ACS 4.2 TACACS と Prime Infrastructure 統合の設定例

目次

概要

この資料は記述したものです Terminal Access Controller Access Control System （TACACS+）のための設定例を

Cisco Prime Infrastructure （PI）アプリケーションの認証 および 権限。

前提条件

要件

次の項目に関する知識が推奨されます。

- 定義して下さい Access Control Server （ACS）のクライアントと PI を
- ACS および PI の IP アドレスおよび同一の共有秘密キーを定義して下さい

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

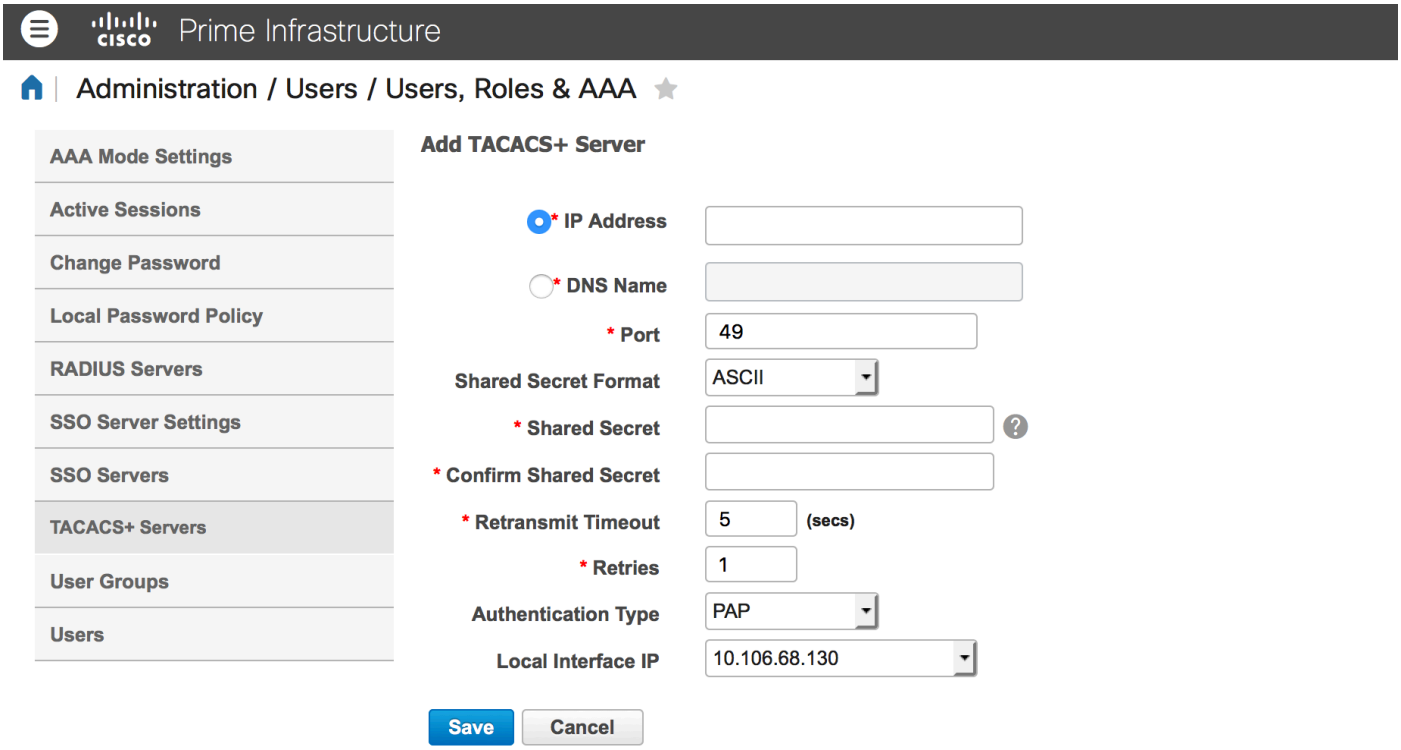
設定

PI の TACACSサーバとして ACS を追加して下さい

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 の**管理** > Users > Users、**ロール及び AAA** へのナビゲート

呼び出します。 左サイドバー メニューから、**サーバを、追加します TACACS+ サーバを**『Go』をクリック します 『TACACS+』 を選択 すればページはイメージに示すように提示されます:



ステップ 3. ACS サーバの IP アドレスを追加して下さい。

ステップ 4.設定される ACS サーバで TACACS+ 共有秘密を入力して下さい。

ステップ 5.**確認共有秘密** テキストボックスで共有秘密を再入力して下さい。

ステップ 6.デフォルト設定でフィールドの他を残して下さい。

ステップ 7. 『SUBMIT』 をクリック して下さい。

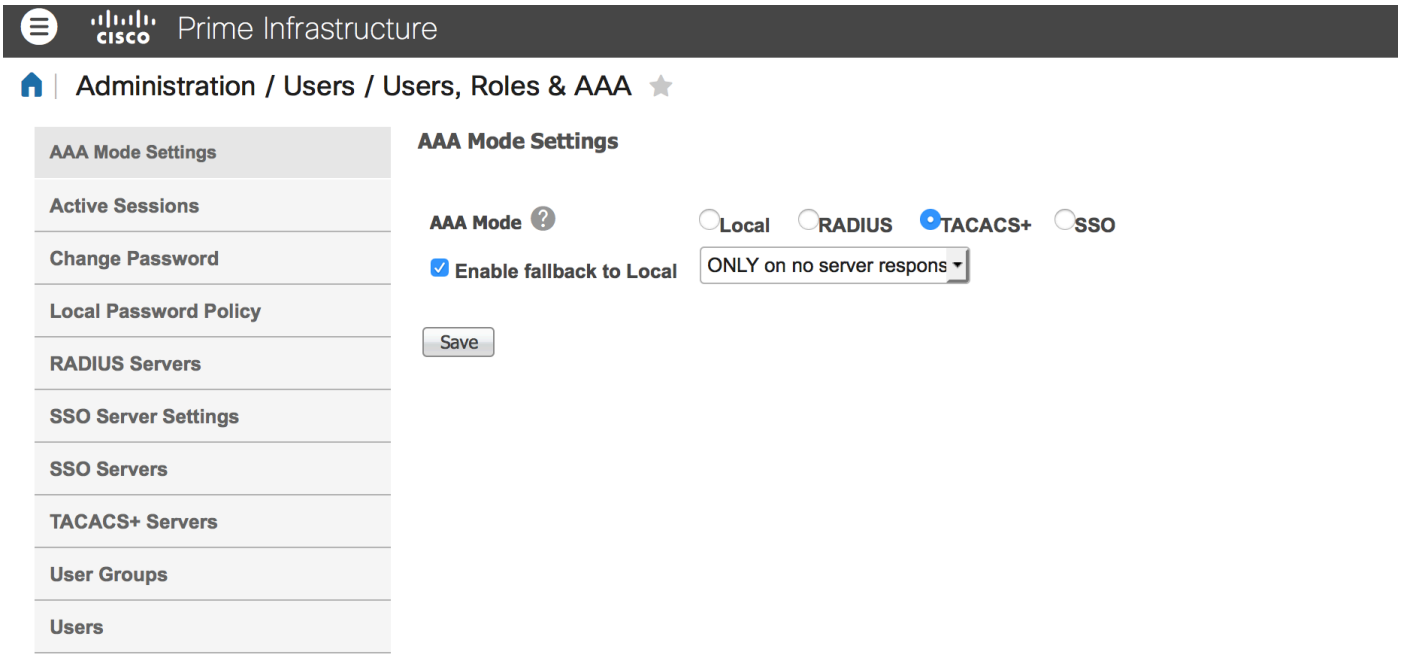
PI の AAA モード設定

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** へのナビゲート。

ステップ 2.左サイドバー メニューから **AAA モードを**、イメージに示すようにページを見る場合

があります選択して下さい:

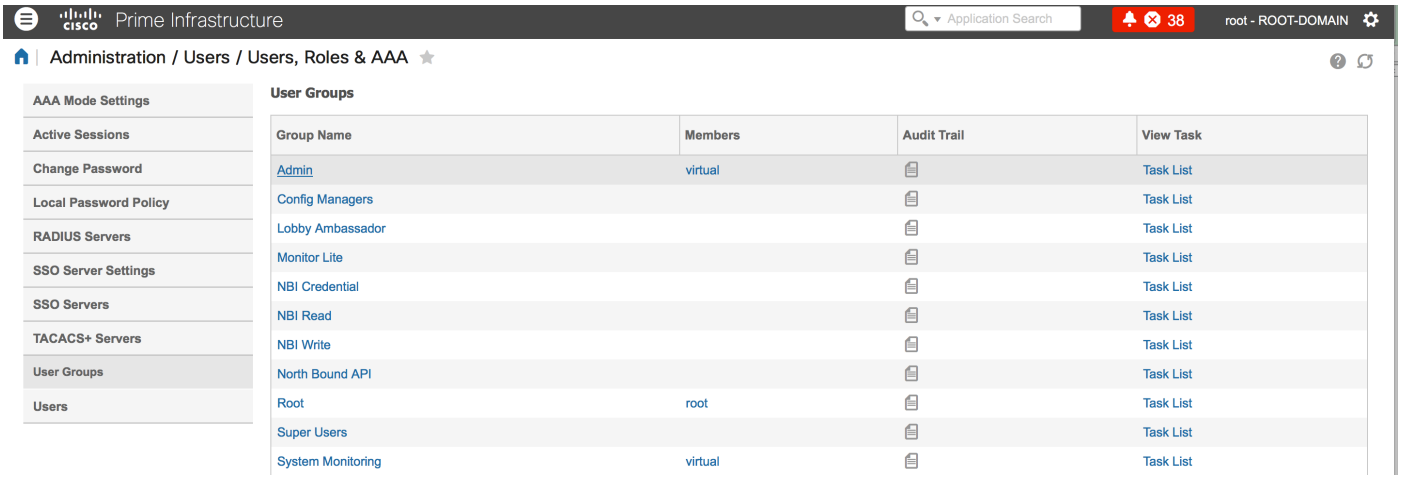


ステップ 3. 『TACACS+』 を選択 して下さい。

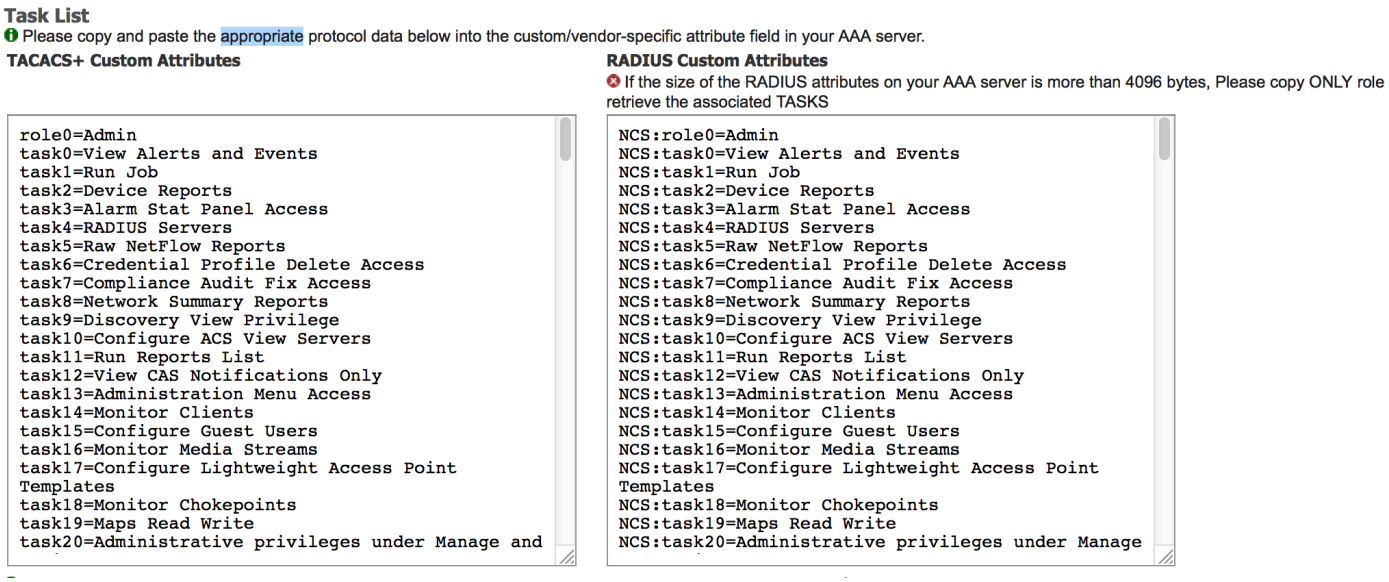
ステップ 4 ACS サーバが到達可能のとき管理者にローカルデータベースを使用してほしい場合、**ローカル** ボックス**にイネーブル フォールバック**をチェックして下さい。 これは推奨 設定です。

PI からの検索ユーザ ロール属性

ステップ 1. **Administration > AAA > ユーザグループ**へのナビゲート。 次の例は、管理者の認証を示しています。 リストの **Admin group 名前**を探し、イメージに示すように右の**課業 表**オプションを、クリックして下さい:



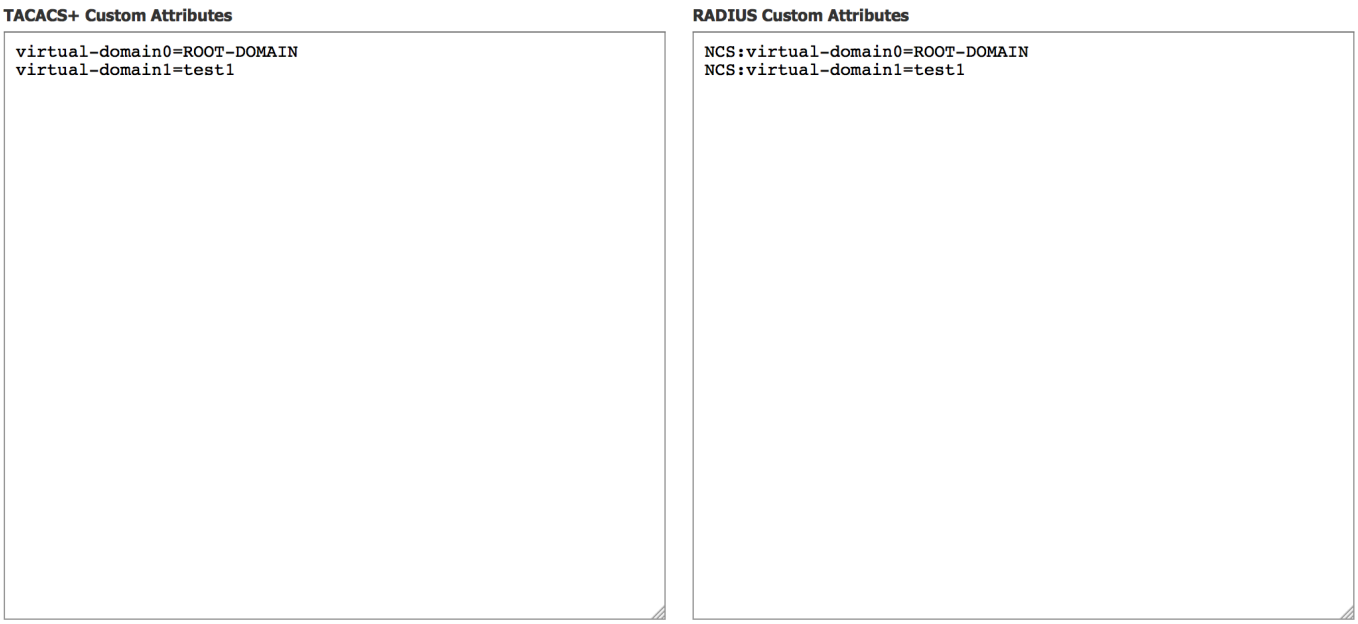
課業 表オプションをクリックすれば、ウィンドウはイメージに示すように、現われます:



ステップ 2.これらの属性をコピーし、テキストエディタ ファイルでそれを保存して下さい。

ステップ 3 ACS サーバのカスタム バーチャル ドメイン属性を追加する必要がある場合もあります。 カスタム バーチャル ドメイン属性は同じ課業 表ページの底に利用できます。

ステップ 4.バーチャル ドメイン属性ページを得るためにオプションを『Click Here』 をクリックすればイメージに示すようにページを、表示できます:

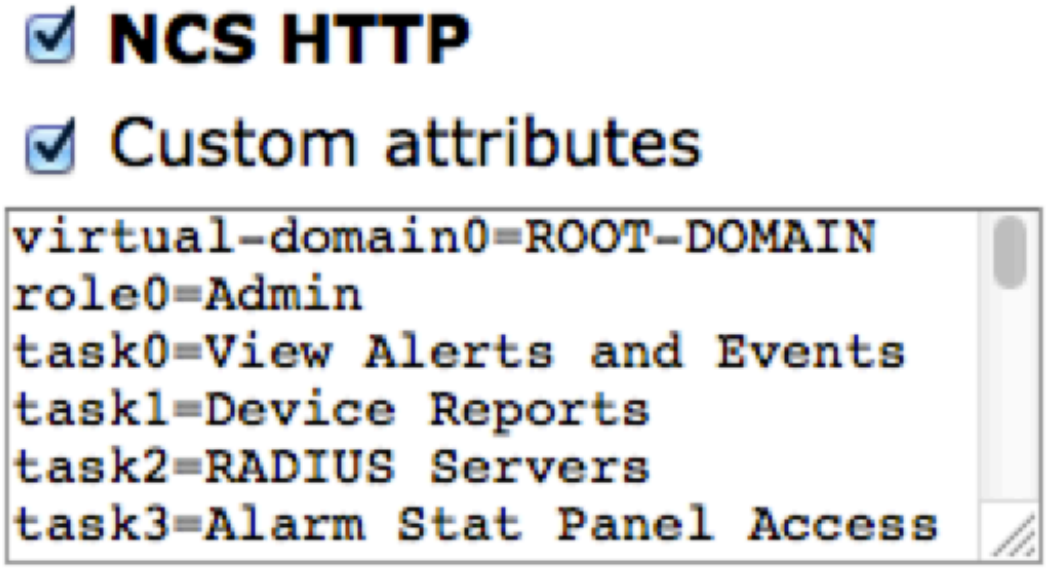


ACS 4.2 を設定して下さい

ステップ 1. ACS Admin GUI へのログインは Interface Configuration > TACACS+ ページに、ナビゲートし。

ステップ 2.プライム記号のための新しいサービスを作成して下さい。 この例はイメージに示すように名前 NCS で、設定されるサービス名を表記したものです:

ステップ 3.ユーザかグループ設定にステップ 2 で作成されるテキストエディタからすべての属性を追加して下さい。 バーチャル ドメイン属性を追加するために確認して下さい。



ステップ 4. 『OK』 をクリック して下さい。

確認

作成し、Admin ロールがあることを確認する新規 ユーザ ユーザー名のプライム記号へのログイン。

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 ディレクトリで利用可能な主なルート CLI からの usermgmt.log を検討して下さい。 エラーメッセージがあるかどうか確認して下さい。

```
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]
```

この例はファイアウォールによって拒否された接続のようなさまざまな原因が原因である可能性があるまたは中間デバイス先祖など示したものです工ラーメッセージのサンプルを