AAA 用の TACACS+ サーバー

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

AAA 用の TACACS+ サーバーについて

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

TACACS+ 属性

ASA は、TACACS+ 属性をサポートします。TACACS+ 属性は、認証、許可、アカウンティング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。サーバー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、必須属性はユーザー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	認証済みユーザー 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	認証済みユーザー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いる絶対時間（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。
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ーの権限レベル、それ以外の場合は 1 に設定されます。
rem_iddr	クライアントの IP アドレスを示します。

属性	説明
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	ユーザーの名前を示します。

AAA 用の TACACS+ サーバーのガイドライン

ここでは、AAA 用の TACACS+ サーバーを設定する前に確認する必要の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 サーバーは、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200個のサーバーグループ、またはマルチモードでコンテキストごとに 4 つのサーバー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 8 台のサーバーを含めることができます。
- ASA アプライアンスモードで実行されている FPR1000、FPR2100、または FPR3100 シリーズの場合は、次のユーザー名規則に従う必要があります。
  - Linux に対して有効である必要があります。
  - 小文字のみを使用してください。
  - 英数字、ピリオド（.）、ハイフン（-）を含めることができます。
  - アット マーク（@）やスラッシュ（/）など、その他の特殊文字を含めることはできません。

TACACS+ サーバーの設定

ここでは、TACACS+ サーバーを設定する方法について説明します。

手順

ステップ 1 TACACS+ サーバー グループの設定 （4 ページ）。
ステップ 2 グループへの TACACS+ サーバーの追加 （6 ページ）。

TACACS+ サーバー グループの設定

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

TACACS+ サーバー 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 サーバー グループ名とプロトコルを指定します。

aaa-server *server_tag* **protocol tacacs+**

例：

```
ciscoasa(config)# aaa-server servergroup1 protocol tacacs+
```

aaa-server protocol コマンドを入力すると、aaa-server グループ コンフィギュレーション モードが開始します。

ステップ 2 次のサーバーを試す前にグループ内の AAA サーバーでの AAA トランザクションの失敗の最大数を指定します。

max-failed-attempts *number*

例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 引数の範囲は 1 ～ 5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定すると、グループ内のすべてのサーバーが応答しないか応答が無効である場合にグループは応答なしと見なされ、フォールバック方式が試行されます。サーバー グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続くと、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。

フォールバック方式として設定されていない場合、ASA は引き続きグループ内のサーバーにアクセスしようとします。

ステップ 3 グループ内で障害の発生したサーバーを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
```

depletion キーワードを指定すると、グループ内のすべてのサーバーが非アクティブになって初めて、障害の発生したサーバーが再度アクティブ化されます。

deadtime *minutes* キーワードと引数のペアは、グループ内の最後のサーバーをディセーブルにしてから次にすべてのサーバーを再度イネーブルにするまでの経過時間を、0 ～ 1440 分の範囲で指定します。デッドタイムは、ローカルデータベースへのフォールバックを設定した場合にのみ適用されます。認証は、デッドタイムが経過するまでローカルで試行されます。デフォルトは 10 分です。

timed キーワードを指定すると、30 秒のダウン時間の後、障害が発生したサーバーが再度アクティブ化されます。

ステップ 4 グループ内のすべてのサーバーにアカウンティング メッセージを送信します。

accounting-mode simultaneous

例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

アクティブ サーバーにのみメッセージを送信するデフォルトに戻すには、**accounting-mode single** コマンドを入力します。

例

次の例では、1 台のプライマリ サーバーと 1 台のバックアップ サーバーで構成された 1 つの TACACS+ グループを追加する例を示します。

```
ciscoasa(config)# aaa-server AuthInbound protocol tacacs+
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.1
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.2
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey2
ciscoasa(config-aaa-server-host)# exit
```

グループへの TACACS+ サーバーの追加

TACACS+ サーバー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 TACACS+ サーバーと、そのサーバーが属するサーバー グループを識別します。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

例：

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

(*interface_name***)** を指定していない場合、ASA はデフォルトで**内部**インターフェイスを使用します。

サーバーは、IPv4 アドレスか IPv6 アドレスのどちらかを使用できます。

ステップ 2 サーバーへの接続試行のタイムアウト値を指定します。

timeout *seconds*

Specify the timeout interval（1-300 seconds）for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts（based on the interval defined on the **retry-interval** command）until the timeout is reached. 連続して失敗したトランザクションの数が AAA サーバーグループ内の max-failed-attempts コマンドで指定された制限に達すると、AAA サーバーは非アクティブ化され、ASA は（設定されている場合は）別の AAA サーバーへの要求の送信を開始します。

例：

```
ciscoasa(config-aaa-server-host)# timeout 15
```

ステップ 3 ポート番号 49、または ASA によって TACACS+ サーバーとの通信に使用される TCP ポート番号を指定します。

server-port *port_number*

例：

```
ciscoasa(config-aaa-server-host)# server-port 49
```

ステップ 4 TACACS+ サーバに対する NAS の認証に使用されるサーバ秘密値を指定します。

key

例：

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

この値は大文字と小文字が区別される、最大127文字の英数字から成るキーワードで、TACACS+サーバー上のキーと同じ値です。127 を超える文字は無視されます。このキーはクライアントとサーバー間でデータを暗号化するために使われ、クライアントとサーバー両方のシステムで同じである必要があります。このキーにスペースを含めることはできませんが、他の特殊文字は使用できます。

AAA 用の TACACS+ サーバーのモニタリング

AAA 用の TACACS+ サーバー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。

- **show aaa-server**

  このコマンドは、設定された TACACS+ サーバーの統計情報を表示します。TACACS+ サーバーの統計情報をクリアするには、**clear aaa-server statistics** コマンドを入力します。

- **show running-config aaa-server**

  このコマンドは、TACACS+ サーバーの実行コンフィギュレーションを表示します。TACACS+ サーバー コンフィギュレーションをクリアするには、**clear configure aaa-server** コマンドを入力します。

AAA 用の TACACS+ サーバーの履歴

表 *3 : AAA* 用の *TACACS+* サーバーの履歴

機能名	プラットフォーム リリース	説明
TACACS+ サーバ	7.0(1)	AAA に TACACS+ サーバーを設定する方法について説明します。 次のコマンドを導入しました。 **aaa-server protocol**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**aaa authorization exec authentication-server**、**server-port**、**key**、**clear aaa-server statistics**、**clear configure aaa-server**、**show aaa-server**、**show running-config aaa-server**、**username**、**service-type**、**timeout**.
AAA 向けの IPv6 アドレス TACACS+ サーバー	9.7(1)	AAA サーバーに IPv4 または IPv6 アドレスを使用できるようになりました。

機能名	プラットフォーム リリース	説明
グループごとのAAAサーバー グループとサーバーの制限が増えました。	9.13(1)	より多くの AAA サーバー グループを設定できます。シングルコンテキストモードでは、200個のAAAサーバーグループを設定できます（以前の制限は 100）。マルチコンテキストモードでは、8 個設定できます（以前の制限は 4）。 さらに、マルチコンテキストモードでは、グループごとに 8 台のサーバーを設定できます（以前の制限はグループごとに4台のサーバー）。シングル コンテキスト モードのグループごとの制限の 16 は変更されていません。 これらの新しい制限を受け入れるために、次のコマンドが変更されました。**aaa-server**、**aaa-server host**

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。