

Splunk DB Connect - Horodatage des événements à venir

Applicabilité

Modules complémentaires des applications Splunk

Description

Les événements proviennent de Microsoft SQL Server à l'aide de db connect. L'horodatage de la table de base de données est en GMT. Lorsque les données sont indexées, la préférence utilisateur est définie sur EST et une recherche est effectuée à l'aide de l'option Afficher les dernières 24 heures. Les données ne sont pas renvoyées car l'horodatage des données est de 6 heures dans le futur.

Enquête

Cette transformation de l'horodatage se produit généralement au moment de l'index. Vous devez vérifier l'origine des données pour voir le nombre de sauts nécessaires pour les envoyer dans le Splunk.

Tenez également compte de ce que dit la documentation Splunk :

"Lorsque vous ajoutez ou modifiez des utilisateurs à l'aide de l'authentification Splunk, vous pouvez définir un fuseau horaire utilisateur. Les résultats de la recherche de cet utilisateur s'affichent dans le fuseau horaire spécifié. Cependant, ce paramètre ne modifie pas les données d'événement réelles, dont le fuseau horaire est déterminé à l'heure de l'index."

Résolution

Pour modifier le fuseau horaire de la base de données :

Accédez à Configuration → Bases de données → Connexions → "votre connexion" → dans la liste déroulante Fuseau horaire, sélectionnez le fuseau horaire approprié.

En outre, réviser le message suivant Splunk Answers :

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

Liens connexes

Réponses du Splunk :

Splunk DB Connect : Comment définir le fuseau horaire correct pour les flux Splunk DB Connect ?

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

Documentation sur le Splunk :

Définir le fuseau horaire des résultats de recherche d'un utilisateur

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.