Configurer le concentrateur de Cisco VPN 3000 avec le RAYON de Microsoft

Contenu

Introduction

Le système commercial de Microsoft Internet Authentication Server (IAS) et d'Internet de Microsoft (MCIS 2.0) sont actuellement disponible. Le serveur de RAYON de Microsoft est commode parce qu'il utilise le Répertoire actif sur Primary Domain Controller pour sa base de données utilisateur. Vous ne devez plus mettre à jour une base de données distincte. Il prend en charge également le cryptage 40-bit et 128-bit pour des connexions VPN de Protocole PPTP (Point-to-Point Tunneling Protocol). Référez-vous à la liste de contrôle de Microsoft : Configurer IAS pour le pour en savoir plus de connexion à distance et de documentation d'accès VPN.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

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

Installez et configurez le serveur de RAYON sur le Windows 2000 et le Windows 2003

Installez le serveur de RAYON

Si vous ne faites pas installer déjà le serveur de RAYON (IAS), exécutez ces étapes afin d'installer. Si vous faites déjà installer le serveur de RAYON, continuez aux étapes de configuration.

1. Insérez le compact disc de Windows Server et commencez le programme de configuration.
2. Cliquez sur **installent les composants ajoutés**, et puis cliquent sur Add**/retirent des composants de Windows**.
3. Dans des composants, les **services de réseau de** clic (mais ne sélectionnez pas ou effacez la case), et cliquent sur alors des **détails**.
4. Vérifiez le **Service d'authentification Internet** et cliquez sur OK.
5. Cliquez sur **Next** (Suivant).

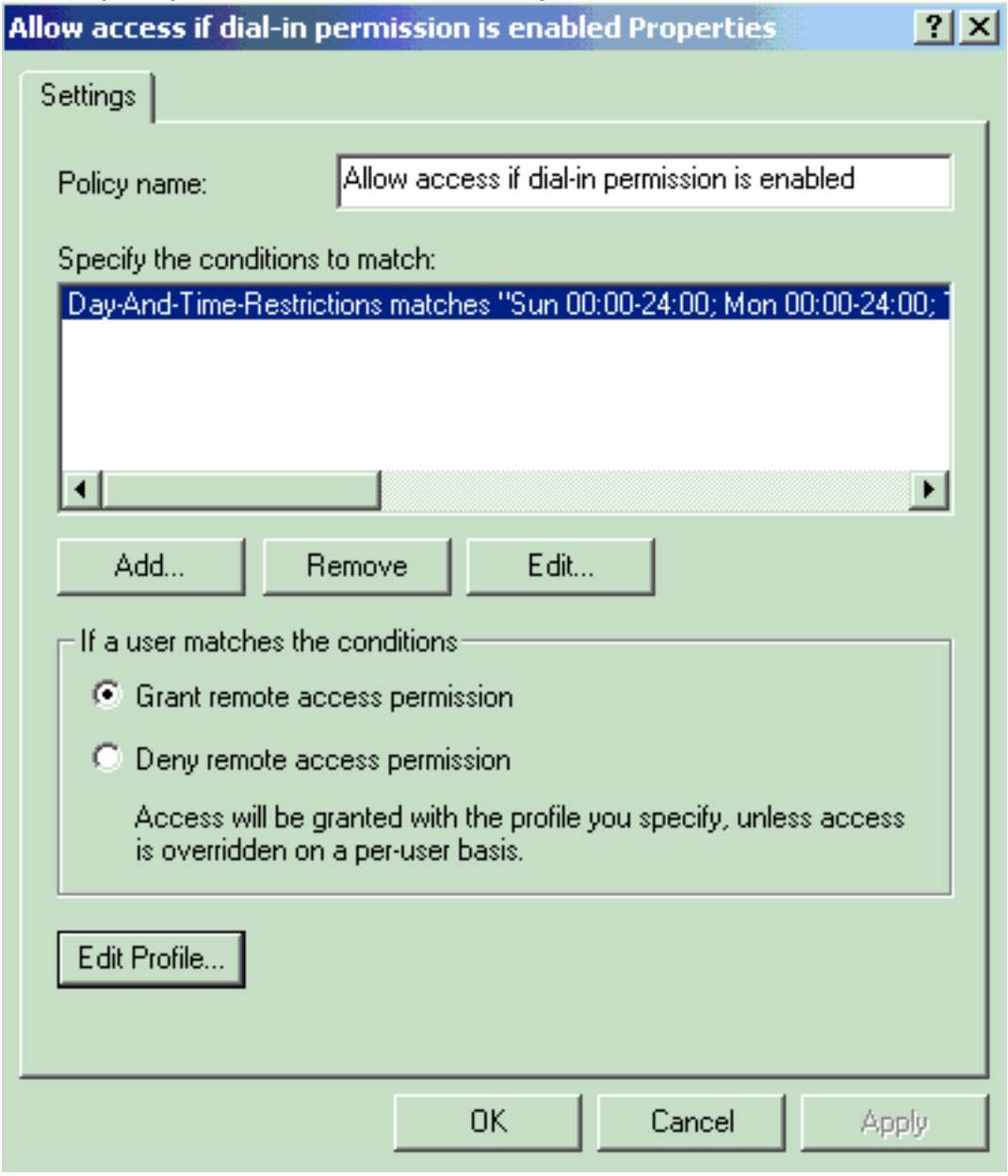
Configurez le Microsoft Windows 2000 Server avec IAS

Terminez-vous ces étapes afin de configurer le serveur de RAYON (IAS) et commencer le service afin de le rendre disponible pour authentifier des utilisateurs sur le concentrateur VPN.

1. Choisissez le **Start > Programs > Administrative tools > le Service d'authentification Internet**.
2. Cliquez avec le bouton droit le **Service d'authentification Internet**, et cliquez sur **Properties du** sous-menu qui apparaît.
3. Allez à l'onglet de RAYON afin d'examiner les configurations pour des ports.Si des ports de Protocole UDP (User Datagram Protocol) votre authentification de RAYON et comptabilité de RAYON diffèrent des valeurs par défaut fournies (1812 et 1645 pour l'authentification, 1813 et 1646 pour la comptabilité) en authentification et comptabilité, tapez vos configurations de port. Cliquez sur **OK** quand vous avez terminé.**Note**: Ne changez pas les ports par défaut. Séparez les ports à l'aide des virgules pour utiliser des configurations de plusieurs ports pour des demandes d'authentification ou de comptabilité.
4. Cliquez avec le bouton droit les **clients** et choisissez le **nouveau client** afin d'ajouter le concentrateur VPN en tant que client d'Authentification, autorisation et comptabilité (AAA) au serveur de RAYON (IAS).**Note**: Si la Redondance est configurée entre deux concentrateurs de Cisco VPN 3000, le concentrateur de sauvegarde de Cisco VPN 3000 doit également être ajouté au serveur de RAYON en tant que client RADIUS.
5. Écrivez un nom amical et le sélectionnez comme **rayon de Protocol**.
6. Définissez le concentrateur VPN avec une adresse IP ou un nom DNS sur la prochaine fenêtre.
7. Choisissez **Cisco de la** barre de défilement de Client-constructeur.
8. Écrivez un secret partagé.**Note**: Vous devez se souvenir le secret *précis* que vous utilisez.

Vous avez besoin de ces informations afin de configurer le concentrateur VPN.

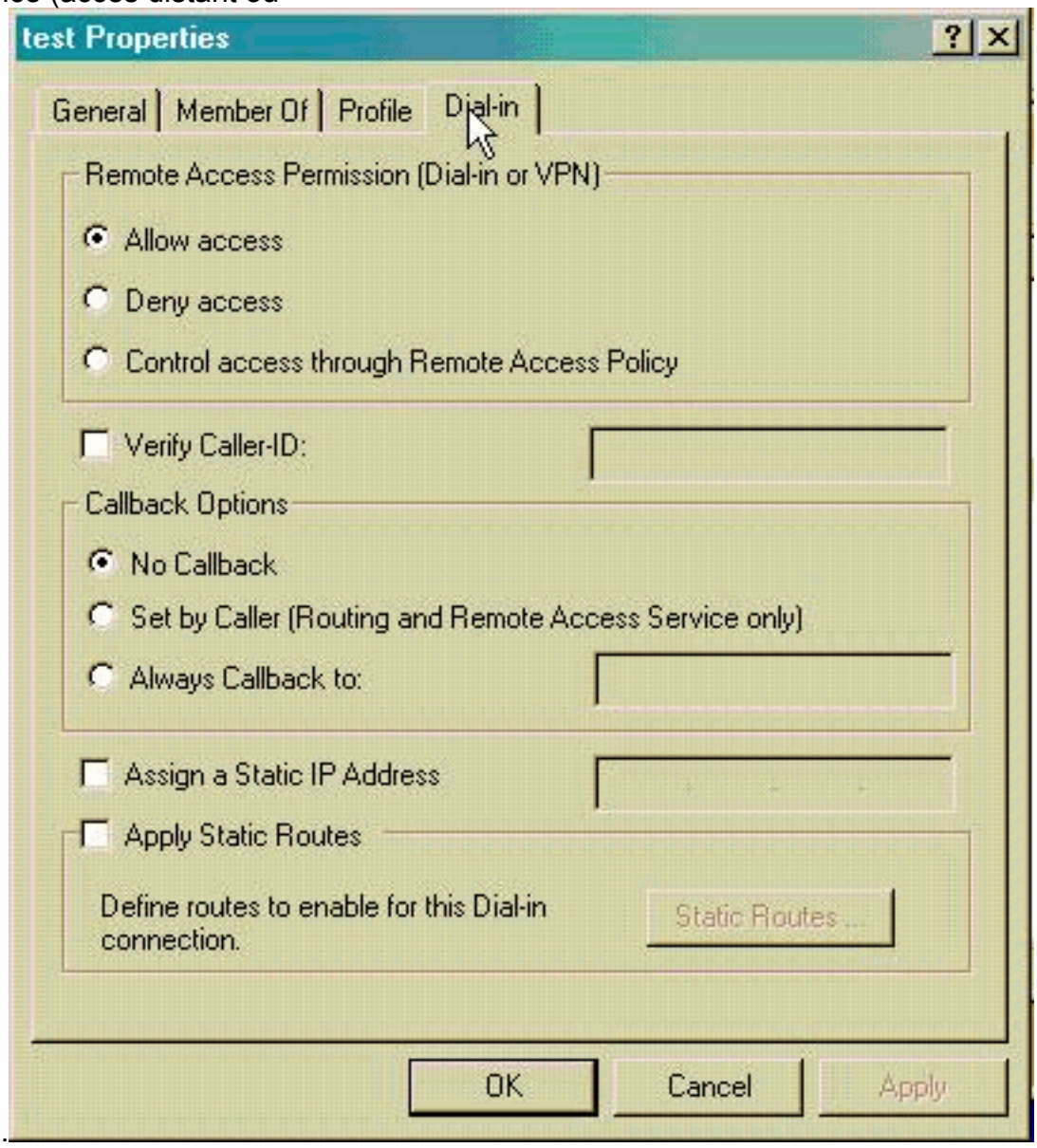
9. Cliquez sur **Finish** (Terminer).
10. Double-cliquer les **stratégies d'accès à distance** et double-cliquer la stratégie qui apparaît dans le côté droit de la fenêtre.**Note**: Après que vous installiez IAS, une stratégie d'accès à distance devrait déjà exister.Dans le Windows 2000, l'autorisation est accordée basée sur les propriétés d'accès distant d'un compte utilisateur et des stratégies d'accès à distance. Les stratégies d'accès à distance sont un ensemble de conditions et les paramètres de connexion qui donnent à des administrateurs réseau plus de flexibilité dans l'autorisation de la connexion tente. Acheminement et service d'accès distant du Windows 2000 et le Windows 2000 IAS les deux stratégies d'accès à distance d'utilisation pour déterminer si recevoir ou rejeter des tentatives de connexion. Dans des les deux cas, les stratégies d'accès à distance sont enregistrées localement. Référez-vous à la documentation d'IAS de Windows 2000 pour plus d'informations sur la façon dont des tentatives de connexion sont traitées.



11. Choisissez l'**autorisation d'Accès à distance de Grant** et cliquez sur Edit le **profil** afin de configurer des propriétés d'accès distant.
12. Sélectionnez le protocole pour l'utiliser pour l'authentification sur l'onglet d'authentification. Vérifiez la **version 2 d'authentification chiffrée par Microsoft** et décochez tous autres Protocoles d'authentification.**Note**: Les configurations dans ce profil d'accès distant doivent

apparier les configurations dans la configuration et le client entrant de concentrateur VPN 3000. Dans cet exemple MS-CHAPv2 l'authentification sans cryptage PPTP est utilisée.

13. Sur le contrôle d'onglet de cryptage **aucun cryptage** seulement.
14. Cliquez sur OK afin de clôturer le profil d'accès distant, puis cliquez sur OK afin de fermer la fenêtre de stratégie d'accès à distance.
15. Cliquez avec le bouton droit le **Service d'authentification Internet** et cliquez sur le **service de début** dans l'arborescence de la console.**Note**: Vous pouvez également employer cette fonction pour arrêter le service.
16. Terminez-vous ces étapes afin de modifier les utilisateurs pour permettre la connexion.Choisissez la **console > l'ajout/suppression SNAP-dans**.Cliquez sur Add et choisissez les **utilisateurs locaux et les groupes SNAP-dans**.Cliquez sur **Add**.Veillez à sélectionner l'**ordinateur local**Cliquez sur Finish et **APPROUVEZ**.
17. Développez l'**utilisateur local et les groupes** et cliquez sur le répertoire d'**utilisateurs** dans le volet gauche. Dans le volet de droite, double-cliquer l'utilisateur (utilisateur VPN) que vous voulez permettre l'accès.
18. Allez à l'onglet Numérotation et choisissez **permettent Access** sous l'autorisation d'Accès à distance (accès distant ou



VPN).

19. Cliquez sur Apply et **APPROUVEZ** afin de se terminer l'action. Vous pouvez fermer la fenêtre de Gestion de console et sauvegarder la session, si désiré.Les utilisateurs que vous

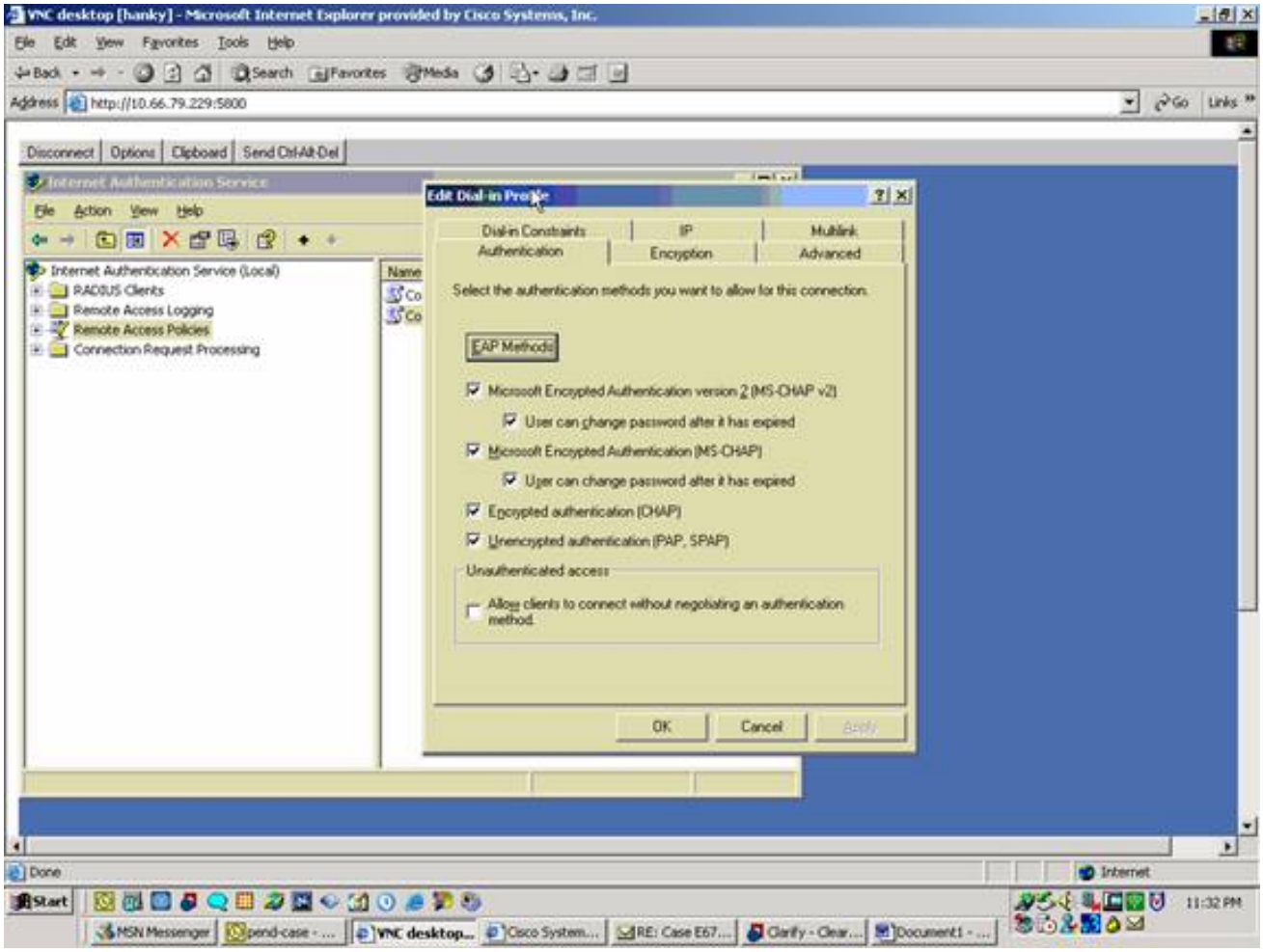
avez modifiés peuvent maintenant accéder au concentrateur VPN avec le client vpn. Maintenez dans l'esprit que le serveur d'IAS authentifie seulement les informations utilisateur. Le concentrateur VPN fait toujours l'authentification de groupe.

Configurez le serveur de Microsoft Windows 2003 avec IAS

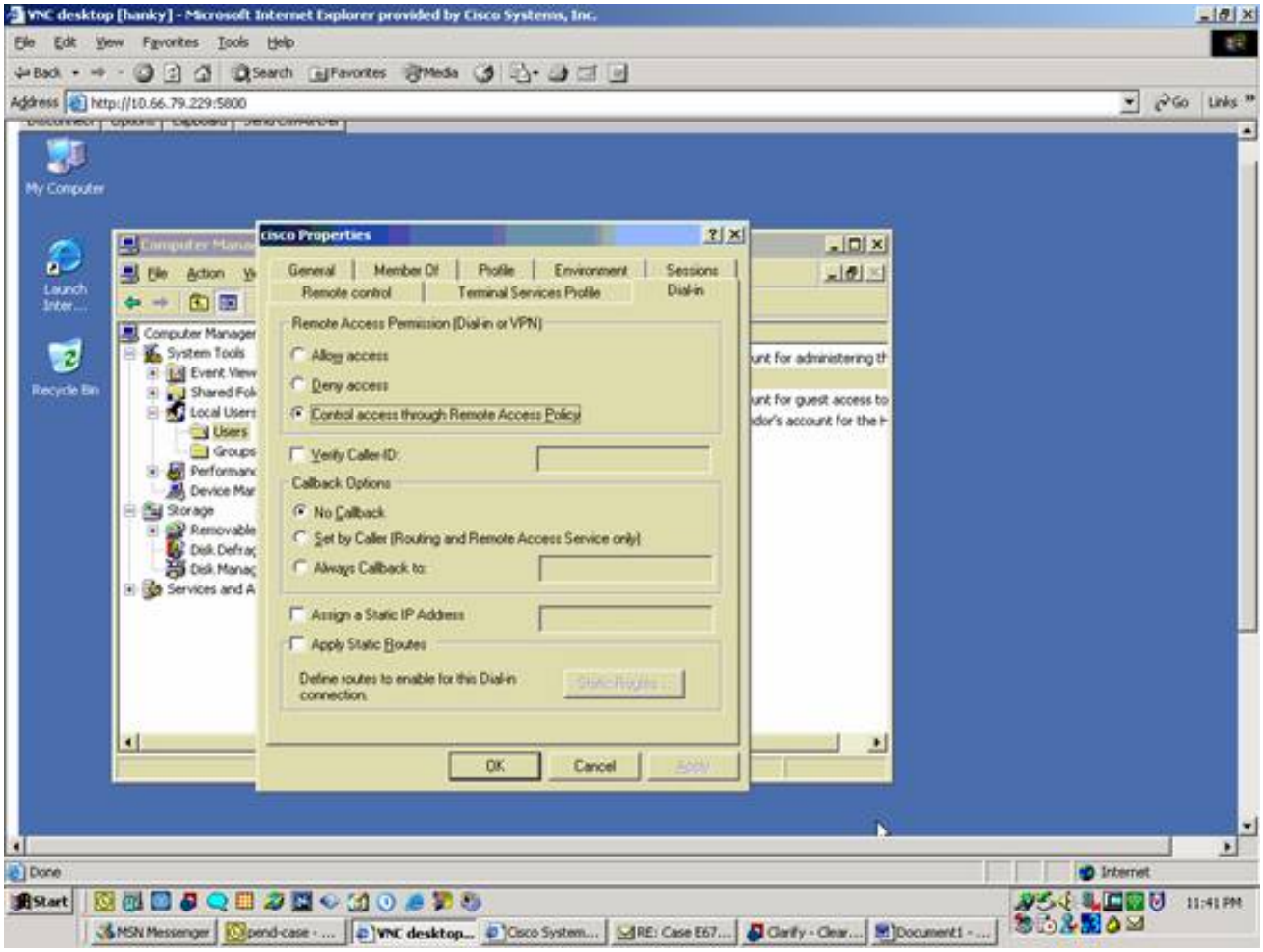
Terminez-vous ces étapes afin de configurer le serveur de Microsoft Windows 2003 avec IAS.

Note: ces étapes supposent que IAS est déjà installé sur l'ordinateur local. Sinon, ajoutez ce composant via **Control Panel > Add/Remove Programs**.

1. Choisissez les **outils d'administration > le Service d'authentification Internet** et cliquez avec le bouton droit sur le **client RADIUS** afin d'ajouter un nouveau client RADIUS. Après que vous tapiez les informations de client, cliquez sur OK.
2. Écrivez un nom amical.
3. Définissez le concentrateur VPN avec une adresse IP ou un nom DNS sur la prochaine fenêtre.
4. Choisissez **Cisco de la** barre de défilement de Client-constructeur.
5. Écrivez un secret partagé.**Note**: Vous devez se souvenir le secret *précis* que vous utilisez. Vous avez besoin de ces informations afin de configurer le concentrateur VPN.
6. Cliquez sur **OK** pour terminer.
7. Allez aux **stratégies d'accès à distance**, cliquez avec le bouton droit sur des **connexions à d'autres serveurs d'accès**, et choisissez Properties.
8. Choisissez l'**autorisation d'Accès à distance de Grant** et cliquez sur Edit le **profil** afin de configurer des propriétés d'accès distant.
9. Sélectionnez le protocole pour l'utiliser pour l'authentification sur l'onglet d'authentification. Vérifiez la **version 2 d'authentification chiffrée par Microsoft** et décochez tous autres Protocoles d'authentification.**Note**: Les configurations dans ce profil d'accès distant doivent apparier les configurations dans la configuration et le client entrant de concentrateur VPN 3000. Dans cet exemple MS-CHAPv2 l'authentification sans cryptage PPTP est utilisée.
10. Sur le contrôle d'onglet de cryptage **aucun cryptage** seulement.
11. Cliquez sur **OK** quand vous avez terminé.



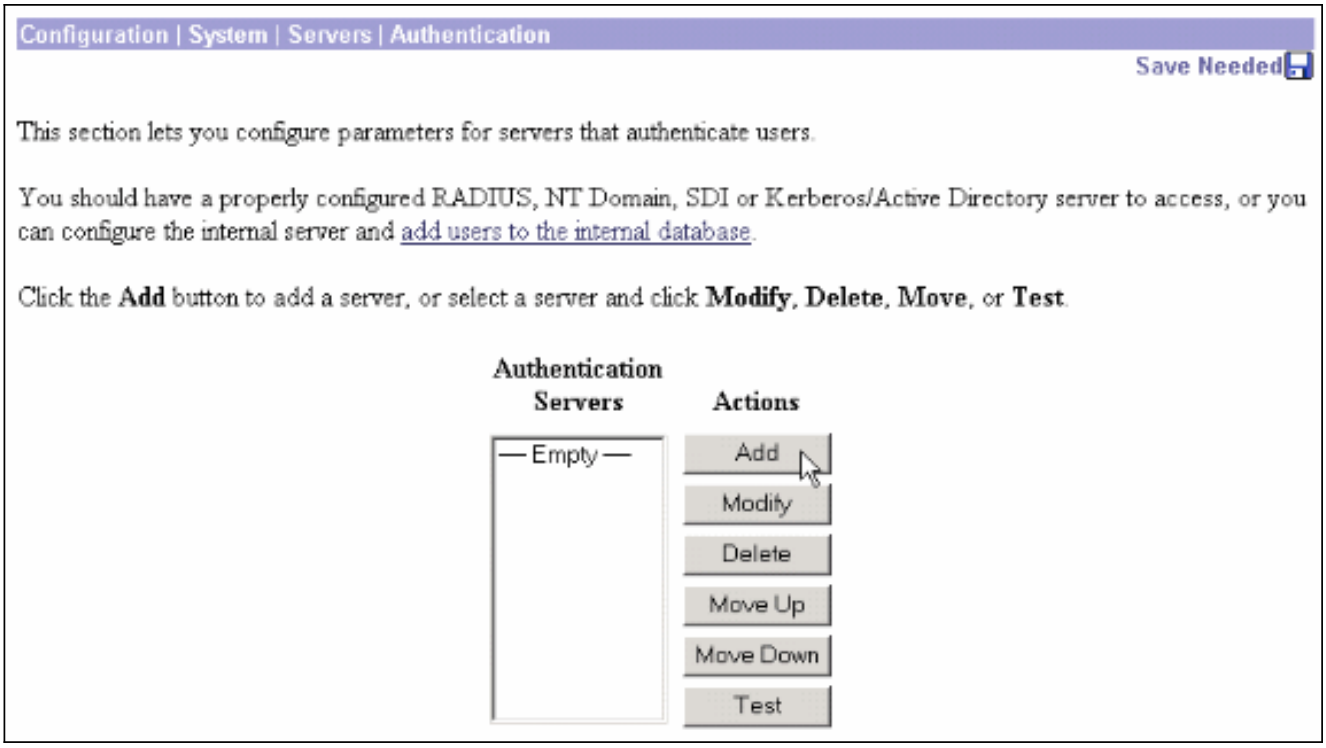
12. Cliquez avec le bouton droit le **Service d'authentification Internet** et cliquez sur le **service de début** dans l'arborescence de la console.**Note**: Vous pouvez également employer cette fonction afin d'arrêter le service.
13. Choisissez l'**Administrative Tools > Computer Management > System Tools > Local Users and Groups**, cliquez avec le bouton droit sur des **utilisateurs** et choisissez les **nouveaux utilisateurs** afin d'ajouter un utilisateur en compte d'ordinateur local.
14. Ajoutez l'utilisateur avec le mot de passe « vpnpassword » de Cisco et vérifiez ces données de profil.Dans l'onglet General, assurez-vous que l'option **Password Never Expired** est sélectionnée au lieu de l'option User Must Change Password.Sur l'onglet Numérotation, choisissez l'option pour l'**accès Allow** (ou laissez la valeur par défaut de l'accès de contrôle par la stratégie d'accès à distance).Cliquez sur **OK** quand vous avez terminé.



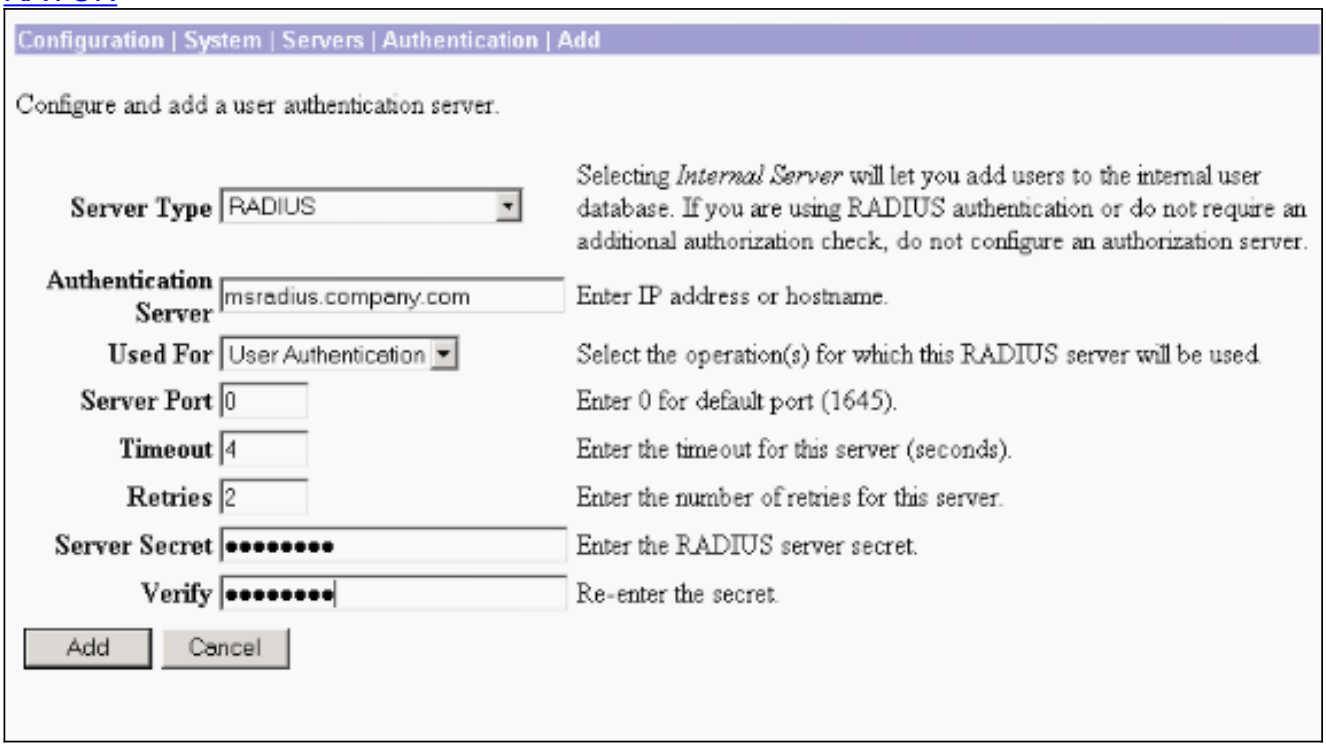
Configurez le concentrateur de Cisco VPN 3000 pour l'authentification de RAYON

Terminez-vous ces étapes afin de configurer le concentrateur de Cisco VPN 3000 pour l'authentification de RAYON.

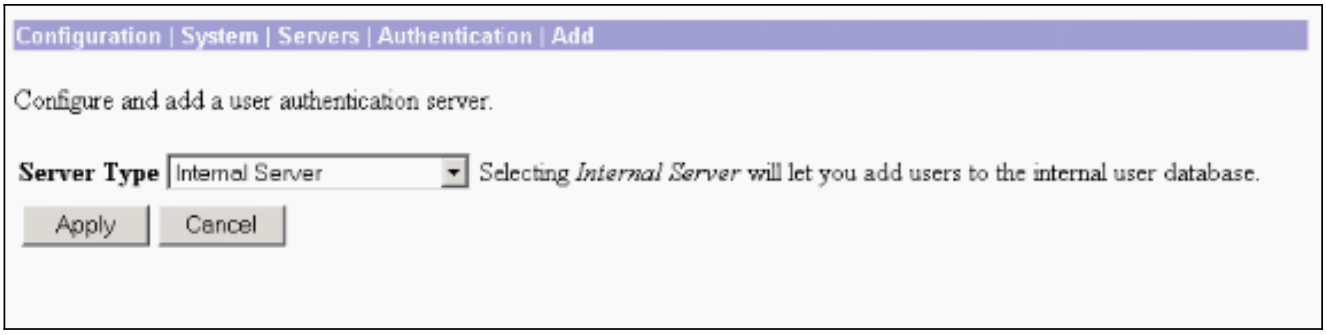
1. Connectez au concentrateur VPN à votre navigateur Web, et choisissez la **configuration > le système > les serveurs > l'authentification du** menu gauche de trame.



2. Cliquez sur Add et configurez ces configurations.Type = RAYON de serveurServeur = adresse IP ou adresse Internet d'authentification de votre serveur de RAYON (IAS)Port de serveur = 0 (0=default=1645)Secret de serveur = mêmes que dans l'étape 8 dans la section sur Configure le serveur de RAYON



3. Cliquez sur Add afin d'ajouter les modifications à la configuration en cours.
4. Cliquez sur Add, choisissez le **serveur interne** pour le type de serveur, et cliquez sur Apply.Vous avez besoin de ceci plus tard afin de configurer un groupe d'IPsec (vous avez besoin seulement du type = du serveur interne de serveur).



5. Configurez le concentrateur VPN pour des utilisateurs PPTP ou pour des utilisateurs de client vpn.**PPTP**Terminez-vous ces étapes afin de configurer pour des utilisateurs PPTP.Choisissez le **Configuration > User Management > groupe de base**, et cliquez sur l'onglet **PPTP/L2TP**.Choisissez **MSCHAPv2** et décochez d'autres Protocoles d'authentification dans la section de Protocoles d'authentification PPTP.

Configuration | User Management | Base Group

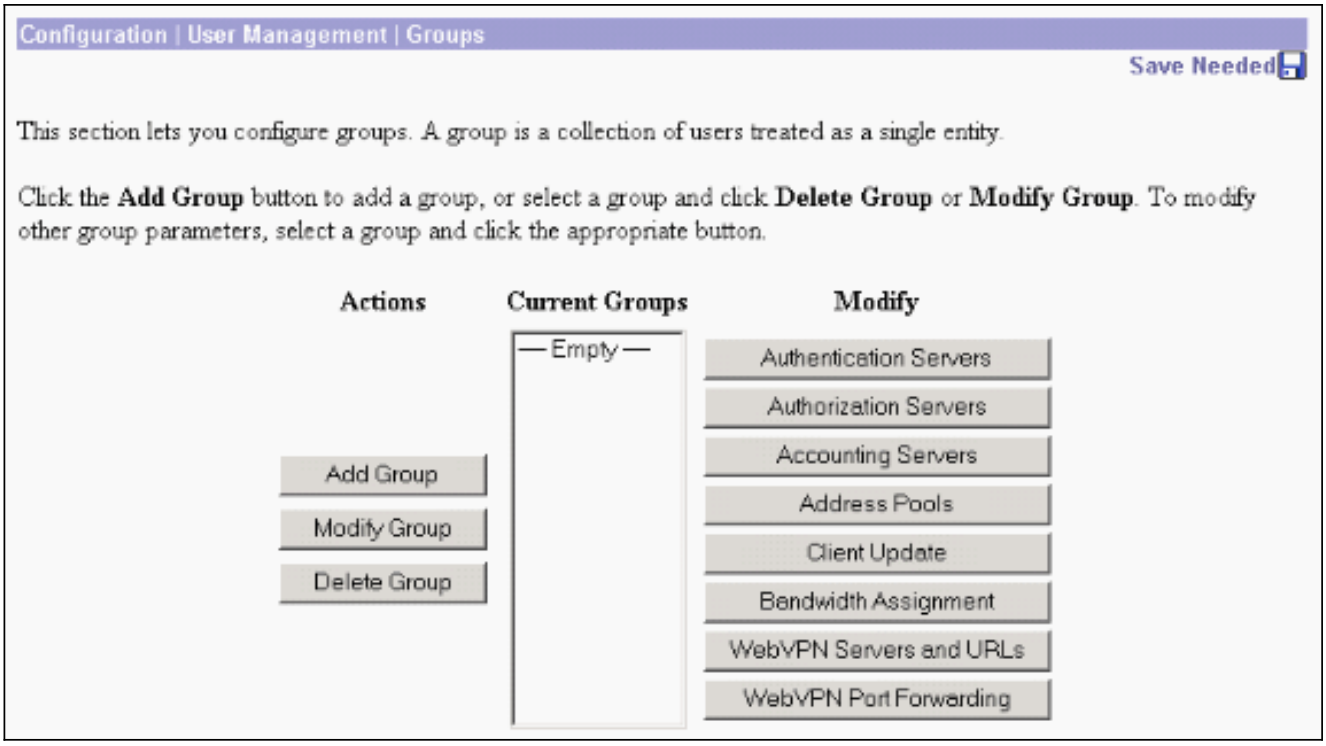
General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN | NAC

PPTP/L2TP Parameters

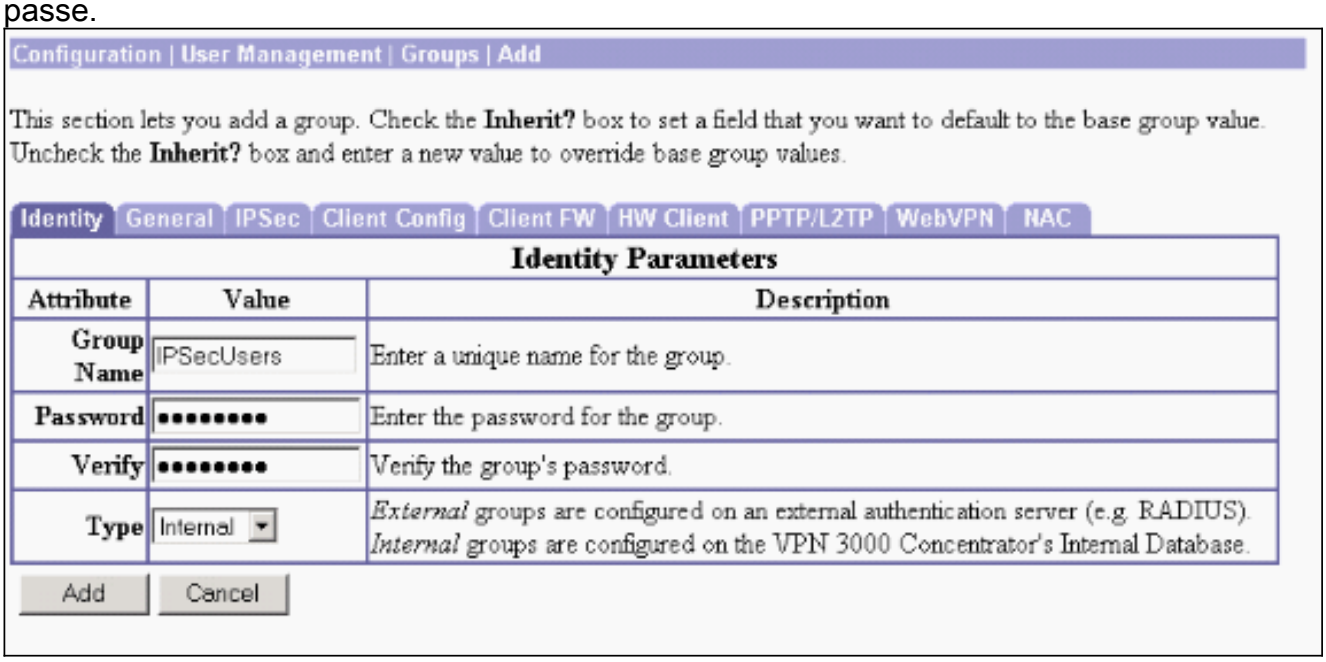
Attribute	Value	Description
Use Client Address	☐	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	☐ PAP ☐ CHAP ☐ MSCHAPv1 ☑ MSCHAPv2 ☐ EAP Proxy	Check the authentication protocols allowed. Refer to the online help for authentication protocol dependencies. **Unchecking *all* options means that *no* authentication is required.**
PPTP Encryption	☐ Required ☐ Require Stateless ☑ 40-bit ☑ 128-bit	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	☐	Check to enable MPPC compression for PPTP connections for this group.
L2TP Authentication Protocols	☐ PAP ☑ CHAP ☑ MSCHAPv1 ☐ MSCHAPv2 ☐ EAP Proxy	Check the authentication protocols allowed. Refer to the online help for authentication protocol dependencies. **Unchecking *all* options means that *no* authentication is required.**
L2TP Encryption	☐ Required ☐ Require Stateless ☑ 40-bit ☑ 128-bit	Select the allowed encryption methods for L2TP connections for this group.
L2TP Compression	☐	Check to enable MPPC compression for L2TP connections for this group.

Apply Cancel

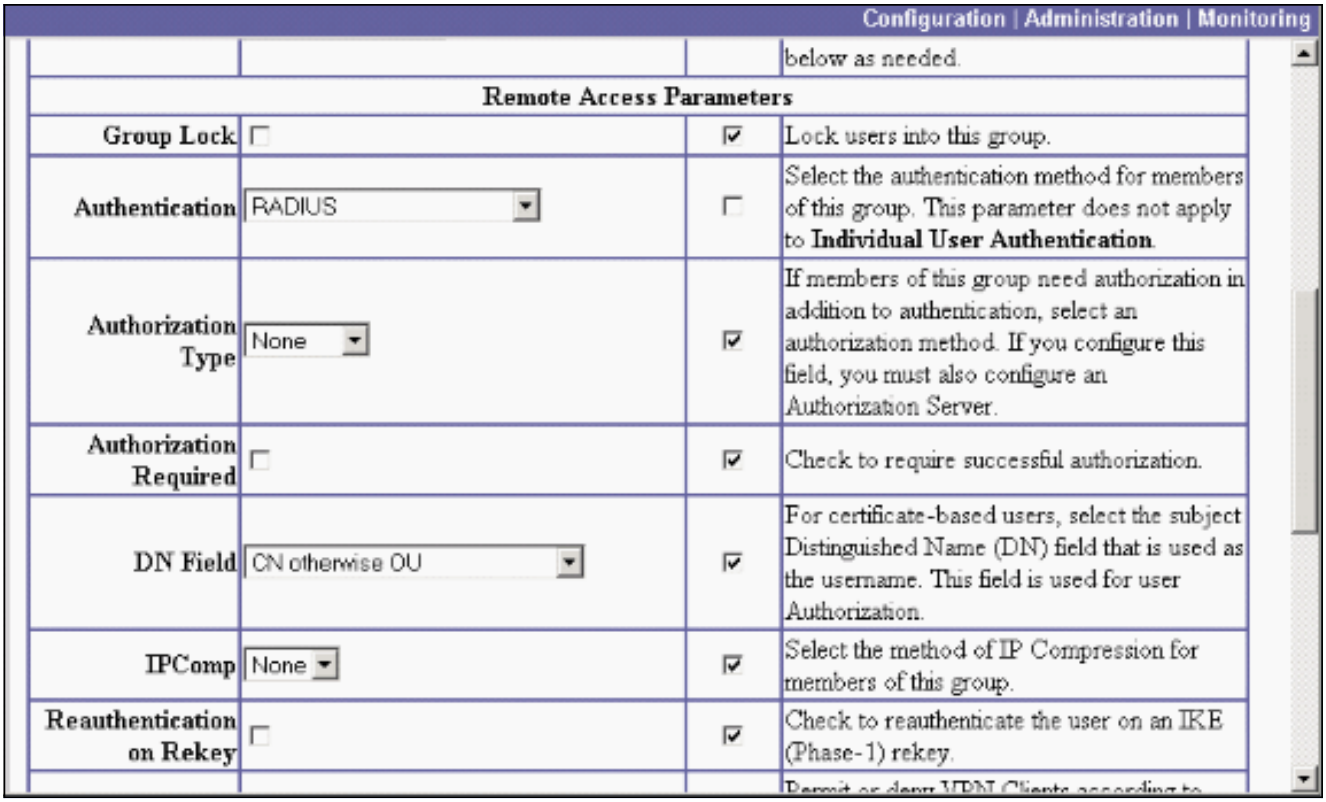
Cliquez sur Apply au bas de page afin d'ajouter les modifications à la configuration en cours.Maintenant où les utilisateurs PPTP se connectent, ils sont authentifiés par le serveur de RAYON (IAS).Client VPNTerminez-vous ces étapes afin de configurer pour des utilisateurs de client vpn.Choisissez le **Configuration > User Management > Groups** et cliquez sur Add afin d'ajouter un nouveau groupe.



Tapez un nom de groupe (par exemple, IPsecUsers) et un mot de passe.



Ce mot de passe est utilisé comme clé pré-partagée pour la négociation de tunnel.Allez à l'onglet d'IPSec et placez l'authentification au RAYON.



Ceci permet des clients d'IPsec à authentifier par l'intermédiaire du serveur d'authentification RADIUS.Cliquez sur Add au bas de page afin d'ajouter les modifications à la configuration en cours.Maintenant où les clients d'IPsec connectent et utilisent le groupe que vous avez configuré, ils sont authentifiés par le serveur de RAYON.

Vérifiez

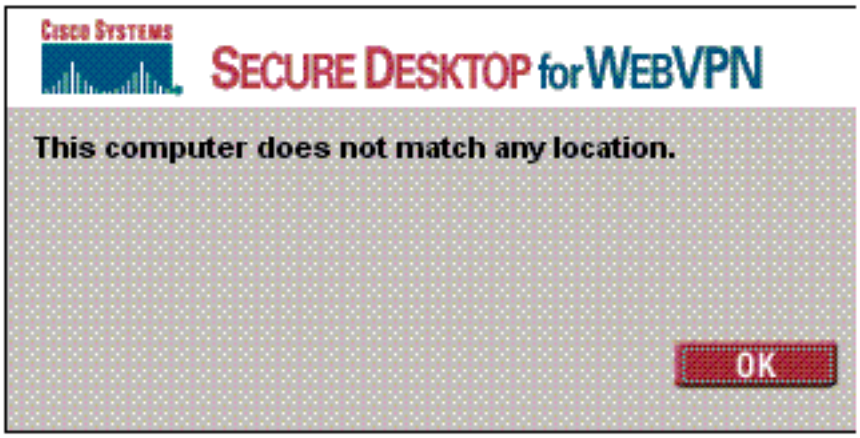
Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

L'authentification de webvpn échoue

Ces sections fournissent des informations que vous pouvez employer pour dépanner votre configuration.

- **Problème** : Les utilisateurs WebVPN ne peuvent pas authentifier contre le serveur de RAYON mais peuvent authentifier avec succès avec la base de données locale du concentrateur VPN. Ils reçoivent des erreurs telles que le « échec de connexion » et ce



message. **Cause** : Ces genres de problèmes se produisent souvent quand n'importe quelle base de données autre que la base de données interne du concentrateur est utilisée. Les utilisateurs WebVPN frappent le groupe de base quand ils d'abord se connectent au concentrateur et doivent utiliser la méthode d'authentification par défaut. Souvent cette méthode est placée à la base de données interne du concentrateur et n'est pas un RAYON configuré ou tout autre serveur.**Solution** : Quand un utilisateur WebVPN authentifie, le concentrateur vérifie la liste de serveurs définis à la **configuration > au système > aux serveurs > à l'authentification** et utilise le principal. Veillez à déplacer le serveur que vous voulez que les utilisateurs WebVPN authentifient avec jusqu'au dessus de cette liste. Par exemple, si le RAYON est la méthode d'authentification, vous devez déplacer le serveur de RAYON au haut de la liste pour pousser l'authentification à elle.**Note**: Juste parce que les utilisateurs WebVPN frappent au commencement le groupe de base ne veut pas dire qu'ils sont confinés au groupe de base. Des groupes supplémentaires de webvpn peuvent être configurés sur le concentrateur, et des utilisateurs peuvent leur être assignés par le serveur de RAYON avec la population de l'attribut 25 avec **OU=groupname**. Référez-vous à verrouiller des utilisateurs sur un groupe de concentrateur VPN 3000 utilisant un serveur de RAYON pour une explication plus détaillée.

L'authentification de l'utilisateur échoue contre le Répertoire actif

Dans le serveur de Répertoire actif, sur l'onglet de compte de l'utilisateur Properties de l'utilisateur manquant, vous pouvez voir cette case :

[x] N'exigez pas la pré-authentification

Si cette case est décochée, **cochez-la**, et l'essayez d'authentifier de nouveau avec cet utilisateur.

Informations connexes

- Concentrateurs VPN de la gamme Cisco 3000
- Cisco VPN 3002 Hardware Clients
- Négociation IPSec/Protocoles IKE
- Page de support de RAYON (Remote Authentication Dial-In User Service)
- Service RADIUS (Remote Authentication Dial-In User Service)
- Support et documentation techniques - Cisco Systems