ACS 5.x et plus tard : Intégration avec l'exemple de configuration de Microsoft Active Directory

Contenu

Introduction

Ce document fournit un exemple de configuration pour intégrer Microsoft Active Directory avec le système de contrôle d'accès sécurisé Cisco (ACS) 5.x et plus. ACS utilise le Microsoft Active Directory (AD) comme mémoire externe d'identité pour enregistrer des ressources comme des utilisateurs, ordinateurs, groupes, et attributs. ACS authentifie ces ressources contre AD.

Conditions préalables

Conditions requises

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

- Domaine de Répertoire actif de Windows à être les besoins utilisés d'être saturés et opérationnels.
- Utilisez le domaine 2003 de Microsoft Windows Server, le domaine 2008 de Microsoft Windows Server ou le domaine R2 de la Microsoft Windows Server 2008 comme ceux-ci sont pris en charge par ACS 5.x.**Remarque:** L'intégration du domaine R2 de la Microsoft Windows Server 2008 avec ACS est prise en charge d'ACS 5.2 et plus tard.

Composants utilisés

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

logiciel suivantes :

- Cisco Secure ACS 5.3
- 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.

Informations générales

Le Répertoire actif de Windows fournit beaucoup de caractéristiques qui sont utilisées dans l'utilisation quotidienne de réseau. L'intégration d'ACS 5.x avec l'AD permet l'utilisation des utilisateurs existants d'AD, des ordinateurs et de leur mappage de groupe.

ACS 5.x intégré avec l'AD fournit ces caractéristiques :

1. Authentification de machine
2. Récupération d'attribut pour l'autorisation
3. Récupération de certificat pour l'authentification d'EAP-TLS
4. Restriction de compte d'utilisateur et d'ordinateur
5. Restrictions d'Access d'ordinateur
6. Contrôle de permissions d'accès commuté entrant
7. Options de rappel pour des utilisateurs en accès entrant
8. Attributs de support d'accès distant

Configuration

Configurez l'engine de déploiement d'applications ACS 5.x (ADE-OS)

Avant que vous intégriez ACS 5.x à l'AD, assurez que cela le **fuseau horaire, la date et l'heure** sur l'ACS apparie avec celui sur le contrôleur principal de domaine d'AD. En outre, définissez le serveur DNS sur l'ACS afin de pouvoir résoudre le nom de domaine de l'ACS 5.x. Terminez-vous ces étapes afin de configurer l'engine de déploiement d'applications ACS 5.x (ADE-OS) :

1. Le SSH à l'appliance ACS et entrent dans les qualifications CLI.
2. Émettez la commande de **clock timezone** en mode de config suivant les indications de la commande de configurer le **FUSEAU HORAIRE** sur l'ACS afin d'apparier avec cela sur le contrôleur de domaine.
   `clock timezone Asia/Kolkata` **Remarque:** L'Asie/Kolkata est le fuseau horaire utilisé dans ce document. Vous pouvez trouver votre fuseau horaire spécifique par commande de **shows timezones de** mode d'exécution.
3. Au cas où votre contrôleur de domaine d'AD serait synchronisé avec un serveur de NTP qui

réside dans votre réseau, il est fortement recommandé d'utiliser le même serveur de NTP sur l'ACS. Si vous n'avez pas le serveur de NTP, alors ignorez à l'**étape 4.** Ce sont les étapes pour configurer le serveur de NTP :Le serveur de NTP peut être configuré avec le **serveur de ntp < l'IP address de la** commande de **server> de NTP** en mode de config comme affiché.`ntp server 192.168.26.55`
`The NTP server was modified.`
`If this action resulted in a clock modification, you must restart ACS.`Référez-vous à ACS 5.x : Synchronisation de Cisco ACS avec l'exemple de configuration du serveur de NTP pour plus d'informations sur la configuration de NTP.

4. Afin de configurer la date et l'heure utilisez manuellement la commande de **clock set** dans le **mode d'exécution**. Un exemple est montré ici :
```
clock set Jun 8 10:36:00 2012
Clock was modified. You must restart ACS.
Do you want to restart ACS now? (yes/no) yes
Stopping ACS.
Stopping Management and View.....................
Stopping Runtime......
Stopping Database....
Cleanup.....
Starting ACS ....

To verify that ACS processes are running, use the
'show application status acs' command.
```
5. Vérifiez maintenant le **fuseau horaire, la date** et l'**heure** avec la commande de **show clock**. La sortie de la commande de show clock est affichée ici :`acs51/admin# **show clock** Fri Jun 8 10:36:05 IST 2012`
6. Configurez les DN sur ACS avec la **name-server de <ip < l'IP address de la** commande **DNS>** en **mode de config** comme affiché ici :`ip name-server 192.168.26.55`**Remarque:** L'adresse IP de DN est fournie par votre administrateur de domaine windows.
7. Émettez la commande de **< nom de domaine > de nslookup** afin de vérifier l'accessibilité de nom de domaine comme affichée.`acs51/admin#**nslookup MCS55.com** Trying "MCS55.com" ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60485 ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1 ;; QUESTION SECTION: ;MCS55.com. IN ANY ;; ANSWER SECTION: MCS55.com. 600 IN A 192.168.26.55 MCS55.com. 3600 IN NS admin-zq2ttn9ux.MCS55.com. MCS55.com. 3600 IN SOA admin-zq2ttn9ux.MCS55.com. hostmaster.MCS55.com. 635 900 600 86400 3600 ;; ADDITIONAL SECTION: admin-zq2ttn9ux.MCS55.com. 3600 IN A 192.168.26.55 Received 136 bytes from 192.168.26.55#53 in 0 ms` **Remarque:** Si la **SECTION de RÉPONSE** est vide, alors contactez votre administrateur de domaine windows pour découvrir le serveur DNS correct pour le domaine.
8. Émettez la commande de **< nom de domaine > d'ip domain-name** afin de configurer le **DOMAIN-NAME** sur l'ACS comme affiché ici :`ip domain-name MCS55.com`
9. Émettez la commande de **<hostname> d'adresse Internet** afin de configurer l'**ADRESSE INTERNET** sur l'ACS comme affiché ici :`hostname acs51`**Remarque:** En raison des limites de NETBIOS, les adresses Internet ACS doivent contenir inférieur ou égal à 15 caractères.
10. Émettez la commande de **write memory** afin de sauvegarder la configuration à ACS.

Joignez ACS 5.x à l'AD

Terminez-vous ces étapes afin de joindre ACS5.x à l'AD :

1. Choisissez les **utilisateurs et l'identité enregistre > identité externe enregistre > Répertoire actif** et fournit le nom de domaine, le compte d'AD (nom d'utilisateur) et son mot de passe et

clique sur en fonction la **connexion de test**.**Remarque:** Le compte d'AD exigé pour l'accès de domaine dans ACS devrait avoir l'un ou l'autre de ces derniers :Ajoutez les postes de travail vers le droit des utilisateurs de domaine dans le domaine correspondant.Créez les objets d'ordinateur ou supprimez l'autorisation d'objets d'ordinateur sur le conteneur correspondant d'ordinateurs où le compte d'ordinateur ACS est créé avant de joindre l'ordinateur ACS au domaine.**Remarque:** Cisco recommande que vous désactiviez la stratégie de verrouillage pour le compte ACS et configuriez l'infrastructure d'AD pour envoyer des alertes à l'admin si un mot de passe incorrect est utilisé pour ce compte. C'est parce que si vous entrez un mot de passe incorrect, ACS ne crée pas ou modifie son compte d'ordinateur quand il est nécessaire et donc pour refuser probablement toutes les authentifications.**Remarque:** Le compte d'AD de Windows, qui joint ACS au domaine d'AD, peut être placé dans sa propre unité organisationnelle (OU). Il réside à sa propre OU l'un ou l'autre quand le compte est créé ou plus tard avec une restriction que le nom d'appareils doit apparier le nom du compte d'AD.

2. Cette copie d'écran prouve que la connexion de test à l'AD est réussie. Cliquez ensuite sur **OK**.**Remarque:** La configuration de Centrify obtient affecté et obtient parfois déconnecté quand il y a une réponse lente du serveur tandis que vous testez la connexion ACS avec le domaine d'AD. Cependant, il fonctionne bien avec les autres applications.
3. **La sauvegarde de** clic **change** pour que l'ACS joigne l'AD.
4. Une fois que l'ACS a avec succès joint le domaine d'AD, il affiche dans l'état de Connectivité.**Remarque:** Quand vous configurez une mémoire d'identité d'AD, ACS crée également :Un nouveau dictionnaire pour cette mémoire avec deux attributs : Un ExternalGroups et un attribut différent pour tout attribut récupéré de la page d'attributs de répertoire.Un nouvel attribut, IdentityAccessRestricted. Vous pouvez manuellement créer un état fait sur commande pour cet attribut.Un état fait sur commande pour le mappage de groupe de l'attribut d'ExternalGroup ; le nom de condition fait sur commande est AD1:ExternalGroups et un autre état fait sur commande pour chaque attribut sélectionné dans le répertoire attribue la page, par exemple, AD1:cn.

Configurez le service d'accès

Terminez-vous ces étapes afin de se terminer la configuration de service d'accès de sorte qu'ACS puisse utiliser l'intégration nouvellement configurée d'AD.

1. Choisissez le service d'où vous comme les utilisateurs seriez authentifié de l'AD et cliquer sur en fonction l'**identité**. Maintenant clic **choisi** à côté du champ de source d'identité.
2. Choisissez **AD1** et cliquez sur OK.
3. **Modifications de sauvegarde de** clic.

Vérifiez

Afin de vérifier l'authentification d'AD, envoyez à une demande d'authentification de l'le NAS avec des qualifications d'AD. Assurez-vous que le NAS est configuré sur l'ACS et la demande serait traitée par le service d'accès configuré dans la section précédente.

1. Après l'authentification réussie du NAS connectez-vous dans le GUI ACS et choisissez la **surveillance et les états > le protocole AAA > le TACACS+Authentication**. Identifiez l'authentification passée de la liste et cliquez sur en fonction le symbole de **loupe** comme

affiché.

2. Vous pouvez vérifier des étapes qu'ACS a envoyées à demande d'authentification à l'AD.

Informations connexes

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