クラウド Web セキュリティ： 認証の時に特定のグループを含むために ADFS を設定して下さい

目次

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 のその実行基づいています。

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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 に送られるとき 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の SAML 認証を（Microsoft ADFS と）設定するとき、ユーザ名およびグループ情報を提供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 を使用する間 PingFederate および ADFS でユーザ/グループ属性をより詳しく記述しますこのステップを設定して下さい。

ユーザがに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。 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:** グループが文字の固定番号を持ってい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。

既にあっている新しく、配備これらの利点を提供する最良の方法設定に続くべきです:

- 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

属性ストア: AD;

LDAP 属性: 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

属性ストア: AD;

LDAP 属性: 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手順で、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。