

ACS 4.2 TACACS と Prime Infrastructure 統合の 設定例

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[設定](#)

[PI に TACACS サーバとして ACS を追加](#)

[PI での AAA モードの設定](#)

[PI からのユーザ ロール属性の取得](#)

[ACS 4.2 の設定](#)

[確認](#)

[トラブルシューティング](#)

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。

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

Add TACACS+ Server

* IP Address

* DNS Name

* Port 49

Shared Secret Format ASCII

* Shared Secret ?

* Confirm Shared Secret

* Retransmit Timeout 5 (secs)

* Retries 1

Authentication Type PAP

Local Interface IP 10.106.68.130

Save Cancel

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、およびアカウントリング (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。

Administration / Users / Users, Roles & AAA ★

AAA Mode Settings

AAA Mode ? Local RADIUS TACACS+ SSO

Enable fallback to Local ONLY on no server respons

Save

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) 。

Administration / Users / Users, Roles & AAA ★

User Groups

Group Name	Members	Audit Trail	View Task
Admin	virtual		Task List
Config Managers			Task List
Lobby Ambassador			Task List
Monitor Lite			Task List
NBI Credential			Task List
NBI Read			Task List
NBI Write			Task List
North Bound API			Task List
Root	root		Task List
Super Users			Task List
System Monitoring	virtual		Task List

[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。

Task List

① Please copy and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

TACACS+ Custom Attributes

```
role0=Admin
task0=View Alerts and Events
task1=Run Job
task2=Device Reports
task3=Alarm Stat Panel Access
task4=RADIUS Servers
task5=Raw NetFlow Reports
task6=Credential Profile Delete Access
task7=Compliance Audit Fix Access
task8=Network Summary Reports
task9=Discovery View Privilege
task10=Configure ACS View Servers
task11=Run Reports List
task12=View CAS Notifications Only
task13=Administration Menu Access
task14=Monitor Clients
task15=Configure Guest Users
task16=Monitor Media Streams
task17=Configure Lightweight Access Point
Templates
task18=Monitor Chokepoints
task19=Maps Read Write
task20=Administrative privileges under Manage and
```

RADIUS Custom Attributes

② If the size of the RADIUS attributes on your AAA server is more than 4096 bytes, Please copy ONLY role retrieve the associated TASKS

```
NCS:role0=Admin
NCS:task0=View Alerts and Events
NCS:task1=Run Job
NCS:task2=Device Reports
NCS:task3=Alarm Stat Panel Access
NCS:task4=RADIUS Servers
NCS:task5=Raw NetFlow Reports
NCS:task6=Credential Profile Delete Access
NCS:task7=Compliance Audit Fix Access
NCS:task8=Network Summary Reports
NCS:task9=Discovery View Privilege
NCS:task10=Configure ACS View Servers
NCS:task11=Run Reports List
NCS:task12=View CAS Notifications Only
NCS:task13=Administration Menu Access
NCS:task14=Monitor Clients
NCS:task15=Configure Guest Users
NCS:task16=Monitor Media Streams
NCS:task17=Configure Lightweight Access Point
Templates
NCS:task18=Monitor Chokepoints
NCS:task19=Maps Read Write
NCS:task20=Administrative privileges under Manage
```

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。

① Virtual Domain custom attributes are mandatory. To add custom attributes related to Virtual Domains, please click [here](#).

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。

TACACS+ Custom Attributes

```
virtual-domain0=ROOT-DOMAIN
virtual-domain1=test1
```

RADIUS Custom Attributes

```
NCS:virtual-domain0=ROOT-DOMAIN
NCS:virtual-domain1=test1
```

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) 。

New Services

		Service	Protocol
<input checked="" type="checkbox"/>	<input type="checkbox"/>	ciscowlc	common
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Wireless-WCS	HTTP
<input checked="" type="checkbox"/>	<input type="checkbox"/>	NCS	HTTP
<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>		

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。

NCS HTTP

Custom attributes

```
virtual-domain0=ROOT-DOMAIN
role0=Admin
task0=View Alerts and Events
task1=Device Reports
task2=RADIUS Servers
task3=Alarm Stat Panel Access
```

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。