

「=」の付いたフィールドは検索できません。

適用性

SplunkエンタープライズSplunkクラウド

説明

Splunkバージョン : 7.0.13

文字列を照合して次のフィールドのいずれかを検索する場合：

- ポッド
- 名前空間
- container_name (コンテナ名)
- コンテナID

container_id=aadd1と同様に、は結果を返しません。

調査

調査の結果、この設定のHECデータには設定ファイルなしでインデックスが付けられていることが判明しましたが、適切に使用するには、いくつかの設定が必要です。実際にフィールドを検索するには、

:: 記号 (メタデータフィールドの指定子) ですが、=記号を使用して検索できないという事実は修正されません。

この機能を有効にするには、検索時に追加の設定を行う必要があります。GCP kubernetesのHEC入力を持っている場合、イベントは検索可能な状態に完全には準備されていないようです。特に、フィールドはインデックス付けされていないように見えます。これは、データrawデータの一部ですが、イベントを取得するための検索では指定されません。

解決方法

イベントはインデックス設定パラメータを取得しないため、次のように追加する必要があります。

インスタンス：検索ヘッド

ファイル：fields.conf

パス：\$SPLUNK_HOME/etc/apps/search/local

設定：次のように、各フィールドをパラメータINDEXED=trueのスタンザとして追加します。

```
[pod]
INDEXED=true[namespace]
INDEXED=true[container_name]
INDEXED=true[container_id]
INDEXED=true
```

この後、検索ヘッドを再起動する必要があります。これにより、新しく発生するイベントは=記号で検索できるようになります。

関連リンク

Splunkの回答

HECの「fields」引数に':'を指定してメタデータを検索する必要があるのはなぜですか。

<https://answers.splunk.com/answers/635676/why-do-i-need-to-search-metadata-in-a-fields-argum.html>

外部リンク

Kubernetes-loggingの設定：

<https://github.com/splunk/splunk-connect-for-kubernetes/tree/develop/helm-chart/splunk-kubernetes-logging>

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。