

Splunk DB Connect - Carimbo de data/hora para eventos no futuro

Aplicabilidade

Complementos de Aplicativos Splunk

Descrição

Os eventos vêm do Microsoft SQL Server usando conexão db. O carimbo de data/hora na tabela do banco de dados está em GMT. Quando os dados são indexados, a preferência do usuário é definida como EST e uma pesquisa é executada usando Mostrar Últimas 24 horas, os dados não são retornados porque o carimbo de data/hora dos dados está no futuro por 6 horas.

Investigação

Essa transformação do timestamp geralmente ocorre no tempo de índice. É necessário verificar a origem dos dados para ver quantos saltos foram necessários para colocar os dados no Splunk.

Leve também em consideração o que a documentação do Splunk diz:

"Ao adicionar ou editar usuários usando a autenticação Splunk, você pode definir um fuso horário do usuário. Os resultados da pesquisa para esse usuário serão exibidos no fuso horário especificado. Essa configuração, no entanto, não altera os dados reais do evento, cujo fuso horário é determinado na hora do índice."

Resolução

Para alterar o fuso horário do banco de dados:

Vá para Configuração → Bancos de dados → conexões → "sua conexão" → na lista suspensa Fuso horário, escolha o fuso horário apropriado.

Além disso, revise a seguinte postagem das Respostas Splunk:

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

Links relacionados

Respostas de Splunk:

Conexão BD Splunk: Como definir o fuso horário correto para feeds do Splunk DB Connect?
<https://answers.splunk.com/answers/512913/splunk-db-connect-how-to-set-correct-timezone-for.html>

Documentação do Splunk:

Definir o fuso horário dos resultados de pesquisa de um usuário
https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Applytimezoneoffsetstotimestamps#Set_the_time_zone_of_search_results

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.