配置思科DCM ？远程验证支持

目录

简介

本文描述思科数字内容管理器(DCM)使用RADIUS， softwareRemote验证。

先决条件

要求

Cisco建议您有知识Cisco DCM软件版本16以上。

使用的组件

本文档中的信息基于以下软件版本：

- 思科DCM软件v16.10以上。
- 与freeRadius开放源软件的RADIUS服务器运行。

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。如果您的网络实际，请保证您了解所有命令潜在影响。

背景信息

在DCM的V16.10中允许在RADIUS服务器配置的用户帐户使用访问DCM GUI.This文档描述在DCM和RADIUS服务器要求的设置利用此功能的新特性介绍。

在DCM的GUI帐户

在版本16.0和以下要求的用户帐户访问GUI是本地对DCM，即已创建，已修改，使用和删除在DCM。

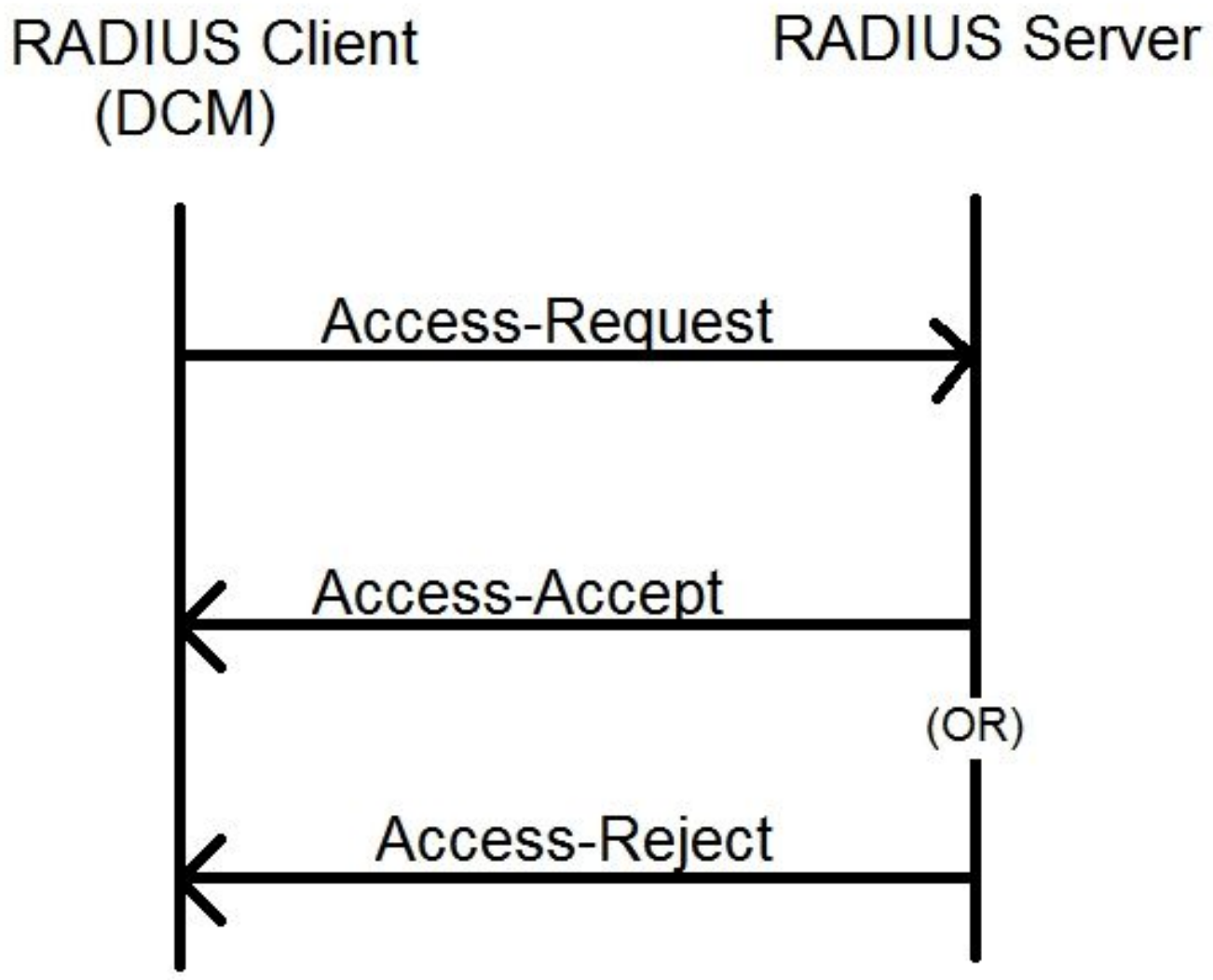
GUI用户帐户能属于到这些组之一：

- 管理员(完全控制)
- 用户(Read-Write)
- 访客(只读)
- 自动化触发(外部触发器)
- DTF管理员(DTF锁上配置)

远程验证

远程验证想法是有可以用于访问设备、应用程序，服务等用户帐户的集中化收藏。

在镜像显示的步骤解释发生了什么，当您使用远程验证：



步骤1.用户输入登录和密码(在RADIUS服务器配置的用户帐户)在登录页在DCM GUI。

第二步：DCM传送与凭证的Access-Request信息到RADIUS服务器。

第三步：RADIUS服务器检查请求是否来自一个配置的客户端和用户帐户的存在的在其DB/File的并且验证，如果密码正确或没有，在后任何一个下列信息返回对DCM

- Access-Accept –这意味着凭证有效。已配置的RADIUS属性返回。
- 访问拒绝–这意味着凭证无效，并且RADIUS服务器可能配置发送一些RADIUS属性通知失败。
- 访问-查询–这意味着RADIUS服务器需要验证的用户的真实性一些其他信息。没处理在DCM。

万一RADIUS服务器发送访问拒绝， DCM检查用户帐户是否是本地对DCM，并且那的认证程序被仿效。
用户重新鉴别在间隔15分钟(内部地)确认用户名/密码有效，并且用户属于到其中一GUI帐户小组。如果验证发生故障当前运行用户会话视为无效，并且所有权限为用户取消。

配置RADIUS服务器

要使用用户帐户在RADIUS服务器访问的GUI这些步骤请需要被跟随：

应该配置DCM作为RADIUS服务器的一个客户端。

1. 添加DCM的IP作为RADIUS服务器的一个客户端。
2. 添加共享机密到客户端配置(此共享机密应该是相同的象在DCM配置的那个，参见部分配置DCM)。
3. 推荐有每个DCM的一不同的共享机密。
4. 共享机密的长度应该是长至少22个的字符。
5. 共享机密应该是一样随机尽可能。

   一好共享机密的示例
   ：“89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345’

对于用户帐户从RADIUS服务器的Access-Accept消息应该有识别GUI帐户小组用户属于的RADIUS属性。属性名称在DCM的设置文件可以选择和需要配置。

这是需要被发送作为一个属性的一个值从RADIUS服务器字符串的格式：

group_name_string的**OU=<group_name_string>**可以是这些中的一个：

组	**组名字符串**
管理员(完全控制)	管理员
用户(Read-Write)	用户
访客(只读)	访客
自动化触发(外部	自动化

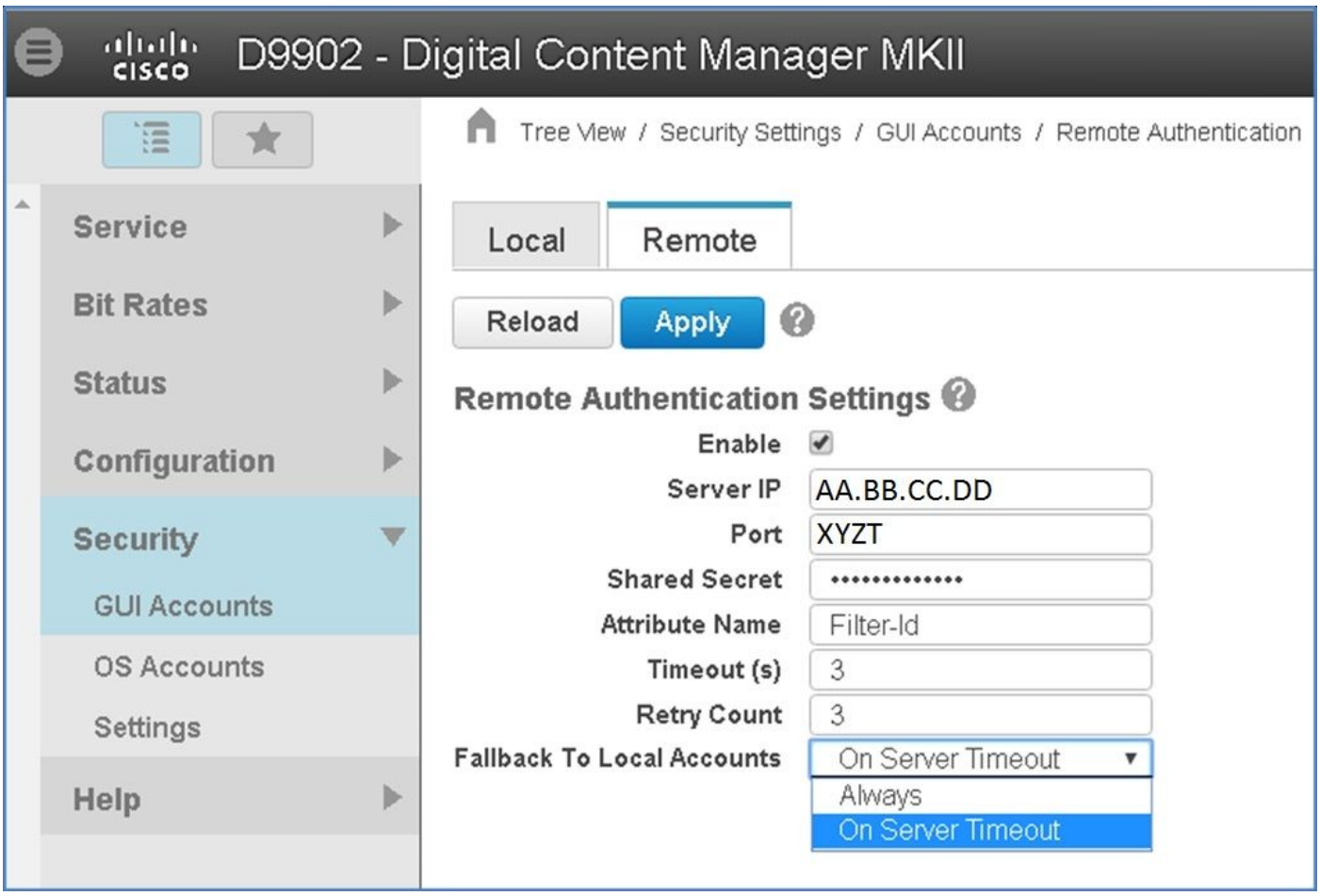
触发)
DTF管理员(DTF密钥配置) dtfadmins

配置思科DCM

要启用/请配置在GUI管理员帐户要求的DCM的远程验证功能。
这些步骤指示如何配置远程验证：

步骤1. DCM的洛金使用管理员帐户。

步骤2.如镜像所显示，导航对**安全> GUI帐户**并且选择**远程**选项卡， ：



步骤3.配置为RADIUS通信要求的参数：

- Enable (event) -此设置确定远程验证支持应该是否启用。当检查参数字段的其余启用。
- 服务器IP - RADIUS服务器的IP地址。
- 波尔特- RADIUS服务器细听认证信息包的波尔特(通常1812，但是可以配置到其他值)。
- 塞克雷-用于在发送RADIUS信息包前加密密码对服务器的这是共享机密。此机密应该是相同的象在用于解密密码的RADIUS服务器配置的那。

- 属性名称-授权数据从RADIUS服务器接收属性的名称。
- 超时(以秒钟) -此设置使用RADIUS服务器和DCM之间的通信。这是时间DCM应该在终止请求前等待从RADIUS服务器的一答复一特定的请求的。
- 重试计数-次数RADIUS请求，万一先前的请求被计时，必须发送。
- 对本地帐户的Fallback -此设置从DCM版本19.0向前是可得到。DCM准许登录使用使用GUI，创建的GUI (本地)帐户。选项，**在服务器超时**允许对fallback对本地帐户，万一RADIUS服务器不可能被到达，并且没有，当验证失败。选项，总是**总是**允许对fallback –，既使当验证失败。

第四步：当变化应用显示的警告在镜像上显示。点击OK键，并且用户界面重新启动。

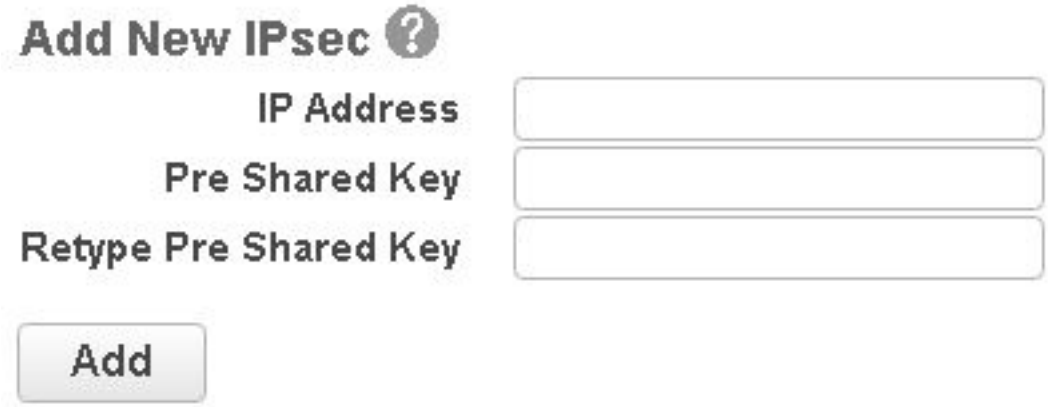
第五步：现在DCM为远程验证准备好。

配置在DCM的IPSec ：

1. 登录到DCM使用属于管理员安全组的GUI帐户。

2.导航对**Configuration > System**。系统设置页出版。

3. 参考**添加新建IPsec**地区，如镜像所显示。



4. 在IP地址字段，请输入新的IPSec对等体(RADIUS服务器)的IP地址。

5. 在**预共用的**密钥和请重新代表*预共用的密钥字段*，输入新的IPSec对等体的*预共用的密钥*。

6. 单击 **Add**。新的IPSec对等体被添加到IPsec设置表。

Note:对于IPSec的配置在RADIUS服务器运行的计算机的参考文档/出版物带有产品。

安全考虑

- 共享机密在DCM的文件系统无危险存储。
- 加密密码在DCM的内存存储用于再验证处于会话的。
- 给以上两个的项目，建议限制谁得以进入对DCM的故障排除。
- 强烈建议使用IPSec巩固在DCM和RADIUS之间的通信信道
  服务器。

限制条件和限制

- 远程验证支持只是可用的为GUI帐户，不为OS帐户。
- 再验证完成在间隔15分钟。**示例：**如果用户组更改，花费的最坏情况时间的更改采取影响是15分钟。
- 如果远程验证启用， DCM用RADIUS服务器首先检查，如果用户帐户有效或然后检查本地数据库。在使用不存在于RADIUS服务器的本地帐户的情况下有在RADIUS服务器的一个认证失败消息。

设置freeRadius

此部分显示为例如何设置freeRadius使用作为远程验证服务器DCM。这只是作为提供情报的目的，

思科不提供也不支持freeRadius。假设， freeRadius的配置文件被找到在**/etc/freeRadius/** (检查分配)下。

在安装freeRadius包修改以后这些文件。

- 修改**/etc/freeradius/clients.conf**
  步骤1.添加DCM的IP的一个条目到客户端列表。
  步骤2.Add共享密钥在客户端配置里和离开其他参数默认。

  推荐有每个DCM的一唯一共享机密。
  共享机密的长度应该是至少长22个的字符。共享机密应该是一样随机尽可能。

  一好共享机密的示例：
  “89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345’

- 修改**/etc/freeradius/radiusd.conf**更换RADIUS服务器应该侦听的端口(通常1812)
- 修改**/etc/freeradius/users**添加新用户。
- 保证添加验证信息发送对在此格式的DCM的RADIUS属性：
  <Attribute Name> = '**OU=<group_name>**'

  属性名称：这是授权数据发送对DCM group_name可以是下列之一标准RADIUS属性的名称：
  管理员-属于此组即的用户将有管理员权限完全控制。
  用户-属于此组的用户将有读写权限。
  访客-属于此组的用户将有只读权限。
  自动化-使用自动化(外部触发器)。
  dtfadmins - DTF管理员(DTF锁上配置)

  示例：
  史蒂夫明文密码：= "测试"
  过滤器ID = "OU=administrators"
- (关于)请开始RADIUS服务器使更改生效。
- 保证RADIUS服务器的防火墙配置允许对选定的外部访问
  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。

对于调试purposses一些另外的日志介绍到安全日志。为了查看此日志导航**帮助>**在DCM GUI的**跟踪页**。

此部分在日志描述怎样寻找，什么问题可能是和可能的解决方案。

记录行	失败的远程登录尝试：对RADIUS服务器的请求被计时了。
问题	DCM不能用RADIUS服务器通信。
可能的解决方案	• 验证在DCM的远程验证配置里提供的RADIUS服务器IP地址实际上正确。 • 保证RADIUS服务器从DCM是可访问。 • 保证DCM配置作为RADIUS服务器的一个有效客户端(RADIUS服务器从未知客户端静 • 保证在DCM配置的共享机密是相同的象在该特定的DCM的RADIUS服务器配置的共享 弃。)
记录行	失败的远程登录尝试：[Errno 10054]现有连接由远程主机强迫关闭。
问题	DCM发送RADIUS请求对指定的服务器IP。然而， RADIUS服务器应用程序在远程验证设 定的端口不侦听。
可能的解决方案	• 保证RADIUS服务器运行。 • 检查在服务器的RADIUS配置里指定的端口号是相同的象在DCM配置的那个。

记录行	失败的远程登录尝试：从RADIUS服务器缺少授权数据的属性名称指定的无效或答复。
问题	有与从RADIUS服务器接收的答复的一问题。
可能的解决方案	• 保证RADIUS服务器发送属性(配置在DCM)在“Access-Accept’答复。 • 保证在DCM远程验证设置配置的**属性名称**参数是确切的名字在RADIUS服务器的用户配上指定。
记录行	从RADIUS服务器接收的无效授权数据。
问题	验证成功即，但是从RADIUS服务器接收的答复包含无效授权数据安全组组名。
可能的解决方案	• 保证在是一个在部分的安全组指定的名称配置RADIUS服务器的该用户的RADIUS服务名。 • 保证在RADIUS服务器配置的字符串的格式是根据在部分指定的那个配置RADIUS服务