管理アカウントの TACACS+ 認証をサポートするための Cisco VPN 3000 コンセントレータの設定方法

目次

概要

このドキュメントでは、管理アカウントの TACACS+ 認証をサポートするための Cisco VPN 3000 シリーズ コンセントレータの設定方法を手順を追って説明します。

TACACS+ サーバが VPN 3000 コンセントレータで、ローカルで設定されたアカウント名設定され、admin のようなパスワードが、構成、ISP、等、もはや使用されないとすぐ。 VPN 3000 コンセントレータへのすべてのログオンはユーザおよびパスワード 確認のための設定された外部 TACACS+ サーバに送られます。

TACACS+ サーバの各ユーザ向けの特権レベルの定義は各 TACACS+ ユーザ名のための VPN 3000 コンセントレータの権限を判別します。 それから、AAA アクセスレベルとのの上で VPN 3000 コンセントレータのローカルで設定されたユーザ名の下で定義した一致。 これは TACACS+ サーバが定義されるとすぐ、VPN 3000 コンセントレータのローカルで設定されたユーザ名がもはや有効ではないので重要な点です。 そのローカルユーザの下で AAA アクセスレベルと TACACS+ サーバからの戻された特権レベルを、調和させるためにただしかし、それらはまだ使用されます。 ローカルで設定された VPN 3000 コンセントレータ ユーザがプロファイルの下で定義したこと TACACS+ ユーザ名それから特権は割り当てられます。

たとえば、コンフィギュレーションセクションで詳しく記述されていて、TACACS+ ユーザ/グル

ープは 15 の TACACS+ 特権レベルを返品するために設定されます。 VPN 3000 コンセントレータの管理者 セクションの下で、管理者ユーザはまた AAA アクセスレベルを 15 に設定 してもらいます。 このユーザはすべてのセクションの下で、および読み書きファイルに設定を修正することができます。 TACACS+ 特権レベルおよび AAA アクセスレベルが一致、TACACS+ ユーザ VPN 3000 コンセントレータのそれらの権限を与えられるので。

一例として決定すれば設定を修正できることをユーザーのニーズが読み書きファイルは、それらに TACACS+ サーバの 12 の特権レベルをことを指定します。 1 つと 15 間の数を選ぶことができます。 それから、VPN 3000 コンセントレータで、他のローカルで設定された管理者の 1 人を選んで下さい。 次に、AAA アクセスレベルを 12 に設定 し、設定を修正ことできるためにこのユーザのない読み書きファイルへの権限を設定 して下さい。 一致する特権/アクセスレベルが理由で、ユーザは彼らがログインするときそれらの権限を得ます。

VPN 3000 コンセントレータのローカルで設定されたユーザ名はもはや使用されません。 特定の TACACS+ ユーザが得る特権を定義するためにそれらのユーザのそれぞれはの下のしかし、アクセス 権およびログインするとき AAA アクセスレベル使用されます。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- VPN 3000 コンセントレータからの TACACS+ サーバに IP接続があることを確認して下さい。 TACACS+ サーバがパブリックインターフェイスの方にある場合、TACACS+（パブリックフィルタの 49）TCPポートを開くことを忘れないで下さい。
- コンソールによってバックアップ アクセスを正常に動作しています確認して下さい。 最初にこれをセットしたとき偶然設定からすべてのユーザをロックすることは容易です。 アクセスを回復 するまだローカルで設定されたユーザ名 および パスワードを使用する唯一の方法はコンソールによってあります。

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 VPN 3000 コンセントレータ ソフトウェア リリース 4.7.2.B（代わりに、あらゆるリリース 3.0 またはそれ以降の OS ソフトウェア作業。）
- Cisco Secure Access Control Server for Windows サーバ リリース 4.0（又、あらゆるリリース 2.4 またはそれ以降のソフトウェア作業。）

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。

TACACS+ サーバを設定して下さい

TACACS+ サーバの VPN 3000 コンセントレータのためのエントリを追加して下さい

TACACS+ サーバの VPN 3000 コンセントレータのためのエントリを追加するためにこれらのステップを完了して下さい。

1. 左パネルで『Network Configuration』 をクリック して下さい。 AAA Clients の下で **[Add Entry]** をクリックします。
2. Next ウィンドウで、TACACS+ クライアントとして VPN コンセントレータを追加するために書式に記入して下さい。 この例では次の設定を使用しています。AAA クライアント ホスト名 = **VPN3000**AAA クライアントIPアドレス = **10.1.1.2**キー = **csacs123**認証するを使用して = **TACACS+ （ Cisco IOS ）** [Submit + Restart] をクリックします。

TACACS+ サーバのユーザアカウントを追加して下さい

TACACS+ サーバのユーザアカウントを追加するためにこれらのステップを完了して下さい。

1. TACACS+ 認証のために使用される以降である場合もある TACACS+ サーバのユーザアカウントを作成して下さい。 左パネルで『User Setup』 をクリック し、ユーザ「johnsmith」を追加し、これをするために『Add/Edit』 をクリック して下さい。
2. このユーザ向けのパスワードを追加し、ACS グループに他の VPN 3000 コンセントレータ管理者が含まれているユーザを割り当てて下さい。**注:** この例はこの特定のユーザ ACS グループ プロファイルの下で特権レベルを定義したものです。 これがユーザごとにされるために行われたら Shell （ exec ）サービスがあるように**ユーザ** ボックスを Interface Configuration > TACACS+ （ Cisco IOS ） の順に選択 し、確認して下さい。 この資料 利用可能 な下に説明がある TACACS+ オプションは各ユーザ プロファイルそれからありますただ。

TACACS+ サーバのグループを編集して下さい

TACACS+ サーバのグループを編集するためにこれらのステップを完了して下さい。

1. 左パネルで『Group Setup』 をクリック して下さい。
2. ドロップダウン メニューから、グループをユーザが追加ににこの例のグループ 1 選択しである、『Edit Settings』 をクリック して下さい追加された TACACS+ サーバセクションのユーザアカウント。
3. Next ウィンドウで、これらの属性が TACACS+ 設定の下で選択されることを確かめて下さい:**Shell （ exec ） Privilege level=15**終了したら、『Submit + Restart』 をクリック して下さい。

VPN 3000 コンセントレータの設定

VPN 3000 コンセントレータの TACACS+ サーバのためのエントリを追加して下さい

VPN 3000 コンセントレータの TACACS+ サーバのためのエントリを追加するためにこれらのステップを完了して下さい。

1. 左パネルのナビゲーション ツリーで Administration > Access Rights > AAA Servers > Authentication の順に選択 し、次に右 の パネルで『Add』 をクリック して下さい。このサーバを追加するために『Add』 をクリック するとすぐ VPN 3000 コンセントレータのローカルで設定された username/password はもはや使用されません。 ロックアウトの場合にはコンソール作業によってバックアップ アクセスを確認して下さい。
2. Next ウィンドウで、ここに見られるように書式に記入して下さい:認証サーバ = **10.1.1.1**（TACACS+ サーバの IP アドレス）サーバポート = **0**（デフォルト）タイムアウト = **4**再試行 = **2**サーバシークレット = **csacs123**= **csacs123** 確認して下さい

TACACS+ 認証のための VPN コンセントレータの管理者アカウントを修正して下さい

TACACS+ 認証のための VPN コンセントレータの管理者アカウントを修正するためにこれらのステップを完了して下さい。

1. このユーザのプロパティを修正するためにユーザ admin のために『Modify』 をクリック して下さい。
2. **15** として AAA アクセスレベルを選択して下さい。この値は 1 つと 15 間のどの数である場合もあります。 それが TACACS+ サーバのユーザ/グループ プロファイルの下で定義される TACACS+ 特権レベルを一致する必要があることに注目して下さい。 TACACS+ ユーザはそれから設定の修正のためのこの VPN 3000 コンセントレータ ユーザの下で、読む/書き込みファイル定義される、権限を等取ります。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

設定をトラブルシューティングするためにこれらの手順のステップを完了して下さい。

1. 認証をテストするため:TACACS+ サーバに関してはAdministration > Access Rights > AAA Servers > Authentication の順に選択 して下さい。[サーバ]を選択してから **[Test]** をクリックします。**注:** TACACS+ サーバが管理 タブで設定されるとき、VPN 3000 ローカルデータベースで認証するためにユーザを設定する方法がありません。 別の外部 データベースか TACACSサーバを使用してフォールバックだけできます。TACACS+ ユーザ名 および パスワードを入力し、『OK』 をクリック して下さい。認証が成功したことを示すメッセージが表示されます。
2. 認証が失敗した場合は、設定に問題があるか、IP 接続に問題があります。 ACS サーバの Failed Attempts Log で、この失敗に関連するメッセージがないか確認します。このログにメッセージが表示されない場合は、IP 接続に問題があると考えられます。 TACACS+ 要求は TACACS+ サーバに達しません。 適切な VPN 3000 コンセントレータ インターフェイス割り当て TACACS+（および 49）TCPポート パケットに加えられるフィルターを確認して下さい。サービスとして失敗ディスプレイがログで否定した場合、Shell（exec）サービスは

TACACS+ サーバのユーザかグループ プロファイルの下で正しく有効に なりません でした。

3. テスト認証が成功しても VPN 3000 コンセントレータへのログインが引き続き失敗する場合は、コンソール ポート経由で Filterable Event Log を確認してください。同じようなメッセージが表示されれば:
   65 02/09/2005 13:14:40.150 SEV=5 AUTH/32 RPT=2 User [johnsmith] Protocol [HTTP] attempted ADMIN logon. Status: <REFUSED> authorization failure. NO Admin Rights このメッセージは TACACS+ サーバで指定される特権レベルに VPN 3000 コンセントレータ ユーザの何れかの下で一致する AAA アクセスレベルがないことを示します。 たとえば、ユーザ johnsmith に TACACS+ サーバの 7 の TACACS+ 特権レベルがありますが、5 人の VPN 3000 コンセントレータ 管理者のどれも 7.の AAA アクセスレベルがありません。

関連情報

- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- Cisco VPN 3000 シリーズ クライアントに関するサポート ページ
- IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ
- TACACS/TACACS+ 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
- テクニカルサポートとドキュメント - Cisco Systems