Identity Services Engine ゲスト ポータルのローカル Web 認証の設定例

目次

概要

このドキュメントでは、Cisco Identity Services Engine（ISE）のゲスト ポータルによるローカル Web 認証（LWA）を設定する方法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。

- ISE

- Cisco ワイヤレス LAN コントローラ（WLC）

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。

- ISE バージョン 1.1
- WLC バージョン 7.4

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。

背景説明

このドキュメントでは、LWA の設定について説明します。 ただし、可能な限り ISE による中央集中型 Web 認証（CWA）を使用することを推奨します。 一部のシナリオでは LWA が推奨または唯一のオプションとなるため、ここではそれらのシナリオの設定例を示します。

設定

LWA を使用するには、特定の前提条件、WLC での主要な設定、および ISE でのいくつかの変更が必要です。

これらについて説明する前に、ここでは ISE による LWA プロセスの概要を示します。

ISE ゲスト ポータルでの LWA プロセス

1. ブラウザが Web ページを取得しようとします。
2. WLC は、HTTP 要求を傍受し、それを ISE にリダイレクトします。
   情報のいくつかの重要な部分が HTTP リダイレクト ヘッダーに格納されます。 リダイレクト URL の例を次に示します。
   https://mlatosieise.wlaaan.com:8443/guestportal/Login.action?switch_url=https://1.1.1.1/login.html&ap_mac=b8:be:bf:14:41:90&client_mac=28:cf:e9:13:47:cb&wlan=mlatosie_LWA&redirect=yahoo.com/
   この URL 例から、ユーザが「yahoo.com」に到達しようとしたことがわかります。 この URL には、ワイヤレス ローカル エリア ネットワーク（WLAN）の名前（mlatosie_LWA）、およびクライアントとアクセス ポイント（AP）の MAC アドレスに関する情報が含まれています。 この URL 例では、**1.1.1.1** が WLC であり、**mlatosieise.wlaaan.com** が ISE サーバです。
3. ISE のゲスト ログイン ページが表示され、ユーザがユーザ名とパスワードを入力します。
4. ISE は、設定済みの ID シーケンスに照らして認証を実行します。
5. ブラウザが再びリダイレクトします。 今度は、WLC にクレデンシャルを送信します。 ブラウザは、ユーザが ISE で入力したユーザ名とパスワードを追加のユーザ操作なしで提供します。 WLC に対する GET 要求の例を次に示します。

GET
/login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0
ここにも、元の URL（**yahoo.com**）、ユーザ名（**mlatosie@cisco.com**）、およびパスワード（**ityh**）のすべてが含まれています。
注: ここでは URL を表示していますが、実際の要求は HTTPS で示される Secure Sockets Layer（SSL）を介して送信されるため、傍受は困難です。

6. WLC は、RADIUS を使用してこのユーザ名とパスワードを ISE に対して認証し、アクセスを許可します。
7. ユーザが指定されたポータルにリダイレクトされます。 詳細については、このドキュメントの「**WebAuth URL としての外部 ISE の設定**」の項を参照してください。

ネットワーク図

この図は、この例で使用するデバイスの論理トポロジを示しています。

設定要件

LWA プロセスが正常に動作するには、クライアントが次の情報を取得できる必要があります。

- IP アドレスとネットマスクの設定
- デフォルト ルート
- ドメイン ネーム システム（DNS）サーバ

これらはすべて DHCP または ローカル設定によって提供されます。

LWA が動作するためには、DNS 解決が正常に機能する必要があります。

WLC の設定

WebAuth URL としての外部 ISE の設定

[Security] > [Web Auth] > [Web Login Page] で、この情報にアクセスできます。

> **注:** 次の例は、外部 WebAuth URL を使用しており、ISE バージョン 1.1 から取得したものです。 バージョンが異なる場合は、必要な設定内容を理解するため、コンフィギュレーション ガイドを参照してください。

アクセス コントロール リスト（ACL）の設定

Web 認証が動作するためには、許可するトラフィックを定義する必要があります。

FlexConnect ACL と標準 ACL のどちらを使用する必要があるかを決定します。

FlexConnect AP は FlexConnect ACL を使用しますが、中央集中型スイッチングを使用する AP

は標準 ACL を使用します。

特定の AP がどのモードで動作するかを理解するには、[Wireless] > [Access points] に移動して、[AP name] > [AP Mode] ドロップダウン ボックスを選択します。 一般的な展開は、[local] と [FlexConnect] のいずれかです。

[Security] > [Access Control Lists] で、[FlexConnect ACLs] または [ACLs] を選択します。

この例では、DNS 交換と ISE（10.48.66.107）へのトラフィックを特に許可するため、すべての UDP トラフィックが許可されています。

この例では、FlexConnect を使用するので、FlexConnect ACL と標準 ACL の**両方**が定義されています。

この動作は、WLC 7.4 コントローラに関する Cisco Bug ID CSCue68065 に記述されています。

LWA のサービス セット ID（SSID）の設定

[WLAN] で、編集する [WLAN ID] を選択します。

Web 認証設定

直前の手順で定義した ACL を適用し、Web 認証をイネーブルにします。

> **注:** FlexConnect のローカル スイッチング機能を使用する場合は、ACL のマッピングを AP レベルで追加する必要があります。 これは、[Wireless] > [Access Points] にあります。 適切な [AP Name] > [FlexConnect] > [External WebAuthentication ACLs] を選択します。
> 、

認証、認可、およびアカウンティング（AAA）のサーバ設定

この例では、認証サーバとアカウンティング サーバの両方が、以前に定義した ISE サーバを指しています。

> **注:** [Advanced] タブのデフォルトを追加する必要はありません。

ISE の設定

ISE の設定は複数の手順で構成されます。

まず、デバイスをネットワーク デバイスとして定義します。

次に、この交換に対応する認証ルールと許可ルールが存在することを確認します。

ネットワーク デバイスの定義

[Administration] -> [Network Resources] -> [Network Devices] で、次のフィールドを入力します。

- デバイス名
- デバイスの IP アドレス
- **[Authentication Settings] > [Shared Secret]**

認証ポリシーの設定

[Policy] > [Authentication] で、新しい認証ポリシーを追加します。

この例では、次のパラメータを使用します。

- [Name]： **WLC_LWA_Guests**
- [Condition]： **Airespace: Airespace-Wlan-Id。** この条件は WLAN ID の 3 と一致します。これは、以前に WLC に定義した WLAN **mlatosie_LWA** の ID です。
- （オプション）証明書 **Non_Cert_Auth** を必要としない認証プロトコルを許可しますが、デフォルトを使用できます。
- ユーザがローカルに定義されたゲスト ユーザであることを定義する Guest_Portal_Sequence。

許可ポリシーと許可結果の設定

[Policy] > [Authorization] で、新しいポリシーを定義します。 次のような非常に基本的なポリシーでかまいません。

この設定は、ISE の全体的な設定によって異なります。 この例では、意図的に簡単にしています。

確認

管理者は、ISE の [Operations] > [Authentications] でライブ セッションの監視とトラブルシューティングを行うことができます。

2 つの認証を確認する必要があります。 1 つ目の認証は、ISE のゲスト ポータルで行われます。2 つ目の認証は、WLC から ISE へのアクセス要求として行われます。

どの許可ポリシーと認証ポリシーが選択されているかを確認するには、**認証の詳細レポート** アイコンをクリックします。

管理者は、WLC の [Monitor] > [Client] でクライアントを監視できます。

正常に認証されたクライアントの例を次に示します。

トラブルシューティング

可能な限り、クライアントでデバッグを実行することを推奨します。

これらのデバッグでは、CLI を介して有用な情報が提供されます。

```
debug client MA:CA:DD:RE:SS

debug web-auth redirect enable macMA:CA:DD:RE:SS

debug aaa all enable
```

関連情報

- Cisco ISE 1.x コンフィギュレーション ガイド
- Cisco WLC 7.x コンフィギュレーション ガイド
- テクニカルサポートとドキュメント - Cisco Systems