

Esempio di configurazione di Prime Infrastructure Integration con ACS 4.2 TACACS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazioni](#)

[Aggiungi ACS come server TACACS in IP](#)

[Impostazioni modalità AAA in PI](#)

[Recupera attributi ruolo utente da PI](#)

[Configurazione di ACS 4.2](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive l'esempio di configurazione di Terminal Access Controller Access-Control System (TACACS+)

autenticazione e autorizzazione sull'applicazione Cisco Prime Infrastructure (IP).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Definizione di PI come client in Access Control Server (ACS)
- Definire l'indirizzo IP e una chiave segreta condivisa identica su ACS e PI

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ACS versione 4.2
- Prime Infrastructure release 3.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Configurazioni

Aggiungi ACS come server TACACS in IP

Completare questa procedura per aggiungere un ACS come server TACACS:

Passaggio 1. Passare a **Amministrazione > Utenti > Utenti, ruoli e AAA in PI**

Passaggio 2. Dal menu a sinistra della barra laterale, selezionare **TACACS+ Servers**, in **Add TACACS+ servers** (Aggiungi server TACACS+) fare clic su **Go** (Vai) per visualizzare la pagina come mostrato nell'immagine:

The screenshot shows the Cisco Prime Infrastructure interface for adding a TACACS+ server. The breadcrumb navigation is Administration / Users / Users, Roles & AAA. The left sidebar lists various configuration options, with 'TACACS+ Servers' selected. The main form, titled 'Add TACACS+ Server', includes the following fields:

- IP Address (selected)
- DNS Name
- * Port: 49
- Shared Secret Format: ASCII
- * Shared Secret: [Empty field with help icon]
- * Confirm Shared Secret: [Empty field]
- * Retransmit Timeout: 5 (secs)
- * Retries: 1
- Authentication Type: PAP
- Local Interface IP: 10.106.68.130

Buttons: Save, Cancel

Passaggio 3. Aggiungere l'indirizzo IP del server ACS.

Passaggio 4. Immettere il segreto condiviso TACACS+ configurato nel server ACS.

Passaggio 5. Immettere nuovamente il segreto condiviso nella casella di testo **Conferma segreto condiviso**.

Passaggio 6. Lasciare gli altri campi impostati come predefiniti.

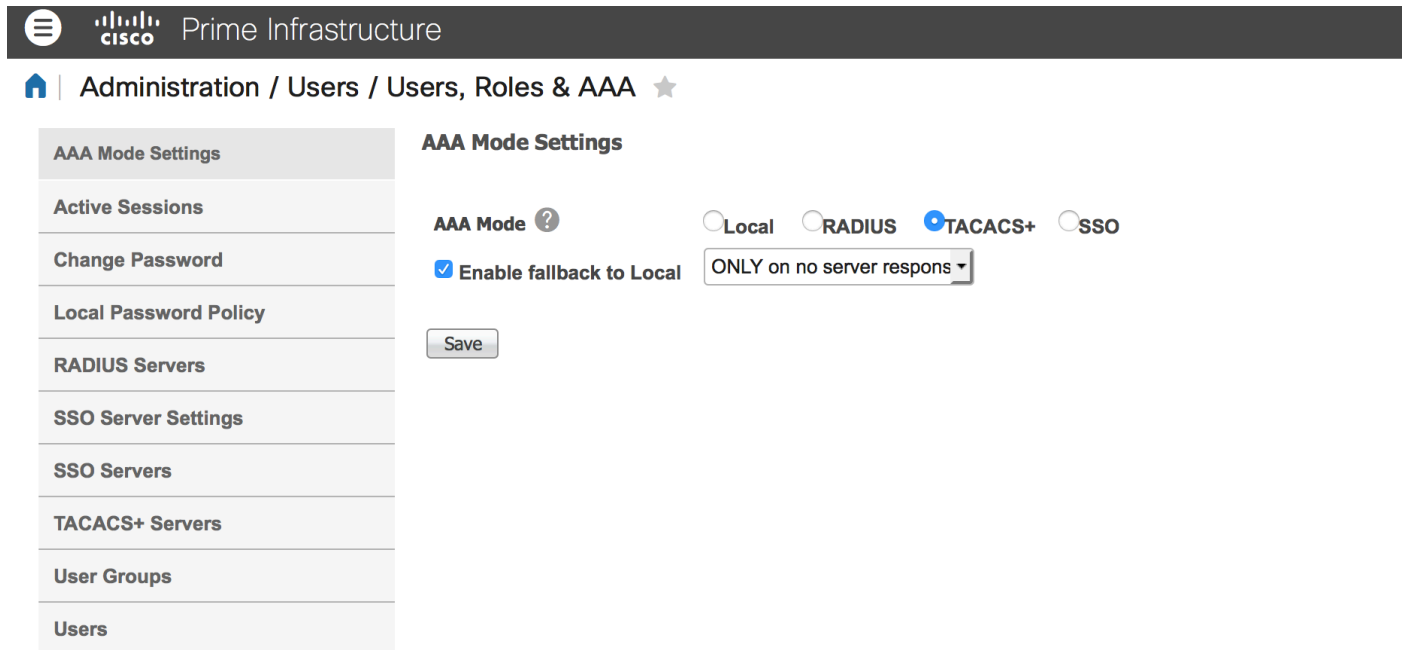
Passaggio 7. Fare clic su **Sottometti**.

Impostazioni modalità AAA in PI

Per scegliere una modalità di autenticazione, autorizzazione e accounting (AAA), attenersi alla seguente procedura:

Passaggio 1. Passare ad **Amministrazione > AAA**.

Passaggio 2. Scegliere **AAA Mode** (Modalità AAA) dal menu a sinistra della barra laterale, in modo da visualizzare la pagina come mostrato nell'immagine:

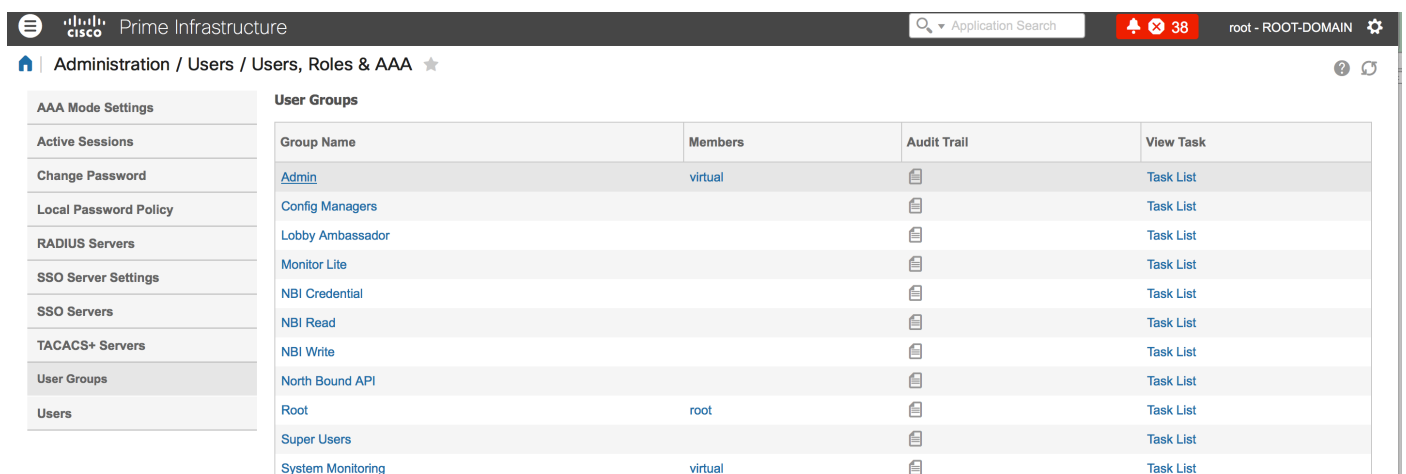


Passaggio 3. Selezionare **TACACS+**.

Passaggio 4. Selezionare la casella **Abilita fallback su locale** se si desidera che l'amministratore utilizzi il database locale quando il server ACS non è raggiungibile. Si tratta di un'impostazione consigliata.

Recupera attributi ruolo utente da PI

Passaggio 1. Passare a **Amministrazione > AAA > Gruppi di utenti**. In questo esempio viene illustrata l'autenticazione dell'amministratore. Cercare il **Nome gruppo amministratori** nell'elenco e fare clic sull'opzione **Elenco attività** a destra, come mostrato nell'immagine:



Dopo aver selezionato l'opzione **Elenco task**, viene visualizzata la finestra, come mostrato nell'immagine:

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
```

Passaggio 2. Copiare questi attributi e salvarli in un file del Blocco note.

Passaggio 3. Potrebbe essere necessario aggiungere attributi di dominio virtuale personalizzati nel server ACS. Gli attributi personalizzati del dominio virtuale sono disponibili nella parte inferiore della stessa pagina elenco operazioni.

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

Passaggio 4. Fare clic sull'opzione **fare clic qui** per ottenere la pagina degli attributi del dominio virtuale ed è possibile visualizzare la pagina, come mostrato nell'immagine:

TACACS+ Custom Attributes

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

RADIUS Custom Attributes

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

Configurazione di ACS 4.2

Passaggio 1. Accedere alla GUI di amministrazione di ACS e selezionare **Configurazione interfaccia > pagina TACACS+**.

Passaggio 2. Creare un nuovo servizio per prime. Nell'esempio viene mostrato un nome di servizio configurato con il nome **NCS**, come mostrato nell'immagine:

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"/>		

Passaggio 3. Aggiungere tutti gli attributi del Blocco note creato nel Passaggio 2 alla configurazione dell'utente o del gruppo. Assicurarsi di aggiungere gli attributi del dominio virtuale.

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
```

Passaggio 4. Fare clic su Ok.

Verifica

Accedere al sistema principale con il nuovo nome utente creato e confermare di disporre del ruolo Admin.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Esaminare il file `usermgmt.log` dalla CLI principale disponibile nella directory `/opt/CSCOlumos/logs`. Verificare se sono presenti messaggi di errore.

```
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]
```

Nell'esempio viene mostrato un esempio di messaggio di errore, che potrebbe essere causato da diversi motivi, ad esempio il rifiuto della connessione da parte di un firewall o di un dispositivo intermedio, ecc.