Offload Server Accounting Enhancement

Offload Server Accounting Enhancement 機能により、ユーザは Network Access Server（NAS; ネットワーク アクセス サーバ）とオフロード サーバとの間の認証情報とアカウンティング情報を維持できます。

NAS でもオフロード サーバと情報を同期することはできますが、この機能は一意のセッション ID を含むように拡張されており、NAS によって収集される既存のセッション ID（NAS-IP-Address）および Class（アトリビュート 25）情報の前に Acct-Session-Id（アトリビュート 44）を追加します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「Offload Server Accounting Enhancement の機能情報」（P.7）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

前提条件

Offload Server Accounting Enhancement を設定する前に、次の作業を実行する必要があります。

- AAA をイネーブルにします。詳細については、「Configuring Authentication」フィーチャ モジュールを参照してください。
- VPN をイネーブルにします。詳細については、『*Cisco IOS Security Configuration Guide: Secure Connectivity*』リリース 12.4T を参照してください。

Offload Server Accounting Enhancement について

Offload Server Accounting Enhancement 機能により、ユーザは認証およびアカウンティング情報（NAS-IP-Address（アトリビュート 4）および Class（アトリビュート 25）がオフロード サーバと同期するように Network Access Server（NAS; ネットワーク アクセス サーバ）を設定できます。

オフロード サーバは、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）経由で NAS と相互作用して、コールに必要な Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）ネゴシエーションを実行します。NAS はコールの事前認証を実行し、オフロード サーバはユーザ認証を実行します。この機能を使用すると、次のように NAS の認証データとアカウンティング データをオフロード サーバと同期できます。

- 事前認証中、NAS は一意のセッション ID を生成し、既存のセッション ID（NAS-IP-Address）の前に Acct-Session-Id（アトリビュート 44）を追加して、Class アトリビュートを取得します。新しいセッション ID は事前認証要求とリソース アカウンティング要求で送信され、Class アトリビュートはリソース アカウンティング要求で送信されます。

（注） 複数の NAS が 1 台のオフロード サーバによって処理される場合は、一意のセッション ID が必要です。

- NAS-IP-Address、Acct-Session-Id、および Class アトリビュートは、Layer 2 Forwarding（L2F; レイヤ 2 フォワーディング）オプションによってオフロード サーバに送信されます。
- オフロード サーバのユーザ アクセス要求、およびユーザ セッション アカウンティング要求には、新しい、一意のセッション ID が含まれます。NAS から渡される Class アトリビュートは、ユーザ アクセス要求に含まれますが、新しい Class アトリビュートは、ユーザ アクセスへの返信で受信します。この新しい Class アトリビュートはユーザ セッション アカウンティング要求に含まれている必要があります。

Offload Server Accounting Enhancement の設定方法

Offload Server Accounting Enhancement の設定作業については、次の項を参照してください。一覧内の各作業は、必須と任意に分けています。

- 「一意のセッション ID の設定」（P.3）（必須）
- 「NAS クライアントとオフロード サーバとの同期の設定」（P.3）（必須）
- 「オフロード サーバ アカウンティングの確認」（P.3）（任意）

一意のセッション ID の設定

NAS 間で一意のセッション ID を維持するには、次のグローバル コンフィギュレーション コマンドを使用します。複数の NAS が 1 台のオフロード サーバによって処理される場合は、すべての NAS およびオフロード サーバでこの機能をイネーブルにし、共通のセッション ID と一意のセッション ID を確認する必要があります。

コマンド	目的
`Router(config)# radius-server attribute 44 extend-with-addr`	既存の AAA セッション ID の前にアカウンティング IP アドレスを追加します。 **（注）** 一意のセッション ID は、既存のセッション ID（NAS-IP-Address）の前に Acct-Session-Id（アトリビュート 44）を追加するため、他の NAS セッション ID とは異なります。

NAS クライアントとオフロード サーバとの同期の設定

アカウンティング セッション情報を NAS クライアントと同期するようにオフロード サーバを設定するには、次のグローバル コンフィギュレーション コマンドを使用します。

コマンド	目的
`Router(config)# radius-server attribute 44 sync-with-client`	アカウンティング セッション情報を NAS クライアントと同期するようにオフロード サーバを設定します。

オフロード サーバ アカウンティングの確認

NAS がオフロード サーバと認証データおよびアカウンティング データを同期しているかを確認するには、特権 EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# more system:running-config`	現在実行されているコンフィギュレーション ファイルの内容を表示します（**show running-config** コマンドが **more system:running-config** に置き換えられていることに注意してください）。
`Router(config)# debug radius`	RADIUS 関連の情報を表示します。このコマンドの出力は、アトリビュート 44 がアクセス要求で送信されているかどうかを示します。ただし、出力にアトリビュート 44 の値全体が示されるわけではありません。アトリビュート 44 の値全体を表示するには、RADIUS サーバ ログを参照してください。

Offload Server Accounting Enhancement の設定例

ここでは、次の設定例について説明します。

一意のセッション ID の設定：例

次に、NAS 間で一意のセッション ID を設定する方法の例を示します。

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
radius-server attribute 44 extend-with-addr
```

NAS クライアントとオフロード サーバとの同期：例

次に、NAS クライアントとアカウンティング セッション情報を同期するようにオフロード サーバを設定する方法の例を示します。

```
radius-server attribute 44 sync-with-client
```

その他の参考資料

ここでは、Offload Server Accounting Enhancement に関する関連資料について説明します。

関連資料

内容	参照先
VPN のイネーブル化	『*Cisco IOS Security Configuration Guide: Secure Connectivity*, Release 12.4T』
AAA のイネーブル化	「Configuring Authentication」モジュール

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに対する MIB を特定してダウンロードするには、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
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

Offload Server Accounting Enhancement の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　Offload Server Accounting Enhancement の機能情報

機能名	リリース	機能情報
Offload Server Accounting Enhancement	12.2(4)T 12.2(28)SB 12.2(33)SRC	Offload Server Accounting Enhancement 機能により、ユーザは Network Access Server（NAS; ネットワーク アクセス サーバ）とオフロード サーバとの間の認証情報とアカウンティング情報を維持できます。 この機能は、Cisco IOS Release 12.2(4)T で導入されました。 この機能は、Cisco IOS Release 12.2(28)SB に統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC に統合されました。 この機能により、次のコマンドが導入または変更されました。**radius-server attribute 44 extend-with-addr**、**radius-server attribute 44 sync-with-client**

用語集

AAA：Authentication, Authorization, and Accounting（認証、認可、およびアカウンティング）。Cisco ルータまたはアクセス サーバにアクセス コントロールを設定できる主要なフレームワークを提供する一連のネットワーク セキュリティ サービスです。

Acct-Session-ID（アトリビュート 44）：ログ ファイル内の開始レコードと終了レコードのマッチングを容易にする一意のアカウンティング ID。Acct-Session ID の番号は、ルータの電源を入れ直したり、ソフトウェアをリロードするたびに、1 から再開します。

Class（アトリビュート 25）：アカウンティング アトリビュート。アトリビュートが RADIUS サーバによって提供されている場合、ネットワーク アクセス サーバがすべてのアカウンティング パケットに含める任意の値。

L2F：レイヤ 2 フォワーディング。レイヤ 2 トンネル プロトコルを使用すると、ISP などのアクセス サービスが仮想トンネルを作成し、顧客のリモート サイトやリモート ユーザを企業のホーム ネットワークにリンクさせることができます。具体的には、ISP Point of Presence（POP; アクセス ポイント）にある Network Access Server（NAS; ネットワーク アクセス サーバ）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

NAS：Network Access Server（NAS; ネットワーク アクセス サーバ）パケットの世界（インターネットなど）と回線の世界（公衆電話交換網など）をインターフェイスするシスコ プラットフォーム（または AccessPath システムなどのプラットフォームの集合）。

NAS-IP Address（アトリビュート 4）：認証を要求するネットワーク アクセス サーバの IP アドレスを指定します。デフォルト値は 0.0.0.0/0 です。

PPP：Point-to-Point Protocol（ポイントツーポイント プロトコル）。同期回線と非同期回線上でルータ間接続とホスト / ネットワーク間接続を提供する SLIP の代替プロトコル。SLIP は IP と連動するように設計されているのに対して、PPP は IP、IPX、ARA などの複数のネットワーク レイヤ プロトコルと連動するように設計されています。PPP には、CHAP および PAP などの組み込みのセキュリティ メカニズムもあります。PPP は LCP と NCP の 2 つのプロトコルに依存します。

RADIUS：Remote Authentication Dial-In User Service。RADIUS は、不正アクセスからネットワークを保護する分散型クライアント / サーバ システムです。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼動します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

VPN：リモートでダイヤルイン ネットワークをホーム ネットワークに存在させ、あたかも直接接続されているかのように見せるシステム。VPN は、L2TP および L2F を使用し、LAC ではなく、LNS でレイヤ 2 およびより高次のネットワーク接続を終了させます。
