集計KPIの値は、エンティティKPIの重大度に関係なく該当なし

適用性

Splunk Enterprise Splunk ITサービスインテリジェンス

説明

サービステンプレートにリンクされているサービス（約850）をサービスアナライザで表示し、関連するKPIを表示すると、エンティティKPIの重大度には正しい値（情報）が表示されますが、サービスKPIの重大度には不明が表示されます。 KPIの集計しきい値とエンティティごとのしきい値の両方が[情報]に設定されています。

解決方法

多数のエンティティと多数のサービス/KPIがあります（テンプレート/サービスあたり8つのKPI）。 その結果、KPIベース検索を実行するたびに数万の結果が返されます。これは、ITSIが処理された検索結果をITSIサマリーインデックスに転送する際の制限を超える可能性があります

問題を回避するには：複数の共有ベース検索にサービスを分散することで、結果の数を減らします。

- 50000以上の結果を返す最大のSharedベース検索を特定します。

検索名のIDは、共有ベース検索のIDです。

```
index=_internal source=*scheduler.log* shared indicator  | stats min(result_count) AS mi
```

- サービス（およびサービスごとのエンティティ）の数を計算し、半分を実行できるかどうかを確認します。

- 共有ベース検索を複製します。次に、新しい共有ベース検索を使用するために、サービスの半分を再割り当てします。
- 実行してから、上の検索を使用して共有ベース検索ごとの結果の新しいパーティションを表示し、制限の下にあることを確認します
- 最後に、KPIに有効な「サービス集約値」があることをサービスで検証します。

または

制限を増やす（100000を超えないこと）

1. $SPLUNK_HOME/etc/system/local内の limits.confを作成または編集します。
2. 次のスタンザを追加します。

```
[scheduler]
* The maximum number of results to load when triggering an alert action.
* Default: 50000
max_action_results = 50000
```

3. 次の式に基づいて、上記の数値を自分で計算して調整する必要があります。

```
limit = (number of KPIs * number of entities for each service) + (number of services) *
```

注：この制限を増やした結果、結果の数をサポートするために割り当てられるメモリが増えるため、ITSIではより多くのメモリが使用されます

4. Splunkを再起動します

関連リンク

Splunkブログ

大規模環境でSplunk ITSIを設定するためのベストプラクティスのトップ3

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。