Kerberos 認証を使用した SAML SSO セットアップの設定例

目次

概要

このドキュメントでは、Jabber クライアントによる Kerberos 認証（Microsoft Windows のみ）を使用するために Active Directory および Active Directory Federation Service （AD FS）バージョン 2.0 を有効にする方法を説明します。これにより、ユーザは Microsoft Windows ログオンでログインし、クレデンシャルの入力を求められません。

> **注意**： このドキュメントは、ラボ環境に基づいており、前提として、変更を実行したことによる影響を認識しておいてください。 実行した変更の影響を理解するために、関連する製品ドキュメントを参照してください。

前提条件

要件

Cisco では次の前提を満たす推奨しています。

- AD FS バージョン 2.0 がインストールされ、シスコ コラボレーション製品を使用して信頼できるパーティとして設定している
- Security Assertion Markup Language （SAML）シングル サインオン（SSO）を使用するために、Cisco Unified Communications Manager （CUCM） IM および Presence、Cisco Unity Connection （UCXN）、CUCM が有効化されている

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Active Directory 2008（ホスト名： ADFS1.ciscolive.com）
- AD FS バージョン 2.0（ホスト名： ADFS1.ciscolive.com）
- CUCM（ホスト名： CUCM1.ciscolive.com）
- Microsoft Internet Explorer バージョン 10
- Mozilla Firefox バージョン 34
- Telerik Fiddler バージョン 4

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。

設定

AD FS の設定

1. Jabber がインストールされているクライアントコンピュータを有効化してチケットをリクエストし、AD FS サービスと通信するためのクライアント コンピュータを有効化するために、Service Principal Name（SPN）を使用して AD FS バージョン 2.0 を設定します。

   詳細については、「AD FS 2.0： サービスアカウント用に SPN（servicePrincipalName）を設定する方法」を参照してください。

2. AD FS サービス用のデフォルトの認証設定（**C:\inetpub\adfs\ls\web.config に含まれる**）が**統合 Windows 認証**であることを確認します。 それが**フォームベース認証**に変更されていないことを確認します。

3. [Windows Authentication] を選択し、右ペインにある [Advanced Settings] をクリックします。 [Advanced Settings] で、[Enable Kernel-mode authentication] をオフにし、[Extended Protection] が [Off] であることを確認し、[OK] をクリックします。

4. Windows 以外のすべてのクライアントは、Kerberos を使用できず、NTLM に依存するため、AD FS バージョン 2.0 が Kerberos プロトコルと NT LAN Manager（NTLM）プロトコルの両方をサポートすることを確認します。

   右ペインで [Providers] を選択し、[Enabled Providers] の下に [Negotiate] と [NTLM] が存在することを確認します。

注: 統合 Windows 認証を使用すると、AD FS は、クライアントの要求を認証するためにネゴシエート セキュリティ ヘッダーを渡します。 ネゴシエート セキュリティ ヘッダーは、クライアントが Kerberos 認証と NTLM 認証のいずれかを選択できるようにします。 次のいずれかの条件に該当する場合を除き、ネゴシエート プロセスは Kerberos 認証を選択します。

- 認証に関与するシステムのいずれかが Kerberos 認証を使用できない。

- 発信側のアプリケーションが、Kerberos 認証を使用するための十分な情報を提供しない。

- ネットワーク認証に Kerberos プロトコルを選択するように、ネゴシエート プロセスを有効化する目的で、クライアント アプリケーションが SPN、ユーザ プリンシパル名（UPN）、または Network Basic Input/Output System（NetBIOS）アカウント名をターゲット名として提供する必要がある。 そうしないと、ネゴシエート プロセスは、優先認証方法として NTLM プロトコルを常に選択します。

ブラウザの設定

Microsoft Internet Explorer

1. [Internet Explorer] > [Advanced] > [Enable Integrated Windows Authentication] がオンになっていることを確認します。

2. [Security] > [Intranet zones] > [sites] に AD FS の URL を追加します。

3. CUCM、IMP、および Unity のホスト名を [Security] > [Trusted sites] に追加します。

4. イントラネット サイト用にログイン クレデンシャルを使用するために、[Internet Exporer] > [security] > [Local Intranet] > [Security Settings] > [User Authentication - Logon] が設定されていることを確認します。

Mozilla FireFox

1. Firefox を開き、アドレス バーに「**about: config** 」と入力します。

2. [I'll be careful, I promise!] をクリックします。

3. 修正するために**本当および network.negotiate-auth.trusted-uris に順序で ciscolive.com,adfs1.ciscolive.com に**プリファレンス名前 network.negotiate auth.allow 非 **fqdn を**ダブルクリックして下さい。

4. Firefox を閉じ、再度開きます。

確認

AD FS サーバの SPN が正しく作成されたことを確認するために、**setspn** コマンドを入力し、出力を表示します。

クライアント マシンが Kerberos チケットを持っているかどうか確認します。

これらの手順を完了し、どの認証（Kerberos または NTLM 認証）が使用されているか検証します。

1. クライアント マシンに Fiddler ツールをダウンロードしてインストールします。

2. すべての Microsoft Internet Explorer ウィンドウを閉じます。

3. Fiddler ツールを実行し、[File] メニューの [Capture Traffic] オプションが有効であることを確認します。 Fiddler は、クライアント マシンとサーバ間でパススループロキシとして動作し、すべてのトラフィックをリッスンします。

4. Microsoft Internet Explorer を開いてから CUCM を参照し、リンクをいくつかクリックしてトラフィックを生成します。

5. Fiddler のメイン ウィンドウに戻り、結果が **200**（成功）であるいずれかのフレームを選択すると、Kerberos が認証メカニズムであることがわかります。

6. 認証タイプが NTLM の場合、次のようにフレームの先頭に [Negotiate - NTLMSSP] と表示されます。

トラブルシューティング

このドキュメントの記載に従って、すべての設定手順および検証手順を完了してもまだログイン

の問題が発生する場合は、Microsoft Windows の Active Directory / AD FS 管理者に相談する必要があります。