LDAP 查询

本章包含以下部分：

- LDAP 查询概述, on page 1
- 处理 LDAP 查询, on page 11
- 使用接受查询进行收件人验证, on page 18
- 使用路由查询将邮件发送到多个目标地址, on page 20
- 使用伪装查询重写信封发件人, on page 21
- 使用组 LDAP 查询确定收件人是否为组成员, on page 22
- 使用基于域的查询路由到特定域, on page 26
- 使用链查询执行一系列 LDAP 查询, on page 27
- 将 LDAP 用于目录搜集攻击预防, on page 28
- 配置 AsyncOS 进行 SMTP 身份验证, on page 30
- 为用户配置外部 LDAP 身份验证, on page 38
- 对垃圾邮件隔离区的最终用户进行身份验证, on page 41
- 垃圾邮件隔离区别名整合查询, on page 42
- 用户可分辨名称设置示例, on page 44
- 将 AsyncOS 配置为与多个 LDAP 服务器配合使用, on page 44
- 测试服务器和查询, on page 45

LDAP 查询概述

如果在网络基础设施的 LDAP 目录中（例如，在 Microsoft Active Directory、SunONE Directory Server 或 OpenLDAP 目录中）存储用户信息，则可以将邮件网关配置为查询 LDAP 服务器以接受、路由和对邮件进行身份验证。可以将邮件网关配置为与一个或多个 LDAP 服务器配合使用。

以下部分概述了可以执行的 LDAP 查询的类型；LDAP 如何与邮件网关配合使用以进行身份验证、接受和路由邮件；以及如何将邮件网关配置为与 LDAP 配合使用。

相关主题

- 了解 LDAP 查询, on page 2
- 了解 LDAP 如何与 AsyncOS 配合使用, on page 3

- 将邮件网关配置为与 LDAP 服务器配合使用, on page 4
- 创建 LDAP 服务器配置文件以存储有关 LDAP 服务器的信息, on page 4
- 测试 LDAP 服务器, on page 6
- 启用 LDAP 查询以在特定侦听程序中运行, on page 6
- 对 Microsoft Exchange 5.5 的增强支持, on page 9

了解 LDAP 查询

如果在网络基础设施的 LDAP 目录中存储用户信息，则可以将邮件网关配置为查询 LDAP 服务器以用于实现以下目的：

- **接受查询**。可以使用现有 LDAP 基础设施来定义如何处理传入邮件的收件人邮件地址（在公共侦听程序中）。有关详细信息，请参阅使用接受查询进行收件人验证, on page 18。
- **路由（别名设置）**。可以将邮件网关配置为根据网络中 LDAP 目录中的可用信息，将邮件路由至相应地址和/或邮件主机。有关详细信息，请参阅使用路由查询将邮件发送到多个目标地址, on page 20。
- **证书身份验证**。可以创建查询来检查客户端证书的有效性，以便对用户的邮件客户端与邮件网关之间的 SMTP 会话进行身份验证。有关详细信息，请参阅检查客户端证书的有效性。
- **伪装**。您可以伪装信封发件人（针对传出邮件）和信头（针对传入邮件，例如，To:、Reply To:、From: 或 CC: 信头）。有关伪装的更多信息，请参阅使用伪装查询重写信封发件人, on page 21。
- **组查询**。可以将邮件网关配置为根据 LDAP 目录中的组对邮件执行操作。为此，可以将组查询与邮件过滤器相关联。可以对与定义的 LDAP 组匹配的邮件执行适用于邮件过滤器的任何邮件操作。有关详细信息，请参阅使用组 LDAP 查询确定收件人是否为组成员, on page 22。
- **基于域的查询**。可以创建基于域的查询，以便邮件网关在单个侦听程序中为不同的域执行不同的查询。当邮件网关运行基于域的查询时，它会根据域确定要使用的查询，并且会查询与该域关联的 LDAP 服务器。
- **链查询**。可以创建链查询来使邮件网关按顺序执行一系列查询。在配置链查询时，邮件网关会按顺序运行每个查询，直到 LDAP 设备返回一个积极的结果。对于链接的路由查询，邮件网关会按顺序对每个重写的邮件地址重新运行已配置的相同链查询。
- **目录搜集预防**。可以将邮件网关配置为使用 LDAP 目录来抵御目录搜集攻击。可以在 SMTP 会话期间或在工作队列中配置目录搜集攻击预防。如果在 LDAP 目录中找不到收件人，可以配置系统以执行延迟退回或彻底丢弃邮件。因此，垃圾邮件发送者无法区分有效和无效的邮件地址。请参阅将 LDAP 用于目录搜集攻击预防, on page 28。
- **SMTP 身份验证**。AsyncOS 支持 SMTP 身份验证。SMTP 身份验证是用于验证连接到 SMTP 服务器的客户端的一种机制。可以使用该功能使贵组织中的用户可以使用邮件服务器发送邮件，即使他们利用远程连接（例如在家中或在旅行时）也是如此。有关详细信息，请参阅配置AsyncOS 进行 SMTP 身份验证, on page 30。
- **外部身份验证**。可以将邮件网关配置为使用 LDAP 目录来对登录到邮件网关的用户进行身份验证。有关详细信息，请参阅为用户配置外部 LDAP 身份验证, on page 38。
- **垃圾邮件隔离区最终用户身份验证**。可以将邮件网关配置为在用户登录最终用户隔离区时对其进行验证。有关详细信息，请参阅对垃圾邮件隔离区的最终用户进行身份验证, on page 41。

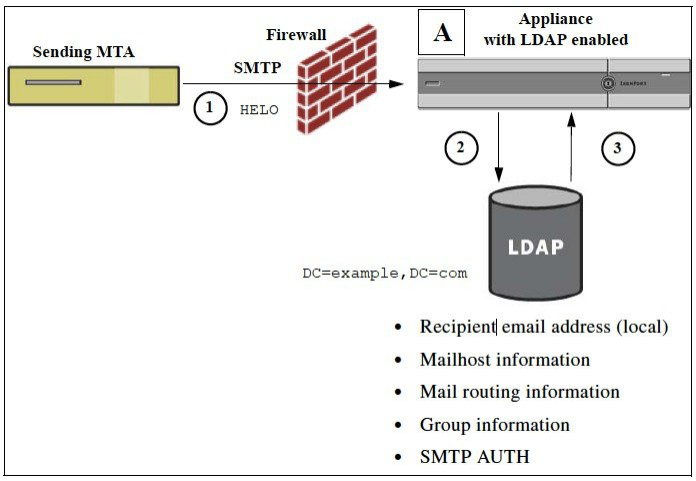
- **垃圾邮件隔离区别名合并**。如果为垃圾邮件使用邮件通知，则此查询会合并最终用户别名，以便最终用户不会根据每个别名邮件地址都收到隔离区通知。有关详细信息，请参阅垃圾邮件隔离区别名整合查询, on page 42。

了解 LDAP 如何与 AsyncOS 配合使用

使用 LDAP 目录时，可以将邮件网关与 LDAP 目录服务器配合使用，以接受收件人、路由邮件和/或伪装邮件信头。还可以将 LDAP 组查询与邮件过滤器配合使用，以创建邮件网关收到邮件时的处理规则。

下图展示邮件网关如何与 LDAP 配合使用：

***Figure 1: LDAP* 配置**



1. 发送 MTA 通过 SMTP 将邮件发送到公共侦听程序。
2. 邮件网关设备通过**系统管理 (System Administration) > LDAP** 页面（或通过全局 **`ldapconfig`** 命令）查询定义的 LDAP 服务器。
3. 将从 LDAP 目录接收数据，而且根据在**系统管理 (System Administration) > LDAP** 页面（或在 **`ldapconfig`** 命令中）定义由侦听程序使用的查询：
   - 邮件将路由到新的收件人地址，或者被丢弃或退回
   - 邮件将路由到新收件人的相应邮件主机
   - 根据查询重写 From:、To: 和 CC: 邮件信头
   - 执行 **`rcpt-to-group`** 或 **`mail-from-group`** 邮件过滤器规则（与配置的组查询配合使用）定义的进一步操作。

Note 可以将邮件网关配置为连接到多个 LDAP 服务器。当这样做时，可以配置用于负载平衡或故障转移的 LDAP 配置文件设置。有关使用多个 LDAP 服务器的详细信息，请参阅将 AsyncOS 配置为与多个 LDAP 服务器配合使用, on page 44。

将邮件网关配置为与 LDAP 服务器配合使用

配置邮件网关以与 LDAP 目录配合使用时，必须完成以下步骤以配置 AsyncOS 邮件网关的接受、路由、别名和伪装设置：

Procedure

步骤 1 **配置 LDAP 服务器配置文件**。服务器配置文件包含用于启用 AsyncOS 以连接到 LDAP 服务器（或多个服务器）的信息，例如：

- 发送查询的服务器和端口的名称，
- 基本 DN，以及
- 有关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 服务器配置文件以存储有关 LDAP 服务器的信息, on page 4。

配置 LDAP 服务器配置文件时，可以配置 AsyncOS 以连接到一个或多个 LDAP 服务器。

有关配置 AsyncOS 以连接到多个服务器的信息，请参阅将 AsyncOS 配置为与多个 LDAP 服务器配合使用, on page 44。

步骤 2 **配置 LDAP 查询**。在 LDAP 服务器配置文件中配置 LDAP 查询。配置的查询应根据特定 LDAP 实施和方案进行定制。

有关的可以创建的 LDAP 查询类型的信息，请参阅了解 LDAP 查询, on page 2。

有关编写查询的信息，请参阅处理 LDAP 查询, on page 11。

步骤 3 **在公共侦听程序或专用侦听程序中启用 LDAP 服务器配置文件**。必须在侦听程序上启用 LDAP 服务器配置文件，以指示侦听程序在接受、路由或发送邮件时运行 LDAP 查询。

有关详细信息，请参阅启用 LDAP 查询以在特定侦听程序中运行, on page 6。

Note 在配置组查询时，需要执行额外的步骤来配置 AsyncOS，以便与 LDAP 服务器配合使用。有关配置组查询的信息，请参阅使用组 LDAP 查询确定收件人是否为组成员, on page 22。当配置最终用户身份验证或垃圾邮件通知整合查询时，必须启用 LDAP 最终用户对垃圾邮件隔离区的访问。有关垃圾邮件隔离区的详细信息，请参阅“垃圾邮件隔离区”一章。

创建 LDAP 服务器配置文件以存储有关 LDAP 服务器的信息

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。

Procedure

步骤 1 在**系统管理 (System Administration) > LDAP** 页面上，点击**添加 LDAP 服务器配置文件 (Add LDAP Server Profile)**。

步骤 2 输入服务器配置文件的名称。

步骤 3 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 44。

步骤 4 选择身份验证方法。可以使用匿名身份验证或指定用户名和密码。

步骤 5 选择 LDAP 服务器类型：Active Directory、OpenLDAP 或“未知或其他 (Unknown or Other)”。

步骤 6 输入端口号。

对于 Active Directory 或任何未知/其他服务器类型，默认端口为 3268（不使用 SSL 时）和 3269（使用 SSL 时）。

对于 Open LDAP 服务器类型，默认端口为 389（不使用 SSL 时）和 636（使用 SSL 时）。

步骤 7 输入 LDAP 服务器的基础 DN（可分辨名称）。

如果通过用户名和密码进行身份验证，则用户名必须包含具有该密码的条目的完整DN。例如，某个用户是营销团队的成员，其邮件地址为 joe@example.com。此用户的条目类似于以下条目：

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

步骤 8 选择在与 LDAP 服务器通信时是否使用 SSL。

Note [可选 - 仅当在“LDAP 全局设置”(LDAP Global Settings) 页面中选择了“验证 LDAP 服务器证书”(Validate LDAP Server Certificate) 选项，并且在“SSL 配置”(SSL Configuration) 设置页面中启用了 FQDN 验证]：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。

Note [可选 - 仅当在“LDAP 全局设置”(LDAP Global Settings) 页面中选择了“验证 LDAP 服务器证书”(Validate LDAP Server Certificate) 选项，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。

步骤 9 在“高级”(Advanced) 下，输入缓存生存时间。此值表示保留缓存的时长。

步骤 10 输入保留缓存条目的最大数量。

Note 此缓存按 LDAP 服务器进行维护。如果要配置多个 LDAP 服务器，则必须设置更小的 LDAP 缓存值以提高性能。此外，如果邮件网关中各种进程的内存使用量较高，则增加此值可能会降低系统性能。

步骤 11 输入同时连接数。

- 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。

Note 最大并发连接数包括用于 LDAP 查询的 LDAP 连接。但是，如果为垃圾邮件隔离区使用 LDAP 身份验证，则邮件网关可能会打开更多连接。

- 您可以配置连接 LDAP 服务器时在连接重置前必须持续的最大时间（秒）。请选择介于 60 至 86400 之间的值。

步骤 12 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 6。

步骤 13 通过标记相应复选框并填写字段来创建查询。可以选择“接受”(Accept)、“路由”(Routing)、“伪装表”(Masquerade)、“组”(Group)、“SMTP 身份验证”(SMTP Authentication)、“外部身份验证”(External Authentication)、“垃圾邮件隔离区最终用户身份验证”(Spam Quarantine End-User Authentication) 和“垃圾邮件隔离区别名合并”(Spam Quarantine Alias Consolidation)。

Note 要允许邮件网关在您接收或发送邮件时运行 LDAP 查询，必须在适当的侦听程序上启用 LDAP 查询。有关详细信息，请参阅启用 LDAP 查询以在特定侦听程序中运行, on page 6。

步骤 14 通过点击**测试查询 (Test Query)** 按钮测试查询。

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)**。有关详细信息，请参阅测试 LDAP 服务器, on page 6。

Note 如果将 LDAP 服务器配置为允许与空密码进行绑定，则查询可以使用空密码字段通过测试。

步骤 15 提交并确认更改。

Note 尽管服务器配置的数量不受限制，但是可以仅为每台服务器配置一个收件人接受、一个路由、一个伪装和一个组查询。

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。

启用 LDAP 查询以在特定侦听程序中运行

要允许邮件网关在您接收或发送邮件时运行 LDAP 查询，必须在适当的侦听程序上启用 LDAP 查询。

相关主题

- 配置 LDAP 查询的全局设置, on page 7
- 创建 LDAP 服务器配置文件示例, on page 7
- 在公共侦听程序上启用 LDAP 查询, on page 8
- 在专用侦听程序上启用 LDAP 查询, on page 9

配置 LDAP 查询的全局设置

LDAP 全局设置定义邮件网关如何处理所有 LDAP 流量。

Procedure

步骤 1 在**系统管理 (System Administration) > LDAP** 页面上，点击**编辑设置 (Edit Settings)**。

步骤 2 选择用于 LDAP 流量的 IP 接口。默认情况下，邮件网关会自动选择接口。

步骤 3 选择用于 LDAP 接口的 TLS 证书（通过**网络 (Web) > 证书 (Certificates)** 页面或 CLI 中的 **certconfig** 命令添加的 TLS 证书在列表中提供，请参阅加密与其他 MTA 的通信概述）。

步骤 4 如果要验证 LDAP 服务器证书，请选择适当的选项。

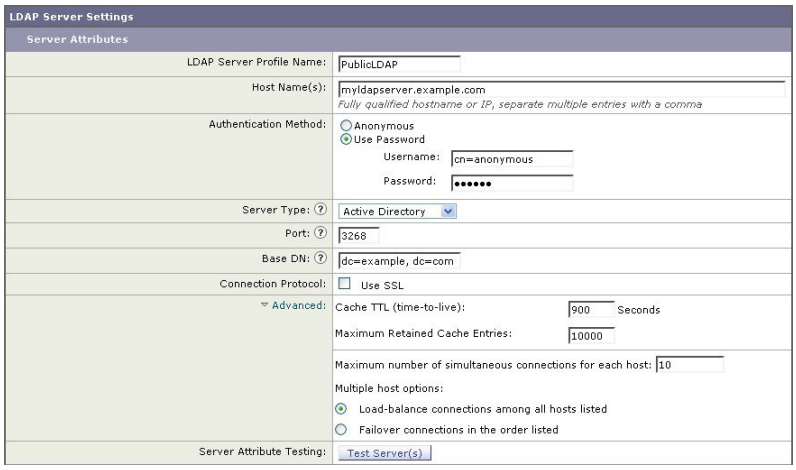
步骤 5 提交并确认更改。

创建 LDAP 服务器配置文件示例

在下面的示例中，“系统管理”(System Administration) > “LDAP”页面用于为要绑定到的邮件网关定义 LDAP 服务器，并为收件人接受、路由和伪装配置查询。

Note LDAP 连接具有 60 秒的连接尝试超时（包括 DNS 查找、连接本身，以及如果适用，邮件网关自身的身份验证绑定）。在第一次失败后，AsyncOS 会立即开始尝试同一服务器中的其他主机（如果以逗号分隔的列表形式指定了多个主机）。如果服务器中只有一个主机， AsyncOS 会继续尝试连接到它。

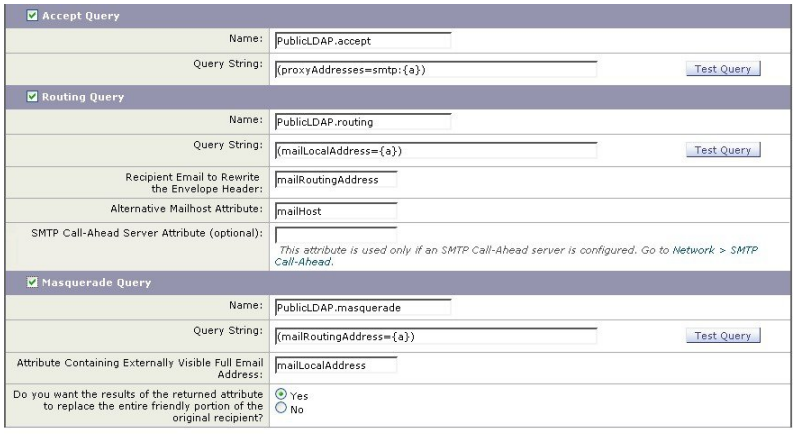
Figure 2: 配置 ***LDAP*** 服务器配置文件 ***(1/2)***



首先，为 myldapserver.example.com LDAP 服务器指定昵称“PublicLDAP”。连接数量设置为 10（默认值），而且多个 LDAP 服务器（主机）负载均衡选项将保留默认设置。可以通过提供一个用逗号分隔的名称列表，在此处指定多个主机。查询将定向到端口 3268（默认值）。对于此主机，未启用 SSL 作为连接协议。定义了 example.com 的基本 DN (dc=example,dc=com)。缓存存活时间设置为 900 秒，缓存条目的最大数量为 10000，而且身份验证方法设置为密码。

定义了用于收件人接受、邮件路由和伪装的查询。确保查询名称区分大小写，必须完全一致才能返回正确的结果。

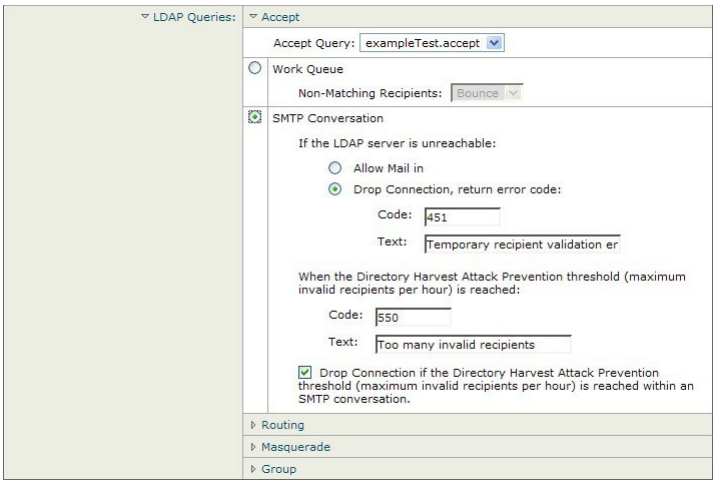
Figure 3: 配置 ***LDAP*** 服务器配置文件 ***(2/2)***



在公共侦听程序上启用 LDAP 查询

在本例中，公共侦听程序“InboundMail”更新为将 LDAP 查询用于收件人接受。此外，收件人接受配置为在 SMTP 会话期间发生（有关详细信息，请参阅使用接受查询进行收件人验证, on page 18）。

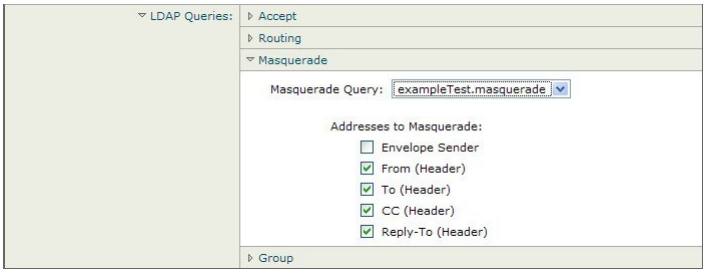
Figure 4: 在侦听程序上启用接受和路由查询



在专用侦听程序上启用 LDAP 查询

在本例中，专用侦听程序“OutboundMail”更新为将 LDAP 查询用于伪装。伪装的字段包括：“发件人”(From)、“收件人”(To)、“抄送”(CC) 和“回复”(Reply-To)。

Figure 5: 在侦听程序上启用伪装查询



对 Microsoft Exchange 5.5 的增强支持

AsyncOS 包含一个配置选项，可用于为 Microsoft Exchange 5.5 提供支持。如果使用较高版本的 Microsoft Exchange，则不需要启用此选项。在配置 LDAP 服务器时，可选择通过在 `ldapconfig -> edit -> server -> compatibility` 子命令（仅通过 CLI 可用）中出现提示时回答“y”来启用 Microsoft Exchange 5.5 支持。

```
mail3.example.com> ldapconfig

Current LDAP server configurations:

1. PublicLDAP: (ldapexample.com:389)


Choose the operation you want to perform:

- NEW - Create a new server configuration.

- EDIT - Modify a server configuration.
```

```
- DELETE - Remove a server configuration.


[]> edit

Enter the name or number of the server configuration you wish to edit.

[]> 1

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com

Choose the operation you want to perform:

- SERVER - Change the server for the query.

- LDAPACCEPT - Configure whether a recipient address should be accepted or
bounced/dropped.

- LDAPROUTING - Configure message routing.

- MASQUERADE - Configure domain masquerading.

- LDAPGROUP - Configure whether a sender or recipient is in a specified group.

- SMTPAUTH - Configure SMTP authentication.

[]> server

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com


Microsoft Exchange 5.5 Compatibility Mode: Disabled

Choose the operation you want to perform:

- NAME - Change the name of this configuration.

- HOSTNAME - Change the hostname used for this query.

- PORT - Configure the port.

- AUTHTYPE - Choose the authentication type.

- BASE - Configure the query base.

- COMPATIBILITY - Set LDAP protocol compatibility options.

[]> compatibility
Would you like to enable Microsoft Exchange 5.5 LDAP compatibility mode? (This is not
recommended for versions of Microsoft Exchange later than 5.5, or other LDAP servers.)
```

```
[N]> y

Do you want to configure advanced LDAP compatibility settings? (Typically not required)

[N]>

Name: PublicLDAP

Hostname: ldapexample.com Port 389

Authentication Type: anonymous

Base: dc=ldapexample,dc=com

Microsoft Exchange 5.5 Compatibility Mode: Enabled (attribute "objectClass")

Choose the operation you want to perform:

- NAME - Change the name of this configuration.

- HOSTNAME - Change the hostname used for this query.

- PORT - Configure the port.

- AUTHTYPE - Choose the authentication type.

- BASE - Configure the query base.

- COMPATIBILITY - Set LDAP protocol compatibility options.

[]>
```

处理 LDAP 查询

在 LDAP 服务器配置文件中为您要执行的每种类型的 LDAP 查询创建一个条目。在创建 LDAP 查询时，必须输入 LDAP 服务器的查询语法。请注意，构建的查询应进行定制并且特定于 LDAP 目录服务的特殊实施，特别是在通过对象类和属性扩展了目录以满足目录的独特需求时。

相关主题

- LDAP 查询的类型, on page 12
- 基本可区别名称 (DN), on page 12
- LDAP 查询语法, on page 12
- 安全 LDAP (SSL), on page 13
- 路由查询, on page 13
- 允许客户端匿名绑定到 LDAP 服务器 , on page 13
- 测试 LDAP 查询, on page 17
- 排除 LDAP 服务器连接故障, on page 18

LDAP 查询的类型

- **接受查询**。有关详细信息，请参阅使用接受查询进行收件人验证, on page 18。
- **路由查询**。有关详细信息，请参阅使用路由查询将邮件发送到多个目标地址, on page 20。
- **证书身份验证查询**。有关详细信息，请参阅检查客户端证书的有效性。
- **伪造查询**。有关详细信息，请参阅使用伪装查询重写信封发件人, on page 21。
- **组查询**。有关详细信息，请参阅使用组 LDAP 查询确定收件人是否为组成员, on page 22。
- **基于域的查询**。有关详细信息，请参阅使用基于域的查询路由到特定域, on page 26。
- **链查询**。有关详细信息，请参阅使用链查询执行一系列 LDAP 查询, on page 27。

还可以为以下目的配置查询：

- **目录搜集预防**。有关详细信息，请参阅了解 LDAP 查询, on page 2。
- **SMTP 身份验证**。有关详细信息，请参阅配置 AsyncOS 进行 SMTP 身份验证, on page 30。
- **外部身份验证**。有关详细信息，请参阅为用户配置外部 LDAP 身份验证, on page 38。
- **垃圾邮件隔离区最终用户身份验证查询**。有关详细信息，请参阅对垃圾邮件隔离区的最终用户进行身份验证, on page 41。
- **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 42。

指定的搜索查询适用于在系统上配置的所有侦听程序。

基本可区别名称 (DN)

目录的根级别称为基本。基本的名称为 DN（可分辨名称）。Active Directory 的基本 DN 格式（以及按照 RFC 2247 的标准）会将 DNS 域转换为域组成部分 (dc=)。例如，example.com 的基本 DN 为：dc=example，dc=com。请注意，DNS 名称的每个部分均按顺序表示。这可能会或不会反映您的配置的 LDAP 设置。

如果目录中包含多个域，则您可能会发现不便为查询输入单个 BASE。在本例中，在配置 LDAP 服务器设置时，请将基本 DN 设置为“无”(NONE)。但是，这会让搜索效率低下。

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 LDAP 实施匹配才能正常工作。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。

相关主题

- 令牌：, on page 13

令牌：

您可以在 LDAP 查询中使用以下令牌：

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

Note {f} 令牌仅在接受查询中有效。

例如，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，Cisco Systems 强烈建议使用“LDAP”页面的测试功能（或 **ldapconfig** 命令的 **test** 子命令）来测试所构建的所有查询，并确保返回预期结果。有关详细信息，请参阅测试 LDAP 查询, on page 17。

安全 LDAP (SSL)

可以指示 AsyncOS 在与 LDAP 服务器通信时使用 SSL。如果将 LDAP 服务器配置文件配置为使用 SSL：

- AsyncOS 将使用通过 CLI 中的 certconfig 配置的 LDAPS 证书（请参阅创建自签名 证书）。

  可能必须将 LDAP 服务器配置为支持使用 LDAPS 证书。

- 如果未配置 LDAPS 证书，则 AsyncOS 将使用演示证书。

路由查询

LDAP 路由查询没有递归限制；路由完全由数据驱动。但是，AsyncOS 会检查循环参考数据以防止无限循环地进行路由。

允许客户端匿名绑定到 LDAP 服务器

可能需要配置LDAP目录服务器以允许匿名查询。（即，客户端可匿名绑定到服务器并执行查询。）有关配置 Active Directory 以允许匿名查询的具体说明，请参阅以下 URL 的“Microsoft 知识库文章 - 320528”：

http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B320528

或者，可以配置一个“用户”，将其专用于身份验证和执行查询，而不是打开 LDAP 目录服务器以从任何客户端进行匿名查询。

此处提供相应步骤的摘要，特别是：

- 如何设置 Microsoft Exchange 2000 服务器以允许“匿名”身份验证。
- 如何设置 Microsoft Exchange 2000 服务器以允许“匿名绑定”。
- 如何使用“匿名绑定”和“匿名”身份验证设置 AsyncOS 以从 Microsoft Exchange 2000 服务器检索 LDAP 数据。

必须为 Microsoft Exchange 2000 服务器提供特定权限，以便允许“匿名”或“匿名绑定”身份验证，从而查询用户邮件地址。当 LDAP 查询用于确定进入 SMTP 网关的传入邮件的有效性时，该操作非常有用。

相关主题

- 匿名身份验证设置, on page 14
- Active Directory 的匿名绑定设置, on page 15
- Active Directory 实施说明, on page 16

匿名身份验证设置

通过下面的设置说明，可以将特定数据提供给 Microsoft Windows Active Directory 中未经身份验证的 Active Directory 和 Exchange 2000 服务器查询。如果希望允许“匿名绑定”到 Active Directory，请参阅Active Directory 的匿名绑定设置, on page 15。

Procedure

步骤 1 确定所需的 Active Directory 权限。

使用 ADSI Edit 管理单元或 LDP 实用程序时，必须修改以下 Active Directory 对象属性的权限：

- 要根据其进行查询的域的域命名上下文根。
- 包含要根据其查询邮件信息的用户的所有 OU 和 CN 对象。

下表显示了要应用到所需容器的所需权限。

用户对象	权限	继承	权限类型
所有人	列出内容	容器对象	对象
所有人	列出内容	组织单位对象	对象
所有人	读取公共信息	用户对象	特性
所有人	读取电话和邮件选项	用户对象	特性

步骤 2 设置 Active Directory 权限

- 打开 Windows 2000 支持工具中的 ADSIEdit。
- 找到**域命名上下文 (Domain Naming Context)** 文件夹。此文件夹包含域的 LDAP 路径。
- 右键点击**域命名上下文 (Domain Naming Context)** 文件夹，然后点击**属性 (Properties)**。
- 点击**安全 (Security)**。
- 点击**高级 (Advanced)**。
- 点击**添加 (Add)**。
- 点击**用户对象 (User Object)**“Everyone”，然后点击**确定 (OK)**。
- 点击**权限类型 (Permission Type)** 选项卡。
- 点击**应用到 (Apply onto)** 框中的**继承 (Inheritance)**。
- 点击以选中**权限 (Permission)** 对应的“允许”(Allow) (Allow) 复选框。

步骤 3 配置思科邮件网关

使用命令行界面 (CLI) 中的 **`ldapconfig`** 创建包含下列信息的 LDAP 服务器条目。

- Active Directory 或 Exchange 服务器的主机名
- 端口 3268
- 与域的根命名上下文匹配的基本 DN
- 匿名身份验证类型

Active Directory 的匿名绑定设置

通过下面的设置说明，可以将特定数据提供给 Microsoft Windows Active Directory 中 Active Directory 和 Exchange 2000 服务器的匿名绑定查询。Active Directory 服务器的匿名绑定将发送用户名 anonymous 且密码为空。

Note 如果将某个密码发送到 Active Directory 服务器并且尝试匿名绑定，则身份验证可能会失败。

Procedure

步骤 1 确定所需的 Active Directory 权限。

使用 ADSI Edit 管理单元或 LDP 实用程序时，必须修改以下 Active Directory 对象属性的权限。

- 要根据其进行查询的域的域命名上下文根。
- 包含要根据其查询邮件信息的用户的所有 OU 和 CN 对象。

下表显示了要应用到所需容器的所需权限。

用户对象	权限	继承	权限类型
ANONYMOUS LOGON	列出内容	容器对象	对象

用户对象	权限	继承	权限类型
ANONYMOUS LOGON	列出内容	组织单位对象	对象
ANONYMOUS LOGON	读取公共信息	用户对象	特性
ANONYMOUS LOGON	读取电话和邮件选项	用户对象	特性

步骤 2 设置 Active Directory 权限

- 打开 Windows 2000 支持工具中的 ADSIEdit。
- 找到**域命名上下文 (Domain Naming Context)** 文件夹。此文件夹包含域的 LDAP 路径。
- 右键点击**域命名上下文 (Domain Naming Context)** 文件夹，然后点击**属性 (Properties)**。
- 点击**安全 (Security)**。
- 点击**高级 (Advanced)**。
- 点击**添加 (Add)**。
- 点击**用户对象 (User Object)**“ANONYMOUS LOGON”，然后点击**确定 (OK)**。
- 点击**权限类型 (Permission Type)** 选项卡。
- 点击**应用到 (Apply onto)** 框中的**继承 (Inheritance)**。
- 点击以选中**权限 (Permission)** 对应的**允许 (Allow)** 复选框。

步骤 3 配置思科邮件网关

使用**系统管理 (System Administration) > LDAP** 页（或 CLI 中的 **`ldapconfig`**）创建包含下列信息的 LDAP 服务器条目。

- Active Directory 或 Exchange 服务器的主机名
- 端口 3268
- 与域的根命名上下文匹配的基本 DN
- 基于密码的身份验证类型，使用 cn=anonymous 作为用户且密码为空

Active Directory 实施说明

- Active Directory 服务器在端口 3268 和 389 上接受 LDAP 连接。用于访问全局目录的默认端口是 3268。
- Active Directory 服务器在端口 636 和 3269 上接受 LDAPS 连接。Microsoft 在 Windows Server 2003 及更高版本上支持 LDAPS。
- 邮件网关应连接到还作为全局目录的域控制器，以便使用同一台服务器对不同的基本 DN 执行查询。
- 在 Active Directory 中，可能需要为“Everyone”组授予对目录对象的读取权限，以便实现成功的查询。这包括域命名上下文的根。
- 通常，在许多 Active Directory 实施中 mail 属性条目的值具有匹配的“ProxyAddresses”属性条目值。

- 基础设施中可相互识别的 Microsoft Exchange 环境通常在彼此之间路由邮件，不会路由回原始 MTA。

测试 LDAP 查询

使用每个查询类型对应的“添加 LDAP 服务器配置文件”(Add LDAP Server Profile)/“编辑 LDAP 服务器配置文件”(Edit LDAP Server Profile) 页面上的“测试查询 (Test Query) 按钮（或 CLI 中的 `test` 子命令）来测试对配置的 LDAP 服务器的查询。除了显示结果之外，AsyncOS 还显示有关查询连接测试每个阶段的详细信息。可以测试每个查询类型。

`ldaptest` 命令以批处理命令的形式提供，例如：

```
ldaptest LDAP.ldapaccept foo@ironport.com
```

如果在 LDAP 服务器属性的“主机名”(Host Name) 字段中输入了多个主机，则邮件网关会在每个 LDAP 服务器上测试查询。

Table 1: 测试 ***LDAP*** 查询

查询类型	如果收件人匹配 **(PASS)**...	如果收件人不匹配 **(FAIL)**...
收件人接受（接受，`ldapaccept`）	接受邮件。	收件人无效：会话、延迟退回或根据侦听程序设置丢弃邮件。DHAP: 丢弃。
路由（路由，`ldaprouting`）	根据查询设置进行路由。	继续处理邮件。
伪装（伪装，`masquerade`）	使用查询定义的变量映射修改信头。	继续处理邮件。
组成员身份（组，`ldapgroup`）	为邮件过滤器规则返回“true”。	为邮件过滤器规则返回“false”。
SMTP Auth（SMTP 身份验证，`smtpauth`）	从 LDAP 服务器返回密码，并将其用于身份验证；发生 SMTP 身份验证。	不会进行任何密码匹配；SMTP 身份验证尝试失败。
外部身份验证 (`externalauth`)	单独为绑定、用户记录和用户的组成员身份分别返回“match positive”。	单独为绑定、用户记录和用户的组成员身份分别返回“match negative”。
垃圾邮件隔离区最终用户身份验证 (`isqauth`)	为最终用户账户返回“match positive”。	不会进行任何密码匹配；最终用户身份验证尝试失败。
垃圾邮件隔离区别名整合 (`isqalias`)	返回将整合的垃圾邮件通知发送到的邮件地址。	不会进行任何垃圾邮件通知整合。

Note 为查询输入的变量名称区分大小写，且必须与 LDAP 实施匹配才能正常工作。例如，在提示符处输入 **mailLocalAddress** 执行的查询与输入 **maillocaladdress** 执行的查询是不同的。思科系统公司强烈建议使用 ldapconfig 命令的 test 子命令来测试所构建的所有查询，并确保返回正确结果。

排除 LDAP 服务器连接故障

如果邮件网关无法连接 LDAP 服务器，将会显示下列错误之一：

- `Error: LDAP authentication failed: <LDAP Error "invalidCredentials" [0x31]>`
- `Error: Server unreachable: unable to connect`
- `Error: Server unreachable: DNS lookup failure`

请注意，可能由于在服务器配置中输入了错误的端口或端口无法在防火墙中打开，无法连接到服务器。LDAP 服务器通常通过端口 3268 或 389 通信。Active Directory 使用端口 3268 访问在多服务器环境中使用的全局目录（有关详细信息，请参阅“防火墙信息”附录。）在 AsyncOS 4.0 中，添加了通过 SSL 与 LDAP 服务器通信（通常通过端口 636）的功能。有关详细信息，请参阅安全 LDAP (SSL), on page 13。

也可能由于输入的主机名无法解析，无法连接服务器。

可以使用“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（或 CLI 中 `ldapconfig` 命令的 `test` 子命令）测试与 LDAP 服务器的连接。有关详细信息，请参阅测试 LDAP 服务器, on page 6。

如果LDAP服务器无法访问:

- 如果在工作队列中启用了 LDAP 接受、伪装或路由，则邮件会保留在工作队列中。
- 如果未启用 LDAP 接受，但在过滤器中使用了其他查询（组策略检查等），则过滤器求值为 False。

使用接受查询进行收件人验证

可以使用现有 LDAP 基础设施来定义如何处理传入邮件的收件人邮件地址（在公共侦听程序中）。邮件网关下次查询目录服务器时，在目录中对用户数据的更改会更新。可以指定缓存的大小以及邮件网关存储其检索到的数据的时间。

Note 您可能希望绕过对特殊收件人的 LDAP 接受查询（例如 administrator@example.com）。可以在收件人访问表 (RAT) 中配置此设置。有关配置此设置的信息，请参阅“配置网关以接收邮件”一章。

相关主题

- 接受查询示例, on page 19
- 为 Lotus Notes 配置接受查询, on page 19

接受查询示例

下表显示了接受查询示例。

Table 2: 常规 ***LDAP*** 实施的 ***LDAP*** 查询字符串示例：接受

查询内容：	收件人验证

OpenLDAP	`(mailLocalAddress={a})`
	`(mail={a})`
	`(mailAlternateAddress={a})`

Microsoft Active Directory 通讯录 **Microsoft Exchange**	`(|(mail={a})(proxyAddresses=smtp:{a}))`

SunONE Directory Server	`(mail={a})`
	`(mailAlternateAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailForwardingAddress={a})`
	`(mailRoutingAddress={a})`

Lotus NotesLotus Domino	`(|(|(mail={a})(uid={u}))(cn={u}))` `(|(ShortName={u})(InternetAddress={a})(FullName={u}))`

还可以验证用户名（左侧）。如果目录不包含要接受其邮件的所有域，则该验证非常有用。将接受查询设置为 (uid={u})。

为 Lotus Notes 配置接受查询

请注意，LDAPACCEPT 和 Lotus Notes 存在潜在问题。如果 Notes LDAP 包含具有如下属性的人员：

```
mail=juser@example.com

cn=Joe User

uid=juser

cn=123456

location=New Jersey
```

Lotus 会接受此人各种不同格式邮件地址而不是指定地址的邮件，例如“Joe_User@example.com”-其在 LDAP 中不存在。因此 AsyncOS 可能找不到该用户的所有有效的用户邮件地址。

一个可能的解决方案是尝试发布其他格式的地址。请联系 Lotus Notes 管理员以获得更多详细信息。

使用路由查询将邮件发送到多个目标地址

AsyncOS 支持别名扩展（具有多个目标地址的 LDAP 路由）。AsyncOS 会将原始邮件替换为针对每个别名目标的新的单独邮件（例如，recipient@yoursite.com 可能会替换为发送到 newrecipient1@hotmail.com 和 recipient2@internal.yourcompany.com 等的新的单独邮件）。路由查询有时在其他邮件处理系统中称为别名查询。

相关主题

• 路由查询示例, on page 20

路由查询示例

Table 3: 常规 ***LDAP*** 实施的 ***LDAP*** 查询字符串示例：路由

查询内容：	路由到其他邮件主机
OpenLDAP	`(mailLocalAddress={a})`
Microsoft Active Directory 通讯录 **Microsoft Exchange**	可能不适用

SunONE Directory Server	`(mail={a})`
	`(mailForwardingAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailRoutingAddress={a})`
	`(otherMailbox={a})`
	`(rfc822Mailbox={a})`

Active Directory 实施可以具有与 `proxyAddresses` 属性对应的多个条目，但是由于 AD 会将该属性值格式化为 `smtp:user@domain.com`，因此该数据无法用于 LDAP 路由/别名扩展。每个目标地址必须在单独的 `attribute:value` 对中。基础设施中可相互识别的 Microsoft Exchange 环境通常在彼此之间路由邮件，不会路由回原始 MTA。

相关主题

• 路由：MAILHOST 和 MAILROUTINGADDRESS, on page 20

路由：MAILHOST 和 MAILROUTINGADDRESS

对于路由查询，MAILHOST 的值不能是 IP 地址；它必须是可解析的主机名。这通常需要使用内部 DNSconfig。

MAILHOST 对于路由查询是可选的。如果未设置 MAILHOST，则 MAILROUTINGADDRESS 是必需项。

使用伪装查询重写信封发件人

伪装是根据构建的查询重写邮件中的信封发件人（也称为发件人或 MAIL FROM）以及 To:、From: 和/或CC:信头的一项功能。该功能的一个典型实施示例是允许从一个站点托管多个域的“虚拟域”。另一个典型实施是通过从邮件信头的字符串中“拆离”子域来“隐藏”网络基础设施。

相关主题

- 伪装查询示例 , on page 21
- 伪装“友好名称”, on page 21

伪装查询示例

Table 4: 常规 ***LDAP*** 实施的 ***LDAP*** 查询字符串示例：伪装

查询内容：	伪装
OpenLDAP	`(mailRoutingAddress={a})`
Microsoft Active Directory 通讯录	`(proxyaddresses=smtp:{a})`

SunONE Directory Server	`(mail={a})`
	`(mailAlternateAddress={a})`
	`(mailEquivalentAddress={a})`
	`(mailForwardingAddress={a})`
	`(mailRoutingAddress={a})`

伪装“友好名称”

在一些用户环境中，LDAP 目录服务器方案除了存储邮件路由地址或本地邮件地址外，可能还存储“友好名称”。AsyncOS 允许您使用此“友好地址”伪装信封发件人（针对传出邮件）和邮件信头（针对传入邮件，例如，To:、Reply To:、From: 或 CC: 信头）- 即使友好地址包含有效邮件地址中通常不允许使用的特殊字符（例如，引号、空格和逗号）。

当通过 LDAP 查询使用伪装信头时，现在可以选择配置是否将整个友好邮件字符串替换为 LDAP 服务器中的结果。请注意，即使启用了该行为，也只能将 user@domain 部分用于信封发件人（友好名称是非法的）。

与常规 LDAP 伪装一样，如果 LDAP 查询返回空结果（长度为零或全部为空格），则不会发生伪装。

要启用此功能，请在为侦听程序配置基于 LDAP 的伪装查询（通过“LDAP”页面或 `ldapconfig` 命令）时，对以下问题回答“y”：

```
Do you want the results of the returned attribute to replace the entire
friendly portion of the original recipient? [N]
```

例如，考虑以下 LDAP 条目示例：

属性	值
mailRoutingAddress	admin\@example.com
mailLocalAddress	joe.smith\@example.com
mailFriendlyAddress	“Administrator for example.com”，<joe.smith\@example.com>

如果启用了此功能，则 (mailRoutingAddress={a}) 的 LDAP 查询和 (mailLocalAddress) 的伪装属性将导致以下替换：

原始地址（发件人、收件人、抄送、回复）	伪装的信头	伪装的信封发件人
admin@example.com	发件人：“Administrator for example.com”，<joe.smith@example.com>	MAIL FROM：<joe.smith@example.com>

使用组 LDAP 查询确定收件人是否为组成员

可以定义对 LDAP 服务器的查询以确定收件人是否为 LDAP 目录所定义的组的成员。

Procedure

步骤 1 创建使用 rcpt-to-group 或 mail-from-group 规则对邮件执行操作的邮件过滤器。

步骤 2 然后，使用**系统管理 (System Administration)** > **LDAP** 页面（或 `ldapconfig` 命令）为要绑定到的邮件网关定义 LDAP 服务器并为组成员配置查询。

步骤 3 使用**网络 (Web)** > **侦听程序 (Listeners)**页面（或 `listenerconfig -> edit -> ldapgroup` 子命令）为侦听程序启用组查询。

What to do next

相关主题

- 组查询示例 , on page 23
- 配置组查询, on page 23

组查询示例

Table 5: 常规 ***LDAP*** 实施的 ***LDAP*** 查询字符串示例：组

查询内容：	组
OpenLDAP	默认情况下，OpenLDAP 不支持 memberOf 属性。LDAP 管理员可以将此属性或类似属性添加到方案。
Microsoft Active Directory	`(&(memberOf={g})(proxyAddresses=smtp:{a}))`
SunONE Directory Server	`(&(memberOf={g})(mailLocalAddress={a}))`

例如，假定您的 LDAP 目录将“营销”组的成员归类为 ou=Marketing。可以使用此分类来处理以特殊方式发送给或来自该组成员的邮件。步骤 1 会创建邮件过滤器以对邮件执行操作，并且步骤 2 和步骤 3 会启用 LDAP 查找机制。

配置组查询

在下面的示例中，来自营销组成员的邮件（如 LDAP 组“营销”所定义）将传输到备用传输主机 `marketingfolks.example.com`。

Procedure

步骤 1 首先，会创建邮件过滤器以对与组成员身份积极匹配的邮件执行操作。在本示例中，使用 `mail-from-group` 规则创建了过滤器。其信封发件人在 LDAP 组“marketing-group1”中的所有邮件都通过备用传输主机进行传输（过滤器 `alt-mailhost` 操作）。

组成员身份字段变量 (groupName) 将在步骤 2 中定义。组属性“groupName”使用值 `marketing-group1` 定义。

```
mail3.example.com> filters

Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> new
Enter filter script. Enter '.' on its own line to end.
MarketingGroupfilter:
if (mail-from-group == "marketing-group1") {
alt-mailhost ('marketingfolks.example.com');}
.
```

```
1 filters added.

Choose the operation you want to perform:

- NEW - Create a new filter.

- DELETE - Remove a filter.

- IMPORT - Import a filter script from a file.

- EXPORT - Export filters to a file

- MOVE - Move a filter to a different position.

- SET - Set a filter attribute.

- LIST - List the filters.

- DETAIL - Get detailed information on the filters.

- LOGCONFIG - Configure log subscriptions used by filters.

- ROLLOVERNOW - Roll over a filter log file.

[]>
```

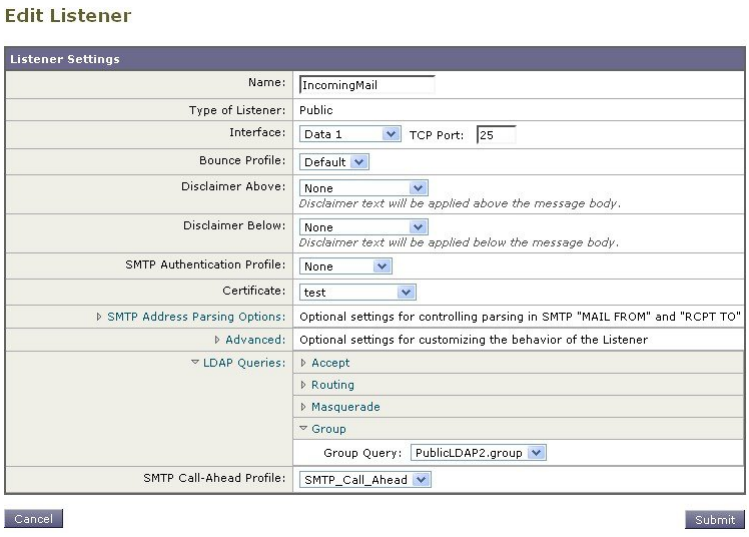
有关 `mail-from-group` 和 `rcpt-to-group` 邮件过滤器规则的详细信息，请参阅邮件过滤器规则。

步骤 2 接下来，使用“添加 LDAP 服务器配置文件”(Add LDAP Server Profile) 页面为要绑定到的邮件网关定义 LDAP 服务器，并为组成员身份配置初始查询。

步骤 3 接下来，公共侦听程序“InboundMail”更新为将LDAP查询用于组路由。使用“编辑侦听程序”(Edit Listener) 页面启用上面指定的 LDAP 查询。

由于此查询，侦听程序所接受的邮件会触发对 LDAP 服务器的查询以确定组成员身份。PublicLDAP2.group 查询先前通过**系统管理 (System Administration) > LDAP** 页定义。

Figure 6: 在侦听程序上指定组查询



步骤 4 提交并确认更改。

示例：使用组查询跳过垃圾邮件和病毒检查

由于邮件过滤器是渠道的早期阶段运行，因此可以使用组查询跳过对指定组的病毒和垃圾邮件检查。例如，您希望 IT 组接收所有邮件并跳过垃圾邮件和病毒检查。在 LDAP 记录中，创建一个使用 DN 作为组名称的组条目。组名称中包含下列 DN 条目：

cn=IT, ou=groups, o=sample.com

通过下列组查询创建 LDAP 服务器配置文件：

(&(memberOf={g})(proxyAddresses=smtp:{a}))

然后在侦听程序中启用此查询，以便在侦听程序收到邮件时，会触发组查询。

要为 IT 组的成员跳过病毒和垃圾邮件过滤，可以创建以下邮件过滤器，从而将传入邮件与 LDAP 组进行比较。

```
[]> - NEW - Create a new filter.

- IMPORT - Import a filter script from a file.

[]> new

Enter filter script. Enter '.' on its own line to end.

IT_Group_Filter:

if (rcpt-to-group == "cn=IT, ou=groups, o=sample.com"){

skip-spamcheck();

skip-viruscheck();

deliver();

}

.
1 filters added.
```


Note 此邮件过滤器中的 rcpt-to-group 反映作为组名称输入的 DN：cn=IT，ou=groups，o=sample.com。确认在邮件过滤器中使用了正确的组名称，以确保过滤器与 LDAP 目录中的名称匹配。

侦听程序所接受的邮件会触发对 LDAP 服务器的查询以确定组成员身份。如果邮件收件人是 IT 组的成员，则邮件过滤器会跳过病毒和垃圾邮件检查并将邮件发送给收件人。要启用该过滤器以检查 LDAP 查询的结果，必须在 LDAP 服务器上创建 LDAP 查询并在侦听程序上启用该 LDAP 查询。

使用基于域的查询路由到特定域

基于域的查询是按类型分组的 LDAP 查询，它们与域相关联，并且分配给特定侦听程序。如果有不同的 LDAP 服务器与不同的域关联，但是要为同一侦听程序上的所有 LDAP 服务器运行查询，则可能需要使用基于域的查询。例如，公司“MyCompany”收购了公司“HisCompany”和公司“HerCompany”，而且 MyCompany 保留其域 MyCompany.example.com 以及所收购公司的域 HisCompany.example.com 和 HerCompany.example.com，其为与每个域相关联的员工维护不同的 LDAP 服务器。要接受这三个域的邮件，MyCompany 会创建基于域的查询。这允许 MyCompany.example.com 在同一侦听程序上接受 Mycompany.example.com、HisCompany.example.com 和 HerCompany.example.com 的邮件。

Procedure

步骤 1 为要在基于域的查询中使用的域创建服务器配置文件。对于每个服务器配置文件，配置要用于基于域的查询的查询（接受、路由等）。有关详细信息，请参阅创建 LDAP 服务器配置文件以存储有关 LDAP 服务器的信息, on page 4。

步骤 2 创建基于域的查询。当创建基于域的查询时，从每个服务器配置文件中选择查询，并使邮件网关能够根据“信封收件人”(Envelope To) 字段中的域确定要运行的查询。有关创建查询的详细信息，请参阅创建基于域的查询, on page 26。

步骤 3 在公共或专用侦听程序上启用基于域的查询。有关配置侦听程序的详细信息，请参阅“配置网关以接收邮件”一章。

Note 还可以启用对垃圾邮件隔离区的 LDAP 最终用户访问或垃圾邮件通知启用基于域的查询。有关详细信息，请参阅“垃圾邮件隔离区”一章。

What to do next

相关主题

- 创建基于域的查询, on page 26

创建基于域的查询

从“系统管理”(System Administration) > “LDAP” > “LDAP 服务器配置文件”(LDAP Server Profiles) 页面创建基于域的查询。

Procedure

步骤 1 从“LDAP 服务器配置文件”(LDAP Server Profiles) 页面上，点击**高级 (Advanced)**。

步骤 2 点击**添加域分配 (Add Domain Assignments)**。

步骤 3 输入基于域的查询的名称。

步骤 4 选择查询类型。

Note 创建基于域的查询时，无法选择不同类型的查询。选择某种查询类型后，邮件网关将使用可用服务器配置文件中该类型的查询来填充查询字段。

步骤 5 在“域分配 (Domain Assignments)”字段中，输入域。

步骤 6 选择要与域关联的查询。

步骤 7 继续添加行，直到将所有域添加到查询。

步骤 8 如果所有其他查询失败，可以输入默认查询。如果不希望输入默认查询，请选择**无 (None)**。

步骤 9 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密码或者邮件地址，以测试查询。结果会显示在“连接状态”(Connection Status) 字段中。

步骤 10 或者，如果在接受查询使用 {f} 令牌，则可以将信封发件人地址添加到测试查询。

Note 创建了基于域的查询后，需要将其与公共或专用侦听程序相关联。

步骤 11 提交并确认更改。

使用链查询执行一系列 LDAP 查询

链查询是邮件网关连续尝试运行的一系列 LDAP 查询。邮件网关会尝试运行“链”中的每个查询，直到 LDAP 服务器返回正面响应（或者“链”中最后一个查询返回负面响应或失败）。对于链接的路由查询，邮件网关会按顺序对每个重写的邮件地址重新运行已配置的相同链查询。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，则链查询会非常有用。例如，您可能已经使用属性 maillocaladdress 和 mail 存储用户邮件地址。为了确保查询根据这两个属性行，可以使用链查询。

Procedure

步骤 1 为要在链查询中使用的每个查询创建服务器配置文件。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 服务器配置文件以存储有关 LDAP 服务器的信息, on page 4。

步骤 2 创建链查询。有关详细信息，请参阅创建链查询, on page 28。

步骤 3 在公共或专用侦听程序上启用链查询。有关配置侦听程序的详细信息，请参阅“配置网关以接收邮件”一章。

Note 还可以启用对垃圾邮件隔离区的LDAP最终用户访问或垃圾邮件通知启用基于域的查询。有关详细信息，请参阅“垃圾邮件隔离区”一章。

What to do next

相关主题

- 创建链查询, on page 28

创建链查询

从“系统管理”(System Administration)>“LDAP”>“LDAP 服务器配置文件”(LDAP Server Profiles)页面创建链查询。

Procedure

步骤 1 从“LDAP 服务器配置文件”(LDAP Server Profiles) 页面上，点击**高级 (Advanced)**。

步骤 2 点击**添加链查询 (Add Chain Query)**。

步骤 3 添加链查询的名称。

步骤 4 选择查询类型。

创建链查询时，无法选择不同类型的查询。选择某种查询类型后，邮件网关将使用可用服务器配置文件中该类型的查询来填充查询字段。

步骤 5 选择查询以添加到链查询。

邮件网关会按照配置顺序运行查询。因此，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，以便更常规的查询在更具体的查询之后。

步骤 6 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密码或者邮件地址，以测试查询。结果会显示在“连接状态”(Connection Status) 字段中。

步骤 7 或者，如果在接受查询使用 {f} 令牌，则可以将信封发件人地址添加到测试查询。

Note 创建了链查询后，需要将其与公共或专用侦听程序相关联。

步骤 8 提交并确认更改。

将 LDAP 用于目录搜集攻击预防

当恶意发件人尝试向具有通用名称的收件人发送邮件时，邮件网关通过验证该位置具有有效有效的收件人进行响应。当大规模执行时，恶意发件人通过“搜集”要发送垃圾邮件的有效地址，可以确定向谁发送邮件。

当使用 LDAP 接受验证查询时，邮件网关可以检测和阻止目录搜集攻击 (DHA)。可以在 SMTP 会话期间或在工作队列中配置 LDAP 接受以阻止目录搜集攻击。

相关主题

- SMTP 会话期间的目录搜集攻击预防, on page 28
- 工作队列中的目录搜集攻击防御, on page 30

SMTP 会话期间的目录搜集攻击预防

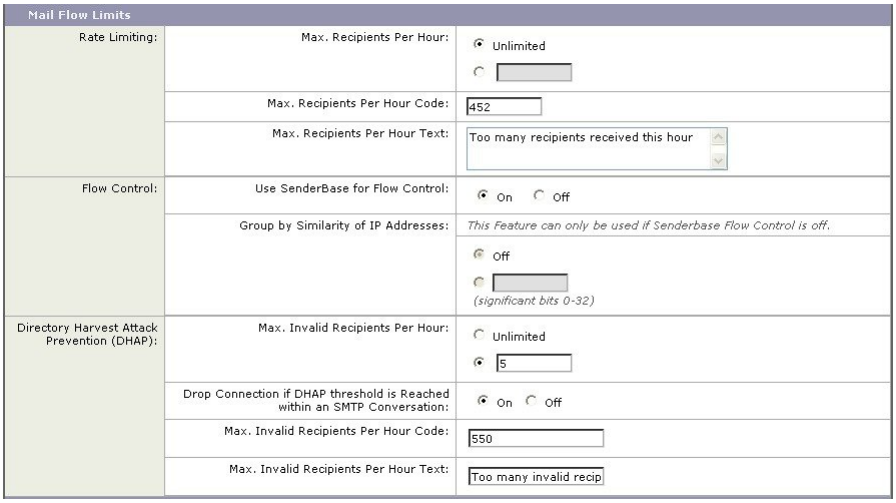
可以通过仅输入收件人访问表 (RAT) 中的域并在 SMTP 会话中执行 LDAP 接受验证来阻止 DHA。

要在 SMTP 会话期间丢弃邮件，请为 LDAP 接受配置 LDAP 服务器配置文件。然后，配置侦听程序以在 SMTP 会话期间执行 LDAP 接受查询。

Figure 7: **配置 *SMTP* 会话期间的接受查询**

为侦听程序配置了 LDAP 接受查询后，必须在与侦听程序关联的邮件流策略中配置 DHAP 设置。

Figure 8: **配置邮件流策略以丢弃 *SMTP* 会话中的连接**



在与侦听程序关联的邮件流策略中，配置以下目录搜集攻击预防设置：

- **每小时的最大无效收件人数量 (Max. Invalid Recipients Per hour)**。此侦听程序每小时将从远程主机接收的最大无效收件人数。此阈值表示 RAT 拒绝总数与在 SMTP 会话中丢弃或在工作队列中退回的无效 LDAP 收件人邮件的总数相结合的结果。例如，将阈值配置为 5，且计数器检测两个 RAT 拒绝和三个到无效 LDAP 收件人的已丢弃邮件。此时，邮件网关确定已达到阈值，并放弃连接。默认情况下，公共侦听程序的每小时最大收件人数量为 25。对于专用侦听程序，默认情况下的每小时最大收件人数量无限制。将其设置为“无限制”(Unlimited) 表示不为邮件流策略启用 DHAP。
- **如果在 SMTP 会话中达到 DHAP 阈值，则放弃连接 (Drop Connection if DHAP Threshold is reached within an SMTP conversation)**。将邮件网关配置为在达到目录搜集攻击预防阈值时放弃连接。
- **每小时最大收件人数代码 (Max. Recipients Per Hour Code)**。指定在放弃连接时使用的代码。默认代码为 550。

- **每小时最大收件人数文本 (Max. Recipients Per Hour Text)**。指定用于放弃的连接的文本。默认文本为“无效收件人过多”(Too many invalid recipients)。

如果达到阈值，当收件人无效时，邮件的信封发件人不会收到退回邮件。

工作队列中的目录搜集攻击防御

可以通过仅输入收件人访问表 (RAT) 中的域并在工作队列中执行 LDAP 接受来阻止大多数 DHA。该技术可防止恶意发件人在 SMTP 会话期间知道收件人是否有效。（如果配置了接受查询，系统会接受邮件并在工作队列中执行 LDAP 接受验证。）但是，当收件人无效时，邮件的信封发件人仍会收到退回邮件。

相关主题

- 在工作队列中配置 Directory Harvest Prevention, on page 30

在工作队列中配置 Directory Harvest Prevention

要阻止目录搜集攻击，首先应配置 LDAP 服务器配置文件，并启用 LDAP 接受。启用了 LDAP 接受查询后，将侦听程序配置为使用接受查询且为不匹配收件人的退回件：

接下来，配置邮件流策略以定义系统将根据特定时段的发送 IP 地址允许的无效收件人地址数。当超过该数字时，系统会将这种情况视为 DHA 并发送警报邮件。警报邮件将包含以下信息：

```
LDAP: Potential Directory Harvest Attack from host=('IP-address', 'domain_name
'), dhap_limit=n, sender_group=sender_group,

listener=listener_name, reverse_dns=(reverse_IP_address, 'domain_name
', 1), sender=envelope_sender, rcpt=envelope_recipients
```

系统将退回邮件，直到达到在邮件流策略中指定的阈值，然后以静默方式接收和丢弃其余邮件，从而通知合法发件人地址是错误的，但是避免恶意发件人确定哪些收件人被接受。

此无效收件人计数器的功能类似于 AsyncOS 中当前提供的速率限制功能：启用该功能并定义限制作为公共侦听程序 HAT 中邮件流策略的一部分（包括 HAT 的默认邮件流策略）。

还可以在命令行界面中使用 `listenerconfig` 命令配置此功能。

在 GUI 中编辑任何邮件流策略时也会显示该功能，只要在对应的侦听程序上配置了 LDAP 查询即可：

输入每小时无效收件人数量可为该邮件流策略启用 DHAP。默认情况下，公共侦听程序允许每小时 25 个无效收件人。对于专用侦听程序，默认情况下的每小时最大无效收件人数量无限制。将其设置为“无限制”(Unlimited) 表示不为邮件流策略启用 DHAP。

配置 AsyncOS 进行 SMTP 身份验证

AsyncOS 支持 SMTP 身份验证。SMTP 身份验证是用于验证连接到 SMTP 服务器的客户端的一种机制。

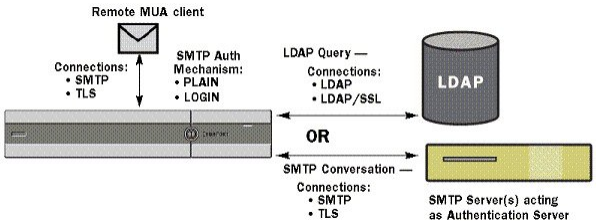
该机制的实用之处是：使给定组织中的用户可以使用该实体的邮件服务器发送邮件，即使他们利用远程连接（例如在家中或在旅行时）也是如此。邮件用户代理(MUA)可以在尝试发送邮件时发出身份验证请求（挑战/响应）。

用户还可以使用 SMTP 身份验证进行传出邮件中继。这允许邮件网关在其不位于网络边缘的配置中与中继服务器建立安全连接。

AsyncOS 支持两种验证用户凭据的方法：

- 可以使用 LDAP 目录。
- 您可以使用其他 SMTP 服务器（SMTP Auth 转发和 SMTP Auth 传出）。

***Figure 9: SMTP Auth* 支持：*LDAP* 目录存储或 *SMTP* 服务器**



然后使用配置的 SMTP 身份验证方法，通过 smtpauthconfig 命令创建 SMTP Auth 配置文件以在 HAT 邮件流策略中使用（请参阅在侦听程序上启用 SMTP 身份验证, on page 34）。

相关主题

- 配置 SMTP 身份验证, on page 31
- 配置 SMTP 身份验证查询, on page 32
- 通过另一个 SMTP 服务器进行 SMTP 身份验证（带转发的 SMTP 身份验证）, on page 33
- 通过 LDAP 进行 SMTP 身份验证, on page 33
- 使用客户端证书对 SMTP 会话进行身份验证, on page 37
- 传出 SMTP 身份验证, on page 37
- 记录和 SMTP 身份验证, on page 38

配置 SMTP 身份验证

如果要通过 LDAP 服务器进行身份验证，请在“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（或在 **`ldapconfig`** 命令中）选择 SMTPAUTH 查询类型以创建 SMTP 身份验证查询。对于配置的每个 LDAP 服务器，可以配置一个 SMTPAUTH 查询以用作 SMTP 身份验证配置文件。

有两种 SMTP 身份验证查询：LDAP 绑定和密码作为属性。当使用密码作为属性时，邮件网关会获取 LDAP 目录中的密码字段。密码可以以纯文本、加密或散列的形式存储。使用 LDAP 绑定时，邮件网关将尝试使用客户端提供的凭据登录到 LDAP 服务器。

相关主题

- 指定密码作为属性, on page 32

指定密码作为属性

根据 RFC 2307，OpenLDAP 中的约定是：用花括号将编码类型括起来作为编码密码的前缀（例如，“{SHA}5en6G6MezRroT3XKqkdPOmY/BfQ=”）。在本例中，应用 SHA 后，密码部分是纯文本密码的 base64 编码。

在获取密码之前，邮件网关与 MUA 协商 SASL 机制，而且邮件网关和 MUA 会决定采用的方法（支持 LOGIN、PLAIN、MD5、SHA、SSHA 和 CRYPT SASL 机制）。然后，设备会查询 LDAP 数据库以获取密码。在 LDAP 中，密码可以具有扩展花括号中的前缀。

- 如果没有前缀，则邮件网关假设密码是以纯文本形式存储在 LDAP 中。
- 如果有前缀，设备将获取散列密码，对 MUA 提供的用户名和/或密码执行散列，然后比较散列版本。根据将散列机制类型附加到密码字段中的散列密码的 RFC 2307 约定，邮件网关支持 SHA1 和 MD5 散列类型。
- 诸如 OpenWave LDAP 服务器等一些 LDAP 服务器不会在加密密码之前附加加密类型前缀；相反，它们将加密类型存储为单独的 LDAP 属性。在这些情况下，可以指定将密码与 SMTP 会话中包含的密码进行比较时邮件网关将使用的默认 SMTP AUTH 加密方法。

邮件网关从 SMTP Auth 交换中获取任意用户名，并将其转换为获取明文或散列密码字段的 LDAP 查询。然后，它对在 SMTP Auth 凭证中提供的密码执行必要的散列并将结果与其从 LDAP 检索到的结果（如有散列类型标记，则将其删除）进行比较。如果结果匹配，则表示 SMTP Auth 会话将继续。匹配失败将产生错误代码。

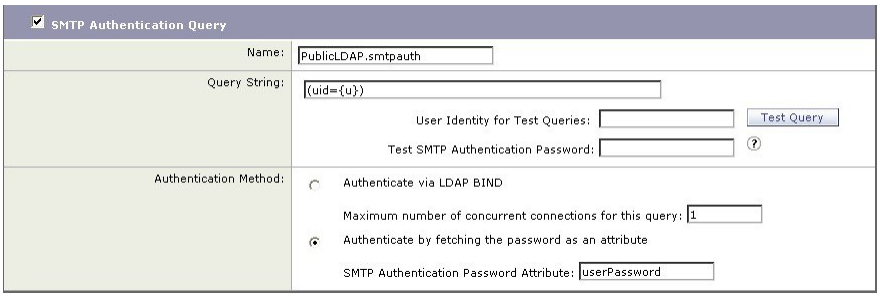
配置 SMTP 身份验证查询

***Table 6: SMTP Auth LDAP* 查询字段**

名称	查询的名称。
查询字符串	可以选择是通过 LDAP 绑定进行身份验证，还是获取密码作为属性。 **绑定**：尝试使用客户端提供的凭据登录到 LDAP 服务器（这称为 LDAP 绑定）。 指定 SMTP Auth 查询将使用的最大并发连接数。此号码不应超过在上述 LDAP 服务器属性中指定的数量。请注意，为了避免绑定身份验证出现大量会话超时，请增加此处的最大并发连接数（通常接近可分配到 SMTP Auth 的所有连接数）。新的连接将用于每个绑定身份验证。连接的其余部分将与其他 LDAP 查询类型共享。 **密码作为属性**：要通过获取密码进行身份验证，请在下面的 SMTP Auth 密码属性字段中指定密码。 指定用于任何一种身份验证的 LDAP 查询。Active Directory 示例查询：(&(samaccountname={u})(objectCategory=person)(objectClass=user))
SMTP 身份验证密码属性	如果选择了“通过获取密码作为属性进行身份验证”，可以在此处指定密码属性。

在下面的示例中，“系统管理”(System Administration)>“LDAP”页面用于编辑名为“PublicLDAP”的 LDAP 配置以包括 SMTPAUTH 查询。将构建查询字符串 (uid={u}) 来匹配 userPassword 属性。

Figure 10: SMTP 身份验证查询



当配置了 SMTPAUTH 配置文件后，可以指定侦听程序使用该查询进行 SMTP 身份验证。

通过另一个 SMTP 服务器进行 SMTP 身份验证（带转发的 SMTP 身份验证）

可以配置邮件网关来验证提供给与其他 SMTP 服务器进行的其他 SMTP 身份验证会话的用户名和密码。

身份验证服务器不是传输邮件的服务器；相反，它只对 SMTP 身份验证请求做出响应。如果身份验证成功，则可通过专用邮件服务器继续进行 SMTP 邮件传输。此功能有时称为“带转发的 SMTP 身份验证”，因为仅会将凭据转发（或“代理”）到另一个 SMTP 服务器进行身份验证。

Procedure

步骤 1 依次选择**网络 (Network) > SMTP 身份验证 (SMTP Authentication)**。

步骤 2 点击**添加配置文件 (Add Profile)**。.

步骤 3 为 SMTP 身份验证配置文件输入唯一的名称。

步骤 4 对于**配置文件类型 (Profile Type)**，选择**转发 (Forward)**。

步骤 5 点击**下一步 (Next)**。

步骤 6 输入转发服务器的主机名/IP 地址和端口。选择用于转发身份验证请求的转发接口。指定最大同时连接数。然后，可以配置是否需要 TLS 以从邮件网关连接到转发服务器。此外，如果可用，还可以选择要使用的 SASL 方法（PLAIN 或 LOGIN）。此选择配置用于每个转发服务器。

步骤 7 提交并确认更改。

步骤 8 创建了身份验证配置文件后，可以在侦听程序上启用该配置文件。有关详细信息，请参阅在侦听程序上启用 SMTP 身份验证, on page 34。

通过 LDAP 进行 SMTP 身份验证

要创建基于 LDAP 的 SMTP 身份验证配置文件，必须先前已使用“系统管理”(System Administration) >“LDAP”页面创建了与 LDAP 服务器配置文件相结合的 SMTP 身份验证查询。然后，可以使用此

配置文件创建 SMTP 身份验证配置文件。有关创建 LDAP 配置文件的详细信息，请参阅了解 LDAP 查询, on page 2。

Procedure

步骤 1 依次选择**网络 (Network) > SMTP 身份验证 (SMTP Authentication)**。

步骤 2 点击**添加配置文件 (Add Profile)**。

步骤 3 为 SMTP 身份验证配置文件输入唯一的名称。

步骤 4 对于“配置文件类型”(Profile Type)，选择 **LDAP**。

步骤 5 点击**下一步 (Next)**。

步骤 6 选择要用于此身份验证配置文件的 LDAP 查询。

步骤 7 从下拉菜单中选择默认加密方法。可以从 SHA、Salted SHA、Crypt、Plain 或 MD5 中进行选择。如果 LDAP 服务器在加密密码前面加上加密类型前缀，请将“无”保持选中状态。如果 LDAP 服务器将加密类型作为单独的实体（例如，OpenWave LDAP 服务器）保存，请从菜单中选择一种加密方法。如果 LDAP 查询使用的是绑定，则不会使用默认加密设置。

步骤 8 点击**完成 (Finish)**。

步骤 9 提交并确认更改。

步骤 10 创建了身份验证配置文件后，可以在侦听程序上启用该配置文件。有关详细信息，请参阅在侦听程序上启用 SMTP 身份验证, on page 34。

What to do next

相关主题

- 在侦听程序上启用 SMTP 身份验证, on page 34

在侦听程序上启用 SMTP 身份验证

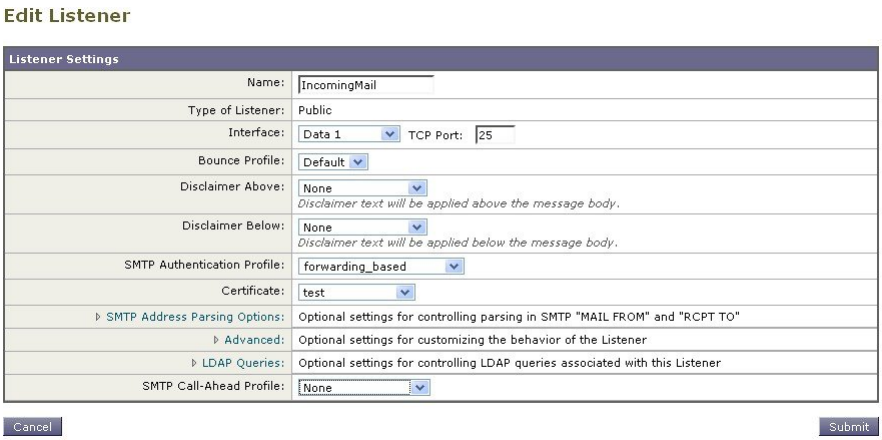
在使用**网络 (Web) > SMTP 身份验证 (SMTP Authentication)** 页面创建了用于指定要执行的 SMTP 身份验证类型（基于 LDAP 或基于 SMTP 转发）的 SMTP 身份验证“配置文件”后，必须使用**网络 (Web) > 侦听程序 (Listeners)** 页面（或 **`listenerconfig`** 命令）将该配置文件与侦听程序相关联。

Note 经过身份验证的用户将在其当前邮件流策略中获得 RELAY 连接行为。

可以在配置文件中指定多个转发服务器。在邮件网关和转发服务器之间不支持SASL机制CRAM-MD5和DIGEST-MD5。

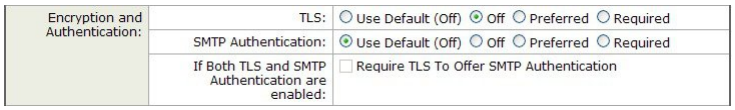
在下面的示例中，编辑了侦听程序“InboundMail”以使用通过“编辑侦听程序”(Edit Listener) 页面配置的 SMTPAUTH 配置文件。

Figure 11: 通过“编辑侦听程序”*(Edit Listener)* 页面选择 *SMTP* 身份验证配置文件



配置了某个侦听程序以使用配置文件后，可以更改主机访问表的默认设置，以使侦听程序允许、禁止或要求 SMTP 身份验证：

Figure 12: 在邮件流策略上启用 *SMTP* 身份验证



编号	说明
1.	“SMTP 身份验证”(SMTP Authentication) 字段为 SMTP 身份验证提供侦听程序级别的控制。如果选择“否”(No)，则不会在侦听程序上启用身份验证，不管配置任何其他 SMTP 身份验证设置都是如此。
2.	如果在第二个提示符（“SMTP 身份验证：”[SMTP Authentication:]）选择“必填”(Required)，则不会发出任何 AUTH 关键字，直到协商 TLS（客户端发出第二个 EHLO 命令）为止。

相关主题

- SMTP 身份验证和 HAT 策略设置, on page 35
- HAT 延迟的拒绝, on page 36

SMTP 身份验证和 HAT 策略设置

由于在 SMTP 身份验证协商开始之前发件人分为适当的发件人组，因此主机访问表 (HAT) 设置不会受到影响。当连接远程邮件主机时，邮件网关会先确定应用哪个发件人组并对该发件人组施加邮件策略。例如，如果远程 MTA“suspicious.com”在您的 SUSPECTLIST 发件人组中，则会应用 THROTTLE 策略，不管“suspicious.com”的 SMTPAUTH 协商结果如何都是如此。

但是，不使用 SMTPAUTH 进行身份验证的发件人将得到与“正常”发件人不同的对待。成功 SMTPAUTH 会话的连接行为会更改为“RELAY”，从而有效地绕过收件人访问表 (RAT) 和

LDAPACCEPT。这允许发件人通过邮件网关中转邮件。如上所述，应用的任何速率限制或限制都将继续有效。

HAT 延迟的拒绝

当配置了 HAT 延迟的拒绝时，根据 HAT 发件人组喝邮件流策略配置将被丢弃的连接可能仍能够成功进行身份验证并获得 RELAY 邮件流策略授权。

配置是否在邮件收件人级别执行 HAT 拒绝。默认情况下，HAT 拒绝的连接将关闭，并且在 SMTP 会话开始处显示标语消息。

当邮件因 HAT“拒绝”(Reject) 设置而被拒绝时，AsyncOS 可在邮件收件人级别 (RCPT TO)（而不是在SMTP会话开始时）执行拒绝。通过此方式拒绝邮件会延迟邮件拒绝并退回邮件，以便AsyncOS保留更多有关已拒绝邮件的详细信息。例如，可以通过被阻止的邮件的地址和每个收件人地址查看邮件。延迟 HAT 拒绝还可以降低发送 MTA 将执行多次重试的可能性。

在启用 HAT 延迟拒绝后，将发生以下行为：

- MAIL FROM 命令将被接受，但不会创建邮件对象。
- 所有 RCPT TO 命令都将被拒绝，并显示一段文本，阐明发送邮件的权限已被拒绝。
- 如果发送 MTA 通过 SMTP AUTH 进行身份验证，则它们将被授予“中继”(RELAY) 策略，并且允许它们正常传送邮件。

可以使用 `listenerconfig --> setup` CLI 命令配置延迟拒绝。默认情况下禁用此行为。

下表显示了如何为 HAT 配置延迟拒绝。

```
example.com> listenerconfig

Currently configured listeners:

1. listener1 (on main, 172.22.138.17) QMQP TCP Port 628 Private

2. listener2 (on main, 172.22.138.17) SMTP TCP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> setup

Enter the global limit for concurrent connections to be allowed across all listeners.

[300]>

[...]
```

```
By default HAT rejected connections will be closed with a banner
message at the start of the SMTP conversation. Would you like to do the rejection at the
message recipient level instead for more detailed logging of rejected mail?

[N]> y

Do you want to modify the SMTP RCPT TO reject response in this case?

[N]> y

Enter the SMTP code to use in the response. 550 is the standard code.

[550]> 551

Enter your custom SMTP response. Press Enter on a blank line to finish.

Sender rejected due to local mail policy.

Contact your mail admin for assistance.
```

使用客户端证书对 SMTP 会话进行身份验证

邮件网关支持使用客户端证书对邮件网关与用户邮件客户端之间的 SMTP 会话进行身份验证。

当创建 SMTP 身份验证配置文件时，选择要用于验证证书的证书身份验证 LDAP 查询。还可以指定客户端证书不可用时，邮件网关是否退回 SMTP AUTH 命令以对用户进行身份验证。

如果贵组织使用客户端证书对用户进行身份验证，则可以选择使用 SMTP 身份验证查询来检查没有客户端证书的用户是否只要其记录指定为允许便可发送邮件。

传出 SMTP 身份验证

SMTP 身份验证还可用于使用用户名和密码为出站邮件中继提供验证。创建“传出”SMTP 身份验证配置文件，然后将配置文件附加到 ALL 域的 SMTP 路由。在每个邮件传输尝试中，邮件网关使用必要的凭据登录到上游邮件中继。SMTP 身份验证支持以下授权协议：PLAIN 和 LOGIN。

Procedure

步骤 1 创建传出 SMTP 身份验证配置文件。

- **a.** 依次选择**网络 (Network) > SMTP 身份验证 (SMTP Authentication)**。
- **b.** 点击**添加配置文件 (Add Profile)**。
- **c.** 为 SMTP 身份验证配置文件输入唯一的名称。
- **d.** 对于配置文件类型，选择**传出 (Outgoing)**。
- **e.** 点击**下一步 (Next)**。
- **f.** 为身份验证配置文件输入身份验证用户名和密码。
- **g.** 点击**完成 (Finish)**。

步骤 2 配置 SMTP 路由以使用在步骤 1 中创建的传出 SMTP 身份验证配置文件。

a. 依次选择**网络 (Network) > SMTP 路由 (SMTP Routes)**。
b. 点击**接收域 (Receiving Domain)** 列中的**所有其他域 (All Other Domains)** 链接。
c. 为 SMTP 路由输入目标主机的名称。这是用于发送传出邮件的外部邮件中继的主机名。
d. 从下拉菜单中选择传出 SMTP 身份验证配置文件。
e. 提交并确认更改。

记录和 SMTP 身份验证

当在邮件网关上配置了 SMTP 身份验证机制（基于 LDAP、基于 SMTP 转发服务器或 SMTP 传出）时，以下事件将记录在邮件日志中：

- [仅供参考] 成功的 SMTP 身份验证尝试 - 包括进行了身份验证的用户和使用的机制。（不会记录纯文本密码。）
- [仅供参考] 未成功的 SMTP 身份验证尝试 - 包括进行了身份验证的用户和使用的机制。
- [警告] 无法连接到身份验证服务器 - 包括服务器名称和机制。
- [警告]等待身份验证请求期间转发服务器（与上游注入邮件网关通信）超时所引起的超时事件。

为用户配置外部 LDAP 身份验证

可以将邮件网关配置为使用网络上的 LDAP 目录对管理用户进行身份验证，方法是允许他们通过其 LDAP 用户名和密码进行登录。为 LDAP 服务器配置了身份验证查询后，在 GUI 的**系统管理 (System Administration) > 用户 (Users)** 页面中（或在 CLI 中使用 **userconfig** 命令）为邮件网关启用使用外部身份验证的功能。

Procedure

步骤 1 **创建查询以查找用户账户**。在 LDAP 服务器配置文件中，创建一个查询以在 LDAP 目录中搜索用户账户。

步骤 2 **创建组成员身份查询**。创建查询来确定用户是否为某个目录组的成员。

步骤 3 **设置外部身份验证以使用 LDAP 服务器**。使邮件网关能够使用 LDAP 服务器进行用户身份验证，将用户角色分配给 LDAP 目录中的组。有关详细信息，请参阅“分配管理任务”一章中的“添加用户”。

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。有关详细信息，请参阅测试 LDAP 查询, on page 17。

What to do next

相关主题

- 用户账户查询, on page 39

• 组成员身份查询, on page 39

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。如果在 LDAP 用户记录的 RFC 2307 中定义了属性（shadowLastChange、shadowMax 和 shadowExpire），则可以选择使邮件网关拒绝帐户过期的用户。在用户记录所在的域级别需要基本 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用户全名属性。

Table 7: 默认用户账户查询字符串和属性：***Active Directory***

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用户全名属性。

Table 8: 默认用户账户查询字符串和属性：***OpenLDAP***

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

组成员身份查询

AsyncOS 还使用查询来确定用户是否为某个目录组的成员。目录组成员身份中的成员身份会确定系统中的用户权限。在 GUI 的“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。

配置 LDAP 配置文件以查询组成员身份时，输入可以找到组记录的目录级别的基本 DN，保存组成员用户名的属性，以及包含组名的属性。根据为 LDAP 服务器配置文件选择的服务器类型，AysncOS 会输入用户名和组名属性的默认值，以及默认查询字符串。

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 LDAP 方案在“memberof”列表中使用可分辨名称而不是用户名，则可以使用 {dn} 而不是 {u}。

下表显示了 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 9: 默认组成员查询字符串和属性：***Active Directory***

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 LDAP 方案在 memberOf 列表中使用可分辨名称而不是用户名，则可以将 {u} 替换为 {dn}。
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

下表显示了 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 10: 默认组成员查询字符串和属性：***OpenLDAP***

服务器类型	**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}))
保存每个成员的用户名（或用户记录的 DN）的属性	memberUid
包含组名的属性	cn

对垃圾邮件隔离区的最终用户进行身份验证

垃圾邮件隔离区最终用户身份验证查询会在用户登录垃圾邮件隔离区时对他们进行验证。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。

如果希望垃圾邮件隔离区将LDAP查询用于最终用户访问，请选中“指定为活动查询”(Designate as the active query) 复选框。如果有现有的有效查询，则禁用此选项。打开**系统管理 (System Administration) > LDAP** 页面后，有效查询旁边会显示一个星号 (*)。

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，Active Directory 服务器的主邮件属性为 proxyAddresses，OpenLDAP 服务器的主邮件属性为 mail。可以输入自己的查询和邮件属性。要通过 CLI 创建查询，请使用 ldapconfig 命令的 isqauth 子命令。

Note 如果希望用户使用其完整邮件地址登录，请将 (mail=smtp:{a}) 用于查询字符串。

相关主题

- Active Directory 最终用户身份验证设置示例, on page 41
- OpenLDAP 别名整合设置示例, on page 43
- 配置最终用户访问垃圾邮件隔离区的权限

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、mail 和 proxyAddresses 邮件属性使用密码身份验证，为 Active Directory 服务器的最终用户身份验证使用默认查询字符串。

Table 11: 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	使用密码（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]

身份验证方法	使用密码（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。）
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、mail 和 mailLocalAddress 邮件属性使用匿名身份验证，为 OpenLDAP 服务器的最终用户身份验证使用默认查询字符串。

Table 12: 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。

如果希望垃圾邮件隔离区将 LDAP 查询用于垃圾邮件通知，请选中“指定为活动查询”(Designate as the active query) 复选框。如果有现有的有效查询，则禁用此选项。打开“系统管理”(System Administration) >“LDAP”页面时，会在有效查询旁边会显示一个星号 (*)。

对于 Active Directory 服务器，默认查询字符串为 (|(proxyAddresses={a})(proxyAddresses=smtp:{a}))，默认邮件属性为 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。

相关主题

- Active Directory 别名整合设置示例, on page 43
- OpenLDAP 别名整合设置示例, on page 43

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 13: 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

Note 本示例仅用于演示。查询和 OU 或树设置可能因环境和配置而异。

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 14: 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

身份验证方法	匿名
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

Note 本示例仅用于演示。查询和 OU 或树设置可能因环境和配置而异。

用户可分辨名称设置示例

此部分显示 Active Directory 服务器和用户可分辨名称查询的设置示例。此示例为 Active Directory 服务器使用匿名身份验证，并且为 Active Directory 服务器的用户可分辨名称检索使用查询字符串。

Table 15: 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	`(proxyAddresses=smtp:{a})`

Note 本示例仅用于演示。查询和 OU 或树设置可能因环境和配置而异。

将 AsyncOS 配置为与多个 LDAP 服务器配合使用

配置LDAP配置文件时，可以配置邮件网关以连接到列表中的多个LDAP服务器。要使用多个LDAP服务器，必需将LDAP服务器配置为包含相同的信息、使用相同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）。

将邮件网关配置为连接到冗余 LDAP 服务器时，可以配置 LDAP 配置以进行故障转移或负载均衡。

可以使用多个 LDAP 服务器以获得以下结果：

- **故障转移**。当配置 LDAP 配置文件以进行故障转移时，如果邮件网关无法连接到第一台 LDAP 服务器，则会故障转移到列表中的下一台 LDAP 服务器。
- **负载均衡**。配置 LDAP 配置文件以实现负载均衡时，邮件网关会在执行 LDAP 查询期间在列出的 LDAP 服务器之间分发连接。

可以在“系统管理”(System Administration) >“LDAP”页面上，或使用 CLI 的 ldapconfig 命令配置冗余 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）来测试与 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。

相关主题

- 故障转移, on page 45
- 负载均衡, on page 46

故障转移

要确保 LDAP 查询得到解决，可以配置 LDAP 配置文件以进行故障转移。如果与 LDAP 服务器的连接失败，或者查询返回特定的错误代码（例如，“不可用”或“忙”），则邮件网关将尝试查询列表中指定的下一台 LDAP 服务器。

邮件网关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。如果邮件网关无法连接到列表中的第一台 LDAP 服务器，或者查询返回特定错误代码（例如，“不可用”或“忙”），则邮件网关将尝试连接到列表中的下一台 LDAP 服务器。默认情况下，邮件网关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。为确保邮件网关在默认情况下连接到主 LDAP 服务器，请务必将其输入为 LDAP 服务器列表中的第一台服务器。

如果邮件网关连接到第二个或后续的 LDAP 服务器，它将保持连接到该服务器的状态，直到出现超时。出现超时后，它会尝试重新连接到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。

相关主题

- 配置邮件网关进行 LDAP 故障转移, on page 46

配置邮件网关进行 LDAP 故障转移

要配置邮件网关进行 LDAP 故障转移，请在 GUI 中完成以下步骤：

Procedure

步骤 1 从“系统管理”(System Administration) >“LDAP”中，选择要编辑的 LDAP 服务器配置文件。

步骤 2 从 LDAP 服务器配置文件中，配置以下设置：

编号	说明
1	列出 LDAP 服务器。
2	配置最大连接数。

步骤 3 配置其他 LDAP 设置并确认更改。

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。

为负载均衡配置 LDAP 配置文件时，邮件网关会在列出的 LDAP 服务器之间分发连接。如果连接失败或超时，邮件网关会确定哪些 LDAP 服务器可用，并重新连接到可用的服务器。邮件网关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，邮件网关将在剩余的 LDAP 服务器之间分发的连接。

相关主题

- 为邮件网关配置负载均衡, on page 46

为邮件网关配置负载均衡

Procedure

步骤 1 从**系统管理 (System Administration) > LDAP** 中，选择要编辑的 LDAP 服务器配置文件。

步骤 2 从 LDAP 服务器配置文件中，配置以下设置：

编号	说明
1	列出 LDAP 服务器
2	配置最大连接数

步骤 3 配置其他 LDAP 设置并确认更改。

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。