

Secure ACS : ユーザおよびユーザグループの AAAクライアントを使用するNAR

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[ネットワーク アクセス制限](#)

[ネットワーク アクセス制限の概要](#)

[共有 NAR の追加](#)

[共有 NAR の編集](#)

[共有 NAR の削除](#)

[ユーザに対するネットワーク アクセス制限の設定](#)

[ユーザグループに対するネットワーク アクセス制限の設定](#)

[関連情報](#)

概要

このドキュメントでは、ユーザとユーザグループの AAA クライアント (ルータ、PIX、ASA、ワイヤレス コントローラを含む) を使用した Cisco Secure Access Control Server (ACS) 4.x バージョンのネットワーク アクセス制限 (NAR) を設定する方法について説明します。

前提条件

要件

このドキュメントは、Cisco Secure ACS および AAA クライアントが正しく設定され、動作すると想定して作成されています。

使用するコンポーネント

このドキュメントの情報は、Cisco Secure ACS 3.0 以降に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

ネットワーク アクセス制限

この項では、NAR について説明した後で、共有 NAR の設定と管理について詳述します。

ここでは、次の内容について説明します。

- [ネットワーク アクセス制限の概要](#)
- [共有 NAR の追加](#)
- [共有 NAR の編集](#)
- [共有 NAR の削除](#)

ネットワーク アクセス制限の概要

NAR とは、ユーザがネットワークにアクセスする前に満たす必要がある追加条件の定義であり、ACS で作成します。ACS は、AAA クライアントから送信される属性の情報を利用して、これらの条件を適用します。NAR をセットアップする方法はいくつかありますが、すべて AAA クライアントから送信される属性情報の対応付けに基づいています。このため、NAR を効果的に利用するには、AAA クライアントが送信する属性の形式と内容を理解しておく必要があります。

NAR を設定すると、フィルタを許可条件または拒否条件のどちらとして動作させるかを選択できます。つまり、NAR では、AAA クライアントから送信された情報と NAR に格納された情報との比較に基づいて、ネットワーク アクセスを許可または拒否するかどうかを指定します。ただし、NAR が動作するために十分な情報が取得できない場合、デフォルトではアクセスが拒否されます。次の表に、これらの条件を示します。

| | IP ベース | 非 IP ベース | 情報不足 |
|----|-----------|-----------|--------|
| 許可 | 許可されるアクセス | アクセス拒否 | アクセス拒否 |
| 拒否 | アクセス拒否 | 許可されるアクセス | アクセス拒否 |

ACS は、次の 2 種類の NAR フィルタをサポートしています。

- **IP ベースのフィルタ**：IP ベースの NAR フィルタは、エンドユーザ クライアントおよび AAA クライアントの IP アドレスに基づいてアクセスを制限します。詳細については、『[IP ベースの NAR フィルタの概要](#)』の項を参照してください。
- **非 IP ベースのフィルタ**：非 IP ベースの NAR フィルタは、AAA クライアントから送信された値の単純な文字列比較に基づいてアクセスを制限します。値には、発信側回線 ID (CLI) 番号、着信番号識別サービス (DNIS) 番号、MAC アドレス、クライアントから送信されるその他の値などを使用できます。このタイプの NAR が動作するためには、NAR の説明にある値がクライアントから送信されている値と (使用されている形式も含めて) 正確に一致する必要があります。たとえば、電話番号 (217) 555-4534 は 217-555-4534 とは一致しません。詳細については、『[IP ベースの NAR フィルタの概要](#)』の項を参照してください。

NAR は特定のユーザまたはユーザ グループに適用するように定義できます。詳細については、『[ユーザに対するネットワーク アクセス制限の設定](#)』または『[ユーザグループに対するネットワーク アクセス制限の設定](#)』の項を参照してください。ただし、ACS の [Shared Profile

Components] セクションでは、どのユーザやユーザグループも直接引用せずに共有 NAR を作成および命名できます。共有 NAR には、ACS Web インターフェイスの別の部分で参照できる名前を付けます。次に、ユーザまたはユーザグループをセットアップするときは、共有制限は 1 つ適用することも、複数適用することも、まったく適用しないことも可能です。ユーザまたはユーザグループに複数の共有 NAR を適用するように指定する場合、次の 2 つのアクセス基準のどちらかを選択します。

- すべての選択されているフィルタが許可
- いずれかの選択されているフィルタが許可

異なるタイプの NAR に関連する優先順位を理解する必要があります。NAR フィルタリングの順序を次に示します。

1. ユーザレベルの共有 NAR
2. グループレベルの共有 NAR
3. ユーザレベルの非共有 NAR
4. グループレベルの非共有 NAR

また、すべてのレベルについて、アクセスの拒否は、アクセスを拒否しない別のレベルの設定に優先することも理解する必要があります。これは、ユーザレベルの設定がグループレベルの設定よりも優先されるというルールに対する ACS の 1 つの例外です。たとえば、あるユーザがユーザレベルの NAR 制限を適用されていない場合でも、共有 NAR または非共有 NAR のどちらかによって制限されたグループに属していれば、そのユーザはアクセスを拒否されます。

共有 NAR は、ACS 内部ユーザデータベースに保持されます。ACS のバックアップと復元機能を使用して、バックアップすることも、復元することもできます。さらに、共有 NAR を他の設定データとともにセカンダリ ACS に複製することもできます。

[IP ベースの NAR フィルタの概要](#)

IP ベースの NAR フィルタに対して、ACS は認証要求の AAA プロトコルに応じて次に示す属性を使用します。

- TACACS+ を使用している場合：TACACS+ 開始パケット部の [rem_addr] フィールドが使用されます。注：認証要求がプロキシによって ACS に転送されると、TACACS+ 要求のすべての NAR は、発信元 AAA クライアントの IP アドレスではなく、転送 AAA サーバの IP アドレスに適用されます。
- RADIUS IETF を使用している場合：calling-station-id (属性 31) を使用する必要があります。注：IP ベースの NAR フィルタは、ACS が Radius Calling-Station-Id(31) 属性を受信した場合にのみ機能します。[Calling-Station-Id (31)] には、有効な IP アドレスが含まれている必要があります。有効な IP アドレスが含まれていない場合は、DNIS 規則に当てはまりません。十分な IP アドレス情報を提示しない AAA クライアント (たとえば、ある種のファイアウォール) は、NAR の機能を完全にはサポートしていません。

プロトコルごとの IP ベースの制約のその他の属性には、次に示す NAR フィールドが含まれます。

- TACACS+ を使用している場合：ACS の NAR フィールドでは次の値を使用します。[AAA client] : [NAS-IP-address] が ACS と TACACS+ クライアント間のソケットの送信元アドレスから取得されます。[Port] : [port] フィールドは TACACS+ 開始パケット部から取得されます。

非 IP ベースの NAR フィルタの概要

非 IP ベースの NAR フィルタ (つまり、DNIS/CLI ベースの NAR フィルタ) は、許可または拒否される「呼び出し」または「アクセス ポイント」位置のリストです。これは、IP ベースの接続が確立されていない場合に AAA クライアントの制限に使用できます。一般に、IP ベース以外の NAR 機能は、CLI 番号と DNIS 番号を使用します。

ただし、CLI の代わりに IP アドレスを入力すると、非 IP ベースのフィルタを使用できます。AAA クライアントが CLI または DNIS をサポートする Cisco IOS® ソフトウェア リリースを使用していない場合でも、CLI 入力のもう 1 つの例外として、アクセスを許可または拒否する MAC アドレスの入力があります。たとえば Cisco Aironet AAA クライアントを使用している場合です。同様に、DNIS の代わりに Cisco Aironet AP MAC アドレスを入力できます。[CLI] ボックスで指定するものは、CLI、IP アドレス、または MAC アドレスのいずれであっても、その形式は、AAA クライアントから受信する番号またはアドレスの形式と一致している必要があります。この形式は、RADIUS アカウンティング ログから判別できます。

プロトコルごとの DNIS/CLI ベースの制限の属性には、次に示す NAR フィールドが含まれます。

- TACACS+ を使用している場合：次に示す NAR フィールドでは次の値を使用します。[AAA client] : [NAS-IP-address] が ACS と TACACS+ クライアント間のソケットの送信元アドレスから取得されます。[Port] : TACACS+ 開始パケット部の [port] フィールドが使用されます。CLI: TACACS+ 開始パケット本文の `rem-addr` フィールドが使用されます。DNIS: TACACS+ 開始パケット本文から取得した `rem-addr` フィールドが使用されます。rem-addr データがスラッシュ (/) で始まる場合、[DNIS] フィールドにはスラッシュ (/) なしの rem-addr データが含まれます。注：認証要求がプロキシによって ACS に転送されると、TACACS+ 要求のすべての NAR は、発信元 AAA クライアントの IP アドレスではなく、転送 AAA サーバの IP アドレスに適用されます。
- RADIUS を使用している場合：次に示す NAR フィールドでは次の値を使用します。[AAA client] : NAS-IP-address (属性 4) または、NAS-IP-address が存在しない場合は NAS-identifier (RADIUS 属性 32) が使用されます。[Port] : NAS-port (属性 5) または、NAS-port が存在しない場合は、NAS-port-ID (属性 87) が使用されます。CLI : calling-station-ID (属性 31) が使用されます。DNIS : called-station-ID (属性 30) が使用されます。

NAR の指定時、アスタリスク (*) を任意の値のワイルドカードとして、または範囲設定のための任意の値の一部として使用できます。NAR でアクセスを制限するためには、NAR の説明におけるすべての値または条件が合致する必要があります。つまり、値にはブール値 AND が含まれます。

共有 NAR の追加

多数のアクセス制限を含む共有 NAR を作成できます。ACS Web インターフェイスは、共有 NAR のアクセス数への制限も、各アクセスの長さへの制限も適用しません。ただし、次の制限に従う必要があります。

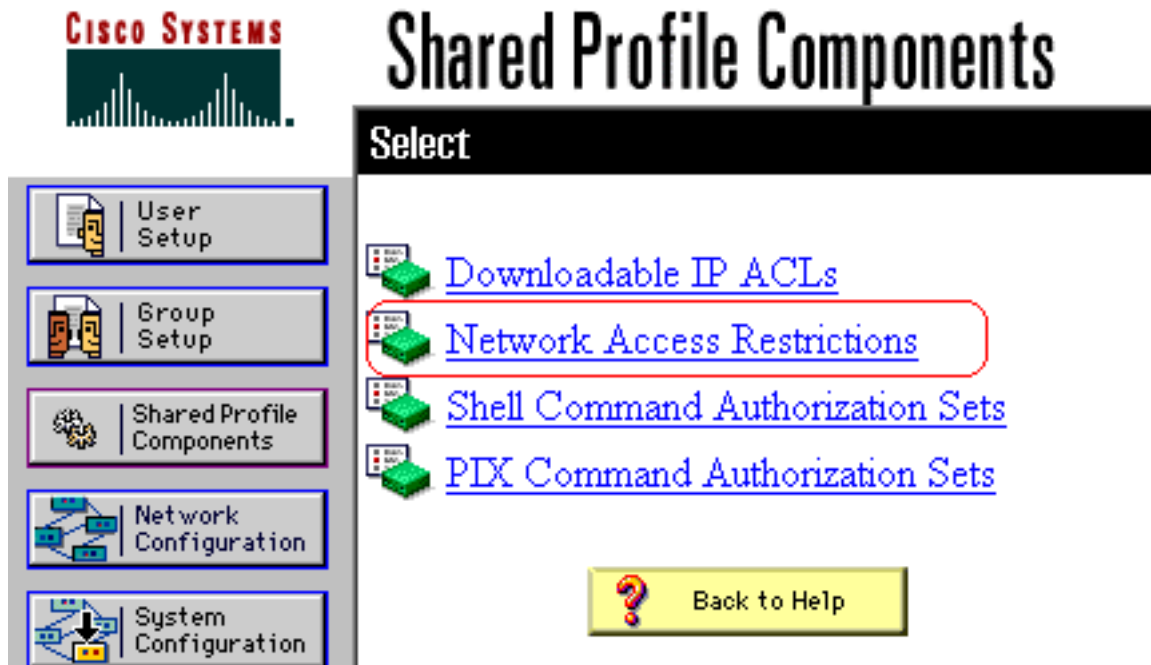
- 行項目それぞれのフィールド長の合計が 1024 文字を超えることはできない。
- 共有 NAR では、文字サイズの合計が 16 KB を超えることはできない。サポートされる行項目の数は、行項目それぞれの長さによって異なります。たとえば、CLI/DNIS ベースの NAR を作成する場合、AAA クライアント名が 10 文字、ポート番号が 5 文字、CLI エントリが 15 文字、DNIS エントリが 20 文字のときは、16 KB 制限に達しない限り、450 行項目を追加できます。

注：NAR を定義する前に、その NAR で使用する要素が設定されていることを確認してください。

このため、すべての NAF と NDG を指定し、関連するすべての AAA クライアントを定義した後に、それらを NAR 定義に加える必要があります。詳細については、「[ネットワークアクセス制限の概要](#)」の項を参照してください。

共有 NAR を追加するには、次の手順を実行します。

1. ナビゲーション バーの [Shared Profile Components] をクリックします。[Shared Profile Components] ウィンドウが表示されます。




2. [Network Access Restrictions] をクリックします。



Shared Profile Components

Select

Network Access Restrictions 

| Name | Description |
|--------------|-------------|
| None Defined | |

Add Cancel

3. [Add] をクリックします。[Network Access Restriction] ウィンドウが表示されます。

Shared Profile Components

Network Access Restriction

Name:

Description:

Define IP-based access restrictions

Table Defines:

| AAA Client | Port | Src IP Address |
|----------------------|------|----------------|
| <input type="text"/> | | |

AAA Client:

Port:

Src IP Address:

Define CLI/DNIS-based access restrictions

Table Defines:

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

- [Name] ボックスに、新しい共有 NAR の名前を入力します。注：名前には31文字まで使用できます。先頭と末尾にスペースを置くことはできません。名前に次の文字を含めることはできません。左角カッコ ([)、右角カッコ (])、カンマ (,)、スラッシュ (/)。
- [Description] ボックスに、新しい共有 NAR の説明を入力します。説明には、最大 30,000 文字を使用できます。
- IP アドレッシングに基づいてアクセスを許可または拒否する場合は、次の手順を実行します。
[Define IP-based access descriptions] **チェックボックスをオンにします**。許可または拒否するアドレスをリストするかどうかを指定するために、[Table Defines] リストで該当する値を選択します。次のボックスで、それぞれ該当する情報を選択するか、または入力します。
[AAA Client] : [All AAA clients] を選択するか、アクセスを許可または拒否する NDG の名前、NAF の名前、または個々の AAA クライアントの名前を入力します。
[Port] : アクセスを許可または拒否するポートの番号を入力します。アスタリスク (*) をワイルドカードとし

て使用すると、選択された AAA クライアント上のすべてのポートに対するアクセスを許可または拒否できます。[Src IP Address] : アクセス制限を実行する場合に、フィルタリングを行う IP アドレスを入力します。アスタリスク (*) をワイルドカードとして使用すると、すべての IP アドレスを指定できます。注 : [AAA Client list] および [Port] ボックスと [Src IP Address] ボックスの文字数の合計は、1024 を超えることはできません。NAR を追加する際に ACS には 1024 を超える文字を入力できませんが、NAR の編集ができなくなるため、ACS は NAR をユーザに正確に適用できなくなります。[Enter] をクリックします。AAA クライアント、ポート、およびアドレス情報が、テーブルの行項目として表示されます。追加の IP ベースの行項目を入力するには、手順 c と d を繰り返します。

7. 発信場所や、IP アドレス以外の値に基づいてアクセスを許可または拒否する場合は、次の手順を実行します。[Define CLI/DNIS based access restrictions] チェック ボックスをオンにします。許可または拒否する場所をリストするかどうかを指定するために、[Table Defines] リストで該当する値を選択します。この NAR を適用するクライアントを指定するために、[AAA Client] リストから、次のいずれか 1 つの値を選択します。NDG の名前特定の AAA クライアントの名前すべての AAA クライアントヒント : 既に設定されている NDG だけが表示されます。この NAR がフィルタリングする情報を指定するには、必要に応じて次のボックスに値を入力します。ヒント : アスタリスク(*)をワイルドカードとして入力すると、すべて値として指定できます。[Port] : フィルタリングするポート番号を入力します。CLI : フィルタリングする CLI 番号を入力します。また、このボックスを使用して、CLI 以外の値、たとえば、IP アドレスや MAC アドレスに基づいてアクセスを制限できます。詳細については、[「ネットワークアクセス制限の概要」の項を参照してください。](#)DNIS : フィルタリングするダイヤルインの番号を入力します。注 : [AAA Client] リストと [Port]、[CLI]、[DNIS] ボックスの文字数の合計は、1024 を超えることはできません。NAR を追加する際に ACS には 1024 を超える文字を入力できませんが、NAR の編集ができなくなるため、ACS は NAR をユーザに正確に適用できなくなります。[Enter] をクリックします。NAR 行項目を指定する情報が、テーブルに表示されます。追加の非 IP ベースの NAR 行項目を入力するには、手順 c ~ d を繰り返します。[Submit] をクリックし、共有 NAR 定義を保存します。ACS は、共有 NAR を保存して、[Network Access Restrictions] テーブルにリストします。

共有 NAR の編集

共有 NAR を編集するには、次の手順を実行します。

1. ナビゲーション バーの [Shared Profile Components] をクリックします。[Shared Profile Components] ウィンドウが表示されます。
2. [Network Access Restrictions] をクリックします。[Network Access Restrictions] テーブルが表示されます。
3. [Name] カラムで、編集する共有 NAR をクリックします。[Network Access Restriction] ウィンドウが表示され、選択した NAR に関する情報が表示されます。
4. 必要に応じて、NAR の名前または説明を編集します。説明には、最大 30,000 文字を使用できます。
5. IP ベースのアクセス制限テーブルの行項目を編集するには、次の手順を実行します。編集する行項目をダブルクリックします。その行項目の情報がテーブルから削除され、テーブル下部のボックスに表示されます。必要に応じて情報を編集します。注 : [AAA Client list] ボックス、[Port] ボックス、および [Src IP Address] ボックスの文字数の合計は、1024 を超えることはできません。NAR を追加する際に ACS には 1024 を超える文字を入力できませんが、このような NAR は編集できなくなるため、ACS は NAR をユーザに正確に適用できなくなります。[Enter] をクリックします。編集した行項目の情報が、IP ベースのアクセス制限テーブ

ルに書き込まれます。

6. IP ベースのアクセス制限テーブルの行項目を削除するには、次の手順を実行します。品目を選択してテーブルの下の [Remove] をクリックします。IP ベースのアクセス制限テーブルから、行項目が削除されます。
7. CLI/DNIS アクセス制限テーブルの行項目を編集するには、次の手順を実行します。編集する行項目をダブルクリックします。その行項目の情報がテーブルから削除され、テーブル下部のボックスに表示されます。必要に応じて情報を編集します。注：[AAA Client]リストと [Port]、[CLI]、[DNIS]ボックスの文字数の合計は、1024を超えることはできません。NAR を追加する際に ACS には 1024 を超える文字を入力できますが、このような NAR は編集できなくなるため、ACS は NAR をユーザに正確に適用できなくなります。[Enter] をクリックします。編集した行項目の情報が、CLI/DNIS アクセス制限テーブルに書き込まれます。
8. CLI/DNIS アクセス制限テーブルの行項目を削除するには、次の手順を実行します。品目を選択してテーブルの下の [Remove] をクリックします。CLI/DNIS アクセス制限テーブルから、行項目が削除されます。
9. [Submit] をクリックし、変更を保存します。ACS によって新しい情報のフィルタが再入力され、すぐに有効になります。

共有 NAR の削除

注：共有NARを削除する前に、共有NARと任意のユーザまたはグループとの関連付けを削除してください。

共有 NAR を削除するには、次の手順を実行します。

1. ナビゲーション バーの [Shared Profile Components] をクリックします。[Shared Profile Components] ウィンドウが表示されます。
2. [Network Access Restrictions] をクリックします。
3. 削除する共有 NAR の名前をクリックします。[Network Access Restriction] ウィンドウが表示され、選択した NAR に関する情報が表示されます。
4. ウィンドウの下部で、[Delete] をクリックします。共有 NAR の削除について警告するダイアログボックスが表示されます。
5. 共有 NAR を削除することを確認するため、[OK] をクリックします。選択した共有 NAR が削除されます。

ユーザに対するネットワーク アクセス制限の設定

[User Setup] の [Advanced Settings] 領域にある [Network Access Restrictions] テーブルでは、次の 3 つの方法で NAR を設定します。

- 名前を指定して既存の共有 NAR を適用する。
- IP に基づいたアクセス制限を定義し、IP 接続確立時に、指定された AAA クライアントまたは AAA クライアントの指定ポートに対するユーザ アクセスを許可または拒否する。
- CLI/DNIS に基づいたアクセス制限を定義し、使用される CLI/DNIS に基づいたユーザ アクセスを許可または拒否する。注：CLI/DNIS ベースのアクセス制限領域を使用して、他の値を指定することもできます。詳細については、[「ネットワーク アクセス制限」の項を参照してください。](#)

通常は、[Shared Components] セクションから (共有) NAR を定義することにより、これらの制限を複数のグループまたはユーザに適用できます。詳細については、[「共有 NAR の追加」の項](#)

[を参照してください。](#) [Interface Configuration] セクションの [Advanced Options] ページにある [User-Level Network Access Restrictions] チェック ボックスをオンにし、これらのオプション セットが Web インターフェイスに表示されるようにしておく必要があります。

ただし、ACS では、[User Setup] セクションから単一のユーザに対して NAR を定義および適用することもできます。単一ユーザの IP に基づいたフィルタ オプション、および単一ユーザの CLI/DNIS に基づいたフィルタ オプションを Web インターフェイスに表示するには、[Interface Configuration] セクションの [Advanced Options] ページで [User-Level Network Access Restrictions] 設定をイネーブルにしておく必要があります。

注： 認証要求がプロキシによってACSに転送されると、Terminal Access Controller Access Control System(TACACS+)要求のすべてのNARが、発信元AAAクライアントのIPアドレスではなく、転送AAAサーバのIPアドレスに適用されます。

アクセス制限をユーザごとに作成する場合、ACS は、アクセス数への制限も、各アクセスの長さへの制限も適用しません。ただし、次の厳しい制限があります。

- 行項目それぞれのフィールド長の合計が 1024 文字を超えることはできない。
- 共有 NAR では、文字サイズの合計が 16 KB を超えることはできない。サポートされる行項目の数は、行項目それぞれの長さによって異なります。たとえば、CLI/DNIS ベースの NAR を作成する場合、AAA クライアント名が 10 文字、ポート番号が 5 文字、CLI エントリが 15 文字、DNIS エントリが 20 文字のときは、16 KB 制限に達しない限り、450 行項目を追加できます。

ユーザに対して NAR を設定するには、次の手順を実行します。

1. 「[基本ユーザアカウントの追加](#)」の手順 1 ~ 3 を実行します。[User Setup Edit] ウィンドウが開きます。追加または編集するユーザ名がウィンドウ上部に表示されます。

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

- 事前に設定された共有 NAR をこのユーザに適用するには、次の手順を実行します。注：共有 NAR を適用するには、[Shared Profile Components] セクションの [Network Access Restrictions] で設定する必要があります。詳細については、「[共有 NAR の追加](#)」の項を参照してください。[Only Allow network access when] チェックボックスをオンにします。ユーザのアクセスを許可するために、1 つの共有 NAR またはすべての共有 NAR のどちらを適用するかを指定するには、必要に応じて次のいずれかを選択します。All selected NARS result

in permitAny one selected NAR results in permit[NARs]リストで共有NAR名を選択し、[→] (右矢印ボタン) をクリックして、[Selected NARs]リストに名前を移動します。ヒント：適用するように選択した共有NARのサーバ詳細を表示するには、必要に応じて[View IP NAR]または[View CLID/DNIS NAR]をクリックします。

- IP アドレス、または IP アドレスとポートに基づいて、この特定のユーザに対してユーザ アクセスを許可または拒否する NAR を定義および適用するには、次の手順を実行します。注：ほとんどのNARは、[Shared Components]セクションから定義して、複数のグループまたはユーザに適用できるようにします。詳細については、[「共有 NAR の追加」の項を参照してください](#)。[Network Access Restrictions] テーブルの [Per User Defined Network Access Restrictions] で、[Define IP-based access restrictions] チェック ボックスをオンにします。後続してリストに追加される IP アドレスを許可または拒否するかを指定するには、[Table Defines] リストから次のいずれかを選択します。[Permitted Calling/Point of Access Locations][Denied Calling/Point of Access Locations]次のボックスで情報を選択するか、または入力します。[AAA Client] : [All AAA Clients] を選択するか、アクセスを許可または拒否するネットワーク デバイス グループ (NDG) の名前、または個々の AAA クライアントの名前を入力します。[Port] : アクセスを許可または拒否するポートの番号を入力します。アスタリスク (*) をワイルドカードとして使用すると、選択された AAA クライアント上のすべてのポートに対するアクセスを許可または拒否できます。[Address] : アクセス制限の実行時に使用する IP アドレス (複数可) を入力します。アスタリスク (*) をワイルドカードとして使用できます。注：[AAA Client list]の文字数と[Port]ボックスと[Src IP Address]ボックスの文字数の合計は、1024を超えることはできません。NAR を追加する際に ACS には 1024 を超える文字を入力できますが、NAR の編集ができなくなるため、ACS は NAR をユーザに正確に適用できなくなります。[Enter] をクリックします。指定した AAA クライアント、ポート、およびアドレス情報が、[AAA Client] リスト上部のテーブルに表示されます。
- 発信場所、または設定された IP アドレス以外の値に基づいて、このユーザのアクセスを許可または拒否するには、次の手順を実行します。[Define CLI/DNIS based access restrictions] チェック ボックスをオンにします。後続してリストに追加される値を許可または拒否するかを指定するには、[Table Defines] リストから次のいずれかを選択します。[Permitted Calling/Point of Access Locations][Denied Calling/Point of Access Locations]次に示すボックスを入力します。注：各ボックスに入力する必要があります。値の全体または一部にアスタリスク (*) をワイルドカードとして使用できます。使用する形式は、AAA クライアントから受信する文字列の形式と一致している必要があります。この形式は、RADIUS アカウンティング ログから判別できます。[AAA Client] : [All AAA Clients] を選択するか、アクセスを許可または拒否する NDG の名前、または個々の AAA クライアントの名前を入力します。[Port] : アクセスを許可または拒否するポートの番号を入力します。アスタリスク (*) をワイルドカードとして使用すると、すべてのポートに対するアクセスを許可または拒否できます。CLI : アクセスを許可または拒否するCLI番号を入力します。アスタリスク (*) をワイルドカードとして使用すると、番号の一部に基づいてアクセスを許可または拒否できます。ヒント：Cisco AironetクライアントのMACアドレスなどの他の値に基づいてアクセスを制限する場合は、CLIエントリを使用します。詳細については、[「ネットワーク アクセス制限の概要」の項を参照してください](#)。DNIS : アクセスを許可または拒否するDNIS番号を入力します。このエントリは、ユーザがダイヤルする番号に基づいてアクセスを制限するために使用します。アスタリスク (*) をワイルドカードとして使用すると、番号の一部に基づいてアクセスを許可または拒否できます。ヒント：Cisco Aironet APのMACアドレスなどの他の値に基づいてアクセスを制限する場合は、DNISを選択します。詳細については、[「ネットワーク アクセス制限の概要」の項を参照してください](#)。注：[AAA Client]リストと[Port]、[CLI]、[DNIS]ボックスの文字数の合計は1024を超えることはできません。NAR を追加する際に ACS には 1024 を超える文字を入力できますが、NAR の編集が

できなくなるため、ACS は NAR をユーザに正確に適用できなくなります。[Enter] をクリックします。AAA クライアント、ポート、CLI、および DNIS を指定する情報が、[AAA Client] リスト上部のテーブルに表示されます。

5. ユーザ アカウント オプションの設定が完了したら、[Submit] をクリックしてオプションを記録します。

ユーザ グループに対するネットワーク アクセス制限の設定

[Group Setup] の [Network Access Restrictions] テーブルで、次の 3 つの方法を使用して、NAR を適用できます。

- 名前を指定して既存の共有 NAR を適用する。
- IP ベースのグループ アクセス制限を定義して、IP 接続が確立された時点で、指定された AAA クライアントまたは AAA クライアントの指定されたポートに対するアクセスを許可または拒否する。
- CLI/DNIS ベースのグループ NAR を定義して、使用されている CLI の番号または DNIS の番号、あるいはその両方に対するアクセスを許可または拒否する。注：CLI/DNIS ベースのアクセス制限領域を使用して、他の値を指定することもできます。詳細については、「[ネットワーク アクセス制限の概要](#)」の項を参照してください。

通常は、[Shared Components] セクションから (共有) NAR を定義することにより、これらの制限を複数のグループまたはユーザに適用します。詳細については、「[共有 NAR の追加](#)」の項を参照してください。これらのオプションが ACS Web インターフェイスに表示されるようにするには、[Interface Configuration] セクションの [Advanced Options] ページで、[Group-Level Shared Network Access Restriction] チェック ボックスをオンにする必要があります。

ただし、ACS では、[Group Setup] セクションで 1 つのグループに対して NAR を定義し、適用することもできます。単一グループの IP に基づいたフィルタ オプション、および単一グループの CLI/DNIS に基づいたフィルタ オプションを ACS Web インターフェイスに表示するには、[Interface Configuration] セクションの [Advanced Options] ページで [Group-Level Network Access Restrictions] 設定をイネーブルにしておく必要があります。

注：認証要求がプロキシによって ACS サーバに転送されると、RADIUS 要求に対する NAR は、発信元の AAA クライアントの IP アドレスではなく、転送先の AAA サーバの IP アドレスに適用されます。

ユーザ グループに対して NAR を設定するには、次の手順を実行します。

1. ナビゲーション バーの [Group Setup] をクリックします。[Group Setup Select] ウィンドウが表示されます。
2. [Group] リストでグループを選択し、[Edit Settings] をクリックします。[Group Settings] ウィンドウの一番上にそのグループの名前が表示されます。

