Firepower 소프트웨어 버전 확인

목차

<u>소</u>개 사전 요구 사항 요구 사항 사용되는 구성 요소 소프트웨어 버전 확인 FMC 소프트웨어 버전 **FMC UI** FMC CLI **FMC REST-API** FMC 문제 해결 파일 FTD 또는 Firepower 모듈 CLI FTD 또는 Firepower 모듈 문제 해결 파일 FDM 소프트웨어 버전 FDM UI **FDM REST API FTD CLI FTD SNMP** FTD 문제 해결 파일 FXOS 소프트웨어 버전 FCM UI **FXOS CLI FXOS REST-API FXOS SNMP** FXOS 섀시 show-tech 파일 FTD 소프트웨어 버전 **FTD CLI FTD SNMP FMC UI FMC REST API** FDM UI **FDM REST-API** FTD 문제 해결 파일 FCM UI **FXOS CLI FXOS REST-API** FXOS 섀시 show-tech 파일 ASA 소프트웨어 버전 ASA CLI **ASA SNMP** ASA show-tech 파일

FCM UI **FXOS CLI FXOS REST-API** FXOS 섀시 show-tech 파일 Firepower Module 소프트웨어 버전 **FMC UI FMC REST-API** Firepower 모듈 CLI Firepower Module 문제 해결 파일 ASA CLI ASA show-tech 파일 Snort, VDB 및 SRU 버전 확인 Deep Packet Inspection Engine(Snort) 버전 FMC UI **FMC REST-API** FDM UI **FDM REST API** FTD 또는 Firepower CLI FTD 또는 Firepower 모듈 문제 해결 파일 VDB(취약성 데이터베이스) 버전 FMC UI FMC CLI **FMC REST-API** FMC 문제 해결 파일 FDM UI **FDM REST API** FTD 또는 Firepower 모듈 CLI FTD 또는 Firepower 모듈 문제 해결 파일 <u>침입 규칙</u> 업데이트 버전 FMC UI FMC CLI **FMC REST-API** FMC 문제 해결 파일 FDM UI **FDM REST API** FTD 또는 Firepower 모듈 CLI FTD 또는 Firepower 모듈 문제 해결 파일 알려진 문제 관련 정보

소개

이 문서에서는 Firepower 소프트웨어 버전 확인에 대해 설명합니다.

사전 요구 사항

요구 사항

기본 제품 지식, REST-API, SNMP.

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Firepower 11xx
- Firepower 21xx
- Firepower 31xx
- Firepower 41xx
- FMC(Firepower Management Center) 버전 7.1.x
- FXOS(Firepower eXtensible Operating System) 2.11.1.x
- FDM(Firepower Device Manager) 7.1.x
- Firepower Threat Defense 7.1.x
- ASA 9.17.x

소프트웨어 버전 확인

FMC 소프트웨어 버전

FMC 소프트웨어 버전은 다음 옵션을 사용하여 확인할 수 있습니다.

- FMC UI
- FMC CLI
- REST API 요청
- FMC 문제 해결 파일
- FTD 또는 Firepower 모듈 CLI
- FTD 또는 Firepower 모듈 문제 해결 파일

FMC UI

다음 단계에 따라 FMC UI에서 FMC 소프트웨어 버전을 확인합니다.

1. 도움말 **> 정보를 선택합니다.**

Firepower Management Center Overview / Dashboards / Management	Overview	Analysis	Policies	Devices	Objects	AMP	Intellige	nce		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 This Software Downloa Secure Firewall Yo	Cisco.com s Release d uTube	2 [Secure Fire Firepower Partner Eco Ask a Ques TAC Suppo About	wall on Cisco.com Migration Tool isystem ition int Cases
Application Statistics (7.1.0) Provides application statistics								admin	No	N	lo	
Connection Summary Provides tables and charts of the activity on your monitored no	etwork segment o	ganized by differ	ent criteria					admin	No	N	lo	E 9/1
Detailed Dashboard Provides a detailed view of activity on the appliance								admin	No	N	lo	C < / 1
Detailed Dashboard (7.0.0) Provides a detailed view of activity on the appliance								admin	No	N	lo	[t Q ≠]
Files Dashboard Provides an overview of Malware and File Events								admin	No	N	lo	C Q 🖉 🗑
Security Intelligence Statistics Provides Security Intelligence statistics								admin	No	N	lo	C Q / T
Summary Dashboard Provides a summary of activity on the appliance								admin	No	Y	es	₫ Q 🖉 🖥

2. 소프트웨어 버전 확인:

Firepower Ma	inagement Center _{Overview}	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	۹	6 ⁰⁰ ¢	🕜 admin 🔻
Model Serial Number Software Version OS Snort Version Rule Update Version Rulepack Version Module Pack Version LSP Version Geolocation Update Version VDB Version Hostname	Cisco Firepower Management Center 4600 001234 7.1.0 (build 90) Cisco Firepower Extensible Operating Syster 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	n (FX-OS) 2.11	1 (build154)			For tec or call Copyri	chnical/system questions us at 1-800-553-2447 of ght 2004-2021, Cisco at	, e-mail tac@cisco.com or 1-408-526-7209 nd/or its affiliates. All rights	reserv	red.	

FMC CLI

다음 단계에 따라 FMC CLI에서 FMC 소프트웨어 버전을 확인합니다.

1. SSH 또는 콘솔 연결을 통해 FMC에 액세스합니다. 배너에는 소프트웨어 버전이 표시됩니다.

Cisco Firepower Extensible Operating System (FX-OS) v2.11.0 (build 154) Cisco Secure Firewall Management Center 4600 v7.1.0 (build 90) 2. CLI에서 show version 명령을 실행합니다.

<pre>> show version</pre>		
[FMC-4600-2.cd	isc	eo.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

FMC REST-API 요청을 통해 FMC 소프트웨어 버전을 확인하려면 다음 단계를 수행하십시오. REST-API 클라이언트를 사용하여 소프트웨어 버전을 확인합니다. 이 예에서는 **curl**이 사용됩니다.

1. 인증 토큰 요청:

```
# 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. 이 쿼리에서 X-auth-access-token을 사용합니다.
# 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
 }
```

참고: 명령 문자열의 "| python -m json.tool" 부분은 JSON 스타일의 출력 형식을 지정하는 데 사용되며 선택 사항입니다.

FMC 문제 해결 파일

문제 해결 파일에서 FMC 소프트웨어 버전을 확인하려면 다음 단계를 수행하십시오.

- 1. 문제 해결 파일을 열고 <filename>.tar/results-<date>---xxxxxx/dir-archives/etc/sf/ 폴더로 이동 합니다.
- 2. ims.conf 파일을 열고 키 SWVERSION 및 SWBUILD가 있는 줄을 찾습니다.

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 또는 Firepower 모듈 CLI

다음 단계에 따라 FTD CLI 또는 Firepower 모듈 CLI에서 FMC 소프트웨어 버전을 확인합니다.

- 1. SSH 또는 콘솔 연결을 통해 FTD에 액세스합니다. Firepower 모듈의 경우 SSH를 통해 또는 ASA CLI에서 session sfr 명령을 통해 모듈에 **액세스합니다**.
- 2. expert 명령을 실행합니다.

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

3. Firepower 모듈에서 less /ngfw/var/sf/detection_engines/<UUID>/ngfw.rules 명령을 FTD 또는 less /var/sf/detection_engines/<UUID>/ngfw.rules 명령을 실행하고 행 DC 버전을 확인합니다.

FTD 또는 Firepower 모듈 문제 해결 파일

다음 단계에 따라 FTD 또는 Firepower 모듈 문제 해결 파일에서 FMC 소프트웨어 버전을 확인합니 다.

- 1. 문제 해결 파일을 열고 <filename>-troubleshoot .tar/results-<date>---xxxxxx/filecontents/ngfw/var/sf/detection-engines/<UUID>/ 폴더로 이동합니다. Firepower 모듈의 경우 폴더 <filename>-troubleshoot .tar/results-<date>---xxxxxx/file-contents/var/sf/detectionengine/<UUID>/
- 2. ngfw.rules 파일을 열고 행 DC 버전을 확인합니다.

pwd /var/tmp/results-05-06-2022--163203/file-contents/ngfw/var/sf/detection_engines/5e9fa23a-5429-11ec-891e-b19e407404d5 # cat ngfw.rules #### nafw.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) # : 7.1.0-90 OS: 90 # DC Version # SRU : 2022-05-11-001-vrt : 354 # VDB # . . .

FDM 소프트웨어 버전

다음 옵션을 사용하여 FDM 소프트웨어 버전을 확인할 수 있습니다.

FDM UI

- FTD CLI
- FTD SNMP 폴링
- FTD 문제 해결 파일
- FDM REST API
- FCM(Firepower Chassis Manager) UI
- FXOS CLI
- FXOS REST API
- FXOS 섀시 show-tech 파일

FDM UI

FDM UI에서 소프트웨어 버전을 확인하려면 기본 페이지에서 소프트웨어를 선택합니다.

Firepower Device Manager	Monitoring Policies Objects De	evice: KSEC-FPR2100	admin · · · · · · · · · · · · · · · · · · ·
Model Cisco Firepower 2120 Three	at Defense Software VDB Intrusion Rule Up 7.1.0-90 346.0 20211110-1348	date Cloud Services High Availa	bility CONFIGURE
Finide Network	Cisco Firepower 2120 Threat Defense MGMT 1/1 1/3 1/5 1/7 1/9 1/11 Consols 1/2 1/4 1/6 1/8 1/10 1/12 CONSOLS 1/2 1/4 1/6 1/8 1/10 1/12	1/13 1/14 1/15 1/16 SFP	teway
	1/1		
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

FDM REST API

다음 단계에 따라 FDM REST-API 요청을 통해 FDM 소프트웨어 버전을 확인합니다. REST-API 클 라이언트를 사용하여 소프트웨어 버전을 확인합니다. 이 예에서는 curl이 사용됩니다.

1. 인증 토큰 요청:

```
# 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
```

Jlc0F0IjoxNjUyMzk10TY5MDcwLCJyZWZyZXNoQ291bnQi0i0xLCJ0b2tlblR5cGUi0iJKV1RfUmVmcmVzaCIsInVzZXJVdW

lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2 luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw", "token_type": "Bearer"

```
2. 이 쿼리에서 액세스 토큰 값을 사용합니다.
```

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyNDk5NTcsInN1Yi16ImFkbWluIiwianRpIjoiNDk3MmRjNjAtZDBmMi0xMWV
jLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2hUb2tlbkV4cGl
yZXNBdCI6MTY1MjI1MjM1NzQ1NywidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC0
xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJlc2V
ybmFtZSI6ImFkbWluIn0.lJLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI'
'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

섹션의 단계를 따릅니다.

FTD SNMP

섹션의 단계를 따릅니다.

FTD 문제 해결 파일

섹션의 단계를 따릅니다.

FCM UI

FCM은 Firepower 4100 및 Firepower 9300 Series에서 사용할 수 있습니다. 섹션의 단계를 따릅니 다.

FXOS CLI

섹션의 단계를 따릅니다.

FXOS REST-API

섹션의 단계를 따릅니다.

FXOS 섀시 show-tech 파일

섹션의 단계를 따릅니다.

FXOS 소프트웨어 버전

FXOS 소프트웨어 버전은 다음 옵션을 사용하여 확인할 수 있습니다.

- FCM UI(Firepower 4100/9300만 해당)
- FXOS CLI
- FXOS REST API

• FXOS SNMP 폴링

• FXOS 섀시 show-tech 파일.

FCM UI

FCM UI에서 FXOS 소프트웨어 버전을 확인하려면 기본 페이지에서 버전을 확인합니다.

Overview Interface	s Logical Devices Security Modules Platform Settings	System	Tools	Help	admin	Î
KSEC-FPR9K-3-A Model: Cisco Firep	10.62.148.239 Operational State: Operable Chassis Uptime	27:00:2	1:03	(U P	0	
	Network Module 1 Network Module 2 Network Module 3 : Empty CONSOLE MGMT US8 1 2 3 4 5 6 7 8 Network Module 2 Network Module 3 : Empty					
	🗑 Security Module 1 - Up					
	🗑 Security Module 3 - Up 🔊 🖉 Power 1 - Running 🗇 🖉 Power 2 - Running					

FXOS CLI

Firepower 4100/9300

다음 단계에 따라 FXOS CLI에서 FXOS 소프트웨어 버전을 확인합니다.

1. 섀시에 콘솔 또는 SSH 연결을 설정합니다.

2. 범위 시스템으로 전환하고 show firmware monitor 명령:

```
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 및 FTD
```

다음 단계에 따라 FXOS CLI에서 FXOS 소프트웨어 버전을 확인합니다.

1. 섀시에 대한 콘솔 연결 또는 FTD에 대한 SSH 연결을 설정합니다. FTD에 대한 SSH 연결의 경우 FTD CLISH에서 **connect fxos** 명령을 실행합니다.

```
<sup>></sup> connect_fxos
2. 범위 시스템으로 전환하고 show firmware detail 명령을 실행합니다.
```

```
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(ASA 사용), Firepower 2100(ASA 사용) 어플라이언스 모드에서

다음 단계에 따라 FXOS CLI에서 FXOS 소프트웨어 버전을 확인합니다.

1. 섀시에 대한 콘솔 연결 또는 ASA에 대한 텔넷/SSH 연결을 설정합니다. ASA에 대한 텔넷/SSH 연결의 경우 ASA CLI에서 connect fxos 명령을 실행합니다.

```
asa# connect fxos
```

2. 범위 시스템으로 전환하고 show firmware detail 명령을 실행합니다.

```
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)
```

플랫폼 모드에서 ASA를 사용하는 Firepower 2100

다음 단계에 따라 FXOS CLI에서 FXOS 소프트웨어 버전을 확인합니다.

1. 섀시에 대한 SSH 또는 콘솔 연결 또는 ASA에 대한 텔넷/SSH 연결을 설정합니다. ASA에 대한 텔넷/SSH 연결의 경우 ASA CLI에서 connect fxos 명령을 실행합니다.

asa# connect fxos

2. 범위 시스템으로 전환하고 show firmware detail 명령을 실행합니다.

```
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-API는 Firepower 4100/9300 Series에서 지원됩니다.

Firepower 4100/9300

다음 단계에 따라 FXOS REST-API 요청을 통해 FXOS 소프트웨어 버전을 확인합니다. REST-API

클라이언트를 사용하여 소프트웨어 버전을 확인합니다. 이 예에서는 curl이 사용됩니다.

1. 인증 토큰 요청:

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

FXOS SNMP

FXOS의 SNMP 컨피그레이션은 플랫폼 모드에서 ASA를 사용하는 Firepower 2100과 Firepower 4100/9300에서 지원됩니다.

Firepower 4100/9300

SNMP를 통해 FXOS 소프트웨어 버전을 확인하려면 다음 단계를 수행하십시오.

- 1. SNMP가 FXOS에 구성되어 있는지 확인합니다. 컨피그레이션 단계<u>는 Firepower NGFW 어플</u> <u>라이언스에서 SNMP 구성</u>을 참조하십시오.
- 2. 폴링 .1.3.6.1.4.1.9.9.826.1.30.47.1.6 또는 CISCO-FIREPOWER-FIRMWARE-MIB: cfpr펌웨 어 실행 패키지 버전:

```
# 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)"
.1.3.6.1.4.1.9.9.826.1.30.47.1.6.30780 = 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"
플랫폼 모드에서 ASA를 사용하는 Firepower 2100
```

SNMP를 통해 FXOS 소프트웨어 버전을 확인하려면 다음 단계를 수행하십시오.

- 1. SNMP가 FXOS에 구성되어 있는지 확인합니다. 컨피그레이션 단계<u>는 Firepower NGFW 어플</u> <u>라이언스에서 SNMP 구성</u>을 참조하십시오.
- 2. poll.1.3.6.1.2.1.1.0 또는 SNMPv2-MIB::sysDescr.0:

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 섀시 show-tech 파일

Firepower 4100/9300

다음 단계에 따라 FXOS 섀시 show-tech 파일에서 FXOS 소프트웨어 버전을 확인합니다.

1. FXOS 버전 2.7 이상의 경우 **<name>_BC1_all.tar**/

FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar에서 sam_techsupportinfo 파일을 엽 니다.

이전 버전의 경우 FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar에서 sam_techsupportinfo를 엽니다.

2. 'show firmware monitor' 명령의 출력을 확인합니다.

```
# 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. 파일 tech_support_brief를 <name>_FPRM.tar.gz/<name>_FPRM.tar에서 엽니다.
- 2. 'show firmware detail' 명령의 출력을 확인합니다.

```
# 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 소프트웨어 버전

FTD 소프트웨어 버전은 다음 옵션을 사용하여 확인할 수 있습니다.

- FTD CLI
- FTD SNMP 폴링
- FTD 문제 해결 파일
- FMC UI
- FMC REST API
- FDM UI
- FDM REST API
- FCM UI
- FXOS CLI
- FXOS REST API
- FXOS 섀시 show-tech 파일

FTD CLI

다음 단계에 따라 FTD CLI에서 FTD 소프트웨어 버전을 확인합니다.

1. 플랫폼 및 구축 모드에 따라 FTD CLI에 액세스하려면 다음 옵션을 사용합니다.

- FTD에 대한 직접 SSH 액세스 모든 플랫폼
- 명령 연결 ftd를 통해 FXOS 콘솔 CLI(Firepower 1000/2100/3100)에서 액세스
- 명령을 통해 FXOS CLI에서 액세스(Firepower 4100/9300):

연결 모듈 <x> [console|telnet], 여기서 x는 슬롯 ID입니다.

ftd [instance]를 연결합니다. 여기서 인스턴스는 다중 인스턴스 구축에만 관련됩니다.

• 가상 FTD의 경우 FTD에 대한 직접 SSH 액세스 또는 하이퍼바이저 또는 클라우드 UI에서 콘솔

2. CLI에서 show version 명령을 실행합니다.

> 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

SNMP를 통해 FTD 소프트웨어 버전을 확인하려면 다음 단계를 수행하십시오.

- 1. SNMP가 구성 및 활성화되었는지 확인합니다. FDM 관리 FTD의 경우 구성 단계<u>는 Firepower</u> FDM에서 SNMP 구성 및 문제 해결을 참조하십시오. FMC 관리 FTD의 경우 컨피그레이션 단 계<u>는 Firepower NGFW 어플라이언스에서 SNMP 구성</u>을 참조하십시오.
- 2. 폴링 OID SNMPv2-MIB::sysDescr.0 또는 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

다음 단계에 따라 FMC UI에서 FTD 소프트웨어 버전을 확인합니다.

1 Devices > Device Management를 선택합니다

Firepower Management Center cisco Overview / Dashboards / Dashboard	Overview	Analysis Policies	1 Devices Objects	AMP Int	elligence	Deploy Q	🧬 🌣 🕜 admin ▾
Summary Dashboard (switch.daahboard) Provides a summary of activity on the appliance Network × Threats Intrusion Events Statu	ıs Geolo	ocation QoS	2 Device Management Device Upgrade NAT QoS Se Platform Settings FlexConfig Certificates	VPN Site To Remote Dynam Trouble Site to	site e Access lic Access Policy eshooting Site Monitoring	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture	Reporting T II Add Widgets
 Unique Applications over Time 	$-\times$	Top Web Application	005 3664	- ^	F TOP OTIGHT APP	JIIUdu0118-30011	- ×
		Application Ubuntu Ubuntu Ubuntu Update Mar	▼ To	tal Bytes (KB) 548.77 5.57	Application Internet Explo	rer kaging Tool	▼ Total Bytes (KB) 5,901,473.76 7.42
Reference of the second					Wget		0.63
 Traffic by Application Risk 	-×						
Risk ▼ Total Byte: Medium 1,671,103, Very Low 5,902,	s (KB) 043.61 307.84	Last updated 8 hours 29	minutes ago		Last updated 8 hour	s 30 minutes ago	

2. **버전** 열을 확인합니다.

ahah cisco	, Firepower Management Center ov Devices / Device Management	verview Analysis	Policies	Devices Objects	AMP		Deploy Q 🌮 🔅	admin 🔻
View B	By: Domain (14) • Error (2) • Warning (0) • Offline (12) • Normal (0)	 Deployme 	nt Pending (7) • Up	grade (0) • Snort 3 (12)		Deploy	ment History
Collaps	so All							
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Group	
	LAB-FPR2K High Availability							×: ^
	fpr2k-1(Primary, Active) Snort 3 192.0.2.140 - Routed	Firepower 2110 with FTD	7.1.0	N/A	Base, Threat (2 more)	LAB-FPR2K-ACL		:
	ftp2k-2(Secondary,Standby) Snort 3 192.0.2.149 - Routed	Firepower 2110 with FTD	7.1.0	N/A	Base, Threat (2 more)	LAB-FPR2K-ACL		:

FMC REST API

FMC REST-API를 통해 FTD 소프트웨어 버전을 확인하려면 다음 단계를 수행하십시오. REST-API 클라이언트를 사용하여 소프트웨어 버전을 확인합니다. 이 예에서는 curl이 사용됩니다.

1. 인증 토큰 요청:

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. 디바이스가 포함된 도메인을 식별합니다. 대부분의 REST API 쿼리에서는 도메인 매개 변수가 필수입니다. 도메인 목록을 검색하려면 이 쿼리에서 X-auth-access-token을 사용합니다.

```
# 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"
        }
    ],
    "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. 도메인 UUID를 사용하여 디바이스 레코드를 쿼리합니다.

```
# 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"
            3.
            "name": "fpr2k-1",
            "type": "Device"
```

4. 도메인 UUID 및 디바이스/컨테이너 UUID를 사용합니다.

```
# 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
                                                              -----\n\nCisco
version
                     : 353\n-----
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:
                       : address is 000f.b748.4801, irq 0\n 3: Ext: Management1/1
Int: Internal-Data0/1
address is 707d.b9e2.836d, irq 0\n 4: Int: Internal-Data1/1
                                                           : address is 0000.0100.0001, irg
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

섹션의 단계를 따릅니다.

FDM REST-API

섹션의 단계를 따릅니다.

FTD 문제 해결 파일

다음 단계에 따라 FTD 트러블슈팅 파일에서 FTD 소프트웨어 버전을 확인합니다.

2. usr-local-sf-bin-sfcli.pl show version.output 파일을 열고 모델이 있는 행을 찾습니다.

<pre># pwd /var/tmp/results-05-06-202 # cat "usr-local-sf-bin-sf</pre>	2199172/dir-archives/etc/sf/
[fpr2 (77) Version 7.1.0 (Build	<pre>k-1] Model : Cisco Firepower 2110 Threat Defense 90)</pre>
UUID LSP version VDB version	: 0bla9c94-8ba8-11ec-b2fd-93263934908d : lsp-rel-20220510-1044 : 354

FCM UI

Firepower 4100/9300에서 FTD의 경우 FCM을 사용하고 Logical Devices 탭에서 Version(버전)을 확인합니다.

O\ Log	erview Inter cal Device List	aces Logical Devices	Security Modules P	latform Settings					System Tools Help admin
Gr	oup By Security M	Iodule 👻							
Se	curity Module	1 (1 Native instance)							0% (0 of 78) Cores Available
	ASA		Standalone	Status:ok					Ø :
	Application	Version	Resource P	rofile	Management IP	Gateway	Management Port	Status	
	ASA	9.16.2.7			10.62.148.240	10.62.148.129	Ethernet1/1	Online	💌 🕅 C 🖄 🐡
Se	curity Module	2 (0 instances)							100% (94 of 94) Cores Available
۲				No logical devices	on this security module.				
Se	curity Module	3 (1 Container instance)							0% (0 of 110) Cores Available
	FTD-MI-1		Standalone	Status:ok					21
	Application	Version	Resource P	rofile	Management IP	Gateway	Management Port	Status	
	FTD	7.1.0.90	RP110		10.62.148.242	10.62.148.129	Ethernet1/1	Online	💌 🕅 C 🖄 🐡
	Interfa Ethe Ethe Port	ce Name smet1/6 smet1/7 -channel1		1 d d	ype ata ata ata	Attribute Cluster FIREPC MGMT- HA-RD UUID	s Operational Status : not-applicable WER-MGMT-IP : 10.62.148.242 URL : https://10.62.148.244 LE : standalone : 3050cf4c-c0aa-11ec-4	9/ 962a-8491ab8d0cc8	

FXOS CLI

Firepower 4100/9300의 FTD

다음 단계에 따라 FXOS CLI에서 FTD 소프트웨어 버전을 확인합니다.

- 1. 섀시에 콘솔 또는 SSH 연결을 설정합니다.
- 2. scope ssa로 전환하고 show app-instance 명령을 실행합니다.

Firepower 1000/2100/3100의 FTD

No

다음 단계에 따라 FXOS CLI에서 FTD 소프트웨어 버전을 확인합니다.

1. 섀시에 대한 콘솔 연결 또는 FTD에 대한 SSH 연결 설정 FTD에 대한 SSH 연결의 경우 FTD CLISH에서 connect fxos 명령을 실행합니다.

> connect fxos

2. scope ssa로 전환하고 show app-instance 명령을 실행합니다.

firepower# scope ssa

firepower /ssa # show app-instance

Applicatio	n Name	Slot ID	Admin State	Operati	onal State	Running Version	n Startup
Version De	ploy Type	Profile Nar	ne Cluster Oper	State C	luster Role		
ftđ		1	Enabled	Online		7.1.0.90	7.1.0.90
Native		Not Ap	plicable	None			

FXOS REST-API

다음 단계에 따라 FXOS REST-API를 통해 FTD 소프트웨어 버전을 확인합니다.

1. 인증 토큰을 요청합니다.

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

2. 이 쿼리에서 토큰을 사용하고 FTD가 설치된 슬롯 ID를 지정합니다.

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
28821660 bc \\ 74e418f \\ 3fadc \\ 443619df \\ 0387d69e7b \\ 150e035f \\ 688bed9d347b \\ 4838 \\ 19469b \\ 19469b \\ 19469b \\ 19460b \\ 1940b \\ 19460b \\ 1940b \\ 1940b
  '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 섀시 show-tech 파일

다음 단계에 따라 FXOS 섀시 show-tech 파일에서 FTD 소프트웨어 버전을 확인합니다.

Firepower 4100/9300의 FTD

1. FXOS 버전 2.7 이상의 경우 **<name>_BC1_all.tar/** FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar에서 sam_techsupportinfo를 엽니다.

이전 버전의 경우 FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar에서 sam_techsupportinfo를 엽니다.

2. 'show slot expand detail' 아래에서 각 슬롯의 섹션을 확인합니다.

Deploy Type: Container

• • •

Firepower 1000/2100/3100의 FTD

- 1. 파일 tech_support_brief를 <name>_FPRM.tar.gz/<name>_FPRM.tar에서 엽니다.
- 2. 'scope ssa' 섹션 및 '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
  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 소프트웨어 버전

ASA 소프트웨어 버전은 다음 옵션을 사용하여 확인할 수 있습니다.

ASA CLI

- ASA SNMP 폴링
- ASA show-tech 파일
- FCM UI
- FXOS CLI
- FXOS REST API
- FXOS 섀시 show-tech 파일

ASA CLI

ASA CLI에서 ASA 소프트웨어 버전을 확인하려면 다음 단계를 수행하십시오.

1. 플랫폼 및 구축 모드에 따라 ASA CLI에 액세스하려면 다음 옵션을 사용합니다.

- 어플라이언스 모드에서 Firepower 1000/3100 및 Firepower 2100에서 ASA에 대한 직접 텔넷 /SSH 액세스
- 플랫폼 모드에서 Firepower 2100의 FXOS 콘솔 CLI에서 액세스하고 **connect asa** 명령을 통해 ASA에 연결
- 명령을 통해 FXOS CLI에서 액세스(Firepower 4100/9300):

connect module <x> [console|telnet](여기서 x는 슬롯 ID입니다)를 연결한 다음 asa를 연결합니다.

- 가상 ASA의 경우 ASA에 대한 직접 SSH 액세스 또는 하이퍼바이저 또는 클라우드 UI에서 콘솔 액세스
- 2. show version 명령을 실행합니다.

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

SNMP를 통해 ASA 소프트웨어 버전을 확인하려면 다음 단계를 수행하십시오.

1. SNMP가 구성 및 활성화되었는지 확인합니다.

2. SNMP 클라이언트를 사용하여 OID SNMPv2-MIB::sysDescr.0 또는 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 파일

```
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

섹션의 단계를 따릅니다..

FXOS CLI

섹션의 단계를 따릅니다.

FXOS REST-API

섹션의 단계를 따릅니다.

FXOS 섀시 show-tech 파일

섹션의 단계를 따릅니다.

Firepower Module 소프트웨어 버전

ASA의 Firepower 모듈은 이전 Sourcefire 모듈 또는 SFR의 새로운 이름입니다.

소프트웨어 버전은 다음 옵션을 사용하여 확인할 수 있습니다.

- FMC UI
- FMC REST-API
- Firepower 모듈 CLI
- Firepower 모듈 문제 해결 파일
- ASA CLI
- ASA show-tech 파일

FMC UI

섹션의 단계를 따릅니다.

FMC REST-API

섹션의 단계를 따릅니다.

Firepower 모듈 CLI

모듈 CLI에서 Firepower 모듈 소프트웨어 버전을 확인하려면 다음 단계를 수행하십시오.

1. SSH를 통해 또는 ASA CLI에서 session sfr 명령을 통해 모듈에 연결합니다.

2. show version 명령을 실행합니다.

> 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 문제 해결 파일

모듈 문제 해결 파일에서 Firepower 모듈 소프트웨어 버전을 확인하려면 다음 단계를 수행하십시오

- 2. usr-local-sf-bin-sfcli.pl show version.output 파일을 열고 모델이 있는 행을 찾습니다.

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				
LSP version	: 2022-05-10-001-vrt				
VDB version	: 354				

ASA CLI

ASA CLI에서 show module sfr details 명령을 실행하고 소프트웨어 버전을 확인합니다.

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 파일

show module sfr detail 문자열로 행을 검색합니다.

----- 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 ASA FirePOWER App. name: 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

Snort, VDB 및 SRU 버전 확인

Deep Packet Inspection Engine(Snort) 버전

Snort 버전은 다음 옵션을 사용하여 확인할 수 있습니다.

- FMC UI
- FMC REST-API
- FDM UI
- FDM REST API
- FTD 또는 Firepower 모듈 CLI
- FTD 또는 Firepower 모듈 문제 해결 파일

FMC UI

다음 단계에 따라 FMC UI에서 FTD Snort 버전을 확인합니다.

1. Devices(**디바이스**) > Device Management(**디바이스 관리)를** 선택합니다.



2. Snort 레이블을 확인합니다.

Firepower Management Center Ce	Overview Analysis	Policies	Devices	Objects	AMP		Deploy Q 🍄 🌣	Ø admin ▼
View By: Domain All (14) Error (2) Warning (0) Offline	(12) • Normal (0)	Deployme	nt Pending (7)	 Upgrad 	le (0) • Snort 3 (12)		Deploym	ent History
Collapse All								
Name	Model	Version	Chassis		Licenses	Access Control Policy	Group	
LAB-FPR2K High Availability								*: ^
fpr2k-1(Primary, Active) Snort 3 192.0.2.140 - Routed	Firepower 2110 with FTD	7.1.0	N/A		Base, Threat (2 more)	LAB-FPR2K-ACL		:
ftp2k-2(Secondary, Standby) Snort 3 192.0.2.149 - Routed	Firepower 2110 with FTD	7.1.0	N/A	I	Base, Threat (2 more)	LAB-FPR2K-ACL		:

FMC REST-API

FMC REST-API를 통해 FTD Snort 버전을 확인하려면 다음 단계를 수행하십시오. REST-API 클라 이언트를 사용하여 소프트웨어 버전을 확인합니다. 이 예에서는 curl이 사용됩니다.

1. 인증 토큰 요청:

```
# 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. 디바이스가 포함된 도메인을 식별합니다. 대부분의 REST API 쿼리에서는 도메인 매개 변수가
필수입니다. 도메인 목록을 검색하려면 이 쿼리에서 X-auth-access-token을 사용합니다.
```

```
# 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
```

```
"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"
    }
],
"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. 도메인 UUID를 사용하여 디바이스 레코드를 쿼리합니다.

}

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/ef0cf3e9-bb07-8f66-5c4e-
00000000001/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/0bla9c94-8ba8-11ec-b2fd-93263934908d"
            },
            "name": "fpr2k-1",
            "type": "Device"
        },
```

4. 이 요청에서 도메인 UUID 및 디바이스/컨테이너 UUID를 사용합니다.

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-accesstoken: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb ' | python -m json.tool | grep -i snort

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

FDM UI

다음 단계에 따라 FDM UI에서 FTD Snort 버전을 확인합니다.

1. 업데이트 페이지로 이동합니다.

CISCO. Firepower Device Manager	Monitoring Policies Objects	Device: KSEC-FPR2100	S → Ø ? ∴ admin Administrator ✓
Model Cisco Firepower 2120 Thr	Software VDB Intrusion Ru eat Defense 7.1.0-90 346.0 20211110-	le Update Cloud Services 1348 Not Registered Register	High Availability High Availability CONFIGURE CONFIGURE
	1/2 Cisco Firepower 2120 Threat Defense		Internet
C Inside Network	NOMT 1/1 1/3 1/5 1/7 1/9	1/11 1/13 1/14 1/15 1/16 1/12 SFP	ISP/WAN/Gateway 💿 NTP Server
	171		
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	pgrade, bgr

2. Snort Inspection Engine 확인

Firepower Device Manager	Monitoring Policies Objects	Device: KSEC-FPR2100
Device Summary Updates		
Geolocation 2020-04-28-002 Latest Update on 05 May 2022	VDB 346.0 Latest Update on 05 May 2022	Security Intelligence Feeds
Configure Set recurring updates	Configure Set recurring updates	Configure Set recurring updates
UPDATE FROM CLOUD	UPDATE FROM CLOUD	
System Upgrade Current version 7.1.0-90		Intrusion Rule 20211110-1348 Latest Update on 05 May 2022
There are no software upgrades available Upload an upgrade file to install.	e on the system.	Configure Set recurring updates Snort UPDATE FROM CLOUD Snort is the main inspection engine in Firepower Threat Defense. It is used for intrusion and file policy analysis, SSL decryption. and Javer 7 Inspection. See more v
		Oue deer proving and regist a mapped and town interest

FDM REST API

다음 단계에 따라 FDM REST-API 요청을 통해 Snort 버전을 확인합니다. REST-API 클라이언트를 사용하여 소프트웨어 버전을 확인합니다. 이 예에서는 curl이 사용됩니다.

1. 인증 토큰 요청:

```
# 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
lyZXNBdCI6MTY1MjI1MjM1NzQ1NywidG9rZW5UeXBIIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC
0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2
VybmFtZSI6ImFkbWluIn0.lJLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI",
```

```
"refresh_expires_in": 2400,
"refresh_token":
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGUONGIxYzQtZDIOMi0xMW
VjLTk4ZWMtYTllOTlkZGMwN2YOIiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIzOTY1NjksImFjY2Vzc1Rva2VuRXhwaX
JlcOFOIjoxNjUyMzk1OTY5MDcwLCJyZWZyZXNoQ291bnQiOi0xLCJ0b2tlblR5cGUiOiJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2
luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
"token_type": "Bearer"
}
2. 이 질의에서 access_token 값을 사용합니다.
```

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIONDU3ODksInN1Yi16ImFkbWluIiwianRpIjoiM2U1Njg0YjYtZDJiYS0xMWV
jLTk4ZWMtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LCJleHAiOjE2NTIONDc1ODksInJlZnJlc2hUb2tlbkV4cGl
yZXNBdCI6MTY1MjQ0ODE4OTMyNSwidG9rZW5UeXB1IjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC0
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 또는 Firepower CLI

"expires_in": 1800,

FTD CLI에서 show snort3 status 명령을 실행합니다.

> show snort3 status Currently running Snort 3 Firepower 모듈은 Snort 2만 지원합니다.

FTD 또는 Firepower 모듈 문제 해결 파일

FTD 문제 해결 파일에서 Snort 버전을 확인하려면 다음 단계를 수행하십시오.

- 2. usr-local-sf-bin-sfcli.pl show snort3.output 파일을 엽니다.

```
# 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 모듈은 Snort 2만 지원합니다.
```

VDB(취약성 데이터베이스) 버전

VDB 버전은 다음 옵션을 사용하여 확인할 수 있습니다.

- FMC UI
- FMC REST-API

- FMC 문제 해결 파일
- FDM UI
- FDM REST API
- FTD CLI
- FTD 또는 Firepower 모듈 문제 해결 파일

FMC UI

다음 단계에 따라 FMC UI에서 VDB 버전을 확인합니다.

1. 도움말 **> 정보를 선택합니다.**

Firepower Management Center Overview / Dashboards / Management	Overview	Analysis	Policies	Devices	Objects	AMP	ntellig	ence		Deploy	۹ 🔮	[™] ‡¶ 🕜 admin v
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 2 A	iecure Firew irepower Mi tartner Ecos sk a Questii AC Support	all on Cisco.com igration Tool ystem on : Cases
Application Statistics (7.1.0) Provides application statistics								admin	No	N	D	C Q 🖉 🗑
Connection Summary Provides tables and charts of the activity on your monitored net	work segment or	ganized by differ	ent criteria					admin	No	N	D	C Q / T
Detailed Dashboard Provides a detailed view of activity on the appliance								admin	No	No	D	C < / 7
Detailed Dashboard (7.0.0) Provides a detailed view of activity on the appliance								admin	No	No	D	C Q / T
Files Dashboard Provides an overview of Malware and File Events								admin	No	N	D	C Q / T
Security Intelligence Statistics Provides Security Intelligence statistics								admin	No	N	D	C < / 7
Summary Dashboard Provides a summary of activity on the appliance								admin	No	Ye	15	Ľ < ∕ ∎

2. VDB 버전 확인:

Firepower Ma	nagement Center	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	۹	¢ 🚱	🕜 admin 🔻
Model Serial Number Software Version OS Snort Version Rule Update Version Rule pack Version Module Pack Version LSP Version Geolocation Update Version VDB Version Hostname	Cisco Firepower Manageme 001234 7.1.0 (build 90) Cisco Firepower Extensible 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: FMC-4600-2	nt Center 4600 Operating System 39:56)	(FX-OS) 2.11	.1 (build154)			For tee or call Copyri	chnical/system question: us at 1-800-553-2447 ight 2004-2021, Cisco a	s, e-mail tac@cisco.com or 1-408-526-7209 nd/or its affiliates. All righ	ts reser	ved.	

FMC CLI

다음 단계에 따라 FMC CLI에서 VDB 버전을 확인합니다.

- 1. SSH 또는 콘솔 연결을 통해 FMC에 액세스합니다.
- 2. **show version** 명령을 실행합니다.

> show version

------[FMC-4600-2.cisco.com]------Model : Cisco Firepower Management Center 4600 (66) Version 7.1.0 (Build 90) UUID : al0ed34e-d127-11e8-b440-728439d95305 Rules update version : 2022-05-02-003-vrt LSP version : lsp-rel-20220502-1613 VDB version : 354

FMC REST-API

FMC REST-API를 통해 VDB 버전을 확인하려면 다음 단계를 수행하십시오. REST-API 클라이언트 를 사용하여 소프트웨어 버전을 확인합니다. 이 예에서는 curl이 사용됩니다.

1. 인증 토큰 요청:

```
# 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. 디바이스가 포함된 도메인을 식별합니다. 대부분의 REST API 쿼리에서는 도메인 매개 변수가
필수입니다. 도메인 목록을 검색하려면 이 쿼리에서 X-auth-access-token을 사용합니다.
```

```
# 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 문제 해결 파일

FMC 문제 해결 파일에서 VDB 버전을 확인하려면 다음 단계를 수행하십시오.

- 1. 문제 해결 파일을 열고 <filename>-troubleshoot .tar/results-<date>---xxxxx/dirarchives/etc/sf/.versiondb 폴더로 이동합니다.
- 2. vdb.conf 파일을 열고 CURRENT_BUILD라는 키가 있는 줄을 찾습니다.

```
# 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

기본 페이지에서 VDB를 **선택합니다**.

CISCO. Firepower Device Manager	Monitoring Policies Objects	Device: KSEC-FPR2100	admin Administrator
Model Cisco Firepower 2120 Thre	Software VDB Intrusion Rule U at Defense 7.1.0-90 346.0 20211110-1348	pdate Cloud Services High Availabil 8 🐼 Not Registered Register Not Configur	ity CONFIGURE
	1/2		Internet
To Inside Network	Cisco Firepower 2120 Threat Defense U 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	1/13 1/14 1/15 1/16 SFP	DNS Server
	1/1		
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
	L		DDNS Service DNS Server

FDM REST API

FDM REST-API 요청을 통해 VDB 버전을 확인하려면 다음 단계를 수행합니다. REST-API 클라이 언트를 사용하여 소프트웨어 버전을 확인합니다. 이 예에서는 curl이 사용됩니다.

1. 인증 토큰 요청:

```
# 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'
ł
"access_token":
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIyNDk5NTcsInN1YiI6ImFkbWluIiwianRpIjoiNDk3MmRjNjAtZDBmMi0xMW "
VjLTk4ZWMtNDdlZTQwODkwMDVjIiwibmJmIjoxNjUyMjQ5OTU3LCJleHAiOjE2NTIyNTE3NTcsInJlZnJlc2hUb2tlbkV4cG
lyZXNBdCI6MTY1MjI1MjM1NzQ1NywidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC
0x \texttt{MWVjLTk4ZWMtZjk4ODexnjnjZWIwIiwidXN1clJvbGUiOiJST0x\texttt{FX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2}{} \\
VybmFtZSI6ImFkbWluIn0.1JLmHddJ2jaVRmpdXF6qg48qdBcyRuit94DLobCJ9LI",
"expires in": 1800,
"refresh_expires_in": 2400,
"refresh_token":
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGU0NGIxYzQtZDI0Mi0xMW
VjLTk4ZWMtYTllOTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIzOTY1NjksImFjY2Vzc1Rva2VuRXhwaX
Jlc0F0IjoxNjUyMzk10TY5MDcwLCJyZWZyZXNoQ291bnQiOi0xLCJ0b2t1blR5cGUiOiJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2
luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
```

```
"token_type": "Bearer"
```

2. 이 질의에서 access_token 값을 사용합니다.

curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIONDU3ODksInN1YiI6ImFkbWluIiwianRpIjoiM2U1Njg0YjYtZDJiYS0xMWV jLTk4ZWMtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LCJleHAiOjE2NTIONDc1ODksInJlZnJlc2hUb2tlbkV4cGl yZXNBdCI6MTY1MjQ0ODE4OTMyNSwidG9rZW5UeXB1IjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTU3ZGVmMjgtY2M3MC0 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 또는 Firepower 모듈 CLI

다음 단계에 따라 FTD CLI 또는 Firepower module (SFR) CLI에서 VDB 버전을 확인합니다.

- 1. SSH 또는 콘솔 연결을 통해 FTD에 액세스합니다. Firepower 모듈의 경우 SSH를 통해 또는 ASA CLI에서 session sfr 명령을 통해 모듈에 **액세스합니다**.
- 2. CLI에서 show version 명령을 실행합니다.

> 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 또는 Firepower 모듈 문제 해결 파일

다음 단계에 따라 FTD 또는 Firepower 모듈 문제 해결 파일의 VDB 버전을 확인합니다.

- 2. usr-local-sf-bin-sfcli.pl show version.output 파일을 열고 VDB 버전의 행을 찾습니다.

# pwd	
/var/tmp/results-05-	06-2022163203/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	: 0bla9c94-8ba8-11ec-b2fd-93263934908d
LSP version	: lsp-rel-20220510-1044

pwd

침입 규칙 업데이트 버전

침입 규칙 업데이트는 새로운/업데이트된 침입 규칙 및 프리프로세서 규칙, 설치된 규칙에 대한 수 정된 상태, 수정된 기본 침입 정책 설정을 제공합니다.

보안 규칙 업데이트(SRU)는 Snort 버전 2에 적용되며 LSP(Lightweight Security Package) 업데이 트는 Snort 버전 3에 적용됩니다.

SRU/LSP 소프트웨어 버전은 다음 옵션을 사용하여 확인할 수 있습니다.

- FMC UI
- FMC REST-API
- FMC 문제 해결 파일
- FDM UI
- FDM REST API
- FTD 또는 Firepower 모듈 CLI
- FTD 또는 Firepower 모듈 문제 해결 파일

FMC UI

FMC UI에서 SRU/LSP 버전을 확인하려면 다음 단계를 수행하십시오.

	1. 도움말 > 정보를 선 택	백합니디	ł.									
ciju Cis	 Firepower Management Center Overview / Dashboards / Management 	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence		Deploy	۹	🚰 🏹 👩 admin 🔻
Ni Ai Pr Aj	me cess Controlled User Statistics ovides traffic and intrusion event statistics by user plication Statistics ovides traffic and intrusion event statistics by application							Page-leve How-Tos Document What's Ne Software I Secure Fir	Help ation on Cisco.co w in This Release Download swall YouTube	m i 2[Secure Fi Firepower Partner Er Ask a Qu TAC Sup; About	rewall on Cisco.com r Migration Tool cosystem estion Joort Cases
A Pr	plication Statistics (7.1.0) wides application statistics							admir	No	N	ю	C < / 7
Pr	nnection Summary ovides tables and charts of the activity on your monitored net	twork segment or	ganized by differ	ent criteria				admir	No	N	ю	C < ≠ ₹
D	tailed Dashboard ovides a detailed view of activity on the appliance							admir	No	N	ю	1ª Q 🖉 🗑
D	tailed Dashboard (7.0.0) ovides a detailed view of activity on the appliance							admir	No	N	ю	1ª Q 🖉 🗑
Fi	es Dashboard ovides an overview of Malware and File Events							admir	No	N	lo	C < / 7
Si Pr	curity Intelligence Statistics ovides Security Intelligence statistics							admir	No	N	lo	Ľ < ≠ ₹
Si Pr	mmary Dashboard ovides a summary of activity on the appliance							admir	No	Y	'es	C < / 7

2. 규칙 **업데이트 버전** 및 **LSP 버전** 확인

Firepower Ma	nagement Center o	overview Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	۹	¢ 😜	🕜 admin 🔻
Model Serial Number Software Version OS Snort Version Rule Update Version Rulepack Version Module Pack Version LSP Version Geolocation Update Version VDB Version Hostname	Cisco Firepower Management Co 001234 7.1.0 (build 90) Cisco Firepower Extensible Oper 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 19:39:5) FMC-4600-2	Center 4600 Irating System (FX-OS) 2.1	1.1 (build154)			For tec or call Copyri	hnical/system questio us at 1-800-553-244 ght 2004-2021, Cisco	ns, e-mail tac@cisco.com 7 or 1-408-526-7209 and/or its affiliates. All right	: reserv	ved.	

FMC CLI

FMC CLI에서 SRU/LSP 버전을 확인하려면 다음 단계를 수행하십시오.

- 1. SSH 또는 콘솔 연결을 통해 FMC에 액세스합니다.
- 2. CLI에서 show version 명령을 실행합니다.

```
> show version
```

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

FMC REST-API

REST-API 요청을 통해 소프트웨어 버전을 확인하려면 다음 단계를 수행하십시오. REST-API 클라 이언트를 사용하여 소프트웨어 버전을 확인합니다. 이 예에서는 curl이 사용됩니다.

1. 인증 토큰 요청:

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. 이 쿼리에서 X-auth-access-token을 사용합니다.

```
"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 문제 해결 파일

FMC 트러블슈팅 파일에서 SRU 버전을 확인하려면 다음 단계를 수행하십시오.

1. 문제 해결 파일을 열고 폴더 <filename>.tar/results-<date>---xxxxxx/dir-archives/etc/sf/

2. sru_versions.conf 파일을 열고 Intrusion_Rules_Update 키가 있는 행을 찾습니다.

```
      # 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

      FMC 문제 해결 파일에서 LSP 버전을 확인하려면 다음 단계를 수행하십시오.
```

- 1. 문제 해결 파일을 열고 폴더 <filename>.tar/results-<date>---xxxxxx/command-outputs로 이동 합니다.
- 2. 파일을 **열고 var-sf-lsp -maxdepth 2 -ls.output**을 찾은 다음 /var/sf/lsp/active-lsp로 **줄을 확인합** 니다.

```
# 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
                                                      4096 May 11 04:01 /var/sf/lsp
                                         root
              0 lrwxrwxrwx 1 root
                                                        33 May 11 04:00 /var/sf/lsp/installed-
19142268
                                         root
lsp -> /var/sf/lsp/lsp-rel-20220510-1044
19138299
              4 drwxrwxr-x
                            5 www
                                                      4096 May 11 04:01 /var/sf/lsp/lsp-rel-
                                         root
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
              4 drwxrwxr-x
                            5 www
                                                      4096 May 11 04:00 /var/sf/lsp/lsp-rel-
19142234
                                         root
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
                            б www
                                                      4096 May 10 14:51 /var/sf/lsp/lsp-rel-
                                         root
20220510-1044/talos_content
19142269 46640 -rw-r--r-- 1 root
                                                  47759360 May 11 04:01 /var/sf/lsp/lsp-rel-
                                         root
```

-> /var/sf/	lsp/lsp-rel-202205	510-	1044						
19142270	0 lrwxrwxrwx	1	root	root	33	May	11	04:01	/var/sf/lsp/active-lsp
all-1644636	642.log								
19139198	260 -rw-rr	1	root	root	264403	Feb	12	03:32	/var/sf/lsp/pigtail-
20220510-10	44/lspd_ver.proper	rtie	S						
19142265	4 -rwxrwxr-x	1	www	root	26	May	10	14:51	/var/sf/lsp/lsp-rel-
20220510-10	44/.snort-versions	3							
19142267	4 -rwxrwxr-x	1	WWW	root	238	May	11	04:00	/var/sf/lsp/lsp-rel-
20220510-10	44/lsp-rel-2022051	L0-1	044.ta	r.xz.REL.tar					

FDM UI

기본 페이지에서 Intrusion Rule Update를 선택합니다.



FDM REST API

FDM REST-API 요청을 통해 VDB 버전을 확인하려면 다음 단계를 수행합니다. REST-API 클라이 언트를 사용하여 소프트웨어 버전을 확인합니다. 이 예에서는 **curl**이 사용됩니다.

1. 인증 토큰 요청:

```
# 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
Jlc0F0IjoxNjUyMzk10TY5MDcwLCJyZWZyZXNoQ291bnQi0i0xLCJ0b2tlblR5cGUi0iJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2
luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
```

```
"token_type": "Bearer"
}
2. 이 질의에서 access_token 값을 사용합니다.
```

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIONDU3ODksInN1Yi16ImFkbWluIiwianRpIjoiM2U1NjgOYjYtZDJiYSOxMWV
jLTk4ZWMtZGI2YjRiYTM1MTU2IiwibmJmIjoxNjUyNDQ1Nzg5LCJleHAiOjE2NTIONDc1ODksInJlZnJlc2hUb2tlbkV4cGl
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 또는 Firepower 모듈 CLI

다음 단계에 따라 FTD CLI 또는 Firepower 모듈 CLI에서 SRU/LSP 버전을 확인합니다.

- 1. SSH 또는 콘솔 연결을 통해 FTD에 액세스합니다. Firepower 모듈의 경우 SSH를 통해 또는 ASA CLI에서 session sfr 명령을 통해 모듈에 **액세스합니다**.
- 2. CLI에서 show version 명령을 실행합니다.

> show version										
[FIREPOWER	(1.cisco.com]									
Model	: Cisco Firepower 2120 Threat Defense (77) Version 7.1.0 (Build									
UUID	: 1cbe9952-cc6f-11ec-b63a-ae4636e42209									
LSP version	: lsp-rel-20211110-1348									
VDB version	: 346									
or										
> snow version										
[FIREPOWER	(1.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									
	·									
<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									

참고: "show version" 명령은 Snort 2를 사용하는 경우 SRU 업데이트 버전을 표시합니다. Snort 3 LSP 버전의 경우 표시됩니다.

FTD 또는 Firepower 모듈 문제 해결 파일

FTD 또는 Firepower 모듈 문제 해결 파일에서 SRU/LSP 버전을 확인하려면 다음 단계를 수행하십 시오.

- 2. usr-local-sf-bin-sfcli.pl show version.output 파일을 열고 SRU/LSP 버전의 행을 찾습니다.

# pwd	
/var/tmp/results-0	5-06-2022163203/command-outputs/
<pre># cat "usr-local-s</pre>	E-bin-sfcli.pl show version.output"
[FIRE:	POWER1.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
VDB version	: 346

or

pwd

/var/tmp/results-05-06-2022163203/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

알려진 문제

Cisco 버그 ID CSCwb34098 ENH: 'show managers' 명령 출력에 FMC 버전 표시

Cisco 버그 ID CSCve13470 ENH: FirePOWER 6.x에서 소프트웨어 관련 OID 활성화

Cisco 버그 ID <u>CSCwb85969</u> ENH: 문제 해결 파일에 "show version" FMC CLISH 명령의 출력 포함

Cisco 버그 ID <u>CSCvu15709</u> ENH: Firepower 플랫폼에서 SRU/VDB/GEO 위치 버전을 폴링하기 위한 SNMP OID 지원

관련 정보

- <u>Secure Firewall Management Center REST API 빠른 시작 가이드, 버전 7.1</u>
- <u>Firepower NGFW 어플라이언스에서 SNMP 구성</u>
- <u>Cisco Firepower Threat Defense REST API 가이드</u>
- <u>Cisco FXOS REST API 참조</u>
- <u>Cisco ASA 호환성</u>
- <u>Firepower 1000/2100 및 Secure Firewall 3100 ASA 및 FXOS 번들 버전</u>
- <u>번들 구성 요소</u>
- <u>Firepower Troubleshoot 파일 생성 절차</u>