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。

この章は、次の項で構成されています。

AAA について

ここでは、Cisco NX-OS デバイスの AAA 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、Cisco 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 System 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。Cisco NX-OS デバイスと AAA サーバの間の通信は、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

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、Cisco 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。

許可

アクセス コントロールを提供します。AAA 許可は、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てるプロセスです。Cisco 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属性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

情報を収集する、情報をローカルのログに記録する、情報を AAA サーバに送信して課金、監査、レポート作成などを行う方法を提供します。

アカウンティング機能では、Cisco 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、トラブルシューティングや監査のためのレポートを生成できます。アカウンティング ログは、ローカルに保存することもできれば、リモート AAA サーバに送信することもできます。

Note Cisco NX-OS ソフトウェアでは、認証、許可、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 Cisco 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 Cisco 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 Cisco NX-OS デバイスについてユーザ属性を管理する方が、Cisco NX-OS デバイスのローカル データベースを使用するより簡単です。

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。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くなったときにフェールオーバー サーバを提供することです。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。Cisco NX-OS デバイスは、最初のグループ内のサーバからエラーを受け取った場合、次のサーバ グループ内のサーバで試行します。

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。

- 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。

***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**

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
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。

すべての RADIUS サーバ

RADIUS サーバのグローバル プールを使用して認証を行います。

指定サーバ グループ

設定した特定の RADIUS、TACACS+、または LDAP サーバ グループを使用して認証を行います。

ローカル

ローカルのユーザ名またはパスワード データベースを使用して認証を行います。

なし

AAA 認証が使用されないように指定します。

Note 「指定サーバ グループ」方式でなく、「すべての RADIUS サーバ」方式を指定した場合、Cisco NX-OS デバイスは、設定された 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 プールからのサーバは、Cisco NX-OS 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 サービスに対応して設定できる AAA 認証方式を示します。

***Table 2: AAA* サービスの *AAA* 認証方式**

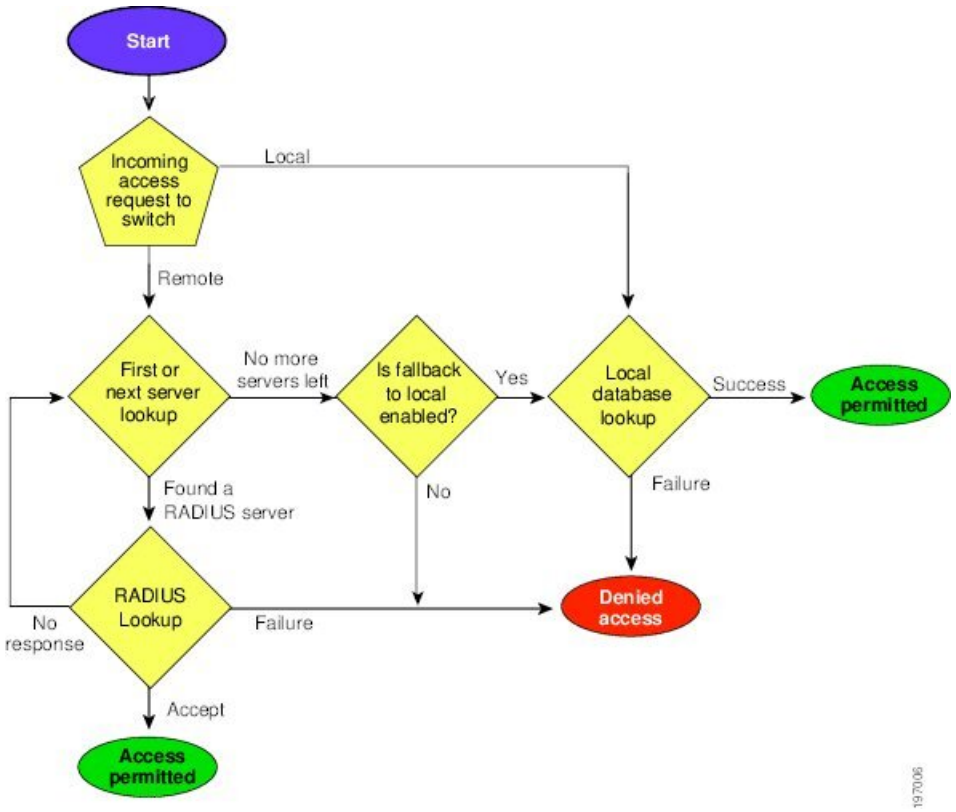
AAA サービス	AAA の方式
コンソール ログイン認証	サーバ グループ、ローカル、なし
ユーザ ログイン認証	サーバ グループ、ローカル、なし
ユーザ管理セッション アカウンティング	サーバ グループ、ローカル

Note 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 アカウンティングについて、Cisco NX-OS 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。コンソールまたはデフォルト ログインのローカル オプションを無効にするには、**no aaa authentication login** {**console** | **default**} **fallback error local** コマンドを使用します。

ユーザ ログインの認証および許可プロセス

図 *1*: ユーザ ログインの認証および許可フロー

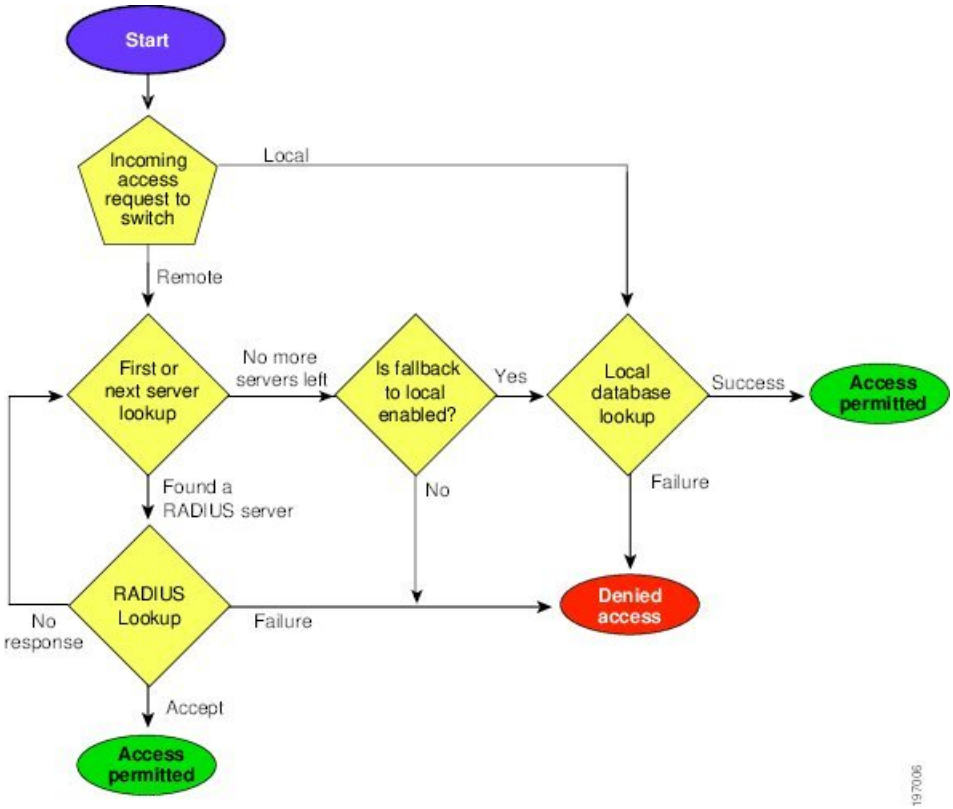
次の図に、ユーザ ログインの認証および許可プロセスのフローチャートを示します。



process_workflow

図 *2:* ユーザ ログインの認証および許可フロー

次の図に、ユーザ ログインの認証および許可プロセスのフローチャートを示します。



次に、このプロセスの動作を示します。

- Telnet、SSH、またはコンソールを使用して Cisco NX-OS デバイスにログインします。
- サーバ グループ認証方式を使用して AAA サーバ グループを構成します。そして、デバイスは、 最初の AAA サーバに要求を送信します。
  - 特定の AAA サーバが応答しなかった場合は、その次の AAA サーバーが試行されます。この処理は、リモート サーバが認証要求に応答するまで続けられます。
  - 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。
  - コンソール ログイン フォールバックが無効で構成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 NX-OS デバイスがリモート AAA サーバ経由で正常に認証を実行した場合は、これらの可能性が適用する場合があります：
  - 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ー ロールが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、デバイスにログインでき、ローカル データベース内で構成されているロールが割り当てられます。

（注） 「残りのサーバ グループなし」とは、すべてのサーバ グループのいずれのサーバからも応答がないということです。「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。

AES パスワード暗号化およびプライマリ暗号キー

強力で、反転可能な 128 ビットの高度暗号化規格（AES）パスワード暗号化（タイプ 6 暗号化ともいう）を有効にすることができます。タイプ 6 暗号化の使用を開始するには、AES パスワード暗号化機能を有効にし、パスワード暗号化および復号化に使用されるプライマリ暗号キーを設定する必要があります。

AES パスワード暗号化をイネーブルにしてプライマリ キーを設定すると、タイプ 6 パスワード暗号化を無効にしない限り、サポートされているアプリケーション（現在は RADIUS と TACACS+）の既存および新規作成されたクリア テキスト パスワードがすべて、タイプ 6 暗号化の形式で保存されます。また、既存の弱いすべての暗号化パスワードをタイプ 6 暗号化パスワードに変換するように Cisco NX-OS を設定することもできます。

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、TACACS+ サーバ、または LDAP サーバが IP を使用して到達可能であることを確認します。
- Cisco 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。
- 秘密キーが、Cisco 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を確認します。
- リモート サーバが Cisco NX-OS デバイスからの AAA 要求に応答することを確認します。

AAA の注意事項と制約事項

AAA に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OSリリース10.2（1）F以降では、cisco-av-pairのshell：roles属性の前にSNMPV3属性を指定できます。
- LDAPは「snmpv3」属性をサポートしていません。
- 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 ロールではなく、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。
- Cisco Nexus 9000 シリーズスイッチは、TACACS +でのみ **aaa authentication login ascii-authentication** コマンドをサポートします（RADIUS ではサポートしません）。
- デフォルトのログイン認証方式を（**local** キーワードを使用せずに）変更すると、コンソール ログイン認証方式が設定によって上書きされます。コンソール認証方式を明示的に設定するには、**aaa authentication login console** {**group** *group-list* [**none**] | **local** | **none**} コマンドを使用します。
- **login block-for** および **login quiet-mode** コンフィギュレーション モード コマンドは、それぞれ **system login block-for** および **system login quiet-mode** に名前が変更されました。
- **system login quiet-mode access-class QUIET_LIST** コマンドを使用する場合は、指定したトラフィックのみをブロックするようにアクセス リストが正しく定義されていることを確認する必要があります。たとえば、信頼できないホストからのユーザ ログインのみをブロックする必要がある場合、アクセス リストは、それらのホストからのSSH、Telnet、および HTTP ベースのアクセスに対応するポート22、23、80、および 443 を指定する必要があります。
- Cisco NX-OS Release 10.2(2)F 以降、新しい非同期化 CLI が導入され、SNMP とセキュリティ コンポーネントの間のユーザー同期を無効にするオプションを提供します。詳細については、システム管理構成ガイドの *SNMP* の構成の章を参照してください。

  リリース 7.0(3)I7(1) から現在のリリースまでのさまざまな機能をサポートする Cisco Nexus 9000 スイッチの詳細については、Nexus スイッチ プラットフォーム サポート マトリックスを参照してください。
- 非同期 CLI が有効になっている場合、リモート ユーザーは SNMP データベースに同期されません。
- DCNM（リリース 12.0.1.a 以降 Nexus Dashboard Fabric Controller とも呼ばれる）を使用したセキュリティ ユーザーには、非同期 CLI が有効でないとき、対応する SNMPv3 プロファイルが存在しません。同期が無効になっている場合、セキュリティ コンポーネントで作成されたユーザーはスイッチにログインできますが、コントローラはスイッチを検出しません。コントローラは、セキュリティ ユーザー用に作成された SNMP 構成を使用してスイッチを検出するためです。さらに、SNMP は、userDB の非同期状態のため、作成されたセキュリティ ユーザーを認識しないので、スイッチを検出できません。したがって、コントローラによってスイッチが検出されるようにするには、SNMP ユーザーを明示的に作成する必要があります。DCNM 機能とともに非同期 CLI を使用することはお勧めしません。詳細については、*Cisco Nexus 9000 NX-OS* セキュリティ構成ガイドを参照してください。

- Cisco NX-OS リリース 10.3(1)F 以降、AAA は Cisco Nexus 9808 スイッチでサポートされます。
  - Cisco NX-OS リリース 10.4(1)F 以降、AAA は、Cisco Nexus X98900CD-A および X9836DM-A ライン カードを搭載した 9808 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、AAA は、X98900CD-A および X9836DM-A ライン カードを搭載した Cisco Nexus 9804 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(3)F 以降、TACACS+ サーバーを使用した X.509 証明書の SSH ベースの認証が、Cisco Nexus 9000 シリーズ プラットフォーム スイッチでサポートされます。この機能は、 **aaa authorization ssh-certificate default group** *tac-group-name* コマンドを使用して有効にできます。詳細については、「TACACS サーバでの AAA SSH 証明書認証の構成, on page 25」を参照してください。

AAA のデフォルト設定

次の表に、AAA パラメータのデフォルト設定を示します。

***Table 3: AAA* パラメータのデフォルト設定**

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
CHAP 認証	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

AAA の設定

ここでは、Cisco NX-OS デバイスで AAA 機能を設定する手順について説明します。

Note Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

Note Cisco Nexus 9K シリーズ スイッチは、TACAAS+ に対してのみ CLI コマンド aaa authentication login ascii-authentication をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、aaa authentication login ascii-authentication スイッチが無効になっていることを確認します。そうしないと、syslog エラーが表示されます。

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。

1. 認証にリモート RADIUS、TACACS+、または LDAP サーバを使用する場合は、Cisco NX-OS デバイス上でホストを設定します。
2. コンソール ログイン認証方式を設定します。
3. ユーザ ログインのためのデフォルトのログイン認証方式を設定します。
4. デフォルト AAA アカウンティングのデフォルト方式を設定します。

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方法を説明します。

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、TACACS+、または LDAP サーバの指定サブセット
- Cisco NX-OS デバイスのローカル データベース
- ユーザ名のみ（none）

デフォルトの方式はローカルですが、無効にするオプションがあります。

Note **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。

Note リモート認証がイネーブルになっているときにパスワード回復を実行すると、パスワード回復の実行後すぐにコンソール ログインのローカル認証がイネーブルになります。そのため、新しいパスワードを使用して、コンソール ポート経由で Cisco NX-OS デバイスにログインできます。ログイン後は、引き続きローカル認証を使用するか、または AAA サーバで設定された管理者パスワードのリセット後にリモート認証をイネーブルにすることができます。パスワード回復プロセスに関する詳細情報については、『*Cisco Nexus 9000* シリーズ *NX-OS* トラブルシューティング ガイド』を参照してください。

Before you begin

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

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**aaa authentication login console** {**group** *group-list* [**none**] | **local** | **none**} **Example:** `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 サーバのグローバル プールを使用して認証を行います。 ***named-group*** RADIUS、TACACS+、または LDAP サーバの指定サブセットを使用して認証を行います。 **local** 方式は、ローカル データベースを認証に使用します。**none** 方式では、AAA 認証が使用されないように指定します。 デフォルトのコンソール ログイン方式は **local** です。これは、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い場合に、コンソール ログインに対して

	Command or Action	Purpose
		ローカルへのフォール バックが無効でない限り、使用されます。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show aaa authentication** **Example:** `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) **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。

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、TACACS+、または LDAP サーバの指定サブセット
- Cisco NX-OS デバイスのローカル データベース
- ユーザ名だけ

デフォルトの方式はローカルですが、無効にするオプションがあります。

Before you begin

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

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**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。

	Command or Action	Purpose
	Example: `switch(config)# aaa authentication login default group radius`	*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 サーバのグローバル プールを使用して認証を行います。 • *named-group*：認証に RADIUS、TACACS+ または LDAP サーバの名前付きサブセットを使用します。 **local** 方式は、ローカル データベースを認証に使用します。**none** 方式では、AAA 認証が使用されないように指定します。デフォルトのログイン方式は**local** です。これは、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い場合に、コンソール ログインに対してローカルへのフォール バックがディセーブルでない限り、使用されます。 次のいずれかを設定できます。 • AAA 認証グループ • 認証なしの AAA 認証グループ • ローカル認証 • 認証なし **Note** **local** キーワードは、AAA 認証グループを設定するときはサポートされません（必須ではありません）。これは、ローカル認証は、リモート サーバが到達不能の場合のデフォルトであるためです。たとえば、**aaa authentication login default group g1** を設定した場合、AAA グループ g1 を使用して認証を行うことができなければ、ローカル認証が試行されます。これに対し、**aaa authentication login default group g1 none** を設定した場合、AAA グループ g1 を使用して認証を行うことができなければ、認証は実行されません。

	Command or Action	Purpose
		Note Cisco NX-OS AAA 認証はハッシュ キーをサポートせず、タイプ 6/7 キーのみをサポートします。

ステップ 3	**exit**
	Example:
	`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	(Optional) **show aaa authentication** **Example:** `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) **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。

ローカル認証へのフォールバックの無効化

デフォルトでは、コンソール ログインまたはデフォルト ログインのリモート認証が設定されている場合、どの AAA サーバにも到達不能なときに（認証エラーになります）、ユーザが Cisco NX-OS デバイスからロックアウトされないように、ローカル認証にフォールバックされます。ただし、セキュリティを向上させるために、ローカル認証へのフォールバックを無効にできます。

Caution ローカル認証へのフォールバックを無効にすると、Cisco NX-OS デバイスがロックされ、パスワード回復を実行しないとアクセスできなくなることがあります。デバイスからロックアウトされないようにするために、ローカル認証へのフォールバックを無効にする対象は、デフォルト ログインとコンソール ログインの両方ではなく、いずれかだけにすることを推奨します。

Before you begin

コンソール ログインまたはデフォルト ログインのリモート認証を設定します。

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:**	コンフィギュレーション モードに入ります。

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
ステップ 2	**no aaa authentication login** {**console** | **default**} **fallback error local** **Example:** `switch(config)# no aaa authentication login console fallback error local`	コンソール ログインまたはデフォルト ログインについて、リモート認証が設定されている場合にどの AAA サーバにも到達不能なときに実行されるローカル認証へのフォールバックを無効にします。 ローカル認証へのフォールバックを無効にすると、次のメッセージが表示されます。 `"WARNING!!! Disabling fallback can lock your switch."`

ステップ 3	(Optional) **exit**
	Example:
	`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	(Optional) **show aaa authentication** **Example:** `switch# show aaa authentication`	コンソール ログインおよびデフォルト ログイン認証方式の設定を表示します。
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。

AAA 認証のデフォルト ユーザ ロールのイネーブル化

ユーザ ロールを持たないリモート ユーザに、デフォルトのユーザ ロールを使用して、RADIUS または TACACS+ リモート認証による Cisco NX-OS デバイスへのログインを許可できます。AAA のデフォルトのユーザ ロール機能をディセーブルにすると、ユーザ ロールを持たないリモート ユーザはデバイスにログインできなくなります。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	Command or Action	Purpose
ステップ 2	**aaa user default-role** **Example:** `switch(config)# aaa user default-role`	AAA 認証のためのデフォルト ユーザ ロールをイネーブルにします。デフォルトではイネーブルになっています。 デフォルト ユーザ ロールの機能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**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	(Optional) **show aaa user default-role** **Example:** `switch# show aaa user default-role`	AAA デフォルト ユーザ ロールの設定を表示します。
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。

ログイン認証失敗メッセージの有効化

ログイン時にリモート AAA サーバが応答しない場合、そのログインは、ローカル ユーザ データベースにロール オーバーして処理されます。このような場合に、ログイン失敗メッセージが有効になっていると、次のメッセージがユーザの端末に表示されます。

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

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

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**aaa authentication login error-enable** **Example:** `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。

	Command or Action	Purpose

ステップ 3	**exit**
	Example:
	`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	(Optional) **show aaa authentication** **Example:** `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) **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。

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

	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`	ロギング レベルが 6 に設定されている場合のみ、失敗した認証に関するすべてのメッセージを設定済みの syslog サーバに記録します。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

	コマンドまたはアクション	目的
		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。

ステップ 3	必須: [**no**] **login on-success log**
	例：
	`switch(config)# login on-success log`
	`switch(config)# logging level authpriv 6`
	`switch(config)# logging level daemon 6`
		ロギング レベルが 6 に設定されている場合のみ、成功した認証に関するすべてのメッセージを設定済みの syslog サーバに記録します。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。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。

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。

ユーザごとのログイン ブロックの設定

スイッチがグローバル コンフィギュレーション モードになっていることを確認します。

ユーザごとのログインブロック機能を使用すると、Denial of Service（DoS）攻撃の疑いを検出して、辞書攻撃の影響を緩和することができます。この機能はローカルおよびリモートユーザ

に適用されます。ログインに失敗した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するには、ここに示す手順を実行します。

（注） リリース 9.3(7) 以降では、リモート ユーザのログイン ブロックを設定できます。

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	**aaa authentication rejected** *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） デフォルトのログイン パラメータに戻すには **no aaa authentication rejected** コマンドを使用します。
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	（任意） **show running config** 例： `switch# show running config`	ログイン パラメータを表示します。
ステップ 5	**show aaa local user blocked** 例： `switch# show aaa local user blocked`	ブロックされたローカル ユーザを表示します。
ステップ 6	**clear aaa local user blocked {username user| all}** 例： `switch(config)# switch# clear aaa local user blocked username testuser`	ブロックされたローカル ユーザをクリアします。 all：ブロックされたすべてのローカル ユーザをクリアします。
ステップ 7	**show aaa user blocked** 例： `switch(config)# show aaa user blocked`	ブロックされたすべてのローカル ユーザとリモート 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 8	（任意） **clear aaa user blocked{username user| all}** 例： `switch# clear aaa user blocked username testuser`	ブロックされたすべてのローカル ユーザとリモート ユーザをクリアします。 all：ブロックされたすべてのローカル ユーザとリモート ユーザをクリアします。

例

（注） network-admin および vdc-admin だけが show および clear コマンドを実行できます。

次に、20 秒の間に 3 回のログイン試行が失敗した場合に、300 秒間ユーザをブロックするログイン パラメータを設定する例を示します。

```
switch(config)# aaa authentication rejected 3 in 20 ban 300
switch# show run | i rejected
aaa authentication rejected 3 in 20 ban 300
switch# show aaa local user blocked
Local-user                  State
testuser                    Watched (till 11:34:42 IST Nov 12 2020)
switch# clear aaa local user blocked username testuser
switch# show aaa user blocked
Local-user                  State
testuser                    Watched (till 11:34:42 IST Nov 12 2020)
switch# clear aaa user blocked username testuser
```

CHAP 認証の有効化

Cisco NX-OS ソフトウェアは、チャレンジ ハンドシェーク認証プロトコル（CHAP）をサポートしています。このプロトコルは、業界標準の Message Digest（MD5）ハッシュ方式を使用して応答を暗号化する、チャレンジ レスポンス認証方式のプロトコルです。リモート認証サーバ（RADIUS または TACACS+）を通じて、Cisco NX-OS スイッチへのユーザ ログインに CHAP を使用できます。

デフォルトでは、Cisco NX-OS デバイスは、Cisco NX-OS デバイスとリモート 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。CHAP が有効の場合は、CHAP ベンダー固有属性（VSA）を認識するように RADIUS サーバまたは TACACS+ サーバを設定する必要があります。

Note Cisco Nexus 9K シリーズ スイッチは、TACAAS+ に対してのみ CLI コマンド aaa authentication login ascii-authentication をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、aaa authentication login ascii-authentication スイッチが無効になっていることを確認します。そうしないと、syslog エラーが表示されます。次に例を示します。

```
2017 Jun 14 16:14:15 N9K-1 %RADIUS-2-RADIUS_NO_AUTHEN_INFO: ASCII authentication not
supported
2017 Jun 14 16:14:16 N9K-1 %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed from
192.168.12.34 - dcos_sshd[16804]
```

次の表に、CHAP に必要な RADIUS および TACACS+ VSA を示します。

Table 4: CHAP RADIUS* および *TACACS+ VSA

ベンダー ID 番号	ベンダータイプ番号	VSA	説明
311	11	CHAP-Challenge	AAA サーバから CHAP 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	CHAP-Response	チャレンジに対する応答として CHAP ユーザが入力した値を保持します。Access-Request パケットだけで使用します。

Before you begin

ログイン用の AAA ASCII 認証を無効にします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**no aaa authentication login ascii-authentication** **Example:** `switch(config)# no aaa authentication login ascii-authentication`	ASCII 認証を無効にします。

	Command or Action	Purpose
ステップ 3	**aaa authentication login chap enable** **Example:** `switch(config)# aaa authentication login chap enable`	CHAP認証を有効にします。デフォルトでは無効になっています。 **Note** Cisco NX-OS デバイスで、CHAP と MSCHAP（または MSCHAP V2）の両方を有効にすることはできません。

ステップ 4	(Optional) **exit**
	Example:
	`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 5	(Optional) **show aaa authentication login chap** **Example:** `switch# show aaa authentication login chap`	CHAP の設定を表示します。
ステップ 6	(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。

MSCHAP または MSCHAP V2 認証の有効化

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。Cisco NX-OS ソフトウェアは、MSCHAP Version 2（MSCHAP V2）にも対応しています。リモート認証サーバ（RADIUS または TACACS+）を通じて、Cisco NX-OS スイッチへのユーザ ログインに MSCHAP を使用できます。MSCHAP V2 では、リモート認証 RADIUS サーバを介した Cisco NX-OS デバイスへのユーザ ログインだけがサポートされます。MSCHAP V2 の場合に TACACS+ グループを設定すると、デフォルトの AAA ログイン認証では、次に設定されている方式が使用されます。他のサーバ グループが設定されていない場合は、ローカル方式が使用されます。

Note Cisco NX-OS ソフトウェアは、次のメッセージを表示する場合があります。

「Warning: MSCHAP V2 is supported only with Radius.」

この警告メッセージは単なる情報メッセージであり、RADIUS での MSCHAP V2 の動作には影響しません。

デフォルトでは、Cisco NX-OS デバイスは、Cisco NX-OS デバイスとリモート 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 または MSCHAP V2 を有効にする場合は、MSCHAP および MSCHAP V2 ベンダー固有属性（VSA）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。

Table 5: MSCHAP* および *MSCHAP V2 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 または MSCHAP V2 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 または MSCHAP V2 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。

Before you begin

ログイン用の AAA ASCII 認証を無効にします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**no aaa authentication login ascii-authentication** **Example:** `switch(config)# no aaa authentication login ascii-authentication`	ASCII 認証を無効にします。
ステップ 3	**aaa authentication login** {**mschap** | **mschapv2**} **enable** **Example:** `switch(config)# aaa authentication login mschap enable`	MSCHAP または MSCHAP V2 認証を有効にします。デフォルトでは無効になっています。 **Note**

	Command or Action	Purpose
		Cisco NX-OS デバイスで、MSCHAP と MSCHAP V2 の両方を有効にすることはできません。

ステップ 4	**exit**
	Example:
	`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 5	(Optional) **show aaa authentication login** {**mschap** | **mschapv2**} **Example:** `switch# show aaa authentication login mschap`	MSCHAP または MSCHAP V2 の設定を表示します。
ステップ 6	(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。

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。

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

	Command or Action	Purpose
		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。
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。

Related Topics

TACACS+ のイネーブル化

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

	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

	コマンドまたはアクション	目的
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。

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 NX-OS ソフトウェアは、アカウンティングに TACACS+ 方式と RADIUS 方式をサポートします。Cisco NX-OS デバイスは、ユーザー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 サーバーにレポートします。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、CiscoNX-OS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リストを作成できます。次の方式を含めることができます。

RADIUS サーバ グループ
RADIUS サーバのグローバル プールを使用してアカウンティングを行います。

指定されたサーバ グループ
指定された RADIUS または TACACS+ サーバ グループを使用してアカウンティングを行います。

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使用してアカウンティングを行います。

Note 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。

Before you begin

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

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**aaa accounting default** {**group** *group-list* | **local**} **Example:** `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*：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。

	Command or Action	Purpose
		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**
	Example:
	`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	(Optional) **show aaa accounting** **Example:** `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。
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。

Cisco NX-OS デバイスによる AAA サーバの VSA の使用

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

VSA の概要

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 separator value *
```

protocol は、特定の許可タイプを表すシスコの属性です。separator は、必須属性の場合は =（等号）、オプションの属性の場合は *（アスタリスク）です。

Cisco NX-OS 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 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 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たすべてのロールの一覧です。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。たとえば、ユーザが network-operator および network-admin のロールに属している場合、値フィールドは network-operator network-admin となります。このサブ属性は 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。この属性は shell プロトコル値とだけ併用できます。次に、ロール属性を使用する例を示します。

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

次に、FreeRADIUS でサポートされるロール属性の例を示します。

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

Note VSA を、shell:roles*"network-operator network-admin" または "shell:roles*\"network-operator network-admin\"" として指定した場合、この VSA はオプション属性としてフラグ設定され、他のシスコ デバイスはこの属性を無視します。

accountinginfo
標準の RADIUS アカウンティング プロトコルに含まれる属性とともにアカウンティング情報を格納します。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 Cisco NX-OS のユーザ ロールおよび SNMPv3 パラメータの指定

AAA サーバで VSA 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 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。

SNMPv3属性は、シェル属性の前または後のいずれかにまとめます。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。

```
snmpv3:auth=”SHA” priv=”AES-128” shell:roles="network-admin" shell:priv-lvl=15
```

```
shell:roles="network-admin" shell:priv-lvl=15 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。

セキュア ログイン機能の設定

ログイン パラメータの設定

可能性のあるサービス妨害（DoS）攻撃が検出された場合に、それ以降のログイン試行を自動的にブロックし、複数回の接続試行の失敗が検出された場合に待機期間を適用することでディクショナリ攻撃を遅らせるように、ログインパラメータを設定できます。

（注） この機能は、システム スイッチオーバーが発生した場合、またはAAA プロセスが再起動した場合に再起動します。

（注） **login block-for** および **login quiet-mode** コンフィギュレーションモードコマンドは、それぞれ **system login block-for** および **system login quiet-mode** に名前が変更されました。

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**] **system login block-for** *seconds* **attempts** *tries* **within** *seconds* 例： `switch(config)# system login block-for 100 attempts 2 within 60`	待機モード期間を設定します。すべての引数の範囲は 1 ～ 65535 です。 60 秒以内に 2 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。

	コマンドまたはアクション	目的
		このコマンドを入力すると、TelnetまたはSSHを介したすべてのログイン試行は、待機期間中に拒否されます。アクセス コントロール リスト (ACL) も、**system** コマンドが入力されます。 （注） 他のログインコマンドを使用する前に、このコマンドを入力する必要があります。
ステップ 3	（任意） [**no**] **system login quiet-mode access-class** *acl-name* 例： `switch(config)# system login quiet-mode access-class myacl`	待機モードに切り替わるときに、スイッチに適用される ACL を指定します。スイッチ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	（任意） **show system login** [**failures**] 例： `switch(config)# show system login`	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。
ステップ 5	（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。

ユーザ ログイン セッションの制限

ユーザ1人あたりのあたりの同時ログインセッションの最大数を制限することができます。これにより、ユーザが複数の不要なセッションを持つことを防止し、有効なSSHまたはTelnetセッションにアクセスする不正ユーザの潜在的なセキュリティ問題を解決します。

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	[**no**] **user max-logins** *max-logins* 例：	ユーザ 1 人あたりの最大同ログイン 時セッション数を制限します。指定できる

	コマンドまたはアクション	目的
	`switch(config)# user max-logins 1`	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1人あたりのTelnetまたはSSHセッションが1に制限されます。 （注） 設定されたログイン制限は、すべてのユーザに適用されます。個々のユーザに異なる制限を設定することはできません。
ステップ3	（任意） **show running-config all | i max-login** 例： `switch(config)# 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。
ステップ4	（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。

パスワードの長さの制限

ユーザパスワードの最小長と最大長を制限できます。この機能を使用すると、ユーザに強力なパスワードの入力を強制することで、システムのセキュリティを強化できます。

始める前に

パスワードの強度の確認を有効にするには、**password strength-check** コマンドを使用する必要があります。パスワードの長さを制限したが、パスワード強度チェックを有効にせず、ユーザが制限された長さの範囲内にないパスワードを入力すると、エラーが表示されますが、ユーザアカウントが作成されます。パスワードの長さを適用し、ユーザアカウントが作成されないようにするには、パスワード強度チェックを有効にし、パスワードの長さを制限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`	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**] **userpassphrase** {**min-length** *min-length* | **max-length** *max-length*} 例： `switch(config)# userpassphrase min-length 8 max-length 80`	ユーザ パスワードの最小長または最大長を制限します。パスワードの最小長は 4 ～ 127 文字にすることができます。パスワードの最大長は 80 ～ 127 文字です。
ステップ 3	（任意） **show userpassphrase** {**length** | **max-length** | **min-length**} 例： `switch(config)# show userpassphrase length`	ユーザ パスワードの最小長と最大長を表示します。
ステップ 4	（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。

ユーザ名のパスワード プロンプトのイネーブル化

ユーザによるユーザ名入力後にパスワード入力を要求するように、スイッチを設定できます。

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	**password prompt username**
	例：
	`switch(config)# password prompt username`
	`Password prompt username is enabled. After providing the required options in the username command, press enter. User will be prompted for the username password and password will be hidden. Note: Choosing password key in the same line while configuring user account, password will not be hidden.`
		password オプションを付けずに **username** コマンドまたは **snmp-server user** コマンドが入力された後に、ユーザに対してパスワード入力要求のプロンプトを表示するようスイッチを設定します。ユーザが入力したパスワードは非表示にされます。この機能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。
		（注）
		Cisco NX-OS リリース 10.5(2)F 以降、**password** プロンプトでの SNMP ユーザー削除の構成では、使いやすいよう

	コマンドまたはアクション	目的
		にパスワード関連のプロンプトがスキップされます。
ステップ 3	（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。

RADIUS または TACACS+ の共有秘密の設定

スイッチとRADIUSまたはTACACS +サーバ間の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、機密情報であるため非表示にする必要があります。これらの暗号化された共有秘密の生成には、 **radius-server** [**host**] **key** および **tacacs-server** [**host**] **key** コマンドをそれぞれ使用します。SHA256ハッシュ方式は、暗号化された共有秘密を保存するために使用されます。

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	**generate type7_encrypted_secret**
	例：
	`switch(config)# generate type7_encrypted_secret`
	`Type-7 (Vigenere) Encryption,`
	`Use this encrypted secret to configure radius and tacacs shared secret with key type 7.`
	`Copy complete secret with double quotes.`
	`Enter plain text secret:`
	`Confirm plain text secret:`
	`Type 7 Encrypted secret is : "fewhg"`
		キー タイプ 7 で RADIUS または TACACS+ の共有秘密を設定します。共有秘密の入力を 2 回平文で求められます。秘密は、入力すると非表示になります。次に、暗号化されたバージョンの秘密が表示されます。
		（注）
		プレーン テキストの秘密情報の暗号化バージョンを別途生成しておき、その後で暗号化された共有秘密を設定することができます。その際には、 **radius-server** [**host**] **key** および **tacacs-server** [**host**] **key** を使用しますコマンドを発行します。

ステップ 3	（任意） **copy running-config startup-config** 例：	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。

	コマンドまたはアクション	目的
	`switch(config)# copy running-config startup-config`	

RADIUS ログイン情報キャッシュ

Cisco NX-OS ソフトウェアは RADIUS ログイン情報のローカル キャッシングをサポートしているため、認証の効率と信頼性がさらに向上します。

Cisco スイッチの RADIUS ログイン情報キャッシング機能は、認証されたユーザー ログイン情報をローカルに保存します。そのため、同じログイン情報をローカルにキャッシュすることで、RADIUS サーバーに何度も認証要求を行う必要がなくなります。これは、同じログイン情報が短時間で繰り返し利用される自動化された環境で特に有利です。

RADIUS ログイン情報のキャッシングの利点

- **パフォーマンスの向上**： RADIUS サーバに送信される認証要求を減らし、パフォーマンスを向上させ、ネットワークの輻輳を軽減します。
- **柔軟性と管理**： 管理者が CLI を介してキャッシュ設定を管理することを許可し、スイッチでのユーザー管理が強化します。

RADIUS クレデンシャルの処理方法

process_workflow

1. ログインした時にスイッチは認証のためにお使いのログイン情報を RADIUS サーバーに転送します。
2. 認証されると、Nexus スイッチはログイン情報をローカルにキャッシュします。

（注） パスワードのハッシュのみがキャッシュに保存され、この目的で最も強力なハッシュ タイプの 1 つが使用されます。これにより、キャッシュにアクセスしても元のパスワードを取得できなくなります。

3. 同じクレデンシャルを使用する将来の認証要求については、スイッチは要求をローカルで処理し、RADIUS サーバに対して要求が繰り返されないように防御します。

（注） キャッシュ エントリは、次の場合に自動的に消去されます：

- 機能が無効な場合。
- clear コマンドが実行された場合。
- RADIUS または AAA 認証の構成に変更がある場合

RADIUS クレデンシャルのキャッシングの注意事項と制約事項

- キャッシング機能を有効または無効にして、キャッシュ タイムアウト値を構成できます。
- キャッシング機能は、RADIUS プロトコル専用です。TACACS や LDAP などの他のプロトコルは、このキャッシング メカニズムではサポートされていません。
- 各キャッシュ エントリはユーザー定義のタイムアウト期間に従い、タイムアウト期間が経過すると、再認証が要求されます。
- 機能が無効になっている場合、clear コマンドを実行した場合、またはスイッチの AAA または RADIUS 構成に変更があった場合、キャッシュはクリアされます。
- キャッシュは、次のシナリオで消去されます：
  - 機能が無効な場合
  - clear コマンドが実行された場合
  - スイッチの AAA または RADIUS 構成に変更がある場合
- 「管理者」権限を持つユーザーは、キャッシュされたユーザーデータベースをクリアできます。

RADIUS クレデンシャル キャッシングの構成

RADIUS ログイン情報キャッシングを有効にして、Cisco Nexus スイッチでの認証プロセスの効率を向上させることができます。ネットワーク パフォーマンスの最適化と認証を効果的に管理するためにこの機能を構成します。Nexus スイッチでこの機能を構成する手順は次のとおりです。

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。

	コマンドまたはアクション	目的
ステップ 2	**aaa authentication cache timeout minutes** 例： `switch(config)# aaa authentication cache timeout 10`	RADIUS ログイン情報キャッシングを有効にします。キャッシュ エントリのタイムアウト期間（分単位）を 1 ～ 1,440 の範囲で指定します。

RADIUS ログイン情報キャッシング構成の検証

手順

	コマンドまたはアクション	目的

ステップ 1	**show running-config aaa**
	例：
	`Switch(config)# show running-config aaa`
	`!Command: show running-config aaa`
	`!Running configuration last done at: Thu Jan 30 08:41:11 2025`
	`!Time: Thu Jan 30 08:41:18 2025`
	
	`version 10.5(3) Bios:version 05.52`
		デバイスの実行コンフィギュレーションの一部として、認証、許可、アカウンティングの詳細を含む現在の AAA コンフィギュレーションの構成を表示します。

ステップ 2	**show aaa authentication cache**
	例：
	`Switch# show aaa authentication cache`
	
	`Remote user cache status: enabled`
	`Remote user cache timeout: 10`
		AAA 認証キャッシュのステータスと構成を表示します。この情報には、キャッシングが有効であるかどうか、およびキャッシュエントリの現在のタイムアウト期間が含まれています。

ステップ 3	（任意） **show aaa authentication cache users**
	例：
	`Switch# show aaa authentication cache users`
	`Total Users: 4`
	`Username Expiry time`
	`bob: Thu Feb 13 06:46:29 2025 UTC`
	`bob1: Thu Feb 13 06:46:42 2025 UTC`
	`bob2: Thu Feb 13 06:46:55 2025 UTC`
	`bob3: Thu Feb 13 06:47:10 2025 UTC`
		AAA 認証システムによって現在キャッシュされているユーザーに関する詳細情報を表示します。この情報には、ユーザー名とそれに対応する有効期限のリストが含まれており、各ユーザーのキャッシュ エントリの期限切れを示します。

ステップ 4	**clear aaa authentication cache** 例：	キャッシュ済みユーザー データベースのすべてのエントリをクリアします。

	コマンドまたはアクション	目的
	`Switch# clear aaa authentication cache`	

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 NX-OS 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。このログはモニタリングしたりクリアしたりできます。

Procedure

	Command or Action	Purpose
ステップ 1	**show accounting log** [*size* | **last-index** | **start-seqnum** *number* | **start-time** *year month day hh*:*mm*:*ss*] **Example:** `switch# show accounting log`	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。コマンドの出力を制限する場合は、*size* 引数を使用します。指定できる範囲は 0 ～ 250000 バイトです。また、ログ出力の開始シーケンス番号または開始時間を指定できます。開始インデックスの範囲は、1 ～ 1000000 です。アカウンティング ログ ファイルにある最後のインデックス番号の値を表示するには、**last-index** キーワードを使用します。
ステップ 2	(Optional) **clear accounting log** [**logflash**] **Example:** `switch# clear aaa accounting log`	アカウンティング ログの内容をクリアします。**logflash** キーワードはログ フラッシュに保存されているアカウンティング ログをクリアします。

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** {**ascii-authentication** | **chap** | **error-enable** | **mschap** | **mschapv2**}]	AAA 認証ログイン設定情報を表示します。
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 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。
show userpassphrase sequence alphabet length	ユーザー パスワードの英字シーケンスの最大長を表示します。
show userpassphrase sequence keyboard length	ユーザー パスワードのキーボード シーケンスの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。

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

ログイン パラメータの設定例

次に、60秒以内に3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。この例は、ログインの失敗を示しません。

```
switch# configure terminal
switch(config)# login block-for 100 attempts 3 within 60
switch(config)# 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 3 login failures occur in 60 seconds or less,
 logins will be disabled for 100 seconds.

 Switch presently in Normal-Mode.
 Current Watch Window remaining time 45 seconds.
 Present login failure count 0.

switch(config)# show login failures
*** No logged failed login attempts with the device.***
```

以下に、待機モードACLの設定例を示します。待機時間中、myaclのACL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。この例は、ログインの失敗も示します。

```
switch# configure terminal
switch(config)# login block-for 100 attempts 3 within 60
switch(config)# login quiet-mode access-class myacl

switch(config)# show login

 Switch is enabled to watch for login Attacks.
 If more than 3 login failures occur in 60 seconds or less,
 logins will be disabled for 100 seconds.

 Switch presently in Quiet-Mode.
 Will remain in Quiet-Mode for 98 seconds.
 Denying logins from all sources.

switch(config)# show login failures
Information about last 20 login failure's with the device.
-------------------------------------------------------------------------------
Username      Line          SourceIPAddr    Appname    TimeStamp
-------------------------------------------------------------------------------
asd           /dev/pts/0    171.70.55.158   login      Mon Aug  3 18:18:54 2015
qweq          /dev/pts/0    171.70.55.158   login      Mon Aug  3 18:19:02 2015
qwe           /dev/pts/0    171.70.55.158   login      Mon Aug  3 18:19:08 2015
```

パスワード プロンプト機能の設定例

次の例では、**username** コマンド入力後にユーザ パスワード入力要求のプロンプトを表示し、パスワードが入力されなかった場合にはエラー メッセージを表示するようスイッチを設定する方法を示します。

```
switch# configure terminal
switch(config)# password prompt username
Password prompt username is enabled.
After providing the required options in the username command, press enter.
User will be prompted for the username password and password will be hidden.
Note: Choosing password key in the same line while configuring user account, password
will not be hidden.


switch(config)# username user1
Enter password:
Confirm password:
warning: password for user:user1 not set. S/he may not be able to login
```

次の例では、**snmp-server user** コマンド入力後にユーザ パスワード入力要求のプロンプトを表示し、その後、ユーザに提示するプロンプトを表示するようにスイッチを設定する方法を示します。

```
switch# configure terminal
switch(config)# password prompt username
Password prompt username is enabled.
After providing the required options in the username command, press enter.
User will be prompted for the username password and password will be hidden.
Note: Choosing password key in the same line while configuring user account, password
will not be hidden.


N9K-1(config)# snmp-server user user1
Enter auth md5 password (Press Enter to Skip):
Enter auth sha password (Press Enter to Skip):
```

AAA に関する追加情報

ここでは、AAA の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	*Cisco NX-OS* ライセンス ガイド

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
AAA に関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html

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。