

Splunk DB Connect — 事件的时间戳将来

适用范围

Splunk应用加载项

描述

事件来自使用db connect的Microsoft SQL server。数据库表中的时间戳以GMT为单位。建立数据索引时，用户首选项设置为EST，使用“显示过去24小时”执行搜索，由于数据时间戳的将来时间为6小时，因此不会返回数据。

调查

时间戳的这种转换通常在索引时发生。 需要检查数据的来源，查看将数据送入Splunk需要多少跳。

还要考虑Splunk文档的内容：

“使用Splunk身份验证添加或编辑用户时，可以设置用户时区。该用户的搜索结果将显示在指定的时区。但是，此设置不会更改实际事件数据，其时区在索引时确定。”

分辨率

要更改数据库的时区，请执行以下操作：

转至Configuration → Databases → Connections → “your connection”→Timezone下拉列表中，选择适当的时区。

此外，请查看以下Splunk Answers文章：

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

相关链接

Splunk答案：

Splunk DB连接：如何为Splunk DB Connect源设置正确的时区？

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

Splunk文档：

设置用户搜索结果的时区

https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Applytimezoneoffsetstotimestamps#Set_the_timezone_for_search_results

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。