

Splunk 전달자가 Splunk 클라우드에 이벤트를 보내지 않습니다.

적용 가능성

Splunk 클라우드

설명

Splunk 전달자는 더 이상 Splunk Cloud에 이벤트를 보내지 않습니다. 이는 Universal Forwarder, Heavy Forwarder 또는 중간 포워딩 계층에 영향을 미칠 수 있습니다.

splunkd.log에 다음 오류가 나타납니다.

```
ERROR TcpOutputFd - Connection to host=1.22.122.222:9997 failed. sock_error = 104. SSL  
Error = No error
```

sock_error = 104 메시지는 전달자가 Splunk Cloud 수신 엔드포인트와 통신을 시도하는 동안 TCP 연결이 재설정되었음을 나타냅니다.

조사

영향을 받는 전달자에서 Splunk 클라우드 입력 엔드포인트로의 기본 네트워크 연결을 확인합니다.

```
telnet inputs1.<stack_id>.splunkcloud.com 9997
```

텔넷 연결에 성공하면 포트에 연결할 수 있음을 확인합니다. 그러나 SSL/TLS 연결을 완전히 검증하거나 중간 네트워크 디바이스에서 트래픽을 재설정하지 않음을 확인하지 않습니다.

연결을 추가로 검증하려면 영향을 받는 전달자에서 다음 명령 중 하나를 실행합니다.

```
openssl s_client -connect inputs1.<stack_id>.splunkcloud.com:9997
```

또는

```
$SPLUNK_HOME/bin/splunk cmd openssl s_client -connect inputs1.<stack_id>.splunkcloud.com
```

다음 출력이 반환되면 연결이 재설정됩니다.

```
CONNECTED(00000003)  
write:errno=104
```

이렇게 하면 전달자가 처음에 TCP 연결을 설정할 수 있지만 SSL/TLS 세션이 완료되기 전에 연결이 강제로 닫힙니다.

또한 `outputs.conf`를 포함하여 영향을 받는 전달자의 전달 컨피그레이션을 검토하여 전달자가 올바른 Splunk Cloud 수신 엔드포인트 및 포트를 사용하고 있는지 확인합니다.

해결

오류 104는 `ECONNRESET`입니다. 즉, "Connection reset by peer"입니다. 이는 연결이 TCP 재설정 패킷으로 강제로 닫혔음을 나타냅니다. 재설정은 대상 엔드포인트 또는 중간 네트워크 디바이스(예: 방화벽, 프록시, 로드 밸런서, IDS/IPS, SSL 검사 디바이스 또는 네트워크 어플라이언스)에 의해 전송될 수 있습니다.

영향을 받는 전달자와 Splunk Cloud 간의 전체 네트워크 경로를 검토합니다. 다음을 확인합니다.

- 포트 9997에서는 Splunk 클라우드 입력 엔드포인트로의 아웃바운드 트래픽이 허용됩니다.

- 방화벽, 프록시 또는 네트워크 어플라이언스는 TCP 세션을 재설정하지 않습니다.
- SSL 검사가 Splunk 포워딩 연결을 방해하지 않습니다.
- 최신 네트워크, 방화벽, 프록시, 라우팅 또는 인증서 관련 변경 사항을 검토합니다.
- Splunk Cloud Forwarder 앱 및 인증서는 현재 구축되어 있으며 올바르게 구축되어 있습니다.
- 중간 전달자는 Splunk Cloud와 통신할 수 있으며, 전달된 트래픽을 삭제 또는 차단하지 않습니다.

네트워크, 방화벽 또는 인증서 컨피그레이션을 수정한 후 필요한 경우 해당 전달자를 다시 시작하거나 자동으로 다시 연결하도록 허용합니다. 그런 다음 Splunk Cloud에서 이벤트가 성공적으로 인덱싱되고 있는지 확인합니다.

관련 링크

[Linux ARM 및 Splunk Cloud용 Universal Forwarder 연결 문제\(SSL 오류\)](#)

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.