検索でloadjob機能コマンドを使用できません。

適用性

Splunkエンタープライズ

説明

ユーザは、レポート結果をダッシュボードにアップロードしたいと考えており、そのスケジュール済みレポートでloadjob機能を使用しようとしていました。

調査

loadjobコマンドはさまざまな理由で失敗する可能性があります。次に、いくつかのヒントを示します。

1. スケジュール済みジョブの所有者を（adminではなく）nobodyに変更してから、loadjobコマンドを適宜変更してください（これを行うには、保存済み検索のアプリケーションコンテキストでlocal.metaを編集します）
2. スケジュールされた検索がスキップされる可能性があります（[設定] -> [システムアクティビティ] -> [スケジューラレポート]で確認してください）
3. 管理者ユーザーのディスパッチディレクトリがいっぱいになっている可能性があります。ディスパッチディレクトリのサイズと制限を確認してください
4. loadjobコマンドで、スケジュールされた検索名のスペルが間違っている可能性があります
5. 保存された検索が存在するアプリケーションコンテキストが、loadjobコマンドで正しくない可能性があります

解決方法

その報告書は誰も所有していないことがわかった。これは、オブジェクトを作成したユーザが認証システムのユーザではなくなったことを意味します。ローカル・ユーザーを作成し、そのユーザーとしてログインし、任意のナレッジ・オブジェクトを作成し、そのユーザーを削除すると、そのユーザーのすべてのナレッジ・オブジェクトがnobodyによって所有されるように切り替わります。

関連リンク

Splunkの回答

Splunk 6.3で最新の保存済み検索結果を取得しようとすると、「Cannot find artifacts for savedsearch_ident...」というloadjobエラーが表示されるのはなぜですか。
https://answers.splunk.com/answers/318096/why-am-i-getting-loadjob-error-cannot-find-artifac.html

Splunkの検索とレポートで、「nobody」（所有者の列の下）は何を意味しますか。
https://answers.splunk.com/answers/425941/what-does-nobody-under-owner-column-signify-in-spl.html

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。