

Oude SAML-gebruikers verwijderen in Splunk

toepasbaarheid

Splunk Cloud Splunk Enterprise-toegangscontroles

Beschrijving

Dit artikel belicht best practice technieken voor het terugtrekken van SAML gebruikers

onderzoek

SAML werkt als een one-way federatie standaard. Dit betekent dat Splunk tijdens de aanmelding uitsluitend informatie ontvangt van de Identity Provider (IdP). Als een gebruiker van de IdP wordt verwijderd, ontvangt Splunk de update niet, omdat die gebruiker zich nooit meer zou aanmelden.

Voorwaarde:

1. Gebruikerskennisobjecten (KO's) beheren

- Wanneer een eigenaar van een kennisobject een afdeling of bedrijf verlaat en zijn Splunk-account wordt gedeactiveerd, blijven de kennisobjecten die hij bezat in het systeem. Dit zijn verweesde kennisobjecten. Kennisobjecten zonder geldige eigenaren kunnen problemen veroorzaken. Zoekopdrachten die verwijzen naar definities van weeskinderen werken bijvoorbeeld mogelijk niet.

2. Volg de stappen die worden beschreven in de documentatielink hieronder om alle KO's van de SAML-gebruikers opnieuw toe te wijzen om te worden gepensioneerd:

[Een of meer gedeelde kennisobjecten opnieuw toewijzen aan een nieuwe eigenaar](#)

resolutie

Zorg ervoor dat u een KO opnieuw toewijst aan de gebruiker(s) die moet/moeten worden verwijderd en die aan u is/zijn gekoppeld (zie de vereisten hierboven).

Optie 1:

Verwijder de SAML-gebruikers door de .conf-bestanden te wijzigen via de REST API:

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

Optie 2:

Voeg een lijst bij van de gebruikers die moeten worden verwijderd in een Support > Splunk Cloud > Cloud Change Request-[ticket](#).

Wat doet Splunk Support:

1. Voor de verstrekte gebruikers wordt een back-up gemaakt van hun \$SPLUNK_HOME/etc/users/<directory> en \$SPLUNK_HOME/etc/system/local/authentication.conf
2. De hoofddirectory's van de gebruiker worden verwijderd.
3. Onder de [userToRoleMap_SAML] stanza in het authentication.conf-bestand worden de regels die overeenkomen met de gepensioneerde gebruikers verwijderd.
4. Voer een foutopsporing/vernieuwing uit en herlaad vervolgens de SAML-configuraties in Instellingen > Toegangsbesturingselementen > Verificatiemethode > SAML-instellingen onderaan het scherm Web UI opnieuw of start de instantie opnieuw op zodat de wijzigingen van kracht worden.

Opmerkingen: Voor de SAML-gebruiker die nooit heeft ingelogd op de zoekkop, is het niet nodig om deze te verwijderen door de bovenstaande oplossing te volgen. Het kan eenvoudig worden verwijderd door Instellingen > Gebruikers > filter gebruikersnaam > Bewerken > Verwijderen.

Gerelateerde links

Splunk-documentatie

[Weeszoekopdrachten oplossen](#)

Splunk Antwoorden

[Hoe verwijder ik oude saml-gebruikers?](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.