

# Prime-infrastructuur voor integratie met ACS 4.2 TACACS-configuratievoorbeeld

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Configuraties](#)

[ACS als TACACS-server in IP toevoegen](#)

[AAA-modus instellingen in IP](#)

[Eigenschappen gebruikersrol van PI ophalen](#)

[ACS 4.2 configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

## Inleiding

Dit document beschrijft het configuratievoorbeeld voor terminaal toegangscontrollerkaart (TACACS+)

Verificatie en autorisatie bij de Cisco Prime Infrastructuur (PI)-toepassing.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- IP als client definiëren in de Access Control Server (ACS)
- Bepaal het IP-adres en een identieke gedeelde geheime sleutel op de ACS en IP

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ACS versie 4.2
- Prime-infrastructuurrelease 3.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

# Configureren

## Configuraties

### ACS als TACACS-server in IP toevoegen

Voltooi deze stappen om ACS als een TACACS-server toe te voegen:

Stap 1. navigeren naar **Administratie > Gebruikers > Gebruikers, rollen en AA in PI**

Stap 2. Selecteer **TACACS+ servers** in het menu links en selecteer **TACACS+ servers** en klik op **Ga** en de pagina verschijnt zoals in de afbeelding:

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

Stap 3. Voeg het IP-adres van de ACS-server toe.

Stap 4. Voer het gedeeld geheim TACACS+ in dat in de ACS-server is ingesteld.

Stap 5. Voer het gedeelde geheim opnieuw in het tekstvak **Gedeeld geheim bevestigen**.

Stap 6. Laat de rest van de velden op hun standaardinstelling staan.

Stap 7. Klik op **Indienen**.

### AAA-modus instellingen in IP

Voltooi de volgende stappen om een AAA-modus (verificatie, autorisatie en accounting) te kiezen:

Stap 1. Navigeer naar **Administratie > AAA**.

Stap 2. Kies **de AAA-modus** in het menu links, u kunt de pagina zien zoals in de afbeelding:

- AAA Mode Settings
- Active Sessions
- Change Password
- Local Password Policy
- RADIUS Servers
- SSO Server Settings
- SSO Servers
- TACACS+ Servers
- User Groups
- Users

### AAA Mode Settings

AAA Mode ?  Local  RADIUS  TACACS+  SSO

Enable fallback to Local ONLY on no server respons

Stap 3. Selecteer **TACACS+**.

Stap 4. Controleer de **Terug naar lokaal** vakje, als u wilt dat de beheerder de lokale gegevensbank gebruikt wanneer de ACS-server niet bereikbaar is. Dit is een aanbevolen instelling.

## Eigenschappen gebruikersrol van PI ophalen

Stap 1. Navigeer naar **Administratie > AAA > gebruikersgroepen**. Dit voorbeeld toont de authenticatie van beheerders. Kijk naar de **Admin Group Name** in de lijst en klik vervolgens op de optie **Automation List** rechts, zoals in de afbeelding:

| Group Name                        | Members | Audit Trail | View Task                 |
|-----------------------------------|---------|-------------|---------------------------|
| <a href="#">Admin</a>             | virtual |             | <a href="#">Task List</a> |
| <a href="#">Config Managers</a>   |         |             | <a href="#">Task List</a> |
| <a href="#">Lobby Ambassador</a>  |         |             | <a href="#">Task List</a> |
| <a href="#">Monitor Lite</a>      |         |             | <a href="#">Task List</a> |
| <a href="#">NBI Credential</a>    |         |             | <a href="#">Task List</a> |
| <a href="#">NBI Read</a>          |         |             | <a href="#">Task List</a> |
| <a href="#">NBI Write</a>         |         |             | <a href="#">Task List</a> |
| <a href="#">North Bound API</a>   |         |             | <a href="#">Task List</a> |
| <a href="#">Root</a>              | root    |             | <a href="#">Task List</a> |
| <a href="#">Super Users</a>       |         |             | <a href="#">Task List</a> |
| <a href="#">System Monitoring</a> | virtual |             | <a href="#">Task List</a> |

Zodra u op de optie **Lijst met taken** klikt, wordt het venster weergegeven, zoals in de afbeelding:

## 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
```

Stap 2. Kopieer deze eigenschappen en bewaar deze in een notebookbestand.

Stap 3. Mogelijk moet u aangepaste virtuele domeineigenschappen in de ACS-server toevoegen. De aangepaste virtuele domeineigenschappen zijn beschikbaar in de onderkant van dezelfde taaklijst.

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

Stap 4. Klik op **deze** optie om de pagina met virtuele domeinmerken te krijgen en u kunt de pagina zien, zoals in de afbeelding:

### 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 configureren

Stap 1. Meld u aan bij de ACS Admin GUI en navigeer naar **interfaceconfiguratie > TACACS+** pagina.

Stap 2. Maak een nieuwe service voor het eerst. Dit voorbeeld toont een servicenaam die met naam **NCS** wordt ingesteld, zoals in de afbeelding wordt weergegeven:

---

## 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"/> |              |          |

Stap 3. Voeg alle eigenschappen van de schrijfblok die in Stap 2 zijn gemaakt toe aan de configuratie van gebruikers of groepen. Zorg ervoor dat u eigenschappen voor een virtueel domein toevoegt.

**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
```

Stap 4. Klik op OK.

## Verifiëren

Meld u aan bij de primeur met de nieuwe gebruikersnaam die u hebt gemaakt en bevestig dat u de Admin-rol hebt.

## Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Bekijk usermgmt.log van prime root CLI beschikbaar in /opt/CSColumos/logs folder. Controleer of er foutmeldingen zijn.

```
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]
```

**Dit voorbeeld toont een monster van foutmelding die om verschillende redenen kan worden veroorzaakt, zoals een verbinding die wordt geweigerd door een firewall of een tijdelijk apparaat enzovoort.**