TACACS+ サーバのクライアントとしての CSS の設定

Terminal Access Controller Access Control System （TACACS+）プロトコルを使用すると、ルータ、network access server （NAS; ネットワーク アクセス サーバ）などのデバイスで、デーモン サーバ経由のアクセスを制御できます。TACACS+ は、NAS とデーモン サーバの間のトラフィックを TCP 通信によってすべて暗号化して、送信内容を保護します。

CSS を TACACS+ サーバのクライアントとして設定し、ユーザ認証の方法、また、設定コマンドやその他のコマンドの権限の付与とアカウンティングの方法とすることもできます。

この章の主な内容は次のとおりです。

- TACACS+ 設定のクイック スタート
- CSS で使用する TACACS+ サーバのユーザ アカウントの設定
- グローバルな TACACS+ アトリビュートの設定
- TACACS+ サーバの定義
- TACACS+ 権限付与の設定
- TACACS+ アカウンティングの設定
- TACACS+ サーバの設定情報の表示

CSS で TACACS+ サーバを設定した後で、仮想認証またはコンソール認証用に TACACS+ 認証を設定します。詳細については、第 1 章「CSS のアクセス制御」を参照してください。

TACACS+ 設定のクイック スタート

表 4-1 に、CSS に TACACS+ 機能を設定するために必要な手順の概要を説明します。それぞれの手順に、作業を行うために必要な CLI コマンドも示します。CLI コマンドに関する各機能とすべてのオプションの詳細については、この手順の後に示す各項を参照してください。

表 4-1　TACACS+ 設定のクイック スタート

作業とコマンドの例
1. Cisco Secure ACS HTML インターフェイスの **Network Configuration** セクション（**Add AAA Client** ページ）で Cisco Secure ACS の認証を設定し、次のフィールドに入力します。 • **AAA Client Hostname** • **AAA Client IP Address** • **Key** • **Authenticate Using** 「認証の設定」を参照してください。
2. CSS　にアクセスするユーザの権限レベルを決定するために、TACACS+ サーバにユーザ アカウントを設定します。「権限付与の設定」を参照してください。
3. （オプション）TACACS+　サーバで使用するグローバルなタイムアウト、キープアライブの間隔、または暗号キーのアトリビュートを設定する場合は、サーバを設定する前にこれらのパラメータを設定する必要があります。グローバルな TACACS+ アトリビュート設定の詳細については、「グローバルな TACACS+ アトリビュートの設定」を参照してください。
4. **tacacs-server** コマンドを使用して、サーバを定義します。このコマンドには、サーバの IP アドレスとポート番号を指定します。オプションで、特定のタイムアウト時間、暗号キーまたはキープアライブ間隔を定義して、このサーバをプライマリ サーバに指定できます。「TACACS+ サーバの定義」を参照してください。 `(config)# tacacs-server 192.168.11.1 12 20 “summary” primary frequency 10`

表 4-1　TACACS+ 設定のクイック スタート（続き）

作業とコマンドの例
5. **virtual authentication** コマンドを使用して、プライマリ、セカンダリ、およびターシャリの仮想認証方式を設定します。 `#(config) virtual authentication primary tacacs`
6. （推奨）TACACS+ サーバの設定を検証します。「TACACS+ サーバの設定情報の表示」を参照してください。 `(config)# show tacacs-server`

次の実行設定例は、表 4-1 のコマンドの入力結果を表しています。

```
!************************* GLOBAL ************************
virtual authentication primary tacacs
tacacs-server 192.168.11.1 12 20 6dab4b3gibcbef3e primary frequency 10
```

CSS で使用する TACACS+ サーバのユーザ アカウントの設定

ここでは、TACACS+ サーバ設定の背景的な情報を説明します。ここで説明する内容は、TACACS+ サーバと、TACACS+ クライアントとして運用する CSS との間で正しく通信するための指針です。

ここでは、Cisco Secure Access Control Server （ACS）TACACS+ のユーザ認証と権限付与に関する推奨設定を説明します。

認証の設定

Cisco Secure ACS の認証を設定するには、Cisco Secure ACS HTML インターフェイスの **Network Configuration** セクション（**Add AAA Client** ページ）に進み、次のフィールドに入力します。

- **AAA Client Hostname**：CSS に割り当てる名前を入力する。
- **AAA Client IP Address** :CSS と Cisco Secure ACS との通信設定に応じて CSS イーサネット管理ポートまたは CSS 回線の IP アドレスを入力する。
- **Key** : CSS と Cisco Secure ACS でトランザクションの認証に使用する共有秘密情報を入力する。正しく動作させるには、CSS と Cisco Secure ACS で同一の共有秘密情報を入力する必要があります。このキーは、大文字と小文字を区別します。
- **Authenticate Using** ：**TACACS+ (Cisco IOS)** を選択する。

権限付与の設定

CSS にアクセスするユーザの特権レベルを決定するために、**privilege** コマンドの実行を許可するか、または拒否するかを、TACACS+ サーバのユーザ アカウントに設定する必要があります。CSS は、**privilege** コマンドの実行権限があるかどうか TACACS+ サーバに照会します。**privilege** コマンドの実行をサーバから許可された場合は、CSS へのアクセス特権（SuperUser モードおよび設定モード）がユーザに認められます。**privilege** コマンドの実行がサーバから拒否された場合は、CSS へのアクセス特権以外のアクセス権限（User モード）がユーザに認められます。

グループ権限付与を設定するには、次の操作を実行します。

1. Cisco Secure ACS HTML インターフェイスの **Group Setup** セクション（**Group Setup Select** ページ）から、TACACS+ 設定を指定するグループを選択します。
2. **Shell Command Authorization Set** ページで、**Per Group Command Authorization** のチェックボックスをクリックします。
3. **Unmatched Cisco IOS Commands** で、privilege コマンドの実行を許可または拒否するように設定します。
   - CSS で SuperUser 特権を持つグループには、**Permit** を選択します。SuperUser は、すべての CSS コマンドを実行できます。
   - CSS で User 権限を持つグループには、**Deny** を選択します。User 権限を持つユーザは、CSS の設定を変更しない CSS コマンド（**show** コマンドなど）を実行できます。

また、次の方法で、グループ認証を設定することもできます。

1. **Shared Profile Components**（**Shell Command Authorization Sets** ページ）を選択します。
2. **Add** ボタンをクリックしてセットを追加するか、または既存のセットを編集します。
3. 名前と説明を入力します。
4. **Unmatched Commands** の隣に移動し、privilege コマンドの実行を許可または拒否するように設定します。
   - CSS で SuperUser 特権を持つユーザには、**Permit** を選択します。SuperUser は、すべての CSS コマンドを実行できます。
   - CSS で User 特権を持つユーザには、**Deny** を選択します。User 権限を持つユーザは、CSS の設定を変更しない CSS コマンド（**show** コマンドなど）を実行できます。
5. **Group Setup Select** ページの **Group Setup** セクションから、TACACS+ 設定を指定するグループを選択します。
6. **Shell Command Authorization Set** セクションで **Assign a Shell Command Authorization Set for any network device** を選択します。
7. リストからセットを選択します。

グループにユーザを追加するには、Cisco Secure ACS HTML インターフェイスの **User Setup** セクションに進みます。

- **User Setup Select** ページでユーザ名を指定します。
- **User Setup Edit** ページで次のように指定します。
  - **Password Authentication** ：リストから適切な認証タイプを選択する。
  - **Password** ：パスワードと確認用パスワードを入力する。
  - **Group** ：事前に作成した TACACS+ グループを選択してユーザを割り当てる。

グローバルな TACACS+ アトリビュートの設定

TACACS+ のタイムアウト時間、暗号キー、およびキープアライブ間隔にはそれぞれデフォルト値があり、TACACS+ サーバにはそれらのデフォルト値が適用されます。サーバの設定時に、これらのアトリビュートをサーバに固有な値に設定することも、サーバに固有な値は設定せず、デフォルト値を使用することもできます。これらのグローバルなアトリビュートのデフォルト値はすべて変更できます。ここでは、次の内容について説明します。

- グローバルな CSS TACACS+ タイムアウト時間の設定
- グローバルな暗号キーの定義
- グローバルな TACACS+ キープアライブ間隔の設定

（注）　TACACS+ サーバの設定時に定義したタイムアウト、暗号キー、キープアライブ間隔は、グローバルなアトリビュートより優先されます（「TACACS+ サーバの定義」参照）。

グローバルな CSS TACACS+ タイムアウト時間の設定

CSS では、設定したすべての TACACS+ サーバで使用するグローバルな TACACS+ タイムアウト時間を定義できます。TACACS+ サーバが使用可能かどうかを判断するために、CSS から TACACS+ サーバに TCP キープアライブ プローブが定期的に送信されます。タイムアウト時間内にサーバがプローブに応答しない場合、CSS ではサーバが使用不能と判断されます。

CSS は、サーバとの通信を試みても、定義されているタイムアウト値以内に応答を得られなかった場合、別のサーバを使用します。設定されている次のサーバとの通信が試みられ、同じ処理が繰り返されます。別の（または 3 つ目）の TACACS+ サーバが認識されている場合は、そのサーバがアクティブなサーバとして選択されます。

CSS から 3 つの TACACS+ サーバのすべてに接続できない場合は、ユーザ認証が実行されず、ユーザは CSS にログインできません。ただし、**virtual** コマンドまたは **console** コマンドを実行して、TACACS+ サーバと RADIUS サーバ（またはローカル サーバ）を併用するように定義している場合を除きます。この 2 つのコマンドの詳細については、第 1 章「CSS のアクセス制御」を参照してください。

タイムアウト時間を変更するには、**tacacs-server timeout** コマンドを使用します。有効な入力値は 1 ～ 255 で、デフォルトは 5 秒です。変更されたグローバルなタイムアウト時間は動的に適用され、新しい値は次の TACACS+ 接続にも自動的に適用されます。

たとえば、タイムアウト時間を 60 秒に設定するには、次のように入力します。

```
#(config) tacacs-server timeout 60
```

タイムアウト時間をデフォルトの 5 秒にリセットするには、次のように入力します。

```
#(config) no tacacs-server timeout
```

（注） TACACS+ サーバの指定時に設定したタイムアウト時間は、グローバルなタイムアウト時間より優先されます（「TACACS+ サーバの定義」参照）。

グローバルな暗号キーの定義

CSS では、設定したすべての TACACS+ サーバとの通信に使用するグローバルな暗号キーを定義できます。CSS と TACACS+ サーバの間の TACACS+ パケット トランザクションを暗号化するには、暗号キーを定義する必要があります。暗号キーを定義しない場合は、パケットは暗号化されません。このキーは、共有秘密情報の値であり、TACACS+ サーバに保存される値と同じになります。CSS とサーバの間の共有秘密情報を指定するには、**tacacs-server key** コマンドを使用します。

共有秘密キーを入力する場合は、クリア テキストを引用符で囲んで入力するか、または、DES 暗号化秘密キーを入力します。クリア テキスト キーは、実行設定に入力される前に DES で暗号化されます。どちらのキーも 100 文字以内で入力します。変更されたキーは動的に適用され、新しい値は次の TACACS+ 接続にも自動的に適用されます。

たとえば、クリア テキスト キーを定義するには、次のように入力します。

```
#(config) tacacs-server key “market”
```

DES 暗号キーを定義するには、次のように入力します。

```
#(config) tacacs-server key acskefterefesdtx
```

キーを削除するには、次のように入力します。

```
#(config) no tacacs-server key
```

（注） TACACS+ サーバの指定時に設定した共有秘密情報は、グローバルな暗号キーより優先されます（「TACACS+ サーバの定義」参照）。

グローバルな TACACS+ キープアライブ間隔の設定

CSS では、設定したすべての TACACS+ サーバで使用するグローバルな TACACS+ キープアライブ間隔を定義できます。TACACS+ サーバが使用可能かどうかを判断するために、CSS から TACACS+ サーバに TCP キープアライブ プローブが定期的に送信されます。設定されたタイムアウト時間内にサーバがプローブに応答しない場合、CSS ではサーバが使用不能と判断されます。

TACACS+ サーバにキープアライブを送信する場合、CSS はサーバとの固定接続を使用しようとします。サーバに固定接続が設定されていない場合、CSS はキープアライブを送信するたびに新しい接続を開きます。

グローバルな TACACS+ キープアライブ間隔を設定するには、グローバル設定モードで **tacacs-server frequency** コマンドを使用します。このコマンドのシンタックスは次のとおりです。

tacacs-server frequency *number*

number 変数は、キープアライブ間隔を秒単位で定義します。0 ～ 255 の整数を入力します。デフォルトは 5 秒です。0 に設定するとキープアライブは無効になります。変更されたキープアライブ間隔は動的に適用され、ただちに新しい値でキープアライブが再開されます。

たとえば、グローバルな TACACS+ キープアライブ間隔を 50 秒に設定するには、次のように入力します。

```
(config)# no tacacs-server frequency 50
```

（注） TACACS+ サーバの指定時に設定したキープアライブ間隔は、グローバルなキープアライブ間隔より優先されます（「TACACS+ サーバの定義」参照）。

グローバルな TACACS+ キープアライブ間隔をデフォルトの 5 秒にリセットするには、**no tacacs-server frequency** コマンドを使用します。

たとえば、次のように入力します。

```
(config)# no tacacs-server frequency
```

TACACS+ サーバの定義

TACACS+ サーバには、TACACS+ の認証情報、権限付与情報、およびアカウンティング データベースが保存されています。CSS には、最大 3 つのサーバを設定できます。ただし、一度に使用できるサーバは 1 つだけです。CSS は、設定されたプライマリ サーバを優先して、利用できるサーバを選択します。CSS からは、定期的に TCP キープアライブ プローブが 5 秒ごとに TACACS+ サーバに送信され、運用状態（Alive、Dying、または Dead）が確認されます。CSS では、TCP キープアライブの間隔を設定できません。

（注） 推奨される TACACS+ サーバ（この例では Cisco Secure Access Control Server）設定の概要については、「TACACS+ 設定のクイック スタート」を参照してください。

タイムアウト時間、キープアライブ間隔、または共有秘密情報などの TACACS+ のグローバルなアトリビュートを TACACS+ サーバに適用するには、グローバルなアトリビュートを設定してからサーバを設定します。変更したグローバルなアトリビュートを設定済みの CSS TACACS+ サーバに適用する場合は、サーバを削除してから再設定してください。

サーバを定義するには、**tacacs-server** コマンドを使用します。このコマンドには、サーバの IP アドレスとポート番号を指定します。オプションで、タイムアウト時間と暗号キーを定義して、このサーバをプライマリ サーバに指定できます。

このグローバル設定コマンドのシンタックスは次のとおりです。

tacacs-server *ip_address port* {*timeout* [**“***cleartext_key***”**|*des_key*]} {**primary**} {**frequency** *number*}

このコマンドの変数とオプションは次のとおりです。

- *ip_address* ：TACACS+ サーバの IP アドレス。IP アドレスはドット付き 10 進表記で入力します。
- *port* ：TACACS+ サーバの TCP ポート。デフォルトのポートは 49 です。1 ～ 65535 のポート番号を入力できます。

- *timeout* ：（オプション）サーバからの応答を待つ時間。有効な入力値は 1 ～ 255 で、デフォルトは 5 秒です。このオプションを定義すると、**tacacs-server timeout** コマンドが無効になります。TACACS+ のタイムアウト時間とグローバルなタイムアウト設定の詳細については「グローバルな CSS TACACS+ タイムアウト時間の設定」を参照してください。
- **“***cleartext_key***”|***des_key*　：（オプション）CSS　とサーバの間の共有秘密情報。CSS と TACACS+ サーバの間の TACACS+ パケット トランザクションを暗号化するには、暗号キーを定義する必要があります。暗号キーを定義しない場合は、パケットは暗号化されません。

  この共有秘密情報の値は、TACACS+ サーバに保存されている値と同じです。共有秘密キーを入力する場合は、クリア テキストを引用符で囲んで入力するか、または、DES 暗号化秘密キーを引用符で囲まずに入力します。クリア テキスト キーは、実行設定に入力される前に DES で暗号化されます。どちらのキーも 100 文字以内で入力します。

  このオプションを定義すると、**tacacs-server key** コマンドが無効になります。グローバルな暗号キーの定義については、「グローバルな暗号キーの定義」を参照してください。
- **primary** ：（オプション）この TACACS+ サーバの優先度を、設定されている他のサーバよりも高く設定する。指定できるプライマリ サーバは、1 つだけです。
- **frequency** *number* ：（オプション）指定された TACACS+ サーバにキープアライブ間隔を設定できるようにする。デフォルトの number 変数は 5 秒です。この変数の範囲は 0 ～ 255 です。0 に設定するとキープアライブは無効になります。このオプションを定義すると、**tacacs-server frequency** コマンドが無効になります。

（注） 特定のサーバのタイムアウト時間や共有秘密情報を変更する場合は、サーバを削除してから、新しいパラメータで再度定義してください。

たとえば、IP アドレスが 192.168.11.1、デフォルト ポートが 49、タイムアウト時間が 12 秒、クリア テキストの共有秘密情報が「summary」、キープアライブ間隔が 10 秒である TACACS+ サーバをプライマリ TACACS+ サーバとして指定するには、次のように入力します。

```
#(config) tacacs-server 192.168.11.1 12 20 “summary” primary frequency 10
```

IP アドレスが 192.168.11.1 でデフォルト ポートが 49 の TACACS+ サーバを削除するには、次のように入力します。

```
#(config) no tacacs-server 192.168.11.1 49
```

TACACS+ サーバを設定した後に、**virtual authentication** コマンドと **console authentication** コマンドを使用して、コンソール ログインと仮想ログイン（ユーザ名とパスワードのペアがローカル ユーザのデータベースに存在しない場合）での TACACS+ 認証を有効にします。この 2 つのコマンドの詳細については、第 1 章「CSS のアクセス制御」を参照してください。

TACACS+ 権限付与の設定

TACACS+ 権限付与を設定すると、ユーザが実行できる CSS コマンドを TACACS+ サーバで個別に制御できます。CSS の権限付与では、コマンド セットが次の 2 種類に分類されます。

- CSS の実行設定を変更するための設定コマンド。たとえば、グローバル設定モードのすべてのコマンドがこのコマンドに該当します。すべてのグローバル設定モード コマンドのリストについては、『*Cisco Content Services Switch Command Reference*』を参照してください。
- 実行設定を変更しない設定用以外のコマンド。これらのコマンドには、モード変更コマンド、表示コマンド、管理コマンドなどが含まれます。たとえば、**cls**（clear screen）、**endbranch**、**help**、**ping**、**show**、**terminal**、**traceroute** などのコマンドがあります。設定用以外のすべてのコマンドのリストについては、『*Cisco Content Services Switch Command Reference*』を参照してください。

（注） CSS に TACACS+ を設定すると、CSS は スクリプトが TACACS+ サーバを通過することを許可しません。CSS はすべての XML コマンドをスクリプトに変換するため、XML コマンドが TACACS+ サーバを通過することも許可しません。

デフォルトでは、権限付与が無効に設定されています。権限付与を有効にすると、試行されたコマンドの実行を許可するか拒否するかが TACACS+ サーバで判断されます。

権限付与を有効にした場合は、TACACS+ サーバと CSS の間の通信によってコマンドの実行が遅延します。TACACS+ サーバに障害が発生すると、すべての権限付与要求が失敗し、ユーザ アクティビティが一時停止します。ただし、別のサーバが接続可能な場合を除きます。この場合にユーザがコマンドを実行できるようにするには、フェールオーバー認証方式をローカル ユーザ データベースに設定します。ユーザは CSS にログインしなおす必要があります。

7.30.1.05 より前のリリースでは、CLI モードの移行時に（設定モードからサービス モードに移る場合など）サービスが存在すると、設定コマンドでもまたは設定以外のコマンドでも、TACACS+ 権限付与が有効になっているかどうかに関係なく、コマンドに対する許可は実行されませんでした。サービスの作成中、設定コマンドの権限付与が有効化されている場合は、TACACS+ サーバに対してユーザにコマンドを実行する権限があるかどうかの照会が行われました。7.30.1.05 以降のソフトウェア バージョンでは、既存のサービス上でモードが移行した場合、設定以外のコマンドが有効化されている場合も、TACACS+ サーバに対してコマンド権限付与要求が送信されます。

実行設定を変更するすべてのコマンドの権限付与を有効にするには、**tacacs-server authorize config** コマンドを使用します。たとえば、次のように入力します。

```
#(config) tacacs-server authorize config
```

実行設定を変更しないすべてのコマンドの権限付与を有効にするには、**tacacs-server authorize non-config** コマンドを使用します。たとえば、次のように設定します。

```
#(config) tacacs-server authorize non-config
```

これらのコマンドに **no** を指定すると、権限付与が無効になります。たとえば、実行設定に影響するコマンドの権限付与を無効にするには、次のように入力します。

```
#(config) no tacacs-server authorize config
```

実行設定に影響しないコマンドの権限付与を無効にするには、次のように入力します。

```
#(config) no tacacs-server authorize non-config
```

TACACS+ サーバへの完全な CSS コマンドの送信

CSS ユーザは、短縮形のシンタックスで入力したコマンドを TACACS+ サーバに送信することができます。デフォルトでは、短縮形でコマンドを入力した場合でも、完全なコマンド シンタックスの形に変換されて送信されます。短縮形のコマンドを完全なシンタックスに変換することにより、TACACS+ 権限付与コマンドが失敗する可能性を減らします。

CSS から完全なコマンドを送らずに、ユーザが入力したとおりにコマンドを送る場合は、コマンドに **no** を指定します。たとえば、次のように入力します。

```
#(config) no tacacs-server send-full-command
```

完全なコマンド シンタックスの送信を再度有効にするには、**tacacs-server send-full-command** コマンドを使用します。たとえば、次のように入力します。

```
#(config) tacacs-server send-full-command
```

TACACS+ アカウンティングの設定

TACACS+ アカウンティングを設定すると、ユーザが実行できるコマンドのアカウンティング レポートを TACACS+ サーバで受信できます。CSS のアカウンティングでは、コマンド セットが次の 2 種類に分類されます。

- CSS の実行設定を変更するための設定コマンド
- 実行設定を変更しない設定用以外のコマンド。これらのコマンドには、モード変更コマンド、表示コマンド、管理コマンドなどが含まれます。

デフォルトでは、CSS のアカウンティングは無効に設定されています。アカウンティングを有効にすると、設定コマンドと非設定コマンドの両方または一方のアカウンティングが可能になります。

（注） TACACS+ サーバに障害が発生しても、ユーザ アクティビティは一時停止しません。

実行設定を変更するすべてのコマンドのアカウンティング レポートを TACACS+ サーバに送信できるようにするには、**tacacs-server account config** コマンドを使用します。たとえば、次のように設定します。

```
#(config) tacacs-server account config
```

実行設定を変更しないすべてのコマンドのアカウンティング レポートを TACACS+ サーバに送信できるようにするには、**tacacs-server account non-config** コマンドを使用します。たとえば、次のように設定します。

```
#(config) tacacs-server account non-config
```

これらのコマンドに **no** を指定すると、アカウンティングが無効になります。たとえば、実行設定に影響するコマンドのアカウンティングを無効にするには、次のように入力します。

```
#(config) no tacacs-server account config
```

実行設定に影響しないコマンドのアカウンティングを無効にするには、次のように入力します。

```
#(config) no tacacs-server account non-config
```

TACACS+ サーバの設定情報の表示

TACACS+ サーバの設定情報を表示するには、**show tacacs-server** コマンドを使用します。この情報を表示するには、次のように入力します。

```
(config)# show tacacs-server
```

表 4-2 に、**show tacacs-server** コマンドで表示されるフィールドを示します。

表 4-2　show tacacs-server コマンドのフィールド

フィールド	説明
IP/Port	TACACS+ サーバの IP アドレスとポート番号
State	内部 TCP キープアライブで判断されるサーバの運用状態（Alive、Dying、または Dead）
Primary	このレコードがプライマリ TACACS+ サーバであるかどうかが表示されます。
Authen	TACACS+ サーバに対する認証要求の数
Author	TACACS+ サーバに対する権限付与要求の数
Account	TACACS+ サーバに対するアカウンティング要求の数
Key	TACACS+ サーバに設定された共有秘密情報
Server Timeout	CSS が TACACS+ サーバからの応答を待機するタイムアウト時間
Server Frequency	TACACS+ サーバのキープアライブ間隔（秒単位）
Global Timeout	CSS が TACACS+ サーバからの応答を待機するグローバルなタイムアウト時間
Global KAL Frequency	TACACS+ サーバのグローバルなキープアライブ間隔（秒単位）

表 4-2　show tacacs-server コマンドのフィールド（続き）

フィールド	説明
Global Key	すべての TACACS+ サーバで使用されるグローバルな共有秘密情報。サーバに対して個別に共有秘密情報が設定されている場合は、個別の共有秘密情報が使用されます。
Authorize Config Commands	設定コマンドが権限付与を受け付けるかどうかが表示されます。
Authorize Non-Config	設定以外のコマンドが権限付与を受け付けるかどうかが表示されます。
Account Config Commands	実行設定を変更するすべてのコマンドのアカウンティング レポートを CSS から TACACS+ サーバに送信するかどうかを示します。
Account Non-Config	実行設定を変更しないすべてのコマンドのアカウンティング レポートを CSS から TACACS+ サーバに送信するかどうかを示します。