Jabber のエンドユーザ SAML SSO 向け ADFS 2.0 での Kerberos 設定例

目次

概要

この資料にアクティブ ディレクトリ フェデレーション サービス (ADFS) で Kerberos を設定する方法を 2.0 記述されています。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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

(SSO) 設定のエンドユーザ セキュリティ アサーション マークアップ言語 (SAML) 単一 サイ

ンは Kerberos が Jabber のためのエンドユーザ SAML SSO をドメイン 認証を使用することを許可するために設定されるように要求します。 SAML SSO が Kerberos と設定されるとき、Lightweight Directory Access Protocol （ LDAP ）は Kerberos は認証を管理するが、すべての許可およびユーザ 同期を処理します。 Kerberos は LDAP 対応 例と共に使用するために意味される認証プロトコルです。

アクティブ ディレクトリ ドメインに加入される Microsoft Windows およびマッキントッシュ マシンで、ユーザは要件なしでシームレスに ユーザ名を入力するために Cisco Jabber にログインすることができますまたはパスワードおよび彼らは Login 画面を見ません。 コンピュータのドメインまだログイン されない ユーザは標準 Login 形式を見ます。

認証がオペレーティング システムから渡される単一 トークンを使用するのでリダイレクトが必要となりません。 トークンは設定されたキー ドメインコントローラ (KDC) に対して確認され、有効なら、ユーザはログオンされます。

設定

ADFS 2.0 で Kerberos を設定するプロシージャはここにあります。

1. マシンで Microsoft Windows サーバ 2008 R2 をインストールして下さい。

2. 同じマシンでアクティブ ディレクトリ ドメイン サービス (追加します) および ADFS をインストールして下さい。

3. Microsoft Windows サーバ 2008 R2-installed マシンで Internet Information Services （ IIS ）をインストールして下さい。

4. IIS のための自己署名証明書を作成して下さい。

5. 自己署名証明書を IIS にインポートし、HTTPS サーバ証明として使用して下さい。

6. Microsoft Windows7 を別のマシンでインストールし、クライアントとしてそれを使用して下さい。

   追加するインストールしたマシンに Domain Name Server （ DNS ）を変更して下さい。

   ADDS のインストールで作成したドメインにこのマシンを追加して下さい。

   開始するに行って下さい。**コンピュータを**右クリックして下さい。**[Properties]**をクリックします。ウィンドウの右側の**設定を**『Change』 をクリック して下さい。**Computer Name** タブをクリックします。[Change] をクリックします。作成したドメインを追加して下さい。

7. Kerberosサービスが両方のマシンで生成するかどうか確認して下さい。

   サーバ マシンの管理者としてログインはコマンド プロンプトを開き。 それからこれらのコマンドを実行して下さい:

cd \windows\System32Klist チケット

クライアントマシンのドメイン ユーザとしてログインは同じコマンドを実行し。

8. 追加するインストールしたマシンの ADFS Kerberos 識別を作成して下さい。

   Microsoft Windows 管理者は Microsoft Windows ドメインコントローラの Microsoft Windows ドメインに（<domainname> \管理者として）、たとえば、作成します ADFS Kerberos 識別をログイン しました。 ADFS HTTP サービスはこの形式のサービス プリンシパル名（SPN）と呼ばれる Kerberos 識別がなければなりません: HTTP/DNS_name_of_ADFS_server.

   この名前は ADFS HTTPサーバ 例を表すアクティブ ディレクトリ ユーザにマッピング する必要があります。 Microsoft Windows 2008 Server でデフォルトで利用可能であるはずである Microsoft Windows setspn ユーティリティを使用して下さい。

   手順 ADFS サーバのための SPNs を登録して下さい。 アクティブ ディレクトリ ドメインコントローラで、setspn コマンドを実行して下さい。

   たとえば ADFS ホストが adfs01.us.renovations.com の、およびアクティブ ディレクトリ ドメイン US.RENOVATIONS.COM は、コマンド次のとおりですときあります:

   ```
   setspn -a HTTP/adfs01.us.renovations.com <ActiveDirectory user>
   setspn -a HTTP/adfs01 <ActiveDirectory user>
   ```

   HTTPS である SPN の HTTP 部分は ADFS サーバが Secure Sockets Layer （SSL）によって一般的にアクセスされるのに、適用します。

   ADFS サーバのための SPNs が setspn コマンドできちんと作成される確認し、出力をことを表示して下さい。

   ```
   setspn -L <ActiveDirectory user>
   ```

9. Microsoft Windows クライアントのブラウザ設定を設定して下さい。

   ツール > InternetOptions に > 統合された Windows 認証を有効に するために進みましたナビゲート して下さい。

   イネーブル統合 Windows Authentication チェックボックスをチェックして下さい:

> ローカル イントラネット > カスタムは Tools > Internet オプション > Security に水平になります...イントラネット ゾーンのだけログオンを『Automatic』 を選択 するためにナビゲート します。

> ローカル イントラネット > サイトは Tools > Internet オプション > Security に > 進みましたローカル イントラネット サイトに侵入検知及び防止（IDP） URL を追加するためにナビゲート します。

注: ローカル イントラネット ダイアログボックスのチェックボックスすべてをチェックし、**Advanced タブを**クリックして下さい。

Tools > Security > 信頼できるサイト > サイトに CUCM ホスト名を信頼できるサイトに追加するためにナビゲート して下さい:

確認

このセクションはどの認証を（Kerberos または NT LAN Manager （NTLM） 認証）使用されるか確認する方法を説明します。

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 Internet Explorer ウィンドウを閉じて下さい。
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。

   バイオリン弾きは一時的にこのような Internet Explorer 設定を行う受信します、すべてのトラフィックをクライアントマシンとサーバ間のパススルー プロキシとしてはたらき、:
4. Internet Explorer を開き、カスタマー リレーションシップ マネージメント（CRM）サーバ URL に参照し、トラフィックを生成するために少数のリンクをクリックして下さい。
5. バイオリン弾きメイン ウィンドウに戻って参照し、結果が 200 である帯の 1 つを選択して下さい（成功）:

   認証種別が NTLM である場合、ここに示されているようにフレームの始めに**- NTLMSSP を**、**ネゴシエートするために**見ます:

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。