Configuración de Cisco DCM - Soporte de autenticación remota

Contenido

Introducción

Este documento describe el software Cisco Digital Content Manager (DCM) Autenticación remota mediante RADIUS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de la versión 16 y posteriores del software Cisco DCM.

Componentes Utilizados

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

- Software Cisco DCM v16.10 y posterior.
- Servidor RADIUS que se ejecuta con software de código abierto 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En V16.10 del DCM se ha introducido una nueva función que permite utilizar las cuentas de usuario configuradas en un servidor RADIUS para acceder a la GUI de DCM.Este documento

describe la configuración requerida en el DCM y el servidor RADIUS para hacer uso de esta función.

Cuentas GUI en DCM

En las versiones 16.0 y posteriores, las cuentas de usuario necesarias para acceder a la GUI eran locales al DCM, es decir, creadas, modificadas, utilizadas y eliminadas en el DCM.

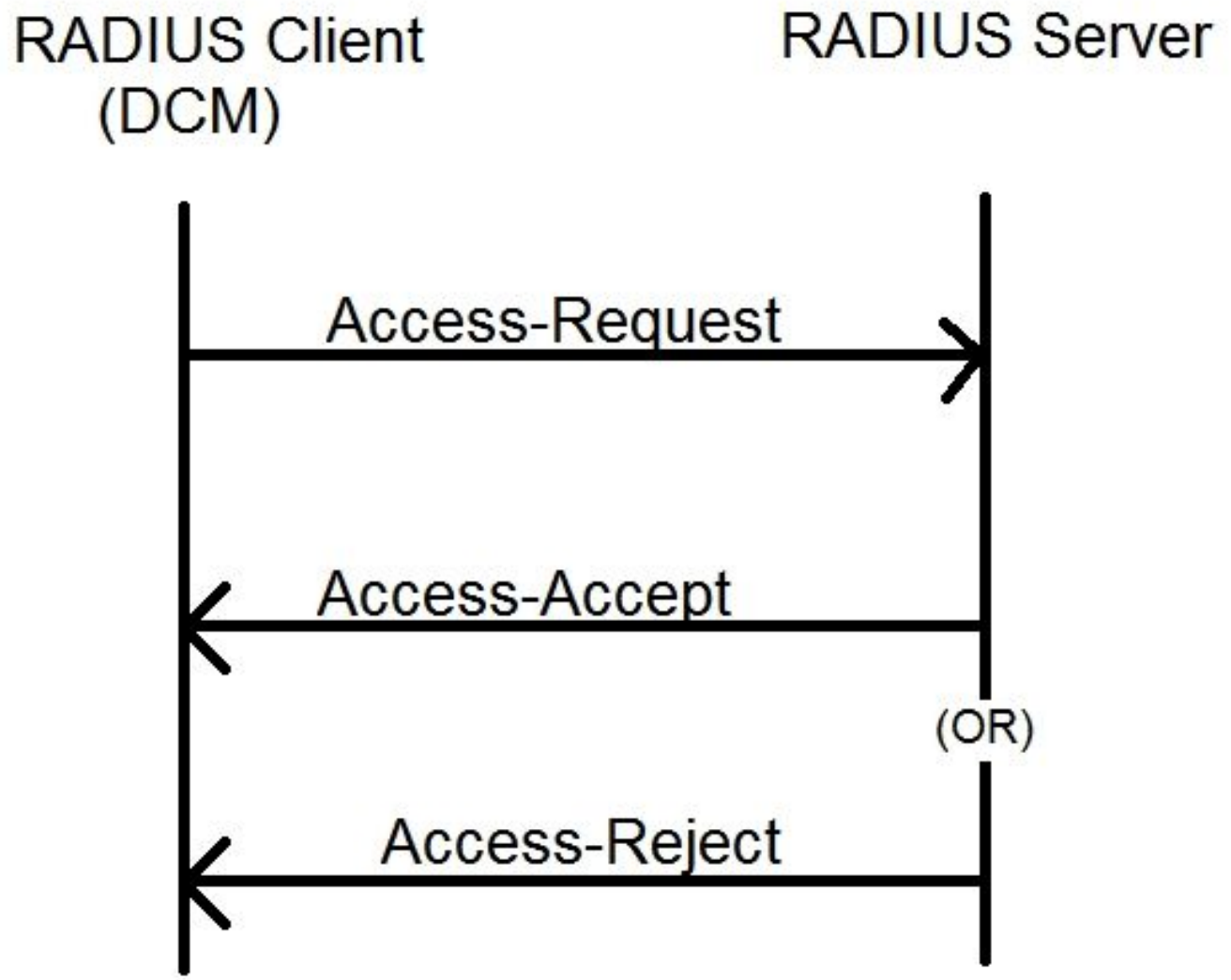
Una cuenta de usuario de GUI puede pertenecer a uno de estos grupos:

- Administradores (control completo)
- Usuarios (lectura y escritura)
- Invitados (sólo lectura)
- Activadores de automatización (disparadores externos)
- Administradores DTF (configuración de clave DTF)

Autenticación remota

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

Los pasos que se muestran en la imagen explican lo que sucede cuando se utiliza la autenticación remota:



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

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

Paso 3. El servidor RADIUS verifica si la solicitud proviene de uno de los clientes configurados y si existe la cuenta de usuario en su DB/Archivo y valida si la contraseña es correcta o no, después de lo cual se devuelve cualquiera de los siguientes mensajes al DCM

- Access-Accept (Aceptar acceso): significa que las credenciales son válidas. Se devuelven los atributos RADIUS configurados.
- Access-Reject - Esto significa que las credenciales no son válidas y el servidor RADIUS puede configurarse para enviar algunos atributos RADIUS para informar la falla.
- Reto de acceso: esto significa que el servidor RADIUS necesita información adicional para validar la autenticidad del usuario. No procesado en el DCM.

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

El usuario se vuelve a autenticar en un intervalo de 15 minutos (internamente) para confirmar que el nombre de usuario/la contraseña sigue siendo válido y que el usuario pertenece a uno de los grupos de cuentas de la GUI. Si la autenticación falla, la sesión de usuario actual se considera no válida y todos los privilegios se revocan para el usuario.

Configurar servidor RADIUS

Para utilizar las cuentas de usuario presentes en el servidor RADIUS para acceder a la GUI, deben seguirse estos pasos:

DCM se debe configurar como cliente para el servidor RADIUS.

1. Agregue la IP del DCM como cliente para el servidor RADIUS.
2. Agregue el secreto compartido a la configuración del cliente (este secreto compartido debe ser el mismo que el configurado en el DCM, consulte la sección Configuración del DCM).
3. Se recomienda tener un secreto compartido diferente para cada DCM.
4. La longitud del secreto compartido debe ser de al menos 22 caracteres.
5. El secreto compartido debe ser lo más aleatorio 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 Access-Accept del servidor RADIUS debe tener un atributo RADIUS que identifique el grupo de cuentas GUI al que pertenece el usuario. Se puede elegir el nombre del atributo y debe configurarse en el archivo de configuración del DCM.

Este es el formato de la cadena que debe enviarse como valor para un atributo desde el servidor RADIUS:

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

Grupo	Cadena de nombre de grupo
Administradores (control completo)	administradores
Usuarios (lectura y escritura)	usuarios
Invitados (sólo lectura)	invitados
Activadores de automatización (externos Disparadores)	automatización
Administradores DTF (Clave DTF) configuración)	dtfadmins

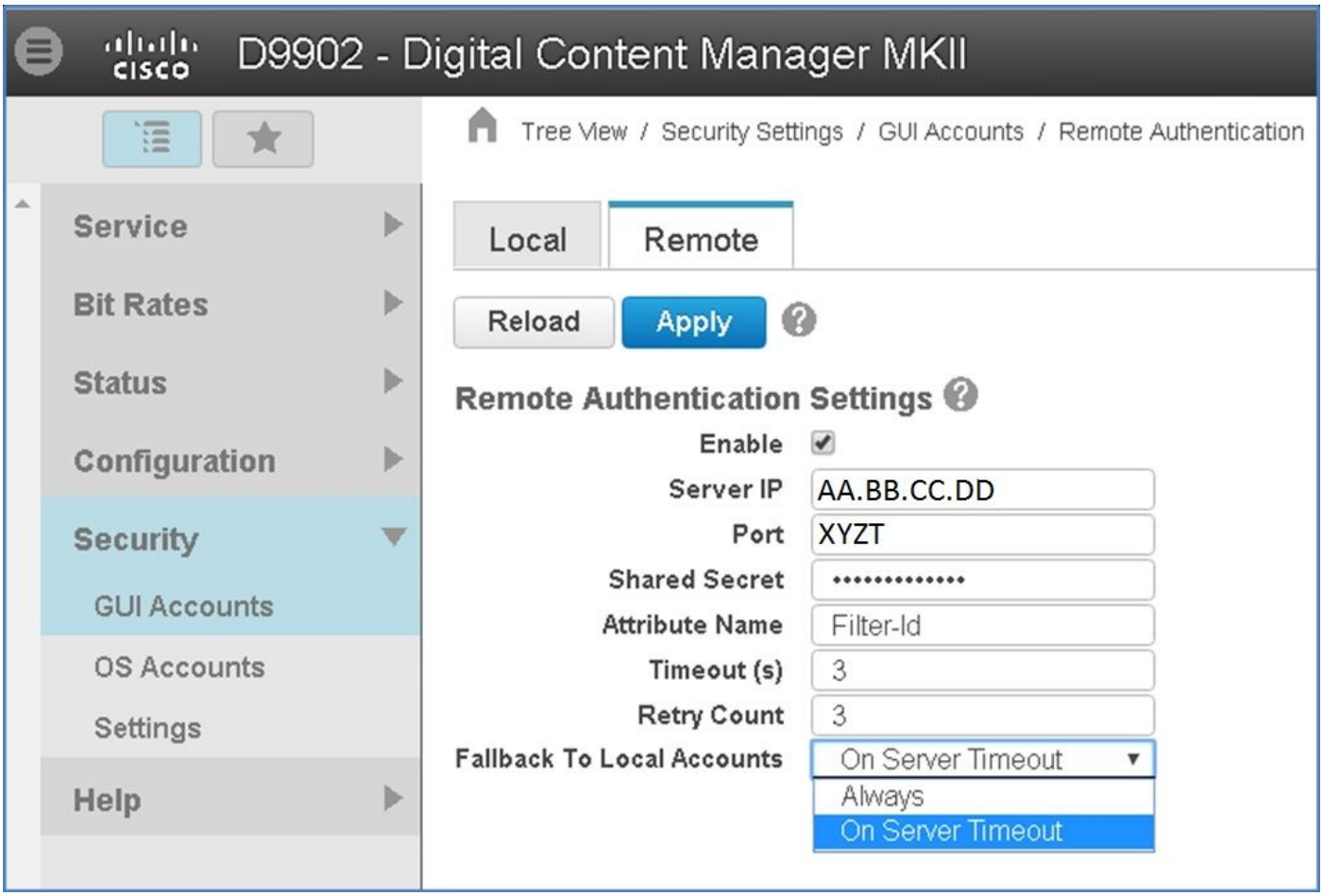
Configuración de Cisco DCM

Para habilitar/configurar la función de autenticación remota en el DCM, se requiere una cuenta de

administrador de GUI.
Estos pasos indican cómo configurar la autenticación remota:

Paso 1. Inicie sesión en DCM con la cuenta de administrador.

Paso 2. Navegue hasta **Seguridad > Cuentas GUI** y seleccione la **pestaña remota**, como se muestra en la imagen:



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

- Enable (Activar): Esta configuración determina si se debe activar o no el soporte de autenticación remota. Cuando se marca, se habilita el resto de los campos de parámetro.
- IP del servidor: dirección IP del servidor RADIUS.
- Puerto: puerto en el que el servidor RADIUS escucha los paquetes de autenticación (generalmente 1812 pero se puede configurar para otros valores).
- Secreto - Este es el secreto compartido que se utiliza para cifrar la contraseña antes de enviar el paquete RADIUS al servidor. Este secreto debe ser el mismo que el configurado en el servidor RADIUS donde se utiliza para descifrar la contraseña.
- Nombre de atributo: el nombre del atributo en el que se reciben los datos de autorización del servidor RADIUS.

- Tiempo de espera (en segundos): esta configuración se utiliza para la comunicación entre el servidor RADIUS y DCM. Este es el momento en que el DCM debe esperar una respuesta del servidor RADIUS para una solicitud determinada antes de terminar la solicitud.

- Recuento de reintentos: número de veces que se debe enviar la solicitud RADIUS en caso de que se agote el tiempo de espera de las solicitudes anteriores.

- Reserva a cuentas locales - Esta configuración está disponible desde la versión 19.0 de DCM en adelante. El DCM permite iniciar sesión mediante una cuenta GUI (local) creada mediante la GUI. Opción, **On Server Timeout** permite realizar un repliegue en las cuentas locales en caso de que no se pueda alcanzar el servidor Radius, y no cuando la autenticación falló. Opción, **Siempre** permite retroceder siempre, incluso cuando se produce un error en la autenticación.

Paso 4. A medida que se aplican los cambios, se muestra la advertencia mostrada en la imagen. Haga clic en **Aceptar** y se reiniciará la interfaz de usuario.

Paso 5. Ahora el DCM está listo para la autenticación remota.

Configuración de IPSec en DCM:

1. Inicie sesión en el DCM mediante una cuenta GUI que pertenece al grupo de seguridad Administradores.

2. Vaya a **Configuration > System**. Aparecerá la página Configuración del sistema.

3. Consulte el área **Add New IPsec**, como se muestra en la imagen.

4. En el campo IP Address (Dirección IP), introduzca la dirección IP del nuevo par IPsec (servidor RADIUS).

5. En los campos **Pre Shared** key y Retype *Pre Shared Key*, ingrese la *Pre Shared Key* para el nuevo peer IPSec.

6. Haga clic en Add (Agregar). El nuevo par IPSec se agrega a la tabla IPsec Settings.

> **Nota:** Para la configuración de IPSec en la máquina en la que se ejecuta el servidor RADIUS, consulte la documentación/publicación proporcionada con el producto.

Observaciones de seguridad

- El secreto compartido se almacena en el claro en el sistema de archivos del DCM.
- La contraseña cifrada se almacena en la memoria del DCM para su uso en la reautenticación durante la sesión.
- Teniendo en cuenta los dos elementos anteriores, se recomienda limitar quién tiene acceso a DCM para la resolución de problemas.
- Se recomienda encarecidamente utilizar IPSec para proteger el canal de comunicación entre DCM y RADIUS
  servidor.

Restricciones y limitaciones

- El soporte de autenticación remota sólo está disponible para las cuentas GUI, no para las cuentas del sistema operativo.
- La reautenticación se realiza a un intervalo de 15 minutos. Ejemplo: Si se ha cambiado el grupo de un usuario, el peor de los casos en el que se produce el cambio es de 15 minutos.
- Si se habilita la autenticación remota, el DCM primero verifica con el servidor RADIUS si la cuenta de usuario es válida o no y luego verifica en la base de datos local. En caso de utilizar cuentas locales que no existen en el servidor RADIUS, habría un mensaje de error de autenticación en el servidor RADIUS.

Configurar freeRadius

Esta sección muestra como ejemplo cómo configurar freeRadius para que se utilice como servidor de autenticación remoto para el DCM. Sólo con fines informativos,

Cisco no proporciona ni admite freeRadius. Se asume que los archivos de configuración para freeRadius se encuentran bajo **/etc/freeRadius/** (verificar distribución).

Después de instalar freeRadius, modifique estos archivos.

- Modifique la **dirección /etc/freeradius/clients.conf**
  Paso 1. Agregue una entrada para la IP del DCM a la lista de clientes.
  Paso 2. Agregue la clave compartida en la configuración del cliente y deje los otros parámetros predeterminados.

  Se recomienda tener un secreto compartido único para cada DCM.
  La longitud del secreto compartido debe tener al menos 22 caracteres. El secreto compartido debe ser lo más aleatorio 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 que el servidor radius debe escuchar (generalmente 1812)

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

- Asegúrese de agregar el atributo RADIUS en el que se envía la información de autorización al DCM con este formato:
  <Nombre de atributo> = '**OU=<nombre_grupo>**'

  Nombre del atributo: Este es el nombre del atributo RADIUS estándar en el que se envían los datos de autorización al nombre_grupo de DCM puede ser uno de los siguientes:
  administradores: un usuario que pertenece a este grupo tendrá privilegios de administrador, es decir, control completo.
  usuarios: un usuario que pertenece a este grupo tendrá privilegios de lectura y escritura.
  invitados: un usuario que pertenece a este grupo tendrá privilegios de sólo lectura.
  automatización: se utiliza para la automatización (disparadores externos).
  dtfadmins - Administrador de DTF (configuración de clave DTF)

  Ejemplo:
  steve Cleartext-Password := "prueba"
  ID de filtro = "OU=administradores"

- (Re)inicie el servidor RADIUS para que los cambios surtan efecto.

- Asegúrese de que la configuración del firewall del servidor RADIUS permita el acceso externo al
  puerto.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Para fines de depuración, se han introducido algunos registros adicionales en el registro de seguridad. Para ver este registro, navegue a la **página Help > Traces** en la GUI de DCM.

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

Línea de registro	Error en el intento de inicio de sesión remoto: Se agotó el tiempo de espera de la solicitud al servidor RADIUS.
Problema	DCM no puede comunicarse con el servidor RADIUS.
Soluciones posibles	• Verifique que la dirección IP del servidor RADIUS proporcionada en la configuración de autenticación remota en el DCM sea realmente correcta. • Asegúrese de que el servidor RADIUS esté accesible desde el DCM. • Asegúrese de que el DCM esté configurado como un cliente válido en el servidor RADIUS (el servidor RADIUS descarta silenciosamente los paquetes de solicitud de acceso de clientes desconocidos). • Asegúrese de que el secreto compartido configurado en el DCM sea el mismo que el secreto compartido configurado en el servidor RADIUS para ese DCM en particular. (Si el servidor no posee un secreto compartido para el cliente, la solicitud se descarta silenciosamente.)
Línea de registro	Error al iniciar sesión de forma remota: [Error 10054] El host remoto cerró por la fuerza una conexión existente.
Problema	El DCM ha enviado una solicitud RADIUS a la IP de servidor especificada. Sin embargo, la aplicación de servidor RADIUS no escucha en el puerto especificado en la configuración de autenticación remota.
Soluciones posibles	• Asegúrese de que el servidor RADIUS se esté ejecutando. • Verifique que el número de puerto especificado en la configuración RADIUS en el servidor sea el mismo que el configurado en el DCM.
Línea de registro	Error en el intento de inicio de sesión remoto: Se especificó un nombre de atributo no válido o la respuesta del servidor RADIUS falta datos de autorización.
Problema	Hay un problema con la respuesta recibida del servidor RADIUS.
Soluciones posibles	• Asegúrese de que el servidor RADIUS envía el atributo (configurado en el DCM) en la respuesta "Access-Accept". • Asegúrese de que el parámetro **Attribute Name** configurado en la configuración de autenticación remota DCM sea el nombre exacto tal como se especifica en la configuración del usuario en el servidor RADIUS.
Línea de registro	Se recibieron datos de autorización no válidos del servidor RADIUS.
Problema	La autenticación se ha realizado correctamente, pero la respuesta recibida del servidor RADIUS contiene datos de autorización no válidos, es decir, el nombre del grupo de seguridad.
Soluciones posibles	• Asegúrese de que el nombre de grupo configurado en el servidor RADIUS para ese usuario sea uno de los nombres de grupo de seguridad especificados en la sección Configuración del servidor RADIUS. • Asegúrese de que el formato de la cadena configurada en el servidor RADIUS sea el

especificado en la sección Configuración del servidor RADIUS.