

소프트웨어 업그레이드 후 ASA/FTD 장애 조치 유닛 간의 일관성 없는 LINA 호스트 이름 동기화 문제 해결

문제

고가용성(HA) 컨피그레이션의 FTD(Secure Firewall Threat Defense)에서 소프트웨어를 업그레이드한 후 다음 증상이 관찰됩니다.

1. Lina 호스트 이름이 configure network hostname CLISH 명령을 사용하여 이전에 구성한 expert 모드 호스트 이름과 일치하지 않습니다. 이 문서에서 시스템 호스트 이름을 Lina 호스트 이름은 피어의 시스템 호스트 이름과 일치합니다. 이 예에서 시스템 호스트 이름이 FPR1100-2인 유닛은 FPR1100-1을 Lina 호스트 이름으로 가집니다.

```
<#root>
```

```
>
```

```
show network
```

```
=====[ System Information ]=====
```

```
Hostname                : FPR1100-2      <----- system hostname
```

```
Domains                  : example.net
```

```
...
```

```
>
```

```
show running-config hostname
```

```
hostname FPR1100-1 <--- Lina hostname is different than the system hostname
```

피어 장치:

```
<#root>
```

```
>
```

```
show network
```

```
=====[ System Information ]====
Hostname           : FPR1100-1           <----- system hostname
Domains           : example.net
...
>
```

```
show running-config hostname
hostname FPR1100-1      <--- Lina hostname
```

2. 이전 예에 따라 유닛의 업그레이드 전 상태에 따라 Lina 호스트 이름이 다음과 같이 변경됩니다.

2.1 - 시나리오 1

- 업그레이드 전 상태: 시스템 호스트 이름이 FPR1100-1인 유닛은 기본/액티브, FPR1100-2는 보조/스탠바이입니다.
- 업그레이드 후 상태: 두 유닛의 Lina 호스트 이름은 FPR1100-1입니다.

2.2 - 시나리오 2

- 업그레이드 전 상태: 시스템 호스트 이름이 FPR1100-1인 유닛은 기본/대기, FPR1100-2는 보조/활성
- 업그레이드 후 상태: 두 유닛의 Lina 호스트 이름은 FPR1100-2입니다.

또한 SNMP(Simple Network Monitoring Protocol) Object Identifier.1.3.6.1.2.1.1.5.0을 사용하여 각 HA 피어의 호스트 이름을 폴링하면 동일한 값이 반환됩니다.

예를 들면 다음과 같습니다.

```
<#root>
```

```
#
```

```
snmpget -On -v2c -c cisco 192.0.2.1 .1.3.6.1.2.1.1.5.0
```

```
.1.3.6.1.2.1.1.5.0 = STRING:
```

```
FPR1100-1
```

```
<#root>
```

```
#
```

```
snmpget -On -v2c -c cisco 192.0.2.2 .1.3.6.1.2.1.1.5.0
```

```
.1.3.6.1.2.1.1.5.0 = STRING:
```

```
FPR1100-1
```

환경

- HA에서 FTD를 실행하는 FMC 관리 Firepower 4112입니다. 다른 하드웨어 플랫폼도 영향을 받습니다.
- 버전 7.6.2.1에서 7.6.4로 소프트웨어를 업그레이드한 후 처음 확인되었습니다. 다른 버전도 영향을 받을 수 있습니다.
- HA의 FTD 피어는 CLISH `configure network hostname` 명령을 사용하여 사용자 지정 및 다른 시스템 호스트 이름으로 구성됩니다.

해결

증상이 재현되고 Cisco 버그 ID CSCwt25171에 문서화됩니다.

Lina 호스트 이름을 `show network` 명령 출력에서 호스트 이름과 동기화된 상태로 유지하려는 경우, 두 가지 알려진 해결 옵션이 있습니다.

1. 영향을 받는 피어에서 `configure network hostname` 명령을 사용하여 원하는 호스트 이름을 다시 구성합니다. 이 명령은 시스템 호스트 이름을 구성하고 Lina 호스트 이름을 업데이트합니다.
2. 영향을 받는 유닛을 재부팅합니다. 환경, 구성 및 트래픽 흐름 재부팅 작업에 따라 업무 시간 중에 위험하고 영향을 받을 수 있습니다. 사용자 재량이 권장됩니다.

원인

Cisco 버그 ID CSCwt25171에 문서화된 증상

관련 콘텐츠

다음은 고가용성 컨피그레이션에서 Secure Firewall ASA 및 FTD를 사용한 재생에서 얻은 추가 결과입니다.

ASA

다음 ASA 예외 중 하나가 발생하지 않는 한 Lina 호스트 이름은 액티브 유닛에서 스탠바이 유닛으로 동기화되지 않습니다.

1. 독립형 유닛(처음에 독립형 또는 HA 중단 후)에서 방화벽 모드가 변경된 경우 다른 호스트 이름이 구성되고 장애 조치가 구성됩니다. 로깅이 활성화된 경우 호스트 이름이 다르더라도 스탠바이 유닛에서는 구성 일치를 보고합니다.

```
<#root>
```

```
ASA2# .  
Detected an Active mate Secondary:  
Switching to Ok for reason Detected an Active peer.
```

```
Configuration on Active and Standby is matching. <-----
```

2. #1 변경 후 no failover 명령을 사용하여 장애 조치가 일시 중단되고 failover 명령을 사용하여 다시 시작됩니다.

ASA 예외

Lina 호스트 이름은 다음 중 하나라도 true이면 동기화됩니다.

1. #1의 경우 장치 구성 간의 차이가 호스트 이름이 아닙니다. 즉, 호스트 이름과 함께 다른 차이점이 있으면 전체 동기화가 시작되어 호스트 이름 동기화가 수행됩니다.

2. 대기 ASA가 업그레이드되거나 재부팅됩니다.

3. 스탠바이 유닛에서 장애 조치가 일시 중지되고(장애 조치 없음), 액티브에서 변경한 일부 내용이 동기화되며, 스탠바이(장애 조치)에서 장애 조치가 다시 시작됩니다(장애 조치). 변경 사항으로 인해 전체 구성 동기화가 수행됩니다.

FTD

다음 중 하나라도 참일 경우 호스트 이름은 활성 유닛에서 대기 유닛으로 동기화되지 않지만 다음 FTD 예외 중 하나가 발생하지 않을 경우 동기화됩니다.

1. FTD는 장애 조치 컨피그레이션이며 스탠바이 유닛에서 사용자가 CLISH 명령 `configure network hostname`을 사용하여 다른 호스트 이름을 구성합니다.
2. 초기 부트스트랩된 독립형 유닛이 CLISH 명령 `configure network hostname`을 사용하여 다른 호스트 이름으로 구성된 경우.
3. 독립형 유닛(처음에 독립형 또는 장애 조치 종료 후)에서 방화벽 모드가 변경된 경우 CLISH `configure network hostname` 명령을 사용하여 다른 호스트 이름을 구성하고 장애 조치를 구성합니다.
4. #1-3 변경 후 HA가 일시 중지되고 다시 시작되거나 대기 유닛이 재부팅되거나 대기 유닛이 패치 또는 주 버전으로 업그레이드되면 동기화가 발생합니다(가상 FTD만 해당).

FTD 예외

다음 중 하나라도 true이면 호스트 이름이 동기화됩니다.

1. #3의 경우 장치 구성 간의 차이가 호스트 이름 이외입니다. 즉, 호스트 이름과 함께 다른 차이점이 있으면 전체 동기화가 시작되어 호스트 이름 동기화가 수행됩니다.
2. 스탠바이 유닛이 주 버전으로 업그레이드됩니다(가상 FTD는 제외하고, 가상 FTD의 호스트 이름에서 주 버전으로 업그레이드하더라도 동기화되지 않음).
3. HA가 일시 중단되고, 액티브 유닛에서 구성이 변경(예: 정책 배포를 통해)되고 장애 조치가 다시 시작됩니다. 이 경우 유닛 간의 구성 차이로 인해 호스트 이름을 포함하여 액티브 유닛에서 스탠바이 유닛으로의 전체 복제가 수행되고 호스트 이름을 동기화합니다.

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.