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

思科 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。

如何使用 LDAP 进行身份验证

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。

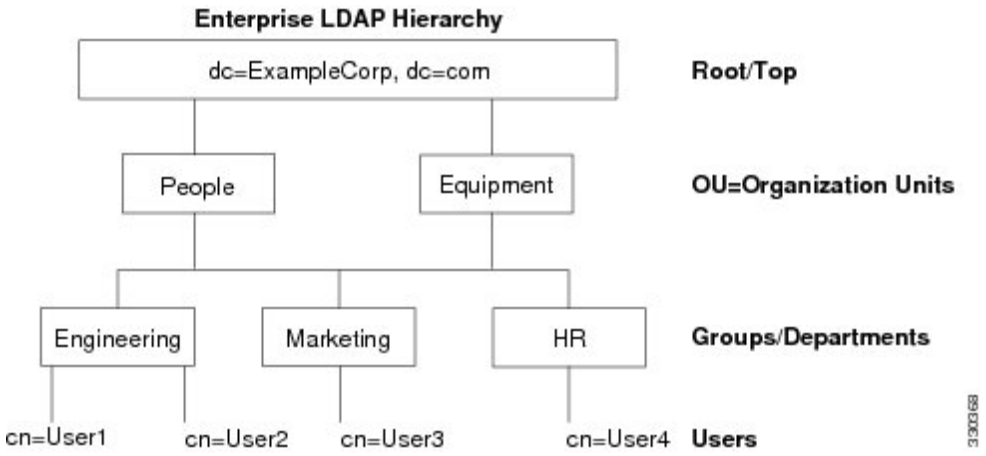
注释 有关 LDAP 协议的详细信息，请参阅 RFC 1777、2251 和 2849。

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 用户属性转换为思科 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 服务器指南

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。

其他规定

- 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 7 页。

步骤 3 （可选）从 LDAP 服务器中配置独立和不同于身份验证机制的授权。请参阅使用 LDAP 为 VPN 配置授权，第 10 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 创建未填充的 LDAP 属性映射表。

ldap-attribute-map *map-name*

示例：

```
ciscoasa(config)# ldap-attribute-map att_map_1
```

步骤 2 将用户定义的属性名称部门映射到思科属性。

map-name *user-attribute-name Cisco-attribute-name*

示例：

```
ciscoasa(config-ldap-attribute-map)# map-name department IETF-Radius-Class
```

步骤 3 将用户定义的映射值部门映射到用户定义的属性值和思科属性值。

map-value *user-attribute-name Cisco-attribute-name*

示例：

```
ciscoasa(config-ldap-attribute-map)# map-value department Engineering group1
```

步骤 4 确定服务器及其所属的 AAA 服务器组。

aaa-server *server_group* [*interface_name*] **host** *server_ip*

示例：

```
ciscoasa(config)# aaa-server ldap_dir_1 host 10.1.1.4
```

步骤 5 将属性映射绑定到 LDAP 服务器。

ldap-attribute-map *map-name*

示例：

```
ciscoasa(config-aaa-server-host)# ldap-attribute-map att_map_1
```

示例

下列显示如何基于名为 accessType 的 LDAP 属性将管理会话限制到 ASA。accessType 属性可能具有下列值之一：

- VPN

- admin
- helpdesk

下列显示每个值与 ASA 支持的其中一个有效 IETF-Radius-Service-Type 属性的对应关系：remote-access（服务类型 5）Outbound、admin（服务类型 6）Administrative 和 nas-prompt（服务类型 7）NAS Prompt。

```
ciscoasa(config)# ldap attribute-map MGMT
ciscoasa(config-ldap-attribute-map)# map-name accessType IETF-Radius-Service-Type
ciscoasa(config-ldap-attribute-map)# map-value accessType VPN 5
ciscoasa(config-ldap-attribute-map)# map-value accessType admin 6
ciscoasa(config-ldap-attribute-map)# map-value accessType helpdesk 7

ciscoasa(config-ldap-attribute-map)# aaa-server LDAP protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 10.1.254.91
ciscoasa(config-aaa-server-host)# ldap-base-dn CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-password test
ciscoasa(config-aaa-server-host)# ldap-login-dn CN=Administrator,CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# server-type auto-detect
ciscoasa(config-aaa-server-host)# ldap-attribute-map MGMT
```

以下示例说明如何显示思科 LDAP 属性名称的完整列表：

```
ciscoasa(config)# ldap attribute-map att_map_1
ciscoasa(config-ldap-attribute-map)# map-name att_map_1?

ldap mode commands/options:
cisco-attribute-names:
  Access-Hours
  Allow-Network-Extension-Mode
  Auth-Service-Type
  Authenticated-User-Idle-Timeout
  Authorization-Required
  Authorization-Type
 :
 :
  X509-Cert-Data
ciscoasa(config-ldap-attribute-map)#
```

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 确定服务器组名称和协议。

aaa-server *server_tag* **protocol ldap**

示例：

```
ciscoasa(config)# aaa-server servergroup1 protocol ldap
ciscoasa(config-aaa-server-group)#
```

当您输入 **aaa-server protocol** 命令时，系统将会进入 aaa-server 组配置模式。

步骤 2 指定在尝试下一服务器前，会向组中带有 LDAP 服务器的失败的 AAA 事务最大数量发送的请求的最大数量。

max-failed-attempts 编号

示例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 参数的范围为 1 至 5。默认值为 3。

如已使用本地数据库（仅限管理访问）配置了回退方法来配置回退机制，并且组中的所有服务器均无法响应，或其响应无效，则将该组视为无响应，并会尝试回退方法。该服务器组会在10分钟（默认值）内保持标记为无响应，以确保该时段内其他AAA请求不会尝试联系该服务器组，而是立即使用回退方法。要更改默认的无响应期间，请参阅下一步中的 **reactivation-mode** 命令。

如果没有回退方法，则 ASA 将继续重试该组中的服务器。

步骤 3 指定用于重新激活组中的故障服务器的方法（重新激活策略）。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

示例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

depletion 关键字用于仅在组中的所有服务器都处于非活动状态后才重新激活故障服务器。

deadtime *minutes* 关键字参数对用于指定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，范围介于 0 到 1440（以分钟为单位）之间。默认值为 10 分钟。

timed 关键字用于在 30 秒的停机时间后重新激活故障服务器。

步骤 4 识别 LDAP 服务器以及其所属的 AAA 服务器组。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

示例：

```
ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1
```

如果不指定 **(***interface_name***)**，则 ASA 默认使用**内部**接口。

当您输入 **aaa-server host** 命令时，系统将会进入 aaa-server 主机配置模式。根据需要，请使用主机配置模式命令进一步配置 AAA 服务器。

下表列出了可用于 LDAP 服务器的命令，以及新的 LDAP 服务器定义是否具有该命令的默认值。如果未提供默认值（以“-”表示），请使用命令指定该值。

表 2: 主机模式命令和默认值

命令	默认值	说明
ldap-attribute-map	-	-
ldap-base-dn	-	-
ldap-login-dn	-	-
ldap-login-password	-	-
ldap-naming-attribute	-	-
ldap-over-ssl	636	如果未设置，则 ASA 将 sAMAccountName 用于 LDAP 请求。无论是使用 SASL 还是明文，都可以通过 SSL 来保护 ASA 与 LDAP 服务器之间的通信。如果未配置 SASL，则强烈建议通过 SSL 来保护 LDAP 通信。
ldap-scope	-	-
sasl-mechanism	-	-
server-port	389	-
server-type	autodiscovery	如果自动检测无法确定 LDAP 服务器类型，并且您知道服务器是 Microsoft、Sun 或通用 LDAP 服务器，则可以手动配置服务器类型。
timeout	10 秒	-

示例

以下示例说明如何配置名为 watchdogs 的 LDAP 服务器组并向该组中添加 LDAP 服务器。由于示例未定义重试间隔或 LDAP 服务器侦听的端口，因此 ASA 使用这两个服务器特定参数的默认值。

```
ciscoasa(config)# aaa-server watchdogs protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

使用 LDAP 为 VPN 配置授权

成功进行 LDAP 用户身份验证以进行 VPN 访问后，ASA 将查询 LDAP 服务器，服务器将返回 LDAP 属性。这些属性通常包括应用于 VPN 会话的授权数据。以这种方式使用 LDAP 可一步完成身份验证和授权。

但是，有些情况下可能需要获得与身份验证机制分开而且不同的 LDAP 目录服务器的授权。例如，如果使用 SDI 或证书服务器执行身份验证，则不返回授权信息。对于这种情况下的用户授权，您可在身份验证成功后查询 LDAP 目录，分两步完成身份验证和授权。

如要使用 LDAP 设置 VPN 用户授权，请执行以下步骤。

过程

步骤 1 创建一个名为 remotegrp 的 IPsec 远程访问隧道组。

tunnel-group *groupname*

示例：

```
ciscoasa(config)# tunnel-group remotegrp
```

步骤 2 将服务器组和隧道组进行关联。

tunnel-group *groupname* **general-attributes**

示例：

```
ciscoasa(config)# tunnel-group remotegrp general-attributes
```

步骤 3 将新隧道组分配到先前创建的 AAA 服务器组以进行授权。

authorization-server-group *group-tag*

示例：

```
ciscoasa(config-general)# authorization-server-group ldap_dir_1
```

示例

虽然有可用于特定要求的其他授权相关命令和选项，但以下示例说明用于使用 LDAP 进行用户授权的命令。然后，示例将创建一个名为 remote-1 的 IPsec 远程访问隧道组，并将新隧道组分配到先前创建的 ldap_dir_1 AAA 服务器组以进行授权：

```
ciscoasa(config)# tunnel-group remote-1 type ipsec-ra
ciscoasa(config)# tunnel-group remote-1 general-attributes
ciscoasa(config-general)# authorization-server-group ldap_dir_1
```

```
ciscoasa(config-general)#
```

在完成此配置工作后，接着您可以通过输入以下命令，配置其他的 LDAP 授权参数，如目录密码、搜索目录的起点和目录搜索的范围：

```
ciscoasa(config)# aaa-server ldap_dir_1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
ciscoasa(config-aaa-server-host)# ldap-login-dn obscurepassword
ciscoasa(config-aaa-server-host)# ldap-base-dn starthere
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)#
```

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：

- **show aaa-server**

  此命令显示已配置的 AAA 服务器统计信息。使用 **clear aaa-server statistics** 命令可清除 AAA 服务器统计信息。

- **show running-config aaa-server**

  此命令可显示 AAA 服务器运行配置。使用 **clear configure aaa-server** 命令可清除 AAA 服务器配置。

用于 AAA 的 LDAP 服务器的历史记录

表 *3: 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。 引入了以下命令： **username**、**aaa authorization exec authentication-server**、**aaa authentication console LOCAL**、**aaa authorization exec LOCAL**、**service-type**、**ldap attribute-map**、**aaa-server protocol**、**aaa authentication telnet | ssh | serial} console LOCAL**、**aaa authentication http console LOCAL**、**aaa authentication enable console LOCAL**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**authorization-server-group**、**tunnel-group**、**tunnel-group general-attributes**、**map-name**、**map-value**、**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。 修改了以下命令以接受这些新限制：**aaa-server**、**aaa-server host**。