로컬 Splunk 계정을 사용하여 Splunk에 로그인하는 방법

적용 가능성

Splunk Enterprise Splunk Cloud

설명

Splunk는 SAML SSO로 구성되어 있으므로, 인증은 로그인 URL을 통해 이루어지며 로컬 Splunk 계정은 인증할 수 없습니다.

로컬 사용자/관리자가 Splunk 인스턴스에서 SplunkWeb에 액세스하기 위해 이 작업을 수행해야 할 수 있으며, 특히 SAML이 작동하지 않는 경우(서비스가 다운되거나 잘못 구성되었을 수 있음) 더욱 그렇습니다.

조사

SAML SSO는 Splunk에 대해 구성되며, SplunkWeb을 통해 로컬 Splunk 계정을 사용하여 로그인해야 합니다.

해결

로컬 Splunk 인증/로그인은 Splunk 인스턴스의 FQDN 및 포트를 통해 다음 형식으로 사용할 수 있습니다.

> fqdn:splunkport/en-US/account/login?loginType=splunk

여기서 Splunk Instance servername 또는 로그인을 위한 위치 및 포트(예: servername:8000 또는 server_ip:8000)의 끝에 "/en-US/account/login?loginType=splunk"가 추가됩니다.

예:

> FQDN이 다음과 같은 Splunk 인스턴스에 로그인하려는 경우 splunksh01.buttercupgames.com, 일반적으로 포트 8000을 통해 splunksh01.buttercupgames.com:8000으로 로그인합니다.
>
> SAML SSO를 구성할 경우 다음과 같이 됩니다. splunksh01.buttercupgames.com:8000/en-US/account/login?loginType=splunk
>
> Splunk Cloud의 경우 로컬 Splunk 인증/로그인 URL은 stackid.splunkcloud.com/en-US/account/login?loginType=splunk입니다 .

관련 링크

SAML 인증이 활성화된 경우 Splunk 로컬 계정 로그인

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.