

如何删除Splunk中的旧SAML用户

适用范围

Splunk云Splunk企业访问控制

描述

本文重点介绍停用SAML用户的最佳实践技术

调查

SAML作为单向联合标准运行。这意味着Splunk在登录期间仅从身份提供程序(IdP)接收信息。因此，如果用户从IdP中删除，Splunk将不会收到更新，因为该用户永远不会再次登录。

前提条件:

1. 管理用户知识对象(KO)

- 当知识对象所有者离开部门或公司并且其Splunk帐户被停用时，他们拥有的知识对象将保留在系统中。这些是孤立的知识对象。没有有效所有者的知识对象可能会导致问题。例如，引用孤立查找定义的搜索可能无法工作。

2.请按照以下“文档”链接中详述的步骤重新分配属于要报废的SAML用户的所有KO:

[将一个或多个共享知识对象重新指派给新所有者](#)

分辨率

请务必重新分配要删除的用户关联的所有帐户（请参阅上述必备条件）。

选项 1：

通过通过REST API修改.conf文件删除SAML用户：

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

选项 2：

在Support > Splunk Cloud > Cloud Change Request 票证中附加要删除的用户列表。

Splunk支持的作用：

- 1.对于所提供的用户，备份其\$SPLUNK_HOME/etc/users/<directories>和\$SPLUNK_HOME/etc/system/local/authentication.conf
- 2.删除用户主目录。
- 3.在authentication.conf文件[userToRoleMap_SAML]的stanza下，删除与已停用用户对应的行。
- 4.执行调试/刷新，然后在Web UI屏幕底部的设置>访问控制>身份验证方法>重新加载SAML设置中重新加载SAML配置，或者重新启动实例以使更改生效。

注意：对于从未登录搜索头的SAML用户，无需按照上述解决方案将其删除。只需按照Settings > Users > filter user name > Edit > Delete将其删除。

相关链接

Splunk文档

[解析孤立搜索](#)

Splunk答案

[如何删除旧saml用户？](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。