HEX 접두사 처리로 인해 ISE 3.4에서 NTP 인증 실패 구성

목차

문제

Cisco ISE(Identity Services Engine) 3.4.0.608 패치 1은 길이가 40자인 SHA1 키로 인증된 NTP를 사용할 때 NTP 서버와 동기화하지 못합니다. NTP authentication key 명령은 오류 없이 CLI에서 수락되지만, 인증이 활성화된 경우 NTP 동기화가 발생하지 않습니다. 인증이 없으면 NTP 동기화가 올바르게 작동합니다. Cisco 스위치를 비롯한 다른 네트워크 디바이스는 동일한 키 ID 및 키 값을 사용하여 동일한 NTP 서버로 성공적으로 인증됩니다.

트러블슈팅 중에 패킷 캡처 분석 결과 ISE가 적절한 키 ID 및 MAC/인증자 필드가 포함된 인증된 NTP 요청을 전송하지만, 서버 회신에 모든 0의 키 ID가 포함되고 MAC/인증자가 없으므로 ISE가 인증을 거부합니다. NTP 서버로 작동하는 Cisco 스위치의 디버그 출력이 "SHA1-Match: 인증 실패를 나타내는 0".

환경

- Cisco ISE(Identity Services Engine) 버전 3.4.0.608(패치 1 포함)
- SHA1 알고리즘을 사용하는 NTP 인증
- 40자의 NTP 인증 키
- 버전 17.12.04를 실행하는 Cisco Catalyst 9500 스위치(C9500-24Y4C)
- 인증된 NTP 컨피그레이션이 있는 NTP 서버 어플라이언스

해결

이 문제는 Cisco 버그 ID로 인해 발생합니다. HEX 접두사가 필요한 경우 ISE가 긴 NTP 인증 키를 처리하는 방식에 영향을 주는 CSCwq79772. 이 버그는 ISE 3.4 패치 8 및 ISE 3.5 패치 3에서 수정되었습니다.

근본 원인 이해

Cisco 디바이스에서 NTP 인증 키를 구성할 때 20자 이상의 키는 일반 텍스트가 아닌 16진수 문자열로 자동 처리됩니다. 이를 위해서는 키를 구성할 때 ISE에서 "HEX:" 접두사를 사용해야 합니다. 그러나 버그로 인해 ISE는 추가 "HEX:" 접두사 처리 때문에 40자 키의 36자만 허용하므로 인증 실패가 발생합니다.

즉각적인 해결 옵션

ISE 소프트웨어를 수정 사항이 포함된 버전으로 업그레이드할 수 있을 때까지 다음 해결 방법 중 하나를 사용합니다.

옵션 1: 36자 SHA1 키 사용

40자 키 대신 36자 SHA1 키로 NTP 서버와 ISE를 모두 구성합니다.

ISE의 경우:

```
ntp authentication-key 1 sha1 plain HEX:1d3f35b762ab7c21e5f1265dc9762fe421fa
```

NTP 서버(Cisco 스위치 예)에서 다음을 수행합니다.

```
ntp authentication-key 1 sha1 1d3f35b762ab7c21e5f1265dc9762fe421fa
ntp authenticate
ntp trusted-key 1
```

옵션 2: MD5 인증 사용

동일한 길이 제한을 나타내지 않는 SHA1에서 MD5 인증으로 전환합니다.

ISE의 경우:

```
ntp authentication-key 1 md5 plain [MD5-key-value]
ntp server [NTP-server-IP] key 1
```

NTP 서버에서 다음을 수행합니다.

```
ntp authentication-key 1 md5 [MD5-key-value]
ntp authenticate
ntp trusted-key 1
```

확인 단계

두 가지 해결 방법 중 하나를 구현한 후 NTP 동기화를 확인합니다.

ISE의 경우:

```
show ntp
show clock
```

스위치에서(스위치를 NTP 서버로 사용하는 경우):

```
show ntp associations
show ntp status
```

성공적인 동기화 표시기를 찾고 한 쪽에서 인증이 비활성화되었지만 다른 쪽에서 활성화된 경우 NTP 동기화가 실패했는지 확인하여 인증이 작동하고 있는지 확인합니다.

영구적 해결

ISE를 Cisco 버그 ID에 대한 수정 사항이 포함된 다음 버전 중 하나로 업그레이드합니다.

CSCwq79772:

- ISE 3.4 패치 8(사용 가능한 경우)
- ISE 3.5 패치 3 이상

업그레이드 후에는 원래 40자 SHA1 키 컨피그레이션이 HEX 접두사와 함께 올바르게 작동합니다.

원인

이 문제는 Cisco 버그 ID로 인해 발생합니다. CSCwq79772, 3.4 Patch 8 및 3.5 Patch 3 이전 ISE 버전. NTP 인증 키가 20자 이상인 경우 Cisco 디바이스는 이를 16진수 문자열로 취급하며 컨피그레이션에 "HEX:" 접두사가 필요합니다. 이 버그로 인해 ISE는 HEX 접두사가 사용될 때 40자 키의 36자만 허용하는 키 길이 계산을 잘못 처리합니다. 이로 인해 ISE와 NTP 서버 간에 키 불일치가 발생하여 NTP 동기화 시도 중에 인증이 실패합니다.

관련 콘텐츠

- Cisco 버그 CSCwq79772
- Cisco Wireless Controller 명령 참조 - NTP 인증
- Cisco 기술 지원 및 다운로드

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.