

Connessione al database splunk - Timestamp degli eventi nel futuro

Applicabilità

Componenti aggiuntivi applicazioni Splunk

Descrizione

Gli eventi provengono da Microsoft SQL Server che utilizza db connect. Il timestamp nella tabella del database è in GMT. Quando i dati vengono indicizzati, la preferenza utente è impostata su EST e viene eseguita una ricerca utilizzando Mostra ultime 24 ore. I dati non vengono restituiti perché l'indicatore data/ora è futuro di 6 ore.

Indagine

Questa trasformazione del timestamp si verifica in genere al momento dell'indice. È necessario controllare l'origine dei dati per verificare il numero di hop necessari per ottenere i dati in Splunk.

Prendere in considerazione anche quanto riportato nella documentazione relativa a Splunk:

"Quando si aggiungono o si modificano utenti utilizzando l'autenticazione Splunk, è possibile impostare un fuso orario utente. I risultati della ricerca per l'utente verranno visualizzati nel fuso orario specificato. Questa impostazione, tuttavia, non modifica i dati effettivi dell'evento, il cui fuso orario viene determinato al momento dell'indice."

Risoluzione

Per modificare il fuso orario del database:

Scegliere Configurazione → Database → Connessioni → "connessione" → nell'elenco a discesa Fuso orario scegliere il fuso orario appropriato.

Inoltre, rivedere il seguente post di Splunk Answers:

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

Collegamenti correlati

Risposte Splunk:

Connessione al database splunk: Come impostare il fuso orario corretto per i feed di Splunk DB Connect?

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

Documentazione Splunk:

Impostare il fuso orario per i risultati di ricerca di un utente

[https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Applytimezoneoffsetstotimestamps#Set the time zone offset](https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Applytimezoneoffsetstotimestamps#Set_the_time_zone_offset)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).