7
Collaps	e All												
	Name		Model	Version	Chassis		Licenses	Access Control Policy	Group				
	~	LAB-FPR2K High Availability										1:	^
		fpr2k-1(Primary, Active) Snort 3 192.0.2.140 - Routed	Firepower 2110 with FTD	7.1.0	N/A	Ba	ase, 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	Ba	ase, Threat (2 more)	LAB-FPR2K-ACL				:	

FMC REST API

Volg deze stappen om de FTD-softwareversie via FMC REST-API te controleren. Gebruik een REST-API client om de softwareversie te controleren. In dit voorbeeld wordt **curl** gebruikt:

1. Echtheidstoken aanvragen:

```
# 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</pre>
```

2. Identificeer het domein dat het apparaat bevat. Bij de meeste REST API-vragen is de **domeinparameter** verplicht. Gebruik het **X-auth-access-token in** deze query om de lijst met domeinen op te halen:

```
# 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-00000000001"
    },
    {
        "name": "Global/domain2",
        "type": "Domain",
        "uuid": "341a8f03-f831-c364-b751-00000000001"
    }
1.
"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. Gebruik het domein UID om vragen te stellen voor de apparaten:

}

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
0000000001/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-
0000000001/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-
0000000001/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-
0000000001/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-
0000000001/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-
0000000001/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-
0000000001/devices/devicerecords/0b1a9c94-8ba8-11ec-b2fd-93263934908d"
            },
            "name": "fpr2k-1",
            "type": "Device"
        },
```

4. Gebruik het domein UID en het hulpmiddel/de container UID:

```
# 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": "-----\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
                    : 353\n-----\n\nCisco
version
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-Datal/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

}

Volg de stappen in het gedeelte.

FDM REST-API

Volg de stappen in het gedeelte.

FTD Problemen oplossen

Volg deze stappen om de FTD-softwareversie in het FTD-bestand voor probleemoplossing te controleren:

- 1. Opent het bestand voor probleemoplossing en navigeer naar de map **<bestandsnaam>-** probleemoplossing .tar/resultaat-<date>—xxxxx/opdrachtoutput/
- 2. Open het bestand **usr-local-sf-bin-sfcli.pl, waarin versie.output wordt getoond** en vind de regel met **model:**

FCM UI

Gebruik voor FTD op Firepower 4100/9300 de FCM en controleer de **versie** in het tabblad **Logical Devices**:

Overview	Interfaces	Logical Devices	Security Modules	Platform Settings							System Tools	Help admin
Logical Dev	/ice List											^
Group By	Security Module	*										
Security	Module I (I N	ative instance)									0% (0 of 78) Cor	es Available
ASA			Standalone	Status:ok								1
Applie	cation	Version	Resource	e Profile	Management IP	Gateway	Manage	ment Port	Status			
B ASA		9.16.2.7			10.62.148.240	10.62.148.129	Ethernet	1/1	Colice		💌 🕅 cúi /	,
									• Online			
												_
Security	Module 2 (0 in	stances)								,	00% (94 of 94) Con	es Available
				No logical devices	on this security module.							
Security	Module 3 (1 C	ontainer instance)									0% (0 of 110) Cor	es Available
FTD-M	1-1		Standalone	Status:ok							(11
- Anna P		Manalan		0	Manager 10	Colonia			Charles			
Арры	cation	Version	Resource	c Profile	Management IP	Gateway	Manage	ement Port	Status			.
FID		7.1.0.90	RP110		10.62.148.242	10.62.148.129	Ethernet	1/1	Online			7
	Interface Name			1	Abe	AI	ttributes					
	Ethernet1/6			6	iata		Cluster Operational Status : FIREPOWER-MGMT-IP	: not-applicable : 10.62.148.242				
	Ethernet1/7				ata		MGMT-URL HA-ROLE	: https://10.62.148.249/				
	- ar or condition						UUID	: 3050cf4c-c0aa-11ec-9b2a-8	491ab8d0cc8			

FXOS CLI

FTD op FirePOWER 4100/9300

Volg deze stappen om de FTD-softwareversie op FXOS CLI te controleren:

- 1. Maak een console of SSH-verbinding met het chassis.
- 2. Switch naar het bereik ssa en voer de opdracht showapp-instantie uit:

firepower#	scope ssa						
firepower	/ssa # show	app-instan	nce				
App Name	Identifier	Slot ID	Admin State	e Oper St	ate	Running Version	Startup Version
Deploy Typ	e Turbo Mod	e Profile M	Name Cluster	State	Cluster Ro	ole	
						-	
asa	ASA	1	Enabled	Online		9.16.2.7	9.16.2.7
Native	No		Not Appl	icable 1	None		
ftd	FTD-MI-1	3	Enabled	Online		7.1.0.90	7.1.0.90
Container	No	RP110	Not Appl	icable 1	None		

FTD op vuurkracht 1000/2100/3100

Volg deze stappen om de FTD-softwareversie op FXOS CLI te controleren:

1. Een console-verbinding maken met het chassis of de SSH-verbinding met de FTD Als er een SSH-verbinding naar de FTD is gemaakt, voert u de opdracht **Connect fxos** op FTD CLISH uit:

> connect fxos

2. Switch naar het bereik van TV en voer de opdracht showapp-instantie uit:

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

Application Na	me Slot	ID Admin State	e Operational S	tate Running Versi	lon Startup
Version Deploy	Type Profil	e Name Cluster Op	per State Cluster	Role	
ftd	1	Enabled	Online	7.1.0.90	7.1.0.90
Native	N	ot Applicable	None		

FXOS REST-API

Volg deze stappen om de FTD-softwareversie via een FXOS REST-API te controleren:

1. Echtheidstoken aanvragen:

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

2. Gebruik het token in deze zoekopdracht en specificeer de sleuf-ID waarin het FTD is geïnstalleerd:

FXOS-chassis testbestand

Volg deze stappen om de FTD-softwareversie in het FXOS-chassis-bestand te controleren:

FTD op FirePOWER 4100/9300

1. Voor FXOS versies 2.7 en later, open bestand **sam_techsupportinfo** in <name>_BC1_all.tar/FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar

Voor eerdere versies open bestand sam_techsupportinfo in FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar.

2. Controleer het gedeelte voor elke sleuf onder de "toonsleuf breek uitvouwen":

```
# 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
```

FTD op vuurkracht 1000/2100/3100

- 1. Bestand tech_support_brief in <name>_FPRM.tar.gz/<name>_FPRM.tar
- 2. Controleer de secties "scope ssa" en "show Sleuf":

```
# pwd
/var/tmp/fp2k-1_FPRM/
# cat tech_support_brief
. . .
`scope ssa` `show slot`
Slot:
  Slot ID Log Level Admin State Operational State
  Info
                Ok
  1
                          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-softwareversie

De ASA-softwareversie kan met het gebruik van deze opties worden geverifieerd:

- ASA CLI
- ASA SNMP-stemming
- ASA show-tech-bestand
- FCM UI
- FXOS CLI
- FXOS REST API
- FXOS chassis tovertech-bestand

ASA CLI

Volg deze stappen om de ASA-softwareversie op ASA CLI te controleren:

1. Gebruik deze opties om toegang te krijgen tot de ASA CLI in overeenstemming met het platform en de implementatiemodus:

• Toegang tot ASA-telefoon/SSH op FirePOWER 1000/3100 en Firepower 2100 in de

toevoermodus

- Toegang van FXOS-console CLI op Firepower 2100 in platform modus en verbinding met ASA via connect als opdracht
- Toegang van FXOS CLI via opdrachten (Firepower 4100/9300):

Sluit module <x> [console|telnet] aan, waar x de sleuf-ID is, en sluit vervolgens aan als

- Voor virtuele ASA directe SSH-toegang tot ASA of console-toegang van de hypersupervisor of cloud UI
- 2. Start de opdracht show versie:

```
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

Volg deze stappen om de ASA-softwareversie via SNMP te controleren:

- 1. Zorg ervoor dat SNMP is ingesteld en ingeschakeld.
- 2. Gebruik SNMP-client om OID SNMPv2-MIB te inroepen::sysDescr.0 of 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 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-bestand

Zoeken naar de lijn met de Cisco adaptieve security applicatie software versie string:

```
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

Volg de stappen in het vak.

FXOS CLI

Volg de stappen in het gedeelte.

FXOS REST-API

Volg de stappen in het gedeelte.

FXOS-chassis testbestand

Volg de stappen in het gedeelte.

Software voor Firepower Module

De Firepower module op ASA is de nieuwe naam voor de oudere Sourcefire-modules of SFR.

De softwareversie kan met behulp van deze opties worden geverifieerd:

- FMC UI
- FMC REST-API
- Firepower module CLI
- Firepower module probleemoplossing bestand
- ASA CLI
- ASA show-tech-bestand

FMC UI

Volg de stappen in het gedeelte.

FMC REST-API

Volg de stappen in het gedeelte.

Firepower Module CLI

Volg deze stappen om de softwareversie van de Firepower module op de module CLI te controleren:

1. Sluit de module aan via SSH of de ASA CLI via de sessie sfr-opdracht.

2. Start de opdracht show versie:

> 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 Module-bestand voor probleemoplossing

Volg deze stappen om de softwareversie van de Firepower module in het bestand voor probleemoplossing van de module te controleren:

- 1. Opent het bestand voor probleemoplossing en navigeer naar de map <bestandsnaam>probleemoplossing .tar/resultaat-<date>--xxxxxx/opdrachtoutput/
- 2. Open het bestand **usr-local-sf-bin-sfcli.pl**, **waarin versie.output wordt getoond** en vind de regel met **model**:

# pwd		
/var/tmp/results-	05-12-2022199172/command-outputs	
# cat "usr-local-	sf-bin-sfcli.pl show version.output"	
[sfr1] Model : ASA5516 (72) Version 7.1.0 (Bui	1đ 90)
UUID	: c049dad8-c42e-11e9-986d-bdeff3ce399e	
LSP version	: 2022-05-10-001-vrt	
VDB version	: 354	

ASA CLI

Start de opdracht voor de **specificaties van de** showmodule op de ASA CLI en controleer de **softwareversie**:

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
Mgmt web ports:	443
Mgmt TLS enabled:	true

ASA show-tech-bestand

Zoek naar de lijn met de sfr string van de showmodule:

Getting details from the Service Module, please wait...

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
Mgmt web ports:	443
Mgmt TLS enabled:	true

Controleer de versies Snort, VDB en SRU

Diepgaande Packet Inspection Engine (snort) versie

De korte versie kan met behulp van deze opties worden geverifieerd:

- FMC UI
- FMC REST-API
- FDM UI
- FDM REST API
- FTD of Firepower module CLI
- FTD of FirePOWER Module probleemoplossingsbestand

FMC UI

Volg deze stappen om de versie van de FTD Snort op FMC UI te controleren:

1. Kies Apparaten > Apparaatbeheer:



2. Controleer het label Snort:

cisco Dev	repower Management Center ovices / Device Management	overview Analysis	Policies	Devices	Objects	AMP		Deploy Q 🌮 🔅	Ø admin ▼
View By: All (14)	Domain	(12) • Normal (0)	Deployme	nt Pending (7)	 Upgrad 	le (0) • Snort 3 (12)		Deploym	nent History
Collapse All									
Nam	10	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

Volg deze stappen om de FTD Snort-versie via FMC REST-API te controleren. Gebruik een REST-API client om de softwareversie te controleren. In dit voorbeeld wordt de curl gebruikt:

1. Echtheidstoken aanvragen:

```
# 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</pre>
```

2. Identificeer het domein dat het apparaat bevat. Bij de meeste REST API-vragen is de **domeinparameter** verplicht. Gebruik het **X-auth-access-token in** deze query om de lijst met domeinen op te halen:

```
# 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-00000000001"
        },
        {
            "name": "Global/domain2",
            "type": "Domain",
            "uuid": "341a8f03-f831-c364-b751-00000000001"
        }
    1.
    "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. Gebruik het domein UID om een vraag te stellen naar de apparaten:

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
0000000001/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-
0000000001/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-
0000000001/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-
0000000001/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-
0000000001/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-
0000000001/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-
0000000001/devices/devicerecords/0b1a9c94-8ba8-11ec-b2fd-93263934908d"
            },
            "name": "fpr2k-1",
            "type": "Device"
        },
```

4. Gebruik het domein UID en het toestel/container UID in dit verzoek:

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
00000000001/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

Volg deze stappen om de versie van de FTD Snort op FDM UI te controleren:

1. Ga naar de pagina updates:

CISCO. Firepower Device Manager	Monitoring Policies Objects	Device: KSEC-FPR2100	(>_) (Administrator) (*
Model Cisco Firepower 2120 Thr	Software VDB Intrusion F eat Defense 7.1.0-90 346.0 20211110	tule Update Cloud Services -1348 Not Registered Register	High Availability CONFIGURE CONFIGURE
C Inside Network	1/1 1/3 1/5 1/7 1/9 Image: Strategy of the stra	1/11 1/13 1/14 1/15 1/16 1/12 SFP	ISP/WAN/Gateway
Interfaces Connected Enabled 3 of 17 View All Interfaces	Routing There are no static routes yet View Configuration	Updates Geolocation, Rule, VDB, System U Security Intelligence Feeds View Configuration	Jpgrade, Jpgrade, System Settings Logging Settings DHCP Server / Relay DDNS Service DNS Server

2. Automatiseringsmotor controleren:

uluiu cisco.	Firepower Device Manager	题 Monitoring	Policies	∰. Objects	Devic	e: KSEC-FPR2100	(ک		0	?	:	admin Administrator	~
Devic Up	be Summary dates												
G	atest Update on 05 May 2022	VDB 346 Latest Upda	.0 ate on 05 May	2022		Security Intelligence Feeds							
C	Configure et recurring updates	Configure Set recurrin	g updates			Configure Set recurring updates							
	UPDATE FROM CLOUD	UPDATE FI	ROM CLOUD	~		UPDATE FROM CLOUD							
s	System Upgrade Current version 7.1.0-90					Intrusion Rule 20211110-134 Latest Update on 05 May 2022	8						
Ţ	here are no software upgrades availai Ipload an upgrade file to install. BROWSE	ble on the system.				Configure Set recurring updates	Sno Insp Sno Defe SSL	ort ection E rt is the ense. It i decryp	ingine: 3 main ins is used f tion, and	3.1.7.1-1 spection for intrusi d layer 7 i	08 Dow engine i on and i inspectio	ngrade to 2.0 n Firepower Threa file policy analysis on. <u>See more</u> ✓	ıt

FDM REST API

Volg deze stappen om de korte versie via een FDM REST-API-verzoek te controleren. Gebruik een REST-API client om de softwareversie te controleren. In dit voorbeeld wordt de curl gebruikt:

1. Echtheidstoken aanvragen:

```
# 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
0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXN1clJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2
VybmFtZSI6ImFkbWluIn0.lJLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI",
```

```
"expires_in": 1800,
"refresh_expires_in": 2400,
"refresh_token":
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGU0NGIxYzQtZDIOMi0xMW
VjLTk4ZWMtYTllOTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIzOTY1NjksImFjY2VzclRva2VuRXhwaX
JlcOFOIjoxNjUyMzk1OTY5MDcwLCJyZWZyZXNoQ291bnQiOi0xLCJ0b2tlblR5cGUiOiJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXN1clJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2
luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
"token_type": "Bearer"
}
```

2. Gebruik de waarde access_token in deze query:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIONDU3ODksInN1Yi16ImFkbWluIiwianRpIjoiM2U1Njg0YjYtZDJiYS0xMWV
jLTk4ZWMtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LCJleHAiOjE2NTIONDc1ODksInJlZnJlc2hUb2tlbkV4cGl
yZXNBdCI6MTY1MjQ0ODE4OTMyNSwidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC0
xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2V
ybmFtZSI6ImFkbWluIn0.kXtsUu3_WWt0Wu9w0mSDfJjwcyiVCa5dgyzNjCGnlF4'
'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 of Firepower CLI

Op FTD CLI voer de opdracht Show snort3 status uit:

> show snort3 status Currently running Snort 3 De Firepower module ondersteunt alleen snort 2.

FTD of FirePOWER Module-bestand voor probleemoplossing

Volg deze stappen om de versie van de Snort in het Wachtwoord voor probleemoplossing te controleren:

- 1. Opent het bestand voor probleemoplossing en navigeer naar de map <bestandsnaam>- probleemoplossing .tar/resultaat-<date>---xxxxxx/opdrachtoutput
- 2. Open het bestand usr-local-sf-bin-sfcli.pl met de 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
De Finance and a condensate wat allocan ensert 2
```

De Firepower module ondersteunt alleen snort 2.

VDB-versie (Vulnerability Database)

De VDB-versie kan met behulp van deze opties worden geverifieerd:

FMC UI

- FMC REST-API
- FMC-bestand voor probleemoplossing
- FDM UI
- FDM REST API
- FTD CLI
- FTD of FirePOWER Module probleemoplossingsbestand

FMC UI

Volg deze stappen om de VDB-versie op FMC UI te controleren:

1. Help kiezen > Over:											
Firepower Management Center Overview / Dashboards / Management	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence		Deploy	۹ 🎸	🚆 🏹 🕜 admin 🔻
Name Access Controlled User Statistics Provides traffic and intrusion event statistics by user Application Statistics Provides Taffic and intrusion event statistics by application							Page-level Help How-Tos Documentation on C What's New in This I Software Download Secure Firewall YouT	lisco.com Release Tube	Se Fin Pa As TA 2 Ab	cure Firev epower M ther Ecos k a Questi C Support out	vall on Cisco.com ligration Tool system ion t Cases
Application Statistics (7.1.0) Provides application statistics							admin	No	No		[° < ∕ ₹
Connection Summary Provides tables and charts of the activity on your monitored net	work segment or	ganized by differ	ent criteria				admin	No	No		12 Q / 1
Detailed Dashboard Provides a detailed view of activity on the appliance							admin	No	No		₫ Q 🖉 🗑
Detailed Dashboard (7.0.0) Provides a detailed view of activity on the appliance							admin	No	No		C Q / T
Files Dashboard Provides an overview of Mahware and File Events							admin	No	No		1 Q / 1
Security Intelligence Statistics Provides Security Intelligence statistics							admin	No	No		[t] Q ≠ 🗑
Summary Dashboard Provides a summary of activity on the appliance							admin	No	Yes		1 Q / 1

2. Controleer VDB versie:

Firepower Ma	nagement Center _{Over}	iew Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	Q	¢ 😜	🕜 admin 🔻
Model Serial Numbor Software Version OS Snort Version Rule Update Version Rule pack Version Module Pack Version LSP Version Geolocation Update Version VDB Version Hostname	Cisco Firepower Management Cent 001234 7.1.0 (build 90) Cisco Firepower Extensible Operati 2.9.19 (Build 92) 3.1.7.1 (Build 108) 2022-05-02-003-vrt 2703 3070 Isp-rel-20220502-1613 2022-04-25-002 build 354 (2022-04-27 19:39:56) FMC-4600-2	r 4600 g System (FX-OS) 2.	11.1 (build154)			For tec or call Copyri	chnical/system questions, e-ma us at 1-800-553-2447 or 1-40 ght 2004-2021, Cisco and/or it	il tac@cisco.com)8-526-7209 Is affiliates. All rights	reser.	red.	

FMC CLI

Volg deze stappen om de VDB-versie op FMC CLI te controleren:

- 1. Toegang tot FMC via SSH of console-verbinding.
- 2. Start de opdracht Versie:

FMC REST-API

Volg deze stappen om de VDB-versie via een FMC REST-API te controleren. Gebruik een REST-API client om de softwareversie te controleren. In dit voorbeeld wordt de curl gebruikt:

1. Echtheidstoken aanvragen:

```
# 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</pre>
```

2. Identificeer het domein dat het apparaat bevat. Bij de meeste REST API-vragen is de **domeinparameter** verplicht. Gebruik het **X-auth-access-token in** deze query om de lijst met domeinen op te halen:

```
# 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-bestand voor probleemoplossing

Volg deze stappen om de VDB-versie in het FMC-bestand voor probleemoplossing te controleren:

- 1. Opent het bestand voor probleemoplossing en navigeer naar de map <bestandsnaam>probleemoplossing .tar/resultaat-<date>—xxxxxx/dir-archives/etc/sf/.versiondb
- 2. Open het bestand vdb.conf en vind de regel met de toets CURRENT_BUILD:

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

VDB:



FDM REST API

Volg deze stappen om de VDB-versie te controleren via een FDM REST-API-verzoek. Gebruik een REST-API client om de softwareversie te controleren. In dit voorbeeld wordt de curl gebruikt:

1. Echtheidstoken aanvragen:

```
# 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
0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXN1clJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2
VybmFtZSI6ImFkbWluIn0.1JLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI",
"expires_in": 1800,
"refresh_expires_in": 2400,
"refresh_token":
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGU0NGIxYzQtZDI0Mi0xMW
VjLTk4ZWMtYTllOTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIzOTY1NjksImFjY2Vzc1Rva2VuRXhwaX
Jlc0F0IjoxNjUyMzk10TY5MDcwLCJyZWZyZXNoQ291bnQi0i0xLCJ0b2tlblR5cGUi0iJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2
luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
"token_type": "Bearer"
```

2. Gebruik de waarde access_token in deze query:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUZI1NiJ9.eyJpYXQiOjE2NTIONDU3ODksInN1YiI6ImFkbWluIiwianRpIjoiM2U1NjgOYjYtZDJYSOxMWV
jLTk4ZWMtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LCJleHAiOjE2NTIONDc1ODksInJlZnJlc2hUb2tlbkV4cGl
yZXNBdCI6MTY1MjQ0ODE4OTMyNSwidG9rZW5UeXBlIjoiSldUXOFjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MCO
xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJlc2V
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 of FirePOWER Module CLI

}

Volg deze stappen om de VDB-versie op de FTD CLI of op de FirePOWER-module (SFR) CLI te controleren:

- 1. Toegang tot FTD via SSH of console verbinding. In het geval van de Firepower module, heb toegang tot de module via SSH, of van de ASA CLI via de **sessie sfr** opdracht.
- 2. Start de opdracht Verkenningsversie op CLI:

<pre>> show version</pre>	
[f;	pr2k-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	
<pre>> show version</pre>	
[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 of FirePOWER Module-bestand voor probleemoplossing

Volg deze stappen om de VDB-versie in het FTD of het bestand voor probleemoplossing in de FirePOWER-module te controleren:

- 1. Opent het bestand voor probleemoplossing en navigeer naar de map **<bestandsnaam>-** probleemoplossing.tar/resultaat-<date>---xxxxxx/opdrachtoutput/
- 2. Open het bestand **usr-local-sf-bin-sfcli.pl, die versie.output toont** en vind de regel met de **VDB-versie**:

cat "usr-local-sf-bin-sfcli.pl show version.output"												
Firepower 2110 Threat Defense (77) Version 7.1.0 (Build 90)												
0c94-8ba8-11ec-b2fd-93263934908d												
cel-20220510-1044												

pwd

/var/tmp/results-05-12-2022199172/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	s update	version	: 202	2-05-10-	001-vr	t VDB v	versi	on :	354	

Inbraakregel Update versies

De inbraakregelupdates bieden nieuwe en bijgewerkte inbraakregels en voorprocessorregels, aangepaste staten voor geïnstalleerde regels en aangepaste standaardinstellingen voor inbraakbeleid.

De veilige regelupdates (SRU) zijn van toepassing op versie 2 van de SNEL, en de lichtgewicht veiligheidspakket (LSP) updates zijn van toepassing op versie 3 van de Kort.

De SRU/LSP-softwareversie kan met het gebruik van deze opties worden geverifieerd:

- FMC UI
- FMC REST-API
- FMC-bestand voor probleemoplossing
- FDM UI
- FDM REST API
- FTD of Firepower module CLI
- FTD of FirePOWER Module probleemoplossingsbestand

FMC UI

Volg deze stappen om SRU/LSP-versies op FMC UI te controleren:

1. Help kiezen > Over:

Firepower Management Center Overview / Dashboards / Management	Overview	Analysis	Policies	Devices	Objects	AMP	Intellig	gence		Deploy	۹ 🌢	🚰 🎝 1 🕜 admin 🔻
Name Access Controlled User Statistics Provides traffic and intrusion event statistics by user Application Statistics Provides traffic and intrusion event statistics by application								Page-level Help How-Tos Documentation on What's New in Thi Software Downloa Secure Firewall Yo	Cisco.com s Release d uTube	S F A T T 2 A	ecure Firen irepower N artner Eco sk a Quest AC Suppor	wall on Cisco.com Aigration Tool system tion rt Cases
Application Statistics (7.1.0) Provides application statistics								admin	No	No		C < ≠ i
Connection Summary Provides tables and charts of the activity on your monitored ne	twork segment or	ganized by differ	ent criteria					admin	No	No	, ,	12 Q / 1
Detailed Dashboard Provides a detailed view of activity on the appliance								admin	No	No	þ	12 Q / 1
Detailed Dashboard (7.0.0) Provides a detailed view of activity on the appliance								admin	No	No	0	12 Q / 1
Files Dashboard Provides an overview of Malware and File Events								admin	No	N	b	12 Q / 1
Security Intelligence Statistics Provides Security Intelligence statistics								admin	No	No	0	12 Q / 1
Summary Dashboard Provides a summary of activity on the appliance								admin	No	Ye	s	

2. Controleer Regel Update versie en LSP versie:



FMC CLI

Volg deze stappen om SRU/LSP-versies op FMC CLI te controleren:

- 1. Toegang tot FMC via SSH of console-verbinding.
- 2. Start de opdracht Verkenningsversie op CLI:

FMC REST-API

Volg deze stappen om de softwareversie via een REST-API-verzoek te controleren. Gebruik een REST-API client om de softwareversie te controleren. In dit voorbeeld wordt **curl** gebruikt:

1. Echtheidstoken aanvragen:

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. Gebruik het X-auth-access-token in deze query:

```
# 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-bestand voor probleemoplossing

Volg deze stappen om de SRU-versie in het FMC-bestand voor probleemoplossing te controleren:

- 1. Opent het bestand voor probleemoplossing en ga naar map <bestandsnaam>.tar/resultaat-
<date>---xxxxxx/dir-archives/etc/sf/
- 2. Open het bestand **sru_versies.conf** en vind de regels met de toetsen **Inbraaksion_Rules_Update**:

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

Volg deze stappen om LSP-versie in het FMC-bestand voor probleemoplossing te controleren:

1. Opent het bestand voor probleemoplossing en ga naar map <bestandsnaam>.tar/resultaat-

2. Bestand openen **om var-sf-lsp-maxdeep 2 -ls.output te vinden** en de lijn te controleren met /var/sf/lsp/active-lsp

# pwd									
/var/tmp/r	esults-05-06-2022	-199	172/co	mmand-outputs	5				
# cat "fin	d var-sf-lsp -maxde	epth	2 -1s	.output"					
• • •									
Output of	find /var/sf/lsp -m	naxd	epth 2	-ls:					
10120102	1 daermaaring in	2		woot	1006	More	1 1	04.01	/www./af/lan
10142269	4 UIWXIWXI-X	1	www	root	4090	мау	11	04.01	/var/si/isp
19142208	U ITWXTWXTWX	1	rool	root	33	мау	ΤT	04.00	/var/si/isp/installed-
lsp -> /va	r/si/isp/isp-rei-20	1220	510-10		1005			0.4.01	
19138299	4 drwxrwxr-x	5	www	root	4096	Мау	11	04:01	/var/st/lsp/lsp-rel-
20220510-1	044								
19142266	600 -rwxrwxr-x	1	www	root	614400	May	10	14:55	/var/sf/lsp/lsp-rel-
20220510-1	044/lsp.icdb.RELEAS	SE.t	ar						
19142234	4 drwxrwxr-x	5	www	root	4096	May	11	04:00	/var/sf/lsp/lsp-rel-
20220510-1	044/ntd_metadata								
19268898	4 drwxrwxr-x	2	www	root	4096	May	10	14:55	/var/sf/lsp/lsp-rel-
20220510-1	044/icdb								
19138303	4 drwxrwxr-x	6	www	root	4096	May	10	14:51	/var/sf/lsp/lsp-rel-
20220510-1	044/talos_content								
19142269	46640 -rw-rr	1	root	root	47759360	May	11	04:01	/var/sf/lsp/lsp-rel-
20220510-1	044/lsp-rel-2022051	L0-1	044.ta	r.xz.REL.tar					
19142267	4 -rwxrwxr-x	1	www	root	238	May	11	04:00	/var/sf/lsp/lsp-rel-
20220510-1	044/.snort-versions	3				-			
19142265	4 -rwxrwxr-x	1	www	root	26	May	10	14:51	/var/sf/lsp/lsp-rel-
20220510-1	044/lspd_ver.proper	rtie	S						
19139198	260 -rw-rr	1	root	root	264403	Feb	12	03:32	/var/sf/lsp/piqtail-
all-164463	6642.log								
19142270	0 1rwxrwxrwx	1	root	root	33	May	11	04:01	/var/sf/lsp/active-lsp
-> /var/sf	/lsp/lsp-rel-202205	510-	1044			2			· · · · · · · · · · · · · · · · · · ·
, , , , , , , , , , , , , , , , , , ,	,,p 101 10110.								

FDM UI

Ga voor de hoofdpagina naar Inbraakregel:

Firepower Device Manager	Monitoring Policies Objects	Device: KSEC-FPR2100	admin · · · · · · · · · · · · · · · · · · ·	
Model Software VDB Intrusion Rule Update 20211110-1348 Cloud Services Not Register Not Configured Not Configured ConFigure				
F Inside Network	12 Cisco Firepower 2120 Threat Defense MOMT 1/1 1/3 1/5 1/7 1/9 1/11 CONSOLE 1/2 1/4 1/6 1/8 1/10 1/12 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/1 1/	1 1/13 1/14 1/15 1/16 2 SFP	Internet IDNS Server IDNS Serv	
Interfaces Connected Enabled 3 of 17 View All Interfaces	Routing There are no static routes yet View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server / Relay DDNS Service DNS Server	

FDM REST API

Volg deze stappen om de VDB-versie te controleren via een FDM REST-API-verzoek. Gebruik een REST-API client om de softwareversie te controleren. In dit voorbeeld wordt **curl** gebruikt:

1. Echtheidstoken aanvragen:

```
# 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
0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXN1clJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2
VybmFtZSI6ImFkbWluIn0.lJLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI",
"expires_in": 1800,
"refresh_expires_in": 2400,
"refresh_token":
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGU0NGIxYzQtZDI0Mi0xMW
VjLTk4ZWMtYTllOTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIzOTY1NjksImFjY2Vzc1Rva2VuRXhwaX
Jlc0F0IjoxNjUyMzk10TY5MDcwLCJyZWZyZXNoQ291bnQiOi0xLCJ0b2tlblR5cGUiOiJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2
luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
"token_type": "Bearer"
ł
Gebruik de waarde access_token in deze query:
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIONDU3ODksInN1YiI6ImFkbWluIiwianRpIjoiM2U1Njg0YjYtZDJiYS0xMWV
jLTk4ZWMtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LCJ1eHAiOjE2NTI0NDc10DksInJ1ZnJ1c2hUb2t1bkV4cG1
```

```
yZXNBdCl6MTY1MjQ0ODE4OTMyNSwidG9rZW5UeXBl1joiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC0
xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2V
ybmFtZSI6ImFkbWluIn0.kXtsUu3_WWt0Wu9w0mSDfJjwcyiVCa5dgyzNjCGnlF4'
'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 of FirePOWER Module CLI

Volg deze stappen om SRU/LSP-versie op FTD CLI of de Firepower module CLI te controleren:

- 1. Toegang tot FTD via SSH of console verbinding. In het geval van de Firepower module, heb toegang tot de module via SSH, of van de ASA CLI via de **sessie sfr** opdracht.
- 2. Start de opdracht Verkenningsversie op CLI:

<pre>> show version</pre>		
[F	FIREPOWER1.ci	3CO.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

<pre>> show version</pre>	
[FIREPOWER	R1.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
s show worsion	
[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

Opmerking: De opdracht **"show version**" toont de SRU update versie als Snort 2 wordt gebruikt. Voor de versie van Kort 3 LSP wordt weergegeven.

FTD of FirePOWER Module-bestand voor probleemoplossing

Volg deze stappen om SRU/LSP-versies in het FTD of het bestand voor probleemoplossing in de Firepower module te controleren:

- 1. Opent het bestand voor probleemoplossing en ga naar map **<bestandsnaam>-** probleemoplossing.tar/resultaten-<date>—xxxxxx/commando-outputs/
- 2. Open het bestand usr-local-sf-bin-sflini.pl, waarvan versie.output wordt weergegeven en vind de regel met SRU/LSP-versie:

```
# pwd
/var/tmp/results-05-06-2022--163203/command-outputs/
# cat "usr-local-sf-bin-sfcli.pl show version.output"
-----[ FIREPOWER1.cisco.com ]------
                      : Cisco Firepower 2120 Threat Defense (77) Version 7.1.0 (Build 90)
Model
                      : 1cbe9952-cc6f-11ec-b63a-ae4636e42209
UUID
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 ]------
                      : Cisco Firepower 2120 Threat Defense (77) Version 7.1.0 (Build 90)
Model
                      : 70727d06-8ba7-11ec-bfcc-999f61f27102
UUID
Rules update version
                      : 2022-05-11-001-vrt
VDB version
                      : 346
_____
```

Bekende problemen

Cisco bug-id CSCwb34098 ENH: FMC-versie in opdracht van 'show managers' tonen

Cisco bug-id <u>CSCve13470</u> ENH: Software-gerelateerde OID's op FirePOWER 6.x inschakelen

Cisco bug-id <u>CSCwb85969</u> ENH: Uitvoer van de opdracht "Show versie" FMC CLISH in het problematische bestand opnemen

Cisco bug-id <u>CSCvu15709</u> ENH: Ondersteuning voor SNMP OID's om SRU/VDB/GEOlocatieversies op FirePOWER-platforms te selecteren

Gerelateerde informatie

- Secure Firewall Management Center REST API Quick Start Guide, versie 7.1
- <u>SNMP configureren op Firepower NGFW applicaties</u>
- <u>Cisco Firepower Threat Defense REST API-gids</u>
- <u>Cisco FXOS REST API-referentie</u>
- <u>Cisco ASA-compatibiliteit</u>
- Firepower 1000/2100 en Secure Firewall 3100 ASA en FXOS-bundelversies
- <u>Gebundelde componenten</u>
- Procedures voor het genereren van bestanden voor firewalls