FXOS CLI를 통한 SFTD/ASA 인스턴스의 비밀번호 복구

목차

소개

이 문서에서는 FXOS CLI를 통해 SFTD 또는 ASA 인스턴스의 비밀번호를 복구하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

FP41XX 또는 FP93XX Secure Firewall Series를 통한 SFTD 또는 ASA 인스턴스

Cisco에서는 다음 항목에 대해 알고 있는 것이 좋습니다.

- Cisco FXOS(Firepower eXtensible 운영 체제) CLI(Command Line Interface)

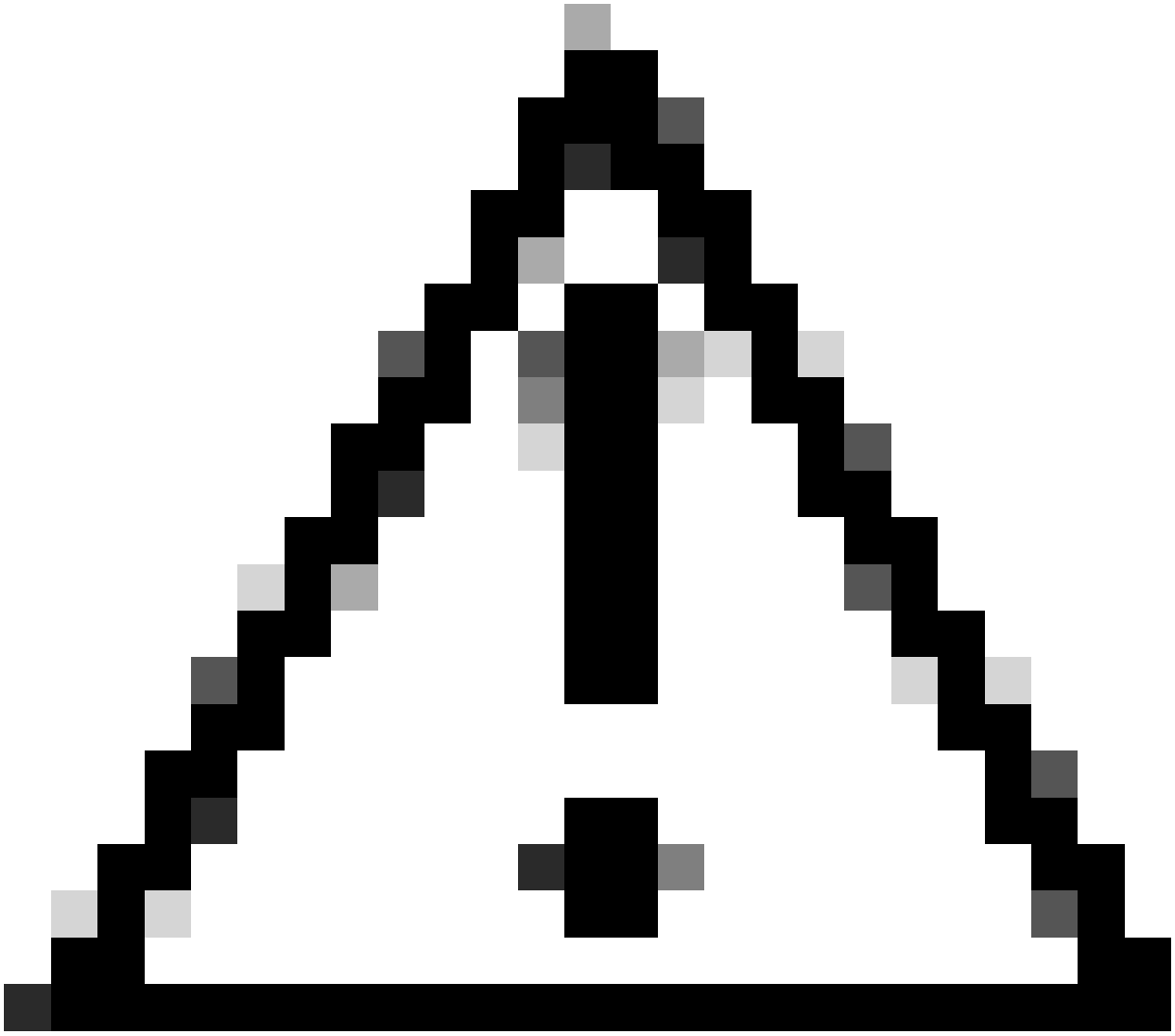
사용되는 구성 요소

- Cisco 보안 방화벽 4110
- Cisco Secure Firewall ASA 소프트웨어

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

디바이스의 비밀번호가 손실되어 복구해야 하는 경우가 있으며 FXOS Firepower 섀시 관리자를 사용할 수 없습니다. FP41XX 또는 FP93XX Secure Firewall Series를 사용하는 SFTD 또는 ASA 인스턴스의 경우 FXOS CLI를 통해 비밀번호 복구를 수행할 수 있습니다.



주의: 이 프로세스에서는 인스턴스를 재부팅해야 하므로 트래픽이 중단될 수 있습니다.

구성

절차

1단계. 관리자 권한 자격 증명을 사용하여 FXOS CLI에 로그인합니다.

2단계. 애플리케이션 이름, 식별자 및 슬롯 ID 정보를 가져옵니다.

스코페사

앱 인스턴스 표시

예:

<#root>

```
FPR4110-K9-1# scope ssa
FPR4110-K9-1 /ssa # show app-instance

App Name Identifier Slot ID

Admin State Oper State   Running Version Startup Version Deploy Type Turbo Mode Profile Name Cluster St
-------- ---------- ------- ----------- -----------  --------------- --------------- ----------- ------

asa      ASA        1

Enabled     Online       9.16.3(14)       9.16.3(14)       Native      No                          Not Appl
```

3단계. 새 admin 및 enable 비밀번호를 지정한 다음 변경 사항을 저장합니다.

범위 논리 장치 식별자

범위 관리 부트스트랩 app_name

범위 부트스트랩 키 암호

설정값

값 입력: password

값 확인: password

커밋 버퍼

종료

종료

예:

```
FPR4110-K9-1 /ssa # scope logical-device ASA
FPR4110-K9-1 /ssa/logical-device # scope mgmt-bootstrap asa
FPR4110-K9-1 /ssa/logical-device/mgmt-bootstrap # scope bootstrap-key-secret PASSWORD
FPR4110-K9-1 /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret # set value

Enter value:

Confirm the value:
Warning: Bootstrap changes are not automatically applied to app-instances. To apply the changes, please
FPR4110-K9-1 /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* #commit-buffer
FPR4110-K9-1 /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret # exit
FPR4110-K9-1 /ssa/logical-device/mgmt-bootstrap # exit
```

4단계. 관리 부트스트랩을 지운 다음 변경 사항을 저장합니다.

scope slot slot_id

범위 app-instance app_name 식별자

clear-mgmt-bootstrap

커밋 버퍼

예:

```
FPR4110-K9-1 /ssa # scope slot 1
FPR4110-K9-1 /ssa/slot # scope app-instance asa ASA
FPR4110-K9-1 /ssa/slot/app-instance # clear-mgmt-bootstrap
Warning: Clears the application management bootstrap. Application needs to be restarted for this action
FPR4110-K9-1 /ssa/slot/app-instance* # commit-buffer
```

5단계. 인스턴스를 다시 시작합니다.

재시작

커밋 버퍼

예:

```
FPR4110-K9-1 /ssa/slot/app-instance # restart
FPR4110-K9-1 /ssa/slot/app-instance* # commit-buffer
```

참고: 변경 사항이 저장되면 인스턴스가 다시 시작됩니다.

6단계. 새 자격 증명을 사용하여 SSH를 통해 SFTD/ASA 인스턴스에 로그인합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.