

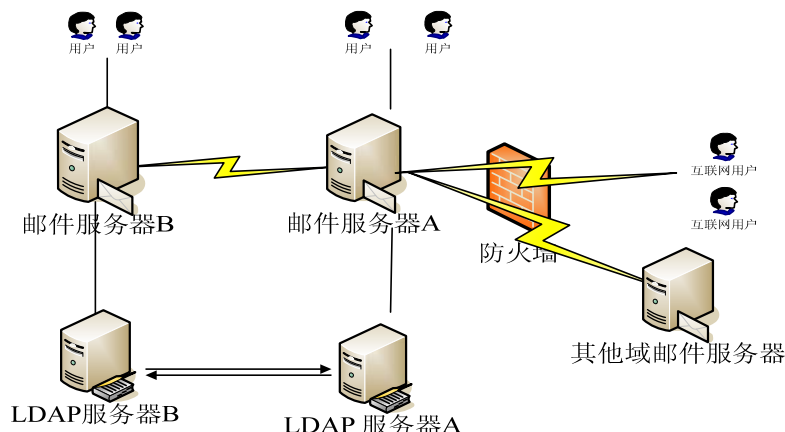
金笛邮件系统 LDAP 分布式设计



1. 分布式架构

系统采用多点平行的分布式结构。

假设客户有多台分布于不同地方的服务邮件服务器，而这些服务器会组成一个统一整体的服务器群组，服务于一个统一的域名。



如图服务器 A,B 分别在城市 A,B, 分别服务于 A, B 两地的用户, A,B 两台服务器都具有统一的域名: test.com。

同时 LDAP 服务器 A,B 分别在 A,B 两地, A,B 两台 LDAP 服务器通过同步服务保持数据同步。

A,B LDAP 服务器保存以下主要用户信息:

- 1.用户名、密码, 域名
- 2.用户所属邮件服务的 IP

A,B you 邮件服务器提供以下功能:

- 1.B 邮件服务器可设置非本地邮件转发服务器地址, 本例子中指定 A 服务器。
- 2.A 邮件服务器可设置, 可转发服务器地址 (B)。同时指定非本域邮件直接投递到互联网。
- 3.当接收用户发来的邮件的时候, 邮件服务器查询 LDAP 服务器, 根据用户所在邮件服务器的 IP, 转发到相应的目的邮件服务器。

系统出现的几种邮件发送投递情况:

1. 同一邮件服务器内用户互发, 此时邮件服务可根据同域内用户邮件服务器 IP 判断目标用户在同一服务器内, 直接进行本地投递。
2. A 邮件服务器用户发给 B 邮件服务器用户, 此时 A 邮件服务器判断到用户在 B 服务器, 邮件被投递到 B 服务器, 无需经过互联网的转送。
3. B 邮件服务器用户发送邮件到互联网, 此时 B 邮件服务器判断到本域的互联网出口在 A 服务器, 会把邮件转发到 A 服务器, 由 A 服务器再转发到互联网。
4. 由外域发到 test.com 整个域内邮件, 由 A 服务器统一接收, A 服务器再根据域内用户分布情况进行分发。



2. ACL 控制

该模块可以提供基于访问列表的邮件发送目标控制，访问列表的大致样式可以如下图所示：

No.	Sender	Department	Receiver	Subject	Content	Subject	of
-----	--------	------------	----------	---------	---------	---------	----

attachment

Deny/ Allow

1

2

3

4

具有优先级功能,例如,No.1---No.4 中 No.1 级别最高,No.4 级别最低.往外网发出的信件只能够发到指定的一些信箱中 (即白名单).其中, 发送方可以是一个具体的邮件地址或者 All@域名。本系统可以配置发送方不能和接收方的邮件地址相同。同时, 系统需要对所有的应用控制协议有明确的、独立的日志, 以标志每一封邮件在什么时间因为何种规则被发送或者被拒绝。

访问控制列表的日志与系统标准日志分开, 可以进行独立管理和备份。

同时, 本系统将对所有拒绝的邮件进行备份, 如保存在: REJECT@test.com

ACL 可根据邮件的: 发送件人, 部门, 收件人, 主题, 内容, 附件名对邮件进行过滤判断。

3. 审核功能

为了保证每一封邮件的发送都是安全的, 在必要的情况下, 系统管理员应该可以手工决定邮件是否被发送。

(1)系统在管理界面上提供一个可选项, 标志是否采用人工手工控制发送的邮件发送模式;

(2) 当管理员不选择该操作模式时, 自动运行的方式来发邮件

当管理员选择该操作模式时, 整个系统的邮件发送工作不会自动完成。每一封邮件的发送都必须等待管理员的手工确认, 之后才会发送出去

4. 日志报表

系统通过服务分类日志系统详细的记录了, 一份邮件通过邮件服务器处理的整个过程。管理员可通过系统的日志报告生成模块, 定义个性化的日志报表统计输出格式, 在一定时间间隔, 自动的生成日志报告, 并可指定这些报告自动发送到指定的邮件账号。

输出格式包含:

1) 文本

2) HTML

3) EXCEL