Prime基礎設施與ACS 4.2 TACACS整合配置示例

目錄

簡介

本檔案介紹終端存取控制器存取控制系統(TACACS+)的組態範例

cisco Prime Infrastructure(PI)應用上的驗證和授權。

必要條件

需求

思科建議您瞭解以下主題：

- 將PI定義為訪問控制伺服器(ACS)中的客戶端
- 在ACS和PI上定義IP地址和相同的共用金鑰

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ACS版本4.2
- Prime基礎架構版本3.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

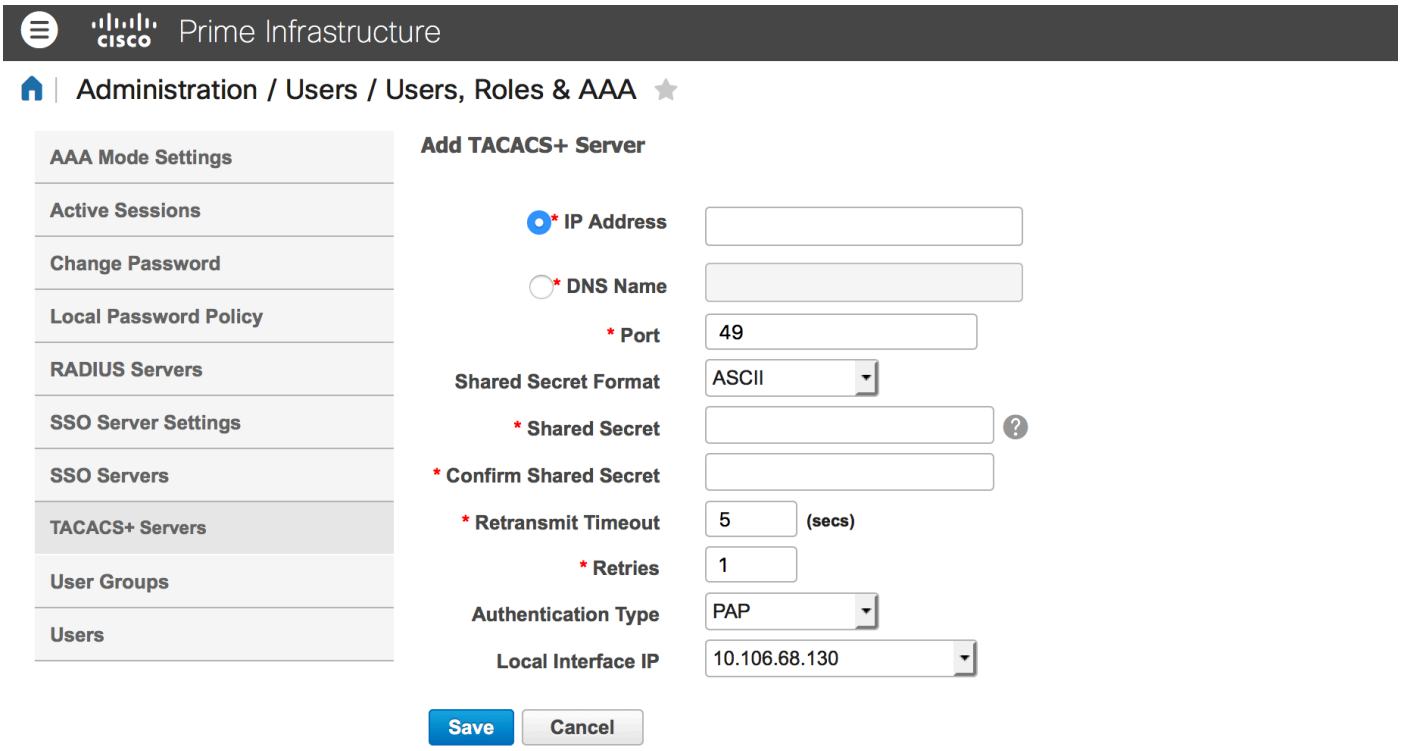
組態

在PI中將ACS新增為TACACS伺服器

完成以下步驟，以便將ACS新增為TACACS伺服器：

步驟1.導航至 **管理 > 使用者 > 使用者、角色和AAA 在PI中**

步驟2.從左側邊欄選單中，選擇**TACACS+伺服器**，在**Add TACACS+伺服器**下按一下**Go**，頁面顯示如下圖所示：



步驟3.新增ACS伺服器的IP地址。

步驟4.輸入在ACS伺服器中配置的TACACS+共用金鑰。

步驟5.在**Confirm Shared Secret**文本框中重新輸入共用金鑰。

步驟6.保留其餘欄位的預設設定。

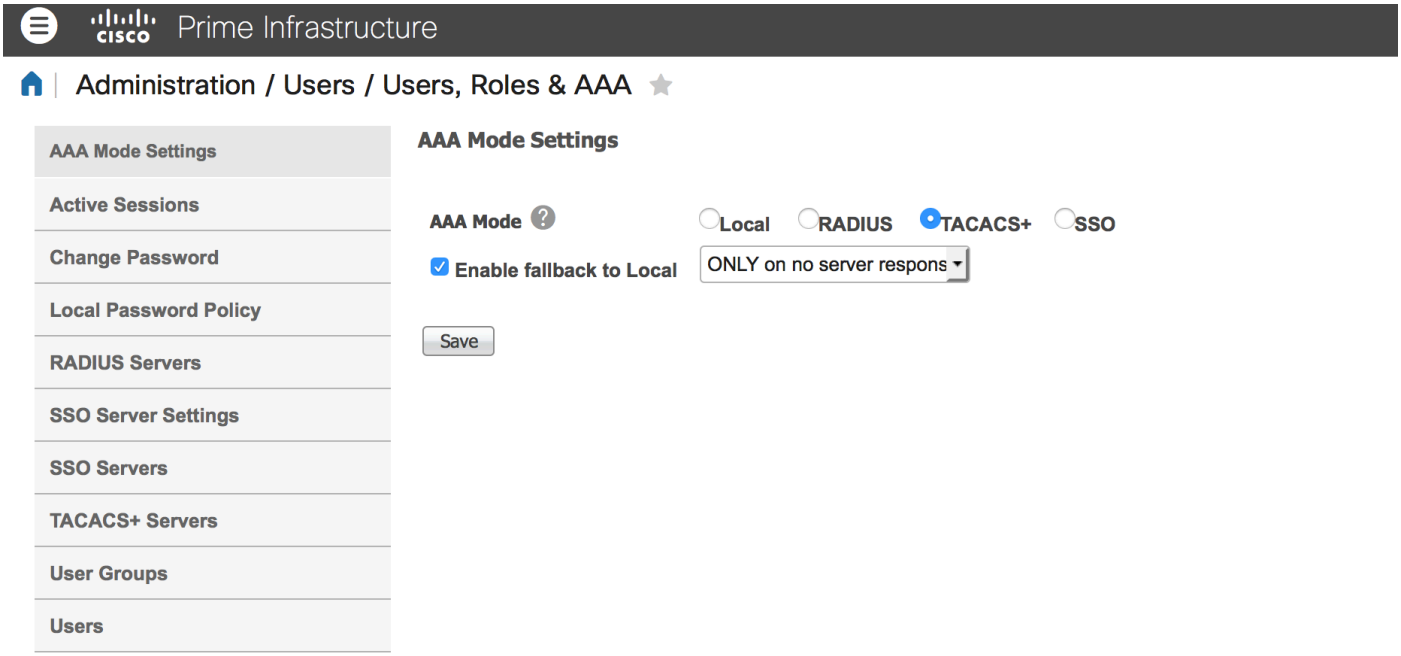
步驟7.按一下「**Submit**」。

PI中的AAA模式設定

若要選擇驗證、授權及記帳(AAA)模式，請完成以下步驟：

步驟1.導覽至**Administration > AAA**。

步驟2.從左側欄選單中選擇**AAA Mode**，您可以看到如下圖所示的頁面：

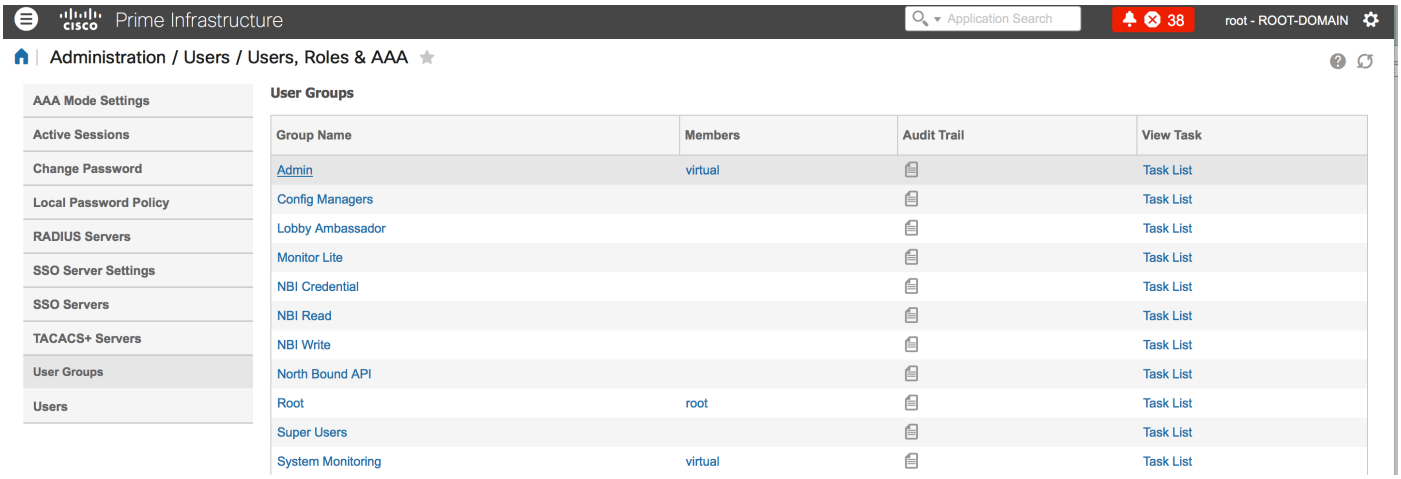


步驟3.選擇TACACS+。

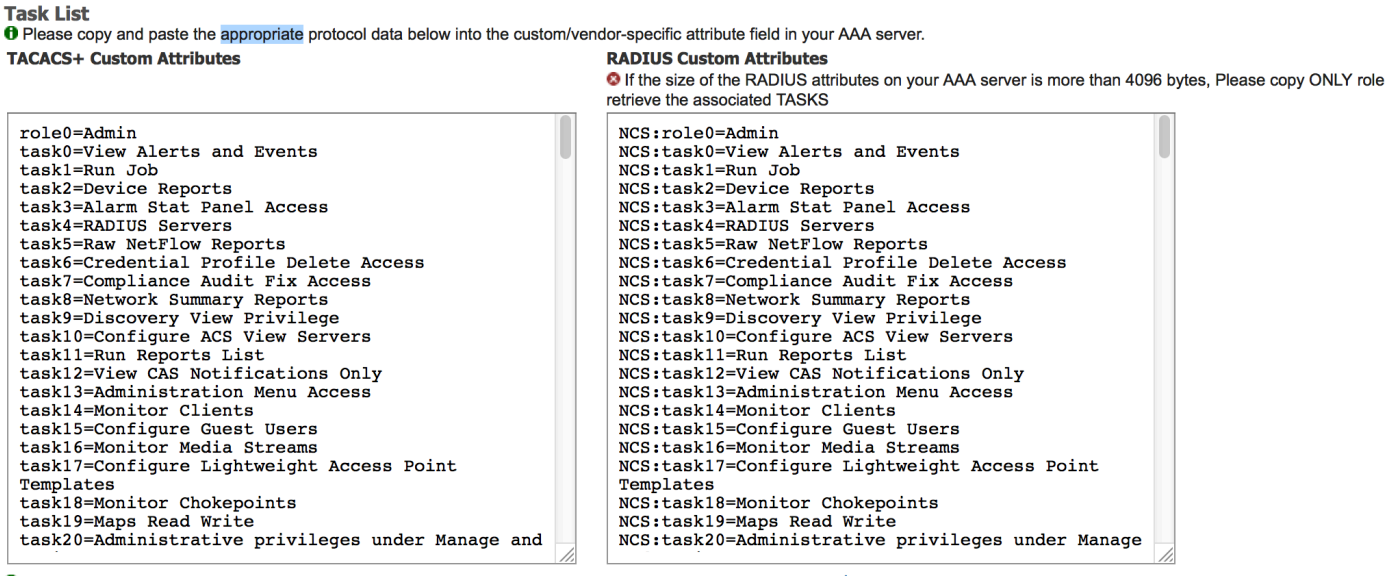
步驟4.如果希望管理員在ACS伺服器無法訪問時使用本地資料庫，請選中**Enable** Fallback to Local框。這是推薦設定。

從PI檢索使用者角色屬性

步驟1。導覽至**Administration > AAA > User Groups**。此示例顯示管理員身份驗證。在清單中查詢**Admin Group Name**，然後按一下右側的**Task List**選項，如下圖所示：



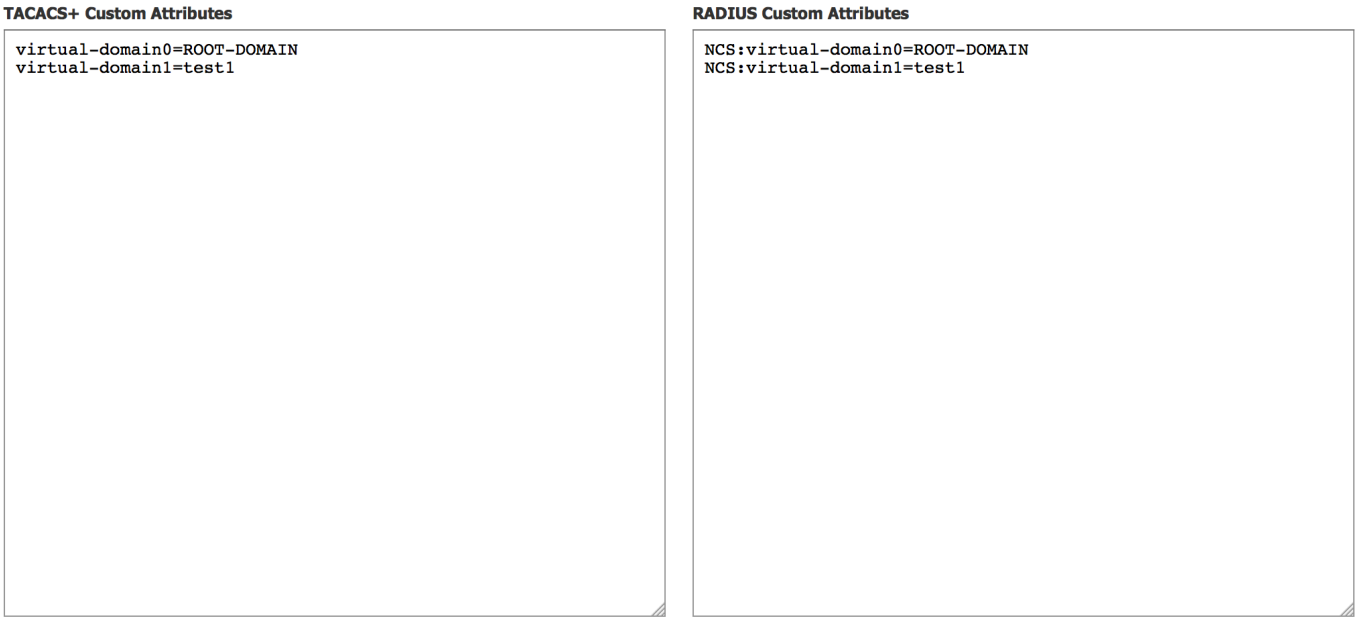
按一下**Task List**選項後，將出現視窗，如下圖所示：



步驟2.複製這些屬性並將其儲存在記事本檔案中。

步驟3.您可能需要在ACS伺服器中新增自定義虛擬域屬性。自定義虛擬域屬性在同一任務清單頁面的底部可用。

步驟4.按一下**按一下此處**選項以獲取「虛擬域」屬性頁，您可以看到該頁，如下圖所示：

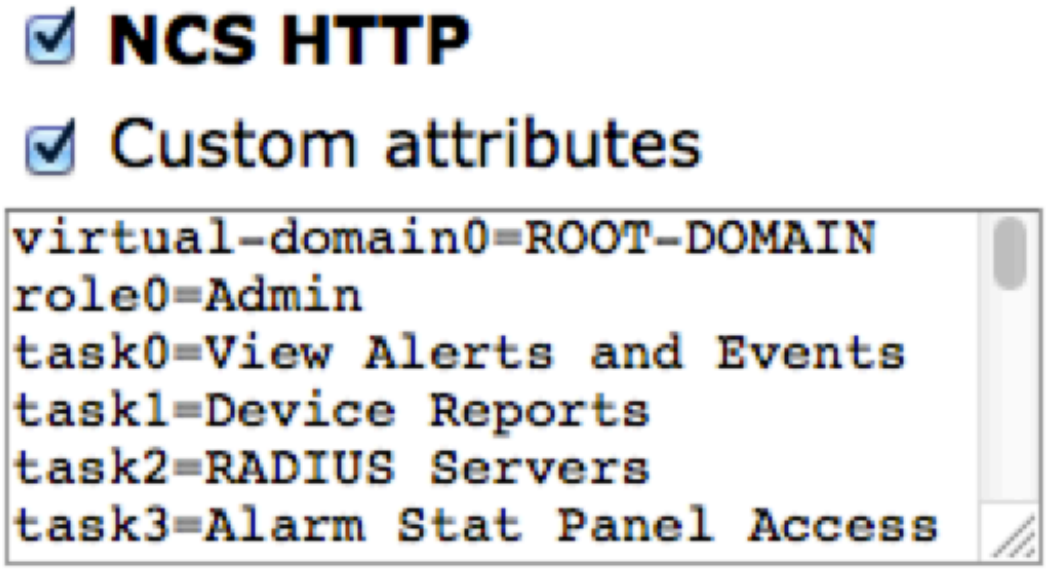


配置ACS 4.2

步驟1.登入**ACS管理員GUI**，然後導覽至**Interface Configuration > TACACS+**頁面。

步驟2.為prime建立新服務。此範例顯示使用名稱**NCS**配置的服務名稱，如下圖所示：

步驟3.將步驟2中建立的記事本中的所有屬性新增到使用者或組配置。確保新增虛擬域屬性。



步驟4.按一下「Ok」。

驗證

使用您建立的新使用者名稱登入到主目錄，並確認您具有Admin角色。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

從/opt/CSCOlumos/logs目錄中的prime根CLI**檢視usermgmt.log**。檢查是否有任何錯誤消息。

```
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]
```

以下範例顯示錯誤訊息範例，可能是由於各種原因，例如防火牆或任何中間裝置拒絕連線。