アカウンティングの設定

AAA アカウンティング機能を使用すると、ユーザーがアクセスするサービス、およびユーザーが消費するネットワーク リソース量を追跡できます。AAA アカウンティングをイネーブルにすると、ネットワーク アクセス サーバーから TACACS+ または RADIUS セキュリティ サーバー（実装しているセキュリティ手法によって異なります）に対して、アカウンティング レコードの形式でユーザー アクティビティがレポートされます。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを分析して、ネットワーク管理、クライアント課金、および監査に利用できます。

アカウンティングを設定するための前提条件

次のタスクを実行してから、名前付き方式リストを使用してアカウンティングを設定します。

- ネットワーク アクセス サーバで AAA をイネーブルにします。
- RADIUS または TACACS+ 認可が発行されている場合、RADIUS または TACACS+ セキュリティ サーバの特性を定義します。シスコのネットワーク アクセス サーバを設定して RADIUS セキュリティ サーバと通信する方法の詳細については、「Configuring RADIUS」の章を参照してください。シスコのネットワーク アクセス サーバを設定して TACACS+ セキュリティ サーバと通信する方法の詳細については、「Configuring TACACS+」の章を参照してください。

アカウンティングの設定の制約事項

AAA アカウンティング機能には次の制限があります。

- アカウンティング情報は、最大 4 台の AAA サーバに同時送信できます。
- Service Selection Gateway（SSG）制限：SSG システムの場合、**aaa accounting network broadcast** コマンドを実行すると、**start-stop** アカウンティングレコードのみがブロードキャストされます。**ssg accounting interval** コマンドを使用して中間アカウンティングレコードを設定する場合、中間アカウンティングレコードは、設定したデフォルトRADIUSサーバーにのみ送信されます。

アカウンティングの設定に関する情報

アカウンティングの名前付き方式リスト

認証および認可方式リストと同様に、アカウンティングの方式リストには、アカウンティングの実行方法とその方式を実行するシーケンスが定義されています。

アカウンティングの方式指定リストには、特定のセキュリティプロトコルを指定し、アカウンティングサービスの特定の行またはインターフェイスに使用できます。唯一の例外はデフォルトの方式リスト（偶然に「default」と名前が付けられている）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストは、順に照会するアカウンティング方式（RADIUS、TACACS+ など）を記述する指定リストです。方式リストでは、アカウンティングに1つまたは複数のセキュリティプロトコルを指定できます。そのため、最初の方式が失敗した場合にアカウンティングのバックアップ システムを確保できます。Cisco IOS XE ソフトウェアでは、方式リストのうち、アカウンティングをサポートする最初の方式が使用されます。その方式が応答しない場合、方式リストの次のアカウンティング方式が選択されます。このプロセスは、リストのいずれかのアカウンティング方式と通信に成功するか、定義されているすべての方式が試行されるまで継続されます。

（注） Cisco IOS XE ソフトウェアでは、前の方式からの応答がない場合にのみ、リストの次のアカウンティング方式でアカウンティングが試行されます。このサイクルの任意の時点でアカウンティングが失敗した場合（つまり、セキュリティ サーバーからユーザー アクセスの拒否応答が返される場合）、アカウンティング プロセスは停止し、その他のアカウンティング方式は試行されません。

アカウンティング方式リストは、要求されるアカウンティングの種類によって変わります。AAA は、次の 6 種類のアカウンティングをサポートしています。

- Network：パケットやバイト カウントなど、すべての PPP、SLIP、または ARAP セッションに関する情報を提供します。
- EXEC：ネットワーク アクセス サーバのユーザ EXEC ターミナル セッションに関する情報を提供します。
- Command：ユーザが発行する EXEC モード コマンドに関する情報を提供します。コマンド アカウンティングは、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、アカウンティング レコードを生成します。
- Connection：Telnet、ローカルエリア トランスポート（LAT）、TN3270、パケット アセンブラ/ディスアセンブラ（PAD）、rlogin などのネットワーク アクセス サーバから行われたすべてのアウトバンド接続に関する情報を出力します。
- System：システムレベルのイベントに関する情報を提供します。
- Resource：ユーザ認証に成功したコールの「開始」および「終了」レコードを提供します。また、認証に失敗したコールの「終了」レコードを提供します。

（注） システム アカウンティングは、名前付きアカウンティング リストを使用しません。システム アカウンティングのデフォルト リストだけを定義できます。

方式指定リストが作成されると、指定したアカウンティング タイプのアカウンティング方式のリストが定義されます。

アカウンティング方式リストを特定の回線またはインターフェイスに適用してから、定義済み方式のいずれかを実行する必要があります。唯一の例外は、デフォルトの方式リスト（「default」という名前）です。特定のアカウンティングの種類の **aaa accounting** コマンドを、名前付き方式リストを指定しないで発行した場合、名前付き方式リストが明示的に定義されているものを除いて、すべてのインターフェイスまたは回線にデフォルトの方式リストが自動的に適用されます（定義済みの方式リストは、デフォルトの方式リストに優先します）。デフォルトの方式リストが定義されていない場合、アカウンティングは実行されません。

ここでは、次の内容について説明します。

方式リストとサーバ グループ

サーバー グループは、方式リストに使用する既存の RADIUS または TACACS+ サーバー ホストをグループ化する方法の 1 つです。次の図に、4 台のセキュリティ サーバ（R1 と R2 は RADIUS サーバ、T1 と T2 は TACACS+ サーバ）が設置された一般的な AAA ネットワーク設定を示します。R1 と R2 は RADIUS サーバーのグループから構成されます。T1 と T2 は TACACS+ サーバーのグループから構成されます。

Cisco IOS XE ソフトウェアでは、RADIUS および TACACS+ サーバ設定はグローバルです。サーバー グループを使用して、設定済みのサーバー ホストのサブセットを指定できます。このようなサーバー グループは、特定のサービスに使用できます。たとえば、サーバー グループを使用すると、R1 と R2 を個別のサーバー グループ（SG1 と SG2）として定義し、T1 と T2 を個別のサーバー グループ（SG3 と SG4）として定義できます。つまり、R1 と T1（SG1 と SG3）を方式リストに指定できるか、または R2 と T2（SG2 と SG4）を方式リストに指定できます。そのため、RADIUS および TACACS+ のリソースを割り当てる場合の柔軟性が高くなります。

サーバ グループには、1 台のサーバに対して複数のホストエントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホストエントリが 1 つのサービス（アカウンティングなど）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。この場合、最初のホスト エントリがアカウンティング サービスを提供できなかった場合、ネットワーク アクセス サーバは同じ装置上でアカウンティング サービス用に設定されている 2 番めのホストエントリを試行します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

DNIS 番号に基づくサーバ グループの設定およびサーバ グループの設定の詳細については、『*Cisco IOS XE Security Configuration Guide: Securing User Services* Release 2』の「Configuring RADIUS」または「Configuring TACACS+」を参照してください。

AAA アカウンティング方式

Cisco IOS XE はアカウンティングについて次の 2 つの方式をサポートします。

- TACACS+：ネットワーク アクセス サーバは、アカウンティング レコードの形式で TACACS+ セキュリティ サーバに対してユーザ アクティビティを報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。
- RADIUS：ネットワーク アクセス サーバは、アカウンティング レコードの形式で RADIUS セキュリティ サーバに対してユーザ アクティビティを報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。

（注） CSCuc32663 では、パスワードおよびアカウンティング ログは、TACACS+ または RADIUS セキュリティ サーバーへ送信される前にマスクされます。マスクされていない情報を TACACS+ または RADIUS セキュリティサーバに送信するには、**aaa accounting commands visible-keys** コマンドを使用します。

アカウンティング レコードの種類

最小限のアカウンティングの場合、**stop-only** キーワードを使用します。このキーワードによって、要求されたユーザープロセスの終了時に、終了レコードアカウンティング通知を送信するよう、指定した方式（RADIUS または TACACS+）に指示します。詳細なアカウンティング情報が必要な場合、**start-stop** キーワードを使用して、要求されたイベントの開始時には開始アカウンティング通知、そのイベントの終了時には修理用アカウンティング通知を送信します。この回線またはインターフェイスですべてのアカウンティング アクティビティを終了するには、**none** キーワードを使用します。

アカウンティング方式

次の表に、サポートされるアカウンティング キーワードを示します。

表 *1 : AAA* アカウンティング方式

キーワード	説明
group radius	アカウンティングにすべての RADIUS サーバーのリストを使用します。
group tacacs+	アカウンティングにすべての TACACS+ サーバーのリストを使用します。
group group-name	*group-name* サーバー グループで定義したように、アカウンティングのための RADIUS サーバーまたは TACACS+ サーバーのサブセットを使用します。

method 引数は、認証アルゴリズムが試行する実際の方式を指します。追加の認証方式は、直前の方式で（失敗した場合ではなく）エラーが返された場合にのみ使用されます。他のすべての方式がエラーを返しても、認証に成功したことを指定するには、コマンドで追加の方式を指定します。たとえば、TACACS+ 認証がエラーを返す場合に認証のバックアップ方式として RADIUS を指定する acct_tac1 という方式リストを作成するには、次のコマンドを入力します。

```
aaa accounting network acct_tac1 stop-only group tacacs+ group radius
```

aaa accounting コマンドで名前付きリストが指定されて「いない」場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。

たとえば、ログイン時のユーザー認証のデフォルト方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa accounting network default stop-only group radius
```

AAA アカウンティングは、次の方式をサポートします。

- **group tacacs** ：ネットワーク アクセス サーバーからアカウンティング情報を TACACS+ セキュリティサーバーに送信するようにするには、**group tacacs+** 方式キーワードを使用します。

- **group radius** ：ネットワーク アクセス サーバーからアカウンティング情報を RADIUS セキュリティサーバーに送信するようにするには、**group radius** 方式キーワードを使用します。

（注） SLIP のアカウンティング方式リストは、関連インターフェイスで PPP に設定されているすべての方式に従います。特定のインターフェイスに定義および適用されるリストがない場合（または PPP 設定が指定されていない場合）、アカウンティングのデフォルト設定が適用されます。

- **group** *group-name* ：RADIUS または TACACS+ サーバーのサブセットを指定して、アカウンティング方式として使用するには、**group** *group-name* 方式を指定して **aaa accounting** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group loginrad** のメンバを最初に定義します。

```
aaa group server radius loginrad
 server 172.16.2.3
 server 172.16.2 17
 server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバーがグループ *loginrad* のメンバとして指定されます。

他の方式リストが定義されていない場合、ネットワークアカウンティングの方式として**group loginrad** を指定するには、次のコマンドを入力します。

```
aaa accounting network default start-stop group loginrad
```

アカウンティング方式としてグループ名を使用するには、事前にRADIUSまたはTACACS+セキュリティ サーバーとの通信をイネーブルにする必要があります。

AAA アカウンティング タイプ

名前付きアカウンティング方式リストは、指定したタイプのアカウンティングに固有です。

- **network**：すべてのネットワーク関連サービス要求（SLIP、PPP、PPP NCP、ARAP などのプロトコル）について認可をイネーブルにする方式リストを作成するには、**aaa accounting** コマンドで**network** キーワードを使用します。たとえば、ARAP（ネットワーク）セッションにアカウント情報を提供する方式リストを作成するには、**accounting** コマンドで **arap** キーワードを使用します。
- **exec**：ネットワーク アクセス サーバー上のユーザー EXEC ターミナルセッションに関するアカウンティングレコード（ユーザー名、日付、開始時刻、終了時刻など）を提供する方式リストを作成するには、**exec** キーワードを使用します。

- **commands**：特定の特権レベルに関連付けられた特定の EXEC コマンドに関するアカウンティング情報を提供する方式リストを作成するには、**commands** キーワードを使用します。
- **connection**：ネットワーク アクセス サーバーから開始されるすべての発信接続に関するアカウンティング情報を提供する方式リストを作成するには、**connection** キーワードを使用します。
- resource：ユーザ認証に成功したコールまたは認証に失敗したコールのアカウンティング レコードを提供する方式リストを作成します。

（注） システム アカウンティングは、名前付き方式リストをサポートしません。

ネットワーク アカウンティング

ネットワーク アカウンティングは、パケットやバイト カウントなど、すべての PPP、SLIP、または ARAP セッションに関する情報を提供します。

次に、EXEC セッションを介して着信する PPP ユーザの RADIUS ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:44:45 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = “0000000D”
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”

Wed Jun 27 04:45:00 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = “0000000E”
        Framed-IP-Address = “10.1.1.2”
        Framed-Protocol = PPP
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
Wed Jun 27 04:47:46 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
```

```
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = “0000000E”
        Framed-IP-Address = “10.1.1.2”
        Framed-Protocol = PPP
        Acct-Input-Octets = 3075
        Acct-Output-Octets = 167
        Acct-Input-Packets = 39
        Acct-Output-Packets = 9
        Acct-Session-Time = 171
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
Wed Jun 27 04:48:45 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 5
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “408”
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = “0000000D”
        Acct-Delay-Time = 0
        User-Id = “username1”
        NAS-Identifier = “172.16.25.15”
```

次に、最初にEXECセッションを開始したPPPユーザのTACACS+ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:00:35 2001 172.16.25.15    username1   tty4    562/4327528
starttask_id=28      service=shell
Wed Jun 27 04:00:46 2001 172.16.25.15    username1   tty4 562/4327528    starttask_id=30
      addr=10.1.1.1   service=ppp
Wed Jun 27 04:00:49 2001 172.16.25.15    username1   tty4    408/4327528     update
   task_id=30      addr=10.1.1.1   service=ppp     protocol=ip     addr=10.1.1.1
Wed Jun 27 04:01:31 2001 172.16.25.15    username1   tty4    562/4327528     stoptask_id=30
       addr=10.1.1.1   service=ppp     protocol=ip     addr=10.1.1.1   bytes_in=2844
     bytes_out=1682  paks_in=36      paks_out=24     elapsed_time=51
Wed Jun 27 04:01:32 2001 172.16.25.15    username1   tty4    562/4327528     stoptask_id=28
       service=shell   elapsed_time=57
```

（注） アカウンティング パケット レコードの正確なフォーマットは、セキュリティ サーバ デーモンに応じて変わります。

次に、autoselectを介して着信するPPPユーザのRADIUSネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:30:52 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 3
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “562”
        Acct-Status-Type = Start
```

```
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = "0000000B"
        Framed-Protocol = PPP
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:36:49 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 3
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "562"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Framed
        Acct-Session-Id = "0000000B"
        Framed-Protocol = PPP
        Framed-IP-Address = "10.1.1.1"
        Acct-Input-Octets = 8630
        Acct-Output-Octets = 5722
        Acct-Input-Packets = 94
        Acct-Output-Packets = 64
        Acct-Session-Time = 357
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、autoselect を介して着信する PPP ユーザの TACACS+ ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:02:19 2001 172.16.25.15    username1   Async5  562/4327528
starttask_id=35      service=ppp
Wed Jun 27 04:02:25 2001 172.16.25.15    username1   Async5  562/4327528     update
   task_id=35      service=ppp     protocol=ip     addr=10.1.1.2
Wed Jun 27 04:05:03 2001 172.16.25.15   username1   Async5  562/4327528    stoptask_id=35
       service=ppp     protocol=ip     addr=10.1.1.2   bytes_in=3366   bytes_out=2149
     paks_in=42      paks_out=28     elapsed_time=164
```

EXEC アカウンティング

EXEC アカウンティングは、ネットワーク アクセス サーバ上にあるユーザ EXEC ターミナル セッション（ユーザ シェル）に関する情報を提供します。たとえば、ユーザ名、日付、開始時刻と終了時刻、アクセス サーバの IP アドレス、および（ダイヤルイン ユーザの場合）発信元の電話番号などです。

次に、ダイヤルイン ユーザの RADIUS EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:26:23 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 1
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329483"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000006"
```

```
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
Wed Jun 27 04:27:25 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 1
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329483"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000006"
        Acct-Session-Time = 62
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、ダイヤルイン ユーザの TACACS+ EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:46:21 2001        172.16.25.15    username1   tty3    5622329430/4327528
 start    task_id=2       service=shell
Wed Jun 27 04:08:55 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=2       service=shell   elapsed_time=1354
```

次に、Telnet ユーザの RADIUS EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:48:32 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 26
        User-Name = "username1"
        Caller-ID = "10.68.202.158"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000010"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:48:46 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 26
        User-Name = "username1"
        Caller-ID = "10.68.202.158"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Exec-User
        Acct-Session-Id = "00000010"
        Acct-Session-Time = 14
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、Telnet ユーザの TACACS+ EXEC アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:06:53 2001        172.16.25.15    username1   tty26   10.68.202.158
starttask_id=41      service=shell
```

```
Wed Jun 27 04:07:02 2001        172.16.25.15    username1   tty26   10.68.202.158
stoptask_id=41       service=shell   elapsed_time=9
```

コマンド アカウンティング

コマンド アカウンティングは、ネットワーク アクセス サーバで実行される各特権レベルの EXEC シェル コマンドに関する情報を提供します。各コマンド アカウンティング レコードには、その特権レベルで実行されるコマンド、各コマンドが実行された日時、および実行したユーザのリストが含まれます。

次に、特権レベル 1 の TACACS+ コマンド アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:46:47 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=3       service=shell   priv-lvl=1      cmd=show version <cr>
Wed Jun 27 03:46:58 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=4       service=shell   priv-lvl=1      cmd=show interfaces <cr>
Wed Jun 27 03:47:03 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=5       service=shell   priv-lvl=1      cmd=show ip route <cr>
```

次に、特権レベル 15 の TACACS+ コマンド アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:47:17 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=6       service=shell   priv-lvl=15     cmd=configure terminal <cr>
Wed Jun 27 03:47:21 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=7       service=shell   priv-lvl=15     cmd=interface
GigabitEthernet0/0/0 <cr>
Wed Jun 27 03:47:29 2001        172.16.25.15    username1   tty3    56223294304327528
stop     task_id=8       service=shell   priv-lvl=15     cmd=ip address 10.1.1.1
255.255.255.0 <cr>
```

（注） シスコの RADIUS 実装は、コマンド アカウンティングをサポートしていません。

接続アカウンティング

接続アカウンティングは、Telnet、LAT、TN3270、PAD、rlogin などのネットワーク アクセス サーバから行われるすべての発信接続に関する情報を提供します。

次に、発信 Telnet 接続の RADIUS 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:28:00 2001
        NAS-IP-Address = “172.16.25.15”
        NAS-Port = 2
        User-Name = “username1”
        Client-Port-DNIS = “4327528”
        Caller-ID = “5622329477”
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = “00000008”
        Login-Service = Telnet
```

```
        Login-IP-Host = "10.68.202.158"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:28:39 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = "00000008"
        Login-Service = Telnet
        Login-IP-Host = "10.68.202.158"
        Acct-Input-Octets = 10774
        Acct-Output-Octets = 112
        Acct-Input-Packets = 91
        Acct-Output-Packets = 99
        Acct-Session-Time = 39
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"
```

次に、発信 Telnet 接続の TACACS+ 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:47:43 2001        172.16.25.15    username1   tty3    5622329430/4327528
 start    task_id=10      service=connection      protocol=telnet addr=10.68.202.158
cmd=telnet username1-sun
Wed Jun 27 03:48:38 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=10      service=connection      protocol=telnet addr=10.68.202.158
cmd=telnet username1-sun     bytes_in=4467   bytes_out=96    paks_in=61      paks_out=72
 elapsed_time=55
```

次に、発信 rlogin 接続の RADIUS 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:29:48 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        Service-Type = Login
        Acct-Session-Id = "0000000A"
        Login-Service = Rlogin
        Login-IP-Host = "10.68.202.158"
        Acct-Delay-Time = 0
        User-Id = "username1"
        NAS-Identifier = "172.16.25.15"

Wed Jun 27 04:30:09 2001
        NAS-IP-Address = "172.16.25.15"
        NAS-Port = 2
        User-Name = "username1"
        Client-Port-DNIS = "4327528"
        Caller-ID = "5622329477"
```

```
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "0000000A"
Login-Service = Rlogin
Login-IP-Host = "10.68.202.158"
Acct-Input-Octets = 18686
Acct-Output-Octets = 86
Acct-Input-Packets = 90
Acct-Output-Packets = 68
Acct-Session-Time = 22
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"
```

次に、発信 rlogin 接続の TACACS+ 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:48:46 2001        172.16.25.15    username1   tty3    5622329430/4327528
 start    task_id=12      service=connection      protocol=rlogin addr=10.68.202.158
cmd=rlogin username1-sun /user username1
Wed Jun 27 03:51:37 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=12      service=connection      protocol=rlogin addr=10.68.202.158
cmd=rlogin username1-sun /user username1 bytes_in=659926 bytes_out=138   paks_in=2378
  paks_
out=1251        elapsed_time=171
```

次に、発信 LAT 接続の TACACS+ 接続アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:53:06 2001        172.16.25.15    username1   tty3    5622329430/4327528
 start    task_id=18      service=connection      protocol=lat    addr=VAX        cmd=lat
 VAX
Wed Jun 27 03:54:15 2001        172.16.25.15    username1   tty3    5622329430/4327528
 stop     task_id=18      service=connection      protocol=lat    addr=VAX        cmd=lat
 VAX  bytes_in=0      bytes_out=0     paks_in=0      paks_out=0      elapsed_time=6
```

システム アカウンティング

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（たとえば、システムのリブート時やアカウンティングのオン/オフ時）に関する情報を提供します。

次のアカウンティング レコードは、AAA アカウンティングがオフになったことを示す一般的な TACACS+ システム アカウンティング レコード サーバを示します。

```
Wed Jun 27 03:55:32 2001       172.16.25.15    unknown unknown unknown start   task_id=25
   service=system  event=sys_acct  reason=reconfigure
```

（注） アカウンティング パケット レコードの正確なフォーマットは、TACACS+デーモンに応じて変わります。

次のアカウンティング レコードは、AAAアカウンティングがオンになったことを示すTACACS+ システム アカウンティング レコードを示します。

```
Wed Jun 27 03:55:22 2001       172.16.25.15    unknown unknown unknown stop    task_id=23
   service=system  event=sys_acct  reason=reconfigure
```

システム リソースを測定する追加のタスクについては、他の Cisco IOS XE ソフトウェア コンフィギュレーション ガイドを参照してください。たとえば、IP アカウンティング タスクについては、『*CiscoIOS XE Application Services Configuration Guide,* Release 2』の「Configuring IP Services」を参照してください。

リソース アカウンティング

シスコが採用している AAA アカウンティングでは、ユーザー認証を通過したコールに対する「開始」レコードと「終了」レコードがサポートされます。ユーザー認証の一部として認証に失敗したコールの「終了」レコードを生成する追加機能もサポートされます。このようなレコードは、ネットワークを管理およびモニタするアカウンティング レコードを採用する場合に必要です。

ここでは、次の内容について説明します。

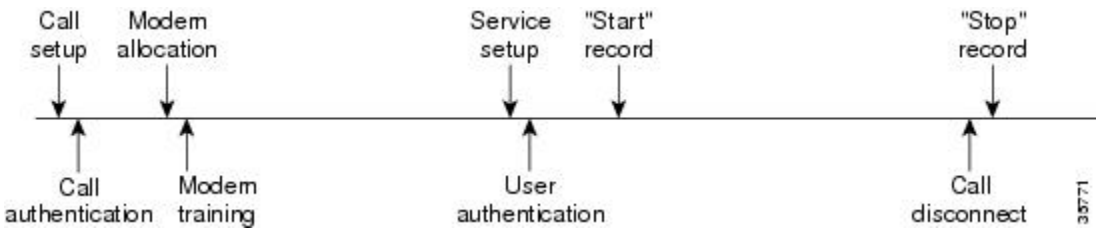
AAA リソース失敗終了アカウンティング

AAA リソース失敗終了アカウンティングの前には、コール設定シーケンスのユーザー認証段階に到達できなかったコールについて、アカウンティング レコードを提供する方式がありませんでした。このようなレコードは、ネットワークおよびその卸売りの顧客を管理およびモニターするアカウンティング レコードを採用する場合に必要です。

この機能によって、ユーザー認証に到達しなかったコールの「終了」アカウンティング レコードが生成されます。「終了」レコードは、コール設定の時点から生成されます。ユーザー認証に成功したすべてのコールは、従来と同様に動作します。つまり、追加のアカウンティング レコードは確認されません。

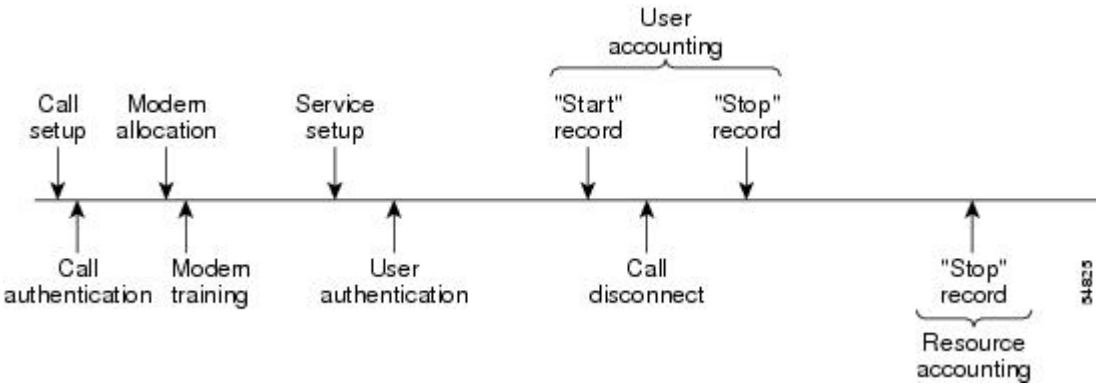
次の図に、通常のコール フローで、AAA リソース失敗終了アカウンティングを有効にしていないコール シーケンスを示します。

図 *1:* 通常のフローで *AAA* リソース失敗終了アカウンティングをイネーブルにしていないモデム ダイヤルイン コール設定シーケンス



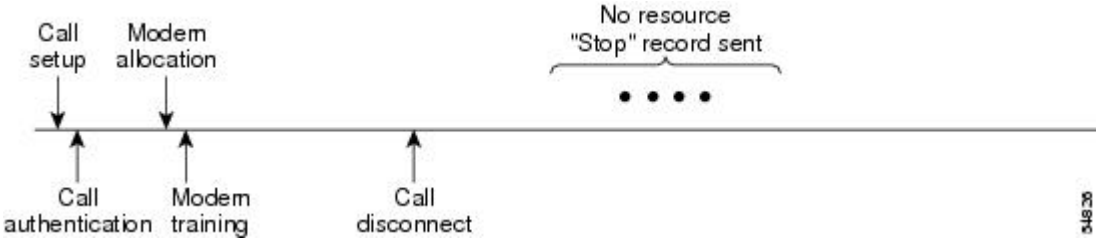
次の図に、通常のコール フローで、AAA リソース失敗終了アカウンティングをイネーブルにしたコール シーケンスを示します。

図 *2:* 通常のフローで *AAA* リソース失敗終了アカウンティングをイネーブルにしたモデム ダイヤルイン コール設定シーケンス



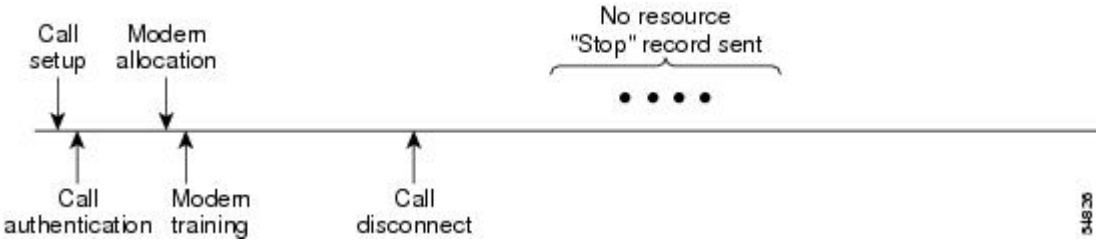
次の図に、ユーザ認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウンティングをイネーブルにしたコール設定シーケンスを示します。

図 *3:* ユーザ認証前にコールの接続解除が発生し、*AAA* リソース失敗終了アカウンティングをイネーブルにしたモデム ダイヤルイン コール設定シーケンス



次の図に、ユーザ認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウンティングをイネーブルにしていないコール設定シーケンスを示します。

図 *4:* ユーザ認証前にコールの接続解除が発生し、*AAA* リソース失敗終了アカウンティングをイネーブルにしていない モデム ダイヤルイン コール設定シーケンス



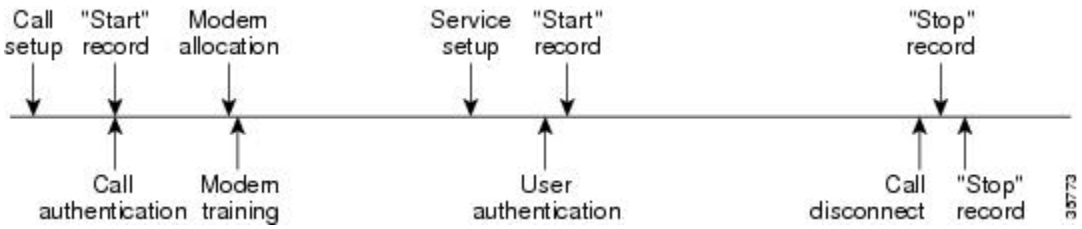
開始 - 終了レコードの AAA リソース アカウンティング

開始 - 終了レコードの AAA リソース アカウンティングは、各コール設定時に「開始」レコードを送信し、コールの接続解除時に対応する「終了」レコードを送信する機能をサポートしています。この機能は、アカウンティング レコードなどを報告するデータの発信元の 1 つから、卸売りの顧客を管理およびモニターするために使用できます。

この機能を使用すると、コール設定およびコールの接続解除の「開始 - 終了」アカウンティング レコードは、デバイスに対するリソース接続の進行状況を追跡します。個別のユーザー認証「開始 - 終了」アカウンティング レコードが、ユーザー管理の進行状況を追跡します。これら 2 セットのアカウンティング レコードは、そのコールで固有のセッション ID を使用して相互リンクされます。

次の図は、AAA リソース開始 - 終了アカウンティングを有効にしたコール設定シーケンスを示します。

図 *5:* リソース開始 - 終了アカウンティングをイネーブルにしたモデム ダイヤルイン コール設定シーケンス



AAA アカウンティングの強化

AAA ブロードキャスト アカウンティング

AAA ブロードキャスト アカウンティングを有効にすると、アカウンティング情報を複数の AAA サーバに同時に送信できます。つまり、アカウンティング情報を 1 つまた複数の AAA サーバに同時にブロードキャストすることが可能です。この機能を使用すると、サービス プロバイダーは自社使用のプライベート AAA サーバやエンドユーザの AAA サーバにアカウンティング情報を送信できるようになります。この機能では、音声アプリケーションによる課金情報も提供されます。

ブロードキャストは、RADIUS または TACACS+ サーバのグループに使用できます。また、各サーバ グループは、他のグループとは関係なく、フェールオーバーの場合のバックアップ サーバを定義できます。

したがって、サービス プロバイダーとそのエンド ユーザは、アカウンティング サーバに異なるプロトコル（RADIUS または TACACS+）を使用できます。また、サービス プロバイダーとそのエンド ユーザは、それぞれ単独でバックアップ サーバを指定することもできます。音声アプリケーションについては、独自のフェールオーバー シーケンスを持つ個別のグループを介して、冗長的なアカウンティング情報を単独で管理できます。

AAA セッション MIB

ユーザが AAA セッション MIB 機能を使用すると、簡易ネットワーク管理プロトコル（SNMP）を使用して自身の認証済みクライアント接続をモニタおよび終了できます。そのクライアントのデータが提示されるため、RADIUS または TACACS+ サーバから報告される AAA アカウンティング情報に直接関連付けることができます。AAA セッション MIB は、次の情報を提供します。

- 各 AAA 機能の統計情報（show radius statistics コマンドと併用する場合）

- AAA 機能を提供するサーバのステータス
- 外部 AAA サーバの ID
- （アイドル時間などの）リアルタイム情報（アクティブ コールを終了するかどうかを評価する SNMP ネットワークが使用する追加基準を提供します）

次の表に、認証済みクライアントと AAA セッション MIB 機能との接続をモニタおよび終了するために使用できる SNMP ユーザエンド データ オブジェクトを示します。

表 *2 : SNMP* エンドユーザ データ オブジェクト

フィールド	**Descriptions**
SessionId	AAA アカウンティング プロトコルに使用されるセッション ID（RADIUS 属性 44（Acct-Session-ID）から報告される値と同じ）
UserId	ユーザ ログイン ID または（ログインが使用できない場合）長さがゼロの文字列
IpAddr	セッションの IP アドレスまたは（IP アドレスが適用されない場合、または使用できない場合）0.0.0.0
IdleTime	セッションがアイドルになってからの経過時間
Disconnect	そのクライアントとの接続を解除するために使用されるセッション終了オブジェクト
CallId	コール トラッカー レコードが保存した、このアカウンティング セッションに対応するエントリ インデックス

次の表に、システム別に SNMP を使用する AAA セッション MIB 機能から提供される AAA の概要情報を示します。

表 *3 : SNMP AAA* セッションの概要

Field	**Descriptions**
ActiveTableEntries	現在アクティブなセッションの数
ActiveTableHighWaterMark	システムが最後に再インストールされてからの接続セッションの最大数
TotalSessions	システムが最後に再インストールされてからのセッションの合計数
DisconnectedSessions	システムが最後に再インストールされてから接続解除されたセッションの合計数

アカウンティング属性と値のペア

ネットワーク アクセス サーバは、TACACS+ 属性と値（AV）のペアまたは RADIUS 属性（実装しているセキュリティ方式によって異なります）に定義されたアカウンティング機能を監視します。

AAA アカウンティングの設定方法

名前付き方式リストによる AAA アカウンティングの設定

名前付き方式リストを使用して AAA アカウンティングを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. **aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [*method1* [*method2...*]]
2. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
3. **accounting** {**arap** | **commands** *level* | **connection** | **exec**} {**default** | *list-name*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [*method1* [*method2...*]]	アカウンティング方式リストを作成し、アカウンティングを有効にします。引数 *list-name* は、作成したリストに名前を付けるときに使用される文字列です。
ステップ 2	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] 例： `Router(config)# interface interface-type interface-number`	アカウンティング方式リストを適用する回線のライン コンフィギュレーション モードを開始するか、アカウンティング方式リストを適用するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**accounting** {**arap** | **commands** *level* | **connection** | **exec**} {**default** | *list-name*} 例： `Router(config-if)# ppp accounting {default | list-name}`	1 つの回線または回線セットにアカウンティング方式リストを適用するか、1 つのインターフェイスまたはインターフェイスセットにアカウンティング方式リストを適用します。

次のタスク

（注） システム アカウンティングは、名前付き方式リストを使用しません。システム アカウンティングの場合、デフォルトの方式リストだけを定義します。

ヌル ユーザ名セッション時のアカウンティング レコード生成の抑制

AAA アカウンティングをアクティブにすると、Cisco IOS XE ソフトウェアは、システム上にあるすべてのユーザにアカウンティング レコードを発行します。このとき、プロトコル変換のためにユーザ名文字列がヌルのユーザも含まれます。この例では、**aaa authentication login** *method-list* **none** コマンドが適用される回線で着信するユーザがそれに該当します。関連付けられているユーザ名がないセッションについて、アカウンティング レコードが生成されないようにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
`Router(config)# aaa accounting suppress null-username`	ユーザ名文字列がヌルのユーザについて、アカウンティング レコードが生成されないようにします。

中間アカウンティング レコードの生成

アカウンティング サーバに定期的な中間アカウンティング レコードを送信できるようにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
`Router(config)# aaa accounting update [newinfo] [periodic] number`	アカウンティング サーバに送信される定期的中間アカウンティング レコードをイネーブルにします。

aaa accounting update コマンド をアクティブにすると、Cisco IOS XE ソフトウェアによってシステム上のすべてのユーザーの中間アカウンティングレコードが発行されます。**newinfo** キーワードを使用した場合は、レポートする新しいアカウンティング情報が発生するたびに、中間アカウンティング レコードがアカウンティング サーバーに送信されます。たとえば、インターネット プロトコル コントロール プロトコル（IPCP）がリモート ピアとの IP アドレスのネゴシエーションを完了したときにこれが発生します。中間アカウンティング レコードには、リモート ピアに使用されるネゴシエート済み IP アドレスが含まれます。

aaa accounting update コマンドを **periodic** キーワードとともに使用すると、中間アカウンティングレコードは引数の数字で定義されたとおり定期的に送信されます。中間アカウンティング レコードには、中間アカウンティング レコードが送信される時間までに、そのユーザについて記録されたすべてのアカウンティング情報が含まれます。

⚠

注意 多数のユーザがネットワークにログインしている場合には、**aaa accounting update periodic** コマンドを使用すると、重度の輻輳が発生する可能性があります。

定期的アカウンティング レコードを有効化する代替手段の設定

次の代替手段を使用して、アカウンティング サーバーに送信される定期的中間アカウンティング レコードをイネーブルにできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa accounting network default**
4. **action-type** {**none** | **start-stop** [**periodic** {**disable** | **interval** *minutes*}] | **stop-only**}
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa accounting network default** 例： `Router(config)# aaa accounting network default`	すべてのネットワーク関連のサービス要求のデフォルトのアカウンティングを設定し、アカウンティング方式リストのコンフィギュレーション モードを開始します。

ステップ 4	**action-type** {**none**	**start-stop** [**periodic** {**disable**	**interval** *minutes*}]	**stop-only**}
				例：
				`Router(cfg-acct-mlist)# action-type start-stop`
				例：
				`periodic interval 5`
					アカウンティング レコードに対して実行されるアクションのタイプを指定します。
					• （任意）periodic キーワードは、定期的なアカウンティング アクションを示します。
					• interval キーワードは、定期的なアカウンティング間隔を指定します。
					• value 引数は、アカウンティング更新レコードの間隔を指定します（分単位）。

	コマンドまたはアクション	目的
		• disable キーワードは、定期的なアカウンティングをディセーブルにします。
ステップ 5	**exit** 例： `Router(cfg-acct-mlist)# exit`	グローバル コンフィギュレーション モードに戻ります。

中間サービス アカウンティング レコードの生成

このタスクを実行して、サブスクライバに対する定期的な間隔での中間サービスアカウンティング レコードの生成をイネーブルにします。

始める前に

ユーザー サービス プロファイルの RADIUS 属性 85 は設定済みの中間の間隔値よりも常に優先されます。RADIUS 属性 85 は、ユーザー サービス プロファイル内にある必要があります。詳細については、RADIUS 属性の概要および RADIUS IETF 属性の機能のドキュメントを参照してください。

（注） RADIUS 属性 85 がユーザー サービス プロファイル内にない場合、中間アカウンティング レコードの生成で設定された中間の間隔値がサービスの中間アカウンティング レコードに使用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **subscriber service accounting interim-interval** *minutes*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**subscriber service accounting interim-interval** *minutes* 例： `Router(config)# subscriber service accounting interim-interval 10`	サブスクライバに対する定期的な間隔での中間サービス アカウンティング レコードの生成をイネーブルにします。*minutes* 引数は、アカウンティング更新レコードを送信する定期的な間隔を 1 ～ 71582 分で示します。

失敗したログインまたはセッションに対するアカウンティングレコードの生成

AAA アカウンティングをアクティブにすると、Cisco IOS XE ソフトウェアは、ログイン認証に失敗したシステム ユーザー、またはログイン認証には成功しても何らかの理由で PPP ネゴシエーションに失敗したユーザーのアカウンティング レコードを生成しません。

ログイン時またはセッション ネゴシエーション中の認証に失敗したユーザーについて、アカウンティング終了レコードを生成するように指定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
aaa accounting send stop-record authentication failure	ログイン時またはセッション ネゴシエーション中の認証に失敗したユーザについて、「終了」レコードを生成します。

EXEC-Stop レコードよりも前のアカウンティング NETWORK-Stop レコードの指定

EXEC 終了セッションを開始する PPP ユーザーの場合、EXEC-stop レコードの前に、NETWORK レコードを生成するように指定できます。特定のサービスについて顧客に課金する場合など、状況によっては、ネットワークの開始レコードと終了レコードを一緒に保持する方が望ましいことがあります。その際、基本的に、EXEC の開始メッセージと終了メッセージのフレームワーク内に「ネスト」にします。たとえば、PPP を使用するユーザー ダイヤルインによって、EXEC-start、NETWORK-start、EXEC-stop、NETWORK-stop というレコードを作成できます。ネットワーク アカウンティング レコードをネストにすることで、NETWORK-stop レコードは NETWORK-start メッセージ（EXEC-start、NETWORK-start、NETWORK-stop、EXEC-stop）に従います。

ユーザー セッションのアカウンティング レコードをネストするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
aaa accounting nested	ネットワーク アカウンティング レコードをネストします。

スイッチオーバー上のシステム アカウンティング レコードの抑制

スイッチオーバー中のシステム アカウンティングオンおよびアカウンティングオフ メッセージを抑制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
aaa accounting redundancy suppress system-records	スイッチオーバー中のシステム アカウンティング レコードを抑制します。

AAA リソース失敗終了アカウンティングの設定

リソース失敗終了アカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
aaa accounting resource *method-list* **stop-failure group** *server-group*	ユーザー認証に到達しないコールについて、「終了」レコードを生成します。 （注） AAA リソース失敗終了アカウンティング機能を設定する前に、アカウンティングを設定するための前提条件 （1 ページ） のセクションに記載されている作業を実行し、ネットワーク アクセス サーバー上でSNMP を有効にしてください。Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ上で SNMP をイネーブルにする方法の詳細については、『Cisco IOS XE Network Management Configuration Guide』の「Configuring SNMP Support」の章を参照してください。

開始 - 終了レコードの AAA リソース アカウンティングの設定

開始 - 終了レコードのフル リソース アカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
aaa accounting resource *method-list* **start-stop group** *server-group*	各コール設定時に「開始」レコードを送信し、コールの接続解除時に対応する「終了」レコードを送信する機能をサポートします。 （注） この機能を設定する前に、アカウンティングを設定するための前提条件 （1 ページ）に記載されている作業を実行し、ネットワーク アクセス サーバ上で SNMP をイネーブルにしてください。Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ上で SNMP をイネーブルにする方法の詳細については、『Cisco IOS XE Network Management Configuration Guide, Release 2』の「Configuring SNMP Support」の章を参照してください。

AAA ブロードキャスト アカウンティングの設定

AAA ブロードキャスト アカウンティングを設定するには、グローバル コンフィギュレーション モードで **aaa accounting** コマンドを使用します。このコマンドは、**broadcast** キーワードを使用できるように変更されました。

コマンドまたはアクション	目的
aaa accounting {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] *method1* [*method2...*]	複数の AAA サーバに対するアカウンティング レコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウンティング レコードを同時に送信します。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。

DNIS による AAA ブロードキャスト アカウンティングの設定

AAA ブロードキャスト アカウンティングを設定するには、グローバル コンフィギュレーション モードで **aaa dnis map accounting network** コマンドを使用します。このコマンドは、**broadcast** キーワードおよび複数のサーバーグループを使用できるように変更されました。

コマンドまたはアクション	目的
aaa dnis map *dnis-number* **accounting network** [**start-stop** | **stop-only** | **none**] [**broadcast**] *method1* [*method2...*]	DNIS によるアカウンティングの設定を許可します。このコマンドは、グローバルの **aaa accounting** コマンドよりも優先されます。 複数の AAA サーバに対するアカウンティング レコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウンティング レコードを同時に送信します。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。

AAA セッション MIB の設定

次のタスクは、次の AAA セッション MIB 機能の設定よりも前に実行する必要があります。

- SNMP を設定します。SNMP については、『Cisco IOS XE Network Management Configuration Guide』の「Configuring SNMP Support」の章を参照してください。
- AAA を設定します。
- RADIUS または TACACS+ サーバの特性を定義します。

（注） SNMP を多用すると、全体のシステム パフォーマンスに影響が出る可能性があります。そのため、この機能を使用するときに、通常のネットワーク管理パフォーマンスを考慮する必要があります。

AAA セッション MIB を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
aaa session-mib disconnect	SNMP を使用して、認証済みクライアント接続をモニタおよび終了します。 コールを終了するには、disconnect キーワードを使用します。

AAA サーバが到達不能な場合のルータとのセッションの確立

AAA サーバが到達不能の場合に、ルータとの間にコンソール セッションを確立するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
no aaa accounting system guarantee-first	**aaa accounting system guarantee-first** コマンドは、システムアカウントを最初のレコードとして保証します。これは、デフォルトの条件です。 状況によっては、システムの再ロードが完了するまで（3分よりも長くかかる可能性があります）、ユーザーがコンソールまたはTelnet接続でセッションを開始できない可能性があります。この問題を解決するには、**no aaa accounting system guarantee-first** コマンドを使用します。

アカウンティングのモニタリング

RADIUS または TACACS+ アカウンティングの場合、特定の **show** コマンドは存在しません。ログインしているユーザーに関する情報を表示するアカウンティング レコードを取得するには、特権 EXEC モードで次のコマンドを使用します。

コマンドまたはアクション	目的
show accounting	ネットワークでアクティブなアカウント可能なイベントの表示を許可し、アカウンティング サーバでデータが損失した場合に情報を収集できます。

アカウンティングのトラブルシューティング

アカウンティング情報の問題を解決するには、特権 EXEC モードで次のコマンドを使用します。

コマンドまたはアクション	目的
debug aaa accounting	説明の義務があるイベントが発生したときに、その情報を表示します。

AAA アカウンティングの設定例

方式指定リストの設定の例

次に、RADIUS サーバーから AAA サービスを提供するために Cisco AS5200（AAA および RADIUSセキュリティ サーバーとの通信で有効）を設定する例を示します。RADIUS サーバーが応答に失敗すると、認証情報と認可情報についてローカルデータベースへの照会が行われ、アカウンティング サービスは TACACS+ サーバーによって処理されます。

```
aaa new-model
aaa authentication login admins local
aaa authentication ppp dialins group radius local
aaa authorization network network1 group radius local
aaa accounting network network2 start-stop group radius group tacacs+
username root password ALongPassword
tacacs-server host 172.31.255.0
tacacs-server key goaway
radius-server host 172.16.2.7
radius-server key myRaDiUSpassWoRd
interface group-async 1
 group-range 1 16
 encapsulation ppp
 ppp authentication chap dialins
 ppp authorization network1
 ppp accounting network2
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem dialin
```

この RADIUS AAA 設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA ネットワーク セキュリティ サービスをイネーブルにします。
- **aaa authentication login admins local** コマンドは、ログイン認証に方式リスト「admins」を定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、認証方式リスト「dialins」を定義します。このリストは、最初にRADIUS認証を指定して、次に（RADIUSサーバーが応答しない場合）PPP を使用してシリアル回線上でローカル認証が使用されます。
- **aaa authorization network network1 group radius local** コマンドで、「network1」というネットワーク許可方式リストを定義します。これにより、PPP を使用してシリアル回線上でRADIUS許可を使用するよう指定されます。RADIUS サーバーが応答に失敗すると、ローカル ネットワークの認可が実行されます。
- **aaa accounting network network2 start-stop group radius group tacacs+** コマンドで、「network2」というネットワーク アカウンティング方式リストを定義します。これにより、PPPを使用してシリアル回線上でRADIUSアカウンティングサービス（この場合、特定のイベントに対する開始レコードと終了レコード）を使用するよう指定されます。RADIUS サーバが応答に失敗すると、アカウンティングサービスは TACACS+ サーバによって処理されます。
- **username** コマンドはユーザ名とパスワードを定義します。これらの情報は、PPPパスワード認証プロトコル（PAP）の発信元身元確認に使用されます。
- **tacacs-server host** コマンドは TACACS+ サーバー ホストの名前を定義します。
- **tacacs-server key** コマンドは、ネットワーク アクセス サーバーと TACACS+ サーバー ホストの間の共有秘密テキスト文字列を定義します。
- **radius-server host** コマンドは RADIUS サーバー ホストの名前を定義します。

- **radius-server key** コマンドは、ネットワーク アクセス サーバーと RADIUS サーバー ホストの間の共有秘密テキスト文字列を定義します。
- **interface group-async** コマンドは、非同期インターフェイス グループを選択して定義します。
- **group-range** コマンドは、インターフェイス グループ内のメンバ非同期インターフェイスを定義します。
- **encapsulation ppp** コマンドは、指定のインターフェイスに使用されるカプセル化方式として PPP を設定します。
- **ppp authentication chap dialins** コマンドは、PPP 認証方式としてチャレンジハンドシェイク認証プロトコル（CHAP）を選択し、指定したインターフェイスに「dialins」方式リストを適用します。
- **ppp authorization network1** コマンドによって、blue1 ネットワーク許可方式リストが、指定したインターフェイスに適用されます。
- **ppp accounting network2** コマンドによって、red1 ネットワーク アカウンティング方式リストが、指定したインターフェイスに適用されます。
- **line** コマンドはコンフィギュレーション モードをグローバル コンフィギュレーションからライン コンフィギュレーションに切り替え、設定対象の回線を指定します。
- **autoselect ppp** コマンドは、選択した回線上で PPP セッションを自動的に開始できるように Cisco IOS XE ソフトウェアを設定します。
- **autoselect during-login** コマンドを使用すると、Return キーを押さずにユーザ名およびパスワードのプロンプトが表示されます。ユーザがログインすると、autoselect 機能（この場合は PPP）が開始します。
- **login authentication admins** コマンドは、ログイン認証に admins 方式リストを適用します。
- **modem dialin** コマンドは、選択した回線に接続されているモデムを設定し、着信コールだけを受け入れるようにします。

show accounting コマンドを使用すると、前述の設定に関する出力が次のように生成されます。

```
Active Accounted actions on tty1, User username2 Priv 1
 Task ID 5, Network Accounting record, 00:00:52 Elapsed
 task_id=5 service=ppp protocol=ip address=10.0.0.98
```

次の表に、前述の出力に含まれるフィールドについて説明します。

表 *4 : show accounting* のフィールドの説明

フィールド	説明
Active Accounted actions on	ユーザがログインに使用する端末回線またはインターフェイス名
User	ユーザの ID。

フィールド	説明
Priv	ユーザの特権レベル。
Task ID	各アカウンティング セッションの固有識別情報
Accounting Record	アカウンティング セッション タイプ
Elapsed	このセッション タイプの期間（hh:mm:ss）
attribute=value	このアカウンティング セッションに関連付けられている AV ペア

AAA リソース アカウンティングの設定の例

次に、リソース失敗終了アカウンティング、および 開始 - 終了レコード機能のリソース アカウンティングを設定する例を示します。

```
!Enable AAA on your network access server.
aaa new-model
!Enable authentication at login and list the AOL string name to use for login
authentication.
aaa authentication login AOL group radius local
!Enable authentication for ppp and list the default method to use for PPP authentication.
aaa authentication ppp default group radius local
!Enable authorization for all exec sessions and list the AOL string name to use for
authorization.
aaa authorization exec AOL group radius if-authenticated
!Enable authorization for all network-related service requests and list the default
method to use for all network-related authorizations.
aaa authorization network default group radius if-authenticated
!Enable accounting for all exec sessions and list the default method to use for all
start-stop accounting services.
aaa accounting exec default start-stop group radius
!Enable accounting for all network-related service requests and list the default method
 to use for all start-stop accounting services.
aaa accounting network default start-stop group radius
!Enable failure stop accounting.
aaa accounting resource default stop-failure group radius
!Enable resource accounting for start-stop records.
aaa accounting resource default start-stop group radius
```

AAA ブロードキャスト アカウンティングの設定の例

次に、グローバル **aaa accounting** コマンドを使用して、ブロードキャスト アカウンティングを有効にする例を示します。

```
aaa group server radius isp
 server 10.0.0.1
 server 10.0.0.2
aaa group server tacacs+ isp_customer
 server 172.0.0.1
aaa accounting network default start-stop broadcast group isp group isp_customer
radius-server host 10.0.0.1
radius-server host 10.0.0.2
```

```
radius-server key key1
tacacs-server host 172.0.0.1 key key2
```

broadcast キーワードによって、ネットワーク接続に関する「開始」および「終了」アカウンティング レコードが、グループ isp ではサーバー 10.0.0.1 に、グループ isp_customer ではサーバー 172.0.0.1 に同時送信されます。サーバ 10.0.0.1 が使用できなくなると、サーバ 10.0.0.2 へのフェールオーバーが行われます。サーバ 172.0.0.1 が使用できなくなっても、グループ isp_customer にはバックアップ サーバが設定されていないため、フェールオーバーは行われません。

DNIS による AAA ブロードキャスト アカウンティングの設定の例

次に、グローバル **aaa dnis map accounting network** コマンドを使用して、DNIS によるブロードキャスト アカウンティングを有効にする例を示します。

```
aaa group server radius isp
 server 10.0.0.1
 server 10.0.0.2
aaa group server tacacs+ isp_customer
 server 172.0.0.1
aaa dnis map enable
aaa dnis map 7777 accounting network start-stop broadcast group isp group isp_customer
radius-server host 10.0.0.1
radius-server host 10.0.0.2
radius-server key key_1
tacacs-server host 172.0.0.1 key key_2
```

broadcast キーワードによって、DNIS 番号 7777 のネットワーク接続コールに関する「開始」および「終了」アカウンティング レコードが、グループ isp ではサーバー 10.0.0.1 に、グループ isp_customer ではサーバー 172.0.0.1 に同時送信されます。サーバ 10.0.0.1 が使用できなくなると、サーバ 10.0.0.2 へのフェールオーバーが行われます。サーバ 172.0.0.1 が使用できなくなっても、グループ isp_customer にはバックアップ サーバが設定されていないため、フェールオーバーは行われません。

AAA セッション MIB の例

次に、AAA セッション MIB 機能を設定して、PPP ユーザの認証済みクライアント接続を解除する例を示します。

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
aaa session-mib disconnect
```

その他の参考資料

ここでは、アカウンティングの設定機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
SNMP の設定	『*Cisco IOS XE Network Management Configuration Guide*』
SNMP コマンド	『*Cisco IOS Network Management Command Reference*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
RADIUS の設定	RADIUS の設定
TACACS+ の設定	TACACS+ の設定
IP サービスの設定	『*Cisco IOS XE Application Services Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
• CISCO-AAA-SESSION-MIB	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

アカウンティングの設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *5:* アカウンティングの設定に関する機能情報

機能名	リリース	機能情報
AAA ブロードキャスト アカウンティング	Cisco IOS XE Release 2.1	AAA ブロードキャスト アカウンティングを有効にすると、アカウンティング情報を複数の AAA サーバに同時に送信できます。つまり、アカウンティング情報を 1 つまた複数の AAA サーバに同時にブロードキャストすることが可能です。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaa accounting**。

機能名	リリース	機能情報
AAAセッションMIB	Cisco IOS XE Release 2.1	ユーザがAAAセッションMIB機能を使用すると、簡易ネットワーク管理プロトコル（SNMP）を使用して自身の認証済みクライアント接続をモニタおよび終了できます。 Cisco IOS XE Release 2.1では、Cisco ASR 1000シリーズAggregation Services Routerにこの機能が実装されました。 次のコマンドが導入または変更されました。**aaa session-mib disconnect**。
接続アカウンティング	Cisco IOS XE Release 2.1	接続アカウンティングは、Telnet、ローカルエリアトランスポート（LAT）、TN3270、Packet Assembler/disassembler（PAD）、rloginなど、ネットワークアクセスサーバからの発信接続すべてに関する情報を提供します。 Cisco IOS XE Release 2.1では、Cisco ASR 1000シリーズAggregation Services Routerにこの機能が実装されました。
AAA中間アカウンティング	Cisco IOS XE Release 2.4	AAA中間アカウンティングにより、レポートする必要がある新しいアカウンティング情報が発生するたびに、または定期的に、アカウンティングサーバに中間アカウンティングレコードを送信できます。 Cisco IOS XE Release 2.4では、Cisco ASR 1000シリーズAggregation Services Routerにこの機能が実装されました。 次のコマンドが導入または変更されました。**aaa accounting update**および**subscriber service accounting interim-interval**。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。