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

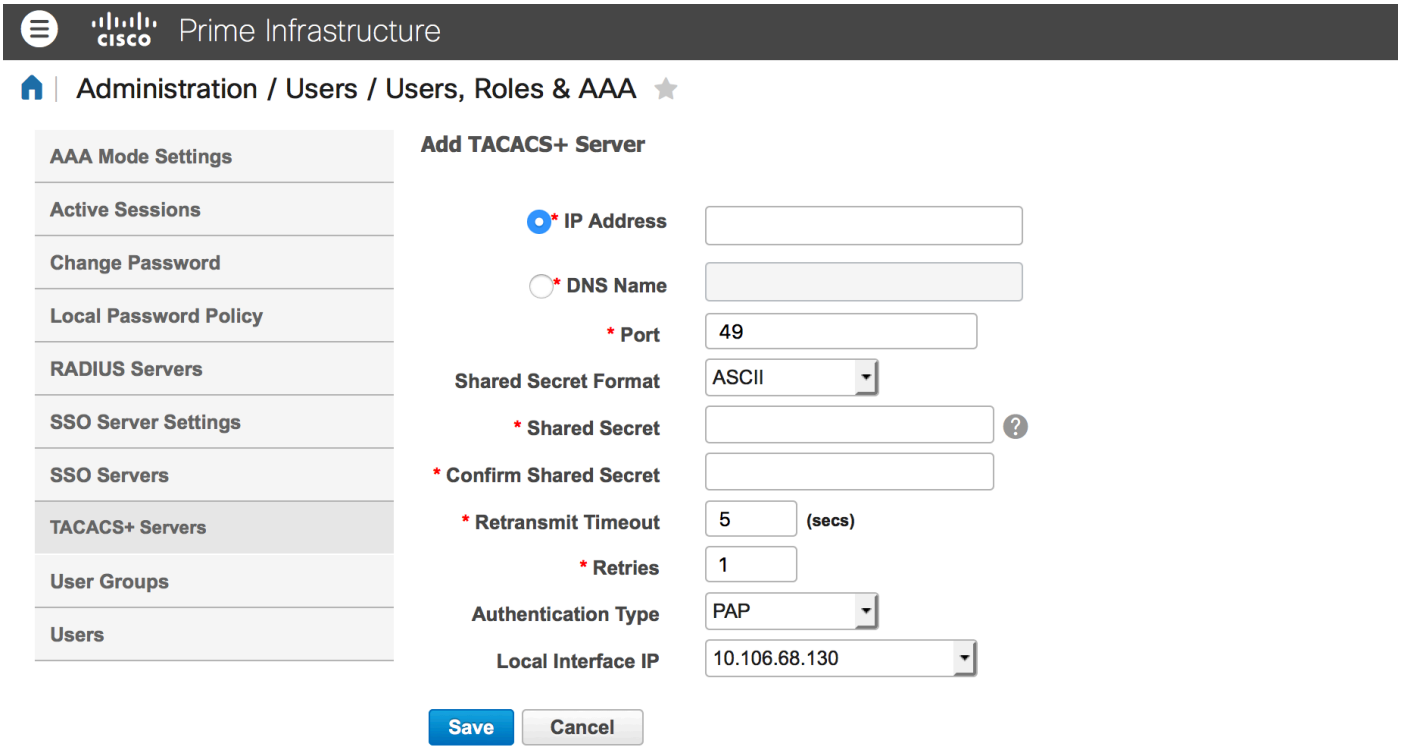
Configuraties

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:



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.

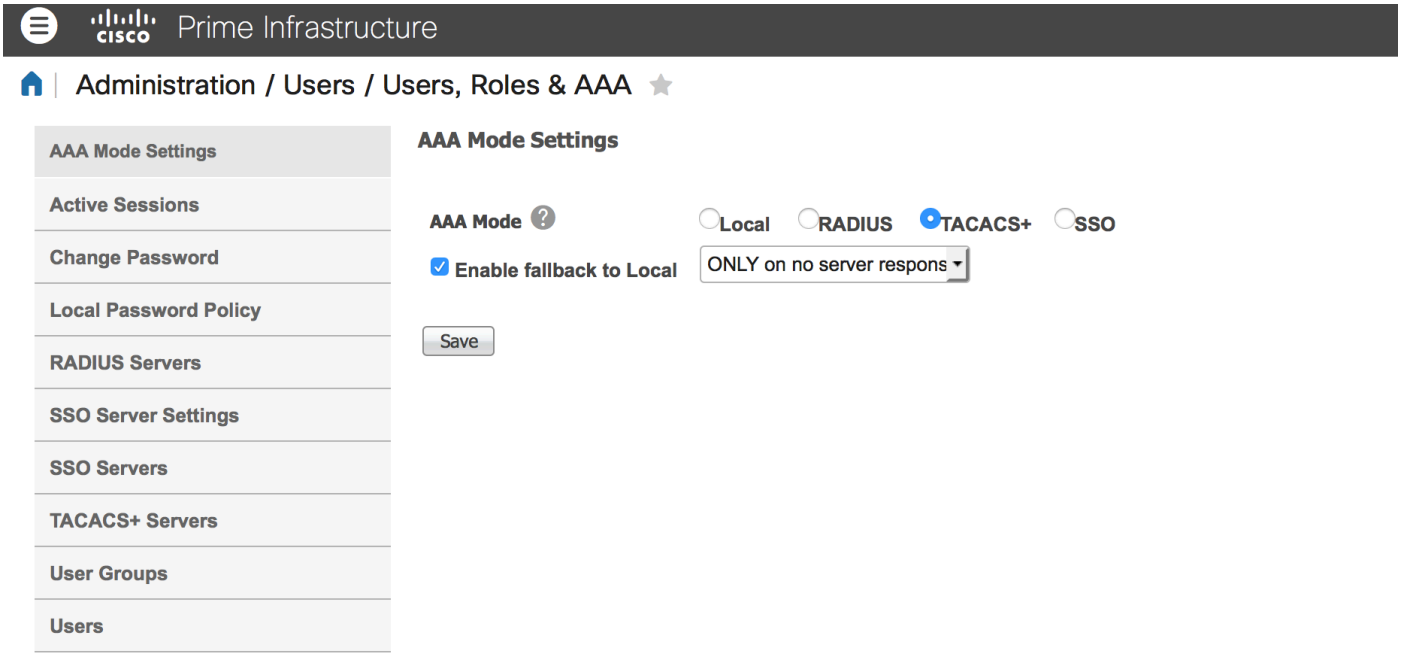
Stap 7. Klik op **Indienen**.

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:

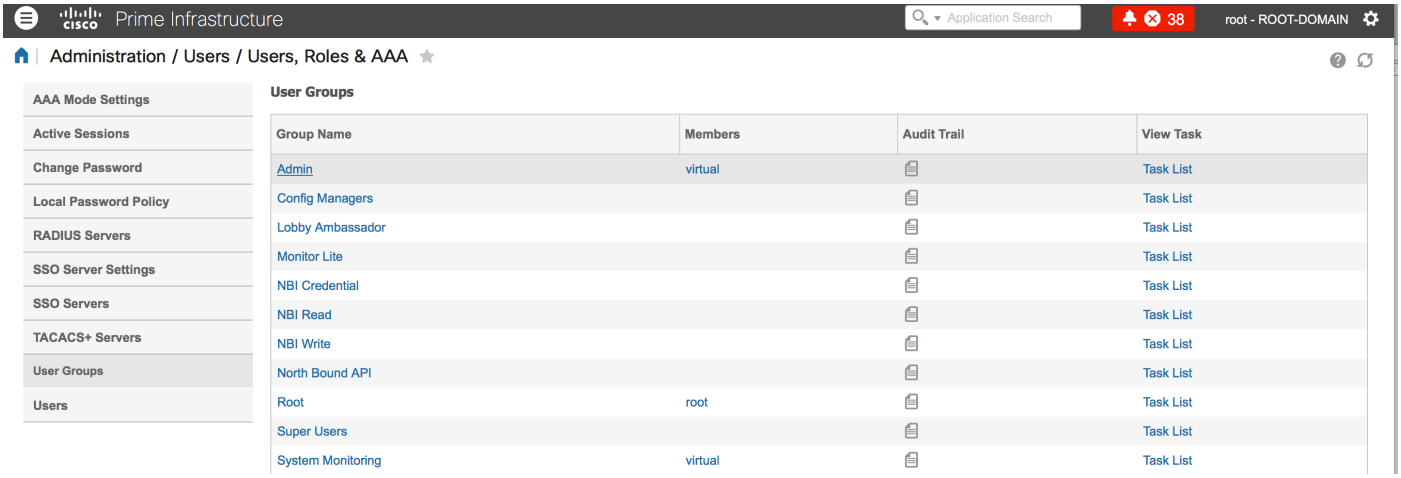


Stap 3. Selecteer **TACACS+**.

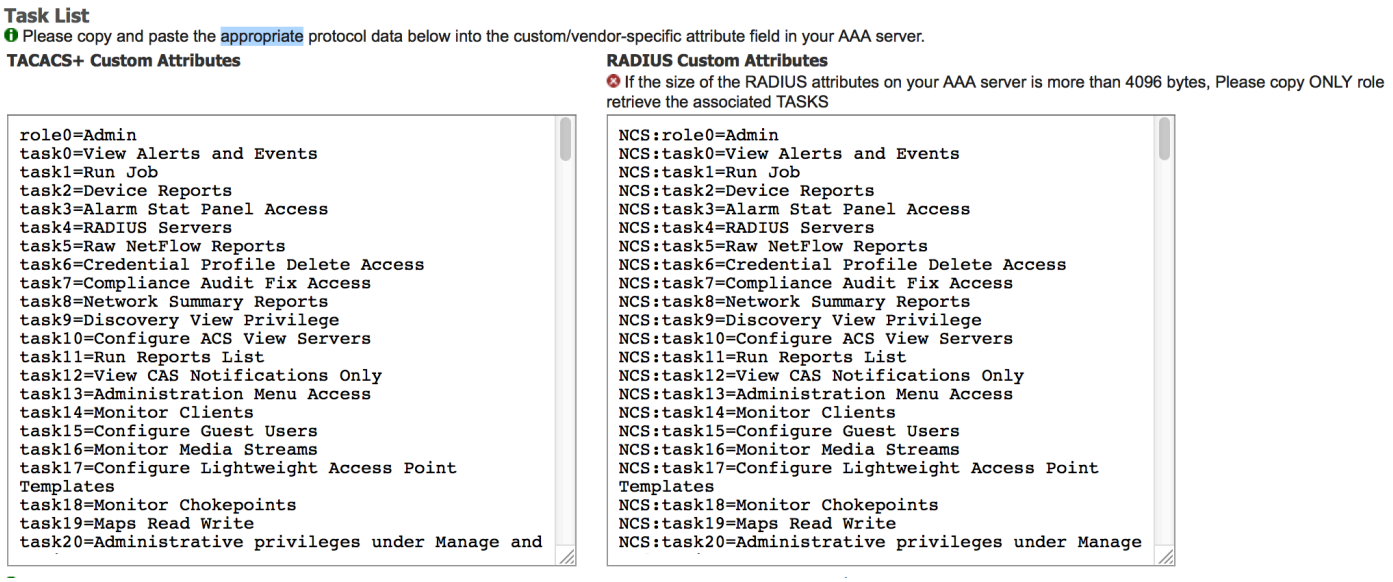
Stap 4. Controleer de **Terug naar lokaal** vakje, als u wilt dat de beheerder de lokale gegevensbank gebruikt wanneer de ACS-server niet bereikbaar is. Dit is een aanbevolen instelling.

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:

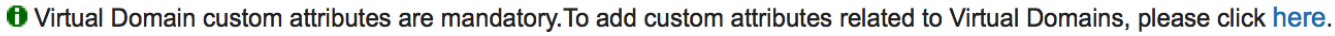


Zodra u op de optie **Lijst met taken** klikt, wordt het venster weergegeven, zoals in de afbeelding:

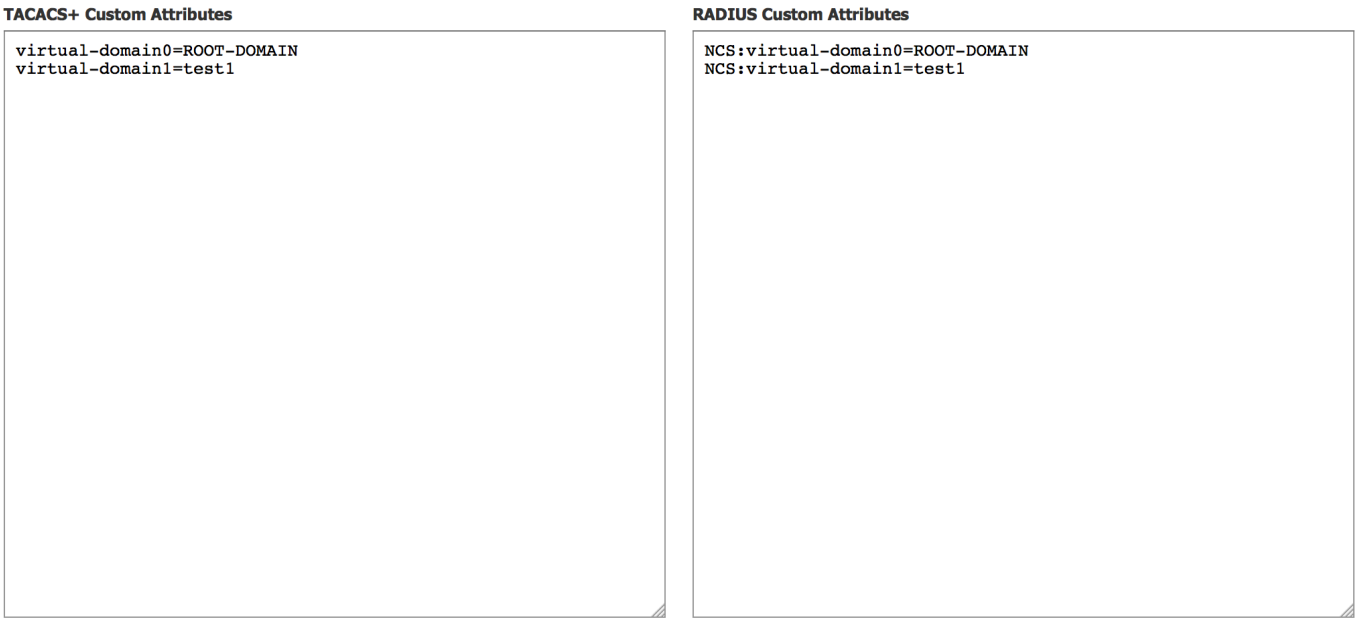


Stap 2. Kopieer deze eigenschappen en bewaar deze in een notebookbestand.

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.



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

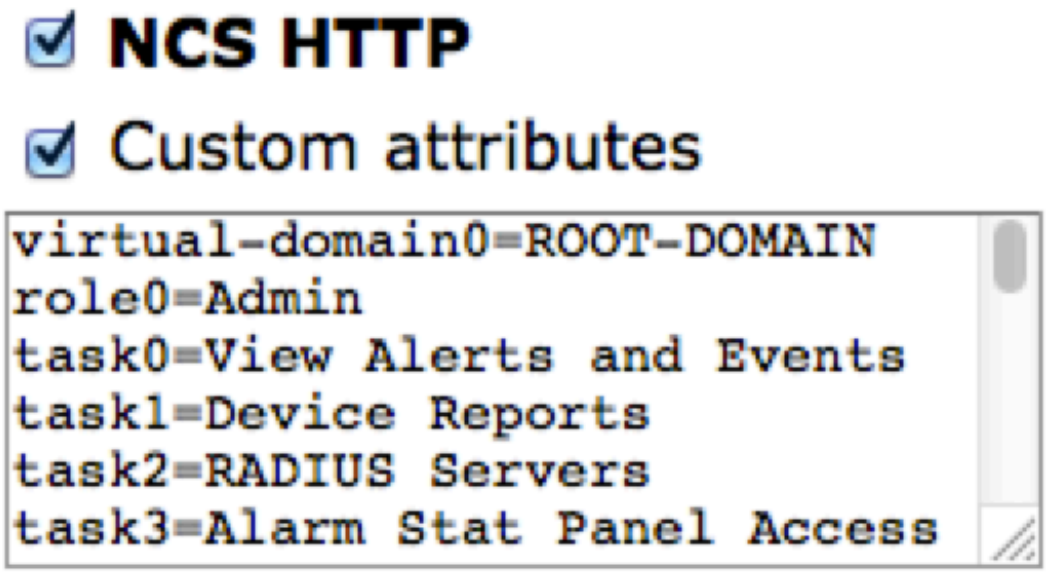


ACS 4.2 configureren

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:

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.



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.