ローカルのSplunkアカウントを使用してSplunkに口グインする方法

適用性

Splunkエンタープライズ Splunkクラウド

説明

SplunkはSAML SSOで設定されているため、認証は口グインURLを経由し、ローカルのSplunkアカウントは認証できません。

これは、特にSAMLが動作していない場合（サービスがダウンしているか、設定が誤っている可能性がある）に、ローカルユーザ/管理者がSplunkインスタンス上のSplunkWebにアクセスするために必要になる場合があります。

調査

SAML SSOはSplunk用に設定されており、SplunkWeb経由でローカルSplunkアカウントを使用してログインする必要があります。

解決方法

ローカルのSplunk認証/口グインは、SplunkインスタンスのFQDNとポートを介して次の形式で使用できます。

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

Splunkインスタンスservernameまたはlocationの最後に「/en-US/account/login?loginType=splunk」を追加し、口グイン用にportを追加します（例：servername:8000またはserver_ip:8000）。

例：

splunksh01.buttercupgames.comというFQDNを持つSplunkインスタンスに口グインする場合、通常はポート 8000経由で splunksh01.buttercupgames.com:8000/

SAML SSOを設定する場合は、splunksh01.buttercupgames.com:8000/en-US/account/login?loginType=splunkになります。

Splunk Cloudの場合、ローカルのSplunk認証/口グインURLはstackid.splunkcloud.com/en-US/account/login?loginType=splunkです。

関連リンク

SAML認証が有効な場合のSplunkローカルアカウントログイン

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。