配置Cisco DCM — 遠端身份驗證支援

目錄

簡介

本檔案介紹思科數位內容管理員(DCM)軟體使用RADIUS的遠端驗證。

必要條件

需求

思科建議您瞭解Cisco DCM軟體版本16及更高版本。

採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco DCM軟體v16.10及更高版本。
- 運行freeRadius開源軟體的RADIUS伺服器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在DCM的V16.10中引入了一項新功能，允許在RADIUS伺服器上配置的使用者帳戶用於訪問DCM GUI。本文檔介紹DCM和RADIUS伺服器上使用此功能所需的設定。

DCM上的GUI帳戶

在16.0及更低版本中，訪問GUI所需的使用者帳戶是DCM的本地帳戶，即在DCM上建立、修改、使用和刪除。

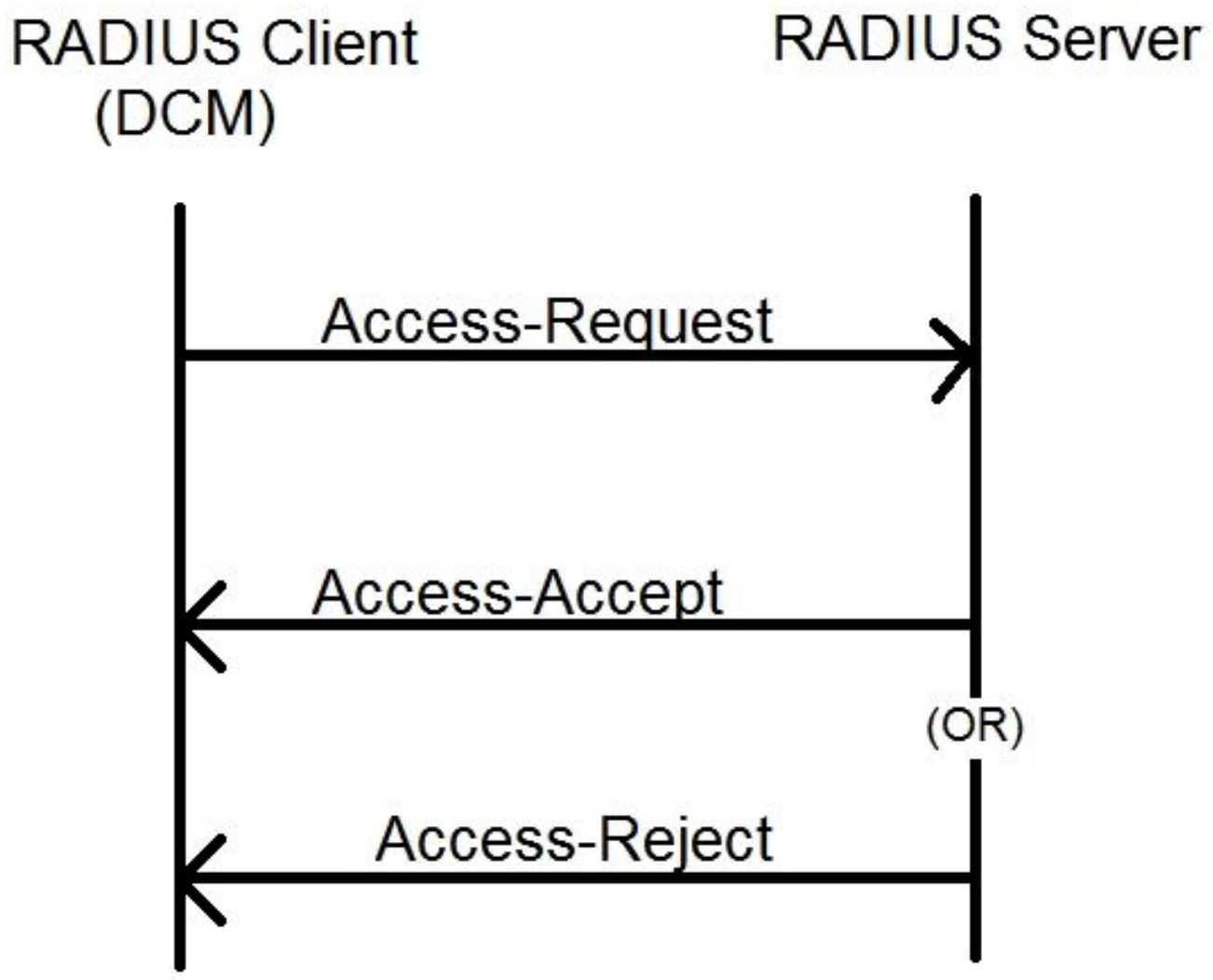
GUI使用者帳戶可以屬於以下組之一：

- 管理員（完全控制）
- 使用者（讀寫）
- 訪客（只讀）
- 自動化觸發器（外部觸發器）
- DTF管理員（DTF金鑰配置）

遠端驗證

遠端身份驗證的思想是集中收集可用於訪問裝置、應用、服務等的使用者帳戶。

圖中所示的步驟說明了使用遠端身份驗證時發生的情況：



步驟1。使用者在DCM GUI的登入頁面上輸入登入和密碼（在RADIUS伺服器上設定的使用者帳號

）。

步驟2. DCM向RADIUS伺服器傳送包含憑據的訪問請求消息。

步驟3. RADIUS伺服器會檢查要求是否來自其中一個已設定的使用者端，以及其資料庫/檔案上是否有使用者帳號，並驗證密碼是否正確，之後將以下任何訊息傳回DCM

- Access-Accept — 表示憑證有效。將返回配置的RADIUS屬性。
- Access-Reject — 表示憑證無效，並且RADIUS伺服器可能設定為傳送某些RADIUS屬性來通知失敗。
- Access-Challenge — 這意味著RADIUS伺服器需要一些附加資訊來驗證使用者的真實性。未在DCM中處理。

如果RADIUS伺服器傳送了Access-Reject，DCM將檢查使用者帳戶是否為DCM自身的本地帳戶，然後執行身份驗證過程。
系統會以15分鐘（內部）的時間間隔對使用者進行重新身份驗證，以確認使用者名稱/密碼是否仍然有效，以及使用者是否屬於某個GUI帳戶組。如果身份驗證失敗，則當前運行的使用者會話將被視為無效，並且撤銷該使用者的所有許可權。

設定RADIUS伺服器

若要使用RADIUS伺服器上的使用者帳戶存取GUI，需要執行以下步驟：

DCM應配置為RADIUS伺服器的客戶端。

1. 將DCM的IP新增為RADIUS伺服器的客戶端。
2. 將共用金鑰新增到客戶端配置（此共用金鑰應與DCM上配置的共用金鑰相同，請參閱配置DCM部分）。
3. 建議為每個DCM使用不同的共用金鑰。
4. 共用金鑰的長度應至少為22個字元。
5. 共用金鑰應儘可能隨機。

   良好共用金鑰的示例：'89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345'

對於使用者帳戶，來自RADIUS伺服器的訪問接受消息應具有標識使用者所屬的GUI帳戶組的RADIUS屬性。可以選擇屬性名稱，需要在DCM上的設定檔案中進行配置。

以下是需要從RADIUS伺服器作為屬性值傳送的字串格式：

OU=<group_name_string> group_name_string可以是以下之一：

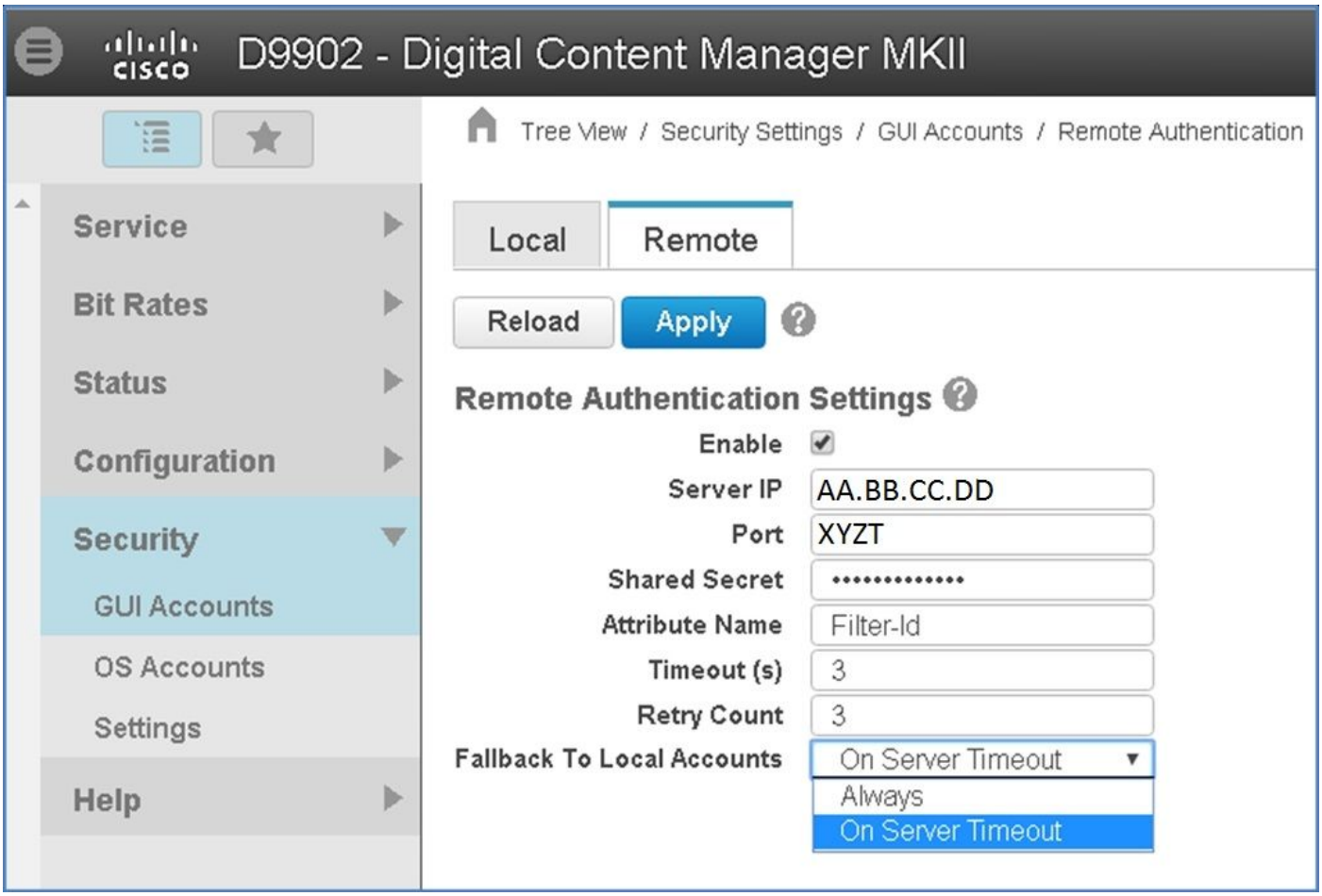
群組	組名稱字串
管理員（完全控制）	管理員
使用者（讀寫）	使用者
訪客（只讀）	訪客
自動化觸發器（外部） 觸發器)	自動化
DTF管理員（DTF金鑰） 組態)	dtfadmins

配置Cisco DCM

要在DCM上啟用/配置遠端身份驗證功能，需要GUI管理員帳戶。
以下步驟指示如何配置遠端身份驗證：

步驟1.使用管理員帳戶登入DCM。

步驟2.導覽至**Security > GUI Accounts**，然後選擇**Remote**頁籤，如下圖所示：



步驟3.配置RADIUS通訊所需的引數：

- Enable — 此設定確定是否應啟用遠端身份驗證支援。選中後，其餘引數欄位將啟用。
- 伺服器IP - RADIUS伺服器的IP地址。

- 連線埠 — RADIUS伺服器正在監聽驗證封包的連線埠（通常為1812，但可以設定為其他值）。
- Secret — 這是用於在將RADIUS封包傳送到伺服器之前加密密碼的共用密碼。此密碼應與RADIUS伺服器上配置的密碼相同，RADIUS伺服器用它來解密密碼。
- Attribute Name — 從RADIUS伺服器接收授權資料的屬性的名稱。
- 超時（秒） — 此設定用於RADIUS伺服器和DCM之間的通訊。這是DCM在終止請求之前等待來自RADIUS伺服器的響應時間。
- Retry Count — 在先前的請求超時的情況下，必須傳送RADIUS請求的次數。
- 回退到本地帳戶 — 此設定從DCM 19.0版開始可用。DCM允許使用使用GUI建立的GUI（本地）帳戶登入。選項，**On Server Timeout**允許回退到本地帳戶，以防無法訪問Radius伺服器，而在身份驗證失敗時則不允許。選項，**Always**允許始終回退 — 即使身份驗證失敗。

步驟4.應用更改後，將顯示影象中所示的警告。按一下**OK**並重新啟動使用者介面。

步驟5.現在DCM已準備好進行遠端身份驗證。

在DCM上配置IPSec:

1.使用屬於管理員安全組的GUI帳戶登入到DCM。

2.導覽至**Configuration > System**。系統將顯示System Settings頁面。

3.請參閱**新增新IPsec**區域，如下圖所示。

4.在「IP地址」欄位中，輸入新IPsec對等體（RADIUS伺服器）的IP地址。

5.在**Pre Shared** Key和Retype *Pre Shared Key*欄位中，輸入新IPsec對等體的*Pre Shared Key*。

6.按一下**Add**。新的IPsec對等體將新增到IPsec設定表中。

附註：有關運行RADIUS伺服器的電腦上的IPSec配置，請參閱產品附帶的文檔/出版物。

安全注意事項

- 共用金鑰以明文形式儲存在DCM的檔案系統中。
- 加密的密碼儲存在DCM的記憶體中，用於在會話期間進行重新身份驗證。
- 鑑於以上兩個專案，建議限制哪些人可以訪問DCM進行故障排除。
- 強烈建議使用IPSec來保護DCM和RADIUS之間的通訊通道
  伺服器.

限制和限制

- 遠端身份驗證支援僅適用於GUI帳戶，而不適用於OS帳戶。
- 重新身份驗證的間隔為15分鐘。範例：如果使用者的組已更改，則更改生效的最壞時間是15分鐘。
- 如果啟用了遠端身份驗證，則DCM首先會檢查RADIUS伺服器使用者帳戶是否有效，然後檢查本地資料庫。如果使用在RADIUS伺服器上不存在的本地帳戶，則RADIUS伺服器上會出現身份驗證失敗消息。

設定freeRadius

本節以示例說明如何設定freeRadius以用作DCM的遠端身份驗證伺服器。這只是為了提供資訊，

思科不提供或支援freeRadius。假定freeRadius的配置檔案位於**/etc/freeRadius/**（檢查分發）下。

安裝freeRadius軟體包後，請修改這些檔案。

- 修改**/etc/freeradius/clients.conf**
  步驟1.將DCM的IP項新增到客戶端清單中。
  步驟2.在客戶端配置中新增共用金鑰，並將其他引數保留為預設值。

  建議為每個DCM使用唯一的共用金鑰。
  共用金鑰的長度應至少為22個字元。共用金鑰應儘可能隨機。

良好共用金鑰的示例：
'89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345'

- 修改**/etc/freeradius/radiusd.conf**以更改radius伺服器應偵聽的埠（通常為1812）

- 修改**/etc/freeradius/users**以新增新使用者。

- 確保新增將授權資訊以以下格式傳送到DCM的RADIUS屬性：
<Attribute Name> = '**OU=<group_name>**'

屬性名稱：這是將授權資料傳送到DCM group_name所依據的標準RADIUS屬性的名稱，可以是以下屬性之一：
管理員 — 屬於該組的使用者將具有管理員許可權，即完全控制。
users — 屬於此組的使用者將具有讀寫許可權。
訪客 — 屬於此組的使用者將具有只讀許可權。
自動化 — 用於自動化（外部觸發器）。
dtfadmins - DTF管理員（DTF金鑰配置）

範例：
steve Cleartext-Password := "測試"
Filter-Id = "OU=administrators"

- （重啟）啟動radius伺服器以使更改生效。

- 確保radius伺服器的防火牆配置允許外部訪問所選的
連接埠.

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

為了進行調試，安全日誌中還引入了一些其他日誌。要檢視此日誌，請導航到DCM GUI中的**幫助>跟蹤**頁。

本節介紹要在日誌中查詢的內容、可能存在的問題以及可能的解決方案。

日誌行	遠端登入嘗試失敗：對RADIUS伺服器的請求超時。
問題	DCM無法與RADIUS伺服器通訊。
可能的解決方案	• 驗證DCM中的遠端身份驗證配置中提供的RADIUS伺服器IP地址是否真正正確。 • 確保可以從DCM訪問RADIUS伺服器。 • 確保DCM已配置為RADIUS伺服器上的有效客戶端（RADIUS伺服器以靜默方式丟棄來 • 確保DCM上配置的共用金鑰與RADIUS伺服器上為該特定DCM配置的共用金鑰相同。

。）

日誌行	遠端登入嘗試失敗：[錯誤號10054]遠端主機強制關閉了現有連線。
問題	DCM向指定的伺服器IP傳送了RADIUS請求。但是，RADIUS伺服器應用程式未在遠端身份
可能的解決方案	• 確保RADIUS伺服器正在運行。 • 檢查伺服器的RADIUS配置中指定的埠號是否與DCM上配置的埠號相同。
日誌行	遠端登入嘗試失敗：指定的屬性名稱無效，或者來自RADIUS伺服器的響應缺少授權資料。
問題	從RADIUS伺服器接收的響應出現問題。
可能的解決方案	• 確保RADIUS伺服器在「Access-Accept」回應中傳送屬性（在DCM上設定）。 • 確保DCM遠端身份驗證設定上配置的**Attribute Name**引數與RADIUS伺服器上的使用者中指定的名稱完全相同。
日誌行	從RADIUS伺服器接收的授權資料無效。
問題	身份驗證成功，但從RADIUS伺服器收到的響應包含無效的授權資料，即安全組名稱。
可能的解決方案	• 確保在RADIUS伺服器上為該使用者配置的組名稱是在配置RADIUS伺服器部分中指定一。 • 確保RADIUS伺服器上配置的字串的格式與配置RADIUS伺服器一節中指定的格式一致