

AWS용 Splunk 추가 기능 - 암호 해독 실패

적용 가능성

Splunk Apps 추가 기능

설명

환경:

Splunk Deployment Server(DS)를 사용하여 AWS용 Splunk-Add-on을 AWS 로그 파일 수집을 위해 구성된 Splunk Heavy Forwarder(HF)에 푸시합니다.

문제:

AWS 로그가 계속 수집되었습니다.

조사

HF 인스턴스의 로그 파일에서 다음 오류 메시지가 발견되었습니다.

splunkd.log:

```
07-03-2019 13:28:35.327 -0600 ERROR Crypto - Decryption operation failed: AES-GCM Decryp
07-03-2019 13:28:35.327 -0600 WARN ConfigEncryptor - Decryption operation failed: AES-GC
```

이 오류 메시지는 다음 Splunk Answers 문서에서 다른 문제와 매우 유사합니다.

Splunk Enterprise 7.2.1을 설치하고 클러스터 마스터로 승격했습니다. Splunk Web이 로드되지 않습니다.

<https://answers.splunk.com/answers/723728/installed-splunk-enterprise-721-and-promoted-it-as.html>

해결

배포 서버에서 다음을 수행합니다.

1. \$SPLUNK_HOME/etc/auth 디렉터리에 splunk.secret의 백업 복사본을 만들었습니다.
2. splunk.secret을 제거했습니다.
3. HF(Heavy Forwarder)에서 DS(Deployment Server)로 splunk.Secret Key를 복사했습니다.
4. /opt/splunk/etc/system/local/server.conf 파일의 백업 복사본을 만들었습니다.
5. server.conf 파일의 pass4SymmKey에 주석 처리
6. server.conf 파일의 [sslConfig] stanza 아래에 sslPassword를 다시 입력했습니다.
7. Splunk 다시 시작
8. HF에 새 Splunk_TA_aws/local/passwords.conf 파일을 푸시했습니다.

향후 권장 사항:

1. HW에서 DS 인스턴스로 splunk.secret key를 복사하는 현재 접근 방식은 실행 가능한 솔루션이지만 다음과 같은 방법이 필요할 수 있습니다
고려해야 합니다.
DS가 다른 전달자/구축 클라이언트와 작동하려면 동일한 splunk.secret 키를 모든 전달자/클라이언트에 배포해야 합니다. 이렇게 하면 오류를 해독하는 데 실패하는 것을 방지할 수 있습니다.

2. 또 다른 방법은 DS 인스턴스의 passwords.conf 파일에 일반 텍스트 형식으로 암호를 설정하는 것입니다.
그런 다음 파일이 DS에서 푸시되면 HF(Deployment Client)가 비밀번호를 암호화하도록 합니다.
HW가 비밀번호를 해독합니다.
다시 시작된 직후.

관련 링크

Splunk Answers

Splunk Enterprise 7.2.1을 설치하고 클러스터 마스터로 승격했습니다. Splunk Web이 로드되지 않습니다. <https://answers.splunk.com/answers/723728/installed-splunk-enterprise-721-and-promoted-it-as.html>

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.