为 VPN 配置外部 AAA 服务器

关于外部 AAA 服务器

此 ASA 可配置为使用外部 LDAP、RADIUS 或 TACACS+ 服务器来支持 ASA 的认证、授权和审计 (AAA)。外部 AAA 服务器会实施配置的权限和属性。将 ASA 配置为使用外部服务器之前，必须使用正确的 ASA 授权属性来配置外部 AAA 服务器，并从其中一部分属性向个人用户分配特定权限。

了解授权属性的策略实施

ASA 支持将用户授权属性（也称为用户授权或权限）应用到 VPN 连接的多种方法。您可以将 ASA 配置为通过以下任意组合获取用户属性：

- ASA 上的动态访问策略 (DAP)
- 外部 RADIUS 或 LDAP 身份验证和/或授权服务器
- ASA 上的组策略

如果ASA收到来自所有来源的属性，将会对这些属性进行评估、合并，并将其应用至用户策略。如果属性之间有冲突，DAP 属性优先。

ASA 按照以下顺序应用属性：

1. ASA 上的 DAP 属性 - 在 8.0(2) 版本中引入，这些属性优先于所有其他的属性。如果您在 DAP 中设置书签或 URL 列表，它会覆盖组策略中设置的书签或 URL 列表。
2. AAA 服务器上的用户属性 - 该服务器在用户身份验证和/或授权成功后返回这些属性。请不要将这些属性与 ASA 本地 AAA 数据库中为单个用户（ASDM 中的用户账户）设置的属性混淆。

3. 在 ASA 上配置的组策略 - 如果 RADIUS 服务器为用户返回 RADIUS CLASS 属性 IETF-Class-25 (OU=*group-policy*) 值， ASA 会将该用户放在名称相同的组策略中，并实施组策略中该服务器未返回的所有属性。

   对于 LDAP 服务器，任何属性名称都可用于设置会话的组策略。您在 ASA 上配置的 LDAP 属性映射会将该 LDAP 属性映射至思科属性 IETF-Radius-Class。

4. 连接配置文件（在 CLI 中称为隧道组）分配的组策略 - 连接配置文件具有该连接的初步设置，包括在进行身份验证前应用于用户的默认组策略。连接至 ASA 的所有用户最初都属于此组，这可以提供 DAP、服务器返回的用户属性或分配给用户的组策略中缺失的所有属性。

5. ASA 分配的默认组策略 (DfltGrpPolicy) - 系统默认属性提供 DAP、用户属性、组策略或连接配置文件中缺失的所有值。

外部 AAA 服务器使用准则

ASA 会根据属性名称而不是数值 ID 来实施 LDAP 属性。RADIUS 属性会按数值 ID 而不是名称来实施。

对于 ASDM 7.0 版本，LDAP 属性包含 cVPN3000 前缀。对于 ASDM 7.1 版本及更高版本，此前缀已移除。

LDAP 属性是已在 Radius 章节中列出的 Radius 属性的子集。

配置多证书身份验证

现在，您可以使用 Secure Client SSL 和 IKEv2 客户端协议验证每个会话的多重证书。例如，可以确保计算机证书的颁发者名称匹配特定的 CA，因此，设备是公司发布的设备。

通过多证书选项，可以同时通过证书对计算机和用户进行证书身份验证。如果没有此选项，则只能对其中之一执行证书身份验证，但不能二者兼顾。

注释 由于多证书身份验证需要一个计算机证书和一个用户证书（或两个用户证书），因此不能使用 Secure Client 登录前启动 (SBL) 功能。

通过预填充用户名字段，可以解析第二个（用户）证书中的字段并将其用于 AAA 和证书身份验证连接中的后续 AAA 身份验证。始终从自客户端收到的第二个（用户）证书检索主用和辅助用户名预填充。

从 9.14(1) 开始，ASA 允许您在配置多证书身份验证并使用“身份验证”或“授权”的预填充用户名选项时指定主用户名和辅助用户名应来自哪个证书。有关信息，请参阅Secure Client 连接配置文件，身份验证属性

通过多证书身份验证对两个证书进行身份验证：从自客户端收到的第二个（用户）证书解析 pre-fill 和 username-from-certificate 主用和辅助用户名。

您也可以配置通过 SAML 进行多证书身份验证。

通过多证书身份验证，可以根据证书字段制定策略决策，该证书用于对该连接尝试进行身份验证。将在多证书身份验证期间从客户端收到的用户和计算机证书加载到 DAP，以确保能够根据证书字段配置策略。要使用动态访问策略 (DAP) 添加多证书身份验证，以设置允许或禁止连接尝试的规则，请参阅中向 *DAP* 添加多证书身份验证一节相应版本的《ASA VPN ASDM 配置指南》。

Active Directory/LDAP VPN 远程访问授权示例

本节提供在 ASA 上使用 Microsoft Active Directory 服务器配置身份验证和授权的示例程序。包括以下主题：

- 基于用户的属性的策略实施 ， 第 3 页
- 为 Secure Client 隧道实施静态 IP 地址分配 ， 第 4 页
- 实施拨入允许或拒绝访问 ， 第 6 页
- 实施登录时长和时间规则 ， 第 8 页

Cisco.com 提供的其他配置示例包括以下技术说明。

- ASA/PIX：通过 LDAP 配置将 VPN 客户端映射至 VPN 组策略的示例
- PIX/ASA 8.0：登录时使用 LDAP 身份验证来分配组策略

基于用户的属性的策略实施

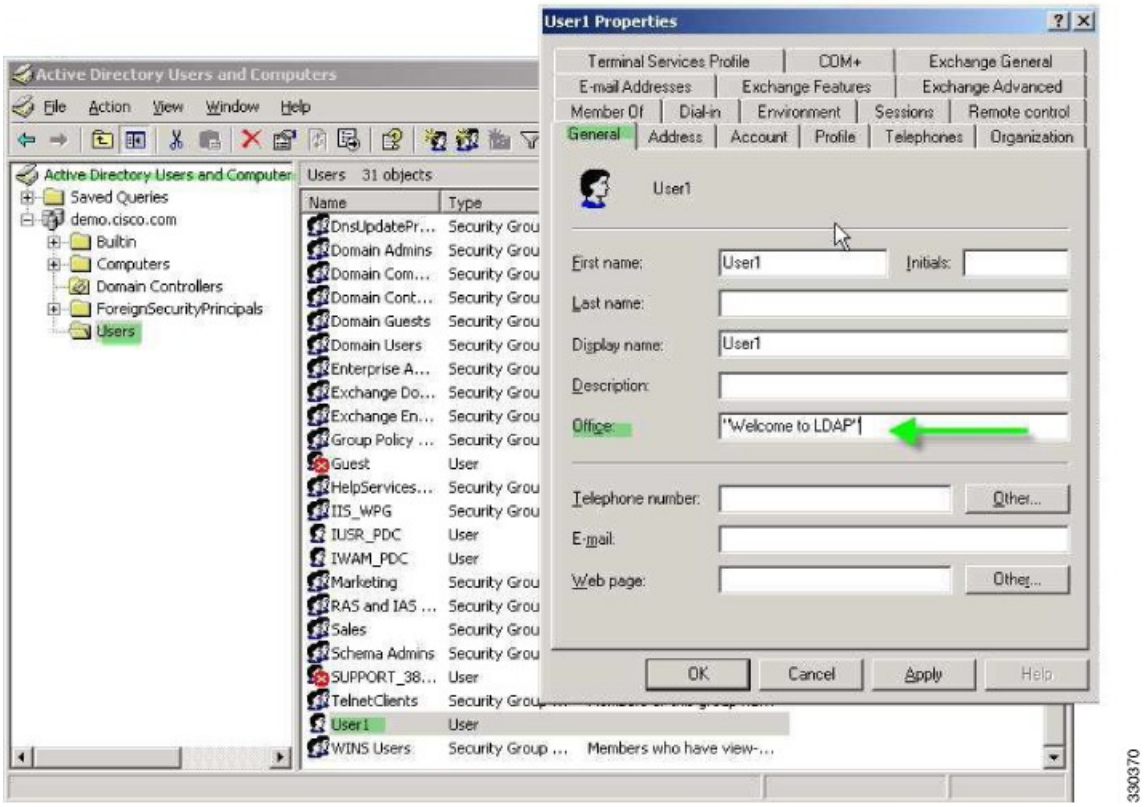
此示例向用户显示一个简单的欢迎信息，说明如何将任意标准 LDAP 属性映射至一个已知的供应商特定属性 (VSA)，或者将一个或多个 LDAP 属性映射至一个或多个思科 LDAP 属性。此示例适用于任意连接类型，包括 IPSec VPN 客户端和 Secure Client。

如要为 AD LDAP 服务器上配置的用户实施简单的欢迎信息，请使用 General 选项卡中的 Office 字段输入欢迎信息文本。此字段使用名为 physicalDeliveryOfficeName 的属性。在 ASA 中，创建将 physicalDeliveryOfficeName 映射至思科属性 Banner1 的属性映射。

在身份验证过程中，ASA 从服务器检索 physicalDeliveryOfficeName 的值，将该值映射至思科属性 Banner1，然后向用户显示该欢迎信息。

过程

步骤 1 右键点击用户名打开“属性”(Properties) 对话框，然后点击**常规 (General)** 选项卡，在“办公室”(Office) 字段中输入欢迎信息文本，该字段使用 AD/LDAP 属性 physicalDeliveryOfficeName。



步骤 2 在 ASA 上创建一个 LDAP 属性映射。

创建映射 Banner，并将 AD/LDAP 属性 physicalDeliveryOfficeName 映射至思科属性 Banner1：

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

步骤 3 将 LDAP 属性映射关联到 AAA 服务器。

进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您先前创建的属性映射 Banner：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

步骤 4 测试此欢迎信息的实施。

为 Secure Client 隧道实施静态 IP 地址分配

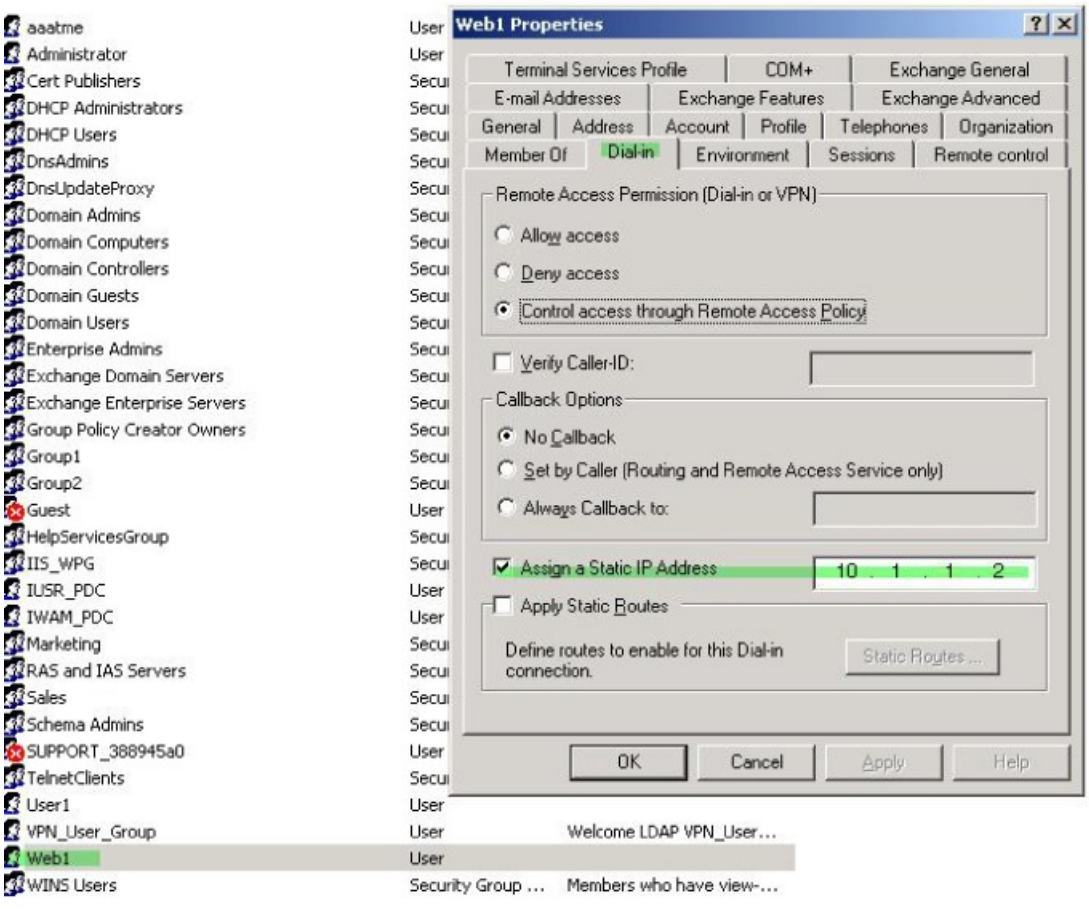
此示例适用于完全隧道客户端，例如 IPsec 客户端和 SSL VPN 客户端。

如要实施静态 Secure Client 静态 IP 分配，请将 Secure Client用户 Web1 配置为接受静态 IP 地址，在 AD LDAP 服务器上的 Dialin 选项卡的 Assign Static IP Address 字段中输入地址（此字段使用 msRADIUSFramedIPAddress 属性），然后创建一个可将该属性映射至思科属性 IETF-Radius-Framed-IP-Address 的属性映射。

在身份验证过程中，ASA 从服务器检索 msRADIUSFramedIPAddress 的值，将该值映射至思科属性 IETF-Radius-Framed-IP-Address，并向 User1 提供静态地址。

过程

步骤 1 右键点击用户名打开“属性”(Properties) 对话框，然后点击**拨入 (Dial-in)** 选项卡，选中**分配静态 IP 地址 (Assign Static IP Address)** 复选框并输入 IP 地址 10.1.1.2。



步骤 2 为显示的 LDAP 配置创建一个属性映射。

将 Static Address 字段使用的 AD 属性 msRADIUSFramedIPAddress 映射至思科属性 IETF-Radius-Framed-IP-Address：

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
```

```
IETF-Radius-Framed-IP-Address
```

步骤 3 将 LDAP 属性映射关联到 AAA 服务器。

进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您先前创建的属性映射 static_address：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

步骤 4 通过查看此部分的配置，验证是否已配置 **vpn-address-assignment** 命令来指定 AAA：

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa   << Make sure this is configured >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

步骤 5 使用 Secure Client建立与 ASA 的连接。观察用户是否收到在服务器上配置并映射至 ASA 的 IP 地址。

步骤 6 使用 **show vpn-sessiondb svc** 命令来查看会话详细信息，并验证分配的地址：

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                   Index        : 31
Assigned IP  : 10.1.1.2              Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 304140                 Bytes Rx     : 470506
Group Policy : VPN_User_Group         Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

实施拨入允许或拒绝访问

本示例创建指定用户允许的隧道协议的 LDAP 属性映射。您可以将 Dialin 选项卡中的允许访问和拒绝访问设置映射至思科属性 Tunneling-Protocol，该属性支持以下映射值：

值	隧道协议
1	PPTP
2	L2TP
4	IPsec (IKEv1)
8	L2TP/IPsec

值	隧道协议
16	无客户端 SSL
32	SSL 客户端 - Secure Client 或 SSL VPN 客户端
64	IPsec (IKEv2)

[1] (1) 不能同时支持 IPsec 和 L2TP over IPsec。因此，值 4 和 8 只能二选其一。
[2] (2) 请参阅注释 1。

使用此属性创建协议的允许访问 (TRUE) 或拒绝访问 (FALSE) 条件，并实施允许用户访问的方法。

有关实施拨入允许访问或拒绝访问的其他示例，请参阅以下技术说明：ASA/PIX：通过 LDAP 配置将 VPN 客户端映射至 VPN 组策略的示例。

过程

步骤 1 右键点击用户名打开“属性”(Properties) 对话框，然后点击**拨入 (Dial-in)** 选项卡，再点击“允许访问”(Allow Access) 单选按钮。

注释　如果您通过“远程访问策略”(Remote Access Policy) 选项选择控制访问，则服务器不会返回值，而实施的权限则根据 ASA 的内部组策略设置而定。

步骤 2 创建一个允许 IPsec 和 Secure Client 连接，但是拒绝无客户端 SSL 连接的属性映射。

a) 创建映射 tunneling_protocols：

```
hostname(config)# ldap attribute-map tunneling_protocols
```

b) 将 Allow Access 设置使用的 AD 属性 msNPAllowDialin 映射至思科属性 Tunneling-Protocols：

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

c) 添加映射值：

```
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

步骤 3 将 LDAP 属性映射关联到 AAA 服务器。

a) 进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

b) 关联您创建的属性映射 tunneling_protocols：

```
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

步骤 4 验证属性映射是否按配置工作。

尝试使用无客户端 SSL 的连接，用户应接到通知，告知其未经授权的连接机制是连接失败的原因。IPSec 客户端应该可以连接，因为根据属性映射，IPsec 是允许的隧道协议。

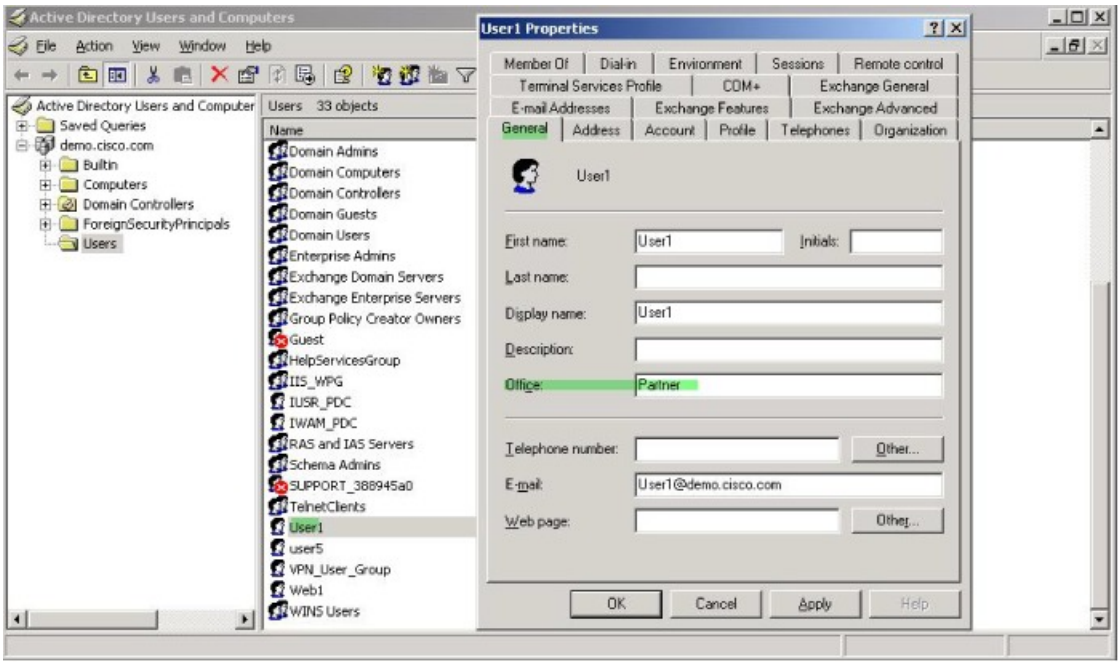
实施登录时长和时间规则

以下示例展示如何配置和实施允许无客户端 SSL 用户（例如业务合作伙伴）访问网络的时长。

在 AD 服务器上，使用 Office 字段输入合作伙伴的名称，该字段使用 physicalDeliveryOfficeName 属性。然后我们在 ASA 上创建一个可将该属性映射至思科属性 Access-Hours 的属性映射。在身份验证过程中，ASA 会检索 physicalDeliveryOfficeName 的值，并将其映射至 Access-Hours。

过程

步骤 1 选择用户，右键点击**属性 (Properties)**，然后打开**常规 (General)** 选项卡：



步骤 2 创建属性映射。

创建属性映射 access_hours，并将 Office 字段使用的 AD 属性 physicalDeliveryOfficeName 映射至思科属性 Access-Hours。

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

步骤 3 将 LDAP 属性映射关联到 AAA 服务器。

进入 AAA 服务器组 MS_LDAP 中的主机 10.1.1.2 的 AAA 服务器主机配置模式，然后关联您创建的属性映射 access_hours：

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

步骤 4 为服务器上允许的每个值配置时间范围。

将合作伙伴访问时长配置为周一至周五上午 9 点到下午 5 点：

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。