PIX/ASA 8.0: Utilice la autenticación ldap para asignar una directiva del grupo en el login

Contenido

Introducción

Este documento describe cómo utilizar la autenticación del Lightweight Directory Access Protocol (LDAP) para asignar una directiva del grupo en el login. Con frecuencia, los administradores quieren proporcionar a los usuarios VPN diversos permisos de acceso o contenido WebVPN. En el dispositivo de seguridad adaptante (ASA) esto se alcanza regularmente con la asignación de diversas directivas del grupo a diversos usuarios. Cuando está en uso la autenticación LDAP, esto se puede conseguir automáticamente con una correspondencia de atributo LDAP.

Para utilizar el LDAP para asignar una directiva del grupo a un usuario, usted necesita configurar una correspondencia que asocie un atributo LDAP, tal como el **memberOf del** atributo del Active Directory (AD), al atributo de la IETF-Radio-**clase** que es entendido por el ASA. La asignación del atributo se establece una vez, usted debe asociar el valor de atributo configurado en el servidor LDAP al nombre de una directiva del grupo en el ASA.

> Nota: El atributo del **memberOf** corresponde al grupo que el usuario es una parte de en el Active Directory. Es posible que un usuario sea un miembro de más de un grupo en el Active Directory. Esto hace los atributos múltiples del **memberOf** ser enviada por el servidor, pero el ASA puede hacer juego solamente un atributo a una directiva del grupo.

Prerrequisitos

Requisitos

Este documento requiere que una configuración de trabajo de la autenticación ldap esté configurada ya en el ASA. Refiera a la autenticación ldap de la configuración para los usuarios de WebVPN para aprender cómo configurar una configuración básica de la autenticación ldap en el ASA.

Componentes Utilizados

La información en este documento se basa en el PIX/ASA 8.0.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

En este ejemplo, el **memberOf del** atributo AD/LDAP se asocia al atributo **CVPN3000-Radius-IETF-Class** ASA. El atributo de clase se utiliza para asignar las directivas del grupo en el ASA. Éste es el proceso general que el ASA completa cuando autentica a los usuarios con el LDAP:

1. El usuario inicia una conexión al ASA.
2. El ASA se configura para autenticar a ese usuario con el servidor de Microsoft AD/LDAP.
3. El ASA ata al servidor LDAP con las credenciales configuradas en el ASA (admin en este caso), y mira para arriba el nombre de usuario proporcionado.
4. Si se encuentra el nombre de usuario, el ASA intenta atar al servidor LDAP con las credenciales que el usuario proporciona en el login.
5. Si el segundo lazo es acertado, el ASA procesa los atributos de los usuarios, que incluye el **memberOf**.
6. El atributo del **memberOf** es asociado a **CVPN3000-Radius-IETF-Class** por la correspondencia configurada LDAP Attibute.El valor que indica la calidad de miembro en el grupo de los **empleados** se asocia a **ExamplePolicy1**.El valor que indica la calidad de miembro en el grupo de **contratistas** se asocia a **ExamplePolicy2**.
7. Se examina el atributo nuevamente asignado **CVPN3000-Radius-IETF-Class** y se hace una determinación de la directiva del grupo.El valor ExamplePolicy1 hace la directiva del grupo ExamplePolicy1 ser asignado al usuario.El valor ExamplePolicy2 hace la directiva del grupo ExamplePolicy2 ser asignado al usuario.

Configurar

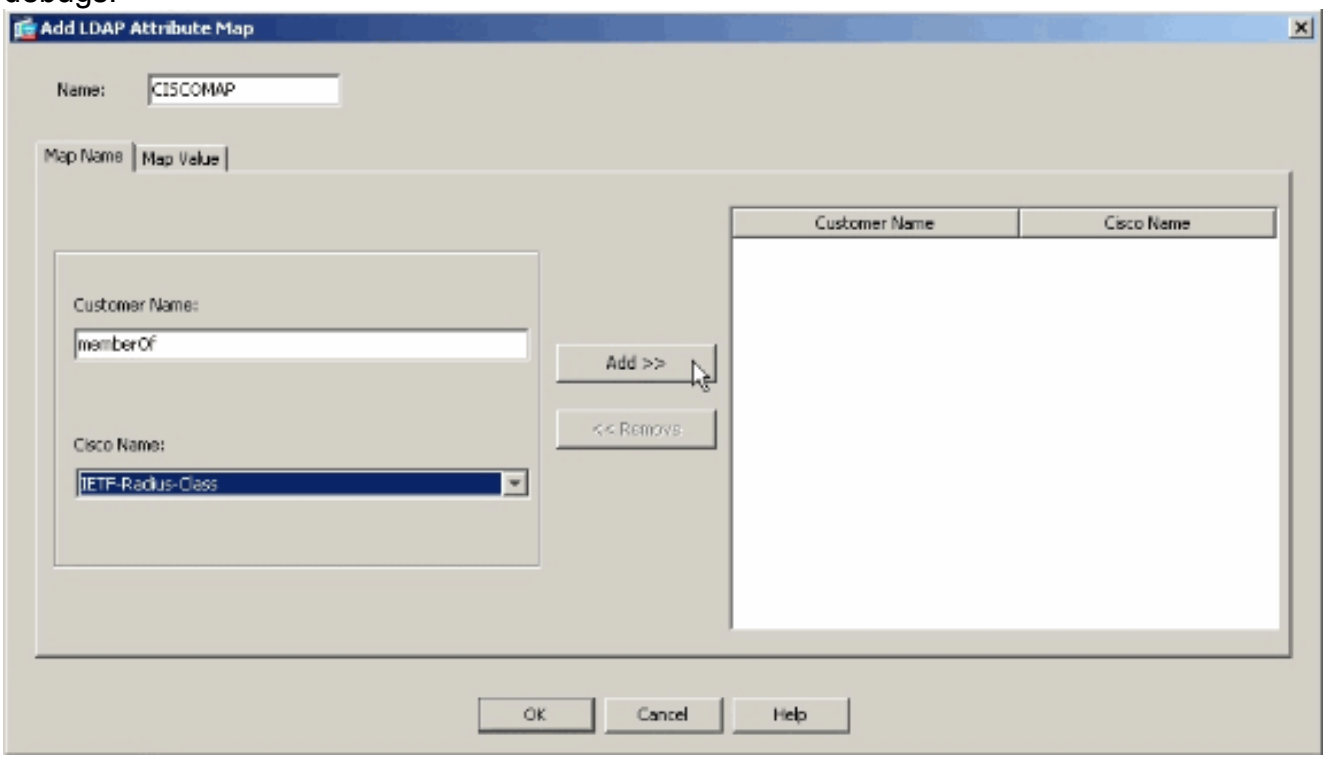
Configure el ASA

En esta sección, le presentan con la información para configurar el ASA para asignar una directiva del grupo a los usuarios basados en sus atributos LDAP.

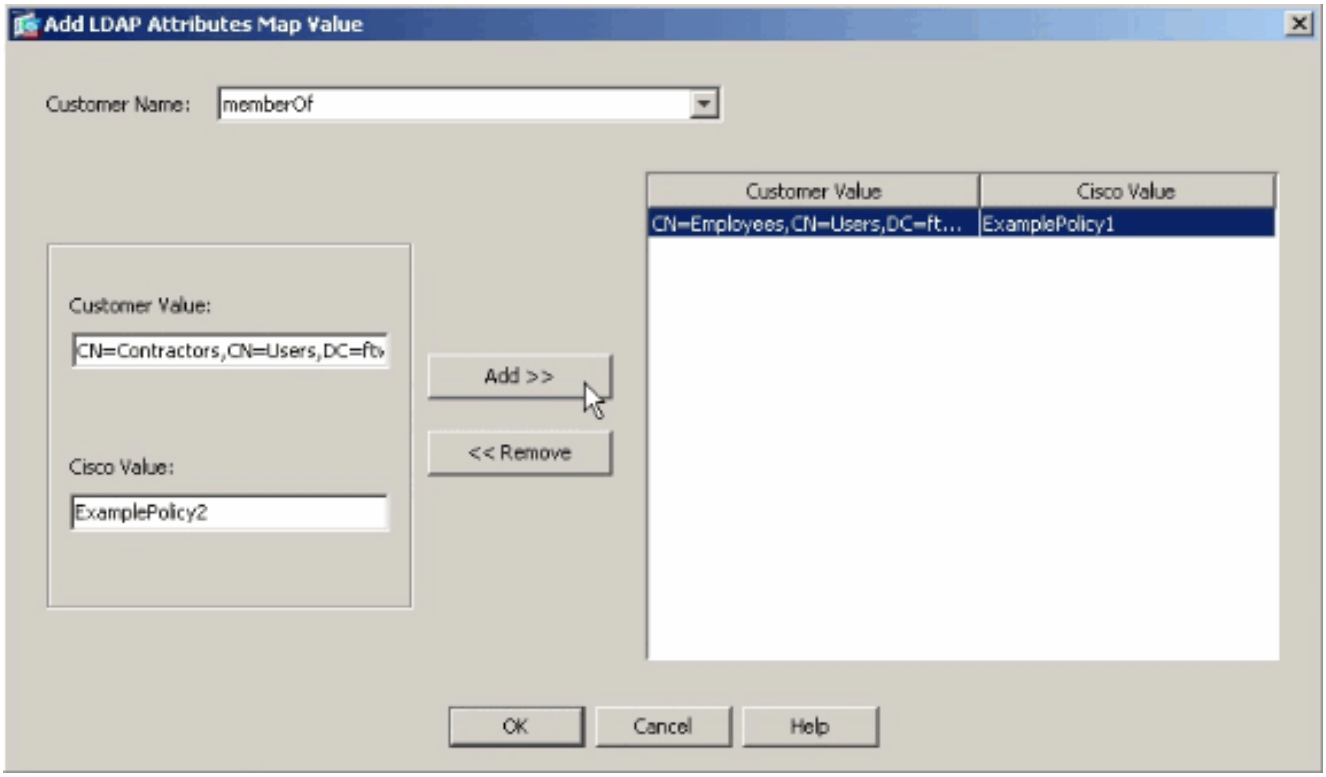
ASDM

Complete estos pasos en el Administrador de dispositivos de seguridad adaptante (ASDM) para configurar la correspondencia LDAP en el ASA.

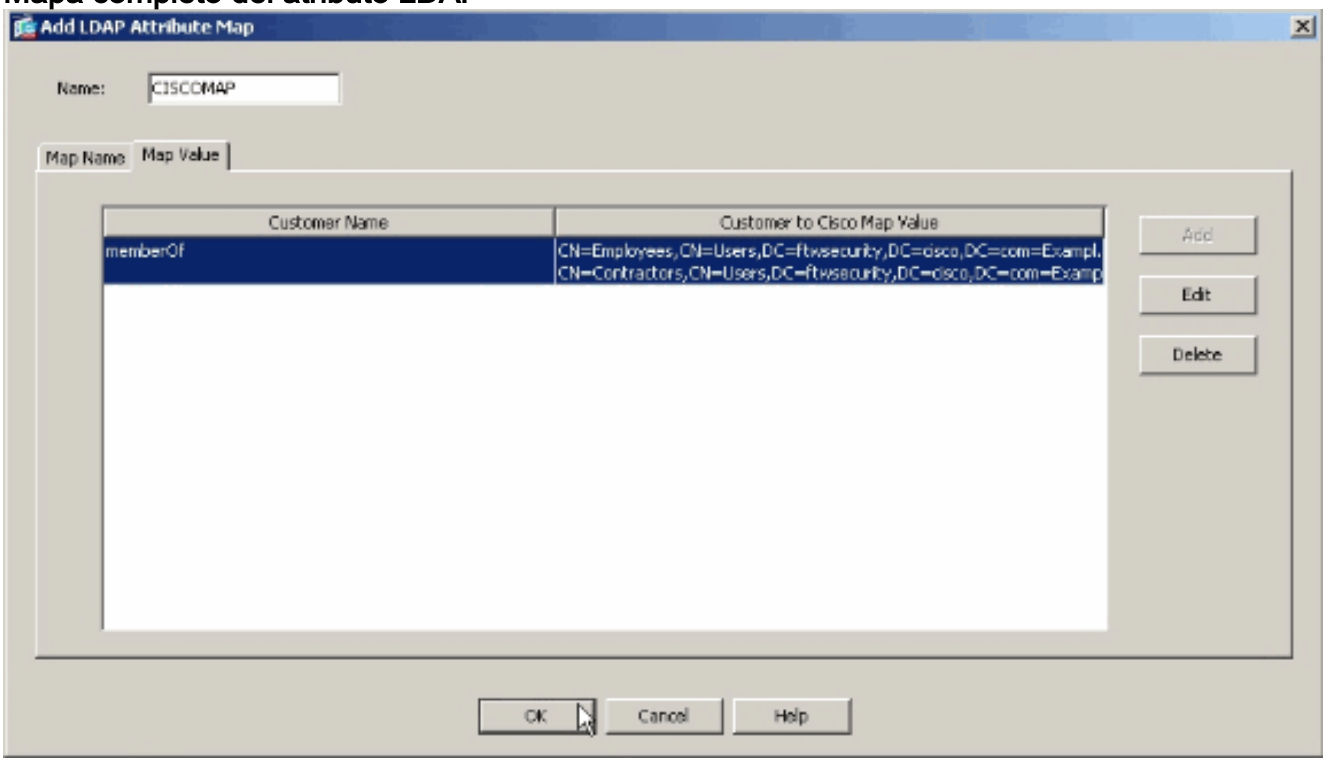
1. Navegue a la **configuración > al VPN de acceso remoto >AAA ponen > mapa del atributo LDAP**.
2. Haga clic en Add (Agregar).
3. Nombre la correspondencia.
4. Cree una asignación entre un atributo LDAP y el atributo de la IETF-Radio-**clase** en el ASA. En este ejemplo, el **nombre del cliente** es el atributo del **memberOf** en el Active Directory. Se asocia al **nombre de Cisco de la IETF-Radio-clase**. Haga clic en Add (Agregar).Nota: Los nombres y los valores del atributo son con diferenciación entre mayúsculas y minúsculas.Nota: Si usted no conoce los nombres o los deletreos exactos del atributo que son proporcionados por el servidor LDAP, puede ser útil examinar los debugs antes de que usted cree la correspondencia. Vea la sección del verificar para más información sobre cómo identificar los atributos LDAP con los
debugs.



5. Después de que usted agregue la asignación del atributo, haga clic la lengueta del **valor del mapa**, y el tecleo **agrega** para crear una asignación del valor. Agregue tantas asignaciones del valor como sea necesario, y haga clic la **AUTORIZACIÓN** cuando está acabado.**Valor del cliente - el** valor de atributo del servidor LDAP**Valor de Cisco - el** nombre de la directiva del grupo en el ASAEn este ejemplo, el **CN=Employees, cn=Users, DC=ftwsecurity, dc=cisco,** valor del memberOf del **dc=com** se asocia a **ExamplePolicy1** y el **CN=Contractors, cn=Users, DC=ftwsecurity, dc=cisco,** valor del memberOf del **dc=com** se asocia a **ExamplePolicy2**.

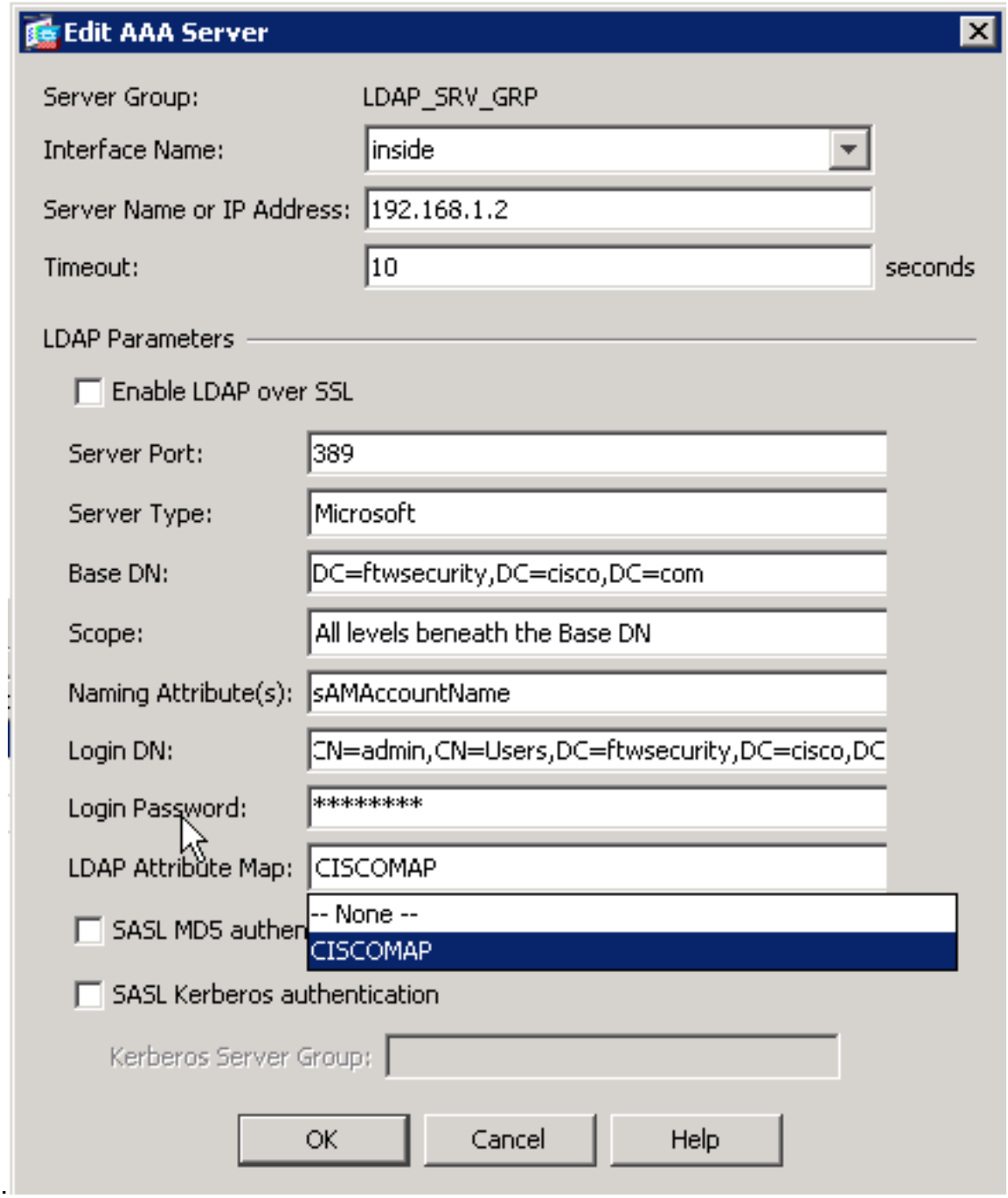


Mapa completo del atributo LDAP



6. Una vez que usted crea la correspondencia, debe ser asignada al servidor del Authentication, Authorization, and Accounting (AAA) que se configura para la autenticación ldap. Elija a los **Grupos de servidores AAA del** panel izquierdo.
7. Seleccione a su servidor de AAA que se configure para el LDAP, y el tecleo **edita**.
8. En la parte inferior de la ventana que aparece, localice la lista desplegable del **mapa del atributo LDAP**. Elija la lista que usted acaba de crear. Haga Click en OK cuando está

acabado.



CLI

Complete estos pasos en el CLI para configurar la correspondencia LDAP en el 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
```

Configure una grupo-directiva NOACCESS

Usted puede crear una grupo-directiva NOACCESS para negar la conexión VPN cuando el usuario no es grupos uces de los de la parte de LDAP. Estos fragmentos de la configuración se

muestran para su referencia:

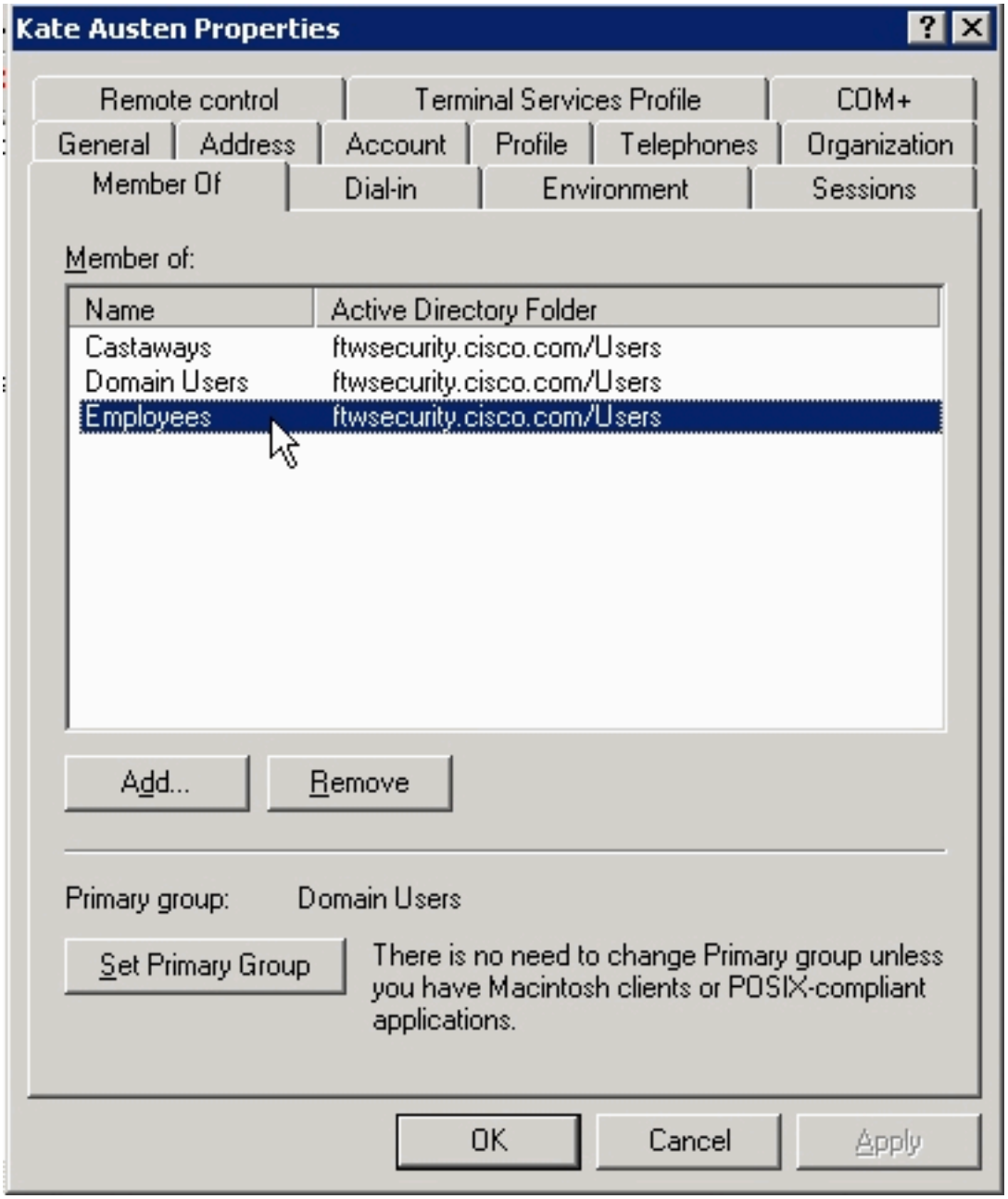
```
group-policy NOACCESS internal
group-policy NOACCESS attributes
 vpn-simultaneous-logins 0
 vpn-tunnel-protocol IPSec webvpn
```

Usted necesita aplicar esta directiva del grupo como directiva del grupo predeterminado al grupo de túnel. De modo que los usuarios que consiguen una asignación de la correspondencia del atributo LDAP, por ejemplo los que pertenezcan a un grupo deseado LDAP, pueda conseguir sus directivas y usuarios deseados del grupo que no consigan ninguna asignación, por ejemplo los que no pertenecen al LDAP deseado un de los agrupan, pueden conseguir la grupo-directiva NOACCESS del grupo de túnel, que bloquea el acceso para ellos.

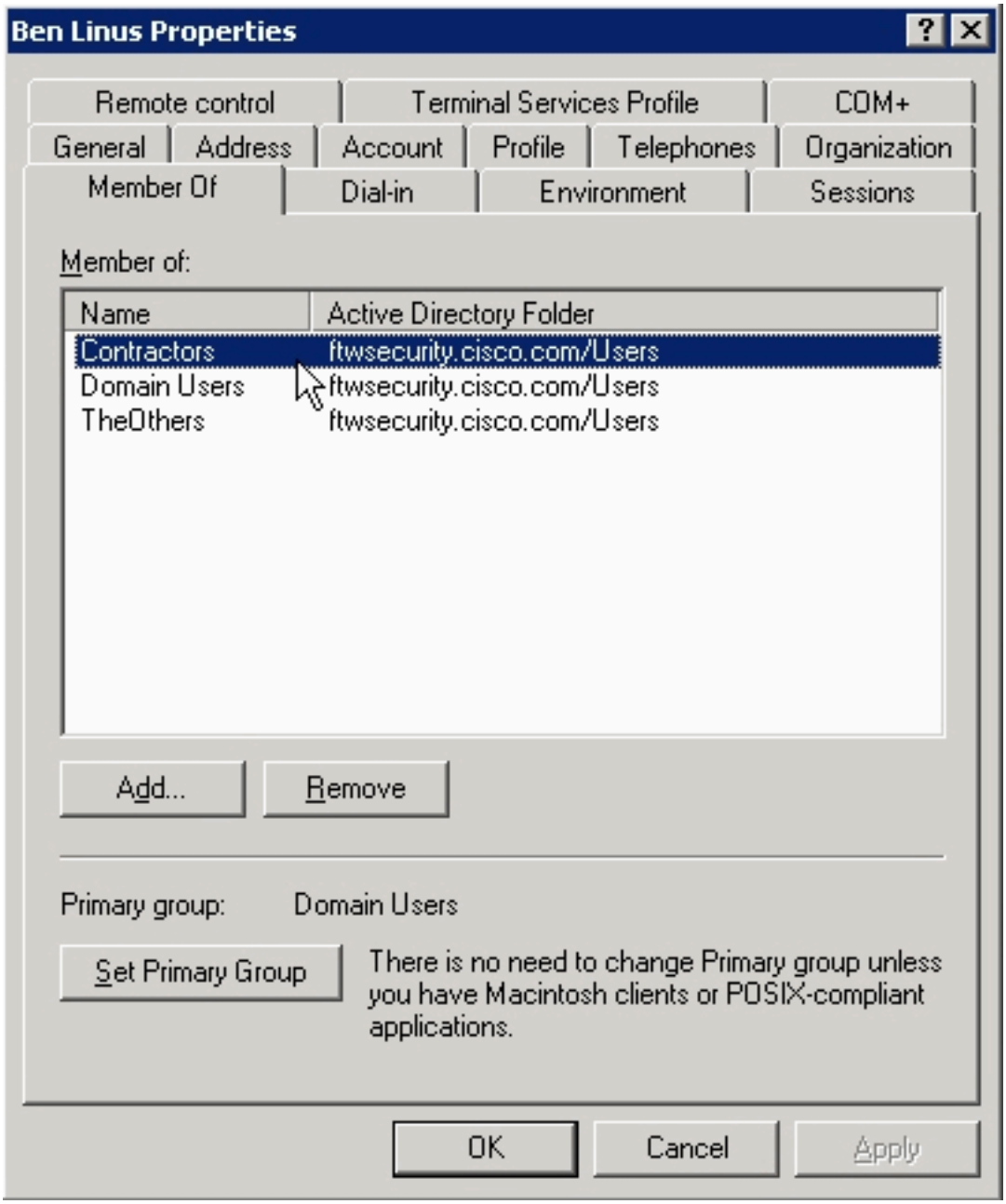
> Nota: Refiérase ASA/PIX: Asociando los clientes VPN a las directivas del grupo VPN con el ejemplo de la Configuración LDAP para más información sobre cómo crear diverso LDAP atribuyen las asignaciones que niegue el acceso a algunos usuarios.

Configure el Active Directory o al otro servidor LDAP

La única configuración requerida en el Active Directory o el otro servidor LDAP se relaciona con los atributos del usuario. En este ejemplo, el usuario Kate Austen es un miembro del grupo de los empleados en el AD:



Ben Linus es un miembro del grupo de contratistas:

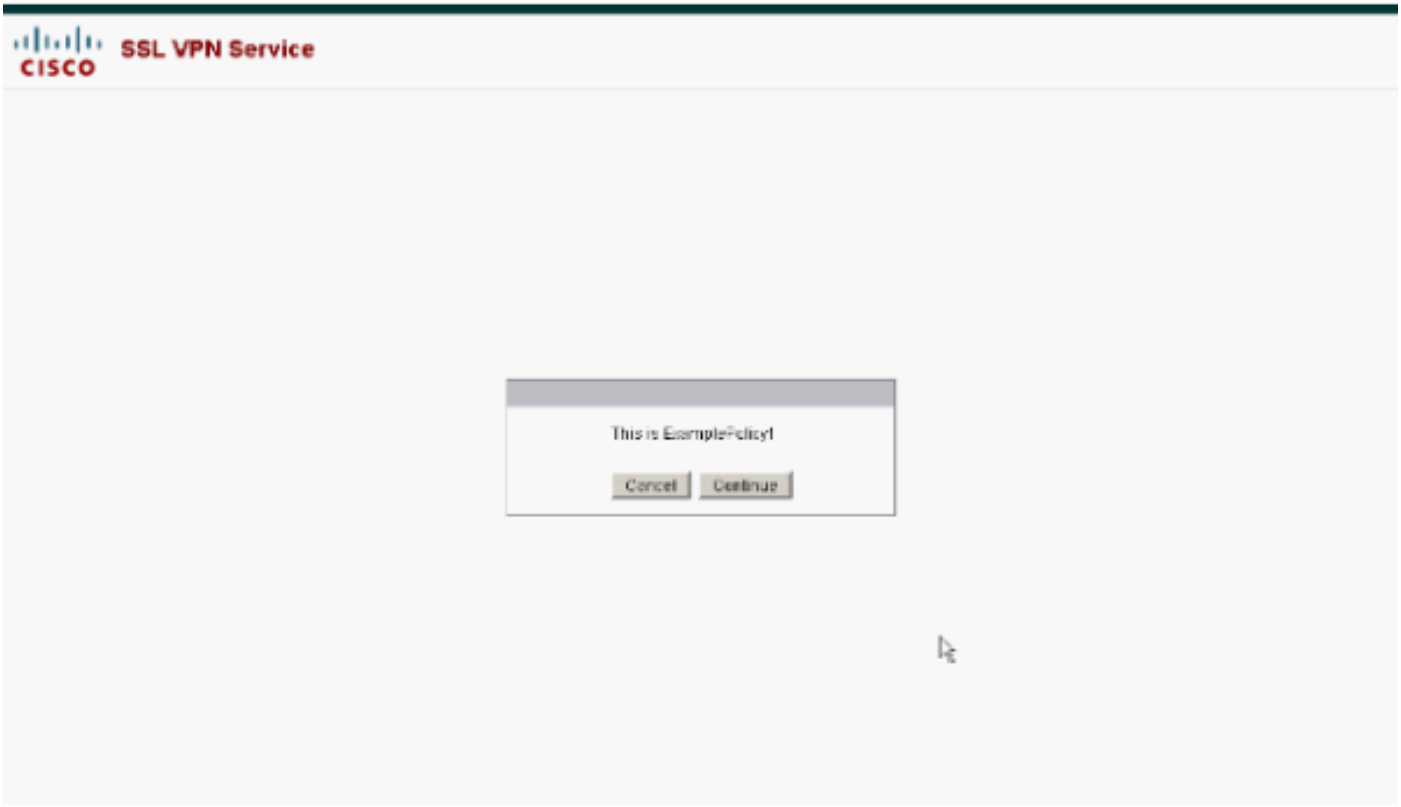


Verificación

Utiliza esta sección para verificar su configuración.

Login

Para verificar el éxito de su configuración, login como usuario que se supone tener una directiva del grupo asignada con la correspondencia del atributo LDAP. En este ejemplo, un banner se configura para cada directiva del grupo. El tiro de pantalla muestra que el **kate del** usuario abre una sesión con éxito y tiene **ExamplePolicy1** aplicado, porque ella es un miembro del grupo de los empleados.



Haga el debug de la transacción LDAP

Para verificar que ocurra la sincronización LDAP, o conseguir más información sobre qué atributos envía el servidor LDAP, publica el comando del **ldap 255 del debug** en la línea de comando ASA, y después intenta la autenticación.

En este debug, el **kate del** usuario se asigna la directiva **ExamplePolicy1 del** grupo porque ella es un miembro del grupo de los **empleados**. Este debug también muestra que el **kate** es un miembro del grupo de los **náufragos**, pero que el atributo no está asociado, así que está ignorado.

```
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 este debug, asignan el usuario **ben la** directiva del grupo **ExamplePolicy2** porque él es un miembro del grupo de **contratistas**. Este debug también muestra que **ben** es miembro del grupo de **TheOthers**, pero que el atributo no está asociado, así que está ignorado.

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

Troubleshooting

Use esta sección para resolver problemas su configuración.

Atribuya los nombres y los valores son con diferenciación entre mayúsculas y minúsculas

Los nombres y los valores del atributo son con diferenciación entre mayúsculas y minúsculas. Si no ocurre su asignación correctamente, esté seguro que usted utiliza el deletreo y la capitalización correctos en su correspondencia del atributo LDAP para los nombres y los valores del atributo de Cisco y LDAP.

El ASA no puede autenticar a los usuarios del servidor LDAP

El ASA no puede autenticar a los usuarios del servidor LDAP. Aquí están los debugs:

```
sesión de la petición de la sesión Start[1555805] del ldap 255 output:[1555805] la nueva, el
contexto 0xcd66c028, reqType = 1[1555805] la fibra started[1555805] que crean el contexto LDAP
con uri=ldaps://172.30.74.70:636[1555805] conecta con el servidor LDAP:
ldaps://172.30.74.70:636, estatus = supportedLDAPVersion Successful[1555805]: valor =
supportedLDAPVersion 3[1555805]: el valor = el atascamiento 2[1555805] como
administrator[1555805] que realiza la autenticación simple para los sysservices a la
autenticación simple 172.30.74.70[1555805] para el código de retorno de los sysservices (49)
credentials[1555805] inválidos no podido para atar como código de retorno del administrador (-1)
no pueden entrar en contacto los bytes de los bytes Rx=605 de la salida Tx=222 de la fibra LDAP
server[1555805], extremo de la sesión status=-2[1555805]
```

En cuanto a los debugs, o el formato del login DN LDAP es incorrecto o la contraseña es incorrecta así que verifique ambos para resolver el problema.