

Prime-Infrastruktur-Integration mit ACS 4.2

TACACS - Konfigurationsbeispiel

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Konfigurationen](#)

[ACS als TACACS-Server in PI hinzufügen](#)

[AAA-Moduseinstellungen in PI](#)

[Abrufen von Benutzerrollenattributen von PI](#)

[Konfigurieren von ACS 4.2](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

Dieses Dokument beschreibt das Konfigurationsbeispiel für das Terminal Access Controller Access-Control System (TACACS+).

Authentifizierung und Autorisierung in der Cisco Prime Infrastructure (PI)-Anwendung.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Definieren von PI als Client im Access Control Server (ACS)
- Definieren Sie die IP-Adresse und einen identischen geheimen Schlüssel für ACS und PI.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ACS Version 4.2
- Prime Infrastructure Version 3.0

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Konfigurationen

ACS als TACACS-Server in PI hinzufügen

Gehen Sie wie folgt vor, um ACS als TACACS-Server hinzuzufügen:

Schritt 1: Navigieren zu **Administration > Benutzer > Benutzer, Rollen und AAA in PI**

Schritt 2: Wählen Sie im linken Seitenleistenmenü **TACACS+ Servers** aus, klicken Sie unter **TACACS+-Server hinzufügen** auf **Go**, und die Seite wird angezeigt, wie im Bild gezeigt:

The screenshot shows the 'Add TACACS+ Server' configuration page in Cisco Prime Infrastructure. On the left is a navigation sidebar with options like 'AAA Mode Settings', 'Active Sessions', 'Change Password', 'Local Password Policy', 'RADIUS Servers', 'SSO Server Settings', 'SSO Servers', 'TACACS+ Servers', 'User Groups', and 'Users'. The main area is titled 'Add TACACS+ Server' and contains the following fields:

- * IP Address (text input)
- * DNS Name (text input)
- * Port: 49 (text input)
- Shared Secret Format: ASCII (dropdown menu)
- * Shared Secret: (text input with a help icon)
- * Confirm Shared Secret: (text input)
- * Retransmit Timeout: 5 (secs) (text input)
- * Retries: 1 (text input)
- Authentication Type: PAP (dropdown menu)
- Local Interface IP: 10.106.68.130 (dropdown menu)

At the bottom are 'Save' and 'Cancel' buttons.

Schritt 3: Fügen Sie die IP-Adresse des ACS-Servers hinzu.

Schritt 4: Geben Sie den im ACS-Server konfigurierten gemeinsamen geheimen TACACS+-Schlüssel ein.

Schritt 5: Geben Sie den freigegebenen geheimen Schlüssel erneut in das Textfeld **Freigegebenen geheimen Schlüssel bestätigen** ein.

Schritt 6: Belassen Sie die übrigen Felder mit den Standardeinstellungen.

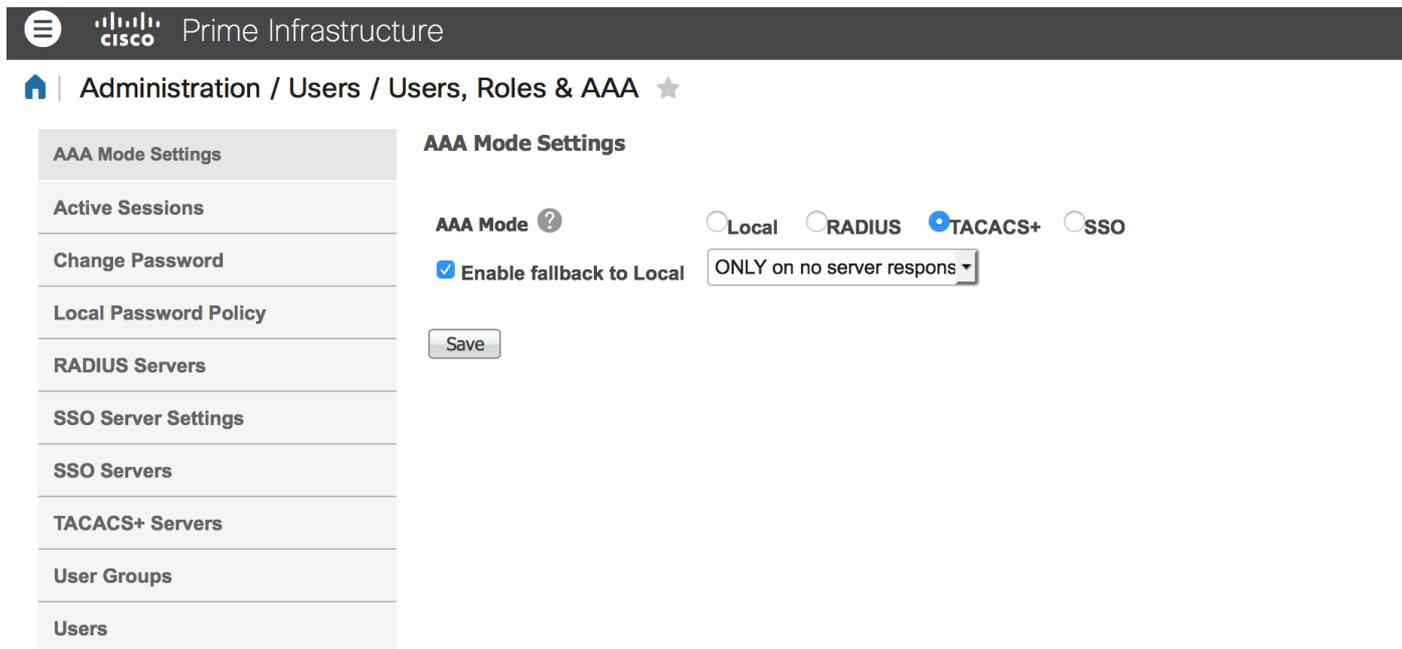
Schritt 7: Klicken Sie auf **Senden**.

AAA-Moduseinstellungen in PI

Gehen Sie wie folgt vor, um einen AAA-Modus (Authentication, Authorization, and Accounting) auszuwählen:

Schritt 1: Navigieren Sie zu **Administration > AAA**.

Schritt 2: Wählen Sie **AAA Mode** aus dem linken Seitenleistenmenü aus. Sie können die Seite wie im Bild gezeigt sehen:

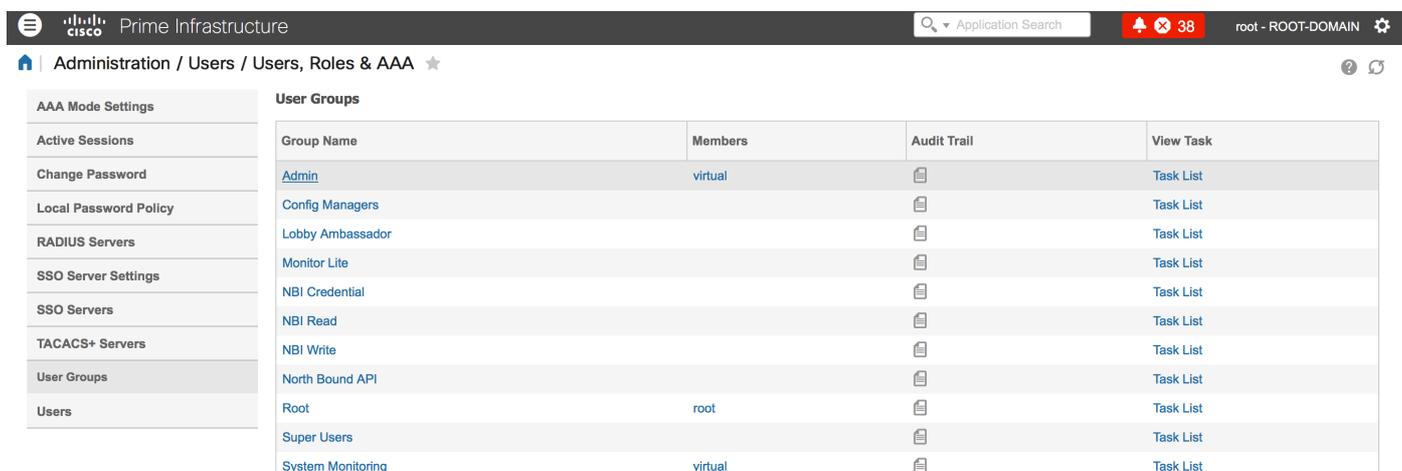


Schritt 3: Wählen Sie **TACACS+** aus.

Schritt 4: Aktivieren Sie das Kontrollkästchen **Enable Fallback to Local (Fallback an Lokalen aktivieren)**, wenn der Administrator die lokale Datenbank verwenden soll, wenn der ACS-Server nicht erreichbar ist. Dies ist eine empfohlene Einstellung.

Abrufen von Benutzerrollenattributen von PI

Schritt 1: Navigieren Sie zu **Administration > AAA > User Groups**. Dieses Beispiel zeigt die Administratorauthentifizierung. Suchen Sie den **Admin-Gruppennamen** in der Liste, und klicken Sie wie im Bild gezeigt auf die Option **Aufgabenliste** rechts:



Wenn Sie auf die Option **Aufgabenliste** klicken, wird das Fenster angezeigt, wie im Bild gezeigt:

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
```

Schritt 2: Kopieren Sie diese Attribute und speichern Sie sie in einer Notizblock-Datei.

Schritt 3: Möglicherweise müssen Sie dem ACS-Server benutzerdefinierte Attribute für virtuelle Domänen hinzufügen. Benutzerdefinierte Attribute virtueller Domänen sind unten auf derselben Seite der Aufgabenliste verfügbar.

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

Schritt 4: Klicken Sie auf **Klicken Sie hier**, um die Attribute "Virtual Domain" (Virtuelle Domäne) anzuzeigen. Die Seite wird angezeigt, wie im Bild gezeigt:

TACACS+ Custom Attributes

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

RADIUS Custom Attributes

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

Konfigurieren von ACS 4.2

Schritt 1: Melden Sie sich bei der **ACS Admin-GUI** an, und navigieren Sie zur **Schnittstellenkonfiguration > TACACS+-Seite**.

Schritt 2: Erstellen Sie einen neuen Service für Prime. Dieses Beispiel zeigt einen Dienstnamen, der mit dem Namen **NCS** konfiguriert wurde, wie in der Abbildung gezeigt:

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"/>		

Schritt 3: Fügen Sie alle in Schritt 2 erstellten Attribute von Notizblock zur Benutzer- oder Gruppenkonfiguration hinzu. Stellen Sie sicher, dass virtuelle Domänenattribute hinzugefügt werden.

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
```

Schritt 4: Klicken Sie auf OK.

Überprüfen

Melden Sie sich mit dem von Ihnen erstellten neuen Benutzernamen beim Prime an, und bestätigen Sie, dass Sie die **Administratorrolle** haben.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Überprüfen Sie usermgmt.log von der primären Root-CLI, die im Verzeichnis `/opt/CSColumos/logs` verfügbar ist. Überprüfen Sie, ob Fehlermeldungen vorliegen.

```
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]
```

Dieses Beispiel zeigt ein Beispiel für eine Fehlermeldung, die möglicherweise auf verschiedene Ursachen zurückzuführen ist, z. B. auf eine von einer Firewall verweigerte Verbindung oder ein zwischengeschaltetes Gerät usw.