「Configuring TACACS+」

TACACS+ について

Terminal Access Controller Access Control System Plus（TACACS+）は、コントローラへの管理アクセスを取得しようとするユーザに中央管理されたセキュリティを提供する、クライアント/サーバプロトコルです。 このプロトコルは、ローカルおよびRADIUS に類似したバックエンドのデータベースとして機能します。 ただし、ローカルおよびRADIUS では、認証サポートと制限のある認可サポートしか提供されないのに対し、TACACS+ では、次の 3 つのサービスが提供されます。

- **認証**：コントローラにログインしようとするユーザを検証するプロセス。

  コントローラで TACACS+ サーバに対してユーザが認証されるようにするには、ユーザは有効なユーザ名とパスワードを入力する必要があります。 認証サービスおよび認可サービスは、互いに密接に関連しています。 たとえば、ローカルまたはRADIUS データベースを使用して認証が実行された場合、認可ではそのローカルまたはRADIUS データベース内のユーザに関連したアクセス権（read-only、read-write、lobby-admin のいずれか）が使用され、TACACS+ は使用されません。 同様に、TACACS+ を使用して認証が実行されると、認可は TACACS+ に関連付けられます。

（注） 複数のデータベースを設定する場合、コントローラ GUI または CLI を使用して、バックエンド データベースが試行される順序を指定できます。

- **認可**：ユーザのアクセス レベルに基づいて、ユーザがコントローラで実行できる処理を決定するプロセス。

  TACACS+ の場合、認可は特定の処理ではなく、権限（またはロール）に基づいて実行されます。 利用可能なロールは、コントローラ GUI の 7 つのメニュー オプション（[MONITOR]、[WLAN]、[CONTROLLER]、[WIRELESS]、[SECURITY]、[MANAGEMENT]、および [COMMANDS]）に対応しています。 ロビー アンバサダー権限のみを必要とするユーザは、追加のロールである LOBBY を使用できます。 ユーザが割り当てられるロールは、TACACS+ サーバ上で設定されます。 ユーザは 1 つまたは複数のロールに対して認可されます。 最小の認可は MONITOR のみで、最大は ALL です。ALL では、ユーザは 7 つのメニュー オプションすべてに関連付けられた機能を実行できるよう認可されます。 たとえば、SECURITY のロールを割り当てられたユーザは、[Security] メニューに表示される（または CLI の場合はセキュリティ コマンドとして指定される）すべてのアイテムに対して変更を実行できます。 ユーザが特定のロール（WLAN など）に対して認可されていない場合でも、そのユーザは読み取り専用モード（または関連する CLI の **show** コマンド）で、そのメニュー オプションにアクセスできます。 TACACS+ 許可サーバが接続不能または認可不能になった場合、ユーザはコントローラにログインできません。

  （注） ユーザが割り当てられたロールでは許可されていないコントローラ GUI のページに変更を加えようとすると、十分な権限がないことを示すメッセージが表示されます。 ユーザが割り当てられたロールでは許可されていないコントローラ CLI コマンドを入力すると、実際にはそのコマンドは実行されていないのに、正常に実行されたというメッセージが表示されます。 この場合、「Insufficient Privilege! Cannot execute command!」というメッセージがさらに表示され、コマンドを実行するための十分な権限がないことがユーザに通知されます。

- **アカウンティング**：ユーザによる処理と変更を記録するプロセス。

  ユーザによる処理が正常に実行される度に、TACACS+ アカウンティング サーバでは、変更された属性、変更を行ったユーザのユーザ ID、ユーザがログインしたリモート ホスト、コマンドが実行された日付と時刻、ユーザの認可レベル、および実行された処理と入力された値の説明がログに記録されます。 TACACS+ アカウンティング サーバが接続不能になった場合、ユーザはセッションを中断されずに続行できます。

RADIUS でユーザ データグラム プロトコル（UDP）を使用するのとは異なり、TACACS+ では、転送にトランスミッション コントロール プロトコル（TCP）を使用します。 1 つのデータベースを維持し、TCP ポート 49 で受信要求をリッスンします。 アクセス コントロールを要求するコントローラは、クライアントとして動作し、サーバから AAA サービスを要求します。 コントローラとサーバ間のトラフィックは、プロトコルで定義されるアルゴリズムと、両方のデバイスにおいて設定される共有秘密キーによって暗号化されます。

最大 3 台の TACACS+ 認証サーバ、認可サーバ、およびアカウンティング サーバをそれぞれ設定できます。 たとえば、1 台の TACACS+ 認証サーバを中央に配置し、複数の TACACS+ 許可サーバを異なる地域に配置できます。 同じタイプの複数のサーバを設定していると、最初のサーバで

障害が発生したり、接続不能になっても、コントローラは自動的に 2 台目、および必要に応じて 3 台目のサーバを試行します。

（注） 複数の TACACS+ サーバが冗長性のために設定されている場合、バックアップが適切に機能するようにするには、すべてのサーバにおいてユーザ データベースを同一にする必要があります。

次に、TACACS+ についての注意事項を示します。

- CiscoSecure Access Control Server（ACS）とコントローラの両方で、TACACS+ を設定する必要があります。 コントローラは、GUI または CLI のいずれかを使用して設定できます。
- TACACS+ は、CiscoSecure ACS バージョン 3.2 以降のリリースでサポートされます。 実行しているバージョンに対応する CiscoSecure ACS のマニュアルを参照してください。
- ワンタイムパスワード（OTP）は、TACACS を使用しているコントローラでサポートされます。 この設定では、コントローラがトランスペアレント パススルー デバイスとして動作します。 コントローラは、クライアント動作をチェックせずにすべてのクライアント要求を TACACS サーバに転送します。 OTP を使用する場合は、クライアントが正しく機能するためにはコントローラへの接続を 1 つ確立する必要があります。 現在、コントローラには、複数の接続を確立しようとしているクライアントを修正するチェック機能はありません。
- 再認証が繰り返し試行されたり、プライマリ サーバがアクティブで接続可能なときにコントローラがバックアップ サーバにフォールバックしたりする場合には、TACACS+ 認証サーバ、認可サーバ、およびアカウンティング サーバの再送信のタイムアウト値を増やすことをお勧めします。 デフォルトの再送信のタイムアウト値は 2 秒です。この値は最大 30 秒まで増やすことができます。

TACACS+ DNS

完全修飾ドメイン名（FQDN）を使用できます。これにより、必要に応じて IP アドレスを変更できます（たとえば、ロード バランシングの更新）。 サブメニューの [DNS] が [Security > AAA > TACACS+] メニューに追加されます。これを使用して、DNS から TACACS+ IP 情報を取得できます。 DNS クエリーはデフォルトでは無効になっています。

（注） TACACS+ DNS は IPv6 に対応していません。

スタティック リストおよび DNS リストを同時に使用することはできません。 DNS によって返されるアドレスはスタティック エントリを上書きします。

スタティック リストおよび DNS リストを同時に使用することはできません。 DNS によって返されるアドレスはスタティック エントリを上書きします。

DNS AAA は、中央認証を使用する FlexConnect AP クライアントに対して有効です。

DNS AAA は、FlexConnect AP グループに対する RADIUS の定義ではサポートされていません。ローカル スイッチングを使用する FlexConnect クライアントの場合、手動で AAA を定義する必要があります。

不正、802.1X、Web 認証、MAC フィルタリング、メッシュ、およびグローバル リストを使用するその他の機能は、DNS 定義のサーバを使用します。

TACACS+ VSA

インターネット技術特別調査委員会（IETF）ドラフト標準には、ネットワーク アクセス サーバと TACACS+ サーバの間でベンダー固有属性（VSA）を伝達する方法が規定されています。 IETF は属性 26 を使用します。 ベンダーは VSA を使用して、一般的な用途には適さない独自の拡張属性をサポートできます。

シスコの TACACS+ 実装では、IETF 仕様で推奨される形式を使用したベンダー固有のオプションを 1 つサポートしています。 シスコのベンダー ID は 9、サポートされるオプションのベンダータイプは 1（名前付き cisco-av-pair）です。 値は次の形式のストリングです。

```
protocol : attribute separator value *
```

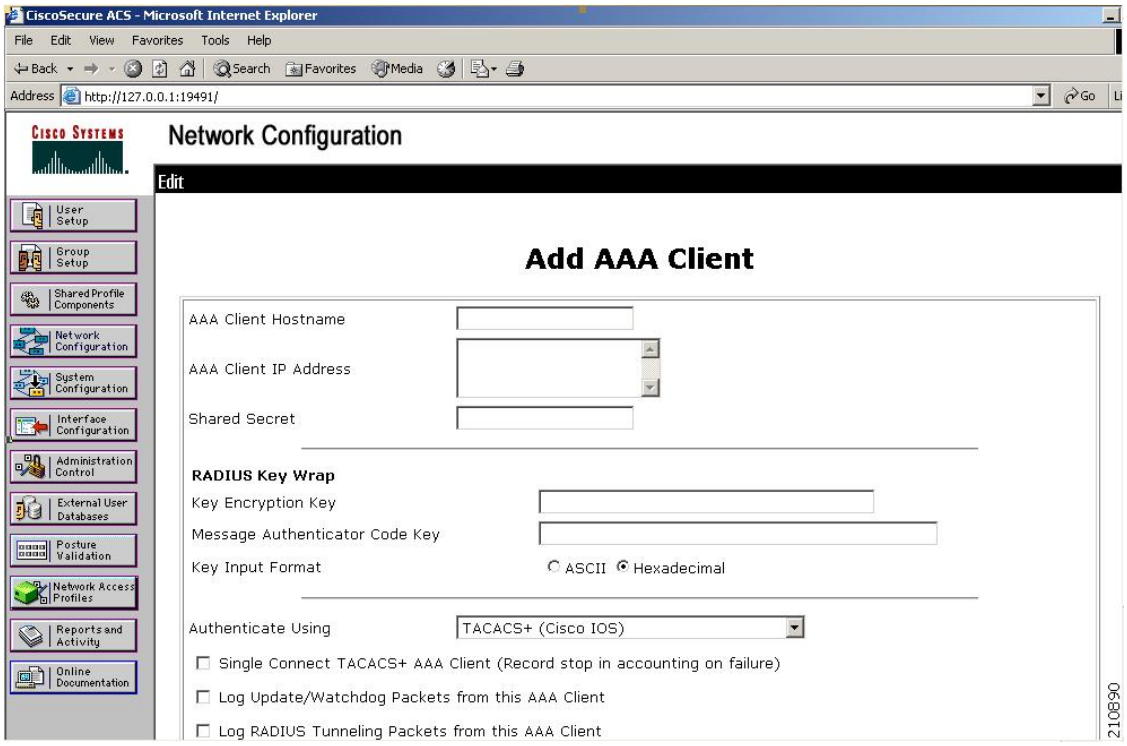
protocol は、特定の許可タイプを表すシスコの属性です。separator は、必須属性の場合は =（等号）、オプションの属性の場合は *（アスタリスク）です。

ACS 上での TACACS+ の設定

ステップ 1 ACS のメイン ページで、[Network Configuration] を選択します。

ステップ 2 [AAA Clients] の下の [Add Entry] を選択し、使用しているコントローラをサーバに追加します。 [Add AAA Client] ページが表示されます。

図 1：***CiscoSecure ACS の [Add AAA Client] ページ***



ステップ 3 [AAA Client Hostname] テキスト ボックスに、コントローラの名前を入力します。

ステップ 4 [AAA Client IP Address] テキスト ボックスに、コントローラの IP アドレスを入力します。

ステップ 5 [Shared Secret] テキスト ボックスに、サーバとコントローラ間の認証に使用する共有秘密キーを入力します。

（注） 共有秘密キーは、サーバとコントローラの両方で同一である必要があります。

ステップ 6 [Authenticate Using] ドロップダウン リストから [TACACS+ (Cisco IOS)] を選択します。

ステップ 7 [Submit + Apply] をクリックして、変更内容を保存します。

ステップ 8 ACS のメイン ページで、左のナビゲーション ペインから [Interface Configuration] を選択します。

ステップ 9 [TACACS+ (Cisco IOS)] を選択します。 [TACACS+ (Cisco)] ページが表示されます。

ステップ 10 [TACACS+ Services] の [Shell (exec)] チェックボックスをオンにします。

ステップ 11 [New Services] で最初のチェックボックスをオンにし、[Service] テキスト ボックスに **ciscowlc**、[Protocol] テキスト ボックスに **common** と入力します。

ステップ 12 [Advanced Configuration] オプションの [Advanced TACACS+ Features] チェックボックスをオンにします。

ステップ 13 [Submit] をクリックして変更を保存します。

ステップ 14 ACS のメイン ページで、左のナビゲーション ペインから [System Configuration] を選択します。

ステップ 15 [Logging] を選択します。

ステップ 16 [Logging Configuration] ページが表示されたら、ログ記録するすべてのイベントを有効にし、変更内容を保存します。

ステップ 17 ACS のメイン ページで、左のナビゲーション ペインから [Group Setup] を選択します。

ステップ 18 [Group] ドロップダウン リストから、以前に作成したグループを選択します。

（注） この手順では、ユーザが割り当てられることになるロールに基づいて、ACS のグループにすでにユーザが割り当てられていることを想定しています。

ステップ 19 [Edit Settings] をクリックします。 [Group Setup] ページが表示されます。

ステップ 20 [TACACS+ Settings] の [ciscowlc common] チェックボックスをオンにします。

ステップ 21 [Custom Attributes] チェックボックスをオンにします。

ステップ 22 [Custom Attributes] の下のテキストボックスで、このグループに割り当てるロールを指定します。 使用可能なロールは、MONITOR、WLAN、CONTROLLER、WIRELESS、SECURITY、MANAGEMENT、COMMANDS、ALL、および LOBBY です。 最初の 7 つのロールは、コントローラ GUI のメニュー オプションに対応しており、これら特定のコントローラ機能へのアクセスを許可します。 特定のタスクに対する権限がユーザに与えられていない場合でも、ユーザは読み取り専用モードでそのタスクにアクセスできるようになります。 グループでの必要性に応じて、1 つまたは複数のロールを入力できます。 7 つのロールすべてを指定するには ALL を、ロビー アンバサダー ロールを指定するには LOBBY を使用します。 次の形式を使用してロールを入力します。

role*x=ROLE*

たとえば、特定のユーザ グループに対して WLAN、CONTROLLER、および SECURITY のロールを指定するには、次のテキストを入力します。

```
role1=WLAN
role2=CONTROLLER
role3=SECURITY?
```

あるユーザ グループに 7 つのロールすべてに対するアクセスを付与するには、次のテキストを入力します。

```
role1=ALL?
```

（注） 必ず上記の形式を使用してロールを入力するようにしてください。 ロールはすべて大文字で入力する必要があり、テキスト間にスペースは挿入できません。

（注） MONITOR ロールまたは LOBBY ロールは、その他のロールと組み合わせることはできません。[Custom Attributes] テキストボックスにこれら 2 つのロールのどちらかを指定すると、追加のロールが指定された場合でも、ユーザには MONITOR または LOBBY 権限のみが付与されます。

ステップ 23 [Submit] をクリックして変更を保存します。

TACACS+ の設定（GUI）

ステップ 1 [Security] > [AAA] > [TACACS+] の順に選択します。

ステップ 2 次のいずれかの操作を行います。

- TACACS+ サーバを認証用に設定する場合は、[Authentication] を選択します。
- TACACS+ サーバを認可用に設定する場合は、[Authorization] を選択します。
- TACACS+ サーバをアカウンティング用に設定する場合、[Accounting] をクリックします。

（注） 認証、許可、アカウンティングの設定に使用されるページでは、すべて同じテキスト ボックスが表示されます。 そのため、ここでは [Authentication] ページを例にとって、設定の手順を一度だけ示します。 同じ手順に従って、複数のサービスまたは複数のサーバを設定できます。

（注） TACACS+ を使用して基本的な管理認証が正常に行われるには、WLC で認証サーバと許可サーバを設定する必要があります。 アカウンティングの設定は任意です。

[TACACS+（Authentication、Authorization、または Accounting）Servers] ページが表示されます。 このページでは、これまでに設定されたすべての TACACS+ サーバが表示されます。

- 既存のサーバを削除するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。
- コントローラが特定のサーバに到達できることを確認するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Ping] を選択します。

ステップ 3 次のいずれかの操作を行います。

- 既存の TACACS+ サーバを編集するには、そのサーバのサーバインデックス番号をクリックします。[TACACS+（Authentication, Authorization, or Accounting）Servers > Edit] ページが表示されます。

- TACACS+ サーバを追加するには、[New] をクリックします。 [TACACS+（Authentication,Authorization,or Accounting） Servers > New] ページが表示されます。

ステップ 4 新しいサーバを追加している場合は、[Server Index (Priority)] ドロップダウン リストから数字を選択し、同じサービスを提供するその他の設定済みの TACACS+ サーバに対してこのサーバの優先順位を指定します。 最大 3 台のサーバを設定できます。 コントローラが最初のサーバに接続できない場合、リスト内の 2 番目および必要に応じて 3 番目のサーバへの接続を試行します。

ステップ 5 新しいサーバを追加している場合は、[Server IP Address] テキスト ボックスに TACACS+ サーバの IP アドレスを入力します。

ステップ 6 [Shared Secret Format] ドロップダウン リストから [ASCII] または [Hex] を選択し、コントローラと TACACS+ サーバ間で使用される共有秘密キーの形式を指定します。 デフォルト値は [ASCII] です。

ステップ 7 [Shared Secret] テキスト ボックスと [Confirm Shared Secret] テキスト ボックスに、コントローラとサーバ間で認証に使用される共有秘密キーを入力します。

（注） 共有秘密キーは、サーバとコントローラの両方で同一である必要があります。

ステップ 8 新しいサーバを追加している場合は、[Port Number] テキスト ボックスに、インターフェイス プロトコルに対応する TACACS+ サーバの TCP ポート番号を入力します。 有効な範囲は 1 ～ 65535 で、デフォルト値は 49 です。

ステップ 9 [Server Status] テキスト ボックスから [Enabled] を選択してこの TACACS+ サーバを有効にするか、[Disabled] を選択して無効にします。 デフォルト値は [Enabled] です。

ステップ 10 [Server Timeout] テキスト ボックスに、再送信の間隔を秒単位で入力します。 有効な範囲は 5 ～ 30 秒で、デフォルト値は 5 秒です。

（注） 再認証が繰り返し試行されたり、プライマリ サーバがアクティブで接続可能なときにコントローラがバックアップ サーバにフォールバックしたりする場合には、タイムアウト値を増やすことをお勧めします。

ステップ 11 [Apply] をクリックします。

ステップ 12 次の手順で、TACACS+ DNS パラメータを指定します。

a) [Security] > [AAA] > [TACACS+] > [DNS] を選択します。 [TACACS DNS Parameters] ページが表示されます。

b) [DNS Query] チェックボックスをオンまたはオフにします。

c) [Port Number] テキスト ボックスに、認証ポート番号を入力します。 有効な範囲は 1 ～ 65535 です。 アカウンティング ポート番号は認証ポート番号に 1 を加えた値です。 たとえば、認証ポート番号を 1812 と定義すると、アカウンティング ポート番号は 1813 です。 アカウンティング ポート番号は常に認証ポート番号から取得されます。

d) [Secret Format] ドロップダウン リストから、秘密を設定する形式を選択します。 有効なオプションは [ASCII] と [Hex] です。

e) 選択した形式に応じて秘密を入力して確定します。

（注） すべてのサーバで同じ認証ポートおよび同じ秘密を使用する必要があります。

f) [DNS Timeout] テキスト ボックスに、DNS サーバから最新の更新を取得するために DNS クエリーがリフレッシュされるまでの日数を入力します。

g) [URL] テキスト ボックスに、TACACS+ サーバの完全修飾ドメイン名または絶対ドメイン名を入力します。

h) [Server IP Address] テキスト ボックスに、DNS サーバの IPv4 アドレスを入力します。

（注） IPv6 は TACACS+ DNS ではサポートされません。

i) [Apply] をクリックします。

ステップ 13 [Save Configuration] をクリックします。

ステップ 14 同じサーバ上で、または追加の TACACS+ サーバ上で追加のサービスを設定する場合は、上記の手順を繰り返します。

ステップ 15 [Security] > [Priority Order] > [Management User] の順に選択し、複数のデータベースを設定する際の認証の順序を指定します。 [Priority Order > Management User] ページが表示されます。

ステップ 16 [Order Used for Authentication] テキスト ボックスで、コントローラが管理ユーザを認証する際にどのサーバを優先するかを指定します。

[Not Used] テキスト ボックスと [Order Used for Authentication] テキスト ボックスの間でサーバを移動するには、[>] および [<] ボタンを使用します。 希望するサーバが [Order Used for Authentication] テキスト ボックスに表示されたら、[Up] ボタンと [Down] ボタンを使用して優先するサーバをリストの先頭に移動します。 デフォルトで、ローカル データベースは常に最初に検索されます。 ユーザ名が見つからない場合、コントローラは、RADIUS に設定されている場合は RADIUS サーバへの切り換え、TACACS+ に設定されている場合は TACACS+ サーバへの切り換えを行います。 デフォルトの設定はローカル、RADIUS の順になっています。

ステップ 17 [Apply] をクリックします。

ステップ 18 [Save Configuration] をクリックします。

TACACS+ の設定（CLI）

- 次のコマンドを入力して、TACACS+ 認証サーバを設定します。
  - **config tacacs auth add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*：TACACS+ 認証サーバを追加します。

    このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。
  - **config tacacs auth delete** *index*：以前に追加された TACACS+ 認証サーバを削除します。
  - **config tacacs auth** (**enable** | **disable**} *index*：TACACS+ 認証サーバを有効または無効にします。
  - **config tacacs auth server-timeout** *index timeout*：TACACS+ 認証サーバの再送信のタイムアウト値を設定します。

- 次のコマンドを入力して、TACACS+ 許可サーバを設定します。
  - **config tacacs athr add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*：TACACS+ 許可サーバを追加します。

    このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。
  - **config tacacs athr delete** *index*：以前に追加された TACACS+ 許可サーバを削除します。
  - **config tacacs athr** (**enable** | **disable**} *index*：TACACS+ 許可サーバを有効または無効にします。
  - **config tacacs athr server-timeout** *index timeout*：TACACS+ 許可サーバの再送信のタイムアウト値を設定します。
  - **config tacacs athr mgmt-server-timeout** *index timeout*：TACACS+ 許可サーバのデフォルト管理ログイン サーバ タイムアウトを設定します。
- 次のコマンドを入力して、TACACS+ アカウンティング サーバを設定します。
  - **config tacacs acct add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*：TACACS+ アカウンティング サーバを追加します。

    このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。
  - **config tacacs acct delete** *index*：以前に追加された TACACS+ アカウンティング サーバを削除します。
  - **config tacacs acct** (**enable** | **disable**} *index*：TACACS+ アカウンティング サーバを有効または無効にします。
  - **config tacacs acct server-timeout** *index timeout*：TACACS+ アカウンティング サーバの再送信のタイムアウト値を設定します。
  - **config tacacs athr mgmt-server-timeout** *index timeout*：TACACS+ アカウンティング サーバのデフォルト管理ログイン サーバ タイムアウトを設定します。
- 次のコマンドを入力して、TACACS+ の統計情報を表示します
  - **show tacacs summary**：TACACS+ サーバと統計情報の概要を表示します。
  - **show tacacs auth stats**：TACACS+ 認証サーバの統計情報を表示します。
  - **show tacacs athr stats**：TACACS+ 許可サーバの統計情報を表示します。
  - **show tacacs acct stats**：TACACS+ アカウンティング サーバの統計情報を表示します。
- 次のコマンドを入力して、1 台または複数の TACACS+ サーバの統計情報をクリアします。
  clear stats tacacs [**auth** | **athr** | **acct**] {*index* | *all*}
- 次のコマンドを入力して、複数のデータベースを設定する際の認証の順序を設定します。デフォルト設定では local、radius の順になっています。
  config aaa auth mgmt [**radius** | **tacacs**]

  現在の管理認証サーバの順序を表示するには、**show aaa auth** コマンドを入力します。

- 次のコマンドを入力して、コントローラが TACACS+ サーバに到達できることを確認します。
  ping *server_ip_address*
- 次のコマンドを入力して、TACACS+ DNS パラメータを設定します。
  - **config tacacs dns global** *port-num* {*ascii* | *hex*} *secret*：TACACS+ DNS のグローバル ポート番号と秘密情報を追加します。
  - **config tacacs dns query** *url timeout-in-days*：TACACS+ サーバの FQDN、および DNS サーバから最新の更新を取得するためにリフレッシュが実行されるまでのタイムアウトを設定します。
  - **config tacacs dns serverip** *ip-addr*：DNS サーバの IP アドレスを設定します。
  - **config tacacs dns** {**enable** | **disable**}：DNS クエリーを有効または無効にします。
- 次のコマンドを入力して、TACACS+ のデバッグを有効または無効にします。
  debug aaa tacacs {**enable** | **disable**}
- 次のコマンドを入力して、変更を保存します。
  save config

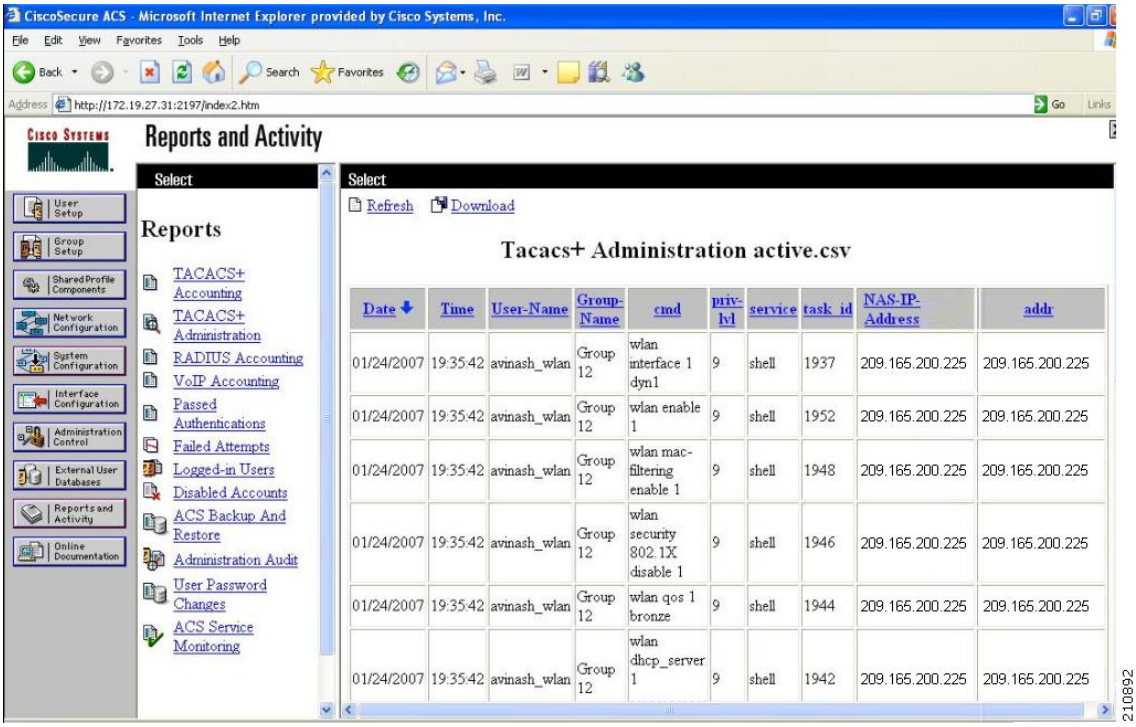
TACACS+ 管理サーバのログの表示

ステップ 1　ACS のメイン ページで、左のナビゲーション ペインから [Reports and Activity] を選択します。

ステップ 2　[Reports] の [TACACS+ Administration] を選択します。

表示するログの日付に対応する .csv ファイルをクリックします。 [TACACS+ Administration .csv] ページが表示されます。

図 *2*：*CiscoSecure ACS* の *[TACACS+ Administration .csv]* ページ



Date	Time	User-Name	Group-Name	cmd	priv-lvl	service	task_id	NAS-IP-Address	addr
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan interface 1 dyn1	9	shell	1937	209.165.200.225	209.165.200.225
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan enable 1	9	shell	1952	209.165.200.225	209.165.200.225
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan mac-filtering enable 1	9	shell	1948	209.165.200.225	209.165.200.225
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan security 802.1X disable 1	9	shell	1946	209.165.200.225	209.165.200.225
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan qos 1 bronze	9	shell	1944	209.165.200.225	209.165.200.225
01/24/2007	19:35:42	avinash_wlan	Group 12	wlan dhcp_server 1	9	shell	1942	209.165.200.225	209.165.200.225

このページは、次の情報を表示します。

- 処理が実行された日付と時刻
- 処理を実行したユーザの名前と割り当てられたロール
- ユーザが属するグループ
- ユーザが実行した特定の処理
- 処理を実行したユーザの権限レベル
- コントローラの IP アドレス
- 処理が実行されたノートパソコンまたはワークステーションの IP アドレス

単一の処理（またはコマンド）が、コマンド内のパラメータごとに、複数回ログ記録される場合があります。 たとえば、**snmp community ipaddr** *ip_address subnet_mask community_name* コマンドを入力すると、ある行では、IP アドレスはログに記録されても、サブネット マスクとコミュニティ名はログに「E」と記録されることがあります。また別の行では、サブネット マスクがログに記録され、IP アドレスとコミュ

ニティ名はログに「E」と記録されることがあります。次の図の例の最初の行と 3 番目の行を参照してください。

図 3：***CiscoSecure ACS の [TACACS+ Administration .csv] ページ***