与 LDAP 集成

本章包含以下部分：

概述

如果您在公司 LDAP 目录（例如，Microsoft Active Directory、SunONE Directory Server 或 OpenLDAP 目录）中维护最终用户口令和邮件别名，可以使用 LDAP 目录对以下用户进行身份验证：

- 访问垃圾邮件隔离区的最终用户和管理用户。

  当用户登录到垃圾邮件隔离区的网络 UI 时，LDAP 服务器会验证登录名和口令，AsyncOS 会检索相应邮件别名的列表。发送到用户的任何一个邮件别名的被隔离邮件可以出现在垃圾邮件隔离区中，只要设备不重写这些邮件即可。

  请参阅将 LDAP 配置为与垃圾邮件隔离区配合使用, on page 1。

- 启用并配置外部身份验证后，登录到思科 安全邮件和 Web 管理器设备的管理用户。

  请参阅使用 LDAP 配置管理用户的外部身份验证 , on page 14。

将 LDAP 配置为与垃圾邮件隔离区配合使用

配置思科内容安全设备以与 LDAP 目录配合使用时，必须完成以下步骤以进行接受、路由、别名和伪装设置：

步骤 1 **配置 LDAP 服务器配置文件**。

服务器配置文件包含使 AsyncOS 能够连接到 LDAP 服务器的信息，例如：

- 服务器名称和端口
- 基本 DN
- 用于绑定到服务器的身份验证要求

有关配置服务器配置文件的详细信息，请参阅创建 LDAP 服务器配置文件, on page 2。

在创建 LDAP 服务器配置文件时，您可以配置 AsyncOS 以连接到多台 LDAP 服务器。有关详细信息，请参阅将 AsyncOS 配置为与多个 LDAP 服务器配合使用, on page 12。

步骤 2 **配置 LDAP 查询**。

您可以使用为 LDAP 服务器配置文件生成的默认垃圾邮件隔离区，或自行创建针对您的特定 LDAP 实施和架构量身定制的查询。然后，您可以指定垃圾邮件通知的活动查询和最终用户对隔离区的访问权限。

有关查询的信息，请参阅配置 LDAP 查询, on page 4。

步骤 3 **为垃圾邮件隔离区启用 LDAP 最终用户访问权限和垃圾邮件通知**。

启用 LDAP 最终用户对垃圾邮件隔离区的访问权限，以使最终用户可以查看和管理其隔离区中的邮件。您还可以为垃圾邮件通知启用别名合并，以防止用户接收多个通知。

有关详细信息，请参阅设置集中垃圾邮件隔离区。

创建 LDAP 服务器配置文件

配置 AsyncOS 以使用 LDAP 目录时，您需要创建 LDAP 服务器配置文件来存储有关 LDAP 服务器的信息。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 2 依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > LDAP**。

步骤 3 点击**添加 LDAP 服务器配置文件 (Add LDAP Server Profile)**。

步骤 4 在 **LDAP 服务器配置文件名称 (LDAP Server Profile Name)** 文本字段中输入服务器配置文件的名称。

步骤 5 在**主机名 (Host Name[s])** 文本字段中输入 LDAP 服务器的主机名。

可以输入多个主机名以配置用于故障转移或负载均衡的 LDAP 服务器。使用逗号分隔多个条目。有关详细信息，请参阅将 AsyncOS 配置为与多个 LDAP 服务器配合使用, on page 12。

步骤 6 选择身份验证方法。您可以使用匿名身份验证或指定用户名口令。

Note 您需要配置 LDAP 身份验证，以在报告上查看客户端用户 ID 而不是客户端 IP 地址。如果没有 LDAP 身份验证，系统只能通过用户的 IP 地址指代用户。选择**使用口令**单选按钮，然后输入用户名和口令。用户名将随即显示在用户邮件摘要页面上。

步骤 7 选择 LDAP 服务器类型：Active Directory、OpenLDAP 或“未知或其他 (Unknown or Other)”。

步骤 8 输入端口号。

默认端口为 `3268`。这是 Active Directory 的默认端口，用于在多服务器环境中访问全局目录。

步骤 9 输入 LDAP 服务器的基本 DN（可区别名称）。

如果通过用户名和口令进行身份验证，则用户名必须包含具有该口令的条目的完整 DN。例如，邮件地址为 `joe@example.com` 的用户是营销部门的用户。此用户的条目类似于以下条目：

```
uid=joe, ou=marketing, dc=example dc=com
```

- [可选 - 仅当在“LDAP 全局设置”(LDAP Global Settings) 中启用了“验证 LDAP 服务器证书”(Validate LDAP Server Certificate) 时]：检查是否上传了自定义证书颁发机构以验证服务器证书。
- 要添加证书颁发机构，请在 CLI 中使用 certconfig > CERTAUTHORITY 子命令。[可选 - 仅当在“LDAP 全局设置”(LDAP Global Settings) 中启用了“验证 LDAP 服务器证书”(Validate LDAP Server Certificate) 并在“SSL 配置”(SSL Configuration) 设置中启用了“FQDN 验证”(FQDN validation) 时]：检查服务器证书中是否存在“公共名称”(Common Name)、“SAN：DNS 名称”(SAN: DNS Name) 字段或两者同时存在，以及是否为 FQDN 格式。
- [可选 - 仅当在“LDAP 全局设置”(LDAP Global Settings) 中启用了“验证 LDAP 服务器证书”(Validate LDAP Server Certificate) 时]：检查服务器证书的“公共名称”(Common Name)、“SAN：DNS 名称”(SAN: DNS Name) 字段是否包含服务器的主机名。如果在“主机名”(Hostname) 字段中配置了 IP，则使用“反向 DNS”(Reverse DNS) 名称。
- [可选 - 仅当在“LDAP 全局设置”(LDAP Global Settings) 页面中启用了“验证 LDAP 服务器证书”(Validate LDAP Server Certificate) 时，并且在“SSL 配置”(SSL Configuration) 设置页面中启用了 X 509 验证]：检查服务器证书的签名算法。
- [可选 - 仅当在“LDAP 全局设置”(LDAP Global Settings) 页面中启用了“验证 LDAP 服务器证书”(Validate LDAP Server Certificate) 时]：检查“公共名称”(Common Name) 中是否存在服务器名称，或者服务器证书中是否存在“SAN：DNS 名称”(SAN: DNS Name) 字段。
- [可选 - 仅当在“LDAP 全局设置”(LDAP Global Settings) 页面中启用了“验证 LDAP 服务器证书”(Validate LDAP Server Certificate) 时：检查服务器证书版本。

  Note 仅允许使用版本 1 和版本 3 服务器证书。

步骤 10 在“高级”(Advanced) 下，选择是否在与 LDAP 服务器通信时使用 SSL。

步骤 11 输入缓存生存时间。此值表示保留缓存的时长。

步骤 12 输入保留缓存条目的最大数量。

步骤 13 输入最大并发连接数。

如果您为进行负载均衡配置 LDAP 服务器配置文件，这些连接会分布在已列出的 LDAP 服务器上。例如，如果配置 10 个并发连接并且通过三台服务器对连接进行负载均衡，则 AsyncOS 会与每台服务器建立 10 个连接，总共建立 30 个连接。有关详细信息，请参阅负载均衡, on page 13。

Note 最大并发连接数包括用于 LDAP 查询的 LDAP 连接。但是，如果您为垃圾邮件隔离区启用 LDAP 身份验证，设备会为最终用户隔离区额外分配 20 个连接，连接总数达到 30 个。

步骤 14 通过点击“测试服务器”(Test Server) 按钮测试服务器连接。如果您指定了多个 LDAP 服务器，则这些服务器都会进行测试。测试结果显示在“连接状态”(Connection Status) 字段中。有关详细信息，请参阅测试 LDAP 服务器, on page 4。

步骤 15 通过选中复选框并填写字段来创建垃圾邮件隔离区查询。

您可以配置隔离区最终用户身份验证查询，以便在用户登录到最终用户隔离区时验证用户。您可以配置别名合并查询，以便最终用户无需为每个邮件别名接收隔离区通知。要使用这些查询，请选中“指定为活动查询”(Designate as the active query) 复选框。有关详细信息，请参阅配置 LDAP 查询, on page 4。

步骤 16 通过点击“测试查询”(Test Query) 按钮测试垃圾邮件隔离区查询。

输入测试参数并点击“运行测试”(Run Test)。测试结果显示在“连接状态”(Connection Status) 字段中。如果对查询定义或属性进行任何更改，请点击**更新 (Update)**。

Note 如果已将 LDAP 服务器配置为允许绑定空口令，则查询可以使用空口令字段通过测试。

步骤 17 提交并确认更改。

对于 Windows 2000，Active Directory 服务器配置不允许通过 TLS 进行身份验证。这是一个已知的 Active Directory 问题。Active Directory 和 Windows 2003 的 TLS 身份验证确实有效。

Note 虽然服务器配置的数量不受限制，但是您只能为每台服务器配置一个最终用户身份验证查询和一个别名合并查询。

测试 LDAP 服务器

使用“添加/编辑 LDAP 服务器配置文件”(Add/Edit LDAP Server Profile) 页面上的“测试服务器”按钮（或 CLI 中 ldapconfig 命令的 test 子命令）测试与 LDAP 服务器的连接。AsyncOS 随即显示一条消息，说明到服务器端口的连接是成功还是失败。如果配置了多台 LDAP 服务器，则 AsyncOS 会测试每台服务器并显示各个测试结果。

配置 LDAP 查询

以下部分提供各类垃圾邮件隔离区查询的默认查询字符串和配置详细信息：

- **垃圾邮件隔离区最终用户身份验证查询**。有关详细信息，请参阅垃圾邮件隔离区最终用户身份验证查询, on page 6。
- **垃圾邮件隔离区别名整合查询**。有关详细信息，请参阅垃圾邮件隔离区别名整合查询, on page 7。

要让隔离区将 LDAP 查询用于最终用户访问权限或垃圾邮件通知，请选中“指定为活动查询”(Designate as the active query) 复选框。您可以指定一个最终用户身份验证查询以控制隔离区访问权限，并且可以为垃圾邮件通知指定一个别名合并查询。任何现有的活动查询都会被禁用。在安全管理设备上，选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > LDAP** 页面，有效查询旁边会显示一个星号 (*)。

您还可以将基于域的查询或链式查询指定为活动的最终用户访问权限或垃圾邮件通知查询。有关详细信息，请参阅基于域的查询, on page 9和链查询, on page 10。

Note 使用“LDAP”页面上的“测试查询”(Test Query) 按钮（或 **ldaptest** 命令）验证查询是否返回了预期结果。

- LDAP 查询语法, on page 5
- 令牌, on page 5

LDAP 查询语法

允许 LDAP 路径中使用空格，而且不需要使用引号。CN 和 DC 语法不区分大小写。

Cn=First Last,oU=user,dc=domain,DC=COM

为查询输入的变量名称区分大小写，且必须与您的 LDAP 实施相匹配才可以正常工作。例如，在提示符中输入 **mailLocalAddress** 执行的查询不同于输入 **maillocaladdress** 执行的查询。

令牌

您可以在 LDAP 查询中使用以下令牌：

- {a} 用户名@域名
- {d} 域
- {dn} 可区别名称
- {g} 组名
- {u} 用户名
- {f} MAILFROM：地址

Note {f} 令牌仅在接受查询中有效。

例如，您可以使用以下查询接受 Active Directory LDAP 服务器的邮件：
(|(mail={a})(proxyAddresses=smtp:{a}))

Note 在侦听程序上启用 LDAP 功能之前，我们强烈建议使用 LDAP 页面的测试功能（或 **ldapconfig** 命令的 **test** 子命令）测试您构建的所有查询并确保返回预期的结果。有关详细信息，请参阅 测试 LDAP 查询, on page 9。

垃圾邮件隔离区最终用户身份验证查询

最终用户身份验证查询会在用户登录到垃圾邮件隔离区时验证用户。令牌 {u} 指定了该用户（它表示用户的登录名）。令牌 {a} 指定用户的邮件地址。LDAP 查询不会从邮件地址中删除“SMTP:”；AsyncOS 会删除地址的该部分。

根据服务器类型，AsyncOS 会将以下默认查询字符串之一用于最终用户身份验证查询：

- **Active Directory**：(sAMAccountName={u})
- OpenLDAP：(uid={u})
- **未知或其他**：[空白]

默认情况下，主邮件属性是 **mail**。您可以输入自己的查询和邮件属性。要在 CLI 中创建查询，请使用 **ldapconfig** 命令的 isqauth 子命令。

Note 如果您希望用户使用其完整的邮件地址登录，请为查询字符串使用 (mail=smtp:{a})。

Active Directory 最终用户身份验证设置示例

本部分介绍 Active Directory 服务器和最终用户身份验证查询设置示例。此示例为 Active Directory 服务器使用口令进行的身份验证，为 Active Directory 服务器的最终用户身份验证使用默认查询字符串，并使用邮件和 proxyAddresses 邮件属性。

Table 1: LDAP* 服务器和垃圾邮件隔离区最终用户身份验证设置示例：*Active Directory

身份验证方法	使用口令（需要创建一个低权限用户以绑定用于搜索，或配置匿名搜索。）
服务器类型	Active Directory
端口	3268
基本 DN	[空白]
连接协议	[空白]
查询字符串	(sAMAccountName={u})
邮件属性	mail,proxyAddresses

OpenLDAP 最终用户身份验证设置示例

本部分介绍 OpenLDAP 服务器和最终用户身份验证查询设置示例。此示例为 OpenLDAP 服务器使用匿名身份验证，为 OpenLDAP 服务器的最终用户身份验证使用默认查询字符串，并使用 mail 和 mailLocalAddress 邮件属性。

Table 2: LDAP 服务器和垃圾邮件隔离区最终用户身份验证设置示例：***OpenLDAP***

身份验证方法	匿名
服务器类型	OpenLDAP
端口	389
基本 DN	[空白]（有些旧方案将使用特定基本 DN。）
连接协议	[空白]
查询字符串	(uid={u})
邮件属性	mail,mailLocalAddress

垃圾邮件隔离区别名整合查询

如果您使用垃圾邮件通知，垃圾邮件隔离区别名合并查询会合并邮件别名，以便收件人无需为每个邮件别名接收隔离区通知。例如，收件人可能收到以下邮件地址的邮件：john@example.com、jsmith@example.com 和 john.smith@example.com。使用别名合并时，对于发送给所有用户别名的邮件，收件人将在选定的主要邮件地址收到一条垃圾邮件通知。

要将邮件整合到主邮件地址，请创建查询来搜索收件人的备用邮件别名，然后在“邮件属性 (Email Attribute)”字段中输入收件人的主邮件地址的属性。

对于 Active Directory 服务器，默认查询字符串（可能与您的部署不同或相同）是 (|(proxyAddresses={a})(proxyAddresses=smtp:{a}))，默认邮件属性是 mail。对于 OpenLDAP 服务器，默认查询字符串为 (mail={a})，默认邮件属性为 mail。可以定义自己的查询和邮件属性，包括逗号分隔的多个属性。如果您输入多个邮件属性，思科建议输入一个使用单个值的唯一属性（例如 mail）作为第一个邮件属性，而不是输入一个具有多个可以更改的值的属性，例如 proxyAddresses。

要在 CLI 中创建查询，请使用 ldapconfig 命令的 isqalias 子命令。

- Active Directory 别名整合设置示例, on page 8
- OpenLDAP 别名整合设置示例, on page 8

Active Directory 别名整合设置示例

此部分显示 Active Directory 服务器和别名整合查询的设置示例。此示例将匿名身份验证用于 Active Directory 服务器，将别名整合的查询字符串用于 Active Directory 服务器，并且使用了 mail 邮件属性。

Table 3: LDAP** 服务器和垃圾邮件隔离区别名合并设置示例：**Active Directory

身份验证方法	匿名
服务器类型	Active Directory
端口	3268
基本 DN	[空白]
连接协议	使用 SSL
查询字符串	(|(mail={a})(mail=smtp:{a}))
邮件属性	mail

OpenLDAP 别名整合设置示例

此部分显示 OpenLDAP 服务器和别名整合查询的设置示例。此示例将匿名身份验证用于 OpenLDAP 服务器，将别名整合的查询字符串用于 OpenLDAP 服务器，并且使用了 mail 邮件属性。

Table 4: LDAP** 服务器和垃圾邮件隔离区别名整合设置示例：**OpenLDAP

身份验证方法	匿名
服务器类型	OpenLDAP
端口	389
基本 DN	[空白]（有些旧方案将使用特定基本DN。）
连接协议	使用 SSL
查询字符串	(mail={a}))
邮件属性	mail

测试 LDAP 查询

使用“添加/编辑 LDAP 服务器配置文件”(Add/Edit LDAP Server Profile) 页面上的“测试查询”(Test Query) 按钮（或 CLI 中的 ldaptest 命令）测试您的查询。AsyncOS 显示有关查询连接测试的每个阶段的详细信息。例如，第一阶段 SMTP 授权是已成功还是已失败，BIND 匹配返回的是 True 还是 False 结果。

ldaptest 命令以批处理命令的形式提供，例如：

ldaptest LDAP.isqalias foo@cisco.com

为查询输入的变量名称区分大小写，且必须与您的 LDAP 实施相匹配才可以正常工作。例如，为邮件属性输入 mailLocalAddress 会执行与输入 maillocaladdress 不同的查询。

要测试查询，您必须输入测试参数，然后点击“运行测试”(Run Test)。结果显示在“测试连接”(Test Connection) 字段中。如果最终用户身份验证查询成功，会显示“成功：操作：匹配阳性”(Success: Action: match positive) 结果。对于别名合并查询，会显示“成功：操作：别名合并”(Success: Action: alias consolidation)，以及合并的垃圾邮件通知的邮件地址。如果查询失败，AsyncOS 会显示失败原因，例如找不到匹配的 LDAP 记录，或者匹配的记录不包含邮件属性。如果使用多个 LDAP 服务器，则思科内容安全设备会在每个 LDAP 服务器上测试查询。

基于域的查询

基于域的查询是由类型分组且与域关联的 LDAP 查询。如果不同的 LDAP 服务器与不同的域关联，您可能希望使用基于域的查询，但是您需要为最终用户隔离区访问权限查询您的所有 LDAP 服务器。例如，一家名为 Bigfish 的公司拥有域 Bigfish.com、Redfish.com 和 Bluefish.com，并且该公司为与每个域关联的员工维护不同的 LDAP 服务器。Bigfish 可以使用基于域的查询，根据所有三个域的 LDAP 目录对最终用户进行身份验证。

要使用基于域的查询控制垃圾邮件隔离区的最终用户访问权限或通知，请完成以下步骤：

步骤 1 为您要在基于域的查询中使用的每个域创建 LDAP 服务器配置文件。在每个服务器配置文件中，配置您要在基于域的查询中使用的查询。有关详细信息，请参阅创建 LDAP 服务器配置文件, on page 2。

步骤 2 创建基于域的查询。在创建基于域的查询时，您从每个服务器配置文件中选择查询，并将基于域的查询指定为垃圾邮件隔离区的活动查询。有关创建查询的详细信息，请参阅创建基于域的查询, on page 9。

步骤 3 为垃圾邮件隔离区启用最终用户访问权限或垃圾邮件通知。有关详细信息，请参阅 设置最终用户通过网络浏览器访问垃圾邮件隔离区的权限。

创建基于域的查询

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 2 依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > LDAP**。

步骤 3 在 LDAP 页面上，点击**高级 (Advanced)**。

步骤 4 输入基于域的查询的名称。

步骤 5 选择查询类型。

Note 在创建基于域的查询时，您指定一种查询类型。在您选择查询类型后，查询字段下拉列表包含来自LDAP服务器配置文件的相应查询。

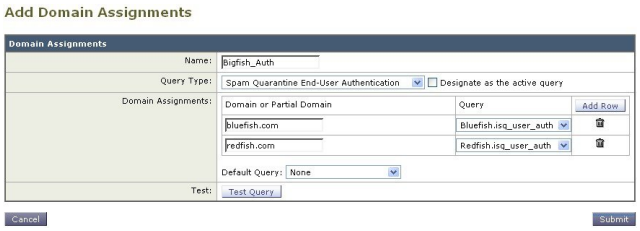
步骤 6 在“域分配 (Domain Assignments)”字段中，输入域。

步骤 7 选择要与域关联的查询。

步骤 8 添加行，并为基于域的查询中的每个域选择查询。

步骤 9 输入在所有其他查询失败时要运行的默认查询。如果您不想输入默认查询，请选择**无 (None)**。

Figure 1: 基于域的查询示例



步骤 10 通过点击“测试查询”(Test Query) 按钮并在测试参数字段中输入要测试的用户登录名和口令或者邮件地址，来测试查询。结果会显示在“连接状态”(Connection Status) 字段中。

步骤 11 如果您希望垃圾邮件隔离区使用基于域的查询，请选中**指定为活动查询**复选框。

Note 基于域的查询成为所指定查询类型的活动LDAP查询。例如，如果基于域的查询用于最终用户身份验证，它将成为垃圾邮件隔离区的活动最终用户身份验证查询。

步骤 12 点击**提交 (Submit)**，然后点击**确认 (Commit)** 确认您所做的更改。

Note 要在命令行界面上执行相同的配置，请在命令行提示符处键入 `ldapconfig` 命令的 `advanced` 子命令。

链查询

链查询是 AsyncOS 连续运行的一系列 LDAP 查询。AsyncOS 运行系列中的每个查询（“链中的每个查询”），直到 LDAP 服务器返回肯定响应或者最终查询返回否定响应或失败。如果 LDAP 目录中的条目使用不同的属性存储相似（或相同）的值，链式查询会非常有用。例如，组织中的各个部门可能使用不同类型的LDAP目录。当销售部门使用 Active Directory 时，IT 部门可能使用 OpenLDAP。要确保查询针对两种类型的 LDAP 目录运行，您可以使用链式查询。

要使用链式查询控制垃圾邮件隔离区的最终用户访问权限或通知，请完成以下步骤：

步骤 1 为您要在链式查询中使用的每个查询创建 LDAP 服务器配置文件。对于每个服务器配置文件，配置要用于链查询的查询。有关详细信息，请参阅创建 LDAP 服务器配置文件, on page 2。

步骤 2 创建链查询并将其指定为垃圾邮件隔离区的活动查询。有关详细信息，请参阅创建链查询, on page 11。

步骤 3 为垃圾邮件隔离区启用 LDAP 最终用户访问权限和垃圾邮件通知。有关垃圾邮件隔离区的详细信息，请参阅设置集中垃圾邮件隔离区。

创建链查询

Tip 您还可以在 CLI 中使用 ldapconfig 命令的 advanced 子命令。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 加载旧 Web 界面。

步骤 2 选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > LDAP > LDAP 服务器 (LDAP Server)**。

步骤 3 从“LDAP 服务器配置文件”(LDAP Server Profiles) 页面，点击**高级 (Advanced)**。

步骤 4 点击**添加链式查询 (Add Chained Query)**。

步骤 5 为链式查询输入名称。

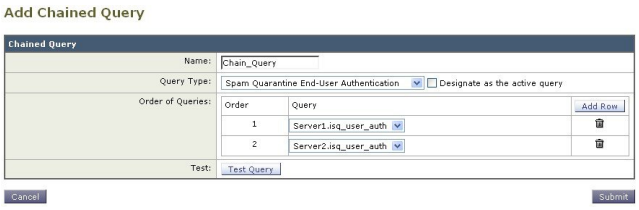
步骤 6 选择查询类型。

当您创建链式查询时，其所有组成查询具有相同的查询类型。在您选择查询类型后，查询字段下拉列表显示来自 LDAP 的相应查询。

步骤 7 选择链中的第一个查询。

思科内容安全设备会按照配置顺序运行查询。如果将多个查询添加到链查询，则可能需要对它们进行排序，以便常规查询在粒度查询之后。

Figure 2: 链式查询示例



步骤 8 通过点击“测试查询”(Test Query) 按钮并在测试参数字段中输入用户登录名和口令或者邮件地址，来测试查询。结果随即会显示在“连接状态”(Connection Status) 字段中。

步骤 9 如果您希望垃圾邮件隔离区使用域查询，请选中**指定为活动查询 (Designate as the active query)** 复选框。

Note 链式查询成为所指定查询类型的活动 LDAP 查询。例如，如果链式查询用于最终用户身份验证，它将成为垃圾邮件隔离区的活动最终用户身份验证查询。

步骤 10 提交并确认更改。

Note 要在命令行界面上执行相同的配置，请在命令行提示符处键入 `ldapconfig` 命令的 `advanced` 子命令。

将 AsyncOS 配置为与多个 LDAP 服务器配合使用

配置 LDAP 服务器配置文件时，可以配置思科内容安全设备以连接到列表中的多个 LDAP 服务器。如果使用多个 LDAP 服务器，它们需要包含相同的信息，具有相同的结构，并且使用相同的身份验证信息。存在可以整合记录的第三方产品。

配置思科内容安全设备以连接到冗余 LDAP 服务器，从而使用以下功能：

- **故障转移**。如果思科内容安全设备无法连接到 LDAP 服务器，它会连接到列表中的下一台服务器。
- **负载均衡**。在执行 LDAP 查询时，思科内容安全设备将在列表中的 LDAP 服务器之间分发连接。

您可以在“管理设备”(Management Appliance) >“系统管理”(System Administration) >“LDAP”页面上或通过使用 CLIldapconfig 命令配置冗余的 LDAP 服务器。

测试服务器和查询

使用“添加 LDAP 服务器配置文件”(Add LDAP Server Profile) 或“编辑 LDAP 服务器配置文件”(Edit LDAP Server Profile) 页面上的测试服务器 (Test Server[s]) 按钮或（CLI 中的 test 子命令）测试到 LDAP 服务器的连接。如果使用多个 LDAP 服务器，AsyncOS 会测试每个服务器，并显示每个服务器的每个结果。AsyncOS 还将测试每个 LDAP 服务器上的查询，并显示每个结果。

故障转移

要确保 LDAP 服务器可用于解析查询，可配置用于故障转移的 LDAP 配置文件。如果与 LDAP 服务器的连接失败，或者查询返回适合这样做的错误，设备会尝试查询列表中指定的下一 LDAP 服务器。

思科内容安全设备会在指定的时间段内尝试连接到 LDAP 服务器列表中的第一台服务器。如果设备无法连接到列表中的第一台 LDAP 服务器，或者查询返回错误，设备会尝试连接到列表中的下一台 LDAP 服务器。默认情况下，设备始终尝试连接到列表中的第一台服务器，而且，会尝试按照列出的顺序连接到后续每台服务器。为确保思科内容安全设备在默认情况下连接到主 LDAP 服务器，请将其输入为 LDAP 服务器列表中的第一台服务器。

Note 只有查询指定 LDAP 服务器的尝试才会进行故障转移。尝试查询与未故障转移的指定的 LDAP 服务器关联的建议或后续服务器。

如果思科内容安全设备连接到第二台或后续的 LDAP 服务器，则会在指定的时间段内保持连接到该服务器。在此时间段结束后，设备会尝试重新连接到列表中的第一台服务器。

为 LDAP 故障切换配置思科内容安全设备

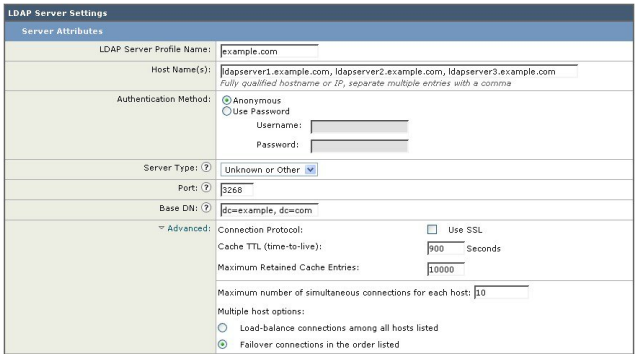
步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 2 依次选择**管理设备 > 系统管理 > LDAP**。

步骤 3 选择您要编辑的 LDAP 服务器配置文件。

在以下示例中，LDAP 服务器名称为 example.com。

***Figure 3: LDAP* 故障切换配置示例**



步骤 4 在“主机名”(Hostname) 文本字段中，键入 LDAP 服务器；例如 **ldapserver.example.com**。

步骤 5 在“每台主机的最大并发连接数”(Maximum number of simultaneous connections for each host) 文本字段中，键入最大连接数。

在本示例中，最大连接数为 **10**。

步骤 6 点击**按列出的顺序对连接进行故障切换 (Failover connections in the order listed)** 旁边的单选按钮。

步骤 7 根据需要配置其他 LDAP 选项。

步骤 8 提交并确认更改。

负载均衡

要在一组 LDAP 服务器中分发 LDAP 连接，可以配置用于负载均衡的 LDAP 配置文件。

使用负载均衡时，思科内容安全设备会在列出的LDAP服务器之间分发连接。如果连接失败或超时，设备会确定哪些 LDAP 服务器可用，并重新连接到可用的服务器。设备根据您配置的最大连接数确定要建立的并发连接数。

如果其中一台所列的 LDAP 服务器未响应，设备将在剩余的 LDAP 服务器之间分发的连接。

为负载均衡配置思科内容安全设备

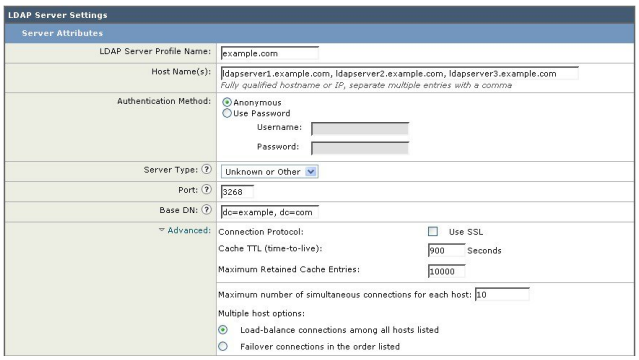
步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 2 依次选择**管理设备 > 系统管理 > LDAP**。

步骤 3 选择您要编辑的 LDAP 服务器配置文件

在以下示例中，LDAP 服务器名称为 example.com。

Figure 4: 负载均衡配置示例



步骤 4 在“主机名”(Hostname) 文本字段中，键入 LDAP 服务器；例如 **ldapserver.example.com**。

步骤 5 在“每台主机的最大并发连接数”(Maximum number of simultaneous connections for each host) 文本字段中，键入最大连接数。

在本示例中，最大连接数为 **10**。

步骤 6 点击**在列出的所有主机之间均衡分配连接的负载 (Load-balance connections among all hosts listed)**。

步骤 7 根据需要配置其他 LDAP 选项。

步骤 8 提交并确认更改。

使用 LDAP 配置管理用户的外部身份验证

可以配置思科内容安全设备以使用网络上的 LDAP 目录对管理用户进行身份验证，方法是允许他们使用 LDAP 用户名和口令登录设备。

步骤 1 **配置 LDAP 服务器配置文件**。请参阅创建 LDAP 服务器配置文件, on page 2。

步骤 2 **创建查询以查找用户账户**。在 LDAP 服务器配置文件的“外部身份验证查询”(External Authentication Queries) 部分，创建一个查询以在 LDAP 目录中搜索用户账户。请参阅用于验证管理用户的用户账户查询 , on page 15。

步骤 3 **创建组成员身份查询**。创建一个查询以确定用户是否是某个目录组的成员，并创建一个单独的查询以查找组的所有成员。有关更多信息，请参阅用于验证管理用户的组成员身份查询 , on page 15以及邮件安全设备文档或在线帮助。

Note 使用页面上“外部身份验证查询”部分中的**测试查询**按钮（或 ldaptest 命令）验证查询是否返回了预期结果。如需相关信息，请参阅测试 LDAP 查询, on page 9。

步骤 4 **设置外部身份验证以使用 LDAP 服务器**。启用设备以将 LDAP 服务器用于用户身份验证，并将用户角色分配给 LDAP 目录中的组。有关更多信息，请参阅启用管理用户外部身份验证 , on page 17以及邮件安全设备文档或在线帮助中的“添加用户”。

用于验证管理用户的用户账户查询

为了验证外部用户，AsyncOS 会使用查询搜索 LDAP 目录中的用户记录以及包含用户全名的属性。根据您选择的服务器类型，AsyncOS 输入默认查询和默认属性。如果您的 LDAP 用户记录中有在 RFC 2307 中定义的属性（**shadowLastChange**、**shadowMax** 和 **shadowExpire**），您可以选择让设备拒绝账户过期的用户。用户记录所驻留的域层需要基本 DN。

下表显示了 AsyncOS 在 Active Directory 服务器上搜索用户账户时使用的默认查询字符串和完整用户名属性。

***Table 5: Active Directory* 服务器的默认查询字符串**

服务器类型	**Active Directory**
基本 DN	[空白]（您需要使用特定的基本 DN 查找用户记录。）
查询字符串	(&(objectClass=user)(sAMAccountName={u}))
包含用户全名的属性	displayName

下表显示了 AsyncOS 在 OpenLDAP 服务器上搜索用户账户时使用的默认查询字符串和完整用户名属性。

***Table 6: OpenLDAP* 服务器的默认查询字符串**

服务器类型	**OpenLDAP**
基本 DN	[空白]（您需要使用特定的基本 DN 查找用户记录。）
查询字符串	(&(objectClass=posixAccount)(uid={u}))
包含用户全名的属性	gecos

用于验证管理用户的组成员身份查询

您可以将 LDAP 组与用户角色关联以便访问设备。

AsyncOS 创建还使用一个查询以确定用户是否是某个目录组的成员，并使用一个单独的查询以查找组的所有成员。目录组成员身份可以确定用户在系统中的权限。在GUI中的“管理设备”(Management Appliance)>“系统管理”(System Administration)>“用户”(Users)页面上（或CLI中的userconfig）启用外部身份验证时，将用户角色分配给 LDAP 目录中的组。用户角色会确定用户在系统中所具有的权限，并且对于在外部进行身份验证的用户，角色将分配给目录组而不是各个用户。例如，您可

以为“IT”目录组中的用户分配“管理员”(Administrator) 角色，为“支持”(Support) 目录组中的用户分配“服务中心用户”(Help Desk User) 角色。

如果用户属于具有不同用户角色的多个 LDAP 组，则 AsyncOS 会授予该用户访问最具限制性角色的权限。例如，如果用户属于具有“操作人员 (Operator)”权限的组和具有“服务中心用户 (Help Desk User)”权限的组，则 AsyncOS 会为该用户授予“服务中心用户 (Help Desk User)”角色的权限。

在配置 LDAP 配置文件以查询组成员身份时，为可以找到组记录的目录级别、保存组成员用户名的属性以及包含组名的属性输入基本 DN。根据您为 LDAP 服务器配置文件选择的服务器类型，AsyncOS 为用户名和组名属性输入默认值并输入默认查询字符串。

Note 对于 Active Directory 服务器，用于确定用户是否是组成员的默认查询字符串是 (&(objectClass=group)(member={u}))。但是，如果您的 LDAP 架构在“memberof”列表中使用可区别名称而不是用户名，您可以使用 {dn} 而不是 {u}。

下表 显示 AsyncOS 在 Active Directory 服务器上搜索组成员身份信息时使用的默认查询字符串和属性。

***Table 7: Active Directory* 服务器的默认查询字符串和属性**

查询字符串	**Active Directory**
基本 DN	[空白]（您需要使用特定的基本 DN 查找组记录。）
用于确定用户是否为组成员的查询字符串	(&(objectClass=group)(member={u})) **Note** 如果您的 LDAP 架构在“memberof”列表中使用可区别名称而不是用户名，您可以将 {u} 替换为 {dn}。
用于确定某个组的所有成员的查询字符串：	(&(objectClass=group)(cn={g}))
保存每个成员的用户名（或用户记录的 DN）的属性	member
包含组名的属性	cn

下表 显示 AsyncOS 在 OpenLDAP 服务器上搜索组成员身份信息时使用的默认查询字符串和属性。

***Table 8: OpenLDAP* 服务器的默认查询字符串和属性**

查询字符串	**OpenLDAP**
基本 DN	[空白]（您需要使用特定的基本 DN 查找组记录。）
用于确定用户是否为组成员的查询字符串	(&(objectClass=posixGroup)(memberUid={u}))
用于确定某个组的所有成员的查询字符串：	(&(objectClass=posixGroup)(cn={g}))
保存每个成员的用户名（或用户记录的 DN）的属性	memberUid

查询字符串	OpenLDAP
包含组名的属性	cn

启用管理用户外部身份验证

在创建 LDAP 服务器配置文件和查询之后，您可以使用 LDAP 启用外部身份验证。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 加载旧 Web 界面。

步骤 2 依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)** 页面。

步骤 3 点击**启用 (Enable)**。

步骤 4 选中**启用外部身份验证 (Enable External Authentication)** 复选框。

步骤 5 选择 **LDAP** 作为身份验证类型。

步骤 6 选择对用户进行身份验证的 LDAP 外部身份验证查询。

步骤 7 输入超时前设备等待服务器响应的秒数。

步骤 8 输入希望设备验证的 LDAP 目录中的组名称，然后选择该组中用户的角色。

步骤 9 （可选）点击**添加行 (Add Row)** 添加另一个目录组。为设备验证的每个目录组重复执行步骤 7 和 8。

步骤 10 提交并确认更改。

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。