Prime-Infrastruktur-Integration mit ACS 4.2 TACACS - Konfigurationsbeispiel

Inhalt

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

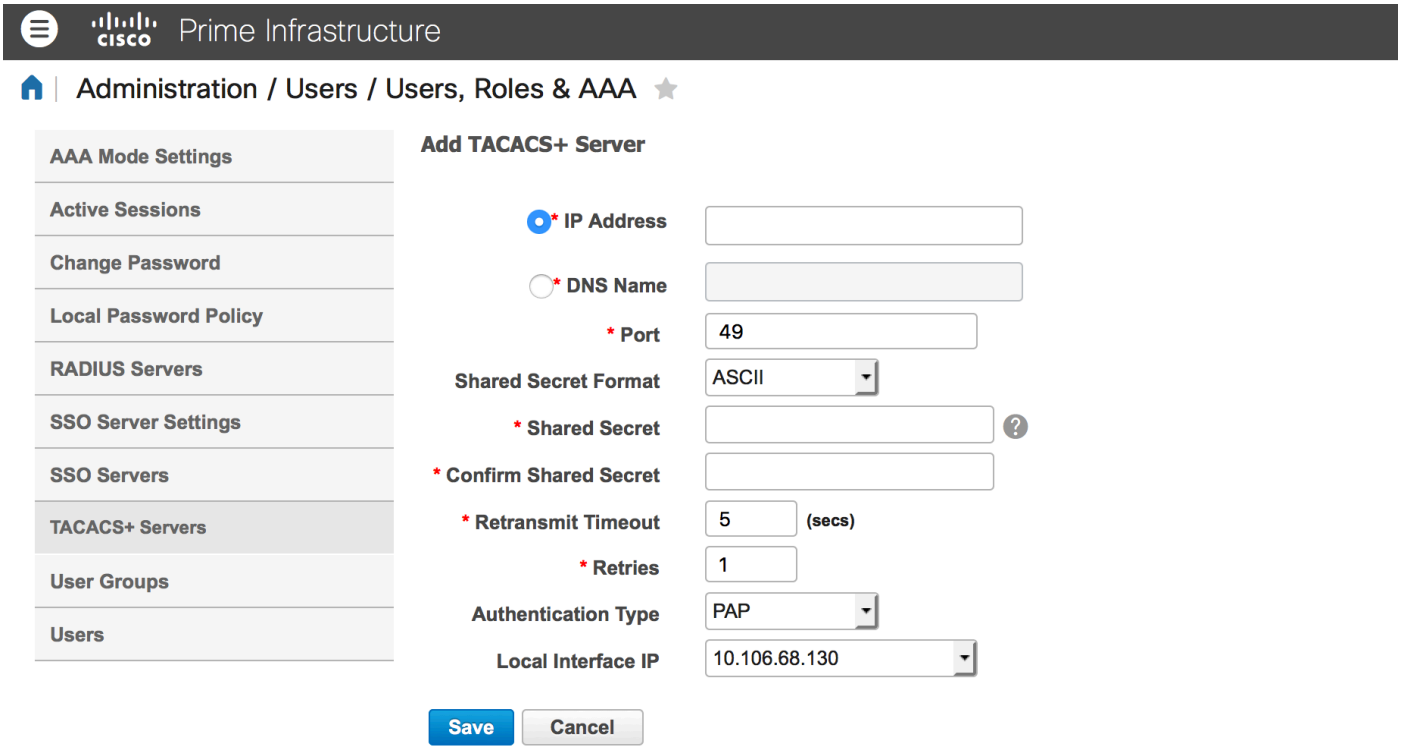
Konfigurationen

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:



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.

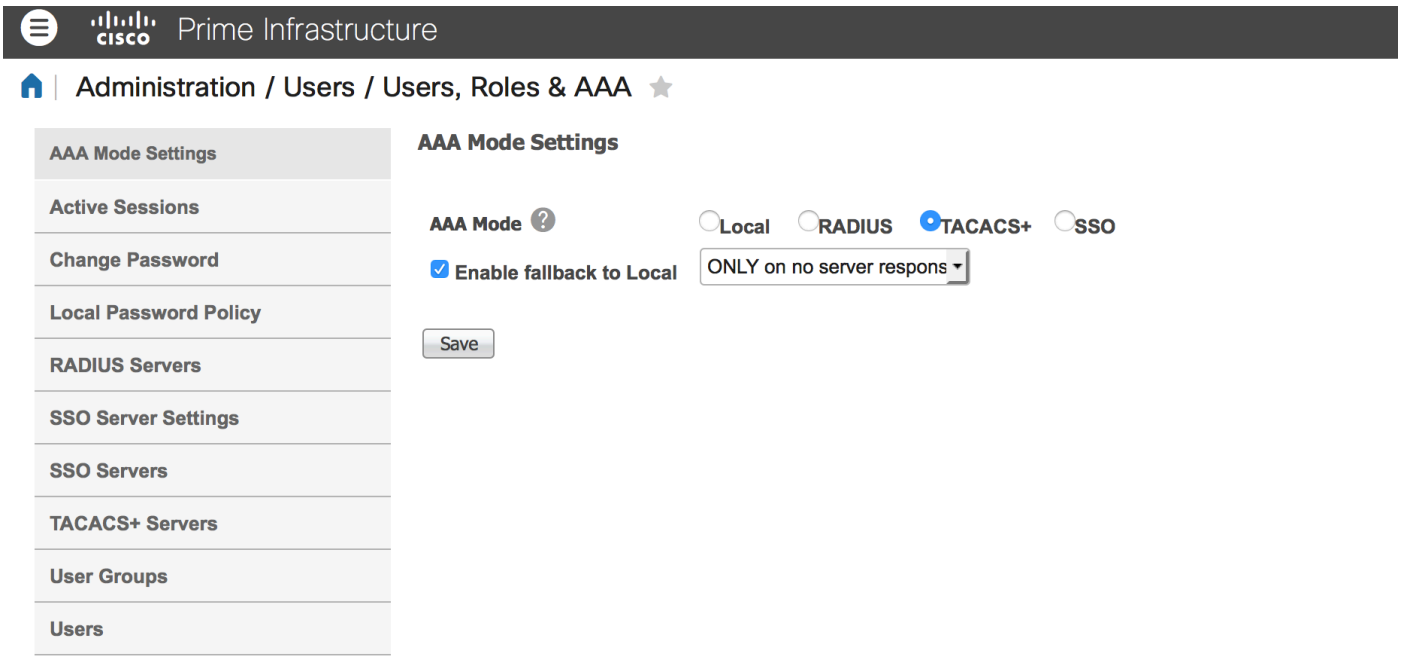
Schritt 7: Klicken Sie auf **Senden**.

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:

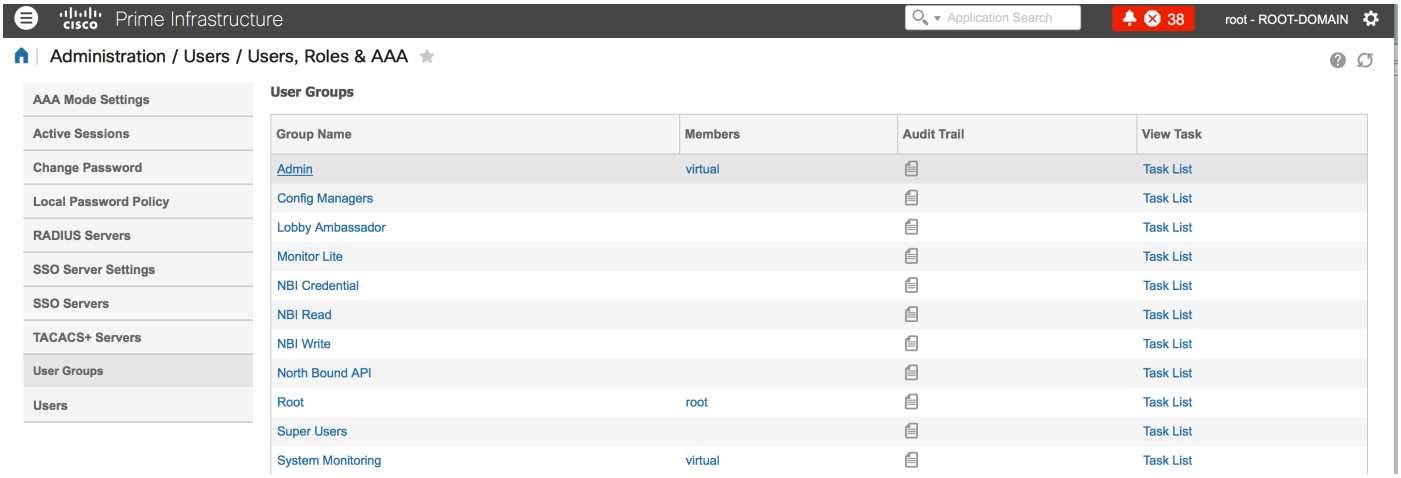


Schritt 3: Wählen Sie **TACACS+** aus.

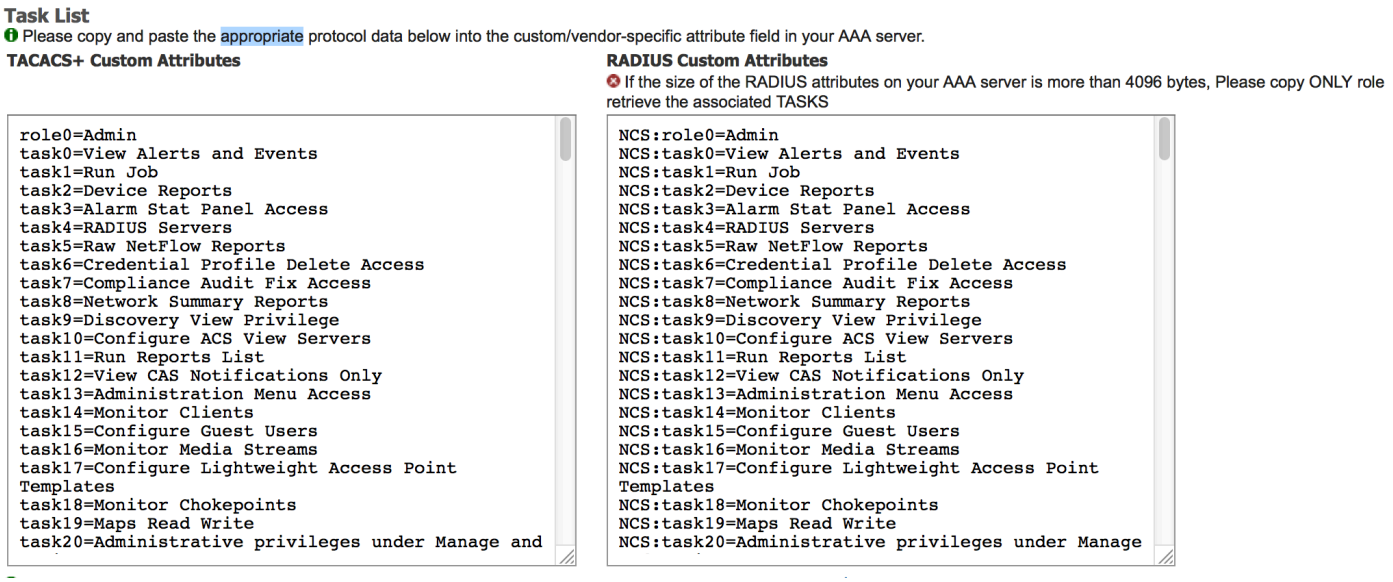
Schritt 4: Aktivieren Sie das Kontrollkästchen **Enable Fallback to Local (Fallback an Lokalen aktivieren)**, wenn der Administrator die lokale Datenbank verwenden soll, wenn der ACS-Server nicht erreichbar ist. Dies ist eine empfohlene Einstellung.

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:

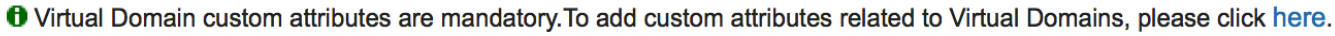


Wenn Sie auf die Option **Aufgabenliste** klicken, wird das Fenster angezeigt, wie im Bild gezeigt:

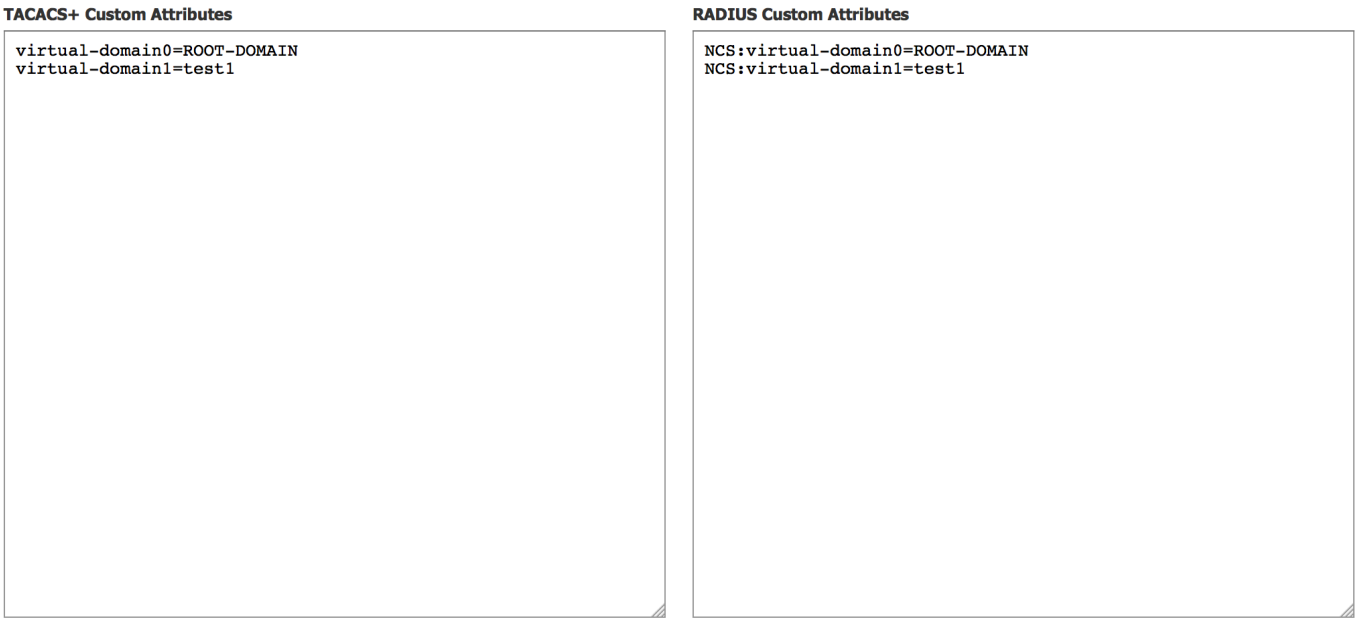


Schritt 2: Kopieren Sie diese Attribute und speichern Sie sie in einer Notizblock-Datei.

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.



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

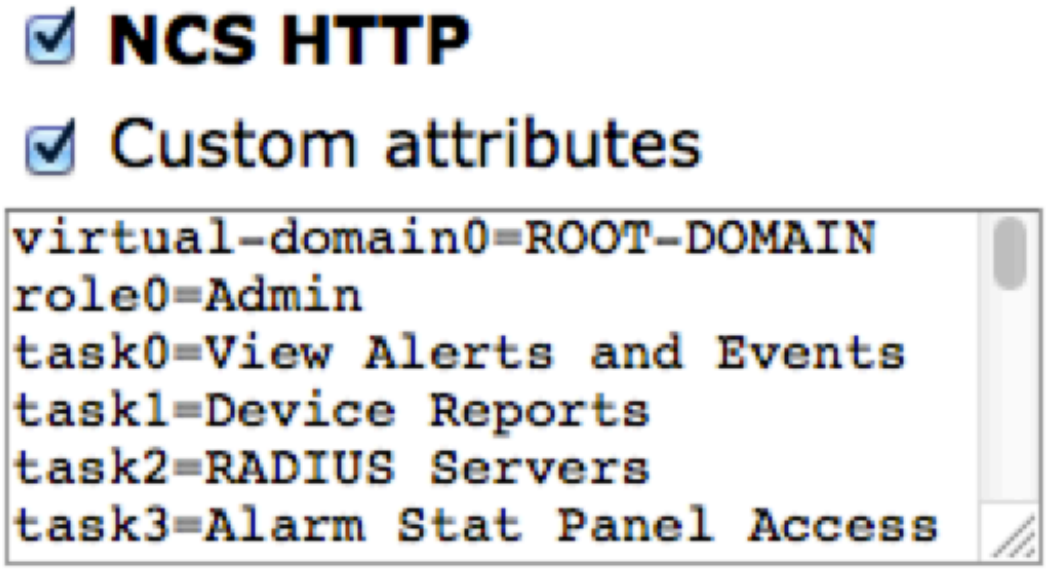


Konfigurieren von ACS 4.2

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:

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.



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.