ONS 15454 バージョン 6.0 での RADIUS 認証の問題

内容

概要

このドキュメントでは、Cisco ONS 15454 環境の ONS 15454 バージョン 6.0 における Remote Authentication Dial-In User Service（RADIUS）サーバ認証に関する既知の問題について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco ONS 15454
- RADIUS サーバ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ONS 15454 バージョン 6.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

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

RADIUSは、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ています。

- ユーザデータグラムプロトコル(UDP)/IPを使用するフレーム形式のプロトコル
- サーバ
- クライアント

ONS 15454ノードは、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、応答に対して動作します。RADIUSサーバは、ユーザ接続要求を受信し、ユーザを認証し、クライアントがユーザにサービスを提供するために必要なすべての設定情報を返します。

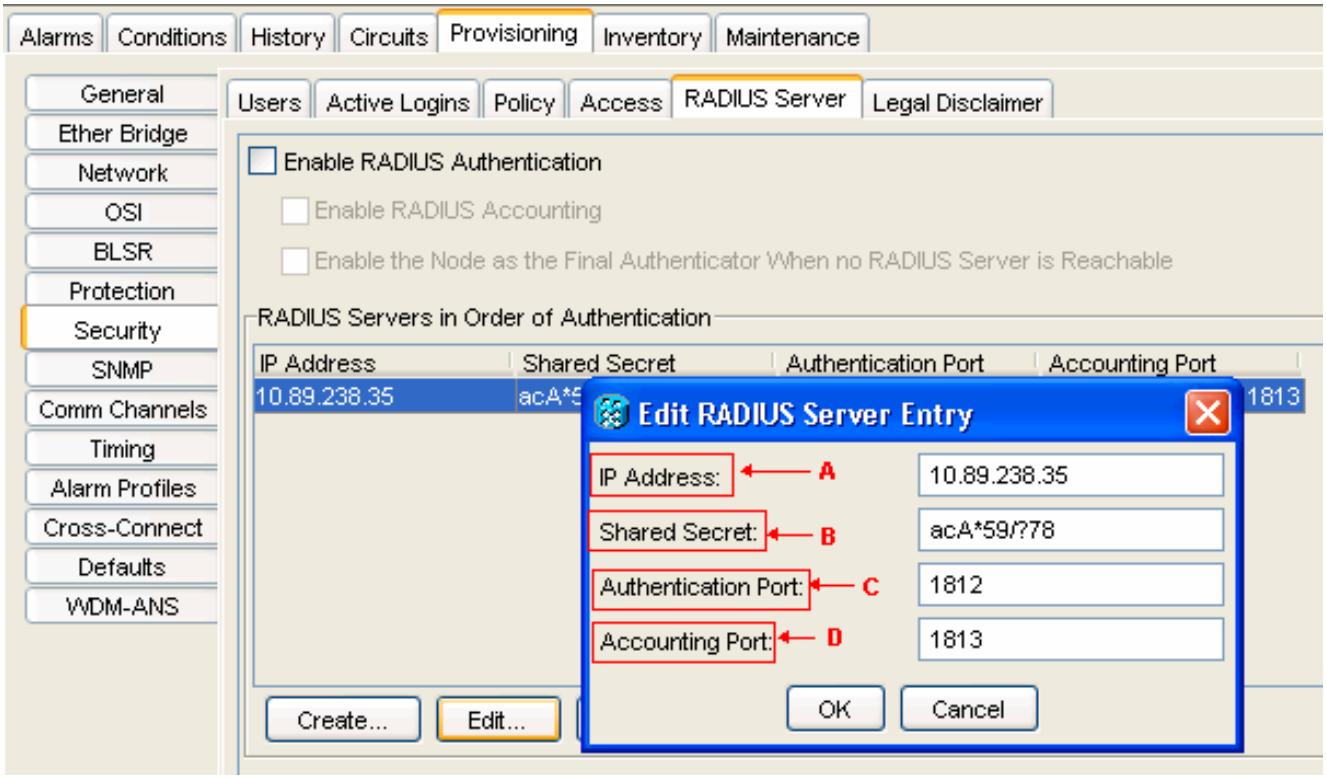
共有秘密は、RADIUSクライアントとサーバ間のトランザクションを認証します。共有秘密はネットワーク経由で送信されません。さらに、クライアントとRADIUSサーバの間でユーザパスワードが交換されると暗号化されます。暗号化プロセスは、ユーザのパスワードを決定するために、セキュリティで保護されていないネットワークを監視する人の可能性を排除します。

共有秘密

共有秘密は、ONS15454 RADIUSクライアントとRADIUSサーバ間のパスワードとして機能するテキスト文字列です。共有秘密を作成するには、次の手順を実行します。

1. Cisco Transport Controller（CTC）にログインします。
2. [Network]ビューに移動します。
3. 特定のONS 15454を選択して、[Shelf]ビューに移動します。
4. **[Provisioning] > [Security] > [RADIUS Server]をクリックします。**
5. [IP Address]フィールドにRADIUSサーバのIPアドレスを入力します(図1の矢印Aを参照してください)。
6. [Shared Secret]フィールドに共有秘密を入力します。共有秘密は、RADIUSクライアントとRADIUSサーバ間のパスワードとして機能するテキスト文字列です(図1の矢印Bを参照してください)。
7. [Authentication Port]フィールドにRADIUS認証ポート番号を入力します(図1の矢印Cを参照してください)。デフォルトの認証ポート番号は1812です。ノードがENEの場合、認証ポートを1860および1869の範囲内の番号に設定します。
8. [Accounting Port]フィールドにRADIUSアカウンティングポート番号を入力します(図1の矢印Dを参照してください)。デフォルトのアカウンティングポート番号は1813です。ノードがENEの場合、アカウンティングポートを1870および1879の範囲内の番号に設定します。

図1 – セキュリティ：RADIUS サーバ



共有秘密を使用して、同じ共有秘密を設定したRADIUS対応デバイスが、Access-Requestメッセージ以外のすべてのRADIUSメッセージを送信することを確認します。

共有秘密は、RADIUSメッセージが転送中に変更されないことを確認します。つまり、共有秘密はメッセージの整合性を維持します。共有秘密は、User-PasswordやTunnel-Passwordなどの一部のRADIUS属性も暗号化します。

ONS 15454バージョン6.0では、共有秘密の長さが16文字に制限されています。ただし、ONS 15454バージョン6.2以降では、最大長を128文字に増やす予定です。詳細は、Cisco Bug ID CSCsc16614(登録ユーザ専用)を参照してください。

共有秘密の文字グループは次をサポートします。

- 文字（大文字と小文字）。たとえば、A、B、a、b。
- 数字（1、2、3など）。
- 記号。文字や数字として定義されていないすべての文字を表します。たとえば、>、(、*)。

ユーザセキュリティグループマッピング

属性値(AV)ペアは、変数と、その変数が保持できる値の1つを表します。ONS 15454では、ユーザはCisco AVペアに基づいて異なるセキュリティグループにマッピングされます。以下が一例です。

"shell:priv-lvl=X"。ここで、Xは0 ~ 3の値にすることができます。

- 0はRTRVを表します。
- 1はPROVを表します。
- 2はMAINTを表します。
- 3はSUPERを表します。

Password

RADIUSサーバとクライアントは、パスワードに使用する文字を制限しません。ただし、CTCには制限があります。ONS 15454バージョン6.0では、CTCがサポートする文字は次のとおりです。

- 文字（大文字と小文字）。たとえば、A、B、a、b。
- 数字（1、2、3など）。
- #、%、および+の特殊文字のみ。

シスコでは、ONS 15454の新しいバージョンの特別なシンボルの制限を撤廃する予定です。詳細については、Cisco Bug ID CSCsc16604（登録ユーザ専用）を参照してください。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems