設定 Cisco DCM か。 リモート 認証 サポート

目次

概要

この資料は RADIUS を使用して Cisco Digital Content Manager （ DCM ） softwareRemote 認証を記述したものです。

前提条件

要件

Cisco は Cisco DCM ソフトウェア バージョン 16 の知識が以上にあることを推奨します。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- Cisco DCM ソフトウェア v16.10 以上に。
- freeRadius オープン ソース ソフトウェアと動作する RADIUSサーバ。

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。 対象のネットワークが実稼働中である場合には、どのような作業についても、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。

背景説明

DCM の V16.10 で DCM GUI.This 資料にアクセスするのに使用されるように RADIUSサーバで設定されるユーザアカウントを記述するこの機能を利用するために DCM および RADIUSサーバで必要なセットアップを可能にする新しい 機能は導入されました。

DCM の GUI アカウント

バージョン 16.0 および それ 以前では GUI にアクセスするために必要なユーザアカウントが DCM にローカル、すなわち作成しました、DCM で修正され、使用され、削除されてでした。

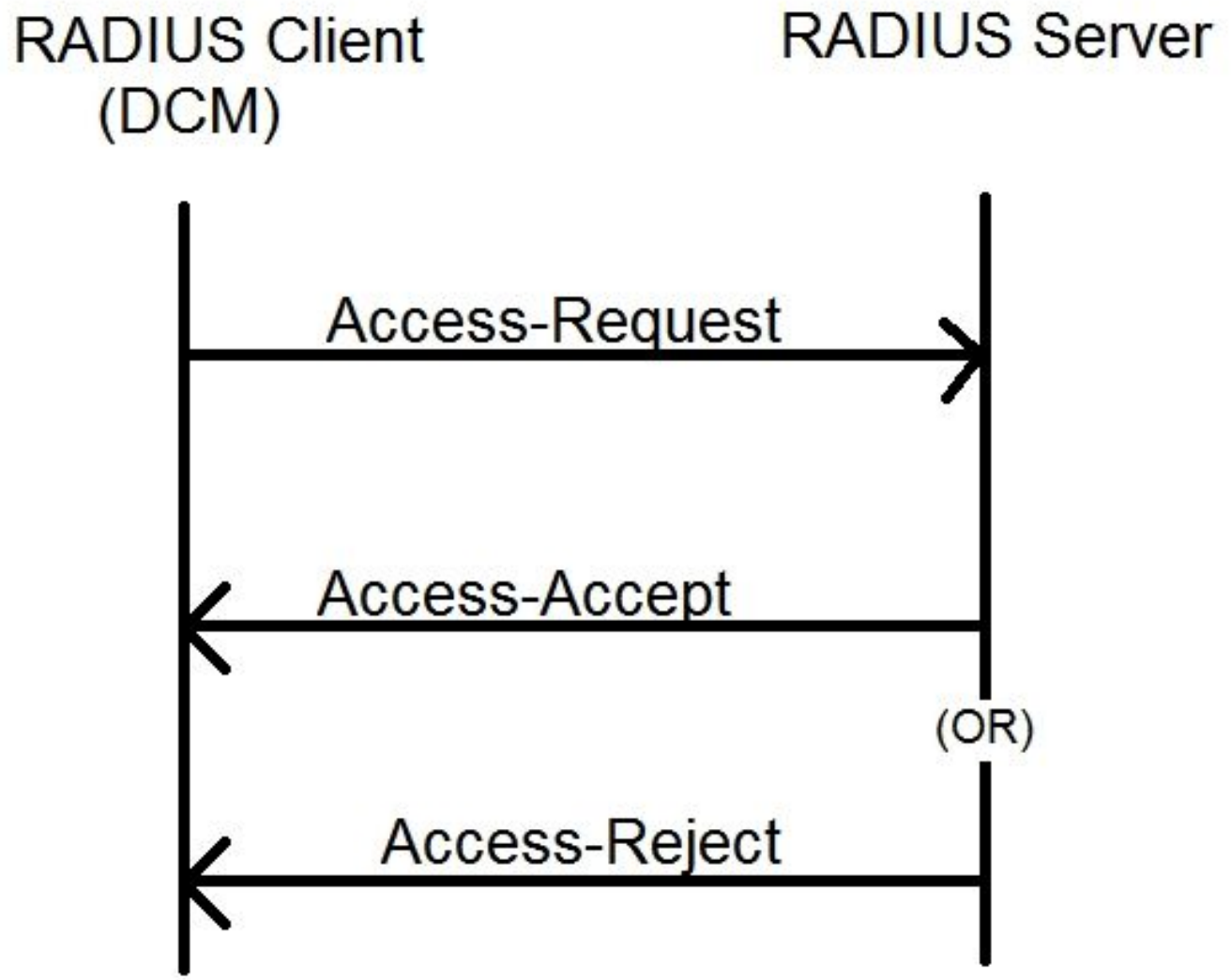
GUI ユーザアカウントはこれらのグループの 1 つに属することができます:

- 管理者（完全 な 制御）
- ユーザ（読み取りと書き込み）
- ゲスト（Read only）
- オートメーション トリガー（外部 の トリガー）
- DTF 管理者（DTF キー 設定）

リモート 認証

リモート 認証の概念はデバイス、アプリケーション、サービス先祖などにアクセスするのに使用することができるユーザアカウントの中央集中型収集を持つことです

イメージで説明されるステップはリモート 認証を使用すると何が起こるか説明します:



ステップ 1.ユーザは DCM GUI のログイン ページのログインおよびパスワード（RADIUSサーバで設定されるユーザアカウント）を入力します。

呼び出します。 DCM は RADIUSサーバに資格情報が付いている Access-Request メッセージを送ります。

ステップ 3 RADIUSサーバはパスワードが正しい、そのあとで次 の メッセージのどれでも DCM に返されますかどうか要求が設定 された クライアントのおよび DB/File のユーザアカウントのプロシージャのための 1 から来た確認し、検証しますかどうか

- Access-Accept –これは資格情報が有効であることを意味します。 設定された RADIUS特性は戻ります。
- Access-Reject –これは資格情報が無効であり、いくつかの RADIUS特性を送信 するように失敗を知らせるために RADIUSサーバが設定されるかもしれないことを意味します。
- アクセス チャレンジ–これは RADIUSサーバがユーザの信頼性を検証するためのその他の情報を必要とすることを意味します。 DCM で処理されなくて。

RADIUSサーバが Access-Reject を送信 すれば、DCM はユーザアカウントが DCM 自体にローカルであるそれにおける認証 の 手順が続かれればかどうか確認し。

ユーザは 15 分の間隔で（内部で） username/password が今でも有効なであり、ユーザが GUI 取引グループの 1 つに属することを確認するために再認証されます。 認証が失敗した現在の動作ユーザセッションは考えられた無効であり、すべての特権はユーザ向けに取り消されます。

RADIUS サーバの設定

RADIUSサーバの GUI これらのステップにアクセスするためのユーザアカウントを使用するために続かれる必要があって下さい:

DCM は RADIUSサーバへのクライアントで設定する必要があります。

1. RADIUSサーバのためのクライアントとして DCM の IP を追加して下さい。
2. DCM で設定される 1 つはセクションが DCM を設定することを見ると）クライアントコンフィギュレーションに共有秘密を追加して下さい（この共有秘密は同じであるはずです。
3. 各 DCM のための別の共有秘密があることを推奨します。
4. 共有秘密の長さは長く少なくとも 22 文字であるはずです。
5. 共有秘密はできるだけランダムであるはずです。

   よい共有秘密の例: 「89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345」

ユーザアカウントに関しては RADIUSサーバからの Access-Accept メッセージはユーザが属する GUI 取引グループを識別する RADIUS特性があるはずです。 属性名は DCM の設定ファイルで設定される必要選択し。

これは RADIUSサーバからのアトリビュートの値として伝送される必要があるストリングの形式です:

group_name_string **OU=<group_name_string> は**これらの 1 つである場合もあります:

Group	グループ名 ストリング
管理者（完全 な 制御）	管理者
ユーザ（読み取りと書き込み）	ユーザ
ゲスト（Read only）	ゲスト
オートメーション トリガー（外部トリガー）	オートメーション
DTF 管理者（DTF キー設定）	dtfadmins

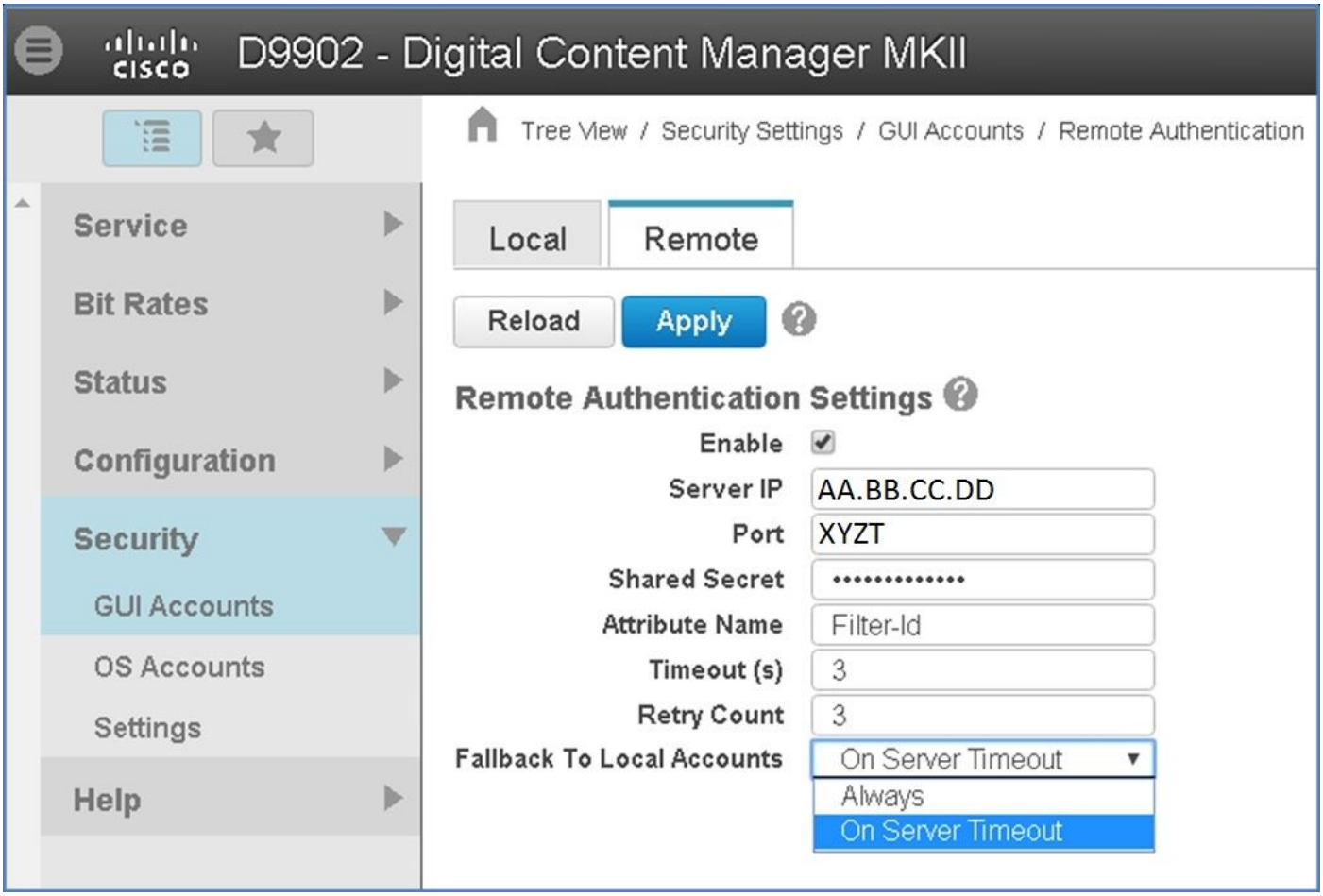
設定 Cisco DCM

有効に なるために/GUI 管理者 アカウントが必要となる DCM のリモート 認証 機能を設定して下さい。

これらのステップはリモート 認証を設定する方法を示します:

ステップ 1.管理者 アカウントを使用して DCM へのログイン。

ステップ 2.**セキュリティ > GUI アカウント**へのナビゲートはイメージに示すようにおよび**リモート** タブを、選択します:



ステップ 3. RADIUS 通信に必要なパラメータを設定して下さい:

- イネーブル-この設定はリモート 認証 サポートが有効に なったかどうか確認します。 チェックされたときパラメータ フィールドの他は有効に なります。
- サーバIP - RADIUSサーバの IP アドレス。
- ポート- RADIUSサーバが認証パケット（一般に 1812 を聞き取っているポートは他の値に設定することができます）。
- シークレット-サーバへ RADIUSパケットを送信 する前にパスワードを暗号化するのに使用されているこれは共有秘密です。 このシークレットはパスワードを復号化することを使用するRADIUSサーバで設定されるそれと同じであるはずです。
- 属性名-許可 データが RADIUSサーバから届くアトリビュートの名前。
- タイムアウト（秒で）-この設定は RADIUSサーバと DCM 間の通信のために使用されます。これは DCM が要求を終える前に特定の要求のための RADIUSサーバからの応答を待つはず

である時間です。

- リトライ回数-回数は RADIUS要求 以前の要求が時間を計られれば送信 する必要があります。
- ローカルアカウントへのフォールバック-この設定は DCM バージョン 19.0 から前に利用できます。 GUI を使用して作成される GUI（ローカル）を使用してログオンする DCM 割り当ては説明します。 **サーバタイムアウトの**オプションは、ローカルアカウントにフォールバックに RADIUSサーバが達することができなければないときに認証が失敗した許し。 オプションはフォールバックに、–認証が失敗した時でさえ**常に**常に許します。

ステップ 4 変更が加えられると同時にイメージで示されている警告は表示する。 『OK』 をクリック すれば ユーザインターフェイスは再起動します。

ステップ 5 この場合 DCM はリモート 認証の準備ができています。

DCM の設定 IPSec:

1. 管理者セキュリティ グループに属する GUI アカウントを使用して DCM へのログイン。

2. **Configuration > System** へのナビゲート。 システム設定 ページは提示されます。

3. イメージに示すように**追加新しい IPsec** エリアを、参照して下さい。

4. IP Address フィールドでは、新しい IPSec ピア（RADIUSサーバ）の IP アドレスを入力して下さい。

5. **事前共有**キーでは*事前共有キー フィールド*を、入力します新しい IPSec ピアのための*事前共*

有キーを再びタイプすれば。

6. [Add] をクリックします。 新しい IPSec ピアは IPsec 設定表に追加されます。

> **注:** RADIUSサーバが動作しているマシンの IPSec の設定には製品を与えられるドキュメント/パブリケーションを参照して下さい。

セキュリティに関する考慮事項

- 共有秘密は DCM のファイル システムで明白に保存されます。
- 暗号化されたパスワードはセッションの間に再認証の使用のための DCM のメモリで保存されます。
- 上記の 2 つの項目を与えられてだれが DCM にトラブルシューティング アクセスがあるか制限することを助言します。
- DCM と RADIUS 間の通信 チャネルを保護するのに IPSec を使用することを強く推奨しますしてください。

制約および制限

- リモート 認証 サポートは GUI アカウントに、ない OS アカウントにだけ利用できます。
- 再認証は 15 分の間隔で行われます。 例： ユーザ・グループが変更される場合、影響を奪取するためにかけられる変更のための最悪の場合時間は 15 分です。
- リモート 認証が有効に なる場合、DCM は RADIUSサーバとユーザアカウントが有効であるまたはまずチェックしましたりおよび次にローカルデータベースでチェックしますかどうか。 RADIUSサーバにないローカルアカウントの使用の場合には RADIUSサーバに認証失敗 メッセージがあります。

セットアップ freeRadius

このセクションは DCM のためにリモート 認証 サーバとして使用するために freeRadius を設定する方法を一例として示します。 これは情報提供だけを目的としています、

Cisco は freeRadius を提供しませんし、サポートしません。 freeRadius のためのコンフィギュレーション ファイルが **/etc/freeRadius/**（チェック ディストリビューション）の下にあることが仮定されます。

freeRadius パッケージ修正するをインストールした後これらのファイル。

- **/etc/freeradius/clients.conf を**修正して下さい
  ステップ 1.クライアントのリストに DCM の IP のためのエントリを追加して下さい。

ステップ 2.Add はディフォルトするためにクライアントコンフィギュレーションの共有鍵他のパラメータを去り。

各 DCM のためのユニークな共有秘密があることを推奨します。
共有秘密の長さは長く atleast 22 文字であるはずです。 共有秘密はできるだけランダムであるはずです。

よい共有秘密の例:
「
89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345」

- RADIUSサーバが受信する必要があるポートを変更するために **/etc/freeradius/radiusd.conf を**修正して下さい（一般に 1812）

- 新規 ユーザを追加するために **/etc/freeradius/users を**修正して下さい。

- 認証情報がこの形式の DCM に送信 される RADIUS特性を追加するために確認して下さい:
<Attribute Name> = 「**OU=<group_name>**」

属性名: これは許可 データが DCM group_name に次のいずれかの場合もある送信 される 標準RADIUS属性の名前です:
管理者-このグループに属するユーザはアドミニストレーター特権すなわち完全 な 制御があります。
ユーザ-このグループに属するユーザは読み取りと書き込み特権があります。
ゲスト-このグループに属するユーザは read only 特権があります。
オートメーション-オートメーション（外部 の トリガー）のために使用される。
dtfadmins - DTF 管理者（DTF キー 設定）

例：
スティーブ クリアテキスト パスワード: = 「テストします」
フィルタid = 「OU=administrators」

- （に関して）RADIUSサーバを変更を有効にするために開始して下さい。

- 選択されるにそれに RADIUSサーバ割り当て外部アクセスのファイアウォール構成を確認して下さい
ポート。

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

デバッグ purposses に関してはいくつかの追加ログはセキュリティ ログに導入されました。 このログ ナビゲートを**助けるために**表示するために > DCM GUI の**トレース ページ**。

このセクションは問題が可能 な 解決策である可能性がある何ログで探せばいいのか何を記述し。

測程線	リモート ログイン試みは失敗しました: RADIUSサーバへの要求は時間を計られまし
問題	DCM は RADIUSサーバと通信できません。
考えられる解決策	• DCM のリモート 認証 設定で提供される RADIUSサーバ IP アドレスが実際に正し • RADIUSサーバが DCM からアクセス可能であることを確認して下さい。 • DCM が RADIUSサーバの有効なクライアントで設定されるようにして下さい（R します）。 • DCM で設定される共有秘密がその特定の DCM のための RADIUSサーバで設定さ のための共有秘密を所有しなければ（、要求は無言で廃棄されます。）
測程線	リモート ログイン試みは失敗しました: [Errno 10054] はリモートホストによって現在 続強力に閉じられました。
問題	DCM は規定 された サーバIP に RADIUS要求を送信 しました。 ただし、RADIUSサ プリケーションはリモート 認証設定で規定 される ポートで受信していません。
考えられる解決策	• RADIUSサーバが動作していることを確認して下さい。 • サーバの RADIUSコンフィギュレーションで規定 される ポート番号が DCM で設 れるものと同じであることを確認して下さい。
測程線	リモート ログイン試みは失敗しました: 規定 される 無効 な属性名か RADIUSサーバ タからの応答。
問題	RADIUSサーバから届く応答に問題があります。
考えられる解決策	• RADIUSサーバが「Access-Accept」応答のアトリビュートを（DCM で設定され うにして下さい。 • DCM リモート 認証設定で設定される**属性名**パラメータが RADIUSサーバのユー レーションで指定どおりに絶対名であることを確認して下さい。
測程線	RADIUSサーバから届く無効 な 許可 データ。
問題	認証は成功しましたが、RADIUSサーバから届く応答は無効 な 許可 データすなわちセ リティグループ名前が含まれています。
考えられる解決策	• そのユーザ向けの RADIUSサーバで設定されるグループ名が RADIUSサーバを設 るセクションで規定 される セキュリティグループ名前の 1 つであることを確認し さい。 • RADIUSサーバで設定される RADIUSサーバを設定するセクションで規定 される に従ってストリングの形式があるようにして下さい。