

Splunk_TA_microsoft-IIS가 설치된 경우 CPU 사용률이 높은 Universal Forwarder

적용 가능성

Splunk Enterprise Universal Forwarder

설명

Splunk_TA_microsoft-IIS를 비활성화하면 CPU 사용률이 ~70%에서 ~10%로 증가할 때 문제가 TA로 격리되었습니다.

조사

식별 방법:

a. 유니버설 전달자는 다음 앱을 가지고 있습니다.

- OS 이름 Microsoft Windows Server 2008 R2 Enterprise
- 버전 6.1.7601 서비스 팩 1 빌드 7601
- Splunk Universal Forwarder 7.2.0
- Splunk_TA_windows 5.0.0
- Splunk_TA_microsoft-IIS 1.0.1

b. Splunk_TA_microsoft-IIS의 구성은 다음과 같습니다.

```
[monitor://C:\inetpub\logs\LogFiles\...\*.log]
disabled = false
sourcetype = ms:iis:auto
index = iis[monitor://D:\inetpub\logs\LogFiles\...\*.log]
disabled = false
sourcetype = ms:iis:auto
index = iis[monitor://D:\inetpub\logs\logfiles\...\*.log]
disabled = false
sourcetype = ms:iis:auto
index = iis[monitor://D:\IISLogs\...\*.log]
disabled = false
```

```
sourcetype = ms:iis:auto  
index = iis
```

- c. 위의 컨피그레이션으로 Splunk_TA_microsoft-IIS 추가 기능을 활성화하면 CPU 사용량이 70%가 됩니다.
- d. 두 점과 세 점을 같은 위치에 입력하면 Windows에서 무시된 경로에 대한 대/소문자 구분만 달라 집니다.

해결

해결 방법:

폴더 트래버스 "..." 많은 CPU 리소스를 훑치는 것으로 잘 알려져 있습니다.

Splunk_TA_microsoft-IIS 추가 기능 공식 문서에서는 단일 입력 항목을 권장합니다.

[컨피그레이션 파일을 사용하여 입력 구성](#)

이 문제를 해결하려면 4개 입력 모두를 단일 입력(암시적 재귀 = true)에 대한 폴더 통과로 바꾸십시오.

```
[monitor://C:\inetpub\logs\LogFiles]  
whitelist = \.log$|\.LOG$  
disabled = false  
sourcetype = ms:iis:auto
```

\$HOME_SPLUNK/etc/apps/Splunk_TA_microsoft-IIS/local/inputs.conf을 수정하고 Splunk를 다시 시작하면 CPU 사용량이 정상(~10%)으로 유지됩니다.

관련 링크

[컨피그레이션 파일을 사용하여 입력 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.