SWAでのKerberosシングルサインオン認証の設定

内容

はじめに

このドキュメントでは、Secure Web Appliance(SWA)でKerberosを介してシングルサインオン(SSO)認証を使用するようにプロキシユーザを設定する手順について説明します。

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。

- SWA管理。
- 基本的なActive Directory管理。

次のツールをインストールしておくことを推奨します。

- 物理または仮想SWA。

- SWAグラフィカルユーザインターフェイス(GUI)への管理アクセス
- Active Directoryへの管理アクセス。

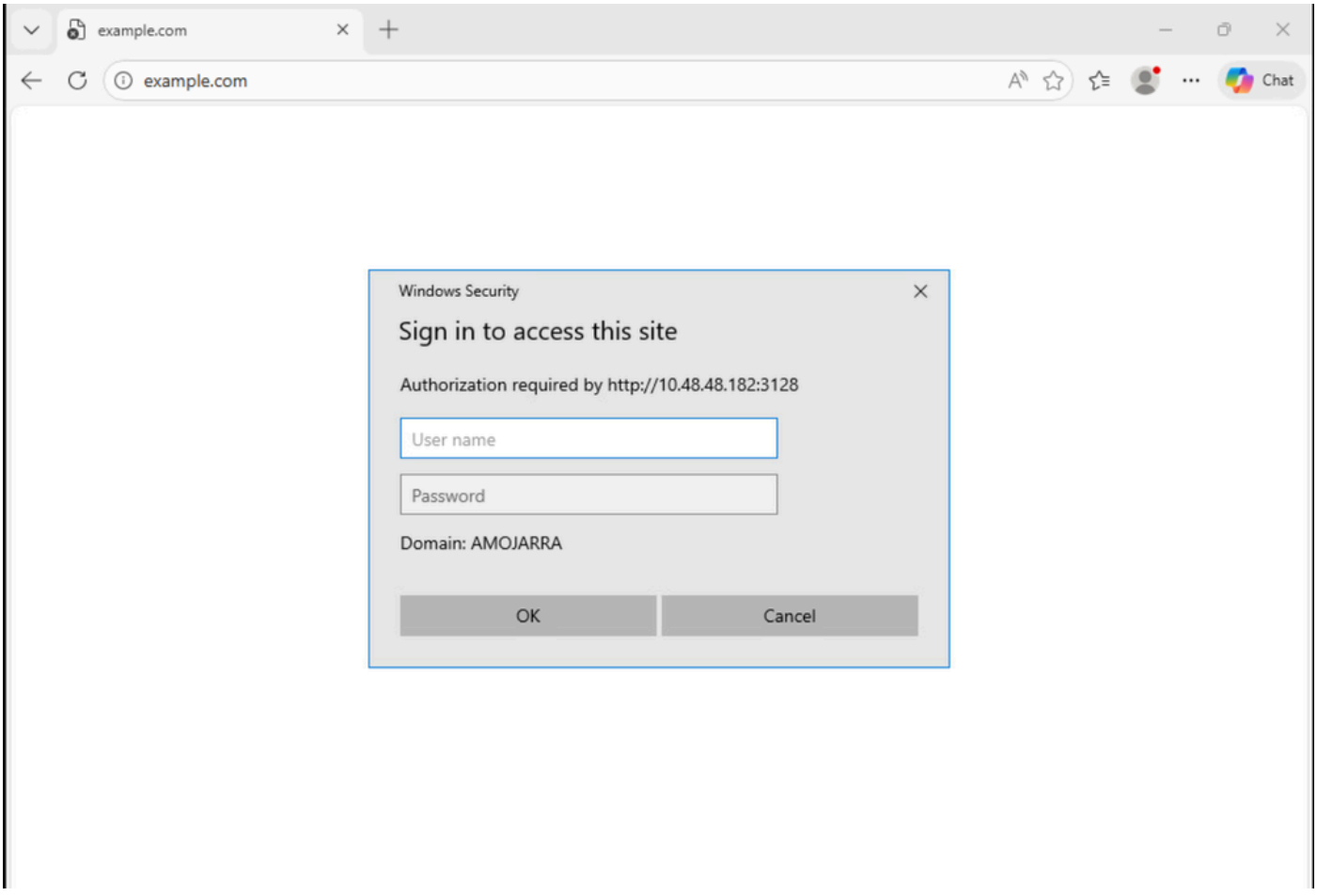
使用するコンポーネント

このドキュメントの内容は、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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

はじめる前に

プロキシクライアントがWebサイトにアクセスしようとして、クレデンシャルを手動で入力するように求められる場合は、次の手順を使用してトラブルシューティングを行います。



イメージ – ユーザ認証プロンプト

ステップ 1：クライアントに関連するアクセスログを確認します。

ステップ 1.1：CLIにログインします。

ステップ 1.2：grepを実行します。

ステップ 1.3：.accesslogsに関連付けられている番号を選択します。

ステップ 1.4：Enter the regular expression to grepで、クライアントのIPアドレスを入力します。

ステップ 1.5：「Do you want to tail the logs」が表示されるまでEnterキーを押し、「Y」と入力して、アクセスログが表示されるまでEnterキーを押します。

ステップ 1.6：クライアントPCから任意のWebサイトへのアクセスを試みることで、問題を再現します。

ステップ1.7：トラフィックが一致しているIDプロファイルを確認します。

次の例では、IDプロファイルはAuth_IDです。

```
1776248928.353 0 10.48.48.195 TCP_DENIED/407 0 GET http://cisco.com/ - NONE/- - OTHER-NONE-Auth_ID-NONE
```

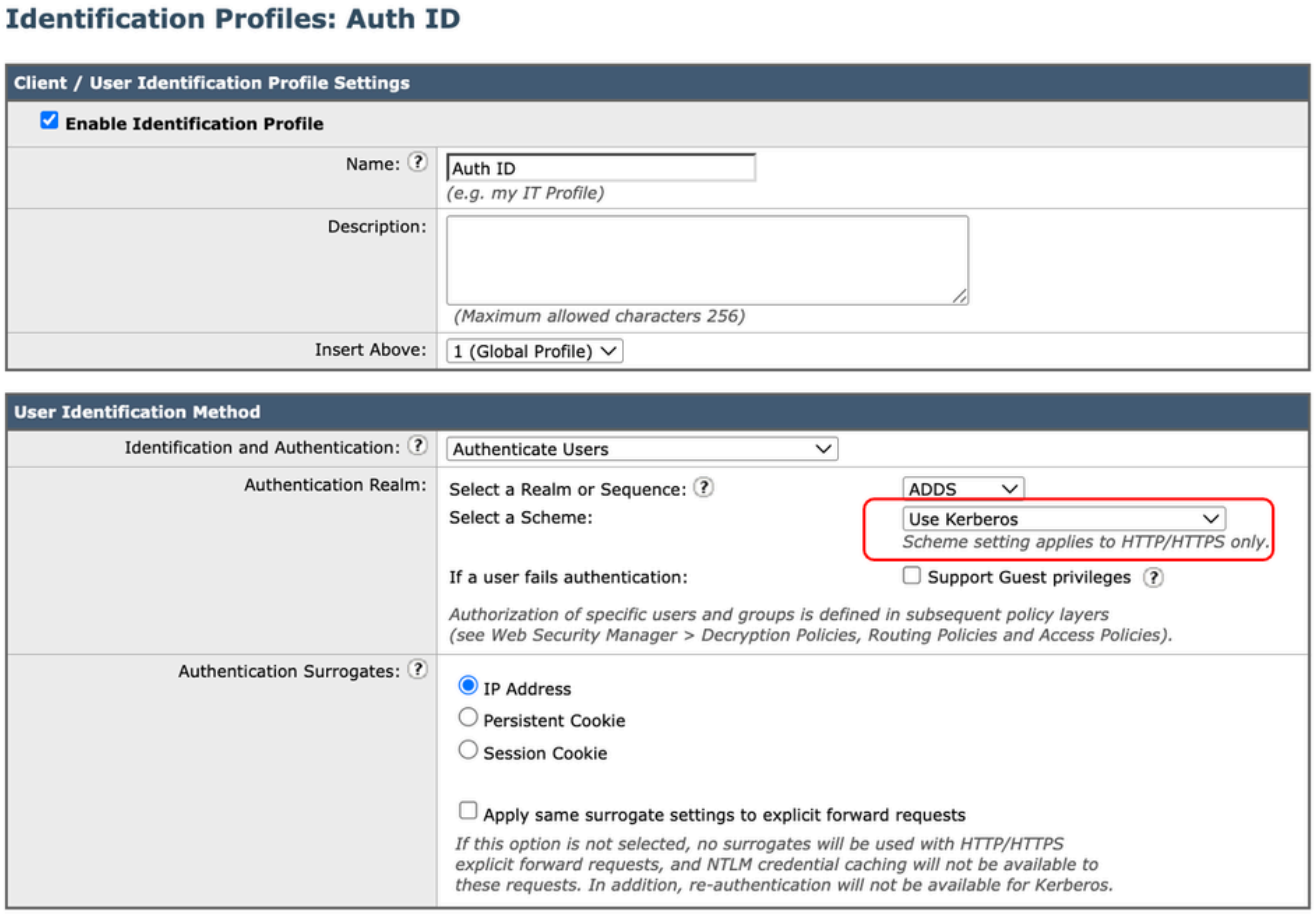
ステップ 2IDプロファイルを確認します。

ステップ 2.1：SWAのGUIにログインします。

ステップ 2.2：Web Security Managerで、Identification Profilesを選択します。

ステップ 2.3：トラフィックがヒットしていたIDプロファイルの名前をクリックします。

ステップ 2.4：認証スキームがBasicに設定されていないことを確認します。



イメージ – 認証スキーマ

ステップ 3SWAとActive Directoryの接続をテストします。

ステップ 3.1：SWAのGUIでNetworkに移動し、Authenticationを選択します。

ステップ 3.2：Authentication Realm Nameをクリックします。

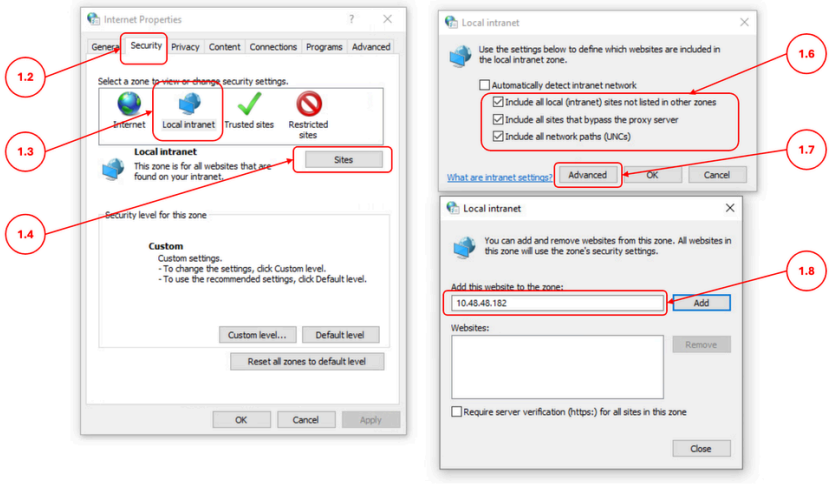
ステップ 3.3：Start Testをクリックして、SWAとActive Directoryの接続ステータスを確認します。

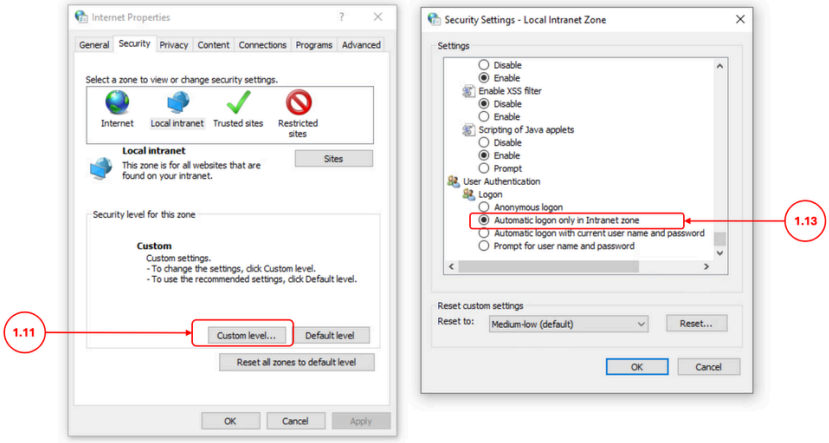
エラーが見つからない場合は、この記事の説明に従ってクライアントPCの設定を確認します。

クライアントPCの設定

クライアントPCの設定を確認するには、次の手順を実行します。

手順	詳細

ステップ 1：ローカルイントラネットサイト	ステップ 1.1： スタートメニューでInternet Optionと入力し、Enterキーを押します。 ステップ 1.2：Internet Propertiesウィンドウで、Security タブをクリックします。 ステップ 1.3：Local Intranetを選択します。 ステップ 1.4：Sitesをクリックします。 ステップ 1.5：Automatically detect intranet networkチェックボックスが選択されていないことを確認します。 ステップ 1.6： 次の3つのオプションをすべて選択します。 • 他のゾーンに含まれていないすべてのローカル（イントラネット）サイトを含める • プロキシサーバーをバイパスするすべてのサイトを含める • すべてのネットワークパス(UNC)を含める ステップ 1.7：[Advanced] をクリックします。 ステップ 1.8：SWAのFQDNまたはIPアドレスを入力し、リストに追加します。 ステップ1.9.（オプション）内部セキュリティポリシーに応じて、「Require Server Verification」を無効にできます。  イメージ：ローカルインターネットサイトの設定 ステップ 1.10：Closeをクリックし、OKをクリックします。 ステップ 1.11：SecurityタブでCustom levelをクリックします。

	ステップ 1.12：User Authenticationまでスクロールします。 ステップ 1.13：Automatic logon only in Intranet zoneが選択されていることを確認します。  イメージ – イントラネットユーザの自動ログイン
ステップ 2ログの収集	手順1で、Kerberos経由のSSO認証が修正されていない場合： ステップ 2.1： SWA認証ログをトレースに変更し、ログを確認します。 ステップ 2.2：[Auth-Method = %m]をカスタムフィールドとしてアクセスログに追加します。詳細については、「アクセスログでパフォーマンスパラメータを設定する」を参照してください。 ステップ 2.3：クライアントIPアドレスとActive Directory IPアドレスのパケットキャプチャフィルタを実行し、クライアントPCがSWAにKerberosサービスチケットを送信していることを確認します。

注：ブラウザのプロキシ設定でSWAのFQDNが設定されていることを確認してください。

関連情報

- AsyncOS 15.0 for Cisco Secure Web Applianceユーザガイド
- セキュアWebアプライアンス用のファイアウォールの設定
- コンテンツセキュリティアプライアンスでのパケットキャプチャの設定
- アクセスログのパフォーマンスパラメータの設定
- セキュアなWebアプライアンスのログへのアクセス

- セキュアなWebアプライアンスのベストプラクティスの使用：シスコ
- Secure Web Applianceでの認証のバイパス：シスコ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。