Configurar Cisco DCM? Apoio da autenticação remota

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[O GUI explica no DCM](#)
[Autenticação remota](#)
[Configurar o servidor Radius](#)
[Configurar Cisco DCM](#)
[Considerações sobre segurança](#)
[Limitações e limitações](#)
[FreeRadius estabelecido](#)
[Troubleshooting](#)

Introdução

Este documento descreve a autenticação do softwareRemote do gerente do conteúdo digital de Cisco (DCM) usando o RAIO.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento da versão de software 16 de Cisco DCM e acima.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Software v16.10 de Cisco DCM e acima.
- Servidor Radius que é executado com software livre do freeRadius.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Informações de Apoio

Em V16.10 do DCM uns novos recursos foram introduzidos que permitissem as contas de usuário configuradas em um servidor Radius a ser usado para alcançar o documento DCM GUI.This descrevessem a instalação exigida no DCM e no servidor Radius para utilizar esta característica.

O GUI explica no DCM

Nas versões 16.0 e anterior as contas de usuário exigidas para alcançar o GUI eram locais ao DCM, isto é criaram, alterado, usado e suprimido no DCM.

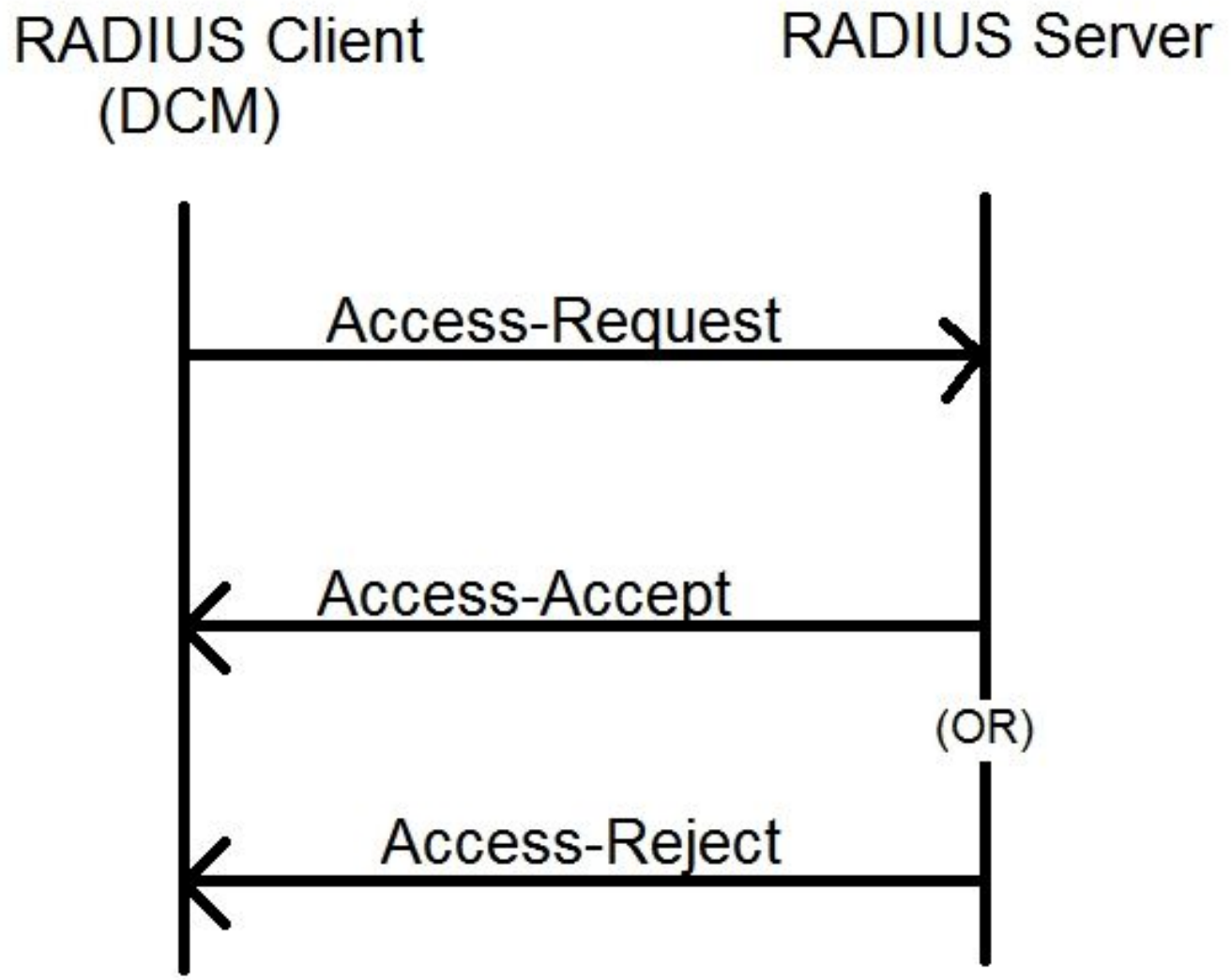
Uma conta de usuário GUI pode pertencer a um destes grupos:

- Administradores (controle total)
- Usuários (Read-Write)
- Convidados (read only)
- Disparadores da automatização (disparadores externos)
- Administradores DTF (configuração da chave DTF)

Autenticação remota

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

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



Etapa 1. O usuário incorpora o início de uma sessão e a senha (conta de usuário configurada no servidor Radius) na página de login no DCM GUI.

Etapa 2. O DCM envia uma mensagem da solicitação de acesso com as credenciais ao servidor Radius.

Etapa 3. O servidor Radius verifica se o pedido veio de um dos clientes configurados e para a existência da conta de usuário em seu DB/File e valida-o se a senha está correta ou não, depois do qual qualquer dos seguintes mensagens está retornado ao DCM

- Aceitação de acesso – Isto significa que as credenciais são válidas. Os atributos RADIUS configurados são retornados.

- Rejeição de acesso – Isto significa que as credenciais são inválidas e o servidor Radius pode ser configurado para enviar alguns atributos RADIUS para informar a falha.

- Acesso-desafio – Isto significa que o servidor Radius precisa alguma informação adicional para validar a autenticidade do usuário. Não processado no DCM.

Caso que o servidor Radius envia uma Rejeição de acesso, o DCM verifica se a conta de usuário é local ao DCM próprio e o procedimento de autenticação para aquele está seguido.

O usuário é autenticar novamente em um intervalo de 15 minutos (internamente) para confirmar que o username/senha é ainda válidos e o usuário pertence a um dos grupos de conta GUI. Se a autenticação falha a sessão do usuário running atual é julgada inválido e todos os privilégios estão revogados para o usuário.

Configurar o servidor Radius

Para usar as contas de usuário atuais no servidor Radius para alcançar estas etapas GUI precise de ser seguido:

O DCM deve ser configurado como um cliente ao servidor Radius.

1. Adicionar o IP do DCM como um cliente para o servidor Radius.

2. Adicionar o segredo compartilhado à configuração de cliente (este segredo compartilhado deve ser o mesmo que esse configurado no DCM, vê a seção configurar o DCM).

3. Recomenda-se ter um segredo compartilhado diferente para cada DCM.

4. O comprimento do segredo compartilhado deve ser pelo menos 22 caráteres por muito tempo.

5. O segredo compartilhado deve ser tão aleatório como 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 da aceitação de acesso do servidor Radius deve ter um atributo RADIUS que identifique o grupo de conta GUI a que o usuário pertence. O nome do atributo pode ser escolhido e as necessidades de ser configurado nos ajustes arquivam no DCM.

Este é o formato da corda que precisa de ser enviada como um valor para um atributo do servidor Radius:

OU=<group_name_string> que group_name_string pode ser um destes:

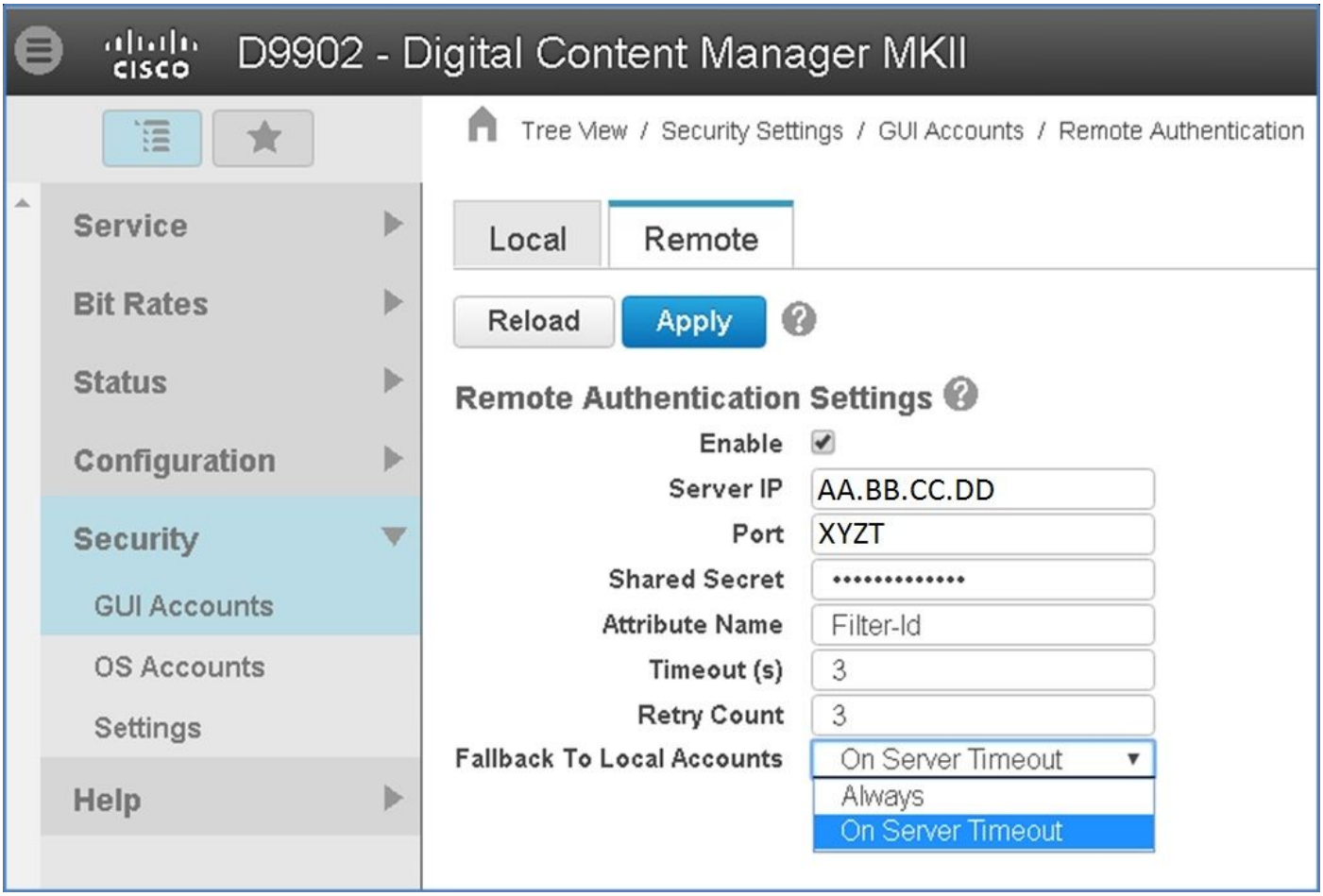
Grupo	Corda do nome do grupo
Administradores (controle total)	administradores
Usuários (Read-Write)	usuários
Convidados (read only)	convidados
Disparadores da automatização (externos Disparadores)	automatização
Administradores DTF (chave DTF configuração)	dtfadmins

Configurar Cisco DCM

Para permitir/configurar a característica da autenticação remota no DCM que uma conta de administrador GUI é exigida.
Estas etapas indicam como configurar a autenticação remota:

Etapa 1. Início de uma sessão ao DCM usando a conta de administrador.

Etapa 2. Navegue à **Segurança > às contas GUI** e selecione a aba **remota**, segundo as indicações da imagem:



Etapa 3. Configurar os parâmetros exigidos para uma comunicação do RAIO:

- Permita - Este ajuste determina se o apoio da autenticação remota for permitido ou não. Quando verificado o resto dos campos do parâmetro é permitido.
- IP de servidor - Endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius.
- Porta - Mova em qual o servidor Radius está escutando pacotes de autenticação (geralmente 1812 mas podem ser configurados a outros valores).
- Segredo - Este é o segredo compartilhado que é usado para cifrar a senha antes de enviar o pacote de informação de RADIUS ao server. Este segredo deve ser o mesmo que aquele configurado no servidor Radius onde é usado para decifrar a senha.
- Nome do atributo - O nome do atributo em que os dados da autorização são recebidos do servidor Radius.

- Intervalo (nos segundos) - Este ajuste é usado para uma comunicação entre o servidor Radius e o DCM. Este é o tempo que o DCM deve esperar uma resposta do servidor Radius para um pedido particular antes de terminar o pedido.

- Contagem de novas tentativas - O número de vezes a requisição RADIUS deve ser enviado caso que as requisições precedente são cronometradas para fora.

- Reserva às contas local - Este ajuste está disponível da versão 19.0 DCM avante. O DCM reserva entrar usando uma conta (local) GUI que seja criada usando o GUI. A opção, no **timeout de servidor** permite à reserva às contas local caso que o servidor Radius não pode ser alcançado, e não quando a autenticação falhou. A opção, permite **sempre à** reserva sempre – mesmo quando a autenticação falhou.

Etapa 4. Enquanto as mudanças são aplicadas o aviso mostrado na imagem está indicado. **A APROVAÇÃO do** clique e a interface do utilizador são reiniciadas.

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

Configurar o IPsec no DCM:

1. Entre ao DCM usando uma conta GUI que pertença ao grupo de segurança dos administradores.

2. Navegue ao **Configuration > System**. A página das configurações de sistema publica-se.

3. Refira a área **nova do IPsec adicionar**, segundo as indicações da imagem.

4. No campo do endereço IP de Um ou Mais Servidores Cisco ICM NT, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do ipsec peer novo (servidor Radius).

5. **Pre na chave compartilhada** e datilografe *pre* campos de *chave compartilhada*, incorporam *pre a chave compartilhada* para o ipsec peer novo.

6. Clique em Add. O ipsec peer novo é adicionado à tabela dos ajustes do IPsec.

> **Note**: Para a configuração do IPsec na máquina em que o servidor Radius está sendo executado refira a documentação/publicação fornecidas com o produto.

Considerações sobre segurança

- O segredo compartilhado é armazenado na claro no sistema de arquivos do DCM.
- A senha criptografada é armazenada na memória do DCM para o uso na reautenticação para a duração da sessão.
- Dado os dois artigos acima, recomenda-se para limitar quem tem o acesso do Troubleshooting ao DCM.
- Recomenda-se fortemente para usar o IPsec para fixar o canal de comunicação entre o DCM e o RAIO
  server.

Limitações e limitações

- O apoio da autenticação remota está somente disponível para as contas GUI, não para as contas do OS.
- Uma reautenticação é feita em um intervalo de 15 minutos. Exemplo: Se um grupo de usuário foi mudado, o momento do pior caso tomado para que a mudança tome a influência é 15 minutos.
- Se a autenticação remota é permitida, as primeiras verificações DCM com o servidor Radius se a conta de usuário é válida ou verificam não e então no base de dados local. Em caso de usar as contas local que não existem no servidor Radius haveria uma mensagem da falha de autenticação no servidor Radius.

FreeRadius estabelecido

Esta seção mostra como um exemplo como setup o freeRadius para usar-se como o server da autenticação remota para o DCM. Isto é apenas para fins informativos,

Cisco não fornece nem apoia o freeRadius. Supõe-se que os arquivos de configuração para o

freeRadius estão encontrados sob **/etc/freeRadius/** (distribuição da verificação).

Após ter instalado o pacote do freeRadius altere estes arquivos.

- Altere **/etc/freeradius/clients.conf**
  Etapa 1. Adicionar uma entrada para o IP do DCM à lista de clientes.
  A etapa 2.Add a chave compartilhada na configuração de cliente e sae dos outros parâmetros para optar.

  Recomenda-se ter um segredo compartilhado original para cada DCM.
  O comprimento do segredo compartilhado deve ser pelo menos 22 caráteres por muito tempo. O segredo compartilhado deve ser tão aleatório como possível.

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

- Altere **/etc/freeradius/radiusd.conf** para mudar a porta em que o servidor Radius deve escutar (geralmente 1812)

- Altere **/etc/freeradius/users** para adicionar novos usuários.

- Assegure para adicionar o atributo RADIUS em que a informação de autorização é enviada ao DCM neste formato:
  <Attribute Name> = “**OU=<group_name>”**

  Nome do atributo: Este é o nome do atributo de RADIUS padrão em que os dados da autorização são enviados ao group_name DCM podem ser um do seguinte:
  administradores - Um usuário que pertença a este grupo terá o controle total dos privilégios do administrado isto é.
  usuários - Um usuário que pertença a este grupo terá privilégios de leitura/gravação.
  convidados - Um usuário que pertença a este grupo terá o privilégio do read only.
  automatização - Usado para a automatização (disparadores externos).
  dtfadmins - Administrador DTF (configuração da chave DTF)

  Exemplo:
  senha de texto claro de steve: = “testes”
  ID de filtro = “OU=administrators”

- (Com referência a) ligue o servidor Radius para que as mudanças tomem o efeito.

- Assegure-se de que a configuração de firewall do servidor Radius permita o acesso externo ao escolhido
  porta.

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Para debugar purposses alguns logs adicionais foram introduzidos no registro de segurança. A fim ver este log navegue **para ajudar > página dos traços em** DCM GUI.

Esta seção descreve o que procurar nos logs, o que as edições poderiam ser e soluções possíveis.

Linha de registro	Tentativa do login remoto falhada: O pedido ao servidor Radius foi cronometrado para fora.
Problema	O DCM não pode comunicar-se com o servidor Radius.
Solução possível	• Verifique que o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius fornecido na configuração da autenticação remota no DCM está realmente correto. • Assegure-se de que o servidor Radius esteja acessível do DCM. • Assegure-se de que o DCM esteja configurado como um cliente válido no servidor Radius servidor Radius deixa cair silenciosamente pacotes de solicitação de acesso dos clientes desconhecidos). • Assegure-se de que o segredo compartilhado configurado no DCM seja o mesmo que o segredo compartilhado configurado no servidor Radius para esse DCM particular. (Se o server não possui um segredo compartilhado para o cliente, o pedido é deixado cair silenciosamente.)
Linha de registro	Tentativa do login remoto falhada: [O errno 10054] uma conexão existente foi fechado forçosamente pelo host remoto.
Problema	O DCM enviou uma requisição RADIUS ao IP de servidor especificado. Contudo, o aplicativo c servidor Radius escutando na porta não está sendo especificado nos ajustes da autenticação remota.
Solução possível	• Assegure-se de que o servidor Radius esteja sendo executado. • Certifique-se do número de porta especificado na configuração RADIUS no server seja o mesmo que esse configurado no DCM.
Linha de registro	Tentativa do login remoto falhada: Nome inválido do atributo especificado ou resposta dos dados faltantes da autorização do servidor Radius.
Problema	Há um problema com a resposta recebida do servidor Radius.
Solução possível	• Assegure-se de que o servidor Radius envie o atributo (configurado no DCM) na resposta da “aceitação de acesso”. • Assegure-se de que o parâmetro do **nome do atributo** configurado nos ajustes da autenticação remota DCM seja o nome exato como especificado na configuração do usuár no servidor Radius.
Linha de registro	Dados inválidos da autorização recebidos do servidor Radius.
Problema	A autenticação sucedeu mas a resposta recebida do servidor Radius contém o nome de grupo de segurança inválido dos dados da autorização isto é.
Solução possível	• Assegure-se de que o nome do grupo configurado no servidor Radius para esse usuário seja um do nome de grupo de segurança especificado na seção que configura o servidor

Radius.

- Assegure-se de que o formato da corda configurada no servidor Radius de acordo com essa esteja especificado na seção que configura o servidor Radius.