

如何刪除Splunk中的舊SAML使用者

適用性

Splunk雲Splunk企業訪問控制

說明

本文重點介紹停用SAML使用者的最佳實踐技術

調查

SAML作為單向聯盟標準運行。這意味著Splunk在登入期間僅從身份提供者(IdP)接收資訊。因此，如果使用者從IdP中刪除，Splunk將不會收到更新，因為該使用者永遠不會再次登入。

必備條件:

1. 管理使用者知識對象(KO)

- 當知識對象所有者離開部門或公司並且其Splunk帳戶被停用時，他們擁有的知識對象將保留在系統中。這些是孤立的知識對象。沒有有效所有者的知識對象可能會導致問題。例如，引用孤立查詢定義的搜尋可能無法工作。

2.請按照下面「文檔」連結中詳述的步驟重新分配屬於要報廢的SAML使用者的所有KO:

[將一個或多個共用知識對象重新指派給新所有者](#)

解析

請務必重新分配要刪除的使用者關聯的所有帳戶（請參閱上述先決條件）。

選項 1:

通過通過REST API修改.conf檔案刪除SAML使用者：

```
CURL\REST API Example:  
curl -k -u admin:{password} --request DELETE https://{hostname}:8089/services/admin/SAML
```

選項 2:

在支援>Splunk Cloud >雲更改請求票證中附加要刪除的使用者清單。

Splunk支援的作用：

- 1.對於所提供的使用者，備份他們的\$SPLUNK_HOME/etc/users/<directories>和\$SPLUNK_HOME/etc/system/local/authentication.conf
- 2.使用者主目錄被刪除。
- 3.在authentication.conf檔案的[userToRoleMap_SAML]指令碼下，刪除與已停用使用者對應的行。
- 4.執行調試/刷新，然後在Web UI螢幕底部的設定>訪問控制>身份驗證方法>重新載入SAML設定中重新載入SAML配置，或者重新啟動例項以使更改生效。

附註：對於從未登入到搜尋頭的SAML使用者，無需通過遵循上述解決方案將其刪除。只需按照Settings > Users > filter user name > Edit > Delete將其刪除。

相關連結

Splunk文檔
[解析孤立搜尋](#)

Splunk答案
[如何刪除舊saml使用者？](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。