Cisco DCMの設定 – リモート認証サポート

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[DCMのGUIアカウント](#)
[リモート認証](#)
[RADIUS サーバの設定](#)
[Cisco DCMの設定](#)
[セキュリティに関する考慮事項](#)
[制約と制限](#)
[freeRadiusの設定](#)
[トラブルシュート](#)

概要

このドキュメントでは、Cisco Digital Content Manager(DCM)ソフトウェアRADIUSを使用したリモート認証について説明します。

前提条件

要件

Cisco DCMソフトウェアバージョン16以降に関する知識があることが推奨されます。

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いています。

- Cisco DCMソフトウェアv16.10以降
- freeRadiusオープンソースソフトウェアで実行されている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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

DCMのV16.10では、RADIUSサーバで設定されたユーザアカウントをDCM GUIにアクセスするための新機能が導入されました。このドキュメントでは、DCMとRADIUSサーバでこの機能を使用するために必要な設定について説明します。

DCMのGUIアカウント

バージョン16.0以降では、GUIへのアクセスに必要なユーザアカウントはDCMに対してローカルでした。つまり、DCM上で作成、変更、使用、削除されています。

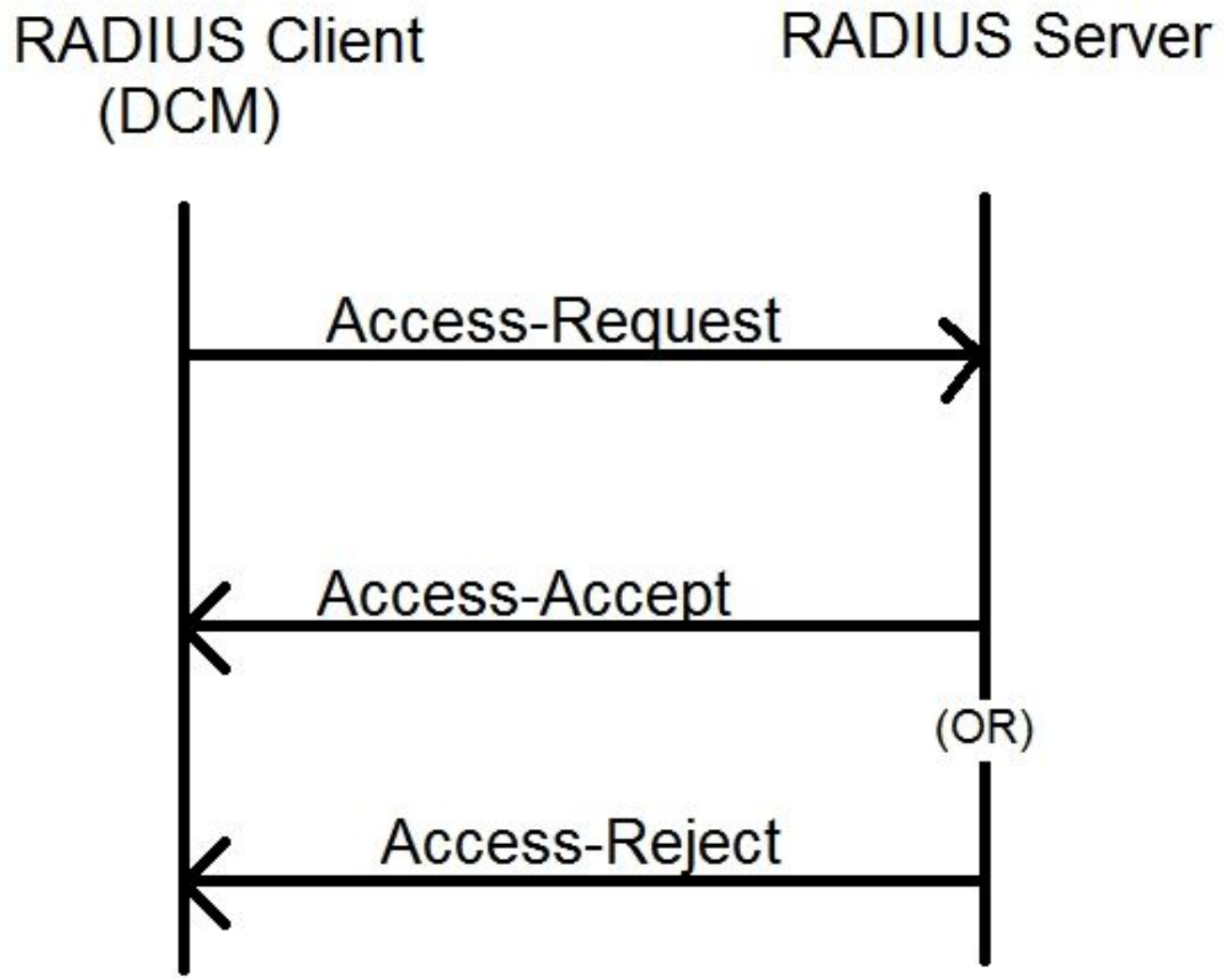
GUIユーザアカウントは、次のいずれかのグループに属できます。

- 管理者（フルコントロール）
- ユーザ（読み取り/書き込み）
- ゲスト（読み取り専用）
- 自動化トリガー（外部トリガー）
- DTF管理者（DTFキーの構成）

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、サービスなどにアクセスするために使用できるユーザアカウントの集中集合を持つことです。

次の図に、リモート認証を使用した場合の動作を示します。



ステップ1:DCM GUIのログインページで、ログインとパスワード（RADIUSサーバで設定されたユーザアカウント）を入力します。

ステップ2:DCMは、クレデンシャルを含むAccess-RequestメッセージをRADIUSサーバに送信します。

ステップ3:RADIUSサーバは、要求が設定済みのクライアントのいずれかから送信され、そのDB/ファイルにユーザアカウントが存在するかどうかを確認し、パスワードが正しいかどうかを検証します。その後、次のいずれかのメッセージがDCMに返されます

- Access-Accept：クレデンシャルが有効であることを意味します。設定されたRADIUS属性が返されます。
- Access-Reject：これは、クレデンシャルが無効であり、RADIUSサーバがRADIUS属性を送信して障害を通知するように設定されていることを意味します。
- Access-Challenge：これは、ユーザの信頼性を検証するために、RADIUSサーバに追加情報が必要であることを意味します。DCMでは処理されません。

RADIUSサーバがAccess-Rejectを送信する場合、DCMはユーザアカウントがDCM自体に対してローカルであるかどうかを確認し、その認証手順に従います。

ユーザは15分（内部）の間隔で再認証され、ユーザ名/パスワードがまだ有効であり、ユーザがGUIアカウントグループのいずれかに属していることを確認します。認証が失敗すると、現在実行中のユーザセッションは無効と見なされ、ユーザのすべての権限が取り消されます。

RADIUS サーバの設定

RADIUSサーバに存在するユーザアカウントを使用してGUIにアクセスするには、次の手順に従う必要があります。

DCMは、RADIUSサーバへのクライアントとして設定する必要があります。

1. DCMのIPをRADIUSサーバのクライアントとして追加します。
2. 共有秘密をクライアント設定に追加します（この共有秘密は、DCMで設定したものと同じである必要があります。DCMの設定の項を参照してください）。
3. DCMごとに異なる共有秘密を設定することをお勧めします。
4. 共有秘密の長さは22文字以上である必要があります。
5. 共有秘密は、できるだけランダムにする必要があります。

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

ユーザアカウントの場合、RADIUSサーバからのAccess-Acceptメッセージには、ユーザが属するGUIアカウントグループを識別するRADIUS属性が必要です。属性名を選択でき、DCMの設定ファイルで設定する必要があります。

RADIUSサーバから属性の値として送信する必要がある文字列の形式を次に示します。

OU=<group_name_string> group_name_stringは次のいずれかです。

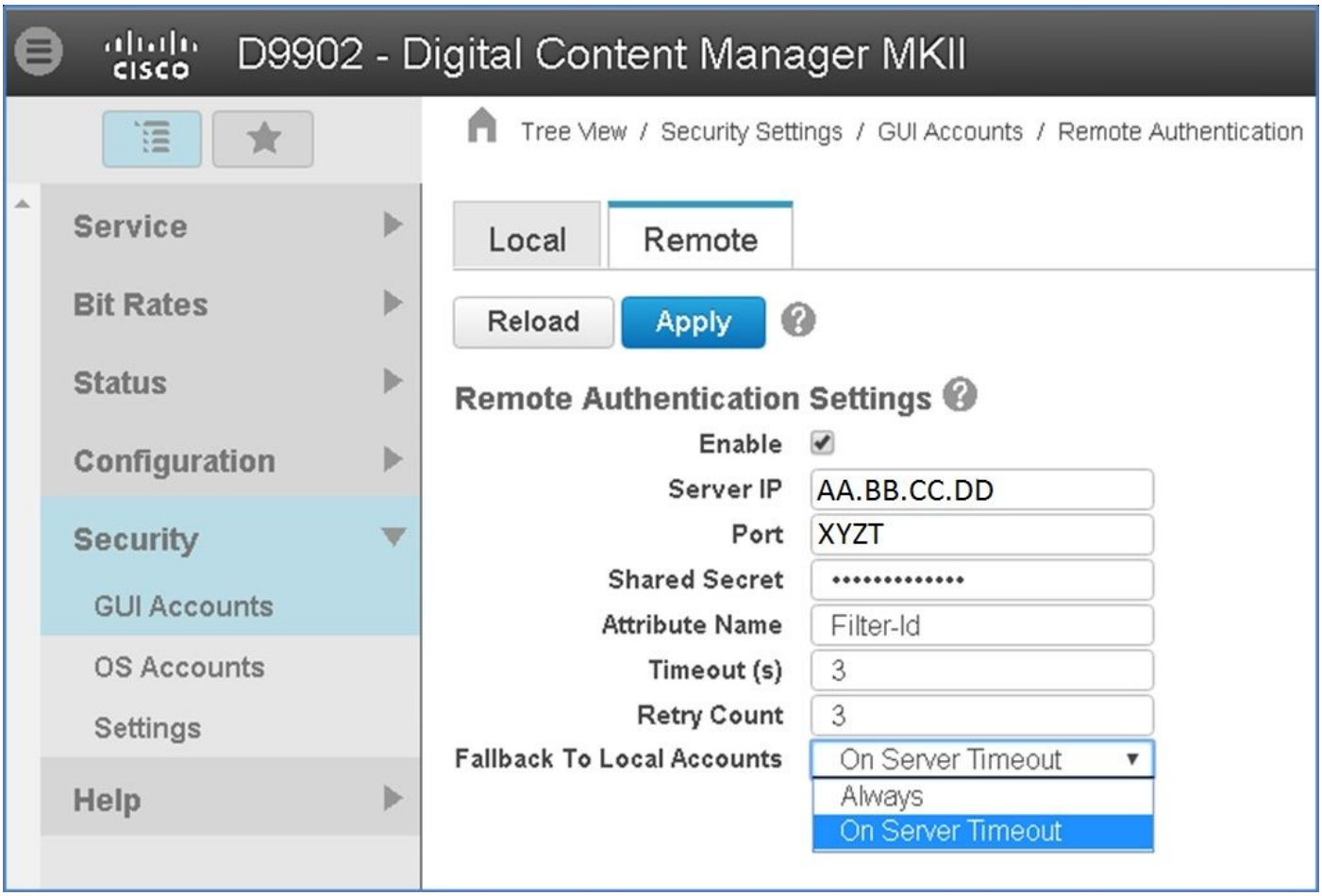
Group	グループ名文字列
管理者（フルコントロール）	管理者
ユーザ（読み取り/書き込み）	[ユーザ（users）]
ゲスト（読み取り専用）	ゲスト
自動化トリガー（外部） トリガ)	自動化
DTF管理者（DTFキー） 設定)	dtfadmins

Cisco DCMの設定

DCMでリモート認証機能を有効または設定するには、GUI管理者アカウントが必要です。
次の手順は、リモート認証の設定方法を示しています。

ステップ1：管理者アカウントを使用してDCMにログインします。

ステップ2：図に示すように、**[Security] > [GUI Accounts]に移動**し、[Remote]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ます。

- [有効(Enable)]：この設定は、リモート認証サポートを有効にするかどうかを決定します。オンにすると、残りのパラメータフィールドが有効になります。
- Server IP:RADIUSサーバのIPアドレス。
- Port:RADIUSサーバが認証パケットをリッスンしているポート（通常は1812、ただし他の値に設定できる）。
- Secret：これは、RADIUSパケットをサーバに送信する前にパスワードを暗号化するために使用される共有秘密です。このシークレットは、パスワードの復号化に使用されるRADIUSサーバで設定されているシークレットと同じである必要があります。
- [Attribute Name]:RADIUSサーバから認可データを受信する属性の名前。
- Timeout (in seconds)：この設定は、RADIUSサーバとDCM間の通信に使用されます。これは、DCMが特定の要求に対するRADIUSサーバからの応答を待ってから、要求を終了する時間です。

- [Retry Count]：以前の要求がタイムアウトになった場合に、RADIUS要求を送信する必要がある回数。

- [ローカルアカウントにフォールバック(Fallback To Local Accounts)]：この設定は、DCMバージョン19.0以降で使用できます。DCMでは、GUIを使用して作成されたGUI（ローカル）アカウントを使用してログオンできます。オプションの[On Server Timeout] を使用すると、RADIUSサーバに到達できない場合にローカルアカウントにフォールバックし、認証に失敗した場合にフォールバックを行うことができます。オプションの[Always]を使用すると、認証が失敗した場合でも常にフォールバックできます。

ステップ4：変更が適用されると、図に示す警告が表示されます。OKをクリックし、ユーザー・インタフェースを再起動します。

ステップ5：これで、DCMはリモート認証の準備ができました。

DCMでIPSecを設定します。

1. Administrators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にログオンします。

2. [Configuration] > [System]に移動します。[System Settings]ページが表示されます。

3.図に示すように、[Add New IPsec]領域を参照してください。

4. [IP Address]フィールドに、新しいIPsecピア（RADIUSサーバ）のIPアドレスを入力します。

5. [事前共有キー]フィールドと[事前共有キーのリタイプ]フィールドに、新しいIPsecピアの*事前共有キー*を入力します。

6. [追加]をクリックします。新しいIPsecピアがIPsec Settingsテーブルに追加されます。

注：RADIUSサーバが実行されているマシンでのIPSecの設定については、製品に付属のマニュアルまたはマニュアルを参照してください。

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のクリアテキストに保存されます。
- 暗号化されたパスワードは、セッション中の再認証に使用するためにDCMのメモリに保存されます。
- 上記の2つの項目を考慮して、DCMへのトラブルシューティングアクセス権を持つユーザを制限することを推奨します。
- DCMとRADIUS間の通信チャネルを保護するためにIPSecを使用することを強く推奨しますしてください。

制約と制限

- リモート認証のサポートは、OSアカウントではなく、GUIアカウントでのみ使用できます。
- 再認証は15分の間隔で実行されます。例：ユーザのグループが変更された場合、変更が有効になるまでの最悪のケース時間は15分です。
- リモート認証が有効な場合、DCMは最初にRADIUSサーバでユーザアカウントが有効かどうかを確認し、次にローカルデータベースを確認します。RADIUSサーバに存在しないローカルアカウントを使用する場合、RADIUSサーバに認証失敗メッセージが表示されます。

freeRadiusの設定

このセクションでは、freeRadiusをDCMのリモート認証サーバとして使用するように設定する例を示します。これは情報提供のみを目的としています

シスコはfreeRadiusを提供またはサポートしていません。freeRadiusの設定ファイルは、/etc/freeRadius/(**ディストリビューションを確認**)にあります。

freeRadiusパッケージをインストールした後、これらのファイルを変更します。

- /etc/freeradius/clients.confを変更します
  ステップ1:DCMのIPのエントリをクライアントのリストに追加します。
  ステップ2：クライアント設定で共有キーを追加し、他のパラメータをデフォルトのままにします。

各DCMに固有の共有秘密を設定することをお勧めします。
共有秘密の長さは22文字以上である必要があります。共有秘密は、できるだけランダムにする必要があります。

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

- RADIUSサーバが**リッスン**するポート（通常は1812）を変更するには、/etc/freeradius/radiusd.confを変更します

- /etc/freeradius/users**を変更して、新しいユ**ーザーを追加します。

- 許可情報がDCMに次の形式で送信されるRADIUS属性を追加します。
<Attribute Name> = **'OU=<group_name>'**

属性名:これは、DCM group_nameに認可データが送信される標準RADIUS属性の名前です。次のいずれかの名前を指定できます。
administrators – このグループに属するユーザーには、管理者権限（フルコントロール）があります。
users：このグループに属するユーザは、読み取り/書き込み権限を持ちます。
guests：このグループに属するユーザには、読み取り専用権限が付与されます。
自動化：自動化に使用されます（外部トリガー）。
dtfadmins - DTF管理者（DTFキーの設定）

例：
steve Cleartext-Password := "testing"
Filter-Id = "OU=administrators"

- 変更を有効にするには、RADIUSサーバを再起動します。

- RADIUSサーバのファイアウォール設定で、選択した
port.

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

デバッグ目的のために、セキュリティログに追加のログがいくつか追加されています。このログを表示するには、DCM GUIで[**Help**] > [**Traces]ページ**に移動します。

このセクションでは、ログの内容、問題の原因、および考えられる解決策について説明します。

ログライン	リモートログイン試行が失敗しました：RADIUSサーバへの要求がタイムアウトしまし
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サーバのIPアドレスが実際に正しい

	• DCMからRADIUSサーバにアクセスできることを確認します。 • DCMがRADIUSサーバ上の有効なクライアントとして設定されていることを確認 • DCMに設定されている共有秘密が、その特定のDCMのRADIUSサーバに設定され ）。
ログライン 問題	リモートログインの試行に失敗しました：[Errno 10054]既存の接続がリモートホスト DCMは指定されたサーバIPにRADIUS要求を送信しました。ただし、RADIUSサーバ
考えられる解決策	• RADIUSサーバが実行されていることを確認します。 • サーバのRADIUS設定で指定されているポート番号が、DCMで設定されているポ
ログライン 問題	リモートログイン試行が失敗しました：無効な属性名が指定されているか、RADIUS RADIUSサーバから受信した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」応答で（DCMに設定された）属性を送信する • DCMリモート認証設定に設定されている**Attribute Nameパラメータ**が、RADIUS であることを確認します。
ログライン 問題	RADIUSサーバから無効な許可データを受信しました。 認証は成功しましたが、RADIUSサーバから受信した応答に無効な許可データ（セキ
考えられる解決策	• そのユーザのRADIUSサーバで設定されているグループ名が、「RADIUSサーバの す。 • RADIUSサーバで設定する文字列の形式が、「RADIUSサーバの設定」セクション