PIX/ASA 8.0： LDAP 認証を使用したログイン時のグループ ポリシーの割り当て

目次

概要

この資料にログオンでグループ ポリシーを割り当てるために Lightweight Directory Access Protocol （ LDAP ） 認証を使用する方法を記述されています。 通常、管理者は、VPN ユーザにさまざまなアクセス権限または WebVPN コンテンツを提供します。 で適応型セキュリティ アプライアンス (ASA) ソフトウェア (ASA) これは異なるユーザーへの異なるグループ ポリシーの割り当てによって規則的に実現します。 LDAP 認証が使用されていると、LDAP 属性マップを使用して自動的に実行できます。

LDAP を使用してグループ ポリシーをユーザに割り当てる場合、Active Directory (AD) 属性 **memberOf** などの LDAP 属性を ASA で認識される **IETF-Radius-Class** 属性にマッピングするマップを設定する必要があります。 属性マッピングが確立されたら、LDAP サーバで設定された属性値を ASA のグループ ポリシーの名前にマッピングする必要があります。

> **注: memberOf** 属性は、ユーザが Active Directory の一部であるグループに対応します。 ユーザは、Active Directory の複数のグループのメンバになることができます。 この場合、複数の **memberOf** 属性がサーバにより送信されますが、ASA は 1 グループ ポリシーに対して 1 属性だけをマッチングできます。

前提条件

要件

このドキュメントの内容は、作業 LDAP 認証セットアップがすでに ASA に設定されていることを必要とします。 ASA で基本 LDAP 認証設定をセットアップする方法については、『Configure LDAP Authentication for WebVPN Users』を参照してください。

使用するコンポーネント

このドキュメントの情報は、PIX/ASA 8.0 に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

この例では、AD/LDAP 属性 **memberOf** は、ASA 属性 **CVPN3000-Radius-IETF-Class** にマッピングされます。 クラス属性は、ASA でのグループ ポリシーの割り当てに使用されます。 これは、LDAP でユーザを認証するときに ASA が完了する通常のプロセスです。

1. ユーザが ASA への接続を開始します。
2. ASA は Microsoft AD/LDAP サーバを使用してユーザを認証するように設定されています。
3. ASA は、ASA 上で設定されたクレデンシャル（この場合は admin）を使用して LDAP サーバにバインドし、指定されたユーザ名を検索します。
4. そのユーザ名が見つかった場合、ASA はユーザがログイン時に指定したクレデンシャルを使用して LDAP サーバへのバインドを試みます。
5. 2 回目のバインドに成功すると、ASA は **memberOf** などのユーザ属性を取得します。
6. 設定済みの LDAP 属性マップによって、**memberOf** 属性が **CVPN3000-Radius-IETF-Class** にマッピングされます。**Employees** グループのメンバシップを示す値が、**ExamplePolicy1** にマッピングされます。**Contractors** グループのメンバシップを示す値が、**ExamplePolicy2** にマッピングされます。
7. 新しく割り当てられた **CVPN3000-Radius-IETF-Class** 属性が検査され、グループ ポリシーが決定されます。値が ExamplePolicy1 の場合、ユーザには ExamplePolicy1 グループ ポリシーが割り当てられます。値が ExamplePolicy2 の場合、ユーザには ExamplePolicy2 グループ ポリシーが割り当てられます。

設定

ASA の設定

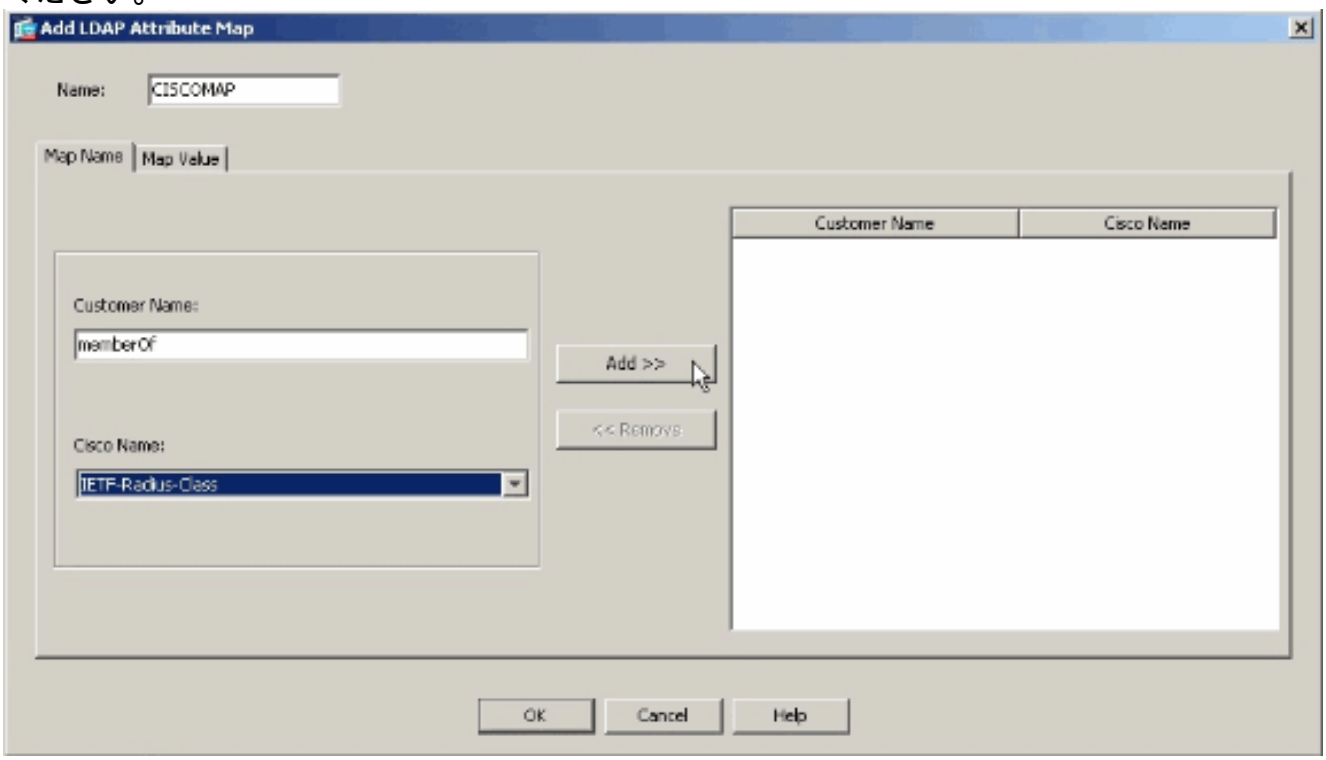
このセクションでは、ASA を設定して、LDAP 属性に基づいてユーザにグループ ポリシーを割り当てる方法について説明します。

ASDM

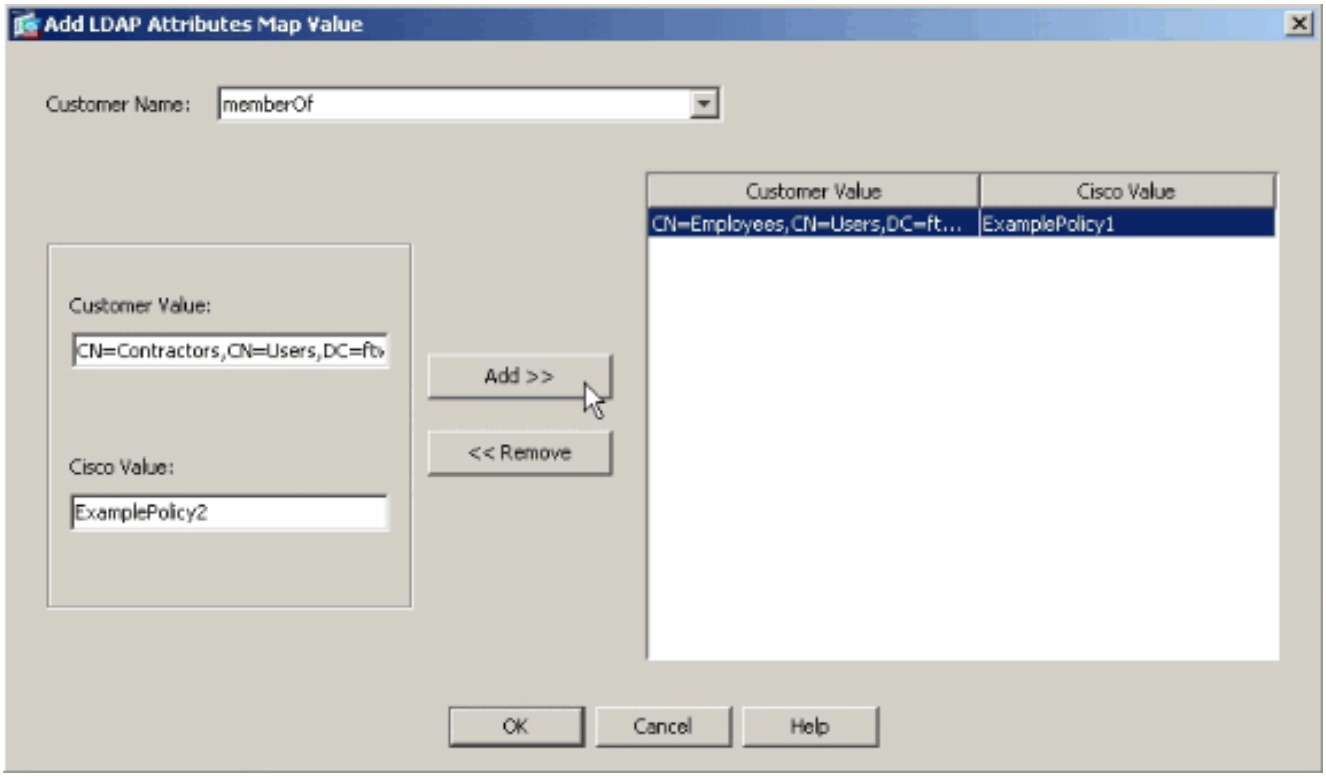
ASA で LDAP マップを設定するには、Adaptive Security Device Manager（ASDM）で次の手順

を実行します。

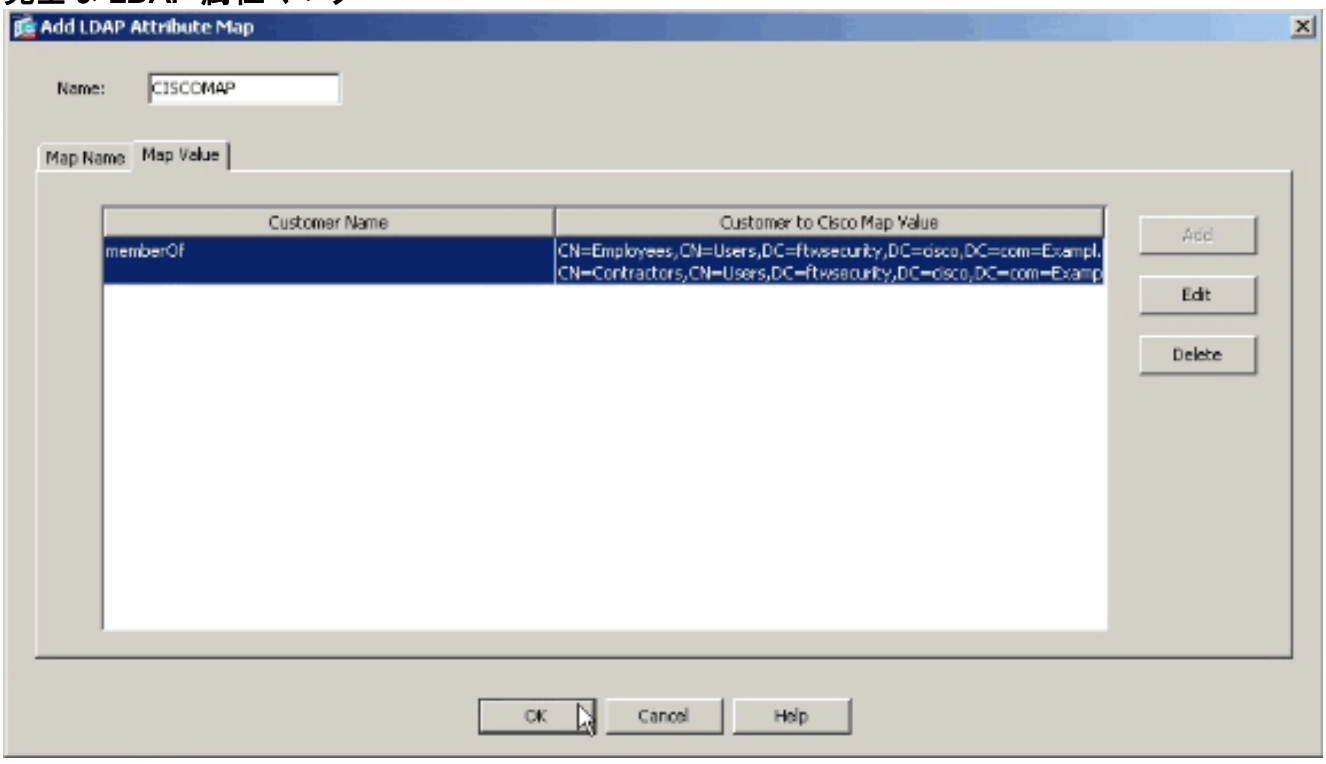
1. [Navigate to Configuration] > [Remote Access VPN] > [AAA Setup] > [LDAP Attribute Map] の順に移動します。
2. [Add] をクリックします。
3. マップに名前を付けます。
4. ASA での LDAP 属性と **IETF-Radius-Class** 属性間のマッピングを作成します。 この例では、**Customer Name** は、Active Directory の **memberOf** 属性です。 これは、**IETF-Radius-Class** の **Cisco Name** にマッピングされます。 [Add] をクリックします。**注:** 属性名および値では大文字と小文字が区別されます。**注:** LDAP サーバにより提供される属性名またはスペルが正確にわからない場合、マップを作成する前にデバッグを検査することを推奨します。デバッグで LDAP 属性を識別する方法の詳細については、「Verify」セクションを参照してください。



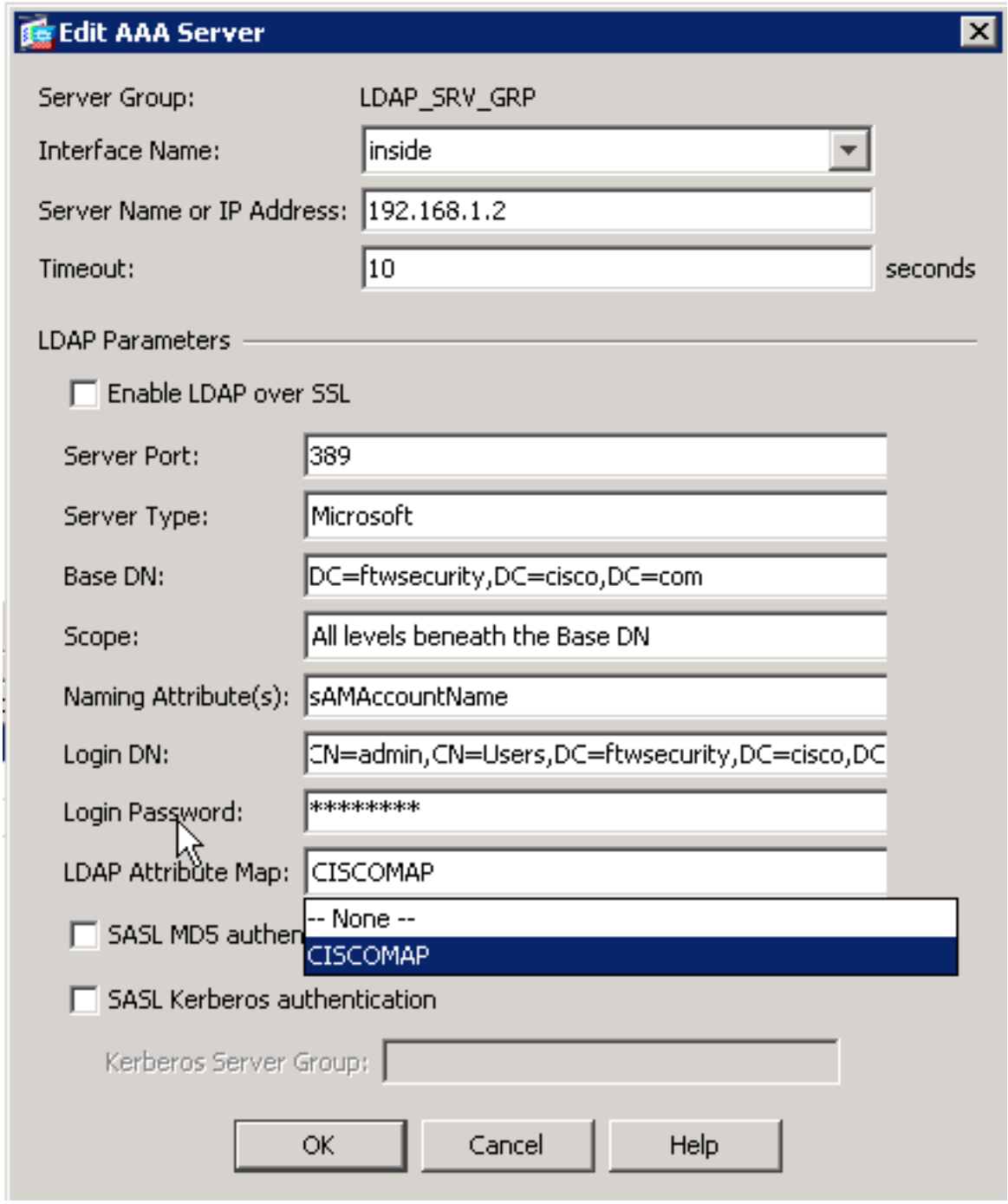
5. 属性マッピングを追加したら、[Map Value] タブをクリックし、[Add] をクリックして、値マッピングを作成します。 必要なだけ値マッピングを追加して、終了したら [OK] をクリックします。**顧客 値-** LDAPサーバからの属性値**Cisco 値-** ASA のグループ ポリシーの名前この例では、**CN=Employees,CN=Users,DC=ftwsecurity,DC=cisco,DC=com** memberOf 値は **ExamplePolicy1** にマッピングされ、**CN=Contractors,CN=Users,DC=ftwsecurity,DC=cisco,DC=com** memberOf 値は **ExamplePolicy2** にマッピングされます。



完全な LDAP 属性マップ



6. マップを作成すれば、LDAP認証のために設定される認証、許可、アカウンティング（AAA）サーバに割り当てる必要があります。 左ペインから [AAA Server Groups] を選択します。
7. LDAP に設定されている AAA サーバを選択して、[Edit] をクリックします。
8. 表示されるウィンドウの下側の [LDAP Attribute Map] ドロップダウン リストを確認します。作成したリストを選択します。 完了したら、[OK] をクリックします。



CLI

ASA の LDAP マップを設定するために CLI のこれらのステップを完了して下さい。

```
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
```

NOACCESS グループ ポリシーの設定

NOACCESS グループ ポリシーを作成して、LDAP グループのメンバでないユーザの VPN 接続を拒否できます。 次に、この設定の一部を例として示します。

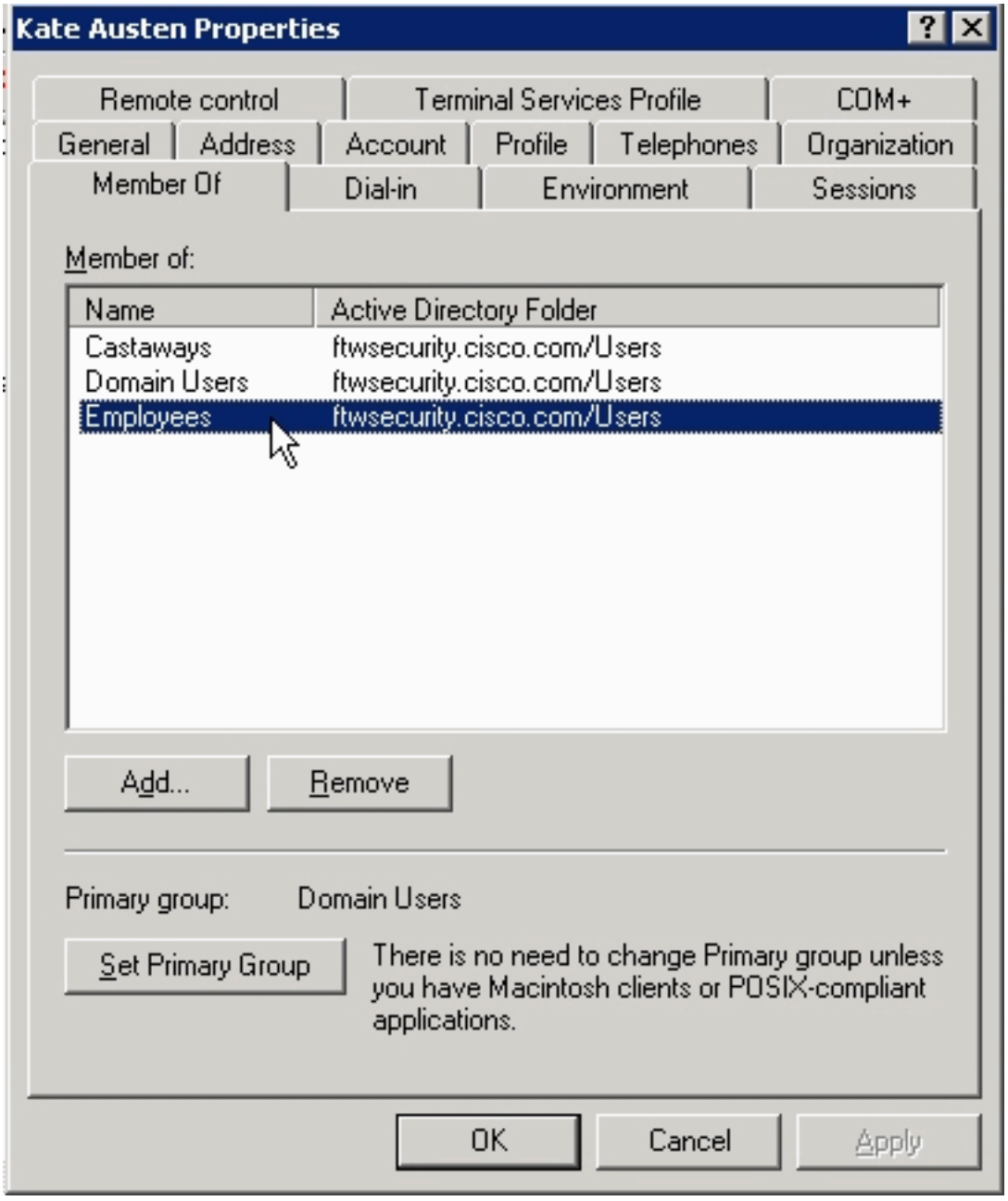
```
group-policy NOACCESS internal
group-policy NOACCESS attributes
 vpn-simultaneous-logins 0
 vpn-tunnel-protocol IPSec webvpn
```

このグループ ポリシーをデフォルト グループ ポリシーとしてトンネル グループに適用する必要があります。 たとえば、目的の LDAP グループに属するユーザなど、LDAP 属性マップからマッピングを取得するユーザは、目的のグループ ポリシーを取得できます。また、たとえば、目的の LDAP グループに属さないユーザなど、マッピングを取得しないユーザは、NOACCESS グループ ポリシーをトンネル グループから取得できます（これにより、これらのユーザのアクセスがブロックされます）。

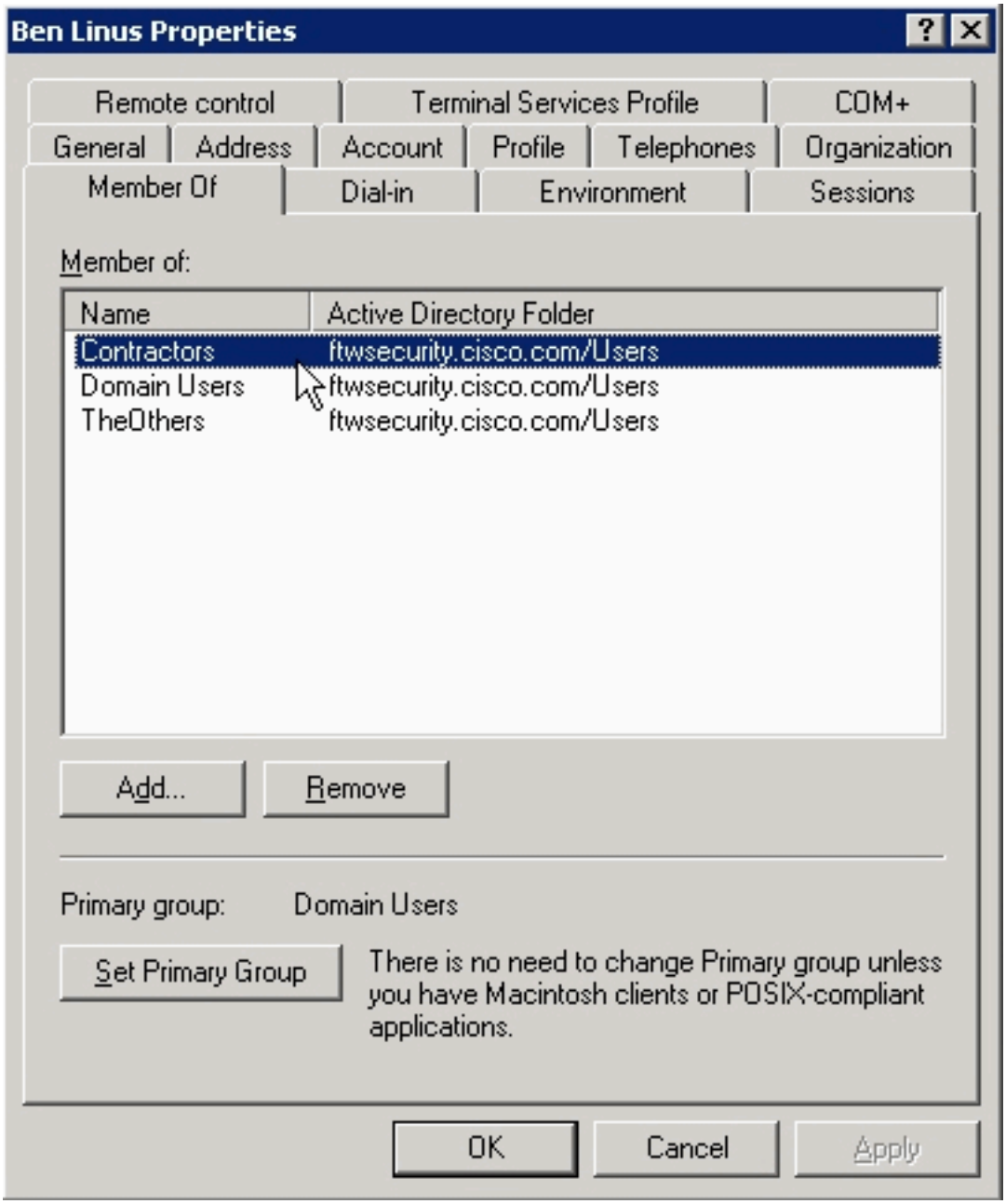
> **注:** 『ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example』を参照して、一部のユーザへのアクセスを拒否するさまざまな LDAP 属性マッピングを作成する方法の詳細を確認してください。

Active Directory または他の LDAP サーバの設定

Active Directory またはその他の LDAP サーバで必要な設定だけが、ユーザの属性に関連します。この例では、Kate Austen ユーザは AD の従業員グループのメンバーです:



Ben Linus は、Contractors グループのメンバです。

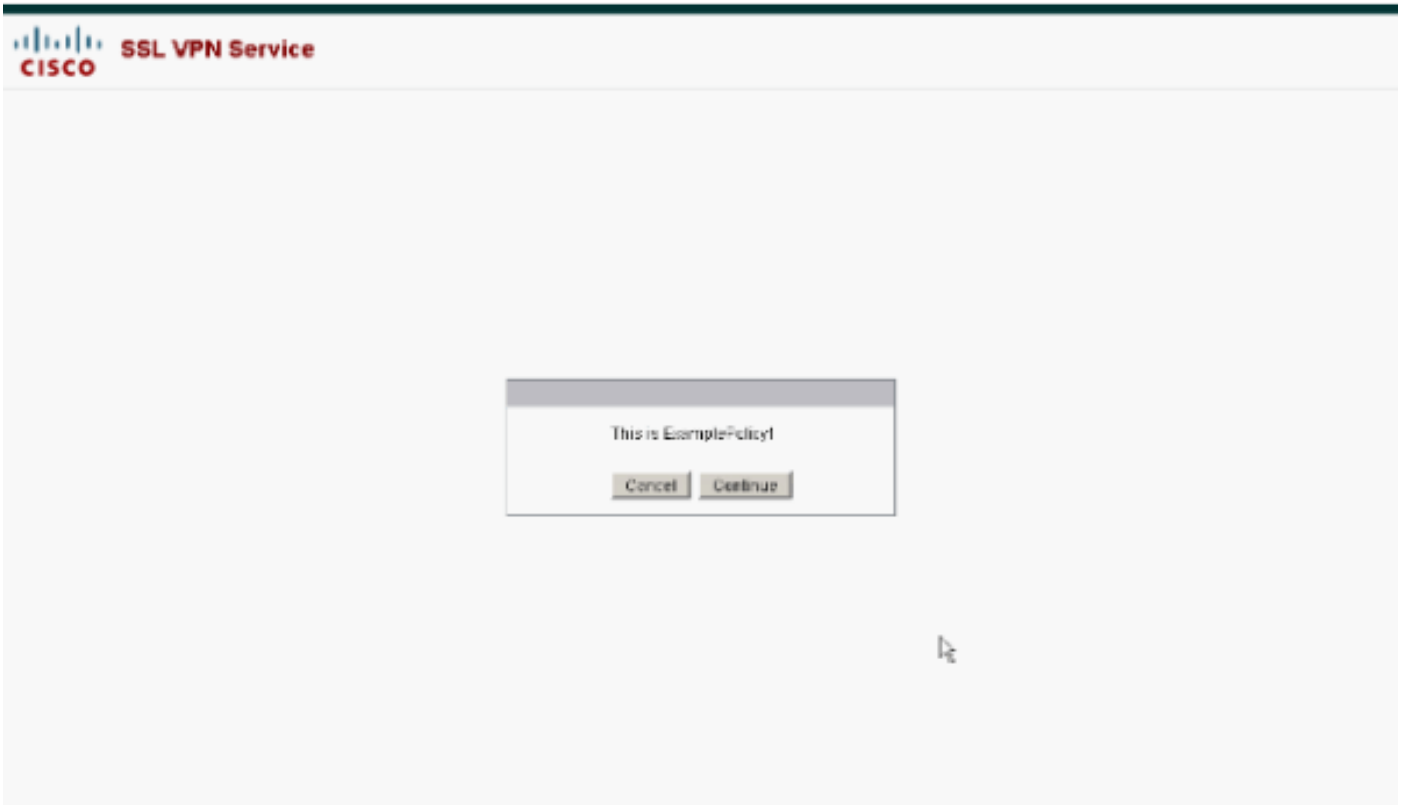


確認

このセクションでは、設定の確認について説明します。

ログイン

設定が正しいことを確認するには、LDAP 属性マップがグループ ポリシーに割り当てられているユーザとしてログインします。 この例では、各グループ ポリシーについてのバナーが設定されています。 このスクリーンショットは、ユーザ **kate** がログインに成功し、Employees グループのメンバであるため、**ExamplePolicy1** が適用されることを示します。



LDAP トランザクションのデバッグ

LDAP マッピングが発生するか確認するには、または LDAP サーバにより送信される属性の詳細を取得するには、ASA コマンド ラインで **debug ldap 255** コマンドを実行して、認証します。

このデバッグでは、ユーザ **kate** は、**Employees** グループのメンバであるため、グループ ポリシー **ExamplePolicy1** が割り当てられます。 このデバッグでは、**kate** が **Castaways** グループのメンバであるが、属性がマッピングされないため無視されます。

```
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

このデバッグでは、ユーザ ben が Contractors グループのメンバであるため、ExamplePolicy2 グループ ポリシーが割り当てられます。 このデバッグでは、ben が TheOthers グループのメンバであるが、属性がマッピングされないため無視されます。

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

トラブルシューティング

このセクションでは、設定のトラブルシューティングについて説明します。

属性名および値では大文字と小文字が区別される

属性名および値では大文字と小文字が区別されます。 マッピングが正しく発生しない場合、Cisco および LDAP 属性の名前と値の両方で、LDAP 属性マップのスペルと大文字小文字が正しいことを確認します。

ASA は LDAPサーバからのユーザを認証できません

ASA は LDAPサーバからのユーザを認証できません。 デバッグはここにあります:

```
LDAP 255 output:[1555805]  Start[1555805] New   0xcd66c028LDAP
uri=ldaps://172.30.74.70:636[1555805]  LDAP  reqType = 1[1555805]  started[1555805]:
ldaps://172.30.74.70:636 = Successful[1555805] supportedLDAPVersion:  = 3[1555805]
supportedLDAPVersion:  = sysservices  172.30.74.70[1555805]  sysservices  administrator[1555805]
 2[1555805] 49  credentials[1555805]   status=-2[1555805]  -1 LDAP server[1555805]  Tx=222
Rx=605
```

デバッグでは、LDAP ログイン DN 形式が間違っているか、パスワードが間違っているので、これらを検証して問題を解決します。