

大規模なルックアップを伴うtstat検索が副検索として失敗し、エラー「コード255で終了」が表示される

適用性

Splunk Enterprise Splunkの検索Splunkのサブ検索Splunk tstat

説明

tstatsコマンドのwhere句でサブ検索を使用する際に、サイズが大きすぎる（5,000行を超えているように見える）場合、検索は失敗し、次のエラーがスローされます。
検索プロセスが正常に終了しませんでした。exit_code=255, description="expired with code 255"。詳細については、ジョブインスペクタで、このピアのsearch.logを参照してください。

```
| tstats count from datamodel=Web where NOT  
[| inputlookup lookup.csv  
| fields dest  
| rename dest as Web.dest  
| format ] by Web.src Web.dest
```

この例では、lookup_name.csvの行数は最大110,000行です。

調査

検索が失敗し、次のエラーが表示された場合。

```
[<INDEXER_NAME>] Search process did not exit cleanly, exit_code=255, description="expired with code 255"
```

このエラーメッセージは、インデクサINDEXER_NAMEの検索プロセスに問題があったことを意味します。ほとんどの場合、クラッシュ (または強制終了) しました。
crash.logがない場合は、外部でSplunkが強制終了したか、crash.logの保存で問題が発生したことを意味します。
検索文字列を見ると (OR-sの数)、再帰によるスタックオーバーフローの可能性が最も高いです。
。

解決方法

再帰によってクラッシュする可能性のある既知の問題です (つまり、多くのOR/ANDを含む非効率な検索文字列)

[SPL-144975](#)により追跡 : [Splunkの一部を再設計し、再帰を削除](#)

この問題を回避する方法の1つは、スタックのulimitを大きくすることです。デフォルトは8064で、128kや256kなどの拡張値で問題に対処できます。

関連リンク

[SPL-144975:Splunkの一部を再設計し、再帰を削除します。](#)

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。