PIX/ASA 8.0 : Utiliser l'authentification LDAP pour affecter une stratégie de groupe lors de la connexion

Contenu

Introduction

Ce document décrit comment employer l'authentification de Protocole LDAP (Lightweight Directory Access Protocol) afin d'assigner une stratégie de groupe à la procédure de connexion. Fréquemment, les administrateurs veulent fournir à des utilisateurs VPN différentes autorisations d'accès ou de contenu WebVPN. Sur l'appliance de sécurité adaptable (ASA) ceci est régulièrement réalisé par l'attribution de différentes stratégies de groupe à différents utilisateurs. Quand l'authentification LDAP est en service, ceci peut être réalisé automatiquement avec une carte d'attribut LDAP.

Afin d'employer le LDAP pour assigner une stratégie de groupe à un utilisateur, vous devez configurer une carte qui trace un attribut de LDAP, tel que le **memberOf d'**attribut de Répertoire actif (AD), à l'attribut d'IETF-Rayon-**classe** qui est compris par l'ASA. Une fois le mappage d'attribut est établi, vous doit tracer la valeur d'attribut configurée sur le serveur LDAP au nom d'une stratégie de groupe sur l'ASA.

> Remarque: L'attribut de **memberOf** correspond au groupe que l'utilisateur est une partie de dans le Répertoire actif. Il est possible que un utilisateur soit un membre de plus d'un groupe dans le Répertoire actif. Ceci cause de plusieurs attributs de **memberOf** d'être envoyés par le serveur, mais l'ASA peut seulement apparier un attribut à une stratégie de groupe.

Conditions préalables

Conditions requises

Ce document exige qu'une installation fonctionnante d'authentification LDAP est déjà configurée sur l'ASA. Référez-vous configurent l'authentification LDAP pour des utilisateurs WebVPN afin d'apprendre comment installer une configuration de base d'authentification LDAP sur l'ASA.

Composants utilisés

Les informations dans ce document sont basées sur le PIX/ASA 8.0.

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.

Informations générales

Dans cet exemple, le **memberOf d'**attribut AD/LDAP est tracé à l'attribut **CVPN3000-Radius-IETF-Class** ASA. L'attribut de classe est utilisé afin d'assigner des stratégies de groupe sur l'ASA. C'est le processus général que l'ASA complète quand elle authentifie des utilisateurs avec le LDAP :

1. L'utilisateur initie une connexion à l'ASA.
2. L'ASA est configurée pour authentifier cet utilisateur avec le serveur de Microsoft AD/LDAP.
3. L'ASA lie au serveur LDAP avec les qualifications configurées sur l'ASA (admin dans ce cas), et aux consultations le nom d'utilisateur fourni.
4. Si le nom d'utilisateur est trouvé, les tentatives ASA de lier au serveur LDAP avec les qualifications que l'utilisateur fournit à la procédure de connexion.
5. Si le deuxième grippage est réussi, l'ASA traite les attributs d'utilisateurs, qui inclut le **memberOf**.
6. L'attribut de **memberOf** est tracé à **CVPN3000-Radius-IETF-Class** par la carte configurée d'Attibute de LDAP.La valeur qui indique l'adhésion dans le groupe des **employés** est tracée à **ExamplePolicy1**.La valeur qui indique l'adhésion dans le groupe de **sous-traitants** est tracée à **ExamplePolicy2**.
7. L'attribut nouvellement assigné **CVPN3000-Radius-IETF-Class** est examiné et une détermination de stratégie de groupe est faite.La valeur ExamplePolicy1 cause la stratégie de groupe ExamplePolicy1 d'être assignée à l'utilisateur.La valeur ExamplePolicy2 cause la stratégie de groupe ExamplePolicy2 d'être assignée à l'utilisateur.

Configurez

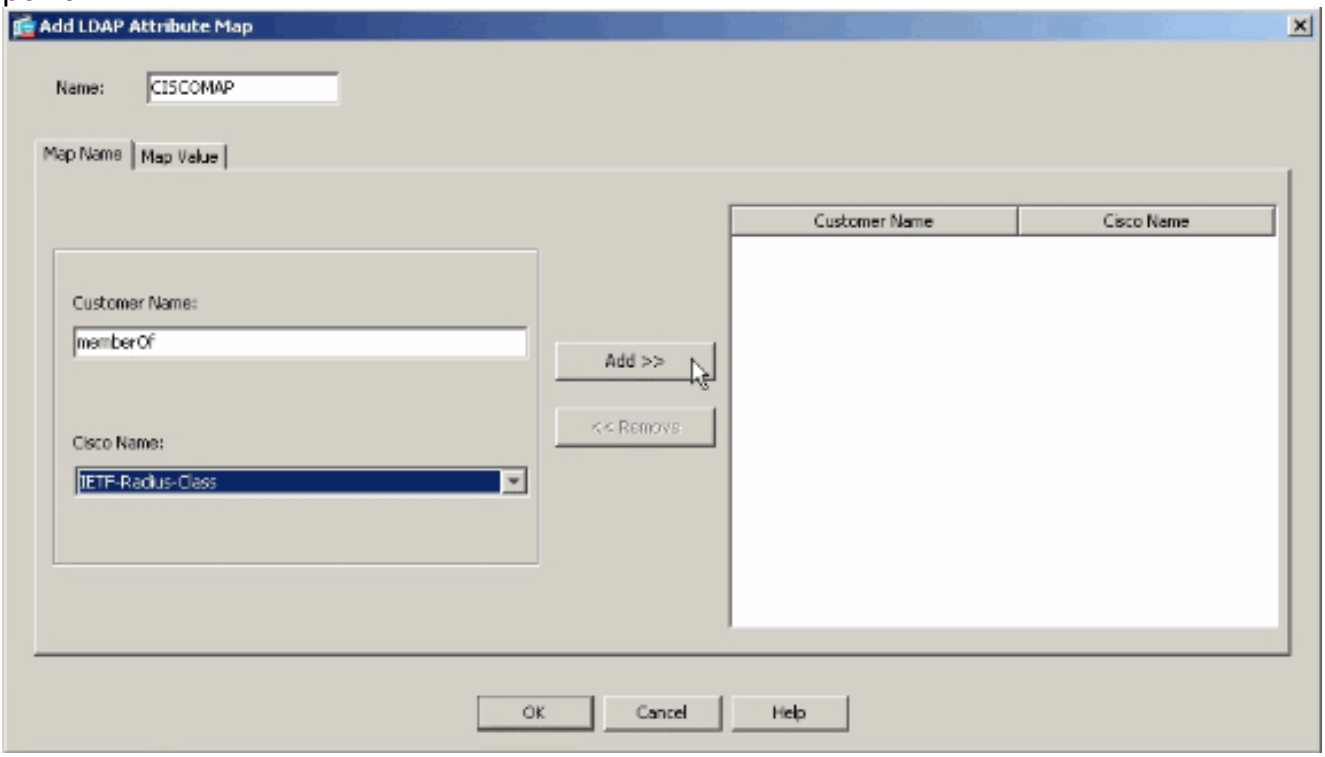
Configurez l'ASA

Dans cette section, vous êtes présenté avec les informations pour configurer l'ASA pour assigner une stratégie de groupe aux utilisateurs basés sur leurs attributs de LDAP.

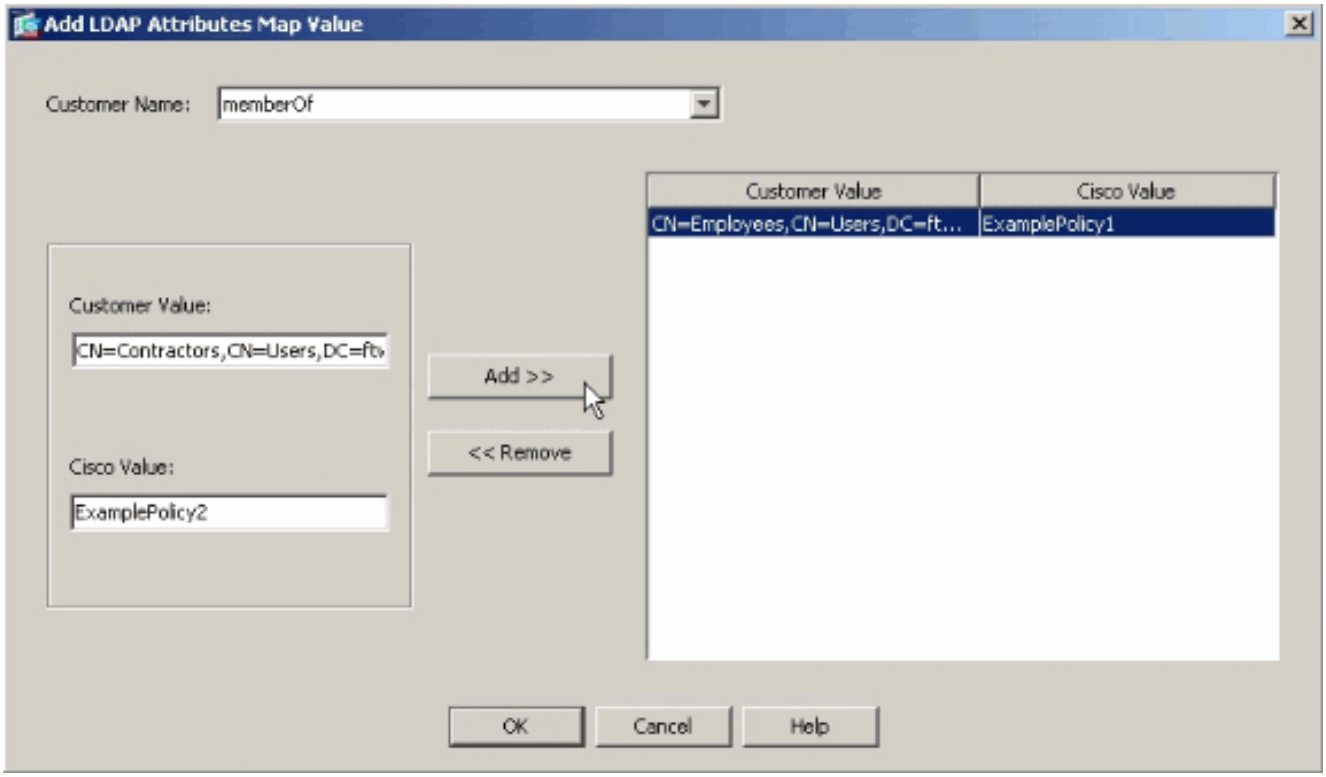
ASDM

Terminez-vous ces étapes dans Adaptive Security Device Manager (ASDM) afin de configurer la carte de LDAP sur l'ASA.

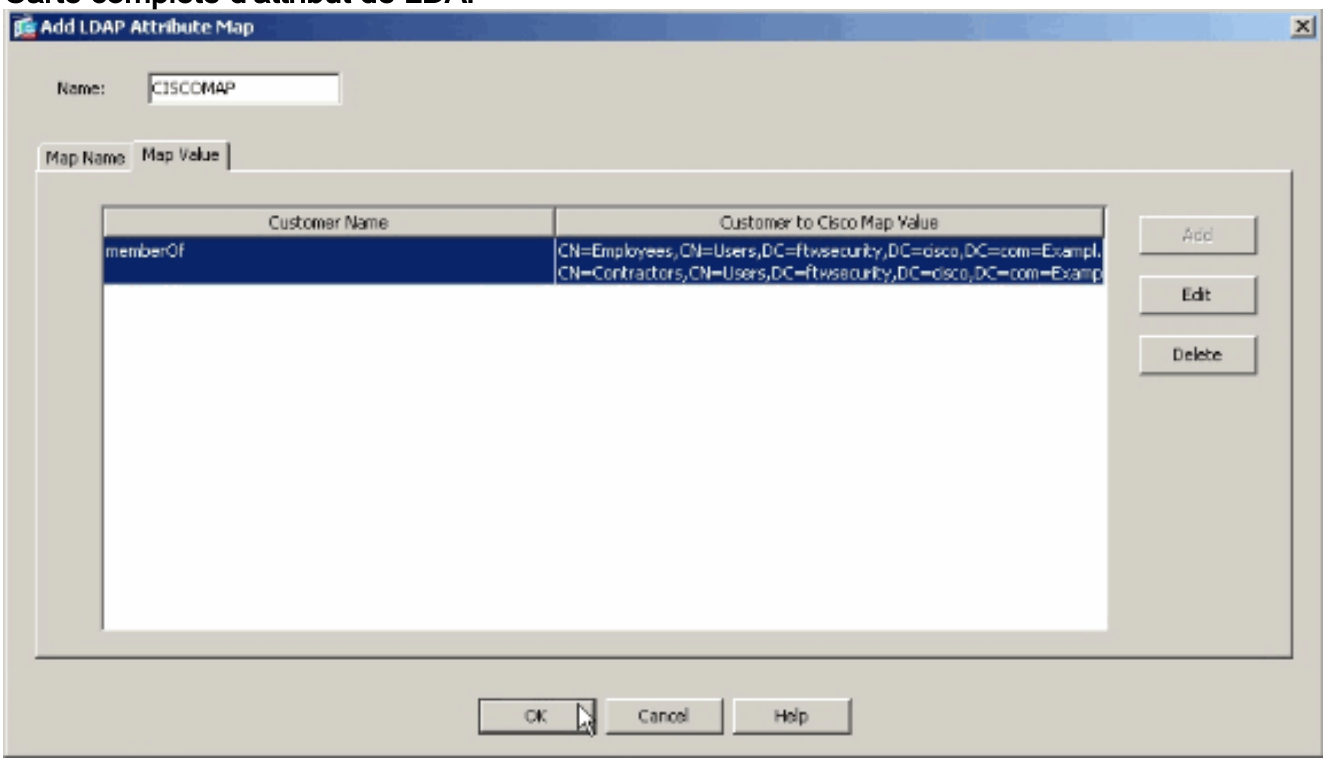
1. Naviguez vers la **configuration > l'Accès à distance VPN > AAA installé > carte d'attribut de LDAP**.
2. Cliquez sur **Add**.
3. Nommez la carte.
4. Créez un mappage entre un attribut de LDAP et l'attribut d'IETF-Rayon-**classe** sur l'ASA. Dans cet exemple, le **nom de client** est l'attribut de **memberOf** dans le Répertoire actif. Il est tracé au **nom de Cisco de l'IETF-Rayon-classe**. Cliquez sur **Add**.Remarque: Les noms et les valeurs d'attribut distinguent les majuscules et minuscules.Remarque: Si vous ne connaissez pas les noms ou les orthographes précis d'attribut qui sont fournis par le serveur LDAP, il peut être utile d'examiner met au point avant que vous créiez la carte. Voyez que la section de vérifier pour plus d'informations sur la façon identifier des attributs de LDAP avec met au point.



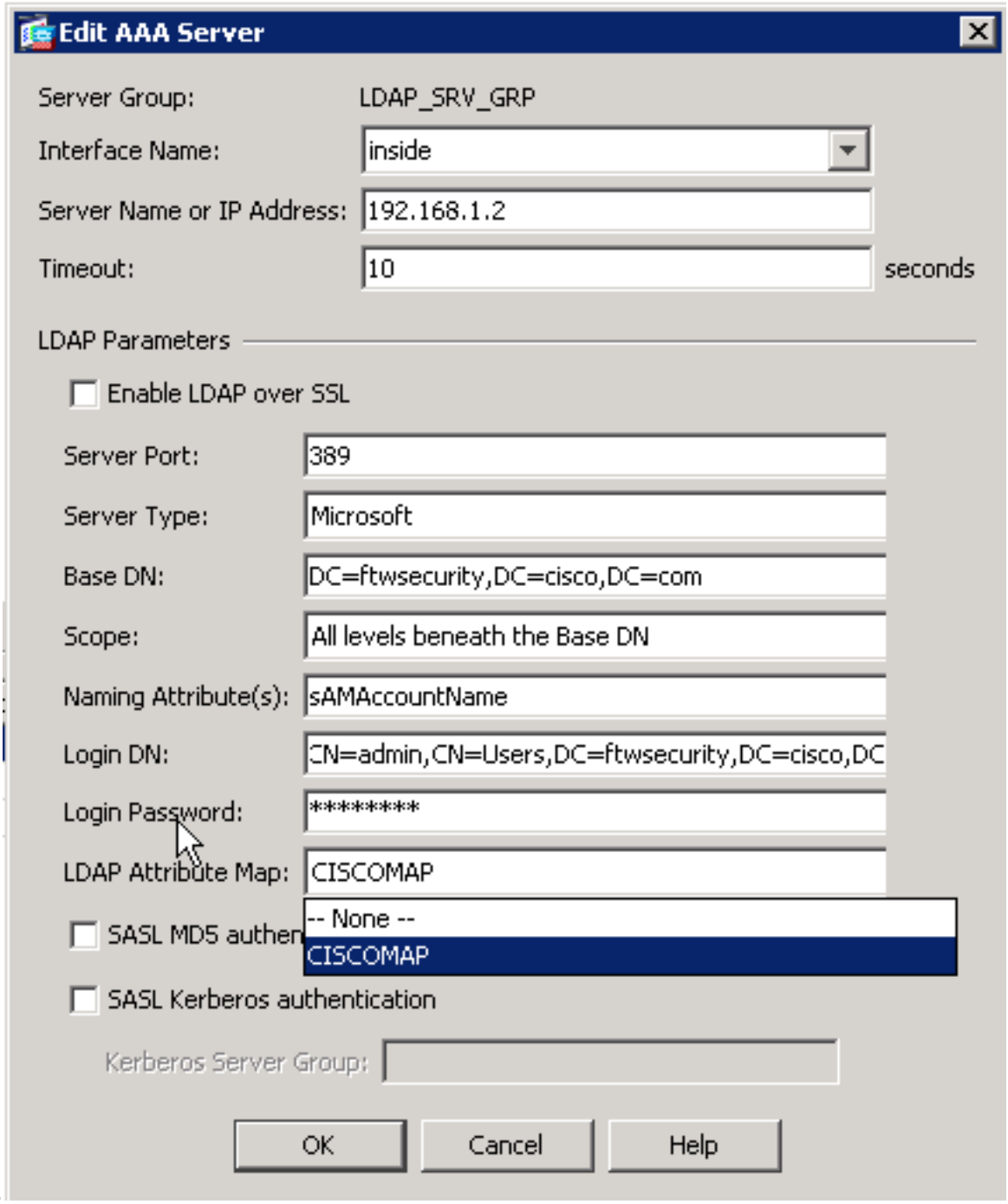
5. Après que vous ajoutiez le mappage d'attribut, cliquez sur l'onglet de **valeur de carte**, et cliquez sur Add afin de créer un mappage de valeur. Ajoutez autant de mappages de valeur au besoin, et cliquez sur OK une fois terminé.**Valeur ajoutée pour le client - la** valeur d'attribut du serveur LDAP**Cisco évaluent - le** nom de la stratégie de groupe sur l'ASADans cet exemple, le **CN=Employees, CN=Users, DC=ftwsecurity, DC=cisco,** valeur de memberOf de **DC=com** est tracé à **ExamplePolicy1** et le **CN=Contractors, CN=Users, DC=ftwsecurity, DC=cisco,** valeur de memberOf de **DC=com** est tracé à **ExamplePolicy2**.



Carte complète d'attribut de LDAP



6. Une fois que vous créez la carte, elle doit être assignée au serveur d'Authentification, autorisation et comptabilité (AAA) qui est configuré pour l'authentification LDAP. Choisissez les **Groupes de serveurs AAA du** volet gauche.
7. Sélectionnez votre serveur d'AAA qui est configuré pour le LDAP, et cliquez sur Edit.
8. Au bas de la fenêtre qui apparaît, localisez la liste déroulante de **carte d'attribut de LDAP**. Choisissez la liste que vous avez juste créée. Cliquez sur OK une fois



terminé.

CLI

Terminez-vous ces étapes dans le CLI afin de configurer la carte de LDAP sur l'ASA.

```
ciscoasa#configure terminal !--- Create the LDAP Attribute Map. ciscoasa(config)#ldap attribute-map CISCOMAP ciscoasa(config-ldap-attribute-map)#map-name memberOf IETF-Radius-Class ciscoasa(config-ldap-attribute-map)#map-value memberOf CN=Employees,CN=Users, DC=ftwsecurity,DC=cisco,DC=com ExamplePolicy1 ciscoasa(config-ldap-attribute-map)#map-value memberOf CN=Contractors,CN=Users, DC=ftwsecurity,DC=cisco,DC=com ExamplePolicy2 ciscoasa(config-ldap-attribute-map)#exit !--- Assign the map to the LDAP AAA server. ciscoasa(config)#aaa-server LDAP_SRV_GRP (inside) host 192.168.1.2 ciscoasa(config-aaa-server-host)#ldap-attribute-map CISCOMAP
```

Configurez une stratégie de groupe NOACCESS

Vous pouvez créer une stratégie de groupe NOACCESS afin de refuser la connexion VPN quand l'utilisateur n'est pas une partie de groupes l'uns des de LDAP. Cet extrait de configuration est

affiché pour votre référence :

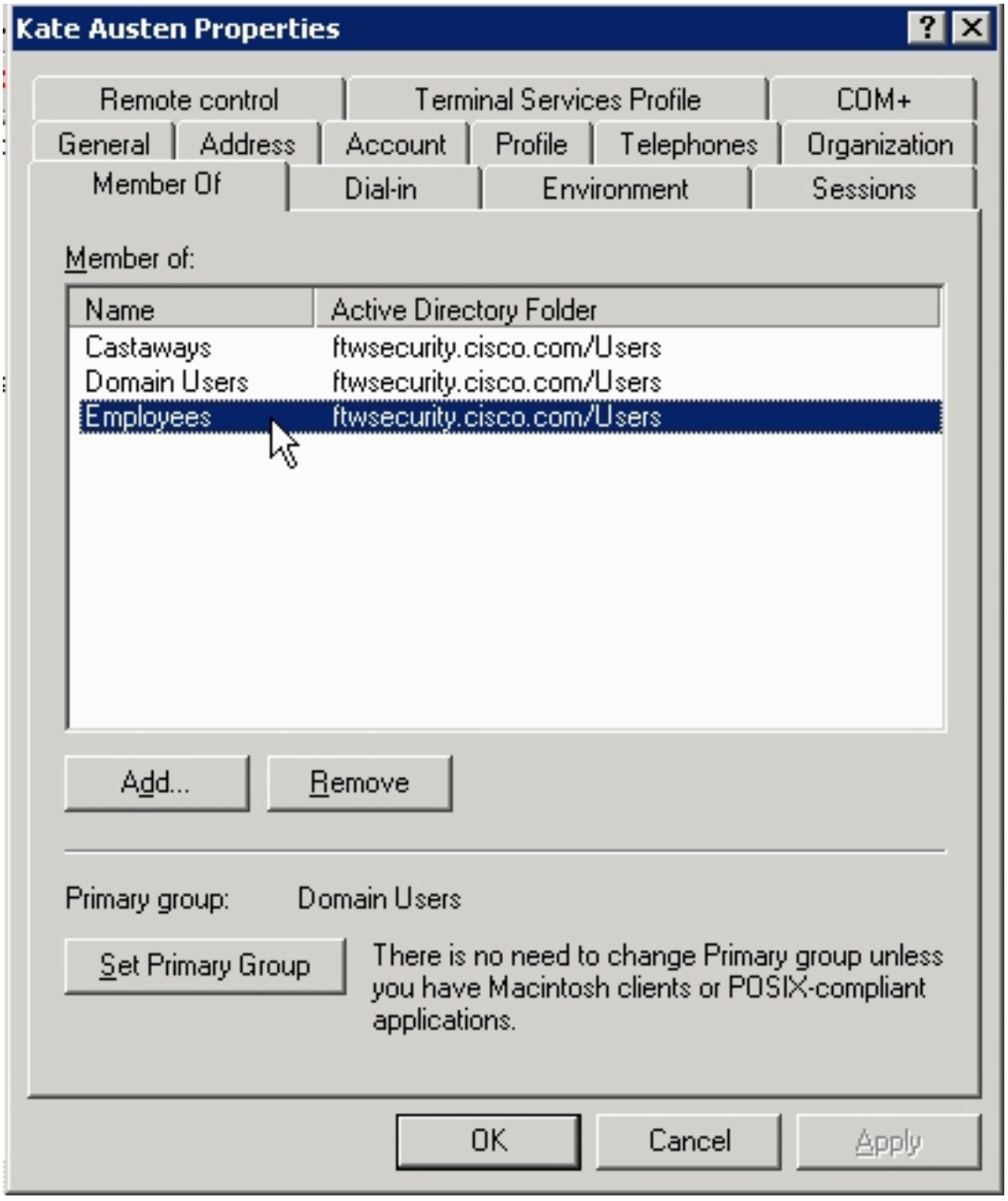
```
group-policy NOACCESS internal
group-policy NOACCESS attributes
 vpn-simultaneous-logins 0
 vpn-tunnel-protocol IPSec webvpn
```

Vous devez appliquer cette stratégie de groupe comme stratégie de groupe par défaut au groupe de tunnels. De sorte que les utilisateurs qui obtiennent un mappage de la carte d'attribut de LDAP, par exemple ceux qui appartiennent à un groupe désiré de LDAP, pouvez obtenir leurs stratégies de groupe et utilisateurs désirés qui n'obtiennent aucun mappage, par exemple ceux qui n'appartiennent pas au LDAP désiré l'un des groupe, peut obtenir la stratégie de groupe NOACCESS du groupe de tunnels, qui bloque l'accès pour eux.

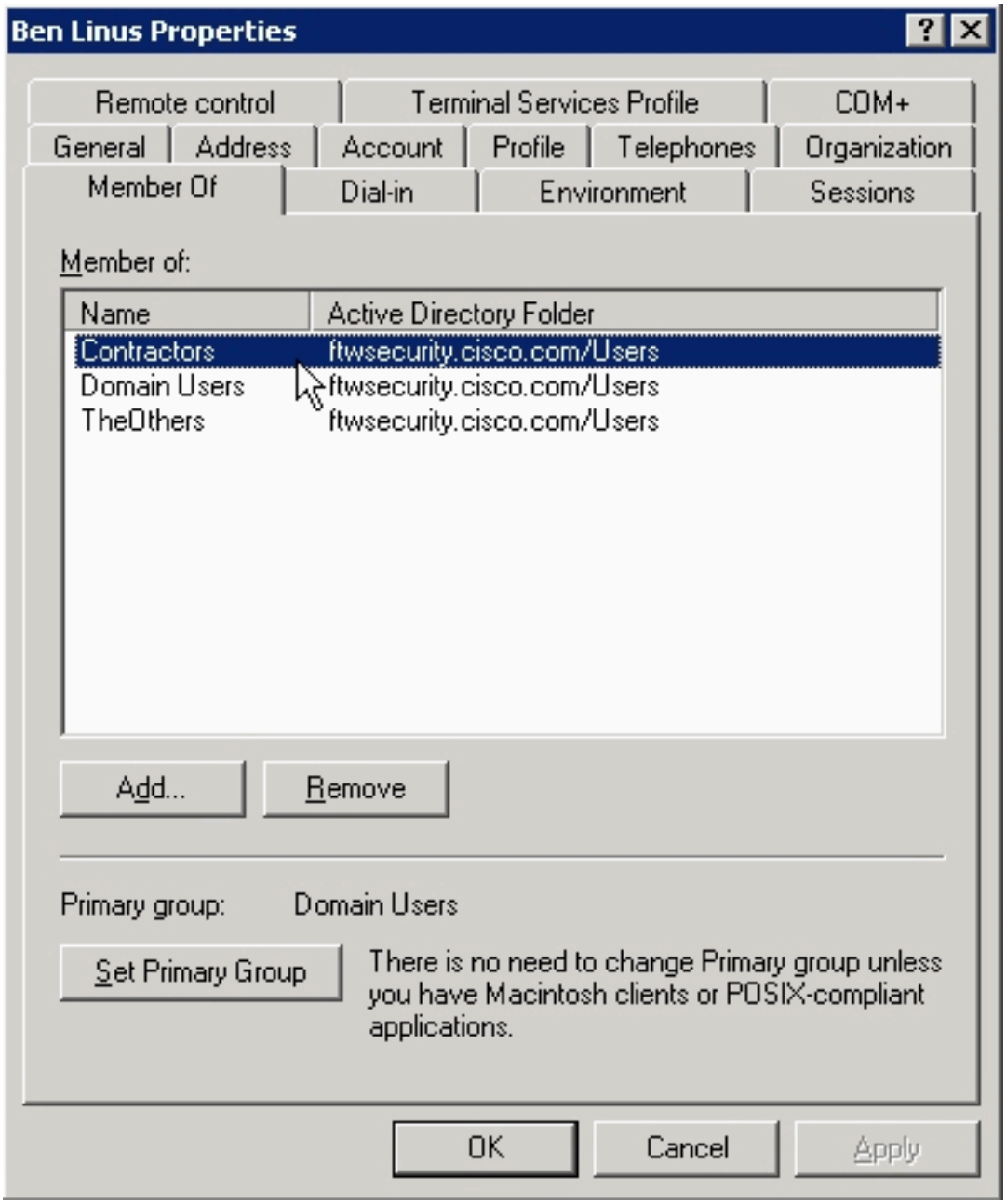
> Remarque: Reportez-vous à la section ASA/PIX : Traçant les clients vpn aux stratégies de groupe VPN par l'exemple de configuration de LDAP pour plus d'informations sur la façon créer le LDAP différent attribuent des mappages qui refuse l'accès à quelques utilisateurs.

Configurez le Répertoire actif ou tout autre serveur LDAP

La seule configuration exigée sur le Répertoire actif ou tout autre serveur LDAP associe aux attributs de l'utilisateur. Dans cet exemple, l'utilisateur Kate Austen est un membre du groupe des employés dans l'AD :



Ben Linus est un membre du groupe de sous-traitants :

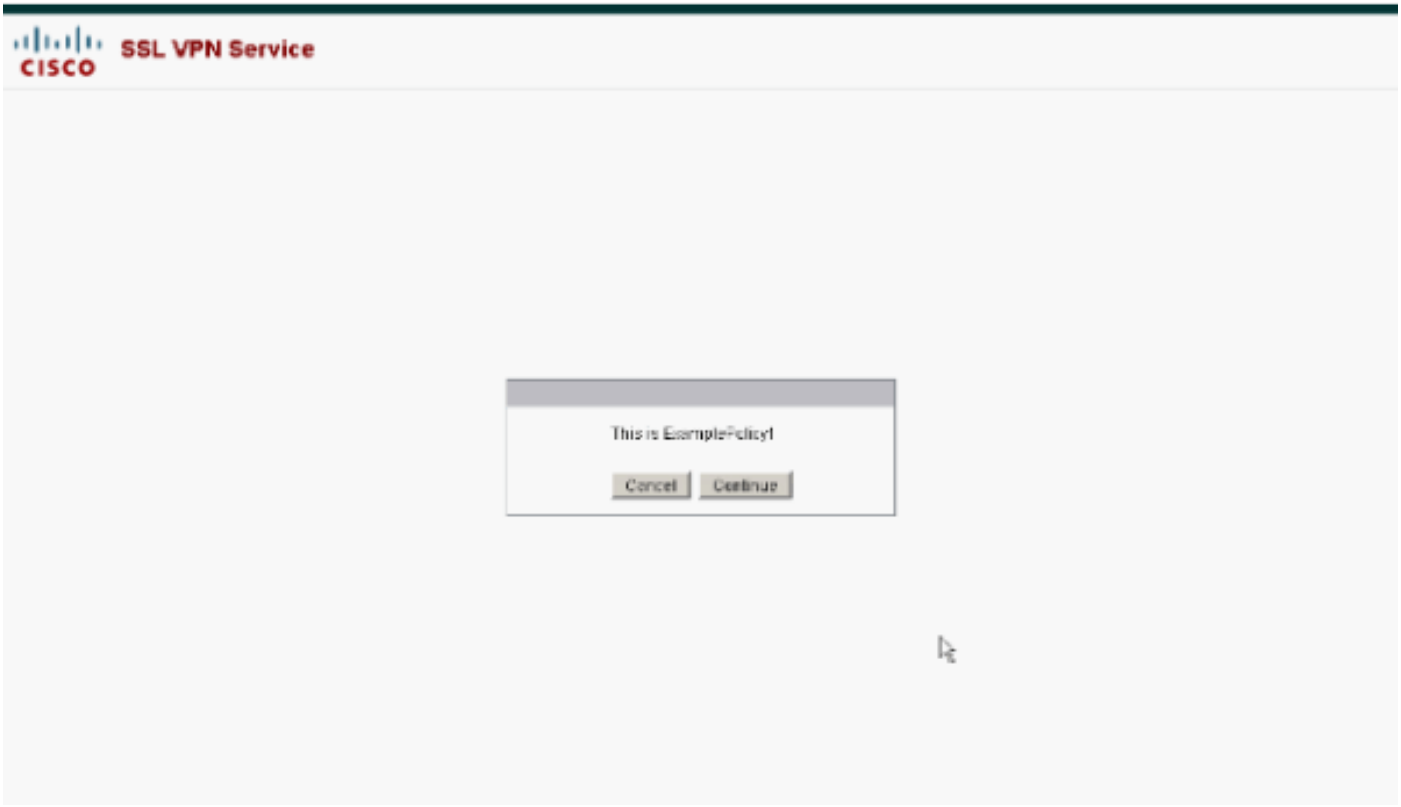


Vérifiez

Utilisez cette section afin de vérifier votre configuration.

Procédure de connexion

Afin de vérifier le succès de votre configuration, procédure de connexion en tant qu'utilisateur qui est censé avoir une stratégie de groupe assignée avec la carte d'attribut de LDAP. Dans cet exemple, une bannière est configurée pour chaque stratégie de groupe. Le tir d'écran prouve que les logins de **kate d'**utilisateur avec succès et a **ExamplePolicy1** appliqué, parce qu'elle est un membre du groupe des employés.



Débuggez la transaction de LDAP

Afin de vérifier que le mappage de LDAP se produit, ou obtenir plus d'informations sur quels attributs le serveur LDAP envoie, émettent la commande du **LDAP 255 de débogage à la** ligne de commande ASA, et puis tentent l'authentification.

En cela mettez au point, l'utilisateur que le **kate** est assigné la stratégie de groupe **ExamplePolicy1** parce qu'elle est un membre du groupe des **employés**. Ceci mettent au point prouve également que le **kate** est un membre du groupe de **naufragés**, mais que l'attribut n'est pas tracé, ainsi il est ignoré.

```
ciscoasa#debug ldap 255 debug ldap enabled at level 255 ciscoasa# [105] Session Start [105] New
request Session, context 0xd5481808, reqType = 1 [105] Fiber started [105] Creating LDAP context
with uri=ldap://192.168.1.2:389 [105] Connect to LDAP server: ldap://192.168.1.2:389, status =
Successful [105] defaultNamingContext: value = DC=ftwsecurity,DC=cisco,DC=com [105]
supportedLDAPVersion: value = 3 [105] supportedLDAPVersion: value = 2 [105]
supportedSASLMechanisms: value = GSSAPI [105] supportedSASLMechanisms: value = GSS-SPNEGO [105]
supportedSASLMechanisms: value = EXTERNAL [105] supportedSASLMechanisms: value = DIGEST-MD5
[105] Binding as administrator [105] Performing Simple authentication for admin to 192.168.1.2
[105] LDAP Search: Base DN = [dc=ftwsecurity, dc=cisco, dc=com] Filter = [sAMAccountName=kate]
Scope = [SUBTREE] [105] User DN = [CN=Kate Austen,CN=Users,DC=ftwsecurity,DC=cisco,DC=com] [105]
Talking to Active Directory server 192.168.1.2 [105] Reading password policy for kate,
dn:CN=Kate Austen,CN=Users, DC=ftwsecurity,DC=cisco,DC=com [105] Read bad password count 0 [105]
Binding as user [105] Performing Simple authentication for kate to 192.168.1.2 [105] Checking
password policy for user kate [105] Binding as administrator [105] Performing Simple
authentication for admin to 192.168.1.2 [105] Authentication successful for kate to 192.168.1.2
[105] Retrieving user attributes from server 192.168.1.2 [105] Retrieved Attributes: [105]
objectClass: value = top [105] objectClass: value = person [105] objectClass: value =
organizationalPerson [105] objectClass: value = user [105] cn: value = Kate Austen [105] sn:
value = Austen [105] givenName: value = Kate [105] distinguishedName: value = CN=Kate
Austen,CN=Users,DC=ftwsecurity, DC=cisco,DC=com [105] instanceType: value = 4 [105] whenCreated:
value = 20070815155224.0Z [105] whenChanged: value = 20070815195813.0Z [105] displayName: value
= Kate Austen [105] uSNCreated: value = 16430 [105] memberOf: value =
CN=Castaways,CN=Users,DC=ftwsecurity,DC=cisco,DC=com [105] mapped to IETF-Radius-Class: value =
CN=Castaways,CN=Users, DC=ftwsecurity,DC=cisco,DC=com [105] memberOf: value =
```

CN=Employees,CN=Users,DC=ftwsecurity,DC=cisco,DC=com [105] mapped to IETF-Radius-Class: value = ExamplePolicy1 [105] uSNChanged: value = 20500 [105] name: value = Kate Austen [105] objectGUID: value = ..z...yC.q0..... [105] userAccountControl: value = 66048 [105] badPwdCount: value = 0 [105] codePage: value = 0 [105] countryCode: value = 0 [105] badPasswordTime: value = 128316837694687500 [105] lastLogoff: value = 0 [105] lastLogon: value = 128316837785000000 [105] pwdLastSet: value = 128316667442656250 [105] primaryGroupID: value = 513 [105] objectSid: value = ...Q..p..*.p?E.Z... [105] accountExpires: value = 9223372036854775807 [105] logonCount: value = 0 [105] sAMAccountName: value = kate [105] sAMAccountType: value = 805306368 [105] userPrincipalName: value = kate@ftwsecurity.cisco.com [105] objectCategory: value = CN=Person,CN=Schema,CN=Configuration, DC=ftwsecurity,DC=cisco,DC=com [105] dSCorePropagationData: value = 20070815195237.0Z [105] dSCorePropagationData: value = 20070815195237.0Z [105] dSCorePropagationData: value = 20070815195237.0Z [105] dSCorePropagationData: value = 16010108151056.0Z [105] Fiber exit Tx=685 bytes Rx=2690 bytes, status=1 [105] Session End

En cela mettez au point, l'utilisateur que **Ben** est assigné la stratégie de groupe **ExamplePolicy2** parce qu'il est un membre du groupe de **sous-traitants**. Ceci mettent au point prouve également que **Ben** est membre du groupe de **TheOthers**, mais que l'attribut n'est pas tracé, ainsi il est ignoré.

ciscoasa#**debug ldap 255** debug ldap enabled at level 255 ciscoasa# [106] Session Start [106] New request Session, context 0xd5481808, reqType = 1 [106] Fiber started [106] Creating LDAP context with uri=ldap://192.168.1.2:389 [106] Connect to LDAP server: ldap://192.168.1.2:389, status = Successful [106] defaultNamingContext: value = DC=ftwsecurity,DC=cisco,DC=com [106] supportedLDAPVersion: value = 3 [106] supportedLDAPVersion: value = 2 [106] supportedSASLMechanisms: value = GSSAPI [106] supportedSASLMechanisms: value = GSS-SPNEGO [106] supportedSASLMechanisms: value = EXTERNAL [106] supportedSASLMechanisms: value = DIGEST-MD5 [106] Binding as administrator [106] Performing Simple authentication for admin to 192.168.1.2 [106] LDAP Search: Base DN = [dc=ftwsecurity, dc=cisco, dc=com] Filter = [sAMAccountName=ben] Scope = [SUBTREE] [106] User DN = [CN=Ben Linus,CN=Users,DC=ftwsecurity,DC=cisco,DC=com] [106] Talking to Active Directory server 192.168.1.2 [106] Reading password policy for ben, dn:CN=Ben Linus,CN=Users,DC=ftwsecurity, DC=cisco,DC=com [106] Read bad password count 0 [106] Binding as user [106] Performing Simple authentication for ben to 192.168.1.2 [106] Checking password policy for user ben [106] Binding as administrator [106] Performing Simple authentication for admin to 192.168.1.2 [106] Authentication successful for ben to 192.168.1.2 [106] Retrieving user attributes from server 192.168.1.2 [106] Retrieved Attributes: [106] objectClass: value = top [106] objectClass: value = person [106] objectClass: value = organizationalPerson [106] objectClass: value = user [106] cn: value = Ben Linus [106] sn: value = Linus [106] givenName: value = Ben [106] distinguishedName: value = CN=Ben Linus,CN=Users,DC=ftwsecurity, DC=cisco,DC=com [106] instanceType: value = 4 [106] whenCreated: value = 20070815160840.0Z [106] whenChanged: value = 20070815195243.0Z [106] displayName: value = Ben Linus [106] uSNCreated: value = 16463 [106] memberOf: value = CN=TheOthers,CN=Users,DC=ftwsecurity,DC=cisco,DC=com [106] mapped to IETF-Radius-Class: value = CN=TheOthers,CN=Users, DC=ftwsecurity,DC=cisco,DC=com **[106] memberOf: value = CN=Contractors,CN=Users,DC=ftwsecurity,DC=cisco,DC=com [106] mapped to IETF-Radius-Class: value = ExamplePolicy2** [106] uSNChanged: value = 20499 [106] name: value = Ben Linus [106] objectGUID: value = ..j...5@.z.|...n [106] userAccountControl: value = 66048 [106] badPwdCount: value = 0 [106] codePage: value = 0 [106] countryCode: value = 0 [106] badPasswordTime: value = 0 [106] lastLogoff: value = 0 [106] lastLogon: value = 0 [106] pwdLastSet: value = 128316677201718750 [106] primaryGroupID: value = 513 [106] objectSid: value = ...Q..p..*.p?E.^... [106] accountExpires: value = 9223372036854775807 [106] logonCount: value = 0 [106] sAMAccountName: value = ben [106] sAMAccountType: value = 805306368 [106] userPrincipalName: value = ben@ftwsecurity.cisco.com [106] objectCategory: value = CN=Person,CN=Schema,CN=Configuration, DC=ftwsecurity,DC=cisco,DC=com [106] dSCorePropagationData: value = 20070815195243.0Z [106] dSCorePropagationData: value = 20070815195243.0Z [106] dSCorePropagationData: value = 20070815195243.0Z [106] dSCorePropagationData: value = 16010108151056.0Z [106] Fiber exit Tx=680 bytes Rx=2642 bytes, status=1 [106] Session End

Dépannez

Utilisez cette section afin de dépanner votre configuration.

Les noms et les valeurs d'attribut distinguent les majuscules et minuscules

Les noms et les valeurs d'attribut distinguent les majuscules et minuscules. Si votre mappage ne se produit pas correctement, soyez certain que vous utilisez l'orthographe et la capitalisation correctes dans votre carte d'attribut de LDAP pour des noms et les valeurs d'attribut de Cisco et de LDAP.

L'ASA ne peut pas authentifier des utilisateurs du serveur LDAP

L'ASA ne peut pas authentifier des utilisateurs du serveur LDAP. Voici met au point :

```
session de demande de la session Start[1555805] du LDAP 255 output:[1555805] la nouvelle, le
contexte 0xcd66c028, reqType = 1[1555805] fibre started[1555805] créant le contexte de LDAP avec
uri=ldaps://172.30.74.70:636[1555805] se connectent au serveur LDAP : ldaps://172.30.74.70:636,
état = supportedLDAPVersion Successful[1555805] : valeur = supportedLDAPVersion 3[1555805] : la
valeur = l'attache 2[1555805] comme administrator[1555805] exécutant l'authentification simple
pour des sysservices à l'authentification 172.30.74.70[1555805] simple pour le code retour de
sysservices (49) credentials[1555805] non valides n'ont pas lié car le code retour
d'administrateur (-1) ne peut pas entrer en contact avec des octets des octets Rx=605 de la
sortie Tx=222 de fibre du LDAP server[1555805], extrémité de session status=-2[1555805]
```

Quant au met au point, ou le format de DN de procédure de connexion de LDAP est incorrect ou le mot de passe est incorrect ainsi vérifiez chacun des deux afin de résoudre le problème.