RADIUS はどのように動作しますか。

目次

概要

Remote Authentication Dial-In User Service (RADIUS) プロトコルは、アクセス サーバ認証およびアカウンティング プロトコルとして、Livingston Enterprises, Inc. によって開発されました。 RADIUS 仕様である RFC 2865 は、RFC 2138 に代わり、 RADIUS アカウンティング規格である RFC 2866 は、RFC 2139 に代わりました。

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。

背景説明

Network Access Server (NAS; ネットワーク アクセス サーバ) と RADIUS サーバ間の通信は、User Datagram Protocol (UDP; ユーザ データグラム プロトコル) に基づいています。 一般に、RADIUS プロトコルはコネクションレス型サービスと見なされています。 サーバのアベイラビリティ、再送信、タイムアウトに関連する問題は、伝送プロトコルではなく、RADIUS 対応デバイ

スによって処理されます。

RADIUS は、クライアント/サーバ プロトコルです。 通常、RADIUS クライアントは NAS で、RADIUS サーバは UNIX または Windows NT コンピュータで実行されるデーモン プロセスです。クライアントは、指定された RADIUS サーバにユーザ情報を送信し、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設定情報を返します。 RADIUS サーバは、その他の RADIUS サーバまた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。

この図は、ダイヤルイン ユーザと RADIUS クライアントおよびサーバ間の相互対話を示しています。

1. ユーザは NAS に PPP 認証を開始します。
2. NAS は、Password Authentication Protocol（PAP; パスワード認証プロトコル）の場合はユーザ名とパスワードを要求し、Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）の場合は、チャレンジを要求します。
3. ユーザが応答します。
4. RADIUS クライアントは、ユーザ名と暗号化されたパスワードを RADIUS サーバに送信します。
5. RADIUS サーバは、Accept、Reject、または Challenge で応答します。
6. RADIUS クライアントは、Accept または Reject にバンドルされたサービスまたはサービス パラメータに基づいて対応します。

認証および許可

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、PAP または 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。

通常、ユーザ ログインは、NAS から RADIUS サーバへのクエリー（Access-Request）と、サーバからの対応する応答（Access-Accept または Access-Reject）で構成されます。 Access-Request パケットには、ユーザ名、暗号化されたパスワード、NAS IP アドレス、ポートが含まれます。 初期の RADIUS 展開に使用されていた UDP ポート番号 1645 は、「datametrics」サービスと競合します。 この競合のため、RFC 2865 によって RADIUS にはポート番号 1812 が正式に割り当てられました。 ほとんどのシスコ デバイスおよびアプリケーションではいずれかのポート番号セットを使用できます。 要求の形式は、ユーザが開始するセッションのタイプに関する情報も提供します。 たとえば、クエリーが文字モードで表現される場合、「Service-Type = Exec-User」と推論されますが、要求が PPP パケット モードで表現される場合は「Service Type = Framed User」および「Framed Type = PPP」と推論されます。

RADIUS サーバは、NAS から Access-Request を受信したときに、リストにあるユーザ名をデータベースで検索します。 ユーザ名がデータベースに存在しない場合は、デフォルトのプロファイルがロードされるか、RADIUS サーバはただちに Access-Reject メッセージを送信します。 Access-Reject メッセージには、拒否の理由を示すテキスト メッセージが添付されることがあります。

RADIUS では、認証と許可は一組です。 ユーザ名が見つかり、パスワードが正しい場合、RADIUS サーバは Access-Accept 応答を返します。これには、このセッションで使用するパラメータを記述した属性 - 値ペアのリストが含まれます。 一般的なパラメータには、サービスの種類（shell または framed）、プロトコルの種類、ユーザに割り当てる（スタティックまたはダイナ

ミック) IP アドレス、適用するアクセス リスト、NAS ルーティング テーブルにインストールするためのスタティック ルートなどがあります。 RADIUS サーバの設定情報は、NAS でインストールする項目を定義します。 次の図は、RADIUS 認証および許可シーケンスを示しています。

アカウンティング

RADIUS プロトコルのアカウンティング機能は、RADIUS 認証または許可からは独立して使用できます。 RADIUS アカウンティング機能を使用すると、セッションの開始時と終了時に、セッション中に使用されたリソースの量 (時間、パケット、バイトなど) を示すデータを送信できます。 Internet Service Provider (ISP; 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 ソフトウェアを使用して、特別なセキュリティおよび課金に関するニーズを満たします。 ほとんどの Ciscoデバイスの RADIUS のためのアカウンティングポートは 1646 です、しかしまた 1813 である場合もあります (RFC 2139 で指定どおりのポートの変更が理由で) 。

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、クライアントと RADIUS サーバ間で暗号化されたユーザ パスワードを送信して、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を解消します。

関連情報

- RADIUS テクノロジーに関するサポート ページ
- Requests for Comments (RFC)
- テクニカルサポート - Cisco Systems