

Splunk DB Connect - 이벤트의 타임스탬프가 미래입니다.

적용 가능성

Splunk Apps 추가 기능

설명

이벤트는 db connect를 사용하는 Microsoft SQL Server에서 발생합니다. 데이터베이스 테이블의 타임스탬프는 GMT입니다. 데이터가 인덱싱되고 사용자 기본 설정이 EST로 설정되며 Show Last 24 hours(지난 24시간 표시)를 사용하여 검색을 수행하면 데이터 타임스탬프가 6시간 이후이므로 데이터가 반환되지 않습니다.

조사

타임스탬프의 이러한 변환은 일반적으로 인덱스 시간에 발생합니다. Splunk에 데이터를 가져오는 데 걸린 hops의 수를 확인하기 위해 데이터가 어디에서 생성되었는지 확인해야 합니다.

또한 Splunk 설명서에 나와 있는 내용도 고려하십시오.

"Splunk 인증을 사용하여 사용자를 추가하거나 수정할 때 사용자 시간대를 설정할 수 있습니다. 해당 사용자에 대한 검색 결과가 지정된 표준 시간대에 표시됩니다. 그러나 이 설정은 표준 시간대가 인덱스 시간에 결정되는 실제 이벤트 데이터를 변경하지 않습니다."

해결

데이터베이스의 표준 시간대를 변경하려면

Timezone 드롭다운 → Configuration → Databases Connections → "your connection" → 으로 이동하여 적절한 시간대를 선택합니다.

또한 다음 Splunk Answers 게시물을 검토합니다.

<https://answers.splunk.com/answers/512913/splunk-db-connect-how-to-set-correct-timezone->

[for.html](#)

관련 링크

Splunk 답변:

Splunk DB Connect: Splunk DB Connect 피드에 대한 올바른 시간대를 설정하는 방법

<https://answers.splunk.com/answers/512913/splunk-db-connect-how-to-set-correct-timezone-for.html>

Splunk 설명서:

사용자의 검색 결과에 대한 표준 시간대 설정

[https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Applytimezoneoffsetstotimestamps#Set the time zone of search results](https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Applytimezoneoffsetstotimestamps#Set_the_time_zone_of_search_results)

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.