Configurar o Cisco DCM - Suporte à autenticação remota

Contents

Introduction

Este documento descreve o software Cisco Digital Content Manager (DCM)Autenticação remota usando RADIUS.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do software Cisco DCM versão 16 e superior.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Software Cisco DCM v16.10 e superior.
- Servidor RADIUS em execução com software de código aberto freeRadius.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

No V16.10 do DCM, foi introduzido um novo recurso que permite que as contas de utilizador configuradas num servidor RADIUS sejam utilizadas para aceder à GUI do DCM.Este documento

descreve a configuração necessária no DCM e no servidor RADIUS para utilizar este recurso.

Contas GUI no DCM

Nas versões 16.0 e abaixo, as contas de usuário necessárias para acessar a GUI eram locais para o DCM, ou seja, criadas, modificadas, usadas e excluídas no DCM.

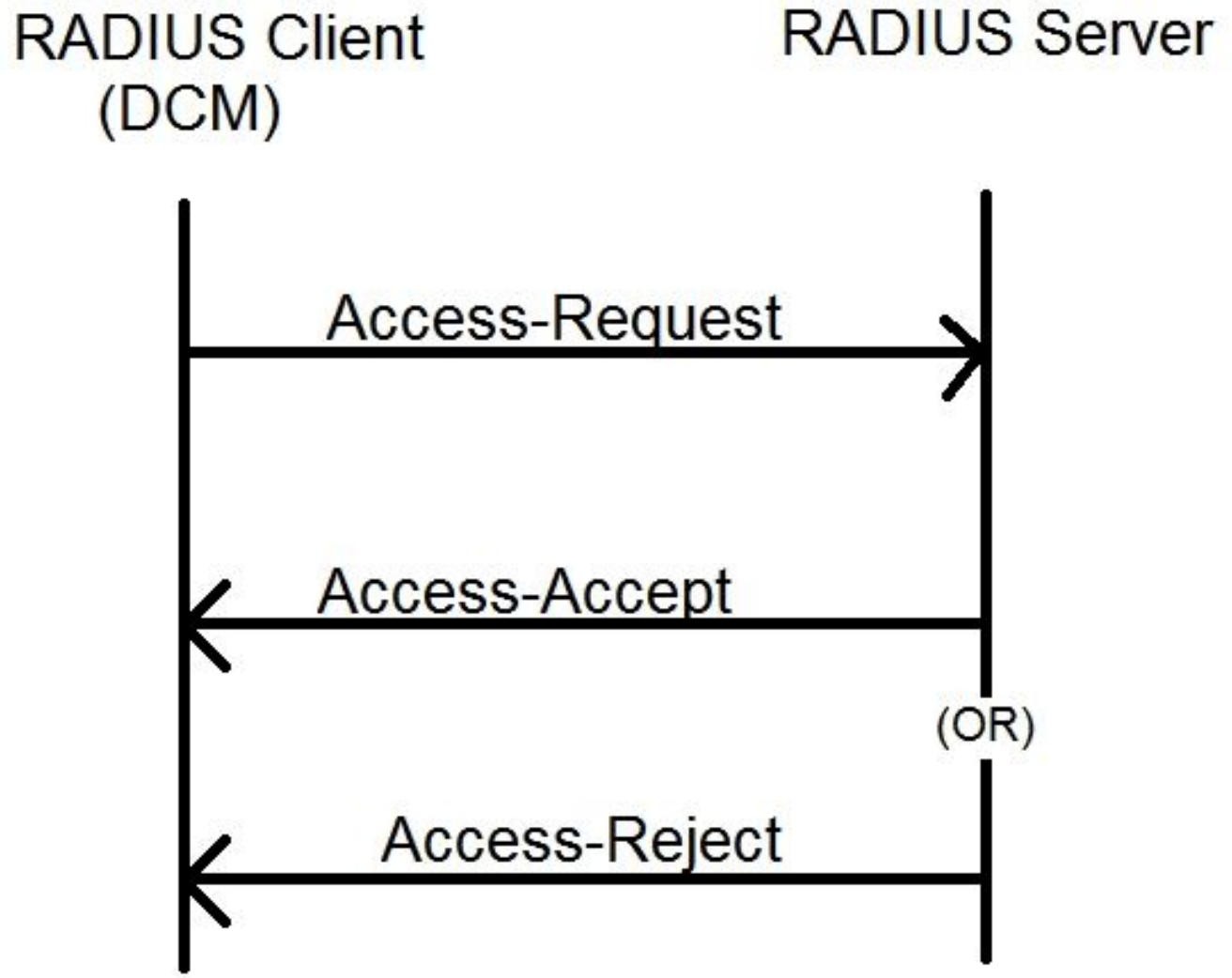
Uma conta de usuário GUI pode pertencer a um destes grupos:

- Administradores (controle total)
- Usuários (leitura e gravação)
- Convidados (somente leitura)
- Disparadores de automação (disparadores externos)
- Administradores DTF (configuração de chave DTF)

Autenticação remota

A ideia da autenticação remota é ter uma coleção centralizada de contas de usuário que podem ser usadas para acessar um dispositivo, aplicativo, serviço etc.

As etapas mostradas na imagem explicam o que acontece quando você usa a autenticação remota:



Etapa 1. O usuário insere o login e a senha (conta de usuário configurada no servidor RADIUS) na página de login na GUI do DCM.

Etapa 2. O DCM envia uma mensagem de solicitação de acesso com as credenciais para o servidor RADIUS.

Etapa 3. O servidor RADIUS verifica se a solicitação veio de um dos clientes configurados e se a conta do usuário está no seu DB/File e valida se a senha está correta ou não, após o que qualquer uma das seguintes mensagens é devolvida ao DCM

- Access-Accept - Isso significa que as credenciais são válidas. Os atributos RADIUS configurados são retornados.
- Access-Reject - Isso significa que as credenciais são inválidas e que o servidor RADIUS pode ser configurado para enviar alguns atributos RADIUS para informar a falha.
- Desafio de acesso - Isso significa que o servidor RADIUS precisa de algumas informações adicionais para validar a autenticidade do usuário. Não processado no DCM.

Caso o servidor RADIUS envie um Access-Reject, o DCM verifica se a conta do usuário é local para o próprio DCM e se o procedimento de autenticação é seguido.

O usuário é autenticado novamente em um intervalo de 15 minutos (internamente) para confirmar que o nome de usuário/senha ainda é válido e que o usuário pertence a um dos grupos de contas da GUI. Se a autenticação falhar, a sessão de usuário atual em execução será considerada inválida e todos os privilégios serão revogados para o usuário.

Configurar servidor RADIUS

Para usar as contas de usuário presentes no servidor RADIUS para acessar a GUI, estas etapas precisam ser seguidas:

O DCM deve ser configurado como um cliente para o servidor RADIUS.

1. Adicione o IP do DCM como um cliente para o servidor RADIUS.
2. Adicione o segredo compartilhado à configuração do cliente (esse segredo compartilhado deve ser o mesmo configurado no DCM, consulte seção Configuração do DCM).
3. Recomenda-se ter um segredo compartilhado diferente para cada DCM.
4. O comprimento do segredo compartilhado deve ter pelo menos 22 caracteres.
5. O segredo compartilhado deve ser o mais aleatório possível.

   Exemplo de um bom segredo compartilhado : '89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345'

Para uma conta de usuário, a mensagem Access-Accept do servidor RADIUS deve ter um atributo RADIUS que identifica o grupo de conta da GUI ao qual o usuário pertence. O nome do atributo pode ser escolhido e precisa ser configurado no arquivo de configurações no DCM.

Este é o formato da string que precisa ser enviada como um valor para um atributo do servidor RADIUS:

OU=<group_name_string> group_name_string pode ser um destes:

Grupo	Sequência de caracteres do nome do grupo
Administradores (controle total)	administradores
Usuários (leitura e gravação)	usuários
Convidados (somente leitura)	hóspedes
Disparadores de automação (externos Acionadores)	automação
DTF Administrators (Chave DTF) configuração)	dtfadmins

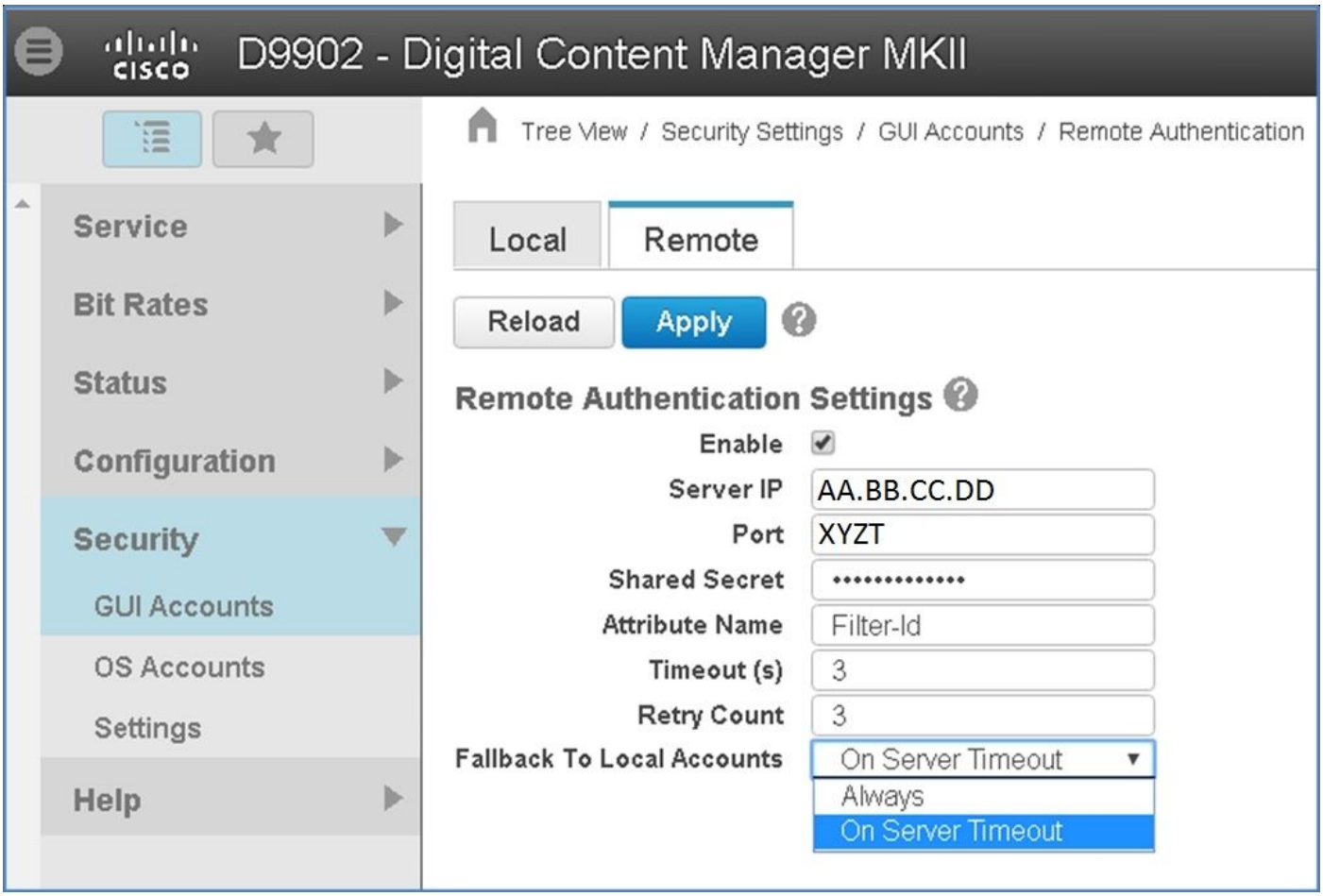
Configurar o Cisco DCM

Para ativar/configurar o recurso de autenticação remota no DCM, é necessária uma conta de

Administrador da GUI.
Estas etapas indicam como configurar a autenticação remota:

Etapa 1. Faça login no DCM usando a conta do Administrador.

Etapa 2. Navegue até **Segurança > Contas GUI** e selecione a guia **Remota**, como mostrado na imagem:



Etapa 3. Configure os parâmetros necessários para a comunicação RADIUS:

- Habilitar - Essa configuração determina se o suporte à autenticação remota deve ser habilitado ou não. Quando marcada, o restante dos campos de parâmetro é ativado.
- IP do servidor - endereço IP do servidor RADIUS.
- Porta - Porta na qual o servidor RADIUS está ouvindo pacotes de autenticação (geralmente 1812, mas pode ser configurado para outros valores).
- Segredo - Este é o segredo compartilhado usado para criptografar a senha antes de enviar o pacote RADIUS ao servidor. Esse segredo deve ser o mesmo que o configurado no servidor RADIUS onde é usado para descriptografar a senha.
- Nome do atributo - O nome do atributo no qual os dados de autorização são recebidos do servidor RADIUS.

- Timeout (em segundos) - Essa configuração é usada para comunicação entre o servidor RADIUS e o DCM. Este é o tempo que o DCM deve aguardar uma resposta do servidor RADIUS para uma solicitação específica antes de encerrar a solicitação.

- Contagem de Tentativas - Número de vezes que a solicitação RADIUS deve ser enviada caso solicitações anteriores tenham expirado.

- Fallback To Local Accounts - Esta configuração está disponível a partir da versão 19.0 do DCM. O DCM permite fazer logon usando uma conta GUI (local) criada com a GUI. Opção, **On Server Timeout** permite voltar às contas locais caso o servidor Radius não possa ser alcançado, e não quando a autenticação falhou. Opção, **sempre** permite o fallback sempre - mesmo quando a autenticação falhou.

Etapa 4. À medida que as alterações são aplicadas, o aviso mostrado na imagem é exibido. Clique em **OK** e a interface do usuário será reiniciada.

Etapa 5. Agora o DCM está pronto para autenticação remota.

Configurar IPSec no DCM:

1. Faça logon no DCM usando uma conta GUI que pertence ao grupo de segurança Administradores.

2. Navegue até **Configuração > Sistema**. A página Configurações do sistema é exibida.

3. Consulte a área **Adicionar novo IPsec**, como mostrado na imagem.

4. No campo Endereço IP, insira o endereço IP do novo peer IPsec (servidor RADIUS).

5. Nos campos **Pre Shared** key e Retype *Pre Shared Key*, insira a *Pre Shared Key* para o novo peer IPsec.

6. Clique em Add. O novo peer IPsec é adicionado à tabela de configurações de IPsec.

> **Note**: Para obter a configuração de IPSec na máquina em que o servidor RADIUS está sendo executado, consulte a documentação/publicação fornecida com o produto.

Considerações sobre segurança

- O segredo compartilhado é armazenado no modo limpo no sistema de arquivos do DCM.
- A senha criptografada é armazenada na memória do DCM para uso na reautenticação durante a sessão.
- Considerando os dois itens acima, é aconselhável limitar quem tem acesso de solução de problemas ao DCM.
- Recomenda-se usar o IPSec para proteger o canal de comunicação entre DCM e RADIUS servidor.

Restrições e limitações

- O suporte à autenticação remota está disponível apenas para as contas GUI, não para as contas do SO.
- Uma reautenticação é feita em um intervalo de 15 minutos. Exemplo: Se o grupo de um usuário tiver sido alterado, o pior caso para a alteração ter efeito é 15 minutos.
- Se a autenticação remota estiver habilitada, o DCM primeiro verifica com o servidor RADIUS se a conta de usuário é válida ou não e, em seguida, verifica o banco de dados local. No caso de usar contas locais que não existem no servidor RADIUS, haveria uma mensagem de falha de autenticação no servidor RADIUS.

Configurar o FreeRadius

Esta seção mostra como configurar freeRadius para usar como servidor de autenticação remota para o DCM. Isso é apenas para fins informativos,

A Cisco não oferece nem oferece suporte a freeRadius. Assume-se que os arquivos de configuração para freeRadius são encontrados em **/etc/freeRadius/** (verificar distribuição).

Depois de instalar o pacote freeRadius, modifique esses arquivos.

- Modifique o **/etc/freeradius/clients.conf**
  Etapa 1. Adicione uma entrada para o IP do DCM à lista de clientes.
  Etapa 2.Adicione a chave compartilhada na configuração do cliente e deixe os outros parâmetros como padrão.

  Recomenda-se ter um segredo compartilhado exclusivo para cada DCM.
  O comprimento do segredo compartilhado deve ter pelo menos 22 caracteres. O segredo compartilhado deve ser o mais aleatório possível.

  Exemplo de um bom segredo compartilhado :
  '89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345'

- Modifique o **/etc/freeradius/radiusd.conf** para alterar a porta na qual o servidor radius deve ouvir (geralmente 1812)

- Modifique os **/etc/freeradius/users** para adicionar novos usuários.

- Certifique-se de adicionar o atributo RADIUS no qual as informações de autorização são enviadas ao DCM neste formato:
  <Nome do atributo> = '**OU=<nome_do_grupo>**'

  Nome do atributo: Este é o nome do atributo RADIUS padrão no qual os dados de autorização são enviados ao nome_do_grupo DCM podem ser um dos seguintes:
  administradores - Um usuário que pertence a esse grupo terá privilégios de administrador, ou seja, controle total.
  usuários - Um usuário que pertence a esse grupo terá privilégios de leitura e gravação.
  convidados - Um usuário que pertence a esse grupo terá privilégio somente leitura.
  automação - Usada para automação (acionadores externos).
  dtfadmins - DTF Administrator (DTF Key Configuration)

  Exemplo:
  steve Cleartext-Password := "teste"
  Filter-Id = "OU=administradores"

- (Re)inicie o servidor radius para que as alterações entrem em vigor.

- Certifique-se de que a configuração de firewall do servidor radius permita o acesso externo ao
  porta.

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Para fins de depuração, alguns registros adicionais foram introduzidos no registro de segurança. Para visualizar esse log, navegue até a **página Ajuda > Rastreamentos** na GUI do DCM.

Esta seção descreve o que procurar nos registros, quais podem ser os problemas e possíveis soluções.

Linha de registro	Falha na tentativa de logon remoto: A solicitação ao servidor RADIUS expirou.
Problema	O DCM não consegue comunicar com o servidor RADIUS.
Solução possível	• Verifique se o endereço IP do servidor RADIUS fornecido na configuração de autenticação remota no DCM está realmente correto. • Certifique-se de que o servidor RADIUS está acessível a partir do DCM. • Certifique-se de que o DCM está configurado como um cliente válido no servidor RADIUS (o servidor RADIUS descarta silenciosamente os pacotes de solicitação de acesso de clientes desconhecidos). • Certifique-se de que o segredo partilhado configurado no DCM é o mesmo do segredo partilhado configurado no servidor RADIUS para esse DCM específico. (Se o servidor não possuir um segredo compartilhado para o cliente, a solicitação será removida silenciosamente.)
Linha de registro	Falha na tentativa de logon remoto: [Errno 10054] Uma conexão existente foi fechada à força pelo host remoto.
Problema	O DCM enviou uma solicitação RADIUS ao IP do servidor especificado. No entanto, o aplicativo de servidor RADIUS não está ouvindo na porta especificada nas configurações de autenticação remota.
Solução possível	• Verifique se o servidor RADIUS está em execução. • Verifique se o número da porta especificado na configuração RADIUS no servidor é igual ao número configurado no DCM.
Linha de registro	Falha na tentativa de logon remoto: Nome de atributo inválido especificado ou resposta do servidor RADIUS sem dados de autorização.
Problema	Há um problema com a resposta recebida do servidor RADIUS.
Solução possível	• Certifique-se de que o servidor RADIUS envia o atributo (configurado no DCM) na resposta "Access-Accept". • Certifique-se de que o parâmetro **Nome do Atributo** configurado nas definições de autenticação remota do DCM é o nome exato especificado na configuração do utilizador no servidor RADIUS.
Linha de registro	Dados de autorização inválidos recebidos do servidor RADIUS.
Problema	Autenticação bem-sucedida, mas a resposta recebida do servidor RADIUS contém dados de autorização inválidos, ou seja, nome do grupo de segurança.
Solução possível	• Certifique-se de que o nome do grupo configurado no servidor RADIUS para esse usuário seja um dos nomes do grupo de segurança especificados na seção Configurando o servidor RADIUS. • Certifique-se de que o formato da cadeia de caracteres configurada no servidor RADIUS esteja de acordo com o especificado na seção Configuração do servidor RADIUS.