



## AAA 用の TACACS+ サーバ

この章では、AAA で使われる TACACS+ サーバの設定方法について説明します。

- [AAA 用の TACACS+ サーバについて \(1 ページ\)](#)
- [AAA 用の TACACS+ サーバのガイドライン \(3 ページ\)](#)
- [TACACS+ サーバの設定 \(3 ページ\)](#)
- [TACACS+ サーバの認証および許可のテスト \(7 ページ\)](#)
- [AAA 用の TACACS+ サーバのモニタリング \(7 ページ\)](#)
- [AAA 用の TACACS+ サーバの履歴 \(8 ページ\)](#)

## AAA 用の TACACS+ サーバについて

ASA は、ASCII、PAP、CHAP、MS-CHAPv1 の各プロトコルで TACACS+ サーバ認証をサポートします。

## TACACS+ 属性

Cisco ASA は、TACACS+ 属性をサポートします。TACACS+ 属性は、認証、許可、アカウントingの機能を分離します。プロトコルでは、必須とオプションの2種類の属性をサポートします。サーバとクライアントの両方で必須属性を解釈できる必要があり、また、必須属性はユーザに適用する必要があります。オプションの属性は、解釈または使用できることも、できないこともあります。



(注) TACACS+ 属性を使用するには、NAS 上で AAA サービスがイネーブルになっていることを確認してください。

次の表に、カットスループロキシ接続に対してサポートされる TACACS+ 許可応答属性の一覧を示します。

表 1: サポートされる TACACS+ 許可応答属性

| 属性       | 説明                                                     |
|----------|--------------------------------------------------------|
| acl      | 接続に適用する、ローカルで設定済みの ACL を識別します。                         |
| idletime | 認証済みユーザセッションが終了する前に許可される非アクティブ時間（分）を示します。              |
| timeout  | 認証済みユーザセッションが終了する前に認証クレデンシャルがアクティブな状態である絶対時間（分）を指定します。 |

次の表に、サポートされる TACACS+ アカウンティング属性の一覧を示します。

。

表 2: サポートされる TACACS+ アカウンティング属性

| 属性           | 説明                                                                        |
|--------------|---------------------------------------------------------------------------|
| bytes_in     | この接続中に転送される入力バイト数を指定します（ストップレコードのみ）。                                      |
| bytes_out    | この接続中に転送される出力バイト数を指定します（ストップレコードのみ）。                                      |
| cmd          | 実行するコマンドを定義します（コマンドアカウンティングのみ）。                                           |
| disc-cause   | 切断理由を特定する数字コードを示します（ストップレコードのみ）。                                          |
| elapsed_time | 接続の経過時間（秒）を定義します（ストップレコードのみ）。                                             |
| foreign_ip   | トンネル接続のクライアントの IP アドレスを指定します。最下位のセキュリティインターフェイスでカットスループロキシ接続のアドレスを定義します。  |
| local_ip     | トンネル接続したクライアントの IP アドレスを指定します。最上位のセキュリティインターフェイスでカットスループロキシ接続のアドレスを定義します。 |
| NAS port     | 接続のセッション ID が含まれます。                                                       |

| 属性         | 説明                                                   |
|------------|------------------------------------------------------|
| packs_in   | この接続中に転送される入力パケット数を指定します。                            |
| packs_out  | この接続中に転送される出力パケット数を指定します。                            |
| priv-level | コマンド アカウンティング要求の場合はユーザの権限レベル、それ以外の場合は 1 に設定されます。     |
| rem_addr   | クライアントの IP アドレスを示します。                                |
| service    | 使用するサービスを指定します。コマンド アカウンティングの場合にのみ、常に「shell」に設定されます。 |
| task_id    | アカウンティング トランザクションに固有のタスク ID を指定します。                  |
| username   | ユーザの名前を示します。                                         |

## AAA 用の TACACS+ サーバのガイドライン

ここでは、AAA 用の TACACS+ サーバを設定する前に確認する必要があるガイドラインおよび制限事項について説明します。

### IPv6

AAA サーバは、IPv4 または IPv6 アドレスを使用できます。

### その他のガイドライン

- シングル モードで最大 100 個のサーバ グループ、またはマルチ モードでコンテキストごとに 4 つのサーバ グループを持つことができます。
- 各グループには、シングル モードで最大 16 台、マルチ モードで最大 4 台のサーバを含めることができます。

## TACACS+ サーバの設定

ここでは、TACACS+ サーバを設定する方法について説明します。

## 手順

- ステップ1 [TACACS+ サーバグループの設定 \(4 ページ\)](#) .
- ステップ2 [グループへの TACACS+ サーバの追加 \(5 ページ\)](#) .
- ステップ3 (任意) [認証プロンプトの追加 \(6 ページ\)](#) .

## TACACS+ サーバグループの設定

認証、許可、アカウントिंगに TACACS+ サーバを使用する場合は、まず TACACS+ サーバグループを少なくとも 1 つ作成し、各グループに 1 台以上のサーバを追加する必要があります。TACACS+ サーバグループは名前で識別されます。

TACACS+ サーバグループを追加するには、次の手順を実行します。

## 手順

- ステップ1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。
- ステップ2 [AAA Server Group] 領域で、[Add] をクリックします。  
[Add AAA Server Group] ダイアログボックスが表示されます。
- ステップ3 [Server Group] フィールドにグループの名前を入力します。
- ステップ4 [Protocol] ドロップダウンリストから、[TACACS+] サーバタイプを選択します。
- ステップ5 [Accounting Mode] フィールドで、[Simultaneous] または [Single] をクリックします。  
[Single] モードの場合、ASA ではアカウントング データが 1 つのサーバにだけ送信されます。  
[Simultaneous] モードの場合、ASA ではアカウントング データがグループ内のすべてのサーバに送信されます。
- ステップ6 [Reactivation Mode] フィールドで、[Depletion] または [Timed] をクリックします。  
[Depletion] モードの場合、障害が発生したサーバは、グループ内のサーバがすべて非アクティブになったときに限り、再アクティブ化されます。depletion モードでは、あるサーバが非アクティブになった場合、そのサーバは、グループの他のすべてのサーバが非アクティブになるまで非アクティブのままとなります。すべてのサーバが非アクティブになると、グループ内のすべてのサーバが再アクティブ化されます。このアプローチでは、障害が発生したサーバに起因する接続遅延の発生を最小限に抑えられます。  
Timed モードでは、障害が発生したサーバは 30 秒の停止時間の後で再アクティブ化されます。
- ステップ7 [Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

デッドタイムは、グループ内の最後のサーバがディセーブルになってから、すべてのサーバが再びイネーブルになるまでの分単位の時間間隔です。

**ステップ 8** 失敗試行の最大許容回数を追加します。

このオプションで設定するのは、応答のないサーバを非アクティブと宣言するまでに許可される接続試行の失敗回数です。

**ステップ 9** [OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバ グループが [AAA Server Groups] テーブルに追加されます。

**ステップ 10** [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

## グループへの TACACS+ サーバの追加

TACACS+ サーバをグループに追加するには、次の手順を実行します。

### 手順

**ステップ 1** [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

**ステップ 2** サーバを追加するサーバ グループをクリックします。

**ステップ 3** [Servers in the Selected Group] 領域で、[Add] をクリックします。

サーバ グループに対応する [Add AAA Server Group] ダイアログボックスが表示されます。

**ステップ 4** 認証サーバが存在するインターフェイス名を選択します。

**ステップ 5** グループに追加するサーバのサーバ名または IP アドレスを追加します。

**ステップ 6** タイムアウト値を入力するか、デフォルトのままにします。[Timeout] フィールドには、バックアップサーバへ要求を送信する前に、ASA がプライマリ サーバからの応答を待機する時間を秒単位で指定します。

**ステップ 7** サーバポートを指定します。サーバポートは、ポート番号 139、または ASA によって TACACS+ サーバとの通信に使用される TCP ポートの番号です。

**ステップ 8** サーバ秘密キーを指定します。ASA で TACACS+ サーバを認証する際に使用される共有秘密キーを指定します。ここで設定したサーバ秘密キーは、TACACS+ サーバで設定されたサーバ秘密キーと一致する必要があります。サーバ秘密キーが不明の場合は、TACACS+ サーバの管理者に問い合わせてください。最大フィールド長は、64 文字です。

**ステップ 9** [OK] をクリックします。

[Add AAA Server Group] ダイアログボックスが閉じ、AAA サーバが AAA サーバ グループに追加されます。

**ステップ 10** [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

## 認証プロンプトの追加

AAA 認証チャレンジプロセスの実行中にユーザに表示するテキストを指定できます。TACACS+ サーバからのユーザ認証が必要な場合に、ASA 経由の HTTP、FTP、Telnet アクセス用の AAA チャレンジテキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワードプロンプトの上に表示されます。

認証プロンプトを指定しない場合、TACACS+ サーバでの認証時にユーザに対して表示される内容は次のようになります。

| Connection Type | デフォルトのプロンプト        |
|-----------------|--------------------|
| FTP             | FTP authentication |
| HTTP            | HTTP 認証            |
| Telnet          | なし                 |

認証プロンプトを追加するには、次の手順を実行します。

### 手順

**ステップ 1** [Configuration] > [Device Management] > [Users/AAA] > [Authentication Prompt] の順に選択します。

**ステップ 2** ログイン時にユーザに表示されるユーザ名とパスワードのプロンプトの上に表示するテキストを追加します。

次の表に、認証プロンプトの文字数制限を示します。

| アプリケーション                    | 認証プロンプトの文字数制限 |
|-----------------------------|---------------|
| Microsoft Internet Explorer | 37            |
| Telnet                      | 235           |
| FTP                         | 235           |

**ステップ 3** [User accepted message] フィールドと [User rejected message] フィールドにメッセージを追加します。

Telnet からのユーザ認証を実行する場合、[User accepted message] オプションおよび [User rejected message] オプションを使用すれば、認証試行が AAA サーバにより受け入れられた、または拒否されたことを示すさまざまな状態のプロンプトを表示できます。

これらのメッセージテキストをそれぞれ指定した場合、ASA では、AAA サーバにより認証されたユーザに対しては [User accepted message] テキストが表示され、認証されなかったユーザに対しては ASA により [User rejected message] テキストが表示されます。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジテキストのみが表示されます。ユーザ承認メッセージテキストおよびユーザ拒否メッセージテキストは表示されません。

ステップ 4 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。

## TACACS+ サーバの認証および許可のテスト

ASA が TACACS+ サーバに接続してユーザを認証または承認できるかどうかを判別するには、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] の順に選択します。

ステップ 2 サーバが存在するサーバグループをクリックします。

ステップ 3 テストするサーバをクリックします。

ステップ 4 [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 5 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 6 ユーザ名を入力します。

ステップ 7 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 8 [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、エラーメッセージが表示されます。

## AAA 用の TACACS+ サーバのモニタリング

AAA 用の TACACS+ サーバ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、設定された TACACS+ サーバの統計情報が表示されます。

- [Tools] > [Command Line Interface]

非対話形式の各種コマンドを発行して結果を表示できます。

## AAA 用の TACACS+ サーバの履歴

表 3: AAA 用の TACACS+ サーバの履歴

| 機能名                           | プラットフォーム リリース | 説明                                                                                                                                                                                                                                                      |
|-------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TACACS+ サーバ                   | 7.0(1)        | <p>AAA に TACACS+ サーバを設定する方法について説明します。</p> <p>次の画面が導入されました。</p> <p>[Configuration] &gt; [Device Management] &gt; [Users/AAA] &gt; [AAA Server Groups]</p> <p>[Configuration] &gt; [Device Management] &gt; [Users/AAA] &gt; [Authentication Prompt]。</p> |
| AAA 向けの IPv6 アドレス TACACS+ サーバ | 9.7(1)        | AAA サーバに IPv4 または IPv6 アドレスを使用できるようになりました。                                                                                                                                                                                                              |