ASA使用LDAP属性映射配置示例

目录

简介

本文描述如何使用轻量级目录访问协议(LDAP)属性地图为了配置在可适应安全工具(ASA)的粒状动态Accesss策略。

先决条件

要求

Cisco 建议您了解以下主题：

- 在Cisco IOS的安全套接字协议层VPN (SSL VPN)
- 在Cisco IOS的LDAP认证
- 目录服务

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CISCO881-SEC-K9
- Cisco IOS软件， C880软件(C880DATA-UNIVERSALK9-M)，版本15.1(4)M，发行软件(fc1)

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

LDAP是访问和保养在IP网络的分布式目录信息服务的一个开放，供应商中立，工业标准的应用协议。因为他们允许关于用户、系统、网络、服务和应用程序的信息共享在网络中，目录服务播放在内联网和互联网应用程序的开发的一重要的角色。

管理员需要经常为 VPN 用户提供不同的访问权限或 WebVPN 内容。如果配置在VPN服务器的不同的VPN策略并且分配这些策略集到根据他们的凭证的每个用户这可以执行。当这可以手工时执行，它是自动化与目录服务的进程的更有效的。为了使用LDAP分配组策略对用户，您需要配置映射一个LDAP属性，例如激活目录(AD)属性**memberOf**，对IETF RADIUS**中集集团**属性由VPN头端了解的地图。

在Cisco IOS，同一件事可以达到，如果配置不同的策略组在WebVPN上下文下并且使用LDAP属性地图为了确定哪个策略组用户将分配正如本文所描述。请参阅策略组分配关于使用在Cisco IOS头端配置示例的LDAP的AnyConnect客户端。

在ASA，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。 为了使用LDAP分配组策略对用户，您必须映射一个LDAP属性，例如AD属性**memberOf**到由ASA了解的策略属性。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。

FAQ

Q. 有没有在LDAP属性MAP数量的配置限制ASA的？

A.不，那里是没有限额。LDAP属性MAP动态地分配在使用LDAP认证/授权的VPN远程访问会话期间。

Q. 有没有在可以每LDAP属性MAP被映射属性的数量的限制？

A.没有配置限制。

Q. 有没有在特定LDAP属性MAP可以应用的多少个LDAP服务器的限制？

A.没有限制。LDAP代码只验证LDAP属性MAP名称有效。

Q. 有没有与LDAP属性MAP的限制和muti被重视的属性类似AD memberOf ？

A.可以。这里，仅AD解释，但是适用于使用多值属性政策决策的所有LDAP服务器。LDAP属性MAP有与多值的属性的一个限制类似AD memberOf。如果用户是(普通)的memberOf几AD组，并且LDAP属性MAP配比超过他们中的一个，根据匹配的条目的字母表选定的被映射的值。因为此行为不是明显或直观的，有关于是重要的如何的清楚知识工作。

摘要： 如果LDAP映射导致属性的多个值，最终属性值选择如下：

- 首先，请选择与字符小数量的值。
- 如果这导致超过一个值，请选择以字母顺序是最低的值。

用例示例

激活目录LDAP返回用户认证或授权请求的这四memberOf实例：

```
memberOf: value = CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com
memberOf: value = CN=Cisco-Eng,CN=Users,DC=stbu,OU=cisco,DC=com
memberOf: value = CN=Employees,CN=Users,OU=stbu,DC=cisco,DC=com
memberOf: value = CN=Engineering,CN=Users,OU=stbu,DC=cisco,DC=com
```

LDAP-MAP #1 ： 假设，此LDAP属性MAP配置映射根据memberOf设置的不同的ASA组政策：

```
ldap attribute-map Class
map-name memberOf Group-Policy
map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup4
map-value memberOf CN=cisco-Eng,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup3
map-value memberOf CN=Employees,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup2
map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup1
```

在这种情况下，匹配在所有四组政策价值(ASAGroup1将发生- ASAGroup4)。然而，因为以字母顺序，首先发生连接将分配到组政策ASAGroup1。

LDAP-MAP #2 ： 此LDAP属性MAP是相同的，除了第一memberOf没有一明确Map值已分配(没有ASAGroup4)。注意，当明确Map值定义，使用从LDAP接收的属性文本。

```
ldap attribute-map Class
map-name memberOf Group-Policy
map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com
map-value memberOf CN=cisco-Eng,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup3
map-value memberOf CN=Employees,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup2
map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=cisco,DC=com ASAGroup1
```

正如在上一个案件，匹配在所有四个条目发生。在这种情况下，因为被映射的值为APP-SSL-VPN条目没有提供，被映射的值将默认为CN=APP-SSL-VPN管理器， Cn=users， OU=stbu， Dc=cisco， Dc=com。因为CN=APP-SSL-VPN首先按aphabetical顺序出现， APP-SSL-VPN将选

择作为政策价值。

参考的Cisco Bug ID CSCub64284欲知更多信息。参考的PIX/ASA 8.0 ：请使用LDAP认证分配组策略在洛金，显示有memberOf的一个简单LDAP事例在您特定的部署也许工作。

应急方案/最佳实践选项

1. 使用动态访问策略(DAP) - DAP没有解析多值的属性的此限制(类似memberOf);但是DAP不能当前设置组政策从本身的内部。这意味着会话会必须通过隧道群/组政策关联方法适当地被分段。 将来， DAP将有功能设置所有authorizaiton属性，包括组政策， (Cisco Bug ID CSCsi54718)，因此需要对于LDAP属性MAP最终为此不会要求。

2. 作为可能替代方案和，如果部署方案允许它，每当您必须使用LDAP属性MAP设置类别属性，您可能也使用一个单一被重视的属性(类似部门)代表您的在AD的组差异化。

   注意： 在memberOf DN中例如“CN=Engineering， OU=Office1， Dc=cisco， Dc=com”，您能只做出在第一个DN的决策，是CN=Engineering，不是组织单位(OU)。有的增强能能过滤在所有DN字段。

配置-采样使用盒

注意：在此部分描述的每示例是独立配置，但是可以彼此混合搭配导致希望的访问策略。

提示：属性名称和值区分大小写。如果映射不适当地发生，肯定正确拼写和资本化用于LDAP属性地图思科和LDAP属性名称和值。

1. 基于用户的属性策略执行

所有标准LDAP属性可以被映射到著名的设备Vendor Specific Attribute (VSA)。一个或更多LDAP属性可以被映射到一个或更多思科LDAP属性。对于思科LDAP VSAs完整列表，为LDAP授权请参考支持的思科属性。 此示例显示如何强制执行LDAP user1的一标语。User1可以是任何VPN远程访问类型：IPsec、SVC或者WebVPN无客户端。 此示例使用属性/常规/办公室属性/字段强制执行Banner1。

注意：您可能使用AD部门属性/字段映射到思科IETF RADIUS中集集团VSA为了强制执行从ASA/PIX组政策的策略。有此的示例以后在本文。

LDAP (Microsoft AD和Sun)属性映射自PIX/ASA版本7.1.x支持。所有Microsoft/AD属性可以被映射到思科属性。 这是执行此的步骤：

1. 在AD/LDAP服务器上：挑选user1。右键单击**>Properties**。选择将使用的选项卡为了设置属性(示例。常规选项卡)。选择字段/属性，例如“办公室”字段，使用为了强制执行time-range，并且输入标语文本(示例，欢迎到LDAP!!!!)。在GUI的“办公室”配置在AD/LDAP属性“physicalDeliveryOfficeName”存储。

2. 在ASA，为了创建LDAP属性映射表，请映射AD/LDAP属性“physicalDeliveryOfficeName”对ASA属性"Banner1" ：

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

3. 关联LDAP属性地图对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且验证班纳“欢迎到LDAP!!!!”被提交给VPN用户。

2. 安置LDAP用户在特定组政策-通用的示例

此示例展示user1的验证在AD-LDAP服务器的并且检索Department字段值，因此可以被映射到策略将被强制执行的ASA/PIX组政策。

1. 在AD/LDAP服务器上：挑选user1。右键单击**>Properties**。选择将使用的选项卡为了设置属性(示例。组织选项卡)。例如选择字段/属性，“部门”，使用为了强制执行组政策，并且输入组政策(Group-Policy1)的值在ASA/PIX。在GUI的“部门”配置在AD/LDAP属性“部门”存储。

2. 定义LDAP属性MAP表。

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

   注意： 由于Cisco Bug ID CSCsv43552的实施，一个新的LDAP属性MAP属性，组政策，介绍为了替换IETF RADIUS中集集团。 在ASA版本8.2的CLI支持IETF RADIUS中集集团关键字作为在映射名和Map值命令的一有效选择为了读8.0配置文件(软件升级方案)。可适应安全设备管理器(ASDM)代码已经更新不再显示IETF RADIUS中集集团作为选择，当您配置属性映射条目时。 另外， ASDM将写出IETF RADIUS中集集团属性(如果写入从8.0设置)作为策略属性。

3. 定义在设备和需要的策略属性的组政策Group_policy1。

4. 设立VPN远程访问隧道并且验证会话继承从Group-Policy1的属性(和从默认组政策的任何其他可适用的属性)。

   注意：添加更多属性到地图如所需求。此示例显示仅最低控制此特定功能(请安置一个用户在一特定ASA/PIX 7.1.x组政策)。第三示例显示此种地图。

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
```

您必须运用此组策略作为默认组策略对隧道群。这允许从LDAP属性地图获得映射没获得任何映射的用户，例如属于一希望的LDAP组的那些人，获得他们的希望的组策略的和用户，例如不属于任何希望的LDAP组的那些人，获得NOACCESS组政策的从隧道群，阻止他们的访问。

> **提示**：因为vpn-simultaneous-logins属性设置到0此处，在所有其他组政策必须明确地定义;否则，它从该隧道组的默认策略将被继承，在这种情况下是NOACCESS策略。

3. 基于组的属性策略执行-示例

> **注意**：Cisco Bug ID CSCse08736实施/修正要求，因此ASA应该运行至少版本7.2.2。

1. 在AD-LDAP服务器上，激活目录用户和计算机，设置代表组VPN属性配置的客户记录(VPNUserGroup)。

2. 在AD-LDAP服务器上，激活目录用户和计算机，定义了每客户记录的Department字段指向成组记录(VPNUserGroup)在Step1。在本例中的用户名是**web1**。

   注意：部门AD属性，只有因为“部门”逻辑上是指组政策，使用了。实际上，能使用所有字段。需求是如此示例所显示，此字段必须映射到思科VPN属性组政策。

3. 定义LDAP属性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)#
   ```

   映射对思科VPN属性Banner1和IETF RADIUS会话超时的两个AD-LDAP属性说明和办公室(代表用AD名称说明和PhysicalDeliveryOfficeName)是成组记录属性(VPNUSerGroup)。

   部门属性是为了客户记录能映射对外部组政策名称在ASA (Vpnuser)的，然后映射回到在AD-LDAP服务器的VPNuserGroup记录，属性定义。

   注意：在LDAP属性MAP必须定义思科属性(组政策)。其被映射的AD属性可以是所有settable AD属性。此示例使用部门，因为它是指组政策的多数逻辑名。

4. 配置aaa-server与将用于LDAP认证、授权和核算(AAA)操作LDAP属性MAP名称：

   ```
   5520-1(config)# show runn aaa-server LDAP-AD11
   aaa-server LDAP-AD11 protocol ldap
   aaa-server LDAP-AD11 host 90.148.1.11
   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. 定义有有LDAP认证的或LDAP授权的一隧道群。

   与LDAP认证的示例。执行验证+ (授权)属性策略执行，如果属性定义。

```
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)#
```

与LDAP授权的示例。为使用数字证书使用的配置。

```
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. 定义一外部组政策。组政策的名称是代表组AD-LDAP客户记录的值(VPNUserGroup)。

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

7. 设立通道并且验证属性被强制执行。在这种情况下，班纳和Session-timeout从在AD的VPNuserGroup记录被强制执行。

4. 活动目录执行“为IPsec和SVC通道分配静态IP地址”

AD属性是msRADIUSFramedIPAddress。属性在AD用户属性配置， Dial-in选项，“分配静态IP地址”。

这是步骤：

1. 在AD服务器上，在用户属性下， Dial-in选项，“分配静态IP地址”，输入IP地址的值为了分配到IPsec/SVC会话(10.20.30.6)。

2. 在ASA请创建与此映射的一LDAP属性MAP ：

```
5540-1# show running-config ldap
ldap attribute-map Assign-IP
map-name msRADIUSFrameIPAdddress IETF-Radius-Framed-IP-Address
5540-1#
```

3. 在ASA，请验证VPN地址assigment配置包括“VPN ADDR分配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远程权限(RA)会话并且验证与“显示vpn-sessiondb远程|“指定IP”字段正确的svc” (10.20.30.6)。

5. “远程访问许可拨入的活动目录执行，允许/拒绝访问”

支持所有VPN远程Acccess会话：IPSec、WebVPN和SVC。允许有值特鲁。拒绝Acccess有值错误。AD属性名称是msNPAllowDialin。

此示例展示使用思科隧道协议创建允许LDAP属性MAP的创建(特鲁)和拒绝(错误)情况。例如，如果映射tunnel-protocol=L2TPover IPsec (8)，您能创造错误条件是否设法强制执行WebVPN和IPsec的访问。反向逻辑也是应用。

这是步骤：

1. 在AD服务器user1属性，拨入，选择适当的允许或拒绝每个用户的访问。

   注意：如果选择第三个选项“控制访问通过Remote access Policy”，值没有从AD服务器返回，如此被强制执行根据ASA/PIX内部组政策的设置的权限。

2. 在ASA，请创建与此映射的一LDAP属性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：添加更多属性到地图如所需求。此示例显示仅最低控制此特定功能(请允许或拒绝根据拨入设置的访问)。

   LDAP属性MAP是什么意思或强制执行？

   Map值msNPAllowDialin错误8

   拒绝user1的访问。错误值情况映射对隧道协议L2TPoverIPsec， (值8)。

   user2的允许。真实值情况映射对隧道协议WebVPN + IPsec， (值20)。

   WebVPN/IPSec用户， authenticaticated作为在AD的user1，将发生故障由于协议不匹配。

   L2TPoverIPsec， authenticaticated作为在AD的user1，将发生故障由于拒绝规则。

   WebVPN/IPSec用户， authenticaticated作为在AD的user2，将成功(请允许规则+匹配的隧道协议)。

L2TPoverIPsec， authenticaticated作为在AD的user2，将发生故障由于协议不匹配。
隧道协议的支持，如对RFCs 2867和2868定义。

6. “”允许或拒绝访问的/Group成员关系的成员的活动目录执行

因为设立组成员检查作为情况，此案件是密切相关案例5，提供一个更加逻辑的流，并且是推荐的方法。

1. 配置AD用户是“”一特定组的成员。请使用放置它在组层级的一名称(ASA VPN顾问)顶部。在AD-LDAP中，组成员由AD属性“memberOf”定义。

   重要的是组是在列表顶部，因为您能只当前运用规则到第一个组“memberOf”字符串。在版本7.3中，您能进行多个组过滤和实施。
2. 在ASA，请创建与最低的映射的一LDAP属性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：添加更多属性到地图如所需求。此示例显示仅最低控制此特定功能(请允许或拒绝根据组成员的访问)。

   LDAP属性MAP是什么意思或强制执行？

   User=joe_consultant，一部分的AD，是AD组“ASA VPN顾问”的成员将允许访问，只有当用户使用IPsec (tunnel-protocol=4=IPSec)。

   在其他远程访问客户端(PPTP/L2TP， L2TP/IPsec期间， User=joe_consultant，一部分的AD，失效VPN访问， WebVPN/SVC，等等)。

   因为用户没有AD会员， User=bill_the_hacker不会允许。

7. “登录小时/时刻的活动目录执行规定”

此用例描述如何设置和强制执行在AD/LDAP的每日定时规则。

这是要执行此的步骤：

1. 在AD/LDAP服务器上：选择用户。用鼠标右键单击**>Properties**。选择将使用的选项卡为了设置属性(示例。常规选项卡)。选择字段/属性，例如“办公室”字段，使用为了强制执行time-range，并且输入time-range的名称(例如，波士顿)。在GUI的“办公室”配置在AD/LDAP属性“physicalDeliveryOfficeName”存储。

2. 在ASA

   创建LDAP属性映射表。映射AD/LDAP属性“physicalDeliveryOfficeName”对ASA属性“访问时

段”。

示例：

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

3. 在ASA，请关联LDAP属性地图对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，请创建有命名值分配到用户的time-range对象(在步骤1)的办公室值：`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：

会话应该成功，如果在time-range内。会话可能失败，如果time-range的外部。

8. 请使用LDAP MAP配置映射用户到特定组政策和使用授权服务器组命令，一旦双重身份验证

1. 在此方案中，使用双重身份验证。使用的第一个认证服务器是RADIUS，并且使用的第二个验证服务器是LDAP服务器。

配置LDAP服务器以及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 *****
```

Definine 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
```

定义隧道群并且关联RADIUS和LDAP服务器验证的。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
```

查看在组配置里使用的组政策：

```
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，正确地映射与使用LDAP属性的AnyConnect用户在组政策未安置， TEST策略Safenet。反而，他们在默认组政策仍然安置了，在这种情况下无法访问。

请参阅调试(调试ldap 255)和Syslog的片断在级别信息性：

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

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 being 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Syslog显示失败，用户给无法访问组政策哪些让同时洛金设置到0，即使Syslog说获取一使用物精确的组政策。

为了根据LDAP MAP有使用者指定在组政策，您必须有此命令：**授权服务器组TEST LDAP** (在这种情况下， 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，如果第一个认证服务器(RADIUS，在本例中)发送使用物精确的属性，例如IEFT中集集团属性，在那种情况下，用户将被映射对RADIUS发送的组政策。因此，即使辅助服务器有配置的一张LDAP地图，并且用户的LDAP属性映射用户对一不同的组政策，第一个认证服务器发送的组政策将被强制执行。

   为了有用户请放置到根据LDAP地图属性的组政策，您必须指定此在隧道群下：**授权服务器组TEST LDAP**。

3. 如果第一个认证服务器是SDI或OTP，不能通过使用物精确的属性，则用户会落入隧道群的默认组政策。在这种情况下，无法访问，即使LDAP映射正确。

   在这种情况下，您也会需要命令，授权服务器**组TEST LDAP**，在用户的隧道群下能被放置到正确组政策。

4. 如果两个服务器是同样RADIUS或LDAP服务器，则您不需要授权服务器**组**命令为了组政策锁定能工作。

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的故障。

调试 LDAP 事务

这些调试可以用于为了帮助查出与DAP配置的问题：

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

ASA不能验证从LDAP服务器的用户

万一ASA不能验证从LDAP的用户服务，这是一些示例调试：

```
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
```

从这些调试，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。