RADIUS サーバのクライアントとしての CSS の設定

Remote Authentication Dial-In User Service（RADIUS）プロトコルは、不正なアクセスからネットワークを保護する、分散型のクライアント サーバ プロトコルです。RADIUS では、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を使用して、CSS 認証クライアントと、ユーザ認証およびネットワーク サービス アクセス情報をすべて格納しているアクティブな認証サーバとの間で認証情報と設定情報を交換します。通常、RADIUS ホストは、RADIUS サーバ ソフトウェアを実行するマルチユーザ システムです。

ユーザが、RADIUS クライアントとして稼働中の CSS にリモートからログインすると、CSS は認証要求（ユーザ名、暗号化パスワード、クライアントの IP アドレス、およびポート ID）を中央の RADIUS サーバに送信します。RADIUS サーバは、ユーザ接続要求の受信、ユーザの認証、およびクライアントでユーザにサービスを提供するために必要な設定情報の返信を行います。RADIUS クライアントと RADIUS サーバの間でのやりとりは、共有秘密情報を使用して認証されます。

RADIUS サーバは、認証要求を受信すると、送信側のクライアントを確認してログイン要求と一致するユーザのデータベースを調べます。一定時間内に RADIUS サーバから応答が得られない場合は、事前定義されている回数だけ認証要求が再送信されます。プライマリ サーバが停止した場合やサーバに到達できない場合、RADIUS クライアントは要求を代わりのセカンダリ RADIUS サーバに転送できます。

プライマリ RADIUS サーバとセカンダリ RADIUS サーバの両方が指定された設定では、どちらか一方または両方の RADIUS サーバが到達不可能になると、CSS は自動的にキープアライブ認証要求を送信して、サーバに問い合せます。CSS は、（RADIUS サーバのキーで暗号化された）ユーザ名「query」とパスワード「areyouup」を RADIUS サーバに送信し、サーバの状態を確認します。CSS は、RADIUS サーバが使用可能になるまで、キープアライブ認証要求を送り続けます。

RADIUS サーバ ホスト（プライマリ RADIUS サーバ、およびオプションでセカンダリ RADIUS サーバ）、通信時間間隔の設定、および共有秘密情報テキスト文字列を指定するには、**radius-server** コマンドとそのオプションを使用します。このコマンドは、グローバル設定モードで実行できます。

この章の主な内容は次のとおりです。

- RADIUS 設定のクイック スタート
- CSS で使用するための RADIUS サーバの設定
- プライマリ RADIUS サーバの指定
- セカンダリ RADIUS サーバの指定
- RADIUS サーバのタイムアウトの設定
- RADIUS サーバの再送信回数の設定
- RADIUS サーバのデッドタイムの設定
- RADIUS サーバ設定情報の表示

RADIUS 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 RADIUS 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。

RADIUS 設定のクイック スタート

表 3-1 に、CSS に RADIUS 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 コマンドの各機能とすべてのオプションの詳細については、次の表の後に示す各項目を参照してください。

表 3-1　RADIUS 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、RADIUS 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. **radius-server primary** コマンドを使用して、CSS RADIUS クライアントからのユーザ情報の認証（コンソール認証または仮想認証）に使用するするプライマリ RADIUS サーバを指定します。「プライマリ RADIUS サーバの指定」を参照してください。 `(config)# radius-server primary 172.27.56.76 secret Hello`
4. **radius-server secondary** コマンドを使用して、CSS RADIUS クライアントからのユーザ情報を認証（コンソール認証または仮想認証）するセカンダリ RADIUS サーバを指定します。「セカンダリ RADIUS サーバの指定」を参照してください。 `(config)# radius-server secondary 172.27.56.79 secret Hello`

表 3-1　RADIUS 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。第 1 章「CSS のアクセス制御」を参照してください。 `#(config) virtual authentication primary radius`

6. （推奨）**show radius** コマンドを使用して、RADIUS サーバ設定に関する情報および統計情報を表示します。「RADIUS サーバ設定情報の表示」を参照してください。
`(config)# show radius config all`
`(config)# show radius statistics all`

次の実行設定例は、表 3-1 で説明したコマンドを入力した結果を示しています。

```
!************************** GLOBAL ***************************
  radius-server primary 172.27.56.76 secret Hello auth-port 1645
  radius-server secondary 172.27.56.79 secret Hello auth-port 1645
  virtual authentication primary radius
```

CSS で使用するための RADIUS サーバの設定

ここでは、RADIUS 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、RADIUS サーバと、RADIUS 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。

次の例は、Cisco Secure Access Control Server （ACS）を中央集中型の RADIUS サーバとして CSS とともに使用する場合に推奨する設定です。

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** ：CSS で標準の IETF RADIUS アトリビュートを使用するために、**RADIUS (IETF)** ネットワーク セキュリティ プロトコルを選択する。

権限付与の設定

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、RADIUS サーバにユーザ アカウントを設定する必要があります。

グループ権限を設定するには、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）で、RADIUS 設定を指定するグループを選択します。

2. Cisco Secure ACS HTML インターフェイスの **Group Settings** セクションで、**IETF RADIUS Attributes, [006] Service-Type** チェックボックスをクリックします。次に **Administrative** を選択します。CSS への特権ユーザ（スーパーユーザ）接続に対する RADIUS 認証を有効にするには、**Administrative** を有効にする必要があります。

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 RADIUS グループを選択してユーザを割り当てる。

プライマリ RADIUS サーバの指定

CSS RADIUS クライアントからのユーザ情報の認証（コンソール認証または仮想認証）に使用するするプライマリ RADIUS サーバを指定するには、**radius-server primary** コマンドを使用します。このグローバル設定モードのコマンドのシンタックスは次のとおりです。

radius-server primary *ip_address* **secret** *string* {**auth-port** *port_number*}

このコマンドのオプションと変数は次のとおりです。

- **primary** *ip_address* ：プライマリ RADIUS サーバの IP アドレスまたはホスト名。ドット付き 10 進表記の IP アドレス（たとえば、192.168.11.1）またはニーモニック ホスト名（たとえば、myhost.mydomain.com）で入力します。
- **secret** *string* ：プライマリ RADIUS サーバと CSS RADIUS クライアント間の共有秘密情報文字列。共有秘密情報により、クライアントとプライマリ RADIUS サーバの間で認証トランザクションを行うことができます。共有秘密情報は、大文字と小文字を区別したスペースを含まない 16 文字以内の文字列で入力します。
- **auth-port** *port_number* ：（オプション）RADIUS クライアントから認証パケットを受信するために割り当てられたプライマリ RADIUS サーバの UDP ポート。有効な入力値は 0 ～ 65535 です。デフォルトは 1645 です。

プライマリ RADIUS サーバを指定するには、次のように入力します。

```
(config)# radius-server primary 172.27.56.76 secret Hello auth-port
30658
```

プライマリ RADIUS サーバを削除するには、次のように入力します。

```
(config)# no radius-server primary
```

セカンダリ RADIUS サーバの指定

CSS は、指定したプライマリ RADIUS サーバが使用できない場合に、認証要求をセカンダリ RADIUS サーバに送信します。CSS RADIUS クライアントからのユーザ情報を認証（コンソール認証または仮想認証）するセカンダリ RADIUS サーバを指定するには、**radius-server secondary** コマンドを使用します。

（注） セカンダリ RADIUS サーバの設定は省略可能です。

このグローバル設定モードのコマンドのシンタックスは次のとおりです。

radius-server secondary *ip_address* **secret** *string* {**auth-port** *port_number*}

このコマンドのオプションと変数は次のとおりです。

- **secondary** *ip_address* ：セカンダリ RADIUS サーバの IP アドレスまたはホスト名。ドット付き 10 進表記の IP アドレス（たとえば、192.168.11.1）またはニーモニック ホスト名（たとえば、myhost.mydomain.com）で入力します。
- **secret** *string* ：セカンダリ RADIUS サーバと CSS RADIUS クライアントの間の共有秘密情報文字列。共有秘密情報により、クライアントとセカンダリ RADIUS サーバの間で認証トランザクションを行うことができます。共有秘密情報は、大文字と小文字を区別したスペースを含まない 16 文字以内の文字列で入力します。
- **auth-port** *port_number* ：（オプション）RADIUS クライアントから認証パケットを受信するために割り当てられたセカンダリ RADIUS サーバの UDP ポート。有効な入力値は 0 ～ 65535 です。デフォルトは 1645 です。

セカンダリ RADIUS サーバを指定するには、次のように入力します。

```
(config) radius-server secondary 172.27.56.79 secret Hello auth-port
30658
```

セカンダリ RADIUS サーバを削除するには、次のように入力します。

```
(config)# no radius-server secondary
```

RADIUS サーバのタイムアウトの設定

CSS は、デフォルトで、RADIUS サーバ（プライマリまたはセカンダリ）への認証要求を再送信するまでに、RADIUS サーバからの応答を 10 秒待機します。CSS で認証応答の待機を開始してから RADIUS サーバ（プライマリまたはセカンダリ）へ要求を再送信するまでの時間間隔を指定するには、**radius-server timeout** コマンドを使用します。サーバへの要求の再送信回数を設定するには、**radius-server retransmit** コマンドを使用します（「RADIUS サーバの再送信回数の設定」を参照）。有効な入力値は、1 ～ 255 秒です。

たとえば、RADIUS サーバのタイムアウト間隔を 1 分（60 秒）に設定するには、次のように入力します。

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

RADIUS サーバの再送信要求間隔をデフォルトの 10 秒にリセットするには、次のコマンドを実行します。

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

RADIUS サーバの再送信回数の設定

CSS は、デフォルトで、タイムアウトした RADIUS サーバへの認証要求の再送信を 3 回行った後、サーバが停止しているものと判断して送信を停止します。タイムアウトした RADIUS サーバへの認証要求の再送信を開始してから、サーバが停止しているものと判断して送信を停止するまでの再送信回数を指定するには、**radius-server retransmit** コマンドを使用します。セカンダリ RADIUS サーバが確認されると、そのサーバがアクティブ サーバとして選択されます。有効な入力値は、1 ～ 30 回です。

RADIUS サーバが要求を再送信した CSS に応答しない場合、その RADIUS サーバは停止したものとみなされ、送信が停止されます。また、この時点から **radius-server dead-time** コマンドで定義したデッド タイマーが起動します（「RADIUS サーバのデッドタイムの設定」を参照）。セカンダリ サーバが設定されている場合、CSS はそのセカンダリ サーバに要求を送信します。セカンダリ サーバが要求に応答しなければ、サーバ停止と判断してデッド タイマーを開始します。アクティブなサーバがない場合は、RADIUS プライマリ サーバが有効になるまで、要求の送信は停止します。

たとえば、RADIUS サーバの再送信回数を 5 回に設定するには、次のように入力します。

```
(config)# radius-server retransmit 5
```

RADIUS サーバの要求の再送信回数をデフォルトの 3 回にリセットするには、次のコマンドを実行します。

```
(config)# no radius-server retransmit
```

RADIUS サーバのデッドタイムの設定

CSS は、デッドタイム時間内にプローブ アクセス要求パケットを送信して、RADIUS サーバ（プライマリまたはセカンダリ）が使用できるかどうか、および認証要求を受信できるかどうかを確認します。デッドタイム間隔は、サーバが応答せずに、認証要求の再送信が **radius-server retransmit** コマンドを使って設定した回数に達した時点から開始されます。サーバがプローブ アクセス要求パケットに応答すると、CSS は認証要求をサーバに送信します。

応答がないサーバが動作中であるかどうかを確認する時間間隔を設定するには、**radius-server dead-time** コマンドを使用します。有効な入力値は、1 ～ 255 秒です。デフォルトは 5 秒に設定されています。

プローブ アクセス要求を有効にして、RADIUS サーバのデッドタイムを 15 秒に設定するには、次のように入力します。

```
(config)# radius-server dead-time 15
```

RADIUS サーバのデッドタイムをデフォルトの 5 秒にリセットするには、次のように入力します。

```
(config)# no radius-server dead-time
```

RADIUS サーバ設定情報の表示

RADIUS サーバ設定に関する情報および統計情報を表示するには、**show radius** コマンドを使用します。このコマンドのシンタックスとオプションは次のとおりです。

- **show radius config [all|primary|secondary]** ：タイプで識別される特定のサーバ、またはすべてのサーバの RADIUS 設定情報を表示する。
- **show radius statistics [all|primary|secondary]** ：タイプで識別される特定のサーバ、またはすべてのサーバの RADIUS 認証統計情報を表示する。

プライマリ RADIUS サーバの設定を表示するには、次のように入力します。

```
(config)# show radius config primary
```

セカンダリ RADIUS サーバの認証統計情報を表示するには、次のように入力します。

```
(config)# show radius statistics secondary
```

表 3-2 に、**show radius config** コマンドで表示されるフィールドを示します。

表 3-2　show radius config コマンドのフィールド

フィールド	説明
Server IP Address	指定された RADIUS サーバの IP アドレスまたはホスト名
Secret	指定された RADIUS サーバと CSS RADIUS クライアントの間の共有秘密情報
Port	指定された RADIUS サーバで CSS RADIUS クライアントから認証パケットを受信するために割り当てられた UDP ポート。デフォルトのポート番号は 1645 です。
State	RADIUS サーバの稼働状態（ALIVE、DOWN、UNKNOWN）
Dead Timer	応答しない RADIUS サーバ（プライマリまたはセカンダリ）を CSS がプローブして、稼働しているかどうか、また認証要求を受信できるかどうかを確認する間隔（秒単位）

表 3-2　show radius config コマンドのフィールド（続き）

フィールド	説明
Timeout	CSS RADIUS クライアントが RADIUS サーバからの応答の待機を開始してから、そのサーバへ要求を再送信するまでの間隔（秒単位）
Retransmit Limit	CSS RADIUS クライアントが、タイムアウトした RADIUS サーバへ認証要求の再送信を開始してから、そのサーバへの送信を停止するまでの再送信回数
Probes	RADIUS サーバが利用可能かどうか、およびそのサーバで認証要求を受信できるかどうかを判断する手段として、CSS RADIUS クライアントから自動的に送信されるパケット

表 3-3 に、**show radius statistics** コマンドで表示されるフィールドを示します。

表 3-3　show radius statistics コマンドのフィールド

フィールド	説明
Server IP address	指定された RADIUS サーバの IP アドレスまたはホスト名
Accepts	RADIUS サーバが CSS RADIUS クライアントからの認証要求を受け付けた回数
Requests	CSS RADIUS クライアントが RADIUS サーバへ認証要求を実行した回数
Retransmits	CSS RADIUS クライアントが、タイムアウトが発生した後にアクティブな RADIUS サーバへ認証要求を再送信した回数
Rejects	CSS RADIUS クライアントが認証要求を確立しようとしている間に RADIUS サーバから拒否通知を受信した回数
Bad Responses	CSS RADIUS クライアントが RADIUS サーバから不正な送信を受信した回数
Bad Authenticators	RADIUS サーバが CSS RADIUS クライアントからの認証要求を拒否した回数
Pending Requests	RADIUS サーバに対して保留中の認証要求の数
Timeouts	CSS RADIUS クライアントが、認証要求に対する RADIUS サーバからの応答を待機している間に指定されているタイムアウト間隔に達した回数
Discarded Authentication Requests	プライマリまたはセカンダリの RADIUS サーバが停止している間に破棄された認証要求数