RADIUS の設定

- 機能情報の確認，1 ページ
- RADIUS によるスイッチ アクセスの制御の前提条件，1 ページ
- RADIUS によるスイッチ アクセスの制御の制約事項，2 ページ
- RADIUS に関する情報，3 ページ
- RADIUS の設定方法，17 ページ
- CoA 機能のモニタリング，33 ページ
- RADIUS によるスイッチ アクセスの制御の設定例，34 ページ

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。

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 には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

RADIUS によるスイッチ アクセスの制御の前提条件

ここでは、RADIUS による Catalyst スイッチ アクセスの制御の前提条件を示します。

General:

- この章のいずれかのコンフィギュレーション コマンドを使用するには、RADIUS および AAA をイネーブルにする必要があります。
- RADIUS は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。

- 最低限、RADIUS サーバ ソフトウェアが稼働するホスト（1 つまたは複数）を特定し、RADIUS 認証の方式リストを定義する必要があります。 また、任意で RADIUS 許可およびアカウンティングの方式リストを定義できます。
- スイッチ上で RADIUS 機能の設定を行う前に、RADIUS サーバにアクセスし、サーバを設定する必要があります。
- RADIUS ホストは、通常、シスコ（Cisco Secure Access Control Server バージョン 3.0）、Livingston、Merit、Microsoft、または他のソフトウェア プロバイダーの RADIUS サーバ ソフトウェアが稼働しているマルチユーザ システムです。 詳細については、RADIUS サーバのマニュアルを参照してください。
- Change-of-Authorization（CoA）インターフェイスを使用するには、スイッチにセッションがすでに存在している必要があります。 CoA を使用すると、セッションの識別と接続解除要求を実行できます。 アップデートは、指定されたセッションにだけ作用します。
- スイッチ スタックと RADIUS サーバとの間に冗長接続を設定することを推奨します。 これによって、接続済みのスタック メンバの 1 つがスイッチ スタックから削除された場合でも、RADIUS サーバにアクセスできます。

RADIUS 操作の場合：

- ユーザは RADIUS 許可に進む前に、まず RADIUS 認証を正常に完了する必要があります（イネーブルに設定されている場合）。

関連トピック

RADIUS およびスイッチ アクセス, （3 ページ）
RADIUS の動作, （5 ページ）

RADIUS によるスイッチ アクセスの制御の制約事項

ここでは、RADIUS によるスイッチ アクセスの制御の制約事項について説明します。

全般：

- セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。

RADIUS は次のネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境。 RADIUS は、AppleTalk Remote Access（ARA）、NetBIOS Frame Control Protocol（NBFCP）、NetWare Asynchronous Services Interface（NASI）、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間状態。 RADIUS は、双方向認証を行いません。 RADIUS は、他社製のデバイスが認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できます。

- 各種のサービスを使用するネットワーク。 RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

関連トピック

RADIUS の概要, （3 ページ）

RADIUS に関する情報

RADIUS およびスイッチ アクセス

この項では、RADIUS をイネーブルにし、設定する方法について説明します。 RADIUS を使用すると、アカウンティングの詳細を取得したり、認証および許可プロセスの柔軟な管理制御を実現できます。

スイッチは、IPv6 対応の RADIUS をサポートしています。 情報については、『*Cisco IOS XE IPv6 Configuration Guide, Release 2*』の「Implementing ADSL for IPv6」の章の「RADIUS Over IPv6」の項を参照してください。 この機能の設定に関する詳細については、『*Cisco IOS XE IPv6 Configuration Guide, Release 2*』の「Implementing ADSL for IPv6」の章の「Configuring the NAS」の項を参照してください。

（注） ここで使用するコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference, Release 12.4*』および『*Cisco IOS IPv6 Command Reference*』を参照してください。

関連トピック

RADIUS によるスイッチ アクセスの制御の前提条件, （1 ページ）
スイッチのローカル認証および許可の設定
SSH サーバ、統合クライアント、およびサポートされているバージョン

RADIUS の概要

RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。 RADIUS クライアントは、サポート対象の Cisco ルータおよびスイッチ上で稼働します。 クライアントは中央の RADIUS サーバに認証要求を送ります。 中央の RADIUS サーバにはすべてのユーザ認証情報、ネットワーク サービス アクセス情報が登録されています。

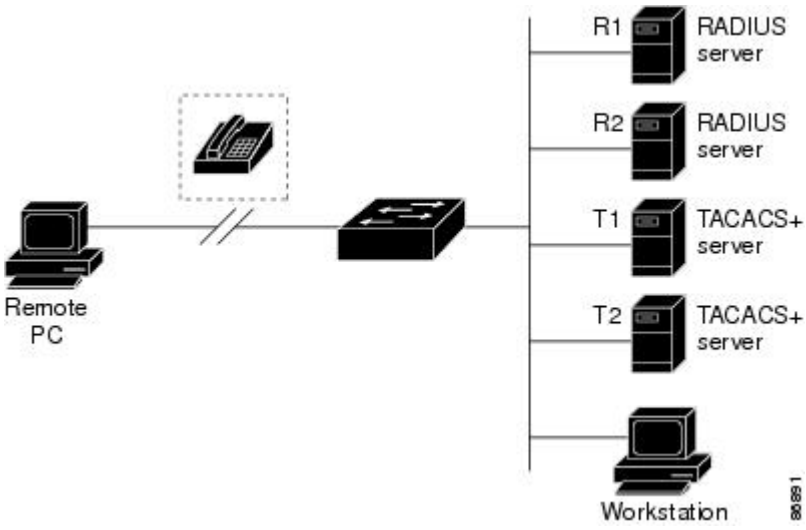
RADIUS は、アクセスのセキュリティが必要な、次のネットワーク環境で使用します。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。 たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データベースを使用します。 複数ベンダーのアクセス サーバからなる IP ベースのネットワー

クでは、ダイヤルインユーザはRADIUSサーバを通じて認証されます。RADIUSサーバは、Kerberos セキュリティ システムで動作するようにカスタマイズされています。

- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、スマート カード アクセス コントロール システムを使用するアクセス環境。 あるケースでは、RADIUS は Enigma のセキュリティ カードとともに使用してユーザを確認し、ネットワーク リソースのアクセスを許可します。
- すでに RADIUS を使用中のネットワーク。 RADIUS クライアント装備の Cisco スイッチをネットワークに追加できます。 これが TACACS+ サーバへの移行の最初のステップとなることもあります。 下の図 2「RADIUS サービスから TACACS+ サービスへの移行」を参照してください。
- ユーザが 1 つのサービスにしかアクセスできないネットワーク。 RADIUS を使用すると、ユーザのアクセスを 1 つのホスト、Telnet などの 1 つのユーティリティ、または IEEE 802.1x などのプロトコルを使用するネットワークに制御できます。 このプロトコルの詳細については、第 11 章「IEEE 802.1x ポートベース認証の設定」を参照してください。
- リソース アカウンティングが必要なネットワーク。 RADIUS 認証または許可とは別個に RADIUS アカウンティングを使用できます。 RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース（時間、パケット、バイトなど）の量を表示できます。 インターネット サービス プロバイダーは、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアのフリーウェアバージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。

図 *1*：*RADIUS* サービスから *TACACS+* サービスへの移行



関連トピック

RADIUS によるスイッチ アクセスの制御の制約事項, （2 ページ）

RADIUS の動作

RADIUS サーバによってアクセス コントロールされるスイッチに、ユーザがログインおよび認証を試みると、次のイベントが発生します。

1. ユーザ名およびパスワードの入力を要求するプロンプトが表示されます。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由でRADIUSサーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
   - ACCEPT：ユーザが認証されたことを表します。
   - REJECT：ユーザの認証が失敗し、ユーザ名およびパスワードの再入力が要求されるか、またはアクセスが拒否されます。
   - CHALLENGE：ユーザに追加データを要求します。
   - CHALLENGE PASSWORD：ユーザは新しいパスワードを選択するように要求されます。

   ACCEPT または REJECT 応答には、特権 EXEC またはネットワーク許可に使用する追加データがバンドルされています。 ACCEPT または REJECT パケットには次の追加データが含まれます。

   - Telnet、SSH、rlogin、または特権 EXEC サービス
   - 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、およびユーザ タイムアウトを含む）

関連トピック

RADIUS によるスイッチ アクセスの制御の前提条件, （1 ページ）

RADIUS 許可の変更

ここでは、使用可能なプリミティブおよびそれらの Change of Authorization（CoA）での使用方法を含む、RADIUS インターフェイスの概要について説明します。

- Change-of-Authorization 要求
- CoA 要求応答コード
- CoA 要求コマンド
- セッション再認証
- セッション強制終了のスタック構成ガイドライン

標準 RADIUS インターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリーが送信されたサーバが応答するプル モデルで使用されます。 Catalyst スイッチは、

通常プッシュ モデルで使用される RFC 5176 で規定された RADIUS Change of Authorization（CoA）拡張機能をサポートし、外部の認証、許可、アカウンティング（AAA）またはポリシーサーバからのセッションのダイナミック再設定ができるようにします。

スイッチは、次のセッション単位の CoA 要求をサポートしています。

- セッション再認証
- セッション終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了

この機能は、Cisco Identity Services Engine と Cisco Secure Access Control Server (ACS) 5.1 に統合されています。

Catalyst スイッチで、RADIUS インターフェイスはデフォルトでイネーブルに設定されています。ただし、次の属性については、一部の基本的な設定が必要になります。

- セキュリティおよびパスワード：このガイドの「スイッチへの不正アクセスの防止」を参照してください。
- アカウンティング：このガイドの「スイッチベース認証の設定」の章の「RADIUS アカウンティングの起動」の項を参照してください。

Change-of-Authorization 要求

Change of Authorization（CoA）要求は、RFC 5176 に記載されているように、プッシュ モデルで使用することによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。 このモデルは、1 つの要求（CoA-Request）と 2 つの可能な応答コードで構成されています。

- CoA acknowledgment（ACK）[CoA-ACK]
- CoA non-acknowledgment（NAK）[CoA-NAK]

要求は CoA クライアント（通常は RADIUS またはポリシー サーバ）から発信されて、リスナーとして動作するスイッチに送信されます。

RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect（POD）とも呼ばれますが、セッション終了に対してスイッチでサポートされています。

次の表に、この機能でサポートされている IETF 属性を示します。

表 *1*：サポートされている *IETF* 属性

属性番号	属性名
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

次の表に、Error-Cause 属性で取ることができる値を示します。

表 *2*：*Error-Cause* の値

値	説明
201	削除された残留セッション コンテキスト
202	無効な EAP パケット（無視）
401	サポートされていない属性
402	見つからない属性
403	NAS 識別情報のミスマッチ
404	無効な要求
405	サポートされていないサービス
406	サポートされていない拡張機能
407	無効な属性値
501	管理上の禁止
502	ルート不可能な要求（プロキシ）
503	セッション コンテキストが検出されない
504	セッション コンテキストが削除できない
505	その他のプロキシ処理エラー

値	説明
506	リソースが使用不可能
507	要求が発信された
508	マルチセッションの選択がサポートされてない

CoA 要求応答コード

CoA 要求応答コードを使用すると、スイッチにコマンドを伝達できます。

関連トピック

CoA 要求コマンド, （9 ページ）

セッションの識別

特定のセッションに向けられた切断と CoA 要求については、スイッチは 1 つ以上の次の属性に基づいて、セッションを検索します。

- Calling-Station-Id（ホスト MAC アドレスを含む IETF 属性 #31）
- Audit-Session-Id VSA（シスコの VSA）
- Acct-Session-Id（IETF 属性 #44）

CoA メッセージに含まれるすべてのセッション ID 属性がそのセッションと一致しない限り、スイッチは「Invalid Attribute Value」エラー コード属性を含む Disconnect-NAK または CoA-NAK を返します。

メッセージに複数のセッション ID 属性が含まれる場合、すべての属性がセッションと一致する必要があります。一致しない場合は、スイッチが「Invalid Attribute Value」エラー コードを含む Disconnect-Negative Acknowledgment（NAK）または CoA-NAK を返します。

RFC 5176 で定義されている CoA 要求コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、および Type Length Value（TLV; タイプ、長さ、値）形式の属性から構成されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                         Authenticator                         |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...
+-+-+-+-+-+-+-+-+-+-+-+-+-
```

属性フィールドは、Cisco ベンダー固有属性（VSA）を送信するために使用します。

関連トピック

CoA 接続解除要求, （11 ページ）
CoA 要求：ホスト ポートのディセーブル化, （11 ページ）
CoA 要求：バウンス ポート, （12 ページ）

CoA ACK 応答コード

許可ステートの変更に成功した場合は、肯定確認応答（ACK）が送信されます。 CoA ACK 内で返される属性は CoA 要求によって異なり、個々の CoA コマンドで検討されます。

CoA NAK 応答コード

否定応答（NAK）は許可ステートの変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。 CoA が成功したかを確認するには、**show** コマンドを使用します。

CoA 要求コマンド

表 *3*：スイッチでサポートされる *CoA* コマンド

コマンド [1]	シスコの VSA
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	これは、VSA を要求しない、標準の接続解除要求です。
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

[1] すべての CoA コマンドには、スイッチと CoA クライアント間のセッション識別情報が含まれている必要があります。

関連トピック

CoA 要求応答コード, （8 ページ）

セッション再認証

不明な ID またはポスチャを持つホストがネットワークに加入して、制限されたアクセス許可プロファイル（たとえば、ゲスト VLAN）に関連付けられると、AAA サーバは通常、セッション再認証要求を生成します。 再認証要求は、クレデンシャルが不明である場合にホストが適切な認証グループに配置されることを許可します。

セッション認証を開始するために、AAA サーバは *Cisco:Avpair="subscriber:command=reauthenticate"* の形式で Cisco VSA と 1 つ以上のセッション ID 属性を含む標準 CoA 要求メッセージを送信します。

現在のセッションステートは、メッセージに対するスイッチの応答を決定します。セッションが現在、IEEE 802.1x によって認証されている場合、スイッチは EAPOL（LAN 経由の拡張認証プロトコル）RequestId メッセージをサーバに送信することで応答します。

現在、セッションが MAC 認証バイパス（MAB）で認証されている場合は、スイッチはサーバにアクセス要求を送信し、初期正常認証で使用されるものと同じ ID 属性を渡します。

スイッチがコマンドを受信したときにセッション認証が実行中である場合は、スイッチはプロセスを終了し、認証シーケンスを再開し、最初に試行されるように設定された方式で開始します。

セッションがまだ認証されてない、あるいはゲスト VLAN、クリティカル VLAN、または同様のポリシーで認証されている場合は、再認証メッセージがアクセス コントロール方式を再開し、最初に試行されるように設定された方式で開始します。 セッションの現在の許可は、再認証によって異なる認証結果になるまで維持されます。

スイッチ スタックでのセッションの再認証

スイッチ スタックでセッション再認証メッセージを受信すると、次の動作が発生します。

- 確認応答（ACK）を戻す前に、再認証の必要性がチェックされます。
- 適切なセッションで再認証が開始されます。
- 認証が成功または失敗のいずれかで完了すると、再認証をトリガーする信号がスタック メンバから削除されます。
- 認証の完了前にスタック マスターに障害が発生すると、（後で削除される）元のコマンドに基づいたスタック マスターの切り替え後、再認証が開始されます。
- ACK の送信前にスタック マスターに障害が発生した場合、新たなスタック マスターでは、再転送コマンドが新しいコマンドとして扱われます。

セッションの終了

セッションを終了させる 3 種類の CoA 要求があります。 CoA 接続解除要求は、ホスト ポートをディセーブルにせずにセッションを終了します。 このコマンドを使用すると、指定されたホストのオーセンティケータ ステートマシンが再初期化されますが、そのホストのネットワークへのアクセスは制限されません。

ホストのネットワークへのアクセスを制限するには、Cisco:Avpair="subscriber:command=disable-host-port" VSA の設定で CoA 要求を使用します。 このコマンドは、ネットワーク上で障害を引き起こしたと認識されているホストがある場合に便利であり、そのホストに対してネットワーク アクセスをただちにブロックする必要があります。 ポートへのネットワーク アクセスを復旧する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

プリンタなどのサプリカントを持たないデバイスが新しいIPアドレスを取得する必要がある場合（たとえば、VLAN 変更後）は、ポート バウンスでホスト ポート上のセッションを終了します（ポートを一時的にディセーブルした後、再びイネーブルにする）。

CoA 接続解除要求

このコマンドは標準の接続解除要求です。 このコマンドはセッション指向であるため、1 つ以上のセッションID属性とともに使用する必要があります。 セッションが見つからない場合、スイッチは Disconnect-NAK メッセージと「Session Context Not Found」エラー コード属性を返します。 セッションがある場合は、スイッチはセッションを終了します。 セッションが完全に削除された後、スイッチは接続解除 ACK を返します。

スイッチがクライアントに接続解除 ACK を返す前にスタンバイ スイッチにフェールオーバーする場合は、クライアントから要求が再送信されるときに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。 再送信後もセッションが見つからない場合は、Disconnect-ACK と「Session Context Not Found」エラー コード属性が送信されます。

関連トピック

セッションの識別, （8 ページ）

CoA 要求：ホスト ポートのディセーブル化

このコマンドは、次の新しい VSA が含まれている標準 CoA 要求メッセージで伝達されます。

Cisco:Avpair="subscriber:command=disable-host-port"

このコマンドはセッション指向であるため、1 つ以上のセッション ID 属性とともに使用する必要があります。 セッションが見つからない場合、スイッチはCoA-NAKメッセージと「Session Context Not Found」エラー コード属性を返します。 このセッションがある場合は、スイッチはホスト ポートをディセーブルにし、CoA-ACK メッセージを返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるときに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。 スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブ スイッチ上でその動作が再開されます。

（注） 再送信コマンドの後に接続解除要求が失敗すると、（接続解除ACKが送信されてない場合に）チェンジオーバー前にセッションが正常終了し、または元のコマンドが実行されてスタンバイ スイッチがアクティブになるまでの間に発生した他の方法（たとえば、リンク障害）によりセッションが終了することがあります。

関連トピック

セッションの識別, （8 ページ）

CoA 要求：バウンス ポート

このコマンドは、次の VSA を含む標準の CoA-Request メッセージで伝達されます。

Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッション指向であるため、1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、スイッチはCoA-NAKメッセージと「Session Context Not Found」エラー コード属性を返します。このセッションがある場合は、スイッチはホスト ポートを 10 秒間ディセーブルし、再びイネーブルにし（ポート バウンス）、CoA-ACK を返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信されるときに、新しいアクティブ スイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブ スイッチ上でその動作が再開されます。

関連トピック

セッションの識別, （8 ページ）

セッション強制終了のスタック構成ガイドライン

スイッチ スタックでは、CoA 接続解除要求メッセージに必要な特別な処理はありません。

CoA 要求バウンス ポートのスタック構成ガイドライン

bounce-port コマンドのターゲットはポートではなくセッションのため、セッションが見つからなかった場合、コマンドは実行できません。

スタック マスターで Auth Manager コマンド ハンドラが有効な **bounce-port** コマンドを受信すると、CoA-ACK メッセージを返す前に次の情報が確認されます。

- ポート バウンスの必要性
- ポート ID（ローカル セッション コンテキストで検出された場合）

スイッチで、ポート バウンスが開始されます（ポートが 10 秒間ディセーブルになり、再びイネーブルにされます）。

ポート バウンスが正常に実行された場合、ポート バウンスをトリガーした信号がスタンバイ スタック マスターから削除されます。

ポートバウンスの完了前にスタックマスターに障害が発生すると、（後で削除される）元のコマンドに基づいたスタック マスターの切り替え後、ポート バウンスが開始されます。

CoA-ACK メッセージの送信前にスタック マスターに障害が発生した場合、新たなスタック マスターでは、再送信コマンドが新しいコマンドとして扱われます。

CoA 要求ディセーブル ポートのスタック構成ガイドライン

disable-port コマンドのターゲットはポートではなくセッションのため、セッションが見つからなかった場合、コマンドは実行できません。

スタック マスターにある Auth Manager コマンド ハンドラで、有効な **disable-port** コマンドを受信した場合、CoA-ACK メッセージを返す前に次の情報が検証されます。

- ポート ディセーブルの必要性
- ポート ID（ローカル セッション コンテキストで検出された場合）

スイッチで、ポートをディセーブルする操作が試行されます。

ポートをディセーブルする操作が正常に実行された場合、ポートをディセーブルする操作をトリガーした信号がスタンバイ スタック マスターから削除されます。

ポートをディセーブルする操作の完了前にスタック マスターに障害が発生すると、（後で削除される）元のコマンドに基づいたスタック マスターの切り替え後、ポートがディセーブルにされます。

CoA-ACK メッセージの送信前にスタック マスターに障害が発生した場合、新たなスタック マスターでは、再送信コマンドが新しいコマンドとして扱われます。

RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。 RADIUS をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

RADIUS サーバ ホスト

スイッチと RADIUS サーバ間の通信には、次の要素が関係します。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- キー文字列
- タイムアウト時間
- 再送信回数

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって特定します。 IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、特定の AAA サービスを提供する RADIUS

ホストとして個々のポートを定義できます。 この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。

同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト 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。 この例では、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、スイッチは「%RADIUS-4-RADIUS_DEAD」メッセージを表示し、その後、同じデバイス上で 2 番めに設定されたホスト エントリでアカウンティング サービスを試みます（RADIUS ホストエントリは、設定した順序に従って試行されます）。

RADIUS サーバとスイッチは、共有するシークレット テキスト ストリングを使用して、パスワードの暗号化および応答の交換を行います。 RADIUS で AAA セキュリティ コマンドを使用するように設定するには、RADIUS サーバ デーモンが稼働するホストと、そのホストがスイッチと共有するシークレット テキスト（キー）ストリングを指定する必要があります。

タイムアウト、再送信回数、および暗号キーの値は、すべての RADIUS サーバに対してグローバルに設定することもできますし、サーバ単位で設定することもできます。また、グローバルな設定とサーバ単位での設定を組み合わせることもできます。

関連トピック

RADIUS サーバ ホストの識別, （17 ページ）
AAA サーバ グループの定義, （21 ページ）
すべての RADIUS サーバの設定, （26 ページ）
RADIUS ログイン認証の設定, （19 ページ）

RADIUS ログイン認証

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。 方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式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です。 デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。 認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。 ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。 このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。 この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

関連トピック

RADIUS ログイン認証の設定, （19 ページ）

AAA サーバ グループ

既存のサーバ ホストを認証用にグループ化するため、AAA サーバ グループを使用するようにスイッチを設定できます。 設定済みのサーバホストのサブセットを選択して、それを特定のサービスに使用します。 サーバ グループは、選択されたサーバ ホストの IP アドレスのリストを含むグローバルなサーバ ホスト リストとともに使用されます。

サーバグループには、同じサーバの複数のホストエントリを含めることもできますが、各エントリが一意の ID（IP アドレスと UDP ポート番号の組み合わせ）を持っていることが条件です。 この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。 同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト 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。

関連トピック

AAA サーバ グループの定義, （21 ページ）

AAA 許可

AAA 許可によってユーザが使用できるサービスが制限されます。 AAA 許可をイネーブルにすると、スイッチは（ローカル ユーザ データベースまたはセキュリティ サーバ上に存在する）ユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。 ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが許可されます。

関連トピック

ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定, （24 ページ）

RADIUS アカウンティング

AAA アカウンティング機能は、ユーザが使用したサービスと、消費したネットワーク リソース量を追跡します。 AAA アカウンティングをイネーブルにすると、スイッチはユーザの活動状況をアカウンティング 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。 これらのデータは、ネットワーク管理、クライアントへの課金、または監査のために後で分析できます。

関連トピック

RADIUS アカウンティングの起動, （25 ページ）

ベンダー固有の RADIUS 属性

Internet Engineering Task Force（IETF）ドラフト規格に、ベンダー固有の属性（属性 26）を使用して、スイッチと RADIUS サーバ間でベンダー固有の情報を通信するための方式が定められています。 各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。 シスコが実装する RADIUS では、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを 1 つサポートしています。 シスコのベンダー ID は 9 であり、サポート対象のオプションはベンダータイプ 1（名前は *cisco-avpair*）です。 この値は、次のフォーマットのストリングです。

```
protocol : attribute sep value *
```

protocol は、特定の許可タイプに使用するシスコのプロトコル属性の値です。 *attribute* および *value* は、シスコの TACACS+ 仕様で定義されている適切な属性値（AV）ペアです。 *sep* は、必須の属性の場合は =、任意指定の属性の場合は * です。 TACACS+ 許可で使用できるすべての機能は、RADIUS でも使用できます。

他のベンダーにも、それぞれ独自のベンダー ID、オプション、および対応する VSA があります。 ベンダー ID および VSA の詳細については、RFC 2138『Remote Authentication Dial-In User Service（RADIUS）』を参照してください。

RADIUS 属性の完全なリスト、またはベンダー固有の属性 26 の詳細については、『*Cisco IOS Security Configuration Guide*』の付録「RADIUS Attributes」を参照してください。

関連トピック

ベンダー固有の RADIUS 属性を使用するスイッチ設定, （28 ページ）

ベンダー独自仕様の RADIUS サーバ通信

RADIUS に関する IETF ドラフト規格では、スイッチと RADIUS サーバ間でベンダー独自仕様の情報を通信する方式について定められていますが、RADIUS 属性セットを独自に機能拡張しているベンダーもあります。 Cisco IOS ソフトウェアは、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

前述したように、RADIUS（ベンダーの独自仕様によるものか、IETF ドラフトに準拠するものかを問わず）を設定するには、RADIUS サーバ デーモンが稼働しているホストと、そのホストがスイッチと共有するシークレット テキスト ストリングを指定する必要があります。 RADIUS ホストおよびシークレット テキスト ストリングを指定するには、**radius-server** 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。

関連トピック

ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定, （29 ページ）

RADIUS の設定方法

RADIUS サーバ ホストの識別

スイッチと通信するすべての RADIUS サーバに対して、これらの設定をグローバルに適用するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** の 3 つの固有のグローバル コンフィギュレーション コマンドを使用します。 これらの設定を特定の RADIUS サーバに適用するには、**radius-server host** 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。

既存のサーバ ホストを認証用にグループ化するため、AAA サーバ グループを使用するようにスイッチを設定できます。 詳細については、次の関連項目を参照してください。

RADIUS サーバ上でも、いくつかの値を設定する必要があります。 これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの双方で共有するキー ストリングがあります。 詳細については、RADIUS サーバのマニュアルを参照してください。

はじめる前に

スイッチ上にグローバルな機能とサーバ単位での機能（タイムアウト、再送信回数、およびキーコマンド）を設定した場合、サーバ単位で設定したタイムアウト、再送信回数、およびキーに関するコマンドは、グローバルに設定したタイムアウト、再送信回数、およびキーに関するコマンドを上書きします。 すべての RADIUS サーバに対してこれらの値を設定する方法については、次の関連項目を参照してください。

手順の概要

1. **configure terminal**
2. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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 2	**radius-server host** {*hostname* | *ip-address*} [**auth-port**	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。

	コマンドまたはアクション	目的
	port-number] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] 例： `Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1`	• （任意）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。 • （任意）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （任意）**timeout** *seconds* には、スイッチが RADIUS サーバの応答を待機して再送信するまでの時間間隔を指定します。 指定できる範囲は 1 ～ 1000 です。 この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドによる設定を上書きします。 **radius-server host** コマンドでタイムアウトを設定しない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。 指定できる範囲は 1 ～ 1000 です。 **radius-server host** コマンドで再送信回数を指定しない場合、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string* には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。 （注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。 キーは常に **radius-server host** コマンドの最後のアイテムとして設定してください。 先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。 キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 1 つの IP アドレスに対応する複数のホスト エントリをスイッチが認識するように設定するには、それぞれ異なる UDP ポート番号を使用して、このコマンドを必要な回数だけ入力します。 スイッチ ソフトウェアは、指定された順序に従って、ホストを検索します。 各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーの値をそれぞれ設定してください。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

RADIUS サーバ ホスト, （13 ページ）
AAA サーバ グループの定義, （21 ページ）

すべての RADIUS サーバの設定, （26 ページ）

RADIUS ログイン認証の設定

RADIUS ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。

はじめる前に

AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。 AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

ip http authentication コマンドの詳細については、『*Cisco IOS Security Command Reference, Release 12.4*』を参照してください。

手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
4. **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]
5. **login authentication** {**default** | *list-name*}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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 2	**aaa new-model** 例： `Switch(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 例： `Switch(config)# aaa`	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定されなかった場合に使用され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する方式を指定します。 デフォルトの方式リストは、自動的にすべてのポートに適用されます。

	コマンドまたはアクション	目的
	authentication login default local	• *list-name* には、作成するリストの名前として使用する文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。 追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 ◦ *enable*：イネーブル パスワードを認証に使用します。 この認証方式を使用するには、あらかじめ **enable** *password* 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イネーブル パスワードを定義しておく必要があります。 ◦ *group radius*：RADIUS 認証を使用します。 この認証方式を使用するには、あらかじめ RADIUS サーバを設定しておく必要があります。 ◦ *line*：回線パスワードを認証に使用します。 この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。 **password** *password* ライン コンフィギュレーション コマンドを使用します。 ◦ *local*：ローカル ユーザ名データベースを認証に使用します。 データベースにユーザ名情報を入力しておく必要があります。 **username** *name* **password** 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。 ◦ *local-case*：大文字と小文字が区別されるローカルユーザ名データベースを認証に使用します。 **username** *password* 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、ユーザ名情報をデータベースに入力する必要があります。 ◦ *none*：ログインに認証を使用しません。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*] 例： `Switch(config)# line 1 4`	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	1 つの回線または複数回線に認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。

	コマンドまたはアクション	目的
	例： `Switch(config)# login authentication default`	• *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

RADIUS ログイン認証, （14 ページ）
RADIUS サーバ ホスト, （13 ページ）

AAA サーバ グループの定義

定義したグループ サーバに特定のサーバを対応付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。 サーバを IP アドレスで特定することもできますし、任意指定の **auth-port** および **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを特定することもできます。

AAA サーバ グループを定義するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
3. **aaa new-model**
4. **aaa group server radius** *group-name*
5. **server** *ip-address*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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 2	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] 例： `Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1`	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。 • （任意）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （任意）**timeout** *seconds* には、スイッチが RADIUS サーバの応答を待機して再送信するまでの時間間隔を指定します。 指定できる範囲は 1 ～ 1000 です。 この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドによる設定を上書きします。 **radius-server host** コマンドでタイムアウトを設定しない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。 指定できる範囲は 1 ～ 1000 です。 **radius-server host** コマンドで再送信回数を指定しない場合、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string* には、RADIUS サーバ上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。 （注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。 キーは常に **radius-server host** コマンドの最後のアイテムとして設定してください。 先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。 キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 1 つの IP アドレスに対応する複数のホスト エントリをスイッチが認識するように設定するには、それぞれ異なる UDP ポート番号を使用して、このコマンドを必要な回数だけ入力します。 スイッチ ソフトウェアは、指定された順序に従って、ホストを検索します。 各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーの値をそれぞれ設定してください。

	コマンドまたはアクション	目的
ステップ 3	**aaa new-model** 例： `Switch(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa group server radius** *group-name* 例： `Switch(config)# aaa group server radius group1`	グループ名を指定して AAA サーバ グループを定義します。 このコマンドを使用すると、スイッチはサーバ グループ コンフィギュレーション モードになります。
ステップ 5	**server** *ip-address* 例： `Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001`	特定の RADIUS サーバを定義済みのサーバ グループと関連付けます。AAA サーバ グループの RADIUS サーバごとに、このステップを繰り返します。 グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

2 台の異なる RADIUS グループ サーバの使用

次の例では、2 つの異なる RADIUS グループ サーバ（*group1* および *group2*）を認識するようにスイッチを設定しています。 group1 では、同じ RADIUS サーバ上の異なる 2 つのホスト エントリを、同じサービス用に設定しています。 2 番目のホスト エントリが、最初の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。

```
Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

関連トピック

RADIUS サーバ ホストの識別, （17 ページ）

RADIUS サーバ ホスト，（13 ページ）
AAA サーバ グループ，（15 ページ）

ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定

（注） 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

ユーザ特権アクセスおよびネットワーク サービスに関する RADIUS 許可を設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **aaa authorization network radius**
3. **aaa authorization exec radius**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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 2	**aaa authorization network radius** 例： `Switch(config)# aaa authorization network radius`	ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可を、スイッチに設定します。
ステップ 3	**aaa authorization exec radius** 例： `Switch(config)# aaa authorization exec radius`	ユーザに特権 EXEC のアクセス権限がある場合、ユーザ RADIUS 許可を、スイッチに設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

次の作業

グローバル コンフィギュレーション コマンド **aaa authorization** と **radius** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

aaa authorization exec radius local コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。

関連トピック

AAA 許可, （15 ページ）

RADIUS アカウンティングの起動

RADIUS アカウンティングを起動するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **aaa accounting network start-stop radius**
3. **aaa accounting exec start-stop radius**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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 2	**aaa accounting network start-stop radius** 例： `Switch(config)# aaa accounting network start-stop radius`	ネットワーク関連のあらゆるサービス要求に関して、RADIUS アカウンティングをイネーブルにします。
ステップ 3	**aaa accounting exec start-stop radius** 例： `Switch(config)# aaa accounting exec start-stop radius`	RADIUS アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

次の作業

AAA サーバが到達不能の場合に、ルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。 このコマンドは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です） 場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合、ルータとのコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

関連トピック

RADIUS アカウンティング，（15 ページ）

すべての RADIUS サーバの設定

すべての RADIUS サーバを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **radius-server key** *string*
3. **radius-server retransmit** *retries*
4. **radius-server timeout** *seconds*
5. **radius-server deadtime** *minutes*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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 2	**radius-server key** *string* 例： `Switch(config)# radius-server key your_server_key`	スイッチとすべての RADIUS サーバ間で共有されるシークレット テキスト ストリングを指定します。 （注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。 先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。 キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 3	**radius-server retransmit** *retries* 例： `Switch(config)# radius-server retransmit 5`	スイッチが RADIUS 要求をサーバに再送信する回数を指定します。 デフォルトは 3 です。指定できる範囲は 1 ～ 1000 です。
ステップ 4	**radius-server timeout** *seconds* 例： `Switch(config)# radius-server timeout 3`	スイッチが RADIUS 要求に対する応答を待って、要求を再送信するまでの時間（秒）を指定します。 デフォルトは 5 秒です。指定できる範囲は 1 ～ 1000 です。
ステップ 5	**radius-server deadtime** *minutes* 例： `Switch(config)# radius-server`	RADIUS サーバが認証要求に応答していない場合、このコマンドはそのサーバに対する要求を停止する時刻を指定します。 これにより、要求がタイムアウトするまで待たずとも、次に設定されているサーバを試行することができます。 デフォルトは 0 です。指定できる範囲は 0 ～ 1440 分です。

	コマンドまたはアクション	目的
	deadtime 0	
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

RADIUS サーバ ホストの識別，（17 ページ）
RADIUS サーバ ホスト，（13 ページ）

ベンダー固有の RADIUS 属性を使用するスイッチ設定

ベンダー固有の RADIUS 属性を使用するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **radius-server vsa send** [**accounting** | **authentication**]
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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 2	**radius-server vsa send** [**accounting** | **authentication**] 例： `Switch(config)# radius-server vsa send`	スイッチが VSA（RADIUS IETF 属性 26 で定義）を認識して使用できるようにします。 • （任意）認識されるベンダー固有属性の集合をアカウンティング属性だけに限定するには、**accounting** キーワードを使用します。

	コマンドまたはアクション	目的
		• （任意）認識されるベンダー固有属性の集合を認証属性だけに限定するには、**authentication** キーワードを使用します。 キーワードを指定せずにこのコマンドを入力すると、アカウンティングおよび認証のベンダー固有属性の両方が使用されます。
ステップ 3	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

ベンダー固有の RADIUS 属性, （16 ページ）

ベンダー独自の RADIUS サーバとの通信に関するスイッチ設定

ベンダー独自仕様の RADIUS サーバ通信を使用するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **radius-server host** {*hostname* | *ip-address*} **non-standard**
3. **radius-server key** *string*
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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 2	**radius-server host** {*hostname* | *ip-address*} **non-standard** 例： `Switch(config)# radius-server host 172.20.30.15 nonstandard`	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、RADIUS のベンダー独自仕様の実装を使用することを指定します。
ステップ 3	**radius-server key** *string* 例： `Switch(config)# radius-server key rad124`	スイッチとベンダー独自仕様の RADIUS サーバとの間で共有されるシークレット テキスト ストリングを指定します。 スイッチおよび RADIUS サーバは、このテキスト ストリングを使用して、パスワードの暗号化および応答の交換を行います。 （注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。 先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。 キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 4	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

次の作業

この機能を使用すると、アクセス要求および認証要求を、サーバ グループ内のすべての RADIUS サーバに対して均等に送信できます。 詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「RADIUS Server Load Balancing」の章を参照してください。

関連トピック

ベンダー独自仕様の RADIUS サーバ通信, （16 ページ）

スイッチ上での CoA の設定

スイッチ上で CoA を設定するには、特権 EXEC モードで次の手順を実行します。 この手順は必須です。

手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **aaa server radius dynamic-author**
4. **client** {*ip-address* | *name*} [**vrf** *vrfname*] [**server-key** *string*]
5. **server-key** [**0** | **7**] *string*
6. **port** *port-number*
7. **auth-type** {**any** | **all** | **session-key**}
8. **ignore session-key**
9. **ignore server-key**
10. **authentication command bounce-port ignore**
11. **authentication command disable-port ignore**
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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 2	**aaa new-model** 例： `Switch(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 3	**aaa server radius dynamic-author** 例： `Switch(config)# aaa server radius dynamic-author`	スイッチを認証、許可、アカウンティング（AAA）サーバに設定し、外部ポリシー サーバとの相互作用を実行します。
ステップ 4	**client** {*ip-address* | *name*} [**vrf** *vrfname*] [**server-key** *string*]	ダイナミック許可ローカル サーバ コンフィギュレーション モードを開始し、デバイスが CoA を受け取り、要求を取り外す RADIUS クライアントを指定します。
ステップ 5	**server-key** [**0** | **7**] *string* 例： `Switch(config-sg-radius)#`	RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。

	コマンドまたはアクション	目的
	server-key your_server_key	
ステップ 6	**port** *port-number* 例： `Switch(config-sg-radius)# port 25`	設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。
ステップ 7	**auth-type** {**any** | **all** | **session-key**} 例： `Switch(config-sg-radius)# auth-type any`	スイッチが RADIUS クライアントに使用する許可のタイプを指定します。 クライアントは、許可用に設定されたすべての属性と一致していなければなりません。
ステップ 8	**ignore session-key**	（任意）セッション キーを無視するようにスイッチを設定します。 **ignore** コマンドの詳細については、Cisco.com 上の『*Cisco IOS Intelligent Services Gateway Command Reference*』を参照してください。
ステップ 9	**ignore server-key** 例： `Switch(config-sg-radius)# ignore server-key`	（任意）サーバキーを無視するようにスイッチを設定します。 **ignore** コマンドの詳細については、Cisco.com 上の『*Cisco IOS Intelligent Services Gateway Command Reference*』を参照してください。
ステップ 10	**authentication command bounce-port ignore** 例： `Switch(config-sg-radius)# authentication command bounce-port ignore`	（任意）CoA 要求を無視して、セッションをホスティングするポートを一時的にディセーブルにするようにスイッチを設定します。 ポートを一時的にディセーブルにする目的は、VLAN の変更が発生しても、その変更を検出するサプリカントがエンドポイント上にない場合に、ホストから DHCP 再ネゴシエーションを行わせることです。
ステップ 11	**authentication command disable-port ignore** 例： `Switch(config-sg-radius)# authentication command disable-port ignore`	（任意）セッションをホスティングしているポートを管理上のシャットダウン状態にすることを要求する非標準コマンドを無視するようにスイッチを設定します。 ポートをシャットダウンすると、セッションが終了します。 ポートを再びイネーブルにするには、標準の CLI または SNMP コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Switch(config-sg-radius)# end`	特権 EXEC モードに戻ります。

CoA 機能のモニタリング

表 *4*：特権 *EXEC* 表示コマンド

コマンド	目的
show aaa attributes protocol radius	RADIUS コマンドの AAA 属性を表示します。

表 *5*：グローバル トラブルシューティング コマンド

コマンド	目的
debug radius	RADIUS のトラブルシューティングを行うための情報を表示します。
debug aaa coa	CoA 処理のトラブルシューティングを行うための情報を表示します。
debug aaa pod	POD パケットのトラブルシューティングを行うための情報を表示します。
debug aaa subsys	POD パケットのトラブルシューティングを行うための情報を表示します。
debug cmdhd [**detail** | **error** | **events**]	コマンドヘッダーのトラブルシューティングを行うための情報を表示します。

出力フィールドの詳細については、このリリースに対応するコマンド リファレンスを参照してください。

RADIUS によるスイッチ アクセスの制御の設定例

例：RADIUS サーバ ホストの識別

次に、1 つの RADIUS サーバを認証用に、もう 1 つの RADIUS サーバをアカウンティング用に設定する例を示します。

```
Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

次に、*host1* を RADIUS サーバとして設定し、認証およびアカウンティングの両方にデフォルトのポートを使用するように設定する例を示します。

```
Switch(config)# radius-server host host1
```

例：ベンダー固有の RADIUS 属性を使用するスイッチ設定

たとえば、次の AV ペアを指定すると、IP 許可時（PPP の IPCP アドレスの割り当て時）に、シスコの複数の名前付き *IP* アドレス プール機能が有効になります。

```
cisco-avpair= ”ip:addr-pool=first“
```

次に、スイッチから特権 EXEC コマンドへの即時アクセスが可能となるユーザ ログインを提供する例を示します。

```
cisco-avpair= ”shell:priv-lvl=15“
```

次に、RADIUS サーバ データベース内の許可 VLAN を指定する例を示します。

```
cisco-avpair= ”tunnel-type(#64)=VLAN(13)”
cisco-avpair= ”tunnel-medium-type(#65)=802 media(6)”
cisco-avpair= ”tunnel-private-group-id(#81)=vlanid”
```

次に、この接続中に ASCII 形式の入力 ACL をインターフェイスに適用する例を示します。

```
cisco-avpair= “ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0”
cisco-avpair= “ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any”
cisco-avpair= “mac:inacl#3=deny any any decnet-iv”
```

次に、この接続中に ASCII 形式の出力 ACL をインターフェイスに適用する例を示します。

```
cisco-avpair= “ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any”
```

例：ベンダー独自仕様の RADIUS サーバとの通信に関するスイッチ設定

次に、ベンダー独自仕様のRADIUSホストを指定し、スイッチとサーバの間で*rad124*という秘密キーを使用する例を示します。

```
Switch(config)# radius-server host 172.20.30.15 nonstandard
Switch(config)# radius-server key rad124
```