

Splunk DB Connect – イベントのタイムスタンプは将来予定されています

適用性

Splunkアプリケーションアドオン

説明

イベントは、データベース接続を使用してMicrosoft SQL Serverから送信されます。データベーステーブルのタイムスタンプはGMTです。データのインデックスが作成され、ユーザー・プリファレンスがESTに設定され、「過去24時間の表示」を使用して検索が実行されると、データのタイムスタンプは6時間先であるため、データは戻されません。

調査

タイムスタンプのこの変換は、通常はインデックス時間に行われます。データの発信元を確認して、データをSplunkに取り込むのに必要なホップ数を確認する必要があります。

また、Splunkのドキュメントに次のように記載されていることを考慮してください。

“Splunk認証を使用してユーザを追加または編集する際に、ユーザのタイムゾーンを設定できます。そのユーザーの検索結果は、指定したタイムゾーンで表示されます。ただし、この設定では、インデックス時刻でタイムゾーンが決定される実際のイベントデータは変更されません。

解決方法

データベースのタイムゾーンを変更するには、次の手順を実行します。

Configuration → Databases → Connections → "your connection" → in the Timezoneドロップダウンに移動し、適切なタイムゾーンを選択します。

また、Splunkの次の回答の投稿を確認してください。

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

[for.html](#)

関連リンク

Splunkの回答：

Splunk DB Connect: Splunk DB Connect フィールドの正しいタイムゾーンを設定する方法

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

Splunkのドキュメント：

ユーザーの検索結果のタイムゾーンを設定する

[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)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。