目次

概要

このドキュメントでは、UNIX で動作する TACACS+ を使用して認証するために Cisco ルータを設定する方法について説明します。 TACACS+ の機能は有償の Cisco Secure ACS for Windows や Cisco Secure ACS UNIX ほど多くありません。

これまでシスコから提供されていた TACACS+ は提供が終了しており、シスコのサポートの対象外になっています。

現在は、任意のインターネット検索エンジンで「TACACS+ フリーウェア」を検索すると、フリーウェア バージョンの TACACS+ が多数見つかります。 シスコでは、特定の TACACS+ フリーウェア の実装を推奨することは特にしていません。

Cisco Secure Access Control Server（ACS）は通常のシスコ営業担当者および世界各地の販売チャネルを通じて購入できます。 Cisco Secure ACS for Windows には、Microsoft Windows ワークステーションへの単体インストールに必要なすべてのコンポーネントが付属しています。 Cisco Secure ACS Solution Engine は Cisco Secure ACS のソフトウェア ライセンスがプリインストールされた状態で出荷されます。 シスコ発注ホームページ（登録ユーザ専用）からご注文ください。

注Cisco Secure ACS for Windows の 90 日間トライアル版を入手するには、関連するサービス契約を結んでいる Cisco.com アカウントが必要です。

このドキュメントで紹介するルータ設定は、Cisco IOS® ソフトウェア リリース 11.3.3 が稼働するルータ上で開発されたものです。 Cisco IOS ソフトウェア リリース 12.0.5.T 以降では **tacacs+** の代わりに **group tacacs+** を使用します。そのため、**aaa authentication login default tacacs+ enable** などのステートメントは **aaa authentication login default group tacacs+ enable** として表示されます。

ルータ コマンドの詳細については、Cisco IOS ソフトウェアに関するドキュメントを参照してください。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco IOS ソフトウェア リリース 11.3.3 および Cisco IOS ソフトウェア リリース 12.0.5.T 以降に基づきます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

認証

次の手順を実行します。

1. コンパイル済みの TACACS+ (TAC+) コードが UNIX サーバ上にあることを確認します。 ここでは、Cisco TAC+ サーバ コードを使用していることを前提に、サーバを設定します。 ルータ設定は、サーバ コードがシスコのサーバに固有のものであるかどうかに関係なく動作するはずです。 TAC+ は root で実行する必要があるため、 必要な場合は su を実行して root になります。
2. このドキュメントの最後にある test_file をコピーして TAC+ サーバ上に配置し、**test_file** という名前を付けます。**tac_plus_executable** デーモンを **test_file** で起動できるか確認します。 次のコマンドの **-P** オプションは、コンパイル エラーをチェックするだけでデーモンは起動しません。test_file のコンテンツがウィンドウをスクロールするのを見るかもしれません のようなメッセージが見るべきではありません--、または}。 エラーがある場合は、test_file へのパスをチェックし、入力内容を再確認して、再度テストしてから次へ進みます。
3. ルータ上で TAC+ の設定を開始します。**イネーブル** モードへ切り換え、コマンドを設定する前に **configure terminal** と入力します。 次のコマンド シンタックスでは、最初からロックアウトが発生していないことを確認します。**tac_plus_executable** が稼働していないことを前提にしています。 *!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication vtymethod
4. 次に進む前に、Telnet およびコンソール ポート経由で引き続きルータへアクセスできるこ

と確認します。 **tac_plus_executable** が稼働していないため、**enable** password は受け入れられるはずです。**注**コンソール ポート セッションをアクティブな状態で維持し、イネーブル モードのままにしておいてください。 このセッションをタイムアウトさせてはいけません。 この時点ではルータへのアクセスが制限されているため、ロックアウトを発生させずに設定を変更できるようにする必要があります。次のコマンドを発行し、ルータ側でサーバと ルータ間のインタラクションを確認します。 *!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication vtymethod

5. サーバ上の TAC+ を root で起動します。 *!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication vtymethod
6. TAC+ が起動したことを確認します。 *!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication vtymethod**または** *!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication vtymethodTAC+ が起動しない場合は、test_file 内のシンタ

ックスに問題があることがほとんどです。 手順 1 に戻って問題を修正します。

7. ルータと サーバ間のインタラクションをサーバ側で確認するために、**tail -f /var/tmp/tac_plus.log** と入力します。**注**手順 5 の -d 16 オプションにより、すべてのトランザクションの出力は /var/tmp/tac_plus.log へ送信されます。
8. この時点から、Telnet (VTY) ユーザは TAC+ を通じて認証を受けることが必要になります。ルータとサーバでデバッグを継続したまま (手順 4 と 7)、ネットワークの別の部分からルータへ telnet します。ユーザ名とパスワードの入力を求めるプロンプトが表示されたら、次のように入力します。*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication vtymethodユーザー authenuser はグループ admin に属しています。このグループは、パスワード admin を使用します。サーバをおよび TAC+ 相互対話を表示できるルータを監視して下さいか。ところ、応答、要求、等送信 される何が。 問題がある場合は修正してから次へ進みます。
9. ユーザを TAC+ で認証してイネーブル モードへ切り換えられるようにする必要もある場合は、コンソール ポート セッションが引き続きアクティブであることを確認してから、次のコマンドをルータへ追加します。*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication vtymethodこの時点から、ユーザは TAC+ を通じてイネーブルに切り換えることが必要になります。
10. ルータとサーバでデバッグを継続したまま (手順 4 と 7)、ネットワークの別の部分からルータへ telnet します。 ユーザ名とパスワードの入力を求めるプロンプトが表示されたら、次のように入力します。*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication vtymethodイネーブル モードに切り換えると、ルータからパスワードの入力

を求められます。これには次のように応答します。*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication vtymethodサーバをおよび TAC+ 相互対話を確認するはずであるルータを監視して下さいか。 ところ、応答、要求、等送信 される何が。 問題がある場合は修正してから次へ進みます。

11. コンソール ポートへ接続したまま、サーバ上の TAC+ プロセスをダウンさせ、TAC+ がダウンした場合でも引き続きユーザがルータにアクセスできることを確認します。*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication vtymethodまたは*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# line con 0 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever *!--- No time-out to prevent being locked out !--- during debugging.* exec-timeout 0 0 login authentication vtymethod前の手順で行った Telnet と enable を繰り返します。 TAC+ プロセスが応答していないことがルータに認識され、ユーザはデフォルト パスワードを使ってログインとイネーブルができるようになります。
12. コンソール ポート ユーザが TAC+ を通じて認証されるかどうか確認します。 これを行うには、TAC+ サーバを再度起動し（手順 5、6）、ルータへの Telnet セッションを確立します（telnet の場合は TAC+ を通じて認証されます）。コンソール ポートを通じてルータへログインできることを確認するまでは、Telnet を通じてイネーブル モードのルータに接続したままにしておきます。コンソール ポート経由でルータに接続した最初の接続をログアウトし、コンソール ポートへ再度接続します。 ユーザ ID とパスワードを使用したログインとイネーブル モードへの切り換え（手順 10 を参照）に必要なコンソール ポート認証は、この時点から TAC+ を通じて実行されます。
13. Telnet セッションまたはコンソール ポートのどちらかを通じて接続したままにして、ルータとサーバ上でデバッグを継続している状態で（手順 4 と 7）、回線 1 へのモデム接続を

確立します。回線ユーザはこの時点から TAC+ を通じてログインし、イネーブル モードへ切り換えることが必要になります。ユーザ名とパスワードの入力を求めるプロンプトが表示されたら、次のように入力します。
```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list.          !         aaa authentication login linmethod tacacs+ enable    aaa authentication login vtymethod tacacs+ enable    aaa authentication login conmethod tacacs+ enable    !    !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod
```
イネーブル モードへ切り換えると、パスワードの入力を要求されます。次のように入力します。
```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same lines are the methods !--- in the order to be tried. As used here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--- enable password is accepted because !--- it is in each list.          !         aaa authentication login linmethod tacacs+ enable    aaa authentication login vtymethod tacacs+ enable    aaa authentication login conmethod tacacs+ enable    !    !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication vtymethod
```
サーバをおよび TAC+ 相互対話を確認するルータを監視して下さいか。 ところ、応答、要求、等送信 される何が。 問題がある場合は修正してから次へ進みます。この時点から、ユーザは TAC+ を通じてイネーブルに切り換えることが必要になります。

認可の追加

認可の追加はオプションです。

デフォルトでは、ルータには次の 3 つのコマンド レベルがあります。

- 特権レベル 0：disable、enable、exit、help、logout を含む
- 特権レベル 1：telnet の通常レベル（プロンプトは router>）
- 特権レベル 15：イネーブル レベル（プロンプトは router#）

使用可能なコマンドは IOS フィーチャ セット、Cisco IOS のバージョン、ルータのモデルなどによって異なるため、レベル 1 と 15 の全コマンドを包括したリストはありません。 たとえば、**show ipx route** は IP 専用フィーチャ セットには存在せず、Cisco IOS ソフトウェア リリース 10.2.x のリリース時には NAT が採用されていなかったため、**show ip nat trans** はこのリリースに含まれていません。また、電源と温度のモニタリング機能を装備していないルータ モデルには **show environment** が存在しません。 特定のレベルで特定 の ルータで利用可能 なコマンドは a を入力するとき見つけることができますか。 ルータのプロンプト場合のその特権レベルで。

コンソール ポート認証が機能として追加されたのは、Cisco Bug ID CSCdi82030（登録ユーザ専用）以降です。 ユーザが誤ってルータからロックアウトされてしまう可能性を減らすために、コンソール ポート認証はデフォルトでオフに設定されています。 ユーザがコンソールを通じて物理

的にアクセスできる場合は、コンソール ポート認証はあまり効果的ではありません。 ただし、コンソール ポート認証は、Cisco Bug ID CSCdi82030（登録ユーザ専用）が実装されたイメージ内で、次のコマンドを使用して、con 0 行の下でオンにすることができます。

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication
methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the
methods !--- listed on the same lines are the methods !--- in the order to be tried. As used
here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !-
-- enable password is accepted because !--- it is in each list.          !         aaa
authentication login linmethod tacacs+ enable    aaa authentication login vtymethod tacacs+
enable    aaa authentication login conmethod tacacs+ enable    !    !--- Point the router to the
server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0
password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-
timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut
transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password
whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0
login authentication vtymethod
```

1. ルータは、すべてまたは一部のレベルで TAC+ を通じてコマンドを許可するように設定できます。次のルータ設定では、すべてのユーザに、サーバ上でのコマンド単位の認証の設定を許可しています。 ここでは、すべてのコマンドが TAC+ を通じて許可されますが、サーバがダウンしている場合は認証が不要です。

   ```
   !--- Turn on TAC+. aaa new-model enable password
   whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod",
   "conmethod", and !--- so on are names of lists, and the methods !--- listed on the same
   lines are the methods !--- in the order to be tried. As used here, if !--- authentication
   fails due to the !--- tac_plus_executable not being started, the !--- enable password is
   accepted because !--- it is in each list.          !         aaa authentication login
   linmethod tacacs+ enable    aaa authentication login vtymethod tacacs+ enable    aaa
   authentication login conmethod tacacs+ enable    !    !--- Point the router to the server,
   where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0
   password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-
   timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem
   InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4
   password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-
   timeout 0 0 login authentication vtymethod
   ```

2. TAC+ サーバが稼働している状態で、ユーザ ID **authenuser** を使用してルータへ telnet します。authenuser には test_file で default service = permit が指定されているため、このユーザはすべての機能を実行できます。ルータ内で**イネーブル** モードへ切り換え、認可のデバッグをオンにします。

   ```
   !--- Turn on TAC+. aaa new-model enable password whatever !--- These
   are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !---
   so on are names of lists, and the methods !--- listed on the same lines are the methods !--
   - in the order to be tried. As used here, if !--- authentication fails due to the !---
   tac_plus_executable not being started, the !--- enable password is accepted because !--- it
   is in each list.          !         aaa authentication login linmethod tacacs+ enable    aaa
   authentication login vtymethod tacacs+ enable    aaa authentication login conmethod tacacs+
   enable    !    !--- Point the router to the server, where #.#.#.# !--- is the server IP
   address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to
   prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
   conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed
   38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to
   prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
   vtymethod
   ```

3. ユーザ ID **authoruser** とパスワード **operator** を使用してルータへ telnet します。このユーザは 2 つの show コマンド **traceroute** および **logout** を実行できません（test_file を参照）。サーバとルータを監視し、TAC+ インタラクション（送信内容、送信先、応答、要求など）を確認します。 問題がある場合は修正してから次へ進みます。
4. ユーザを autocommand 対応として設定する場合は、test_file 内のユーザ transient のコメントアウトを外し、#.#.#.# の部分に有効な宛先 IP アドレスを入力します。TAC+ サーバを一旦停止し、再起動します。ルータ側：

   ```
   !--- Turn on TAC+. aaa new-model enable password
   ```

```
whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod",
"conmethod", and !--- so on are names of lists, and the methods !--- listed on the same
lines are the methods !--- in the order to be tried. As used here, if !--- authentication
fails due to the !--- tac_plus_executable not being started, the !--- enable password is
accepted because !--- it is in each list.          !         aaa authentication login
linmethod tacacs+ enable    aaa authentication login vtymethod tacacs+ enable    aaa
authentication login conmethod tacacs+ enable    !    !--- Point the router to the server,
where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0
password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-
timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem
InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4
password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-
timeout 0 0 login authentication vtymethod
```

ユーザ ID **transient** とパスワード **transient** を使ってルータへ telnet します。 **telnet #.#.#.#** が実行され、ユーザ transient は他の場所へ送信されます。

アカウンティングの追加

アカウンティングの追加はオプションです。

アカウンティング ファイルへの参照は test_file にありますか。 アカウンティング ファイル = /var/log/tac.log。 ただし、アカウンティングはルータ内に設定しない限り実行されません（ルータが Cisco IOS 11.0 以降のバージョンを実行している場合）。

1. ルータ内のアカウンティングをイネーブルにします。
```
!--- Turn on TAC+. aaa new-model
enable password whatever !--- These are lists of authentication methods. !--- "linmethod",
"vtymethod", "conmethod", and !--- so on are names of lists, and the methods !--- listed on
the same lines are the methods !--- in the order to be tried. As used here, if !---
authentication fails due to the !--- tac_plus_executable not being started, the !--- enable
password is accepted because !--- it is in each list.          !         aaa authentication
login linmethod tacacs+ enable    aaa authentication login vtymethod tacacs+ enable    aaa
authentication login conmethod tacacs+ enable    !    !--- Point the router to the server,
where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0
password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-
timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem
InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4
password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-
timeout 0 0 login authentication vtymethod
```
注AAA アカウンティングは、一部のバージョンではコマンド単位のアカウンティングを実行しません。 対処方法として、コマンド単位の認可を使い、それをログとしてアカウンティング ファイルに記録します（Cisco Bug ID CSCdi44140 を参照してください）。 この修正が使用されているイメージ [1997 年 9 月 24 日現在では、Cisco IOS ソフトウェア リリース 11.2(1.3)F、11.2(1.2)、11.1(6.3)、11.1(6.3)AA01、11.1(6.3)CA] を使用している場合も、コマンド アカウンティングをイネーブルにすることができます。
2. サーバ上で TAC+ が稼働している状態で、アカウンティング ファイルに記録されるエントリを確認するために、次のコマンドをサーバで入力します。
```
!--- Turn on TAC+. aaa new-
model enable password whatever !--- These are lists of authentication methods. !---
"linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the methods
!--- listed on the same lines are the methods !--- in the order to be tried. As used here,
if !--- authentication fails due to the !--- tac_plus_executable not being started, the !--
- enable password is accepted because !--- it is in each list.          !         aaa
authentication login linmethod tacacs+ enable    aaa authentication login vtymethod tacacs+
enable    aaa authentication login conmethod tacacs+ enable    !    !--- Point the router to
the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line
con 0 password whatever !--- No time-out to prevent being locked out !--- during debugging.
exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod
```

```
modem InOut transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0
4 password whatever !--- No time-out to prevent being locked out !--- during debugging.
exec-timeout 0 0 login authentication vtymethod
```

その後、ルータへのログイン、ルータからのログアウト、ルータからの telnet などを行います。 必要に応じて、ルータ上で次のように入力します。

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are
names of lists, and the methods !--- listed on the same lines are the methods !--- in the
order to be tried. As used here, if !--- authentication fails due to the !---
tac_plus_executable not being started, the !--- enable password is accepted because !--- it
is in each list.          !         aaa authentication login linmethod tacacs+ enable    aaa
authentication login vtymethod tacacs+ enable    aaa authentication login conmethod tacacs+
enable    !    !--- Point the router to the server, where #.#.#.# !--- is the server IP
address. ! tacacs-server host #.#.#.# line con 0 password whatever !--- No time-out to
prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed
38400 txspeed 38400 flowcontrol hardware line vty 0 4 password whatever !--- No time-out to
prevent being locked out !--- during debugging. exec-timeout 0 0 login authentication
vtymethod
```

テスト ファイル

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication
methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on are names of lists, and the
methods !--- listed on the same lines are the methods !--- in the order to be tried. As used
here, if !--- authentication fails due to the !--- tac_plus_executable not being started, the !-
-- enable password is accepted because !--- it is in each list.          !         aaa
authentication login linmethod tacacs+ enable    aaa authentication login vtymethod tacacs+
enable    aaa authentication login conmethod tacacs+ enable    !    !--- Point the router to the
server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# line con 0
password whatever !--- No time-out to prevent being locked out !--- during debugging. exec-
timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut
transport input all rxspeed 38400 txspeed 38400 flowcontrol hardware line vty 0 4 password
whatever !--- No time-out to prevent being locked out !--- during debugging. exec-timeout 0 0
login authentication vtymethod
```

注TACACS サーバにアクセスできない場合、次のエラー メッセージが生成されます。 `%AAAA-3-DROPACCTSNDFAIL: accounting record dropped,send to server failed:` system-start. TACACS+ サーバが動作していることを確認してください。

関連情報

- シングルユーザ ネットワーク アクセス セキュリティ TACACS+
- Terminal Access Controller Access Control System（TACACS+）
- Cisco Secure Access Control Server for Windows
- テクニカルサポートとドキュメント - Cisco Systems