配置Cisco DCM — 远程身份验证支持

目录

简介

本文档介绍Cisco Digital Content Manager(DCM)软件使用RADIUS进行远程身份验证。

先决条件

要求

思科建议您了解Cisco DCM软件版本16及更高版本。

使用的组件

本文档中的信息基于以下软件版本：

- Cisco DCM软件v16.10及更高版本。
- 使用freeRadius开源软件运行的RADIUS服务器。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在DCM的V16.10中引入了一项新功能，允许在RADIUS服务器上配置的用户帐户用于访问DCM GUI。本文档介绍在DCM和RADIUS服务器上使用此功能所需的设置。

DCM上的GUI帐户

在版本16.0及更低版本中，访问GUI所需的用户帐户是DCM的本地帐户，即在DCM上创建、修改、使用和删除。

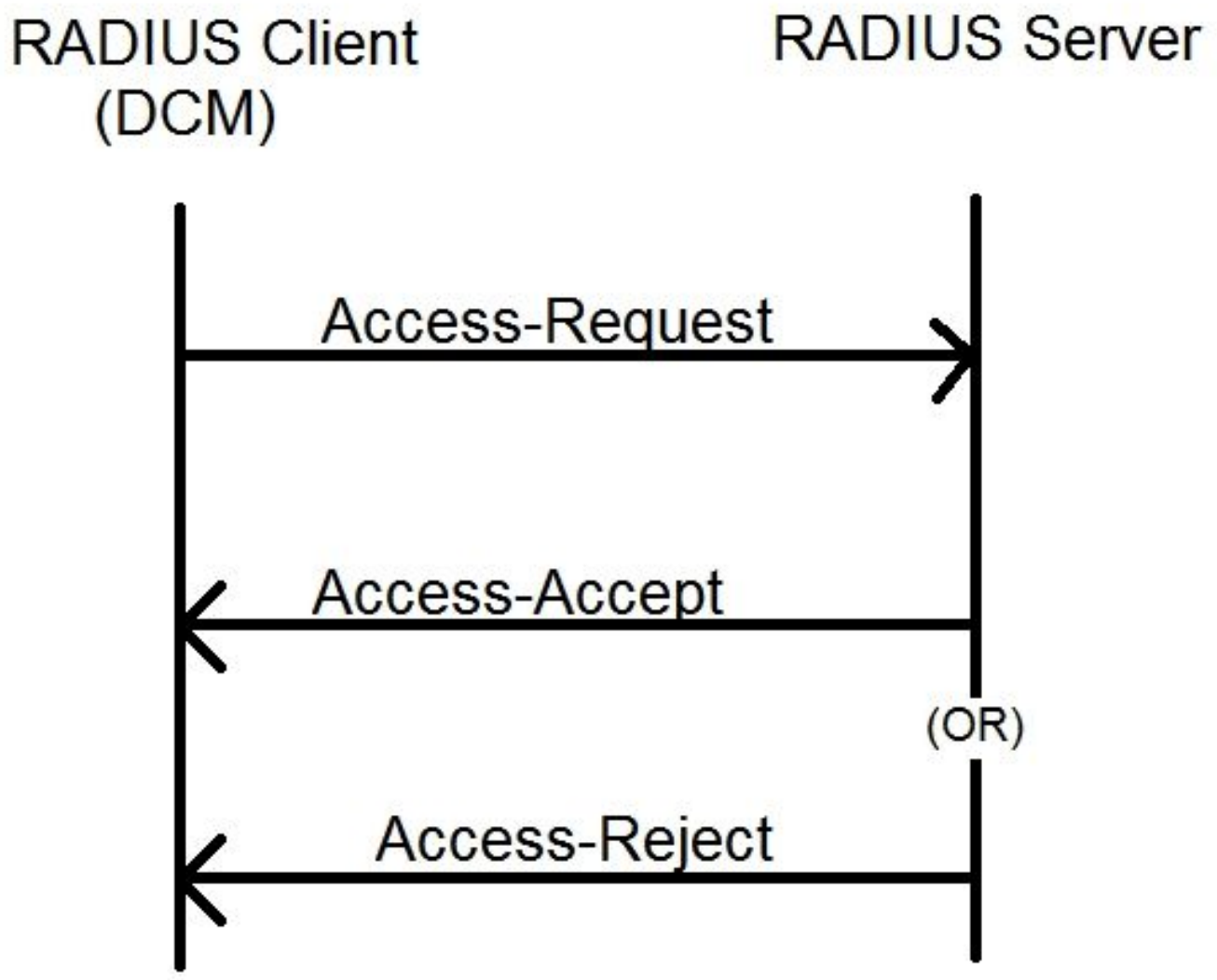
GUI用户帐户可以属于以下组之一：

- 管理员（完全控制）
- 用户（读写）
- 访客（只读）
- 自动化触发器（外部触发器）
- DTF管理员（DTF密钥配置）

远程身份验证

远程身份验证的思想是集中收集用户帐户，这些帐户可用于访问设备、应用、服务等。

图中显示的步骤说明了使用远程身份验证时会发生什么情况：



步骤1.用户在DCM GUI的登录页上输入登录和密码（在RADIUS服务器上配置的用户帐户）。

步骤2. DCM向RADIUS服务器发送包含凭证的Access-Request消息。

步骤3. RADIUS服务器检查请求是否来自已配置的客户端之一，以及其DB/File上是否存在用户帐户，并验证密码是否正确，然后将以下任一消息返回给DCM

- Access-Accept — 这意味着凭证有效。返回已配置的RADIUS属性。
- Access-Reject — 这意味着凭证无效，并且RADIUS服务器可能配置为发送某些RADIUS属性以通知故障。
- 访问质询 — 这意味着RADIUS服务器需要一些附加信息来验证用户的真实性。未在DCM中处理。

如果RADIUS服务器发送Access-Reject，DCM会检查用户帐户是否是DCM本身的本地帐户，并遵循该帐户的身份验证过程。
在15分钟（内部）的间隔内对用户重新进行身份验证，以确认用户名/密码仍然有效且用户属于GUI帐户组之一。如果身份验证失败，当前正在运行的用户会话将被视为无效，并且会撤销该用户的所有权限。

配置RADIUS服务器

要使用RADIUS服务器上的用户帐户访问GUI，需要执行以下步骤：

DCM应配置为RADIUS服务器的客户端。

1. 将DCM的IP添加为RADIUS服务器的客户端。
2. 将共享密钥添加到客户端配置（此共享密钥应与DCM上配置的共享密钥相同，请参阅配置DCM一节）。
3. 建议为每个DCM使用不同的共享密钥。
4. 共享密钥的长度应至少为22个字符。
5. 共享密钥应尽可能随机。

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

对于用户帐户，来自RADIUS服务器的Access-Accept消息应具有标识用户所属的GUI帐户组的RADIUS属性。可以选择属性名称，并需要在DCM的设置文件中配置。

以下是需要作为RADIUS服务器属性值发送的字符串的格式：

OU=<group_name_string>group_name_string可以是以下其中之一：

组	**组名称字符串**

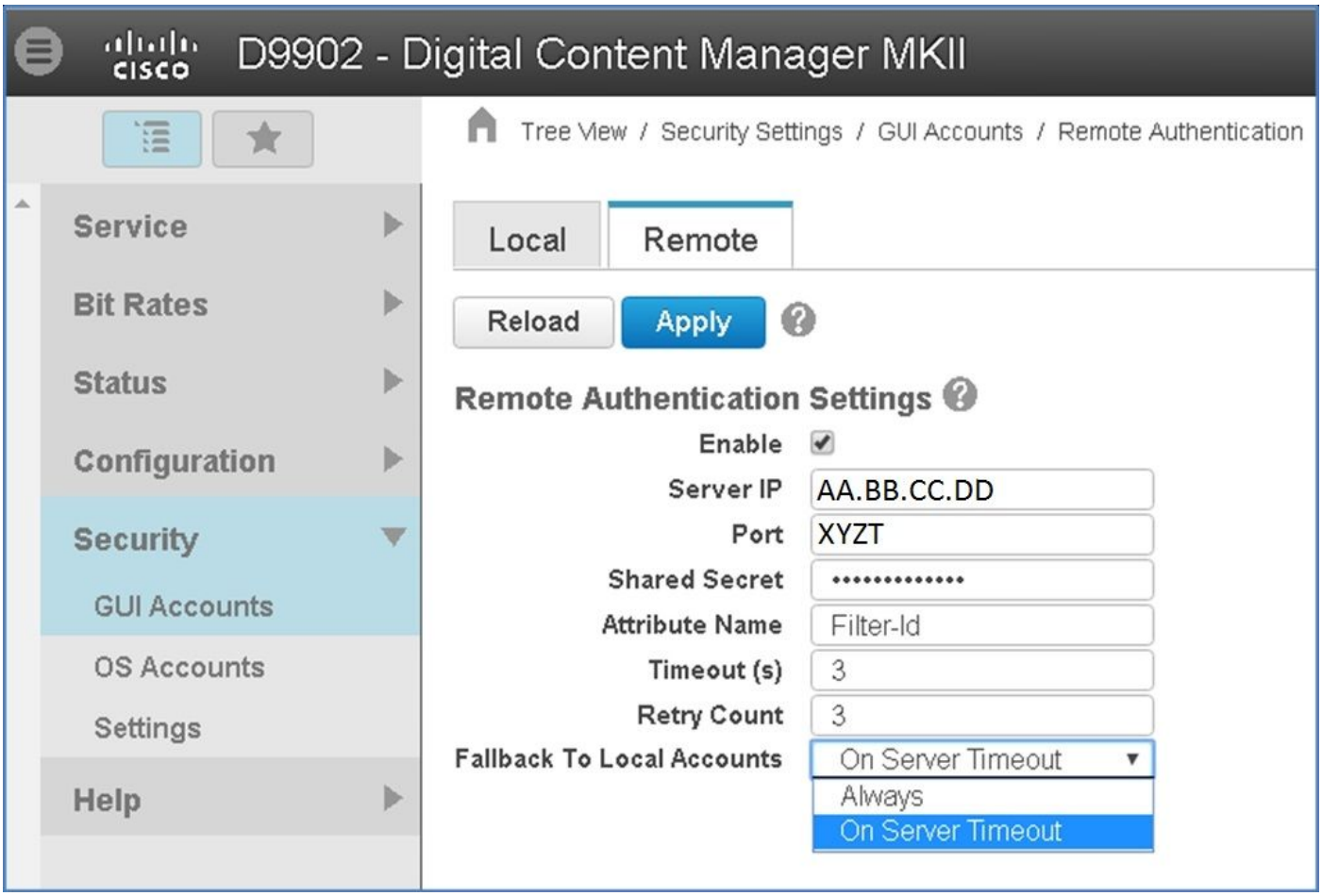
管理员（完全控制）	管理员
用户（读写）	用户
访客（只读）	客人
自动化触发器(外部触发器)	自动化
DTF管理员（DTF密钥）配置)	dtfadmin

配置Cisco DCM

要在DCM上启用/配置远程身份验证功能，需要GUI管理员帐户。
以下步骤说明如何配置远程身份验证：

步骤1.使用管理员帐户登录DCM。

步骤2.导航至“安**全”>“GUI帐户”**并选择**“远**程”选项卡，如图所示：



步骤3.配置RADIUS通信所需的参数：

- 启用 — 此设置确定是否应启用远程身份验证支持。选中后，其余参数字段将启用。
- 服务器IP - RADIUS服务器的IP地址。
- 端口 — RADIUS服务器侦听身份验证数据包的端口（通常为1812，但可以配置为其他值）。

- Secret — 这是用于在将RADIUS数据包发送到服务器之前加密密码的共享密钥。此密钥应与RADIUS服务器上配置的密码相同，RADIUS服务器使用此密钥解密密码。
- Attribute Name — 从RADIUS服务器接收授权数据的属性的名称。
- 超时（秒） — 此设置用于RADIUS服务器与DCM之间的通信。这是DCM在终止请求之前应等待RADIUS服务器对特定请求做出响应的时间。
- 重试计数 — 在以前的请求超时时必须发送RADIUS请求的次数。
- 回退到本地帐户 — 从DCM 19.0版开始，此设置可用。DCM允许使用使用GUI创建的GUI（本地）帐户登录。选项， **On Server Timeout** 允许在Radius服务器无法访问时回退到本地帐户，而在身份验证失败时不能回退到本地帐户。选项，**Always** 允许始终回退 — 即使身份验证失败。

步骤4.应用更改时，将显示图像中显示的警告。单击**OK**，然后重新启动用户界面。

步骤5.现在DCM已准备好进行远程身份验证。

在DCM上配置IPSec:

1.使用属于Administrators安全组的GUI帐户登录DCM。

2.导航至“**配置**”>“**系统**”。系统将显示System Settings页面。

3.请参阅“添**加新IPsec**”区域，如图所示。

4.在IP Address字段中，输入新IPsec对等体（RADIUS服务器）的IP地址。

5.在“预共**享密**钥”和“重*新键入预共享密*钥”字段中，输*入新IPsec对*等体的预共享密钥。

6.单击“添**加”**。新的IPsec对等体将添加到IPsec Settings（IPsec设置）表。

> **注意：**有关在运行RADIUS服务器的计算机上配置IPSec的信息，请参阅随产品提供的文档/发布。

安全考虑

- 共享密钥以明文形式存储在DCM的文件系统中。
- 加密密码存储在DCM的内存中，以在会话期间用于重新身份验证。
- 根据以上两项，建议限制对DCM的故障排除访问权限。
- 强烈建议使用IPSec保护DCM和RADIUS之间的通信通道
  服务器。

限制和限制

- 远程身份验证支持仅适用于GUI帐户，而不适用于操作系统帐户。
- 重新身份验证的间隔为15分钟。示例：如果用户组已更改，则更改生效的最坏情况时间为15分钟。
- 如果启用远程身份验证，DCM首先与RADIUS服务器检查用户帐户是否有效，然后检查本地数据库。如果使用RADIUS服务器上不存在的本地帐户，则RADIUS服务器上会出现身份验证失败消息。

设置freeRadius

本部分显示如何设置freeRadius以用作DCM的远程身份验证服务器。这仅供参考，

思科不提供或支持freeRadius。假设在/etc/freeRadius/（检查分发）下**找到freeRadius的配**置文件。

安装freeRadius软件包后，请修改这些文件。

- 修改/etc/freeradius/clients.conf**目录**
  步骤1.将DCM的IP条目添加到客户端列表。
  步骤2.在客户端配置中添加共享密钥，并将其他参数保留为默认值。

  建议为每个DCM使用唯一的共享密钥。

共享密钥的长度应至少为22个字符。共享密钥应尽可能随机。

良好共享密钥的示例：
'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服务器应侦听的端口（通常为1812）
- 修改/etc**/freeradius/users**以添加新用户。
- 确保以以下格式将授权信息发送到DCM的RADIUS属性：
  <属性名称> = 'OU=<group_name>'

  属性名称:这是将授权数据发送到DCM group_name的标准RADIUS属性的名称，可以是以下其中一项：
  管理员 — 属于此组的用户将具有管理员权限，即完全控制。
  users — 属于此组的用户将具有读写权限。
  guests — 属于此组的用户将具有只读权限。
  自动化 — 用于自动化（外部触发器）。
  dtfadmins - DTF管理员（DTF密钥配置）

  示例：
  steve cleartext-Password := "testing"
  Filter-Id = "OU=administrators"
- （重新）启动RADIUS服务器以使更改生效。
- 确保RADIUS服务器的防火墙配置允许外部访问所选端口。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

为了调试目的，安全日志中引入了一些其他日志。要查看此日志，请导航至DCM GUI中**的“帮助”>“**跟踪”页。

本节介绍日志中要查找的内容、可能存在的问题和可能的解决方案。

日志行	远程登录尝试失败：对RADIUS服务器的请求超时。
问题	DCM无法与RADIUS服务器通信。
可能的解决方案	• 验证DCM中远程身份验证配置中提供的RADIUS服务器IP地址实际正确。 • 确保RADIUS服务器可从DCM访问。 • 确保DCM配置为RADIUS服务器上的有效客户端（RADIUS服务器以静默方式丢弃来自

- 确保在DCM上配置的共享密钥与在RADIUS服务器上为特定DCM配置的共享密钥相同。）

日志行	远程登录尝试失败：[错误10054]远程主机强制关闭了现有连接。
问题	DCM已向指定的服务器IP发送RADIUS请求。但是，RADIUS服务器应用程序未侦听远程
可能的解决方案	• 确保RADIUS服务器正在运行。 • 检查服务器上RADIUS配置中指定的端口号是否与DCM上配置的端口号相同。
日志行	远程登录尝试失败：指定的属性名称无效或RADIUS服务器的响应缺少授权数据。
问题	从RADIUS服务器收到的响应有问题。
可能的解决方案	• 确保RADIUS服务器在“Access-Accept”响应中发送属性（在DCM上配置）。 • 确保在DCM远程身份验证设置上配置的**Attribute Name**参数是RADIUS服务器上用户配指定的确切名称。
日志行	从RADIUS服务器接收的授权数据无效。
问题	身份验证成功，但从RADIUS服务器收到的响应包含无效的授权数据，即安全组名称。
可能的解决方案	• 确保在RADIUS服务器上为该用户配置的组名称是配置RADIUS服务器一节中指定的安一。 • 确保在RADIUS服务器上配置的字符串的格式与配置RADIUS服务器一节中指定的格式