



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 \(3 ページ\)](#)
- [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 \(7 ページ\)](#)

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、アカウントリ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)。
-

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 サーバ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 次のサーバを試す前にグループ内の AAA サーバでの 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）を設定している場合で、グループ内のすべてのサーバが応答しないとき、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 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が非アクティブになって初めて、障害の発生したサーバ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をディセーブルにしてから次にすべてのサーバ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。デフォルトは 10 分です。

timed キーワードは、30 秒間のダウンタイムの後に障害が発生したサーバを再度アクティブ化します。

- ステップ 4** グループ内のすべてのサーバにアカウントिंग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と 1 台のバックアップサーバで構成された 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 TACACS+ サーバと、そのサーバが属するサーバ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 サーバへの接続試行のタイムアウト値を指定します。

```
timeout seconds
```

サーバのタイムアウト間隔（1～300 秒）を指定します。デフォルトは 10 秒です。各 AAA トランザクションに対して、タイムアウトに達するまで（**retry-interval** コマンドで定義された間隔に基づいて）ASA による接続の再試行が行われます。連続して失敗したトランザクションの数が AAA サーバグループ内の **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両方のシステムで同じ

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。

- **show aaa-server**

このコマンドは、設定された TACACS+ サーバの統計情報を表示します。TACACS+ サーバ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+サーバの実行コンフィギュレーションを表示します。TACACS+サーバ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)	AAA に TACACS+ サーバ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	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。

