

クラウド Web セキュリティ : 認証の時に特定のグループが含まれる設定 ADFS

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

概要

この資料に団体会員の詳細なリストよりもむしろ識別プロバイダ (IdP) Cisco クラウド Web セキュリティ (CWS) サービスに特定のグループ詳細を送るで Microsoft Active Directory フェデレーション サービス (ADFS) を設定する方法を記述されています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ScanCenter ポータルとのクラウド Web セキュリティ 設定
- セキュリティ アサーション マークアップ言語 (SAML) 認証
- Microsoft ADFS サーバの管理

使用するコンポーネント

この文書に記載されている情報は Microsoft ADFS バージョン 2.0 に、Windows サーバ 2008 R2 のその実行に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

クライアント ブラウザ間の認証プロセスが行われる時、ADFS サーバ (IdP) および CWS (サービスプロバイダー (SP))、すべての情報はクライアント ブラウザの URL ストリングに暗号化され追加されます。これは詳細が CWS に送信 される時 URL ストリングがより長いことを

意味します。

CWS サービスと併用するため SAML 認証を (Microsoft ADFS と) 設定するとき、ユーザ名を提供し、情報をグループ化するために依存パーティ信頼を設定する必要があります。 [クラウド Web セキュリティ : SAML を使用して間 PingFederate および ADFS の設定 ユーザ/グループ属性](#)はこのステップをより詳しく記述します。

ユーザが追加されるグループの数は URL サイズを増加します。ユーザが多数の Active Directory (AD) グループに属する場合、URL はサイズにブラウザによって課される URL 制限が達する、認証プロセスは失敗しますというなり。

各ブラウザは URL 長さを与えられる自身の最大を定義するかもしれませんが。 [RFC 2616](#) は最大長を規定しませんが、実際の限界はブラウザベンダーによって課されます。

注: グループに文字の固定番号がないので明示的にグループの最大数を定義することはできません。たとえば、GroupA に Test_Group_A よりより少ない文字があります。何人かのグループを定義することはドメイン名 + グループ名の文字数によって URL 制限の下にとどまる決まります。

設定

認証プロセスに特定のグループを含めるために Microsoft ADFS サーバを設定できます。通常 CWS Web フィルタリング規則で使用されたグループだけ選択します。あるポリシーの監査を実行するとき、既に使用中であるグループの判別を助けます。

既にある新しく、配備最良の方法設定に続くべきですこれらの利点を提供する:

- 最低限に URL サイズを保ちます
- 高速化します IdP (ADFS) と SP (CWS) 間の認証プロセスを
- 各認証要求で帯域幅を保存します

最良の方法設定

開いたクレームプロバイダ信頼は 2 つの承認トランスフォームルールを作成し、:

クレームとしてクレームルールテンプレート送信 LDAP 属性を利用して下さい

アトリビュートストア: AD;

LDAP アトリビュート: トークン グループ-非修飾名;

発信クレームの種類: グループ

クレームとしてクレームルールテンプレート送信 LDAP 属性を利用して下さい

アトリビュートストア: AD;

LDAP アトリビュート: SAM アカウント名前;

発信クレームの種類: 名前

依存一部信頼を開き、2つのトランスフォームルールを作成することによって発行トランスフォームルールを作成して下さい:

トランスフォームを着信クレーム テンプレート使用して下さい

着信クレームの種類: 名前

形式: unspecified

発信クレームの種類: Name ID

形式: unspecified

パススルーをすべてのクレーム値選択して下さい

パススルーを使用するか、または着信クレームをフィルタリングして下さい

着信クレームの種類: グループ

パススルー特定の値から開始するクレーム値だけ選択して下さい:

AD グループ名を規定して下さい

確認

ここでは、設定が正常に動作していることを確認します。

- エンドユーザとしてログオンされている間、<http://whoami.scansafe.net> に参照して下さい。
- 出力は団体会員の詳細なリストよりもむしろ以前に述べられたプロシージャで、規定されるグループだけリストする必要があります。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。