

Splunkで古いSAMLユーザを削除する方法

適用性

Splunk Cloud Splunk Enterpriseのアクセスコントロール

説明

この記事では、SAMLユーザの退職に関するベストプラクティスのテクニックを紹介します

調査

SAMLは、一方向のフェデレーション標準として動作します。つまり、Splunkはサインイン時にアイデンティティプロバイダー(IdP)からのみ情報を受信します。その結果、ユーザがIdPから削除されても、そのユーザは再びサインインすることがないため、Splunkは更新を受信しません。

前提条件：

1. ユーザー・ナレッジ・オブジェクト(KO)の管理

- ナレッジオブジェクトの所有者が部署または会社を退職し、Splunkアカウントが非アクティブ化されると、その所有者が所有していたナレッジオブジェクトはシステムに残ります。これらは孤立したナレッジ・オブジェクトです。有効な所有者を持たないナレッジ・オブジェクトは問題を引き起こす可能性があります。たとえば、孤立した参照定義を参照する検索は機能しない場合があります。

2. 次のドキュメントリンクに記載されている手順に従って、廃止するSAMLユーザに属するすべてのKOを再割り当てしてください。

[1つ以上の共有知識オブジェクトを新しい所有者に再割り当てする](#)

解決方法

削除するユーザに関連付けられているKOを再度割り当ててください（上記の前提条件を参照）。

オプション 1：

REST APIを使用して.confファイルを変更し、SAMLユーザを削除します。

CURL\REST API Example:

```
curl -k -u admin:{password} --request DELETE https://{hostname}:8089/services/admin/SAML
```

オプション 2：

Support > Splunk Cloud > Cloud Change Request [ticket](#)で削除するユーザのリストを添付してください。

Splunkサポートの機能：

1. 提供されたユーザの場合、バックアップは\$SPLUNK_HOME/etc/users/<directories>と\$SPLUNK_HOME/etc/system/local/authentication.confから作成されます。

2. ユーザー・ホーム・ディレクトリが削除されます。

3. authentication.confファイルの[userToRoleMap_SAML]スタンザの下で、リタイアされたユーザに対応する行が削除されます。

4. Web UI画面下部のSettings > Access Controls > Authentication Method > Reload SAML Settingsでデバッグ/更新を実行し、SAML設定をリロードするか、インスタンスを再起動して変更を有効にします。

注：検索ヘッドにログインしたことがないSAMLユーザについては、上記の解決策に従って削除する必要はありません。これは、Settings > Users > filter user name > Edit > Deleteの順に選択することで、簡単に削除できます。

関連リンク

Splunkドキュメント

[孤立した検索の解決](#)

Splunkの回答

古いsamlユーザを削除するにはどうすればよいですか。

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。