

So entfernen Sie alte SAML-Benutzer in Splunk

Geltungsbereich

Splunk Cloud Splunk Enterprise Access Controls

Beschreibung

In diesem Artikel werden Best Practice-Verfahren für die Einstellung von SAML-Benutzern vorgestellt.

Untersuchung

SAML arbeitet als unidirektionaler Verbundstandard. Das bedeutet, dass Splunk während der Anmeldung Informationen ausschließlich vom Identity Provider (IdP) empfängt. Wenn ein Benutzer aus dem IdP gelöscht wird, erhält Splunk das Update daher nicht, da sich der Benutzer nie wieder anmelden würde.

Voraussetzung:

1. Verwaltung von Wissensdatenobjekten (KOs)

- Wenn ein Eigentümer eines Wissensobjekts eine Abteilung oder ein Unternehmen verlässt und sein Splunk-Konto deaktiviert wird, verbleiben die Wissensobjekte, die ihm gehören, im System. Dies sind verwaiste Wissensobjekte. Wissensobjekte ohne gültige Besitzer können Probleme verursachen. Suchen, die auf verwaiste Nachschlagedefinitionen verweisen, funktionieren beispielsweise möglicherweise nicht.

2. Befolgen Sie die Schritte, die unter dem unten stehenden Link "Dokumentation" beschrieben sind, um KOs, die zu den SAML-Benutzern gehören, neu zuzuweisen und abzuziehen:

[Ein oder mehrere gemeinsam genutzte Wissensobjekte einem neuen Besitzer neu zuweisen](#)

Auflösung

Weisen Sie KOs erneut zu, denen die zu entfernenden Benutzer zugeordnet sind (siehe Voraussetzungen oben).

Option 1:

Entfernen Sie die SAML-Benutzer, indem Sie die CONF-Dateien über die REST-API ändern:

CURL\REST API Example:

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

Option 2:

Hängen Sie eine Liste der zu entfernenden Benutzer in einem [Ticket](#) für Support > Splunk Cloud > Cloud Change Request an.

Was der Splunk-Support bewirkt:

1. Für die angegebenen Benutzer wird eine Sicherung ihrer \$SPLUNK_HOME/etc/users/<Verzeichnisse> und \$SPLUNK_HOME/etc/system/local/authentication.conf erstellt.
2. Die Stammverzeichnisse des Benutzers werden entfernt.
3. Unter der Strophe [userToRoleMap_SAML] in der Datei authentication.conf werden die Zeilen gelöscht, die den ausgesetzten Benutzern entsprechen.
4. Führen Sie ein Debugging/eine Aktualisierung durch, laden Sie dann die SAML-Konfigurationen unter Einstellungen > Zugriffskontrollen > Authentifizierungsmethode > SAML-Einstellungen erneut am unteren Rand des Bildschirms der Webbenutzeroberfläche, oder starten Sie die Instanz neu, damit die Änderungen wirksam werden.

Hinweise: Für den SAML-Benutzer, der sich nie beim Suchkopf angemeldet hat, besteht keine Notwendigkeit, diesen zu löschen, indem er der obigen Lösung folgt. Es kann einfach entfernt werden, indem Sie Einstellungen > Benutzer > Filter Benutzername > Bearbeiten > Löschen.

Verwandte Links

Splunk-Dokumentation

[Verwaiste Suchvorgänge auflösen](#)

Punktantworten

[Wie entferne ich alte kleine Benutzer?](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.