ACS 4.2 TACACS と Prime Infrastructure 統合の設定例

目次

概要

このドキュメントでは、Cisco Prime Infrastructure（PI）アプリケーションでの Terminal Access Controller Access Control System（TACACS+）の

認証および認可について、設定例を示して説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- アクセス コントロール サーバ（ACS）でクライアントとして PI を定義します。
- ACS と PI で IP アドレスおよび同一の共有秘密キーを定義します。

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。

- ACS バージョン 4.2
- Prime Infrastructure リリース 3.0

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。

設定

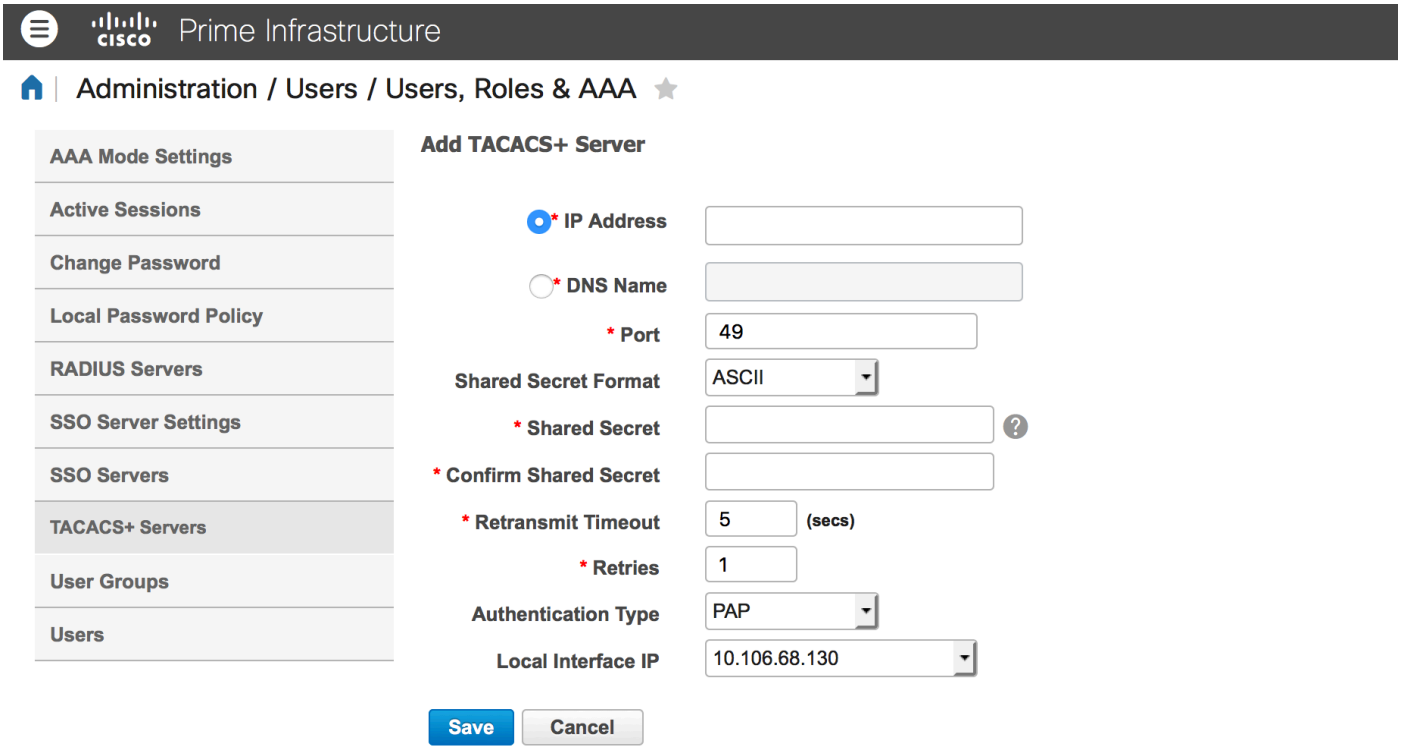
設定

PI に TACACS サーバとして ACS を追加

次の手順を実行して、ACS を TACACS サーバとして追加します。

ステップ 1：PI で [Administration] > [Users] > [Users, Roles & AAA] に移動します。

呼び出します。 左側のサイドバー メニューから [TACACS+ Servers] を選択し、[Add TACACS+ servers] で [Go] をクリックすると、次のようなページが表示されます。



手順 3：ACS サーバの IP アドレスを追加します。

手順 4：ACS サーバに設定されている TACACS+ 共有秘密を入力します。

ステップ 5：[Confirm Shared Secret] テキスト ボックスに共有秘密を再度入力します。

ステップ 6：デフォルト設定のフィールドの他のままにします。

ステップ 7：[Submit] をクリックします。

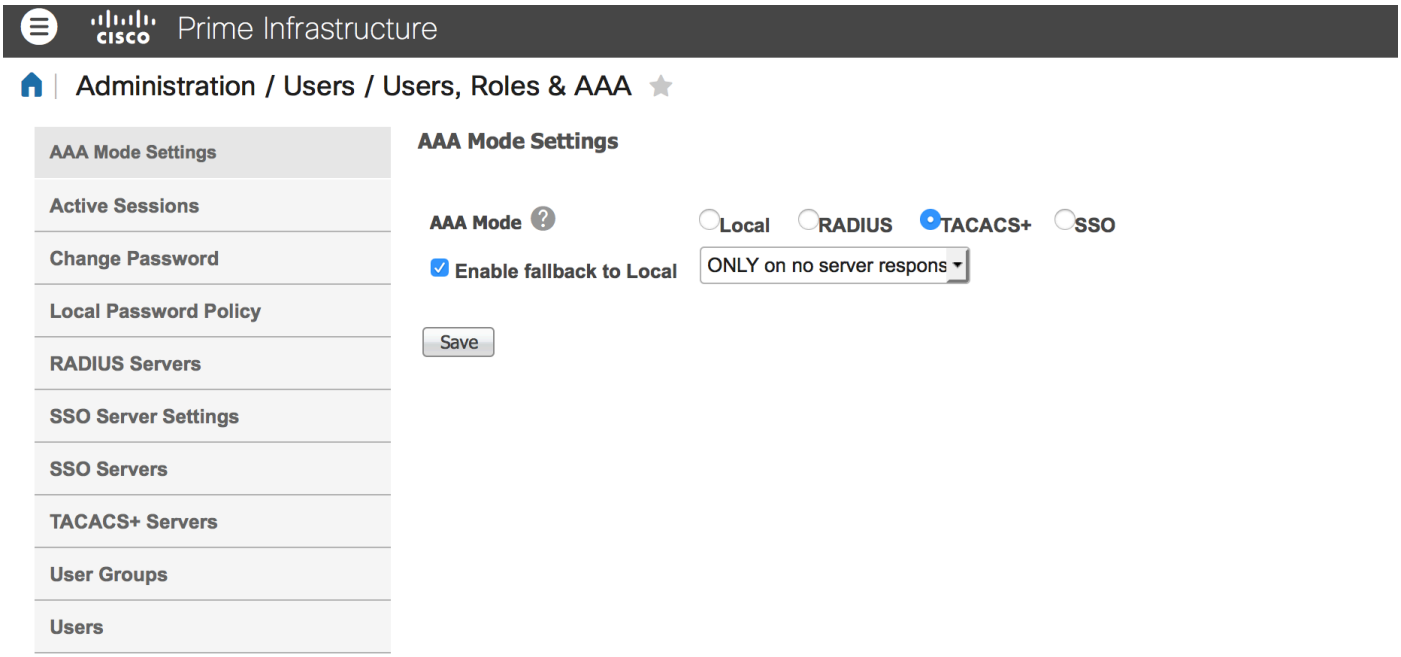
PI での AAA モードの設定

認証、認可、およびアカウンティング（ AAA ）モードを選択するには、次の手順を実行します。

ステップ 1：[Administration] > [AAA] に移動します。

手順 2：左側のサイドバー メニューから [AAA Mode] を選択すると、次のようなページが表示さ

れます。

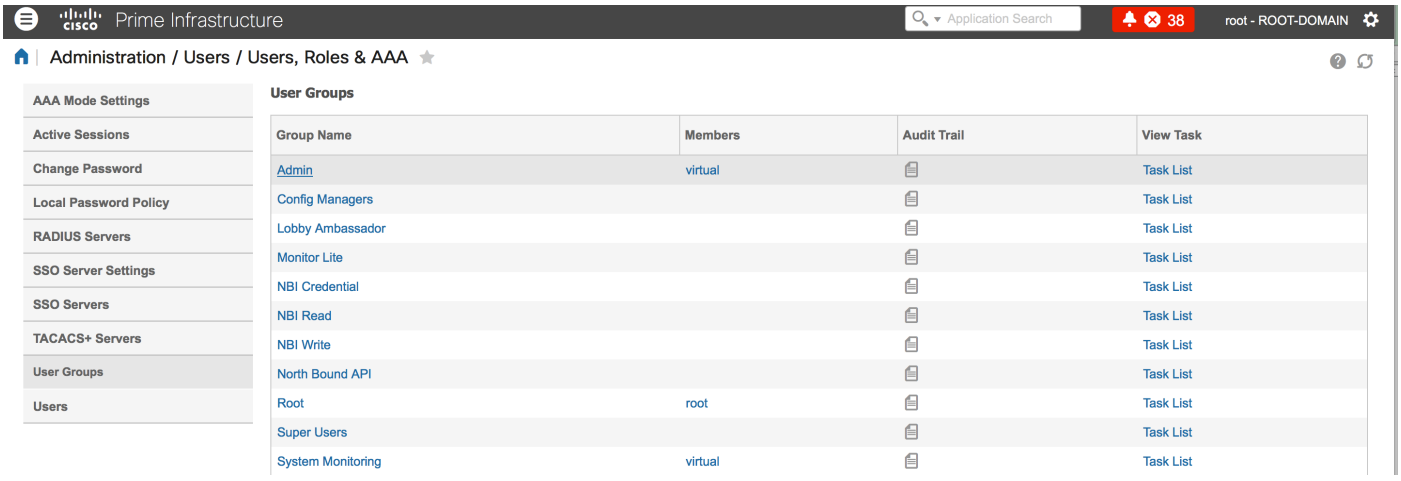


手順 3：[TACACS+] を選択します。

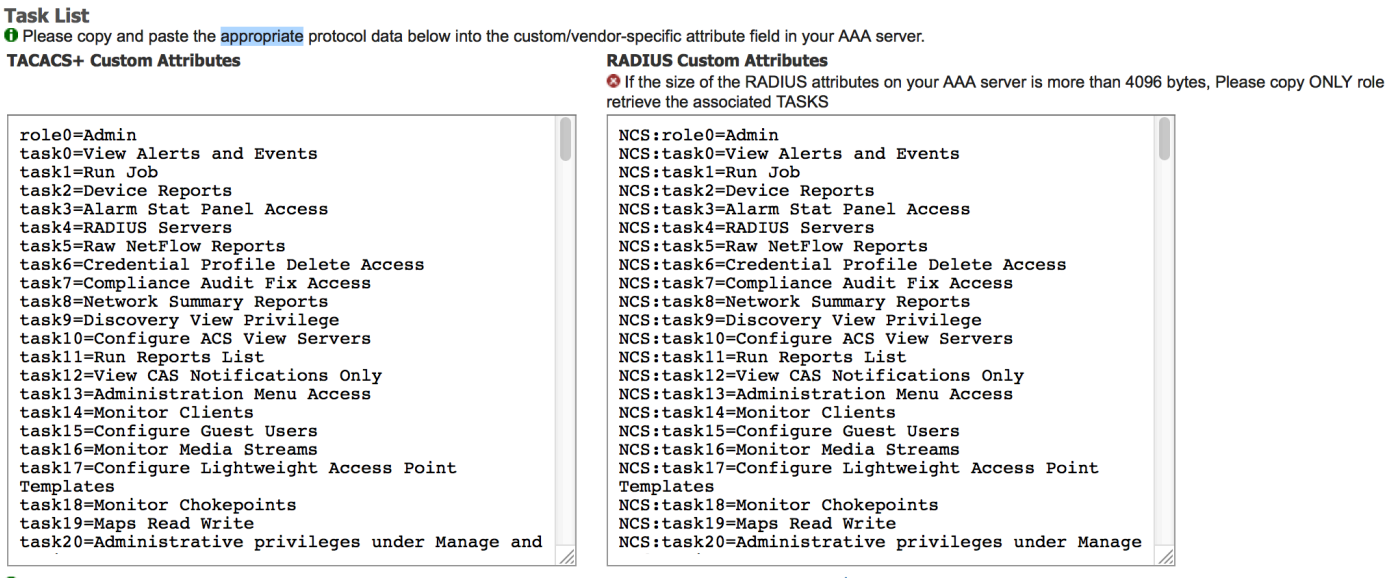
ステップ 4 ACS サーバに到達できないときに管理者にローカル データベースを使用させる場合は、[Enable Fallback to Local] チェックボックスをオンにします。 これは推奨設定です。

PI からのユーザ ロール属性の取得

ステップ 1：[Administration] > [AAA] > [User Groups] の順に移動します。 次の例は、管理者の認証を示しています。 リストで [Admin] グループ名を探し、右側の [Task List] オプションをクリックします（下記の図を参照）。



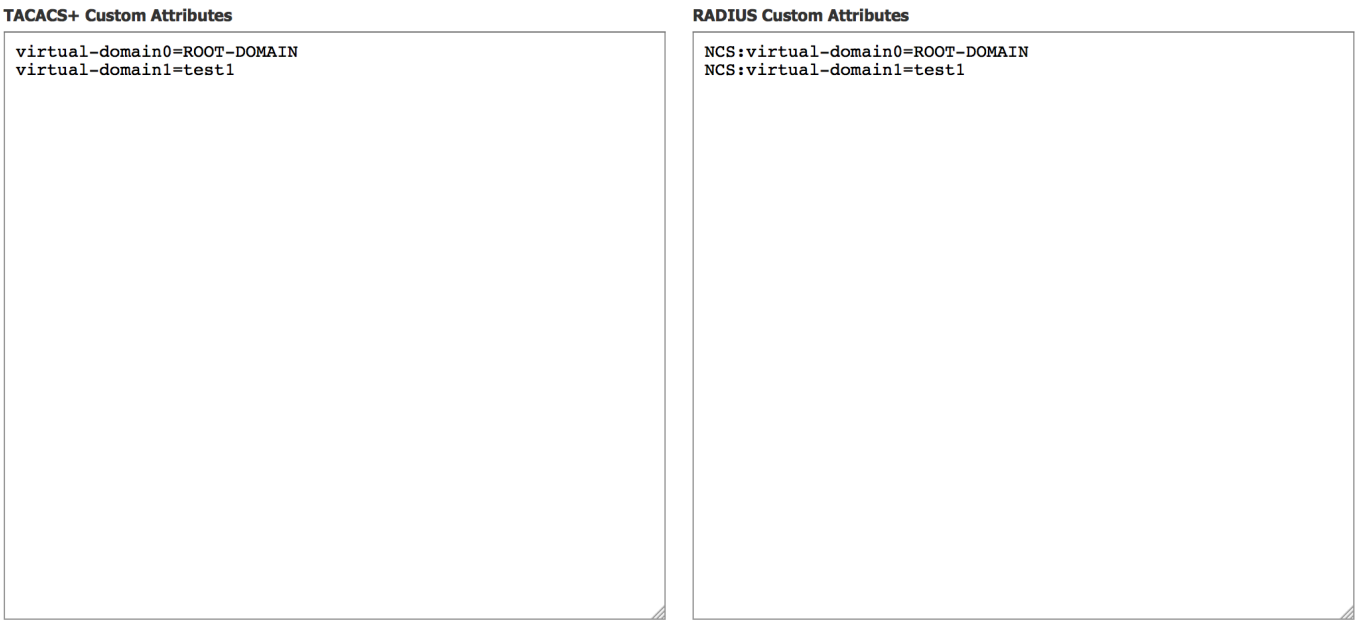
[Task List] オプションをクリックすると、次のようなウィンドウが表示されます。



手順 2：これらの属性をコピーしてメモ帳ファイルに保存します。

ステップ 3 ACS サーバにカスタム仮想ドメイン属性を追加する必要がある場合があります。 カスタム仮想ドメイン属性は、同じ [Task List] ページの下部から利用できます。

手順 4：仮想ドメイン属性ページに移動するための [click here] オプションをクリックすると、次ようなページが表示されます。

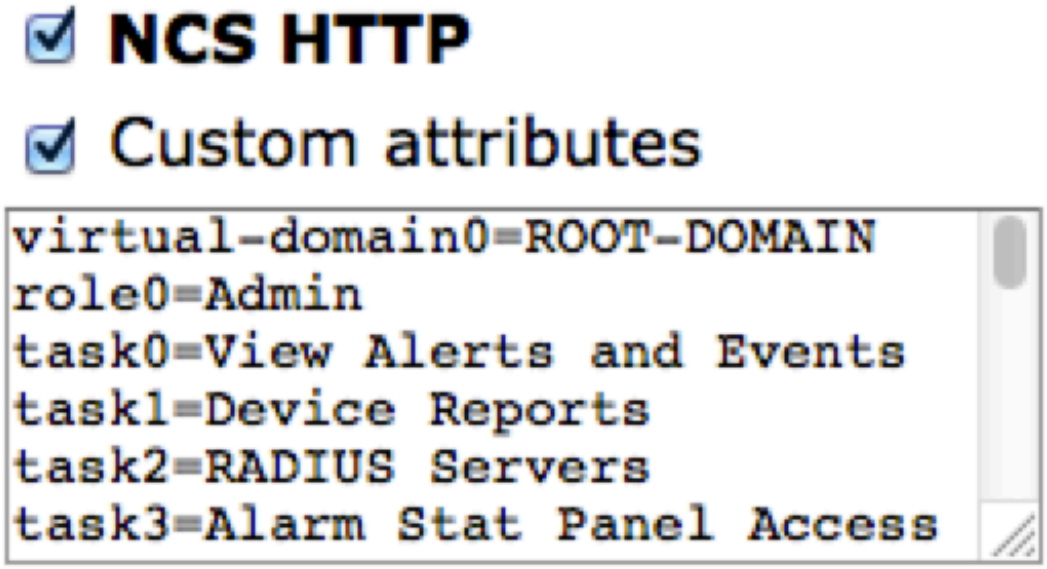


ACS 4.2 の設定

ステップ 1：[ACS Admin GUI] にログインして、[Interface Configuration] > [TACACS+] に移動します。

手順 2：Prime 用の新しいサービスを作成します。 この例では、**NCS** というサービス名が設定されています（ 下記の図を参照 ）。

手順 3：ステップ 2 で作成したメモ帳から、すべての属性をユーザまたはグループの設定に追加します。 仮想ドメイン属性が追加されたことを確認します。



手順 4：[OK] をクリックします。

確認

作成した新しいユーザ名で Prime にログインして、**Admin** ロールを持っていることを確認します。

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

/opt/CSCOlumos/logs ディレクトリで Prime の root CLI を使用して、usermgmt.log を検査します。 エラー メッセージがないことを確認します。

```
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - [        [TacacsLoginModule]
user entered username: 138527]
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - [        [TacacsLoginModule]
Primary server=172.18.70.243:49]
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - Thread Id : [835], Entering
Method : [login], Class : [com.cisco.xmp.jaas.tacacs.TacacsLoginClient].
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - Thread Id : [835], Entering
Method : [login], Class : [com.cisco.xmp.jaas.tacacs.SecondaryTacacsLoginClient].
2016-05-12 15:24:18,518 [http-bio-443-exec-10] INFO  usermgmt - [Tacacs:connectTacacs()] :
[prepare to ping TACACS+ server (> 0):/172.18.70.243 (-1)].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] INFO  usermgmt - [Tacacs:connectTacacs()] :
[Tacacs: Num of ACS is  3].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] INFO  usermgmt - [Tacacs:connectTacacs()] :
[Tacacs:activeACSIndex is  0].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] INFO  usermgmt - [Tacacs:connectTacacs()] :
[Tacacs: Unable to connect to Server 2: /172.18.70.243 Reason: Connection refused].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] DEBUG usermgmt - [        [Thu May 12 15:24:18
EST 2016] [TacacsLoginModule] exception in client.login( primaryServer, primaryPort,seconda..:
com.cisco.xmp.jaas.XmpAuthenticationServerException: Server Not Reachable: Connection refused]
```

この例はエラー メッセージのサンプルを示しています。エラー メッセージは、ファイアウォールや中間デバイス等により接続を拒否された場合など、さまざまな原因によって発生します。