如何配置Cisco VPN 3000集中器以支援管理帳戶的TACACS+身份驗證

目錄

簡介

本文檔提供了逐步說明，以便配置Cisco VPN 3000系列集中器以支援管理帳戶的TACACS+身份驗證。

在VPN 3000集中器上配置TACACS+伺服器後，不再使用本地配置的帳戶名和密碼（如admin、config、isp等）。所有對VPN 3000集中器的登入都將傳送到已配置的外部TACACS+伺服器以進行使用者和密碼驗證。

TACACS+伺服器上每個使用者的許可權級別定義確定了每個TACACS+使用者名稱在VPN 3000集中器上的許可權。然後，將該級別與VPN 3000集中器上本地配置的使用者名稱下定義的AAA訪問級別進行匹配。這一點非常重要，因為一旦定義TACACS+伺服器，VPN 3000集中器上的本地配置使用者名稱就不再有效。但是，它們仍然僅用於匹配從TACACS+伺服器返回的許可權級別，以及該本地使用者下的AAA訪問級別。然後為TACACS+使用者名稱分配本地配置的VPN 3000集中器使用者在其配置檔案中定義的許可權。

例如，如配置章節中詳細描述的，將TACACS+使用者/組配置為返回15的TACACS+許可權級別。在VPN 3000集中器的「管理員」部分下，管理員使用者的AAA訪問級別也設定為15。允許此使用者修改所有部分下的配置，以及讀取/寫入檔案。由於TACACS+許可權級別和AAA訪問級別匹配，因此TACACS+使用者在VPN 3000集中器上被授予這些許可權。

例如，如果您決定使用者需要能夠修改配置，但不能修改讀/寫文*件，請在*TACACS+伺服器上為其

分配12的許可權級別。您可以選擇1到15之間的任何數字。然後，在VPN 3000集中器上，選擇其他本地配置的管理員。接下來，將其AAA訪問級別設定為12，並設定此使用者的許可權，以便能夠修改配置，但不能讀取/寫入檔案。由於具有匹配的許可權/訪問級別，使用者登入時可以獲得這些許可權。

不再使用VPN 3000 Concentrator上本地配置的使用者名稱。但是，系統會使用每個使用者下的存取許可權和AAA存取層來定義特定TACACS+使用者在登入時獲得的許可權。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 確保您從VPN 3000集中器到TACACS+伺服器的IP連線。如果您的TACACS+伺服器朝向公用介面，請不要忘記在公共過濾器上開啟TACACS+（TCP連線埠49）。
- 確保通過控制檯進行的備份訪問可正常運行。首次設定此配置時，很容易意外將所有使用者鎖定在配置之外。恢復訪問的唯一方法是通過控制檯，該控制檯仍使用本地配置的使用者名稱和密碼。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco VPN 3000 Concentrator Software Release 4.7.2.B（或者，3.0或更高版本的作業系統軟體均正常工作。）
- 適用於Windows伺服器的思科安全存取控制伺服器版本4.0（或者，2.4或更高版本的軟體也可以使用。）

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。

慣例

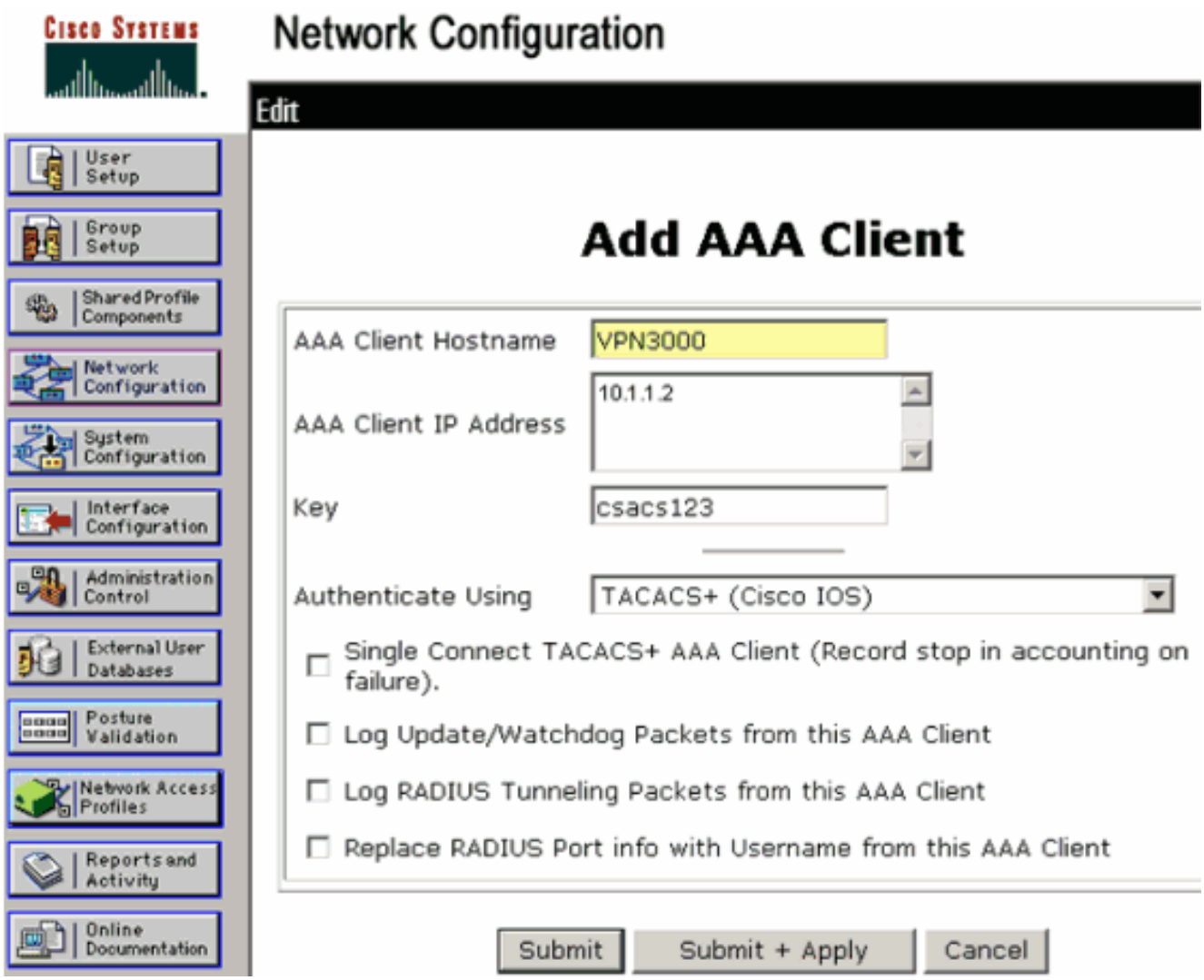
如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

配置TACACS+伺服器

在TACACS+伺服器中為VPN 3000集中器新增條目

完成這些步驟，以便在TACACS+伺服器中新增VPN 3000集中器的條目。

1. 按一下左側面板中的**Network Configuration**。在AAA Clients下，按一下**Add Entry**。
2. 在下一個視窗中，填寫表格以將VPN集中器新增為TACACS+客戶端。此示例使用：AAA客戶端主機名= **VPN3000**AAA客戶端IP地址= **10.1.1.2**金鑰= **csacs123**使用= **TACACS+(Cisco IOS)進行身份驗證**按一下「**Submit + Restart**」。



在TACACS+伺服器中新增使用者帳戶

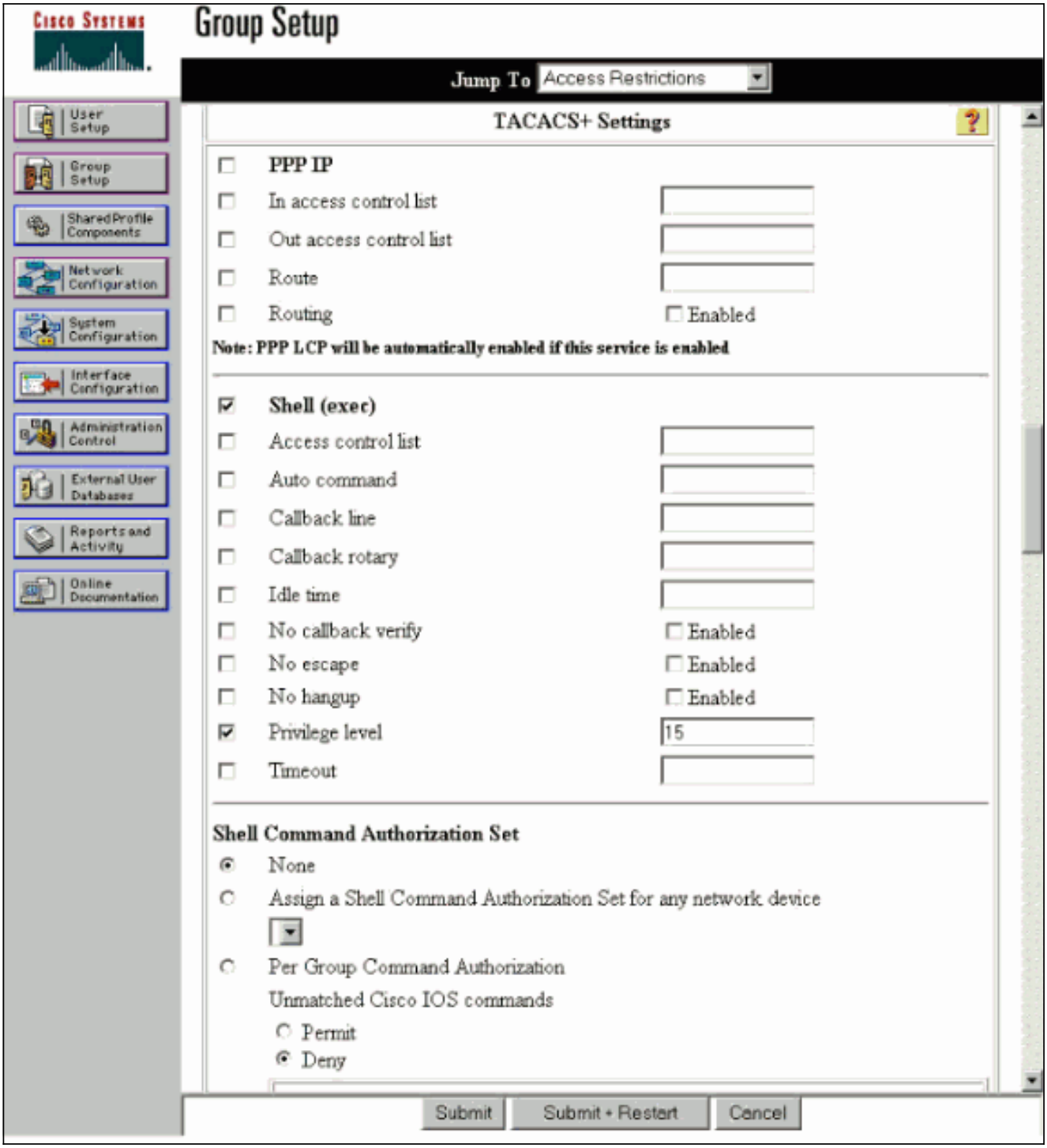
完成以下步驟，以便在TACACS+伺服器中新增使用者帳戶。

1. 在TACACS+伺服器中建立稍後可用於TACACS+驗證的使用者帳戶。在左側面板中按一下**User Setup**，新增使用者「johnsmith」，然後按一下**Add/Edit**以執行此操作。
2. 為此使用者新增密碼，並將該使用者分配到包含其他VPN 3000集中器管理員的ACS組。**注意**：此示例定義此特定使用者ACS組配置檔案下的許可權級別。如果要針對每個使用者執行此操作，請選擇**Interface Configuration > TACACS+(Cisco IOS)**，然後選中**Shell(exec)服務的User**框。只有這樣，本文檔中所述的TACACS+選項才在每個使用者配置檔案下可用。

編輯TACACS+伺服器上的組

完成以下步驟即可編輯TACACS+伺服器上的組。

1. 按一下左側面板中的**Group Setup**。
2. 從下拉選單中，在「Add a User Account in the TACACS+ Server」部分中選擇使用者新增到的組（在本示例中為Group 1），然後按一下**Edit Settings**。
3. 在下一個視窗中，確保在「TACACS+設定」下選擇以下屬性：**外殼(exec)許可權級別= 15**完成後，按一下**Submit + Restart**。



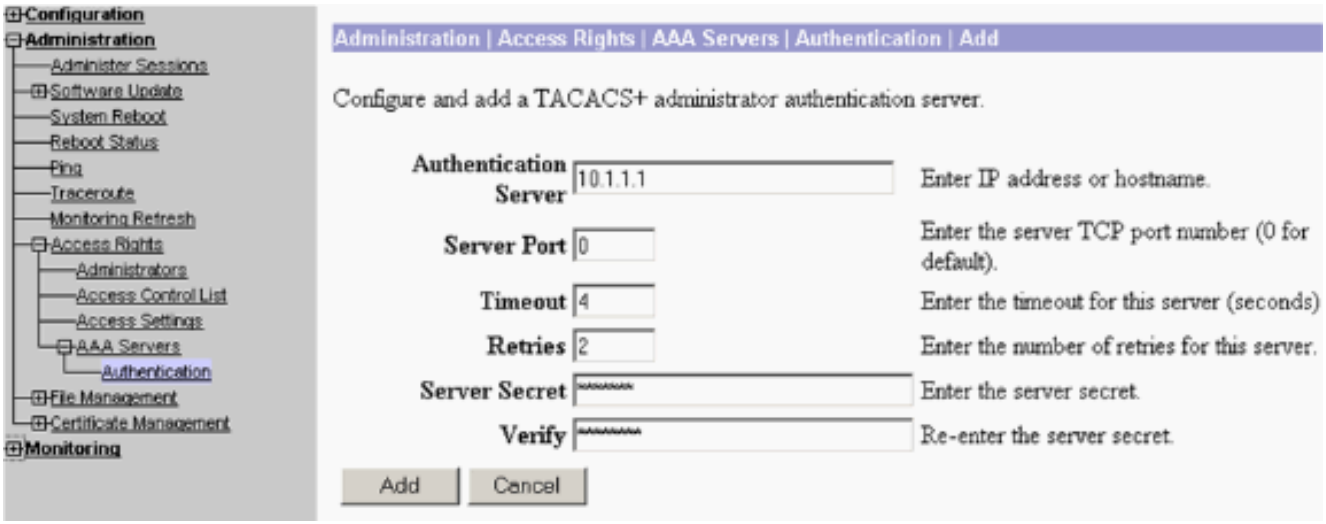
配置VPN 3000 Concentrator

為VPN 3000集中器中的TACACS+伺服器新增條目

完成這些步驟，以便在VPN 3000集中器中新增TACACS+伺服器的條目。

1. 在左側面板的導航樹中選擇**Administration > Access Rights > AAA Servers > Authentication**，然後按一下右側面板中的**Add**。一旦按一下**Add**以新增此伺服器，將不再使用VPN 3000 Concentrator上本地配置的使用者名稱/密碼。確保通過控制檯進行的備份訪問在出現鎖定時能夠正常工作。
2. 在下一個視窗中，填寫表格，如下所示：身份驗證伺服器= **10.1.1.1**（TACACS+伺服器的IP地址）伺服器埠= **0**（預設值）超時= **4**重試= **2**伺服器金鑰= **csacs123**驗證=

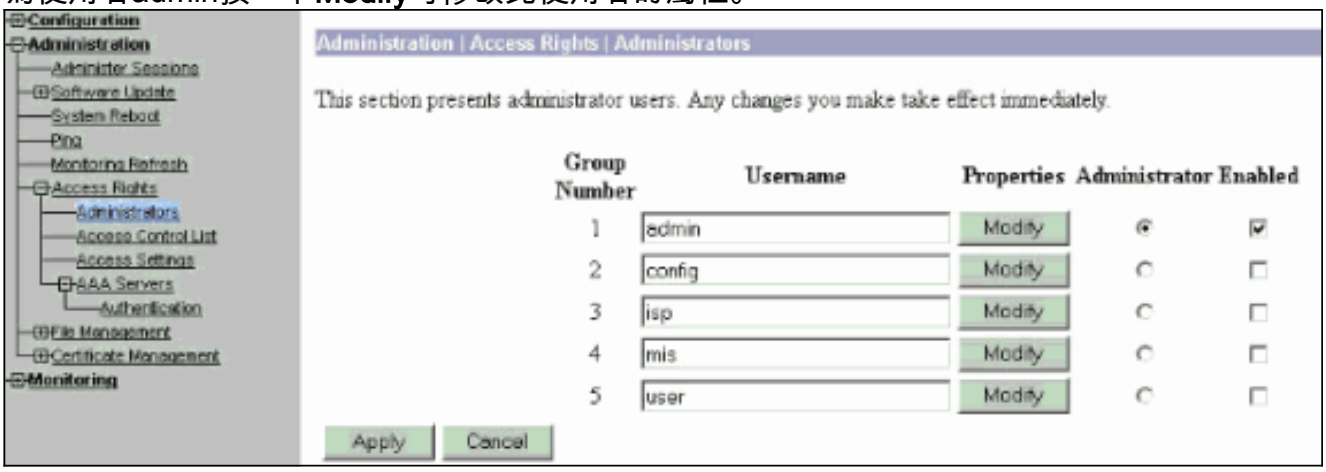
csacs123



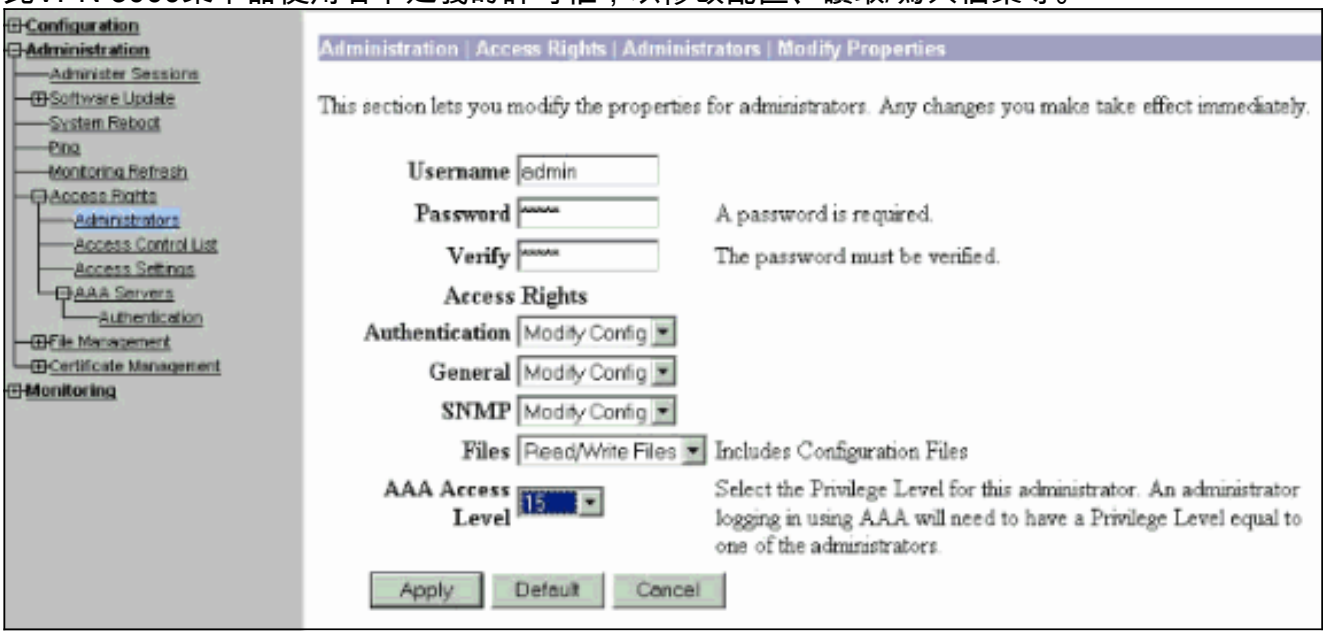
修改VPN集中器上的Admin帳戶以進行TACACS+身份驗證

完成以下步驟，在VPN集中器上修改TACACS+身份驗證的管理帳戶。

1. 為使用者admin按一下**Modify**可修改此使用者的屬性。



2. 選擇AAA訪問級別**15**。此值可以是1到15之間的任意數字。請注意，它必須與TACACS+伺服器上的使用者/組配置檔案下定義的TACACS+許可權級別匹配。然後TACACS+使用者提取在此VPN 3000集中器使用者下定義的許可權，以修改配置、讀取/寫入檔案等。



驗證

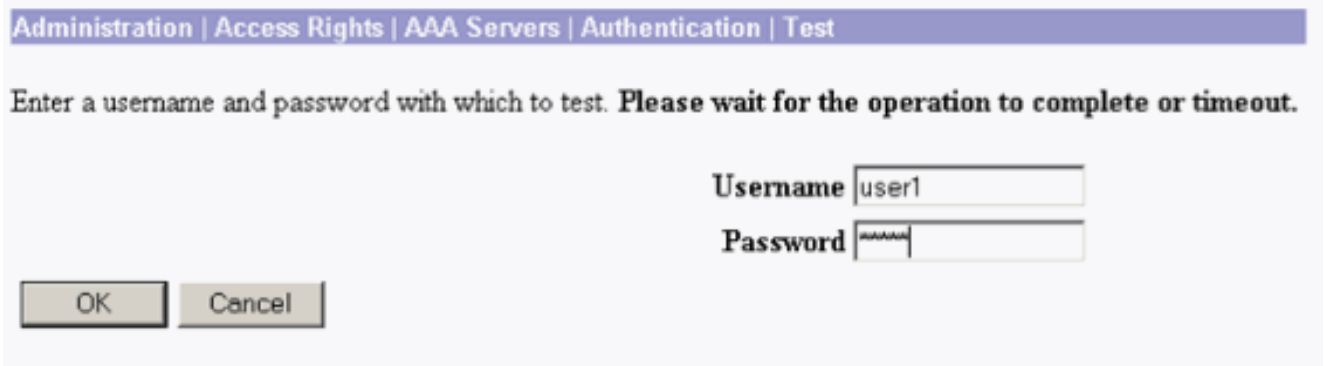
目前沒有適用於此組態的驗證程序。

疑難排解

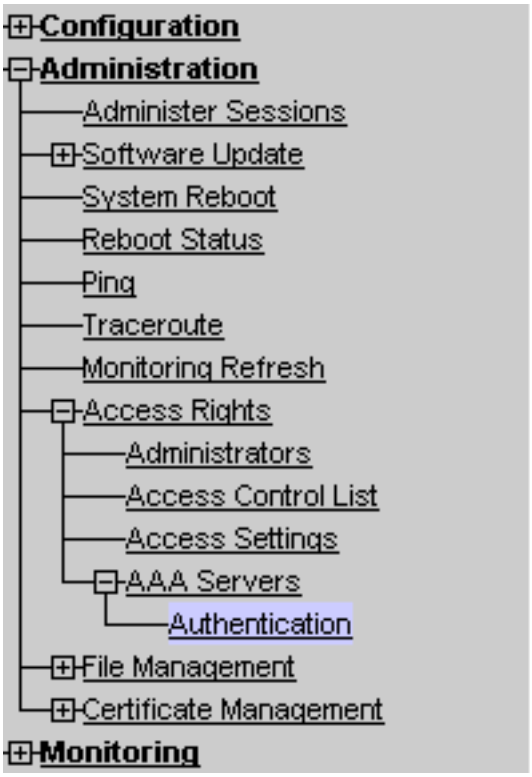
完成這些說明中的步驟，對組態進行疑難排解。

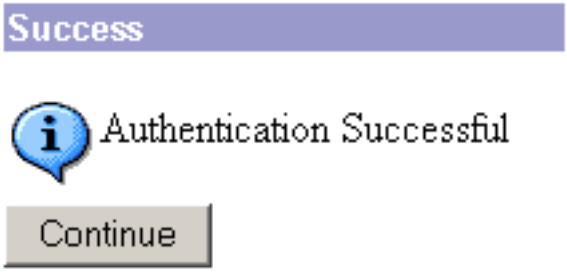
1. 若要測試驗證：適用於TACACS+伺服器選擇**Administration > Access Rights > AAA Servers > Authentication**。選擇伺服器，然後按一下**測試**。

注意：在Administration頁籤上配置TACACS+伺服器時，沒有方法設定使用者在VPN 3000本地資料庫上進行身份驗證。您只能使用其他外部資料庫或TACACS伺服器進行回退。輸入TACACS+使用者名稱和密碼，然後按一下**OK**。



身份驗證成功。





2. 如果失敗，則可能是配置問題或IP連線問題。檢查ACS伺服器上的失敗嘗試日誌中是否存在與失敗相關的消息。如果此日誌中未顯示消息，則可能存在IP連線問題。TACACS+請求未到達TACACS+伺服器。驗證應用到適當VPN 3000集中器介面的過濾器允許傳入和傳出TACACS+（TCP埠49）資料包。如果故障在日誌中顯示為服務已拒絕，則說明在TACACS+伺服器上的使用者或組配置檔案下未正確啟用外殼(exec)服務。
3. 如果測試身份驗證成功，但登入VPN 3000集中器仍失敗，請通過控制檯埠檢查可過濾事件日誌。如果您看到類似消息：

```
65 02/09/2005 13:14:40.150 SEV=5 AUTH/32 RPT=2
User [ johnsmith ] Protocol [ HTTP ] attempted ADMIN logon.
Status: <REFUSED> authorization failure. NO Admin Rights
```

此訊息表示在任一VPN 3000集中器使用者下，在TACACS+伺服器上指派的許可權層級沒有相符的AAA存取層級。例如，使用者johnsmith在TACACS+伺服器上的TACACS+許可權級別為7，但是五個VPN 3000集中器管理員都沒有具有7的AAA訪問級別。

相關資訊

- Cisco VPN 3000系列集中器支援頁面
- Cisco VPN 3000系列使用者端支援頁面
- IPSec協商/IKE通訊協定支援頁面
- TACACS/TACACS+ 支援頁面
- IOS 文件中的 TACACS+
- 技術支援與文件 - Cisco Systems