

ONS 15454 バージョン 6.0 での RADIUS 認証の問題

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[共有秘密](#)

[ユーザー セキュリティ グループ マッピング すること](#)

[Password](#)

[関連情報](#)

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くものです。

- 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たものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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 は不正アクセスに対してネットワークおよびネットワークサービスにリモートアクセスを確保する分散セキュリティのシステムです。RADIUS はこの 3 つのコンポーネントから成り立ちます:





- 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、次に応答で行動します。RADIUSサーバ レシーブ ユーザ接続 要求は、クライアントがユーザにサービスを提供することができるのによりユーザを認証し、必要なすべての構成情報を返します。

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に決して送信されません。さらにクライアントと RADIUSサーバの間で交換されたとき、どのユーザパスワードでも暗号化されます。暗号化 プロセスはユーザのパスワードを判別するために保護されていない ネットワークを監視する誰かの可能性を軽減します。

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動作する文字列です。共有秘密を作成するためにこれらのステップを完了して下さい:

1. Cisco Transport Controller (CTC) にログインします。
2. Network ビューに行ってください。
3. Shelf ビューに行くために特定の ONS 15454 を選択して下さい。
4. Provisioning > Security > RADIUS Server の順にクリックして下さい。
5. IP Address フィールドの RADIUSサーバの IP アドレスをタイプして下さい ( の矢印 A を [1](#)) 参照して下さい。
6. 共有秘密 フィールドの共有秘密を入力して下さい。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サブ文字列です ( の矢印 B を [1](#)) 参照して下さい。
7. 認証 ポート フィールドの RADIUS認証 ポート番号をタイプして下さい ( の矢印 C を [1](#)) 参照して下さい。デフォルトの認証 ポート番号は 1812 です。ノードが ENE である場合、1860 および 1869 の範囲内の数に認証 ポートを設定して下さい。
8. アカウンティングポート フィールドの RADIUS アカウンティングポート番号をタイプして下さい ( の矢印 D を [1](#)) 参照して下さい。デフォルト アカウンティングポート数は 1813 です。ノードが ENE である場合、1870 および 1879 の範囲内の数にアカウンティングポートを設定して下さい。 **図 1-セキュリティ: RADIUS サーバ**

同じ共有秘密で設定した RADIUS 対応 デバイスが Access-Request メッセージを除くすべての RADIUS メッセージを送信 するようにするのに共有シークレットを使用して下さい。

共有シークレットは RADIUS メッセージが送信中に修正されて得ないことを確かめます。すなわち、共有シークレットはメッセージ整合性を維持します。共有シークレットはまたいくつかの

RADIUS特性、たとえば、ユーザパスワードおよびトンネルパスワードを暗号化します。

ONS 15454 バージョン 6.0 は 16 文字に共有秘密の長さを制限します。ただし、前の ONS 15454 バージョン 6.2 から、Cisco は 128 文字に最大長を増加することを計画しています。詳細については Cisco バグ ID [CSCsc16614](#) ([登録ユーザのみ](#)) を参照して下さい。

共有秘密 文字 グループ サポート:

- 文字 (大文字および小文字)、たとえば、A、B、a および b。
- 数字、たとえば、1、2 および 3。
- 文字か数字と定義されないすべての文字を表すシンボル、たとえば、>、(、および*。

ユーザー セキュリティ グループ マッピング すること

attribute-value (AV) ペアは保持変数ができる有効値の変数および 1 表します。ONS 15454 の中では、ユーザは異なるセキュリティグループによって基づく AVペアに on Cisco マッピング されます。次に例を示します。

「シェル: X が 0 から 3 という値である場合もあるところ priv-lvl=X」:

- 0 は RTRV を表します。
- 1 つは PROV を表します。
- 2 つは MAINT を表します。
- 3 つは極度を表します。

Password

RADIUSサーバおよびクライアントはパスワードのために使用する文字を制限しません。ただし、CTC に制限があります。ONS 15454 バージョン 6.0 に関しては、CTC がサポートする文字はここにあります:

- 文字 (大文字および小文字)、たとえば、A、B、a および b。
- 数字、たとえば、1、2 および 3。
- ただ#、%、および + 特別なシンボル。

ONS 15454 の以降のバージョンの特別なシンボルの制限を取除く Cisco 計画。詳細については Cisco バグ ID [CSCsc16604](#) ([登録ユーザのみ](#)) を参照して下さい。

関連情報

- [テクニカルサポートとドキュメント - Cisco Systems](#)