PIX/ASA 8.0: Использование проверки подлинности с помощью LDAP для назначения групповой политики при входе в систему

Содержание

Введение

Этот документ описывает, как использовать Аутентификация Протокола LDAP для присвоения групповой политики при входе в систему . Часто у администраторов возникает необходимость предоставить пользователям сети VPN различные разрешения на доступ или различное содержание WebVPN. На Устройстве адаптивной защиты (ASA) это регулярно достигается через присвоение политики другой группы другим пользователям. В случае использования аутентификации посредством LDAP это может быть выполнено автоматически путем привязки атрибутов LDAP.

Чтобы посредством LDAP назначить групповую политику пользователю, необходимо настроить карту, которая будет привязывать атрибут LDAP, например атрибут memberOf Active Directory (AD) к атрибуту IETF-Radius-Class, воспринимаемому устройством ASA. После установления карты атрибутов необходимо привязать значение атрибута, настроенное на сервере LDAP, к имени групповой политики в устройстве ASA.

> **Примечание:** Атрибут **memberOf** соответствует группе, что пользователь является частью в Active Directory. Пользователь может быть членом сразу нескольких групп в Active Directory. В этом случае сервер отправляет несколько атрибутов memberOf, но

устройство ASA может связать с одной политикой группы только один атрибут.

Предварительные условия

Требования

Этот документ предполагает, что на устройстве ASA уже настроена аутентификация LDAP. Настройка аутентификации LDAP в устройстве ASA на базовом уровне описана в документе Настройка аутентификации LDAP для пользователей WebVPN.

Используемые компоненты

Сведения в этом документе основываются на PIX/ASA 8.0.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

В данном примере атрибут memberOf AD/LDAP связывается с атрибутом ASA CVPN3000-Radius-IETF-Class. Для назначения групповых политик на устройстве ASA используется атрибут класса. При аутентификации пользователей посредством LDAP устройство ASA выполняет следующий общий процесс:

1. Пользователь инициирует подключение к устройству ASA.
2. Устройство ASA настроено на аутентификацию пользователя посредством сервера Microsoft AD/LDAP.
3. ASA связывается с сервером LDAP с учетными данными (в данном случае admin), настроенными на ASA, и ищет предоставленное имя пользователя.
4. Если имя пользователя найдено, ASA предпринимает попытку связаться с сервером LDAP с использованием указанных пользователем учетных данных при входе.
5. **При успешном выполнении второй привязки ASA обрабатывает атрибуты пользователей, включая memberOf.**
6. **Атрибут memberOf сопоставляется с CVPN3000-Radius-IETF-Class при помощи настроенной карты атрибутов LDAP.Значение, указывающее членство в группе Employees, назначается на ExamplePolicy1.Значение, указывающее членство в группе Contractors, назначается на ExamplePolicy2.**
7. **Проверяется вновь назначенный атрибут CVPN3000-Radius-IETF-Class, и выполняется определение групповой политики.**Значение ExamplePolicy1 приводит к назначению пользователю групповой политики ExamplePolicy1.Значение ExamplePolicy2 приводит к назначению пользователю групповой политики ExamplePolicy2.

Настройка

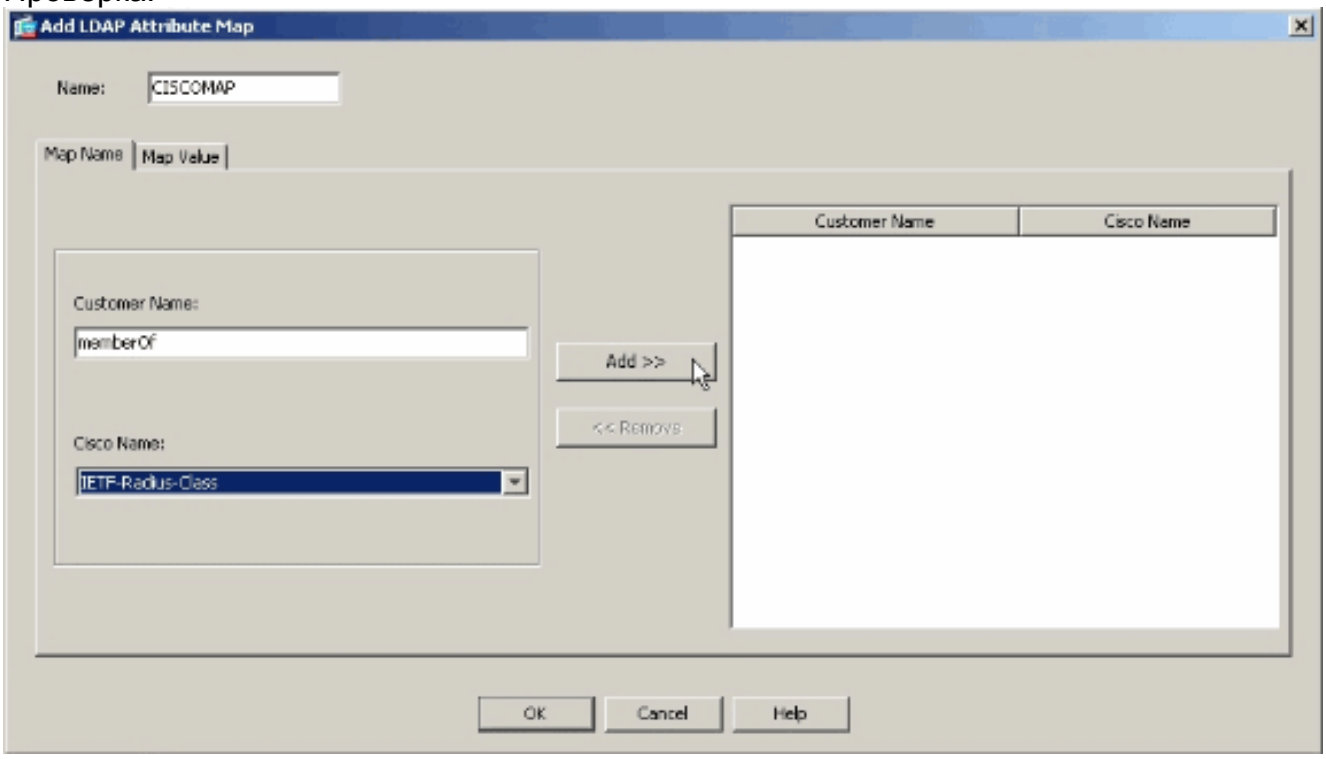
Настройка устройства ASA

В этом разделе приведены сведения, необходимые для настройки устройства ASA с назначением пользователям групповой политики в зависимости от их атрибутов LDAP.

ASDM

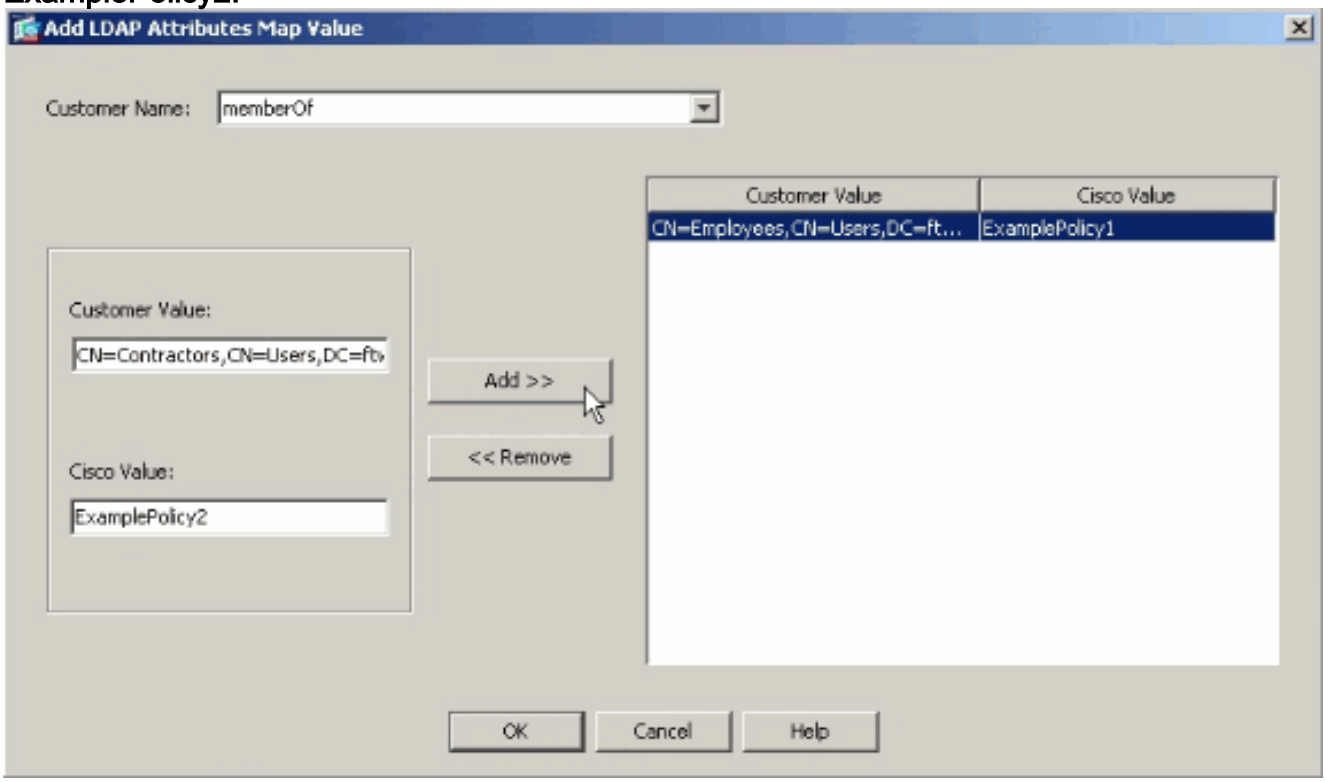
Для настройки карты LDAP на ASA выполните следующие шаги в Диспетчере устройств адаптивной защиты (ASDM).

1. **Перейдите в раздел Configuration > Remote Access VPN > AAA Setup > LDAP Attribute Map (Настройка > VPN для удаленного доступа > Настройка AAA > Карта атрибутов LDAP).**
2. **Нажмите Add.**
3. Введите название карты.
4. **Создайте назначение между атрибутом LDAP и атрибутом IETF-Radius-Class в устройстве ASA. В данном примере Customer Name – это атрибут memberOf в Active Directory. Ему соответствует значение Cisco Name как атрибут IETF-Radius-Class. Нажмите Add.Примечание:** Имена и значения атрибутов воспринимаются с учетом регистра.**Примечание:** Если вы не знаете точные названия атрибута или написания, которые предоставлены Сервером LDAP, может быть полезно исследовать отладки перед созданием карты. Порядок определения атрибутов LDAP по данным отладочных сообщений описан в разделе
Проверка.

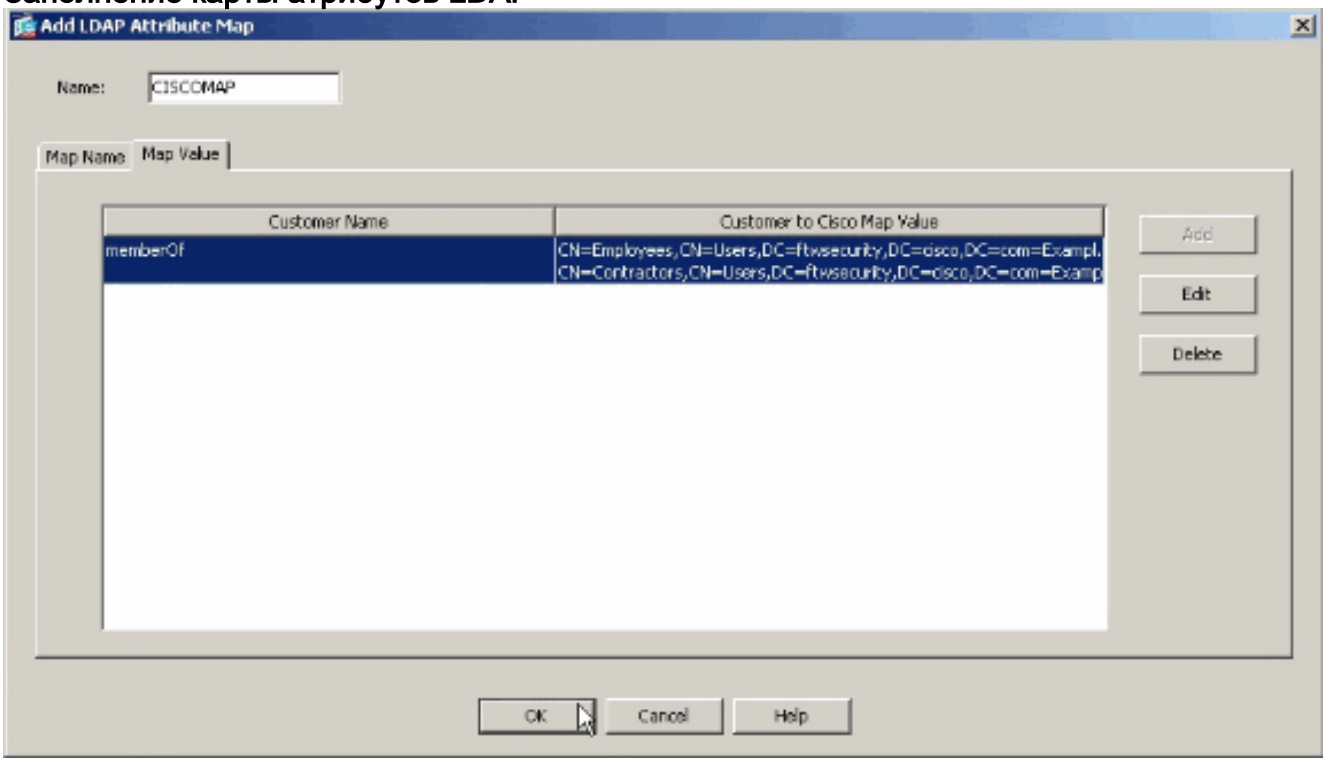


5. **После добавления карты атрибутов щелкните мышью вкладку Map Value (Привязать значение) и нажмите Add (Добавить), чтобы создать карту для привязки значений. При необходимости добавьте дополнительные привязки и по окончании нажмите OK. Customer Value (Значение заказчика) – значение атрибута от сервера LDAP Cisco Value (Значение Cisco) – имя групповой политики в устройстве ASAB данном примере значение memberOf CN=Employees,CN=Users,DC=ftwsecurity,DC=cisco,DC=com**

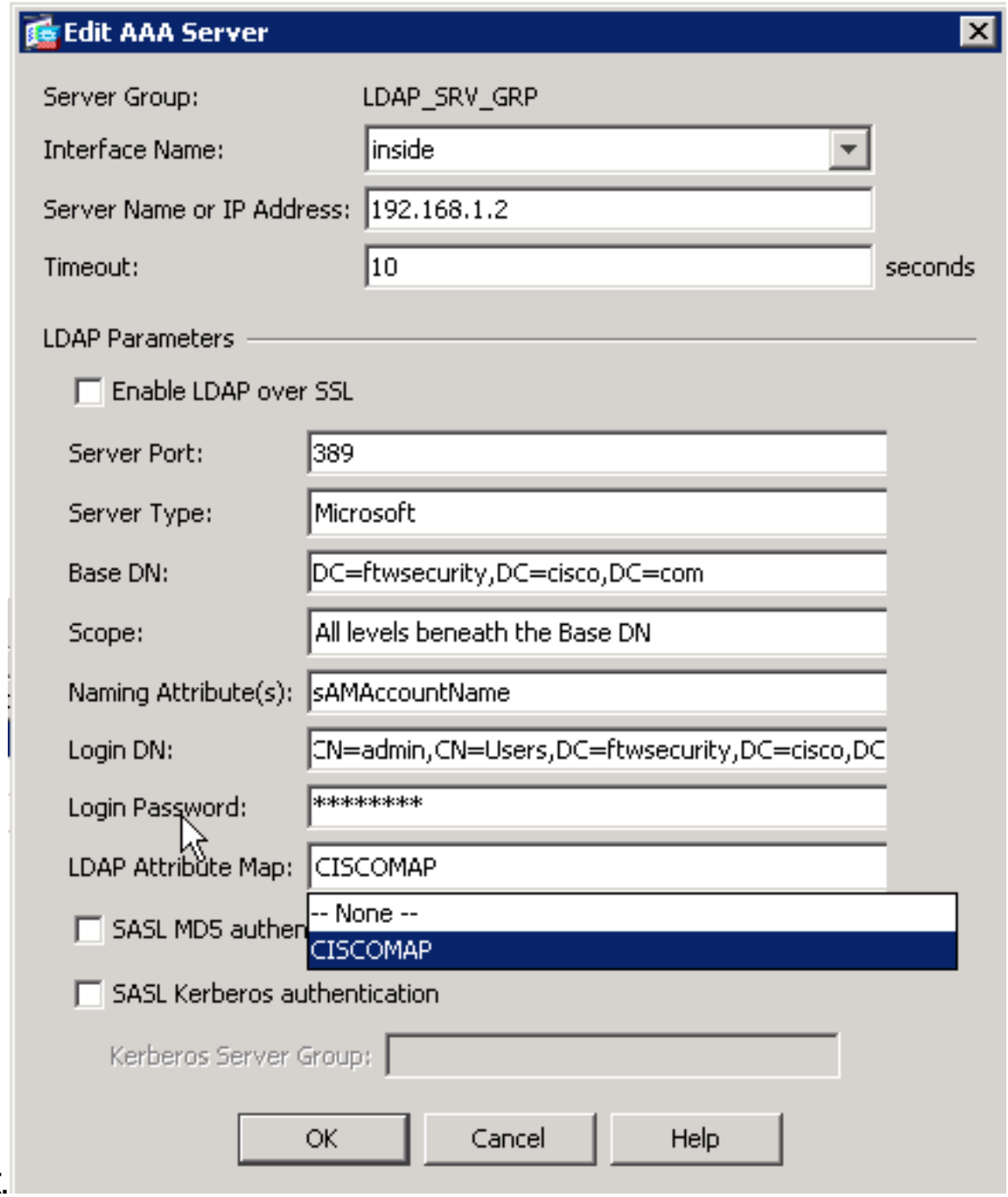
привязывается к политике ExamplePolicy1, а значение memberOf CN=Contractors,CN=Users,DC=ftwsecurity,DC=cisco,DC=com – к политике ExamplePolicy2.



Заполнение карты атрибутов LDAP



6. Как только вы создаете карту, это должно быть назначенный на аутентификацию, авторизацию и учет (AAA) , которая настроена для проверки подлинности LDAP. **В левой экранной области выберите AAA Server Groups (Группы серверов AAA).**
7. **Выберите сервер AAA, настроенный для протокола LDAP, и нажмите кнопку Edit (Изменить).**
8. **Перейдите к раскрывающемуся списку LDAP Attribute Map (Карта атрибутов LDAP) в левой нижней части окна.** Выберите список, который только что был создан. **По окончании нажмите**



OK.

CLI

Выполните эти шаги в CLI для настройки карты LDAP на 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
```

Настройте групповую политику NOACCESS

Когда пользователь не является частью ни одной из групп LDAP, можно создать групповую политику NOACCESS для запрета VPN-подключения. Этот фрагмент конфигурации

показывают для вашей ссылки:

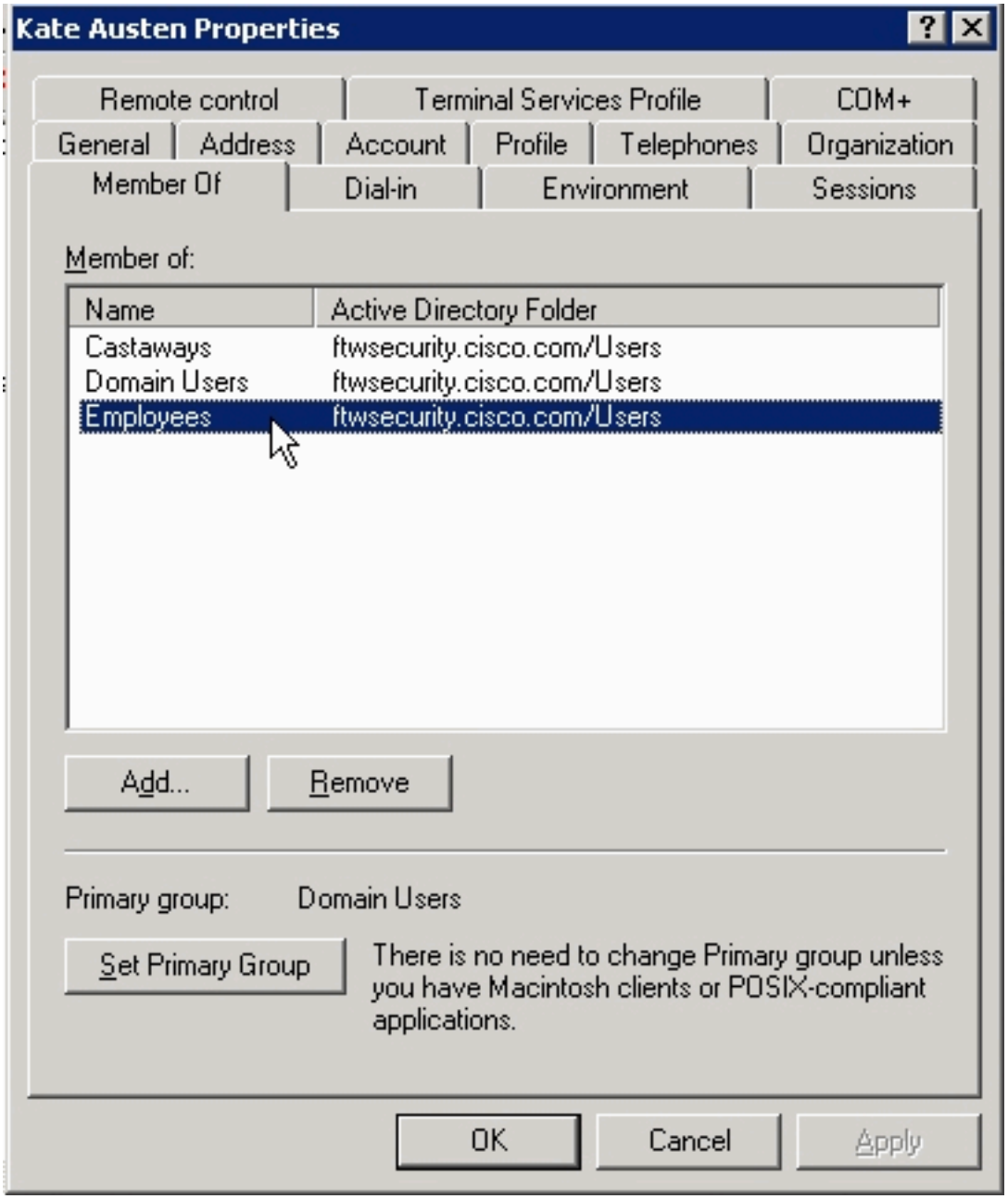
```
group-policy NOACCESS internal
group-policy NOACCESS attributes
 vpn-simultaneous-logins 0
 vpn-tunnel-protocol IPSec webvpn
```

Необходимо применить эту групповую политику как политику группы по умолчанию к туннельной группе. Так, чтобы пользователи, которые получают сопоставление от Карты атрибутов LDAP, например те, кто принадлежит желаемой группе LDAP, были в состоянии получить их желаемые групповые политики и пользователей, которые не получают сопоставления, например те, кто не принадлежит ни одной из желаемых групп LDAP, в состоянии получить групповую политику NOACCESS от туннельной группы, которая блокирует доступ для них.

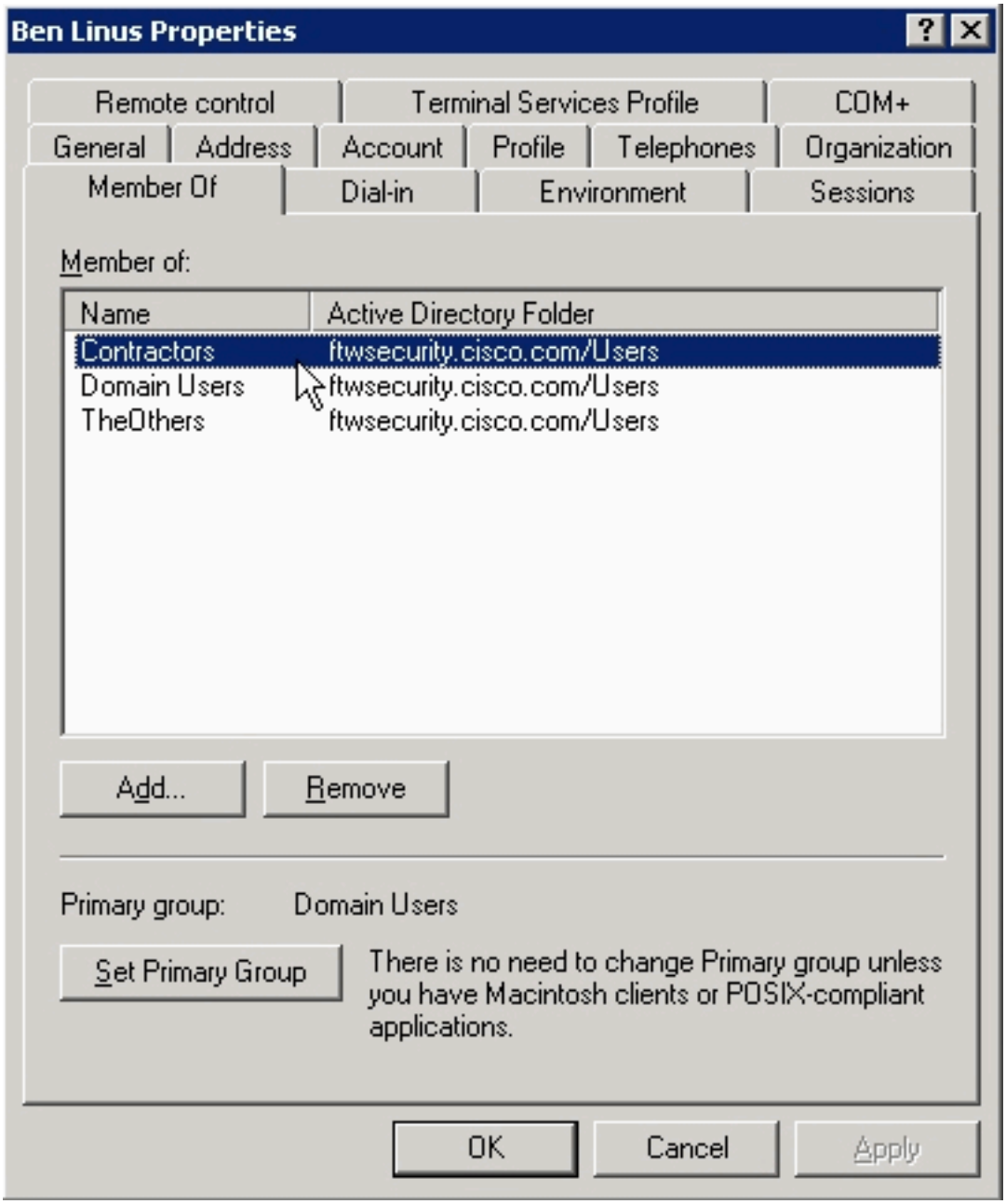
> **Примечание:** В документе ASA/PIX: Сопоставление Клиентов VPN к Политике Группы VPN Через Пример Конфигурации LDAP для получения дополнительной информации о том, как создать другой LDAP, приписывает сопоставления, который запрещает доступ некоторым пользователям.

Настройка Active Directory и других серверов LDAP

Настройка, которую требуется выполнит на сервере Active Directory или другом сервере LDAP, касается только атрибутов пользователя. В данном примере пользователь Кейт Остин является участником группы Сотрудников в AD:



Ben Linus – член группы Contractors:

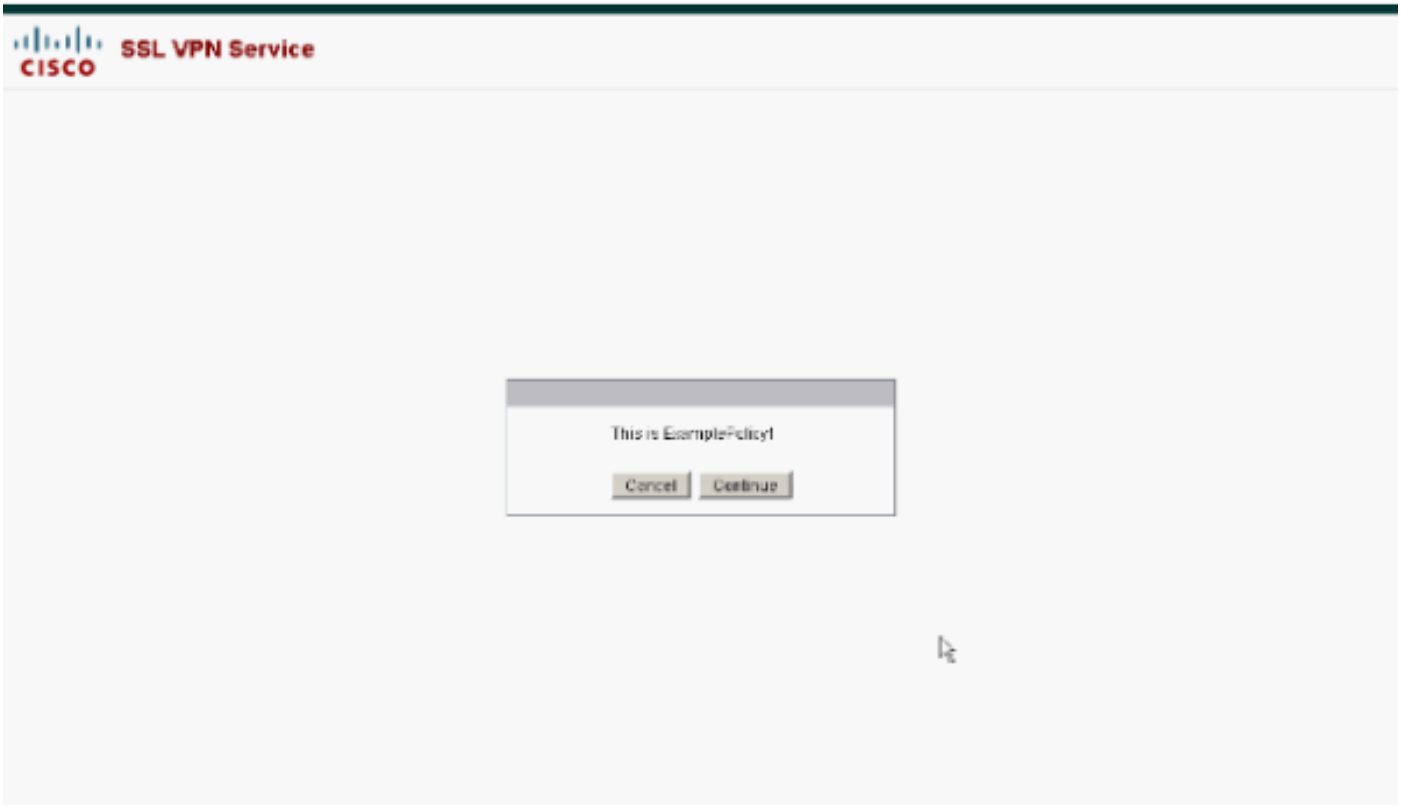


Проверка

В этом разделе приведены указания по проверке конфигурации.

Вход в систему

Для проверки работоспособности конфигурации войдите в систему как пользователь, которому предположительно назначена групповая политика с картой атрибута LDAP. В этом примере для каждой групповой политики настроено объявление. **На снимке экрана видно, что пользователю kate после успешного входа в систему назначена политика ExamplePolicy1 по причине членства в группе Employees.**



Отладка транзакции LDAP

Чтобы проверить выполнение назначения LDAP или получить подробную информацию об атрибутах, отправляемых сервером LDAP, введите команду debug ldap 255 в командной строке ASA и затем попробуйте выполнить аутентификацию.

В этом фрагменте отладочных данных пользователю kate назначается групповая политика ExamplePolicy1 по причине членства в группе Employees. Отладочные данные также показывают, что kate является членом группы Castaways, но соответствующий атрибут не назначен, поэтому членство в этой группе игнорируется.

```
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

В этом фрагменте отладочных данных пользователю ben назначается групповая политика ExamplePolicy2 по причине членства в группе Contractors. Отладочные данные также показывают, что ben является членом группы TheOthers, но соответствующий атрибут не назначен, поэтому членство в этой группе игнорируется.

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

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Имена и значения атрибутов воспринимаются с учетом регистра

Имена и значения атрибутов воспринимаются с учетом регистра. ***Если назначение не выполняется требуемым образом, убедитесь в том, что в карте привязок MAP нет опечаток и правильно выбран регистр букв для имен и значений атрибутов Cisco и LDAP.***

ASA не в состоянии Аутентифицировать Пользователей от Сервера LDAP

ASA не в состоянии аутентифицировать пользователей от Сервера LDAP. Вот отладки:

```
ldap 255 output:[1555805] Session Start[1555805] New request Session, context 0xcd66c028,
reqType = 1[1555805] Fiber started[1555805] Creating LDAP context with
uri=ldaps://172.30.74.70:636[1555805] Connect to LDAP server: ldaps://172.30.74.70:636, status =
Successful[1555805] supportedLDAPVersion: value = 3[1555805] supportedLDAPVersion: value =
2[1555805] Binding as administrator[1555805] Performing Simple authentication for sysservices to
172.30.74.70[1555805] Simple authentication for sysservices returned code (49) Invalid
credentials[1555805] Failed to bind as administrator returned code (-1) Can't contact LDAP
server[1555805] Fiber exit Tx=222 bytes Rx=605 bytes, status=-2[1555805] Session End
```

Что касается отладок, или формат DN Входа в систему LDAP является неправильным или пароль, является неправильным, так проверьте обоих для решения вопроса.