使用LDAP属性映射配置示例

目录

简介

本文档介绍如何将任何Microsoft/AD属性映射到Cisco属性。

步骤

1. 在Active Directory(AD)/轻量级目录访问协议(LDAP)服务器上：选择**user1**。右键单击**> Properties**。选择要用于设置属性的选项卡（例如，常规选项卡）。选择用于实施时间范围的字段/属性，例如Office字段，并输入标语文本(例如，欢迎使用LDAP服务!!!!)。GUI上的Office配置存储在AD/LDAP属性physicalDeliveryOfficeName中。
2. 在自适应安全设备(ASA)上，为了创建LDAP属性映射表，请将AD/LDAP属性physicalDeliveryOfficeName映射到ASA属性Banner1:

```
B200-54(config)# show run ldap
ldap attribute-map Banner
map-name physicalDeliveryOfficeName Banner1
```

3. 将LDAP属性映射关联到aaa-server条目：

```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map Banner
```

4. 建立远程访问会话并验证是否向VPN用户显示!!!!欢迎使用LDAP服务的横幅。

将LDAP用户置于特定组策略（通用示例）

此示例演示AD-LDAP服务器上user1的身份验证，并检索department字段值，以便可以将其映射至可从其实施策略的ASA/PIX组策略。

1. 在AD/LDAP服务器上：选择**user1**。右键单击**> Properties**。选择要用于设置属性的选项卡（例如，“组织”选项卡）。选择要用于实施组策略的字段/属性，例如Department，并在ASA/PIX上输入组策略(Group-Policy1)的值。GUI上的部门配置存储在AD/LDAP属性部门中。
2. 定义ldap-attribute-map表。

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department Group-Policy
5520-1(config)#
```

3. 定义设备上的组策略Group_policy1和所需的策略属性。
4. 建立VPN远程访问隧道并验证会话是否继承来自Group-Policy1的属性（以及来自默认组策略的任何其他适用属性）。 **注意**：根据需要向映射添加更多属性。此示例仅显示控制此特定功能的最小值（将用户置于特定ASA/PIX 7.1.x组策略中）。第三个示例显示这种类型的映射。

配置NOACCESS组策略

您可以创建NOACCESS组策略，以便在用户不属于任何LDAP组时拒绝VPN连接。显示以下配置片段供您参考：

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

您必须将此组策略作为默认组策略应用到隧道组。这允许从LDAP属性映射获取映射的用户（例如，属于所需LDAP组的用户）获取其所需的组策略，以及未获取任何映射的用户（例如，不属于任何所需LDAP组的用户）从隧道组获取NOACCESS组策略，该隧道组会阻止其访问。

> **提示**：由于vpn-simultaneous-logins属性在此设置为0，因此它也必须在所有其他组策略中显式定义；否则，它可以从该隧道组的默认组策略继承，在本例中该隧道组为NOACCESS策略。

基于组的属性策略实施（示例）

1. 在AD-LDAP服务器、Active Directory用户和计算机上，设置代表配置VPN属性的组的用户记录(VPNUserGroup)。
2. 在AD-LDAP服务器、Active Directory用户和计算机上，定义每个用户记录的Department字段以指向步骤1中的组记录(VPNUserGroup)。本示例中的用户名是web1。 **注意**：之所以使用Department AD属性，只是因为逻辑上部门引用组策略。实际上，任何领域都可以使用。要求此字段必须映射到Cisco VPN属性Group-Policy，如本示例所示。
3. 定义ldap-attribute-map表：

```
5520-1(config)# show runn ldap
ldap attribute-map Our-AD-Map
map-name department IETF-Radius-Class
map-name description\Banner1
```

```
map-name physicalDeliveryOfficeName IETF-Radius-Session-Timeout
5520-1(config)#
```

两个AD-LDAP属性Description和Office（由AD名称description和PhysicalDeliveryOfficeName表示）是映射到Cisco VPN属性Banner1和IETF-Radius-Session-Timeout的组记录属性（对于VPNUSerGroup）。department属性用于用户记录映射到ASA(VPNUSer)上的外部组策略名称，然后映射回AD-LDAP服务器上的VPNuserGroup记录，其中定义了属性。**注**：必须在ldap-attribute-map中定义Cisco属性(Group-Policy)。其映射的AD属性可以是任何可设置的AD属性。此示例使用department，因为它是引用组策略的最逻辑名称。

4. 使用ldap-attribute-map name配置aaa-server以用于LDAP身份验证、授权和记帐(AAA)操作：

```
5520-1(config)# show runn aaa-server LDAP-AD11
aaa-server LDAP-AD11 protocol ldap
aaa-server LDAP-AD11 host 10.148.1.11
ldap-base-dn cn=Users,dc=nelson,dc=cisco,dc=com
ldap-scope onelevel
ldap-naming-attribute sAMAccountName
ldap-login-password altiga
ldap-login-dn cn=Administrator,cn=Users,dc=nelson,dc=cisco,dc=com
ldap-attribute-map Our-AD-Map
5520-1(config)#
```

5. 使用LDAP身份验证或LDAP授权定义隧道组。 LDAP身份验证示例。如果定义了属性，则执行身份验证+（授权）属性策略实施。

```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group LDAP-AD11
accounting-server-group RadiusACS28
5520-1(config)#
```

LDAP授权示例。用于数字证书的配置。

```
5520-1(config)# show runn tunnel-group
remoteAccessLDAPTunnelGroup
tunnel-group RemoteAccessLDAPTunnelGroup general-attributes
authentication-server-group none
authorization-server-group LDAP-AD11
accounting-server-group RadiusACS28
authorization-required
authorization-dn-attributes ea
5520-1(config)#
```

6. 定义外部组策略。group-policy的名称是代表组(VPNUserGroup)的AD-LDAP用户记录的值。

```
5520-1(config)# show runn group-policy VPNUserGroup
group-policy VPNUserGroup external server-group LDAP-AD11
5520-1(config)#
```

7. 建立隧道并检验属性是否已实施。在这种情况下，Banner和Session-Timeout从AD上的VPNuserGroup记录中实施。

为IPsec和SVC隧道实施“分配静态IP地址”的Active Directory

AD属性为msRADIUSFramedIPAddress。该属性在AD用户属性、拨入选项卡、分配静态IP地址中配置。

步骤如下：

1. 在AD服务器上的user Properties， Dial-in tab， Assign a Static IP Address下，输入IP Address的值以分配给IPsec/SVC会话(10.20.30.6)。
2. 在ASA上，使用以下映射创建ldap属性映射：

```
5540-1# show running-config ldap
```

```
ldap attribute-map Assign-IP
map-name msRADIUSFramedIPAddress IETF-Radius-Framed-IP-Address
5540-1#
```

3. 在ASA上，验证vpn-address-assign已配置为包含vpn-addr-assign-aaa:
```
5520-1(config)# show runn all vpn-addr-assign
vpn-addr-assign aaa
no vpn-addr-assign dhcp
vpn-addr-assign local
5520-1(config)#
```
4. 建立IPsec/SVC Remote Authority(RA)会话并验证show vpn-sessiondb remote|svc以确保“已分配的IP”字段正确(10.20.30.6)。

Active Directory实施“远程访问权限拨入，允许/拒绝访问”

支持所有VPN远程访问会话：IPSec、WebVPN和SVC。Allow Access的值为TRUE。Deny Access的值为FALSE。AD属性名称为msNPAllowDialin。

此示例演示如何创建使用Cisco隧道协议创建Allow Access(TRUE)和Deny(FALSE)条件的ldap-attribute-map。例如，如果映射tunnel-protocol=L2TPover IPsec(8)，则尝试为WebVPN和IPsec实施访问时，可以创建FALSE条件。相反的逻辑也适用。

步骤如下：

1. 在AD服务器user1 Properties（属性）的Dial-In（拨入）中，为每个用户选择适当的allow Access（允许访问）或Deny access（拒绝访问）。 **注意**：如果选择第三个选项“通过远程访问策略控制访问”，则不会从AD服务器返回任何值，因此实施的权限基于ASA/PIX的内部组策略设置。
2. 在ASA上，使用以下映射创建ldap-attribute-map:
```
ldap attribute-map LDAP-MAP
map-name msNPAllowDialin Tunneling-Protocols
map-value msNPAllowDialin FALSE 8
map-value msNPAllowDialin TRUE 20
5540-1#
```
注意：根据需要向映射添加更多属性。此示例仅显示控制此特定功能的最小值（根据拨入设置允许或拒绝访问）。ldap-attribute-map是什么意思或强制执行？map-value msNPAllowDialin FALSE 8拒绝用户1的访问。FALSE值条件映射到隧道协议L2TPoverIPsec（值8）。允许用户2访问。TRUE值条件映射到隧道协议WebVPN + IPsec（值20）。由于隧道协议不匹配，在AD上验证为user1的WebVPN/IPsec用户将失败。L2TPoverIPsec在AD上身份验证为user1，由于Deny规则将会失败。在AD上身份验证为user2的WebVPN/IPsec用户将成功（允许规则+匹配的隧道协议）。由于隧道协议不匹配，在AD上身份验证为user2的L2TPoverIPsec将会失败。
支持RFC 2867和2868中定义的隧道协议。

Active Directory强制“/组成员”成员以允许或拒绝访问

此案例与案例5密切相关，可提供更加逻辑的流程，并且是推荐方法，因为它将组成员身份检查作为条件来建立。

1. 将AD用户配置为特定组的成员。使用将其置于group-hierarchy(ASA-VPN-Consultants)顶部的名称。在AD-LDAP中，组成员资格由AD属性memberOf定义。组位于列表顶部非常重要，因为您当前只能将规则应用于第一个group/memberOf字符串。在版本7.3中，您可以执行多组过滤和实施。

2. 在ASA上，创建具有最小映射的ldap-attribute-map:

```
ldap attribute-map LDAP-MAP
map-name memberOf Tunneling-Protocols
map-value memberOf cn=ASA-VPN-Consultants,cn=Users,dc=abcd,dc=com 4
5540-1#
```

注意：根据需要向映射添加更多属性。此示例仅显示控制此特定功能的最小值（根据组成员资格允许或拒绝访问）。ldap-attribute-map是什么意思或强制执行
？User=joe_consultant，AD的一部分，是AD组ASA-VPN-Consultants的成员，仅当用户使用IPsec(tunnel-protocol=4=IPSec)时，才允许访问。User=joe_consultant（AD的一部分）在任何其他远程访问客户端（PPTP/L2TP、L2TP/IPSec、WebVPN/SVC等）期间，VPN访问可能会失败。无法允许User=bill_the_hacker进入，因为用户没有AD成员资格。

Active Directory实施“登录时间/时间规则”

此使用案例介绍如何在AD/LDAP上设置和实施时间规则。

以下是执行此操作的步骤：

1. 在AD/LDAP服务器上：选择用户。右键单击**> Properties**。选择要用于设置属性的选项卡（“示例”、“常规”选项卡）。选择用于实施时间范围的字段/属性，例如Office字段，然后输入时间范围的名称（例如，波士顿）。GUI上的Office配置存储在AD/LDAP属性physicalDeliveryOfficeName中。
2. 在ASA上 创建LDAP属性映射表。将AD/LDAP属性“physicalDeliveryOfficeName”映射到ASA属性“Access-Hours”。示例：

```
B200-54(config-time-range)# show run ldap
ldap attribute-map TimeOfDay
map-name physicalDeliveryOfficeName Access-Hours
```

3. 在ASA上，将LDAP属性映射关联到aaa-server条目：

```
B200-54(config-time-range)# show runn aaa-server microsoft
aaa-server microsoft protocol ldap
aaa-server microsoft host audi-qa.frdevtestad.local
ldap-base-dn dc=frdevtestad,dc=local
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password hello
ldap-login-dn cn=Administrator,cn=Users,dc=frdevtestad,dc=local
ldap-attribute-map TimeOfDay
```

4. 在ASA上，创建具有分配给用户的名称值（步骤1中的Office值）的时间范围对象：

```
B200-54(config-time-range)# show runn time-range
!
time-range Boston
periodic weekdays 8:00 to 17:00
!
```

5. 建立VPN远程访问会话： 如果在时间范围内，会话可以成功。如果超出时间范围，会话可能会失败。

使用ldap-map配置将用户映射到特定组策略，并在双重身份验证的情况下使用authorization-server-group命令

1. 在这种情况下，使用双重身份验证。使用的第一个身份验证服务器是RADIUS，使用的第二个身份验证服务器是LDAP服务器。 配置LDAP服务器和RADIUS服务器。示例如下：

```
ASA5585-S10-K9# show runn aaa-server
aaa-server test-ldap protocol ldap
aaa-server test-ldap (out) host 10.201.246.130
```

```
 ldap-base-dn cn=users, dc=htts-sec, dc=com
 ldap-login-password *****
 ldap-login-dn cn=Administrator, cn=Users, dc=htts-sec, dc=com
 server-type microsoft
 ldap-attribute-map Test-Safenet-MAP
aaa-server test-rad protocol radius
aaa-server test-rad (out) host 10.201.249.102
 key *****
```

定义LDAP属性映射。示例如下：

```
ASA5585-S10-K9# show runn ldap
ldap attribute-map Test-Safenet-MAP
map-name memberOf IETF-Radius-Class
map-value memberOf "CN=DHCP Users,CN=Users,DC=htts-sec,DC=com" Test-Policy-Safenet
```

定义隧道组并关联RADIUS和LDAP服务器进行身份验证。示例如下：

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

查看隧道组配置中使用的组策略：

```
ASA5585-S10-K9# show runn group-policy
group-policy NoAccess internal
group-policy NoAccess attributes
wins-server none
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 0
default-domain none
group-policy Test-Policy-Safenet internal
group-policy Test-Policy-Safenet attributes
dns-server value 10.34.32.227 10.34.32.237
vpn-simultaneous-logins 15
vpn-idle-timeout 30
vpn-tunnel-protocol ikev1 ssl-client ssl-clientless
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Safenet-Group-Policy-SplitAcl
default-domain none
```

使用此配置时，使用LDAP属性正确映射的AnyConnect用户不会放置在组策略Test-Policy-Safenet中。相反，它们仍位于默认组策略中，在本例中为NoAccess。请参阅调试代码段(debug ldap 255)和syslogs的级别信息：

```
----------------------------------------------------------------------------

memberOf: value = CN=DHCP Users,CN=Users,DC=htts-sec,DC=com

[47]                        mapped to IETF-Radius-Class: value = Test-Policy-Safenet

[47]                        mapped to LDAP-Class: value = Test-Policy-Safenet

----------------------------------------------------------------------------

Syslogs :

%ASA-6-113004: AAA user authentication Successful : server = 10.201.246.130 : user =
test123

%ASA-6-113003: AAA group policy for user test123 is set to Test-Policy-Safenet

%ASA-6-113011: AAA retrieved user specific group policy (Test-Policy-Safenet) for user =
test123
```

```
%ASA-6-113009: AAA retrieved default group policy (NoAccess) for user = test123

%ASA-6-113013: AAA unable to complete the request Error : reason = Simultaneous logins
exceeded for user : user = test123

%ASA-6-716039: Group <DfltGrpPolicy> User <test123> IP <10.116.122.154> Authentication:
rejected, Session Type: WebVPN.
```

这些系统日志显示失败，因为向用户授予了同时登录设置为0的NoAccess组策略，即使系统日志声称它检索了用户特定的组策略。为了根据LDAP映射在组策略中分配用户，您必须使用以下命令：**authorization-server-group test-ldap**(在本例中，**test-ldap**是LDAP服务器名称)。示例如下：

```
ASA5585-S10-K9# show runn tunnel-group
tunnel-group Test_Safenet type remote-access
tunnel-group Test_Safenet general-attributes
address-pool RA_VPN_IP_Pool
authentication-server-group test-rad
 secondary-authentication-server-group test-ldap use-primary-username
authorization-server-group test-ldap
default-group-policy NoAccess
tunnel-group Test_Safenet webvpn-attributes
group-alias Test_Safenet enable
```

2. 现在，如果第一个身份验证服务器（在本例中为RADIUS）确实发送了用户特定属性，例如IEFT类属性，在这种情况下，用户可以映射到RADIUS发送的组策略。因此，即使辅助服务器配置了LDAP映射，并且用户的LDAP属性确实将用户映射到其他组策略，也可以实施由第一身份验证服务器发送的组策略。 要使用户根据LDAP映射属性置于组策略中，必须在隧道组：**authorization-server-group test-ldap**下指定此命令。
3. 如果第一个身份验证服务器是SDI或OTP，无法传递用户特定属性，则用户将归入隧道组的默认组策略。在本例中，即使LDAP映射正确，也不要访问。 在这种情况下，您还需要在隧道组下使用命令**authorization-server-group test-ldap**，以便将该用户置于正确的组策略中。
4. 如果两个服务器都是相同的RADIUS或LDAP服务器，则无需使用**authorization-server-group**命令即可使组策略锁定生效。

验证

```
ASA5585-S10-K9# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : test123                  Index        : 2
Assigned IP  : 10.34.63.1             Public IP    : 10.116.122.154
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : 3DES 3DES 3DES         Hashing      : SHA1 SHA1 SHA1
Bytes Tx     : 14042                  Bytes Rx     : 8872
Group Policy : Test-Policy-Safenet    Tunnel Group : Test_Safenet
Login Time   : 10:45:28 UTC Fri Sep 12 2014
Duration     : 0h:01m:12s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

故障排除

使用本部分可排除配置故障。

调试 LDAP 事务

可以使用以下调试来帮助隔离DAP配置的问题：

- debug ldap 255
- debug dap trace
- debug aaa authentication

ASA无法从LDAP服务器对用户进行身份验证

如果ASA无法从LDAP服务器对用户进行身份验证，以下是一些示例调试：

```
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
```

在这些调试中，LDAP登录DN格式不正确或密码不正确，因此请检验这两种格式以解决问题。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。