Comment configurer le concentrateur Cisco VPN 3000 pour une prise en charge de l'authentification TACACS+ pour les comptes de gestion

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Conventions
Configurer le serveur TACACS+
Ajouter une entrée pour le concentrateur VPN 3000 dans le serveur TACACS+
Ajouter un compte d'utilisateur dans le serveur TACACS+
Modifier le groupe sur le serveur TACACS+
Configurer le concentrateur VPN 3000
Ajouter une entrée pour le serveur TACACS+ dans le concentrateur VPN 3000
Modifier le compte Admin sur le concentrateur VPN pour l'authentification TACACS+
Vérification
Dépannage
Informations connexes

Introduction

Ce document fournit des instructions détaillées afin de configurer les concentrateurs de la gamme Cisco VPN 3000 pour prendre en charge l'authentification TACACS+ pour les comptes de gestion.

Dès qu'un serveur TACACS+ est configuré sur le concentrateur VPN 3000, les noms de compte et mots de passe configurés localement, tels que admin, config, isp, etc., ne sont plus utilisés. Toutes les connexions au concentrateur VPN 3000 sont envoyées au serveur TACACS+ externe configuré pour la vérification des utilisateurs et des mots de passe.

La définition d'un niveau de privilège pour chaque utilisateur sur le serveur TACACS+ détermine les autorisations sur le concentrateur VPN 3000 pour chaque nom d'utilisateur TACACS+. Ensuite, associez-le au niveau d'accès AAA défini sous le nom d'utilisateur configuré localement sur le concentrateur VPN 3000. C'est un point important car dès qu'un serveur TACACS+ est défini, les noms d'utilisateur configurés localement sur le concentrateur VPN 3000 ne sont plus valides. Cependant, ils sont toujours utilisés uniquement afin de faire correspondre le niveau de privilège retourné par le serveur TACACS+, avec le niveau d'accès AAA sous cet utilisateur local. Le nom d'utilisateur TACACS+ se voit ensuite attribuer les privilèges définis par l'utilisateur du

concentrateur VPN 3000 configuré localement sous son profil.

Par exemple, décrit en détail dans les sections de configuration, un utilisateur/groupe TACACS+ est configuré pour renvoyer un niveau de privilège TACACS+ de 15. Dans la section Administrateurs du concentrateur VPN 3000, le niveau d'accès AAA de l'utilisateur administrateur est également défini sur 15. Cet utilisateur est autorisé à modifier la configuration sous toutes les sections et à lire/écrire des fichiers. Comme les niveaux de privilège TACACS+ et AAA correspondent, l'utilisateur TACACS+ bénéficie de ces autorisations sur le concentrateur VPN 3000.

Par exemple, si vous décidez qu'un utilisateur doit pouvoir modifier la configuration, mais *non* les fichiers en lecture/écriture, attribuez-lui un niveau de privilège de 12 sur le serveur TACACS+. Vous pouvez choisir n'importe quel nombre entre un et 15. Ensuite, sur le concentrateur VPN 3000, sélectionnez l'un des autres administrateurs configurés localement. Ensuite, définissez son niveau d'accès AAA sur 12, et définissez les autorisations sur cet utilisateur afin de pouvoir modifier la configuration, mais pas pour lire/écrire des fichiers. En raison du niveau d'accès/privilège correspondant, l'utilisateur obtient ces autorisations lorsqu'il se connecte.

Les noms d'utilisateur configurés localement sur le concentrateur VPN 3000 ne sont plus utilisés. Mais les droits d'accès et les niveaux d'accès AAA sous chacun de ces utilisateurs sont utilisés afin de définir les privilèges qu'un utilisateur TACACS+ particulier obtient lors de votre connexion.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Assurez-vous que vous disposez d'une connectivité IP au serveur TACACS+ à partir du concentrateur VPN 3000. Si votre serveur TACACS+ est orienté vers l'interface publique, n'oubliez pas d'ouvrir TACACS+ (port TCP 49) sur le filtre public .
- Assurez-vous que l'accès de sauvegarde via la console est opérationnel. Il est facile de verrouiller accidentellement tous les utilisateurs de la configuration lors de la première configuration. La seule façon de récupérer l'accès est via la console, qui utilise toujours les noms d'utilisateur et les mots de passe configurés localement.

Components Used

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

- Logiciel du concentrateur VPN Cisco 3000 version 4.7.2.B (sinon, toute version du logiciel du système d'exploitation 3.0 ou ultérieure fonctionne.)
- Cisco Secure Access Control Server pour serveurs Windows version 4.0 (toute version de logiciel 2.4 ou ultérieure fonctionne également.)

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

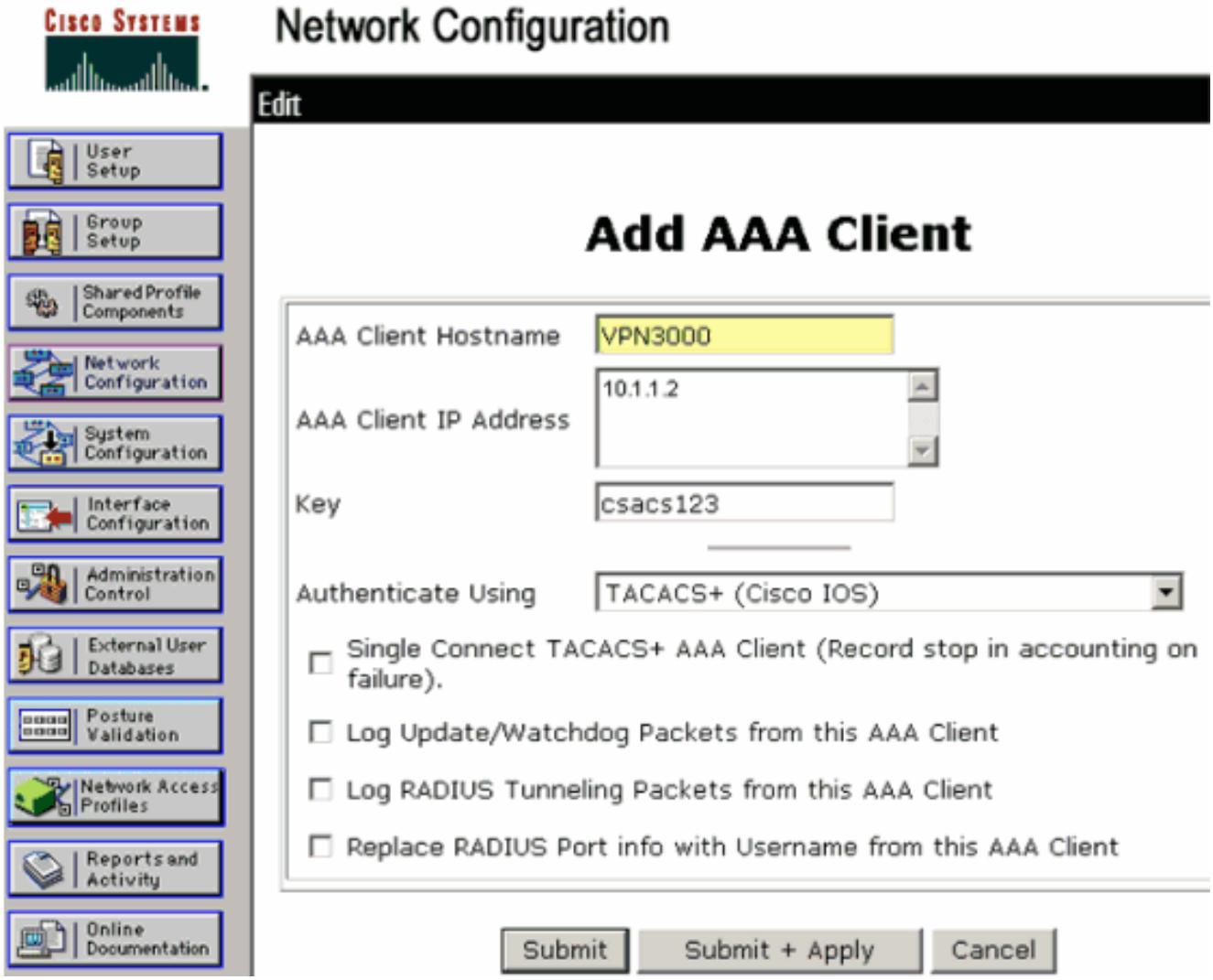
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurer le serveur TACACS+

Ajouter une entrée pour le concentrateur VPN 3000 dans le serveur TACACS+

Complétez ces étapes afin d'ajouter une entrée pour le concentrateur VPN 3000 dans le serveur TACACS+.

1. Cliquez sur **Configuration réseau** dans le panneau de gauche. Sous Clients AAA, cliquez sur **Ajouter une entrée**.
2. Dans la fenêtre suivante, remplissez le formulaire pour ajouter le concentrateur VPN en tant que client TACACS+. Cet exemple utilise :Nom d'hôte du client AAA = **VPN3000**Adresse IP du client AAA = **10.1.1.2**Clé = **csac123**Authentifier à l'aide de = **TACACS+ (Cisco IOS)**Cliquez sur **Soumettre + Redémarrer**.



Ajouter un compte d'utilisateur dans le serveur TACACS+

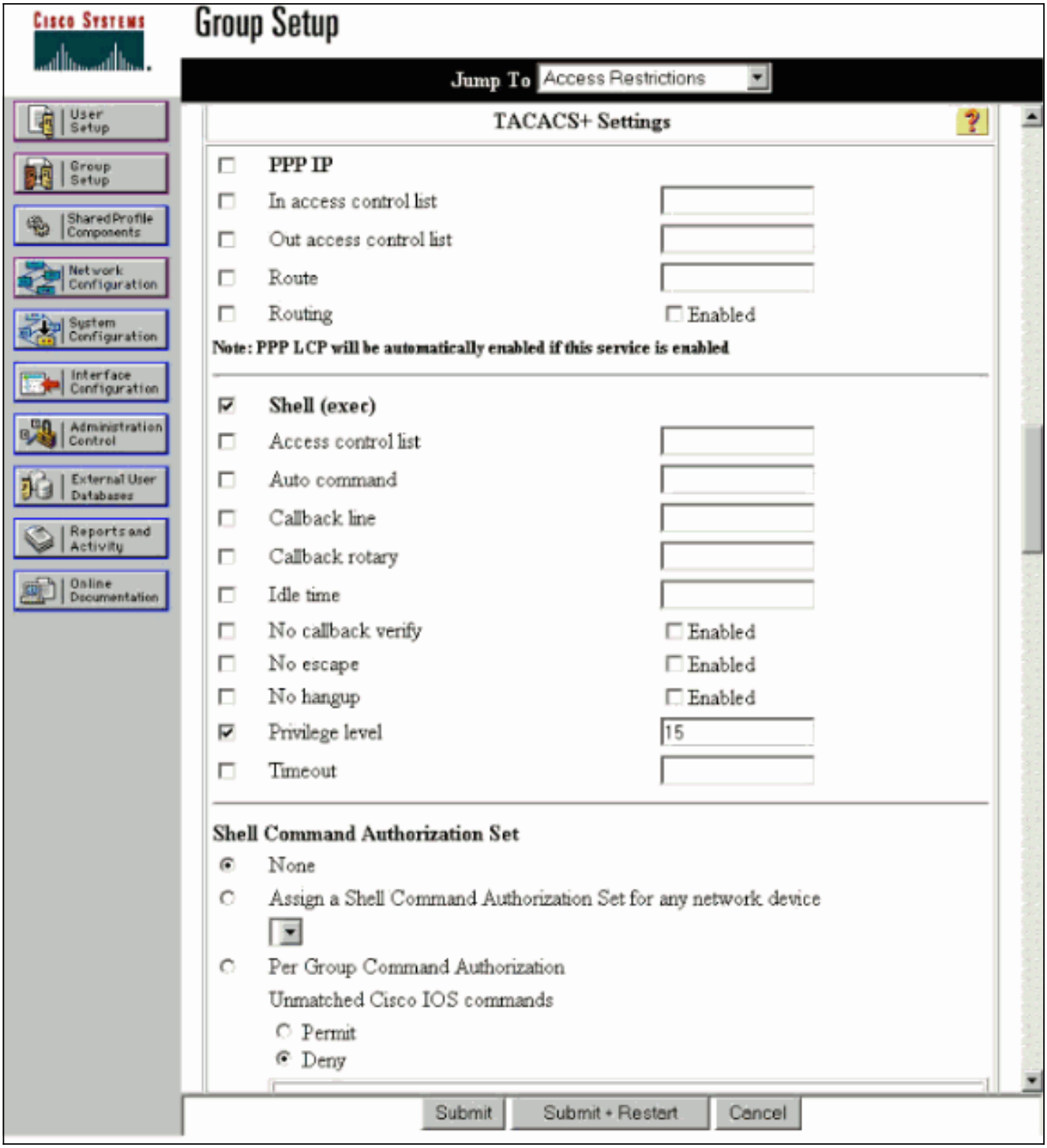
Complétez ces étapes afin d'ajouter un compte d'utilisateur dans le serveur TACACS+.

1. Créez un compte d'utilisateur dans le serveur TACACS+ qui pourra être utilisé ultérieurement pour l'authentification TACACS+. Cliquez sur **Configuration utilisateur** dans le panneau de gauche, ajoutez l'utilisateur « johnsmith » et cliquez sur **Ajouter/Modifier** pour faire ceci.
2. Ajoutez un mot de passe pour cet utilisateur et affectez-le à un groupe ACS qui contient les autres administrateurs du concentrateur VPN 3000.**Remarque :** Cet exemple définit le niveau de privilège sous ce profil de groupe ACS utilisateur particulier. Si cela doit être fait par utilisateur, choisissez **Interface Configuration > TACACS+ (Cisco IOS)** et cochez la case **User** pour le service Shell (exec). Les options TACACS+ décrites dans ce document sont alors disponibles sous chaque profil utilisateur.

Modifier le groupe sur le serveur TACACS+

Exécutez ces étapes pour modifier le groupe sur le serveur TACACS+.

1. Cliquez sur **Configuration du groupe** dans le panneau de gauche.
2. Dans le menu déroulant, sélectionnez le groupe auquel l'utilisateur a été ajouté dans la section Ajouter un compte d'utilisateur de la section Serveur TACACS+, qui est le groupe 1 dans cet exemple, puis cliquez sur **Modifier les paramètres**.
3. Dans la fenêtre suivante, assurez-vous que ces attributs sont sélectionnés sous Paramètres TACACS+ :**Shell (exec)Niveau de privilège = 15**Une fois terminé, cliquez sur **Soumettre + Redémarrer**.



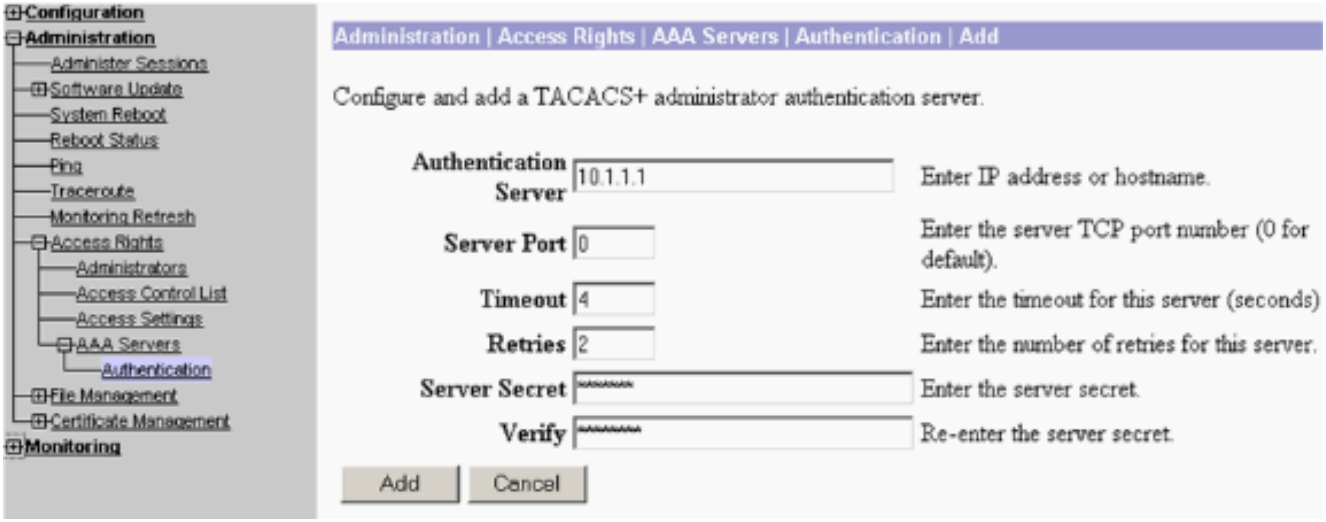
Configurer le concentrateur VPN 3000

Ajouter une entrée pour le serveur TACACS+ dans le concentrateur VPN 3000

Complétez ces étapes afin d'ajouter une entrée pour le serveur TACACS+ dans le concentrateur VPN 3000.

1. Choisissez **Administration > Access Rights > AAA Servers > Authentication** dans l'arborescence de navigation du panneau de gauche, puis cliquez sur **Add** dans le panneau de droite.Dès que vous cliquez sur **Add** afin d'ajouter ce serveur, les mots de passe/nom d'utilisateur configurés localement sur le concentrateur VPN 3000 ne sont plus utilisés. Assurez-vous que l'accès de sauvegarde via la console fonctionne en cas de verrouillage.

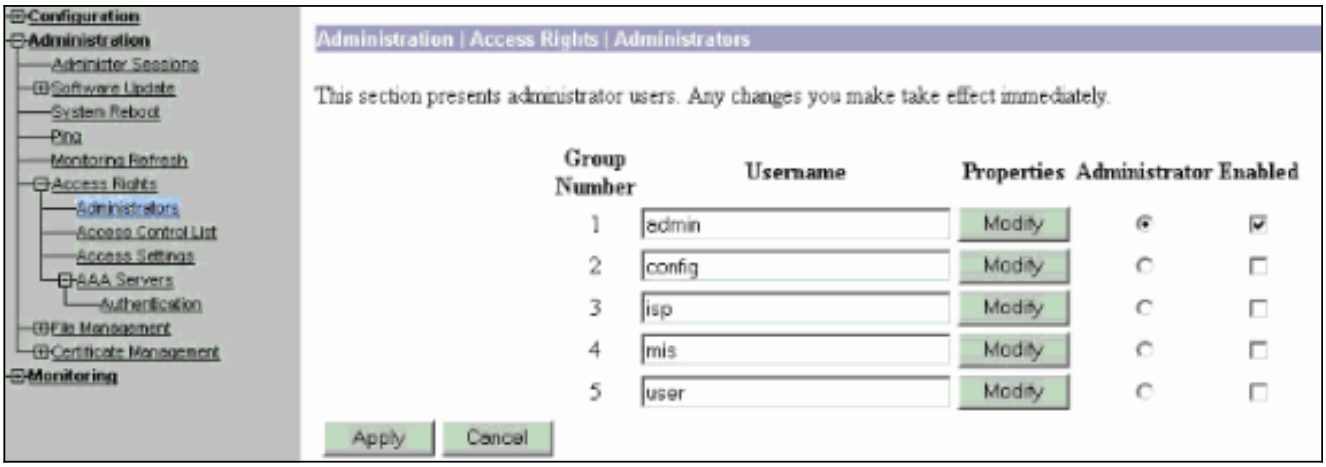
2. Dans la fenêtre suivante, remplissez le formulaire comme indiqué ici :Serveur d'authentification = **10.1.1.1** (adresse IP du serveur TACACS+)Port du serveur = **0** (valeur par défaut)Délai d'attente = **4**Nouvelles tentatives = **2**Secret du serveur = **csac123**Verify = **csac123**



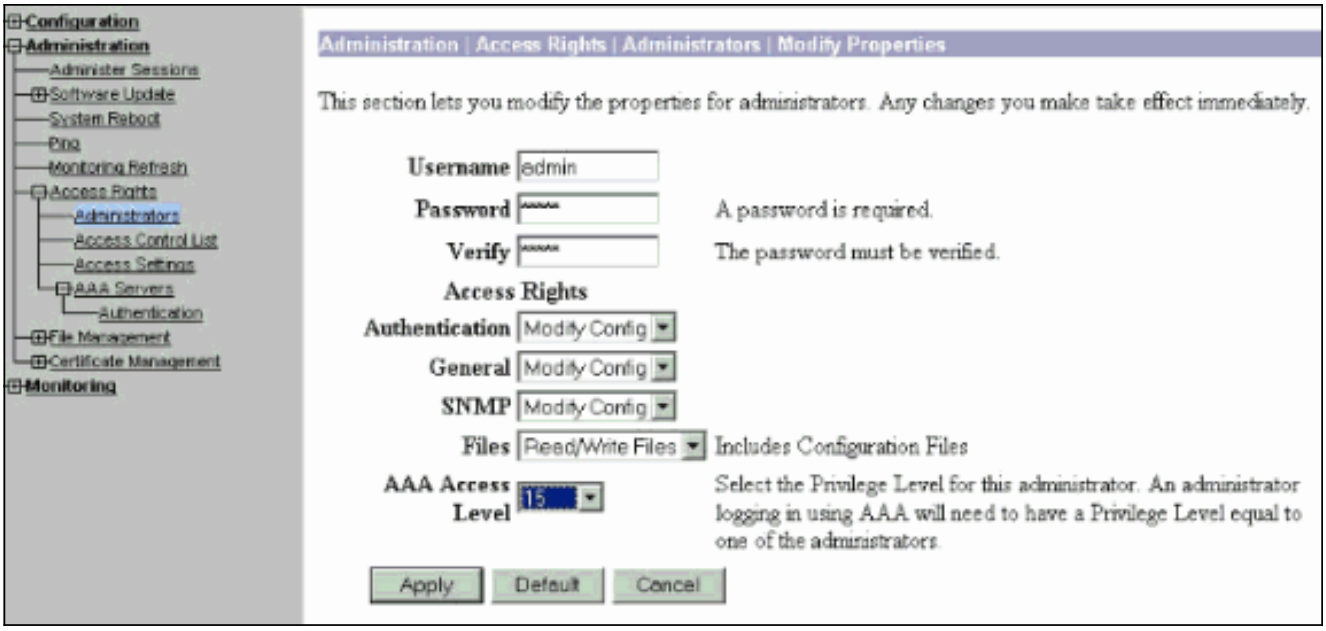
Modifier le compte Admin sur le concentrateur VPN pour l'authentification TACACS+

Complétez ces étapes pour modifier le compte d'administration sur le concentrateur VPN pour l'authentification TACACS+.

1. Cliquez sur **Modifier** pour l'administrateur de l'utilisateur afin de modifier les propriétés de cet utilisateur.



2. Choisissez le niveau d'accès AAA **15**.Cette valeur peut être un nombre compris entre un et 15. Notez qu'il doit correspondre au niveau de privilège TACACS+ défini sous le profil utilisateur/groupe sur le serveur TACACS+. L'utilisateur TACACS+ récupère ensuite les autorisations définies sous cet utilisateur du concentrateur VPN 3000 pour la modification de la configuration, la lecture/écriture de fichiers,
etc.



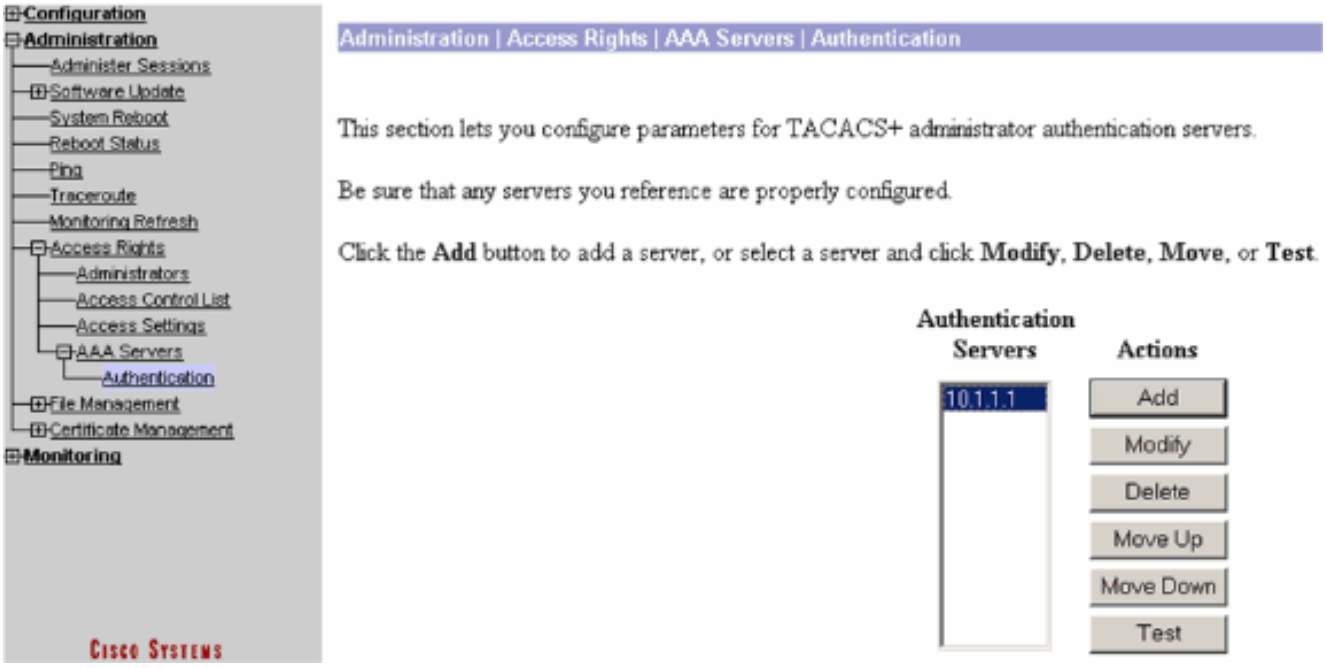
Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Suivez les étapes de ces instructions afin de dépanner votre configuration.

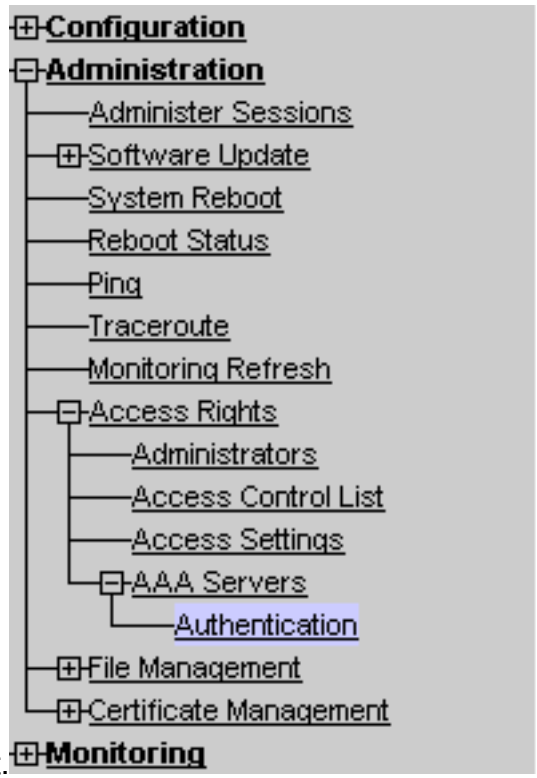
1. Afin de tester l'authentification :Pour les serveurs TACACS+Choisissez **Administration > Access Rights > AAA Servers > Authentication**.Sélectionnez votre serveur, puis cliquez sur **Test**.

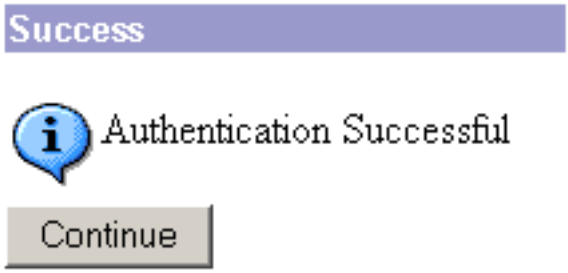


Remarque : lorsque le serveur TACACS+ est configuré dans l'onglet Administration, il n'est pas possible de configurer l'utilisateur pour l'authentification sur la base de données locale VPN 3000. Vous ne pouvez effectuer une reprise qu'à l'aide d'une autre base de données externe ou d'un serveur TACACS.Entrez le nom d'utilisateur et le mot de passe TACACS+, puis cliquez sur

OK.

Une authentification réussie





apparaît.

2. En cas d'échec, un problème de configuration ou de connectivité IP se produit. Vérifiez les messages liés à l'échec de la connexion sur le serveur ACS.Si aucun message n'apparaît dans ce journal, il y a probablement un problème de connectivité IP. La demande TACACS+ n'atteint pas le serveur TACACS+. Vérifiez que les filtres appliqués à l'interface du concentrateur VPN 3000 appropriée permettent l'entrée et la sortie de paquets TACACS+ (port TCP 49).Si l'échec s'affiche en tant que service refusé dans le journal, le service Shell (exec) n'a pas été correctement activé sous le profil utilisateur ou de groupe sur le serveur TACACS+.
3. Si l'authentification de test réussit, mais que les connexions au concentrateur VPN 3000 continuent à échouer, vérifiez le journal des événements filtrables via le port de console.Si vous voyez un message similaire :

```
65 02/09/2005 13:14:40.150 SEV=5 AUTH/32 RPT=2
User [ johnsmith ] Protocol [ HTTP ] attempted ADMIN logon.
Status: <REFUSED> authorization failure. NO Admin Rights
```

Ce message indique que le niveau de privilège attribué sur le serveur TACACS+ ne correspond à aucun niveau d'accès AAA pour les utilisateurs du concentrateur VPN 3000. Par exemple, l'utilisateur johnsmith a un niveau de privilège TACACS+ de 7 sur le serveur TACACS+, mais aucun des cinq administrateurs de concentrateur VPN 3000 n'a un niveau d'accès AAA de 7.

Informations connexes

- Page d'assistance des concentrateurs VPN Cisco 3000
- Page d'assistance du Client VPN 3000 Series Cisco
- Page de support de la négociation IPSec/des protocoles IKE
- Page de support TACACS/TACACS+
- TACACS+ dans la documentation d'IOS
- Support et documentation techniques - Cisco Systems