¿Configuración Cisco DCM? Soporte de la autenticación remota

Contenido

Introducción

Este documento describe la autenticación del softwareRemote del Administrador de contenido de Cisco Digital (DCM) usando el RADIUS.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento de la versión de software 16 de Cisco DCM y arriba.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Software v16.10 de Cisco DCM y arriba.
- Servidor de RADIUS que se ejecuta con el software libre del freeRadius.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Antecedentes

En V16.10 del DCM se ha introducido una nueva función que permite las cuentas de usuario configuradas en un servidor de RADIUS que se utilizará para acceder el documento DCM GUI.This describe la configuración requerida en el DCM y el servidor de RADIUS para hacer uso de esta característica.

El GUI considera en el DCM

En las versiones 16.0 y debajo de las cuentas de usuario requeridas para acceder el GUI eran local al DCM, es decir creó, modificado, utilizado y borrado en el DCM.

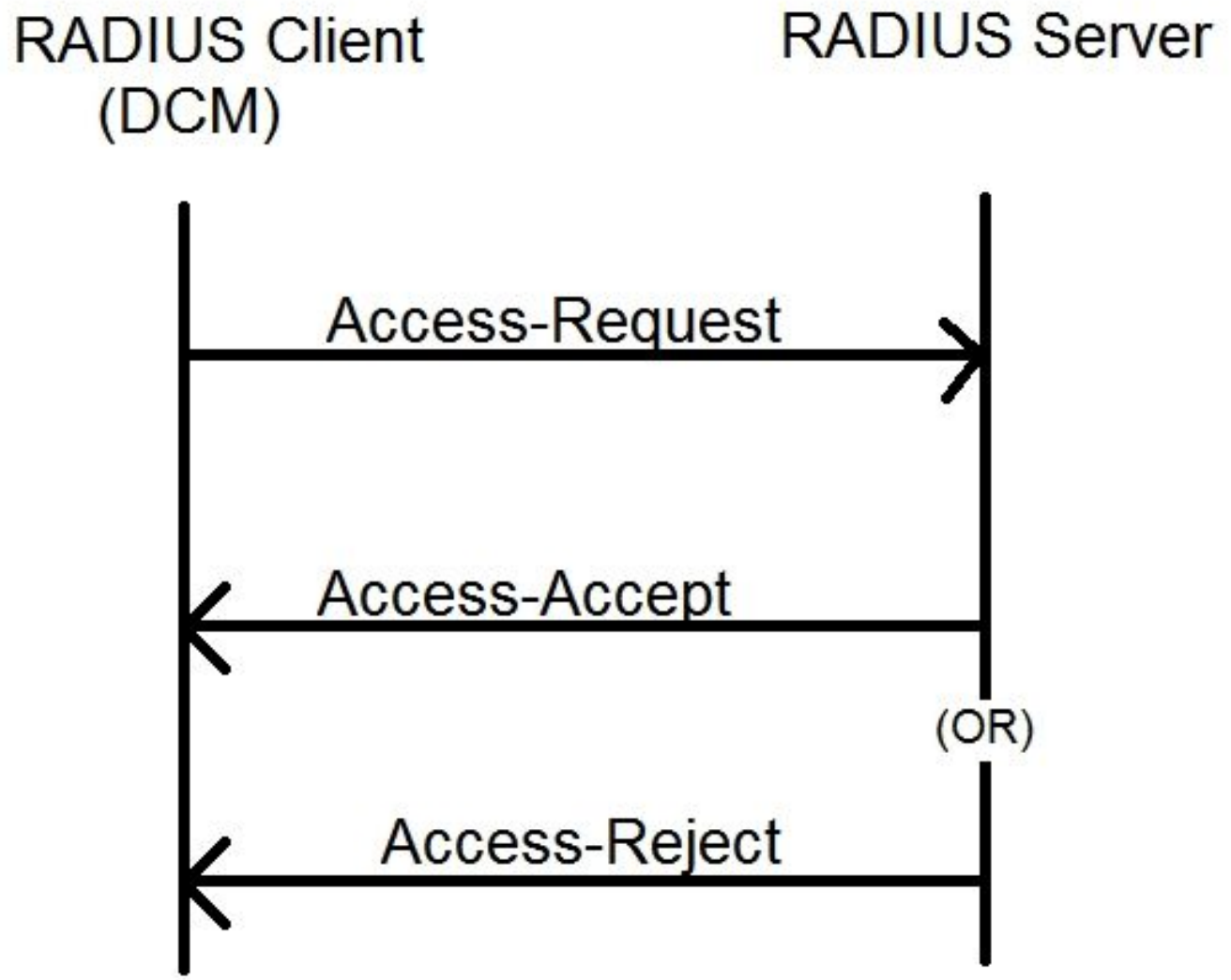
Una cuenta de usuarios de GUI puede pertenecer a uno de estos grupos:

- Administradores (control total)
- Usuarios (Read-Write)
- Invitados (read only)
- Activadores de la automatización (disparadores externos)
- Administradores DTF (configuración de la clave DTF)

Autenticación remota

La idea de la autenticación remota es tener una colección centralizada de cuentas de usuario que se puedan utilizar para acceder un dispositivo, una aplicación, un servicio etc.

Los pasos mostrados en la imagen explican qué sucede cuando usted utiliza la autenticación remota:



Paso 1. El usuario ingresa el login y la contraseña (cuenta de usuario configurada en el servidor de RADIUS) en la página de registro en el DCM GUI.

Paso 2. El DCM envía un mensaje del pedido de acceso con las credenciales al servidor de RADIUS.

Paso 3. El servidor de RADIUS marca si la petición ha venido a partir de la una de los clientes configurados y para la existencia de la cuenta de usuario en su DB/File y valida si la contraseña está correcta o no, después de lo cual de los siguientes mensajes se devuelve al DCM

- Access-accept – Esto significa que las credenciales son válidas. Se vuelven los atributos de RADIUS configurados.
- Access-Reject – Esto significa que las credenciales son inválidas y el servidor de RADIUS puede ser configurado para enviar algunos atributos de RADIUS para informar al error.
- Acceso-desafío – Esto significa que el servidor de RADIUS necesita una cierta información adicional para validar la autenticidad del usuario. No procesado en el DCM.

En caso de que el servidor de RADIUS envíe un Access-Reject, el DCM marca si la cuenta de usuario es local al DCM sí mismo y el procedimiento de autenticación para ése se sigue.

Reautentifican al usuario en un intervalo de 15 minutos (internamente) para confirmar que el nombre de usuario/la contraseña es todavía válidos y el usuario pertenece a uno de los grupos de cuenta GUI. Si la autenticación falla a la sesión del usuario corriente actual se juzga inválido y todos los privilegios se revocan para el usuario.

Servidor de RADIUS de la configuración

Para utilizar las cuentas de usuario presentes en el servidor de RADIUS para acceder los estos pasos GUI necesite ser seguido:

El DCM se debe configurar como cliente al servidor de RADIUS.

1. Agregue el IP del DCM como cliente para el servidor de RADIUS.
2. Agregue el secreto compartido a la configuración del cliente (este secreto compartido debe ser lo mismo que el que está configurado en el DCM, ve la sección el configurar del DCM).
3. Se recomienda para tener un diverso secreto compartido para cada DCM.
4. La longitud del secreto compartido debe ser por lo menos 22 caracteres de largo.
5. El secreto compartido debe ser tan al azar como sea posible.

   Ejemplo de un buen secreto compartido: “89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345”

Para una cuenta de usuario el mensaje del access-accept del servidor de RADIUS debe tener un atributo de RADIUS que identifique al grupo de cuenta GUI a quien el usuario pertenece. El nombre del atributo se puede elegir y las necesidades de ser configurado en el archivo de configuración en el DCM.

Éste es el formato de la cadena que necesita ser enviada como valor para un atributo del servidor de RADIUS:

OU=<group_name_string> group_name_string puede ser uno de éstos:

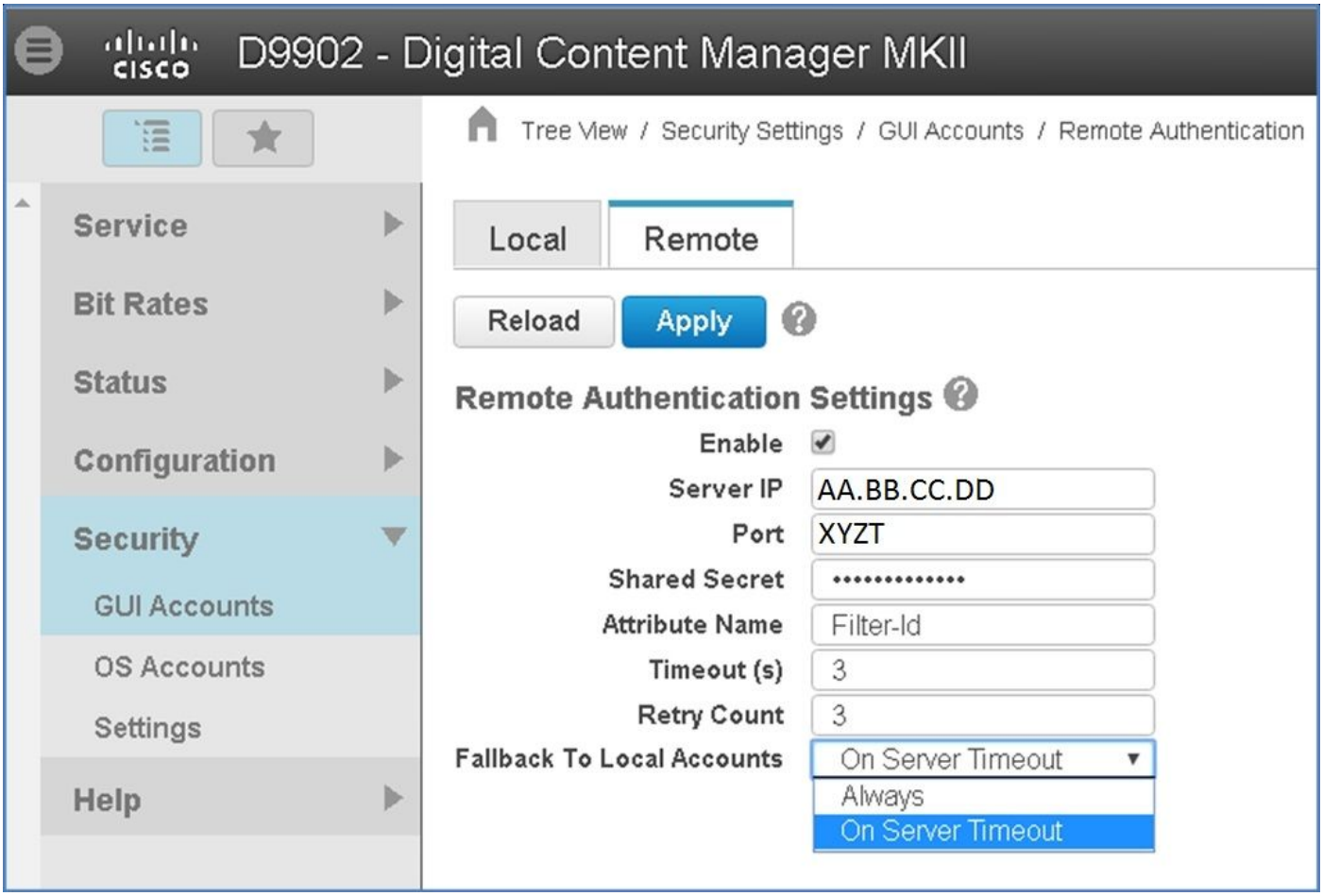
Grupo	Cadena del nombre del grupo
Administradores (control total)	administradores
Usuarios (Read-Write)	usuarios
Invitados (read only)	invitados
Activadores de la automatización (externo Activadores)	automatización
Administradores DTF (clave DTF configuración)	dtfadmins

Configuración Cisco DCM

Para habilitar/la característica de la autenticación remota de la configuración en el DCM una cuenta del administrador GUI se requiere.
Estos pasos indican cómo configurar la autenticación remota:

Paso 1. Login al DCM usando la cuenta del administrador.

Paso 2. Navegue a la **Seguridad > a las cuentas GUI** y a la lengueta **remota** selecta, tal y como se muestra en de la imagen:



Paso 3. Configure los parámetros requeridos para la comunicación RADIUS:

- Habilite - Esta configuración determina si se habilita el soporte de la autenticación remota o no. Cuando está marcado el resto de los campos del parámetro se habilita.
- IP del servidor - Dirección IP del servidor de RADIUS.
- Puerto - Vire hacia el lado de babor en cuál está estando atentos el servidor de RADIUS los paquetes de autenticación (generalmente 1812 pero se pueden configurar a otros valores).
- Secreto - Éste es el secreto compartido que se utiliza para cifrar la contraseña antes de enviar el paquete RADIUS al servidor. Este secreto debe ser lo mismo que eso configurada en el servidor de RADIUS donde se utiliza para desencriptar la contraseña.
- Nombre del atributo - El nombre del atributo en el cual los datos de la autorización se reciben del servidor de RADIUS.

- Descanso (en los segundos) - Esta configuración se utiliza para la comunicación entre el servidor de RADIUS y el DCM. Éste es el tiempo que el DCM debe esperar una respuesta del servidor de RADIUS para una petición determinada antes de terminar la petición.

- Cuenta de reintentos - La cantidad de veces el pedido de RADIUS debe ser enviada en caso de que los pedidos anteriores se midan el tiempo hacia fuera.

- Retraso a las cuentas locales - Esta configuración es disponible desde versión 19.0 DCM hacia adelante. El DCM permite abrir una sesión usando una cuenta (local) GUI que se cree usando el GUI. La opción, **en el tiempo de espera del servidor** permite al retraso a las cuentas locales en caso de que el servidor de RADIUS no pueda ser alcanzado, y no cuando la autenticación falló. La opción, permite **siempre al** retraso siempre – incluso cuando la autenticación falló.

Paso 4. Mientras que se aplican los cambios la advertencia mostrada en la imagen se visualiza. Se recomienza el Haga Click en OK y la interfaz de usuario.

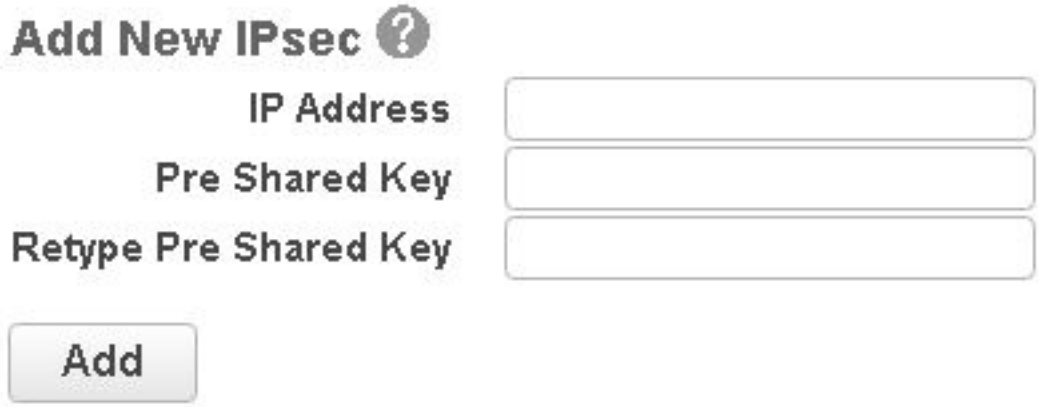
Paso 5. El DCM está listo ahora para la autenticación remota.

IPSec de la configuración en el DCM:

1. Inicio al DCM usando una cuenta GUI que pertenece al grupo de seguridad de los administradores.

2. Navegue a **Configuration > System**. La página de los ajustes de sistema aparece.

3. Refiera a la **nueva** área del **IPSec del agregar**, tal y como se muestra en de la imagen.



4. En el campo del IP Address, ingrese el IP Address del nuevo peer IPSec (servidor de RADIUS).

5. En **pre la clave compartida** y escriba de nuevo *pre los* campos de *clave compartida a máquina*, ingresan *pre la clave compartida* para el nuevo peer IPSec.

6. Haga clic en Add (Agregar). Agregan al nuevo peer IPSec a la tabla de las configuraciones del IPSec.

> **Note**: Para la configuración del IPSec en la máquina en la cual el servidor de RADIUS se está ejecutando refiera a la documentación/a la publicación proporcionadas el producto.

Observaciones de seguridad

- El secreto compartido se salva en el claro en el sistema de archivos del DCM.
- La contraseña encriptada se salva en la memoria del DCM para el uso en la reautentificación para la duración de la sesión.
- Dado los dos elementos arriba, se aconseja para limitar quién tiene acceso del troubleshooting al DCM.
- Se aconseja fuertemente para utilizar el IPSec para asegurar el canal de comunicación entre el DCM y el RADIUS
  servidor.

Apremios y limitaciones

- El soporte de la autenticación remota está solamente disponible para las cuentas GUI, no para las cuentas OS.
- Una reautentificación se hace en un intervalo de 15 minutos. Ejemplo: Si han cambiado a un grupo de usuario, la época del peor caso llevada para que el cambio tome la influencia es 15 minutos.
- Si se habilita la autenticación remota, las en primer lugar controles DCM con el servidor de RADIUS si la cuenta de usuario es válida o no y después comprueban la base de datos local.

En caso de usar las cuentas locales que no existen en el servidor de RADIUS habría un mensaje de la falla de autenticación en el servidor de RADIUS.

FreeRadius de la configuración

Esta sección muestra como un ejemplo cómo poner el freeRadius para utilizar como servidor de la autenticación remota para el DCM. Esto está sólo con fines informativos,

Cisco no proporciona ni soporta el freeRadius. Se asume que los archivos de configuración para el freeRadius están encontrados bajo **/etc/freeRadius/** (distribución del control).

Después de instalar el paquete del freeRadius modifique estos archivos.

- Modifique **/etc/freeradius/clients.conf**
  Paso 1. Agregue una entrada para el IP del DCM a la lista de clientes.
  El paso 2.Add la clave compartida en la configuración del cliente y sale de los otros parámetros para omitir.

  Se recomienda para tener un secreto compartido único para cada DCM.
  La longitud del secreto compartido debe ser por lo menos 22 caracteres de largo. El secreto compartido debe ser tan al azar como sea posible.

  Ejemplo de un buen secreto compartido:
  “89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345”

- Modifique **/etc/freeradius/radiusd.conf** para cambiar el puerto en el cual el servidor de RADIUS debe escuchar (generalmente 1812)

- Modifique **/etc/freeradius/users** para agregar a los usuarios nuevos.

- Asegure para agregar el atributo de RADIUS en el cual la información de autorización se envía al DCM en este formato:
  Name> del <Attribute = “**OU=<group_name>”**

  Nombre del atributo: Éste es el nombre del atributo RADIUS estándar en el cual los datos de la autorización se envían al group_name DCM pueden ser uno del siguiente:
  administradores - Un usuario que pertenece a este grupo tendrá control total de los privilegios de administrador es decir.
  usuarios - Un usuario que pertenece a este grupo tendrá privilegios de lectura/grabación.
  invitados - Un usuario que pertenece a este grupo tendrá privilegio del read only.
  automatización - Utilizado para la automatización (disparadores externos).
  dtfadmins - Administrador DTF (configuración de la clave DTF)

  Ejemplo:
  contraseña de texto sin cifrar de steve: = “prueba”

Id del filtro = “OU=administrators”

- (Con referencia a) encienda al servidor de RADIUS para que los cambios tomen el efecto.
- Asegúrese de que la configuración de escudo de protección del servidor de RADIUS permita el acceso externo al elegido
  puerto.

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Para hacer el debug de los purposses algunos registros adicionales se han introducido en el registro de seguridad. Para ver este registro navegue **para ayudar > página de las trazas** en DCM GUI.

Esta sección describe qué buscar en los registros, qué los problemas podrían ser y las Soluciones posibles.

Línea del registro	Tentativa del registro remoto fallada: La petición al servidor de RADIUS fue medida el tiempo hacia fuera.
Problema	El DCM no puede comunicar con el servidor de RADIUS.
Soluciones posibles	• Verifique que la dirección IP del servidor de RADIUS proporcionada en la configuración d la autenticación remota en el DCM esté realmente correcta. • Asegúrese de que el servidor de RADIUS sea accesible del DCM. • Asegúrese de que el DCM esté configurado como cliente válido en el servidor de RADIUS (el servidor de RADIUS cae silenciosamente los paquetes access-request de los clientes desconocidos). • Asegúrese de que el secreto compartido configurado en el DCM sea lo mismo que el secreto compartido configurado en el servidor de RADIUS para ese DCM determinado. (S el servidor no posee un secreto compartido para el cliente, la petición se cae silenciosamente.)
Línea del registro	Tentativa del registro remoto fallada: [El errno 10054] una conexión existente fue cerrado fuertemente por el host remoto.
Problema	El DCM ha enviado un pedido de RADIUS al especificado IP del servidor. Sin embargo, la aplicación de servidor de RADIUS escuchando en el puerto no se está especificando en las configuraciones de la autenticación remota.
Soluciones posibles	• Asegúrese de que el servidor de RADIUS se esté ejecutando. • Marque que el número del puerto especificado en la configuración de RADIUS en el servidor es lo mismo que el que está configurado en el DCM.
Línea del registro	Tentativa del registro remoto fallada: Nombre inválido del atributo especificado o respuesta de los datos que falta de la autorización del servidor de RADIUS.
Problema	Hay un problema con la respuesta recibida del servidor de RADIUS.
Soluciones	• Asegúrese de que el servidor de RADIUS envíe el atributo (configurado en el DCM) en la

	respuesta del “access-accept”.
posibles	• Asegúrese de que el parámetro del **nombre del atributo** configurado en las configuracione de la autenticación remota DCM sea el nombre exacto como se especifica en la configuración de usuario en el servidor de RADIUS.
Línea del registro	Datos inválidos de la autorización recibidos del servidor de RADIUS.
Problema	La autenticación tuvo éxito pero la respuesta recibida del servidor de RADIUS contiene el nombre de grupo de seguridad inválido de los datos de la autorización es decir.
Soluciones posibles	• Asegúrese de que el nombre del grupo configurado en el servidor de RADIUS para ese usuario sea uno del nombre de grupo de seguridad especificado en la sección que configura al servidor de RADIUS. • Asegúrese de que el formato de la cadena configurada en el servidor de RADIUS según la esté especificado en la sección que configura al servidor de RADIUS.