AP バージョン 1.01 の HTTP Admin の認証

目次

概要

このドキュメントでは、Access Point (AP) バージョン 1.01 の HTTP 管理の設定例を説明します。

前提条件

要件

このドキュメントに関しては個別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。

- Access Control Server (ACS) バージョン 2.6.4 以降

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。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

GUI には、TACACS+ または RADIUS アカウンティングや EXEC セッションでのコマンド許可を設定するためのオプションはありません。 これらのオプションは CLI で設定できますが、設定することは*推奨されません*。 これらのオプションを設定すると、アカウンティング要求や許可要求によって AP と ACS の動作速度を極度に低下させる可能性があります（ページの各要素がアカウンティングまたは許可の対象になるため）。

ACS 設定

インターフェイスの設定

以下の手順に従って、インターフェイスを設定します。

1. TACACS+（Cisco IOS）で、定義されていない最初の新規サービス フィールドのグループ ボックスを選択します。
2. [Service] フィールドに **Aironet** と入力します。
3. [Protocol] フィールドに **Shell** と入力します。
4. [Advanced Configuration Options] で、[Advanced TACACS+ Features] > [Display a window for each service selected] の順に選択します。
5. [Submit] をクリックします。

ユーザの設定

以下の手順に従って、ユーザを設定します。

1. [Advanced TACACS+ Settings] で、[Shell (exec)] を選択します。
2. 権限レベルを選択します。
3. フィールドに **15** と入力します。
4. [Submit] をクリックします。

グループの設定

以下の手順に従って、グループを設定します。

1. [TACACS+] を選択します。
2. [Aironet Shell] > [Custom attributes] の順に選択します。
3. [Custom Attributes] フィールドに **aironet: admin-capability=write+ident+firmware+admin+snmp** と入力します。
4. [Submit] をクリックします。
5. 再起動します。

ネットワーク構成

以下の手順に従って、ネットワークを設定します。

1. TACACS+ をプロトコルとして使用して、AP の NAS を作成します。
2. キーは、AP から共有される秘密キーです。
3. [Submit] をクリックします。
4. 再起動します。

注: トークン サーバとワンタイム パスワードを使用する場合、レベル 1 とレベル 15 のパスワードを常にプロンプトしなくても済むように、トークン キャッシングを設定する必要があります。トークン キャッシングを設定するには、以下の手順に従います。

1. 管理者ユーザが属しているグループのグループ設定を入力します。
2. [Token Card Settings] を選択します。
3. [Duration] を選択します。
4. セキュリティのニーズと利便性のバランスがとれた期間を選択します。

標準的な管理セッションの継続時間が 5 分以下の場合、期間の値は 5 分に設定するのが最善です。 この場合、セッションが 5 分を超えて実行されていると、5 分間隔で再度パスワードを求めるプロンプトが表示されます。 アカウンティングが有効にされていない場合、[Session] オプションは機能しないことに注意してください。 また、トークン キャッシングは、グループ内の すべてのユーザに対して適用され、すべてのデバイスとの すべてのグループ セッションに対して適用されることにも注意してください（AP に対する EXEC セッションだけに適用されるのではありません）。

VxWorks 用 AP の設定

ユーザの設定

次の手順を実行します。

1. [Setup] > [Security] > [User Information] > [Add New User] の順に選択します。
2. 全管理機能を持つ新しいユーザを追加します（すべての機能設定をオンにします）。
3. [Back] をクリックします。 [Security Setup] ページに戻ります。
4. [User Manager] をクリックします。 [User Manager Setup] ページが表示されます。
5. [User Manager] を有効にします。
6. [OK] をクリックします。

サーバ設定

次の手順を実行します。

1. [Setup] > [Security] > [Authentication Server] の順に選択します。
2. TACACS+ サーバの IP アドレスを入力します。
3. TACACS サーバのタイプを選択します。
4. フィールドに **port 49** と入力します。
5. フィールドに **shared secret** と入力します。
6. [User Authentication] チェックボックスをオンにします。

IOS 用 AP の設定

以下の手順に従って、IOS 用の AP を設定します。

1. [Security] > [Server Manager] を選択します。
2. 設定済みの TACACS+ サーバを選択するか、新しい TACACS+ サーバを設定します。
3. [Apply] をクリックします。
4. [Admin Authentication (TACACS+)] ドロップダウンから、TACACS+ の IP を選択します。
5. [Apply] をクリックします。
6. [Security] > [Admin Access] の順に選択します。
7. 読み取り/書き込みアクセス権を割り当てたローカル ユーザを作成します（まだ作成していない場合）。
8. [Apply] をクリックします。
9. [Authentication Server Only] または [Authentication Server] を選択します（[Local List] に含まれていない場合）。
10. [Apply] をクリックします。

確認

現在、この設定に使用できる確認手順はありません。

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。

関連情報

- Aironet 1200 シリーズ製品のサポート
- Terminal Access Controller Access Control System（TACACS+）テクノロジーのサポート
- Cisco Secure Access Control Server for Windows 製品のサポート
- Cisco Secure Access Control Server for UNIX 製品に関するサポート ページ
- テクニカルサポート - Cisco Systems