配置CSU for UNIX(Solaris)

目錄

簡介

Cisco Secure ACS for UNIX(CSU)軟體有助於確保網路安全，並跟蹤成功連線到網路的人員的活動。CSU充當TACACS+或RADIUS伺服器，並使用身份驗證、授權和記帳(AAA)來提供網路安全。

CSU支援以下資料庫選項來儲存組和使用者配置檔案以及記帳資訊：

- SQLAnywhere（隨CSU提供）。此版本的Sybase SQLAnywhere不支援客戶端/伺服器。但是，它經過最佳化，可以通過CSU執行基本的AAA服務。**注意：**SQLAnywhere資料庫選項不支援超過5,000個使用者的配置檔案資料庫、資料庫站點間配置檔案資訊的複製或思科安全分發會話管理器(DSM)功能。
- Oracle或Sybase關聯式資料庫管理系統(RDBMS)。要支援5,000個或更多使用者的Cisco Secure配置檔案資料庫、資料庫複製或Cisco Secure DSM功能，必須預先安裝Oracle（版本7.3.2、7.3.3或8.0.3）或Sybase SQL server（版本11）RDBMS以儲存Cisco Secure配置檔案資訊。在Cisco Secure安裝完成後，資料庫複製需要進一步的RDBMS配置。
- 從CSU的早期(2.x)版本升級現有資料庫。如果您從早期的Cisco Secure 2.x版本升級，Cisco Secure安裝程式會自動升級配置檔案資料庫，使其與UNIX的CSU 2.3相容。
- 匯入現有配置檔案資料庫。您可以轉換現有的免費軟體TACACS+或RADIUS配置檔案資料庫或平面檔案，以便用於此版本的CSU。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco Secure ACS 2.3 for UNIX。

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。

CSU配置

使用以下過程配置CSU。

啟動Cisco Secure Administrator介面

使用此過程可以登入到Cisco Secure Administrator。

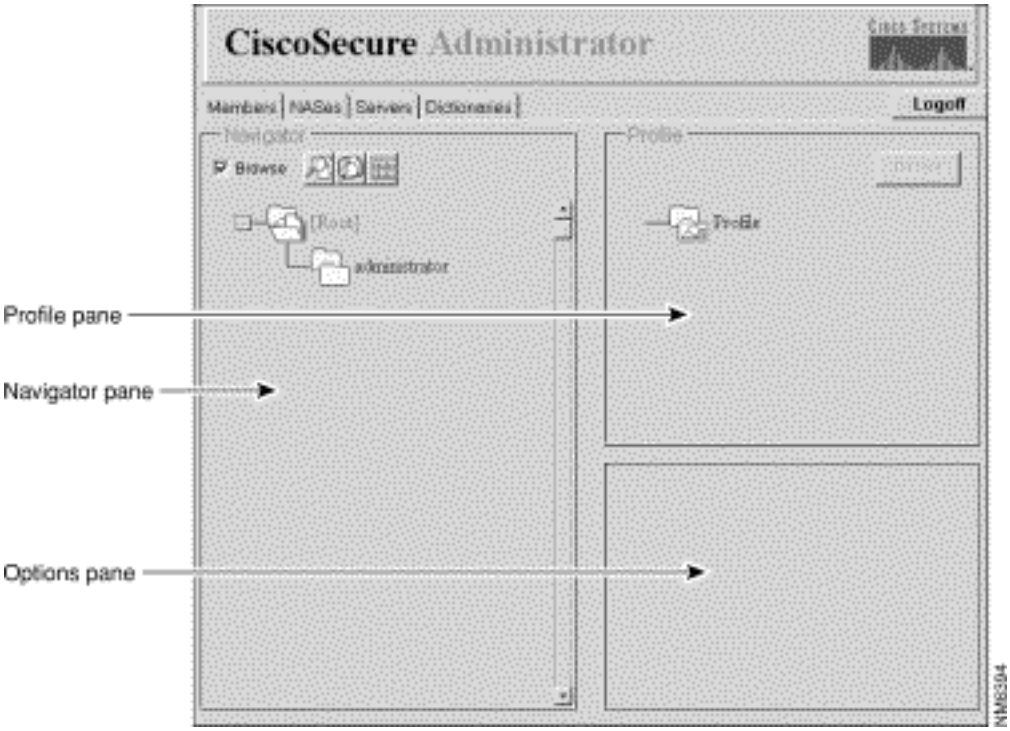
1. 從通過Web連線到ACS的任何工作站啟動Web瀏覽器。
2. 為Cisco Secure Administrator網站輸入以下URL之一：如果未啟用瀏覽器上的安全套接字層功能，請輸入：
   ```
   http://your_server/cs
   ```
   其中your_server是安裝CSU的SPARCstation的主機名(或完全限定的域名(FQDN)，如果主機名和FQDN不同)。您還可以將SPARCstation的IP地址替換為your_server。如果啟用瀏覽器上的安全套接字層功能，請指定「https」而不是「http」作為超文本傳輸協定。輸入：
   ```
   https://your_server/cs
   ```
   其中your_server是安裝CSU的SPARCstation的主機名（如果主機名和FQDN不同，則為FQDN）。您還可以將SPARCstation的IP地址替換為your_server。**注意：**URL和伺服器名稱區分大小寫。必須以大寫和小寫字母準確鍵入，如圖所示。將顯示CSU登入頁。

3. 輸入您的使用者名稱和密碼。按一下「**Submit**」。**注意：**初始預設使用者名稱是「superuser」。 初始預設密碼為「changeme」。 首次登入後，您需要立即更改使用者名稱和密碼以獲得最大安全性。登入後，將顯示CSU首頁，其中主選單欄位於頂部。僅當使用者提供具有管理員級許可權的名稱和密碼時，才會顯示CSU主選單頁。如果使用者提供的名稱和密碼僅具有使用者級許可權，則會顯示不同的螢幕。

啟動高級配置程式

從任何CSU管理員網頁啟動基於Java的Cisco Secure Administrator Advanced Configuration程式。在CSU Web介面的選單欄中，按一下**Advanced**，然後再次按一下**Advanced**。

將顯示Cisco Secure Administrator Advanced Configuration程式。載入可能需要幾分鐘時間。

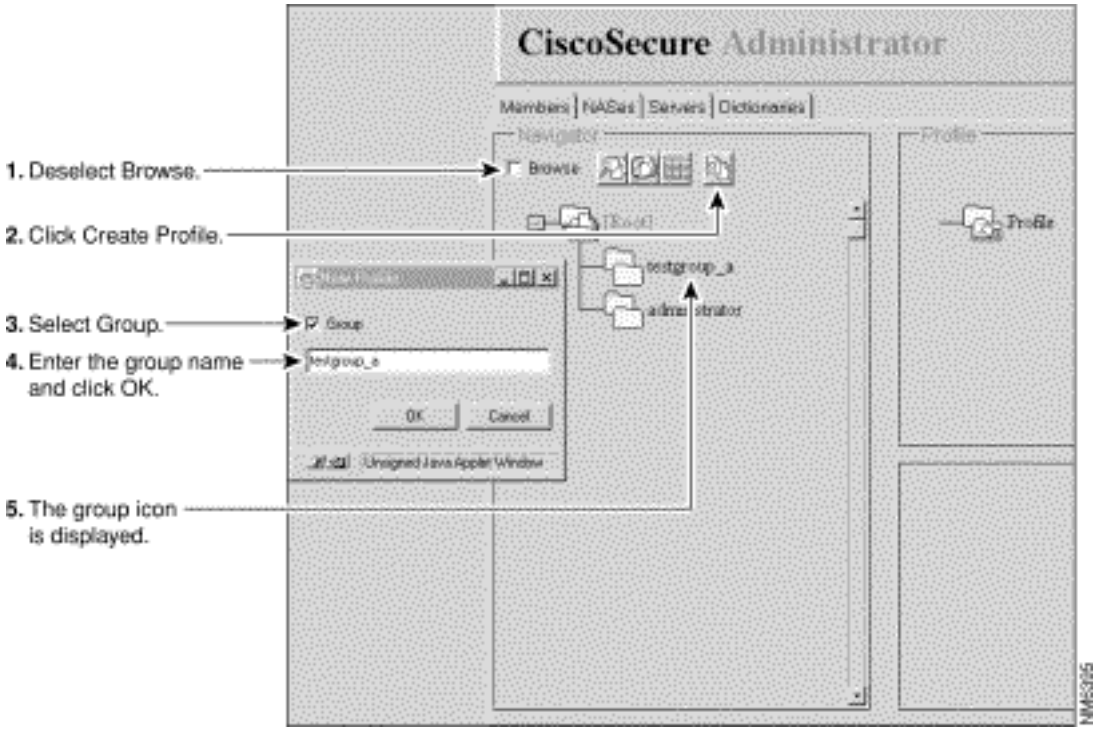


建立組配置檔案

使用Cisco Secure Administrator Advanced Configuration程式建立和配置組配置檔案。思科建議您建立組配置檔案，為大量類似使用者配置詳細的AAA要求。定義組配置檔案後，使用CSU Add a User網頁將使用者配置檔案快速新增到組配置檔案中。為組配置的高級要求適用於每個成員使用者。

使用此過程建立組配置檔案。

1. 在Cisco Secure Administrator Advanced Configuration程式中，選擇**Members**頁籤。在「導航器」窗格中，取消選中「**瀏覽**」覈取方塊。系統隨即會顯示「建立新配置檔案」圖示。
2. 在「導航器」窗格中，執行以下操作之一：要建立沒有父項的組配置檔案，請找到並按一下**[Root]**文件夾圖示。要建立組配置檔案作為另一個組配置檔案的子項，請找到要作為父項的組，然後按一下它。如果要作為父組的組是子組，請按一下其父組的資料夾以顯示它。
3. 按一下**Create New Profile**。將顯示「新建配置檔案」(New Profile)對話方塊。
4. 選中**Group**覈取方塊，鍵入要建立的組的名稱，然後按一下**OK**。新組將顯示在樹中。
5. 建立組配置檔案後，指定TACACS+或RADIUS屬性以配置特定AAA屬性。



在高級配置模式下建立使用者配置檔案

使用Cisco Secure Administrator高級配置模式建立和配置使用者配置檔案。您可以執行此操作以自定義使用者配置檔案的授權和記帳相關屬性，其詳細資訊要比「新增使用者」頁面所能提供的更為詳細。

使用以下過程建立使用者配置檔案：

1. 在Cisco Secure Administrator Advanced Configuration程式中，選擇**Members**頁籤。在「導航器」窗格中，找到並取消選擇**瀏覽**。系統隨即會顯示「建立新配置檔案」圖示。
2. 在「導航器」窗格中，執行以下操作之一：找到並按一下使用者所屬的組。如果不希望使用者屬於某個組，請按一下**[Root]**文件夾圖示。
3. 按一下**Create Profile**。將顯示「新建配置檔案」(New Profile)對話方塊。
4. 確保取消選中**Group**覈取方塊。
5. 輸入要建立的使用者的名稱，然後按一下**確定**。新使用者將顯示在樹中。
6. 建立使用者配置檔案後，分配特定TACACS+或RADIUS屬性以配置特定AAA屬性：要將TACACS+配置檔案分配給使用者配置檔案，請參閱將TACACS+屬性分配給組或使用者配置檔案。要將RADIUS配置檔案分配給使用者配置檔案，請參閱將RADIUS屬性分配給組或使用者配置檔案。

應用屬性的策略

使用CSU組配置檔案功能以及TACACS+和RADIUS屬性通過CSU實施網路使用者的身份驗證和授權。

組和使用者的計畫屬性

CSU的組配置檔案功能使您可以為大量使用者定義一組通用的AAA要求。

您可以將一組TACACS+或RADIUS屬性值分配給組配置檔案。分配給組的這些屬性值適用於作為該組的成員或被新增為該組成員的任何使用者。

有效使用組配置檔案功能

要配置CSU來管理具有複雜AAA要求的大量不同型別的使用者，思科建議您使用Cisco Secure Administrator Advanced Configuration程式的功能來建立和配置組配置檔案。

組配置檔案需要包含並非特定於使用者的所有屬性。這通常表示除密碼以外的所有屬性。然後，您可以使用Cisco Secure Administrator的「新增使用者」頁面建立具有密碼屬性的簡單使用者配置檔案，並將這些使用者配置檔案分配給相應的組配置檔案。然後，為特定組定義的功能和屬性值將應用於其成員使用者。

父組和子組

您可以建立組的層次結構。在組配置檔案中，您可以建立子組配置檔案。分配給父組配置檔案的屬性值是子組配置檔案的預設值。

組級管理

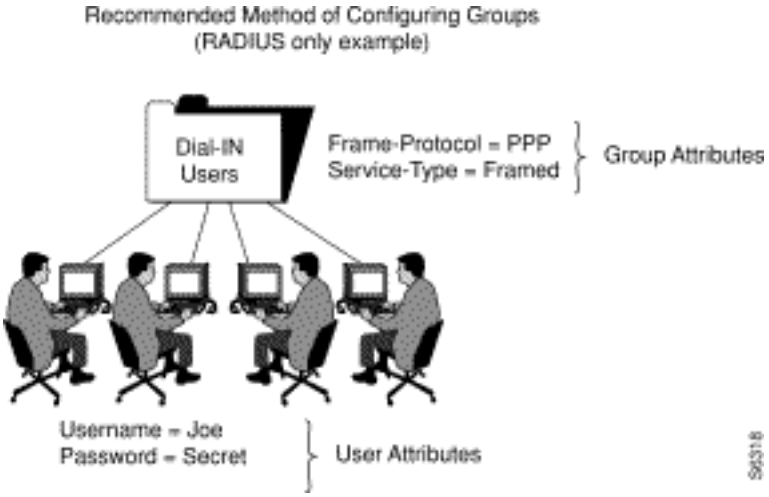
Cisco Secure系統管理員可以分配各個Cisco Secure使用者組管理員狀態。「組管理員」狀態允許單個使用者管理其組從屬的任何子組配置檔案和使用者配置檔案。但是，不允許他們管理屬於其組層次結構之外的任何組或使用者。因此，系統管理員將管理大型網路的任務外包給其他人，而未授予每個人平等的許可權。

我應該為單個使用者定義哪些屬性？

思科建議您為單個使用者分配使用者唯一的基本身份驗證屬性值，例如定義使用者名稱、密碼、密碼型別和Web許可權的屬性。通過CSU的Edit a User或Add a User頁向使用者分配基本身份驗證屬性值。

為組配置檔案定義哪些屬性？

思科建議您定義組級別的資格審批、授權和記帳相關屬性。



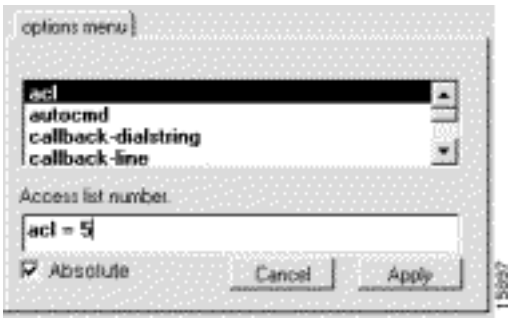
在本示例中，為名為「撥入使用者」的組配置檔案分配了屬性值對Frame-Protocol=PPP和Service-Type=Framed。

什麼是絕對屬性？

CSU中TACACS+和RADIUS屬性的子集可以在組配置檔案級別分配絕對狀態。在組配置檔案層為絕對狀態啟用的屬性值將覆蓋子組配置檔案層或成員使用者配置檔案層的任何衝突屬性值。

在具有若干級別組管理員的多級網路中，通過絕對屬性，系統管理員可以設定選定組屬性值，而較低級別的組管理員無法覆蓋這些值。

可分配絕對狀態的屬性在Cisco Secure Administrator高級配置程式的「屬性」框中顯示「絕對」覈取方塊。選中此覈取方塊可啟用絕對狀態。



組屬性值和使用者屬性值是否衝突？

指派給父組配置檔案、子組配置檔案和成員使用者配置檔案的屬性值之間的衝突解決取決於屬性值是絕對屬性值還是是TACACS+或RADIUS屬性：

- 分配給具有絕對狀態的組配置檔案的TACACS+或RADIUS屬性值會覆蓋在子組或使用者配置檔案級別設定的任何衝突屬性值。
- 如果在組配置檔案級別未啟用TACACS+屬性值的絕對狀態，則任何在子組或使用者配置檔案級別設定的衝突屬性值都將覆蓋該屬性。
- 如果在父組級別未啟用RADIUS屬性值的絕對狀態，則在子組設定的任何衝突屬性值都將導致不可預測的結果。為組及其成員使用者定義RADIUS屬性值時，請避免為使用者和組配置檔案分配相同的屬性。

使用禁止和允許選項

對於TACACS+，請通過將關鍵字**prohibit**或**permit**置於服務規範的字首來覆蓋繼承的服務值的可用性。**permit**關鍵字允許指定的服務。**prohibit**關鍵字不允許使用指定的服務。結合使用這些關鍵字，您可以構建「除外的一切」配置。例如，此組態允許從X.25以外的所有服務存取：

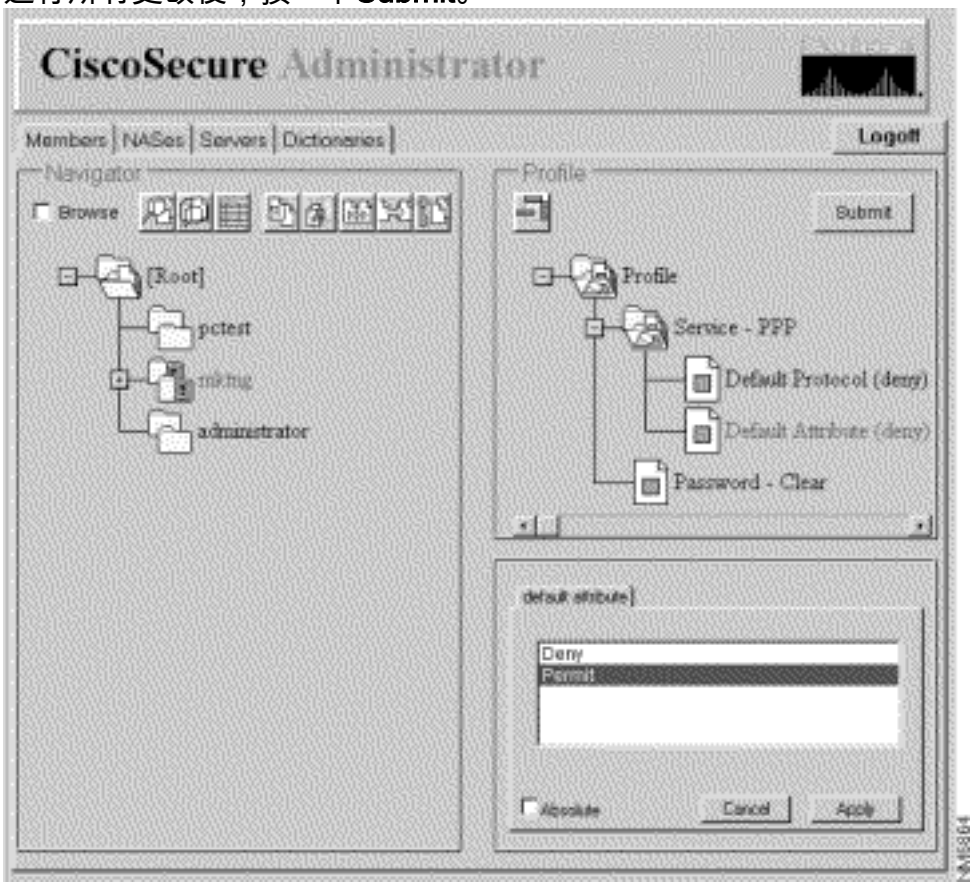
```
default service = permit
prohibit service = x25
```

將TACACS+屬性分配給組或使用者配置檔案

要將特定TACACS+服務和屬性分配給組或使用者配置檔案，請執行以下步驟：

1. 在Cisco Secure Administrator Advanced Configuration程式中，選擇**Members**頁籤。在「導航器」窗格中，點選分配TACACS+屬性的組或使用者配置檔案的圖示。
2. 如有必要，在Profile窗格中，按一下**Profile**圖示將其展開。螢幕右下方的視窗中將顯示一個清單或對話方塊，其中包含適用於選定配置檔案或服務的屬性。此視窗中的資訊會根據您在「配置檔案」窗格中選擇的配置檔案或服務而更改。
3. 按一下要新增的服務或協定，然後按一下**Apply**。該服務將新增到配置檔案。

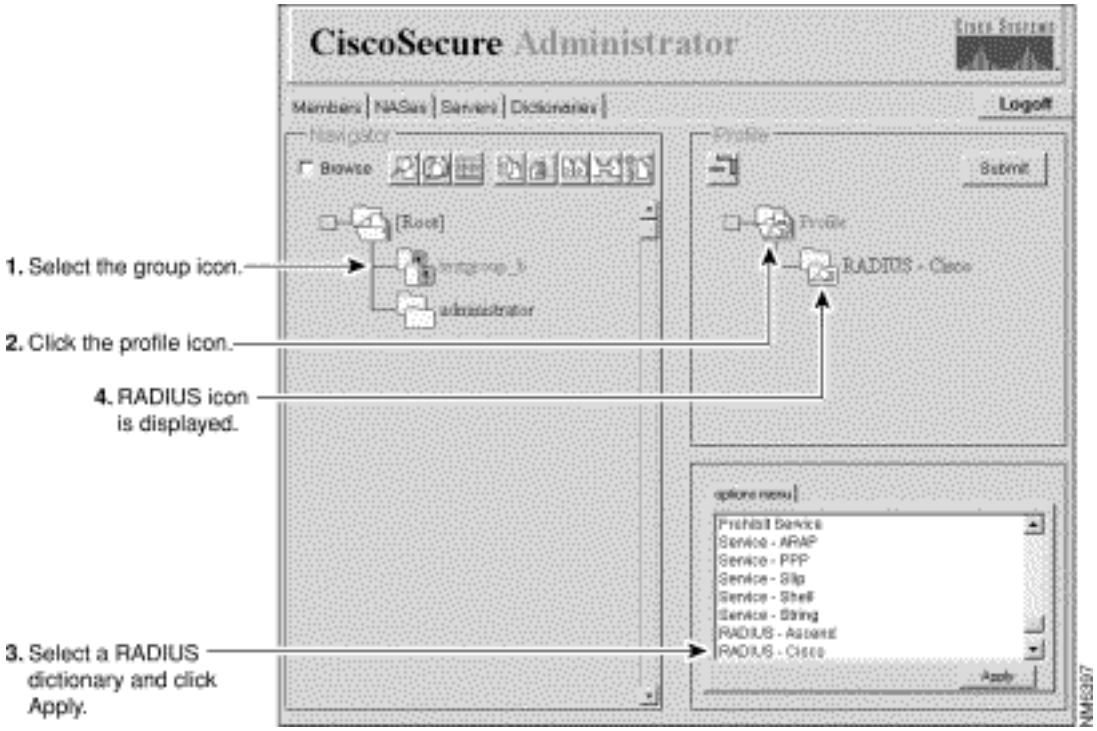
4. 在「屬性」視窗中輸入或選擇所需的文本。有效條目在CSU 2.3 for UNIX參考指南的Strategies for Applying Attributes一節中說明。**註：如**果您在組配置檔案層分配了屬性值，並且指定的屬性顯示**了「絕對」複選**框，請選中該覈取方塊以分配值絕對狀態。值分配的絕對狀態不能被從屬組配置檔案層或使用者配置檔案層分配的任何衝突值覆蓋。
5. 對需要新增的每個其他服務或協定重複步驟1到。
6. 進行所有更改後，按一下**Submit**。



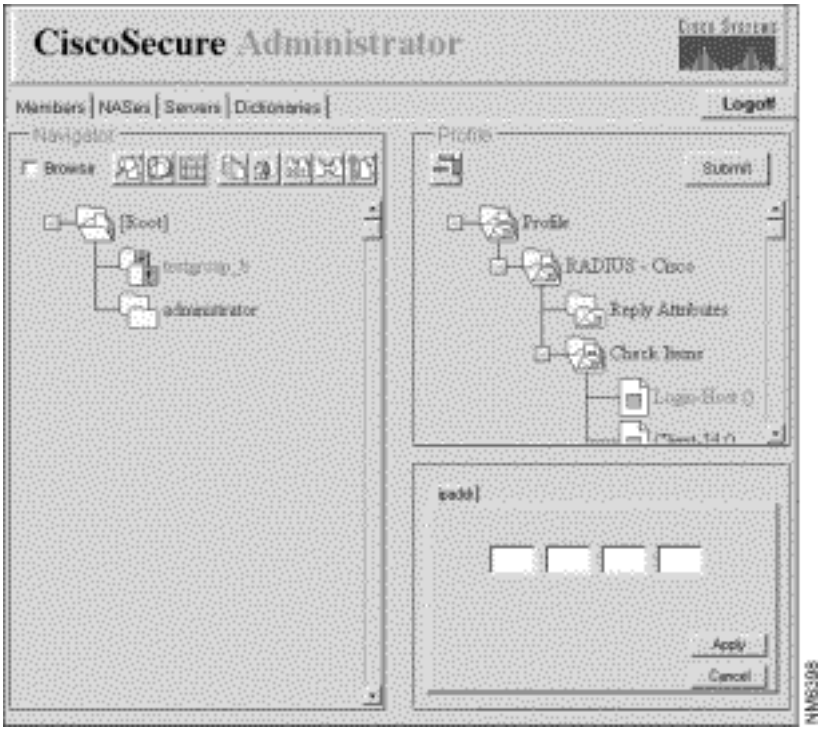
將RADIUS屬性分配給組或使用者配置檔案

要將特定RADIUS屬性分配給組或使用者配置檔案，請執行以下操作：

1. 為組配置檔案分配RADIUS字典：在Cisco Secure Administrator Advanced Configuration程式的「成員」頁面上，按一下**Group**或**User**圖示，然後按一下「配置檔案」窗格中的**Profile**圖示。在「屬性」窗格中，將顯示「選項」選單。在「**選項**」選單中，按一下希望組或使用者使用的RADIUS字典的名稱。（例如，RADIUS - Cisco。）按一下「**Apply**」。



2. 將所需的檢查專案和回覆屬性新增到RADIUS配置檔案：**注意：**檢查項是身份驗證所需的屬性，如使用者ID和密碼。應答屬性是在配置檔案通過身份驗證過程（例如Framed-Protocol）之後傳送到網路訪問伺服器(NAS)的屬性。有關檢查項和回覆屬性的清單和說明，請參閱《CSU 2.3 for UNIX Reference Guide》中的RADIUS Attribute-Value Pairs and Dictionary Management。在「配置檔案」視窗中，按一下RADIUS - dictionaryname資料夾圖示。（您可能需要按一下配置檔案的+符號來展開RADIUS資料夾。）「檢查專案」和「回覆屬性」選項將顯示在「屬性組」視窗中。要使用一個或多個這些屬性，請按一下要使用的屬性，然後按一下**應用**。一次可以新增多個屬性。按一下RADIUS - dictionaryname的**+**符號以展開資料夾。**注意：**如果選擇RADIUS-Cisco11.3選項，請確保在連線的NAS上安裝了Cisco IOS®軟體版本11.3.3(T)或更高版本，並將新命令列新增到NAS配置中。請參閱《CSU 2.3 for UNIX參考指南》中的完全啟用RADIUS-Cisco11.3字典。
3. 為新增的檢查項和回覆屬性指定值：**注意：**對於RADIUS協定，繼承是累加的，而不是分層的。（TACACS+通訊協定使用階層繼承）。 例如，如果您將相同的應答屬性分配給使用者和組配置檔案，授權將失敗，因為NAS收到的屬性數是此屬性的兩倍。它無法理解回覆屬性。不要將相同的檢查項或回覆屬性同時分配給組和使用者配置檔案。按一下**Check Items**或**Reply Attributes**，或者同時按一下兩者。右下視窗將顯示適用的「檢查專案」和「回覆屬性」值清單。按一下**+**符號展開資料夾。按一下要指定的值，然後按一下**應用**。有關這些值的詳細資訊，請參閱《CSU 2.3 for UNIX Reference Guide》中的RADIUS Attribute-Value Pairs and Dictionary Management。**註：如**果您在組配置檔案層分配屬性值，並且指定的屬性顯示一個絕對覈取方塊，則選擇該覈取方塊以分配值絕對狀態。分配的絕對狀態值不能被在從屬組配置檔案層或使用者配置檔案層分配的任何衝突值覆蓋。完成更改後，按一下**Submit**。



4. 要使用一個或多個這些屬性，請按一下要使用的屬性，然後按一下**應用**。一次可以應用多個屬性。

分配訪問控制許可權級別

超級使用者管理員使用Web許可權屬性為Cisco Secure使用者分配一定級別的訪問控制許可權。

1. 在Cisco Secure Administrator Advanced Configuration程式中，按一下要分配其訪問控制許可權的使用者，然後按一下Profiles窗格中的Profile圖示。
2. 在「選項」選單中，按一下**Web許可權**，然後選擇其中一個值。**0** — 拒絕使用者包括更改使用者的Cisco Secure密碼在內的任何訪問控制許可權。**1** — 授予使用者訪問CSUser網頁的許可權。這允許Cisco Secure使用者更改其Cisco Secure密碼。有關如何更改密碼的詳細資訊，請參閱簡單使用者和ACS管理中的使用者級功能（更改密碼）。**12** — 授予使用者組管理員許可權。**15** — 授予使用者系統管理員許可權。**註：如**果選擇除0之外的任何Web許可權選項，還必須指定口令。為了滿足Web許可權密碼要求，最小可以接受單個空格。

啟動和停止CSU

通常，CSU在您啟動或重新啟動安裝它的SPARCstation時自動啟動。但是，您可以手動啟動CSU，或者在不關閉整個SPARCtation的情況下將其關閉。

以[Root]身份登入到安裝CSU的SPARCStation。

要手動啟動CSU，請鍵入：

```
# /etc/rc2.d/S80CiscoSecure
```

要手動停止CSU，請鍵入：

```
# /etc/rc0.d/K80CiscoSecure
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- Cisco Secure ACS for UNIX支援頁
- TACACS+支援頁面
- RADIUS 支援頁面
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems