AAA サーバとローカル データベース

この章では、認証、認可、アカウンティング（AAA は「トリプル A」と読む）について説明します。AAA は、コンピュータ リソースへのアクセスを制御するための一連のサービスで、サービスの課金に必要な情報を提供します。これらの処理は、効果的なネットワーク管理およびセキュリティにとって重要です。

この章では、AAA 機能用にローカル データベースを設定する方法について説明します。外部 AAA サーバについては、ご使用のサーバ タイプに関する章を参照してください。

AAA とローカル データベースについて

ここでは、AAA とローカル データベースについて説明します。

認証

認証はユーザを特定する方法です。アクセスが許可されるには、ユーザは通常、有効なユーザ名と有効なパスワードが必要です。AAA サーバは、データベースに保存されている他のユーザ クレデンシャルとユーザの認証資格情報を比較します。クレデンシャルが一致する場合、ユーザはネットワークへのアクセスが許可されます。クレデンシャルが一致しない場合は、認証は失敗し、ネットワーク アクセスは拒否されます。

次の項目を認証するように、Cisco ASA を設定できます。

- ASA へのすべての管理接続（この接続には、次のセッションが含まれます）
  - Telnet
  - SSH

- シリアル コンソール
- ASDM（HTTPS を使用）
- VPN 管理アクセス

- **enable** コマンド
- ネットワーク アクセス層
- VPN アクセス

認証

許可はポリシーを適用するプロセスです。どのようなアクティビティ、リソース、サービスに対するアクセス許可をユーザが持っているのかを判断します。ユーザが認証されると、そのユーザはさまざまなタイプのアクセスやアクティビティを認可される可能性があります。

次の項目を認可するように、ASA を設定できます。

- 管理コマンド
- ネットワーク アクセス層
- VPN アクセス

Accounting

アカウンティングは、アクセス時にユーザが消費したリソースを測定します。これには、システム時間またはセッション中にユーザが送受信したデータ量などが含まれます。アカウンティングは、許可制御、課金、トレンド分析、リソース使用率、キャパシティプランニングのアクティビティに使用されるセッションの統計情報と使用状況情報のログを通じて行われます。

認証、認可、アカウンティング間の相互作用

認証だけで使用することも、認可およびアカウンティングとともに使用することもできます。認可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングだけで使用することも、認証および認可とともに使用することもできます。

AAA Servers

AAA サーバは、アクセス制御に使用されるネットワーク サーバです。認証は、ユーザを識別します。認可は、認証されたユーザがアクセスする可能性があるリソースとサービスを決定するポリシーを実行します。アカウンティングは、課金と分析に使用される時間とデータのリソースを追跡します。

AAA Server Groups

認証、許可、またはアカウンティングに外部 AAA サーバを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの AAA サーバ グループを作成して、各グループに 1 つ以上のサーバを追加する必要があります。AAA サーバ グループは名前で識別されます。各サーバ グループは、あるサーバまたはサービスに固有です。

次の項を参照してください。

- RADIUS サーバ グループの設定
- TACACS+ サーバ グループの設定
- LDAP サーバ グループの設定

Kerberos、SDI および HTTP フォーム用のサーバ グループも設定できます。これらのグループは VPN 設定で使用されます。これらのグループのタイプについては、『VPN 構成ガイド』を参照してください。

ローカル データベースについて

ASA は、ユーザ プロファイルを取り込むことができるローカル データベースを管理します。AAA サーバの代わりにローカル データベースを使用して、ユーザ認証、認可、アカウンティングを提供することもできます。

次の機能にローカル データベースを使用できます。

- ASDM ユーザごとのアクセス
- コンソール認証
- Telnet 認証および SSH 認証
- **enable** コマンド認証

  この設定は、CLI アクセスにだけ使用され、Cisco ASDM ログインには影響しません。
- コマンド許可

  ローカル データベースを使用するコマンド許可を有効にすると、Cisco ASA では、ユーザ特権レベルを参照して、どのコマンドが使用できるかが特定されます。コマンド許可がディセーブルの場合は通常、特権レベルは参照されません。デフォルトでは、コマンドの特権レベルはすべて、0 または 15 のどちらかです。 ASDM には、コマンドへの割り当てをイネーブルにできる特権レベルが事前に定義されています。割り当てることができるレベルは、15（管理）、5（読み取り専用）、3（監視専用）の 3 種類です。事前定義済みのレベルを使用する場合は、ユーザを 3 種類の特権レベルのいずれかに割り当てます。
- ネットワーク アクセス認証
- VPN クライアント認証

マルチ コンテキスト モードの場合、システム実行スペースでユーザ名を設定し、**login** コマンドを使用して CLI で個々にログインできます。ただし、システム実行スペースではローカル データベースを参照する AAA ルールは設定できません。

（注） ローカル データベースはネットワーク アクセス認可には使用できません。

フォールバック サポート

ローカル データベースは、複数の機能のフォールバック方式として動作できます。この動作は、ASA から誤ってロックアウトされないように設計されています。

ログインすると、コンフィギュレーション内で指定されている最初のサーバから、応答があるまでグループ内のサーバが順に 1 つずつアクセスされます。グループ内のすべてのサーバが使用できない場合、ローカル データベースがフォールバック方式（管理認証および許可限定）として設定されていると、ASA はローカル データベースに接続しようとします。フォールバック方式として設定されていない場合、ASA は引き続き AAA サーバにアクセスしようとします。

フォールバック サポートを必要とするユーザについては、ローカル データベース内のユーザ名およびパスワードと、AAA サーバ上のユーザ名およびパスワードとを一致させることを推奨します。これにより、透過フォールバックがサポートされます。ユーザは、AAA サーバとローカル データベースのどちらがサービスを提供しているかが判別できないので、ローカル データベースのユーザ名およびパスワードとは異なるユーザ名およびパスワードを AAA サーバで使用することは、指定するべきユーザ名とパスワードをユーザが確信できないことを意味します。

ローカル データベースでサポートされているフォールバック機能は次のとおりです。

- コンソールおよびイネーブル パスワード認証：グループ内のサーバがすべて使用できない場合、ASA ではローカル データベースを使用して管理アクセスを認証します。これには、イネーブル パスワード認証が含まれる場合があります。
- コマンド許可：グループ内の TACACS+ サーバがすべて使用できない場合、特権レベルに基づいてコマンドを認可するためにローカル データベースが使用されます。
- VPN 認証および認可：VPN 認証および認可は、通常この VPN サービスをサポートしている AAA サーバが使用できない場合、ASA へのリモート アクセスをイネーブルにするためにサポートされます。管理者である VPN クライアントが、ローカル データベースへのフォールバックを設定されたトンネル グループを指定する場合、AAA サーバ グループが使用できない場合でも、ローカル データベースが必要な属性で設定されていれば、VPN トンネルが確立できます。

グループ内の複数のサーバを使用したフォールバックの仕組み

サーバ グループ内に複数のサーバを設定し、サーバ グループのローカル データベースへのフォールバックをイネーブルにしている場合、ASA からの認証要求に対してグループ内のどのサーバからも応答がないと、フォールバックが発生します。次のシナリオで例証します。

サーバ 1、サーバ 2 の順で、LDAP サーバ グループに 2 台の Active Directory サーバを設定します。リモート ユーザがログインすると、ASA によってサーバ 1 に対する認証が試みられます。

サーバ 1 から認証エラー（「user not found」など）が返されると、ASA によるサーバ 2 に対する認証は試みられません。

タイムアウト期間内にサーバ 1 から応答がないと（または認証回数が、設定されている最大数を超えている場合）、ASA によってサーバ 2 に対する認証が試みられます。

グループ内のどちらのサーバからも応答がなく、ASA にローカル データベースへのフォールバックが設定されている場合、ASA によってローカル データベースに対する認証が試みられます。

ローカル データベースのガイドライン

ローカル データベースを認証または認可に使用する場合、ASA からのロックアウトを必ず防止してください。

ローカル データベースへのユーザ アカウントの追加

ユーザをローカル データベースに追加するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[User Accounts]** を選択し、次に [Add] をクリックします。

[Add User Account-Identity] ダイアログボックスが表示されます。

ステップ 2 4 ～ 64 文字の長さのユーザ名を入力します。

ステップ 3 （オプション）3 ～ 127 文字のパスワードを入力します。パスワードでは大文字と小文字が区別されます。フィールドには、アスタリスクだけが表示されます。セキュリティを確保するために、パスワードの長さは 8 文字以上にすることを推奨します。 SSH 公開キー認証を使用している場合など、パスワードを指定せずにユーザ名を作成することもできます。

（注） [User Accounts] ペインでイネーブル パスワードを設定する場合は、ユーザ名 enable_15 に対するパスワードを変更します。ユーザ名 enable_15 は常に [User Accounts] ペインに表示され、デフォルト ユーザ名を表します。この方法は、ASDM のシステム コンフィギュレーションでイネーブル パスワードを設定する唯一の方法です。CLI で他のイネーブル レベル パスワード（enable password 10 など）を設定すると、そのユーザ名は enable_10 という形式で表示されます。

ステップ 4 パスワードを再度入力します。

セキュリティ上の理由から、パスワードを入力するこの 2 つのフィールドには、アスタリスクだけが表示されます。

ステップ 5 MSCHAP を認証に使用している場合は、[User authenticated using MSCHAP] チェックボックスをオンにします。

ステップ 6 [Access Restriction] 領域で、ユーザの管理アクセス レベルを設定します。まず、**[Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authorization]** タブの順に移動し、[Perform authorization for exec shell access] オプションをクリックして、管理認可を有効にする必要があります。

次のいずれかのオプションを選択します。

- [Full Access (ASDM, Telnet, SSH and console)]：ローカル データベースを使用した管理アクセスの認証を設定する場合、このオプションを指定するとユーザは ASDM、SSH、Telnet、およびコンソール ポートを使用できます。さらに認証もイネーブルにすると、ユーザはグローバル コンフィギュレーション モードにアクセスできます。
  - [Privilege Level]：ASDM およびローカル コマンド認可用の特権レベルを設定します。範囲は、0（最低）～ 15（最高）です。無制限の管理者アクセス権を付与するには、15 を指定します。事前定義された ASDM ロールでは、管理者用の 15、読み取り専用の 5、およびモニタ専用の 3（ユーザによる [Home] ペインと [Monitoring] ペインの使用を制限する）が使用されます。
- [CLI login prompt for SSH, Telnet and console (no ASDM access)]：ローカル データベースを使用した管理アクセスの認証を設定する場合、このオプションを指定するとユーザは SSH、Telnet、およびコンソール ポートを使用できます。ユーザは設定に ASDM を使用できません（HTTP 認証を設定している場合）。ASDM 監視は可能です。さらにイネーブル認証も設定すると、ユーザはグローバル コンフィギュレーション モードにアクセスできません。
- [No ASDM, SSH, Telnet, or console access]：ローカル データベースを使用した管理アクセスの認証を設定する場合、このオプションを指定すると、ユーザは認証用に設定した管理アクセス方式を利用できなくなります（ただし、[Serial] オプションは除きます。つまり、シリアル アクセスは許可されます）。

ステップ 7 （オプション）ユーザ単位で ASA への SSH 接続の公開キー認証をイネーブルにする方法については、HTTPS（ASDM）アクセスの設定 を参照してください。

ステップ 8 [VPN Policy] をクリックして、このユーザの VPN ポリシー属性を設定します。VPN 構成ガイドを参照してください。

ステップ 9 [Apply] をクリックします。

ユーザがローカルデータベースに追加され、変更内容が実行コンフィギュレーションに保存されます。

ヒント **[Configuration]** > **[Device Management]** > [Users/AAA] > [User Accounts] ペインの各カラムで特定のテキストを検索できます。[Find] ボックスに検索する特定のテキストを入力し、[Up] または [Down] 矢印をクリックします。テキスト検索にアスタリスク（「*」）と疑問符（「?」）をワイルドカードとして使用することもできます。

ローカル データベースの認証および認可のテスト

ASA がローカル データベースに接続してユーザを認証または許可できるかどうか確認するには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Users/AAA]** > **[AAA Server Groups]** > **[AAA Server Groups]** テーブルで、サーバが含まれるサーバ グループをクリックします。

ステップ 2 [Servers in the Selected Group] テーブルでテストするサーバをクリックします。

ステップ 3 [Test] をクリックします。

選択したサーバに対応する [Test AAA Server] ダイアログボックスが表示されます。

ステップ 4 実行するテストのタイプ（[Authentication] または [Authorization]）をクリックします。

ステップ 5 ユーザ名を入力します。

ステップ 6 認証をテストする場合は、ユーザ名のパスワードを入力します。

ステップ 7 [OK] をクリックします。

認証または認可のテスト メッセージが ASA からサーバへ送信されます。テストが失敗した場合は、ASDM によりエラー メッセージが表示されます。

ローカル データベースのモニタリング

ローカル データベースのモニタリングについては、次のコマンドを参照してください。

- **[Monitoring] > [Properties] > [AAA Servers]**

  このペインには、AAA サーバの統計情報が表示されます。

- **[Tools] > [Command Line Interface]**

このペインでは、さまざまな非インタラクティブ コマンドを発行し、結果を表示することができます。

ローカル データベースの履歴

表 *1:* ローカル データベースの履歴

機能名	プラットフォーム リリース	説明
AAA のローカル データベース設定	7.0(1)	AAA 用にローカル データベースを設定する方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] [Configuration] > [Device Management] > [Users/AAA] > [User Accounts]
SSH 公開キー認証のサポート	9.1(2)	ASA への SSH 接続の公開キー認証は、ユーザ単位で有効にできるようになりました。公開キー ファイル（PKF）でフォーマットされたキーまたは Base64 キーを指定できます。PKF キーは、4096 ビットまで使用できます。ASA がサポートする Base64 形式（最大 2048 ビット）では大きすぎるキーについては、PKF 形式を使用します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Authentication][Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Edit User Account] > [Public Key Using PKF]。 *8.4(4.1)* でも使用可能。*PKF* キー形式は *9.1(2)* でのみサポートされます。

機能名	プラットフォーム リリース	説明
ローカルの **username** および **enable** パスワードでより長いパスワード（127 文字まで）がサポートされます。	9.6(1)	127 文字までのローカル **username** および **enable** パスワードを作成できます（以前の制限は 32 文字でした）。32 文字以上のパスワードを作成すると、PBKDF2（パスワードベース キー派生関数 2）のハッシュを使用して設定に保存されます。これよりも短いパスワードは引き続き MD5 ベースのハッシュを使用します。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Device Name/Password] > [Enable Password]** **[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Add/Edit User Account] > [Identity]**
SSH 公開キー認証の改善	9.6(2)	以前のリリースでは、ローカルユーザ データベース（）を使用して AAA SSH 認証を有効にしなくても、SSH 公開キー認証（）を有効にすることができました。この設定は修正されたため、AAA SSH 認証を明示的に有効にする必要があります。ユーザが秘密キーの代わりにパスワードを使用できないよう、パスワード未定義のユーザ名を作成できるようになりました。 次の画面が変更されました。 **[Configuration] > [Device Management] > [Management Access] > [ASDM/HTTPS/Telnet/SSH]** **[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Add/Edit User Account]**

機能名	プラットフォーム リリース	説明
すべてのローカル **username** および **enable** パスワードに対する PBKDF2 ハッシュ	9.7(1)	長さ制限内のすべてのローカル **username** および **enable** パスワードは、PBKDF2（パスワード ベース キー派生関数 2）のハッシュを使用して設定に保存されます。以前は、32 文字以下のパスワードが MD5 ベースのハッシュ メソッドを使用していました。既存のパスワードでは、ユーザが新しいパスワードを入力しない限り、MD5 ベースのハッシュが引き続き使用されます。ダウングレードのガイドラインについては、『一般操作構成ガイド』の「ソフトウェアおよびコンフィギュレーション」の章を参照してください。 次の画面が変更されました。 **[Configuration] > [Device Setup] > [Device Name/Password] > [Enable Password]** **[Configuration] > [Device Management] > [Users/AAA] > [User Accounts] > [Add/Edit User Account] > [Identity]**

機能名	プラットフォーム リリース	説明
SSH 公開キー認証を使用するユーザの認証とパスワードを使用するユーザの認証を区別します。	9.6(3)/9.8(1)	9.6(2) より前のリリースでは、ローカル ユーザ データベース（**ssh authentication**）を使用して AAA SSH 認証を明示的に有効にしなくても、SSH 公開キー認証（**aaa authentication ssh console LOCAL**）を有効にすることができました。9.6(2) では、ASA で AAA SSH 認証を明示的に有効にする必要がありました。このリリースでは、AAA SSH 認証を明示的に有効にする必要はありません。ユーザに対して **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザのローカル認証がデフォルトで有効になります。さらに、明示的に AAA SSH 認証を設定すると、この設定はパスワード付きのユーザ名にのみ適用されます。また、任意の AAA サーバ タイプ（**aaa authentication ssh console radius_1** など）を使用できます。たとえば、一部のユーザはローカルデータベースを使用して公開キー認証を使用し、他のユーザは RADIUS でパスワードを使用できます。 変更された画面はありません。