PIX/ASA 8.0: Use a autenticação LDAP para atribuir uma política do grupo no início de uma sessão

Índice

Introdução

Este documento descreve como usar a autenticação do Lightweight Directory Access Protocol (LDAP) a fim atribuir uma política do grupo no início de uma sessão. Frequentemente, os administradores querem fornecer aos usuários VPN diferentes permissões de acesso ou conteúdo WebVPN. Na ferramenta de segurança adaptável (ASA) isto é conseguido regularmente com a atribuição de políticas diferentes do grupo aos usuários diferentes. Quando a autenticação LDAP está em uso, esta pode ser obtida automaticamente com um mapa do atributos LDAP.

A fim usar o LDAP para atribuir uma política do grupo a um usuário, você precisa de configurar um mapa que trace um atributo LDAP, tal como o **memberOf do** atributo do diretório ativo (AD), ao atributo da IETF-Raio-**classe** que é compreendido pelo ASA. O mapeamento do atributo é estabelecido uma vez, você deve traçar o valor de atributo configurado no servidor ldap ao nome de uma política do grupo no ASA.

> Nota: O atributo do **memberOf** corresponde ao grupo que o usuário é um a parte de no diretório ativo. É possível para um usuário ser um membro de mais de um grupo no diretório ativo. Isto faz com que os atributos múltiplos do **memberOf** sejam enviados pelo server, mas o ASA pode somente combinar um atributo a uma política do grupo.

Pré-requisitos

Requisitos

Este documento exige que uma instalação de trabalho da autenticação LDAP está configurada já no ASA. Consulte para configurar a autenticação LDAP para usuários WebVPN a fim aprender como estabelecer uma configuração básica da autenticação LDAP no ASA.

Componentes Utilizados

A informação neste documento é baseada no PIX/ASA 8.0.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Neste exemplo, o **memberOf do** atributo AD/LDAP é traçado ao atributo **CVPN3000-Radius-IETF-Class** ASA. O atributo de classe é usado a fim atribuir políticas do grupo no ASA. Este é o processo geral que o ASA termina quando autentica usuários com LDAP:

1. O usuário inicia uma conexão ao ASA.
2. O ASA é configurado para autenticar esse usuário com o server de Microsoft AD/LDAP.
3. O ASA liga ao servidor ldap com as credenciais configuradas no ASA (admin neste caso), e olha acima o username fornecido.
4. Se o username é encontrado, o ASA tenta ligar ao servidor ldap com as credenciais que o usuário fornece no início de uma sessão.
5. Se o segundo ligamento é bem sucedido, o ASA processa os atributos dos usuários, que inclui o **memberOf**.
6. O atributo do **memberOf** é traçado a **CVPN3000-Radius-IETF-Class pelo** mapa configurado LDAP Attibute.O valor que indica a sociedade no grupo dos **empregados** é traçado a **ExamplePolicy1**.O valor que indica a sociedade no grupo de **contratantes** é traçado a **ExamplePolicy2**.
7. O atributo recentemente atribuído **CVPN3000-Radius-IETF-Class** é examinado e uma determinação da política do grupo é feita.O valor ExamplePolicy1 faz com que a política do grupo ExamplePolicy1 seja atribuída ao usuário.O valor ExamplePolicy2 faz com que a política do grupo ExamplePolicy2 seja atribuída ao usuário.

Configurar

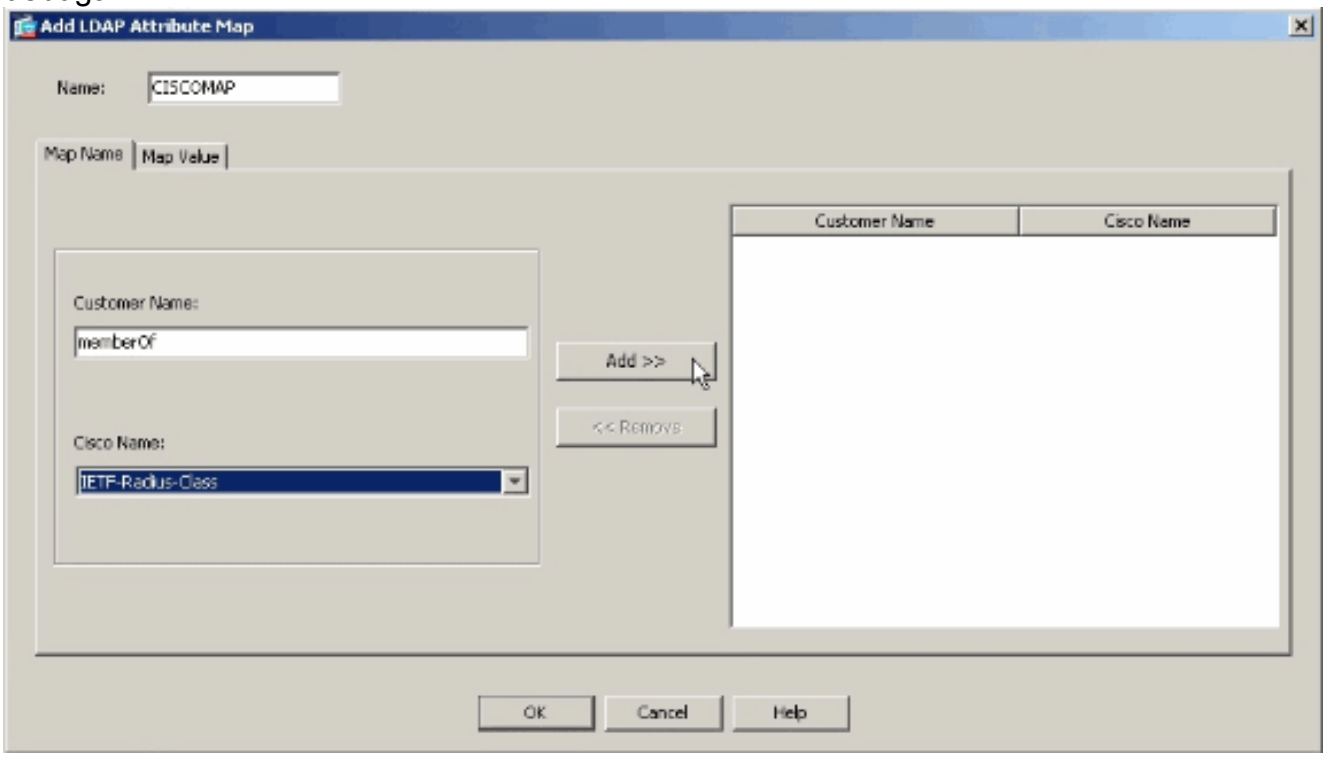
Configurar o ASA

Nesta seção, você é presentado com a informação para configurar o ASA para atribuir uma política do grupo aos usuários baseados em seus atributos LDAP.

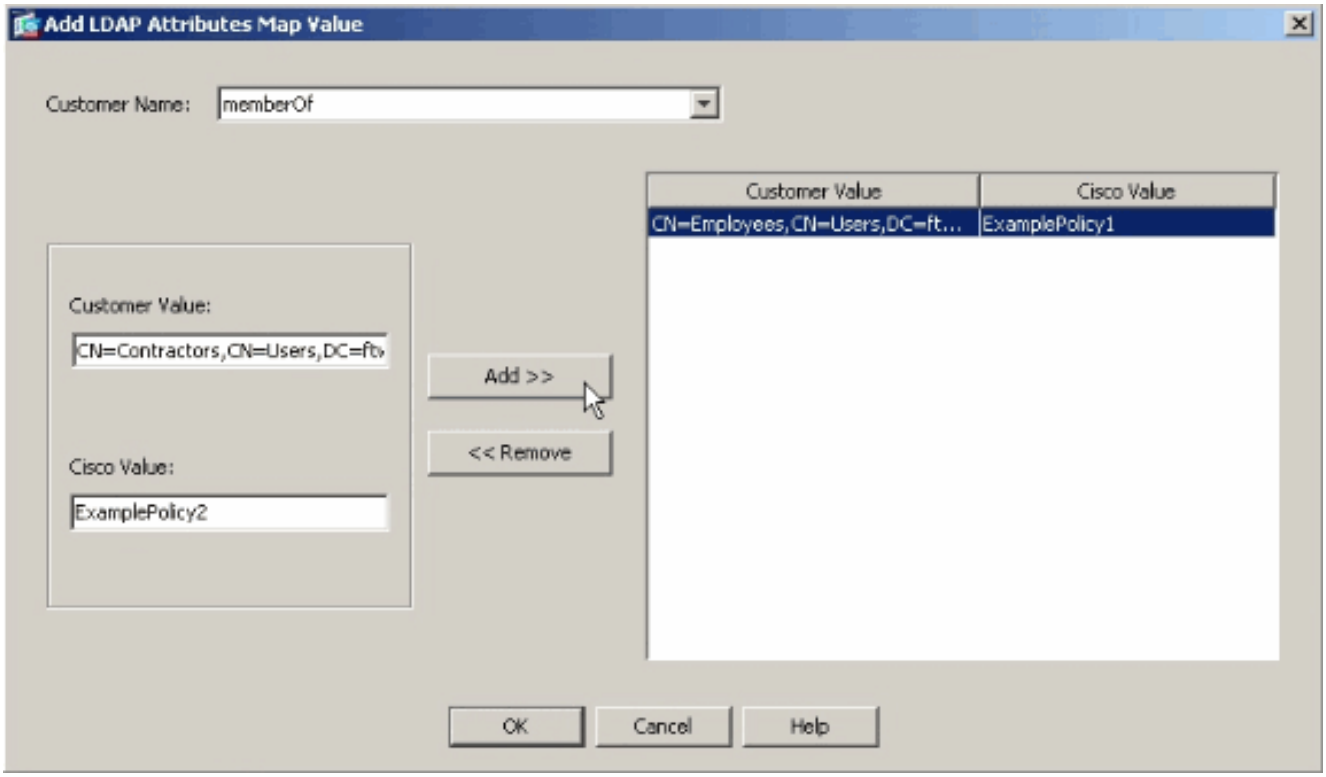
ASDM

Termine estas etapas no Security Device Manager adaptável (ASDM) a fim configurar o mapa LDAP no ASA.

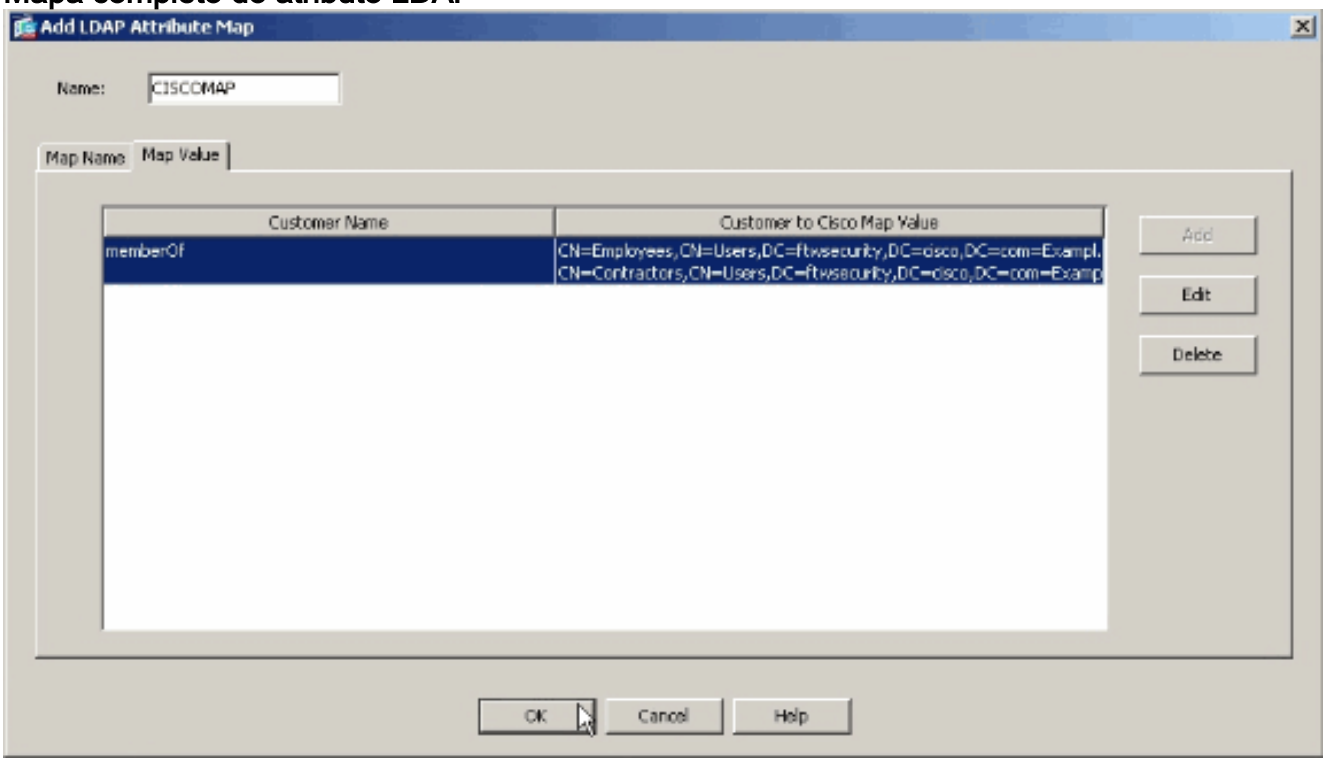
1. Navegue à **configuração > ao acesso remoto VPN > ao AAA Setup > mapa do atributo LDAP**.
2. Clique em Add.
3. Nomeie o mapa.
4. Crie um mapeamento entre um atributo LDAP e o atributo da IETF-Raio-**classe no** ASA. Neste exemplo, o **nome do cliente** é o atributo do **memberOf no** diretório ativo. É traçado ao **nome de Cisco da IETF-Raio-classe**. Clique em Add.Nota: Os nomes e os valores do atributo são diferenciando maiúsculas e minúsculas.Nota: Se você não conhece os nomes ou as soletrações exatas do atributo que estão fornecidos pelo servidor ldap, pode ser útil examinar debuga antes que você crie o mapa. Veja que a seção da verificação para obter mais informações sobre de como identificar atributos LDAP com debuga.



5. Depois que você adiciona o mapeamento do atributo, clique a aba do **valor do mapa**, e o clique **adiciona** a fim criar um mapeamento do valor. Adicionar tantos como mapeamentos do valor como necessário, e clique a **APROVAÇÃO** quando terminado.**Valor do cliente - o** valor de atributo do servidor ldap**Cisco avalia - o** nome da política do grupo no ASANeste exemplo, o **CN=Employees, cn=Users, DC=ftwsecurity, dc=cisco,** valor do memberOf do **dc=com** é traçado a **ExamplePolicy1** e o **CN=Contractors, cn=Users, DC=ftwsecurity, dc=cisco,** valor do memberOf do **dc=com** é traçado a **ExamplePolicy2**.

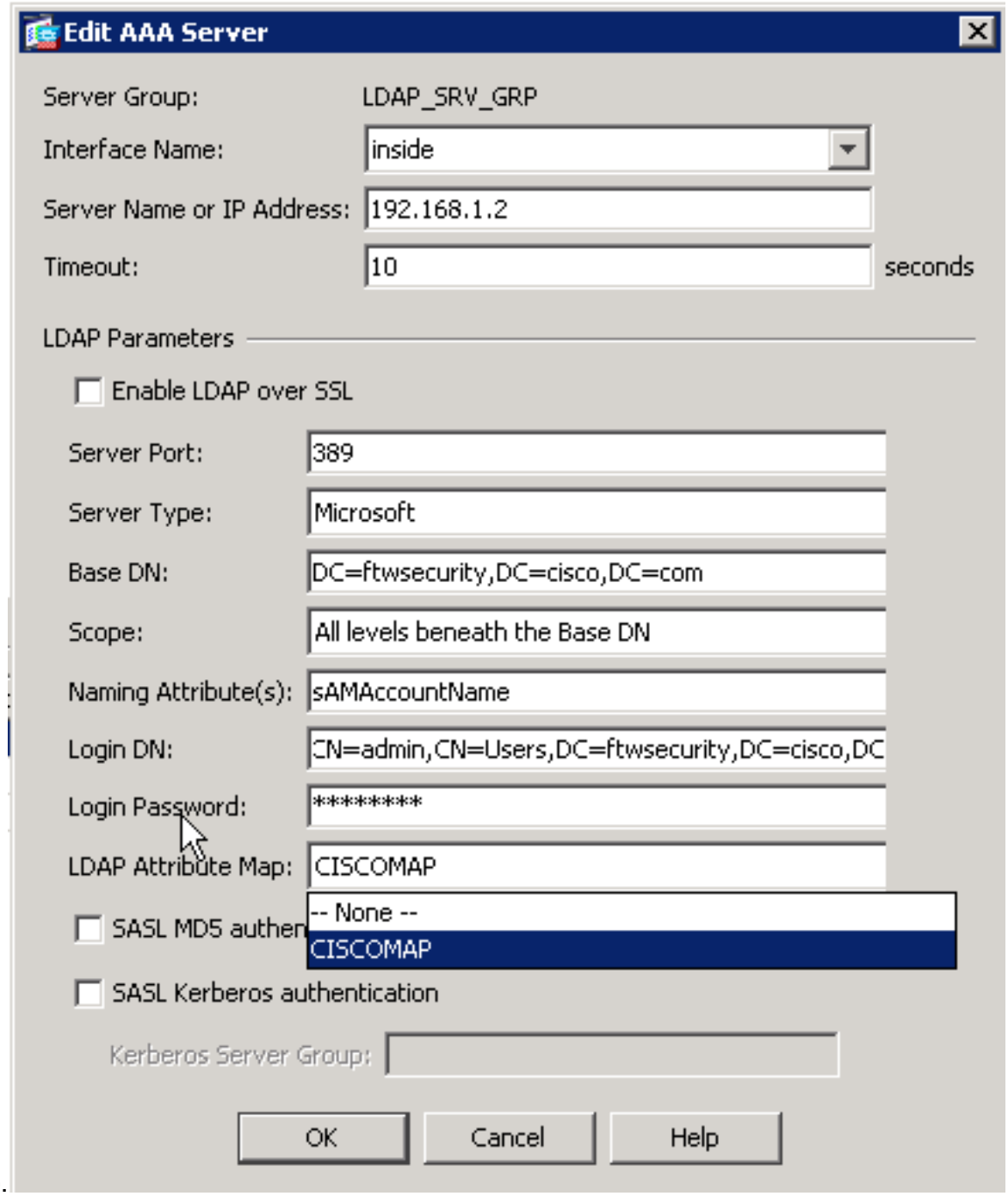


Mapa completo do atributo LDAP



6. Uma vez que você cria o mapa, deve ser atribuído ao server do Authentication, Authorization, and Accounting (AAA) que é configurado para a autenticação LDAP. Escolha **Grupos de servidores AAA do** painel esquerdo.
7. Selecione seu servidor AAA que é configurado para o LDAP, e o clique **edita**.
8. Na parte inferior do indicador que aparece, encontre a lista de drop-down do **mapa do atributo LDAP**. Escolha a lista que você apenas criou. Clique a **APROVAÇÃO** quando

terminado.



CLI

Termine estas etapas no CLI a fim configurar o mapa LDAP no 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
```

Configurar uma grupo-política NOACCESS

Você pode criar uma grupo-política NOACCESS a fim negar a conexão de VPN quando o usuário não é parte de alguns dos grupos LDAP. Este snippet de configuração é mostrado para sua

referência:

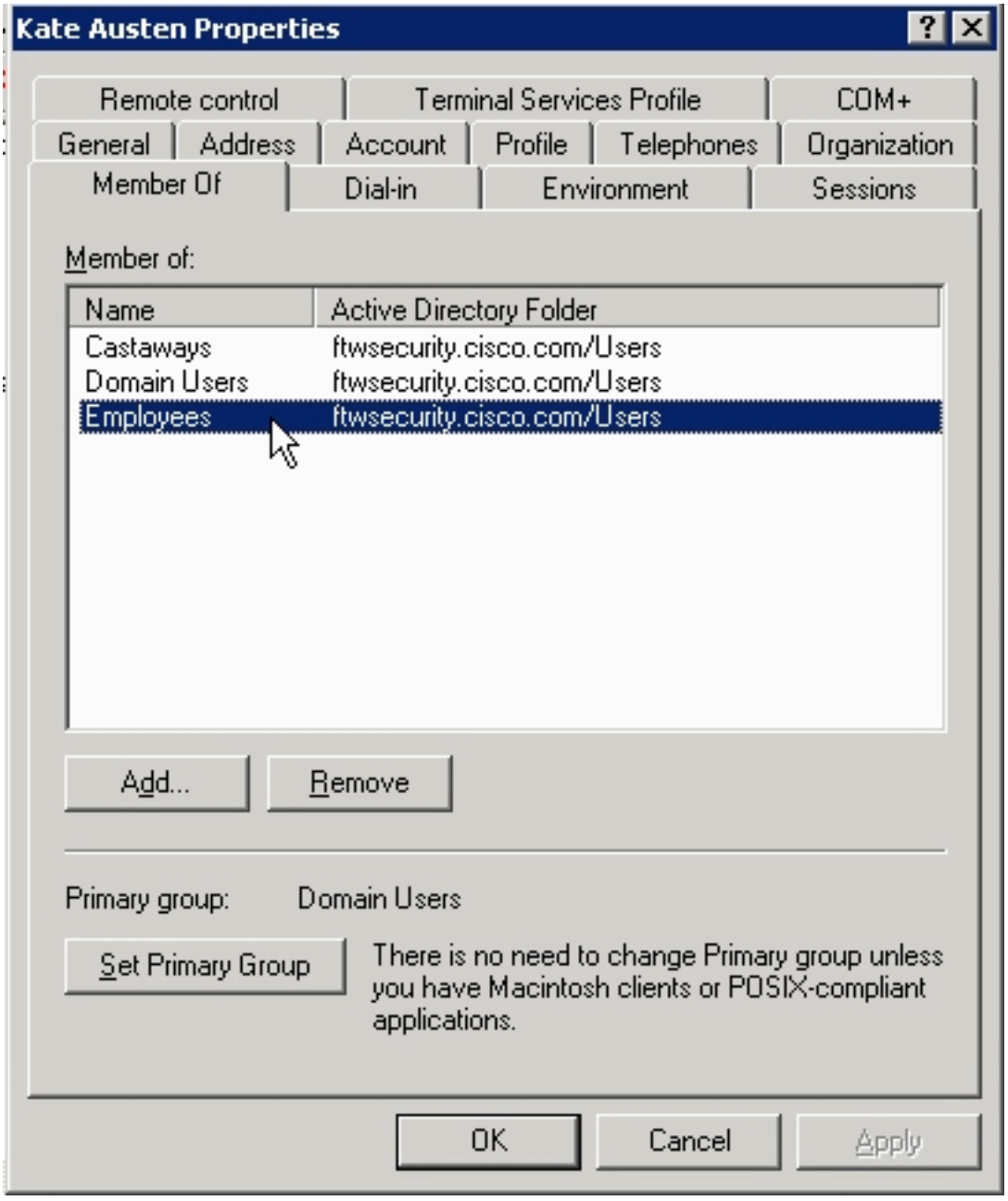
```
group-policy NOACCESS internal
group-policy NOACCESS attributes
 vpn-simultaneous-logins 0
 vpn-tunnel-protocol IPSec webvpn
```

Você precisa de aplicar esta política do grupo como uma política do grupo padrão ao grupo de túneis. De modo que os usuários que obtêm um mapeamento do mapa do atributo LDAP, por exemplo aqueles que pertencem a um grupo desejado LDAP, possa obter seus políticas e usuários desejados do grupo que não obtêm nenhum mapeamento, por exemplo aqueles que não pertencem a algum do LDAP desejado agrupam, podem obter a grupo-política NOACCESS do grupo de túneis, que obstrui o acesso para ele.

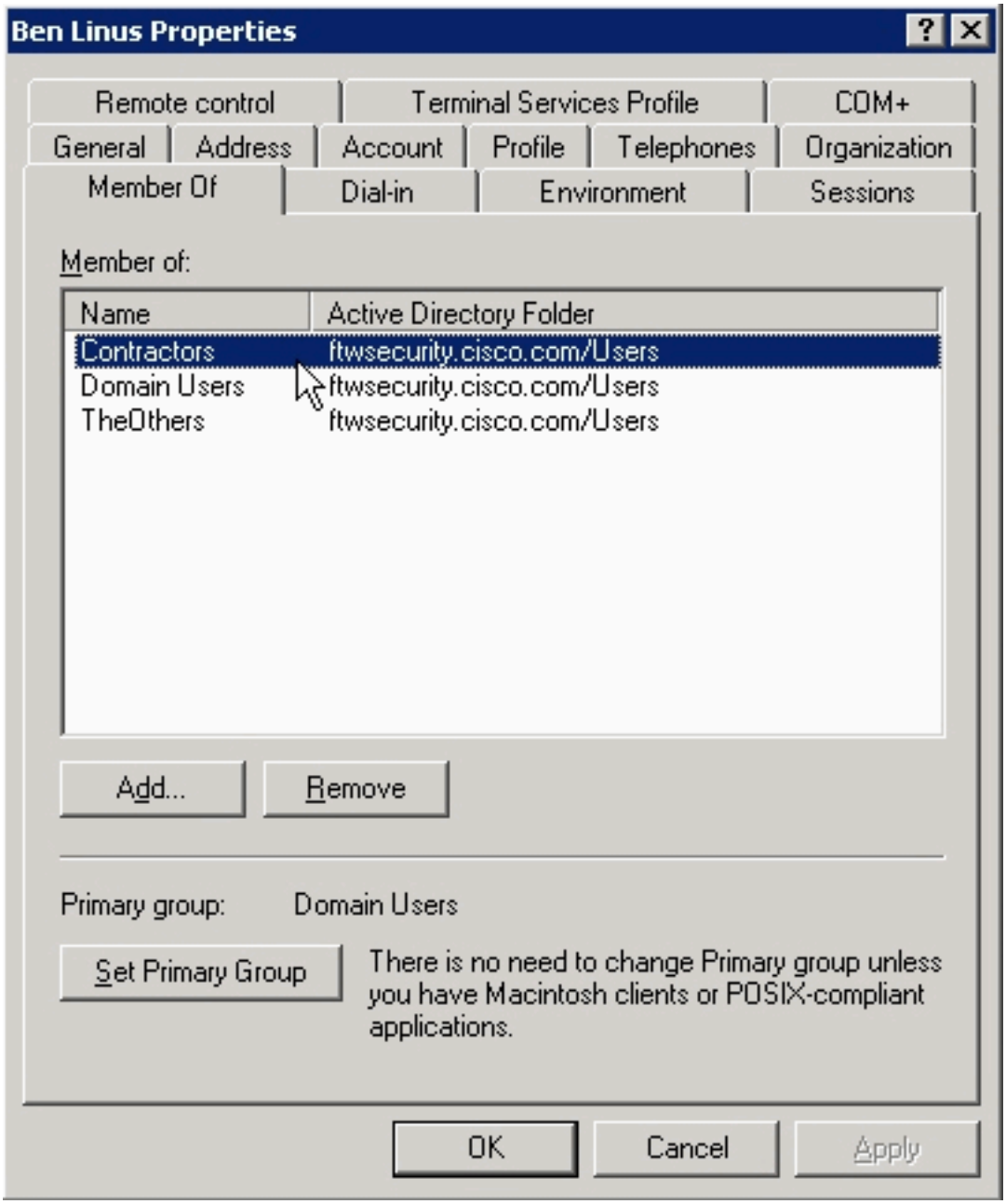
> Nota: Refira ASA/PIX: Traçando os clientes VPN às políticas do grupo de VPN com o exemplo da configuração ldap para obter mais informações sobre de como criar o LDAP diferente atribuem mapeamentos que nega o acesso a alguns usuários.

Configurar o diretório ativo ou o outro servidor ldap

A única configuração exigida no diretório ativo ou no outro servidor ldap relaciona-se aos atributos do usuário. Neste exemplo, o usuário Kate Austen é um membro do grupo dos empregados no AD:



Ben Linus é um membro do grupo de contratantes:

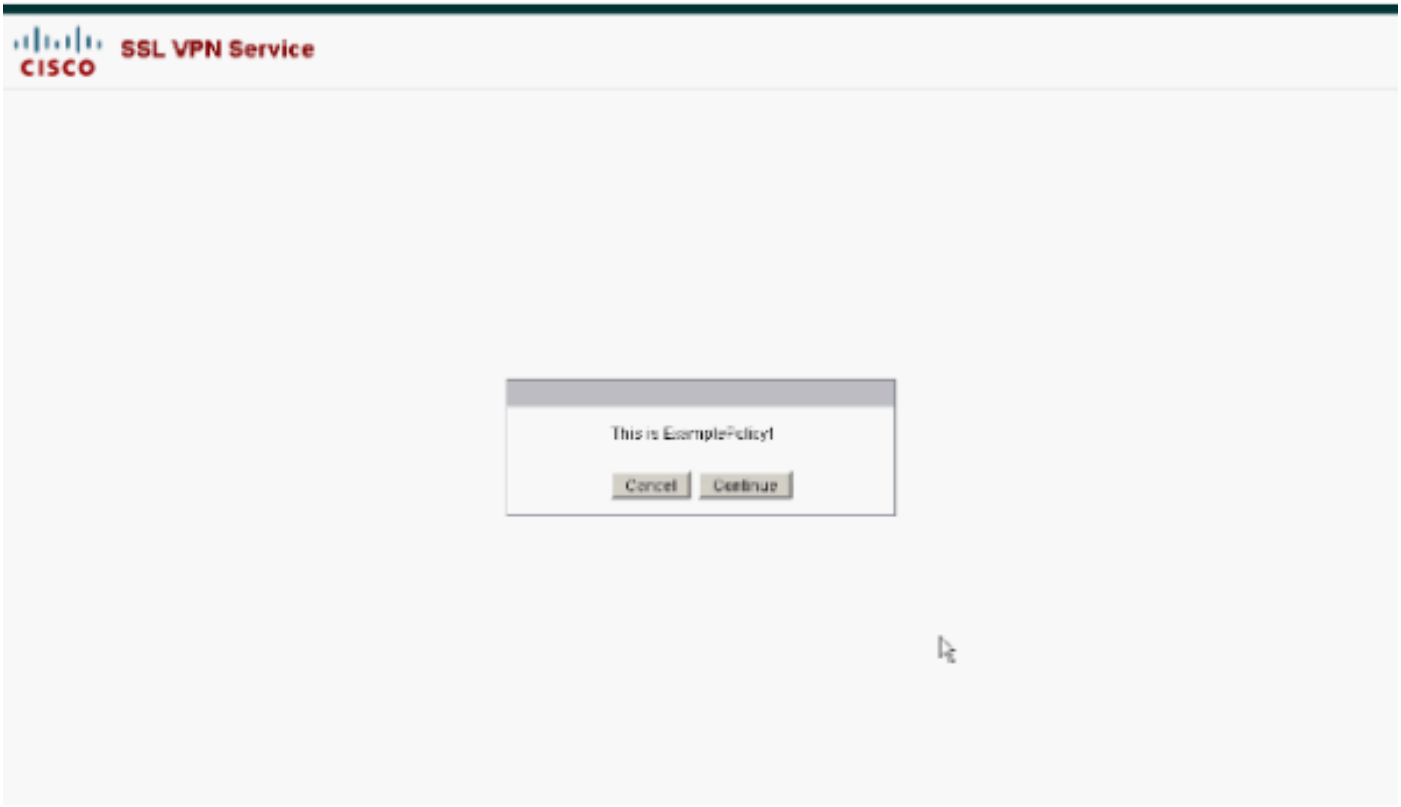


Verificar

Use esta seção para verificar a sua configuração.

Login

A fim verificar o sucesso de sua configuração, início de uma sessão como um usuário que seja suposto ter uma política do grupo atribuída com o mapa do atributo LDAP. Neste exemplo, uma bandeira é configurada para cada política do grupo. O tiro de tela mostra que o **kate do** usuário entra com sucesso e tem **ExamplePolicy1** aplicado, porque é um membro do grupo dos empregados.



Debugar a transação LDAP

A fim verificar que o mapeamento LDAP ocorre, ou obter mais informação no que atributos o servidor ldap envia, emitem o comando do **ldap 255 debugar na** linha de comando ASA, e tentam então a autenticação.

Nisto debugar, o usuário que **kate** é atribuído a política **ExamplePolicy1 do** grupo porque é um membro do grupo dos **empregados**. Isto debuga igualmente mostra que o **kate** é um membro do grupo dos **naufrágios**, mas que o atributo não está traçado, assim 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

Nisto debugar, o usuário que **ben** é atribuído a política do grupo **ExamplePolicy2** porque é um membro do grupo de **contratantes**. Isto debuga igualmente mostra que **ben** é membro do grupo de **TheOthers**, mas que o atributo não está traçado, assim 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 seção para fazer o troubleshooting da sua configuração.

Atribua nomes e os valores são diferenciando maiúsculas e minúsculas

Os nomes e os valores do atributo são diferenciando maiúsculas e minúsculas. Se seu mapeamento não ocorre corretamente, esteja certo que você usa a soletração e a capitalização corretas em seu mapa do atributo LDAP para Cisco e valores do atributo LDAP nomes e.

O ASA não pode autenticar usuários do servidor ldap

O ASA não pode autenticar usuários do servidor ldap. Seja aqui debuga:

```
a sessão nova do pedido da sessão Start[1555805] do ldap 255 output:[1555805], o contexto
0xcd66c028, reqType = 1[1555805] fibra started[1555805] que criam o contexto LDAP com o
uri=ldaps://172.30.74.70:636[1555805] conecta ao servidor ldap: ldaps://172.30.74.70:636, estado
= supportedLDAPVersion Successful[1555805]: valor = supportedLDAPVersion 3[1555805]: valor =
emperramento 2[1555805] como administrator[1555805] que executa a autenticação simples para
sysservices à autenticação simples 172.30.74.70[1555805] para o código retornado dos sysservices
(49) credentials[1555805] inválidos não estão ligados como o código retornado do administrador
(-1) não pode contactar bytes dos bytes Rx=605 da saída Tx=222 da fibra LDAP server[1555805],
extremidade da sessão status=-2[1555805]
```

Quanto para ao debuga, ou o formato do início de uma sessão DN LDAP está incorreto ou a senha está incorreta assim que verifique ambos a fim resolver a edição.