

安全ACS - NAR與使用者和使用者組的AAA客戶端

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[網路訪問限制](#)

[關於網路訪問限制](#)

[新增共用NAR](#)

[編輯共用NAR](#)

[刪除共用NAR](#)

[為使用者設定網路訪問限制](#)

[設定使用者組的網路訪問限制](#)

[相關資訊](#)

簡介

本檔案介紹如何使用AAA使用者端 (包括路由器、PIX、ASA和無線控制器) 為使用者和使用者組設定Cisco安全存取控制伺服器(ACS)4.x版中的網路存取限制(NAR)。

必要條件

需求

本文的建立假設前提是Cisco Secure ACS和AAA客戶端已配置且工作正常。

採用元件

本檔案中的資訊是根據Cisco Secure ACS 3.0及更新版本。

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](#)。

網路訪問限制

本節介紹NAR，並提供配置和管理共用NAR的詳細說明。

本節包含以下主題：

- [關於網路訪問限制](#)
- [新增共用NAR](#)
- [編輯共用NAR](#)
- [刪除共用NAR](#)

關於網路訪問限制

NAR是在ACS中定義的附加條件，使用者必須滿足這些條件才能訪問網路。ACS通過使用來自AAA客戶端傳送的屬性的資訊來應用這些條件。雖然可以通過多種方式設定NAR，但所有這些都基於AAA客戶端傳送的匹配屬性資訊。因此，如果要使用有效的NAR，您必須瞭解AAA客戶端傳送的屬性的格式和內容。

設定NAR時，您可以選擇過濾器是執行正值還是負值。也就是說，在NAR中，您根據與NAR中儲存的資訊比較時從AAA客戶端傳送的資訊指定是允許還是拒絕網路訪問。但是，如果NAR沒有獲得足夠的資訊來運行，則預設設定為拒絕訪問。下表顯示了以下條件：

	基於IP	非IP型	資訊不足
允許	已授予訪問許可權	拒絕訪問	拒絕訪問
拒絕	拒絕訪問	已授予訪問許可權	拒絕訪問

ACS支援兩種型別的NAR過濾器：

- **基於IP的過濾器** — 基於IP的NAR過濾器根據終端使用者客戶端和AAA客戶端的IP地址限制訪問。有關詳細資訊，請參閱[關於基於IP的NAR過濾器](#)部分。
- **非基於IP的過濾器** — 非基於IP的NAR過濾器基於從AAA客戶端傳送的值的簡單字串比較來限制訪問。該值可以是主叫線路標識(CLI)號碼、被叫號碼標識服務(DNIS)號碼、MAC地址或來自客戶端的其他值。為了使此型別的NAR運行，NAR描述中的值必須與從客戶端傳送的内容完全匹配，其中包括使用的所有格式。例如，電話號碼(217)555-4534與217-555-4534不匹配。有關詳細資訊，請參閱[關於非IP型NAR過濾器](#)部分。

您可以為特定使用者或使用者組定義NAR並將其應用於特定使用者或使用者組。有關詳細資訊，請參閱[設定使用者的網路訪問限制](#)或[設定使用者組的網路訪問限制](#)部分。但是，在ACS的共用配置檔案元件部分中，您可以建立和命名共用NAR，而無需直接引用任何使用者或使用者組。您可以為共用NAR指定一個名稱，該名稱可在ACS Web介面的其他部分中引用。然後，當您設定使用者或使用者組時，可以選擇要應用的無、一個或多個共用限制。當您指定將多個共用NAR應用到使用者或使用者組時，請選擇以下兩個訪問條件之一：

- 所有選定的過濾器都必須允許。
- 任何選定的篩選器都必須允許。

您必須瞭解與不同型別的NAR相關的優先順序順序。這是NAR過濾的順序：

1. 使用者級別的共用NAR
2. 在組級別共用NAR
3. 使用者級別的非共用NAR

4. 組級別的非共用NAR

您還應該瞭解，拒絕任何級別的訪問優先於不拒絕訪問的另一級別的設定。這是ACS中使用者級別設定替代組級別設定的規則的一個例外。例如，某個特定使用者在適用的使用者級別可能沒有NAR限制。但是，如果該使用者屬於受共用或非共用NAR限制的組，則該使用者將被拒絕訪問。

共用的NAR儲存在ACS內部資料庫中。您可以使用ACS備份和還原功能來備份和還原它們。您還可將共用NAR以及其他配置複製到輔助ACS。

[關於基於IP的NAR過濾器](#)

對於基於IP的NAR過濾器，ACS使用如下所示的屬性，這取決於身份驗證請求的AAA協定：

- **如果您使用的是TACACS+** — 會使用TACACS+起始封包正文中的`rem_addr`欄位。**注意：**當身份驗證請求通過代理轉發到ACS時，TACACS+請求的任何NAR都會應用到轉發AAA伺服器的IP地址，而不是源AAA客戶端的IP地址。
- **如果您使用的是RADIUS IETF** — 必`calling-station-id` (屬性31)。**注意：**只有當ACS收到Radius Calling-Station-Id(31)屬性時，基於IP的NAR過濾器才能正常工作。Calling-Station-Id(31)必須包含有效的IP地址。如果沒有，它將歸於DNIS規則。

沒有提供足夠IP地址資訊的AAA客戶端 (例如，某些型別的防火牆) 不支援完整的NAR功能。

每個協定的基於IP限制的其他屬性包括NAR欄位，如下所示：

- **如果您使用的是TACACS+** - ACS中的NAR欄位使用以下值：**AAA客戶端** — NAS-IP地址取自ACS和TACACS+客戶端之間的套接字中的源地址。**Port** — 連線埠欄位來自TACACS+起始封包主體。

[關於非IP型NAR過濾器](#)

非基於IP的NAR過濾器 (即基於DNIS/CLI的NAR過濾器) 是允許或拒絕的呼叫或訪問點位置的清單，可用於在沒有已建立的基於IP的連線時限制AAA客戶端。非基於IP的NAR功能通常使用CLI編號和DNIS編號。

但是，當您輸入IP地址代替CLI時，您可以使用非基於IP的過濾器；即使AAA客戶端不使用支援CLI或DNIS的Cisco IOS®軟體版本。在輸入CLI的另一個例外情況中，您可以輸入MAC地址來允許或拒絕訪問。例如，當您使用Cisco Aironet AAA客戶端時。同樣，您可以輸入Cisco Aironet AP MAC地址來代替DNIS。在CLI框中指定的格式 (CLI、IP地址或MAC地址) 必須與從AAA客戶端接收的格式匹配。您可以從RADIUS計費日誌確定此格式。

每個協定基於DNIS/CLI的限制的屬性包括NAR欄位，如下所示：

- **如果您使用的是TACACS+** — 列出的NAR欄位使用以下值：**AAA client** - `NAS-IP-address`取自ACS和TACACS+客戶端之間的套接字中的源地址。**Port** — 使用TACACS+啟動封包主體中的**CLI** — 使用TACACS+開始封包主體中的`rem-addr`**DNIS** — 使用從TACACS+起始封包主體取得的`rem-addr`欄位。如果`rem-addr`資料以斜槓(/)開頭，則DNIS欄位包含不帶斜槓(/)的`rem-addr`資料。**注意：**當身份驗證請求通過代理轉發到ACS時，TACACS+請求的任何NAR都會應用到轉發AAA伺服器的IP地址，而不是源AAA客戶端的IP地址。
- **如果使用的是RADIUS** — 列出的NAR欄位使用以下值：**AAA客戶端** — 使用`NAS-IP-address` (屬性4)，如果不存在`NAS-IP-address`，則使用`NAS-identifier` (RADIUS屬性32)。**Port** — 使用`NAS-port` (屬性5)，如果沒有`NAS-port`，則使用`NAS-port-ID` (屬性87)。**CLI** — 使`ID` (屬性

31)。DNIS — 使ID (屬性30)。

指定NAR時，可以使用星號(*)作為任何值的萬用字元，或者作為任何值的一部分來建立範圍。必須滿足NAR說明中的所有值或條件，NAR才能限制訪問。這表示這些值包含布林AND。

新增共用NAR

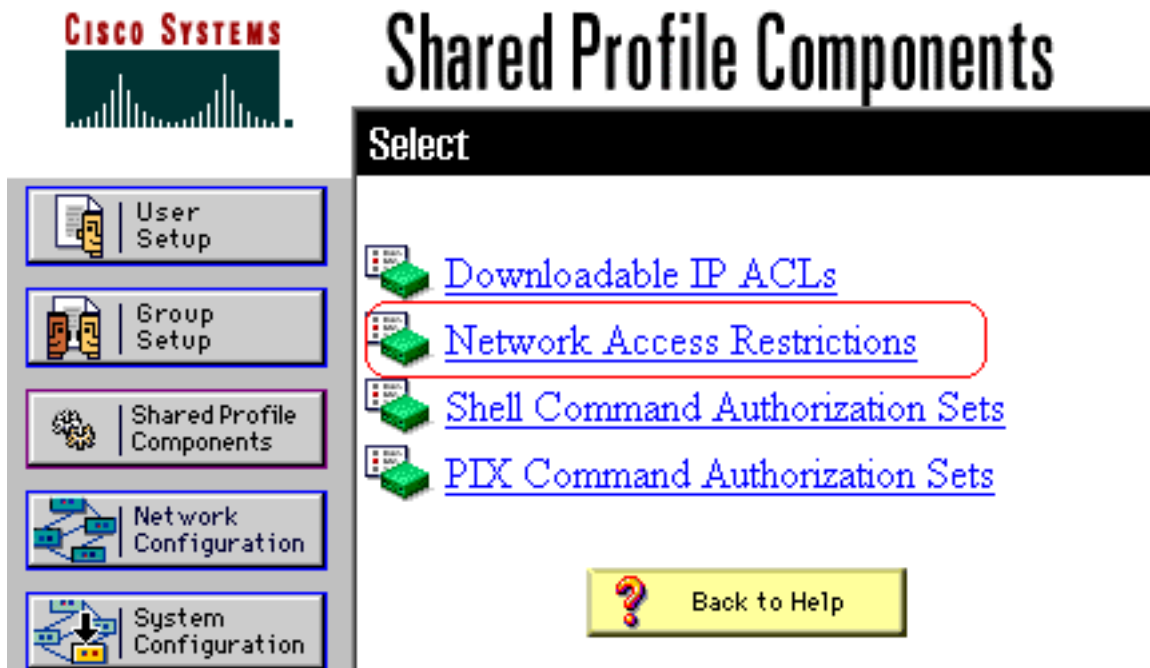
您可以建立一個包含許多訪問限制的共用NAR。雖然ACS Web介面不對共用NAR中的訪問限制數量或每個訪問限制的長度實施限制，但是您必須遵守以下限制：

- 每個行項的欄位組合不能超過1024個字元。
- 共用NAR的字元數不能超過16 KB。支援的行專案數取決於每個行專案的長度。例如，如果建立基於CLI/DNIS的NAR，其中AAA客戶端名稱為10個字元，埠號為5個字元，CLI條目為15個字元，DNIS條目為20個字元，則可以在達到16 KB限制之前新增450行專案。

注意：在定義NAR之前，請確保已經建立了要在該NAR中使用的元素。因此，您必須先指定所有NAF和NDG，並定義所有相關的AAA客戶端，然後才能將其作為NAR定義的一部分。有關詳細資訊，請參閱[關於網路訪問限制](#)部分。

完成以下步驟以新增共用NAR:

1. 在導航欄中，按一下Shared Profile Components。此時將出現「共用配置檔案元件」視窗。




2. 按一下「Network Access Restrictions」。



Shared Profile Components

Select

Network Access Restrictions 

Name	Description
None Defined	

Add Cancel

3. 按一下「Add」。出現「Network Access Restriction (網路訪問限制)」視窗。

Shared Profile Components

Network Access Restriction

Name:

Description:

Define IP-based access restrictions

Table Defines:

AAA Client	Port	Src IP Address
<input type="text"/>		
<input type="button" value="remove"/>		
AAA Client	<input type="text" value="All AAA Clients"/>	<input type="text"/>
Port	<input type="text"/>	<input type="text"/>
Src IP Address	<input type="text"/>	<input type="text"/>
<input type="button" value="enter"/>		

Define CLI/DNIS-based access restrictions

Table Defines:

AAA Client	Port	CLI	DNIS
<input type="text"/>			

- 在名稱框中，輸入新共用NAR的名稱。**注意：**名稱最多可包含31個字元。不允許使用前導空格和尾隨空格。名稱不能包含以下字元：左括弧(())、右括弧(())、逗號(,)或斜線(/)。
- 在Description框中，輸入新共用NAR的說明。描述最多可包含30,000個字元。
- 如果要允許或拒絕基於IP地址的訪問：選中**Define IP-based access descriptions**釐取方塊。要指定是否列出允許或拒絕的地址，請從表定義清單中選擇適用的值。在這些框中選擇或輸入適用資訊：**AAA Client** — 選擇**所有AAA客戶端**，或者允許或拒絕訪問的NDG或NAF或單個AAA客戶端的名稱。**Port** — 輸入要允許或拒絕訪問的埠編號。您可以使用星號(*)作為萬用字元，允許或拒絕訪問所選AAA客戶端上的所有埠。**Src IP Address** — 輸入執行訪問限制時過濾的IP地址。可以使用星號(*)作為萬用字元指定所有IP地址。**注意：**AAA客戶端清單、埠和源IP地址框中的字元總數不得超過1024。儘管ACS在新增NAR時接受超過1024個字元，但您無法編輯NAR，並且ACS無法將其準確地應用到使用者。按一下「Enter」。AAA客戶端、埠和地址資訊在表中顯示為行專案。重複步驟c和d以輸入其他基於IP的行專案。

7. 如果要根據呼叫位置或IP地址以外的值允許或拒絕訪問：選中**Define CLI/DNIS based access restrictions** 覆取方塊。要指定是否從「表定義」清單中列出允許或拒絕的位置，請選擇適用的值。要指定此NAR應用到的客戶端，請從AAA客戶端清單中選擇以下值之一：NDG的名稱特定AAA客戶端的名稱所有AAA客戶端**提示**：僅列出您已配置的NDG。要指定此NAR應過濾的資訊，請在下列框中輸入值（如果適用）：**提示**：可以輸入星號(*)作為萬用字元來指定**全部**為一個值。**Port** — 輸入要過濾的埠的編號。**CLI** — 輸入要過濾的CLI編號。您還可以使用此框基於CLI以外的值（如IP地址或MAC地址）限制訪問。有關詳細資訊，請參閱[關於網路訪問限制](#)部分。**DNIS** — 輸入撥號到的號碼進行過濾。**注意**：AAA客戶端清單以及Port、CLI和DNIS框中的字元總數不得超過1024。儘管ACS在新增NAR時接受超過1024個字元，但您無法編輯NAR，並且ACS無法將其準確地應用到使用者。按一下「**Enter**」。表中將顯示指定NAR行專案的資訊。重複步驟c至e以輸入其他非基於IP的NAR行專案。按一下**Submit**以儲存共用NAR定義。ACS儲存共用NAR並將其列在**網路訪問限制**表中。

編輯共用NAR

完成以下步驟即可編輯共用NAR：

1. 在導航欄中，按一下**Shared Profile Components**。此時將出現「共用配置檔案元件」視窗。
2. 按一下「**Network Access Restrictions**」。此時會顯示「網路訪問限制」表。
3. 在「名稱」列中，按一下要編輯的共用NAR。出現「Network Access Restriction (網路訪問限制)」視窗，並顯示所選NAR的資訊。
4. 根據需要編輯NAR的名稱或說明。描述最多可包含30,000個字元。
5. 若要編輯基於IP的訪問限制表中的行專案：按兩下要編輯的行專案。行專案資訊將從表中刪除，並寫入表格下的框。根據需要編輯資訊。**注意**：AAA Client清單以及Port和Src IP Address框中的字元總數不得超過1024。儘管ACS在新增NAR時可以接受超過1024個字元，但您無法編輯此類NAR，並且ACS無法將其準確地應用於使用者。按一下「**Enter**」。此行專案的編輯資訊將寫入基於IP的訪問限制表中。
6. 要從基於IP的訪問限制表中刪除行專案，請執行以下操作：選擇行專案。在表下，按一下**Remove**。行專案將從基於IP的訪問限制表中刪除。
7. 要編輯CLI/DNIS訪問限制表中的行專案，請執行以下操作：按兩下要編輯的行專案。行專案資訊將從表中刪除，並寫入表格下的框。根據需要編輯資訊。**注意**：AAA客戶端清單以及Port、CLI和DNIS框中的字元總數不得超過1024。儘管ACS在新增NAR時可以接受超過1024個字元，但您無法編輯此類NAR，並且ACS無法將其準確地應用於使用者。按一下「**Enter**」此行專案的編輯資訊將寫入CLI/DNIS訪問限制表。
8. 若要從CLI/DNIS存取限制表中移除行專案：選擇行專案。在表下，按一下**Remove**。該行專案將從CLI/DNIS訪問限制表中刪除。
9. 按一下「**Submit**」以儲存變更內容。ACS使用新資訊重新輸入過濾器，立即生效。

刪除共用NAR

注意：在刪除共用NAR之前，請確保刪除與任何使用者或組的關聯。

完成以下步驟即可刪除共用NAR：

1. 在導航欄中，按一下**Shared Profile Components**。此時將出現「共用配置檔案元件」視窗。
2. 按一下「**Network Access Restrictions**」。
3. 按一下要刪除的共用NAR的名稱。出現「Network Access Restriction (網路訪問限制)」視窗，並顯示所選NAR的資訊。

4. 在視窗底部，按一下**Delete**。對話方塊會警告您即將刪除共用NAR。
5. 按一下**OK**以確認要刪除共用NAR。所選共用NAR即被刪除。

為使用者設定網路訪問限制

可以使用使用者設定的「高級設定」區域中的「網路訪問限制」表以三種方式設定NAR:

- 按名稱應用現有共用NAR。
 - 定義基於IP的訪問限制，以便在建立IP連線時允許或拒絕使用者訪問指定的AAA客戶端或AAA客戶端上的指定埠。
 - 定義基於CLI/DNIS的訪問限制，以根據使用的CLI/DNIS允許或拒絕使用者訪問。**注意：**您還可以使用基於CLI/DNIS的訪問限制區域指定其他值。有關詳細資訊，請參閱[網路訪問限制](#)部分。
- 通常，您可以從「共用元件」部分定義（共用）NAR，以便將這些限制應用到多個組或使用者。有關詳細資訊，請參閱[新增共用NAR](#)部分。您必須在「介面配置」部分的「高級選項」頁中選中**User-Level Network Access Restrictions**覈取方塊，此組選項才能顯示在Web介面中。

但是，您還可以使用ACS在「使用者設定」部分中為單個使用者定義並應用NAR。您必須在「介面配置」部分的「高級選項」頁中啟用**User-Level Network Access Restrictions**設定，才能在Web介面中顯示基於IP的單個使用者過濾器選項和基於CLI/DNIS的單個使用者過濾器選項。

注意：當身份驗證請求通過代理轉發到ACS時，終端訪問控制器訪問控制系統(TACACS+)請求的任何NAR都應用於轉發AAA伺服器的IP地址，而不是源AAA客戶端的IP地址。

當您基於每個使用者建立訪問限制時，ACS不會強制限制訪問限制的數量，也不會強制限制每個訪問限制的長度。然而，這些限制非常嚴格：

- 每個行項的欄位組合長度不能超過1024個字元。
- 共用NAR的字元數不能超過16 KB。支援的行專案數取決於每個行專案的長度。例如，如果建立基於CLI/DNIS的NAR，其中AAA客戶端名稱為10個字元，埠號為5個字元，CLI條目為15個字元，DNIS條目為20個字元，則可以在達到16 KB限制之前新增450行專案。

完成以下步驟，為使用者設定NAR:

1. 執行[新增基本使用者帳戶](#)的步驟1至3。將開啟「使用者設定編輯」視窗。您新增或編輯的使用者名稱將顯示在視窗頂部。

User Setup

Advanced Settings

Network Access Restrictions (NAR) ?

Shared Network Access Restrictions

Only Allow network access when

- All selected NARs result in permit
- Any one selected NAR results in permit

NARs

testnar

>>

->

<-

<<

Selected NARs

View IP NAR

View CLI/DNIS NAR

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	Address

remove

AAA Client All AAA Clients

Port

Address

Submit

Delete

Cancel

2. 要將以前配置的共用NAR應用到此使用者，請執行以下操作：**注意**：要應用共用NAR，必須在「共用配置檔案元件」部分的「網路訪問限制」下配置它。有關詳細資訊，請參閱[新增共用NAR](#)部分。選中**Only Allow network access when** 覆取方塊。要指定必須應用一個還是所有共用NAR才能允許使用者訪問，請選擇一個（如果適用）：所有選定的NARS都會得到允許。任何選定的NAR都會導致permit。在NAR清單中選擇一個共用NAR名稱，然後按一下 **—>**（右箭頭按鈕）將該名稱移到「選定NAR」清單中。**提示**：要檢視已選擇要應用的共用NAR的伺服器

器詳細資訊，可根據需要按一下**View IP NAR**或**View CLID/DNIS NAR**。

3. 要為此特定使用者定義並應用NAR，以根據IP地址或IP地址和埠允許或拒絕此使用者訪問：**注意**：您應該從「共用元件」部分中定義大多數NAR，以便將其應用於多個組或使用者。有關詳細資訊，請參閱[新增共用NAR](#)部分。在Network Access Restrictions表中的Per User Defined Network Access Restrictions下，選中**Define IP-based access restrictions**覈取方塊。要指定後續清單是指定允許還是拒絕的IP地址，請從表定義清單中選擇一個：**允許的呼叫/接入點位置** **拒絕的呼叫/接入點位置**在以下框中選擇或輸入資訊：**AAA Client** — 選擇**所有AAA Clients**，或者要允許或拒絕訪問的網路裝置組(NDG)的名稱，或者單個AAA客戶端的名稱。**Port** — 輸入要允許或拒絕訪問的埠編號。您可以使用星號(*)作為萬用字元，允許或拒絕訪問所選AAA客戶端上的所有埠。**Address** — 輸入執行訪問限制時要使用的IP地址。可以使用星號(*)作為萬用字元。**注意**：AAA客戶端清單、埠和源IP地址框中的字元總數不得超過1024。儘管ACS在新增NAR時接受超過1024個字元，但您無法編輯NAR，並且ACS無法將其準確地應用到使用者。按一下「**Enter**」。指定的AAA客戶端、埠和地址資訊顯示在AAA客戶端清單上方的表中。
4. 若要根據呼叫位置或除已建立IP地址以外的值來允許或拒絕此使用者訪問：選中**Define CLI/DNIS based access restrictions**覈取方塊。要指定後續清單是指定允許值還是拒絕值，請從表定義清單中選擇一個：**允許的呼叫/接入點位置** **拒絕的呼叫/接入點位置**按如下所示完成框：**注意**：必須在每個框中建立一個條目。可以使用星號(*)作為萬用字元表示全部或部分值。使用的格式必須與從AAA客戶端接收的字串的格式匹配。您可以從RADIUS計費日誌確定此格式。**AAA Client** — 選擇**所有AAA Clients**，或選擇要允許或拒絕其訪問的NDG名稱或單個AAA客戶端的名稱。**PORT** — 輸入要允許或拒絕訪問的埠編號。您可以使用星號(*)作為萬用字元來允許或拒絕對所有埠的訪問。**CLI** — 輸入允許或拒絕訪問的CLI編號。您可以使用星號(*)作為萬用字元，根據數字的一部分允許或拒絕訪問。**提示**：如果要根據其他值（例如Cisco Aironet客戶端MAC地址）限制訪問，請使用CLI條目。有關詳細資訊，請參閱[關於網路訪問限制](#)部分。**DNIS** — 輸入要允許或拒絕訪問的DNIS編號。使用此條目根據使用者要撥打的號碼限制訪問。您可以使用星號(*)作為萬用字元，根據數字的一部分允許或拒絕訪問。**提示**：如果要根據其他值（例如Cisco Aironet AP MAC地址）限制訪問，請使用DNIS選擇。有關詳細資訊，請參閱[關於網路訪問限制](#)部分。**注意**：AAA客戶端清單以及**Port**、**CLI**和**DNIS**框中的字元總數不得超過1024。儘管ACS在新增NAR時接受超過1024個字元，但您無法編輯NAR，並且ACS無法將其準確地應用到使用者。按一下「**Enter**」。指定AAA客戶端、埠、CLI和DNIS的資訊顯示在AAA客戶端清單上方的表中。
5. 如果已完成使用者帳戶選項的配置，請按一下**Submit**以記錄選項。

[設定使用者組的網路訪問限制](#)

可以使用組設定中的「網路訪問限制」表以三種不同方式應用NAR：

- 按名稱應用現有共用NAR。
- 定義基於IP的組訪問限制，以允許或拒絕在建立IP連線後訪問指定的AAA客戶端或AAA客戶端上的指定埠。
- 定義基於CLI/DNIS的組NAR，以允許或拒絕對所用的CLI編號或DNIS編號的任一或兩者的訪問。**注意**：您還可以使用基於CLI/DNIS的訪問限制區域指定其他值。有關詳細資訊，請參閱[關於網路訪問限制](#)部分。

通常，您可以從「共用元件」部分定義（共用）NAR，以便這些限制可以應用於多個組或使用者。有關詳細資訊，請參閱[新增共用NAR](#)部分。您必須在「介面配置」部分的「高級選項」頁上選中**組級共用網路訪問限制**覈取方塊，才能在ACS Web介面中顯示這些選項。

但是，您還可以使用ACS在**Group Setup**部分中為單個組定義和應用NAR。您必須檢查ACS Web介面中顯示的基於IP的單個組過濾器選項和基於CLI/DNIS的單個組過濾器選項在「介面配置」部分的

「高級選項」頁下的**組級網路訪問限制**設定。

注意：代理向ACS伺服器轉發身份驗證請求時，RADIUS請求的任何NAR將應用到轉發AAA伺服器的IP地址，而不是源AAA客戶端的IP地址。

完成以下步驟，為使用者組設定NAR:

1. 在導航欄中，按一下**Group Setup**。將開啟「組設定選擇」(Group Setup Select)視窗。
2. 從「組」清單中選擇一個組，然後按一下**編輯設定**。組的名稱顯示在「組設定」視窗的頂部。

