

Comment supprimer les anciens utilisateurs SAML dans Splunk

Applicabilité

Splunk Cloud Splunk Enterprise Access Controls

Description

Cet article présente les meilleures pratiques de retrait des utilisateurs SAML

Enquête

SAML fonctionne comme une norme de fédération unidirectionnelle. Cela signifie que le Splunk reçoit des informations uniquement du fournisseur d'identité (IdP) lors de la connexion. Par conséquent, si un utilisateur est supprimé du fournisseur d'identité, le Splunk ne recevra pas la mise à jour, car cet utilisateur ne se reconnectera plus jamais.

Prérequis:

1. Gérer les objets de connaissance utilisateur (KO)

- Lorsqu'un propriétaire d'objet de connaissances quitte un service ou une société et que son compte Splunk est désactivé, les objets de connaissances qu'il possédait restent dans le système. Ce sont des objets de connaissance orphelins. Des objets de connaissance sans propriétaires valides peuvent causer des problèmes. Par exemple, les recherches qui font référence à des définitions de recherche orphelines peuvent ne pas fonctionner.

2. Veuillez suivre les étapes détaillées dans le lien Documentation ci-dessous, pour réattribuer les KO appartenant aux utilisateurs SAML à retirer :

[Réaffecter un ou plusieurs objets de connaissances partagés à un nouveau propriétaire](#)

Résolution

Veillez à réattribuer les KO associés au(x) utilisateur(s) à supprimer (voir les conditions préalables ci-dessus).

Option 1:

Supprimez les utilisateurs SAML en modifiant les fichiers .conf via l'API REST :

CURL\REST API Example:

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

Option 2:

Joignez une liste des utilisateurs à supprimer dans un [ticket](#) Support > Splunk Cloud > Cloud Change Request.

Fonctions du support Splunk :

1. Pour les utilisateurs fournis, une sauvegarde de leur répertoire

\$SPLUNK_HOME/etc/users/<directories> et

\$SPLUNK_HOME/etc/system/local/authentication.conf est effectuée

2. Les répertoires d'accueil de l'utilisateur sont supprimés.

3. Sous la strophe[userToRoleMap_SAML] dans le fichier authentication.conf, les lignes correspondant aux utilisateurs retirés sont supprimées.

4. Effectuez un débogage/actualisation, puis rechargez les configurations SAML dans Paramètres > Contrôles d'accès > Méthode d'authentification > Recharger les paramètres SAML au bas de l'écran de l'interface utilisateur Web ou redémarrez l'instance pour que les modifications prennent effet.

Remarques : Pour l'utilisateur SAML qui ne s'est jamais connecté à l'en-tête de recherche, il n'est pas nécessaire de le supprimer en suivant la solution ci-dessus. Il peut être simplement supprimé en suivant Settings > Users > filter user name > Edit > Delete.

Liens connexes

Documentation Splunk

[Résoudre les recherches orphelines](#)

Réponses Splunk

[Comment supprimer d'anciens utilisateurs de petite taille ?](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.