

ISE SFTP RSA 키 인증 시간 초과 오류

목차

문제

RSA 키 인증으로 구성된 SFTP 리포지토리는 한 ISE 노드(ise1)에서 성공적으로 작동하지만 ISE 3.4를 실행하는 다른 ISE 노드(ise2)에서는 실패합니다. 오류가 발생한 노드에서 SSH 핸드셰이크 및 서버 검증은 성공적으로 완료되지만 공개 키 인증이 완료되지 않고 SFTP 세션이 "sftp_select 오류: 시간 초과!" 오류 메시지가 표시됩니다.

영향을 받는 ISE 노드에서 show repository SFTP 명령을 사용하여 SFTP 리포지토리 콘텐츠를 나열하려고 하면 다음 오류 시퀀스가 발생합니다.

```
device/admin# show repository SFTP
6 [4005534]:[info] transfer: cars_xfer.c[333] [system]: sftp dir of repository SFTP requested
6 [4005534]:[info] transfer: cars_xfer_util.c[2654] [system]: Server validation successful 10.50.60.200
7 [4005534]:[debug] transfer: sftp_handler.c[1295] [system]: Running sftp command: 10.50.60.200 will.ki
6 [4005534]:[info] transfer: sftp_handler.c[695] [system]: DEBUG: local user: admin UID: 0 sftp_run_par
7 [4005534]:[debug] transfer: sftp_handler.c[705] [system]: fd is:7
7 [4005535]:[debug] transfer: sftp_handler.c[327] [system]: Executing SFTP command: 0 admin /usr/bin/sf
3 [4005534]:[error] transfer: sftp_handler.c[417] [system]: sftp_select Error: timeout!
7 [4005534]:[debug] transfer: sftp_handler.c[1136] [system]: sftp parent status -999
% Failure occurred during request
```

이렇게 하면 백업 작업과 같은 중요한 ISE 기능에 영향을 받는 ISE 노드에서 SFTP 리포지토리를 사용할 수 없게 됩니다.

환경

- Cisco ISE(Identity Services Engine) 버전 3.4.0
- 최소 2개의 노드가 있는 다중 노드 ISE 구축(ise1 및 ise2)
- RSA 키 인증으로 구성된 SFTP 저장소

- RSA 개인 키를 사용하는 SSH 키 기반 인증(/home/admin/.ssh/id_rsa)
- SFTP 서버 액세스 가능
- 비밀번호 인증이 비활성화되었습니다(-oPasswordAuthentication=no).

해결

이 사건은 현재 엔지니어링팀에서 조사 중입니다. 영향받는 ISE 노드에서 SFTP 시간 초과의 기본 원인을 확인하기 위해 루트 로그 분석을 위해 문제가 에스컬레이션되었습니다.

디버그 출력을 기반으로 다음 섹션에 설명된 트러블슈팅 단계를 수행하여 추가 정보를 수집합니다.

1단계: 노드 간의 SFTP 저장소 구성 일관성 확인

두 ISE 노드의 SFTP 리포지토리 컨피그레이션을 비교하여 동일한지 확인합니다.

2단계: SSH 키 파일 권한 및 소유권 확인

SSH 개인 키 파일(/home/admin/.ssh/id_rsa)에 영향을 받는 노드에 대한 올바른 권한 및 소유권이 있는지 확인합니다.

3단계: 네트워크 연결 테스트

영향을 받는 ISE 노드가 포트 22의 SFTP 서버에 연결할 수 있고 네트워크 레벨 차단 문제가 없는지 확인합니다.

4단계: 추가 디버깅 사용

인증 실패에 대한 자세한 정보를 캡처하려면 더 자세한 SSH/SFTP 디버깅을 활성화합니다.

영향을 받는 노드 CLI에서 다음을 수행합니다.

1.- 다음 명령을 사용하여 이러한 디버그를 활성화합니다.

- 디버그 복사본 7
- 전송 디버그 7

2.- 디버그를 활성화한 후 `show repository xxxxx` 명령을 사용하여 추가 정보를 캡처합니다.

5단계: SSH 키 핑거프린트 비교

SFTP 서버의 SSH 공개 키가 영향받는 ISE 노드에서 사용 중인 개인 키와 일치하는지 확인합니다.

SPAN 노드에서 RSA 키를 생성하는 데 사용된 올바른 패스프레이즈를 식별하고 유효한 자격 증명과 일치하도록 저장소 설정을 다시 구성함으로써 문제가 해결되었습니다.

임시 해결 방법

CLI에서 `ssh-keygen -y -f /home/admin/.ssh/id_rsa`를 사용하여 비밀번호를 수동으로 확인하여 어떤 비밀번호가 성공적으로 개인 키의 잠금을 해제했는지 확인한 다음 GUI에서 리포지토리 컨피그레이션을 다시 적용하는 것이 좋습니다.

RSA 키를 다시 생성하는 단계:

1.- 영향을 받는 노드 CLI를 엽니다.

2.- `crypto key delete rsa` 명령으로 이전 RSA 키를 삭제합니다.

3.- `crypto key generate rsa passphrase XXXXXXXXXXXXXXX` 명령을 사용하여 원하는 패스프레이즈를 사용하여 새 RSA 키를 생성합니다.



참고: 암호는 13자 이상이어야 합니다.

4.- show crypto key 명령을 사용하여 다른 시스템으로 가져올 새 RSA 공개 키를 가져옵니다.

원인

사용자 오류/구성 오류입니다. 조사 결과 보조 노드의 저장소 인증 실패가 예상 패스프레이즈와 저장된 RSA 개인 키를 보호하는 데 사용된 패스프레이즈가 일치하지 않아 발생한 것으로 확인되었습니다. 이로 인해 암호화 하위 시스템이 SSH 인증 챌린지에 서명하기 위해 키의 암호를 해독하지 못했습니다.

관련 콘텐츠

- [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.