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

ASDM

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

Перейдите в раздел Configuration > Remote Access VPN > AAA Setup > LDAP Attribute Map (Настройка > VPN для удаленного доступа > Настройка AAA > Карта атрибутов LDAP).

Щелкните **Add**.

Введите название карты.

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**. Щелкните **Add**.

Примечание. Имена и значения атрибутов воспринимаются с учетом регистра.

Примечание. Если у предоставляемых сервером LDAP атрибутов неизвестны имена или их точное написание, то перед созданием карты полезно проанализировать отладочные сообщения. Порядок определения атрибутов LDAP по данным отладочных сообщений описан в разделе Проверка.

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 ASA.

В 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

После создания карты необходимо назначить ее серверу AAA, настроенному для аутентификации LDAP. В левой экранной области выберите **AAA Server Groups** (Группы серверов AAA).

Выберите сервер AAA, настроенный для протокола LDAP, и нажмите кнопку **Edit** (Изменить).

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**.

Интерфейс командной строки

Для настройки карты LDAP на ASA выполните следующие шаги в интерфейсе командной строки.

```
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
```

Настройка Active Directory и других серверов LDAP

Настройка, которую требуется выполнит на сервере Active Directory или другом сервере LDAP, касается только атрибутов пользователя. В этом примере пользователь Kate Austin – член группы Employees 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
```

Поиск и 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.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация