

REST APIが解析状態の検索を完了しません

適用性

Splunkエンタープライズ

説明

[REST APIリファレンスマニュアル](#)に記載されているように、「finalize」アクションを使用すると検索を停止できます。

複数の検索が24時間以上にわたって実行されている環境では、REST APIを使用して、このような長時間の結果を生成しないこれらの検索を停止します。使用するコマンドは次のとおりです。

```
curl method=post uri=https://localhost:8801/services/search/jobs/$sid$/control splunkauth
```

ただし、このコマンドはほとんどの検索では成功しますが、解析状態の検索を停止することはできません。これらのプロセスを停止して、OSプロセスを強制終了する必要があります。

調査

CONTROLエンドポイントは、操作の一覧を受け入れます（一時停止|一時停止|終了|キャンセル|タッチ|settl|setpriority|enablepreview|disablepreview|setworkloadpool）

finalize：検索を停止し、/resultsエンドポイントに中間結果を提供します。

検索がSHから送出されると、SHはそれを解析して分散化された中央集中型の部分を作成し、後でインデクサに送信します。この時点では、検索の結果はまだ生成されていないため、'finalize'アクションでは中間結果を提供できません。

ただし、解析状態の検索では、「キャンセル」アクションは正常に機能します。この操作によって検索が停止し、結果が返されなくなります。

cancel：現在の検索を停止し、結果のキャッシュを削除します。

解決方法

解析状態の検索の場合、このコマンドはジョブを正しく停止します。

```
curl method=post uri=https://localhost:8801/services/search/jobs/$sid$/control splunkauth=
```

関連リンク

Splunkドキュメント

REST APIリファレンスマニュアル

[RESTsearch](#)

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。