Configurazione di Cisco DCM - Supporto autenticazione remota

Sommario

Introduzione

In questo documento viene descritto il software Cisco Digital Content Manager (DCM)Autenticazione remota con RADIUS.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza del software Cisco DCM versione 16 e successive.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Software Cisco DCM v16.10 e versioni successive.
- Server RADIUS in esecuzione con software open source freeRadius.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Nella versione V16.10 di DCM è stata introdotta una nuova funzionalità che consente di utilizzare

gli account utente configurati su un server RADIUS per accedere all'interfaccia utente di DCM.In questo documento viene descritta la configurazione richiesta su DCM e sul server RADIUS per utilizzare questa funzionalità.

Account GUI su DCM

Nelle versioni 16.0 e successive, gli account utente necessari per accedere alla GUI erano locali di DCM, ovvero creati, modificati, utilizzati ed eliminati in DCM.

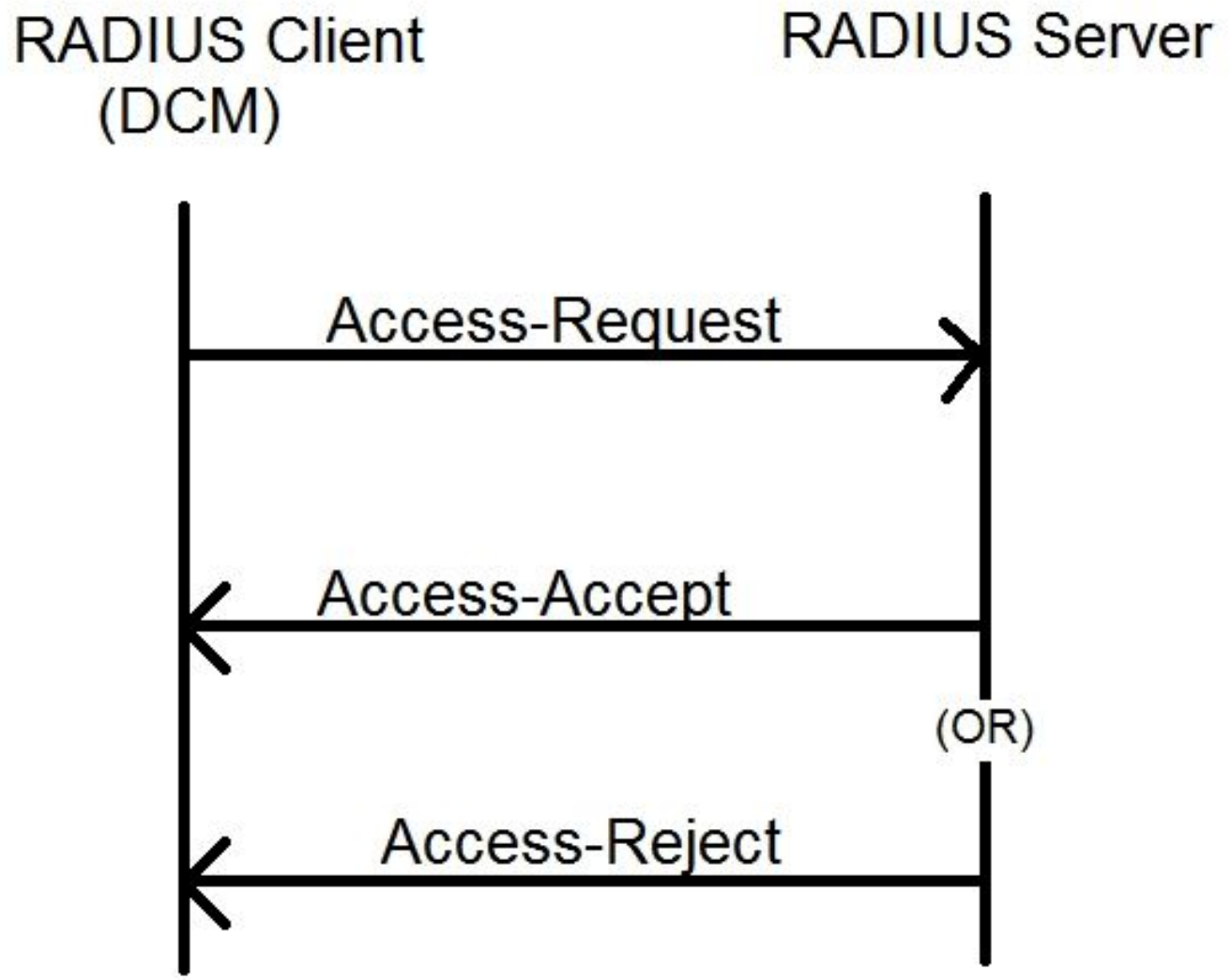
Un account utente GUI può appartenere a uno di questi gruppi:

- Amministratori (controllo completo)
- Utenti (lettura/scrittura)
- Guests (sola lettura)
- Trigger di automazione (trigger esterni)
- Amministratori DTF (configurazione chiave DTF)

Autenticazione remota

L'idea dell'autenticazione remota è quella di disporre di una raccolta centralizzata di account utente utilizzabili per accedere a un dispositivo, un'applicazione, un servizio, ecc.

La procedura illustrata nell'immagine spiega cosa accade quando si utilizza l'autenticazione remota:



Passaggio 1. L'utente immette il login e la password (account utente configurato sul server RADIUS) nella pagina di login nell'interfaccia utente di DCM.

Passaggio 2. DCM invia un messaggio di richiesta di accesso con le credenziali al server RADIUS.

Passaggio 3. Il server RADIUS verifica se la richiesta proviene da uno dei client configurati e l'esistenza dell'account utente nel relativo database/file e verifica se la password è corretta, dopodiché uno dei messaggi seguenti viene restituito a DCM

- Access-Accept - Le credenziali sono valide. Vengono restituiti gli attributi RADIUS configurati.
- Access-Reject: le credenziali non sono valide e il server RADIUS potrebbe essere configurato per inviare alcuni attributi RADIUS per informare l'errore.
- Access-Challenge: il server RADIUS necessita di ulteriori informazioni per convalidare l'autenticità dell'utente. Non elaborato in DCM.

Se il server RADIUS invia un messaggio di rifiuto dell'accesso, DCM verifica se l'account utente è locale rispetto a DCM e segue la procedura di autenticazione.
L'utente viene riautenticato a intervalli di 15 minuti (internamente) per confermare che il nome

utente/password è ancora valido e che l'utente appartiene a uno dei gruppi di account GUI. Se l'autenticazione ha esito negativo, la sessione utente corrente in esecuzione viene considerata non valida e tutti i privilegi vengono revocati per l'utente.

Configura server RADIUS

Per utilizzare gli account utente presenti sul server RADIUS per accedere alla GUI, è necessario effettuare le seguenti operazioni:

DCM deve essere configurato come client per il server RADIUS.

1. Aggiungere l'indirizzo IP di DCM come client per il server RADIUS.
2. Aggiungere il segreto condiviso alla configurazione del client (questo segreto condiviso deve essere uguale a quello configurato in DCM, vedere la sezione Configurazione di DCM).
3. Èconsigliabile disporre di un segreto condiviso diverso per ogni DCM.
4. La lunghezza del segreto condiviso deve essere di almeno 22 caratteri.
5. Il segreto condiviso deve essere il più possibile casuale.

   Esempio di segreto condiviso valido:
   '89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345'

Per un account utente, il messaggio Access-Accept inviato dal server RADIUS deve avere un attributo RADIUS che identifica il gruppo di account GUI a cui appartiene l'utente. È possibile scegliere il nome dell'attributo che deve essere configurato nel file delle impostazioni di DCM.

Questo è il formato della stringa che deve essere inviata come valore per un attributo dal server RADIUS:

OU=<group_name_string> nome_gruppo può essere uno dei seguenti:

Group	Stringa nome gruppo
Amministratori (controllo completo)	amministratori
Utenti (lettura/scrittura)	utenti
Guests (sola lettura)	ospiti
Trigger di automazione (esterni) trigger)	automazione
Chiave DTF Administrators configurazione)	dtfadmins

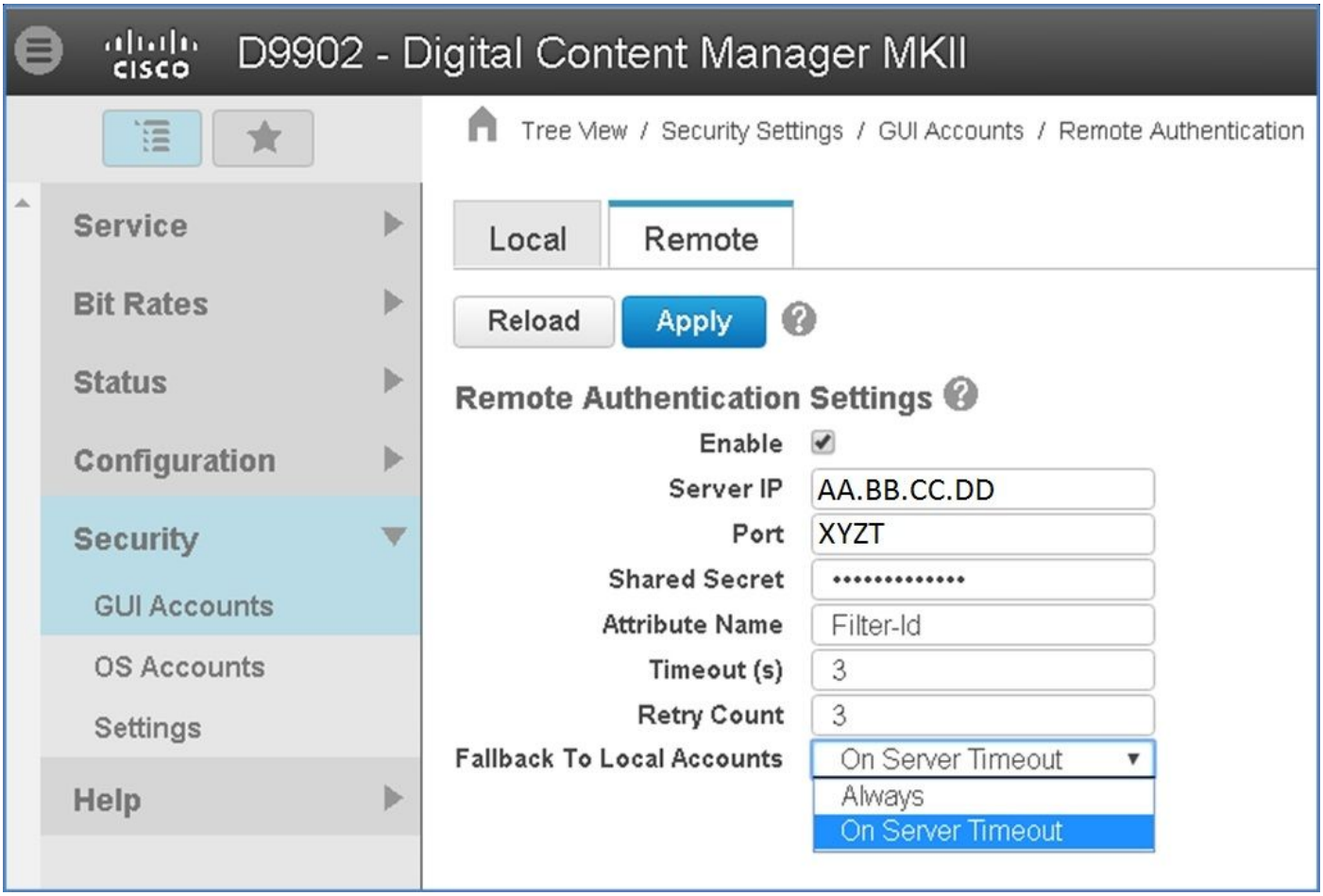
Configurazione di Cisco DCM

Per attivare/configurare la funzionalità di autenticazione remota in DCM è necessario un account di amministratore GUI.

I passaggi seguenti indicano come configurare l'autenticazione remota:

Passaggio 1. Accedere a DCM utilizzando l'account Administrator.

Passaggio 2. Passare a **Sicurezza > Account GUI** e selezionare la scheda **Remoto**, come mostrato nell'immagine:



Passaggio 3. Configurare i parametri necessari per la comunicazione RADIUS:

- Enable - Questa impostazione determina se il supporto dell'autenticazione remota deve essere attivato o meno. Se questa opzione è selezionata, gli altri campi dei parametri sono attivati.
- IP server: indirizzo IP del server RADIUS.
- Porta: la porta sulla quale il server RADIUS è in ascolto dei pacchetti di autenticazione (generalmente la porta 1812, ma può essere configurata per altri valori).
- Secret - Si tratta del segreto condiviso utilizzato per crittografare la password prima di inviare il pacchetto RADIUS al server. Questo segreto deve essere lo stesso di quello configurato nel server RADIUS in cui viene utilizzato per decrittografare la password.
- Nome attributo: il nome dell'attributo in cui i dati di autorizzazione vengono ricevuti dal server RADIUS.

- Timeout (in secondi): questa impostazione viene utilizzata per la comunicazione tra il server RADIUS e DCM. Tempo di attesa da parte di DCM di una risposta dal server RADIUS per una richiesta specifica prima di terminare la richiesta.

- Conteggio tentativi: numero di volte in cui la richiesta RADIUS deve essere inviata in caso di timeout delle richieste precedenti.

- Fallback agli account locali: questa impostazione è disponibile a partire dalla versione 19.0 di DCM. DCM consente di accedere utilizzando un account GUI (locale) creato mediante l'interfaccia utente. Opzione, **On Server Timeout** consente di eseguire il fallback agli account locali nel caso in cui non sia possibile raggiungere il server Radius e non quando l'autenticazione non è riuscita. Opzione, **Sempre** consente di eseguire sempre il fallback, anche se l'autenticazione non è riuscita.

Passaggio 4. Quando vengono applicate le modifiche, viene visualizzato il messaggio di avvertenza mostrato nell'immagine. Fare clic su **OK** per riavviare l'interfaccia utente.

Passaggio 5. DCM è pronto per l'autenticazione remota.

Configurare IPSec in DCM:

1. Accedere a DCM utilizzando un account GUI appartenente al gruppo di sicurezza Administrators.

2. Passare a **Configurazione > Sistema**. Viene visualizzata la pagina Impostazioni di sistema.

3. Fare riferimento all'area **Add New IPsec** (Aggiungi nuovo IPSec), come mostrato nell'immagine.

4. Nel campo Indirizzo IP, immettere l'indirizzo IP del nuovo peer IPsec (server RADIUS).

5. Nei campi Chiave **già condivisa** e Digita nuovamente *Chiave già condivisa*, immettere la *Chiave già condivisa* per il nuovo peer IPSec.

6. Fare clic su **Aggiungi**. Il nuovo peer IPSec viene aggiunto alla tabella Impostazioni IPSec.

> **Nota:** Per la configurazione di IPSec nel computer in cui è in esecuzione il server RADIUS, vedere la documentazione/pubblicazione fornita con il prodotto.

Considerazioni sulla sicurezza

- Il segreto condiviso viene memorizzato in chiaro nel file system di DCM.
- La password crittografata viene memorizzata nella memoria di DCM e utilizzata per la riautenticazione per l'intera durata della sessione.
- Considerati i due elementi sopra indicati, si consiglia di limitare gli utenti autorizzati ad accedere a DCM per la risoluzione dei problemi.
- Èconsigliabile utilizzare IPSec per proteggere il canale di comunicazione tra DCM e RADIUS server.

Vincoli e limitazioni

- Il supporto dell'autenticazione remota è disponibile solo per gli account GUI, non per gli account del sistema operativo.
- La riautenticazione viene eseguita a intervalli di 15 minuti. Esempio: Se il gruppo di un utente è stato modificato, il tempo peggiore impiegato per rendere effettiva la modifica è 15 minuti.
- Se l'autenticazione remota è abilitata, DCM verifica innanzitutto con il server RADIUS se l'account utente è valido e quindi controlla il database locale. Se si utilizzano account locali che non esistono sul server RADIUS, verrà visualizzato un messaggio di errore di autenticazione sul server RADIUS.

Imposta freeRadius

In questa sezione viene illustrato come configurare freeRadius per l'utilizzo come server di autenticazione remota per DCM. Questo documento ha solo scopo informativo,

Cisco non fornisce o supporta freeRadius. Si presume che i file di configurazione per freeRadius si trovino in **/etc/freeRadius/** (controllare la distribuzione).

Dopo aver installato il pacchetto freeRadius, modificare questi file.

- Modificare il **/etc/freeradius/clients.conf**
  Passaggio 1. Aggiungere una voce per l'indirizzo IP di DCM all'elenco dei client.
  Passaggio 2. Aggiungere la chiave condivisa nella configurazione del client e lasciare gli altri parametri predefiniti.

  Èconsigliabile disporre di un segreto condiviso univoco per ogni DCM.
  La lunghezza del segreto condiviso deve essere di almeno 22 caratteri. Il segreto condiviso deve essere il più possibile casuale.

  Esempio di segreto condiviso valido:
  '89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345'

- Modificare la chiave **/etc/freeradius/radiusd.conf** per cambiare la porta di ascolto del server radius (generalmente 1812)

- Modificare **/etc/freeradius/users** per aggiungere nuovi utenti.

- Assicurarsi di aggiungere l'attributo RADIUS in cui le informazioni di autorizzazione vengono inviate a DCM nel seguente formato:
  <Nome attributo> = '**OU=<nome_gruppo>'**

  Nome attributo: Il nome dell'attributo RADIUS standard in base al quale i dati di autorizzazione vengono inviati al nome_gruppo DCM può corrispondere a uno dei valori seguenti:
  Administrators - Un utente appartenente a questo gruppo disporrà dei privilegi di amministratore, ad esempio il controllo completo.
  utenti - Un utente che appartiene a questo gruppo disporrà di privilegi di lettura/scrittura.
  guest: un utente appartenente a questo gruppo disporrà del privilegio di sola lettura.
  automazione: utilizzata per l'automazione (trigger esterni).
  dtfadmins - Amministratore DTF (configurazione chiave DTF)

  Esempio:
  steve Cleartext-Password := "prova"
  Filter-Id = "OU=amministratori"

- Riavviare il server radius per rendere effettive le modifiche.

- Assicurarsi che la configurazione firewall del server radius consenta l'accesso esterno al server
  port.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

A scopo di debug, nel registro protezione sono stati introdotti alcuni log aggiuntivi. Per visualizzare

questo log, passare alla **pagina Guida > Tracce** nell'interfaccia utente di DCM.

In questa sezione vengono descritti gli elementi da cercare nei registri, i possibili problemi e le possibili soluzioni.

Riga registro	Tentativo di accesso remoto non riuscito: Timeout della richiesta al server RADIUS.
Problema	DCM non è in grado di comunicare con il server RADIUS.
Soluzione possibile	• Verificare che l'indirizzo IP del server RADIUS specificato nella configurazione di autenticazione remota in DCM sia effettivamente corretto. • Verificare che il server RADIUS sia accessibile da DCM. • Verificare che DCM sia configurato come client valido nel server RADIUS (il server RADIU elimina automaticamente i pacchetti di richiesta di accesso da client sconosciuti). • Verificare che il segreto condiviso configurato in DCM sia uguale al segreto condiviso configurato nel server RADIUS per il DCM specifico. Se il server non possiede un segreto condiviso per il client, la richiesta viene automaticamente eliminata.
Riga registro	Tentativo di accesso remoto non riuscito: [Errore 10054] Una connessione esistente è stata chiusa forzatamente dall'host remoto.
Problema	DCM ha inviato una richiesta RADIUS all'indirizzo IP del server specificato. L'applicazione server RADIUS non è tuttavia in ascolto sulla porta specificata nelle impostazioni di autenticazione remota.
Soluzione possibile	• Verificare che il server RADIUS sia in esecuzione. • Verificare che il numero di porta specificato nella configurazione RADIUS sul server sia uguale a quello configurato su DCM.
Riga registro	Tentativo di accesso remoto non riuscito: Nome di attributo specificato non valido o dati di autorizzazione mancanti nella risposta dal server RADIUS.
Problema	Problema con la risposta ricevuta dal server RADIUS.
Soluzione possibile	• Assicurarsi che il server RADIUS invii l'attributo (configurato su DCM) nella risposta "Access-Accept". • Verificare che il parametro **Attribute Name** configurato nelle impostazioni di autenticazione remota di DCM corrisponda esattamente al nome specificato nella configurazione utente sul server RADIUS.
Riga registro	Dati di autorizzazione non validi ricevuti dal server RADIUS.
Problema	L'autenticazione è stata completata, ma la risposta ricevuta dal server RADIUS contiene dati d autorizzazione non validi, ad esempio il nome del gruppo di sicurezza.
Soluzione possibile	• Verificare che il nome del gruppo configurato nel server RADIUS per l'utente sia uno dei n del gruppo di sicurezza specificati nella sezione Configurazione del server RADIUS. • Verificare che il formato della stringa configurata nel server RADIUS sia conforme a quello specificato nella sezione Configurazione del server RADIUS.