RFC-2867 RADIUS トンネル アカウンティング

RFC-2867 RADIUS トンネル アカウンティングは、6 つの新しい RADIUS アカウンティング タイプを導入しています。これらのタイプは、アカウンティング要求がユーザー サービスの始まり（開始）と終わり（終了）のどちらを表しているかを示す、RADIUS アカウンティング属性の Acct-Status-Type（属性 40）と一緒に使用されます。

また、この機能は、ユーザーによる VPDN セッション イベントのトラブルシューティングを支援する 2 つの新しい仮想プライベート ダイヤルアップ ネットワーク（VPDN）コマンドを導入しています。

RFC-2867 RADIUS トンネル アカウンティングの制約事項

RADIUS トンネル アカウンティングは、L2TP トンネル サポートがなければ動作しません。

RFC-2867 RADIUS トンネル アカウンティングに関する情報

RFC-2867 RADIUS トンネル アカウンティングの利点

ユーザーが tunnel-link ステータスの変化を判断できるようにするネットワーク アカウンティングを使用した VPDN では、RADIUS トンネル アカウンティングがサポートされていないため、

使用可能なすべての属性がアカウンティング レコード ファイルに書き込まれませんでした。現在は使用可能なすべての属性を表示できるため、ユーザーはアカウンティング レコードをインターネット サービス プロバイダー（ISP）に確認しやすくなりました。

RADIUS トンネル アカウンティングのための RADIUS 属性サポート

以下の表に、ダイヤルアップ ネットワーク内の Compulsory Tunneling のプロビジョンをサポートするように設計された新しい RADIUS アカウンティング タイプの概要を示します。これらの属性タイプを使用すると、トンネル ステータスの変化をより適切に追跡できます。

（注） アカウンティング タイプは 2 つのトンネル タイプに分けられるため、ユーザーは、トンネル タイプが必要なのか、tunnel-link タイプが必要なのか、両方のアカウンティング タイプが必要なのかを判断できます。

表 *1 : Acct-Status-Type* 属性用の *RADIUS* アカウンティング タイプ

タイプ名	ケース	説明	追加属性[1]
Tunnel-Start	9	別のノードとのトンネルセットアップの始まりを示します。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから

タイプ名	ケース	説明	追加属性[1]
Tunnel-Stop	10	別のノードへの、または別のノードからのトンネル接続の終わりを示します。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Input-Octets（42）：AAA から • Acct-Output-Octets（43）：AAA から • Acct-Session-Id（44）：AAA から • Acct-Session-Time（46）：AAA から • Acct-Input-Packets（47）：AAA から • Acct-Output-Packets（48）：AAA から • Acct-Terminate-Cause（49）：AAA から • Acct-Multi-Session-Id（51）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから • Acct-Tunnel-Packets-Lost（86）：クライアントから

タイプ名	ケース	説明	追加属性[1]
Tunnel-Reject	11	別のノードとのトンネルセットアップの拒否を示します。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Terminate-Cause（49）：クライアントから • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから
Tunnel-Link-Start	12	トンネル リンクの構築を示します。一部のトンネル タイプ（レイヤ 2 トランスポート プロトコル（L2TP）しか、トンネル当たりの複数リンクをサポートしていません。この値は、トンネル当たりの複数リンクをサポートしているトンネル タイプのアカウンティング パケット以外には含めないでください。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • NAS-Port（5）：AAA から • Acct-Delay-Time（41）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから

タイプ名	ケース	説明	追加属性[1]
Tunnel-Link-Stop	13	トンネル リンクの終わりを示します。一部のトンネル タイプ（L2TP）しか、トンネル当たりの複数リンクをサポートしていません。この値は、トンネル当たりの複数リンクをサポートしているトンネル タイプのアカウンティング パケット以外には含めないでください。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • NAS-Port（5）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Input-Octets（42）：AAA から • Acct-Output-Octets（43）：AAA から • Acct-Session-Id（44）：AAA から • Acct-Session-Time（46）：AAA から • Acct-Input-Packets（47）：AAA から • Acct-Output-Packets（48）：AAA から • Acct-Terminate-Cause（49）：AAA から • Acct-Multi-Session-Id（51）：AAA から • Event-Timestamp（55）：AAA から • NAS-Port-Type（61）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから • Acct-Tunnel-Packets-Lost（86）：クライアントから

タイプ名	ケース	説明	追加属性[1]
Tunnel-Link-Reject	14	既存のトンネル内の新しいリンクに対するトンネルセットアップの拒否を示します。一部のトンネル タイプ（L2TP）しか、トンネル当たりの複数リンクをサポートしていません。この値は、トンネル当たりの複数リンクをサポートしているトンネル タイプのアカウンティング パケット以外には含めないでください。	• User-Name（1）：クライアントから • NAS-IP-Address（4）：AAA から • Acct-Delay-Time（41）：AAA から • Acct-Terminate-Cause（49）：AAA から • Event-Timestamp（55）：AAA から • Tunnel-Type（64）：クライアントから • Tunnel-Medium-Type（65）：クライアントから • Tunnel-Client-Endpoint（66）：クライアントから • Tunnel-Server-Endpoint（67）：クライアントから • Acct-Tunnel-Connection（68）：クライアントから

[1] 指定されたトンネル タイプが使用されている場合は、これらの属性もアカウンティング要求パケットに含める必要があります。

RADIUS トンネル アカウンティングの設定方法

トンネル タイプ アカウンティング レコードの有効化

このタスクを使用して、トンネル レコードと tunnel-link アカウンティング レコードを RADIUS サーバーに送信するように LAC を設定します。

vpdn セッション アカウンティング ネットワーク（tunnel-link-type レコード）と vpdn トンネル アカウンティング ネットワーク（tunnel-type レコード）という 2 つの新しいコマンドライン インターフェイス（CLI）が、次のイベントの特定を支援するためにサポートされています。

- VPDN トンネルが構築または破壊された。
- VPDN トンネルの作成要求が拒否された。
- VPDN トンネル内のユーザー セッションが起動または停止された。
- ユーザー セッション作成要求が拒否された。

（注） 最初の 2 つのイベントは、tunnel-type アカウンティング レコードです。認証、許可、アカウンティング（AAA）が、Tunnel-Start、Tunnel-Stop、または Tunnel-Reject アカウンティング レコードを RADIUS サーバーに送信します。次の 2 つのイベントは、tunnel-link-type アカウンティング レコードです。AAA が、Tunnel-Link-Start、Tunnel-Link-Stop、または Tunnel-Link-Reject アカウンティング レコードを RADIUS サーバーに送信します。

手順の概要

1. **enable**
2. **configure terminal**
3. Router(config)# **aaa accounting network default** *list-name*} {**start-stop** | **stop-only** | **wait-start** | **none group** *groupname*
4. Router(config)# **vpdn enable**
5. Router(config)# **vpdn tunnel accounting network** *list-name*
6. Router(config)# **vpdn session accounting network** *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	**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	Router(config)# **aaa accounting network default** *list-name*} {**start-stop** | **stop-only** | **wait-start** | **none group** *groupname* 例： 例： 例： 例： 例：	ネットワーク アカウンティングを有効にします。 • **default** ：デフォルトのネットワーク アカウンティングの方式リストが設定され、インターフェイス上でどの追加のアカウンティング設定も有効になっていない場合は、デフォルトで、ネットワーク アカウンティングが有効になります。 **vpdn session accounting network** コマンドまたは **vpdn tunnel accounting network** コマンドが **default** 方式リストにリンクされている場合、すべてのトンネルおよびトンネルリンク アカウンティング レコードが、これらのセッションで有効になります。

	コマンドまたはアクション	目的
	例： 例： 例： 例： 例： 例： `Router(config)# aaa accounting network m1 start-stop group radius`	• *list-name* ：**aaa accounting** コマンドで定義された *list-name* は、VPDN コマンドで定義された *list-name* と同一である必要があります。そうでない場合、アカウンティングは発生しません。
ステップ 4	Router(config)# **vpdn enable** 例： `Router(config)# vpdn enable`	ルータ上のバーチャル プライベート ダイヤルアップ ネットワーキングを有効にして、ルータにローカル データベースとリモート認可サーバー（該当する場合）上でトンネル定義を検索するように指示します。
ステップ 5	Router(config)# **vpdn tunnel accounting network** *list-name* 例： `Router(config)# vpdn tunnel accounting network m1`	Tunnel-Start、Tunnel-Stop、および Tunnel-Reject アカウンティング レコードを有効にします。 • *list-name* ：*list-name* は、**aaa accounting** コマンドで定義された *list-name* と一致している必要があります。そうでない場合、ネットワーク アカウンティングは発生しません。
ステップ 6	Router(config)# **vpdn session accounting network** *list-name* 例： `Router(config)# vpdn session accounting network m1`	Tunnel-Link-Start、Tunnel-Link-Stop、および Tunnel-Link-Reject アカウンティング レコードを有効にします。 • *list-name* ：*list-name* は、**aaa accounting** コマンドで定義された *list-name* と一致している必要があります。そうでない場合、ネットワーク アカウンティングは発生しません。

次の作業

RADIUS トンネル アカウンティングを有効にしたら、次のオプション タスク「RADIUS トンネル アカウンティングの確認」で設定を確認できます。

RADIUS トンネル アカウンティングの確認

次のオプション手順のどちらかまたは両方を使用して、RADIUS トンネルアカウンティング設定を確認します。

手順の概要

1. **enable**
2. Router# **show accounting**
3. Router# **show vpdn** [**session**] [**tunnel**]

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	Router# **show accounting** 例： `Router# show accounting`	ネットワーク上でアクティブなアカウント可能イベントを表示して、アカウンティング サーバー上でのデータ消失イベント時の情報収集を支援します。
ステップ 3	Router# **show vpdn** [**session**] [**tunnel**] 例： 例： 例： 例： `Router# show vpdn session`	VPDN 内のアクティブな L2TP トンネルとメッセージ識別子に関する情報を表示します。 • **session** ：すべてのアクティブなトンネルのステータス サマリーを表示します。 • **tunnel** ：すべてのアクティブな L2TP トンネルに関する情報をサマリー形式で表示します。

RADIUS トンネル アカウンティングの設定例

LAC 上での RADIUS トンネル アカウンティングの設定例

次の例は、トンネル レコードと tunnel-link アカウンティング レコードを RADIUS サーバーに送信するように L2TP アクセス コンセントレータ（LAC）を設定する方法を示しています。

```
aaa new-model
!
!
aaa authentication ppp default group radius
aaa authorization network default local
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$IDjH$iL7puCja1RM1yOM.JAeuf/
enable password lab
!
username ISP_LAC password 0 tunnelpass
!
!
resource-pool disable
!
!
ip subnet-zero
ip cef
no ip domain-lookup
ip host dirt 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
vpdn search-order domain dnis
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain cisco.com
 initiate-to ip 10.1.26.71
 local name ISP_LAC
!
mta receive maximum-recipients 0
!
interface GigabitEthernet0/0/0
 ip address 10.1.27.74 255.255.255.0
 no ip mroute-cache
 duplex half
 speed auto
 no cdp enable
!
interface FastEthernet0/0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
ip default-gateway 10.1.27.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.27.254
no ip http server
ip pim bidir-enable
!
no cdp run
!
!
radius-server host 172.19.192.26 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
```

```
call rsvp-sync
!
```

LNS 上での RADIUS トンネル アカウンティングの設定例

次の例は、トンネル レコードと tunnel-link アカウンティング レコードを RADIUS サーバーに送信するように L2TP ネットワーク サーバー（LNS）を設定する方法を示しています。

```
aaa new-model
!
!
aaa accounting network m1 start-stop group radius
aaa accounting network m2 stop-only group radius
aaa session-id common
enable secret 5 $1$ftf.$wE6Q5Yv6hmQiwL9pizPCg1
!
username ENT_LNS password 0 tunnelpass
username user1@cisco.com password 0 lab
username user2@cisco.com password 0 lab
spe 1/0 1/7
 firmware location system:/ucode/mica_port_firmware
spe 2/0 2/9
 firmware location system:/ucode/mica_port_firmware
!
!
resource-pool disable
clock timezone est 2
!
ip subnet-zero
no ip domain-lookup
ip host CALLGEN-SECURITY-V2 172.24.80.28 10.47.0.0
ip host dirt 172.16.1.129
!
vpdn enable
vpdn tunnel accounting network m1
vpdn session accounting network m1
!
vpdn-group 1
accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname ISP_LAC
 local name ENT_LNS
!
mta receive maximum-recipients 0
!
interface Loopback0
 ip address 192.168.70.101 255.255.255.0
!
interface Loopback1
 ip address 192.168.80.101 255.255.255.0
!
interface FastEthernet0/0/0
 ip address 10.1.26.71 255.255.255.0
 no ip mroute-cache
 no cdp enable
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool vpdn-pool1
 ppp authentication chap
```

```
!
interface Virtual-Template2
 ip unnumbered Loopback1
 peer default ip address pool vpdn-pool2
 ppp authentication chap
!
interface FastEthernet0/0/1
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
ip local pool vpdn-pool1 192.168.70.1 192.168.70.100
ip local pool vpdn-pool2 192.168.80.1 192.168.80.100
ip default-gateway 10.1.26.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.26.254
ip route 10.90.1.2 255.255.255.255 10.1.26.254
no ip http server
ip pim bidir-enable
!
no cdp run
!
radius-server host 172.19.192.80 auth-port 1645 acct-port 1646 key rad123
radius-server retransmit 3
call rsvp-sync
```

その他の参考資料

次の項で、RFC-2867 RADIUS トンネル アカウンティングに関する参考資料を紹介します。

関連資料

関連項目	マニュアル タイトル
RADIUS 属性	『*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2』の「RADIUS Attributes Overview and RADIUS IETF Attributes」
VPDN	『*Cisco IOS XE VPDN Configuration Guide* , Release 2』
ネットワーク アカウンティング	『*Cisco IOS XE Security Configuration Guide: Securing User Services* , Release 2』の「Configuring Accounting」
コマンド	• 『*Cisco IOS Security Command Reference*』 • 『*Cisco IOS VPDN Command Reference*』

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
この機能がサポートする新しいMIBまたは変更されたMIBはありません。また、この機能で変更された既存規格のサポートはありません。	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、およびフィーチャ セットの MIB の場所を検索し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
RFC 2867	『*RADIUS Accounting Modifications for Tunnel Protocol Support*』

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

RFC-2867 RADIUS トンネル アカウンティングの機能情報

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 *2 : RFC-2867 RADIUS* トンネル アカウンティングの機能情報

機能名	リリース	機能情報
RFC-2867 RADIUS トンネル アカウンティング	Cisco IOS XE Release 2.1	RFC-2867 RADIUS トンネル アカウンティングは、6 つの新しい RADIUS アカウンティング タイプを導入しています。これらのタイプは、アカウンティング要求がユーザー サービスの始まり（開始）と終わり（終了）のどちらを表しているかを示す、RADIUS アカウンティング属性の Acct-Status-Type（属性 40）と一緒に使用されます。 また、この機能は、ユーザーによる VPDN セッション イベントのトラブルシューティングを支援する 2 つの新しい仮想プライベート ダイヤルアップ ネットワーク（VPDN）コマンドを導入しています。 この機能は、Cisco IOS XE Release 2.1 で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 次のコマンドが導入または変更されました。**aaa accounting**、**vpdn session accounting network**、**vpdn tunnel accounting network**

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。