# TACACS+ と RADIUS の比較

## 目次



## 概要

ネットワークへのアクセスを制御するために使用される 2 つの主要なセキュリティ プロトコルは、Cisco TACACS+ および RADIUS です。 RADIUS の仕様は、RFC 2865 に記述されています（これにより、RFC 2138 は廃止されました）。 Cisco では、クラス最高のサービスとともに両方のプロトコルをサポートするよう尽力しています。 RADIUS と競合したり、お客様に TACACS+ の使用を促すことは、Cisco の意図ではありません。 お客様が各自のニーズに最適なソリューションを、ご自分で選択することが必要です。 この文書では、情報に基づいた選択を行えるように、TACACS+ と RADIUS の違いについて説明します。

Cisco は 1996 年 2 月の Cisco IOS® ソフトウェア リリース 11.1 以来の RADIUSプロトコルをサポートしました。 Cisco では、引き続き RADIUS クライアントを新機能で強化し、RADIUS を標準としてサポートします。

Cisco では、TACACS+ を開発前する前に、RADIUS をセキュリティ プロトコルとして真剣に評価していました。 TACACS+ プロトコルには、成長するセキュリティ市場のニーズを満たす多くの機能が組み込まれました。 このプロトコルは、ネットワークの成長に伴って拡大し、市場の熟成に伴って新しいセキュリティ テクノロジーに対応する設計になっています。 TACACS+ プロトコルの基本アーキテクチャは、独立した Authentication, Authorization, and Accounting（AAA; 認

証、認可、およびアカウンティング）アーキテクチャを補完します。

# 前提条件

## 要件

このドキュメントに関する固有の要件はありません。

## 使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

## 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# RADIUS の背景説明

RADIUS は、AAA プロトコルを使用するアクセス サーバです。 また、ネットワークおよびネットワーク サービスへのリモート アクセスを不正アクセスから保護する分散セキュリティ システムです。 RADIUS は、次の 3 つのコンポーネントで構成されます。

- User Datagram Protocol（UDP; ユーザ データグラム プロトコル）/IP を利用するフレーム形式を持つプロトコル
- サーバ
- クライアント。

サーバは、通常はカスタマー サイトにある中央コンピュータで動作します。クライアントは、ダイヤルアップ アクセス サーバに常駐し、ネットワーク全体に分散させることができます。 Cisco では、RADIUS クライアントを、Cisco IOS ソフトウェア リリース 11.1 以降および他のデバイス ソフトウェアに組み込んでいます。

## クライアント/サーバ モデル

Network Access Server（NAS; ネットワーク アクセス サーバ）は、RADIUS のクライアントとして動作します。 クライアントは、指定された RADIUS サーバにユーザ情報を渡し、返された応答に基づいて対応します。 RADIUS サーバは、ユーザ接続要求を受信し、ユーザを認証してから、そのユーザにサービスを配信するためにクライアントに必要な構成情報をすべて返します。 RADIUS サーバは、その他の種類の認証サーバのプロキシ クライアントとしての役割を果たすこともできます。

## ネットワーク セキュリティ

クライアントと RADIUS サーバ間のトランザクションは、ネットワークを通じて送信されることのない共有秘密情報を使用して認証されます。 また、ユーザ パスワードはすべて、クライアントと RADIUS サーバ間で暗号化されて送信されます。 これにより、セキュリティで保護されていないネットワークをスヌーピングしている何者かにユーザのパスワードが盗まれる可能性が解消されます。

### 柔軟な認証メカニズム

RADIUS サーバは、ユーザを認証するためにさまざまな方法をサポートします。 ユーザが入力したユーザ名とオリジナル パスワードが提供された場合、RADIUS サーバは PPP、Password Authentication Protocol（PAP; パスワード認証プロトコル）、または Challenge Handshake Authentication Protocol（CHAP）、UNIX ログイン、およびその他の認証機構をサポートできます。

### サーバ コードのアベイラビリティ

各種のサーバ コードが有償または無償で配布されています。 Cisco サーバには、Cisco Secure ACS for Windows、Cisco Secure ACS for UNIX、および Cisco Access Registrar があります。

## TACACS+ と RADIUS の比較

この項では、TACACS+ と RADIUS の機能をいくつか比較します。

### UDP と TCP

RADIUS では UDP を使用し、TACACS+ では TCP を使用します。 TCP には、UDP に比べていくつかの利点があります。 TCP はコネクション型転送、UDP はベストエフォート型配送を行います。 RADIUS には、追加のプログラマブル変数（ベストエフォート型転送を補正するための再送信試行、タイムアウトなど）が必要ですが、TCP 転送が提供する組み込みサポートのレベルはありません。

- TCP を使用すると、バックエンドの認証メカニズム（TCP ACK）の負荷がどれだけ高くて低速でも、（おおよその）ネットワークの Round-Trip Time（RTT; ラウンドトリップ時間）以内に、要求が受信されたことを示す確認応答が別に送信されます。
- TCP では、クラッシュしている（動作していない）サーバがリセット（RST）によって即座に示されます。 長期 TCP 接続を使用している場合は、サーバがいつクラッシュし、いつサービスに戻るかを判別できます。 UDP では、ダウンしているサーバ、低速なサーバ、存在しないサーバを区別することができません。
- TCP キープアライブを使用すると、サーバのクラッシュは実際の要求によってアウトバンドで検出できます。 複数サーバへの接続を同時に維持することができます。また、起動して実行中であることがわかっているサーバにだけメッセージを送信する必要があります。
- TCP は、よりスケーラブルであり、ネットワークの成長および輻輳に対応が可能です。

### パケット暗号化

RADIUS では、クライアントからサーバへのアクセス要求パケット内のパスワードだけが暗号化されます。 パケット内の残りの内容は暗号化されません。 他の情報（ユーザ名、認可されたサービス、アカウンティングなど）は、第三者によってキャプチャされる可能性があります。

TACACS+ では、パケットの本体全体が暗号化されますが、標準 TACACS+ ヘッダーはそのままになります。 ヘッダー内には、本体が暗号化されているかどうかを示すフィールドがあります。 デバッグ目的のために、パケットの本体は暗号化しないままにしておくと便利です。 ただし、通常の動作時には、より安全な通信を行うためにパケットの本体は完全に暗号化されています。

### 認証および許可

RADIUS では、認証と許可が組み合せて使用されます。 RADIUS サーバからクライアントに送信されるアクセス許可パケットには、許可情報が含まれています。 これにより、認証と認可を切り離すことが困難になります。

TACACS+ では AAA アーキテクチャが使用され、AAA が分離されます。 これにより、TACACS+ を認可およびアカウンティングに使用できる別個の認証ソリューションが可能になります。 たとえば、TACACS+ では、Kerberos 認証と TACACS+ 認可およびアカウンティングを使用することが可能です。 NAS は Kerberos サーバ上で認証を行った後、再認証を行わずに TACACS+ サーバから認可情報を要求できます。 NAS が Kerberos サーバでの認証に成功したことを TACACS+ サーバに通知すると、サーバは認可情報を提供します。

セッション中、追加の認可チェックが必要になった場合、アクセス サーバは TACACS+ サーバを使用して、ユーザに特定のコマンドを使用する権限が付与されているかどうかを確認します。 これにより、アクセス サーバで実行可能なコマンドを、認証メカニズムと切り離して制御できます。

## マルチプロトコル サポート

RADIUS では、次のプロトコルはサポートしていません。

- AppleTalk Remote Access（ARA）プロトコル
- NetBIOS Frame Protocol Control プロトコル
- Novell Asynchronous Services Interface（NASI）
- X.25 PAD 接続

TACACS+ では、マルチプロトコル サポートを提供しています。

## ルータの管理

RADIUS の場合、ユーザがルータ上で実行できるコマンドと実行できないコマンドを制御することはできません。 したがって、RADIUS は比較的ルータ管理については有用ではなく、ターミナル サービスについては柔軟ではありません。

TACACS+ では、ユーザ単位またはグループ単位でルータ コマンドの許可を制御できる 2 つの方式があります。 1 つ目の方式では、特権レベルをコマンドに割り当てて、ルータが TACACS+ サーバを使用して、特定の特権レベルでユーザが許可されているかどうかを検証します。 2 つ目の方式では、TACACS+ サーバ内で、許可するコマンドをユーザ単位またはグループ単位で明示的に指定します。

## 相互運用性

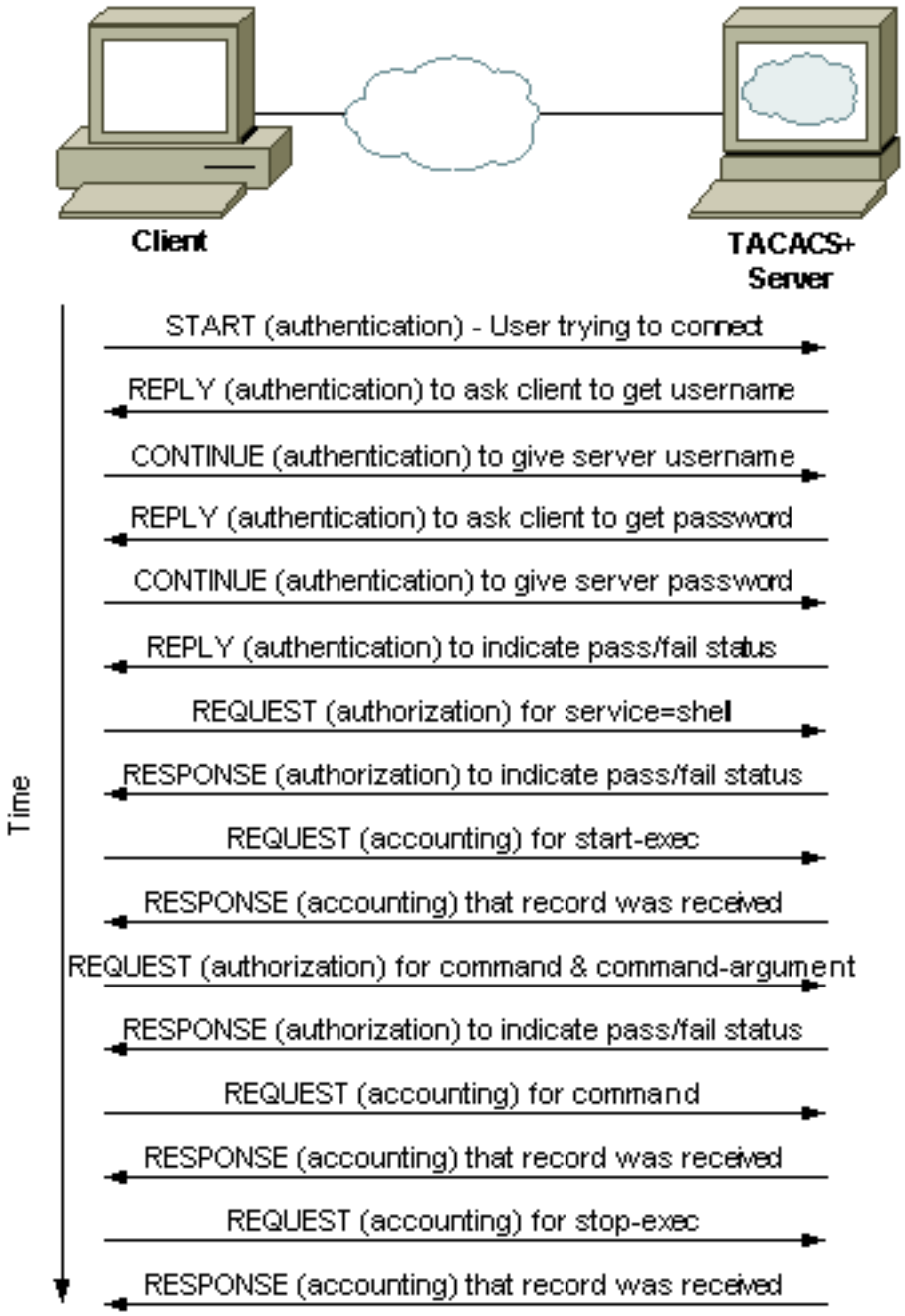
RADIUS Request for Comment（RFC; コメント要求）にはさまざまな解釈があるため、RADIUS RFC への準拠性によって相互運用性は保証されません。 複数のベンダーが RADIUS クライアントを実装していますが、これは相互運用性を意味するものではありません。 Cisco では、ほとんどの RADIUS アトリビュートを実装し、常時追加しています。 お客様が標準の RADIUS アトリビュートだけをサーバで使用する場合、複数のベンダーが同じアトリビュートを実装している限り、それらのベンダー間で相互運用が可能です。 ただし、多くのベンダーは、独自のアトリビュートである拡張機能を実装しています。 お客様がベンダー固有の拡張アトリビュートを使用している場合、相互運用は可能ではありません。

## トラフィック

前述の TACACS+ と RADIUS の違いにより、クライアントとサーバとでは生成されるトラフィックの量が異なります。 次の例では、認証、exec 認可、コマンド認可（RADIUS では不可）、exec アカウンティング、およびコマンド アカウンティング（RADIUS では不可）によるルータ管理に使用する場合の、TACACS+ および RADIUS でのクライアントとサーバ間のトラフィックを示しています。

## TACACS+ トラフィックの例

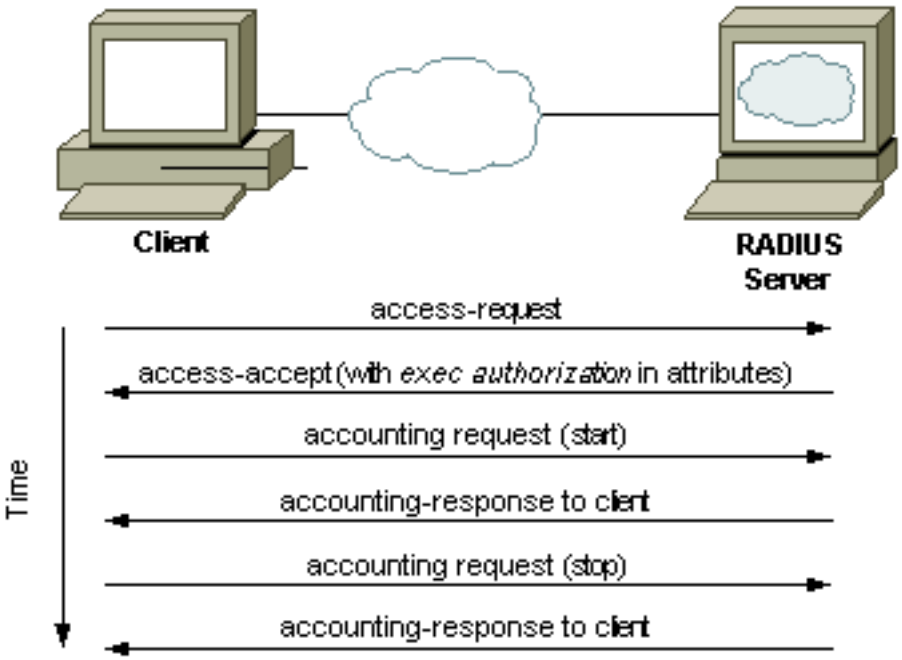
この例では、ユーザがルータに Telnet 接続し、コマンドを実行し、ルータを終了する場合に、TACACS+ を使用してログイン認証、exec 認可、コマンド認可、開始/停止 exec アカウンティング、およびコマンド アカウンティングが実装されていることを想定しています。




## RADIUS トラフィックの例

この例では、ユーザがルータに Telnet 接続し、コマンドを実行し、ルータを終了する場合に（他の管理サービスは利用できません）、RADIUS を使用してログイン認証、exec 許可、および開始

/停止 exec アカウンティングが実装されていることを想定しています。




## デバイス サポート

次の表に、TACACS+ および RADIUS での AAA サポートを、選択されたプラットフォームのデバイス タイプごとに示します。 また、サポートが追加されたソフトウェア バージョンも示します。 お使いの製品がこのリストにない場合は、製品リリース ノートを参照してください。

| Cisco デバイス | TACACS+ 認証 | TACACS+ 認可 | TACACS+ アカウンティング | RADIUS 認証 | RADIUS 許可 | RADIUS アカウンティング |
|---|---|---|---|---|---|---|
| Cisco Aironet1 | 12.2(4)JA | 12.2(4)JA | 12.2(4)JA | すべてのアクセス ポイント | すべてのアクセス ポイント | すべてのアクセス ポイント |
| Cisco IOS ソフトウェア2 | 10.33 | 10.33 | 10.33[3] | 11.1.1 | 11.1.1[4] | 11.1.1[5] |
| Cisco キャッシュ エンジン | -- | -- | -- | 1.5 | 1.5[6] | -- |
| Cisco Catalyst スイッ | 2.2 | 5.4.1 | 5.4.1 | 5.1 | 5.4.1[4] | 5.4.1[5] |

| | | | | | | |
|---|---|---|---|---|---|---|
| チ | | | | | | |
| Cisco CSS 11000 コンテント サービス スイッチ | 5.03 | 5.03 | 5.03 | 5.0 | 5.0[4] | -- |
| Cisco CSS 11500 コンテント サービス スイッチ | 5.20 | 5.20 | 5.20 | 5.20 | 5.20[4] | -- |
| Cisco PIX ファイアウォール | 4.0 | 4.0[7] | 4.2[8,5] | 4.0 | 5.2[7] | 4.2[8,5] |
| Cisco Catalyst 1900/2820 スイッチ | 8.x enterprise 9 | -- | -- | -- | -- | -- |
| Cisco Catalyst 2900XL/3500XL スイッチ | 11.2.(8)SA6[10] | 11.2.(8)SA6[10] | 11.2.(8)SA6[10] | 12.0(5)WC5[11] | 12.0(5)WC5[11、4] | 12.0(5)WC5[11、5] |
| Cisco VPN 3000 コンセントレータ6 | 3.0 | 3.0 | -- | 2.0[12] | 2.0 | 2.0[12] |
| Cisco VPN | -- | -- | -- | 5.2X12 | 5.2X12 | 5.2X12 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 5000 コンセントレータ | | | | | | |

### 表の注意事項

1. Cisco IOS ソフトウェア リリース 12.2(4)JA より前のバージョンでは、無線クライアントの終端だけであり、管理トラフィックは含まれません。 Cisco IOS ソフトウェア リリース 12.2.(4)JA 以降では、無線クライアントと管理トラフィックの両方の終端で認証が可能になりました。
2. Cisco IOS ソフトウェア内でのプラットフォーム サポートについては、Feature Navigator（現在では Software Advisor（登録ユーザ専用）に置き換わっています）をチェックしてください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことを、ご了承ください。
3. コマンド アカウンティングは、Cisco IOS ソフトウェア リリース 11.1.6.3 より前のバージョンでは実装されていません。
4. コマンド認可は行えません。
5. コマンド アカウンティングは行えません。
6. URL ブロッキングだけであり、管理トラフィックは含まれません。
7. PIX 経由の非 VPN トラフィックに対する認可です。**注:** リリース 5.2：PIX で終端する VPN トラフィックに対する Access Control List（ACL; アクセス コントロール リスト）RADIUS Vendor-Specific Attribute（VSA; ベンダー固有属性）または TACACS+ 認可のアクセスリスト サポート。リリース 6.1：PIX で終端する VPN トラフィックに対する ACL RADIUS アトリビュート 11 認可のサポート。リリース 6.2.2：PIX で終端する VPN トラフィックに対する RADIUS 認可でダウンロード可能な ACL のサポート。リリース 6.2：TACACS+ 経由の PIX 管理トラフィックに対する認可のサポート。
8. PIX 経由の非 VPN トラフィックだけのアカウンティングです。管理トラフィックは含まれません。**注:** リリース 5.2：PIX 経由の VPN クライアント TCP パケットに対するアカウンティングのサポート。
9. エンタープライズ ソフトウェアだけです。
10. イメージ用に 8M のフラッシュが必要です。
11. VPN の終端だけです。

## 関連情報

- RADIUS に関するサポート ページ
- IOS での TACACS+ に関するドキュメント
- TACACS/TACACS+ に関するサポートページ
- Requests for Comments（RFC）
- テクニカルサポートとドキュメント - Cisco Systems