PIX/ASA 8.0 ：在登录时使用LDAP认证分配组策略

目录

简介
先决条件
要求
使用的组件
背景信息
配置
配置 ASA
ASDM
CLI
配置NOACCESS组政策
配置 Active Directory 或其他 LDAP 服务器
验证
洛金
调试 LDAP 事务
故障排除
属性名称和值区分大小写
ASA不能验证从LDAP服务器的用户

简介

本文描述如何使用轻量级目录访问协议(LDAP)验证为了分配组策略在登录。 管理员需要经常为 VPN 用户提供不同的访问权限或 WebVPN 内容。在可适应安全工具(ASA)上这通过不同的组策略的分配对不同的用户的有规律地达到。如果 LDAP 身份验证正在使用中，则可使用 LDAP 属性映射来自动实现此目标。

要使用 LDAP 将组策略分配给某个用户，需要对映射进行配置，使之将 Active Directory (AD) 属性 **memberOf** 等 LDAP 属性映射到 ASA 能够识别的 **IETF-Radius-Class** 属性。建立属性映射后，您必须将在 LDAP 服务器上配置的属性值映射到 ASA 上的组策略名称。

> **注意**：**memberOf** 属性对应于 Active Directory 中用户所在的组。在 Active Directory 中，一个用户可以是多个组的成员。这将导致服务器发送多个 **memberOf** 属性，但 ASA 只能将其中一个属性与一个组策略进行匹配。

先决条件

要求

本文档要求在 ASA 上已经配置了适用的 LDAP 身份验证设置。要了解如何在 ASA 上设置基本的 LDAP 身份验证配置，请参阅为 WebVPN 用户配置 LDAP 身份验证。

使用的组件

本文档中的信息根据PIX/ASA 8.0。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

在本示例中，AD/LDAP 属性 **memberOf** 映射到 ASA 属性 **CVPN3000-Radius-IETF-Class**。该类属性用于在 ASA 上分配组策略。下面是 ASA 在使用 LDAP 对用户进行身份验证时完成的一般步骤：

1. 用户发起到 ASA 的连接。
2. ASA 配置为使用 Microsoft AD/LDAP 服务器对该用户进行身份验证。
3. ASA 使用在 ASA 上配置的凭据（本例中为 admin）绑定到 LDAP 服务器，并查找所提供的用户名。
4. 如果找到用户名，则 ASA 尝试使用用户在登录时提供的凭据绑定到 LDAP 服务器。
5. 如果第二次绑定成功，则 ASA 将处理用户属性（包括 **memberOf**）。
6. 根据配置的 LDAP 属性映射，**memberOf** 属性将映射到 **CVPN3000-Radius-IETF-Class**。用于指示 **Employees** 组中成员资格的值将映射到 **ExamplePolicy1**。用于指示 **Contractors** 组中成员资格的值将映射到 **ExamplePolicy2**。
7. 检查新分配的 **CVPN3000-Radius-IETF-Class** 属性并确定组策略。使用 ExamplePolicy1 值时，将导致 ExamplePolicy1 组策略分配给用户。使用 ExamplePolicy2 值时，将导致 ExamplePolicy2 组策略分配给用户。

配置

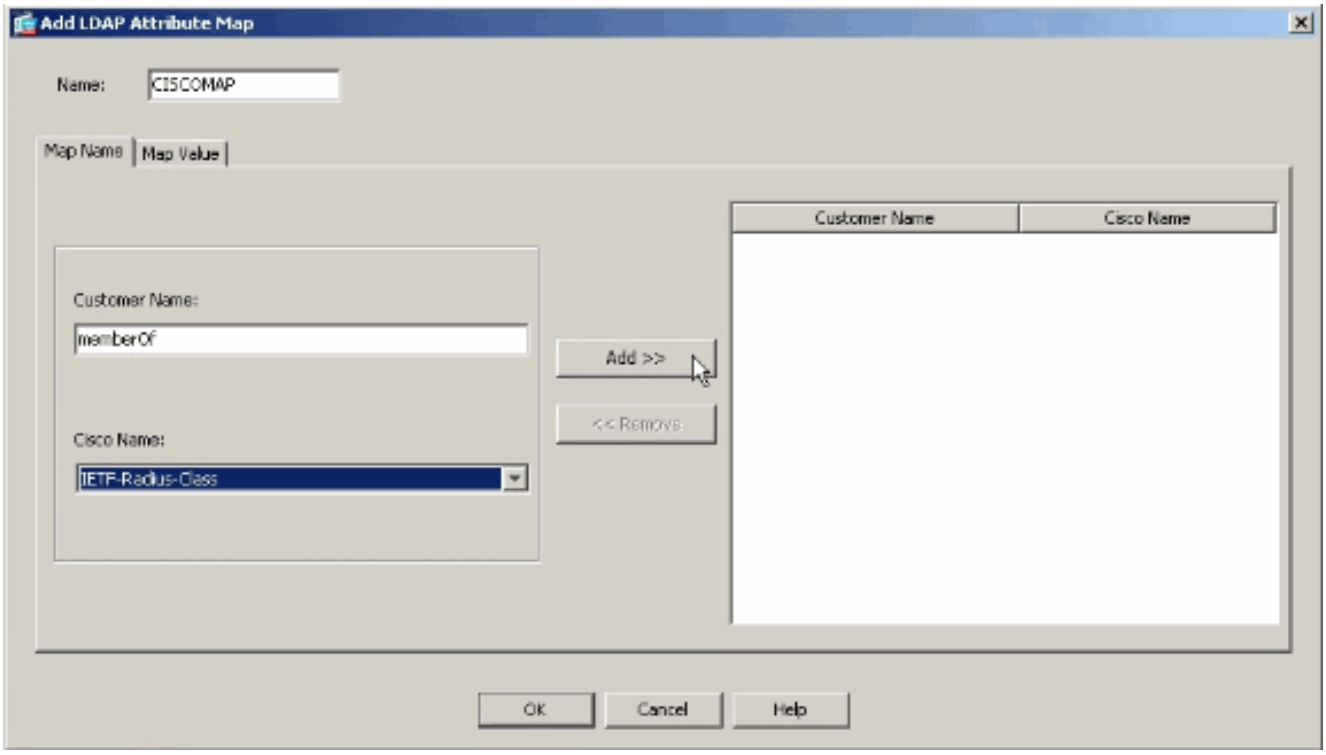
配置 ASA

本部分提供有关如何配置 ASA，以便根据用户的 LDAP 属性将组策略分配给用户的信息。

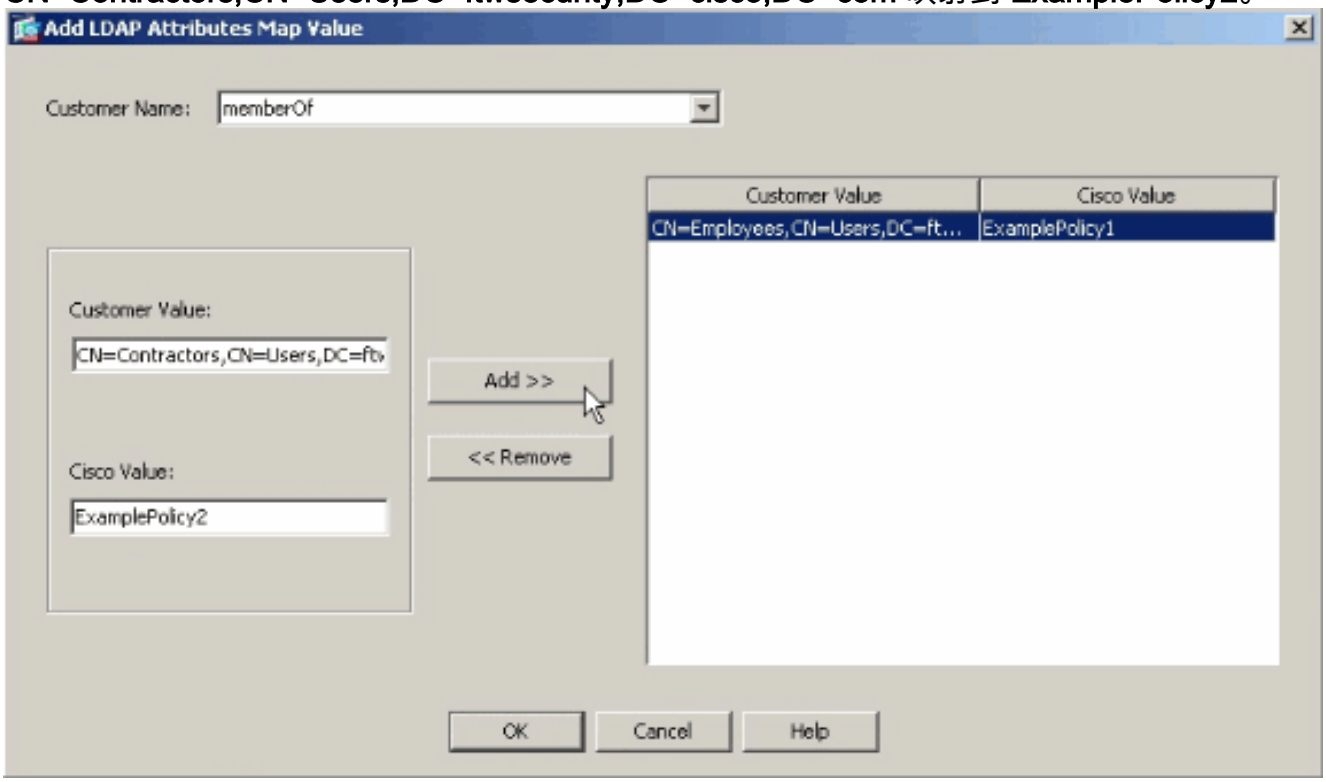
ASDM

在自适应安全设备管理器 (ASDM) 中完成下述步骤，以便在 ASA 上配置 LDAP 映射。

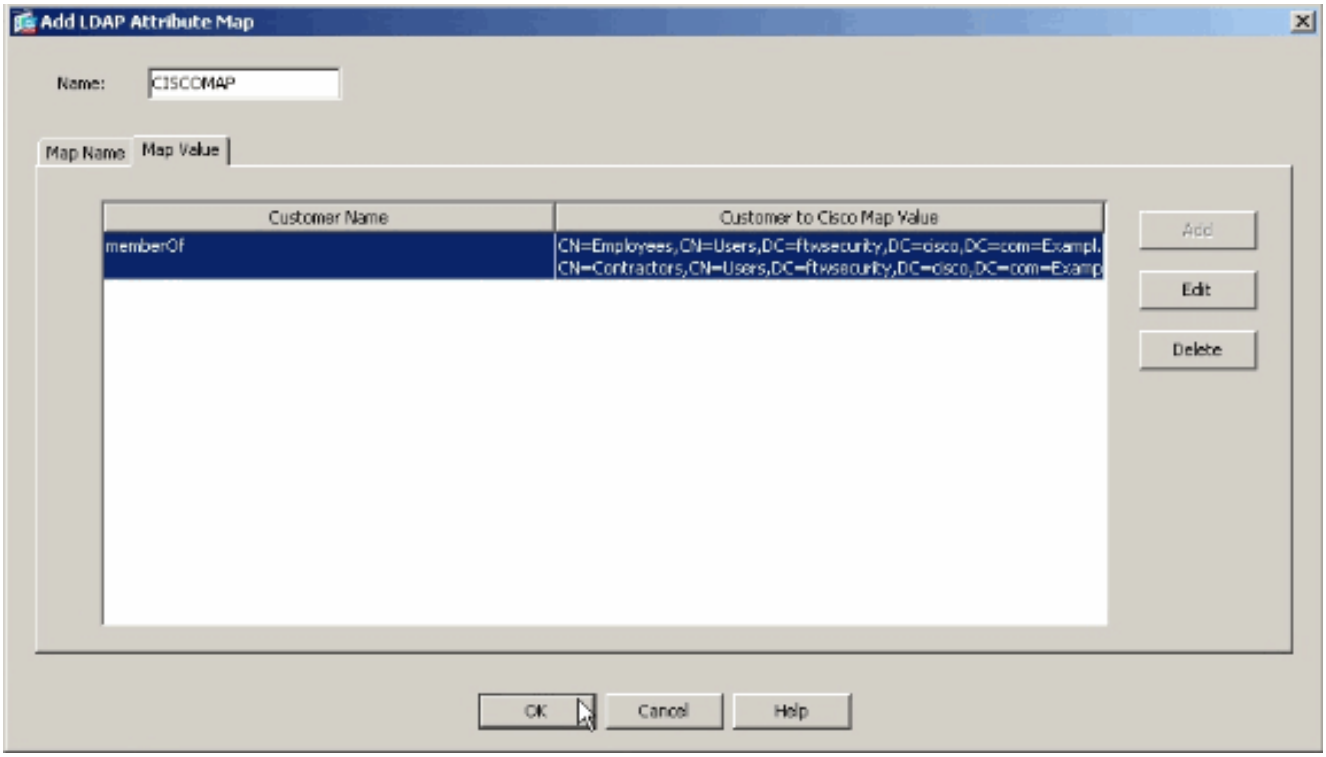
1. 导航到 Configuration > Remote Access VPN > AAA Setup > LDAP Attribute Map。
2. 单击 **Add**。
3. 为映射命名。
4. 在 LDAP 属性和 ASA 上的 **IETF-Radius-Class** 属性之间创建一个映射。在本示例中，**Customer Name** 是 Active Directory 中的 **memberOf** 属性。该属性将映射到 **IETF-Radius-Class** 的 **Cisco Name** 。单击 **Add**。**注意**：属性名称和值区分大小写。**注意**：如果不知道 LDAP 服务器所提供的确切属性名称或拼写，在创建映射之前查看调试结果可能很有帮助。有关如何通过调试来确定 LDAP 属性的详细信息，请参阅验证部分。



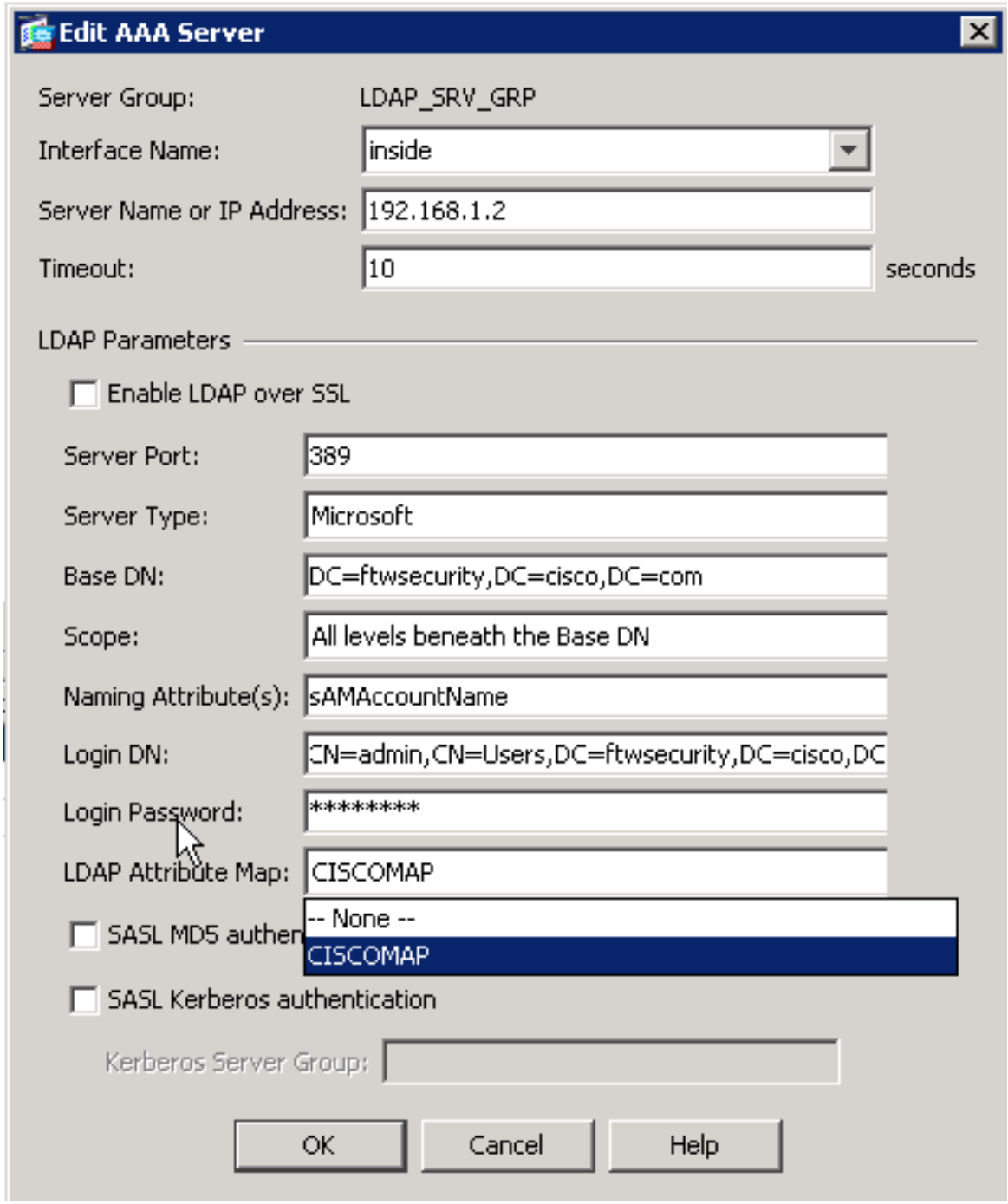
5. 添加属性映射后，单击 **Map Value** 选项卡，然后再单击 **Add** 可创建值映射。根据需要添加多个值映射，然后在完成时单击 **OK**。**客户值-**从LDAP服务器的属性值**思科值-**组策略的名称在ASA的在本示例中，memberOf 值 **CN=Employees,CN=Users,DC=ftwsecurity,DC=cisco,DC=com** 映射到 **ExamplePolicy1**，memberOf 值 **CN=Contractors,CN=Users,DC=ftwsecurity,DC=cisco,DC=com** 映射到 **ExamplePolicy2**。



完成 LDAP 属性映射



6. 一旦创建地图，必须分配到为LDAP认证配置的验证、授权和统计(AAA)服务器。从左窗格中选择 **AAA Server Groups**。
7. 选择已针对 LDAP 进行配置的 AAA 服务器，然后单击 **Edit**。
8. 在所显示的窗口底部，找到 **LDAP Attribute Map** 下拉列表。选择刚创建的列表。完成后单击



OK。

CLI

完成在CLI的这些步骤为了配置在ASA的LDAP地图。

```
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
```

配置NOACCESS组政策

当用户不作为的部分任何LDAP组时，您能创建NOACCESS组政策为了拒绝VPN连接。此配置片断显示供您的参考：

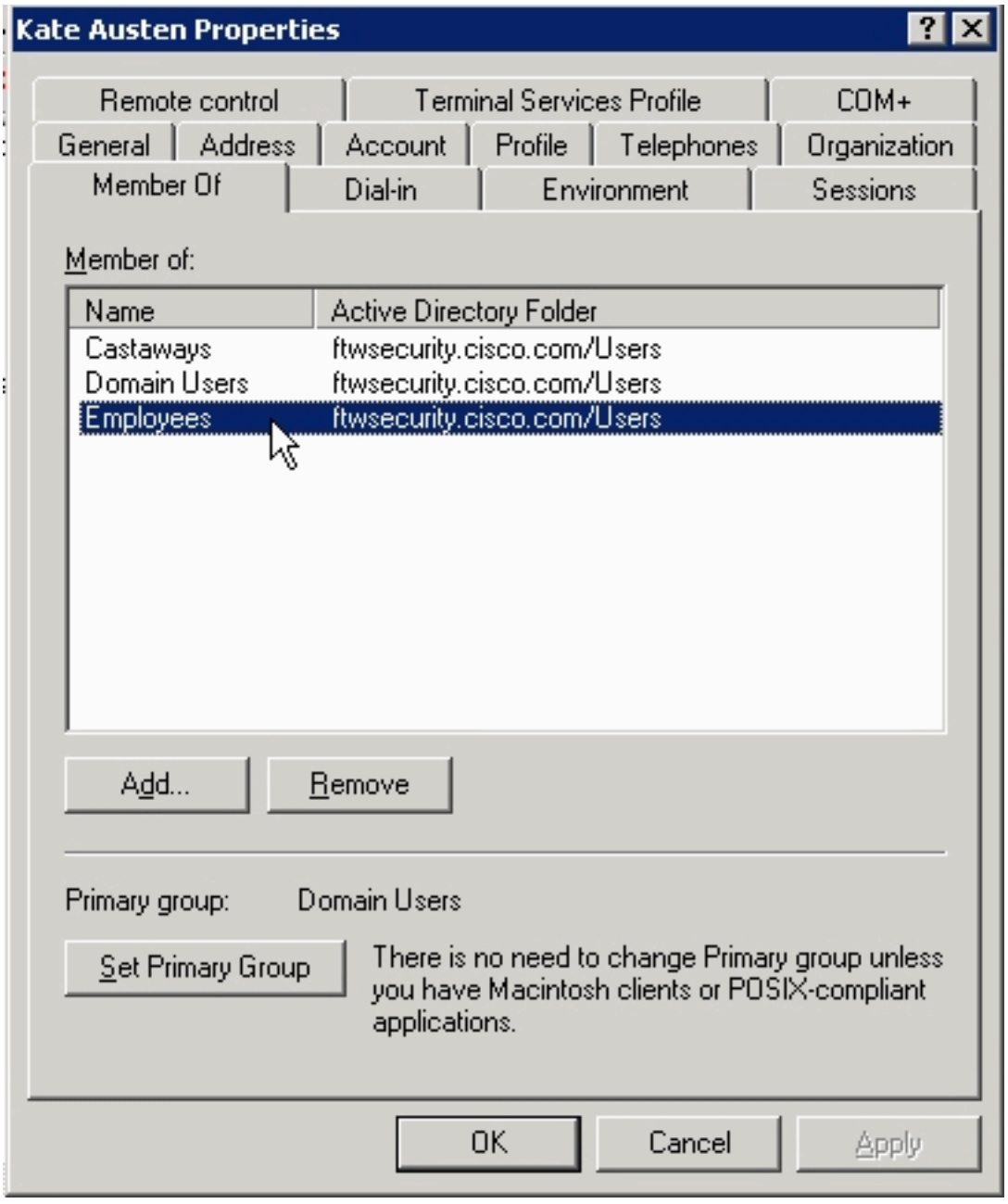
```
group-policy NOACCESS internal
group-policy NOACCESS attributes
 vpn-simultaneous-logins 0
 vpn-tunnel-protocol IPSec webvpn
```

您需要运用此组策略作为默认组策略对隧道群。因此从LDAP属性地图获得映射的用户，例如属于一希望的LDAP组的那些人，能获得没获得任何映射的他们的希望的组策略和用户，例如不属于任何希望的LDAP的那些人分组，能从隧道群获得NOACCESS组政策，阻止他们的访问。

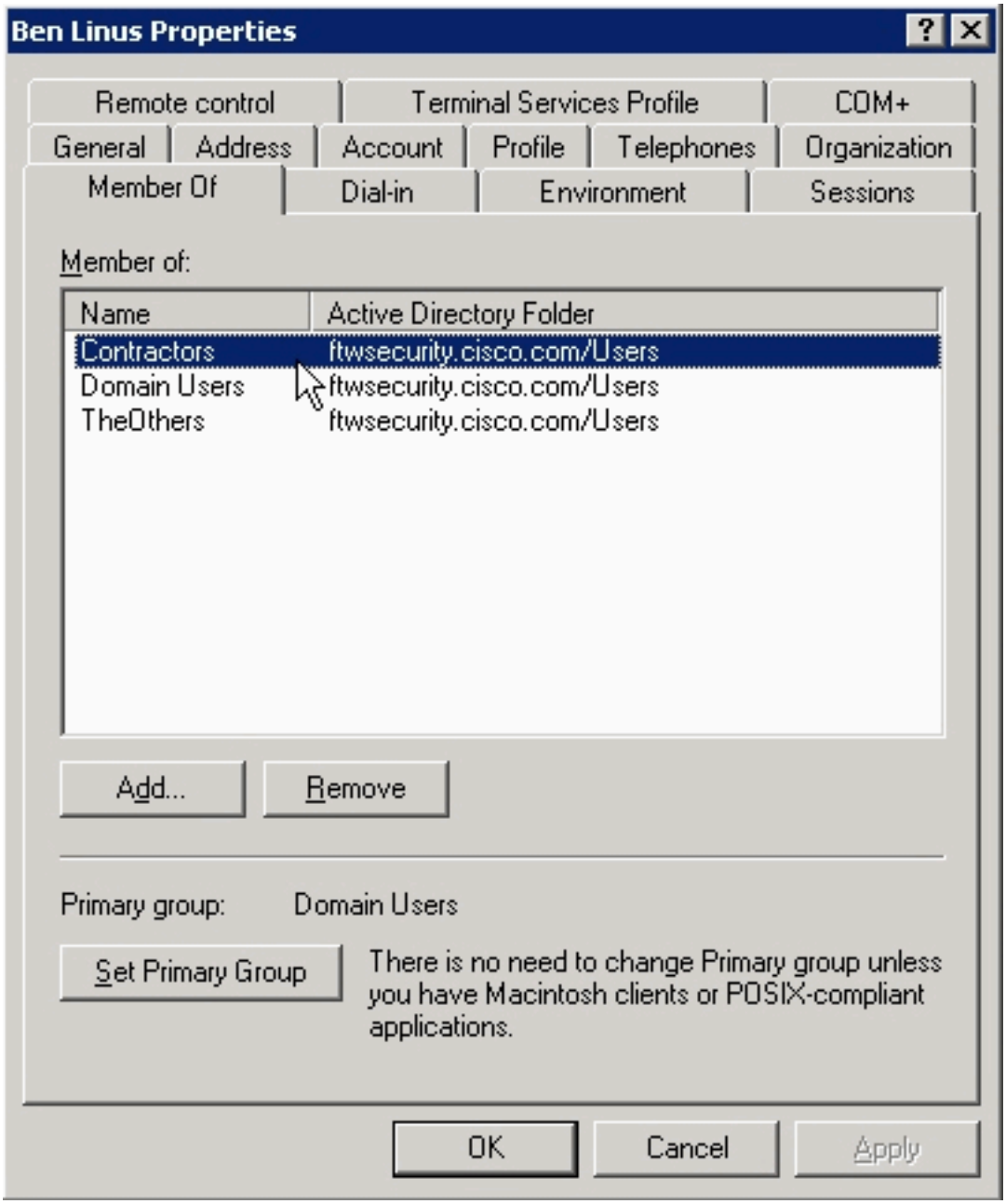
> **注意**：请参阅 ASA/PIX：映射VPN客户端对VPN组策略通过拒绝对一些用户的访问的IDAP配置示例关于如何创建不同的LDAP属性映射的更多信息。

配置 Active Directory 或其他 LDAP 服务器

Active Directory 或其他 LDAP 服务器上唯一需要的配置与用户的属性相关。在本例中，用户凯特·奥斯顿是雇员组的成员AD的：



Ben Linus 是 Contractors 组的成员：

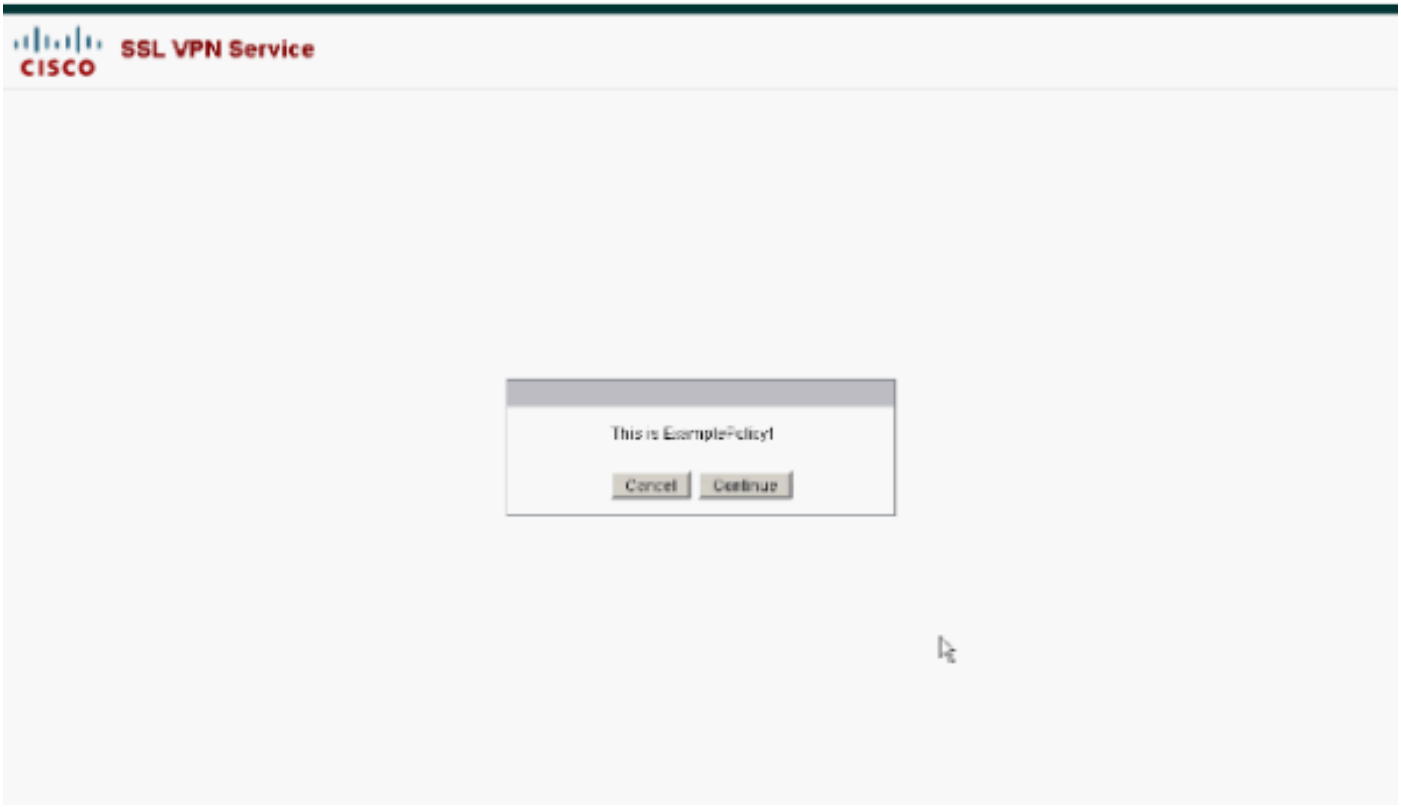


验证

使用此部分以验证配置。

洛金

为了验证配置是否成功，请以一个应已使用 LDAP 属性映射分配了组策略的用户身份登录。在本示例中，已为每个组策略配置了标语。由于 kate 是 Employees 组的成员，因此屏幕截图显示用户 **kate** 已成功登录并应用了 **ExamplePolicy1**。



调试 LDAP 事务

为了验证 LDAP 映射是否已经发生，或者为了获取 LDAP 服务器所发送属性的详细信息，可在 ASA 命令行上发出 **debug ldap 255** 命令，然后尝试进行身份验证。

在此调试中，为用户 **kate** 分配了组策略 **ExamplePolicy1**，因为她是 **Employees** 组的成员。此调试还显示 **kate** 是 **Castaways** 组的成员，但该属性尚未进行映射，因此被忽略。

```
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

在此调试中，为用户 ben 分配了 ExamplePolicy2 组策略，因为他是 Contractors 组的成员。此调试还显示 ben 是 TheOthers 组的成员，但该属性尚未进行映射，因此被忽略。

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

故障排除

使用本部分可排除配置的故障。

属性名称和值区分大小写

属性名称和值区分大小写。如果映射未能正确进行，请确保 LDAP 属性映射中 Cisco 和 LDAP 的属性名称和值*均*使用了正确的拼写和大小写。

ASA不能验证从LDAP服务器的用户

ASA不能验证从LDAP服务器的用户。这是调试：

```
ldap 255 output:[1555805]Start[1555805]0xcd66c028 reqType = 1[1555805]started[1555805]
uri=ldaps://172.30.74.70:636[1555805]LDAPLDAPldaps://172.30.74.70:636= Successful[1555805]
supportedLDAPVersion value= 3[1555805] supportedLDAPVersion administrator[1555805] 2[1555805]
value=sysservices172.30.74.70[1555805] sysservices (49)credentials[1555805](-1)LDAP
server[1555805]Tx=222Rx=605 status=-2[1555805]
```

关于调试，或者LDAP洛金DN格式不正确或密码不正确，因此请验证两个为了解决问题。