

Come rimuovere i vecchi utenti SAML in Splunk

Applicabilità

Controlli di accesso Enterprise per Splunk Cloud

Descrizione

In questo articolo vengono illustrate le tecniche ottimali per il ritiro degli utenti SAML

Indagine

SAML funziona come standard di federazione unidirezionale. Ciò significa che Splunk riceve le informazioni esclusivamente dal provider di identità (IdP) durante l'accesso. Di conseguenza, se un utente viene eliminato dall'IdP, Splunk non riceverà l'aggiornamento, in quanto l'utente non accederà mai più.

Prerequisito:

1. Gestire gli oggetti della Knowledge Base dell'utente

- Quando un proprietario di un oggetto conoscenza lascia un reparto o una società e il relativo account Splunk viene disattivato, gli oggetti conoscenza di cui è proprietario rimangono nel sistema. Questi sono oggetti della Knowledge Base orfani. Gli oggetti della Knowledge Base senza proprietari validi possono causare problemi. Ad esempio, le ricerche che fanno riferimento a definizioni di ricerca orfane potrebbero non funzionare.

2. Per riassegnare eventuali KO appartenenti agli utenti SAML da ritirare, attenersi alla procedura descritta nel collegamento Documentazione riportato di seguito:

[Riassegnazione di uno o più oggetti della Knowledge Base condivisi a un nuovo proprietario](#)

Risoluzione

Accertarsi di riassegnare qualsiasi KO associato agli utenti da rimuovere (vedere i prerequisiti sopra riportati).

Opzione 1:

Rimuovere gli utenti SAML modificando i file .conf tramite l'API REST:

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

Opzione 2:

Allegare un elenco degli utenti da rimuovere in un [ticket](#) Supporto > Splunk Cloud > Richiesta di modifica cloud.

Operazioni eseguite dal supporto Splunk:

1. Per gli utenti specificati viene eseguito un backup di \$SPLUNK_HOME/etc/users/<directory> e \$SPLUNK_HOME/etc/system/local/authentication.conf
2. Le home directory utente vengono rimosse.
3. Nella stanza[userToRoleMap_SAML] del file authentication.conf, vengono eliminate le righe corrispondenti agli utenti ritirati.
4. Eseguire un'operazione di debug/aggiornamento, quindi ricaricare le configurazioni SAML in Impostazioni > Controlli di accesso > Metodo di autenticazione > Ricarica impostazioni SAML nella parte inferiore della schermata dell'interfaccia utente Web oppure riavviare l'istanza per rendere effettive le modifiche.

Note: Per l'utente SAML che non ha mai effettuato l'accesso alla testa di ricerca, non è necessario eliminarla seguendo la soluzione precedente. Può essere semplicemente rimosso seguendo Impostazioni > Utenti > filtro nome utente > Modifica > Elimina.

Collegamenti correlati

Documentazione relativa a Splunk
[Risolvi ricerche orfane](#)

Risposte Splunk

[Come rimuovere i vecchi utenti SAML?](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).