用于 AAA 的 LDAP 服务器

本章介绍如何配置 AAA 中使用的 LDAP 服务器。

关于 LDAP 和 ASA

ASA 与大多数 LDAPv3 目录服务器兼容，包括：

- Sun Microsystems JAVA System Directory Server，目前是 Oracle Directory Server Enterprise Edition 的一部分，以前称为 Sun ONE Directory Server
- Microsoft Active Directory
- Novell
- OpenLDAP

默认情况下，ASA 会自动检测其是否连接到 Microsoft Active Directory、Sun LDAP、Novell、OpenLDAP 或通用 LDAPv3 目录服务器。但是，如果自动检测无法确定 LDAP 服务器类型，则可以手动对其进行配置。

身份验证如何与 LDAP 配合使用

在身份验证过程中，ASA 将充当用户的 LDAP 服务器的客户端代理，并以明文形式或通过使用 SASL 协议对 LDAP 服务器执行身份验证。默认情况下，ASA 以明文形式将身份验证参数（通常是用户名和密码）传递到 LDAP 服务器。

ASA 支持以下 SASL 机制，按强度递增的顺序列出：

- Digest-MD5 - ASA 使用从用户名和密码计算的 MD5 值来响应 LDAP 服务器。

• Kerberos - ASA 通过使用 GSSAPI Kerberos 机制发送用户名和领域来响应 LDAP 服务器。

ASA 和 LDAP 服务器支持这些 SASL 机制的任意组合。如果配置多个机制，则 ASA 将检索服务器上配置的 SASL 机制的列表，并将身份验证机制设置为 ASA 和服务器上配置的最强机制。例如，如果 LDAP 服务器和 ASA 支持这两种机制，则 ASA 将选择两者中较强的 Kerberos 机制。

对用户成功执行 LDAP 身份验证后，LDAP 服务器将返回已通过身份验证的用户的属性。对于 VPN 身份验证，这些属性通常包括已应用于 VPN 会话的授权数据。在此情况下，使用 LDAP 即可一步完成身份验证和授权。

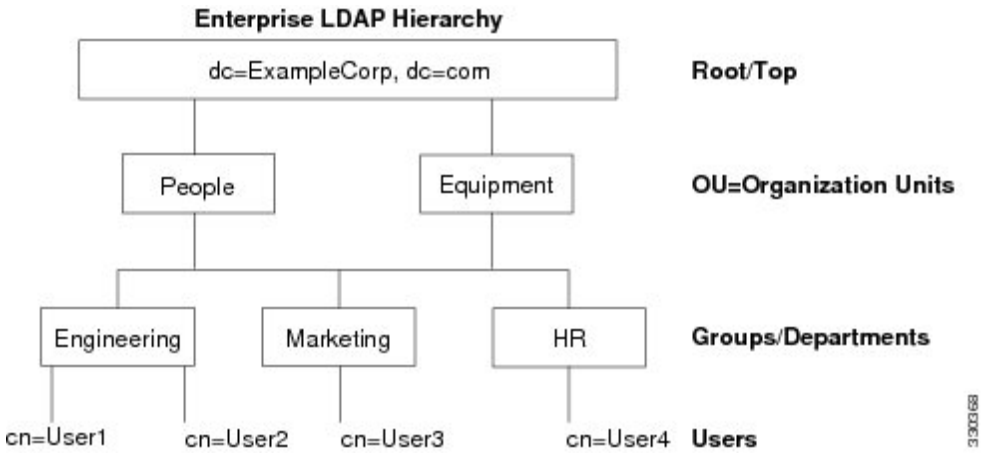
注释 有关 LDAP 协议的详细信息，请参阅 RFC 1777、2251 和 2849。

LDAP 层次结构

您的 LDAP 配置应反映贵组织的逻辑层次结构。例如，假设贵公司 Example Corporation 的一名员工名为 Employee1。Employee1 在 Engineering 组工作。您的 LDAP 层次结构可能有一个或多个级别。您可能决定设置一个单级别层次结构，在其中 Employee1 被视为 Example Corporation 的一名成员。您也可以设置一个多级别层次结构，在其中 Employee1 被视为 Engineering 部门的一名成员，该部门是一个称为 People 的组织单位的成员，而该组织单位本身是 Example Corporation 的成员。有关多级别层次结构的示例，请参阅下图。

虽然多级层次结构包含较多详细信息，但在单级层次结构中搜索结果返回的速度更快。

图 *1:* 多级 *LDAP* 层次结构



搜索 LDAP 层次结构

通过 ASA，可以在 LDAP 层次结构中定制搜索。在 ASA 上配置以下三个字段，以定义在 LDAP 层次结构中开始搜索的位置、搜索范围和查找的信息类型。这些字段共同将层次结构的搜索仅限于包含用户权限的部分。

- LDAP Base DN 定义服务器从 ASA 收到授权请求时应开始在 LDAP 层次结构中搜索用户信息的位置。
- Search Scope 定义在 LDAP 层次结构中的搜索范围。搜索继续在层次结构中 LDAP Base DN 下方的多个级别进行。您可以选择使服务器仅搜索其正下方的级别，否则，它可能搜索整个子树。单级别搜索速度更快，但子树搜索更加广泛。
- Naming Attribute 定义唯一识别 LDAP 服务器中条目的 RDN。常用命名属性可以包括 cn（通用名称）、sAMAccountName 和 userPrincipalName。

该图显示 Example Corporation 的样本 LDAP 层次结构。鉴于该层次结构，您能够以不同的方式定义搜索。下表显示两种样本搜索配置。

在第一个配置示例中，当 Employee1 使用所需的 LDAP 授权建立 IPsec 隧道时，ASA 将向 LDAP 服务器发送一个搜索请求，指明其应在 Engineering 组中搜索 Employee1。此搜索速度很快。

在第二个配置示例中，ASA 发送一个搜索请求，指明服务器应在 Example Corporation 内搜索 Employee1。此搜索需要更长时间。

表 *1:* 搜索配置示例

编号	LDAP Base DN	搜索范围	命名属性	结果
1	group= Engineering,ou=People,dc=ExampleCorporation, dc=com	一个级别	cn=Employee1	搜索速度较快
2	dc=ExampleCorporation,dc=com	子树	cn=Employee1	搜索时间较长

绑定到 LDAP 服务器

ASA 使用登录 DN 和登录密码与 LDAP 服务器建立信任（绑定）。执行 Microsoft Active Directory 只读操作（例如身份验证、授权或组搜索）时，ASA 可以使用权限较少的登录 DN 进行绑定。例如，登录 DN 可能是其 AD“Member Of”指定属于 Domain Users 的一部分的用户。对于 VPN 密码管理操作，登录 DN 需要提升的权限，而且必须是 Account Operators AD 组的一部分。

以下是登录 DN 的一个示例：

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

ASA 支持以下身份验证 方法：

- 在端口 389 上使用未加密密码执行简单 LDAP 身份验证
- 在端口 636 上执行安全 LDAP (LDAP-S)
- 简单身份验证和安全层 (SASL) MD5
- SASL Kerberos

ASA 不支持自治身份验证。

注释 作为 LDAP 客户端，ASA 不支持传输自治绑定或请求。

LDAP 属性映射

ASA 可为以下选项使用 LDAP 目录对用户进行身份验证：

- VPN 远程访问用户
- 防火墙网络访问/直通代理会话
- 设置策略权限（也称为授权属性），例如 ACL、书签列表、DNS 或 WINS 设置，以及会话计时器。
- 在本地组策略中设置关键属性

ASA 使用 LDAP 属性映射将本地 LDAP 用户属性转换为 ASA 属性。您可以将这些属性映射绑定到 LDAP 服务器或将其删除。您还可以显示或清除属性映射。

LDAP 属性映射不支持多值属性。例如，如果用户是多个 AD 组的成员，并且 LDAP 属性映射与多个组匹配，则根据匹配条目的字母顺序选择值。

要正确使用属性映射功能，您需要了解 LDAP 属性名称和值，以及用户定义的属性名称和值。

频繁映射的 LDAP 属性的名称以及经常将其映射到的用户定义属性的类型包括：

- IETF-Radius-Class（ASA 8.2 或更高版本中的 Group_Policy）- 根据目录部门或用户组（例如，Microsoft Active Directory memberOf）属性值设置组策略。组策略属性将 IETF-Radius-Class 属性替换为 ASDM V6.2/ASA V8.2 或更高版本。
- IETF-Radius-Filter-Id - 将访问控制列表或 ACL 应用于 VPN 客户端、IPsec 和 SSL。
- IETF-Radius-Framed-IP-Address - 将已分配的静态 IP 地址分配到 VPN 远程访问客户端、IPsec 和 SSL。
- Banner1 - 在 VPN 远程访问用户登录时显示文本横幅。
- Tunneling-Protocols - 根据访问类型，允许或拒绝 VPN 远程访问会话。

注释 单一 LDAP 属性映射可以包含一个或多个属性。只能从特定 LDAP 服务器映射一个 LDAP 属性。

AAA 的 LDAP 服务器准则

本节包含您在配置 AAA 的 LDAP 服务器之前应检查的准则和限制。

IPv6

AAA 服务器可以使用 IPv4 或 IPv6 地址。

其他准则

- ASA 上配置的用于访问 Sun 目录的 DN 必须可以访问该服务器上的默认密码策略。建议使用目录管理员或具有目录管理员权限的用户作为 DN。或者，也可以将 ACL 放在默认密码策略上。
- 您必须通过 SSL 配置 LDAP，以便对 Microsoft Active Directory 和 Sun 服务器启用密码管理。
- ASA 不支持使用 Novell、OpenLDAP 和其他 LDAPv3 目录服务器进行密码管理。
- 自版本 7.1(x) 开始，ASA 将使用本地 LDAP 机制执行身份验证和授权，而不再需要思科机制。
- 在单模式下可以有最多 200 个服务器组，在多模式下每个情景可以有 4 个服务器组。
- 在单模式下每个组可以有最多 16 个服务器，在多模式下每个组可以有 8 个服务器。
- 当用户登录时，从您在配置中指定的第一个服务器开始，一次访问一个 LDAP 服务器，直到服务器响应为止。如果组中的所有服务器均不可用，在将本地数据库配置为回退方法（仅限管理身份验证和授权）时，ASA 将尝试本地数据库。如果没有回退方法，ASA 将继续尝试 LDAP 服务器。

配置用于 AAA 的 LDAP 服务器

本节介绍如何配置用于 AAA 的 LDAP 服务器。

过程

步骤 1 配置 LDAP 属性映射。请参阅配置 LDAP 属性映射，第 5 页。

步骤 2 添加 LDAP 服务器组。请参阅配置 LDAP 服务器组，第 6 页。

步骤 3 向组中添加服务器，然后配置服务器参数。请参阅向服务器组添加 LDAP 服务器，第 7 页。

配置 LDAP 属性映射

要配置 LDAP 属性映射，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **远程访问 VPN** > **AAA 本地用户** > **LDAP 属性映射**（对于本地用户），或**配置** > **设备管理** > **用户/AAA** > **LDAP 属性映射**（对于所有其他用户），然后点击 **Add**。

Add LDAP Attribute Map dialog 对话框随即显示，其中 **Mapping of Attribute Name** 选项卡处于活动状态。

步骤 2 创建此属性映射的名称。

步骤 3 添加要映射的其中一个 LDAP 属性的名称。

步骤 4 选择思科属性。

步骤 5 点击**添加**。

步骤 6 要映射更多属性，请重复步骤 1 至 5。

步骤 7 点击 **Mapping of Attribute Value** 选项卡以将任何 LDAP 属性的值映射到已映射的思科属性中的新值。

步骤 8 点击 **Add** 以显示 **Add Mapping of Attribute Value** 对话框。

步骤 9 输入您希望从 LDAP 服务器返回的此 LDAP 属性的值。

步骤 10 当此 LDAP 属性包含以前的 LDAP 属性值时，输入要在思科属性中使用的值。

步骤 11 点击**添加**。

步骤 12 要映射更多属性值，请重复步骤 8 至 11。

步骤 13 点击两下 **OK** 以关闭每个对话框。

步骤 14 点击 **Apply** 以将设置保存到运行配置。

配置 LDAP 服务器组

要创建和配置 LDAP 服务器组，然后向该组中添加 LDAP 服务器，请执行以下步骤：

开始之前

您必须先添加属性映射，然后才能向 LDAP 服务器组中添加 LDAP 服务器。

过程

步骤 1 依次选择**配置** > **设备管理** > **用户/AAA** > **AAA 服务器组**，或**配置** > **远程访问 VPN** > **AAA/本地用户** > **AAA 服务器组**（对于 VPN 用户）。

步骤 2 点击 **Add**。

系统将显示 **Add AAA Server Group** 对话框。

步骤 3 输入 AAA 服务器组的名称。

步骤 4 从 **Protocol** 下拉列表中选择 LDAP 服务器类型。

步骤 5 点击要使用的重新激活模式的对应单选按钮（**Depletion** 或 **Timed**）。

在 Depletion 模式下，只有在组中所有服务器都处于非活动状态后，故障服务器才重新激活。

在 Timed 模式下，故障服务器会在 30 秒停机时间后被重新激活。

a) 如果选择 Depletion 重新激活模式，请在 **Dead Time** 字段中输入时间间隔。

Dead Time 是从禁用组中的最后一个服务器到随后重新启用所有服务器所经过的时间，以分钟为单位。仅当配置回退到本地数据库时，失效时间时间才适用；身份验证将在本地尝试，直到失效时间结束。

步骤 6 添加允许的失败AAA事务的最大数量。

此选项设置在宣布无响应服务器为非活动状态之前允许的失败连接尝试次数。

步骤 7 点击 **OK**。

系统将关闭 **Add AAA Server Group** 对话框，并会将新服务器组添加到 AAA 服务器组。

步骤 8 点击 **Apply** 以将更改保存到运行配置。

向服务器组添加 LDAP 服务器

要向服务器组中添加 LDAP 服务器，请执行以下步骤：

过程

步骤 1 选择以下其中一个选项：

- **Configuration Remote Access VPN AAA/Local Users AAA Server Groups**（对于 VPN 用户）。
- **Configuration >Device Management > Users/AAA > AAA Server Groups**

步骤 2 选择要向其添加服务器的服务器组，然后点击 **Add**。

系统将针对选定服务器组显示 **Add AAA Server** 对话框。

步骤 3 选择连接到 LDAP 服务器的接口的名称。

步骤 4 输入 LDAP 服务器的服务器名称或 IP 地址。

步骤 5 添加超时值或保留默认值。超时是ASA在将请求发送至备份服务器之前从主服务器等待该请求的时长（以秒为单位）。

步骤 6 在 **LDAP Parameters for authentication/authorization** 区域中，配置以下设置：

- **Enable LDAP over SSL**（也称为安全 LDAP 或 LDAP-S）- 如果要使用 SSL 保护 ASA 与 LDAP 服务器之间的通信，请选中此复选框。

  注释 如果未配置 SASL 协议，则强烈建议通过 SSL 来保护 LDAP 通信。

- **引用身份名称**- 输入引用身份名称以验证 LDAP 服务器身份。
- **Server Port** - 输入 TCP 端口号 389，ASA 使用该端口访问 LDAP 服务器进行简单（非安全）身份验证；或输入 TCP 端口 636 以进行安全身份验证 (LDAP-S)。所有 LDAP 服务器都支持身份验证和授权。仅 Microsoft AD 和 Sun LDAP 服务器另行提供 VPN 远程访问密码管理功能，该功能需要 LDAP-S。

- **Server Type** - 从下拉列表中指定 LDAP 服务器类型。可用选项包括：
  - **Detect Automatically/Use Generic Type**
  - **Microsoft**
  - **Novell**
  - **OpenLDAP**
  - **Sun，现在是 Oracle Directory Server Enterprise Edition 的一部分**
- **Base DN** - 在 LDAP 层次结构中输入基准可分辨名称 (DN) 或服务器在收到 LDAP 请求（例如，OU=people, dc=cisco, dc=com）时应开始搜索的位置。
- **Scope** - 指定服务器在收到来自下拉列表中的授权请求时应在 LDAP 层次结构中执行搜索的范围。可提供以下选项：
  - **One Level** - 仅搜索 Base DN 以下的一个级别。此选项速度更快。
  - **All Levels** - 搜索 Base DN 以下的所有级别（即搜索整个子树层次结构）。此选项需要更长的时间。
- **Naming Attribute(s)** - 输入唯一识别 LDAP 服务器上的某个条目的相对可分辨名称属性。常用命名属性为通用名称 (CN)、sAMAccountName、userPrincipalName 和用户 ID (uid)。
- **Login DN and Login Password** - ASA 使用登录 DN 和登录密码与 LDAP 服务器建立信任（绑定）。指定登录密码，该密码是登录 DN 用户帐户的密码。
- **LDAP Attribute Map** - 选择所创建的供该 LDAP 服务器使用的属性映射之一。这些属性映射将 LDAP 属性名称映射到思科属性名称和值。
- **SASL MD5 authentication** - 该选项使 SASL 的 MD5 机制能够对 ASA 与 LDAP 服务器之间的通信进行身份验证。
- **SASL Kerberos authentication** - 使 SASL 的 Kerberos 机制能够对 ASA 与 LDAP 服务器之间的通信进行安全身份验证。您必须已定义 Kerberos 服务器，才能启用该选项。
- **LDAP Parameters for Group Search** - 该区域中的字段配置 ASA 向 AD 组提出请求的方式。
  - **Group Base DN** - 指定在 LDAP 层次结构中开始搜索 AD 组（即 memberOf 枚举列表）的位置。如果未配置此字段，ASA 将使用基础 DN 执行 AD 组检索。ASDM 使用检索到的 AD 组列表定义动态访问策略的 AAA 选择条件。如需了解更多信息，请参阅 **show ad-groups** 命令。
  - **Group Search Timeout** - 指定等待来自 AD 服务器（已查询来获取可用组）的响应的最长时间。
- **LDAP SSL 客户端证书/客户端身份证书信任点**- 如果启用基于 SSL 的 LDAP，则可以选择 ASA 客户端应提供给 LDAP 服务器进行身份验证的证书信任点。如果将 LDAP 服务器配置为对客户端证书进行身份验证，则需要信任点。如果不配置证书，当 LDAP 服务器要求时，ASA 不会提

供证书。如果 LDAP 服务器配置为需要对等证书，则安全 LDAP 会话将无法完成，并且身份验证/授权请求将失败。

步骤 7 点击 **OK**。

系统将关闭 **Add AAA Server** 对话框，并会将 AAA 服务器添加到 AAA 服务器组。

步骤 8 点击 **Apply** 以将更改保存到运行配置。

测试 LDAP 服务器身份验证和授权

要确定 ASA 是否可以联系 LDAP 服务器并对用户进行身份验证或授权，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **用户/AAA** > **AAA 服务器组**。

步骤 2 选择服务器驻留所在的服务器组。

步骤 3 选择要测试的服务器。

步骤 4 点击 **Test**。

系统将针对所选服务器显示 **Test AAA Server** 对话框。

步骤 5 点击要执行的测试的类型 - **Authentication** 或 **Authorization**。

步骤 6 输入用户名。

步骤 7 如果要测试身份验证，请输入该用户名的密码。

步骤 8 点击 **OK**。

ASA 将向服务器发送身份验证或授权测试消息。如果测试失败，系统会显示错误消息。

监控用于 AAA 的 LDAP 服务器

有关监控用于 AAA 的 LDAP 服务器的信息，请参阅以下命令：

- **Monitoring > Properties > AAA Servers**

  此窗格显示已配置的 AAA 服务器统计信息。

- **Tools > Command Line Interface**

  您可以在此窗格中发出各种非交互式命令并查看结果。

用于 AAA 的 LDAP 服务器的历史记录

表 *2: AAA* 服务器的历史记录

功能名称	平台版本	说明
用于 AAA 的 LDAP 服务器	7.0(1)	LDAP 服务器介绍对 AAA 的支持以及如何配置 LDAP 服务器。 引入了以下屏幕： Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Remote Access VPN > AAA Local Users > LDAP Attribute Map。
用于 AAA 的使用 IPv6 地址的 LDAP 服务器	9.7(1)	现在可以将 IPv4 或 IPv6 地址用于 AAA 服务器。
每个组的 AAA 服务器组和服务器的数量上限都增加了。	9.13(1)	您可以配置更多 AAA 服务器组。在单情景模式下，您可以配置 200 AAA 服务器组（前一个限制为100）。在多情景模式下，您可以配置 8（前一个限制为4个）。 此外，在多情景模式下，您可以每组配置 8 个服务器（每个组的前一个限制为 4 个服务器）。单情景模式的每组限制 16，保持不变。 修改了 AAA 屏幕以接受这些新的限制。
相互 LDAPS 身份验证。	9.18(1)	您可以为 ASA 配置客户端证书，以便在请求证书进行身份验证时提供给 LDAP 服务器。此功能在通过 SSL 使用 LDAP 时适用。如果 LDAP 服务器配置为需要对等证书，则安全 LDAP 会话将无法完成，并且身份验证/授权请求将失败。 我们修改了以下菜单： **配置** > **设备管理** > **用户/AAA** > > **AAA 服务器组**, 添加/编辑 LDAP 服务器。

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。