Esempio di configurazione di Prime Infrastructure Integration con ACS 4.2 TACACS

Sommario

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

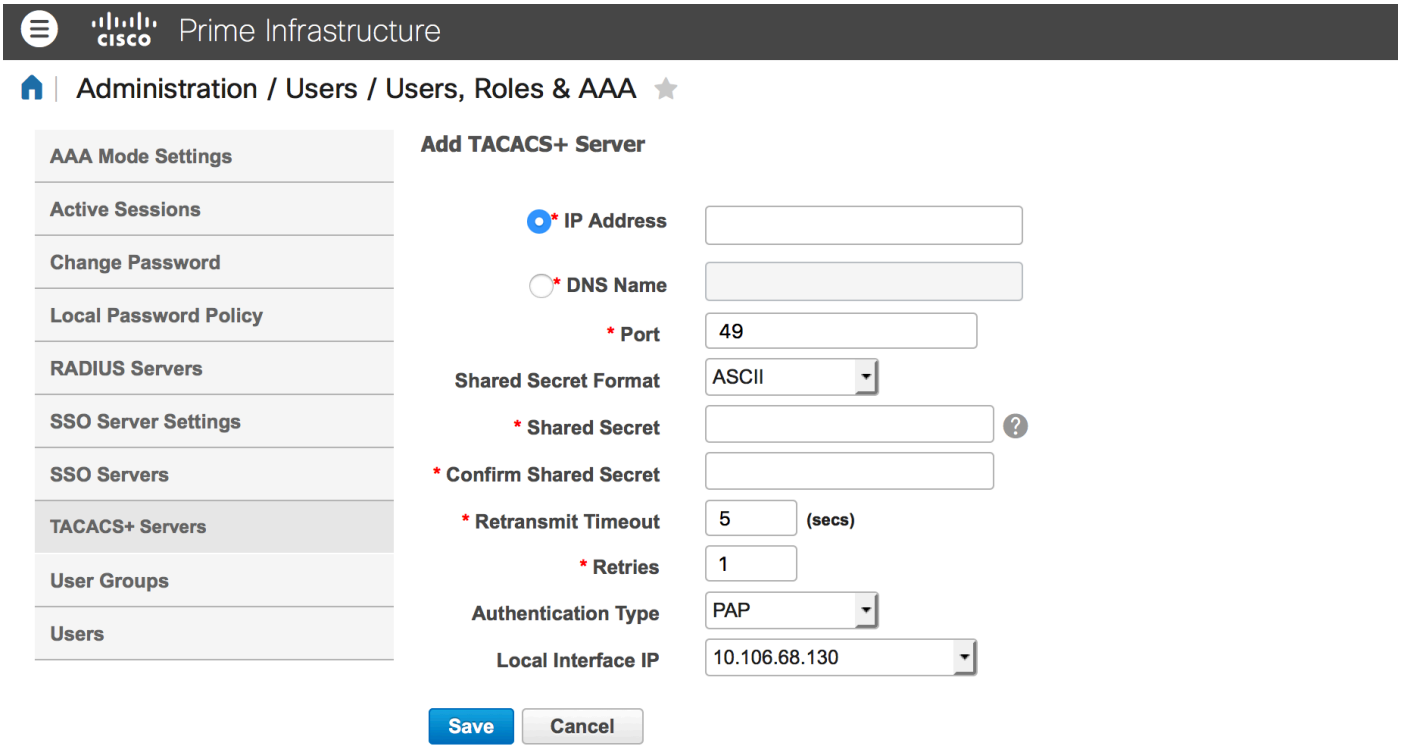
Configurazioni

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:



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.

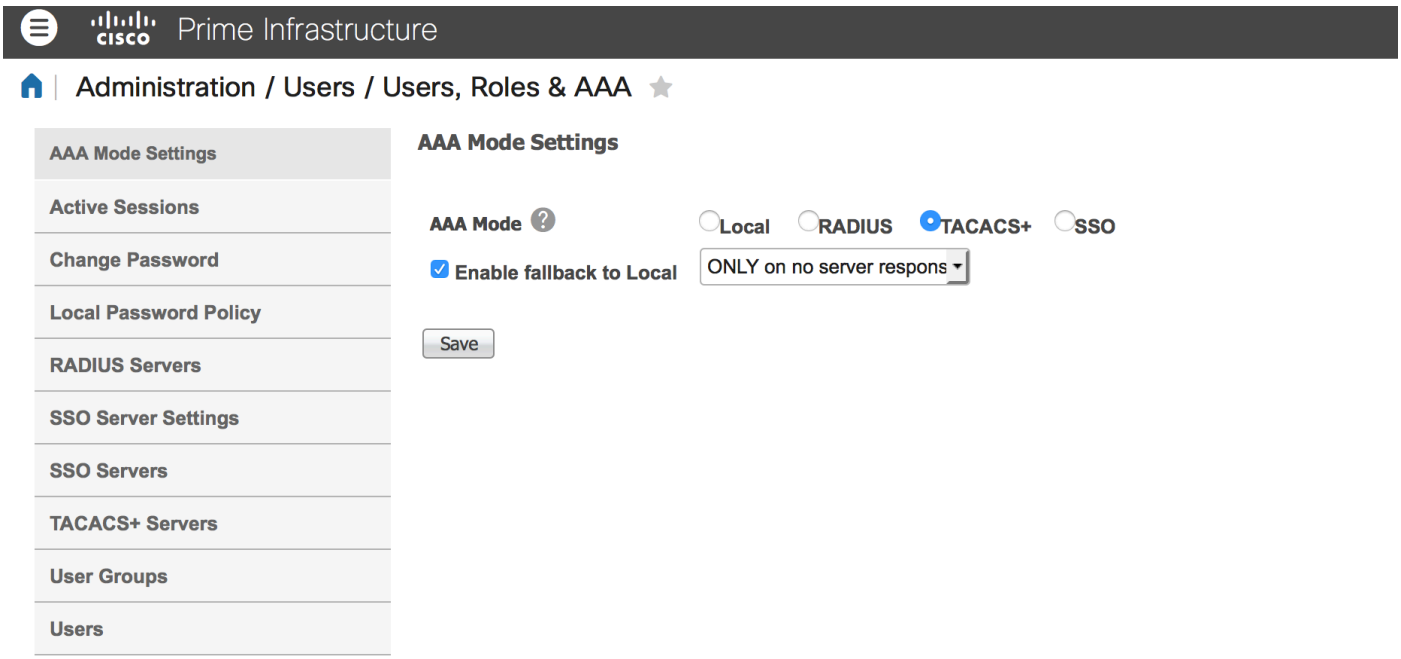
Passaggio 7. Fare clic su **Sottometti**.

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:

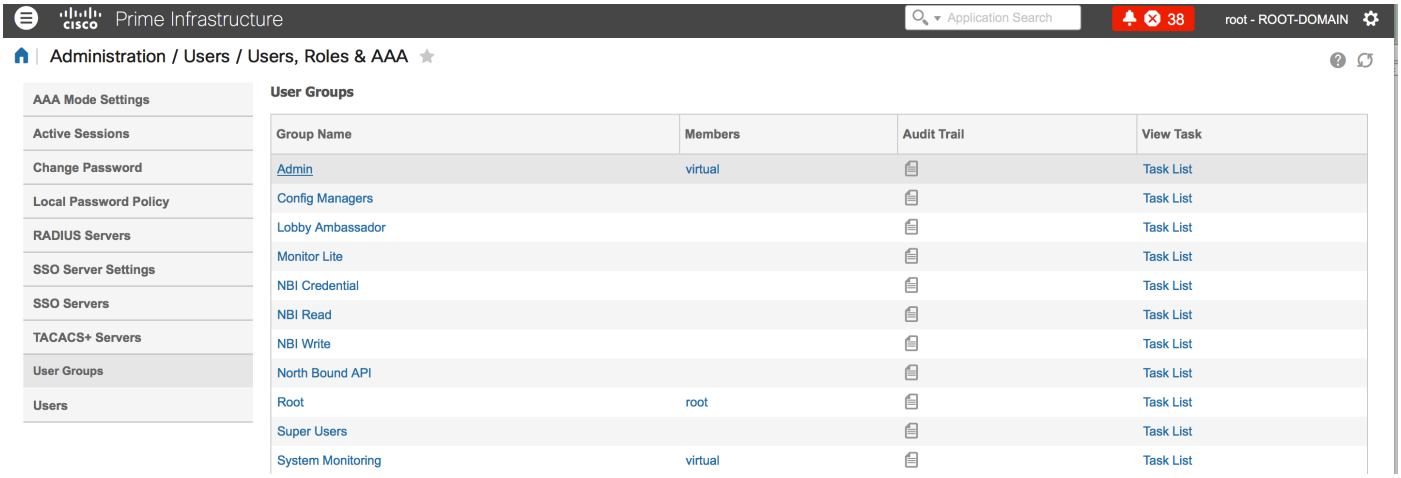


Passaggio 3. Selezionare **TACACS+**.

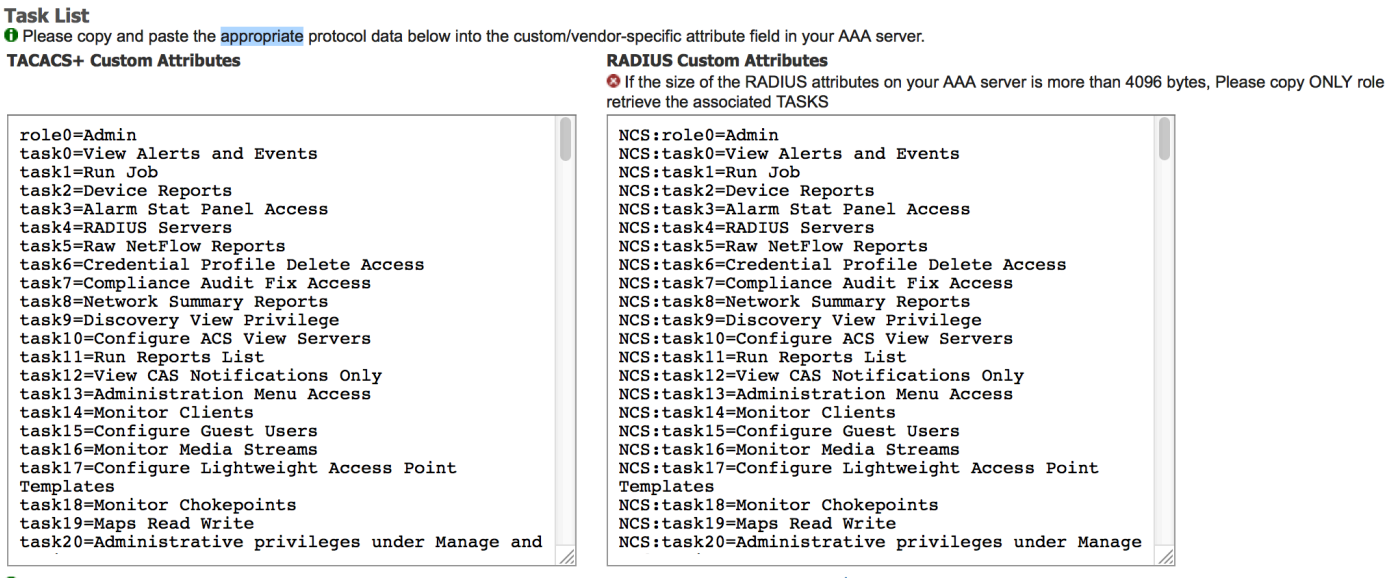
Passaggio 4. Selezionare la casella **Abilita fallback su locale** se si desidera che l'amministratore utilizzi il database locale quando il server ACS non è raggiungibile. Si tratta di un'impostazione consigliata.

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:



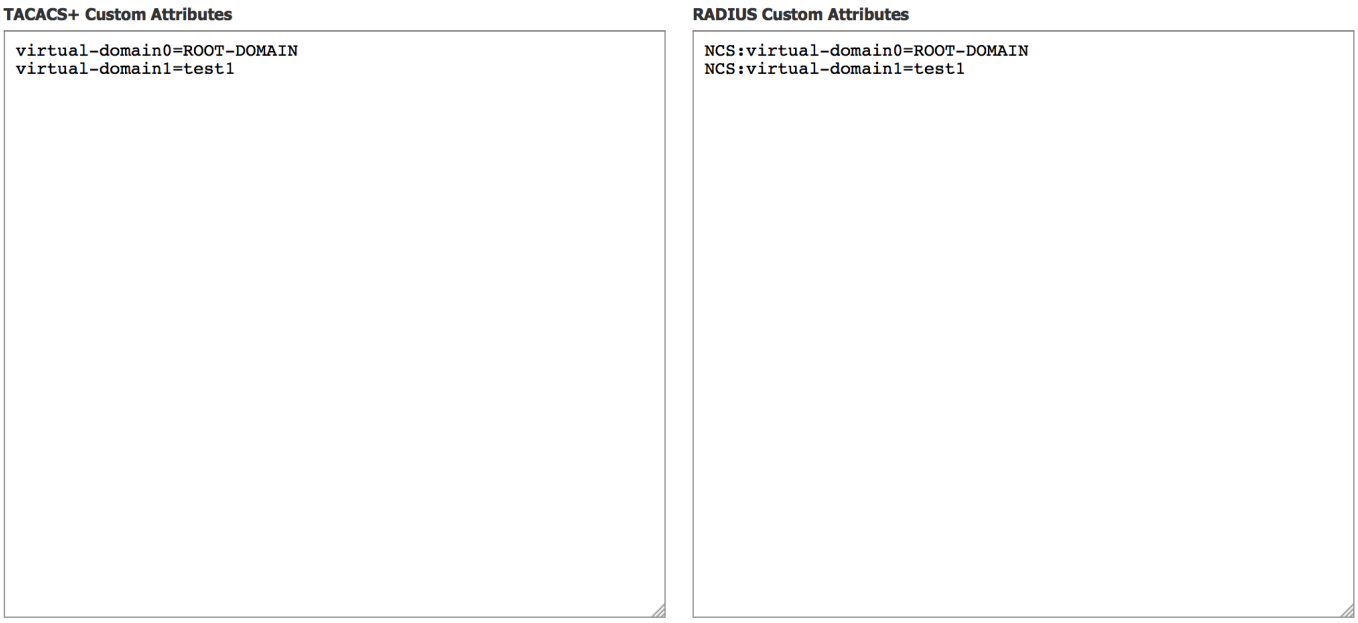
Dopo aver selezionato l'opzione **Elenco task**, viene visualizzata la finestra, come mostrato nell'immagine:



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.

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:

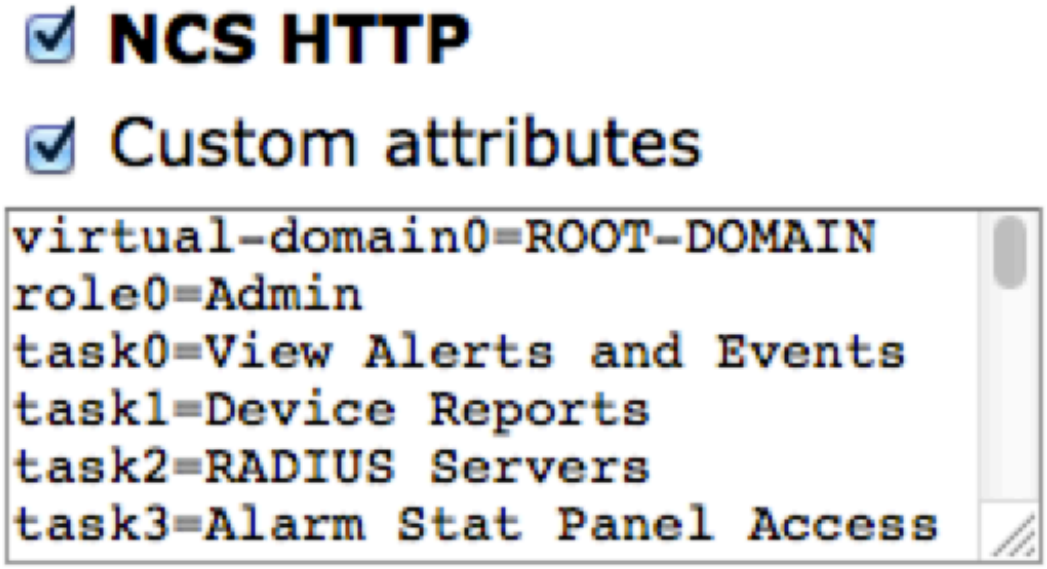


Configurazione di ACS 4.2

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:

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.



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.