

ACS 4.2 TACACS と Prime Infrastructure 統合の 設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[設定](#)

[PI の TACACSサーバとして ACS を追加して下さい](#)

[PI の AAA モード設定](#)

[PI からの検索ユーザ ロール属性](#)

[ACS 4.2 を設定して下さい](#)

[確認](#)

[トラブルシューティング](#)

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:

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

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 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:

AAA Mode Settings

AAA Mode [?] Local RADIUS TACACS+ SSO

Enable fallback to Local

Save

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:

Administration / Users / Users, Roles & AAA

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

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:

Task List

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

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
```

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。

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

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:

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 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:

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"/>		

ステップ 3. ユーザ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。

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
```

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エラーメッセージのサンプルを