

Como remover usuários SAML antigos no Splunk

Aplicabilidade

Splunk Cloud Splunk Enterprise Access Controls

Descrição

Este artigo destaca as práticas recomendadas para desativar usuários SAML

Investigação

A SAML opera como um padrão de federação unidirecional. Isso significa que o Splunk recebe informações somente do Provedor de Identidade (IdP) durante a entrada. Consequentemente, se um usuário for excluído do IdP, o Splunk não receberá a atualização, pois esse usuário nunca entrará novamente.

Pré-requisito:

1. Gerenciar objetos de conhecimento do usuário (KOs)
 - Quando um proprietário de objeto de conhecimento deixa um departamento ou empresa e sua conta Splunk é desativada, os objetos de conhecimento que possuíam permanecem no sistema. Esses são objetos de conhecimento órfãos. Objetos de conhecimento sem proprietários válidos podem causar problemas. Por exemplo, pesquisas que se referem a definições de pesquisa órfãs podem não funcionar.
2. Siga as etapas detalhadas no link Documentação abaixo para reatribuir qualquer KOs pertencente aos usuários SAML a serem desativados:

[Reatribuir um ou mais objetos de conhecimento compartilhados a um novo proprietário](#)

Resolução

Certifique-se de reatribuir qualquer KO que os usuários a serem removidos tenham associado (consulte os pré-requisitos acima).

Opção 1:

Remova os usuários SAML modificando os arquivos .conf por meio da API REST:

CURL\REST API Example:

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

Opção 2:

Anexe uma lista dos usuários a serem removidos em um [tíquete](#) Support > Splunk Cloud > Cloud Change Request.

O que o Splunk Support faz:

1. Para os Usuários fornecidos, é feito um backup de seus \$SPLUNK_HOME/etc/users/<diretories> e \$SPLUNK_HOME/etc/system/local/authentication.conf
2. Os diretórios de início do usuário são removidos.
3. Na estrofe[userToRoleMap_SAML] do arquivo authentication.conf, as linhas correspondentes aos usuários desativados são deletadas.
4. Execute uma depuração/atualização e recarregue as configurações SAML em Configurações > Controles de Acesso > Método de Autenticação > Recarregar Configurações SAML na parte inferior da tela Web UI ou reinicie a instância para que as alterações tenham efeito.

Notas: Para o usuário SAML que nunca fez login no cabeçalho de pesquisa, não há necessidade de excluí-lo seguindo a solução acima. Ele pode ser simplesmente removido seguindo-se Configurações > Usuários > filtrar nome de usuário > Editar > Excluir.

Links relacionados

Documentação do Splunk

[Resolver pesquisas órfãs](#)

Respostas de Splunk

[Como faço para remover usuários saml antigos?](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.