AAA の設定

この章では、Cisco NX-OS デバイスで認証、許可、アカウンティング（AAA）を設定する手順について説明します。

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ーの 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。

ユーザーが入力したユーザー 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 サーバー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 サーバー間の通信は、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：ユーザーを識別します。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 サーバー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 サーバーは、適切なユーザー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、ユーザー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 サーバーへの情報の送信の方式を提供します。

Note 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ーパスワードリストを簡単に管理できます。
- AAA サーバー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ー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。サーバー 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 サーバーです。リモート AAA サーバーが応答しなかった場合、サーバー グループは、フェールオーバー サーバーを提供します。グループ内の最初のリモート サーバーが応答しなかった

場合、いずれかのサーバー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ーで試行が行われます。サーバー グループ内のすべての AAA サーバーが応答しなかった場合、そのサーバー 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、複数のサーバー 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ーからエラーを受信すると、次のサーバー グループのサーバーが試行されます。

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
- ユーザー管理セッション 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。

***Table 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**
ユーザー 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 サーバー グループ：RADIUS サーバーのグローバル プールを認証に使用します。
- 特定のサーバー グループ：指定した RADIUS または TACACS+ サーバー グループを認証に使用します。
- ローカル：ユーザー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：ユーザー名だけを使用します。

Note 方式がすべて RADIUS サーバーになっており、特定のサーバー 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 サーバーのグローバル プールから、設定された順序で RADIUS サーバーを選択します。このグローバル プールからのサーバーは、Cisco Nexus デバイス上の RADIUS サーバー グループ内で選択的に設定できるサーバーです。

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。

Table 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
ユーザー ログイン認証	サーバ グループ、ローカル、なし
ユーザー管理セッション アカウンティング	サーバ グループ、ローカル

Note コンソール ログイン認証、ユーザー ログイン認証、およびユーザー管理セッション 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。

ユーザー ログインの認証および許可プロセス

ユーザー 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。
- サーバー グループ認証方式を使用して AAA サーバー 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 サーバーに認証要求を送信し、次のように処理されます。

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

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

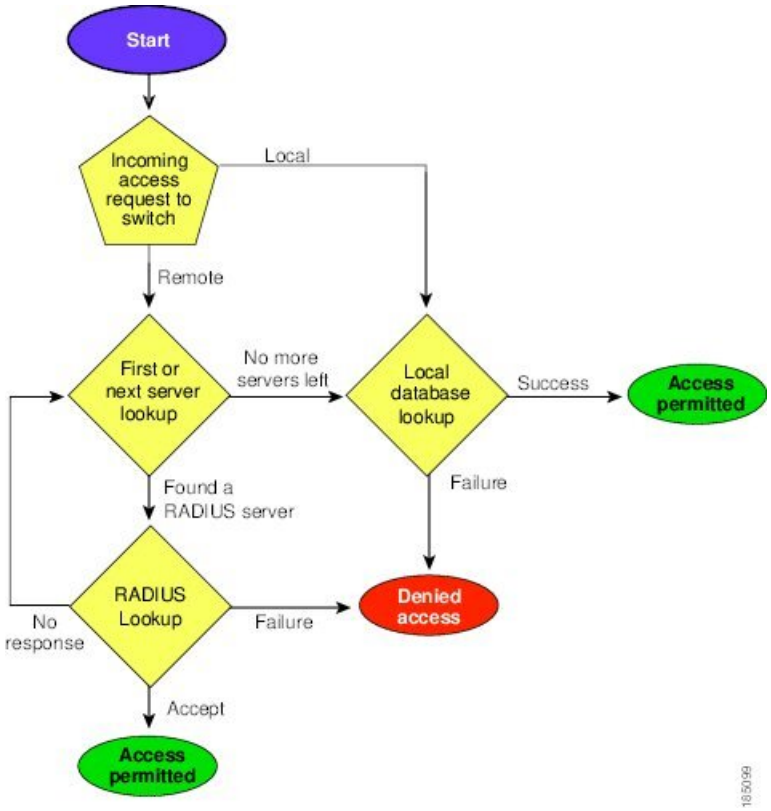
  設定されているすべての認証方式が失敗した場合、ローカルデータベースを使用して認証が実行されます。
- Cisco Nexus デバイスがリモート AAA サーバーで正常に認証できた場合は、次の条件が適用されます。

  AAA サーバー 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ー ロールが認証応答とともにダウンロードされます。

  AAA サーバー 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ー ロールを取得するために、もう 1 つの要求が同じサーバーに送信されます。
- ユーザー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。

Figure 1: ユーザー ログインの認証および許可のフロー



Note この図は、ユーザー名パスワード SSH 認証にのみ適用されます。公開キー SSH 認証には適用されません。すべてのユーザー名、パスワード、SSH 認証は AAA を通過します。

この図に示されている「残りのサーバーなし」とは、現在のサーバー グループ内のいずれのサーバー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 サーバーまたは TACACS+ サーバーが、IP で到達可能であること。
- Cisco Nexus デバイスが AAA サーバー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 サーバー上で設定されている。
- リモート サーバーが 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

そのユーザー名が 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ー名はサポートされません。AAA サーバーに数字だけのユーザー名が存在し、ログイン時にその名前を入力した場合でも、ユーザーは Cisco Nexus デバイスにログインを許可されます。

AAA ログイン認証のデフォルト グループ TACACS-SERVER-GROUP を構成すると、コンソールのログインも上書きされます。このオーバーライドは、**aaa authentication login console local** がスイッチのデフォルト コマンドである場合でも発生します。これを防ぐには、**aaa authentication login console local** を構成する必要があります。

注意 すべて数字のユーザー名でユーザー 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 サーバーまたは TACACS+ サーバー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
- ユーザー名だけ **none**

デフォルトの方式は、ローカルです。

Note 事前に設定されている一連の RADIUS サーバーに関しては、**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 サーバーを設定するには、radius server-host コマンドを使用します。サーバー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。

Note AAA ログイン認証のデフォルト グループ TACACS-SERVER-GROUP を構成すると、コンソールのログインも上書きされます。このオーバーライドは、**aaa authentication login console local** がスイッチのデフォルト コマンドである場合でも発生します。これを防ぐには、**aaa authentication login console local** を構成する必要があります。

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+ サーバー グループを設定します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **aaa authentication login console** { **group** *group-list* [**none**] | **local** | **none**}
3. switch(config)# **exit**
4. (Optional) switch# **show aaa authentication**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
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** RADIUS サーバーのグローバル プールを使用して認証を行います。 • *named-group* を指定すると、TACACS+ サーバーまたは RADIUS サーバー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、ユーザー名だけが使用されます。 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	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	(Optional) switch# **show aaa authentication**	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	(Optional) switch# **copy running-config startup-config**	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。

Example

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+サーバー グループを設定します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **aaa authentication login default** { **group** *group-list* [**none**] | **local** | **none**}
3. switch(config)# **exit**
4. (Optional) switch# **show aaa authentication**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
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** RADIUS サーバーのグローバル プールを使用して認証を行います。 • *named-group* を指定すると、TACACS+ サーバーまたはRADIUS サーバーの名前付きサブセットが認証に使用されます。

	Command or Action	Purpose
		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、ユーザー名だけが使用されます。 デフォルトのログイン方式は **local** です。この方式は、方式が一切設定されていない場合、または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**	コンフィグレーション モードを終了します。
ステップ 4	(Optional) switch# **show aaa authentication**	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	(Optional) switch# **copy running-config startup-config**	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有効化

ユーザーがログインして、リモート AAA サーバーが応答しなかった場合は、ローカル ユーザー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.
```

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **aaa authentication login error-enable**
3. switch(config)# **exit**
4. (Optional) switch# **show aaa authentication**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
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有効にします。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**	コンフィグレーション モードを終了します。

	Command or Action	Purpose
ステップ 4	(Optional) switch# **show aaa authentication**	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	(Optional) switch# **copy running-config startup-config**	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。

成功したログイン試行と失敗したログイン試行

成功したログイン試行と失敗したログイン試行をすべて、設定されたsyslogサーバに記録するようにスイッチを設定できます。

手順の概要

1. **configure terminal**
2. [**no**] **login on-failure log**
3. [**no**] **login on-success log**
4. （任意） **show login on-failure log**
5. （任意） **show login on-successful log**
6. （任意） **copy running-config startup-config**

手順の詳細

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`	グローバル設定モードを開始します。
ステップ 2	必須: [**no**] **login on-failure log** 例： `switch(config)# login on-failure log`	失敗した認証に関するすべてのメッセージを構成済みの syslog サーバーに記録します。この設定では、ログイン失敗後に次のsyslogメッセージが表示されます。 AUTHPRIV-3-SYSTEM_MSG：pam_aaa：Authentication failed for user admin from 172.22.00.00 （注） ロギング レベル authpriv が 6 の場合、追加の Linux カーネル認証メッセージが以前のメッセージとともに表示されます。これらの追加のメッセージを無視する必要がある場合、authpriv 値を 3 に設定する必要があります。

	コマンドまたはアクション	目的
ステップ 3	必須: [**no**] **login on-success log** 例： `switch(config)# login on-success log`	成功した認証に関するすべてのメッセージを構成済みの syslog サーバーに記録します。この設定では、ログインに成功すると次のsyslogメッセージが表示されます。 AUTHPRIV-6-SYSTEM_MSG：pam_aaa：Authentication success for user admin from 172.22.00.00 （注） ロギング レベル authpriv が 6 の場合、追加の Linux カーネル認証メッセージが以前のメッセージとともに表示されます。
ステップ 4	（任意） **show login on-failure log** 例： `switch(config)# show login on-failure log`	失敗した認証メッセージをsyslogサーバに記録するようにスイッチが設定されているかどうかを表示します。
ステップ 5	（任意） **show login on-successful log** 例： `switch(config)# show login on-successful log`	成功した認証メッセージをsyslogサーバに記録するようにスイッチが設定されているかどうかを表示します。
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	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+ サーバーの許可方式が構成されている場合は、ユーザーが TACACS+ サーバー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構成モード 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+ サーバー 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 セッションでは承認は行えません。

始める前に

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。

手順の概要

1. **configure terminal**
2. **aaa authorization** {**commands** | **config-commands**} {**default**} {{[**group** *group-name*] | [**local**]} | {[**group** *group-name*] | [**none**]}}

手順の詳細

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。
						構成モード コマンドを許可するには、**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。

例

次に、TACACS+ サーバー 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+ サーバー 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+ サーバー 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。

- サーバーが到達可能である場合、コマンドはサーバー応答に基づいて許可され、または許可されません。
- サーバーに到達する際にエラーが生じた場合、コマンドはユーザーのローカル 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+ サーバー 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。

- サーバーが到達可能である場合、コマンドはサーバー応答に基づいて許可され、または許可されません。
- サーバー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ー（RADIUS または TACACS+）を通じて、Cisco Nexus デバイスへのユーザー 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 サーバー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 サーバー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。

Table 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 サーバーから MSCHAP ユーザー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 ユーザー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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **aaa authentication login mschap enable**
3. switch(config)# **exit**
4. (Optional) switch# **show aaa authentication login mschap**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
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**	コンフィグレーション モードを終了します。
ステップ 4	(Optional) switch# **show aaa authentication login mschap**	MS-CHAP 設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	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。

LDAP サーバでの AAA 許可の設定

LDAP サーバのデフォルトの AAA 許可方式を設定できます。

Before you begin

LDAP を有効にします。

SUMMARY STEPS

1. **configure terminal**
2. **aaa authorization ssh-certificate default** { **group** *group-list* [**none**] | **local** | **none**}
3. **exit**
4. (Optional) **show aaa authorization** [**all**]
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`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 ssh-certificate default** { **group** *group-list* [**none**]	**local**	**none**} **Example:** `switch(config)# aaa authorization ssh-certificate default group ldap1 ldap2`	LDAP サーバのデフォルトの AAA 許可方式を設定します。 **ssh-certificate** キーワードは、証明書認証を使用した LDAP許可またはローカル許可を設定します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。 *group-list* 引数には、LDAP サーバ グループ名をスペースで区切ったリストを指定します。このグループに属するサーバに対して、AAA許可のためのアクセスが行われます。**local** 方式では、ローカル データベースを認証に使用します。**none** 方式では、AAA認証が使用されないように指定します。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		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	(Optional) **show aaa authorization** [**all**] **Example:** `switch# show aaa authorization`	AAA 許可設定を表示します。**all** キーワードを指定すると、デフォルト値が表示されます。

	Command or Action	Purpose
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	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。

TACACS サーバでの AAA SSH 証明書認証の構成

TACACS サーバーに AAA SSH 証明書認証を設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **aaa authorization ssh-certificate default** { **group** *group-list* [**none**] | **local** | **none**}
3. **exit**
4. （任意） **show aaa authorization** [**all**]
5. （任意） **copy running-config startup-config**

手順の詳細

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 ssh-certificate default** { **group** *group-list* [**none**]	**local**	**none**} 例： `switch(config)# aaa authorization ssh-certificate default group tac1`	TACACS サーバー グループとして X509 証明書を持つ SSH 要求のデフォルトの AAA 認証方式を設定します。 **ssh-certificate** キーワードは、証明書認証を使用した TACACS 許可またはローカル許可を構成します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。 *group-list* 引数には、TACACS サーバ グループの名前をスペースで区切ったリストを指定します。このグループに属するサーバに対して、AAA 許可のためのアクセスが行われます。**local** 方式では、ローカル データベースを認証に使用します。**none** 方式では、AAA 認証が使用されないように指定します。

	コマンドまたはアクション	目的

ステップ 3	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		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	（任意） **show aaa authorization** [**all**] 例： `switch# show aaa authorization`	AAA 許可設定を表示します。**all** キーワードを指定すると、デフォルト値が表示されます。
ステップ 5	（任意） **copy running-config startup-config** 例： `switch# copy running-config startup-config`	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、ユーザー 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 サーバーまたは RADIUS セキュリティ サーバーに報告します。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 サーバーに格納されます。

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 サーバー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 サーバー グループ：RADIUS サーバーのグローバル プールをアカウンティングに使用します。
- 特定のサーバー グループ：指定した RADIUS または TACACS+ サーバー グループをアカウンティングに使用します。
- ローカル：ユーザー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。

Note サーバー グループが設定されていて、そのサーバー 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。

Before you begin

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+ サーバー グループを設定します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **aaa accounting default** { **group** *group-list* | **local**}
3. switch(config)# **exit**
4. (Optional) switch# **show aaa accounting**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
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ー 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。 • **radius** RADIUS サーバーのグローバル プールを使用してアカウンティングを行います。 • *named-group* を指定すると、TACACS+ サーバーまたは RADIUS サーバー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** 方式はローカル データベースを使用してアカウンティングを行います。 デフォルトの方式は **local** です。サーバー 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ー グループから応答がないときに、このデフォルトの方式が使用されます。
ステップ 3	switch(config)# **exit**	コンフィグレーション モードを終了します。
ステップ 4	(Optional) switch# **show aaa accounting**	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。

	Command or Action	Purpose
ステップ 5	(Optional) switch# **copy running-config startup-config**	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。

No Service Password-Recovery について

No Service Password-Recovery 機能により、コンソールへのアクセスを持つ誰もがルータおよびルータのネットワークにアクセスする機能を与えられることになります。

No Service Password-Recovery のイネーブル化

No Service Password-Recovery 機能が有効になっている場合、ネットワーク権限を持つ管理者以外は管理者パスワードを変更できません。

始める前に

no service password-recovery コマンドを開始する場合、シスコでは、デバイスから離れた場所にシステム コンフィギュレーション ファイルのコピーを保存することを推奨しています。

手順の概要

1. **configure terminal**
2. **no service password-recovery**
3. （任意） **copy running-config startup-config**
4. **Reload**
5. **exit**
6. （任意） **show user-account**
7. （任意） **copy running-config startup-config**

手順の詳細

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	**no service password-recovery**
	例：
	`switch(config)# no service password-recovery`
	`WARNING: Executing this command will disable the password recovery mechanism. Do not execute this`
		パスワード回復メカニズムを無効にします。

	コマンドまたはアクション	目的
	command without another plan for password recovery. Are you sure you want to continue? (y/n) : [y] y switch(config)# copy run start [##] 100% Copy complete, now saving to disk (please wait)... Copy complete.	
ステップ 3	（任意） **copy running-config startup-config** 例： switch# copy running-config startup-config	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。
ステップ 4	**Reload** 例： switch(config)# Reload This command will reboot the system. (y/n)? [n] y 2018 Jun 26 16:23:19 BAR %$ VDC-1 %$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line Interface CISCO SWITCH Ver 8.34 CISCO SWITCH Ver 8.34 Manual system restart from Command Line Interface writing reset reason 9, ... switch(boot)# config t Enter configuration commands, one per line. End with CNTL/Z. switch(boot)(config)# admin-password Abcd!123$ ERROR: service password-recovery disabled. Cannot change password! switch(boot)(config)#	
ステップ 5	**exit** 例： switch(config)# exit switch#	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 6	（任意） **show user-account** 例： switch# show user-account	ロール設定を表示します。
ステップ 7	（任意） **copy running-config startup-config** 例： switch# copy running-config startup-config	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 サーバーの VSA の使用

VSA

ベンダー固有属性（VSA）を使用して、AAA サーバー上でのCisco Nexus デバイスのユーザー 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 サーバーを使用する場合は、認証結果とともに許可情報などのユーザー属性を返すよう、RADIUS プロトコルが RADIUS サーバーに指示します。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：ユーザー 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：ユーザー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 サーバー上でのスイッチのユーザー ロールと SNMPv3 パラメータの指定

AAA サーバーで VSA cisco-av-pair を使用して、次の形式で、Cisco Nexus デバイスのユーザー 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ー ロールは、network-operator です。

Note Cisco Unified Wireless Network TACACS+ 設定と、ユーザー 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

セキュア ログインの機能拡張

Cisco NX-OS では、次のセキュアなログイン拡張機能がサポートされています：

- ログイン パラメータの設定
- ログイン パラメータの設定例
- ユーザー 1 人あたりのセッション数の制限（ユーザー 1 人あたり、ログイン 1 回あたり）
- ユーザー名のパスワード プロンプトの有効化
- RADIUS/TACACS+ を使用するための共有キー値の設定

ログイン パラメータの設定

Cisco NX-OS デバイスへの DoS 攻撃の疑いを検出し、辞書攻撃による影響の緩和に役立つログイン パラメータを設定するには、ここに示す手順を実行します。

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有効にする **login block-for** コマンドを入力する必要があります。**login block-for** コマンドを有効にすると、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、**login quiet-mode access-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。

手順の概要

1. **configure terminal**

2. **[no] login block-for** *seconds* **attempts** *tries* **within** *seconds*
3. **[no] login quiet-mode access-class** {*acl-name* | *acl-number*}
4. **exit**
5. **show login failures**

手順の詳細

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] login block-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 パラメータを構成します。 （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] login quiet-mode access-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。デバイスが待機モードになっている間は、すべてのログイン要求が拒否され、使用できる接続はコンソール経由の接続のみになります。
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 login failures** 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.***
```

ユーザー1人あたりのセッション数の制限（ユーザー1人あたり、ログイン1回あたり）

このタスクは、ユーザーごとの最大セッション数を制限するために使用します。

手順の概要

1. **configure terminal**
2. **[no] user max-logins** *max-logins*
3. **exit**

手順の詳細

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] user max-logins** *max-logins* 例： `Switch(config)# user max-logins 1`	ユーザー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。最大ログイン制限を 1 に設定すると、ユーザー 1 人あたりのセッション数（telnet/SSH）が 1 に制限されます。
ステップ 3	**exit** 例： `Switch(config)# exit`	特権 EXEC モードに戻ります。

ユーザー名のパスワード プロンプトの有効化

手順の概要

1. **configure terminal**
2. **[no] password prompt username**
3. **exit**

手順の詳細

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。

	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 ノブを有効にします。このコマンドが有効ににになっている場合、ユーザーが **username** コマンドをパスワードオプションなしで入力すると、パスワードを入力するよう求められます。パスワードの入力には隠し文字を使用できます。ログイン パスワード入力要求を無効にするには、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。

RADIUS/TACACS+ を使用するための共有キー値の設定

リモート認証およびアカウンティング用に設定する共有秘密は非表示にする必要があります。**radius-server key** および **tacacs-server key** コマンドでは、別のコマンドを使用して暗号化された共有秘密を使用できます。

手順の概要

1. **configure terminal**
2. **generate type7_encrypted_secret**
3. **exit**

手順の詳細

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	**generate type7_encrypted_secret** 例： `Switch(config)# generate type7_encrypted_secret`	キー タイプ 7 で RADIUS および TACACS の共有秘密を構成します。暗号化された共有秘密を生成する間はユーザー入力が非表示になります。 （注） プレーン テキストから暗号化された文字列を別個に生成して、暗号化された共有秘密を後から設定することもできます。

	コマンドまたはアクション	目的
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。

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
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	(Optional) switch# **clear accounting log**	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。
show aaa authentication [**login** {**error-enable** |**mschap**}]	AAA 認証情報を表示します。

コマンド	目的
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 login [**failures**]	ログイン パラメータを表示します。**failures** オプションは、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。 **Note** **clear login failures** コマンドは、現在の監視期間内のログイン失敗をクリアします。
show login on-failure log	syslog サーバに対して認証失敗メッセージをログ記録するようにスイッチが設定されているか表示します。
show login on-successful log	syslog サーバに対して認証成功メッセージをログ記録するようにスイッチが設定されているか表示します。
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 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 running-config all | i max-login	ユーザ 1 人あたりの最大同時セッション数を表示します。
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。
show userpassphrase {**length** | **max-length** | **min-length**}	ユーザ パスワードの最小長と最大長を表示します。

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。

Table 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	ローカル
アカウンティング ログの表示サイズ	250 KB

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。