



# WAE での AAA アカウンティングの設定

認証、許可、アカウンティングは、まとめて、AAA ( Authentication, Authorization, and Accounting ) と呼ばれることがあります。AAA アカウンティングは、システム アカウンティングを目的に管理ユーザのアクティビティを追跡する機能です。この章では、WAFS 3.x ソフトウェアを稼働する Wide Area Application Engine( WAE )に AAA アカウンティングを設定する方法について説明します。

この章には、次の項があります。

- [AAA アカウンティングについて、9-2 ページ](#)
- [WAE での AAA アカウンティング設定値の設定、9-5 ページ](#)
- [WAE の AAA アカウンティング設定の表示、9-8 ページ](#)
- [WAE での AAA アカウンティング統計情報の表示とクリア、9-8 ページ](#)



(注)

Cisco WAFS 3.0 ソフトウェアは、FE-511 File Engine と、WAE-611 および WAE-7326 Wide Area Application Engine で動作します。簡潔にするため、説明文の中や使用例のコマンド プロンプトの部分では、単に WAE と記述していますが、特に注釈がないかぎり、3 つのプラットフォームすべてに当てはまります。

この章で取り上げる CLI コマンドの完全な構文と使用方法の詳細については、『Cisco WAFS 3.0 Command Reference』を参照してください。

## AAA アカウンティングについて

AAA アカウンティングは、管理ユーザのアクティビティを追跡します。監査証跡、接続時間や使用したリソース（転送されたバイト数）への課金の基礎情報、レポート、またはセキュリティなどのシステム アカウンティングを目的として使用できます。WAFS 3.x ソフトウェアでは、TACACS+ は AAA アカウンティングをサポートしていますが、RADIUS はサポートしていません。

TACACS+ プロトコルを使用すると、WAE と中央サーバの間で、AAA 情報を効率的に通信できます。TACACS+ は、クライアントとサーバの間に信頼できる接続を確立するために、TCP を使用します。WAE は、認証および許可要求とアカウンティング情報を、指定された TACACS+ サーバへ送信します。TACACS+ を使用して AAA アカウンティングを設定することで、この AAA 情報を中央データベースに格納できます。

4 つの異なるタイプのイベントに対して、AAA アカウンティングを有効にすることができます。表 9-1 を参照してください。

表 9-1 AAA アカウンティングでサポートされるイベントのタイプ

イベントのタイプ	説明および詳細の参照先	対応する WAFS CLI コマンド
システム イベント	リロードなどの管理者に関連付けられていないすべてのシステムレベルのイベントに対するシステム アカウンティング。9-3 ページの「システム アカウンティングについて」を参照してください。	<code>aaa accounting system default {start-stop   stop-only} tacacs</code>
EXEC シェルおよびログイン / ログアウト イベント	EXEC プロセスに対する EXEC シェル アカウンティング（ユーザシェル）。9-3 ページの「EXEC シェル アカウンティングについて」を参照してください。	<code>aaa accounting exec default {start-stop   stop-only   wait-start} tacacs</code>
通常の（非スーパーユーザ）管理 CLI コマンド	通常特権を持つ管理者によって WAE 上で実行されるすべての CLI コマンドに対するコマンド アカウンティング。9-4 ページの「コマンド アカウンティングについて」を参照してください。	<code>aaa accounting commands 0 default {start-stop   stop-only   wait-start} tacacs</code>
スーパーユーザ管理 CLI コマンド	スーパーユーザによって WAE 上で実行されるすべての CLI コマンドに対するコマンド アカウンティング。9-4 ページの「コマンド アカウンティングについて」を参照してください。	<code>aaa accounting commands 15 default {start-stop   stop-only   wait-start} tacacs</code>

管理者は、管理ログイン要求によって、設定、モニタリング、およびトラブルシューティングを目的に、WAE にログインします。管理者は、事前に定義されたスーパーユーザ管理アカウント、または WAE 上に作成されている別の管理アカウントを使用します。WAE は、ローカル データベース、外部 RADIUS サーバ、または外部 TACACS+ サーバのうち 1 つ以上のログイン認証方式を使用して、管理ログイン要求を処理します。この章では、管理ログイン要求とアクティビティに対する AAA アカウンティングを設定する方法を説明します。AAA 認証および許可を設定する方法の詳細については、第 7 章「管理ログインの認証および許可の設定」を参照してください。

## システム アカウンティングについて

システム アカウンティングは、すべてのシステムレベル イベントに関する情報を提供します（たとえば、システム リブート）。TACACS+ サーバのアカウンティング ログ ファイルを通じて、システム アカウンティング情報にアクセスできます。このログ ファイルでは、このタイプのアカウンティング情報用に次のレポート形式を使用しています。

```
WeekDay#Month#Day#Time#Year#CEaddress#username#terminal#RemoteHost#Event#
EventTime#TaskId#Timezone#SystemService#SystemAccountingEvent#EventReason
```

次に、TACACS+ サーバで使用可能なシステム アカウンティング レポートの例をいくつか示します。

```
Wed Apr 14 08:37:14 2004 172.16.0.0 unknown unknown 0.0.0.0 start
start_time=1081909831
task_id=2725    timezone=PST    service=system    event=sys_acct    reason=reload
Wed Apr 14 10:19:18 2004 172.16.0.0 admin ttyS0 0.0.0.0 stop stop_time=1081915955
task_id=5358    timezone=PST    service=system    event=sys_acct    reason=shutdown
```

## EXEC シェル アカウンティングについて

EXEC シェル アカウンティングは、管理者が Telnet、FTP、または SSH（SSH バージョン 1 またはバージョン 2）を使用して、EXEC シェルにログインおよびログアウトしたイベントをレポートします。このタイプのアカウンティングは、ユーザ名、日付、開始および停止時間、アクセスしたサーバの IP アドレス（たとえば、FTP サーバの IP アドレス）を含む、ユーザ EXEC ターミナル セッション（ユーザ シェル） イベントに関する情報を提供します。

TACACS+ サーバのアカウンティング ログ ファイルを通じて、EXEC シェル アカウンティング情報にアクセスできます。このログ ファイルでは、このタイプのアカウンティング情報用に次のレポート形式を使用しています。

```
WeekDay#Month#Day#Time#Year#CEaddress#username#terminal#RemoteHost#Event#
EventTime#TaskId#Timezone#Service
```

次に、TACACS+ サーバで使用可能な EXEC シェル アカウンティング レポートの例を示します。

```
Wed Apr 14 11:19:19 2004 172.16.0.0 super10 pts/0 172.31.0.0 start
start_time=1081919558 task_id=3028    timezone=PST    service=shell
Wed Apr 14 11:19:23 2004 172.16.0.0 super10 pts/0 172.31.0.0
stop stop_time=1081919562 task_id=3028    timezone=PST    service=shell
Wed Apr 14 11:22:13 2004 172.16.0.0 normal20 pts/0 via5.abc.com start
start_time=1081919732 task_id=3048    timezone=PST    service=shell
Wed Apr 14 11:22:16 2004 172.16.0.0 normal20 pts/0 via5.abc.com stop
stop_time=1081919735 task_id=3048    timezone=PST    service=shell
Wed Apr 14 11:25:29 2004 172.16.0.0 admin ftp via5.abc.com start start_time=1081919928
task_id=3069    timezone=PST    service=shell
Wed Apr 14 11:25:33 2004 172.16.0.0 admin ftp via5.abc.com stop
stop_time=1081919931
task_id=3069    timezone=PST    service=shell
```

## コマンド アカウンティングについて

WAE は、WAE (EXEC モードまたはコンフィギュレーション モードのどちらか) 上で実行される各 CLI コマンドに関する情報を記録します。各コマンドのアカウンティング レコードには、次の情報が含まれます。

- 実行されたコマンドの構文。
- 特定の CLI コマンドを実行した管理者のユーザ名。
- 特定の CLI コマンドを実行した管理者の特権レベル。通常特権 (特権レベル 0) では、WAE への限定されたアクセスが許可され、スーパーユーザ特権 (特権レベル 15) では、モニタリング、設定、またはトラブルシューティングを実行するための WAE への無制限のアクセスが許可されます。コマンド アカウントでは、特定の管理者によって実行された、コンフィギュレーション モードおよび EXEC モードのすべての CLI コマンドについては、同じ特権レベルをレポートします。

記録される CLI コマンドの特権レベルは、ログインしたユーザの特権レベルと同じです。

- スーパーユーザ特権を持つ管理者は、特権レベル 15 としてアカウンティング レコードに記録されます。
- 通常特権を持つ管理者は、特権レベル 0 としてアカウンティング レコードに記録されます。
- 各コマンドが実行された日付と時刻。

TACACS+ サーバのアカウンティング ログ ファイルを通じて、コマンド アカウンティング情報にアクセスできます。このログ ファイルでは、このタイプのアカウンティング情報用に次のレポート形式を使用しています。

```
WeekDay#Month#Day#Time#Year#CEaddress#username#terminal#RemoteHost#Event#
EventTime#TaskId#Timezone#Service#PrivilegeLevel#CLICommand
```

次に、TACACS+ サーバで使用可能なコマンド アカウンティング レポートの例をいくつか示します。

```
Wed Apr 14 12:35:38 2004 172.16.0.0 admin ttyS0 0.0.0.0 start start_time=1081924137
task_id=3511 timezone=PST service=shell -lvl=0 cmd=logging console enable
Wed Apr 14 12:35:39 2004 172.16.0.0 admin ttyS0 0.0.0.0 stop stop_time=1081924137
task_id=3511 timezone=PST service=shell priv-lvl=0 cmd=logging console enable
```

コマンド アカウンティング以外に、WAE は実行されたすべての CLI コマンドをシステム ログ (syslog) に記録します。メッセージの形式は、次のとおりです。

```
ce_syslog(LOG_INFO, CESM_PARSER, PARSER_ALL, CESM_350232,
"CLI_LOG %s: %s \n", __FUNCTION__, pd->command_line);
```

## WAE での AAA アカウンティング設定値の設定

AAA アカウンティングを WAE に設定する場合は、次のガイドラインにしたがってください。

- WAE は、AAA アカウンティング情報を TACACS+ サーバにのみ送信し、コンソールまたはその他のデバイスには送信しません。
- RADIUS を使用した AAA アカウンティングは、現在、サポートされていません。
- デフォルトでは、AAA アカウンティングは WAE 上ではディセーブルです。WAE 上の AAA をイネーブルにして設定するには、CLI を使用する必要があります（現在、この機能は WAFS Manager GUI を使用して設定することはできません）。
- AAA アカウンティングを有効にすると、`aaa accounting` コマンドのオプションを使用して、いつ TACACS+ アカウンティングを実行するかを指定できます。
  - **start-stop** WAE は、プロセスの最初に開始レコード アカウンティング通知を、プロセスの終わりに停止レコードを、TACACS+ アカウンティング サーバへ送信します。開始アカウンティング レコードは、バックグラウンドで送信されます。開始アカウンティング レコードが TACACS+ アカウンティング サーバによって受信応答されたかどうかに関係なく、要求されたユーザ プロセスが開始します。
  - **stop-only** WAE は、指定されたアクティビティまたはイベントの終わりに、停止レコード アカウンティング通知を TACACS+ アカウンティング サーバへ送信します。

TACACS+ を使用して AAA アカウンティングをサポートするように WAE を設定する手順は、次のとおりです。

ステップ 1 少なくとも 1 台の TACACS+ サーバが WAE に設定されていることを確認します。



(注) 最初に WAE に TACACS+ サーバを設定していないと、WAE に AAA アカウンティング設定値を設定することはできません。たとえば、TACACS+ キー、および WAE が AAA 情報を送信する TACACS+ サーバのホスト名または IP アドレスを指定する必要があります。WAE には、TACACS+ サーバ設定は事前には定義されていません。

a. WAE に TACACS+ キーを指定します。

```
WAE(config)# tacacs key key
```

*key* は、WAE が TACACS+ サーバとの通信に使用する秘密鍵です。デフォルト値はありません。必ず、TACACS+ サーバにも同じ TACACS+ キーを指定してください。たとえば、キーとして「abc」を指定するには、次のコマンドを入力します。

```
WAE(config)# tacacs key abc
```

b. 特定の TACACS+ サーバをアカウンティングサーバとして指定します。

プライマリ TACACS+ サーバは明示的に指定します。そうしないと、WAE が自分で決定してしまいます。1 台のプライマリ TACACS+ サーバと 2 台のバックアップ TACACS+ サーバを設定できます。TACACS+ は、通信用の標準ポートとして、ポート 49 を使用します。`tacacs host` グローバル コンフィギュレーション コマンドを使用すると、複数の TACACS+ サーバを指定できます。

```
WAE(config)# tacacs host ip_addr [primary]
```

次の例では、`primary` オプションを使用して、IP アドレス 172.16.50.1 の TACACS+ サーバをプライマリサーバとして明示的に設定しています。

```
WAE(config)# tacacs host 172.16.50.1 primary
```

次の例では、IP アドレス 172.16.50.2 の TACACS+ サーバをバックアップサーバとして設定しています。primary キーワードが指定されていないため、このサーバがバックアップサーバとして設定されます。

```
WAE(config)# tacacs host 172.16.50.2
```

WAE に TACACS+ サーバを設定する方法の詳細については、7-11 ページの「TACACS+ サーバ認証の設定値の指定」を参照してください。

- ステップ 2 **aaa accounting system default tacacs** 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、システム イベントのアカウントングを有効にし、アカウントングをいつ実行するかを指定します。

```
aaa accounting system default {start-stop | stop-only} tacacs
```

次の例では、WAE がすべてのシステム アクティビティを記録するように設定されています。また、指定されたアクティビティまたはイベントの終わりに、停止レコード アカウンティング通知を TACACS+ アカウンティングサーバへ送信するように、WAE を設定しています。

```
WAE(config)# aaa accounting system default stop-only tacacs
```

- ステップ 3 **EXEC モード プロセス**に対するアカウントングを有効にするには、**aaa accounting exec default {start-stop | stop-only | wait-start} tacacs** 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、アカウントングをいつ実行するかを指定します。

次の例では、WAE がすべてのユーザ EXEC セッションを記録するように設定されています。また、プロセスの最初に開始レコード アカウンティング通知を、プロセスの終わりに停止レコードを、TACACS+ サーバへ送信するように WAE を設定しています。

```
WAE(config)# aaa accounting exec default start-stop tacacs
```

- ステップ 4 通常特権レベル（特権レベル 0）のすべての CLI コマンドに対するアカウントングを有効にするには、**aaa accounting commands 0 default {start-stop | stop-only} tacacs** 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、アカウントングをいつ実行するかを指定します。fm

次の例では、通常特権（特権レベル 0）のアカウントを使用して WAE にログインした管理者が実行したすべての CLI コマンドを記録するように、WAE が設定されています。また、プロセスの最初に開始レコード アカウンティング通知を、プロセスの終わりに停止レコードを、TACACS+ サーバへ送信するように WAE を設定しています（「プロセス」は、限定された特権（特権レベル 0）を持つ管理者によって実行された各 CLI コマンドです）。

```
WAE(config)# aaa accounting commands 0 default start-stop tacacs
```

- ステップ 5 スーパーユーザ特権レベルのすべてのコマンドに対するアカウントングを有効にするには、**aaa accounting commands 15 default {start-stop | stop-only} tacacs** 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、アカウントングをいつ実行するかを指定します。

次の例では、スーパーユーザによって実行されたすべての CLI コマンドを記録するように WAE を設定しています。また、プロセスの最初に開始レコード アカウンティング通知を、プロセスの終わりに停止レコードを、TACACS+ サーバへ送信するように WAE を設定しています（「プロセス」は、スーパーユーザ（特権レベル 15 を持つ）によって実行された各 CLI コマンドです）。

```
WAE(config)# aaa accounting commands 15 default start-stop tacacs
```

ステップ 6 WAE に AAA アカウンティングを設定した後、要望通りに設定されたことを確認するため、現在のアカウンティング設定を表示します。

```
WAE# show aaa accounting
Accounting Type Record event(s) Protocol
-----
Exec shell      start-stop      TACACS+
Command level 0 start-stop      TACACS+
Command level 15 start-stop      TACACS+
System         stop-only       TACACS+
```

---

## WAE の AAA アカウンティング設定の表示

WAE の現在の AAA 設定を表示するには、`show aaa accounting EXEC` コマンドを入力します。

```
WAE# show aaa accounting
Accounting Type   Record event(s)  Protocol
-----
Exec shell        unknown          unknown
Command level 0   unknown          unknown
Command level 15  unknown          unknown
System            start-stop       TACACS+
```

出力例が示すとおり、このコマンドは、次のアカウンティング タイプの AAA アカウンティング設定を表示します。

- EXEC シェル (EXEC プロセスに対するアカウンティング (ユーザ シェル))
- 通常特権を持つ管理者のコマンド レベル (特権レベル 0)
- スーパーユーザ特権を持つ管理者のコマンド レベル (特権レベル 15)
- システム (リロードなどの管理者に関連付けられていないすべてのシステムレベル イベントに対するアカウンティング)

## WAE での AAA アカウンティング統計情報の表示とクリア

WAE で AAA アカウンティング統計情報を表示するには、`show statistics tacacs EXEC` コマンドを入力します。

```
WAE# show statistics tacacs
TACACS+ Statistics
-----
Authentication:
  Number of access requests:          0
  Number of access deny responses:    0
  Number of access allow responses:   0

Authorization:
  Number of authorization requests:    0
  Number of authorization failure responses: 0
  Number of authorization success responses: 0

Accounting:
  Number of accounting requests:       0
  Number of accounting failure responses: 0
  Number of accounting success responses: 15
```

WAE で TACACS+ アカウンティング統計情報をクリアするには、`clear statistics tacacs EXEC` コマンドを入力します。