



「Configuring TACACS+」

- 機能情報の確認, 1 ページ
- TACACS+ の前提条件, 1 ページ
- TACACS+ の概要, 3 ページ
- TACACS+ とスイッチアクセスを設定する方法, 8 ページ
- TACACS+ のモニタリング, 17 ページ
- セキュア シェルの設定に関するその他の参考資料, 17 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

TACACS+ の前提条件

TACACS+ によるスイッチアクセスのセットアップと設定の前提条件は、次のとおりです（示されている順序で実行する必要があります）。

- 1 スイッチに TACACS+ サーバアドレスとスイッチを設定します。
- 2 認証キーを設定します。
- 3 TACACS+ サーバでステップ 2 からキーを設定します。

- 4 認証、許可、アカウントिंग (AAA) をイネーブルにする。
- 5 ログイン認証方式リストを作成します。
- 6 端末回線にリストを適用します。
- 7 認証およびアカウントング方式のリストを作成します。

TACACS+ によるスイッチ アクセスの制御の前提条件は、次のとおりです。

- スイッチ上で TACACS+ 機能を設定するには、設定済みの TACACS+ サーバにアクセスする必要があります。また、通常 LINUX または Windows ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されている TACACS+ サービスにもアクセスする必要があります。
- スイッチ スタックと TACACS+ サーバとの間に冗長接続を設定することを推奨します。これによって、接続済みのスタックメンバの1つがスイッチスタックから削除された場合でも、TACACS+ サーバにアクセスできます。
- スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアが稼働するシステムが必要です。
- TACACS+ を使用するには、それをイネーブルにする必要があります。
- 許可は、使用するスイッチでイネーブルにする必要があります。
- ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。
- この項または他の項で示す AAA コマンドを使用するには、まず **aaa new-model** コマンドを使用して AAA をイネーブルにする必要があります。
- 最低限、TACACS+ デーモンを維持するホスト (1つまたは複数) を特定し、TACACS+ 認証の方式リストを定義する必要があります。また、任意で TACACS+ 許可およびアカウントングの方式リストを定義できます。
- 方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト (偶然に *default* と名前が付けられている) です。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。
- TACACS+ を使用して認証を行った場合は、TACACS+ を使用して特権 EXEC アクセスを許可します。
- 認証に TACACS+ を使用しなかった場合は、ローカルデータベースを使用します。

関連トピック

[TACACS+ の概要, \(3 ページ\)](#)

[TACACS+ の動作, \(5 ページ\)](#)

[TACACS+ とスイッチ アクセスを設定する方法, \(8 ページ\)](#)

[方式リスト, \(6 ページ\)](#)

[TACACS+ ログイン認証の設定, \(10 ページ\)](#)

[TACACS+ ログイン認証, \(6 ページ\)](#)

[特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定, \(13 ページ\)](#)

[特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可, \(7 ページ\)](#)

TACACS+ の概要

TACACS+ およびスイッチ アクセス

ここでは、TACACS+ について説明します。TACACS+ は詳細なアカウント情報を提供し、認証と許可のプロセスを柔軟に管理します。TACACS+ は、認証、許可、アカウントング (AAA) 機能により拡張されており、TACACS+ をイネーブルにするには AAA コマンドを使用する必要があります。

関連トピック

[不正アクセスの防止](#)

[スイッチのローカル認証および許可の設定](#)

[SSH サーバ、統合クライアント、およびサポートされているバージョン](#)

TACACS+ の概要

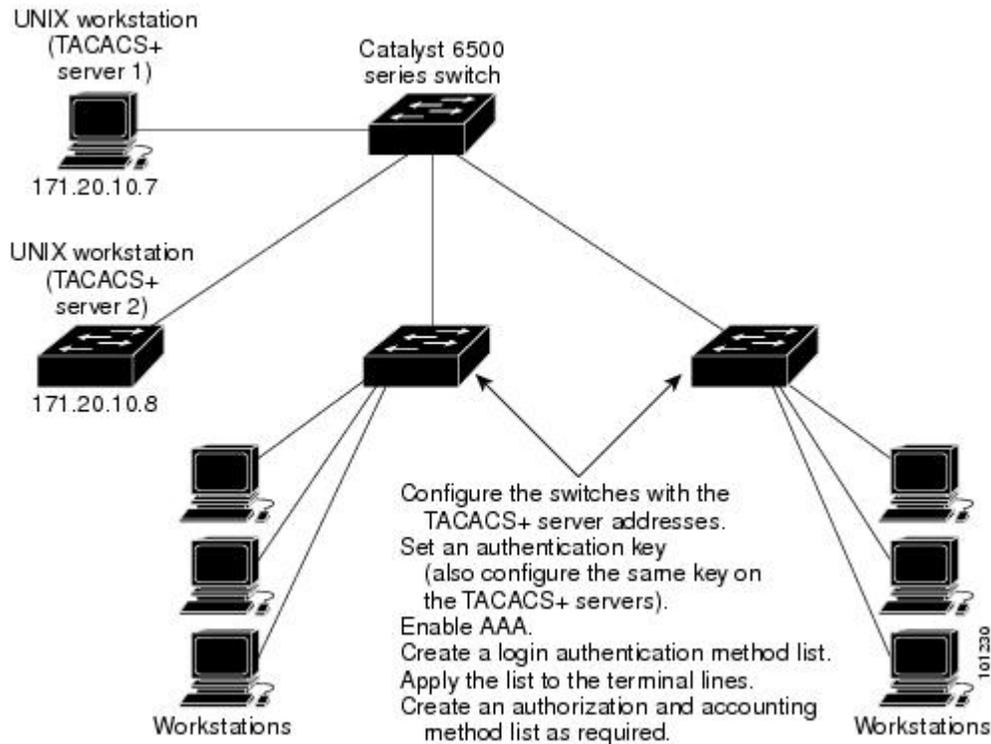
TACACS+ は、スイッチにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションです。

TACACS+ では、独立したモジュラ型の認証、許可、アカウントング機能が提供されます。

TACACS+ では、単一のアクセス コントロール サーバ (TACACS+ デーモン) が各サービス (認証、許可、およびアカウントング) を別個に提供します。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

TACACS+ の目的は、1つの管理サービスから複数のネットワーク アクセス ポイントを管理する方式を提供することです。スイッチは、他の Cisco ルータやアクセス サーバとともにネットワーク アクセス サーバにできます。

図 1：一般的な TACACS+ ネットワーク構成



TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証：ログインおよびパスワード ダイアログ、チャレンジおよび応答、メッセージ サポートによって認証の完全制御を行います。

認証機能は、ユーザとの対話を実行できます（たとえば、ユーザ名とパスワードが入力された後、自宅の住所、母親の旧姓、サービスタイプ、社会保険番号などのいくつかの質問をすることによりユーザを試します）。TACACS+ 認証サービスは、ユーザ画面にメッセージを送信することもできます。たとえば、会社のパスワード有効期間ポリシーに従い、パスワードの変更の必要があることをユーザに通知することもできます。

- 許可：autocommand、アクセスコントロール、セッション期間、プロトコルサポートの設定といった、ユーザセッション時のユーザ機能についてきめ細かく制御します。また、TACACS+ 許可機能によって、ユーザが実行できるコマンドを制限することもできます。
- アカウンティング：課金、監査、およびレポートに使用する情報を収集して TACACS+ デモンに送信します。ネットワークの管理者は、アカウンティング機能を使用して、セキュリティ監査のためにユーザの活動状況をトラッキングしたり、ユーザ課金用の情報を提供した

りできます。アカウントレコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP など）、パケット数、およびバイト数が含まれます。

TACACS+ プロトコルは、スイッチと TACACS+ デーモン間の認証を行い、スイッチと TACACS+ デーモン間のプロトコル交換をすべて暗号化することによって機密保持を実現します。

関連トピック

[TACACS+ の前提条件](#)、(1 ページ)

TACACS+ の動作

ユーザが、TACACS+ を使用しているスイッチに対して簡易 ASCII ログインを試行し、認証が必要になると、次のプロセスが発生します。

- 1 接続が確立されると、スイッチは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、これをユーザに表示します。ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンに接続してパスワードプロンプトを取得します。スイッチによってパスワードプロンプトが表示され、ユーザがパスワードを入力すると、そのパスワードが TACACS+ デーモンに送信されます。

TACACS+ によって、デーモンとユーザとの間の対話が可能になり、デーモンはユーザを認証できるだけの情報を取得できるようになります。デーモンは、ユーザ名とパスワードの組み合わせを入力するよう求めますが、ユーザの母親の旧姓など、その他の項目を含めることもできます。

- 2 スイッチは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。
 - **ACCEPT** : ユーザが認証され、サービスを開始できます。許可を必要とするようにスイッチが設定されている場合は、この時点で許可処理が開始されます。
 - **REJECT** : ユーザは認証されません。TACACS+ デーモンに応じて、ユーザはアクセスを拒否されるか、ログインシーケンスを再試行するよう求められます。
 - **ERROR** : デーモンによる認証サービスのある時点で、またはデーモンとスイッチの間のネットワーク接続においてエラーが発生しました。**ERROR** 応答が表示された場合は、スイッチは、通常別の方法でユーザを認証しようとします。
 - **CONTINUE** : ユーザは、さらに認証情報の入力を求められます。

認証後、スイッチで許可がイネーブルになっている場合、ユーザは追加の許可フェーズに入ります。ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

- 3 TACACS+ 許可が必要な場合は、再び TACACS+ デーモンに接続し、デーモンが **ACCEPT** または **REJECT** の許可応答を返します。**ACCEPT** 応答が返された場合は、その応答に、そのユーザおよびそのユーザがアクセスできるサービスの、**EXEC** または **NETWORK** セッション宛ての属性の形式でデータが含まれています。

• Telnet、セキュア シェル (SSH)、rlogin、または特権 EXEC サービス

- 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセスリスト、およびユーザタイムアウトを含む）

関連トピック

[TACACS+ の前提条件, \(1 ページ\)](#)

方式リスト

方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。方式リストを使用して、使用するセキュリティプロトコルを1つまたは複数指定できるので、最初の方式が失敗した場合のバックアップシステムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

関連トピック

[TACACS+ とスイッチ アクセスを設定する方法, \(8 ページ\)](#)

[TACACS+ の前提条件, \(1 ページ\)](#)

TACACS+ 設定オプション

認証用に1つのサーバを使用することも、また、既存のサーバホストをグループ化するためにAAAサーバグループを使用するように設定することもできます。サーバをグループ化して設定済みサーバホストのサブセットを選択し、特定のサービスにそのサーバを使用できます。サーバグループは、グローバルサーバホストリストとともに使用され、選択されたサーバホストのIPアドレスのリストが含まれています。

関連トピック

[TACACS+ サーバホストの指定および認証キーの設定, \(8 ページ\)](#)

TACACS+ ログイン認証

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する1つまたは複数のセキュリティプロトコルを指定できるので、最初の方式が失敗した場合のバックアップシステムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティサーバまたはローカルのユーザ名データベースがユーザアクセスを拒否

すると応答した場合)、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

関連トピック

[TACACS+ ログイン認証の設定, \(10 ページ\)](#)

[TACACS+ の前提条件, \(1 ページ\)](#)

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可

AAA 許可によってユーザが利用できるサービスが制限されます。AAA 許可がイネーブルに設定されていると、スイッチはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザデータベースまたはセキュリティサーバ上にあり、ユーザのセッションを設定します。ユーザは、ユーザプロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

関連トピック

[特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定, \(13 ページ\)](#)

[TACACS+ の前提条件, \(1 ページ\)](#)

TACACS+ Accounting

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワークリソース量をトラッキングします。AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティングレコードの形式で TACACS+ セキュリティサーバに報告します。各アカウンティングレコードにはアカウンティングの Attribute-Value (AV) ペアが含まれ、レコードはセキュリティサーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

関連トピック

[TACACS+ アカウンティングの起動, \(14 ページ\)](#)

TACACS+ のデフォルト設定

TACACS+ および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。TACACS+ をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。



(注) TACACS+ の設定は CLI を使用して行いますが、TACACS+ サーバは権限レベル 15 に設定された HTTP 接続を許可します。

TACACS+ とスイッチ アクセスを設定する方法

ここでは、TACACS+ をサポートするようにスイッチを設定する方法について説明します。

関連トピック

[方式リスト, \(6 ページ\)](#)

[TACACS+ の前提条件, \(1 ページ\)](#)

TACACS+ サーバホストの指定および認証キーの設定

TACACS+ サーバホストを特定し、認証キーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **tacacs-server host hostname**
4. **aaa new-model**
5. **aaa group server tacacs+ group-name**
6. **server ip-address**
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Switch> enable	特権 EXEC モードをイネーブルにします。パスワードを入力します (要求された場合)。
ステップ 2	configureterminal 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 3	tacacs-server host <i>hostname</i> 例 : Switch(config)# tacacs-server host yourserver	TACACS+サーバを維持する IP ホストを特定します。このコマンドを複数回入力して、優先ホストのリストを作成します。ソフトウェアは、指定された順序でホストを検索します。 <i>hostname</i> には、ホストの名前または IP アドレスを指定します。
ステップ 4	aaa new-model 例 : Switch(config)# aaa new-model	AAA をイネーブルにします。
ステップ 5	aaa group server tacacs+ <i>group-name</i> 例 : Switch(config)# aaa group server tacacs+ your_server_group	(任意) グループ名で AAA サーバグループを定義します。 このコマンドによって、Switchをサーバグループサブコンフィギュレーションモードにします。
ステップ 6	server <i>ip-address</i> 例 : Switch(config)# server 10.1.2.3	(任意) 特定の TACACS+サーバを定義済みサーバグループに関連付けます。AAA サーバグループの TACACS+サーバごとに、このステップを繰り返します。 グループの各サーバは、ステップ 3 で定義済みのものでなければなりません。
ステップ 7	end 例 : Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 8	show running-config 例 : Switch# show running-config	入力を確認します。
ステップ 9	copy running-config startup-config 例 : Switch# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

関連トピック

[TACACS+ 設定オプション, \(6 ページ\)](#)

TACACS+ ログイン認証の設定

TACACS+ ログイン認証を設定するには、次の手順を実行します。

はじめる前に

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。



(注) AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

ip http authentication コマンドの詳細については、『*Cisco IOS Security Command Reference, Release 12.4*』を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa new-model**
4. **aaa authentication login {default | list-name} method1 [method2...]**
5. **line [console | tty | vty] line-number [ending-line-number]**
6. **login authentication {default | list-name}**
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Switch> enable	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	configureterminal 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 3	aaa new-model 例： Switch(config)# aaa new-model	AAA をイネーブルにします。
ステップ 4	aaa authentication login {default list-name} method1 [method2...] 例： Switch(config)# aaa authentication login default tacacs+ local	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> • login authentication コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、default キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • list-name には、作成するリストの名前として使用する文字列を指定します。 • method1... には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> • enable : イネーブル パスワードを認証に使用します。この認証方式を使用するには、あらかじめ enable password グローバル コンフィギュレーション コマンドを使用してイネーブルパスワードを定義しておく必要があります。 • group tacacs+ : TACACS+ 認証を使用します。この認証方式を使用するには、あらかじめ TACACS+ サーバを設定しておく必要があります。詳細については、TACACS+ サーバホストの指定および認証キーの設定、(8 ページ) を参照してください。 • line : 回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。 password password ライン コンフィギュレーション コマンドを使用します。 • local : ローカルユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。 username

	コマンドまたはアクション	目的
		<p><i>password</i> グローバル コンフィギュレーション コマンドを使用します。</p> <ul style="list-style-type: none"> • <i>local-case</i> : 大文字と小文字が区別されるローカルユーザ名データベースを認証に使用します。 username namepassword グローバル コンフィギュレーション コマンドを使用して、ユーザ名情報をデータベースに入力する必要があります。 • <i>none</i> : ログインに認証を使用しません。
ステップ 5	line [console tty vty] <i>line-number [ending-line-number]</i> 例 : Switch(config)# line 2 4	ラインコンフィギュレーションモードを開始し、認証リストを適用する回線を設定します。
ステップ 6	login authentication {default list-name} 例 : Switch(config-line)# login authentication default	1つの回線または複数回線に認証リストを適用します。 <ul style="list-style-type: none"> • default を指定する場合は、aaa authentication login コマンドで作成したデフォルトのリストを使用します。 • <i>list-name</i> には、aaa authentication login コマンドで作成したリストを指定します。
ステップ 7	end 例 : Switch(config-line)# end	特権 EXEC モードに戻ります。
ステップ 8	show running-config 例 : Switch# show running-config	入力を確認します。
ステップ 9	copy running-config startup-config 例 : Switch# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

関連トピック

[TACACS+ ログイン認証, \(6 ページ\)](#)[TACACS+ の前提条件, \(1 ページ\)](#)

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

aaa authorization グローバル コンフィギュレーション コマンドと **tacacs+** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。



(注) 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa authorization network tacacs+**
4. **aaa authorization exec tacacs+**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Switch> enable	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	configureterminal 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 3	aaa authorization network tacacs+ 例： <pre>Switch(config)# aaa authorization network tacacs+</pre>	ネットワーク関連のすべてのサービス要求に対してユーザ TACACS+ 認可を行うことを設定します。
ステップ 4	aaa authorization exec tacacs+ 例： <pre>Switch(config)# aaa authorization exec tacacs+</pre>	ユーザの特権 EXEC アクセスに対してユーザ TACACS+ 認可を行うことを設定します。 exec キーワードを指定すると、ユーザプロファイル情報 (autocommand 情報など) が返される場合があります。
ステップ 5	end 例： <pre>Switch(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例： <pre>Switch# show running-config</pre>	入力を確認します。
ステップ 7	copy running-config startup-config 例： <pre>Switch# copy running-config startup-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

関連トピック

[特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可, \(7 ページ\)](#)

[TACACS+ の前提条件, \(1 ページ\)](#)

TACACS+ アカウンティングの起動

TACACS+ アカウンティングを開始するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **aaa accounting network start-stop tacacs+**
4. **aaa accounting exec start-stop tacacs+**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Switch> enable	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	configureterminal 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 3	aaa accounting network start-stop tacacs+ 例： Switch(config)# aaa accounting network start-stop tacacs+	ネットワーク関連のすべてのサービス要求について、TACACS+ アカウンティングをイネーブルにします。
ステップ 4	aaa accounting exec start-stop tacacs+ 例： Switch(config)# aaa accounting exec start-stop tacacs+	TACACS+ アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。
ステップ 5	end 例： Switch(config)# end	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	show running-config 例： Switch# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例： Switch# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

次の作業

AAA サーバが到達不能の場合に、ルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。これは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

関連トピック

[TACACS+ Accounting](#), (7 ページ)

AAA サーバが到達不能な場合のルータとのセッションの確立

AAA サーバが到達不能の場合に、ルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。これは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

TACACS+ のモニタリング

表 1: TACACS+ 情報を表示するためのコマンド

コマンド	目的
show tacacs	TACACS+ サーバの統計情報を表示します。

セキュア シェルの設定に関するその他の参考資料

関連資料

関連項目	マニュアルタイトル
セッションウェアなネットワークングに対するアイデンティティ コントロール ポリシーおよびアイデンティティ サービス テンプレートの設定。	『 Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) 』
RADIUS、TACACS+、Secure Shell、802.1x および AAA の設定。	『 Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) 』

エラー メッセージ デコーダ

説明	リンク
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	<p>選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。</p> <p>http://www.cisco.com/go/mibs</p>

シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/support</p>