Configurez Cisco DCM ? Support d'authentification à distance

Contenu

Introduction

Ce document décrit l'authentification de softwareRemote du gestionnaire de contenu numérique de Cisco (DCM) utilisant le RAYON.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de la version de logiciel 16 de Cisco DCM et en haut.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Logiciel v16.10 de Cisco DCM et en haut.
- Serveur exécutant de RAYON avec le logiciel libre de freeRadius.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Informations générales

Dans V16.10 du DCM on a introduit une nouvelle caractéristique qui permet des comptes utilisateurs configurés sur un serveur de RAYON à utiliser pour accéder au document DCM GUI.This décrit l'installation exigée sur le DCM et le serveur de RAYON pour se servir de cette caractéristique.

Le GUI rend compte sur DCM

Dans les versions 16.0 et antérieures les comptes d'utilisateur exigés pour accéder au GUI étaient locaux au DCM, ont c.-à-d. créé, modifié, utilisé et supprimé sur le DCM.

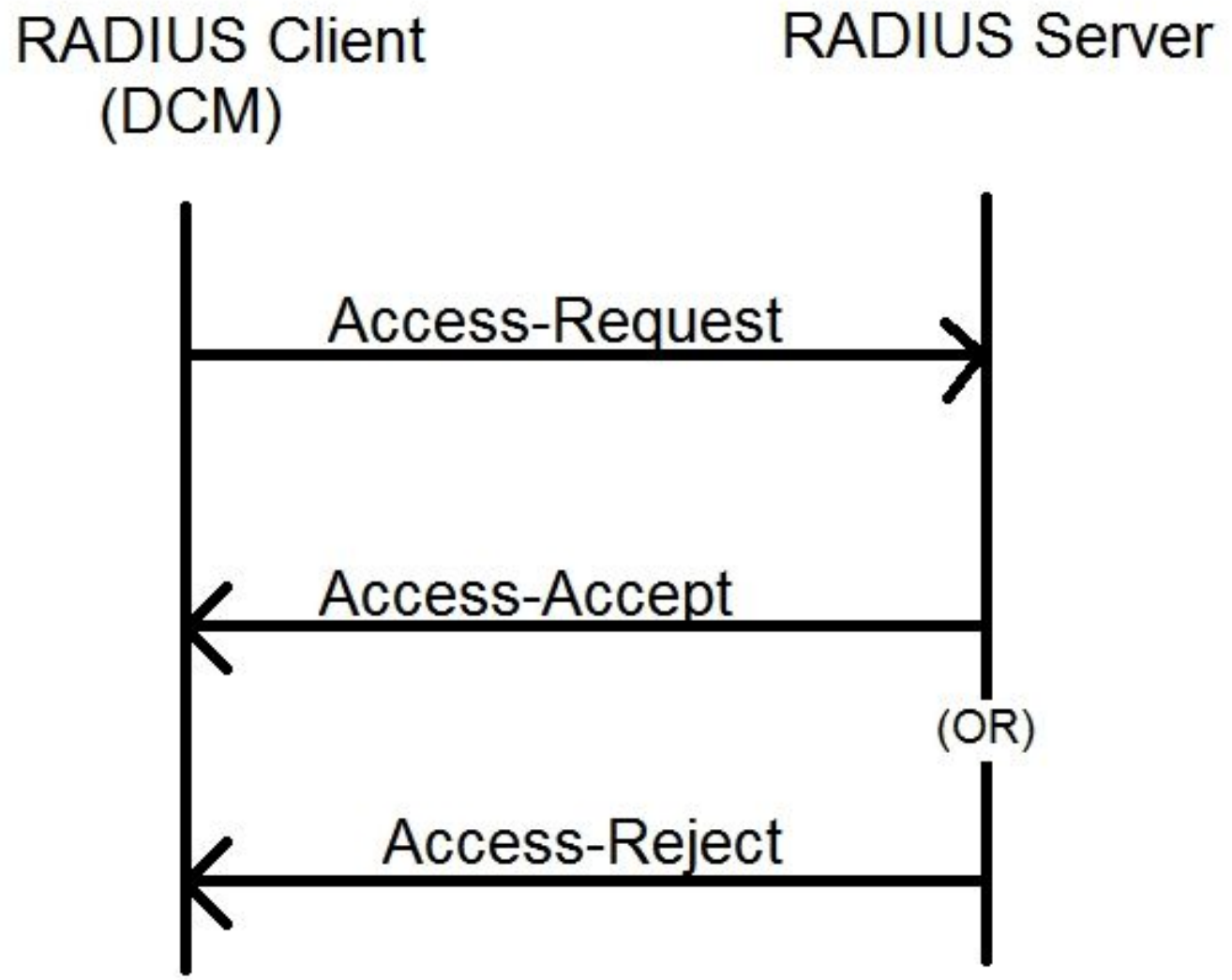
Un compte utilisateur GUI peut appartenir à un de ces groupes :

- Administrateurs (plein contrôle)
- Utilisateurs (lecture/écriture)
- Invités (lus seulement)
- Déclencheurs d'automatisation (déclencheurs externes)
- Administrateurs DTF (configuration de clé DTF)

Authentification à distance

L'idée de l'authentification à distance est d'avoir une collection centralisée de comptes utilisateurs qui peuvent être utilisés pour accéder à un périphérique, une application, un service etc.

Les étapes affichées dans l'image explique ce qui se produit quand vous utilisez l'authentification à distance :



Étape 1. L'utilisateur entre la procédure de connexion et le mot de passe (compte utilisateur configuré sur le serveur de RAYON) sur la page de connexion sur le GUI DCM.

Étape 2. Le DCM envoie un message d'Access-demande avec les qualifications au serveur de RAYON.

Étape 3. Le serveur de RAYON vérifie si la demande est provenue un des clients configurés et pour l'existence du compte utilisateur sur son DB/File et valide si le mot de passe est correct ou pas, après quoi des n'importe quels des messages suivants sont retournés au DCM

- Access-recevez – Ceci signifie que les qualifications sont valides. Les attributs RADIUS configurés sont retournés.
- Access-anomalie – Ceci signifie que les qualifications sont non valides et le serveur de RAYON peut être configuré pour envoyer quelques attributs RADIUS pour informer la panne.
- Access-défi – Ceci signifie que le serveur de RAYON a besoin de quelques informations complémentaires pour valider l'authenticité de l'utilisateur. Non traité dans le DCM.

Au cas où le serveur de RAYON enverrait une Access-anomalie, le DCM vérifie si le compte utilisateur est local au DCM lui-même et procédure d'authentification pour cela est suivie.

L'utilisateur est authentifié à nouveau à un intervalle de 15 minutes (intérieurement) pour confirmer que le nom d'utilisateur/mot de passe est encore valide et l'utilisateur appartient à un des groupes de compte GUI. Si l'authentification échoue la session d'utilisateur courante en cours est considérée non valide et tous les privilèges sont retirés pour l'utilisateur.

Configurez le serveur de RAYON

Pour utiliser les comptes utilisateurs actuels sur le serveur de RAYON pour accéder aux ces étapes GUI devez être suivi :

DCM devrait être configuré en tant que client au serveur de RAYON.

1. Ajoutez l'IP du DCM en tant que client pour le serveur de RAYON.

2. Ajoutez le secret partagé à la configuration de client (ce secret partagé devrait être identique que celui configuré sur le DCM, voient la section configurer le DCM).

3. Il est recommandé pour avoir un secret partagé différent pour chaque DCM.

4. La longueur du secret partagé devrait être au moins 22 caractères longs.

5. Le secret partagé devrait être aussi aléatoire comme possible.

   Exemple d'un bon secret partagé :
   « 89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345 »

Pour un compte utilisateur le message d'Access-recevoir du serveur de RAYON devrait avoir un attribut RADIUS qui identifie le groupe de compte GUI auquel l'utilisateur appartient. Le nom d'attribut peut être choisi et les besoins d'être configuré dans les configurations introduisent sur le DCM.

C'est le format de la chaîne qui doit être envoyée comme valeur pour un attribut du serveur de RAYON :

OU=<group_name_string> group_name_string peut être l'un de ces derniers :

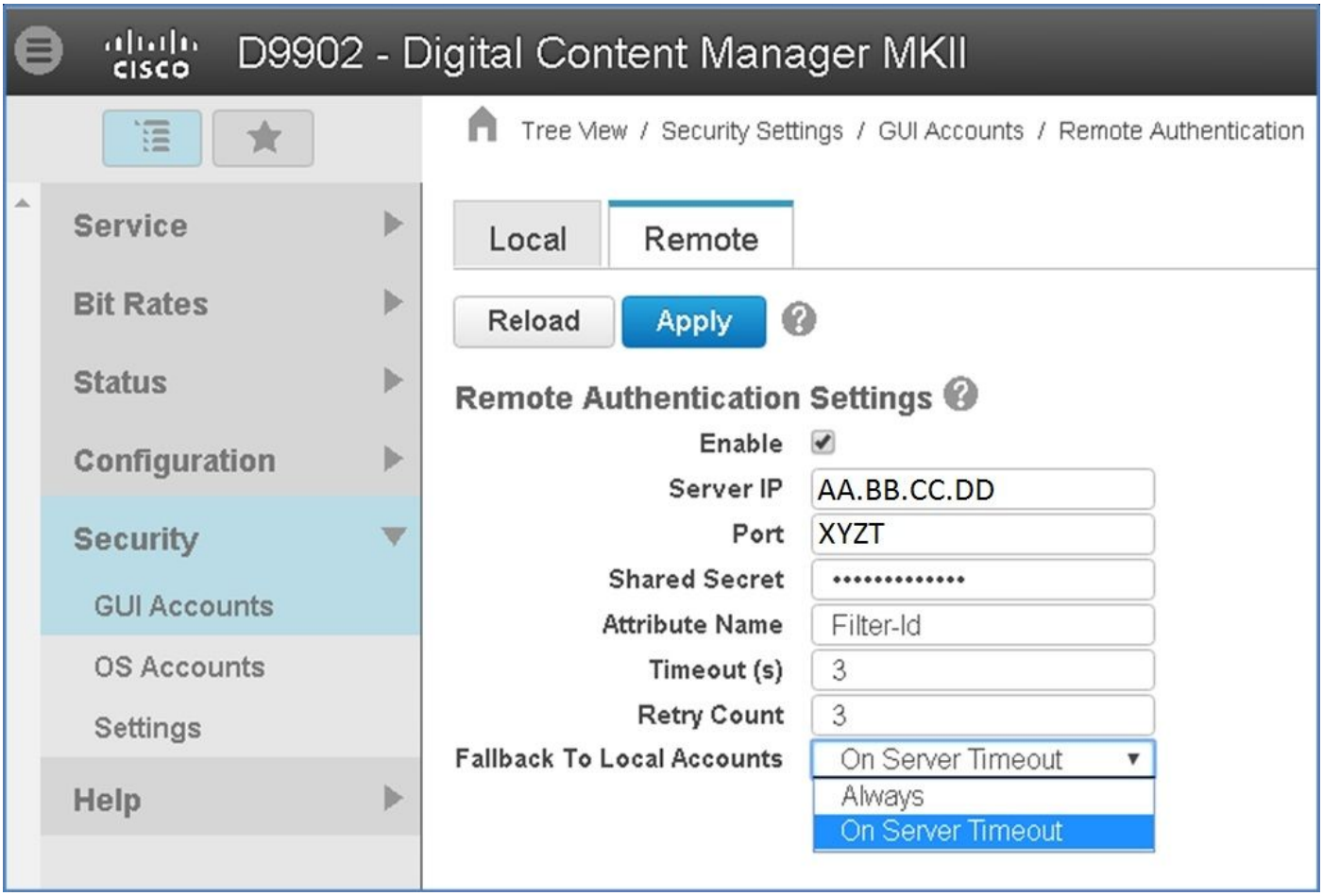
Groupe	Chaîne de nom de groupe
Administrateurs (plein contrôle)	administrateurs
Utilisateurs (lecture/écriture)	utilisateurs
Invités (lus seulement)	invités
Déclencheurs d'automatisation (externes Déclencheurs)	automatisation
Administrateurs DTF (clé DTF configuration)	dtfadmins

Configurez Cisco DCM

Pour activer/configurez la caractéristique d'authentification à distance sur le DCM qu'un compte administrateur GUI est exigé.
Ces étapes indiquent comment configurer l'authentification à distance :

Étape 1. Procédure de connexion au DCM utilisant le compte administrateur.

Étape 2. Naviguez vers la **Sécurité > les comptes GUI** et l'onglet **distant** choisi, suivant les indications de l'image :



Étape 3. Configurez les paramètres requis pour la transmission de RAYON :

- Enable - Cette configuration détermine si le support d'authentification à distance est activé ou pas. Une fois vérifié le reste des champs de paramètre sont activés.
- IP de serveur - Adresse IP du serveur de RAYON.
- Port - Mettez en communication sur ce que le serveur de RAYON écoute des paquets d'authentification (généralement 1812 mais peuvent être configurés à d'autres valeurs).
- Secret - C'est le secret partagé qui est utilisé pour chiffrer le mot de passe avant d'envoyer le paquet RADIUS au serveur. Ce secret devrait être identique que cela configuré sur le serveur de RAYON où il est utilisé pour déchiffrer le mot de passe.
- Nom d'attribut - Le nom de l'attribut dans lequel les données d'autorisation sont reçues du serveur de RAYON.

- Délai d'attente (en quelques secondes) - Cette configuration est utilisée pour la transmission entre le serveur de RAYON et le DCM. C'est le temps que le DCM devrait attendre une réponse du serveur de RAYON pour une demande particulière avant de terminer la demande.

- Nombre de tentatives - Nombre de fois où la demande RADIUS doit être envoyée au cas où des demandes précédentes seraient chronométrées.

- Retour aux comptes locaux - Cette configuration est fournie par la version 19.0 DCM en avant. Le DCM laisse ouvrir une session utilisant un compte GUI (gens du pays) qui est créé utilisant le GUI. L'option, **sur le délai de temporisation du serveur** autorise au retour aux comptes locaux au cas où le serveur de rayon ne pourrait pas être atteint, et pas quand échec de l'authentification. L'option, autorise **toujours au** retour toujours – même lorsqu'échec de l'authentification.

Étape 4. Pendant que les modifications sont appliquées l'avertissement affiché dans l'image est affiché. Cliquez sur OK et l'interface utilisateur est redémarrée.

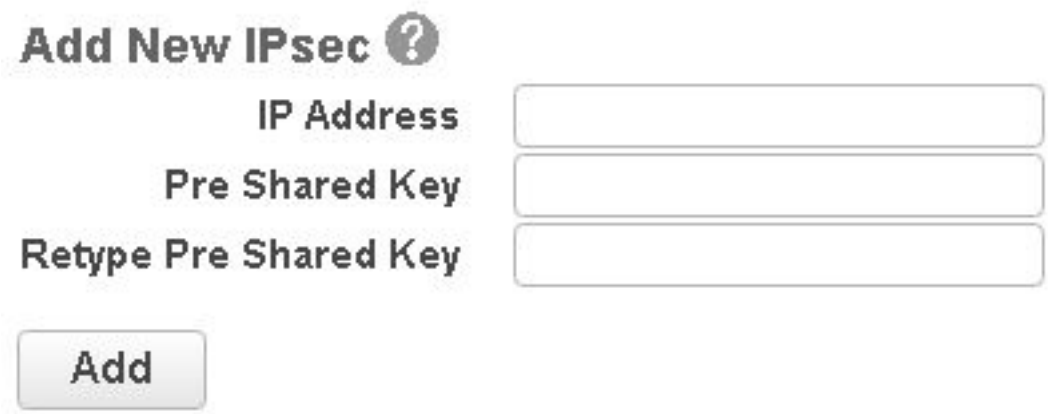
Étape 5. Maintenant le DCM est prêt pour l'authentification à distance.

Configurez IPSec sur DCM :

1. Login au DCM utilisant un compte GUI qui appartient au groupe de sécurité d'administrateurs.

2. Naviguez vers la **configuration > le système**. La page de paramètres système paraît.

3. Référez-vous à la **nouvelle** région d'**IPsec d'ajouter**, suivant les indications de l'image.



4. Dans le champ IP Address, écrivez l'adresse IP du nouveau pair d'IPsec (serveur de RAYON).

5. Dans la clé **pré partagée** et retapez les zones de tri *pré partagées*, introduisent la *clé pré partagée* pour le nouveau pair d'IPsec.

6. Cliquez sur **Add**. Le nouveau pair d'IPsec est ajouté à la table de configurations d'IPsec.

> **Note**: Pour la configuration d'IPSec sur l'ordinateur sur lequel le serveur de RAYON s'exécute référez-vous à la documentation/à publication équipées de produit.

Considérations liées à la sécurité

- Le secret partagé est enregistré en clair dans le système de fichiers du DCM.
- Le mot de passe chiffré est enregistré dans la mémoire du DCM pour l'usage dans la ré-authentification pour la durée de la session.
- Etant donné les deux éléments ci-dessus, on lui informe pour limiter qui a accès de dépannage au DCM.
- On lui informe fortement employer IPSec pour sécuriser la voie de transmission entre DCM et RAYON
  serveur.

Contraintes et limites

- Le support d'authentification à distance est seulement disponible pour les comptes GUI, pas pour les comptes de SYSTÈME D'EXPLOITATION.
- Une ré-authentification est faite à un intervalle de 15 minutes. Exemple : Si un Groupe d'utilisateurs a été changé, le moment de le pire des cas pris pour que la modification prenne l'affect est de 15 minutes.
- Si l'authentification à distance est activée, le DCM vérifie d'abord avec le serveur de RAYON si le compte utilisateur est valide ou vérifie et ensuite la base de données locale. En cas d'utiliser les comptes locaux qui n'existent pas sur le serveur de RAYON il y aurait un message d'échec d'authentification sur le serveur de RAYON.

FreeRadius d'installation

Cette section affiche comme exemple comment installer le freeRadius pour utiliser comme serveur d'authentification à distance pour le DCM. C'est à des fins d'information seulement,

Cisco ne fournit pas ou prend en charge le freeRadius. On le suppose que les fichiers de configuration pour le freeRadius sont trouvés sous **/etc/freeRadius/** (distribution de contrôle).

Après avoir installé le module de freeRadius modifiez ces fichiers.

- Modifiez **/etc/freeradius/clients.conf**
  Étape 1. Ajoutez une entrée pour l'IP du DCM à la liste de clients.
  L'étape 2.Add la clé partagée dans la configuration de client et laissent les autres paramètres pour se transférer.

  Il est recommandé pour avoir un seul secret partagé pour chaque DCM.
  La longueur du secret partagé devrait être au moins 22 caractères longs. Le secret partagé devrait être aussi aléatoire comme possible.

  Exemple d'un bon secret partagé :
  « 89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345 »

- Modifiez **/etc/freeradius/radiusd.conf** pour changer le port sur lequel le serveur de rayon devrait écouter (généralement 1812)

- Modifiez **/etc/freeradius/users** pour ajouter de nouveaux utilisateurs.

- Assurez pour ajouter l'attribut RADIUS dans lequel les informations d'autorisation sont envoyées au DCM dans ce format :
  <Attribute Name> = « **OU=<group_name> »**

  Nom d'attribut : C'est le nom de l'attribut RADIUS standard sur lequel les données d'autorisation sont envoyées au group_name DCM peuvent être l'une de ce qui suit :
  administrateurs - Un utilisateur qui appartient à ce groupe aura le plein contrôle de privilèges d'administrateur c.-à-d.
  utilisateurs - Un utilisateur qui appartient à ce groupe aura des privilèges lecture/écriture.
  invités - Un utilisateur qui appartient à ce groupe aura lu seulement le privilège.
  automatisation - Utilisé pour l'automatisation (déclencheurs externes).
  dtfadmins - Administrateur DTF (configuration de clé DTF)

  Exemple :
  Libellé-mot de passe de steve : = « test »
  Filtre-id = « OU=administrators »

- (Au sujet de) mettez en marche le serveur de rayon pour les modifications pour le prendre effet.

- Assurez-vous que la configuration de Pare-feu du serveur de rayon permet l'accès externe au choisi
  port.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Pour des purposses de débogage quelques logs supplémentaires ont été introduits dans le log de sécurité. Afin de visualiser ce log naviguez **pour aider > page de suivis** dans le GUI DCM.

Cette section décrit quoi rechercher dans les logs, ce qui être les questions pourraient et les solutions possibles.

Ligne de log	La tentative de remote login a manqué : La demande au serveur de RAYON a été chronométré
Question	DCM ne peut pas communiquer avec le serveur de RAYON.
Solution possible	• Vérifiez que l'adresse IP du serveur de RAYON fournie dans la configuration d'authentificat à distance dans le DCM est réellement correcte. • Assurez-vous que le serveur de RAYON est accessible du DCM. • Assurez-vous que le DCM est configuré en tant que client valide sur le serveur de RAYON serveur de RAYON relâche silencieusement des paquets de demande d'accès des clients inconnus). • Assurez-vous que le secret partagé configuré sur le DCM est identique que le secret partag configuré sur le serveur de RAYON pour cela DCM particulier. (Si le serveur ne possède pa un secret partagé pour le client, la demande est silencieusement abandonnée.)
Ligne de log	La tentative de remote login a manqué : [Errno 10054] une connexion existante a été de force clôturé par le serveur distant.
Question	Le DCM a envoyé une demande RADIUS à l'IP spécifié de serveur. Cependant, le serveur d'application de RAYON n'écoute pas sur le port spécifié dans les configurations d'authentification à distance.
Solution possible	• Assurez-vous que le serveur de RAYON s'exécute. • Vérifiez que le numéro de port spécifié en configuration RADIUS sur le serveur est identiqu que celui configuré sur le DCM.
Ligne de log	La tentative de remote login a manqué : Nom non valide d'attribut spécifié ou réponse des données manquantes d'autorisation de serveur de RAYON.
Question	Il y a un problème avec la réponse reçue du serveur de RAYON.
Solution possible	• Assurez-vous que le serveur de RAYON envoie l'attribut (configuré sur le DCM) dans « Access-reçoivent » la réponse. • Assurez-vous que le paramètre de **nom d'attribut** configuré sur les configurations d'authentification à distance DCM est le nom précis comme spécifié en configuration utilisateur sur le serveur de RAYON.
Ligne de log	Données non valides d'autorisation reçues du serveur de RAYON.
Question	L'authentification a réussi mais la réponse reçue du serveur de RAYON contient le nom de groupe de sécurité non valide de données d'autorisation c.-à-d.
Solution possible	• Assurez-vous que le nom de groupe configuré sur le serveur de RAYON pour cet utilisateur est un du nom de groupe de sécurité spécifié dans la section configurant le serveur de RAYON. • Assurez-vous que le format de la chaîne configurée sur le serveur de RAYON est selon cel spécifié dans la section configurant le serveur de RAYON.