Microsoft Azure ADのSAML構成では、グループがマップされません。

適用性

Splunkクラウド

説明

SAML認証は、Splunkのドキュメントに従って設定します。
Microsoft Azure ADまたはAD FSをIDプロバイダーとして使用してSSOを構成する
ただし、権限が正しくマップされませんでした。

調査

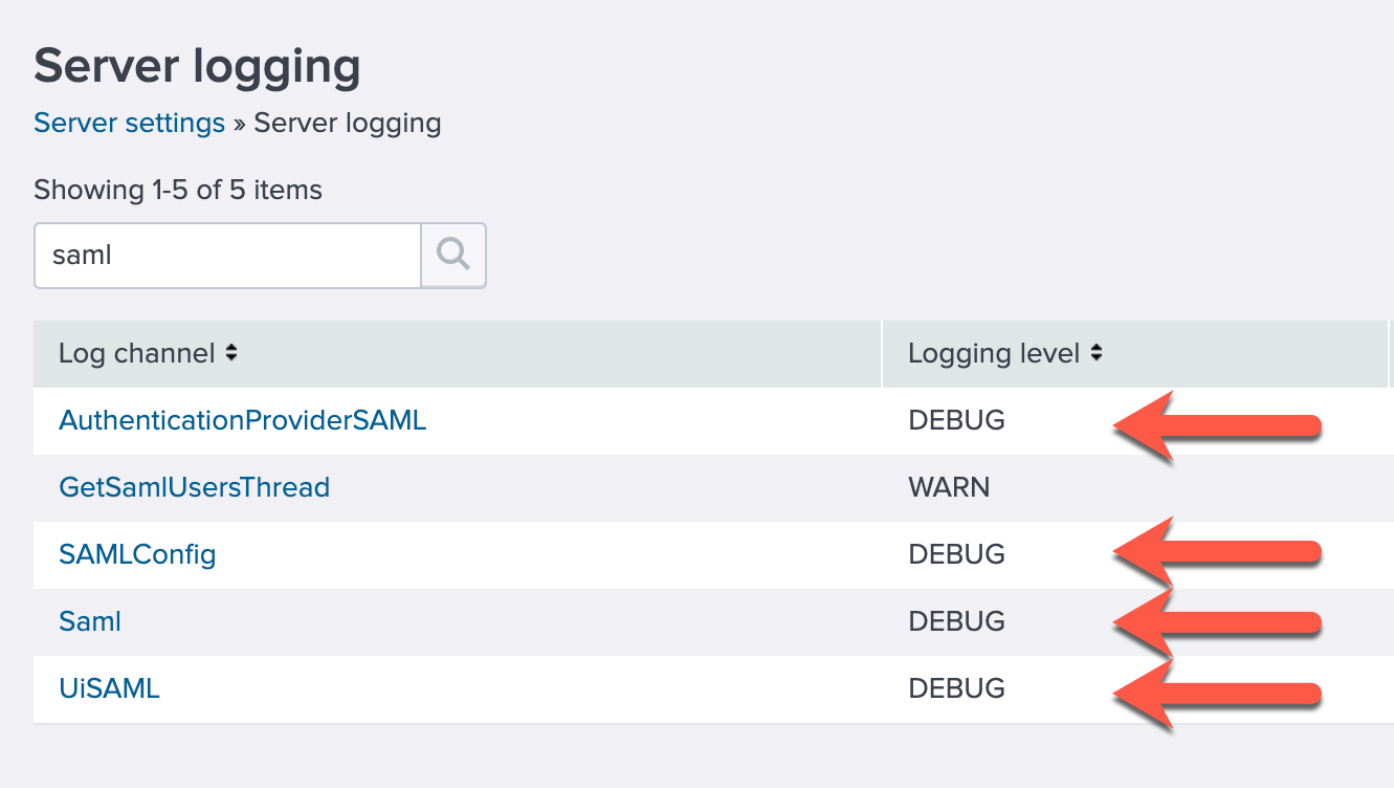
ユーザがSplunk Web UIからログインしようとすると、次のエラーが発生します。

```
'no valid role found in local mapping'
```

Splunk Cloud内のマッピンググループが一致しません。グループ名がAzure ADグループのObjectIdと一致しません。Splunkマッピンググループは、SplunkにマッピングするグループのAzure AD ObjectIdで呼び出す必要があります。たとえば、次の条件が期待されます。

マップするグループのAzure AD ObjectId: 99fvd7-fvddfv999-99999njhhb
Splunkマッピンググループ名：99fvd7-fvddfv999-99999njhhb

ログイン時にユーザが所有するグループを検証するには、Splunk GUIでSAMLのデバッグをオンにします。



次に、ユーザに再度ログインしてもらい、次のSPLを実行して、返されるグループを表示します。

```
index=_internal sourcetype=splunkd samlp
```

ここから、splunkのsamlマッピングがIdPによって返されるマッピングと一致するかどうかを確認できます。

解決方法

このシナリオでは、既存のマッピンググループを削除して再作成する必要があるため、構成が更新され、IdP Azure ADグループから返される内容と一致します。マッピングされたAzure ADグループのユーザがSplunk Cloudにログインすると、認証セクションの設定>アクセスコントロール>ユーザにSAML認証タイプが表示されます。

関連リンク

Microsoft Azure ADまたはAD FSをIDプロバイダーとして使用してSSOを構成する

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。