

Universal Forwarder가 데이터를 Splunk 인덱서로 전달하지 않습니다.

적용 가능성

유니버설 포워더

설명

\$SPLUNK_HOME/etc/system/local/outputs.conf의 잘못된 컨피그레이션으로 인해 Splunk Universal Forwarder에서 예상대로 데이터를 전달하지 않습니다.

조사

Universal Forwarder의 \$SPLUNK_HOME/var/log/splunk/splunkd.log에서 다음 오류 메시지가 표시됩니다.

```
'09-06-2019 10:53:39.389 -0400 ERROR TcpOutputProc - LightWeightForwarder/UniversalForwa
```

해결

이 오류 메시지는 \$SPLUNK_HOME/etc/system/local/outputs.conf 파일에서 다음 설정을 구성하여 해결할 수 있습니다.

```
[tcpout]defaultGroup = <target_group>, <target_group>, ...
* A comma-separated list of one or more target group names, specified later in [tcpout:<
* The forwarder sends all data to the specified groups.
* If you don't want to forward data automatically, don't set this setting.
* Can be overridden by an inputs.conf '_TCP_ROUTING' setting, which in turn can be overr
* Starting with version 4.2, this setting is no longer required.
```

```
[tcpout:<target_group>]server = [<ip>|<servername>]:<port>, [<ip>|<servername>]:<port>,
```

- * A comma-separated list of one or more systems to send data to over a TCP socket.
- * Required if the 'indexerDiscovery' setting is not set.
- * Typically used to specify receiving Splunk systems, although you can use it to send data to other systems.
- * For each system you list, the following information is required:
 - a. The IP address or server name where one or more systems are listening.
 - b. The port on which the syslog server is listening.

output.conf의 추가 예는 다음에서 찾을 수 있습니다.

[output.conf.example](#)

[outputs.conf로 전달자 구성](#)

구성된 후 파일을 저장하고 다음 명령을 사용하여 \$SPLUNK_HOME/bin에서 실행하여 Splunk를 다시 시작합니다

```
./splunk restart
```

관련 링크

[output.conf.example](#)

[outputs.conf로 전달자 구성](#)

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.