



認証、許可、アカウントिंगの設定

この章の内容は、次のとおりです。

- [AAA の概要, 1 ページ](#)
- [リモート AAA の前提条件, 6 ページ](#)
- [AAA の注意事項と制約事項, 6 ページ](#)
- [AAA の設定, 6 ページ](#)
- [ローカル AAA アカウントング ログのモニタリングとクリア, 16 ページ](#)
- [AAA 設定の確認, 16 ページ](#)
- [AAA の設定例, 17 ページ](#)
- [デフォルトの AAA 設定, 17 ページ](#)

AAA の概要

AAA セキュリティ サービス

認証、許可、アカウントング（AAA）機能では、Cisco Nexus デバイスを管理するユーザの ID 確認、アクセス権付与、およびアクション追跡を実行できます。Cisco Nexus デバイスは、Remote Access Dial-In User Service（RADIUS）プロトコルまたは Terminal Access Controller Access Control device Plus（TACACS+）プロトコルをサポートします。

ユーザが入力したユーザ ID とパスワードに基づいて、スイッチは、ローカル データベースを使用してローカル認証/ローカル許可を実行するか、1つまたは複数の AAA サーバを使用してリモート認証/リモート許可を実行します。スイッチと AAA サーバ間の通信は、事前共有秘密キーによって保護されます。すべての AAA サーバ用または特定の AAA サーバ専用 to 共通秘密キーを設定できます。

AAA セキュリティは、次のサービスを実行します。

- 認証：ユーザを識別します。選択したセキュリティプロトコルに応じて、ログインとパスワードのダイアログ、チャレンジ/レスポンス、メッセージングサポート、暗号化などが行われます。
- 許可：アクセスコントロールを実行します。

Cisco Nexus デバイスにアクセスする許可は、AAA サーバからダウンロードされる属性によって提供されます。RADIUS や TACACS+ などのリモートセキュリティサーバは、適切なユーザで該当する権利を定義した属性値 (AV) のペアをアソシエートすることによって、ユーザに特定の権限を付与します。

- アカウンティング：課金、監査、レポートのための情報収集、ローカルでの情報のログイン、および AAA サーバへの情報の送信の方式を提供します。



(注) Cisco NX-OS ソフトウェアは、認証、許可、アカウントングをそれぞれ個別にサポートします。たとえば、アカウントングは設定せずに、認証と許可を設定したりできます。

AAA を使用する利点

AAA は、次のような利点を提供します。

- アクセス設定の柔軟性と制御性の向上
- 拡張性
- 標準化された認証方式 (RADIUS、TACACS+ など)
- 複数のバックアップ デバイス

リモート AAA サービス

RADIUS プロトコルおよび TACACS+ プロトコルを介して提供されるリモート AAA サービスには、ローカル AAA サービスと比べて次のような利点があります。

- ファブリック内の各スイッチに関するユーザパスワードリストを簡単に管理できます。
- AAA サーバはすでに企業内に幅広く導入されており、簡単に AAA サービスに使用できます。
- ファブリック内のすべてのスイッチのアカウントングログを集中管理できます。
- スイッチ上のローカルデータベースを使用する方法に比べて、ファブリック内の各スイッチのユーザ属性は管理が簡単です。

AAA サーバグループ

認証、許可、アカウントングのためのリモート AAA サーバは、サーバグループを使用して指定できます。サーバグループとは、同じ AAA プロトコルを実装した一連のリモート AAA サーバです。リモート AAA サーバが応答しなかった場合、サーバグループは、フェールオーバーサーバを提供します。グループ内の最初のリモートサーバが応答しなかった場合、いずれかのサーバが応答を送信するまで、グループ内の次のリモートサーバで試行が行われます。サーバグループ内のすべての AAA サーバが応答しなかった場合、そのサーバグループ オプションには障害が発生しているものと見なされます。必要に応じて、複数のサーバグループを指定できます。スイッチが最初のグループ内のサーバからエラーを受信すると、次のサーバグループのサーバが試行されます。

AAA サービス設定オプション

Cisco Nexus デバイスでは、次のサービスに個別の AAA 設定を使用できます。

- User Telnet または Secure Shell (SSH) ログイン認証
- コンソール ログイン認証
- ユーザ管理セッション アカウントング

次の表に、AAA サービス設定オプションの CLI コマンドを示します。

表 1: AAA サービス コンフィギュレーション コマンド

AAA サービス コンフィギュレーション オプション	関連コマンド
Telnet または SSH ログイン	aaa authentication login default
コンソール ログイン	aaa authentication login console
ユーザ セッション アカウントング	aaa accounting default

AAA サービスには、次の認証方式を指定できます。

- RADIUS サーバグループ : RADIUS サーバのグローバル プールを認証に使用します。
- 特定のサーバグループ : 指定した RADIUS または TACACS+ サーバグループを認証に使用します。
- ローカル : ユーザ名またはパスワードのローカル データベースを認証に使用します。
- なし : ユーザ名だけを使用します。



(注) 方式がすべて RADIUS サーバになっており、特定のサーバグループが指定されていない場合、Cisco Nexus デバイスは、設定されている RADIUS サーバのグローバルプールから、設定された順序で RADIUS サーバを選択します。このグローバルプールからのサーバは、Cisco Nexus デバイス上の RADIUS サーバグループ内で選択的に設定できるサーバです。

次の表に、AAA サービスに対して設定できる AAA 認証方式を示します。

表 2: AAA サービスの AAA 認証方式

AAA サービス	AAA の方式
コンソール ログイン認証	サーバグループ、ローカル、なし
ユーザ ログイン認証	サーバグループ、ローカル、なし
ユーザ管理セッション アカウンティング	サーバグループ、ローカル



(注) コンソール ログイン認証、ユーザ ログイン認証、およびユーザ管理セッション アカウンティングでは、Cisco Nexus デバイスは、各オプションを指定された順序で試行します。その他の設定済みオプションが失敗した場合、ローカル オプションがデフォルト方式です。

ユーザ ログインの認証および許可プロセス

ユーザ ログインの認証および許可プロセスは、次のように実行されます。

- 目的の Cisco Nexus デバイスにログインする際、Telnet、SSH、Fabric Manager または Device Manager、コンソール ログインのいずれかのオプションを使用できます。
- サーバグループ認証方式を使用して AAA サーバグループが設定してある場合は、Cisco Nexus デバイスが、グループ内の最初の AAA サーバに認証要求を送信し、次のように処理されます。

その AAA サーバが応答しなかった場合、リモートのいずれかの AAA サーバが認証要求に回答するまで、試行が継続されます。

サーバグループのすべての AAA サーバが応答しなかった場合、その次のサーバグループのサーバが試行されます。

設定されているすべての認証方式が失敗した場合、ローカルデータベースを使用して認証が実行されます。
- Cisco Nexus デバイスがリモート AAA サーバで正常に認証できた場合は、次の条件が適用されます。

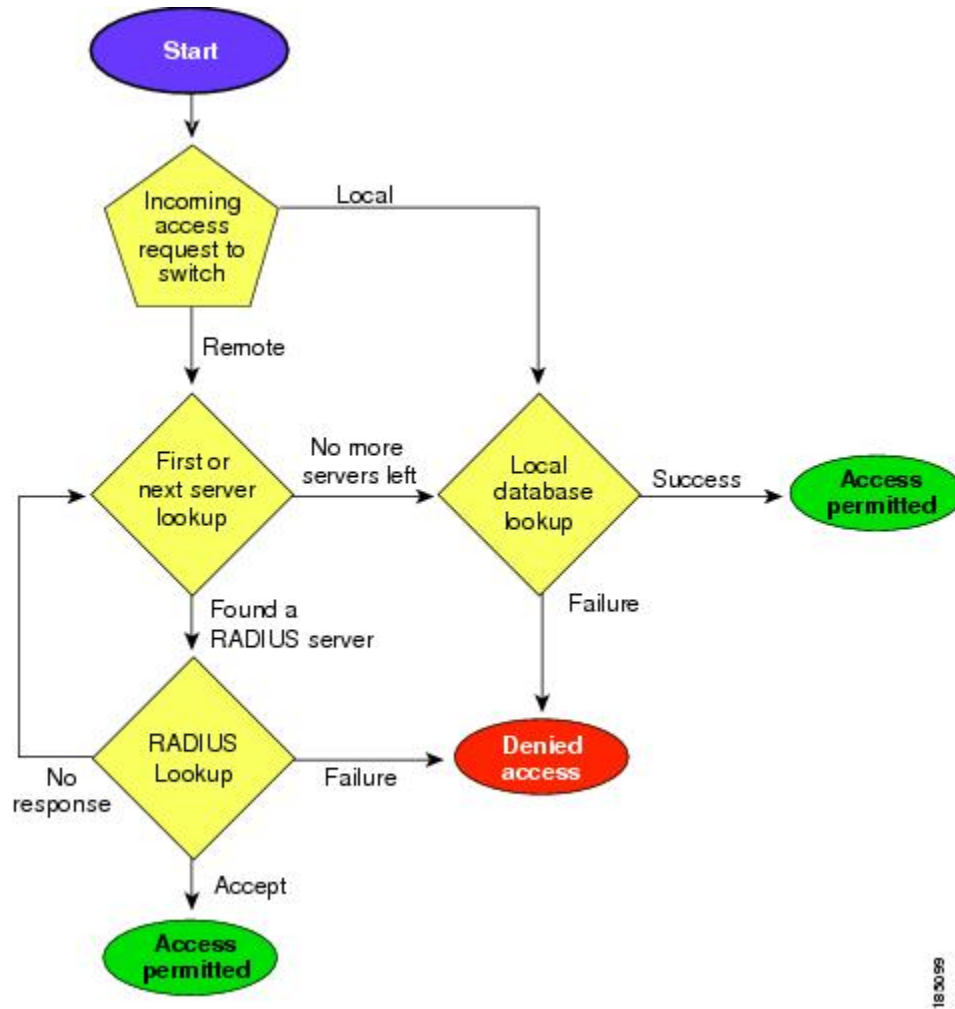
AAA サーバプロトコルが RADIUS の場合、cisco-av-pair 属性で指定されているユーザ ロールが認証応答とともにダウンロードされます。

AAA サーバプロトコルが TACACS+ の場合、シェルのカスタム属性として指定されているユーザ ロールを取得するために、もう 1 つの要求が同じサーバに送信されます。

- ユーザ名とパスワードがローカルで正常に認証された場合は、Cisco Nexus デバイスにログインでき、ローカル データベース内で設定されているロールが割り当てられます。

次の図に、認証および許可プロセスのフローチャートを示します。

図 1: ユーザ ログインの認証および許可のフロー



(注) この図は、ユーザ名とパスワードによる SSH 認証にのみ該当します。公開キー SSH 認証には適用されません。ユーザ名とパスワードによる SSH 認証は、常に AAA を介して行われます。

この図に示されている「残りのサーバなし」とは、現在のサーバグループ内のいずれのサーバからも応答がないということです。

リモート AAA の前提条件

リモート AAA サーバには、次の前提条件があります。

- 少なくとも 1 台の RADIUS サーバまたは TACACS+ サーバが、IP で到達可能であること。
- Cisco Nexus デバイスが AAA サーバのクライアントとして設定されている。
- 事前に共有された秘密キーが Cisco Nexus デバイス上およびリモート AAA サーバ上で設定されている。
- リモート サーバが Cisco Nexus デバイスからの AAA 要求に応答する。

AAA の注意事項と制約事項

そのユーザ名が TACACS+ または RADIUS で作成されたのか、ローカルで作成されたのかに関係なく、Cisco Nexus デバイスでは、すべて数値のユーザ名はサポートされません。AAA サーバに数字だけのユーザ名が存在し、ログイン時にその名前を入力した場合でも、ユーザは Cisco Nexus デバイスにログインを許可されます。



注意

すべて数字のユーザ名でユーザ アカウントを作成しないでください。

AAA の設定

コンソール ログイン認証方式の設定

認証方式には、次のものがあります。

- RADIUS サーバのグローバル プール
- RADIUS サーバまたは TACACS+ サーバの名前付きサブセット
- Cisco Nexus デバイス上のローカル データベース
- ユーザ名のみ (**none**)

デフォルトの方式は、ローカルです。



(注) 事前に設定されている一連の RADIUS サーバに関しては、**aaa authentication** コマンドの **group radius** 形式および **groupserver-name** 形式を使用します。ホストサーバを設定するには、**radius server-host** コマンドを使用します。サーバの名前付きグループを作成するには、**aaa group server radius** コマンドを使用します。

必要に応じて、コンソール ログイン認証方式を設定する前に RADIUS または TACACS+ サーバグループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# aaa authentication login console {groupgroup-list [none] local none}	<p>コンソールのログイン認証方式を設定します。</p> <p><i>group-list</i> 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。</p> <ul style="list-style-type: none"> • radius を指定すると、RADIUS サーバのグローバルプールが認証に使用されます。 • <i>named-group</i> を指定すると、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットが認証に使用されます。 <p>local 方式では、ローカルデータベースが認証に使用されます。none 方式では、ユーザ名のみが使用されます。</p> <p>デフォルトのコンソール ログイン方式は local です。この方式は、方式が一切設定されていない場合、および設定済みのどの方式でも応答が得られなかった場合に使用されます。</p>
ステップ 3	switch(config)# exit	グローバル コンフィギュレーション モードを終了します。
ステップ 4	switch# show aaa authentication	(任意) コンソール ログイン認証方式の設定を表示します。
ステップ 5	switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、コンソール ログインの認証方式を設定する例を示します。

```
switch# configure terminal
switch(config)# aaa authentication login console group radius
switch(config)# exit
switch# show aaa authentication
switch# copy running-config startup-config
```

デフォルトのログイン認証方式の設定

デフォルトの方式は、ローカルです。

必要に応じて、デフォルトのログイン認証方式を設定する前に RADIUS または TACACS+ サーバグループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# aaa authentication login default {groupgroup-list [none] local none}	<p>デフォルト認証方式を設定します。</p> <p><i>group-list</i> 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。</p> <ul style="list-style-type: none"> • radius を指定すると、RADIUS サーバのグローバル プールが認証に使用されます。 • named-group を指定すると、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットが認証に使用されます。 <p>local 方式では、ローカル データベースが認証に使用されます。none 方式では、ユーザ名のみが使用されます。</p> <p>デフォルトのログイン方式は local です。これは、方式が一切設定されていない場合、および設定済みのどの方式でも応答が得られなかった場合に使用されます。</p>
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show aaa authentication	(任意) デフォルトのログイン認証方式の設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ログイン認証失敗メッセージのイネーブル化

ユーザがログインして、リモート AAA サーバが応答しなかった場合は、ローカルユーザ データベースによってログインが処理されます。ログイン失敗メッセージの表示をイネーブルにしている場合は、次のようなメッセージが表示されます。

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# aaa authentication login error-enable	ログイン認証失敗メッセージをイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show aaa authentication	(任意) ログイン失敗メッセージの設定を表示します。
ステップ 5	switch# copy running-config startup-config	(任意) 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

AAA コマンド許可の設定

TACACS+ サーバの許可方式が設定されている場合は、ユーザが TACACS+ サーバで実行するすべてのコマンド（すべての EXEC モード コマンドおよびすべてのコンフィギュレーションモード コマンドを含む）を許可できます。

許可方式には、次のものがあります。

- Group : TACACS+ サーバグループ
- Local : ローカル ロールベース許可
- None : 許可は実行されません

デフォルトの方式は、Local です。



(注) コンソールセッションでの認証は、Cisco Nexus 5000 プラットフォームではサポートされません。Cisco Nexus 5500 プラットフォーム リリース 6.x 以降ではサポートされています。

はじめる前に

AAA コマンドの許可を設定する前に、TACACS+ をイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	グローバル コンフィギュレーション モードを開始します。
ステップ 2	aaa authorization {commands config-commands} {default} {[groupgroup-name] [[local]]} [groupgroup-name] [[none]]} 例： switch(config)# aaa authorization config-commands default group tac1 例： switch# aaa authorization commands default group tac1	許可パラメータを設定します。 EXEC モード コマンドを許可するには、 commands キーワードを使用します。 コンフィギュレーション モード コマンドの許可には、 config-commands キーワードを使用します。 許可方式を指定するには、 group 、 local 、または none キーワードを使用します。

次に、TACACS+ サーバグループ *tac1* で EXEC モード コマンドを許可する例を示します。

```
switch# aaa authorization commands default group tac1
```

次に、TACACS+ サーバグループ *tac1* でコンフィギュレーション モード コマンドを許可する例を示します。

```
switch(config)# aaa authorization config-commands default group tac1
```

次に、TACACS+ サーバグループ *tac1* でコンフィギュレーション モード コマンドを許可する例を示します。

- サーバが到達可能である場合、コマンドはサーバ応答に基づいて許可され、または許可されません。
- サーバに到達する際にエラーが生じた場合、コマンドはユーザのローカルロールに基づいて許可されます。

```
switch(config)# aaa authorization config-commands default group tac1 local
```

次に、TACACS+ サーバグループ *tac1* でコンフィギュレーション モード コマンドを許可する例を示します。

- サーバが到達可能である場合、コマンドはサーバ応答に基づいて許可され、または許可されません。
- サーバに到達する際にエラーが生じた場合は、ローカルロールにかかわらずコマンドを許可します。

```
switch# aaa authorization commands default group tac1 none
```

次に、ローカル ロールにかかわらず EXEC モード コマンドを許可する例を示します。

```
switch# aaa authorization commands default none
```

次に、ローカル ロールを使用して EXEC モード コマンドを許可する例を示します。

```
switch# aaa authorization commands default local
```

MSCHAP 認証のイネーブル化

マイクロソフトチャレンジハンドシェーク認証プロトコル (MSCHAP) は、マイクロソフト版の CHAP です。リモート認証サーバ (RADIUS または TACACS+) を通じて、Cisco Nexus デバイスへのユーザ ログインに MSCHAP を使用できます。

デフォルトでは、Cisco Nexus デバイスはスイッチとリモートサーバの間でパスワード認証プロトコル (PAP) 認証を使用します。MSCHAP がイネーブルの場合は、MSCHAP VSA (Vendor-Specific Attribute; ベンダー固有属性) を認識するように RADIUS サーバを設定する必要があります。

次の表に、MSCHAP に必要な RADIUS VSA を示します。

表 3: MSCHAP RADIUS VSA

ベンダー ID 番号	ベンダー タイプ番号	VSA	説明
311	11	MSCHAP-Challenge	AAA サーバから MSCHAP ユーザに送信されるチャレンジを保持します。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。
211	11	MSCHAP-Response	チャレンジに対する応答として MSCHAP ユーザが入力した値を保持します。Access-Request パケットでしか使用されません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# aaa authentication login mschap enable	MS-CHAP 認証をイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show aaa authentication login mschap	(任意) MS-CHAP 設定を表示します。
ステップ 5	switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

デフォルトの AAA アカウントング方式の設定

Cisco Nexus デバイスは、アカウントングに TACACS+ 方式と RADIUS 方式をサポートします。スイッチは、ユーザアクティビティをアカウントングレコードの形で TACACS+ セキュリティサーバまたは RADIUS セキュリティサーバに報告します。各アカウントングレコードに、アカウントング属性値 (AV) のペアが入っており、それが AAA サーバに格納されます。

AAA アカウントングをアクティブにすると、Cisco Nexus デバイスは、これらの属性をアカウントングレコードとして報告します。そのアカウントングレコードは、セキュリティサーバ上のアカウントングログに格納されます。

特定のアカウントング方式を定義するデフォルト方式のリストを作成できます。それには次の方式があります。

- RADIUS サーバグループ：RADIUS サーバのグローバルプールをアカウントングに使用します。
- 特定のサーバグループ：指定した RADIUS または TACACS+ サーバグループをアカウントングに使用します。
- ローカル：ユーザ名またはパスワードのローカルデータベースをアカウントングに使用します。



(注) サーバグループが設定されていて、そのサーバグループが応答しない場合、デフォルトではローカルデータベースが認証に使用されます。

はじめる前に

必要に応じて、AAA アカウントングのデフォルト方式を設定する前に RADIUS または TACACS+ サーバグループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	<code>switch# configure terminal</code>	グローバルコンフィギュレーションモードを開始します。
ステップ 2	<code>switch(config)# aaa accounting default {groupgroup-list local}</code>	デフォルトのアカウントング方式を設定します。スペースで区切ったリストで、1 つまたは複数のサーバグループ名を指定できます。 <i>group-list</i> 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • radius を指定すると、RADIUS サーバのグローバルプールがアカウントングに使用されます。 • named-group を指定すると、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットがアカウントングに使用されます。 <p>local 方式では、アカウントングにローカル データベースが使用されます。</p> <p>デフォルトの方式は local です。サーバグループが設定されていないとき、または設定済みのすべてのサーバグループから応答がないときに、このデフォルト方式が使用されます。</p>
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	switch# show aaa accounting	(任意) デフォルトの AAA アカウントング方式の設定を表示します。
ステップ 5	switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

AAA サーバの VSA の使用

VSA

ベンダー固有属性 (VSA) を使用して、AAA サーバ上での Cisco Nexus デバイスのユーザ ロールおよび SNMPv3 パラメータを指定できます。

インターネット技術特別調査委員会 (IETF) が、ネットワーク アクセス サーバと RADIUS サーバの間での VSA の通信のための方式を規定する標準を作成しています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、一般的な用途には適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダータイプは 1 (名前付き **cisco-av-pair**) です。値は次の形式のストリングです。

protocol : attribute seperator value *

プロトコルは、特定のタイプの許可用のシスコ属性です。必須属性の区切り文字は等号 (=) で、アスタリスク (*) は任意属性を示します。

Cisco Nexus デバイスでの認証に RADIUS サーバを使用する場合は、許可情報などのユーザ属性を認証結果とともに返すように、RADIUS サーバに RADIUS プロトコルで指示します。この許可情報は、VSA で指定されます。

VSA の形式

次の VSA プロトコル オプションが、Cisco Nexus デバイスでサポートされています。

- **Shell** : ユーザ プロファイル情報を提供する `access-accept` パケットで使用されます。
- **Accounting** : `accounting-request` パケットで使用されます。値にスペースが含まれている場合は、二重引用符で囲んでください。

次の属性が Cisco Nexus デバイスでサポートされています。

- **roles** : ユーザに割り当てるすべてのロールをリストします。値フィールドは、グループ名を空白で区切ったリストの入ったストリングです。
- **accountinginfo** : 標準の RADIUS アカウンティングプロトコルで処理される属性に加えて、追加のアカウンティング情報が格納されます。この属性が送信されるのは、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分内だけです。この属性は、アカウンティングプロトコル関連の PDU でしか使用できません。

AAA サーバ上でのスイッチのユーザ ロールと SNMPv3 パラメータの指定

AAA サーバで VSA `cisco-av-pair` を使用して、次の形式で、Cisco Nexus デバイスのユーザ ロール マッピングを指定できます。

```
shell:roles="roleA roleB ..."
```

`cisco-av-pair` 属性にロール オプションを指定しなかった場合のデフォルトのユーザ ロールは、`network-operator` です。



- (注) Cisco Unified Wireless Network TACACS+ 設定と、ユーザ ロールの変更については、『[Cisco Unified Wireless Network TACACS+ Configuration](#)』を参照してください。

次のように SNMPv3 認証とプライバシー プロトコル属性を指定することもできます。

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

SNMPv3 認証プロトコルに指定できるオプションは、SHA と MD5 です。プライバシー プロトコルに指定できるオプションは、AES-128 と DES です。`cisco-av-pair` 属性にこれらのオプションを指定しなかった場合のデフォルトの認証プロトコルは、MD5 と DES です。

追加情報については、Cisco Nexus デバイスの『[System Management Configuration Guide](#)』の「[Configuring User Accounts and RBAC](#)」の章を参照してください。

ローカル AAA アカウントティング ログのモニタリングとクリア

Cisco Nexus デバイスは、AAA アカウントティング アクティビティのローカル ログを保持しています。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# show accounting log [size] [start-time year month day hh:mm:ss]	アカウントティング ログを表示します。このコマンド出力には、デフォルトで最大 250,000 バイトのアカウントティング ログが表示されます。サイズ引数を指定すれば、コマンドの出力を制限できます。指定できる範囲は 0 ~ 250000 バイトです。ログ出力の開始時刻を指定することもできます。
ステップ 2	switch# clear accounting log	(任意) アカウントティング ログの内容をクリアします。

AAA 設定の確認

AAA の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show aaa accounting	AAA アカウントティングの設定を表示します。
show aaa authentication [login {error-enable mschap}]	AAA 認証情報を表示します。
show aaa authorization	AAA 許可の情報を表示します。
show aaa groups	AAA サーバグループの設定を表示します。
show running-config aaa [all]	実行コンフィギュレーションの AAA 設定を表示します。
show startup-config aaa	スタートアップコンフィギュレーションの AAA 設定を表示します。

AAA の設定例

次に、AAA を設定する例を示します。

```
switch(config)# aaa authentication login default group radius
switch(config)# aaa authentication login console group radius
switch(config)# aaa accounting default group radius
```

デフォルトの AAA 設定

次の表に、AAA パラメータのデフォルト設定を示します。

表 4: デフォルトの AAA パラメータ

パラメータ	デフォルト
コンソール認証方式	local
デフォルト認証方式	local
ログイン認証失敗メッセージ	ディセーブル
MSCHAP 認証	ディセーブル
デフォルト アカウンティング方式	local
アカウンティング ログの表示サイズ	250 KB

