Configuration de Cisco DCM - Prise en charge de l'authentification à distance

Contenu

Introduction

Ce document décrit le logiciel Cisco Digital Content Manager (DCM)Authentification à distance à l'aide de RADIUS.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître le logiciel Cisco DCM version 16 et ultérieure.

Components Used

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

- Logiciel Cisco DCM v16.10 et versions ultérieures.
- Serveur RADIUS fonctionnant avec le logiciel libre 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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Dans la version V16.10 du DCM, une nouvelle fonctionnalité a été introduite qui permet aux comptes d'utilisateurs configurés sur un serveur RADIUS d'être utilisés pour accéder à l'interface

utilisateur graphique DCM.Ce document décrit la configuration requise sur le DCM et le serveur RADIUS pour utiliser cette fonctionnalité.

Comptes GUI sur DCM

Dans les versions 16.0 et inférieures, les comptes d'utilisateurs requis pour accéder à l'interface utilisateur graphique étaient locaux au DCM, c'est-à-dire créés, modifiés, utilisés et supprimés sur le DCM.

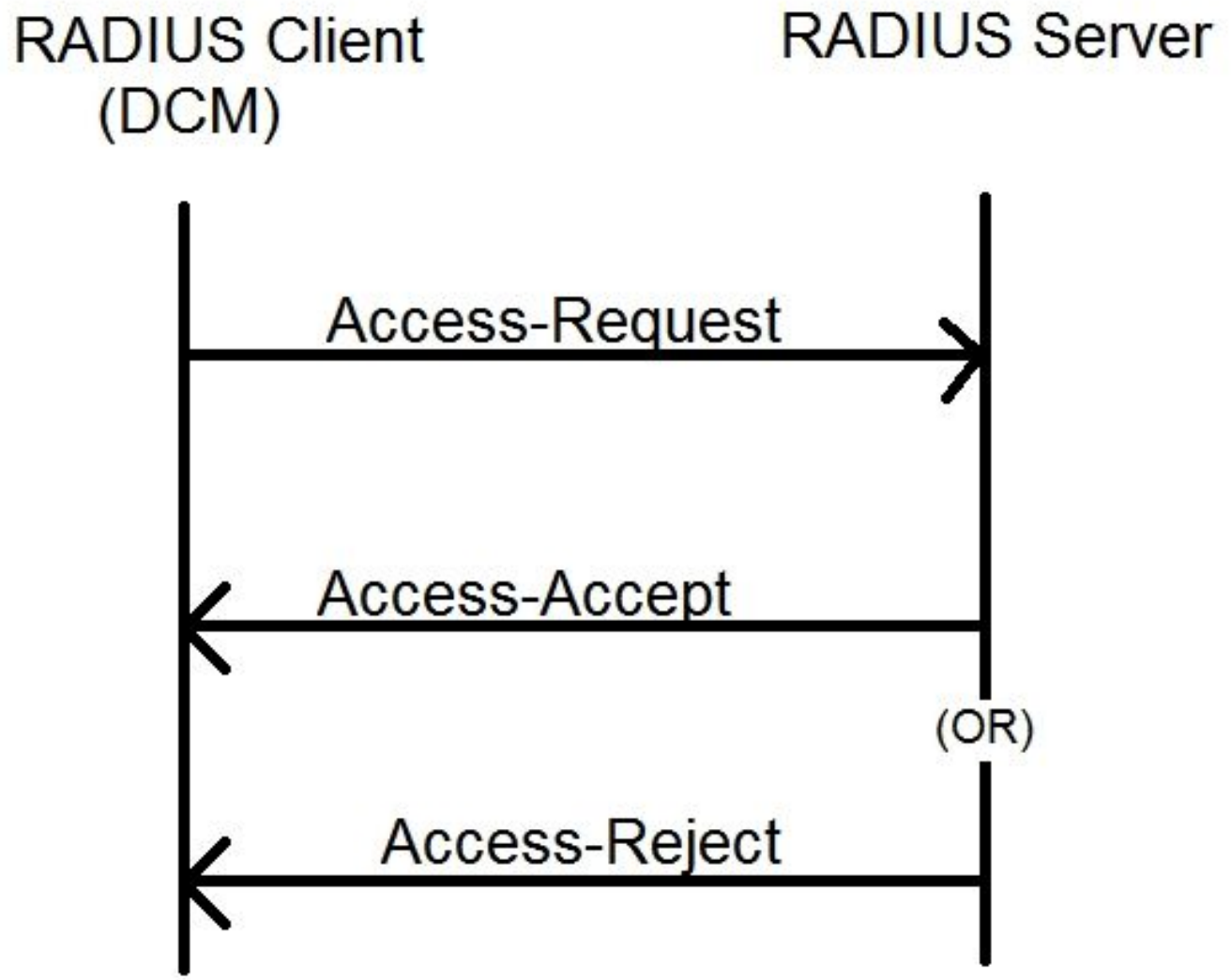
Un compte utilisateur GUI peut appartenir à l'un des groupes suivants :

- Administrateurs (contrôle total)
- Utilisateurs (lecture-écriture)
- Invités (lecture seule)
- Déclencheurs d'automatisation (déclencheurs externes)
- Administrateurs DTF (configuration de clé DTF)

Authentification distante

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

Les étapes indiquées dans l'image expliquent ce qui se passe lorsque vous utilisez l'authentification à distance :



Étape 1. L'utilisateur entre la connexion et le mot de passe (compte d'utilisateur configuré sur le serveur RADIUS) sur la page de connexion de l'interface utilisateur graphique DCM.

Étape 2. Le DCM envoie un message de demande d'accès avec les informations d'identification au serveur RADIUS.

Étape 3. Le serveur RADIUS vérifie si la demande provient de l'un des clients configurés et si le compte d'utilisateur se trouve sur sa base de données/fichier et vérifie si le mot de passe est correct ou non, après quoi l'un des messages suivants est renvoyé au DCM

- Access-Accepcept : signifie que les informations d'identification sont valides. Les attributs RADIUS configurés sont retournés.

- Access-Reject : cela signifie que les informations d'identification ne sont pas valides et que le serveur RADIUS peut être configuré pour envoyer certains attributs RADIUS pour informer l'échec.

- Access-Challenge : cela signifie que le serveur RADIUS a besoin d'informations supplémentaires pour valider l'authenticité de l'utilisateur. Non traité dans le DCM.

Dans le cas où le serveur RADIUS envoie un Access-Reject, le DCM vérifie si le compte

d'utilisateur est local au DCM lui-même et la procédure d'authentification pour ce compte est suivie.
L'utilisateur est réauthentifié à un intervalle de 15 minutes (en interne) pour confirmer que le nom d'utilisateur/mot de passe est toujours valide et qu'il appartient à l'un des groupes de comptes de l'interface utilisateur graphique. Si l'authentification échoue, la session actuelle de l'utilisateur en cours est considérée comme non valide et tous les privilèges sont révoqués pour l'utilisateur.

Configurer le serveur RADIUS

Pour utiliser les comptes d'utilisateurs présents sur le serveur RADIUS pour accéder à l'interface utilisateur graphique, procédez comme suit :

DCM doit être configuré en tant que client du serveur RADIUS.

1. Ajoutez l'adresse IP du DCM en tant que client pour le serveur RADIUS.

2. Ajoutez le secret partagé à la configuration du client (ce secret partagé doit être identique à celui configuré sur le DCM, voir la section Configuration du DCM).

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

4. La longueur du secret partagé doit être d'au moins 22 caractères.

5. Le secret partagé doit être aussi aléatoire que possible.

   Exemple de bon secret partagé : ‘89w%$w*78619ew8r4$7$6@q ! 9we#%^rnEWR@#QEws13&4^%sf54gsf4@ ! fg3sdf#@sdf$d3g44fg3%2s2345’

Pour un compte utilisateur, le message Access-Accept du serveur RADIUS doit comporter un attribut RADIUS qui identifie le groupe de comptes de l'interface utilisateur graphique auquel l'utilisateur appartient. Le nom de l'attribut peut être choisi et doit être configuré dans le fichier de paramètres du DCM.

Il s'agit du format de la chaîne qui doit être envoyée en tant que valeur pour un attribut du serveur RADIUS :

OU=<group_name_string> group_name_string peut être l'une des suivantes :

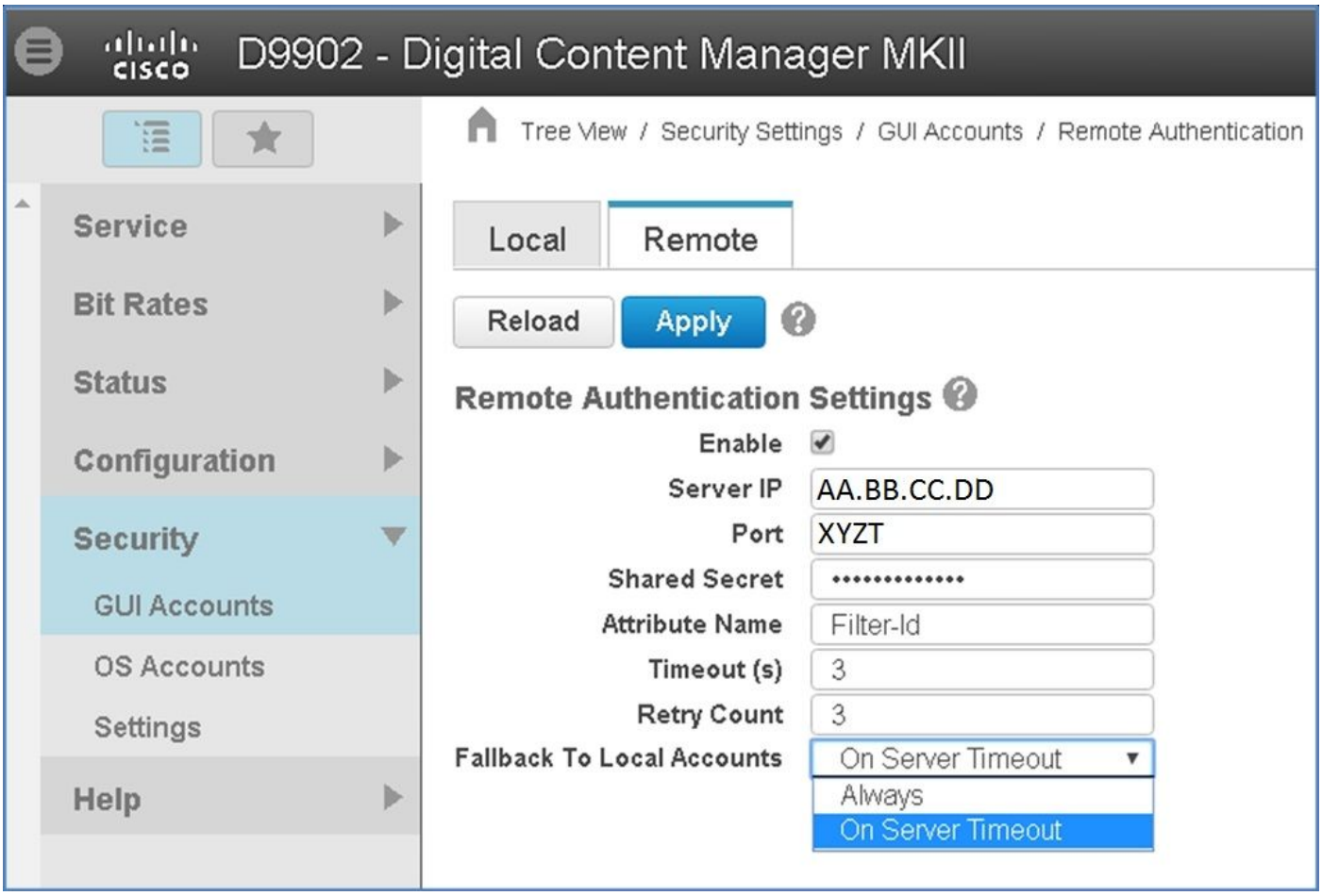
Groupe	Chaîne de nom de groupe
Administrateurs (contrôle total)	administrateurs
Utilisateurs (lecture-écriture)	utilisateurs
Invités (lecture seule)	invités
Déclencheurs d'automatisation (externe) Déclencheurs)	automatisation
Administrateurs DTF (clé DTF) configuration)	dtfadmins

Configurer Cisco DCM

Pour activer/configurer la fonction d'authentification à distance sur le DCM, un compte administrateur de l'interface utilisateur graphique est requis.
Ces étapes indiquent comment configurer l'authentification distante :

Étape 1. Connectez-vous au DCM à l'aide du compte Administrateur.

Étape 2. Accédez à **Security > GUI Accounts** et sélectionnez **Remote** tab, comme illustré dans l'image :



Étape 3. Configurez les paramètres requis pour la communication RADIUS :

- Enable : ce paramètre détermine si la prise en charge de l'authentification à distance doit être activée ou non. Lorsque cette case est cochée, les autres champs de paramètres sont activés.
- Server IP : adresse IP du serveur RADIUS.
- Port : port sur lequel le serveur RADIUS écoute les paquets d'authentification (généralement 1812, mais peut être configuré avec d'autres valeurs).
- Secret : secret partagé utilisé pour chiffrer le mot de passe avant d'envoyer le paquet RADIUS au serveur. Ce secret doit être identique à celui configuré sur le serveur RADIUS où il est utilisé pour déchiffrer le mot de passe.

- Nom d'attribut : nom de l'attribut dans lequel les données d'autorisation sont reçues du serveur RADIUS.

- Timeout (en secondes) : ce paramètre est utilisé pour la communication entre le serveur RADIUS et DCM. C'est le moment où le DCM doit attendre une réponse du serveur RADIUS pour une requête particulière avant de mettre fin à la requête.

- Nombre de tentatives : nombre de fois que la demande RADIUS doit être envoyée au cas où les demandes précédentes seraient dépassées.

- Restaurer les comptes locaux : ce paramètre est disponible à partir de la version 19.0 de DCM. Le DCM permet de se connecter à l'aide d'un compte d'interface utilisateur graphique (local) créé à l'aide de l'interface utilisateur graphique. Option, **On Server Timeout** permet de revenir aux comptes locaux au cas où le serveur Radius ne serait pas accessible, et non en cas d'échec de l'authentification. Option, **Always** permet de toujours basculer - même en cas d'échec de l'authentification.

Étape 4. Lorsque les modifications sont appliquées, l'avertissement affiché dans l'image s'affiche. Cliquez sur **OK** et l'interface utilisateur est redémarrée.

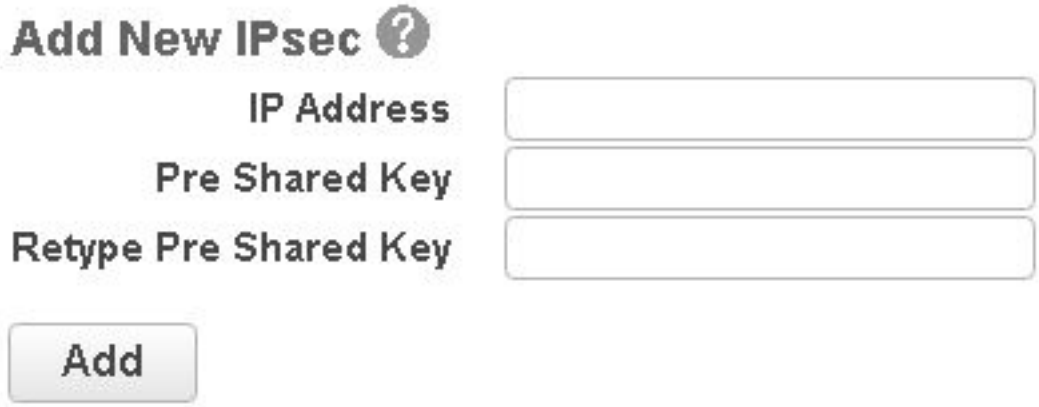
Étape 5. Désormais, le DCM est prêt pour l'authentification à distance.

Configurez IPSec sur DCM :

1. Connectez-vous au DCM à l'aide d'un compte GUI appartenant au groupe de sécurité Administrateurs.

2. Accédez à **Configuration > System**. La page Paramètres système s'affiche.

3. Reportez-vous à la zone **Add New IPsec**, comme illustré dans l'image.



4. Dans le champ IP Address, saisissez l'adresse IP du nouvel homologue IPsec (serveur RADIUS).

5. Dans les champs **Pre Shared** key et Retype *Pre Shared Key*, saisissez la *Pre Shared Key* pour le nouvel homologue IPsec.

6. Cliquez sur **Add**. Le nouvel homologue IPsec est ajouté à la table Paramètres IPsec.

> **Note**: Pour la configuration d'IPSec sur la machine sur laquelle le serveur RADIUS est exécuté, reportez-vous à la documentation/publication fournie avec le produit.

Considérations relatives à la sécurité

- Le secret partagé est stocké en clair dans le système de fichiers du DCM.
- Le mot de passe chiffré est stocké dans la mémoire du DCM pour être utilisé lors de la réauthentification pendant la durée de la session.
- Compte tenu des deux éléments ci-dessus, il est conseillé de limiter l'accès de dépannage au DCM.
- Il est fortement conseillé d'utiliser IPSec pour sécuriser le canal de communication entre DCM et RADIUS
  serveur .

Contraintes et limitations

- La prise en charge de l'authentification à distance est uniquement disponible pour les comptes de l'interface utilisateur graphique, et non pour les comptes du système d'exploitation.
- Une nouvelle authentification est effectuée à un intervalle de 15 minutes. Exemple : Si le groupe d'un utilisateur a été modifié, le délai le plus long pour que la modification prenne effet est de 15 minutes.
- Si l'authentification à distance est activée, le DCM vérifie d'abord auprès du serveur RADIUS

si le compte d'utilisateur est valide ou non, puis vérifie la base de données locale. En cas d'utilisation de comptes locaux qui n'existent pas sur le serveur RADIUS, il y aurait un message d'échec d'authentification sur le serveur RADIUS.

Configurer freeRadius

Cette section présente un exemple de configuration de freeRadius à utiliser comme serveur d'authentification à distance pour le DCM. Il n'a qu'un but informatif,

Cisco ne fournit ni ne prend en charge freeRadius. On suppose que les fichiers de configuration pour freeRadius se trouvent sous **/etc/freeRadius/** (vérifier la distribution).

Après avoir installé le paquet freeRadius, modifiez ces fichiers.

- Modifiez le **répertoire /etc/freeradius/clients.conf**
  Étape 1. Ajoutez une entrée pour l'adresse IP du DCM à la liste des clients.
  Étape 2. Ajoutez la clé partagée dans la configuration du client et conservez les autres paramètres par défaut.

  Il est recommandé d'avoir un secret partagé unique pour chaque DCM.
  La longueur du secret partagé doit être d'au moins 22 caractères. Le secret partagé doit être aussi aléatoire que possible.

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

- Modifiez l'adresse **/etc/freeradius/radiusd.conf** pour modifier le port sur lequel le serveur radius doit écouter (généralement 1812)

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

- Assurez-vous d'ajouter l'attribut RADIUS dans lequel les informations d'autorisation sont envoyées au DCM au format suivant :
  <Nom de l'attribut> = '**OU=<nom_groupe>**'

  Nom de l'attribut : Il s'agit du nom de l'attribut RADIUS standard sur lequel les données d'autorisation sont envoyées au nom de groupe DCM. Il peut s'agir de l'un des éléments suivants :
  administrateurs : un utilisateur appartenant à ce groupe disposera de privilèges d'administrateur, c'est-à-dire d'un contrôle total.
  utilisateurs : un utilisateur appartenant à ce groupe dispose de privilèges de lecture-écriture.
  invités : un utilisateur appartenant à ce groupe aura un privilège de lecture seule.
  Automatisation : utilisée pour l'automatisation (déclencheurs externes).
  dtfadmins - Administrateur DTF (configuration de clé DTF)

Exemple :
steve Cleartext-Password := « Test »
Filter-Id = « OU=administrateurs »

- (Re)démarrez le serveur radius pour que les modifications prennent effet.
- Assurez-vous que la configuration du pare-feu du serveur radius permet un accès externe au port.

Dépannage

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

Àdes fins de débogage, des journaux supplémentaires ont été introduits dans le journal de sécurité. Afin d'afficher ce journal, accédez à **Aide > Page Traces** dans l'interface graphique de DCM.

Cette section décrit les éléments à rechercher dans les journaux, les problèmes éventuels et les solutions possibles.

Ligne de journal	Échec de la tentative de connexion à distance : La demande au serveur RADIUS a expiré.
Problème	DCM ne peut pas communiquer avec le serveur RADIUS.
Solution possible	• Vérifiez que l'adresse IP du serveur RADIUS fournie dans la configuration d'authentificatio distance du DCM est correcte. • Assurez-vous que le serveur RADIUS est accessible à partir du DCM. • Assurez-vous que le DCM est configuré en tant que client valide sur le serveur RADIUS (le serveur RADIUS abandonne silencieusement les paquets Access-Request de clients inconnus). • Assurez-vous que le secret partagé configuré sur le DCM est le même que le secret partag configuré sur le serveur RADIUS pour ce DCM particulier. (Si le serveur ne possède pas d secret partagé pour le client, la demande est abandonnée silencieusement.)
Ligne de journal	Échec de la tentative de connexion à distance : [Erreur 10054] Une connexion existante a été fermée de force par l'hôte distant.
Problème	Le DCM a envoyé une requête RADIUS à l'adresse IP du serveur spécifié. Cependant, l'application serveur RADIUS n'écoute pas le port spécifié dans les paramètres d'authentificatio distante.
Solution possible	• Vérifiez que le serveur RADIUS est en cours d'exécution. • Vérifiez que le numéro de port spécifié dans la configuration RADIUS sur le serveur est identique à celui configuré sur le DCM.
Ligne de journal	Échec de la tentative de connexion à distance : Nom d'attribut spécifié ou réponse non valide à partir des données d'autorisation manquantes du serveur RADIUS.
Problème	Il y a un problème avec la réponse reçue du serveur RADIUS.
Solution possible	• Assurez-vous que le serveur RADIUS envoie l'attribut (configuré sur le DCM) dans la réponse Access-Accept.

	• Assurez-vous que le paramètre **Attribute Name** configuré sur les paramètres d'authentification distante DCM est le nom exact spécifié dans la configuration utilisateur su le serveur RADIUS.
Ligne de journal	Données d'autorisation non valides reçues du serveur RADIUS.
Problème	L'authentification a réussi mais la réponse reçue du serveur RADIUS contient des données d'autorisation non valides, par exemple le nom du groupe de sécurité.
Solution possible	• Assurez-vous que le nom de groupe configuré sur le serveur RADIUS pour cet utilisateur e l'un des noms de groupe de sécurité spécifiés dans la section Configuration du serveur RADIUS. • Assurez-vous que le format de la chaîne configurée sur le serveur RADIUS est celui spécif dans la section Configuration du serveur RADIUS.