認証、許可、アカウンティングの設定

この章の内容は、次のとおりです。

AAA の概要

AAA セキュリティ サービス

認証、許可、アカウンティング（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 サーバ専用に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ギング、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、アカウンティングをそれぞれ個別にサポートします。たとえば、アカウンティングは設定せずに、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ティング 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、アカウンティ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 アカウンティング

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 アカウンティング	**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応答するまで、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。

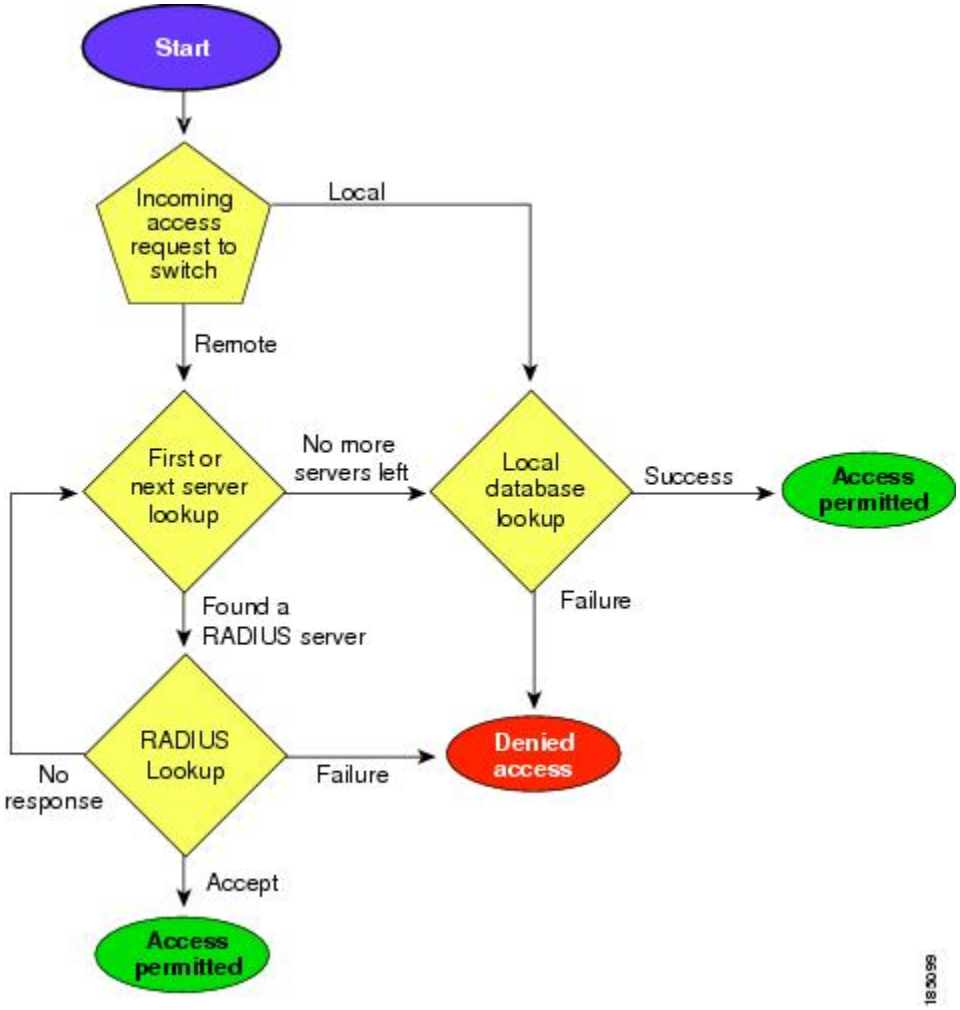
AAA サーバ プロトコルが RADIUS の場合、cisco-av-pair 属性で指定されているユーザ ロールが認証応答とともにダウンロードされます。

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 RADIUL サーバに関しては、**aaa authentication** コマンドの **group radius** 形式および **group** *server-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** {**group***group-list* [**none**] | **local** | **none**}	コンソールのログイン認証方式を設定します。 *group-list* 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。 • **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。 **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。 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。
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** {**group***group-list* [**none**] | **local** | **none**}	デフォルト認証方式を設定します。 *group-list* 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。 • **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。 **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。 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。
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。
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た場合は、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 セッションの許可は、Cisco Nexus 5000 プラットフォームではサポートされていません。Cisco Nexus 5500 プラットフォームでは、リリース 6.x 以降で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**} {{[**group***group-name*] |[**local**]} | {[**group***group-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
```

コンソール許可コマンドの設定

許可方式には、次のものがあります。

- 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。

必要に応じて、コンソール許可コマンドを設定する前に 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 authorization commands console** {**group***group-list* [**none**] | **local** | **none**}	コンソールの許可を設定します。 *group-list* 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。グループ名を次に示します。

	コマンドまたはアクション	目的
		• *named-group*：TACACS+ サーバの名前付きサブセットを許可に使用します。 **local** 方式では、許可にローカル データベースが使用されます。**none** 方式では、ユーザ名のみが使用されます。 デフォルトのコンソール許可は **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。
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 authorization**	（任意） コンソール許可コマンド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、コンソール許可コマンドを設定する例を示します。

```
switch# configure terminal
switch(config)# aaa authorization commands console group tacacs+
switch(config)# exit
switch# show aaa authorization
switch# copy running-config startup-config
```

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。

関連トピック

VSA, （15 ページ）

デフォルトの AAA アカウンティング方式の設定

Cisco Nexus デバイスは、アカウンティングに 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ティング 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。各アカウンティング レコードに、アカウンティング属性値（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 アカウンティ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ティング レコードとして報告します。そのアカウンティング レコードは、セキュリティ サーバ上のアカウンティング ログに格納されます。

特定のアカウンティ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 プールをアカウンティングに使用します。
- 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ティングに使用します。
- 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。

はじめる前に

必要に応じて、AAA アカウンティ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	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 accounting default** {**group***group-list*| **local**}	デフォルトのアカウンティ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。 *group-list* 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
		• **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ティ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ティングに使用されます。 **local** 方式では、アカウンティングにローカル データベースが使用されます。 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。
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 アカウンティ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。

セキュア ログインの機能拡張

次のセキュア ログインの機能拡張は、Cisco NX-OS でサポートされています。

ログイン パラメータの設定

Cisco NX-OS デバイスへの DoS 攻撃と思われる攻撃の検出と辞書攻撃の低減に役立つログイン パラメータを設定するには、次の作業を実行します。

すべてのログインパラメータは、デフォルトではディセーブルです。他のログインコマンドを使用する前に、デフォルトのログイン機能をイネーブルにする **loginblock-for** コマンドを入力する必要があります。**loginblock-for** コマンドをイネーブルにすると、次のデフォルトが強制されます。

- Telnet または SSH を通じて行われるすべてのログイン試行は、待機時間中拒否されます。つまり、**loginquiet-modeaccess-class** コマンドが入力されるまで、ACL はログイン時間から除外されません。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `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	**[no] loginblock-for***seconds***attempts***tries***within***seconds* 例： `Switch(config)# login block-for 100 attempts 2 within 100`	Cisco NX-OS デバイスで DoS 検出の提供に役立つログインパラメータを設定します。 （注） このコマンドは、その他のログイン コマンドを使用する前に発行する必要があります。
ステップ 3	**[no] loginquiet-modeaccess-class** {*acl-name* | *acl-number*} 例： `Switch(config)# login quiet-mode access-class myacl`	（任意）このコマンドはオプションですが、デバイスが静音モードに切り替わるときにデバイスに適用される ACL を指定するように設定することを推奨します。デバイスが静音モードのときは、すべてのログイン要求は拒否され、利用可能な接続のみコンソールで使用できます。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**showloginfailures** 例： `Switch# show login`	ログイン パラメータを表示します。 • **failures**：失敗したログイン試行に関連する情報のみを表示します。

ログイン パラメータの設定例

ログイン パラメータの設定：例

次に、100 秒以内に 15 回ログイン要求が失敗した場合に 100 秒の待機モードに入るようにスイッチを設定する例を示します。待機時間中、ACL「myacl」からのホスト以外、すべてのログイン要求が拒否されます。

```
Switch(config)# login block-for 100 attempts 15 within 100
Switch(config)# login quiet-mode access-class myacl
```

ログイン パラメータの表示：例

show login コマンドからの次のサンプル出力は、ログイン パラメータが指定されていないことを確認します。

```
Switch# show login

No Quiet-Mode access list has been configured, default ACL will be applied.

Switch is enabled to watch for login Attacks.
If more than 2 login failures occur in 45 seconds or less,  logins will be disabled for 70
 seconds.

Switch presently in Normal-Mode.
Current Watch Window remaining time 10 seconds.
Present login failure count 0.
```

show login failures コマンドからの次のサンプル出力は、スイッチ上で失敗したすべてのログイン試行を表示します。

```
Switch# show login failures

Information about last 20 login failures with the device.
--------------------------------------------------------------------------------
Username                                Line    Source                Appname
TimeStamp
--------------------------------------------------------------------------------
admin                                    pts/0   bgl-ads-728.cisco.com   login
```

```
        Wed Jun 10 04:56:16 2015
admin                                pts/0   bgl-ads-728.cisco.com   login
        Wed Jun 10 04:56:19 2015
-------------------------------------------------------------------------------
```

show login failures コマンドからの次のサンプル出力は、現在記録されている情報がないことを確認します。

```
Switch# show login failures
*** No logged failed login attempts with the device.***
```

ユーザごとのログイン ブロックの設定

ユーザごとのログイン ブロックは、サービス拒否（DoS）と思われる攻撃を検出して辞書攻撃を低減します。この機能はロカール ユーザにのみ適用されます。このタスクを使用して、ログイン パラメータを設定しログイン失敗時にユーザをブロックします。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `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	**aaa authenticationrejected***attempts***in***seconds***ban***seconds* 例： `switch(config)# aaa authentication rejected 3 in 20 ban 300`	ユーザをブロックするようにログイン パラメータを設定します。 （注） **no aaa authenticationrejected** コマンドを使用して、デフォルトのログイン パラメータに復元します。
ステップ 3	**exit** 例： `switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 4	**showrunningconfig** 例： `switch# show running config`	（任意）ログイン パラメータを表示します。
ステップ 5	**showaaalocal userblocked** 例： `switch# show aaa local user blocked`	（任意）ブロックされたローカル ユーザを表示します。

	コマンドまたはアクション	目的
ステップ 6	**clearaaalocal userblocked** {**username***user* | **all**} 例： `switch# clear aaa local user blocked username testuser`	（任意）ブロックされたローカル ユーザをクリアします。 • **all**：すべてのブロックされたローカルユーザをクリアします。

ユーザごとのログイン ブロックの設定例

ユーザごとのログイン ブロックのパラメータの設定

次の例では、60 秒の期間内で 5 回のログイン試行に失敗した場合にユーザを 300 秒間ブロックするようにログイン パラメータを設定する方法を示しています。

```
switch(config)# aaa authentication rejected 5 in 60 ban 300
```

ログイン パラメータの表示

次の例では、スイッチに設定されるログイン パラメータを示しています。

```
switch# show run | i rejected
aaa authentication rejected 5 in 60 ban 300
```

ブロックされたローカル ユーザの表示

次の例では、ブロックされたローカル ユーザを示しています。

```
switch# show aaa local user blocked
Local-user                  State

testuser                    Watched (till 11:34:42 IST Feb 5 2015)
```

ブロックされたローカル ユーザのクリア

次の例では、ブロックされたローカル ユーザの testuser をクリアする方法を示しています。

```
switch# clear aaa local user blocked username testuser
```

ユーザごとのセッション制限：ユーザごとのログインごと

ユーザごとの最大セッション数を制限するにはこのタスクを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `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	**[no] user max-logins***max-logins* 例： `Switch(config)# user max-logins 1`	ユーザごとの最大セッション数を制限します。指定できる範囲は1～7です。最大ログイン数の制限を1に設定すると、ユーザごとに1つのセッションのみ（telnet/SSH）が許可されます。
ステップ 3	**exit** 例： `Switch(config)# exit`	特権 EXEC モードに戻ります。

パスフレーズ長の設定

最大および最小のパスフレーズ長を設定するには、このタスクを使用します。

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`	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	**userpassphrase** {{**min-length***value* | **max-length***value*} | **min-length***value***max-length***value*} 例： `switch(config)# userpassphrase max-length 127`	ユーザのパスフレーズ長を設定します。最小パスフレーズ長の値の範囲は 8 ～ 127 です。最大パスフレーズ長の値の範囲は 80 ～127 です。デフォルトの最小パスフレーズ長は8であり、デフォルトの最大パスフレーズ長は 127 です。

	コマンドまたはアクション	目的
ステップ 3	**no userpassphrase** {**min-length** | **max-length** | **length**} 例： `switch(config)# no userpassphrase max-length`	パスフレーズ長の設定をデフォルト設定にリセットします。
ステップ 4	**exit** 例： `switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**show userpassphrase** {**min-length** | **max-length** | **length**} 例： `switch# show userpassphrase length`	最大および最小のユーザ パスフレーズ長を表示します。

パスフレーズの時間値の設定

以下のユーザのパスフレーズの時間値を設定できます。

- Lifetime：パスフレーズのライフタイム（日数）です。パスフレーズが期限切れになった後、ユーザは最初のログイン時にパスフレーズを変更するよう求められます。
- Gracetime：パスフレーズの猶予期間（日数）です。Gracetime は、パスフレーズの有効期限が切れてからアカウントがロックされるまでの、アクティビティがなかった日数です。
- Warntime：パスフレーズの期限切れの警告期間（日数）です。Warntime は、ユーザのパスフレーズが期限切れになる前の日数であり、このときパスフレーズが期限切れになることをユーザに警告します。

  デフォルトの時間値は、ライフタイムは 99999 日、warntime は 14 日、gracetime は 3 日です。値 99999 は、デフォルトでユーザのパスフレーズが期限切れしていないことを示します。

（注） デフォルトでは、「admin」以外のユーザの実行コンフィギュレーションに追加の設定が追加されます。これはユーザのパスフレーズの時間値を示します。デフォルトでは、追加の設定は、ユーザのデフォルトのパスフレーズの時間値を表示します。

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`	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	**username***username***passphrase** {{**lifetime** | **warntime** | **gracetime**} *time-value* | {**lifetime***time-value***warntime***time-value***gracetime***time-value*}} 例： `switch(config)# username test-user passphrase lifetime 990`	ユーザのパスフレーズの時間値を設定します。 このステップは network-admin でのみ実行できることに注意してください。
ステップ 3	**no username***username***passphrase** {**lifetime** | **warntime** | **gracetime** | **timevalues**} 例： `switch(config)# no username test-user passphrase lifetime`	（任意） ユーザのパスフレーズの時間値をデフォルト値にリセットします。 このステップは network-admin でのみ実行できることに注意してください。
ステップ 4	**userpassphrase** {**default-lifetime** | **default-warntime** | **default-gracetime**} *time-value* 例： `switch(config)# userpassphrase default-lifetime 990`	（任意） デフォルトのパスフレーズの時間値を更新します。 このステップは network-admin でのみ実行できることに注意してください。
ステップ 5	**no userpassphrase** {**default-lifetime** | **default-warntime** | **default-gracetimetimevalue**} 例： `switch(config)# no userpassphrase default-lifetime`	（任意） 設定されているデフォルト値が初期のデフォルト値にリセットされます。 このステップは network-admin でのみ実行できることに注意してください。
ステップ 6	**username***username***expire-userpassphrase** 例： `switch(config)# username john expire-userpassphrase`	（任意） 任意の userpassphrase をすぐに期限切れに設定します。パスフレーズの期限切れ後にログインしようとすると、古いパスワードを正しく入力した

	コマンドまたはアクション	目的
		後に新しいパスワードを入力して作成するように求められます。 このステップはadminでのみ実行できることに注意してください。
ステップ 7	**exit** 例： `switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 8	**show userpassphrase** {**default-lifetime** | **default-warntime** | **default-gracetime** | **timevalues**} 例： `switch# show userpassphrase default-lifetime`	パスフレーズの時間値を表示します。
ステップ 9	**show username***username***passphrase timevalues** 例： `switch# show username john passphrase timevalues`	特定のユーザのパスフレーズのライフタイム、警告期間、および猶予期間を表示します。
ステップ 10	**show running-config** 例： `switch# show running-config`	（任意） 設定されている値を表示します。

パスフレーズの時間値の設定

次の例では、test-user のパスフレーズの時間値を設定する方法を示しています。

```
switch(config)# username test-user passphrase lifetime 365 warntime 10 gracetime 5
switch(config)# show username test-user passphrase timevalues
Last passphrase change(Y-M-D):  2016-01-28
Passphrase lifetime:            365 days after last passphrase change
Passphrase warning time starts: 10 days before passphrase lifetime
Passphrase Gracetime ends:      5 days after passphrase lifetime

switch# show running-config

!Command: show running-config
!Time: Mon Nov 30 02:32:51 2015

version 7.3(0)N1(1)
hostname switch

role name test
username admin password 5 5$0sCUUZQm$fXdGj90e9yXv1XeuY9qResKmLGKQtn8Tj6ab4s4IcVA  role
network-admin username test-user password 5
5$c9Gmvm8E$aoSQ1X7vfphlJ6WeRQl3C0Py6TlpiDjhWcF6kYi4hg6 expire 1970-01-01 role network-operator
```

```
username test-user passphrase  lifetime 365 warntime 10 gracetime 5
```

ユーザ アカウントのロック

管理者として、任意のユーザ アカウントをロックまたはロック解除できます。

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`	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	**[no] username***username***lock-user-account** 例： `switch(config)# username john lock-user-account`	指定したユーザ アカウントをロックします。ユーザ アカウントのロックを解除するには、このコマンドの **no** 形式を使用します。
ステップ 3	**unlock locked-users** 例： `switch(config)# unlock locked-users`	（任意） すべてのロックされたユーザ アカウントをロック解除します。
ステップ 4	**exit** 例： `switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**show locked-users** 例： `switch# show locked-users`	すべてのロックされたユーザを表示します。

無効なユーザ名のロギング

管理者として、認証の失敗時にログに無効なユーザ名のロギング、またはロギングがないことを確認できます。デフォルトでは、認証の失敗時の無効なユーザ名はロギングされません。認証が通らないユーザ名は、無効なユーザ名とみなされて記録されません。これは、パスワードを誤っ

てユーザ名フィールドに入力した場合に記録される可能性があるためです。この機能はパスワードを記録するリスクを軽減できます。

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`	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	**[no] aaa authentication login invalid-username-log** 例： `switch(config)# aaa authentication login invalid-username-log`	認証失敗時の無効なユーザ名のロギングをイネーブルにします。無効なユーザ名のロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 3	**exit** 例： `switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 4	**show aaa authentication login invalid-username-log** 例： `switch# show aaa authentication login invalid-username-log`	無効なユーザ名のロギングがイネーブルかどうかを表示します。

パスワードの変更

パスワードを変更するには、このタスクを使用します。

手順

ステップ 1 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。
switch# **configure terminal**

ステップ 2 パスワードを変更するには、次のいずれかを実行します。

- 古いパスワードで認証を行い、新しいパスワードを入力します。
  switch(config)# **change-password**

（注） デフォルトでは、**password secure-mode** は有効化されています。したがって、ユーザはパスワードを変更する前に古いパスワードを認証に使用する必要があります。管理者ユーザは、**no password secure-mode** コマンドを使用して、パスワード セキュア モードを無効にできます。これによりユーザは、**username***username***password***new_password* コマンドを使用して、古いパスワードでの認証を行わずにパスワードを変更できます。

- パスワード セキュア モードが有効の場合、管理者ユーザは、**username** コマンドを使用してパスワードを変更できます。

  switch(config)# **username admin password***new-password***role***role-name*

  （注） パスワードセキュア モードが無効の場合、どのユーザでも、**username** コマンドを使用してパスワードを変更できます。

ステップ 3 特権モードを終了します。
switch(config)# **exit**

ステップ 4 パスワード セキュア モードのステータスを表示します。
switch# **show password secure-mode**

パスワードの変更

この例では、パスワードを変更するための実行コンフィギュレーションを示しています。プレースホルダを、セットアップに関連する値に置き換えます。

```
config t
 change-password
 Enter old password:
 Enter new password:
 Confirm new password:
 exit
```

ユーザ名のパスワード プロンプトの有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `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。

	コマンドまたはアクション	目的
ステップ 2	**[no] password prompt username** 例： `Switch(config)# password prompt username`	ログイン ノブをイネーブルにします。このコマンドをイネーブルにして、ユーザがパスワード オプションなしで **username** コマンドを入力すると、パスワードが求められます。パスワードは隠し文字を受け入れます。ログイン ノブをディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 3	**exit** 例： `Switch(config)# exit`	特権 EXEC モードに戻ります。

OS の整合性を確認するための SHA-256 アルゴリズムのサポート

show file bootflash:/ sha256sum コマンドを使用してファイルの sha256sum を表示します。このコマンドのサンプル出力を次に示します。

```
Switch# show file bootflash:/ sha256sum
abd9d40020538acc363df3d1bae7d1df16841e4903fca2c07c7898bf4f549ef5
```

RADIUS/TACACS+ を使用するための共有キー値の設定

ユーザがリモート認証およびアカウンティング用に設定した共有秘密は隠す必要があります。**radius-server key** および **tacacs-server key** コマンドについては、暗号化された共有秘密鍵を生成するために別のコマンドを使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `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	**generate type7_encrypted_secret** 例： `Switch(config)# generate type7_encrypted_secret`	RADIUS および TACACS 共有秘密をキー タイプ 7 で設定します。暗号化された共有秘密の生成中、ユーザの入力は非表示になります。

	コマンドまたはアクション	目的
		（注） プレーン テキストに相当する暗号化を別に生成し、暗号化された共有秘密を後で設定できます。
ステップ 3	**exit** 例： `Switch(config)# exit`	特権 EXEC モードに戻ります。

ローカルAAAアカウン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 アカウンティングの設定を表示します。

コマンド	目的
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