CHAPTER 2

AAA の設定

この章では、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）を設定する手順について説明します。

ここでは、次の内容を説明します。

AAA の概要

ここでは、次の内容について説明します。

AAA セキュリティ サービス

AAA 機能を使用すると、NX-OS デバイスを管理するユーザの ID を確認し、ユーザにアクセスを許可し、ユーザの実行するアクションを追跡できます。Cisco NX-OS 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。

Cisco NX-OS は入力されたユーザ ID およびパスワードの組み合わせに基づいて、ローカル データベースによるローカル認証または許可、あるいは 1 つまたは複数の AAA サーバによるリモート認証または許可を実行します。NX-OS デバイスと AAA サーバの間の通信は、事前共有秘密鍵によって保護されます。共有する秘密鍵は、すべての AAA サーバに設定することも、特定の AAA サーバにのみ設定することもできます

AAA セキュリティでは、次のサービスが提供されます。

- 認証 — ログインとパスワードのダイアログ、チャレンジとレスポンス、メッセージング サポート、および選択したセキュリティ プロトコルに応じた暗号化などを使用してユーザを識別します。

  認証は、デバイスにアクセスする人物またはデバイスの ID を確認するプロセスです。この ID の確認は、NX-OS デバイスにアクセスするエンティティから提供されるユーザ ID とパスワードの組み合わせに基づいて行われます。Cisco NX-OS デバイスでは、ローカル認証（ローカル ルックアップ データベースを使用）またはリモート認証（1 台または複数の RADIUS サーバまたは TACACS+ サーバを使用）を実行できます。
- 認可 — アクセス制御を提供します。

  AAA 認可は、ユーザの実行可能な内容を指定したアトリビュートをまとめるプロセスです。NX-OS ソフトウェアでは、AAA サーバからダウンロードされるアトリビュートを使用して権限付与が行われます。RADIUS や TACACS+ などのリモート セキュリティ サーバでは、権限が定義された AV のペアを適切なユーザに関連付けることにより、ユーザに所定の権限を許可します。
- アカウンティング — 情報の収集、ローカルでの情報のロギング、およびこれらの情報を AAA サーバに送信して課金、監査、およびレポートに使用する手段を提供します。

  アカウンティング機能では、NX-OS デバイスへのアクセスに使用されるすべての管理セッションを追跡し、ログに記録して管理します。この情報を使用してレポートを生成し、トラブルシューティングや監査に役立てることができます。アカウンティング ログは、ローカルに保存したり、リモートの AAA サーバに送信することができます。

（注）　NX-OS ソフトウェアでは、認証、認可、およびアカウンティングを個別にサポートしています。たとえば、アカウンティングを設定しなくても、認証と認可を設定できます。

AAA を使用することの利点

AAA には次の利点があります。

- アクセス設定の柔軟性と操作性の向上
- スケーラビリティ
- RADIUS、TACACS+ などの標準化された認証方式
- 複数のバックアップ装置

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、ローカルの AAA サービスと比較して次の利点があります。

- ファブリック内の各 NX-OS デバイスのユーザ パスワード リストの管理が容易になります。
- AAA サーバはすでに多くの企業で幅広く導入されているので、容易に AAA サービスに使用できます。
- ファブリック内のすべての NX-OS デバイスのアカウンティング ログを中央で管理できます。
- ファブリック内の各 NX-OS デバイスのユーザ アトリビュートの管理が、NX-OS デバイスのローカル データベースを使用するよりも容易になります。

AAA サーバ グループ

AAA に対応するリモート AAA サーバの指定に、サーバ グループを使用できます。サーバ グループは、同じ AAA プロトコルを実装したリモート AAA サーバのセットです。サーバ グループの目的は、リモート AAA サーバが応答できない場合に備えて、フェールオーバー サーバを用意しておくことにあります。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には、同じグループ内の次のリモート サーバが試行されます。サーバのどれかが応答するまでこの処理が行われます。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、このサーバ グループは使用不可能であるとみなされます。必要であれば、サーバ グループを複数指定できます。Cisco NX-OS デバイスは、最初のサーバ グループのすべてのサーバからエラーを受信した場合に、次のサーバ グループのサーバを試行します。

AAA サービス設定オプション

Cisco NX-OS デバイスの AAA 設定は、サービス ベースです。次のサービスごとに異なった AAA 設定を作成できます。

- ユーザの Telnet または Secure Shell（SSH; セキュア シェル）ログイン認証
- コンソール ログイン認証
- Cisco TrustSec 認証（第 9 章「Cisco TrustSec の設定」を参照）
- 802.1X 認証（第 7 章「802.1X の設定」を参照）
- Network Admission Control（NAC）の Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）認証（第 8 章「NAC の設定」を参照）
- ユーザ管理セッション アカウンティング
- 802.1X アカウンティング（第 7 章「802.1X の設定」を参照）

表 2-1 に、AAA サービス設定オプションごとに CLI（コマンドライン インターフェイス）の関連コマンドを示します。

表 2-1　AAA サービス設定コマンド

AAA サービス設定オプション	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**
Cisco TrustSec 認証	**aaa authentication cts default**
802.1X 認証	**aaa authentication dot1x default**
EAPoUDP 認証	**aaa authentication eou default**
ユーザ セッション アカウンティング	**aaa accounting default**
802.1X アカウンティング	**aaa accounting dot1x 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。
- 指定サーバ グループ — 指定の 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 — ローカルのユーザ名またはパスワード データベースを認証に使用します。
- なし（none）— ユーザ名のみを使用します。

（注）　認証方式が特定のサーバ グループでなく、すべて RADIUS サーバの場合は、NX-OS デバイスが指定された RADIUS サーバのグローバル プールから設定の順に RADIUS サーバを選択します。このグローバル プールから選択されるサーバは、NX-OS デバイス上で RADIUS サーバ グループに選択的に設定できるサーバです。

表 2-2 に、AAA サービスに対応して設定できる AAA 認証方式を示します。

表 2-2　AAA サービスに対応する AAA 認証方式

AAA サービス	AAA 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（none）
ユーザ ログイン認証	サーバ グループ、ローカル、なし（none）
Cisco TrustSec 認証	サーバ グループのみ
802.1X 認証	サーバ グループのみ
EAPoUDP 認証	サーバ グループのみ
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
802.1X アカウンティング	サーバ グループ、ローカル

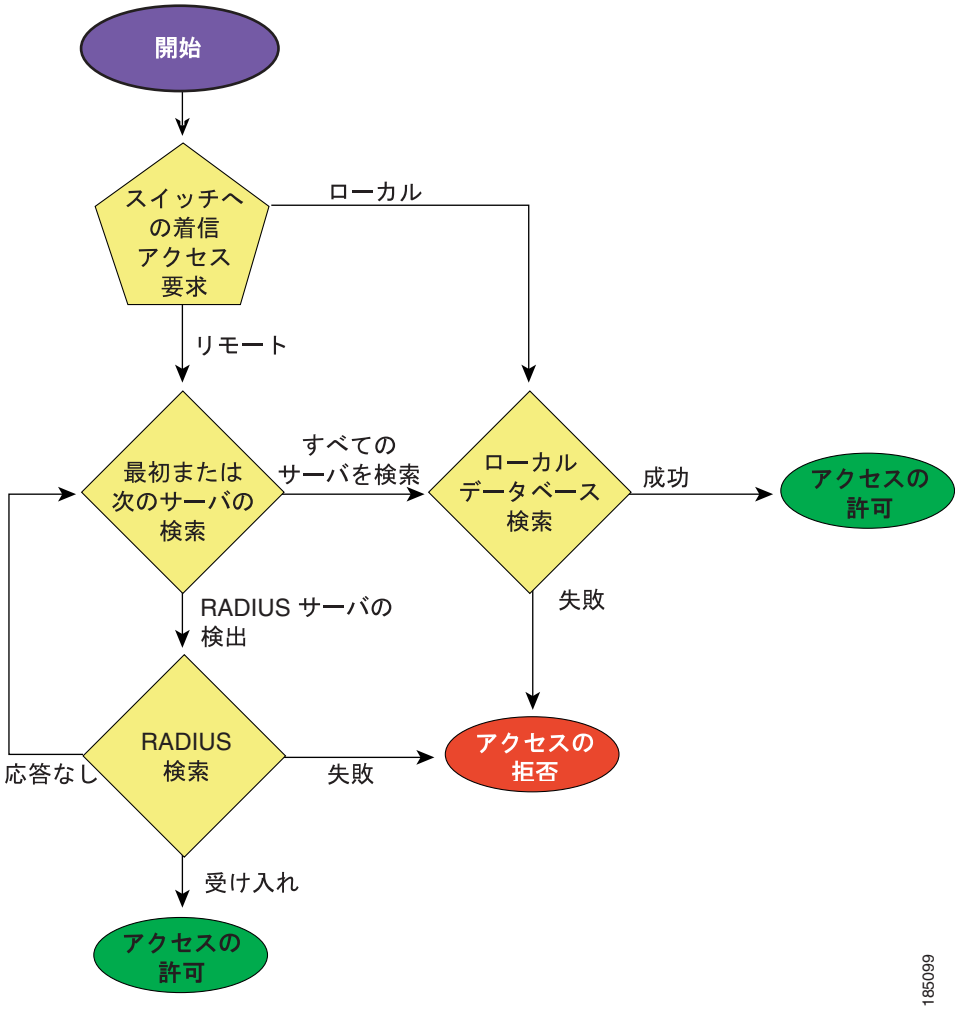
（注）　コンソール ログイン認証、ユーザ ログイン認証、およびユーザ管理セッション アカウンティングの場合は、NX-OS デバイスが指定された順序で各オプションを試行します。ローカル オプションは、他の設定オプションが失敗した場合のデフォルト方式です。

ユーザ ログインの認証および認可プロセス

図 2-1 に、ユーザ ログインの認証および認可プロセスのフローチャートを示します。次に、このプロセスについて順番に説明します。

1. Cisco NX-OS デバイスにログインする場合、Telnet、SSH、またはコンソール ログインのオプションが使用できます。
2. サーバ グループ認証方式を使用して AAA サーバ グループを設定した場合は、NX-OS デバイスが次のように認証要求をグループ内の最初の AAA サーバに送信します。
   - この AAA サーバが応答しなかった場合には、次の AAA サーバが試行されます。リモート サーバが認証要求に応答するまでこの処理が行われます。
   - 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、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は、ローカル データベースが認証に使用されます。
3. NX-OS デバイスがリモート AAA サーバでユーザの認証に成功した場合は、次のいずれかが適用されます。
   - AAA サーバ プロトコルが RADIUS の場合、cisco-av-pair アトリビュートに指定されているユーザ ロールが認証応答を使用してダウンロードされます。
   - AAA プロトコルが TACACS+ の場合、同じサーバに別の要求が送信されて、シェルのカスタム アトリビュートとして指定されているユーザ ロールが取得されます。
   - リモート AAA サーバからのユーザ ロールの取得に成功しない場合、ユーザに vdc-operator ロールが割り当てられます。
4. ローカルでユーザ名とパスワードの認証が成功した場合は、ログインが許可され、ローカル データベースに設定されているロールが割り当てられます。

図 2-1　ユーザ ログインの認証および許可のフロー



（注）　「すべてのサーバ グループを検索」は、全サーバ グループのどのサーバからも応答がないことを意味します。
「すべてのサーバを検索」は、このサーバ グループのどのサーバからも応答がないことを意味します。

バーチャライゼーション サポート

デフォルトのコンソール方式と AAA アカウンティング ログを除き、すべての AAA 設定と操作は VDC に対してローカルです。コンソール ログインの AAA 認証方式の設定と操作は、デフォルト VDC に対してのみ適用されます。AAA アカウンティング ログは、デフォルト VDC にのみ存在します。任意の VDC から内容を表示できますが、内容のクリアはデフォルト VDC で行う必要があります。

VDC の詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide, Release 4.0*』を参照してください。

AAA のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
NX-OS	AAA にライセンスは必要ありません。ライセンス パッケージに含まれない機能はすべて、Cisco NX-OS システム イメージにバンドルされており、無償で提供されます。NX-OS のライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide, Release 4.0*』を参照してください。

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 で到達可能になっていること（「RADIUS サーバ ホストの設定」[p.3-7] および「TACACS+ サーバ ホストの設定」[p.4-9] を参照）。
- NX-OS 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こと
- 事前共有秘密鍵が NX-OS デバイスおよびリモート AAA サーバに設定されていること
- リモート サーバが NX-OS デバイスの要求に応答すること（「RADIUS サーバまたはサーバ グループの手動でのモニタリング」[p.3-18] および「TACACS+ サーバまたはサーバ グループの手動でのモニタリング」[p.4-20] を参照）

AAA の注意事項および制限事項

RADIUS には、次の注意事項と制限事項があります。

- Cisco NX-OS ソフトウェアは、ユーザ名が RADIUS または TACACS+ によって作成されたのかローカルに作成されたのかに関係なく、すべて数字のユーザ名をサポートしていません。そのため、すべて数字のユーザ名は作成されません。すべて数字のユーザ名が AAA サーバ上に存在していて、ログイン時に入力された場合、NX-OS デバイスはそのユーザのログインを受け入れません。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールでなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。

AAA の設定

ここでは、次の内容について説明します。

（注）　Cisco IOS CLI の知識があるユーザは、この機能に関する Cisco NX-OS のコマンドが Cisco IOS のコマンドで使用されるものと異なる場合があることに注意してください。

AAA の設定プロセス

AAA 認証およびアカウンティングを設定するには、次の作業を行います。

ステップ 1　認証に RADIUS または TACACS+ サーバを使用する場合は、NX-OS デバイス上でホストを設定します（第 3 章「RADIUS の設定」および第 4 章「TACACS+ の設定」を参照）。

ステップ 2　コンソール ログイン認証方式を設定します（「コンソール ログイン認証方式の設定」[p.2-8] を参照）。

ステップ 3　ユーザ ログインのデフォルトのログイン認証方式を設定します（「デフォルトのログイン認証方式の設定」[p.2-10] を参照）。

ステップ 4　AAA アカウンティングのデフォルト方式を設定します（「AAA アカウンティングのデフォルト方式の設定」[p.2-13] を参照）。

（注）　802.1X の認証方式を設定するには、「802.1X の AAA 認証方式の設定」（p.7-11）を参照してください。EAPoUDP の認証方式を設定するには、「EAPoUDP のデフォルト AAA 認証方式のイネーブル化」（p.8-17）を参照してください。

コンソール ログイン認証方式の設定

ここでは、コンソール ログインの認証方式を設定する手順について説明します。

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 または TACACS+ サーバの名前付きサブセット
- NX-OS デバイスのローカル データベース
- ユーザ名のみ（**none**）

デフォルト方式はローカルです。

（注）　コンソール ログインの AAA の設定と操作は、デフォルト VDC に対してのみ適用されます。

（注）　**aaa authentication** コマンドの ***group radius*** および ***group*** *server-name* 形式は、以前に定義された RADIUS サーバのセットを参照します。ホスト サーバを設定する場合は、**radius server-host** コマンドを使用してください。サーバの名前付きグループを作成する場合は、**aaa group server radius** コマンドを使用してください。

作業を開始する前に

デフォルト VDC にいることを確認します。

必要に応じて RADIUS または TACACS+ サーバ グループを設定します。

手順の概要

1. **config t**
2. **aaa authentication login console** {**group** *group-list* [**none**] | **local** | **none**}
3. **exit**
4. **show aaa authentication**
5. **copy running-config start-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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 authentication login console** {**group** *group-list* [**none**]	**local**	**none**} **例：** `switch(config)# aaa authentication login console group radius`	コンソールのログイン認証方式を設定します。 *group-list* 引数は、グループ名をスペースで区切ったリストです。グループ名は次のとおりです。 • **radius** — RADIUS サーバのグローバル プールを認証に使用します。 • *named-group* — TACACS+ または RADIUS サーバの名前付きサブセットを認証に使用します。 **local** 方式は、ローカル データベースを認証に使用します。**none** 方式は、ユーザ名のみを使用します。 デフォルトのコンソール ログイン方式は、**local** です。これは認証方式が何も設定されていない場合、または設定された認証方式すべてについて応答が得られなかった場合に使用されます。

	コマンド	目的
ステップ 3	**exit** **例：** switch(config)# exit switch#	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	**show aaa authentication** **例：** 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	**copy running-config startup-config** **例：** 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 または TACACS+ サーバの名前付きサブセット
- NX-OS デバイスのローカル データベース
- ユーザ名のみ

デフォルト方式はローカルです。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

必要に応じて RADIUS または TACACS+ サーバ グループを設定します。

手順の概要

1. **config t**
2. **aaa authentication login default** {**group** *group-list* [**none**] | **local** | **none**}
3. **exit**
4. **show aaa authentication**
5. **copy running-config start-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 2	**aaa authentication login default** {**group** *group-list* [**none**] | **local** | **none**} **例**： `switch(config)# aaa authentication login default group radius`	デフォルトの認証方式を設定します。 *group-list* 引数は、グループ名をスペースで区切ったリストです。グループ名は次のとおりです。 • **radius** — RADIUS サーバのグローバル プールを認証に使用します。 • *named-group* — TACACS+ または RADIUS サーバの名前付きサブセットを認証に使用します。 **local** 方式は、ローカル データベースを認証に使用します。**none** 方式は、ユーザ名のみを使用します。 デフォルトのログイン方式は、**local** です。これは認証方式が何も設定されていない場合、または設定された認証方式すべてについて応答が得られなかった場合に使用されます。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		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	**show aaa authentication** **例**： `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。
ステップ 5	**copy running-config startup-config** **例**： `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。

ログイン認証エラー メッセージのイネーブル化

ログインする際にリモート AAA サーバが応答しない場合、ログインはローカルのユーザ データベースにロールオーバーされて処理されます。ログイン エラー メッセージの表示をイネーブルにしておくと、このような場合にはユーザの端末に次の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.
```

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **config t**
2. **aaa authentication login error-enable**
3. **exit**
4. **show aaa authentication**
5. **copy running-config start-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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 authentication login error-enable** **例：** `switch(config)# aaa authentication login error-enable`	ログイン認証エラー メッセージをイネーブルにします。デフォルトはディセーブルです。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		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	**show aaa authentication** **例：** `switch# show aaa authentication`	（任意）ログイン エラー メッセージの設定を表示します。
ステップ 5	**copy running-config startup-config** **例：** `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。

MSCHAP 認証のイネーブル化

Microsoft Challenge Handshake Authentication Protocol（MS-CHAP; 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）は CHAP の Microsoft バージョンです。リモート認証サーバ（RADIUS または TACACS+）を介した NX-OS 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、NX-OS デバイスとリモート サーバの間で Password Authentication Protocol（PAP; パスワード認証プロトコル）認証が使用されます。MSCHAP をイネーブルにする場合は、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。「Cisco NX-OS デバイスによる AAA サーバの VSA の使用」（p.2-15）を参照してください。表 2-3 に、MSCHAP に必要な RADIUS の VSA を示します。

表 2-3　MSCHAP RADIUS VSA

Vendor-ID 番号	Vendor-Type 番号	VSA	説明
311	11	MSCHAP-Challenge	AAA サーバが MSCHAP ユーザに送信するチャレンジが含まれます。Access-Request パケットと Access-Challenge パケットの両方に使用できます。
211	11	MSCHAP-Response	MSCHAP ユーザがチャレンジに対する応答で提供するレスポンス値が含まれます。Access-Request パケットでのみ使用されます。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **config t**

2. **aaa authentication login mschap enable**
3. **exit**
4. **show aaa authentication login mschap**
5. **copy running-config start-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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 authentication login mschap enable** **例**： `switch(config)# aaa authentication mschap enable`	MS-CHAP 認証をイネーブルにします。デフォルトはディセーブルです。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		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	**show aaa authentication login mschap** **例**： `switch# show aaa authentication login mschap`	（任意）MS-CHAP の設定を表示します。
ステップ 5	**copy running-config startup-config** **例**： `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 アカウンティングのデフォルト方式の設定

Cisco NX-OS ソフトウェアは、アカウンティングに TACACS+ および RADIUS 方式をサポートします。NX-OS デバイスは、ユーザのアクティビティを、アカウンティング レコードの形式で TACACS+ または RADIUS セキュリティ サーバにレポートします。アカウンティング レコードにはアカウンティング AV のペアが含まれ、AAA サーバに保存されます。

AAA アカウンティングをアクティブにすると、NX-OS デバイスは、これらのアトリビュートをアカウンティング レコードとしてレポートします。アカウンティング レコードはその後セキュリティ サーバのアカウンティング ログに保存されます。

デフォルトのアカウンティング方式リストを作成して、そこに所定のアカウンティング方式を定義できます。このアカウンティング方式には次のものが含まれます。

- RADIUS サーバ グループ — RADIUS サーバのグローバル プールをアカウンティングに使用します。
- 指定サーバ グループ — 指定の RADIUS または TACACS+ サーバ グループをアカウンティングに使用します。
- ローカル — ローカルのユーザ名またはパスワード データベースをアカウンティングに使用します。

（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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

必要に応じて RADIUS または TACACS+ サーバ グループを設定します。

手順の概要

1. **config t**
2. **aaa accounting default** {**group** *group-list* | **local**}
3. **exit**
4. **show aaa accounting**
5. **copy running-config start-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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 accounting default** {**group** *group-list* | **local**} **例：** `switch(config)# aaa accounting default group radius`	デフォルトのアカウンティング方式を設定します。 *group-list* 引数は、グループ名をスペースで区切ったリストです。グループ名は次のとおりです。 • **radius** — RADIUS サーバのグローバル プールをアカウンティングに使用します。 • *named-group* — TACACS+ または RADIUS サーバの名前付きサブセットをアカウンティングに使用します。 **local** 方式は、ローカル データベースをアカウンティングに使用します。 デフォルトのアカウンティング方式は、**local** です。これはサーバ グループが何も設定されていない場合、または設定されたすべてのサーバ グループから応答が得られなかった場合に使用されます。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 4	**show aaa accounting** **例：** switch# show aaa accounting	（任意）AAA アカウンティングのデフォルト方式の設定を表示します。
ステップ 5	**copy running-config startup-config** **例：** 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。

Cisco NX-OS デバイスによる AAA サーバの VSA の使用

VSA を使用して、AAA サーバ上で Cisco NX-OS のユーザ ロールおよび SNMPv3 パラメータを指定できます。

ここでは、次の内容について説明します。

VSA の概要

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）ドラフト標準には、ネットワーク アクセス サーバと RADIUS サーバの間で VSA（vendor-specific attribute; ベンダー固有属性）を伝達する方法が規定されています。IETF はアトリビュート 26 を使用しています。VSA を使用すると、ベンダーは一般的な用途に適さない独自の拡張アトリビュートをサポートできます。シスコの RADIUS 実装では、IETF 仕様で推奨される形式を使用したベンダー固有オプションを 1 つサポートしています。シスコのベンダー ID は 9 で、サポートするオプションはベンダー タイプ 1、名前は cisco-av-pair です。値は、次の形式のストリングです。

```
protocol : attribute seperator value *
```

protocol は、特定の許可タイプを表すシスコのアトリビュートです。separator は、必須アトリビュートの場合に =（等号）、オプションのアトリビュートの場合に *（アスタリスク）です。

Cisco NX-OS デバイス上の認証に RADIUS サーバを使用した場合、RADIUS プロトコルでは RADIUS サーバに対して、認証結果とともに権限付与情報などのユーザ アトリビュートを返すように指示します。この権限付与情報は、VSA を通じて指定されます。

VSA の形式

次の VSA プロトコル オプションが Cisco NX-OS ソフトウェア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るプロトコル
- Accounting — accounting-request パケットで使用されるプロトコル。値にスペースが含まれる場合は、二重引用符で囲む必要があります。

次のアトリビュートが Cisco NX-OS ソフトウェアでサポートされています。

- roles — ユーザに割り当てられているすべてのロールをリストします。値フィールドは、グループ名をスペースで区切ったストリングです。たとえば、ユーザが network-operator および vdc?admin のロールに属している場合、値フィールドは「network-operator vdc-admin」となりま

す。このサブアトリビュートは Access-Accept フレームの VSA 部分に格納され、RADIUS サーバから送信されます。このアトリビュートはシェル プロトコル値とだけ併用できます。次に、ロール アトリビュートを使用する例を示します。

```
shell:roles="network-operator vdc-admin"
shell:roles*"network-operator vdc-admin"
```

次に、FreeRADIUS でサポートされるロール アトリビュートの例を示します。

```
Cisco-AVPair = "shell:roles=\"network-operator vdc-admin\""
Cisco-AVPair = "shell:roles*\"network-operator vdc-admin\""
```

（注）　VSA を shell:roles*"network-operator vdc-admin" または "shell:roles*\"network-operator vdc-admin\"" として指定した場合、この VSA はオプション アトリビュートとしてフラグ設定され、他のシスコ製装置はこのアトリビュートを無視します。

- accountinginfo — 標準の RADIUS アカウンティング プロトコルに含まれるアトリビュートとともにアカウンティング情報を格納します。このアトリビュートは、スイッチ上の RADIUS クライアントから、Account-Request フレームの VSA 部分にだけ格納されて送信されます。このアトリビュートはアカウンティング プロトコル関連の PDU とだけ併用できます。

AAA サーバ上での Cisco NX-OS のユーザ ロールおよび SNMPv3 パラメータの指定

AAA サーバ上で VSA に cisco-av-pair を使用して、次の形式で Cisco NX-OS デバイスのユーザ ロールのマッピングを指定できます。

```
shell:roles="roleA roleB …"
```

cisco-av-pair アトリビュートにロール オプションを指定しなかった場合、デフォルトのユーザ ロールは network-operator です。

また、次のように、SNMPv3 認証アトリビュートとプライバシ プロトコル アトリビュートも指定できます。

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

SNMPv3 認証プロトコル オプションは、SHA および MD5 です。プライバシー プロトコル オプションは、AES-128 および DES です。cisco-av-pair アトリビュートにこれらのオプションを指定しなかった場合、デフォルトの認証プロトコルは MD5 と DES です。

ユーザ ロールの詳細については、第 6 章「ユーザ アカウントおよび RBAC の設定」を参照してください。

ローカル AAA アカウンティング ログの表示およびクリア

NX-OS デバイスは、AAA アカウンティングのアクティビティに関するローカル ログを維持しています。このログは表示したりクリアしたりできます。

（注）　AAA アカウンティング ログは、デフォルト VDC に対してローカルです。任意の VDC から内容を表示できますが、内容のクリアはデフォルト VDC で行う必要があります。

作業を開始する前に

AAA アカウンティング ログをクリアする前に、正しい VDC にいることを確認します。

手順の概要

1. **show accounting log** [*size*] [**start-time** *year month day hh*:*mm*:*ss*]
2. **clear accounting log**

詳細な手順

	コマンド	目的
ステップ 1	**show accounting log** [*size*] [**start-time** *year month day hh*:*mm*:*ss*] **例**： `switch# show accounting log`	アカウンティング ログの内容を表示します。デフォルトでは、最大 250,000 バイトのアカウンティング ログを出力できます。コマンドの出力を制限する場合は、*size* 引数を使用します。有効値の範囲は 0 ～ 250000 バイトです。また、ログの出力の開始時刻も指定できます。
ステップ 2	**clear accounting log** **例**： `switch# clear aaa accounting log`	（任意）アカウンティング 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、次の作業のいずれかを行います。

コマンド	目的
show aaa accounting	AAA アカウン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 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内の 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内の AAA 設定を表示します。

このコマンドの出力に表示されるフィールドの詳細については、『*Cisco NX-OS Security Command Reference, Release 4.0*』を参照してください。

AAA 設定例

次に、AAA を設定する例を示します。

```
aaa authentication login default group radius
aaa authentication login console group radius
aaa accounting default group radius
```

デフォルト設定

表 2-4 に、AAA パラメータのデフォルト設定を示します。

表 2-4　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	**ローカル**
デフォルト認証方式	**ローカル**
ログイン認証エラー 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	**ローカル**
アカウンティング ログの表示サイズ	250 KB

その他の参考資料

AAA の実装に関連する詳細情報については、次を参照してください。

- 関連資料（p.2-19）
- 規格（p.2-19）
- MIB（p.2-19）

関連資料

関連事項	タイトル
NX-OS ライセンス	『*Cisco NX-OS Licensing Guide, Release 4.0*』
コマンド リファレンス	『*Cisco NX-OS Security Command Reference, Release 4.0*』
RADIUS セキュリティ プロトコル	第 3 章「RADIUS の設定」
TACACS+ セキュリティ プロトコル	第 4 章「TACACS+ の設定」

規格

規格	タイトル
この機能によりサポートされた新規規格または改訂規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB のリンク
• CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB	MIB の確認とダウンロードを行うには、次の URL にアクセスします。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml