CSU for UNIX（Solaris）の設定

目次

概要

Cisco Secure ACS for UNIX（CSU）ソフトウェアは、ネットワークのセキュリティの確保、およびネットワークに正常に接続しているユーザのアクティビティを追跡するのに役立ちます。 CSU は TACACS+ または RADIUS サーバとして機能し、認証、許可、およびアカウンティング（AAA）を使用してネットワークのセキュリティを提供します。

CSU はグループおよびユーザ プロファイルおよびアカウンティング 情報保存するこれらのデータベース オプションをサポートします:

- SQLAnywhere（CSU と含まれている）。Sybase SQLAnywhere のこのバージョンにクライアント/サーバ サポートがありません。 ただし CSU と必要な AAA サービスを行うことを、最適化します。**注意：** SQLAnywhereデータベース オプションはデータベース サイト間のプロファイル情報の 5,000 人のユーザ、複製、または Cisco Secure Distribute Session Manager（DSM）機能を超過するプロファイル データベースをサポートしません。
- Oracle か Sybase Relational Database Management System（RDBMS）。5,000 人またはより多くのユーザの Cisco Secure プロファイル データベースを、データベース複製、または Cisco Secure DSM 機能サポートするため、RDBMS Oracle（バージョン 7.3.2、7.3.3、または 8.0.3）または Cisco Secure プロファイル情報を保持する Sybase SQL サーバ（バージョン 11）をプレインストールして下さい。 データベース複製は Cisco Secure インストールが

完了する後それ以上の RDBMS 設定を必要とします。
- CSU の前の（2.x）バージョンからの既存のデータベースのアップグレード。Cisco Secure の以前の 2.x バージョンからアップグレードする場合、Cisco Secure インストール プログラムは UNIX 用の CSU 2.3 と互換性があるために自動的にプロファイル データベースをアップグレードします。
- 既存のプロファイル データベースのインポート。既存のフリーウェア TACACS+ か CSU のこのバージョンと併用するための RADIUSプロファイル データベースまたはフラットファイル変換できます。

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

この文書に記載されている情報は UNIX 用の Cisco Secure ACS 2.3 に基づいています。

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。

CSU設定

CSU を設定するのにこれらの手順を使用して下さい。

Cisco Secure Administrator Interface を開始して下さい

Cisco Secure 管理者にログインにこのプロシージャを使用して下さい。

1. ウェブ接続のあらゆるワークステーションから ACS への、Webブラウザを起動させて下さい。
2. Cisco Secure 管理者 Webサイトのためのこれらの URL の 1 つを入力して下さい:ブラウザの Security Socket Layer 機能が有効に ならない場合、入力して下さい :`http://your_server/cs`your_server が CSU をインストールした SPARCstation のホスト名 ホスト名および FQDN が異なる場合、（または完全修飾ドメイン名 （FQDN））であるところ。 また your_server の SPARCstation の IP アドレスを代わりにすることができます。ブラウザの Security Socket Layer 機能が有効に なる場合、ハイパーテキスト 伝送プロトコルとして「http」よりもむしろ「https」を規定 して下さい。 次のように入力します。 `https://your_server/cs`your_server が CSU をインストールした SPARCstation のホスト名 ホスト名および FQDN が異なる場合、（または FQDN）であるところ。 また your_server

の SPARCstation の IP アドレスを代わりにすることができます。**注:** URL およびサーバ名は大文字/小文字の区別があります。 それらは示されているように大文字および小文字と丁度入力する必要があります。CSU ログオン ページは表示する。
3. ユーザ名とパスワードを入力します。 [Submit] をクリックします。**注:** 最初のデフォルトのユーザ名はです「スーパーユーザ」。 最初のデフォルトパスワードはです「changeme」。最初のログインの後で、最大のセキュリティのためにユーザ名 および パスワードをすぐに変更する必要があります。上に沿うメインメニュー メニュー· バーとログイン、CSU メイン ページ 表示する後。 CSU メインメニューページはユーザが管理者レベル特権があるパスワードおよび名前を提供するときだけ表示する。 ユーザがユーザー レベル特権だけあるパスワードおよび名前を提供すれば、別の画面は表示する。

拡張設定プログラムを開始して下さい

CSU 管理者 Webページの何れかからの Javaベース Cisco Secure 管理者 拡張設定プログラムを開始して下さい。 CSU Webインターフェイスのメニューバーから、『Advanced』 をクリックし、次に再度『Advanced』 をクリック して下さい。

Cisco Secure 管理者 拡張設定プログラムは表示する。 ロードするために可能性のある数分かかるかもしれません。

グループ プロファイルを作成して下さい

グループ プロファイルを作成し、設定するのに Cisco Secure 管理者 拡張設定プログラムを使用して下さい。 Cisco は多数の同じようなユーザ向けの詳しい AAA 必要条件を設定するためにグループ プロファイルを作成することを推奨します。 グループ プロファイルが定義された後、すぐにグループ プロファイルにユーザ プロファイルを追加するのに CSU Add a User web ページを使用して下さい。 グループのために設定される高度 の 要件は各メンバーにユーザを加えます。

グループ プロファイルを作成するのにこのプロシージャを使用して下さい。

1. Cisco Secure 管理者 拡張設定プログラムで、**Members タブを**選択して下さい。 操縦士ペインでは、**Browse チェックボックスを**選択解除して下さい。 Create New Profile アイコン ディスプレイ。
2. ナビゲーター ペインでは、これらの 1 つをして下さい:グループ プロファイルを親無しで作成するために、[**ルート**]フォルダ の アイコンを見つけ、クリックして下さい。グループ プロファイルを別のグループ プロファイルの子として作成するために、親としてほしいと思い、それをクリックするグループを見つけて下さい。親でほしいグループが子グループである場合、それを表示するために親 グループのフォルダをクリックして下さい。
3. 『Create New Profile』 をクリック して下さい。 New Profile ダイアログボックス ディスプレイ。
4. **Group チェックボックスを**選択し、作成したいと思うグループの名前をタイプし『OK』 をクリック して下さい。 ツリーの新しいグループ ディスプレイ。
5. グループ プロファイルを作成した後、特定の AAA プロパティを設定するために TACACS+ か RADIUS特性を割り当てて下さい。

拡張設定 モードのユーザ プロファイルを作成して下さい

ユーザ プロファイルを作成し、設定するのに Cisco Secure Administrator 拡張 設定 モードを使用

して下さい。 ユーザページが追加と可能性のあるであるよりユーザ プロファイルの許可およびアカウンティング関連の属性をより詳しくカスタマイズするためにこれをすることができます。

ユーザ プロファイルを作成するのにこのプロシージャを使用して下さい:

1. Cisco Secure 管理者 拡張設定プログラムで、**Members タブを**選択して下さい。 ナビゲーター ペインでは、**参照します**置き、選択解除して下さい。 Create New Profile アイコン ディスプレイ。
2. ナビゲーター ペインでは、これらの 1 つをして下さい:ユーザが属するグループを見つけ、クリックして下さい。ユーザにグループに属してほしくない場合[**ルート**]フォルダ の アイコンをクリックして下さい。
3. 『Create Profile』 をクリック して下さい。 New Profile ダイアログボックス ディスプレイ。
4. **Group チェックボックスが**選択解除されることを確かめて下さい。
5. 作成し、『OK』 をクリック したいと思うユーザの名前を入力して下さい。 ツリーの新規ユーザ ディスプレイ。
6. ユーザ プロファイルを作成した後、特定の AAA プロパティを設定するために仕様 TACACS+ か RADIUS特性を割り当てて下さい:TACACS+ プロファイルをユーザ プロファイルに割り当てるために、グループプロファイルまたはユーザプロファイルに TACACS+ 属性を割り当てるために参照して下さい。RADIUSプロファイルをユーザ プロファイルに割り当てるために、グループプロファイルまたはユーザプロファイルに RADIUS特性を割り当てるために参照して下さい。

属性を適用する戦略

CSU によってネットワーク ユーザの認証 および 権限を設定するのに CSU グループ プロファイル 機能および TACACS+ および RADIUS特性使用して下さい。

グループおよびユーザ向けに属性を計画して下さい

CSU のグループ プロファイル 機能は多数のユーザ向けの AAA 必要条件の共通セットを定義することを可能にします。

グループ プロファイルに一組の TACACS+ または RADIUS特性値を割り当てることができます。グループに割り当てられるこれらの属性値はメンバーであるか、またはそのグループのメンバーとして追加されるあらゆるユーザに適用します。

グループ プロファイル 機能を効果的に使用して下さい

CSU を複雑な AAA 必要条件のたくさんのさまざまなタイプのユーザを管理するために設定するために Cisco はグループ プロファイルを作成し、設定するのに Cisco Secure 管理者 拡張設定プログラムの機能を使用することを推奨します。

グループ プロファイルはユーザに特定ではないすべての属性が含まれている必要があります。 これは通常パスワードを除いてすべての属性を意味します。 Cisco Secure 管理者のユーザページそれから簡単なユーザ プロファイルをパスワード属性で作成し、適切なグループ プロファイルにこれらのユーザ プロファイルを割り当てるのに追加を使用できます。 特定のグループのために定義される機能および属性値はメンバーにそれからユーザを加えます。

親 グループおよび子グループ

グループの階層を作成できます。 グループ プロファイルの中では、子グループ の プロファイルを作成できます。 親 グループ プロファイルに割り当てられる属性値は子グループ の プロファイルのデフォルト値です。

グループ レベル 管理

Cisco Secure システム アドミニストレータは個々の Cisco Secure ユーザ· グループ管理者ステータスを割り当てることができます。 グループに従属であるユーザ プロファイルおよびグループ管理者ステータスは子グループ の プロファイルを管理することを個々のユーザが可能にします。 ただし、グループの階層の外部で下るユーザまたはそれはそれらがグループを管理しないようにしません。 従って、システム アドミニストレータは他のユーザーに全部に等しい機関を許可しないで大規模なネットワークの管理のタスクを分配します。

どんな属性を個々のユーザ向けに定義しますか。

Cisco は個々のユーザにユーザ名、パスワード、パスワードタイプおよび Web 特権を定義する属性のようなユーザにユニーク、である基本的な認証 属性値を割り当てることを推奨します。 基本的な認証 属性値をユーザに CSU の Edit a User によって割り当てるか、またはユーザページを追加して下さい。

どんな属性をグループ プロファイルのために定義しますか。

Cisco はグループ レベルで修飾、許可およびアカウンティング関連の属性を定義することを推奨します。

この例では、「ダイヤルインユーザ」と指名されるグループ プロファイル =Framed 属性値ペア Frame-Protocol=PPP およびサービス タイプを割り当てられます。

絶対属性とは何か。

TACACS+ のサブセットおよび CSU の RADIUS特性はグループ プロファイル レベルの絶対ステータスを割り当てることができます。 グループ プロファイル レベルで絶対ステータスのために有効に なる 属性値は子グループ の プロファイルかメンバー ユーザ プロファイル レベルで対立する属性値を無効にします。

グループ 管理者の複数のレベルとの多重レベル ネットワークの中では、絶対属性はより低いレベルで管理者を無効になることができないグループ化する選択したグループ属性値を設定 することをシステム アドミニストレータが可能にします。

絶対ステータス ディスプレイに Cisco Secure 管理者 拡張設定プログラムの属性ボックスの絶対チェックボックスを割り当てることができる属性。 絶対ステータスを有効に するためにチェックボックスを選択して下さい。

グループ属性 値およびユーザ属性 値は競合できますか。

属性値間の競合解決は親 グループ プロファイルに、子グループ の プロファイル割り当て、属性値が絶対であるかどうか、そして TACACS+ または RADIUS特性であるかどうかメンバー ユーザ プロファイルはに左右されます:

- TACACS+ か絶対ステータス 上書きするのグループ プロファイルに割り当てられるRADIUS特性値子グループかユーザ プロファイル レベルで設定 される 対立する属性値。
- TACACS+ 属性値の絶対ステータスがグループ プロファイル レベルで有効に ならない場合、子グループかユーザ プロファイル レベルで設定 されるあらゆる対立する属性値によって無効になります。
- RADIUS特性値の絶対ステータスが親 グループ レベルで有効に ならない場合、子グループで設定 されるどの対立する属性値でも予測不可能な結果という結果に終ります。 グループおよびメンバー ユーザ向けの RADIUS特性値を定義するとき、ユーザおよびグループ プロファイル両方に同じアトリビュートを割り当てることを避けて下さい。

Prohibit および Permit オプションを使用して下さい

TACACS+ に関しては、キーワードの前に付けることによって受継がれたサービス値のアベイラビリティを**禁止します**サービス仕様にまたは**割り当て**無効にして下さい。 **割り当て**キーワードは指定 サービスを可能にします。 **禁止**キーワードは指定 サービスを拒否します。 一緒のこれらのキーワードの使用によって」、コンフィギュレーションを除いて「すべてを組み立てることができます。 たとえば、この設定は X.25 を除くすべてのサービスからアクセスを許可します:

```
default service = permit
prohibit service = x25
```

グループプロファイルまたはユーザプロファイルに TACACS+ 属性を割り当てて下さい

特定の TACACS+ サービスおよび属性をグループプロファイルまたはユーザプロファイルに割り当てるために、次の手順に従って下さい:

1. Cisco Secure 管理者 拡張設定プログラムで、**Members タブを**選択して下さい。 ナビゲーター ペインで、TACACS+ 属性が割り当てられるグループプロファイルまたはユーザプロファイルのためのアイコンをクリックして下さい。
2. 必要ならば、プロファイル ペインで、それを拡張するために **Profile アイコンを**クリックして下さい。『Profile』 を選択 されるに適当な属性が含まれているまたはサービスは画面の右下でウィンドウで表示するリストかダイアログボックス。 このウィンドウの情報は基づいてプロファイルがプロファイル ペインでまたは選択する保守するかどれに変わります。
3. 追加し、『Apply』 をクリック してほしいプロトコルかサービスをクリックして下さい。 サービスはプロファイルに追加されます。
4. Attribute ウィンドウの必要なテキストを入力するか、または選択して下さい。有効なエントリは UNIXリファレンスガイドのための CSU 2.3 の属性セクションを適用するための戦略で説明されます。**注:** グループ プロファイル レベルでディスプレイを**絶対**チェックボックス 規定 する アトリビュートおよび属性値を、割り当てたら、値絶対ステータスを割り当てるためにそのチェックボックスを選択して下さい。 絶対ステータス が 割り当てられた 値は下位グループプロファイルかユーザ プロファイル レベルで割り当てられるあらゆる競合する値によって無効にすることができません。
5. 追加する必要があるプロトコルか各付加サービスのためにステップ 1 を繰り返して下さい。
6. すべての変更を行うとき、『SUBMIT』 をクリック して下さい。

グループプロファイルまたはユーザプロファイルに RADIUS特性を割り当てて下さい

特定の RADIUS特性をグループプロファイルまたはユーザプロファイルに割り当てるため:

1. グループ プロファイルに RADIUS 辞書を割り当てて下さい:Cisco Secure 管理者 拡張設定 プログラムのメンバー ページで、**グループか User アイコンを**クリックし、そしてプロファイル ペインの **Profile アイコンを**クリックして下さい。 属性ペインでは、Options メニュー ディスプレイ。**Options メニュー**で、グループかユーザに使用してほしい RADIUS 辞書の名前をクリックして下さい。 （ たとえば、RADIUS - Cisco。 ）[Apply] をクリックします。
2. 必須チェック 項目を追加し、RADIUSプロファイルに属性を答えて下さい:**注:** チェック 項目がユーザ ID およびパスワードのような認証に、必要な属性です。 応答属性はプロファイルが認証 の 手順を渡した後フレーム化プロトコルのようなに VPDN ダイヤルインのネットワーク アクセス サーバ（NAS）送られる属性（NAS）です。 チェック 項目および応答属性のリストおよび説明に関しては、UNIXリファレンスガイドのための CSU 2.3 の RADIUS 属性値ペアおよび辞書 管理を参照して下さい。Profile ウィンドウで、RADIUS を-dictionaryname フォルダ の アイコン クリックして下さい。 （おそらく RADIUS フォルダを開くプロファイル + 記号をクリックする必要があります。 ） Attribute Group ウィンドウのチェック 項目および応答属性オプション ディスプレイ。これらの属性の何れか一つ以上を利用するために、利用したいと思うアトリビュートをクリックしそして『Apply』 をクリック して下さい。 複数のアトリビュートを一度に追加できます。フォルダを開くために + RADIUS のための記号- dictionaryname クリックして下さい。**注:** RADIUS-Cisco11.3 オプションを選択する場合、Cisco IOS ® ソフトウェア リリース 11.3.3(T) または それ 以降が NAS の接続でインストールされている確かめ、NAS コンフィギュレーションに新しいコマンド・ラインをことを追加して下さい。 十分に UNIXリファレンスガイドのための CSU 2.3 の RADIUS-Cisco11.3 辞書を有効に することを参照して下さい。
3. 追加されたチェック 項目の値を規定 し、属性を答えて下さい:**注意：** RADIUSプロトコルに関しては、遺産は階層的に対して付加的にです。 （TACACS+ プロトコルは階層的 な遺産を使用します）。 たとえば、ユーザおよびグループ プロファイル両方に同じ応答属性を割り当てれば、許可は NAS が属性の数を二度受け取るので失敗します。 それは応答属性の理にかなっていません。 グループおよびユーザ プロファイル両方に同じチェック 項目か応答アトリビュートを割り当てないで下さい。『Check Items』 をクリック するか、または**属性を答えるか**、または両方をクリックして下さい。 適当なチェック 項目および応答属性値のリストはより低い右側のウィンドウに現われます。 + フォルダを開く記号クリックして下さい。割り当てたいと思う値をクリックしそして『Apply』 をクリック して下さい。 値に関する詳細については、UNIXリファレンスガイドのための CSU 2.3 の RADIUS 属性値ペアおよび辞書 管理を参照して下さい。**注:** グループ プロファイル レベルでディスプレイを絶対チェックボックス 規定 する アトリビュートおよび属性値を、割り当てたら、値絶対ステータスを割り当てるためにそのチェックボックスを選択して下さい。 絶対ステータスを割り当てられる値は下位グループプロファイルかユーザ プロファイル レベルで割り当てられるあらゆる競合する値によって無効にすることができません。変更を行なうことを終わったら『SUBMIT』 をクリック して下さい。
4. これらの属性の何れか一つ以上を利用するために、利用したいと思うアトリビュートをクリックしそして『Apply』 をクリック して下さい。 複数のアトリビュートを一度に適用できます。

アクセス コントロール 特権 レベルを指定して下さい

スーパーユーザ 管理者は Cisco Secure ユーザにアクセス コントロール 特権のレベルを指定するのに Web 特権 アトリビュートを利用します。

1. Cisco Secure 管理者 拡張設定プログラムで、アクセス コントロール 特権を割り当てたいと思ったり、そしてプロファイル ペインの Profile アイコンをクリックするユーザをクリックして下さい。
2. Options メニューで、これらの値の 1 つを『Web Privilege』 をクリック し、選択して下さい。**0** -ユーザにユーザの Cisco Secure パスワードを変更する機能を含むアクセス コントロール 特権を否定します。**1** - CSUser Webページにユーザアクセスを認めます。 これは Cisco Secure ユーザが Cisco Secure パスワードを変更することを可能にします。 詳細についてはパスワードの変更に、Simple User and ACS Management のユーザー レベル機能を（パスワードの変更）どのようににについての参照しなさいか。**12** -ユーザグループのアドミニストレーター権限を許可します。**15** -ユーザシステム の アドミニストレーター特権を許可します。**注:** 0 以外 Web 特権 オプションを選択する場合、またパスワードを規定 して下さい。 Web 特権 パスワード要件を満たすために、単一 余白は最低基準です。

CSU を開始し、停止して下さい

通常、CSU はインストールされている SPARCstation を開始するか、または再起動するとき自動的に開始します。 ただし、CSU を手動で開始するか、または全体の SPARCStation をシャットダウンしないで停止できます。

CSU をインストールした SPARCStation へのログインとして[ルート]。

CSU を手動で開始するために、入力して下さい:

```
# /etc/rc2.d/S80CiscoSecure
```

CSU を手動で停止するために、入力して下さい:

```
# /etc/rc0.d/K80CiscoSecure
```

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

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco Secure ACS for UNIX に関するサポート ページ
- TACACS+ Support Page
- RADIUS 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