

Cómo eliminar usuarios antiguos de SAML en Splunk

Aplicabilidad

Splunk Cloud Controles de acceso empresarial Splunk

Descripción

En este artículo se destacan las técnicas de prácticas recomendadas para retirar usuarios SAML

Investigación

SAML funciona como un estándar de federación unidireccional. Esto significa que Splunk recibe información únicamente del proveedor de identidad (IdP) durante el inicio de sesión. Por consiguiente, si se elimina un usuario del IdP, Splunk no recibirá la actualización, ya que ese usuario nunca volverá a iniciar sesión.

Requisito previo:

1. Administrar objetos de conocimiento de usuario (KO)

- Cuando el propietario de un objeto de conocimiento abandona un departamento o empresa y su cuenta Splunk se desactiva, los objetos de conocimiento que poseía permanecen en el sistema. Se trata de objetos de conocimiento huérfanos. Los objetos de conocimiento sin propietarios válidos pueden causar problemas. Por ejemplo, es posible que las búsquedas que hacen referencia a definiciones de búsqueda huérfanas no funcionen.

2. Siga los pasos detallados en el enlace Documentación a continuación, para reasignar cualquier KO que pertenezca a los usuarios SAML que se retirarán:

[Reasignar uno o más objetos de conocimiento compartido a un nuevo propietario](#)

Resolución

Asegúrese de volver a asignar cualquier SKU que los usuarios que se van a eliminar tengan asociados (consulte los requisitos previos anteriores).

Opción 1:

Elimine los usuarios SAML modificando los archivos .conf a través de la API REST:

CURL\REST API Example:

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

Opción 2:

Adjunte una lista de los usuarios que se eliminarán en un ticket de Support > Splunk Cloud > Cloud Change Request.

Qué hace Splunk Support:

1. Para los usuarios proporcionados, se toma una copia de seguridad de sus

\$SPLUNK_HOME/etc/users/<directorios> y

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

2. Los directorios de inicio del usuario se eliminan.

3. Bajo la [userToRoleMap_SAML] stanza en el archivo authentication.conf, se eliminan las líneas correspondientes a los usuarios retirados.

4. Realice un debug/refresh y luego recargue las configuraciones SAML en Settings > Access Controls > Authentication Method > Reload SAML Settings en la parte inferior de la pantalla Web UI o reinicie la instancia para que los cambios surtan efecto.

Notas: Para el usuario SAML que nunca inició sesión en el encabezado de búsqueda, no hay necesidad de eliminarlo siguiendo la solución anterior. Puede eliminarla simplemente siguiendo Settings > Users > filter user name > Edit > Delete.

Enlaces relacionados

Documentación de Splunk

[Resolver búsquedas huérfanas](#)

Respuestas de Splunk

[¿Cómo elimino a los usuarios antiguos de saml?](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).