

クラウド Web セキュリティ : SAML の使用時に PingFederate と ADFS を使用してユーザ/グループ属性を設定する。

内容

[概要](#)

[要件](#)

[コンフィギュレーション](#)

[PingFed](#)

[ADFS](#)

[確認](#)

[トラブルシュート](#)

[関連するシスコ サポート コミュニティ ディスカッション](#)

概要

このドキュメントでは、ポリシーを細かくフィルタリングするためにユーザ/グループの詳細をクラウド Web セキュリティ サービスに送信するように、PingFederate および ADFS (Active Directory Federated Services) IDP サーバを設定する方法について説明します。

要件

次の項目に関する基本的な知識があることが推奨されます。

- PingFed/ADFS サーバへの管理ログイン/アクセス
- PingFed/ADFS サーバの操作方法に関する知識
- HTTPS トラフィックで粒度を使用できるようにするため、HTTPS インспекションをすべてのトラフィックに適用する必要があります。

コンフィギュレーション

PingFederate と ADFS のユーザ/グループ属性を設定するには、次の手順を実行します。

PingFed

[Attribute sources] > [User lookup] タブで次のように設定します。

- [Attribute Contract] : AUTHENTICATED_GROUPS
出典 : LDAP

[Value] : memberOf

- [Attribute Contract] : **SAML_SUBJECT**
送信元 : [LDAP]

[Value] : **sAMAccountName**

ADFS

[Trust relationships] > [Relying party trusts] タブで、次のように設定します。

- [LDAP Attribute Contract] : **SAM-Account-Name**
[Outgoing Claim Type LDAP] : **Name ID**
- [LDAP Attribute Contract] : **Token-Groups**
[Outgoing Claim Type LDAP] : **Group**

確認

トラブルシューティング

このドキュメントに、トラブルシューティングのセクションはありません。