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

Contenu

Introduction

Ce document fournit des instructions pas à pas afin de configurer les Concentrateurs de la gamme Cisco VPN 3000 pour prendre en charge l'authentification TACACS+ pour des comptes de Gestion.

Dès qu'un serveur TACACS+ sera configuré sur le concentrateur VPN 3000, les noms du compte localement configurés et des mots de passe tels que l'admin, config, fournisseur d'accès internet, et ainsi de suite, ne sont plus utilisés. Toutes les procédures de connexion au concentrateur VPN 3000 sont envoyées au serveur externe configuré TACACS+ pour l'utilisateur et la vérification de mot 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+. Puis, correspondance qui vers le haut de avec le niveau d'accès d'AAA a défini sous le nom d'utilisateur localement configuré sur le concentrateur VPN 3000. C'est un point important parce que dès qu'un serveur TACACS+ sera défini, les noms d'utilisateur localement configurés sur le concentrateur VPN 3000 ne sont plus valides. Mais, ils sont encore utilisés afin de s'assortir seulement vers le

haut du niveau de privilège retourné du serveur TACACS+, avec le niveau d'accès d'AAA sous cet utilisateur local. Le nom d'utilisateur TACACS+ est alors assigné les privilèges que l'utilisateur localement configuré de concentrateur VPN 3000 a défini sous leur profil.

Par exemple, décrit en détail dans les sections de configuration, un utilisateur TACACS+/groupe est configuré pour renvoyer un niveau de privilège TACACS+ de 15. Sous la section d'administrateurs du concentrateur VPN 3000, l'utilisateur d'admin fait placer également son niveau d'accès d'AAA à 15. On permet à cet utilisateur pour modifier la configuration sous toutes les sections, et aux fichiers lecture/écriture. Puisque le niveau de privilège TACACS+ et niveau d'accès d'AAA s'assortissent, l'utilisateur TACACS+ est donné ces autorisations sur le concentrateur VPN 3000.

Comme exemple, si vous décidez que les besoins de l'utilisateur de pouvoir modifier la configuration, mais les fichiers non lecture/écriture, leur assignent un niveau de privilège de 12 sur le serveur TACACS+. Vous pouvez sélectionner tout nombre entre un et 15. Puis, sur le concentrateur VPN 3000, sélectionnez un des autres administrateurs localement configurés. Ensuite, placez son niveau d'accès d'AAA à 12, et placez les autorisations sur cet utilisateur afin de pouvoir modifier la configuration, mais pas aux fichiers lecture/écriture. En raison du privilège/du niveau d'accès assortis, l'utilisateur obtient autorisations quand ils ouvrent une session.

Les noms d'utilisateur localement configurés sur le concentrateur VPN 3000 ne sont plus utilisés. Mais, les droits d'accès et des niveaux d'accès d'AAA sous chacun de ces utilisateurs sont utilisés afin de définir les privilèges qu'un utilisateur particulier TACACS+ obtient quand vous ouvrez une session.

Conditions préalables

Conditions requises

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

- Assurez-vous que vous avez la connectivité IP au serveur TACACS+ du concentrateur VPN 3000. Si votre serveur TACACS+ est vers l'interface publique, n'oubliez pas d'ouvrir le TACACS+ (port TCP 49) sur le filtre public.
- Assurez que l'accès de sauvegarde par l'intermédiaire de la console est opérationnel. Il est facile de verrouiller accidentellement tous les utilisateurs hors de la configuration quand vous établissez d'abord ceci. La seule manière de récupérer l'accès est par l'intermédiaire de la console, qui utilise toujours les noms d'utilisateur et mot de passe localement configurés.

Composants utilisés

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

- Version de logiciel de logiciel du concentrateur de Cisco VPN 3000 4.7.2.B (alternativement, toute version de 3.0 ou travaux postérieurs de logiciel OS.)
- Version 4.0 de serveurs de Cisco Secure Access Control Server pour Windows (alternativement, toute version de 2.4 ou travaux postérieurs de logiciel.)

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 opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

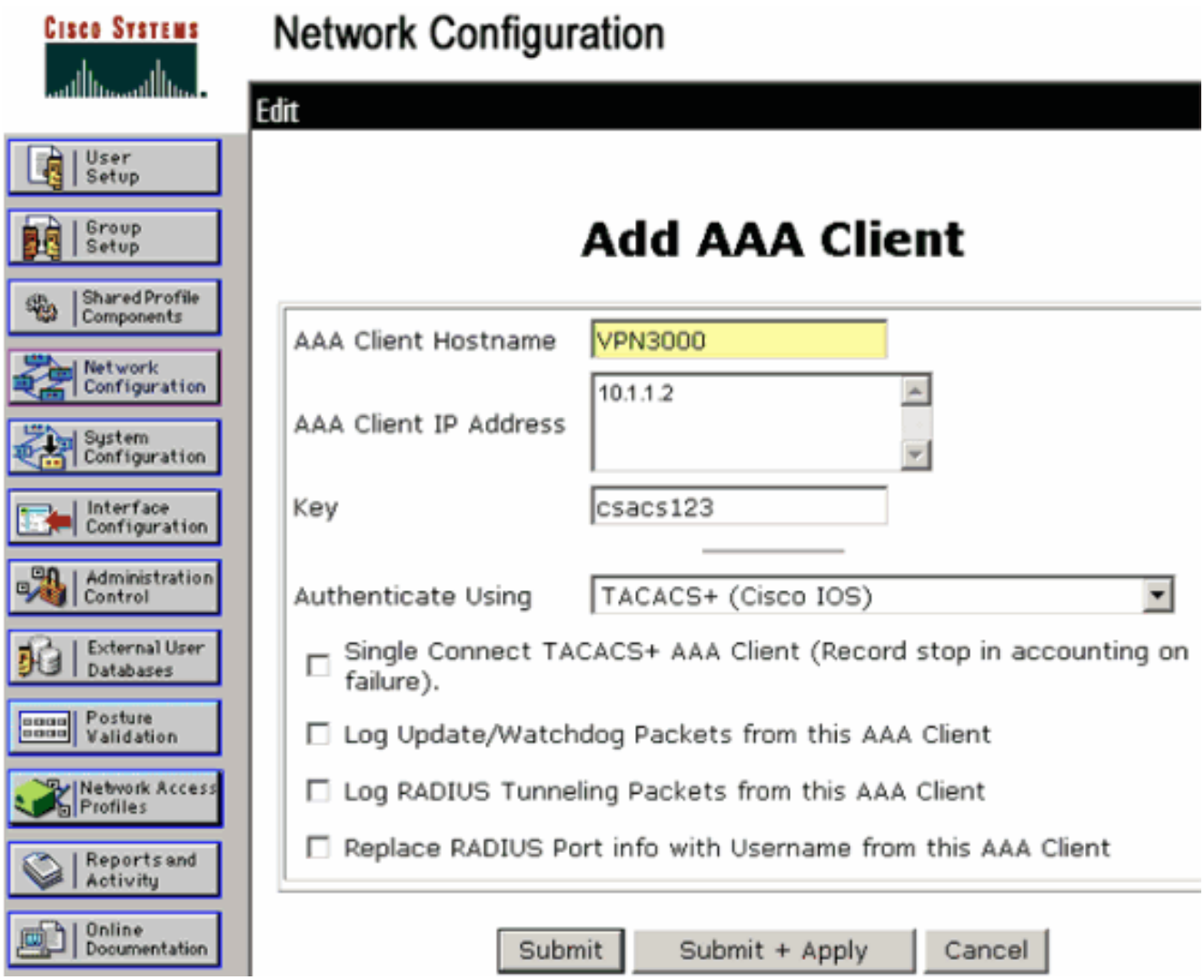
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez le serveur TACACS+

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

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

1. Cliquez sur Network Configuration dans le panneau gauche. Sous des clients d'AAA, cliquez sur Add l'**entrée**.
2. Sur la prochaine fenêtre, complétez la forme pour ajouter le concentrateur VPN en tant que client TACACS+. Cet exemple l'utilise :Adresse Internet de client d'AAA = **VPN3000**Adresse IP = **10.1.1.2 de** client d'AAAClé = **csacs123**Authentifiez utilisant = **TACACS+ (le Cisco IOS)**Cliquez sur Submit **+**
   reprise.



Ajoutez un compte utilisateur dans le serveur TACACS+

Terminez-vous ces étapes afin d'ajouter un compte utilisateur dans le serveur TACACS+.

1. Créez un compte utilisateur dans le serveur TACACS+ qui peut plus tard être utilisé pour l'authentification TACACS+. Cliquez sur User Setup dans le panneau gauche, ajoutez l'utilisateur « johnsmith » et cliquez sur Add**/l'éditez** afin de faire ceci.
2. Ajoutez un mot de passe pour cet utilisateur, et affectez l'utilisateur à un groupe ACS qui contient les autres administrateurs de concentrateur VPN 3000.**Remarque:** Cet exemple définit le niveau de privilège sous ce profil de groupe de l'utilisateur particulier ACS. Si ce doit être fait sur une base par utilisateur, choisissez la **configuration d'interface > le TACACS+ (Cisco IOS)** et cochez la case d'**utilisateur** pour le service de shell (exécutif). Sont seulement alors les options TACACS+ décrites dans ce de dessous disponible de document chaque profil utilisateur.

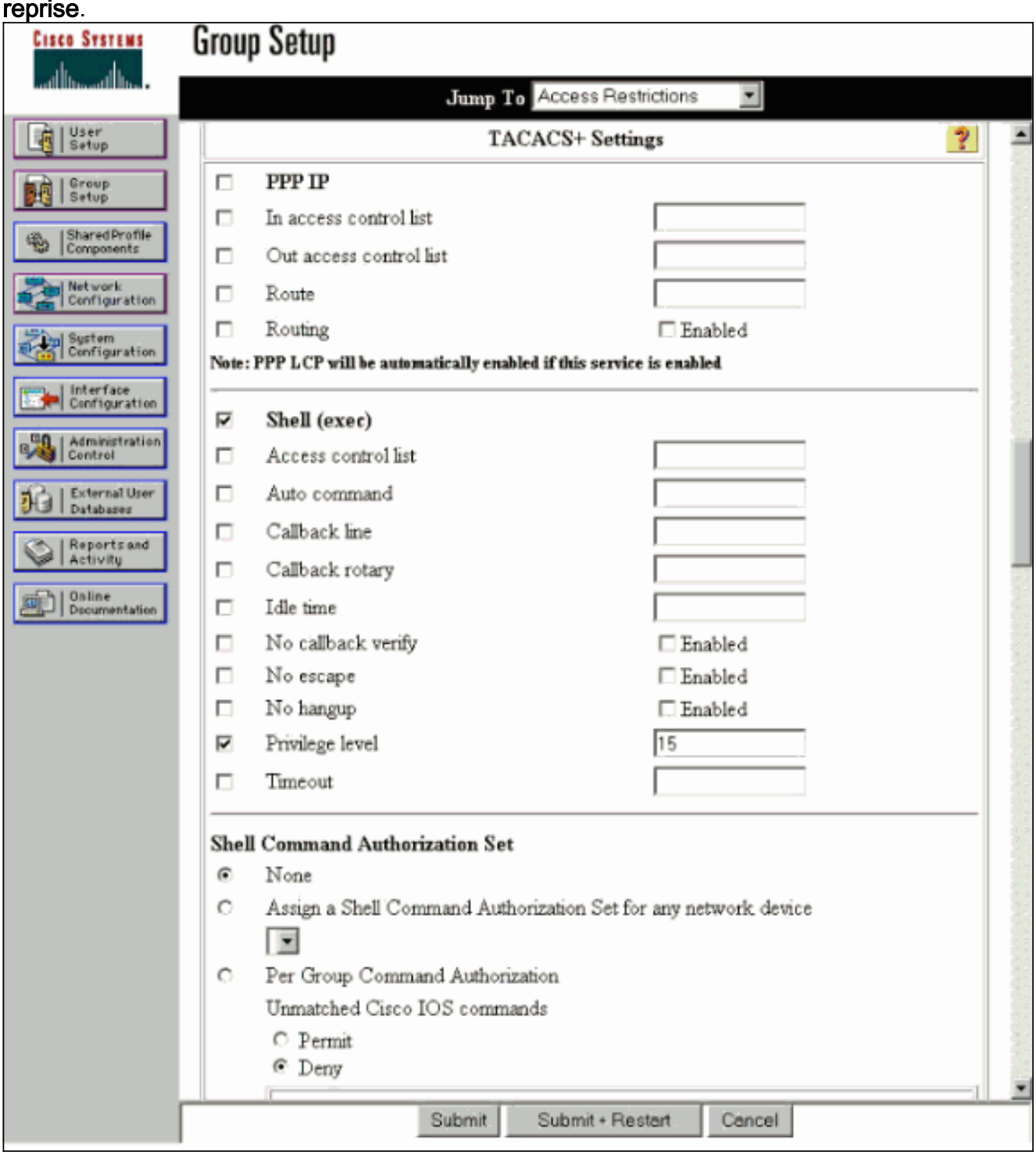
Éditez le groupe sur le serveur TACACS+

Terminez-vous ces étapes pour éditer le groupe sur le serveur TACACS+.

1. **Group Setup de** clic dans le panneau gauche.
2. Du menu déroulant, choisissez le groupe que l'utilisateur a été ajouté à dans l'ajouter un compte utilisateur dans la section Serveur TACACS+, qui est le groupe 1 dans cet exemple,

et cliquez sur Edit les **configurations**.

3. Sur la prochaine fenêtre, assurez-vous que ces attributs sont sélectionnés sous des configurations TACACS+ :**Shell (exécutif)Niveau de privilège = 15**Une fois que fait, cliquez sur Submit **+**
reprise.

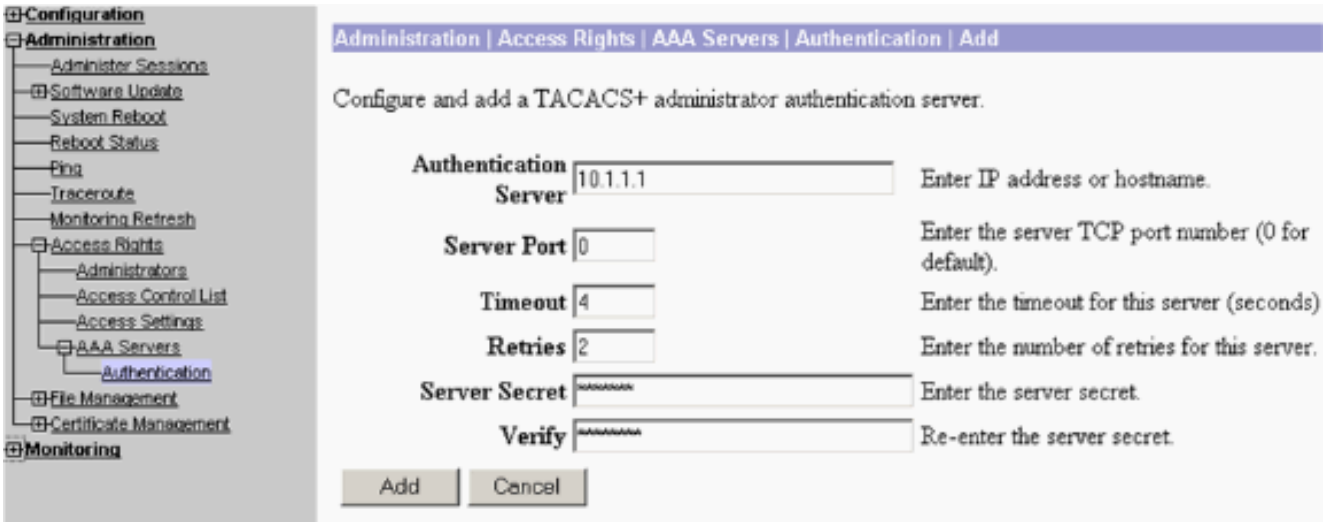


Configurez le concentrateur VPN 3000

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

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

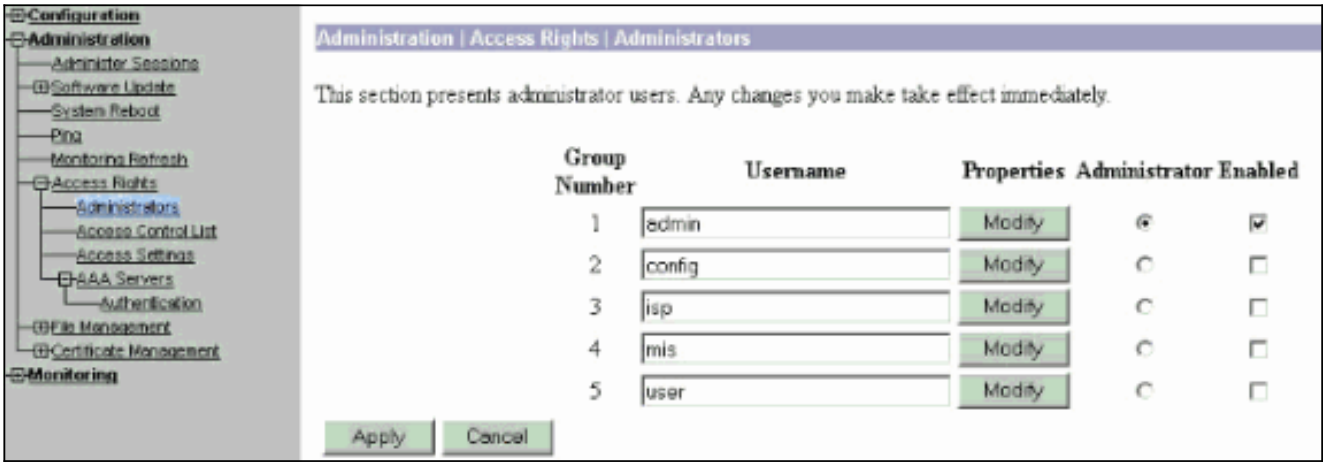
1. Choisissez la **gestion > les droits d'accès > les serveurs > l'authentification d'AAA** dans l'arborescence dans le panneau gauche, et puis cliquez sur Add au panneau de droite.Dès que vous cliquerez sur Add afin d'ajouter ce serveur, le nom d'utilisateur/mots de passe localement configurés sur le concentrateur VPN 3000 ne sont plus utilisés. Assurez l'accès de sauvegarde par l'intermédiaire des travaux de console en cas de lock-out.
2. Sur la prochaine fenêtre, complétez la forme comme vu ici :Serveur d'authentification = **10.1.1.1** (adresse IP de serveur TACACS+)Port de serveur = **0** (par défaut)Délai d'attente = **4**Relances = **2**Secret de serveur = **csacs123**Vérifiez = **csacs123**



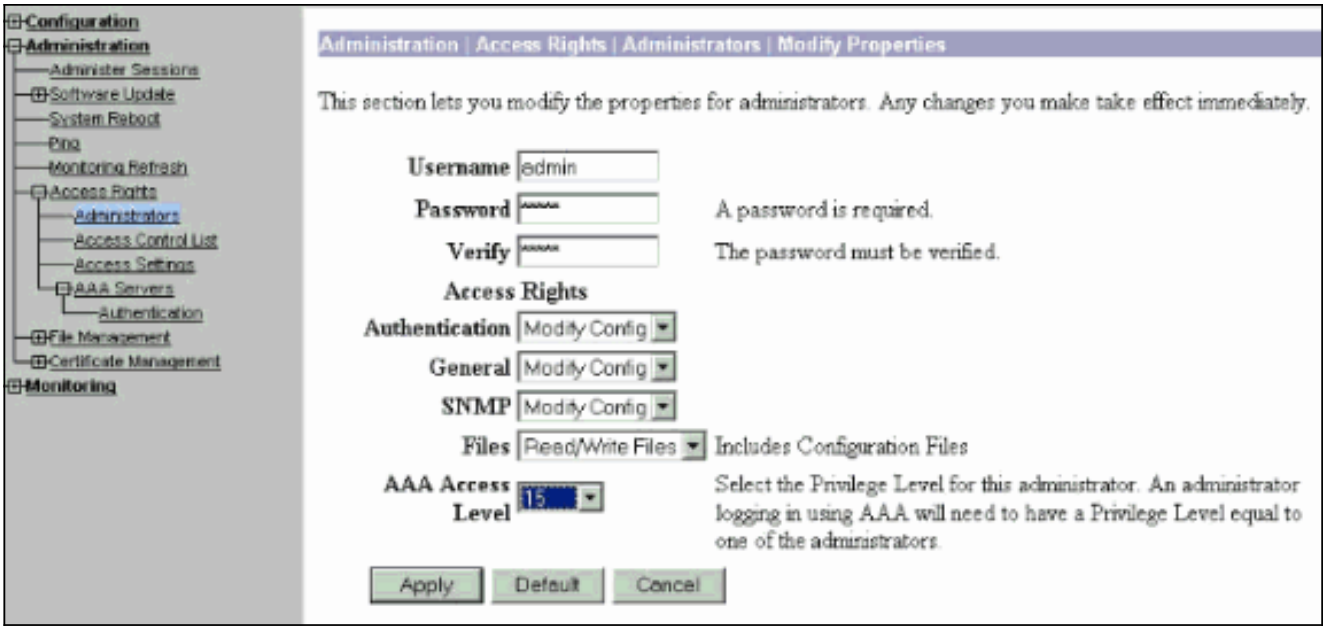
Modifiez le compte d'admin sur le concentrateur VPN pour l'authentification TACACS+

Terminez-vous ces étapes pour modifier le compte d'admin sur le concentrateur VPN pour l'authentification TACACS+.

1. Le clic **modifient** pour l'admin d'utilisateur afin de modifier les propriétés de cet utilisateur.



2. Choisissez le niveau d'accès d'AAA en tant que **15**.Cette valeur peut être tout nombre entre une et 15. Notez qu'il doit apparier le niveau de privilège TACACS+ défini sous le profil d'utilisateur/groupe sur le serveur TACACS+. L'utilisateur TACACS+ prend alors les autorisations définies sous cet utilisateur de concentrateur VPN 3000 pour la modification de la configuration, des fichiers de lecture/écriture, et ainsi de suite.



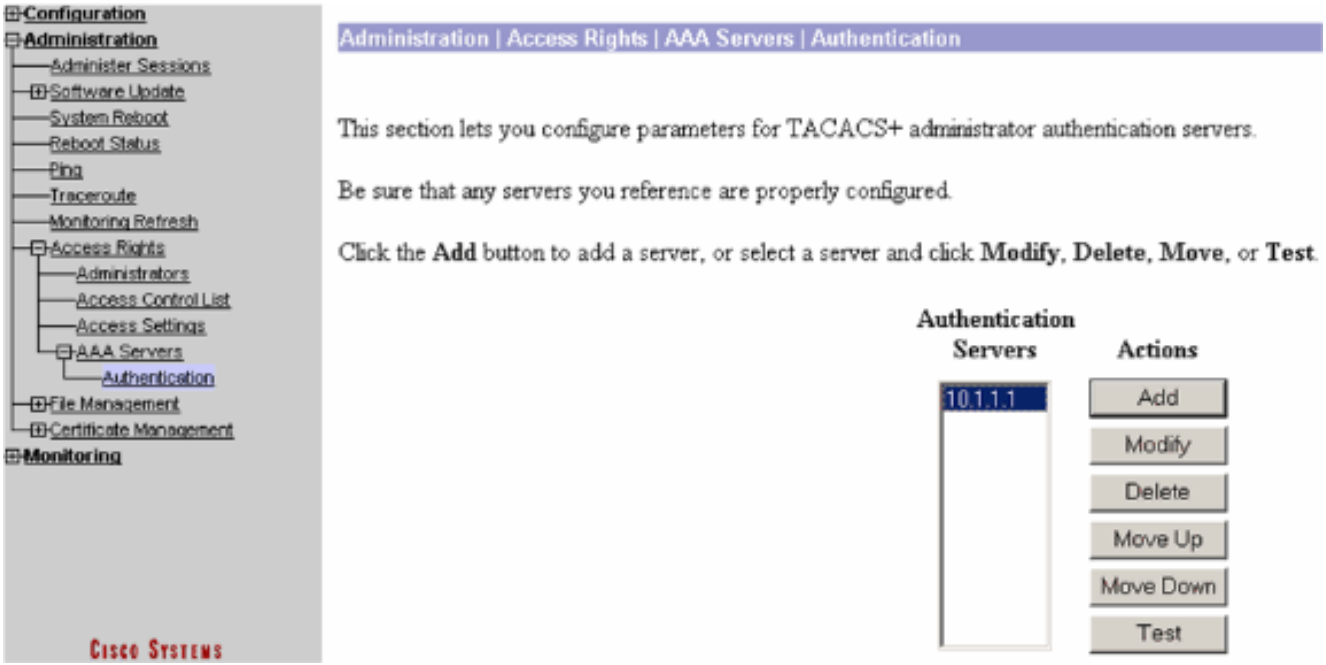
Vérifiez

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

Dépannez

Terminez-vous les étapes dans ces instructions afin de dépanner votre configuration.

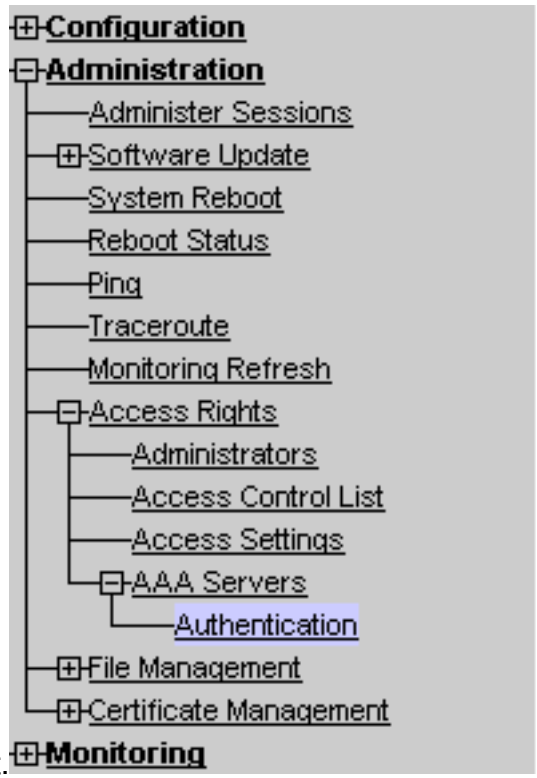
1. Afin de tester l'authentification :Pour des serveurs TACACS+Choisissez la **gestion > les droits d'accès > les serveurs > l'authentification d'AAA**.Sélectionnez votre serveur, et puis cliquez sur le
test.

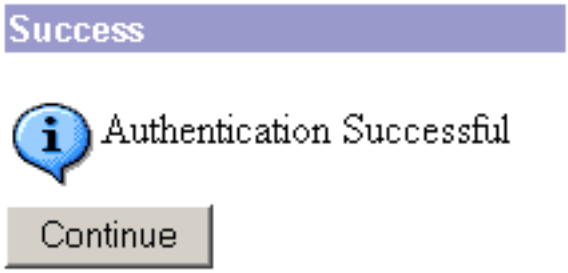


Remarque: Quand le serveur TACACS+ est configuré sur l'onglet Administration, il n'y a aucune manière d'installer l'utilisateur pour authentifier sur la base de données locale VPN 3000. Vous pouvez seulement retour utilisant une base de données externe ou un serveur TACACS différente.Écrivez le nom d'utilisateur et mot de passe TACACS+ et cliquez sur

OK.

Une authentification réussie





apparaît.

2. S'il échoue, il y a un problème de configuration ou un problème de connectivité IP. Vérifiez le login d'essais ratés le serveur ACS pour des messages liés à la panne.Si message n'apparaît pas dans ce log puis il y a probablement un problème de connectivité IP. La demande TACACS+ n'atteint pas le serveur TACACS+. Vérifiez les filtres appliqués à l'interface appropriée de concentrateur VPN 3000 permet des paquets TACACS+ (port TCP 49) dedans et.Si les affichages de panne comme service refusaient dans le log, alors le service de shell (exécutif) n'a pas été correctement activé sous le profil d'utilisateur ou de groupe sur le serveur TACACS+.
3. Si le test d'authentification est réussi, mais les procédures de connexion au concentrateur VPN 3000 continuent à échouer, vérifiez le journal d'événements filtrables par l'intermédiaire du port de console.Si vous voyez un message semblable :
   `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 assigné sur le serveur TACACS+ n'a aucun niveau d'accès assorti d'AAA sous les utilisateurs l'uns des de concentrateur VPN 3000. Par exemple, le johnsmith d'utilisateur 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 d'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