ACS 5.x : Autorisation d'authentification et de commande TACACS+ basée sur l'exemple de configuration d'adhésion à des associations d'AD

Contenu

Introduction

Ce document fournit à un exemple de configurer l'autorisation d'authentification et de commande TACACS+ basée sur l'adhésion à des associations d'AD d'un utilisateur le Système de contrôle d'accès sécurisé Cisco (ACS) 5.x et plus tard. ACS utilise le Microsoft Active Directory (AD) comme mémoire externe d'identité pour enregistrer des ressources comme des utilisateurs, ordinateurs, groupes, et attributs.

Conditions préalables

Conditions requises

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

- ACS 5.x est entièrement intégré au domaine désiré d'AD. Si l'ACS n'est pas intégré avec le domaine désiré d'AD, référez-vous à ACS 5.x et plus tard : Intégration avec le pour en savoir plus d'exemple de configuration de Microsoft Active Directory afin d'effectuer la tâche d'intégration.

Composants utilisés

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

- Cisco Secure ACS 5.3
- Version de logiciel 12.2(44)SE6 de Cisco IOS®.**Remarque:** Cette configuration peut être faite sur tous les périphériques de Cisco IOS.
- Domaine 2003 de Microsoft Windows Server

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.

Configuration

Configurez ACS 5.x pour l'authentification et l'autorisation

Avant que vous commenciez la configuration de l'ACS 5.x pour l'authentification et l'autorisation, ACS devrait avoir été intégré avec succès avec l'AD de Microsoft. Si l'ACS n'est pas intégré avec le domaine désiré d'AD, référez-vous à ACS 5.x et plus tard : Intégration avec le pour en savoir plus d'exemple de configuration de Microsoft Active Directory afin d'effectuer la tâche d'intégration.

Dans cette section, vous tracez deux groupes d'AD à deux positionnements différents de commande et deux profils de shell, un avec l'accès complet et l'autre avec limité-Access sur les périphériques de Cisco IOS.

1. Connectez-vous dans le GUI ACS utilisant des qualifications d'admin.
2. Choisissez les **utilisateurs et l'identité enregistre > identité externe enregistre > Répertoire actif** et vérifie que l'ACS a joint le domaine désiré et aussi que l'**état de Connectivité** est affiché comme **connecté**.Cliquez sur en fonction l'onglet de **groupes de répertoire**.
3. Clic **choisi**.
4. Choisissez les groupes qui doivent être tracés aux profils de shell et la commande place dans la partie postérieure de la configuration. Cliquez sur **OK**.
5. **Modifications de sauvegarde de** clic.
6. Choisissez les **stratégies d'Access > les services d'accès > les règles de sélection de service** et identifiez le service d'accès, qui traite l'authentification TACACS+. Dans cet exemple, c'est **admin par défaut de périphérique**.
7. Choisissez les **stratégies d'Access > les services d'accès > l'admin > l'identité de périphérique de par défaut** et cliquez sur **choisi** à côté de la **source d'identité**.
8. Choisissez **AD1** et cliquez sur OK.
9. **Modifications de sauvegarde de** clic.
10. Choisissez les **stratégies d'Access > les services d'accès > l'admin > l'autorisation de périphérique de par défaut** et cliquez sur en fonction **Customize**.
11. La copie **AD1:ExternalGroups de disponible à la** section **sélectionnée d'états Customize** et alors déplacent le **profil de shell** et **commandent des positionnements de disponible à la** section **sélectionnée de résultats Customize**. Cliquez sur OK maintenant.
12. Le clic **créent** afin de créer une nouvelle règle.

13. Clic **choisi** en état **AD1:ExternalGroups**.
14. Choisissez le groupe que vous voulez fournir l'accès complet sur le périphérique de Cisco IOS. Cliquez sur **OK**.
15. Clic **choisi** dans le domaine de profil de shell.
16. Le clic **créent** afin de créer un nouveau **profil de shell** pour des utilisateurs d'accès complet.
17. Fournissez un **nom** et un **Description(optional)** dans l'**onglet Général** et cliquez sur en fonction l'onglet de **fonctionnalités usuelles**.
18. Changez le **privilège par défaut** et le **privilège de maximum à la charge statique** avec la **valeur 15**. Cliquez sur **Submit**.
19. Maintenant choisissez le **profil** de création récente de **shell d'**accès complet (Plein-privilège dans cet exemple) et cliquez sur OK.
20. Clic **choisi** dans le domaine de positionnements de commande.
21. Le clic **créent** afin de créer une nouvelle **commande réglée** pour des utilisateurs d'**accès complet**.
22. Fournissez un **nom** et assurez-vous que la case à côté de l'**autorisation n'importe quelle commande qui n'est pas dans la table ci-dessous** est cochée. Cliquez sur **Submit**.**Remarque:** Référez-vous à créer, à reproduire, et à éditer des positionnements de commande pour la gestion de périphérique pour plus d'informations sur des positionnements de commande.
23. Cliquez sur **OK**.
24. Cliquez sur **OK**. Ceci se termine la configuration de **Rule-1**.
25. Le clic **créent** afin de créer une nouvelle règle pour les utilisateurs **limités d'accès**.
26. Choisissez **AD1:ExternalGroups** et cliquez sur **choisi**.
27. Choisissez les groupes de groupe (ou) que vous voulez fournir l'accès limité à et cliquer sur OK.
28. Clic **choisi** dans le domaine de profil de shell.
29. Le clic **créent** afin de créer un nouveau **profil de shell** pour l'accès limité.
30. Fournissez un **nom** et un **Description(optional)** dans l'**onglet Général** et cliquez sur en fonction l'onglet de **fonctionnalités usuelles**.
31. Changez le **privilège par défaut** et le **privilège de maximum à la charge statique** avec les valeurs **1** et **15** respectivement. Cliquez sur **Submit**.
32. Cliquez sur **OK**.
33. Clic **choisi** dans le domaine de positionnements de commande.
34. Le clic **créent** pour créer une nouvelle **commande réglée** pour le groupe d'accès limité.
35. Fournissez un **nom** et assurez-vous que la case à cocher à côté de l'**autorisation aucune commande qui n'est pas dans la table ci-dessous** n'est pas sélectionnée. Cliquez sur Add après avoir tapé l'**exposition** dans l'espace prévu dans la section de **commande** et choisissez l'**autorisation** dans la section de **Grant** de sorte que seulement on permette les commandes show pour les utilisateurs dans le groupe d'accès limité.
36. Ajoutez de même toutes les autres commandes d'être tenu compte des utilisateurs dans le groupe d'accès limité avec l'utilisation **Add**. Cliquez sur **Submit**.**Remarque:** Référez-vous à créer, à reproduire, et à éditer des positionnements de commande pour la gestion de périphérique pour plus d'informations sur des positionnements de commande.
37. Cliquez sur **OK**.
38. Cliquez sur **OK**.
39. **Modifications de sauvegarde de** clic.
40. Le clic **créent** afin d'ajouter le périphérique de **Cisco IOS** en tant que **client d'AAA** sur l'ACS.
41. Fournissez un **nom, adresse IP, secret partagé** pour **TACACS+** et cliquez sur Submit.

Configurez le périphérique de Cisco IOS pour l'authentification et l'autorisation

Terminez-vous ces étapes afin de configurer le périphérique de Cisco IOS et l'ACS pour l'authentification et l'autorisation.

1. Créez un utilisateur local avec le plein privilège pour le retour avec la commande de **nom d'utilisateur** comme affiché ici :`username admin privilege 15 password 0 cisco123!`
2. Fournissez l'adresse IP de l'ACS afin d'activer l'AAA et ajouter ACS 5.x comme serveur TACACS.`aaa new-model`
   `tacacs-server host 192.168.26.51 key cisco123`**Remarque:** La clé devrait s'assortir avec le Partager-secret donné sur l'ACS pour ce périphérique de Cisco IOS.
3. Testez l'accessibilité de serveur TACACS avec la commande d'AAA de test comme affichée.`test aaa group tacacs+ user1 xxxxx legacy`
   `Attempting authentication test to server-group tacacs+ using tacacs+`
   `User was successfully authenticated.`La sortie de la commande précédente prouve que le serveur TACACS est accessible et l'utilisateur a été avec succès authentifié.**Remarque:** User1 et mot de passe xxx appartiennent à l'AD. Si le test veuillez échouer assurez-vous que le Partager-secret fourni dans l'étape précédente est correct.
4. Configurez la procédure de connexion et activez les authentifications et puis utilisez les autorisations d'exécutif et de commande comme affiché ici :
   ```
   aaa authentication login default group tacacs+ local
   aaa authentication enable default group tacacs+ enable
   aaa authorization exec default group tacacs+ local
   aaa authorization commands 0 default group tacacs+ local
   aaa authorization commands 1 default group tacacs+ local
   aaa authorization commands 15 default group tacacs+ local
   ```
   `aaa authorization config-commands`**Remarque:** Les mots clé de gens du pays et d'enable sont utilisés pour le retour au Cisco IOS utilisateur local et enable secret respectivement si le serveur TACACS est inaccessible.

Vérifiez

Afin de vérifier l'authentification et l'autorisation ouvrez une session au périphérique de Cisco IOS par le telnet.

1. Telnet au périphérique de Cisco IOS comme user1 qui appartient au groupe d'accès complet dans l'AD. Le groupe d'admins de réseau est le groupe dans l'AD qui est commande tracée de profil et d'accès complet de shell de Plein-privilège réglée sur l'ACS. Essayez d'exécuter n'importe quelle commande de s'assurer que vous avez l'accès complet.
2. Telnet au périphérique de Cisco IOS comme user2 qui appartient au groupe de limité-Access dans l'AD. (Le groupe d'**équipe de maintenance du réseau** est le groupe dans l'AD qui est **commande** tracée de **profil** et d'Exposition-**Access de shell de Limité-privilège réglée** sur l'ACS). Si vous essayez d'exécuter n'importe quelle commande autre que celle mentionnée dans le positionnement de commande d'Exposition-Access, vous devriez obtenir une `autorisation de commande avez manqué l'`erreur, qui prouve que l'user2 a limité l'accès.
3. Ouvrez une session au GUI ACS et lancez la **surveillance et signalez le visualiseur**. Choisissez le **protocole AAA > le TACACS+Authorization** afin de vérifier les activités exercées par user1 et user2.

Informations connexes

- Système de contrôle d'accès sécurisé Cisco
- Support et documentation techniques - Cisco Systems