

Zimbra Daffodil (v10)管理员指南

Zimbra 水仙花 (v10)

目录

执照

介绍

观众

第三方组件

支持和联系信息

产品生命周期

组件弃用声明

产品概述

架构概述

核心电子邮件、日历和协作功能

Zimbra 组件

Zimbra 应用程序包

邮件流 - 多服务器配置

Zimbra 系统目录树

Zimbra Web 应用程序

Web 服务和桌面客户端

离线模式

安全措施

身份和访问管理

信息安全和隐私

系统日志 Zimbra

Daffodil (v10.1) 许可

LDAP 属性

许可证功能

Zimbra Daffodil (v10.1) 许可证要求 许可证使用情况 (按

Zimbra 协作帐户类型)

许可证激活

在线激活许可证

管理控制台

命令行

离线许可证激活

先决条件

安装离线守护程序包

申请并激活脱机许可证

当未安装或激活许可证时

获取License

许可证协调和数据收集通知

管理控制台增强功能

概述

存储管理功能的许可证检查

宽限期

LDS/第三方许可证服务器不可用

许可证到期

宽限期内的功能

许可证到期

宽限期内的功能

通知

使用预防

增强的zmlicense命令

激活在线许可证密钥 - zmlicense -a

激活脱机许可证 XML 文件 - zmlicense -A

打印许可证详细信息 - zmlicense -p

检查许可证状态 - zmlicense -c

检查单个功能状态 - zmlicense -fc <feature-code>

刷新许可证缓存 - zmlicense -rc

许可证守护程序服务 [LDS]

概述

系统要求

端口

安装单独的许可证守护程序服务节点

在单独的服务器上安装zimbra-license-daemon包

设置邮箱服务器

LDS 管理命令zmlicensectl

故障排除

Zimbra 邮箱服务器

邮箱服务器

消息存储

数据存储

索引存储

Web 应用程序服务器

邮件存储服务

用户界面服务

备份邮箱服务器

邮箱服务器日志

信息访问协议

常见的 IMAP 配置设置

Zimbra LDAP 服务

LDAP 流量

LDAP 目录层次结构

Zimbra 协作 LDAP 模式

Zimbra 协作对象

账户认证

内部认证机制

外部 LDAP 和外部 AD 身份验证机制

自定义身份验证

Kerberos5 身份验证机制

全局地址列表

Zimbra Collaboration 中的 GAL 属性

Zimbra Collaboration GAL 搜索参数

修改属性

刷新 LDAP 缓存

清除主题和区域设置的缓存

清除账户、组、COS、域和服务器

刷新全局属性

Zimbra 邮件传输代理

传入邮件路由概述

Zimbra MTA 部署

Postfix 配置文件

SMTP 身份验证

SMTP 限制

将非本地邮件发送到不同的服务器

防病毒和反垃圾邮件保护

防病毒保护

反垃圾邮件保护

接收和发送邮件

消息队列

来自外部域的邮件的消息横幅

修改消息

Zimbra 代理服务器

使用 Zimbra Proxy 的好处

Zimbra 代理组件

代理架构和流程

更改 Zimbra 代理配置

Zimbra 代理

Zimbra 代理端口

严格执行服务器名称

安装 HTTP 代理后设置 IMAP 和 POP 代理

配置 Zimbra HTTP 代理

设置 HTTP 代理

设置代理信任的 IP 地址

配置 Zimbra 代理进行 Kerberos 身份验证

Zimbra 管理控制台

管理员帐户

登录管理控制台

修改管理员密码

自定义登录和注销页面

管理任务

浏览用户界面

主页导航窗格

主页界面

监控界面

管理用户界面

配置 UI

全局设置用户界面

工具和迁移 UI

搜索用户界面

设置简单搜索

帮助中心界面

协作者表中的工具

每日讯息

结束当天的信息

创建每日讯息

删除每日消息

功能参考

GUI 路线图

弹出菜单选项

容器

管理配置

全局配置

常规信息配置

附件配置

设置电子邮件附件规则

按文件类型阻止电子邮件附件

MTA 配置

全局 IMAP 和 POP 配置

使用域

域常规信息配置

全局地址列表 (GAL) 模式配置

使用 GAL 同步帐户更快地访问 GAL

身份验证模式

虚拟主机

设置账户限制

重命名域

添加域别名

启用对域免责声明的支持

禁用域内电子邮件的免责声明

禁用免责声明功能

域中的 Zimlets

管理服务器设置

常规服务器设置

更改 MTA 服务器设置

设置 IP 地址绑定

管理 Zimbra 的 SSL 证书

安装证书

查看已安装的证书

维护有效证书

为域安装 SSL 证书

使用 DKIM 验证电子邮件消息

配置 Zimbra Collaboration 进行 DKIM 签名

更新域的 DKIM 数据

从 Zimbra 中删除 DKIM 签名

检索域的 DKIM 数据

反垃圾邮件设置

反垃圾邮件训练过滤器

禁用垃圾邮件训练邮箱

手动训练垃圾邮件过滤器

保护别名域免受反向散射垃圾邮件的侵害

禁用 Postfix 策略守护进程

使用 CLI 添加 RBL

为标记为垃圾邮件和白名单的邮件设置全局规则

防病毒设置

Zimbra 空闲/忙碌日历安排

Exchange 设置要求

在 Zimbra Collaboration 上配置空闲/忙碌

Zimbra Collaboration 与 Zimbra Collaboration 空闲/忙碌互操作性

设置 S/MIME

使用基于客户端的解决方案设置使用 S/MIME 功能

使用基于服务器的解决方案设置使用 S/MIME 功能

电子邮件保留管理

配置电子邮件生命周期规则

清除电子邮件

配置消息保留和删除策略

全球保留政策

COS 保留政策

管理垃圾箱

配置帐户的合法保留

定制管理扩展

部署新的管理控制台 UI 模块

删除管理扩展模块

短暂数据

配置正在运行的 Zimbra 协作以使用 SSDB

迁移程序

迁移详情

移民信息

更改临时后端 URL

转发短暂数据

高级迁移选项

迁移限制

对 zmprov 的更改

迁移 CSV 输出

账户删除行为

SSDB 安装和配置

安装

配置选项概述

通过主从复制实现高可用性

通过主-主复制实现高可用性

通过多主配置进行水平扩展

主从复制

概述

所需软件包

先决条件

配置

主-主复制

概述

所需软件包

先决条件

配置

多主扩展/复制

概述

LDAP 属性

使所有用户会话无效

与 Zimbra Collaboration 合作扩展 SSDB 以满足生产负载

最低推荐 SSDB 配置

结论

服务等级和账户

使用 COS 管理功能和设置

选择功能和首选项

禁用偏好设置

设置默认时区

使用服务器池

设置账户配额

查看账户配额

在域中设置配额

管理超额配额

管理密码

将用户引导至您的“更改密码”页面

配置密码策略

阻止常用密码

管理登录策略

关于双重身份验证

管理会话超时策略

管理默认外部 COS

自定义帐户

消息传递和协作应用程序

电子邮件消息功能

联系人功能

日历功能

解决日历约会问题

更改远程日历更新间隔

禁止与会者编辑约会

设置其他用户日历首选项

设置 Zimbra 任务

Zimbra Classic Web 应用程序用户界面主题

两因素认证

新用户账户双重认证

现有用户账户的双重身份验证

服务等级双重认证

电子邮件作为双因素身份验证的附加因素

账户的其他配置设置

启用共享

配置短信通知

配置附件查看

当用户尝试离开时显示警告

启用 Web 客户端的复选框

偏好导入/导出

将单词添加到拼写词典

Zimbra 中的分层地址簿 (HAB)

什么是 HAB?

使用分层地址簿

资历指数

配置分层地址簿

创建组织单位 (OU)

在此 OU 内创建组

创建层次结构

获取 Zimbra ID

将用户添加到组

设置排序顺序

指定 HAB 的根组织

它有效吗?

管理组织单位 (OU)

列出组织单位 (OU)

重命名组织单位 (OU)

重命名组织单位 (OU)

配置用户帐户

创建单个用户帐户

迁移账户并导入账户邮箱

从 Zimbra 服务器迁移账户

从通用 IMAP 服务器迁移账户

使用 XML 文件迁移账户

为选定账户导入电子邮件

XML 文件示例

从外部 LDAP 自动配置新帐户

概述

自动配置属性

占位符

Eager 模式配置

懒惰模式配置

手动模式配置

管理资源

设置调度策略

管理用户帐户

用户帐户状态

删除账户

查看账户邮箱

使用电子邮件别名

隐藏 GAL 中的别名

使用分发列表

设置分发列表的订阅策略

分发列表所有者的管理选项

创建分发列表

管理分发列表的访问

使用动态分发列表

创建动态分发列表

移动邮箱

移动邮箱的全局配置选项

监控 Zimbra 服务器

Zimbra 记录器

启用服务器统计

查看服务器状态

启用或禁用服务器服务

查看服务器性能统计信息

配置记录器邮件报告

配置磁盘空间通知

监控服务器

配置拒绝服务过滤器参数

识别误报

自定义 DoSFilter 配置

Zimbra Collaboration 8.0.3 及更高版本的调整注意事项

使用邮件队列

更改退回队列生命周期

通知发件人邮件被退回

查看邮件队列

刷新消息队列

监控邮箱配额

观看限额

增加或减少配额

查看 MobileSync 统计数据

监控身份验证失败

查看日志文件

系统日志

使用 log4j 配置日志记录

日志级别

协议追踪

查看 mailbox.log 记录

读取邮件头

修复损坏的邮箱索引

检查索引损坏

修复并重新索引损坏的索引

SNMP 监控和配置

SNMP 监控工具

SNMP 配置

生成 SNMP 陷阱的错误

检查 MariaDB

检查 Zimbra 协作软件更新

更新 Zimbra Connector for Microsoft Outlook

Zimbra Collaboration 发送的通知和警报

服务状态变更通知

重复的 mysqld 进程运行通知

SSL 证书到期通知

每日报告通知

数据库完整性检查通知

备份完成通知

归档和发现

归档的工作原理

发现的工作原理

安装归档包

在单服务器环境中安装zimbra-archiving

在多服务器环境中安装zimbra-archiving

从管理控制台管理归档

启用存档

创建专用存档 COS

设置存档帐户名

设置用户邮箱存档

存档邮箱

创建存档邮箱并分配 COS

创建没有 COS 或密码的存档邮箱

启用存档转发到第三方存档服务器

跨邮箱搜索

从管理控制台进行跨邮箱搜索

法律信息请求

合法拦截设置

设置合法拦截

设置合法拦截以转发邮件头

修改拦截封面电子邮件信息

创建邮箱快照以进行法律调查

创建邮箱快照zip文件

颜色和徽标管理

更改 Zimbra Classic Web 应用程序上的主题颜色和徽标

自定义基本主题颜色

更换经典 Web 应用程序徽标

使用管理控制台修改主题颜色和徽标

使用 CLI 更改主题颜色和徽标

定制现代 Web 应用程序

可以定制哪些内容

哪些不能定制

设置

创建空 Bundle

自定义徽标

可定制的细分

自定义文本和链接

定制颜色和尺寸

自定义 PWA

自定义登录页面

部署说明

存储管理

统一存储

结构

使用统一存储的优势

使用统一存储的局限性

如何设置统一存储

卷管理

指数成交量

留言量

管理控制台 : 存储管理页面

卷的类型

如何将卷分配为辅助卷

向服务器添加新的存储卷

存储管理策略

存储管理 CLI 实用程序

使用zms3config CLI管理全局 S3 配置

使用zmvolume CLI管理内部和外部卷

使用zmschedulesmpolicy CLI管理策略的调度

使用zmhsm CLI管理 SM 会话

管理存储管理策略

自定义存储管理器

概述

配置

基本集成

HTTP 存储

基于内容的存储

续传上传 (只限八达通)

Zimbra 移动同步

设置 ActiveSync 协议版本

句法

设置协议版本的示例：

移动设备安全策略

在 Zimbra 中设置移动策略

移动设备安全策略属性

移动设备管理

移动设备管理允许/阻止规则 (ABQ)

隔离通知

注册设备

支持自动发现

为用户帐户设置移动同步

更改移动设备密码策略

用户移动设备自助功能

备份和恢复

备份邮箱服务器

重做日志

备份方法

备份方法概述

自动分组备份方法

标准备份

备份文件的目录结构

使用管理控制台进行备份和恢复

从管理控制台配置备份/恢复

使用存储卷的建议

邮件恢复设置

使用命令行界面备份和恢复

使用标准方法备份

安排标准备份

完整备份过程

增量备份过程

查找特定备份

中止正在进行的完整备份

使用自动分组方法备份

从 CLI 配置自动分组备份

安排自动组备份

备份选项

备份内容选项

备份MariaDB数据库

管理备份的磁盘空间

恢复数据

恢复过程

停止恢复过程

当邮件服务器瘫痪时恢复邮箱

在实时系统上恢复个人账户

从还原中排除项目

恢复 LDAP 服务器

灾难恢复的一般步骤

准备

恢复

崩溃恢复服务器启动

恢复 Zimbra 协作

在新服务器上安装 Zimbra

从不同的故障场景中恢复

恢复 Zimbra 后更改本地配置文件

使用快照备份和恢复

关于短暂数据的说明

临时存储 SSDB 后端

使用 LDAP 后端备份

从备份恢复到 Zimbra 10

迁移的目的

句法

使用示例

先决条件

迁移顺序

委派管理

授予管理权限的目标类型

权利

系统定义的权利

属性权

使用权限列表

实施委派管理

管理员组和管理员

配置管理员帐户或管理员组的授权

向目标授予 ACL

撤销权利

暂时撤销委派的管理员权限

查看授予管理员的权限

授予预定义权限

域管理员

重置密码

编辑联系信息

预定义委派管理员角色

域管理组

分发列表管理组

创建委派管理员角色

管理多个域

管理分发列表

更改密码

查看邮件访问权限

管理分配给用户的服务类别

管理跨邮箱搜索

管理 Zimlets

管理资源

访问已保存的搜索

访问服务器状态页面

聊天和视频

安装

聊天和视频云权限

免费一对聊天

齐姆莱茨

经典 Web 应用程序中的默认 zimlets

从管理控制台管理 Zimlets

部署定制 Zimlets

启用、禁用或强制使用 Zimlets

取消部署 Zimlet

将允许代理的域添加到 Zimlet

升级 Zimlet

从命令行界面管理 Zimlets

部署 Zimlets

将代理允许域添加到 Zimlet

部署 Zimlet 并授予 COS 访问权限

查看已安装的 Zimlet

更改 Zimlet 配置

升级 Zimlet

使用 Zimbra 图库

开发定制 Zimlets

为现代 Web 应用配置 Zimlets

现代 Web 应用中的默认 zimlets

配置 LDAP

基本信息

客户端示例

设置Dropbox

设置Google云端硬盘

设置OneDrive

设置 Slack

设置 Zoom

设置 NextCloud

设置 Jitsi 视频会议解决方案

为组织设置单独的 Jitsi 服务器

设置签名模板

预防外出警报

如何配置预防外出警报

自定义字体

自定义字体列表（管理员）

个人字体列表（用户）

在 Composer 中选择字体

默认作曲家字体

已知限制

自定义字体配置

如何在服务器上配置管理员定义的自定义字体

附录 A:命令行实用程序

常规工具信息

语法约定

命令行实用程序的位置

Zimbra CLI 命令

在 CLI 中使用非 ASCII 字符

zmprov (配置)

韓國

归档配置

归档

归档搜索

备份

兹姆布洛布克

计算校验

zmschedulebackup

zmbackupabort

zmbackupquery

校长

zmrestoreoffline (离线恢复) zmrestoreldap

zmcontrol (启动/停止/重启服务)

zmmboxsearch (跨邮箱搜索)

zmmbox移动

zmmboxmovequery

zmpurgeoldmbox

zmgsutil

zmldapppasswd

zmlocalconfig

zmmailbox

兹米特斯特尔

韓國

许可协议

元数据转储

zmmypasswd

zmplayredo

zmproxyconfgen

代理服务器

zmredodump

zmskindeploy

皂化物

zmstat 图表

zmstat-图表配置

zmstatctl

转储

兹姆特兰萨

zmtz更新

zmvolume

兹姆齐姆莱特特尔

代理配置

zmsyncreverseproxy

附录 B:配置 SPNEGO 单点登录

配置流程

创建 Kerberos Keytab 文件

配置 Zimbra

配置您的浏览器

测试您的设置

故障排除设置

使用 SPNEGO Auth 配置 Kerberos Auth

为 ZCO 设置单点登录选项

附录 C:Zimbra Crontab 作业

如何读取 crontab

Zimbra Cron 作业

预定作业

crontab.store 的职位

crontab.logger 的任务

crontab.mta 的职位

单服务器 Crontab -l 示例

使用 SimpleSAMLphp 和 SAML 进行 Zimbra 单点登录

在 SimpleSAMLphp 中设置 Zimbra SP

设置 Zimbra

创建用户

saml-config.properties中的可配置属性

SLO 端点

CsrfRefererCheck

词汇表

本文档适用于 Zimbra Daffodil 版本 10.0 和 10.1.0。

执照



Synacor, Inc., 2024-2025 年

© 2024-2025 Synacor, Inc. Zimbra 协作管理员指南

本作品根据 Creative Commons Attribution-ShareAlike 4.0 国际许可协议获得许可,除非您与 Synacor, Inc. 之间的其他许可协议另有规定。要查看此许可证的副本,请访问<https://creativecommons.org/licenses/by-sa/4.0>或寄信至 Creative Commons, PO Box 1866, Mountain View, CA 94042, USA。

Synacor, Inc., 2024-2025 505 Ellicott

Street, Suite A39 Buffalo, NY 14203 美国

<https://www.synacor.com>

介绍

Zimbra Collaboration 是一款功能齐全的消息传递和协作解决方案,其中包括电子邮件、地址簿、日历、任务和 Web 文档创作。

Zimbra Daffodil (v10.1) 引入了新的许可服务,许可管理方面发生了重大变化。请参阅许可部分了解更多详细信息

观众

本指南适用于负责安装、维护和支持 Zimbra Collaboration 服务器部署的系统管理员。

本指南的读者应具备以下建议的知识和技能：

- 熟悉相关技术和标准
- Linux 操作系统和开源概念
- 邮件系统管理的行业实践

第三方组件

在可能的情况下,Zimbra Collaboration 遵循现有的行业标准和开源实现,用于备份管理、用户身份验证、操作平台和数据库管理。但是,它仅支持 “产品概述”一章中 Zimbra Collaboration 架构概述中所述的经过官方测试和认证的特定实现。本文档可能偶尔会提及市场上是否有其他工具,但此类提及并不构成认可或认证。

支持和联系信息

- 联系 Zimbra 销售部门购买 Zimbra Daffodil (v10)。
- Zimbra Collaboration 客户可以通过support@zimbra.com 联系支持人员。
- 探索Zimbra 论坛 (<https://forums.zimbra.org/>)寻找安装或配置问题的答案。
- 加入 Zimbra 社区论坛,参与并了解有关 Zimbra Collaboration 的更多信息。
- 发送电子邮件至feedback@zimbra.com ,告诉我们您对产品的喜好以及希望在产品中看到哪些功能。如果您愿意,可以将您的想法发布到 Zimbra 论坛。

如需更多产品信息,可参考以下资源:

- [Zimbra 维基](https://wiki.zimbra.com)(<https://wiki.zimbra.com>)
- [安全中心](https://wiki.zimbra.com/wiki/Security_Center) (https://wiki.zimbra.com/wiki/Security_Center)

产品生命周期

本章提供有关 Zimbra 组件产品生命周期阶段的信息。

组件弃用声明

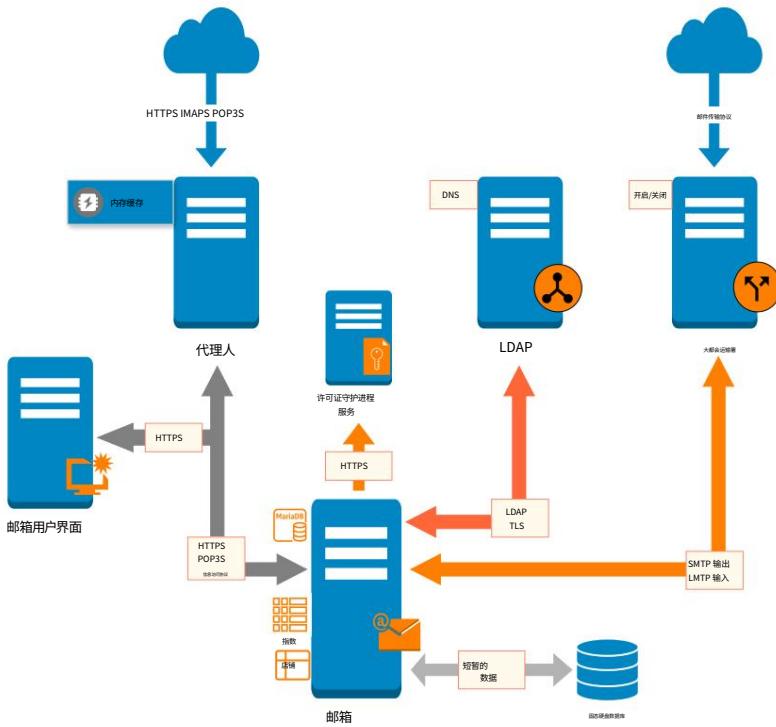
成分	弃用声明
Zextras/NG 模块	HSM、备份、移动、ABQ、驱动器、文档、身份验证、连接和管理 已被删除。
免疫组化	已移除

产品概述

本章提供 Zimbra 组件的系统概述。

架构概述

Zimbra 协作架构采用知名的开源技术和基于标准的协议。该架构由可以作为单个节点运行的客户端接口和服务器组件组成，配置或部署在多台服务器上，以实现高可用性和增强的可扩展性。



该架构包含以下核心优势：

核心优势	组件/描述
开源集成	Linux®、Jetty、Postfix、MariaDB、OpenLDAP®
行业标准开放协议	SMTP、LMTP、SOAP、XML、IMAP、POP
现代技术设计	HTML5、Javascript、XML 和 Java
可扩展性	每个 Zimbra 邮箱服务器都有自己的邮箱帐户以及相关的消息存储和索引。Zimbra 平台垂直扩展（通过添加更多系统资源）和水平（通过添加更多服务器）
基于浏览器的客户端界面	使用
基于浏览器的管理控制台	标准的网络平台。

核心电子邮件、日历和协作功能

Zimbra Collaboration 是一款创新的消息传递和协作应用程序，它提供可通过基于浏览器的 Web 客户端访问的以下最先进的解决方案。

- 直观的消息管理、搜索、标记和共享。
- 个人、外部和共享日历。
- 个人和共享地址簿和分发列表。
- 个人和共享任务列表。

Zimbra 组件

Zimbra 架构包括使用行业标准协议的开源集成。第三方软件中列出的软件与 Zimbra 软件捆绑在一起，并作为安装的一部分进行安装过程。这些组件已经过测试并配置，可以与软件配合使用。

表 1. 第三方软件

第三方组件	描述
码头	运行 Zimbra 软件的 Web 应用程序服务器。
后缀	开源邮件传输代理 (MTA)，用于将邮件消息路由到适当的 Zimbra 服务器
打开 LDAP 软件	轻量级目录访问协议 (LDAP) 的开源实现 存储 Zimbra 系统配置、Zimbra 全局地址列表以及 提供用户身份验证。Zimbra 还可以与 GAL 和身份验证配合使用 外部 LDAP 目录（例如 Active Directory）提供的服务
玛拉雅数据库	数据库软件
Lucene	开源全功能文本和搜索引擎
	将某些附件文件类型转换为 HTML 的第三方来源
防病毒/反垃圾邮件	开源组件包括： <ul style="list-style-type: none"> ClamAV，一款可防御恶意文件的防病毒扫描程序 SpamAssassin，一种尝试识别垃圾邮件的邮件过滤器 Amavisd MTA 与一个或多个内容检查器之间的新接口
Apache JSieve	管理电子邮件过滤器
自由办公室	高保真文档预览
仅限办公室	协作文档编辑

Zimbra 应用程序包

Zimbra Collaboration 提供应用程序包中列出的应用程序包。

表 2. 申请材料

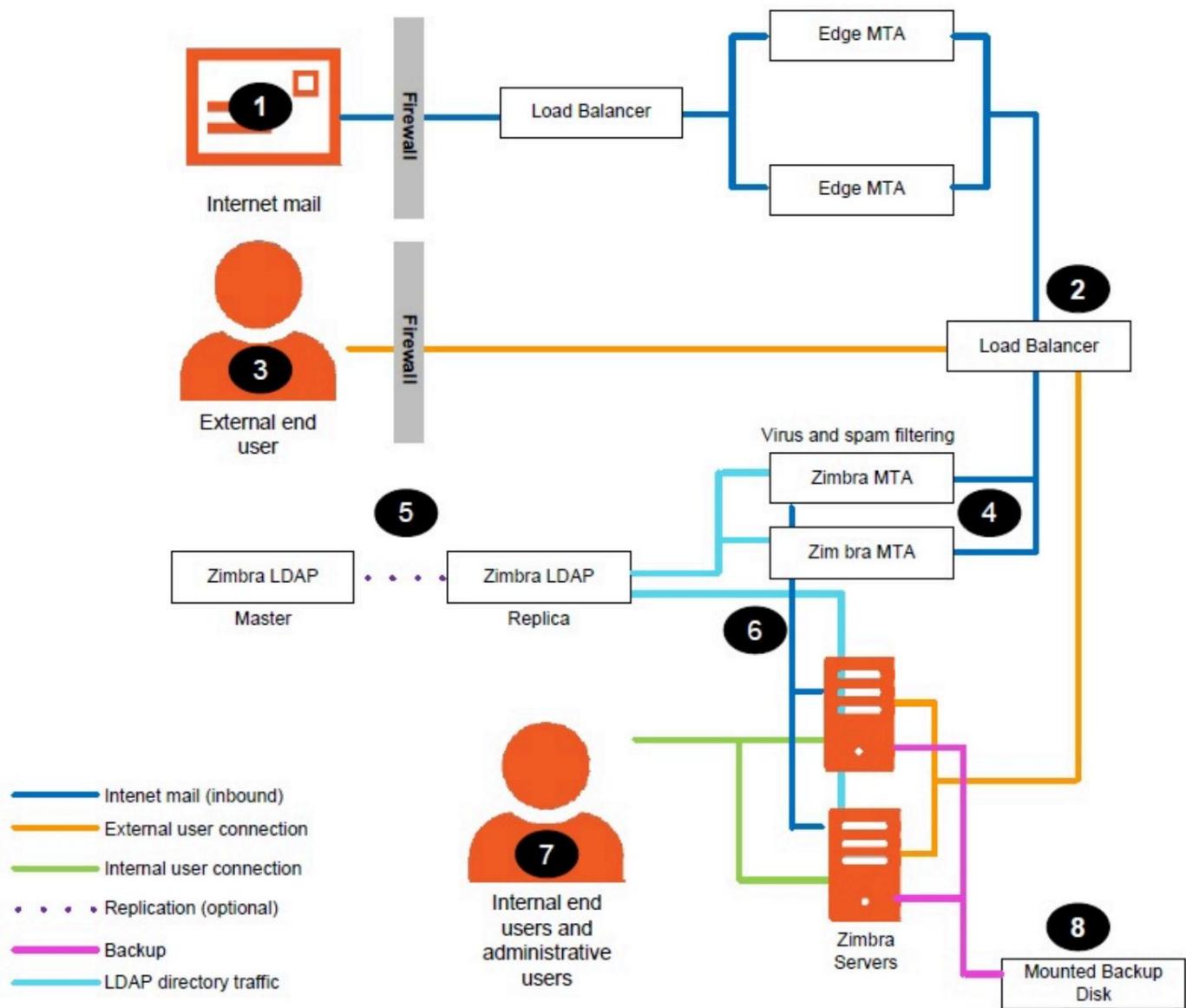
包裹	描述
Zimbra 核心	库、实用程序、监控工具和基本配置文件。zmconfigd 包含在 zimbra-core 中并自动启用在所有系统上运行。

包裹	描述
Zimbra 现代网络客户	Zimbra Modern Web App 所需的资产。此包会自动安装在每台服务器上。
Zimbra 商店	<p>邮箱服务器的组件（包括 Jetty）。Zimbra 邮箱服务器包括以下组件：</p> <ul style="list-style-type: none"> • 数据存储 - MariaDB 数据库。 • 消息存储 所有电子邮件消息和文件附件的位置。 • 索引存储 通过 Lucene 提供索引和搜索技术。每个邮箱都维护索引文件。 • Web 应用程序服务 Jetty Web 应用程序服务器可在任何商店服务器上运行 Web 应用程序 (webapps)。它提供一个或多个 Web 应用程序服务。
Zimbra LDAP	Zimbra Collaboration 使用 OpenLDAP® 软件，这是一种开源 LDAP 目录服务器。用户身份验证、Zimbra 全局地址列表和配置属性是通过 OpenLDAP 提供的服务。请注意，Zimbra GAL 和身份验证服务可以由外部 LDAP 目录（例如 Active Directory）提供。
Zimbra MTA	Postfix 是一个开源邮件传输代理 (MTA)，它通过 SMTP 接收电子邮件，并使用本地邮件传输协议 (LMTP) 将每封邮件路由到相应的 Zimbra 邮箱服务器。Zimbra MTA 还包括防病毒和反垃圾邮件组件。
Zimbra 代理	Zimbra Proxy 是一种高性能反向代理服务，用于将 IMAP[S]/POP[S]/HTTP[S] 客户端请求传递到其他内部 Zimbra 服务。此包通常安装在 MTA 服务器或其自己的独立服务器上。安装 zimbra-proxy 包后，默认启用代理功能。强烈建议安装 Zimbra Proxy，如果使用单独的 Web 应用程序服务器，则必须安装。
Zimbra Memcached	安装 zimbra-proxy 时会自动选择 Memcached。使用代理时，至少有一台服务器必须运行 zimbra-memcached。您可以将单个 memcached 服务器与一个或多个 Zimbra 代理一起使用。如果使用单独的 Web 应用程序服务器，则需要 zimbra-memcached。
Zimbra SNMP (可选)	如果您选择安装 zimbra-SNMP 进行监控，则应在每个 Zimbra 服务器上安装此软件包。
Zimbra Logger (可选)	如果使用，则安装在一个邮箱服务器上，并且必须安装在同一个时间与邮箱服务器相同。Zimbra Logger 安装用于系统日志聚合和报告的工具。如果您未安装 Logger，管理控制台的服务器统计信息部分将不会显示。
Zimbra 法术 (可选)	Aspell 是 Zimbra Classic Web App 上使用的开源拼写检查器。安装 Zimbra-Spell 时，也会安装 Zimbra-Apache 包。

包裹	描述
Zimbra 阿帕奇	当安装 Zimbra Spell 或 Zimbra Convertd 时,此包会自动安装。
Zimbra 转换	此软件包安装在 zimbra-store 服务器上。Zimbra Collaboration 环境中只需要有一个 Zimbra-convertd 软件包。默认情况下,每个 zimbra-store 服务器上都安装一个 zimbra-convertd。当 Zimbra-Convertd 已安装,Zimbra-Apache 包也已安装。
Zimbra 归档 (选修的)	归档和发现功能可以存储和搜索所有发送到 Zimbra Collaboration Server 或由其发送的消息。此软件包包括跨邮箱搜索功能,可用于实时邮箱和存档邮箱 搜索。注意:使用 Archiving and Discovery 可能会触发额外的邮箱许可证使用。要了解有关 Zimbra Archiving and Discovery 的更多信息,请联系 Zimbra 销售人员。
Zimbra OnlyOffice	此软件包安装是协作编辑由 Onlyoffice 提供支持的文档所必需的,可协作编辑存储在 Briefcase 中的文档。此软件包可以安装和设置在代理服务器、邮箱服务器或单独的文档服务器上。
许可证守护程序服务 (摩门教)	随着 Zimbra Daffodil (v10.1) 中新许可证服务的引入,添加了一项名为许可证守护程序服务(LDS)的新许可证服务,以实现增强且灵活的许可证管理。LDS 是支持许可证管理的必需服务。

邮件流 - 多服务器配置

每个部署的配置取决于许多变量,例如邮箱数量、邮箱配额、性能要求、现有网络基础设施、IT 策略、安全方法、垃圾邮件过滤要求等。一般而言,部署在传入流量和用户连接方面具有共同的特征,如下图所示。也可以使用其他方法来配置网络内的多个点。



编号序列描述如下：

1. 入站互联网邮件经过防火墙和负载平衡到边缘 MTA 进行垃圾邮件过滤。
2. 过滤后的邮件然后经过第二个负载均衡器。
3. 连接到消息传递服务器的外部用户也穿过防火墙到达第二个负载均衡器。
4. 入站互联网邮件将发送到任意 Zimbra Collaboration MTA 服务器，并经过垃圾邮件和病毒过滤。
5. 指定的 Zimbra Collaboration MTA 服务器从 Zimbra Collaboration LDAP 副本服务器。
6. 从 Zimbra Collaboration LDPA 服务器获取用户的信息后，MTA 服务器将邮件发送到相应的 Zimbra Collaboration 服务器。
7. 内部最终用户直接与任何 Zimbra Collaboration 服务器建立连接，然后该服务器从 Zimbra Collaboration LDAP 获取用户的目录信息并根据需要重定向用户。
8. 可以将来自 Zimbra Collaboration 服务器的备份处理到已安装的磁盘。

Zimbra 系统目录树

下表列出了 Zimbra 安装包创建的主要目录。在 (父级) /opt/zimbra 下安装时，Zimbra Collaboration 中的任何服务器的目录组织都是相同的。

下表中未列出的目录是用于构建核心 Zimbra 的库
软件或其他第三方工具。

表 3 下的系统目录树。

/opt/zimbra

文件	描述
备份/	备份目标包含完整和增量备份数据
垃圾桶/	Zimbra 协作应用程序文件,包括以下描述的实用程序 命令行实用程序
政策法规	策略功能、限制
克拉马夫/	用于病毒和垃圾邮件控制的 Clam AV 应用程序文件
配置/	配置信息
贡献/	第三方脚本传输
已转换/	转换服务
cyrus-sasl/	SASL AUTH 守护进程
数据/	包括 LDAP、mailboxd、postfix、amavisd、clamav 的数据目录
分贝/	数据存储
文档/	SOAP txt 文件和技术 txt 文件
扩展-extra/	不同身份验证类型的服务器扩展
扩展网络额外/	不同网络版本身份验证类型的服务器扩展
httpd/	包含 Apache Web 服务器。用于 aspell 和 convertd as 单独的进程
指数/	索引存储
Java/	包含 Java 应用程序文件
码头/	mailboxd 应用程序服务器实例。在此目录中, webapps/zimbra/skins 文件夹包含 Zimbra UI 主题文件
库/	图书馆
库执行/	内部使用的可执行文件
日志/	Zimbra Collaboration 服务器应用程序的本地日志
记录器/	记录器服务的 RRD 和 SQLite 数据文件
mariadb/	MariaDB 数据库文件
网络-snmp/	用于收集统计数据

文件	描述
openldap/	OpenLDAP 服务器安装,已预先配置好
后缀/	Postfix 服务器安装,预先配置为与 Zimbra Collaboration 配合使用
重做日志/	包含 Zimbra 协作服务器的当前事务日志
SNMP/	SNMP 监控文件
SSL/SSL	证书
店铺/	消息存储
zimbramon/	包含控制脚本和 Perl 模块
齐姆莱茨/	包含与 Zimbra 一起安装的Zimlet zip文件
zimlets-部署/	包含可与 Zimbra Classic Web App 配合使用的 Zimlet
zimlets 网络/	包含随网络安装的功能的Zimlet zip文件 版
复仇/	mailboxd 统计数据,保存为.csv文件

Zimbra Web 应用程序

Zimbra 提供多种 Web 应用类型供使用 Zimbra 功能。Web 应用提供邮件、日历、地址书籍和任务功能。

表 Zimbra Web 应用程序

客户端类型	描述
现代 Web 应用程序	使用现代技术、UI 设计,并提供相同的用户体验 台式机、手机和平板电脑等设备。
经典 Web 应用程序	包括 Ajax 功能并提供全套 Web 协作功能。支持 仅适用于桌面网络浏览器;不提供适合较小尺寸的用户体验 屏幕、触摸功能或手势。

用户可以在登录前从登录页面的“版本”下拉菜单中选择 Web 应用。管理员可以将 COS 的默认 Web 应用设置为经典 Web 应用或现代 Web 应用。用户可以覆盖此设置默认:

- 在现代 Web 应用程序中,用户可以进入设置→常规来更改他们登录的默认 Web 应用程序的值
- 在经典 Web 应用中,用户可以前往“首选项”→“常规”→“登录”来更改默认 Web 应用的值
他们登录到

建议管理员将默认值设置为现代 Web 应用程序。

Web 服务和桌面客户端

除了使用 Web 浏览器或移动设备连接到 Zimbra Collaboration 外,还可以使用 Web 服务 (例如 Exchange Web Services (EWS))或桌面客户端 (例如 Zimbra Connector to Microsoft Outlook)进行连接。支持以下内容:

- Exchange Web Services (EWS)提供客户端访问,使 Zimbra Collaboration 能够在 Mac 设备上使用 Microsoft Outlook 时与 Exchange Server 进行通信。要启用 EWS 客户端访问,请参阅服务类别部分。EWS 是一项单独授权的附加功能。
- 消息传递应用程序编程接口 (MAPI)可与受支持的 Microsoft Outlook 版本同步,具有完全委托、离线访问和 S/MIME 支持。在 Windows 设备上使用 Microsoft Outlook 时,使用 Zimbra Connector for Outlook 连接到 Zimbra Collaboration。要启用 MAPI (Microsoft Outlook) Connector,请参阅服务类别部分。
- 支持所有 POP3、IMAP4、Web 分布式创作和版本控制 (CalDAV) 的日历扩展以及 Web 分布式创作和版本控制 (CardDAV) 的 vCard 扩展客户端。

离线模式

对于经典 Web 应用,Chrome 85 及以上版本不再支持离线模式 (影响 Kepler9-Patch9 及以上版本)。用户仍可在之前的浏览器版本中继续使用离线模式。

使用 Zimbra Modern Web App 时,Zimbra 离线模式允许访问数据 (无需网络连接)。

例如,如果没有服务器连接或服务器连接丢失,Web App 会自动转换为“离线模式”。当服务器连接恢复时,Web App 会自动恢复到“在线模式”。

此离线模式利用了现代浏览器中 HTML5 提供的缓存功能。

安全措施

协调使用多种安全措施以提高整个系统的安全性是保护信息基础设施的最佳方法之一。这些措施是在 Zimbra 协作平台中实施的,其防御机制总结如下:

要查看当前和详细的安全新闻和警报,请参阅安全中心 (https://wiki.zimbra.com/wiki/Security_Center) 在 Zimbra Wiki 上 (<https://wiki.zimbra.com/>)。

身份和访问管理

系统内置的用户身份管理关键功能总结如下表:

表身份和访问管理功能5.

功能	描述
身份生命周期管理	利用 LDAP 目录实现与 Zimbra Collaboration 用户管理相关的所有创建、读取、更新和删除 (CRUD) 功能。LDAP 使用是可选的,但所有特定于 Zimbra Collaboration 的属性都通过本机 LDAP 目录进行存储和管理。

功能	描述
第一因素 验证	授权用户尝试访问系统时主要使用的组合用户名和密码。这些凭据保留在用户存储中：密码以加盐哈希的形式存储，并与输入的密码进行比较，以拒绝（不匹配）或接受（匹配）。如果首选外部目录（LDAP 或 Active Directory），则可以将适当的登录凭据存储在此外部 LDAP 目录中。另请参阅 Zimbra LDAP 服务以了解更多详细信息。
双因素 验证	在管理控制台上配置的第二层身份安全，用于启用或禁用与 Zimbra Collaboration 关联的移动设备的密码生成。启用后，用户或 COS 帐户必须使用生成的密码才能访问其客户端服务。另请参阅关于 2 因素身份验证和双因素身份验证。
授权访问	<p>用户帐户由各种属性、权限级别和策略定义，以允许或禁止查看哪些数据以及执行哪些功能。</p> <p>管理控制台管理员可以创建组并分配访问权限以支持目标业务目标。</p>

信息安全和隐私

系统内置的保护数据安全的功能总结如下表：

表 6. 信息安全和 隐私功能

关键概念	描述
安全性、完整性和隐私管理	Zimbra Collaboration 支持使用 S/MIME 证书（由公众信任的认证机构（CA）提供）以及内部 PKI；域名密钥识别邮件（DKIM）；基于域的消息认证、报告和一致性（DMARC）；Amavisd-new，位于邮件传输代理（MTA）中，用于管理传入和传出的 DMARC 策略。
加密方法：	
在途中	端点和服务之间的安全连接除了使用其他各种协议外，还使用 TLS：SMTP、LMTP+STARTTLS、HTTPS、IMAPS/IMAP+STARTTLS、POP3S/POP3+STARTTLS。
休息时	使用 S/MIME 进行端到端加密，存储在 Zimbra Collaboration 消息存储中的数据会被加密，直到使用适当的私钥进行解密。
防病毒和防 垃圾邮件	恶意软件和垃圾邮件都面临着 Zimbra Collaboration 原生功能和第三方插件（Amavisd-new、ClamAV 和 Spam Assassin）的挑战。

此功能仅在经典 Web 应用程序中受支持。

系统日志

Zimbra 协作系统日志（由 SNMP 触发器生成）可用于记录用户和管理员活动、登录失败、慢速查询、邮箱活动、移动同步活动和数据。基于错误的事件、警报和陷阱可以转发到日志管理和事件关联系统，以创建根据您的安全性和合规性要求制定集中的政策和通知。

表安全数据

功能	描述
事件响应	管理员可以在以下情况下使用远程设备擦除和/或帐户锁定： 恶意或意外活动（例如用户帐户凭证被盗，或丢失 手机）。
归档和发现	此可选功能允许管理员选择特定用户的电子邮件消息 用于归档和应用保留策略，可用于 存档邮箱和实时邮箱。

Zimbra Daffodil (v10.1) 许可

Zimbra Daffodil (v10.1) 引入了自动许可和授权系统,以便更灵活地管理许可证并允许未来的增长。

随着 Zimbra Daffodil (v10.1) 中新许可证服务的引入,已添加一项名为许可证守护进程服务 (LDS) 的新许可证服务,以实现增强和灵活的许可证管理。

请参阅许可证守护程序服务部分以获取有关 LDS 及其设置方法的更多信息。

需要 Zimbra Collaboration 许可证才能启用许可证功能并创建帐户。

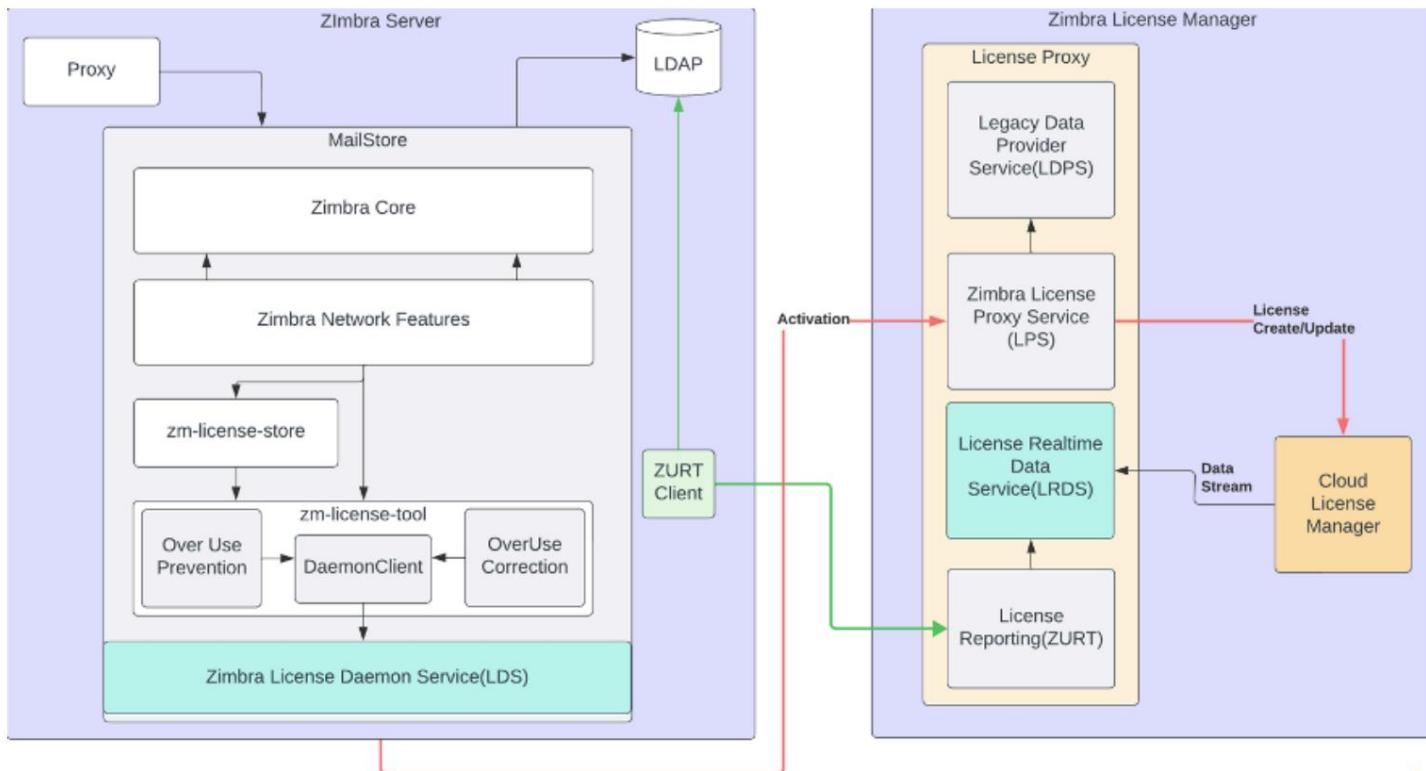
以下是 Zimbra Daffodil (v10.1) 许可更新:

1. 新的许可证守护程序是 Zimbra 安装的一部分。它在模块列表,以及 Zimbra 正常运行所需的模块。
2. 需要一个 18-26 个字母数字字符的密钥来取代旧的license.xml文件。
3. Zimbra Collaboration 许可证限制了许可证中定义的权利,并且不支持多次激活。
4. 一旦 Zimbra Collaboration 许可证被激活,用户就无需再进行许可证管理。许可证管理是实时的,由 Zimbra 管理。
5. 引入了离线许可证服务器,以支持无法向公众开放的环境网络。
6. 所有数据收集均基于许可要求和总使用量,符合 GDPR 和其他法律规定规章制度。

记录 LDAP 和 LDS 主机名以用于许可证注册和激活。

7. 提供独立实验室许可证。请联系 Zimbra 销售或支持团队。

以下是架构视图:



LDAP 属性

以下是 Zimbra Daffodil (v10.1) 许可的新属性：

- `zimbraNetworkRealtimeLicense` - 存储在线和离线激活所需的许可证密钥。
- `zimbraNetworkRealtimeActivation` - 包含激活详细信息、激活产品版本、已激活的许可证。
- `zimbraOfflineNetworkRealtimeLicense` - 存储离线激活所需的网络密钥。
- `zimbraFeatureActualUsageCount` - 存储报告和强制功能的过度使用次数。

许可证功能

Zimbra Collaboration 许可使管理员能够查看和控制他们计划使用的许可证功能

部署。您可以监控使用情况并管理以下许可证功能。

Zimbra Daffodil (v10.1) 引入了许可和未许可功能的详细视图，以便更好地管理

在管理界面或命令行中。以下是跟踪的许可证功能：

特征	许可属性	描述	特征代码
帐户	账户限制	您可以创建的帐户。	艾尔
零碳	MAP连接器帐户限制	可以使用 Zimbra 的账户 Microsoft Outlook 连接器 (ZCO)。	MCAL
远程预警系统	EwsAccountsLimit	可以使用 EWS 的帐户连接到 Exchange 服务器。EWS 是单独许可的附加功能。	语言辅助学习

特征	许可属性	描述	特征 代码
Zimbra 移动	MobileSyncAccountsLimit	可以使用 ActiveSync 的帐户协议来访问其电子邮件移动设备。	例子
邮件/多用途邮件	SMIME 帐户限制	可以使用 S/MIME 的账户特征。	狭窄的
归档	归档帐户限制	允许存档帐户。存档功能安装是必需的。	亚洲航空协会
Zimbra 办公室	文档编辑帐户限制	文档协作功能这使得创建/编辑/共享文档在组织内。OnlyOffice 安装是必需的。	交易
分享	共享帐户限制	控制共享和委派为用户提供的功能。	沙尔
公文包	公文包帐户限制	控制公文包功能用户。	平衡阿尔法
备份和恢复	备份已启用	允许管理员使用备份和恢复功能	是
贮存 管理 (内部卷)	已启用存储管理	允许管理员使用存储管理功能和创建使用内部存储的卷。	我们是 骨头
贮存 管理 (外部 (S3) 卷)	已启用对象存储支持	允许管理员使用存储管理功能和创建使用外部 S3 的卷提供商 (例如AWS,Ceph) 。	骨头
依恋 索引	附件索引已启用	允许索引附件内容	艾因
日历	日历帐户限制	启用日历功能用户	布
对话	对话已启用帐户限制	启用对话功能用户	类型
CrossMailboxSearch	CrossMailboxSearchEnabled	允许搜索内容跨实时和存档邮箱。	中枢神经系统疾病
委派管理员	委派管理员帐户限制	委派管理员帐户可以创建	向下

特征	许可属性	描述	特征 代码
团体日历	组日历帐户限制	让您能够看到多个同时查看日历	GCAL
标签	启用标记的帐户限制	启用标记功能用户	青色
任务	任务启用帐户限制	启用任务功能用户	特凯尔
HTML 视图附件	查看HtmlEnabledAccountsLimit	以 HTML 格式查看电子邮件附件格式	维艾尔
齐姆莱茨	ManageZimletsEnabledAccountsLimit	可以管理的用户帐户 齐姆莱茨	热情
多因素认证	已启用多重身份验证	控制两个因素 身份验证功能 用户。	金属氧化物助剂

短代码可用于使用zmlicense检查单个服务的状态命令。请参阅zmlicense部分了解更多详细信息。

Zimbra Daffodil (v10.1)许可证要求

您需要 Zimbra 许可证才能在 Zimbra Collaboration 中创建帐户并使用现代 Web 应用程序。

试用许可证仅限于一个电子邮件地址,可以通过联系申请延期 Zimbra 销售。

要试用 Zimbra Collaboration,您可以免费获得试用版。一旦您的系统安装在生产环境,您需要购买订阅或永久许可证。

许可证类型	描述
审判	您可以从 Zimbra 网站获取免费试用许可证,网址为 https://www.zimbra.com →产品→下载→获取试用许可证。试用许可证允许您创建最多 50 个用户。有效期为 60 天。
订阅	Zimbra 订阅许可证只能通过购买获得。此许可证对于特定的 Zimbra 协作系统有效,使用以下数量进行加密: 您购买的 Zimbra 帐户 (席位)、生效日期和到期日期 订阅许可证的日期。

许可证类型	描述
永久	Zimbra 永久许可证只能通过购买获得。此许可证类似于订阅许可证。它适用于特定的 Zimbra 协作系统,使用您购买的 Zimbra 帐户 (席位) 数量、生效日期和到期日期 2099-12-31 进行加密。当您续订支持协议时,您不会收到新的永久许可证,但系统中的帐户记录会更新为新的支持结束日期。

按 Zimbra 协作帐户类型划分的许可证使用情况

分配给个人的帐户 (包括为存档创建的帐户) 需要邮箱许可证。

分发列表、别名、位置和资源不计入许可证。

以下是 Zimbra Collaboration 帐户类型的描述以及它们是否影响您的许可证限制。

许可证帐户类型	描述
系统帐户	系统帐户是 Zimbra Collaboration 使用的特定帐户。它们包括垃圾邮件 (垃圾邮件和正常邮件) 的垃圾邮件过滤帐户、带有病毒的电子邮件的病毒隔离帐户以及 GALsync 帐户 (如果您为域配置了 GAL)。
	不要删除这些帐户!这些帐户不计入您的许可证。
管理员帐户	管理员和委派管理员帐户将计入您的许可证。
用户帐户	用户帐户会计入您的许可证帐户限制。 当您删除一个帐户时,许可证帐户限制会反映出该变化。
别名帐户	
分发列表	这些类型不计入您的许可证。
资源帐户	

许可证激活

所有 Zimbra Daffodil (v10.1) 安装都需要许可证激活,并继续支持自动和手动许可证方法。在 Daffodil (v10.1) 中,条款已更改为在线激活和离线激活。

管理控制台已得到增强,具有更直观且易于遵循的用户界面,其中与许可证部署相关的所有操作都在一个屏幕上。

Zimbra Daffodil (v10.1) 许可证的激活可以在安装、升级或安装后进行。一旦激活许可证,服务器上就无需进行后续许可证管理。

如果不激活许可证,Zimbra 服务将无法启动。

在线激活许可证

如果 Zimbra Collaboration 服务器已连接到互联网,则许可证会自动激活,并且可以与 Zimbra 许可证服务器通信。

以下是在线许可证的适用激活规则:

- 帐户应具有有效的支持结束日期。
- 许可证应有效 (不得过期)。
- 可以切换许可证,只要新的许可证限制大于或等于当前许可证使用量。
- 不允许在任何现有许可证 (试用版、常规版、永久版)上激活试用许可证。

以下是激活许可证的步骤:

管理控制台

- 登录管理控制台,进入主页→开始→安装许可证→在线激活
- 在密钥文本框中,指定 18-26 个字母数字字符的许可证密钥,然后单击激活。
- 激活成功后,您将看到一条成功消息 - 您的许可证是 已成功激活。

命令行

您还可以从命令行界面激活您的许可证。

- 以zimbra用户身份运行命令:

```
zmlicense -a <许可证密钥>
```

- 激活成功后,您将看到一条成功消息 - 您的许可证是 已成功激活。

升级后的 Zimbra Collaboration 版本需要立即激活才能维持网络
特色功能。

如果您无法自动激活许可证,请参阅下一节“离线许可证激活”。

离线许可证激活

Zimbra Daffodil (v10.1) 中生成和激活离线许可证的方法已更改。作为先决条件,必须在运行

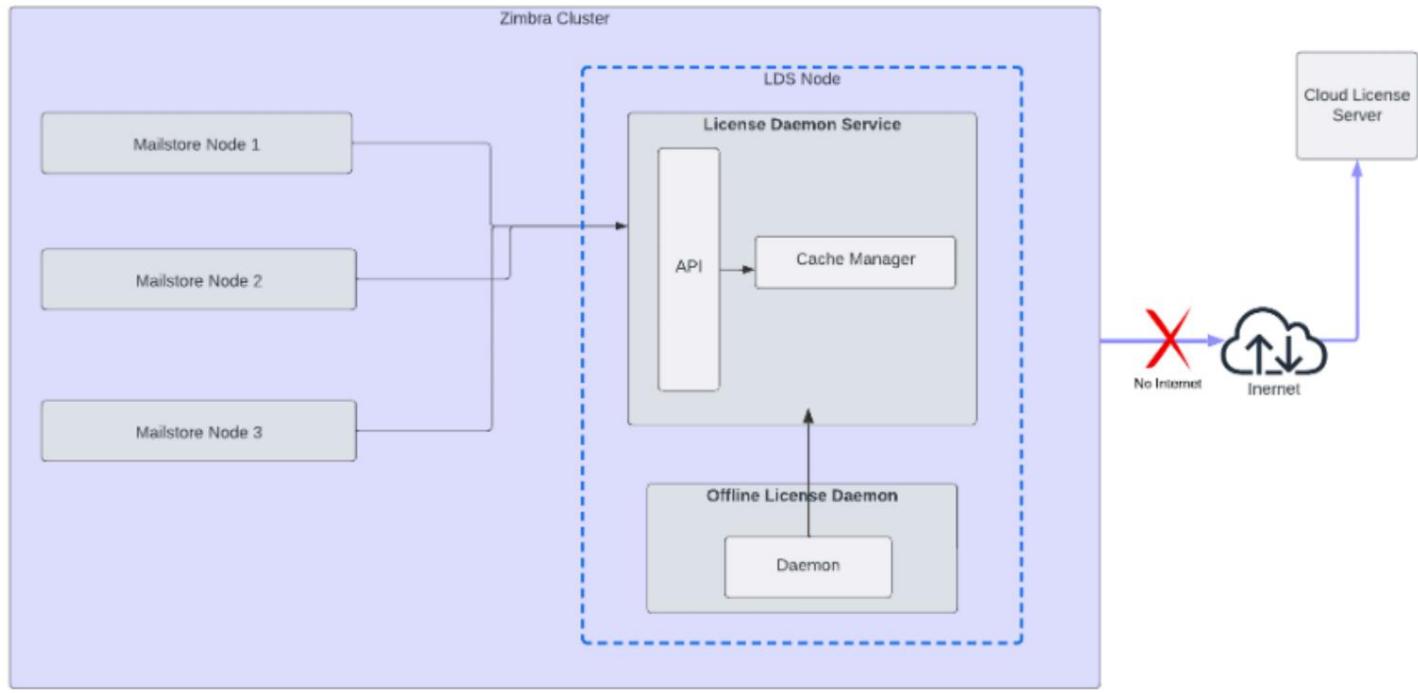
许可证守护程序服务。安装包后,将启动一个离线守护程序服务,该服务充当本地运行的许可证管理器。

如果未安装该软件包或离线守护程序,则离线许可证激活将不起作用

脱机守护程序服务是脱机运行的关键且重要的服务
许可证及其管理。建议您设置服务监控来检查
服务状态。

离线许可证可能需要最多 48 小时才能颁发。

以下是脱机许可证流程的架构视图：



先决条件

以下是安装离线守护程序包之前需要完成的先决条件：

禁用 FIPS

在安装离线守护程序包之前,应该在系统上禁用 FIPS。

以下是禁用 FIPS 的步骤。以root用户身份执行命令：

- 对于 RHEL/CentOS/Rocky Linux 系统：

```
sudo fips-mode-setup --disable sudo reboot
```

- 验证 FIPS 是否已禁用。检查/proc/sys/crypto/fips_enabled文件。如果已禁用,则输出如下：

```
$ cat /proc/sys/crypto/fips_enabled 0
```

- 对于 Ubuntu 系统：

```
sudo ua 禁用 fips sudo 重启
```

- 验证 FIPS 是否已禁用。检查/proc/sys/crypto/fips_enabled文件。如果已禁用,则输出如下：

```
$ cat /proc/sys/crypto/fips_enabled 0
```

禁用 SELinux

在安装离线守护程序包之前,应在系统上禁用 SELinux。您必须重新启动以使变更生效。

以下是禁用 SELinux 的步骤。以root用户身份执行命令：

- 对于 RHEL/CentOS/Rocky Linux 系统：

- 检查 SELinux 状态。如果状态显示已启用 , 执行进一步的步骤来禁用：

```
$ 状态| grep SELinux 状态\|当前模式
SELinux 状态: 已启用
当前模式: 执行
```

- 编辑/etc/sysconfig/selinux :

六、/etc/selinux/config

- 将 SELINUX 指令更改为禁用。

SELINUX=已禁用

- 保存并退出文件。重新启动系统：

重启

- 重启后,检查状态。SELinux 应该显示为已禁用：

```
$ 状态| grep SELinux 状态
SELinux 状态:已禁用
```

- 对于 Ubuntu 系统：

- 检查 SELinux 状态。如果状态显示已启用

, 执行进一步的步骤来禁用：

```
$ 状态| grep SELinux 状态\|当前模式
SELinux 状态:已启用
当前模式: 执行
```

- 编辑/etc/selinux/config :

六、/etc/selinux/config

- 将 SELINUX 指令更改为禁用。

SELINUX=已禁用

- 保存并退出文件。重新启动系统：

重启

- 重启后,检查状态。SELinux 应该显示为已禁用：

```
$ 状态| grep SELinux 状态  
SELinux 状态: 已禁用
```

添加语言环境en_US.UTF-8

离线守护程序包需要语言环境en_US.UTF-8。

以下是检查和添加语言环境的步骤。以root用户身份执行命令：

- 对于 RHEL/CentOS/Rocky/Ubuntu Linux 系统：
 - 检查系统上是否支持所需的语言环境en_US.UTF-8。如果可用,将显示以下内容：

```
$ locale -a |grep en_US.UTF-8
```

- 如果不可用,请添加语言环境：

```
$ localeddef -i en_US -f UTF-8 en_US.UTF-8
```

安装离线守护程序包

以下是安装离线守护程序包的步骤。以root用户身份执行命令：

- 对于 RHEL/CentOS/Rocky Linux 系统：

```
yum 清理元数据 yum 检查更新  
yum 安装 zimbra-nalpeiron-  
offline-daemon
```

- 对于 Ubuntu 系统：

```
apt-get 更新 apt-get 安  
装 zimbra-nalpeiron-离线守护进程
```

- 验证 nalpdaemon 服务是否处于活动状态：

```
$ systemctl status nalpdaemon .  
nalpdaemon.service - Nalpeiron 许可守护进程已加载:已加载 (/usr/lib/systemd/  
system/nalpdaemon.service;已启用;供应商预设:已禁用)  
活跃:自 2024-06-08 星期六 02:03:37 EDT;1 秒前开始活跃 (运行)
```

如果服务未处于活动状态,请重新启动服务：

```
$ systemctl 重新启动 nalpdaemon
```

作为zimbra用户,重新启动 LDS 和 configdctl 服务：

```
$ su - zimbra $  
zmlicensectl --service restart $ zmconfigdctl restart
```

申请并激活脱机许可证

该方法通过管理控制台和 CLI 支持。

步骤如下：

管理控制台

- 1.联系支持团队获取网络密钥和许可证密钥。
2. 登录管理控制台 ,进入主页→开始→安装许可证→离线激活
3. 在步骤1下 ,指定网络密钥和许可证密钥,然后单击生成激活请求。
4. 网络和产品激活文件生成成功后,会出现下载按钮
文本框。
5. 单击文本框旁边的下载按钮并保存文件。保存时将预先填充名称和文件类型 - network_activation_fingerprint、
product_activation_fingerprint。
6. 登录支持门户并选择 “许可证”选项卡。
7. 选择为版本 10.1 或更高版本生成脱机许可证激活文件。
8. 指定产品许可证密钥和网络许可证密钥。
- 9.复制network_activation_fingerprint.txt文件的内容并粘贴网络激活指纹
文本框。
- 10.复制product_activation_fingerprint.txt文件的内容并粘贴到产品激活指纹文本中
盒子。
11. 在产品版本文本框中指定产品版本。
- 12.点击生成许可证证书
- 13.保存生成的许可证激活 XML 文件。
- 14.返回管理控制台许可证页面。
15. 在离线激活→步骤 3 下 ,上传许可证激活 XML 文件并单击激活。
16. 激活成功后 ,您将看到一条成功消息 - 您的许可证是 已成功激活 。

命令行

1. 联系销售并获取网络密钥和许可证密钥。
2. 以zimbra用户身份运行zmlicense命令生成Network Key和License Key


```
zmlicense --offlineActivationRequestCert --network <网络密钥> --product <产品密钥>
```
3. 将屏幕上打印的证书保存为 network_activation_fingerprint.txt,并
产品_激活_指纹.txt。
4. 登录支持门户并选择 “许可证”选项卡。
5. 选择为版本 10.1 或更高版本生成脱机许可证激活文件。
6. 指定产品许可证密钥和网络许可证密钥。
7. 复制network_activation_fingerprint.txt文件的内容并粘贴网络激活指纹
文本框。
- 8.复制product_activation_fingerprint.txt文件的内容并粘贴到产品激活指纹文本中
盒子。

9. 在产品版本文本框中指定产品版本。

10. 点击生成许可证证书

11. 将生成的许可证激活 XML 文件保存在服务器上。

12. 以zimbra用户身份运行zmlicense命令激活离线许可证

```
zmlicense -A /path_to_XML/activation_file.xml
```

13. 成功激活后,您将看到一条成功消息 - 如果您在访问支持门户时遇到问题或在激活 您的许可证已成功激活
离线许可证时遇到任何问题,请联系
Zimbra 销售或支持。

当未安装或激活许可证时

如果您无法安装或激活 Zimbra 协作服务器许可证,以下情况将描述您的
Zimbra 协作服务器将受到影响。

牌照条件	描述/影响
未安装	如果没有安装许可证,Zimbra Collaboration 服务器默认为单用户 所有许可限制功能仅限于一个用户的模式。
无效	如果许可证文件被发现伪造或由于其他原因验证失败,Zimbra 协作服务器默认为单用户模式。
未激活	许可证激活宽限期为 10 天。如果此期限已过而未激活, Zimbra 协作服务器默认为单用户模式。
未来日期	如果许可证开始日期在未来,则 Zimbra 协作服务器默认 进入单用户模式。
宽限期内	Zimbra Daffodil (v10.1) 开始,宽限期功能已发生改变。 有关更多详细信息,请参阅管理指南中的宽限期部分。
已到期	如果许可证到期日期已过,30 天的宽限期已到期,并且用户 决定不获取新许可证,以下功能将停止工作 - 所有 网络功能,账户操作 (创建、编辑、删除),现代用户界面。正常 电子邮件操作将继续进行。
续约	如果许可证在宽限期内或到期后续期,网络 功能将可用,包括帐户操作和现代用户界面。邮箱 许可证激活成功后需要重新启动服务。

获取License

访问 Zimbra 网站<https://www.zimbra.com> → 产品 → 下载 → 获取试用许可证以获得试用
许可证。联系 Zimbra 销售人员延长试用许可证,或购买订阅许可证或永久许可证,
发送电子邮件至sales@zimbra.com或致电1-972-407-0688。

订阅和永久许可证只能安装在安装过程中确定的 Zimbra 协作系统上
购买。您的 Zimbra Collaboration 环境只需要一个 Zimbra 许可证。此许可证设置
系统上的最大帐户数。

您可以在管理控制台中查看当前许可证信息,包括购买的账户数量、使用的账户数量以及到期日期。

管理控制台：

主页→开始→安装许可证→当前许可证信息。

许可证协调和数据收集通知

通过同意最终用户许可协议,您授予 Synacor Inc. 及其某些许可人从您的 Zimbra 协作服务器收集许可和不可识别个人身份的使用数据的权限。

在安装、升级和使用过程中,Zimbra 协作服务器会传输信息以核对计费和许可证数据。

此项数据收集的许可是根据 Zimbra Collaboration 最终用户许可协议第 11.4 和 11.6 条授予的。许可证副本可在<https://www.zimbra.com/legal/licensing/> 找到。

正在收集的数据包括当前许可信息的元素,并受 Synacor 的隐私政策管辖,该政策可在<https://www.synacor.com/privacy-policy/> 找到。

管理控制台增强功能

许可证管理 UI 已得到增强,变得更加直观和易于遵循,其中所有与许可证部署相关的操作都在一个屏幕上。

可以通过两种方式访问许可证管理页面：

1. 登录管理控制台,进入主页→开始→安装许可证
2. 登录管理控制台,进入主页→配置→全局设置→许可证

概述

现在,所有许可证操作均可在一个屏幕上完成。以下是该部分的详细信息：

当前许可信息

显示许可证的详细信息、功能的状态以及每个功能的使用情况。

在线激活

在 Zimbra Daffodil (v10.1) 之前,这种方法被称为自动激活。

如果您的服务器直接连接到互联网,您可以使用在线方法激活许可证。

指定 18-26 个字母数字字符的许可证密钥,然后单击“激活”以激活您的许可证。成功后
激活后,您将看到一条成功消息 - 您的许可证已成功激活

离线激活

在 Zimbra Daffodil (v10.1) 之前,此方法称为手动激活。

如果您的服务器没有直接连接到互联网,您可以使用离线方法激活许可证。

有关生成离线许可证的详细步骤,请参阅离线许可证激活部分。

存储管理功能的许可证检查

Zimbra Daffodil (v10.1) 及更高版本,存储管理功能的许可证分为两部分：

1. StorageManagementEnabled - 用于启用/禁用存储管理功能的属性,以及
允许/禁止在内部存储上创建卷。
2. ObjectStoreSupportEnabled 允许/禁止在外部存储上创建卷的属性。

ObjectStoreSupportEnabled 属性依赖于 StorageManagementEnabled 属性。因此
如果不启用 StorageManagementEnabled ,则无法启用 ObjectStoreSupportEnabled
以获得许可证。

管理控制台更新

根据许可证中启用的属性,将出现以下行为：

StorageManagementEnabled = FALSE 或许可证已过期

1. 如果您尝试访问存储管理选项卡主页→配置→<服务器>→<服务器名称>→存储
管理,显示错误对话框 - 此功能许可已过期
配置 - 全局设置 - 许可证以获取更多信息。
有效。请勿或查看

2. 如果您尝试访问“全局设置主页” → “配置” → “全局设置” → “存储管理”选项卡
 存储管理显示错误对话框 - 此功能许可已过期 或者 是有效的。
 请参阅 配置 - 全局设置 - 许可证以获取更多信息。

StorageManagementEnabled = TRUE 且 ObjectStoreSupportEnabled = FALSE

如果 ObjectStoreSupportEnabled 为 false 且 StorageManagementEnabled 为 true:

1. 如果您尝试访问存储管理选项卡主页→配置→<服务器>→<服务器名称>→存储
 管理,横幅显示在页面顶部 - 你不是 目前已获得外部许可
 卷。请参阅 配置 - 全局设置 - 许可证以获取更多信息。
2. 尝试添加卷时,外部卷的选择将被禁用。
3. 您无法执行 SM 会话。“开始”按钮显示为禁用。您可以通过 CLI 执行它。
4. 您无法安排 SM 会话。安排显示为已禁用。
5. 您将能够创建新的政策。
6. 如果您尝试访问“全局设置主页” → “配置” → “全局设置” → “存储管理”选项卡
 存储管理,您将无法查看存储桶信息。
7. 设置卷时,如果之前创建过外部卷,则它们将不会出现在列表中。

StorageManagementEnabled = TRUE 且 ObjectStoreSupportEnabled = TRUE

1. 存储管理功能的所有功能均可用。
2. 您可以创建内部和外部卷。

宽限期

从 Zimbra Daffodil (v10.1)开始,邮箱服务器将在以下两种情况下进入 Grace Period:

1. LDS/第三方许可证服务器不可用。
2. 执照到期。

LDS/第三方许可证服务器不可用

如果邮箱服务器与 LDS 节点或第三方许可证服务器之间的连接丢失
 大约 30 分钟后,邮箱服务器进入宽限期。

服务器将继续在宽限期内运行,直到与 LDS / 第三方建立连接
 许可证服务器或直到许可证到期日期。

许可证到期

许可证到期后,邮箱服务器将进入宽限期。服务器将继续在宽限期内运行
 期限为30天。

管理员将继续看到许可证续订提示。当管理员登录到管理控制台时,
 主屏幕上将显示一条消息横幅,其中包含一条消息 - (N 天是许可证到期剩余的天数) 许可证处于宽限期 即将到期
 在 N 天

宽限期内的功能

当系统处于宽限期时,以下功能可用:

- 电子邮件操作-所有电子邮件操作将继续运行,不会受到影响或中断
 对于最终用户来说。

- 账户修改- 用户可以修改其账户的任何设置。例如创建签名或过滤器、更改密码等。

- 网络功能- 除恢复帐户外，所有网络功能将继续运行。

当系统处于宽限期时，以下功能不可用：

- 账户操作：

- 您不能创建新用户或删除现有用户。
- 您无法修改/更新现有用户的以下功能 - EWS、SMIME、ActiveSync 和 ZCO
- 您无法从备份中恢复帐户。

许可证到期

如果您未在 30 天的宽限期内续订许可证，则许可证将过期并且所有网络功能将停止运行。

宽限期内的功能

从 Zimbra Daffodil (v10.1.1) 开始，如果功能使用量超出允许的许可限制，则该功能将进入为期 10 天的宽限期。在此期间，将向管理员发送为期 10 天的定期通知，以通知他们宽限期内的功能。

当该功能处于宽限期时，无法为新帐户/现有帐户启用该功能。

如果该功能仍处于宽限期，则 10 天后将触发更正流程，并在帐户级别禁用过度使用的功能。通知电子邮件包含有关已禁用该功能的帐户的信息。

超出限制后，以下功能将进入宽限期：

- SMIME - 许可属性SMIMEAccountsLimit
- EWS - 许可属性EwsAccountsLimit
- MAPI (ZCO) - 许可属性MAPIConnectorAccountsLimit
- Zimbra Mobile - 许可属性MobileSyncAccountsLimit

以下是该功能进入宽限期时需要采取的纠正措施：

1. 在帐户或 COS 级别禁用该功能：例如，SMIME 功能限制为 10，使用次数为 21。管理员应为 11 个或更多用户禁用该功能，以使该功能超出宽限期并处于许可限制内。一旦该功能处于许可限制内，它将在 24 小时内恢复正常状态。

2. 增加许可限制：例如，如果 MAPI 的限制是 10，而使用的计数是 25，您可以联系我们的销售团队并请求将许可限制增加 15。限制更新后，该功能将在 24 小时内恢复正常状态。

以下是这些功能可以进入宽限期的情况：

- 升级到 Zimbra Daffodil (v10.1.1) 或更高版本：

- 升级到 Zimbra Daffodil (v10.1.1) 或更高版本后，如果功能限制超出许可账户，则该功能将进入宽限期。

- 降低许可限制：
 - 如果许可限制降低导致该功能超出限制,则该功能将进入宽限期。例如,许可证的 SMIME 限制为 100 个帐户 ,而您为 100 个帐户启用了此功能。如果将此限制降低到 50 个帐户 ,则该功能将进入宽限期。
- 恢复帐户：
 - 如果您恢复已启用功能的帐户 ,则可能会导致超出许可限制。

通知

默认情况下,服务器安装时提供的管理员账户被设置为通知电子邮件。通知电子邮件地址存储在 LDAP 属性 zimbraLicenseNotificationEmail 中,可以更改。

- 以 zimbra 用户身份执行以下操作：

```
zmprov mcf zimbraLicenseNotificationEmail newemail@domain.com
```

在以下情况下会发送通知：

1. 当超出功能限制并进入宽限期时。
2. 当宽限期功能未采取任何措施且该功能对账户禁用时。
3. 如果禁用该功能的账户超过 100 个 ,则账户列表将附加在通知电子邮件中。

以下是超出功能限制并进入宽限期时的示例通知电子邮件：

主题:Zimbra 系统警报:功能使用量超出限制

以下功能的许可账户数量已达到或超出：

MobileSyncAccountsLimit:

- 授权用户 :10
- 当前用户 :20
- 使用量超标日期 :2024 年 8 月 29 日

MAPIConnectorAccountsLimit:

- 授权用户 :10
- 当前用户 :21
- 使用量超标日期 :2024 年 8 月 29 日

SMIMEAccountsLimit:

- 授权用户 :10
- 当前用户 :20
- 使用量超标日期 :2024 年 8 月 29 日

EwsAccountsLimit:

- 授权用户 :10
- 当前用户 :20
- 使用量超标日期 :2024 年 8 月 29 日

您可以减少现有用户的使用量或增加功能许可证限制。

要增加功能许可限制,请联系 Zimbra 销售部门 sales@zimbra.com

要管理帐户功能分配,请登录管理门户。

请注意以下事项:1. 自使用量超出日期起,您将继续收到 10 天内的通知。
2. 您将无法为任何帐户启用过度使用功能。
3. 如果您不对过度使用的功能采取任何措施,该功能将被禁用,以便用户在许可限制以下使用此功能。

问候,
Zimbra 支持

以下是在宽限期内未对某项功能采取任何行动且针对少于 100 个帐户禁用该功能时的示例通知电子邮件:

主题:Zimbra 系统警报:由于使用量过大,功能已被禁用

已超出许可的账户数量,并针对以下功能在账户级别自动调整:

MobileSyncAccountsLimit

- 授权用户 :10
- 当前用户 :14
- 用户减少 :4

以下帐户已禁用该功能 :test10@domain.com test11@domain.com

test13@domain.com

test14@domain.com

EwsAccountsLimit

- 授权用户 :10
- 当前用户 :15
- 用户减少 :5

以下帐户已禁用该功能 :test10@domain.com test11@domain.com

test12@domain.com

test13@domain.com

test14@domain.com

MAPI连接器帐户限制

- 授权用户 :10
- 当前用户 :15
- 用户减少 :5

以下帐户已禁用该功能 :admin@domain.com test10@domain.com

test11@domain.com

test12@domain.com

test13@domain.com

要增加许可证数量,请访问 Zimbra 支持门户。

要管理帐户的许可证分配,请登录管理门户。

问候,

Zimbra 支持

以下是示例通知电子邮件,宽限期内未对某项功能采取任何行动,并且已为 100 多个帐户禁用该功能。帐户列表附在通知电子邮件中:

主题:Zimbra 系统警报:由于使用量过大,功能已被禁用

已超出许可的账户数量,并针对以下功能在账户级别自动调整:

SMIME 帐户限制

- 授权用户:10
- 当前用户:211
- 用户减少:201

MAPI连接器帐户限制

- 授权用户:10
- 当前用户:211
- 用户减少:201

要增加许可证数量,请访问 Zimbra 支持门户。

要管理帐户的许可证分配,请登录管理门户。

问候,

Zimbra 支持

使用预防

当为帐户或 cos 启用某项功能时,使用预防模块可防止管理员过度配置该功能。

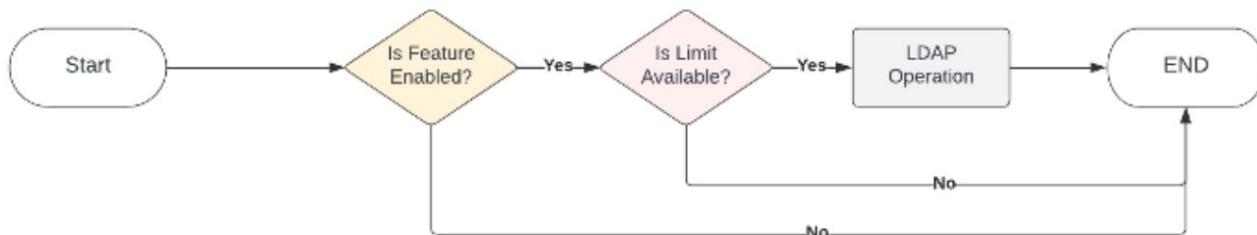
将针对以下功能执行使用预防:

- SMIME - 许可属性SMIMEAccountsLimit
- EWS - 许可属性EwsAccountsLimit
- MAPI (ZCO) - 许可属性MAPIConnectorAccountsLimit
- Zimbra Mobile - MobileSyncAccountsLimit

执行以下操作时将执行使用预防:

- 创建账户。
- 修改帐户。
- 修改 COS。

下图解释了该流程:



以下是为帐户启用该功能时将遇到的场景及其结果或 COS:

- 启用过度使用的功能- 如果您想在拥有 120 个账户的 cos 上启用 SMIME 功能,并且 SMIME 功能的许可限制为 100。由于超出了许可限制,因此将不允许该操作。

您将看到以下错误:

- 角色:

Cos 修改失败:

请禁用已使用的功能才能继续,功能列表 :zimbraFeatureSMIMEEnabled

- 帐户:

帐户修改失败:

超出以下功能的限制 :zimbraFeatureSMIMEEnabled

- 启用未经许可的功能- 如果您尝试为未经许可的 COS/帐户启用功能,您将看到以下错误:

- 角色:

Cos 修改失败:

请禁用未经授权使用的功能 :zimbraFeatureMobileSyncEnabled

- 对于帐户:

帐户修改失败:

以下功能未获得使用许可 :zimbraFeatureMobileSyncEnabled

- 启用过度使用和未经许可的功能- 当尝试为 COS/帐户启用过度使用的功能以及未经许可的功能时,您将看到以下错误:

- 角色:

Cos 修改失败:

请禁用已使用的功能才能继续,功能列表 :zimbraFeatureSMIMEEnabled

请禁用未经授权使用的功能 :zimbraFeatureMobileSyncEnabled

- 帐户:

帐户修改失败:

超出以下功能的限制 :SMIME

以下功能未获得使用许可 :zimbraFeatureMobileSyncEnabled

增强的zmlicense命令

Zimbra Daffodil (v10.1)及以后版本,许可证管理是实时的,并为管理员提供功能的整体使用情况视图。

以下是该命令现有功能的一些增强功能

[激活在线许可证密钥 - zmlicense -a](#)

- 作为 zimbra 用户,执行zmlicense -a :

```
$ zmlicense -a <激活密钥>
```

如果激活密钥有效,则会显示成功消息,否则会显示错误。

[激活脱机许可证 XML 文件 - zmlicense -A](#)

- 作为 zimbra 用户,执行zmlicense -A :

```
$ zmlicense -A <许可证激活 XML>
```

如果激活密钥有效,则会显示成功消息,否则会显示错误。

[打印许可证详细信息 - zmlicense -p](#)

- 作为 zimbra 用户,执行zmlicense -p :

```
$ zmlicense -p
```

当前激活的许可证:512345113142067890

激活产品版本:10.1.0_GA_4629 LDS 设备 ID:KgQIAuHG5gjU2kKo3VBk

功能:账户限制

状态:已授权使用

最大限制:10

使用限制:1

功能:ArchivingAccountsLimit

状态:已授权使用

最大限制:10

已使用限制:0

功能:AttachmentIndexingEnabled

状态:已授权使用

.

.

.

以下是输出的详细信息:

- 功能:许可功能的名称。
- 状态:许可功能是否有权使用:
 - 授权使用- 该功能已获得使用许可。
 - 未授权使用- 该功能未获得使用许可。
- 最大限制- 可启用该功能的最大账户数量。
- 已用限制- 该功能的使用限制。

[检查许可证状态 - zmlicense -c](#)

- 作为 zimbra 用户,执行zmlicense -c :

```
$ zmlicense -c 检查许可  
证状态。 .  
当前许可证代码:53944123451399294,激活状态:许可证正常
```

如果许可证有效,将显示成功消息,否则显示错误。

[检查单个功能状态 - zmlicense -fc <feature-code>](#)

请参阅许可证功能部分中的表格来了解功能代码。

- 作为 zimbra 用户 ,执行zmlicense -fc :

```
$ zmlicense-fc AL  
功能 AccountsLimit[AL] 状态:功能已授权使用
```

```
$ zmlicense -fc SHAL 功能  
SharingAccountsLimit[SHAL] 状态:功能未授权,请联系 zimbra 支持寻求帮助。
```

[刷新许可证缓存 - zmlicense -rc](#)

要刷新邮箱上的许可证缓存（从许可证守护程序服务重新加载数据）,您可以使用rc选项:

- 作为 zimbra 用户 ,执行zmlicense -rc :

```
$ zmlicense -rc 刷新许可  
证缓存..  
缓存刷新状态: true
```

许可证守护程序服务 [LDS]

许可证守护程序服务 (LDS) 是一项新服务,它在在线模式下与 Zimbra 许可证服务器通信,在离线模式下与 LAN 守护程序 (本地安装) 通信。

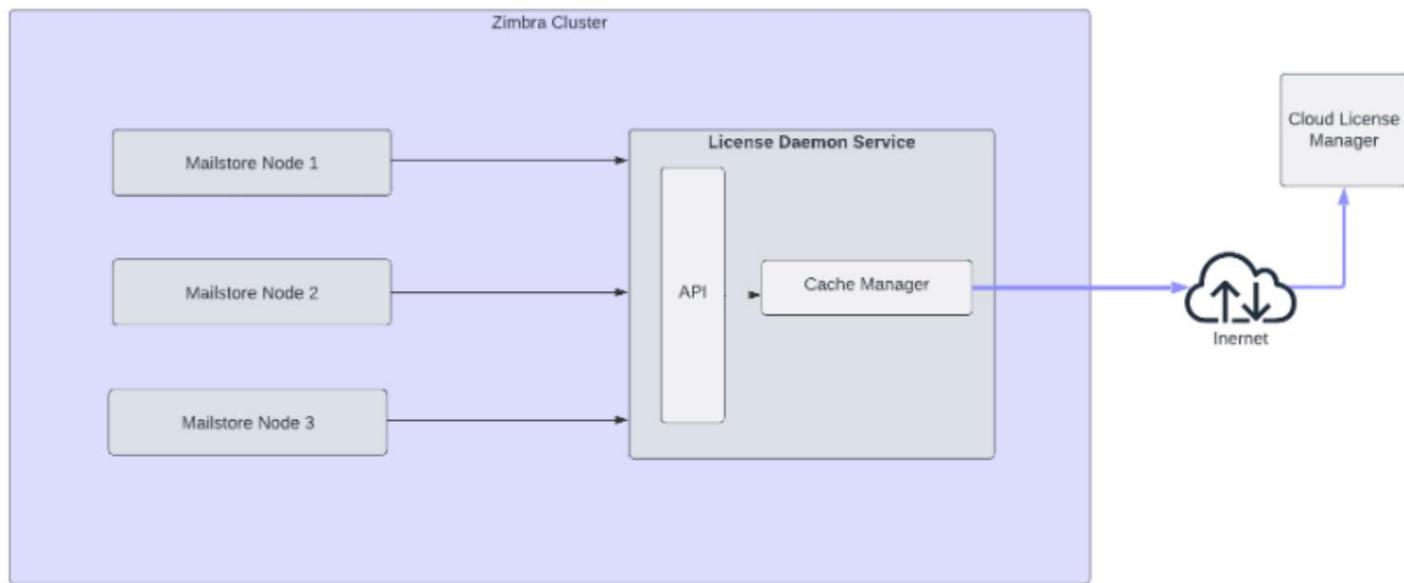
LDS 负责使用 Zimbra License Server 管理许可证信息。在安装/升级期间,它会在模块列表中显示为 zimbra-license-daemon ,并且是一项必需服务。所有实时许可操作均通过 LDS 执行。

许可证守护程序服务是 Zimbra 正常运行和许可证管理的关键且重要的服务。建议您设置服务监控来检查服务状态。

概述

1. LDS 是安装 Zimbra 时包含的简单 Java 服务。
2. 它提供了用于管理许可证的 API,例如激活许可证、为帐户分配功能或发布许可证。
3. 它是安全的,因为它使用 TLS 身份验证,并且只有邮件存储可以访问它。
4. 它保留许可证的本地缓存。
5. LDS 是支持许可证管理的必需服务。
6. 如果许可证守护程序服务未安装或未运行,Zimbra 的网络功能将无法验证并将被禁用,这将影响许可证功能和帐户管理。
7. 您可以使用 `zmlicensectl` 命令来管理服务。

以下是架构视图:



系统要求

LDS 不是资源密集型 (CPU/内存) 服务。

如果部署在专用节点上,则需要以下最低配置: 如果部署在专用节点上,以下是最低系统要求:

- 处理器系列:Intel/AMD,带 PassMark CPU 分数 > 7,000

- vCPU 数量 :2
- 内存 (GB) :8

端口

LDS 节点上的以下端口应该可以从 Mailbox 内部访问：

过程	港口
轻型结构	8081
离线 LAN 守护进程	80
离线 pg 守护进程	16700

以下端口应该可以从 LDS 到 my.nalpeiron.com 和 license.zimbra.com 主机进行外部访问：

过程	港口
Http	80
Https	443

安装单独的许可证守护程序服务节点

要将许可证守护程序服务与其他 Zimbra 服务分开，您可以设置专用的 LDS 节点。

在升级 LDAP 服务器之后和开始升级邮箱服务器之前需要设置此节点。

除非管理员在 Zimbra 安装过程中默认安装 zimbra-license-daemon 软件包

Zimbra 安装期间对包进行标记。

键入并按回车

进入

安装 zimbra-license-daemon 包。

重击

安装 zimbra-license-daemon [Y]

在单独的服务器上安装 zimbra-license-daemon 包

解压 Zimbra Daffodil (v10.1) 并执行安装程序脚本 ./install.sh。

键入并按回车

进入

安装 zimbra-license-daemon 包。

选择要安装的软件包

安装 zimbra-ldap [Y] N

安装 zimbra-logger [Y] N

安装 zimbra-mta [Y] N

安装 zimbra-dnscache [Y] N

安装 zimbra-snmp [Y] N

安装 zimbra-license-daemon [Y] Y

安装 zimbra-store [Y] N

安装 zimbra-apache [Y] N

安装 zimbra-spell [Y] N

安装 zimbra-convertd [Y] N

安装 zimbra-memcached [Y] N

安装 zimbra-proxy [Y] N

安装 zimbra-archiving [N] N

安装 zimbra-onlyoffice [Y] N

安装 zimbra-patch [Y] N

安装 zimbra-mta-patch [Y] N

安装 zimbra-proxy-patch [Y] N

完成剩余的安装。

设置邮箱服务器

LDS 节点安装成功完成后,您现在可以安装/升级邮箱服务器。

解压 Zimbra Daffodil (v10.1) 并执行安装程序脚本./install.sh 。

如果升级现有的邮箱服务器,请在提示时提供有效的许可证密钥并继续直到包选择步骤。

ZCS 将从 8.8.15 升级到 10.1.0。

验证现有许可证是否已过期并检查其是否有资格升级

请输入许可证密钥 (18-24 个字符的字母数字字符串,不含任何特殊字符) :5332567329720607741

成功:许可证有效

许可证有效并支持此次升级。继续。

验证 ldap 配置

您还可以使用./install.sh命令指定许可证密钥。如果验证成功,安装程序将继续:

```
./install.sh --许可证密钥 5332567329720607741
```

如果安装新的邮箱服务器,请继续至包选择步骤。

- 以下是设置邮箱服务器以使用专用 LDS 节点的步骤:
- 选择N作为安装 zimbra-license-daemon选项。

安装 zimbra-license-daemon [Y] N

- 安装程序将显示以下提示。输入Y

您是否在不同节点上安装了 zimbra-license-daemon 包 [N] Y

- 安装程序将提示输入安装 LDS 的主机。指定 LDS 主机名:

请输入 zimbra-license-daemon 主机 [] <LDS_Hostname>

- 如果 LDS 正在服务器上运行,安装将继续。
- 如果服务器无法连接 LDS,安装程序将显示许可证守护程序应该正在运行
并且正常运行并中止安装。请检查与服务器的连接并重新启动安装。
请参阅故障排除部分,了解常见错误及其解决方案。

LDS 管理命令zmlicensectl

引入了新命令zmlicensectl来管理 LDS 的各种操作。

由于许可证守护程序服务是一项关键且重要的服务,因此它不通过 zmcontrol命令。zmcontrol命令将显示状态,但您无法启动/停止/重新启动 LDS。

以下是有关选项的详细信息:

运营	范围	描述
显示帮助	- 帮助	显示帮助
服务管理	--service <参数>	管理各种 运营
	--服务启动、重启、停止、状态	启动、重新启动、停止或 检查服务状态
	--service setLogLevel=INFO,DEBUG,ERROR,WARN	设置各种日志级别。 有助于调试。
	--service设置离线模式 = true,false	启用/禁用离线 模式

运营	范围	描述
离线服务 管理	--nalpeiron <参数>	离线许可证 模式启用,此参数用于管理离 线服务
	--nalpeiron启动、重启、停止、状态	启动、重新启动、停止或 检查离线服务 地位
导出离线数据	--exportOfflineLicenseData	提取离线许可证 用于分析和计费的使用数据
清除许可证目录	--clearLicenseWorkDir	解决潜在许可证缓存问题的故障排 除选项 轻型结构

例子：

- 要重新启动 LDS,请以zimbra用户身份执行以下命令：

```
zmlicensectl --service restart
```

- 要在调试模式下设置日志级别,请以zimbra用户身份执行以下命令：

```
zmlicensectl --service setLogLevel=DEBUG
```

- 要将许可模式从在线更改为离线,请以zimbra用户身份执行以下命令：

```
zmlicensectl --service setOfflineMode=true
```

- 要重新启动离线模式所需的 LAN 守护程序,请以zimbra用户身份执行以下命令：

```
zmlicensectl --nalpeiron 重启
```

- 要导出离线使用数据（仅 BSP 需要）,请以zimbra用户身份执行以下命令：

```
zmlicensectl --exportOfflineLicenseData
```

故障排除

日志记录

以下是记录所有许可操作的日志：

- 邮件存储日志：

- 包含邮件存储操作的日志
- 位置： /opt/zimbra/log/mailbox.log 许可证守护
- 进程服务日志
 - 包含与邮件存储和 LDS 之间的 API 通信相关的日志
 - 位置： /opt/zimbra/log/license-daemon-service.log
- 本地库日志
 - 包含与 nalpeiron 服务器通信时发生的库错误。
 - 位置： /opt/zimbra/license/work/15xx.log

许可证守护程序服务日志

LDS 的文件日志记录机制已通过滚动策略得到增强,该策略根据大小和时间管理日志文件。这可确保高效存储日志,并根据定义的时间归档或删除较旧的日志标准。

以下是详细信息：

1. 文件位置： /opt/zimbra/log/license-daemon-service.log

2. 日志格式：日志包括时间戳、线程名称、日志级别和消息。例如

```
2024-08-01 10:11:03 [main] INFO c.zimbra.license.service.Application - 以下 1 个配置文件处于活动状态：“dev”
```

3. 历史记录管理：保留指定天数的日志文件历史记录。日志文件保留最多 15 天。超过 15 天的文件将自动删除,以遵守保留策略。

4. 大小上限：所有日志文件的总大小不得超过 5 GB。一旦达到此限制，较旧的日志文件将被删除以便为新文件腾出空间。

5. 基于大小的滚动：当日志文件达到指定的最大大小（最大限制：500 MB）时,就会进行轮换。这意味着在创建新文件之前,每个日志文件的大小将被限制为 500 MB。

6. 基于时间的滚动：基于时间的滚动配置可确保日志文件按日期组织,并且每天都创建一个新的日志文件。

◦ 基于时间大小的滚动

每日文件：

- 每日创建：每天都会创建一个新的日志文件,其基本名称为 license-daemon-service.log。例如,2024 年 9 月 1 日的日志将保存在名为 license-daemon-service.log 的文件中。
- 每日结束时滚动：在每日结束时,日志文件将滚动并使用 YYYY-MM-DD 格式的日期戳重命名。例如,2024 年 9 月 1 日的日志将保存为 license-daemon-service-2024-09-01.0.log,如果文件在一天内滚动多次,则后续文件将按顺序编号,例如 license-daemon-service-2024-09-01.1.log、license-daemon-service-2024-09-01.2.log 等。

访问日志：

- 当前日期日志：要访问当前日期的日志文件,可以使用命令 tail -f /opt/zimbra/log/license-daemon-service.log。

- 前一天的日志:要访问前一天的日志,您应该使用带日期戳的日志文件。例如,可以使用 cat /opt/zimbra/log/license-daemon-service-2024-09-01.0.log 访问 2024 年 9 月 1 日的日志。

文件索引:

- 顺序编号:如果由于超出最大文件大小 (maxFileSize)而在同一天内生成多个日志文件,则文件将按顺序编号。例如,

许可证守护进程服务-2024-09-01.0.log 许可证守护进程服务-2024-09-01.1.log 许可证守护进程服务-2024-09-01.2.log

错误条件/代码

您可能会遇到各种许可证错误/代码或特定错误。

以下是一些常见情况及其解决方法:

许可证激活失败:

- 当邮件存储尝试连接到 LDS 时, license-daemon 应该正在运行并且出现健康错误:
 - 确保 LDS 已启动并正在运行。
 - 检查状态 - zmlicensectl --service status
 - 如果没有运行,请重新启动服务 - zmlicensectl --service restart
- 无法激活许可证:
 - 确保 LDS 节点可以访问互联网。
- 无效许可证错误,代码为“4001”:
 - 验证许可证未过期。
- 无效许可证错误,代码为“-10116”:
 - 检查帐户是否有有效的支持结束日期。
- 无效许可证错误,代码为“-5000”:
 - 支持结束日期可能为空。
- 无效许可证错误,代码为“-401”:
 - 许可证激活受到限制或许可证不活动。
- 无效许可证错误,错误代码为“4000”:
 - 许可证使用无效。如果您尝试更改许可证,则可能会发生这种情况。
- 无效许可证错误,代码为“4002”:
 - 在常规许可证设置下无法激活试用版。

功能检查失败:

- 确保 LDS 已启动并正在运行 - zmlicensectl --service status
 - 如果没有运行,请重新启动 LDS 服务 - zmlicensectl --service restart
- 无法使用服务器级功能,例如备份还原、存储管理等。

- 确保功能已被授权使用 - zmlicense -fc <feature_code>
zmmailboxdctl restart
** 如果已启用,则重新启动邮箱 -
- 无法启用帐户/cos 上的功能:
 - 确保功能已被授权使用 - zmlicense -fc <feature_code>
 - 如果功能属于限制类型,请确保您有足够的限制 - zmlicense -p | grep -E
(EwsAccountsLimit) -A3
 - 如果功能属于限制类型,请确保您有足够的限制 - zmlicense -p | grep -E
(EwsAccountsLimit) -A3

Zimbra 邮箱服务器

Zimbra 邮箱服务器是一个专用服务器,用于管理所有邮箱内容,包括消息、联系人、日历和附件。

Zimbra 邮箱服务器有专用的卷用于备份和日志文件。每个 Zimbra 邮箱服务器只能看到自己的存储卷。Zimbra 邮箱服务器无法查看、读取或写入其他服务器。

邮箱服务器

每个帐户都配置在一个邮箱服务器上,并且该帐户与一个邮箱相关联,该邮箱包含该帐户的电子邮件、附件、日历、联系人和协作文件。

每个邮箱服务器都有自己的独立邮件存储、数据存储和索引存储,用于存储该服务器上的邮箱。以下是每个存储及其目录位置的概述。

消息存储

所有电子邮件消息均以 MIME 格式存储在消息存储中,包括消息正文和文件附件。

默认情况下,邮件存储位于每个邮箱服务器的/opt/zimbra/store下。每个邮箱都有自己的目录,以其内部邮箱 ID 命名。邮箱 ID 对于每个服务器都是唯一的,而不是系统范围内的。

有多个收件人的邮件在邮件存储中存储为单个副本。在 UNIX 系统上,每个用户的邮箱目录都包含指向实际文件的硬链接。

安装 Zimbra Collaboration 后,每个邮箱服务器上都会配置一个索引卷和一个消息卷。每个邮箱都会被分配到当前索引卷上的永久目录。当有新消息被发送或创建时,该消息会保存在当前消息卷中。

要管理电子邮件存储资源,您可以通过实施存储管理 (SM) 策略来配置旧邮件的存储卷。请参阅管理配置。

数据存储

数据存储是一个 SQL 数据库,其中内部邮箱 ID 与用户帐户相关联。所有消息元数据 (包括标签、对话和指针) 都指示消息在文件系统中的存储位置。SQL 数据库文件位于/opt/zimbra/db 中。

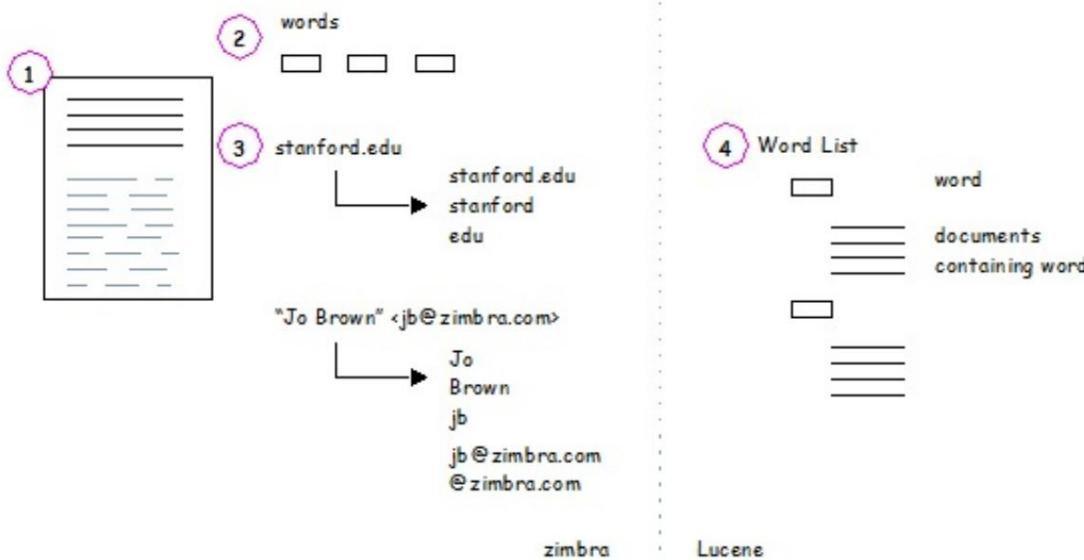
每个帐户 (邮箱) 仅驻留在一台服务器上。每台服务器都有自己的独立数据存储,其中包含该服务器上邮箱的数据。

- 数据存储将邮箱 ID 映射到用户的 LDAP 帐户。Zimbra Collaboration 数据库中的主要标识符是邮箱 ID,而不是用户名或帐户名。邮箱 ID 仅在单个邮箱服务器内是唯一的。
- 数据存储数据库中包含用户的标签定义、文件夹、联系人、日历约会、任务、公文包文件夹和过滤规则等元数据。
- 有关每封邮件的信息 (包括是否已读或未读以及关联的标签) 都存储在数据存储数据库中。

索引存储

索引和搜索技术通过 Apache Lucene 提供。每封电子邮件消息和附件在消息到达时都会自动编入索引。每个帐户都关联一个索引文件。索引文件位于 /opt/zimbra/index。

管理员或用户无法配置标记和索引过程。



流程如下：

1. Zimbra MTA 将收到的电子邮件路由到包含该帐户邮箱的邮箱服务器。
2. 邮箱服务器解析邮件,包括邮件头、邮件正文以及所有可读文件附件,如作为 PDF 文件或 Microsoft Word 文档,以便标记单词。
3. 邮箱服务器将标记化的信息传递给Lucene以创建索引文件。

标记化是按每个单词进行索引的方法。某些常见模式 (例如电话号码、电子邮件地址和域名)被标记化,如消息标记化图示所示。

Web 应用程序服务器

Jetty Web 应用服务器在任何商店服务器上运行 Web 应用程序 (webapps)。它提供一个或多个 Web 应用程序服务。

邮件存储服务

邮件存储服务提供对邮箱/帐户数据的后端访问。邮件存储的 Web 应用程序包括：

- Mailstore (邮件服务器)= /opt/zimbra/jetty/webapps/service
- Zimlets = /opt/zimbra/jetty/webapps/zimlet

用户界面服务

用户界面服务提供对邮箱帐户数据和管理的前端用户界面访问

控制台,包括：

- Web 应用程序 = /opt/zimbra/jetty/webapps/zimbra
- Zimbra 管理员控制台 = /opt/zimbra/jetty/webapps/zimbraAdmin

- Zimlets = /opt/zimbra/jetty/webapps/zimlet

备份邮箱服务器

Zimbra Collaboration 包含一个可配置的备份管理器,它驻留在每个 Zimbra Collaboration 服务器上,并执行备份和恢复功能。您不必停止 Zimbra Collaboration 服务器即可运行备份过程。备份管理器可用于恢复单个用户,而不必在某个用户的邮箱损坏时恢复整个系统。完整备份和增量备份位于/opt/zimbra/backup中。请参阅备份和恢复。

每个 Zimbra 邮箱服务器都会生成重做日志,其中包含自上次增量备份以来邮件存储服务器处理的当前事务和存档事务。服务器恢复时,在备份文件完全恢复后,将重播存档中的所有重做日志和当前正在使用的重做日志,以使系统恢复到故障前的状态。

邮箱服务器日志

Zimbra Collaboration 部署由各种第三方组件和一个或多个邮箱服务器组成。

每个组件都可以生成自己的日志输出。本地日志位于/opt/zimbra/log中。

选定的 Zimbra Collaboration 日志消息会生成 SNMP 陷阱,您可以使用任何 SNMP 监控软件捕获这些陷阱。请参阅监控 Zimbra 服务器。

系统日志、重做日志和备份会话应该放在单独的磁盘上,以尽量减少其中一个磁盘发生故障时发生不可恢复的数据丢失的可能性。

信息访问协议

Zimbra Collaboration 有一个内置的 IMAP 服务器,该服务器默认安装,是 zimbra-mailboxd 进程 (Zimbra 邮箱服务器)的一部分。

常见的 IMAP 配置设置

以下全局和服务器级配置属性可用于控制和调整 IMAP 服务。

- zimbralmapServerEnabled。设置为 TRUE 时,进程内 IMAP 服务器启用。设置为 FALSE 时,进程内 IMAP 服务器禁用。默认值为 TRUE。
- zimbralmapSSLServerEnabled。设置为 TRUE 时,进程内 IMAP SSL 服务器启用。设置为 FALSE 时,进程内 IMAP SSL 服务器禁用。默认值为 TRUE。
- zimbralmapBindAddress (只能在服务器级别设置)。指定进程内 IMAP 服务器应侦听的接口地址;如果为空,则绑定到所有接口。
- zimbralmapBindPort。指定进程内 IMAP 服务器应监听的端口号。默认值为 7143。
- zimbralmapSSLBindAddress (只能在服务器级别设置)。指定进程内 IMAP SSL 服务器应侦听的接口地址;如果为空,则绑定到所有接口。
- zimbralmapSSLBindPort。指定进程内 IMAP SSL 服务器应侦听的端口号。默认值为 7993。
- zimbralmapNumThreads。指定 IMAP 处理程序线程池中的线程数。Zimbra Collaboration 默认使用 IMAP NIO,这允许每个 IMAP 处理程序线程处理多个连接。默认值 200 足以处理最多 10,000 个活动 IMAP 客户端。
- zimbralmapCleartextLoginEnabled。指定是否允许通过非 SSL/TLS 连接进行明文登录。默认值为 FALSE。
- zimbralmapProxyBindPort。指定 IMAP 代理服务器应侦听的端口号。默认值为 143。有关更多信息,请参阅 Zimbra 代理组件。
- zimbralmapSSLProxyBindPort。指定 IMAP SSL 代理服务器应侦听的端口号。默认值为 993。有关更多信息,请参阅 Zimbra 代理组件。
- zimbralmapMaxRequestSize。指定 IMAP 请求的最大大小 (以字节为单位,不包括文字数据)。注意:此设置不适用于 IMAP LOGIN 请求。IMAP LOGIN 请求由 IMAP 代理 (Zimbra 代理组件) 处理,限制为 256 个字符。
- zimbralmapInactiveSessionCacheMaxDiskSize。指定驱逐前非活动 IMAP 缓存的最大磁盘大小 (以字节为单位)。默认情况下,此值为 10GB。这是一个粗略的限制,因为由于 Ehcache 的内部结构,磁盘上的实际大小通常会略微超过此限制。
- zimbralmapInactiveSessionEhcsize。指定驱逐前非活动会话缓存的最大堆大小 (以字节为单位)。默认情况下,此值为 1 兆字节。这是一个粗略的限制,因为由于 Ehcache 的内部结构,内存中的实际大小通常会略微超过此限制。
- zimbralmapActiveSessionEhcsize。指定 imap 活动会话缓存在驱逐前将占用的最大磁盘空间量 (以字节为单位)。默认情况下,此值为 100 GB。这是一个粗略的限制,因为由于 ehcache 的内部结构,内存中的实际大小通常会略微超过此限制。

Zimbra LDAP 服务

LDAP 目录服务为有权使用 Zimbra 服务的用户和设备的信息提供了一个集中存储库。Zimbra 的 LDAP 数据使用的中央存储库是 OpenLDAP 目录服务器。

Zimbra Collaboration 支持与 Microsoft 的 Active Directory Server 集成。请联系支持人员以获取有关特定目录实施方案的信息。

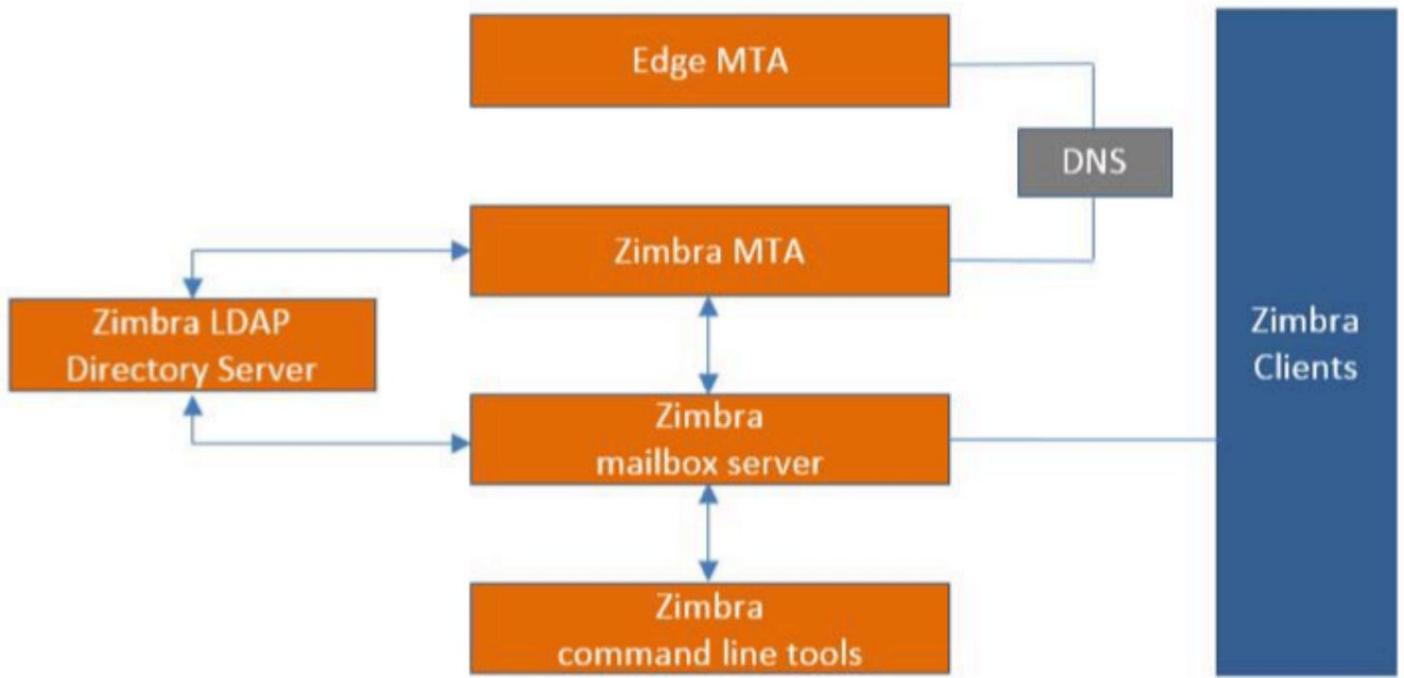
安装 Zimbra 时会安装 LDAP 服务器。每个服务器都有自己的 LDAP 条目，其中包含指定操作参数的属性。此外，全局配置对象会为条目未指定每个属性的任何服务器设置默认值。

可以通过 Zimbra 管理控制台修改这些属性的子集，并通过 zmprov 命令修改其他属性。

LDAP 流量

LDAP 目录流量图显示了 Zimbra-LDAP 目录服务器与 Zimbra Collaboration 系统中其他服务器之间的流量。Zimbra MTA 和 Zimbra Collaboration 邮箱服务器从目录服务器上的 LDAP 数据库读取或写入。

Zimbra 客户端通过 Zimbra 服务器进行连接，而 Zimbra 服务器则连接到 LDAP。

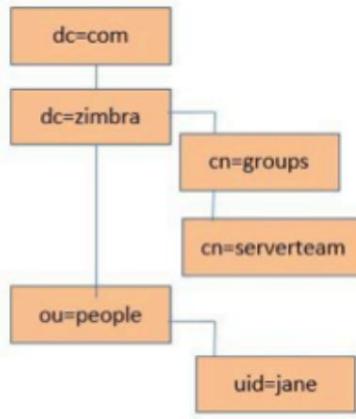


LDAP 目录层次结构

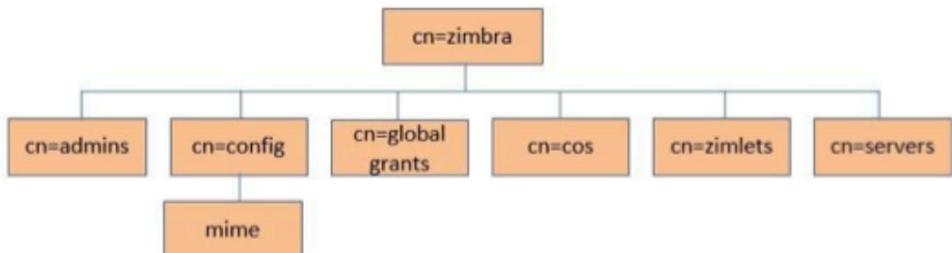
LDAP 目录采用分层树状结构排列，包含两种类型的分支：邮件分支和配置分支。邮件分支按域组织。属于域的条目（例如帐户、组、别名）在目录中的域 DN 下配置。配置分支包含不属于域的管理系统条目。配置分支条目包括系统管理员帐户、全局配置、全局授权、COS、服务器、MIME 类型和 Zimlet。

Zimbra LDAP 层次结构图显示了 Zimbra LDAP 层次结构。每种类型的条目（对象）都有某些关联的对象类。

Domain Branch



Config Branch



LDAP 目录条目由一组属性组成，具有全局唯一的专有名称 (dn)。

条目允许的属性由与该条目关联的对象类属性决定。对象类属性的值决定了条目遵循的架构规则。

条目的对象类决定了条目的类型，称为结构对象类，不可更改。其他对象类称为辅助对象类，可以在条目中添加或删除。

在 LDAP 中使用辅助对象类可以将对象类与现有对象类相结合。例如，具有结构对象类inetOrgPerson和辅助对象类zimbraAccount的条目将是一个帐户。具有结构对象类zimbraServer的条目将是 Zimbra 系统中安装了一个或多个 Zimbra 包的服务器。

Zimbra 协作 LDAP 模式

每个 LDAP 实现的核心都是使用模式组织的数据库。

Zimbra LDAP 架构扩展了 OpenLDAP 软件中包含的通用架构。它旨在与现有目录安装共存。

所有专为 Zimbra Collaboration 创建的属性和对象类都以“zimbra”开头，例如zimbraAccount对象类或zimbraAttachmentsBlocked属性。

OpenLDAP 实现中包含以下模式文件：

- 核心架构
- 余弦模式
- inetorgperson.schema
- zimbra.schema
- amavisd 架构
- dyngroup.schema
- nis.schema

您不能修改 Zimbra 模式。

Zimbra 协作对象

目的	描述	对象类
帐户	<p>表示 Zimbra 邮箱服务器上可登录的帐户。帐户条目可以是管理员帐户，也可以是用户帐户。对象类名称为zimbraAccount。此对象类扩展了zimbraMailRecipient对象类。</p> <p>所有帐户均具有以下属性：</p> <ul style="list-style-type: none"> • 格式为 user@example.domain 的名称，永不改变且永不重复使用的唯一 ID。 • 一组属性，其中一些是用户可修改的（首选项），而其他属性只能由管理员配置。 • 所有用户帐户都与一个域相关联，因此在创建任何用户帐户之前必须先创建域帐户。 	zimbra账户
服务等级 (COS)	<p>定义帐户的默认属性以及允许或拒绝功能。COS 控制功能、默认首选项设置、邮箱配额、邮件生存期、密码限制、附件阻止以及用于创建新邮件的服务器池</p> <p>帐户。</p>	zimbraCOS
域	<p>表示电子邮件域，例如example.com或example.org。必须先存在该域，然后才能向该域中的用户发送电子邮件。</p>	zimbra域名
分发列表	<p>也称为邮件列表，用于通过向列表地址发送单封电子邮件来向列表的所有成员发送邮件。</p>	zimbra 分发列表
动态组	<p>类似于分发列表。不同之处在于成员动态组的搜索由 LDAP 搜索动态计算。LDAP 搜索过滤器在动态组条目上的属性。</p> <p>分发列表和动态组均可用作委派管理员框架中的被授权者或目标。</p>	zimbra集团

目的	描述	对象类
服务器	表示 Zimbra 系统中安装了一个或多个 Zimbra 软件包的特定服务器。属性描述服务器配置信息,例如服务器上正在运行哪些服务。	zimbra服务器
全局配置	为以下对象指定默认值:服务器和域。如果未设置属性 其他对象,这些值是从全局设置中继承的。全局配置值是必需的,并在安装期间作为 Zimbra 核心包的一部分进行设置。这些将成为系统的默认值。	zimbra全局配置
别名	表示帐户、分发列表或动态组的别名。zimbraAliasTarget属性指向此别名条目 的目标条目。	zimbra别名
齐姆莱特	定义在 Zimbra 中安装和配置的 Zimlet。	zimbraZimletEntry
日历资源	定义日历资源,例如会议室 或可以选择用于会议的设备。日历资源是具有其他 zimbraCalendarResource对象类的属性。	zimbraCalendarResource
身份	代表用户的角色。角色包含用户的身份,例如显示名称和用于发送电子邮件的签名条目的链接。用户可以创建多个角色。身份条目在 DIT 中用户的 LDAP 条目下创建。	zimbra身份
数据源	表示用户的外部邮件源。数据源的两个示例是 POP3 和 IMAP。数据源 包含用户外部电子邮件帐户的 POP3/IMAP 服务器名称、端口和密码。 数据源还包含个人信息,包括显示名称和代表外部帐户发送的外发电子邮件 签名条目的链接。数据源条目的创建 在 DIT 中的用户 LDAP 条目下。	zimbra数据源
签名	代表用户的签名。用户可以创建多个签名。签名条目在 DIT 中的用户 LDAP 条目下创建。	zimbra签名

账户认证

支持的身份验证机制包括内部、外部 LDAP 和外部 Active Directory。身份验证方法类型是按域设置的。如果未设置zimbraAuthMech属性，则默认使用内部身份验证。

内部身份验证方法使用在 OpenLDAP 服务器上运行的 Zimbra 模式。

可以启用zimbraAuthFallbackToLocal属性，以便当外部身份验证失败时系统返回到本地身份验证。默认值为 FALSE。

内部认证机制

内部身份验证方法使用在 OpenLDAP 目录服务器上运行的 Zimbra 架构。对于存储在 OpenLDAP 服务器中的帐户，userPassword属性存储用户密码的加盐 SHA512 (SSHA512) 摘要。用户提供的密码被计算到 SSHA 摘要中，然后与存储的值进行比较。

外部 LDAP 和外部 AD 身份验证机制

如果电子邮件环境使用另一个 LDAP 服务器或 Microsoft Active Directory 进行身份验证，并使用 Zimbra LDAP 进行所有其他 Zimbra Collaboration 相关事务，则可以使用外部 LDAP 和外部 Active Directory 身份验证。这要求用户同时存在于 OpenLDAP 和外部 LDAP 服务器中。

外部身份验证方法尝试使用提供的用户名和密码绑定到指定的 LDAP 服务器。如果绑定成功，则关闭连接并认为密码有效。

外部身份验证需要zimbraAuthLdapURL和zimbraAuthLdapBindDn属性。

- zimbraAuthLdapURL属性ldap://ldapserver:port/标识外部目录服务器的 IP 地址或主机名，port 是端口号。您也可以使用完全限定的主机名代替端口号。

例如：

```
ldap://server1:3268 ldap://  
exch1.acme.com
```

如果是SSL连接，请使用ldaps:而不是ldap:，服务器使用的SSL证书必须配置为受信任的证书。

- zimbraAuthLdapBindDn属性是一个格式字符串，用于确定绑定到外部目录服务器时使用哪个 DN。

在身份验证过程中，用户名的起始格式为： user@example.com

用户名可能需要转换为外部目录中的有效 LDAP 绑定DN（可分辨名称）。在 Active Directory 的情况下，该绑定DN可能位于不同的域中。

自定义身份验证

您可以实施自定义身份验证，将外部身份验证集成到您的专有身份数据库中。当身份验证请求进入时，Zimbra 会检查域的指定身份验证机制。如果身份验证机制设置为自定义身份验证，Zimbra 会调用已注册的自定义身份验证处理程序来对用户进行身份验证。

要设置自定义身份验证,请为自定义身份验证准备域并注册自定义身份验证
處理程序。

准备用于自定义身份验证的域

要为自定义身份验证启用域,请将域属性zimbraAuthMech 设置为 custom:{registered-custom-auth-handler-name}。

在以下示例中,“sample”是注册自定义身份验证的名称。

例 为自定义身份验证启用域

```
zmprov 修改域 {域|id} zimbraAuthMech 自定义 :示例
```

重击

注册自定义身份验证处理程序

要注册自定义身份验证处理程序,请调用:

```
ZimbraCustomAuth.register (处理程序名称,处理程序)
```

爪哇

在扩展的 init 方法中。

- 类: com.zimbra.cs.account.ldap.ZimbraCustomAuth
- 方法: public synchronized static void register (String handlerName, ZimbraCustomAuth handler)
 定义:
 - handlerName是此自定义身份验证处理程序在 Zimbra 身份验证中注册的名称
基础设施。此名称在域的 zimbraAuthMech 属性中设置。
 - handler是调用此自定义身份验证处理程序的 authenticate 方法的对象。该对象
必须是ZimbraCustomAuth (或其子类)的实例。

例子 2. 注册 → 自定义身份验证处理程序

```
公共类SampleExtensionCustomAuth实现ZimbraExtension {
    公共无效初始化 ()抛出服务异常{
        /*
         *   注册自定义:样本 到 Zimbra 的身份验证基础设施
         *   应该是 */
        ZimbraCustomAuth.注册 ( “样本” , new SampleCustomAuth () );
    }
    ...
}
```

爪哇

自定义身份验证的工作原理

当身份验证请求进入并且指定域使用自定义身份验证时,
身份验证框架调用作为传递的ZimbraCustomAuth实例上的身份验证方法
处理程序参数到ZimbraCustomAuth.register() 。

需要认证的主体的账户对象和用户输入的明文密码被传递到ZimbraCustomAuth.authenticate()。

可以从帐户对象中检索帐户的所有属性。

Kerberos5 身份验证机制

Kerberos5 身份验证机制根据外部 Kerberos 服务器对用户进行身份验证。

1.将域属性zimbraAuthMech设置为kerberos5。

2.将域属性zimbraAuthKerberos5Realm设置为该域中的用户所在的 Kerberos5 领域

在 Kerberos 数据库中创建。当用户使用电子邮件密码和域登录时， zimbraAuthMech 设置为kerberos5 ，服务器通过{localpart-of-the-email}@{value-of-zimbraAuthKerberos5Realm}构建 Kerberos5 主体并使用它来向 kerberos5 服务器进行身份验证。

要为个人帐户指定 Kerberos5,请将帐户的zimbraForeignPrincipal设置为kerberos5:

{kerberos5-principal} 。例如:kerberos5:user1@MYREALM.COM。

全局地址列表

全局地址列表 (GAL) 是公司用户目录,通常在组织内部,即可供电子邮件系统的所有用户使用。Zimbra Collaboration 使用公司目录来查找用户公司内部的地址。

对于每个 Zimbra Collaboration 域,您可以配置 GAL 以使用:

- 外部 LDAP 服务器
- Zimbra Collaboration 内部 LDAP 服务器
- GAL 搜索中的外部 LDAP 服务器和 Zimbra Collabre LDAP

Zimbra Collaboration Web Client 可以搜索 GAL。当用户搜索某个名称时,该名称会显示类似于以下示例的 LDAP 搜索过滤器,其中字符串%s是用户正在搜索的名称为了。

搜索 GAL 的示例

```
((cn=%s*)(sn=%s*)(gn=%s*)(mail=%s*)
(zimbraMailDeliveryAddress = %s*)
(zimbraMailAlias=%s*)
(zimbraMailAddress = %s*))
```

Zimbra Collaboration 中的 GAL 属性

映射到 Zimbra 协作联系人表的属性将通用 GAL 搜索属性映射到其Zimbra 协作联系人字段。

LDAP 属性映射到 GAL 条目字段。例如,LDAP 属性displayName和cn可以映射到 GAL 条目字段fullName 。映射在zimbraGalLdapAttrMap属性中配置。

表属性映射至Zimbra 协作联系人

标准 LDAP 属性	Zimbra 协作联系人字段

标准 LDAP 属性	Zimbra 协作联系人字段
合作	工作国家
公司	公司
名字/gn	名
锡	姓
中国	全名
首字母	首字母
升	工作城市
街道,街道地址	工作街
邮政编码	工作邮政编码
電話號碼	工作电话
移动的	移动的
寻呼机	寻呼机
传真电话号码	传真号码
英石	工作状态
标题	职称
邮件	电子邮件
缩略图照片	缩略图照片
对象类	当前未映射

Zimbra Collaboration GAL 搜索参数

GAL 是按域配置的。要配置属性，您可以运行 GAL 配置向导从管理控制台。

修改属性

通过 Zimbra 管理控制台或来自 zmprov 命令。

用户可以在目录中修改其帐户的属性。当用户从 Zimbra 更改其选项时经典的 Web App，当他们改变偏好设置时，他们也会修改属性。

刷新 LDAP 缓存

当您修改 Zimbra LDAP 服务器中的以下类型的条目时，可能需要刷新 LDAP 缓存使更改在服务器上可用。

- 主题

- 前提
- 帐户
- 群组
- 操作系统
- 域
- 全局配置
- 服务器
- Zimlet 配置

[清除主题和区域设置的缓存](#)

当您在服务器上添加或更改 Zimbra 的主题（皮肤）属性文件和语言环境资源文件时，必须刷新缓存以使新内容可用。

到 冲洗皮肤：

`zmprov flushCache 皮肤`

重击

[刷新区域](#)

`zmprov flush本地缓存`

重击

[清除账户、组、COS、域和服务器](#)

当您修改账户、COS、组、域和服务器属性时，更改将在修改的服务器上立即生效。在其他服务器上，如果属性被缓存，LDAP 条目将在一段时间后自动更新。

Zimbra 默认的服务器更新时间为 15 分钟。缓存周期在本地配置键上配置。

到 更改设置：

`zmlocalconfig ldap_cache_<对象>_maxage`

重击

到 立即启用更改：

`zmprov flushCache {帐户|cos|域|组|服务器|...} [名称|id]...`

重击

如果您没有指定名称或 ID 以及类型，则会刷新缓存中该类型的所有条目并重新加载缓存。

某些服务器属性即使在刷新缓存后也需要重新启动服务器。例如，绑定端口或处理线程数等设置。

[刷新全局属性](#)

修改全局配置属性时，更改将在修改的服务器上立即生效。在其他邮箱服务器上，您必须刷新缓存以使更改可用或重新启动服务器。全局配置属性的 LDAP 条目不会过期。

某些全局配置属性在服务器每次重启时仅计算一次到内部表示中。出于效率原因,对这些属性的更改只有在服务器重启后才会生效,即使在刷新缓存后也是如此。此外,某些全局配置设置和从全局配置继承的服务器设置仅在服务器启动时读取一次,例如端口或处理线程数。修改这些类型的属性需要重启服务器。

要刷新所有服务器上的全局配置更改的缓存:

1. 修改本地服务器的设置

```
zmprov mcf zimbraMailmapClearTextLoginEnabled TRUE
```

重击

更改是通过本地配置键zimbra_zmprov_default_soap_server和
zimbra_admin_service_port标识的服务器执行的。

2. 要刷新所有其他服务器上的全局配置缓存,必须在所有服务器上逐个发出zmprov flushCache 时间 (或使用zmprov flushCache -a)。

例如:

```
zmprov -s server2 flushCache 配置 zmprov -s server3  
flushCache 配置
```

重击

3. 确定操作是否需要重新启动

```
zmprov desc -a <属性名称>
```

重击

如果需要重新启动,则将 requireRestart值添加到输出中。

Zimbra 邮件传输代理

Zimbra MTA (邮件传输代理)通过 SMTP 接收邮件，并使用本地邮件传输路由每封邮件协议 (LMTP)到适当的 Zimbra 邮箱服务器。

您可以使用管理控制台和 CLI 设置 MTA 参数。但是，
建议您使用 CLI 进行 MTA 配置以确保最佳效果。

Zimbra MTA 服务器包括以下程序：

MTA 服务器程序	目的/描述
Postfix MTA	邮件路由、邮件中继和附件阻止
蛤抗病毒	扫描电子邮件和电子邮件附件中的病毒
垃圾邮件杀手	识别未经请求的商业电子邮件（垃圾邮件）
Amavisd-新	Postfix 与 ClamAV / SpamAssassin 之间的接口
Zimbra 军事服务器	强制限制哪些地址可以发送到分发列表并添加 从分发列表发送的消息的Reply-To和X-Zimbra-DL标头
Zimbra 策略服务器	帮助保护别名域免受反向散射垃圾邮件的侵害
线索使者	策略守护进程/cbpolicyd 用于强制执行操作,例如速率限制。有关详细信息 信息,请参阅 https://wiki.zimbra.com/wiki/Postfix_Policyd
开放金	如果已配置为对发送的电子邮件进行签名,则签名。有关更多信息,请参阅 https://wiki.zimbra.com/wiki/Configuring_for_DKIM_Signing

在 Zimbra Collaboration 配置中,邮件传输和投递是不同的功能:Postfix 充当 MTA,
Zimbra 邮件服务器充当邮件传递代理 (MDA)。

MTA 配置存储在 LDAP 中,zmconfigd进程每两分钟轮询一次 LDAP 目录,以检查
修改并更新 Postfix 配置文件。

传入邮件路由概述

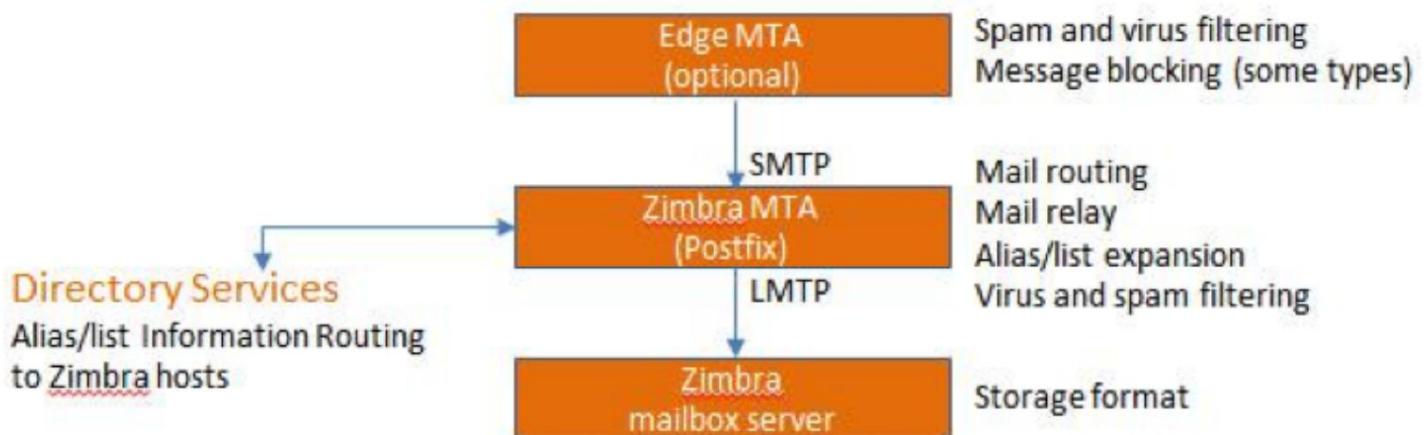
Zimbra 邮箱服务器从 Zimbra MTA 服务器接收邮件,并将其传递给任何过滤器
已创建的。

MTA 服务器通过 SMTP 接收邮件,并使用以下方式将每封邮件路由到相应的邮箱服务器：
LMTP。每封邮件到达时,其内容都会被索引,以便可以搜索所有元素。

Zimbra MTA 部署

Zimbra 包含 Postfix 的预编译版本,用于路由和中继邮件以及管理附件。Postfix 接收
通过 SMTP 接收入站邮件,执行防病毒和反垃圾邮件过滤,并将邮件消息转交给
通过 LMTP 的 Zimbra 协作服务器。

Postfix 还在传输出站消息方面发挥着作用。Zimbra Classic Web App 编写的消息由 Zimbra 服务器通过 Postfix 发送,包括发送给同一服务器上其他用户的消息。



Edge MTA 可以是任何邮件边缘安全解决方案。您可能已经部署了此类解决方案以实现过滤等功能。边缘 MTA 和 Zimbra MTA 之间的某些过滤功能可能会重复。

Postfix 配置文件

Zimbra 修改了 Postfix 文件 (main.cf 和 master.cf) ,以便专门与 Zimbra 配合使用：

- main.cf 已修改以包含 LDAP 表。Zimbra MTA 中的 zmconfigd 从 Zimbra LDAP 中提取数据并修改 Postfix 配置文件。
- master.cf 修改为使用 Amavisd-New。

每次升级后,对 postfix 配置文件所做的更改都会被覆盖,因此应做好记录。如果可能,请尝试使用 Zimbra 定义的参数来实现任何必要的配置更改。

SMTP 身份验证

SMTP 身份验证允许外部网络的授权邮件客户端通过 Zimbra MTA 中继邮件。SMTP 客户端发送邮件时,用户 ID 和密码会发送到 MTA,以便 MTA 可以验证用户是否被允许中继邮件。

当 SMTP 客户端发送邮件时,用户 ID 和密码会发送给 MTA。这确保 MTA 可以通过检查与 LDAP 帐户关联的凭据来验证用户是否有权中继邮件。

用户身份验证通过 Zimbra LDAP 目录服务器提供,或者如果实施,则通过 Microsoft Active Directory Sever 提供。

SMTP 限制

您可以启用限制,这样当传入 SMTP 客户端表现出非标准或其他不被认可的行为时,Postfix 就不会接受邮件。这些限制提供了一些针对垃圾邮件发件人的保护。默认情况下,不使用完全合格域名进行问候的客户端会受到限制。还提供基于 DNS 的限制。

在实施这些限制之前,请先了解其含义。您可能不得不在这些检查上做出妥协,以适应系统之外那些邮件系统实施不佳的人。

将非本地邮件发送到不同的服务器

您可以配置 Postfix 将非本地邮件发送到不同的 SMTP 服务器,通常称为中继或智能主机。

中继主机的一个常见用例是当 ISP 要求您的所有电子邮件通过指定主机中继时,或者当您有过滤 SMTP 代理服务器时。

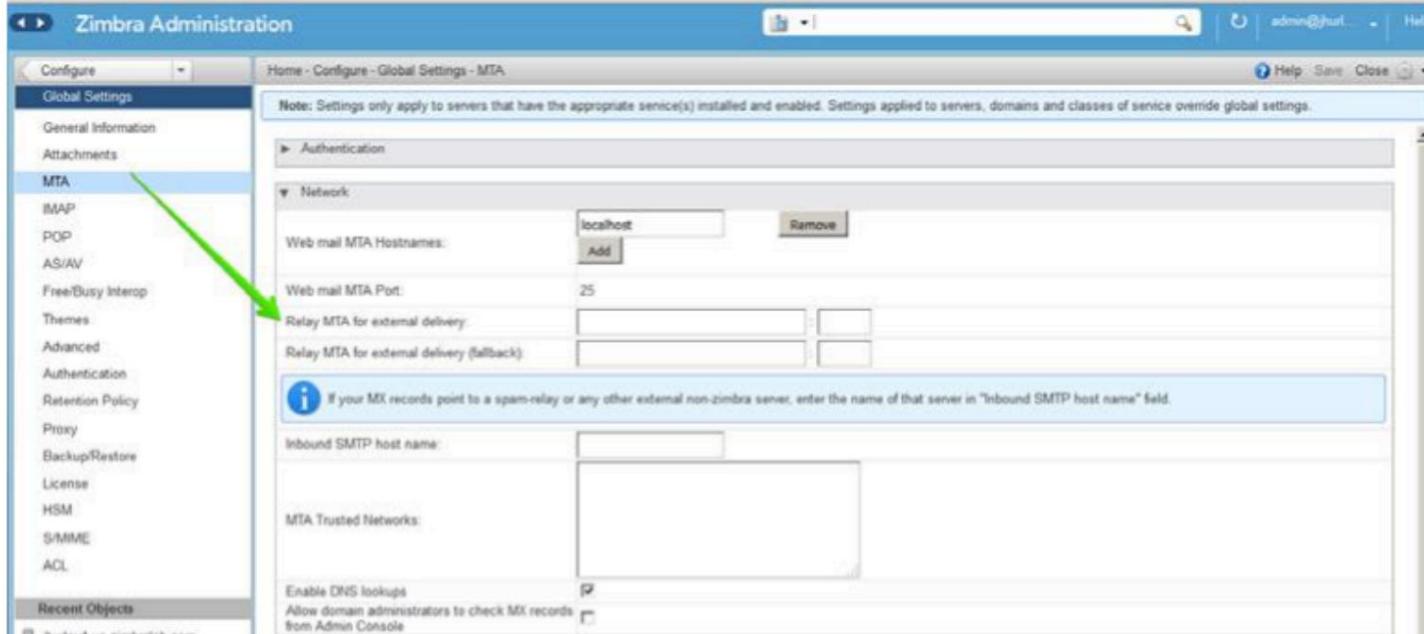
中继主机设置不能与 Web 邮件 MTA 设置混淆。中继主机是 Postfix 将非本地电子邮件中继到的 MTA。Zimbra 服务器使用 Webmail MTA 来撰写邮件,并且必须是 Zimbra MTA 包中 Postfix 服务器的位置。

要使用管理控制台配置中继 MTA 以进行外部传送:

管理控制台:

主页→配置→全局设置→MTA→网络

为防止邮件循环,请小心设置中继主机。



防病毒和反垃圾邮件保护

Amavisd-New 实用程序是 Zimbra MTA 与 Clam Anti-Virus (ClamAV) 和 SpamAssassin 扫描程序之间的接口。

防病毒保护

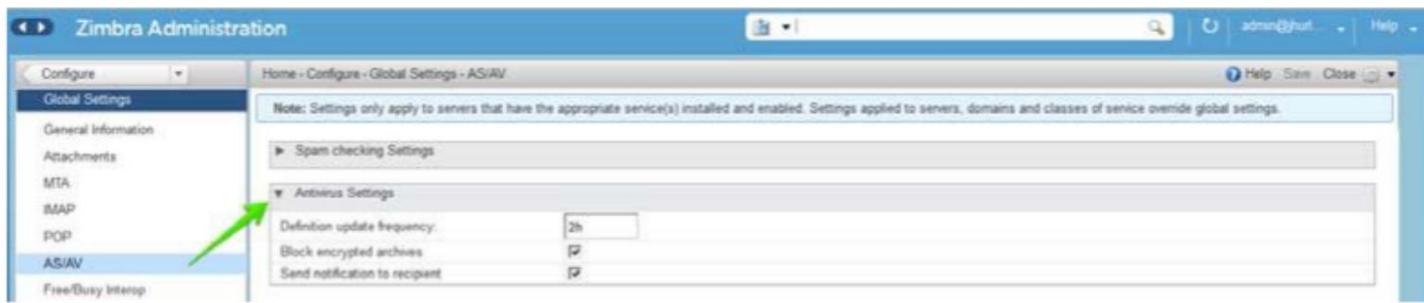
ClamAV 软件是为每个 Zimbra 服务器启用的病毒防护引擎。

防病毒软件配置为将已识别为带有病毒的邮件放入病毒隔离邮箱。默认情况下,Zimbra MTA 每两小时检查一次是否有来自 ClamAV 的新防病毒更新。

您可以在管理控制台更改防病毒设置。

管理控制台：

主页→配置→全局设置→AS/AV→防病毒设置



通过 HTTP 从 ClamAV 网站获取更新。

扫描外发邮件中的附件

您可以启用对使用 Zimbra Classic Web App 发送的外发电子邮件中的附件的实时扫描。如果启用，则在将附件添加到电子邮件时，将在发送邮件之前使用 ClamAV 对其进行扫描。如果 ClamAV 检测到病毒，它将阻止将文件附加到邮件。默认情况下，扫描配置为单节点安装。

要启用扫描，请使用单个节点：

```
zmprov mcf zimbraAttachmentsScanURL clam://localhost:3310/ zmprov mcf  
zimbraAttachmentsScanEnabled TRUE
```

重击

要在多节点环境中启用扫描：

1. 指定 MTA 节点来处理 ClamAV 扫描。
2. 启用，如下：

```
zmprov ms <mta_服务器> zimbraClamAVBindAddress <mta_服务器> zmprov mcf  
zimbraAttachmentsScanURL clam://<mta_服务器>:3310/ zmprov mcf zimbraAttachmentsScanEnabled  
TRUE
```

重击

反垃圾邮件保护

Zimbra 使用 SpamAssassin 识别未经请求的商业电子邮件（垃圾邮件），并将学习到的数据存储在 Berkeley DB 数据库或 MariaDB 数据库中。您还可以使用 Postscreen 功能提供额外的保护，防止邮件服务器过载。以下主题介绍了这两种策略：

- 垃圾邮件杀手避免垃圾邮件的方法
- 避免垃圾邮件的后期筛选方法

垃圾邮件杀手避免垃圾邮件的方法

以下主题提供了使用指南：

- 管理垃圾邮件杀手分数
- 训练垃圾邮件过滤器

- 配置垃圾邮件的最终目的地
- 设置可信网络
- 启用军事服务器

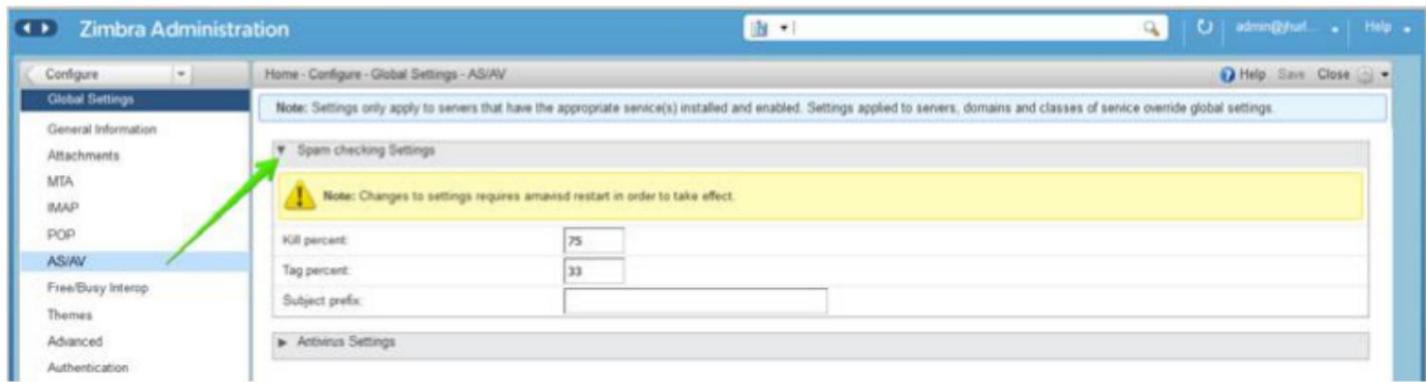
有关如何自定义 SpamAssassin 的信息,请参阅 https://wiki.zimbra.com/wiki/Anti-spam_strategies。

管理垃圾邮件刺客分数:垃圾邮件刺客使用预定义规则以及贝叶斯数据库对具有数值范围的邮件进行评分。Zimbra 使用百分比值来确定“垃圾邮件”,基于垃圾邮件刺客分数 20 为 100%。任何标记在 33%-75% 之间的邮件都被视为垃圾邮件,并被发送到用户的垃圾邮件文件夹。标记在 75% 以上的邮件始终被视为垃圾邮件并被丢弃。

您可以在管理控制台更改垃圾邮件百分比设置和主题前缀。

管理控制台:

主页→配置→全局设置→AS/AV→垃圾邮件检查设置



默认情况下,Zimbra 使用 Berkeley DB 数据库进行垃圾邮件训练。您也可以使用 MariaDB 数据库。

要在 MTA 服务器上使用 MariaDB 方法:

```
zmlocalconfig -e antispam_mysql_enabled=TRUE
```

重击

启用此功能后,Berkeley DB 数据库将不会启用。

训练垃圾邮件过滤器 反垃圾邮件过滤器的有效性取决于用户输入以区分垃圾邮件或正常邮件。SpamAssassin 过滤器会从用户明确标记为垃圾邮件 (发送至垃圾邮件文件夹) 或非垃圾邮件 (从垃圾邮件文件夹删除) 的邮件中学习。这些标记邮件的副本会发送到相应的垃圾邮件训练邮箱。

在安装时,仅在第一个 MTA 上配置垃圾邮件/非垃圾邮件清理过滤器。Zimbra 垃圾邮件培训工具

兹姆特兰萨 ,配置为自动检索这些邮件并训练垃圾邮件过滤器。zmtrainsa脚本

每天清空这些邮箱。

新安装的 Zimbra 将垃圾邮件/非垃圾邮件训练限制在安装的第一个 MTA 上。如果您卸载或移动此 MTA，则需要在另一个 MTA 上启用垃圾邮件/非垃圾邮件训练，因为一台主机应该启用此功能才能运行 `zmtrainsa --cleanup`。

要在新的 MTA 服务器上进行此项设置：

```
zmlocalconfig -e zmtrainsa_cleanup_host=TRUE
```

重击

最初，您可能希望手动训练垃圾邮件过滤器，以快速构建垃圾邮件和非垃圾邮件标记、单词或短字符序列的数据库，这些标记、单词或短字符序列通常出现在垃圾邮件或正常邮件中。为此，您可以手动将邮件作为 message/rfc822 附件转发到垃圾邮件和非垃圾邮件邮箱。当 `zmtrainsa` 运行时，这些邮件用于训练垃圾邮件过滤器。请确保添加足够多的邮件样本以获得准确的分数。要确定是否将邮件标记为垃圾邮件，必须识别至少 200 个已知垃圾邮件和 200 个已知正常邮件。

SpamAssassin 的 `sa-update` 工具包含在 SpamAssassin 中。此工具可从 SA 组织更新 SpamAssassin 规则。该工具安装在 `/opt/zimbra/common/bin` 中。

配置垃圾邮件的最终目的地 - 您可以使用以下属性配置 Amavis 行为来处理垃圾邮件项目的最终目的地：

`zimbraAmavisFinalSpamDestiny`

默认值为 `D_DISCARD`（不会将电子邮件发送给收件人）。

设置最终垃圾邮件目的地属性：

```
zmprov mcf "zimbraAmavisFinalSpamDestiny" D_PASS zmprov ms  
serverhostname.com D_PASS
```

重击

表可配置的属性值9.

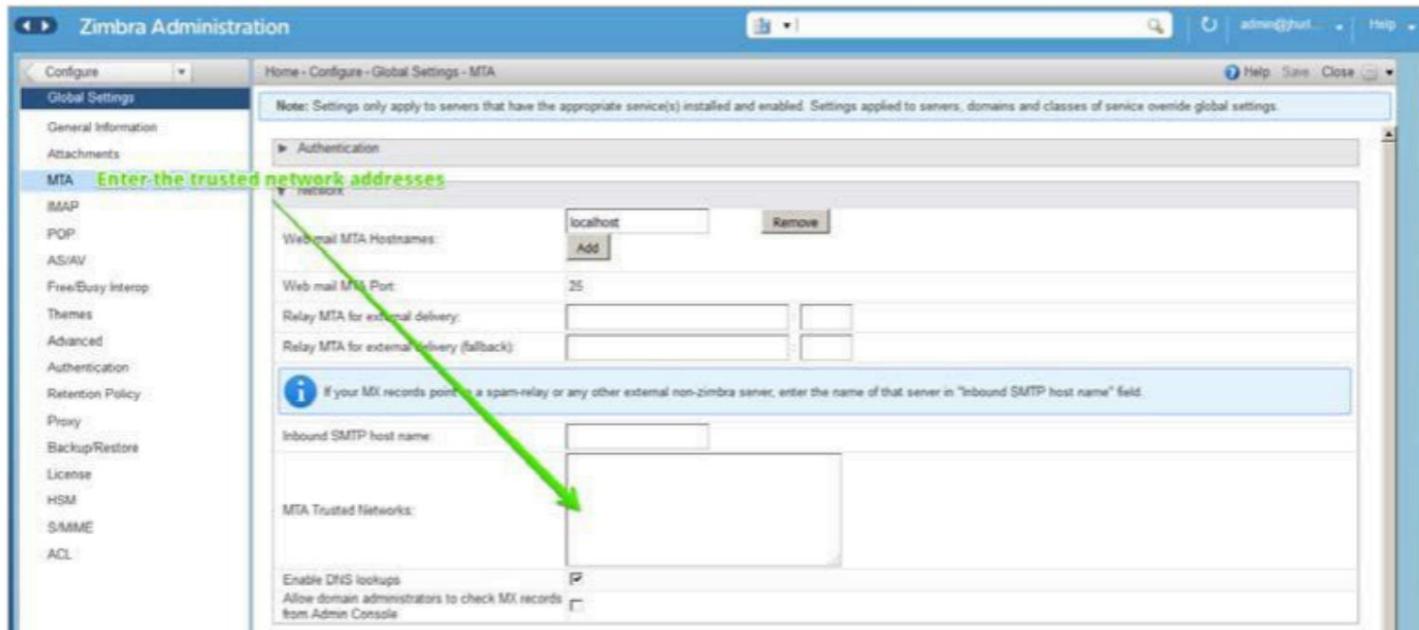
价值	描述
传递	将电子邮件发送给收件人。该电子邮件可能会被放入收件人的垃圾邮件文件夹中（尽管有些网站会禁用垃圾邮件）。
反弹	电子邮件被退回给发件人。由于此设置可能造成反向散射 因为“发件人”不是实际发送电子邮件的人 因此不建议这样做。
拒绝	拒绝电子邮件。此设置可降低反向散射的可能性： <ul style="list-style-type: none"> • 如果发件人有效，MTA 将通知此人有关拒绝的信息。 • 如果发件人无效，则关联的 MTA 将丢弃该电子邮件（即由垃圾邮件发送者冒充他人发送的电子邮件）。
丢弃	该电子邮件被默默丢弃（未送达）。

设置可信网络：Zimbra 配置仅允许在本地网络进行中继,但您可以
配置允许中继邮件的受信任网络。您可以将 MTA 受信任网络设置为全局设置,但
您可以将受信任网络配置为服务器设置。服务器设置将覆盖全局设置。

要使用管理控制台将 MTA 信任网络设置为全局设置：

管理控制台：

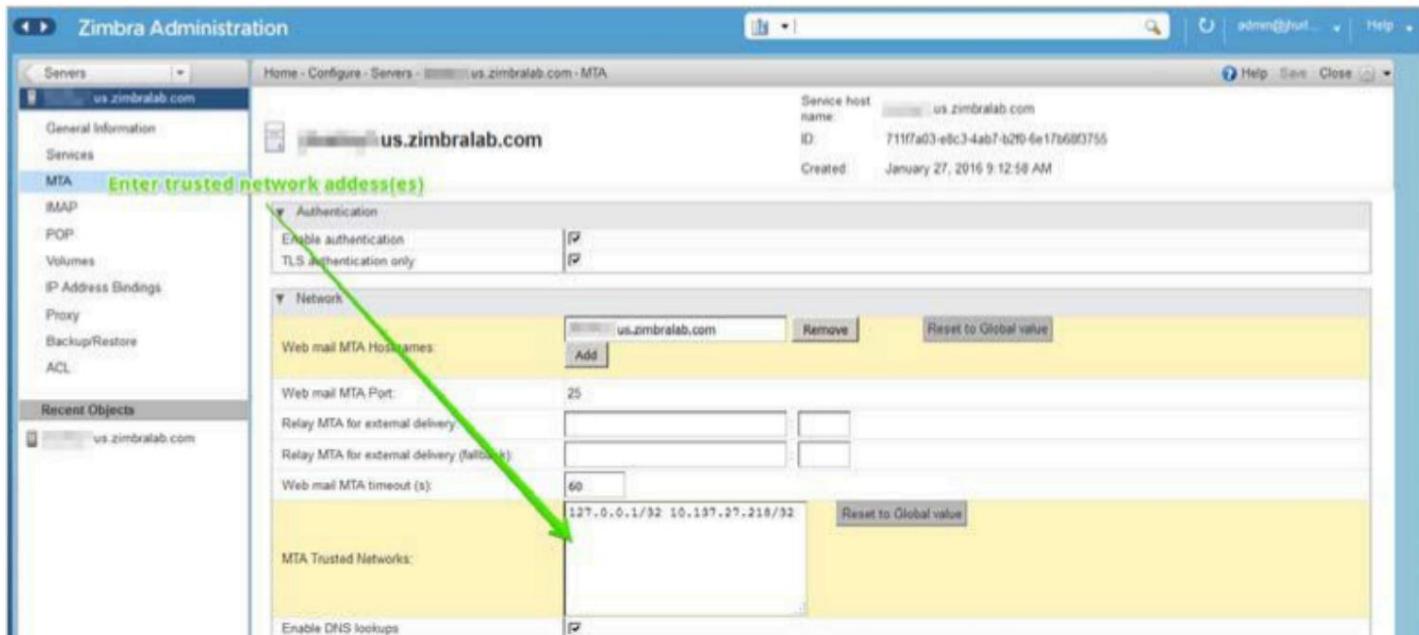
主页→配置→全局设置→MTA→网络



使用管理控制台为每个服务器设置 MTA 信任网络时,首先确保 MTA
可信网络已被设为全局设置。

管理控制台：

主页→配置→服务器→
服务器 → MTA → 网络



输入以空格分隔的网络地址,类似以下示例： 逗号 和/或 空间 . 继续长行,用以下方式开始下一行

```
127.0.0.0/8, 168.100.189.0/24 127.0.0.0/8
168.100.189.0/24 10.0.0.0/8 [::1]/128 [fe80::%eth0]/64
```

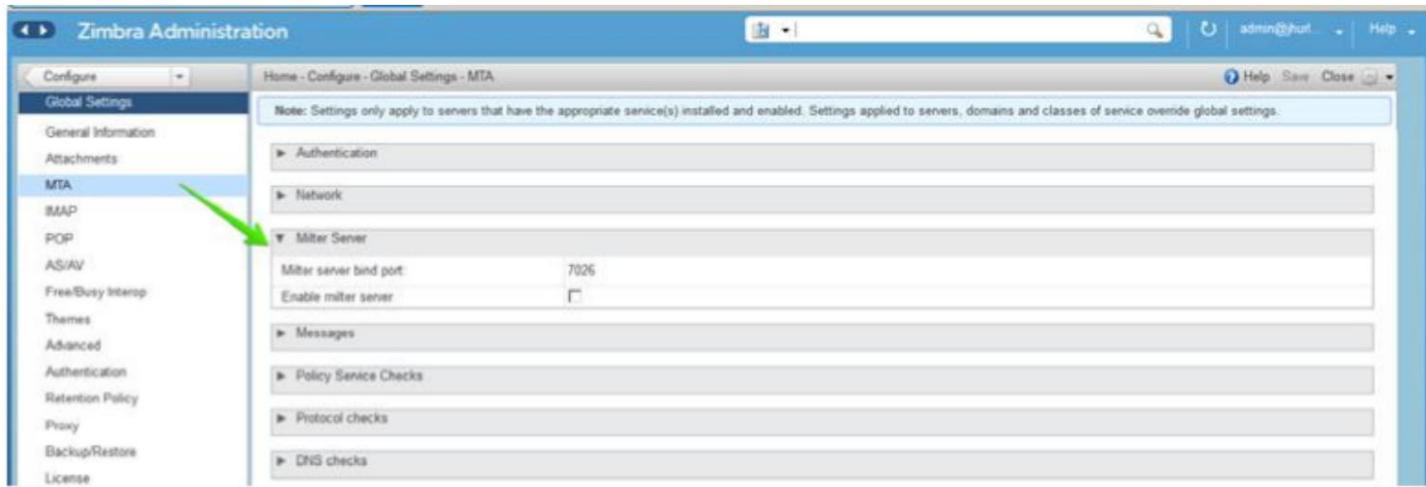
启用 Milter 服务器:可以启用 Milter 服务器来强制限制哪些地址可以发送到分发列表,并向分发列表发送的消息添加Reply-To和X-Zimbra-DL标头。可以从管理控制台全局启用此功能,也可以针对特定服务器启用此功能。

仅在运行 MTA 的服务器上启用 Milter 服务器。

对于全局配置,从管理控制台启用 milter 服务器:

管理控制台:

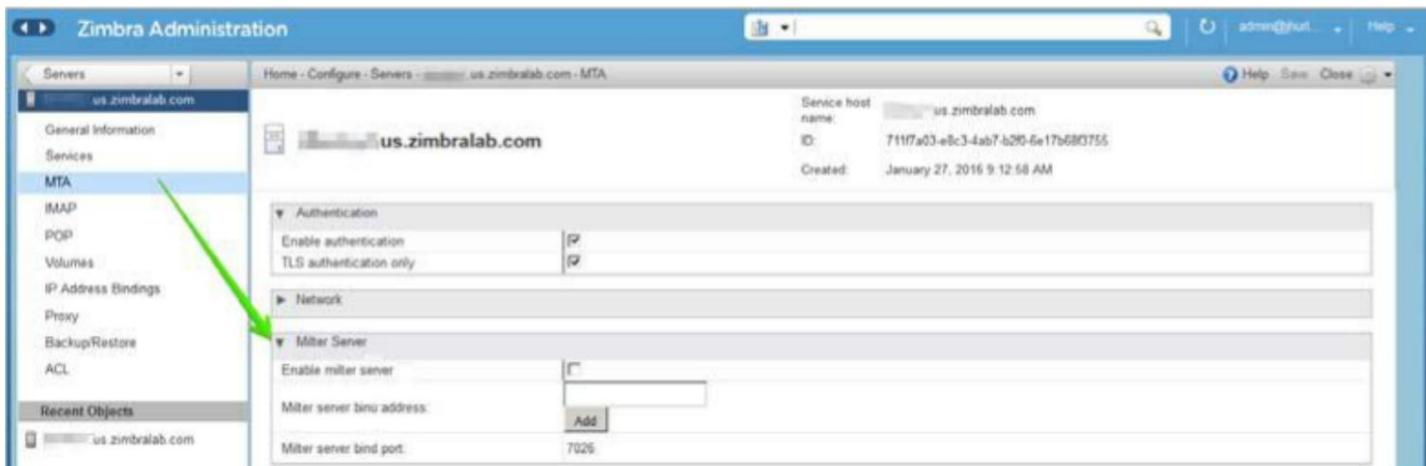
主页→配置→全局设置→ MTA → Milter 服务器



使用管理控制台启用特定的邮件服务器,并为各个服务器设置绑定寻址。

管理控制台:

主页→配置→服务器→ 服务器 → MTA → 军事服务器



避免垃圾邮件的后期筛选方法

Zimbra Postscreen 是 Zimbra Collaboration 反垃圾邮件策略的 8.7 增强版,可提供额外的保护以防止邮件服务器过载。根据设计,Postscreen 不是 SMTP 代理。其目的是使垃圾邮件机器人远离 Postfix SMTP 服务器进程,同时最大限度地减少合法流量的开销。单个

Postscreen 进程处理多个入站 SMTP 连接，并决定哪些客户端可以与 Postfix SMTP 服务器进程通信。通过阻止垃圾邮件机器人，Postscreen 释放了 SMTP 服务器进程以供合法客户端使用，并延迟了服务器过载情况的发生。

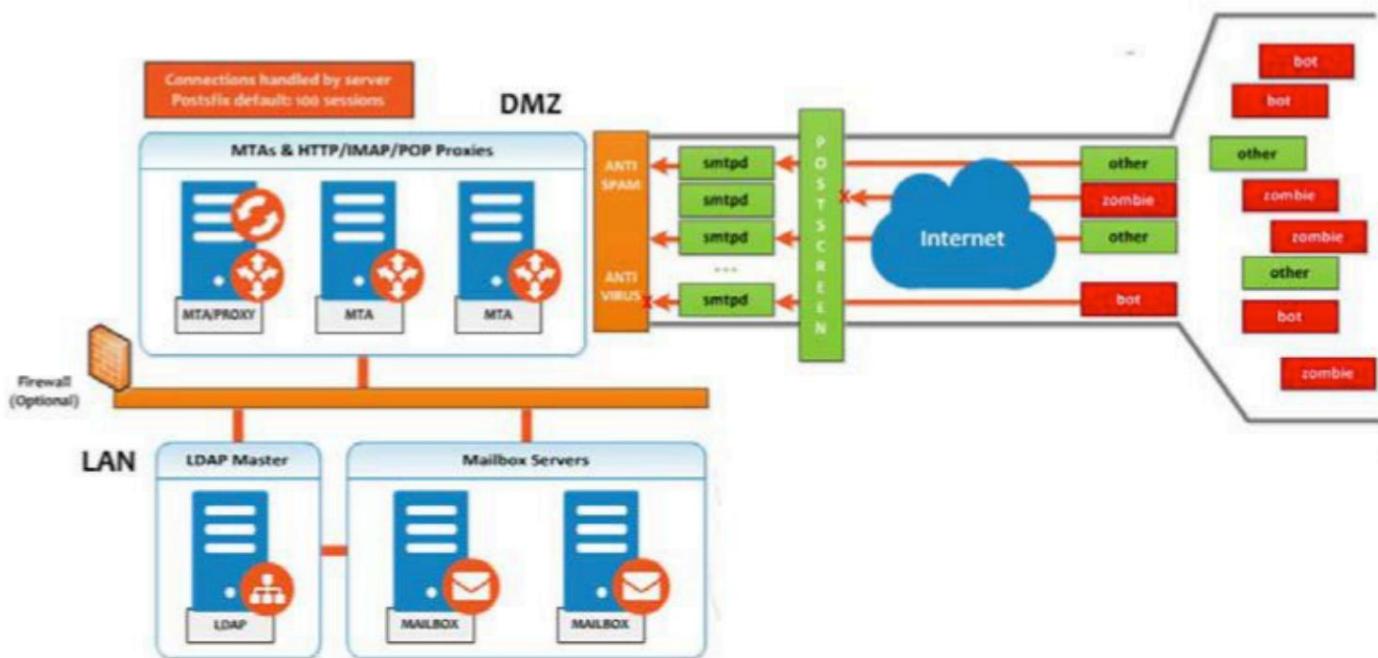
在典型的部署中，Postscreen 在 TCP 端口 25 上处理 MX 服务，而 MUA 客户端通过 TCP 端口 587 上的提交服务提交邮件，这需要客户端身份验证。或者，网站可以设置专用的非 Postscreen “端口 25”服务器，该服务器提供提交服务和客户端身份验证，而无需 MX 服务。

不应在从最终用户客户端 (MUA) 接收邮件的 SMTP 端口上使用 Postscreen。

Zimbra Collaboration Postscreen 为通过了多项测试的客户端维护一个临时白名单。

当 SMTP 客户端 IP 地址被列入白名单时，Postscreen 会立即将连接传递给 Postfix SMTP 服务器进程。这最大限度地减少了合法邮件的开销。

在使用 Postscreen 服务的典型场景中，可以合理地预期潜在的恶意电子邮件实体（例如机器人和僵尸）会与电子邮件负载中的友好候选实体混合在一起。下图说明了这一概念，其中不良实体以红色表示；良好电子邮件候选实体以绿色表示。



Postscreen 执行基本检查并拒绝明显来自机器人或僵尸的连接。如果连接不在临时白名单中，Postscreen 会将电子邮件传递给本地反垃圾邮件和反病毒引擎，后者可以接受或拒绝它。良好的连接通过 Postscreen 安全接受，然后允许直接与 SMTP 守护程序通信，后者使用 AS/AV 扫描电子邮件（照常）。默认情况下，所有机器人或僵尸都被拒绝。

使用 Zimbra CLI 属性设置 Postscreen 操作的参数。对于提供忽略、强制或删除指令的任何 Postscreen 属性，请使用以下指南：

- 忽略 忽略此结果。允许其他测试完成。对后续客户端连接重复此测试。
这是默认设置，对于在不阻止邮件的情况下进行测试和收集统计信息很有用。
- 执行 允许其他测试完成。拒绝使用 550 SMTP 回复发送邮件的尝试，并记录
你好/发送者/接收者信息。对后续客户端连接重复此测试。

- 降低 立即断开连接并回复 521 SMTP。对后续客户端重复此测试连接。

后期筛选属性：

转到zmprov mcf提示符（版本 8.7+）以使用 Postscreen 命令。您可以在启用 Postscreen 中查看这些属性的示例用法。

- zimbraMtaPostscreenAccessList 默认 = permit_my networks

Postconf postscreen_access_list设置,这是远程 SMTP 客户端 IP 地址的永久白名单/黑名单。Postscreen(8) 在远程 SMTP 客户端连接后立即搜索此列表。指定逗号或空格分隔的命令列表（大写或小写）或查找表。搜索在针对客户端 IP 地址触发的第一个命令时停止。

- zimbraMtaPostscreenBareNewlineAction 默认 = 忽略

当远程 SMTP 客户端发送裸换行符（即,换行符前面没有回车符）时,postscreen(8) 要采取的操作是忽略、强制或删除。

- zimbraMtaPostscreenBareNewlineEnable 默认 = 否

在 postscreen(8) 服务器中启用（是）或禁用（否）“裸换行符”SMTP 协议测试。这些测试非常昂贵：远程 SMTP 客户端在通过测试后必须断开连接,然后才能与真正的 Postfix SMTP 通信服务器。

- zimbraMtaPostscreenBareNewlineTTL 默认 = 30d

postscreen(8) 使用成功的“裸换行符”SMTP 协议测试结果的允许时间量。在此期间,客户端 IP 地址被排除在此测试之外。默认设置很长,因为远程 SMTP 客户端在通过测试后必须断开连接,然后才能与真正的 Postfix SMTP 服务器通信。

指定非零时间值（一个整数值加上一个可选的指定时间单位的单字母后缀）。

时间单位:s（秒）、m（分钟）、h（小时）、d（天）、w（星期）。

- zimbraMtaPostscreenBlacklistAction 默认 = 忽略

当远程 SMTP 客户端被postscreen_access_list参数永久列入黑名单时,postscreen(8) 要采取的操作是忽略、强制执行或删除。

- zimbraMtaPostscreenCacheCleanupInterval 默认值 = 12h

postscreen(8) 缓存清理运行间隔允许的时间。缓存清理会增加缓存数据库的负载,因此不应频繁运行。此功能要求缓存数据库支持“删除”和“序列”运算符。指定零间隔可禁用缓存清理。

每次缓存清理运行后,postscreen(8) 守护进程都会记录保留和删除的条目数。如果守护进程在postfix 重新加载后提前终止,或者在\$max_idle 秒内没有请求,则清理运行将记录为“部分”。

后缀停止 ,

时间单位:s（秒）、m（分钟）、h（小时）、d（天）、w（星期）。

- zimbraMtaPostscreenCacheRetentionTime 默认值 = 7d

postscreen(8) 在删除过期的临时白名单条目之前允许缓存该条目的时间。这可以防止客户端仅因为其缓存条目在一小时前过期而被记录为“NEW”。

它还可以防止缓存被那些曾经通过深度协议测试并且不再回来的客户端填满。

时间单位:s（秒）、m（分钟）、h（小时）、d（天）、w（星期）。

- zimbraMtaPostscreenCommandCountLimit 默认值 = 20

用于设置 postscreen(8) 内置 SMTP 协议引擎的每个 SMTP 会话的总命令数限制的值。此 SMTP 引擎会推迟或拒绝所有邮件投递尝试，因此无需对垃圾命令和错误命令的数量实施单独的限制。zimbraMtaPostscreenDnsblAction 默认值 = ignore

-

当远程 SMTP 客户端的组合 DNSBL 分数等于或大于阈值（由postscren_dnsbl_sites和postscren_dnsbl_threshold参数定义）时，postscren(8) 要采取的操作是忽略、强制执行或删除。

- zimbraMtaPostscreenDnsblSites

DNS 白名单/黑名单域、过滤器和权重因子的可选列表。当列表非空时，dnsblog(8) 守护进程将使用远程 SMTP 客户端的 IP 地址查询这些域，并且 postscren(8) 将使用每个非错误回复更新 SMTP 客户端的 DNSBL 分数。

当 postscren 拒绝邮件时，它会使用 DNSBL 域名进行回复。使用postscren_dnsbl_reply_map 功能隐藏 DNSBL 域中的“密码”信息名字。

当客户端的分数等于或大于postscren_dnsbl_threshold指定的阈值时，postscren(8) 可以断开与远程 SMTP 客户端的连接。

指定domain=filter*weight条目列表，以逗号或空格分隔。

- 如果未指定=filter，postscren(8) 将使用任何非错误 DNSBL 回复。否则，postscren(8) 仅使用与过滤器匹配的 DNSBL 回复。过滤器的形式为[]内的dddd模式，其中包含一个或多个以“；”分隔的数字或数字..数字范围。其中每个 d 是一个数字，或一个
- 当未指定*weight时，postscren(8) 会将远程 SMTP 客户端的 DNSBL 分数增加 1。否则，权重必须为整数，postscren(8) 会将指定的权重添加到远程 SMTP 客户端的 DNSBL 分数中。指定负数以加入白名单。
- 当一个postscren_dnsbl_sites条目产生多个 DNSBL 响应时，postscren(8) 最多应用一次权重。

例子：

要使用 example.com 作为高信任度阻止列表，并且仅当两者都同意时才阻止来自 example.net 和 example.org 的邮件：

```
postscren_dnsbl_threshold = 2
postscren_dnsbl_sites = example.com*2, example.net, example.org
```

要仅过滤包含 127.0.0.4 的 DNSBL 回复：

```
postscren_dnsbl_sites = example.com=127.0.0.4
```

- zimbraMtaPostscreenDnsblThreshold 默认值 = 1

根据使用postscren_dnsbl_sites参数定义的组合 DNSBL 分数，定义阻止远程 SMTP 客户端的包含下限的值。

- zimbraMtaPostscreenDnsblTTL 默认 = 1h

在客户端 IP 地址需要再次通过该测试之前，postscren(8) 使用成功的基于 DNS 的信誉测试的结果所允许的时间量。

指定非零时间值（一个整数值加上一个可选的指定时间单位的单字母后缀）。

时间单位:s (秒)、m (分钟)、h (小时)、d (天)、w (星期)。

- zimbraMtaPostscreenDnsblWhitelistThreshold 默认值 = 0

允许远程 SMTP 客户端根据使用postscreen_dnsbl_sites参数定义的组合 DNSBL 分数跳过“之前”和“220 问候之后”协议测试。

指定负值以启用此功能。当客户端通过postscreen_dnsbl_whitelist_threshold且没有失

败其他测试时,所有待处理或禁用的测试都将标记为已完成,其生存时间值等于postscreen_dnsbl_ttl。当测试已完成时,如果其生存时间值小于postscreen_dnsbl_ttl,则会更新其生存时间值。

- zimbraMtaPostscreenGreetAction 默认 = 忽略

当远程 SMTP 客户端在postscreen_greet_wait参数指定的时间内轮到自己发言之前发言时,postscreen(8) 要采取的操作是忽略、强制或删除。

- zimbraMtaPostscreenGreetTTL 默认值 = 1d

允许 postscreen(8) 使用成功 PREGREET 测试结果的时间量。在此期间,客户端 IP 地址被排除在此测试之外。默认值相对较短,因为良好的客户端可以立即与真正的 Postfix SMTP 服务器通信。

指定非零时间值（一个整数值加上一个可选的指定时间单位的单字母后缀）。

时间单位:s (秒)、m (分钟)、h (小时)、d (天)、w (星期)。

- zimbraMtaPostscreenNonSmtpCommandAction 默认值 = 删除

当远程 SMTP 客户端发送非 SMTP 命令时,postscreen(8) 会采取以下操作:按照postscreen_forbidden_commands 参数的指定,忽略、强制或删除。

- zimbraMtaPostscreenNonSmtpCommandEnable 默认 = 否

在 postscreen(8) 服务器中启用(是)或禁用(否)“非 SMTP 命令”测试。这些测试非常昂贵:客户端在通过测试后必须断开连接,然后才能与真正的 Postfix SMTP 服务器通信。

- zimbraMtaPostscreenNonSmtpCommandTTL 默认 = 30d

postscreen(8) 使用成功“non_smtp_command”结果所允许的时间

SMTP 协议测试。在此期间,客户端 IP 地址不包括在此测试中。默认值为长,因为客户端在通过测试后必须断开连接,然后才能与真正的 Postfix SMTP 服务器通信。

指定非零时间值（一个整数值加上一个可选的指定时间单位的单字母后缀）。

时间单位:s (秒)、m (分钟)、h (小时)、d (天)、w (星期)。

- zimbraMtaPostscreenPipeliningAction 默认 = 强制

当远程 SMTP 客户端发送多个命令而不是发送一个命令并等待服务器响应时,postscreen(8) 要采取的操作是忽略、强制或删除。

- zimbraMtaPostscreenPipeliningEnable 默认 = 否

在 postscreen(8) 服务器中启用(yes)或禁用(no)“流水线”SMTP 协议测试。这些测试非常昂贵:好的客户端在通过测试后必须断开连接,然后才能与真正的 Postfix SMTP 服务器通信。

- zimbraMtaPostscreenPipeliningTTL 默认 = 30d

postscreen(8) 使用成功的“流水线”SMTP 协议测试结果的允许时间。在此期间,客户端 IP 地址被排除在此测试之外。默认值很长,因为良好的客户端在通过测试后必须断开连接,然后才能与真正的 Postfix SMTP 服务器通信。

指定非零时间值（一个整数值加上一个可选的指定时间单位的单字母后缀）。

时间单位:s (秒)、m (分钟)、h (小时)、d (天)、w (星期)。

- zimbraMtaPostscreenWatchdogTimeout 默认值 = 10s

在被内置看门狗定时器终止之前,postscreen(8) 进程响应远程 SMTP 客户端命令或执行缓存操作的允许时间。这是一种安全机制,可防止 postscreen(8) 因 Postfix 本身或系统软件中的错误而变得无响应。为了避免误报和不必要的缓存损坏,此限制不能设置为低于 10 秒。

指定非零时间值（一个整数值加上一个可选的指定时间单位的单字母后缀）。

时间单位:s (秒)、m (分钟)、h (小时)、d (天)、w (星期)。

- zimbraMtaPostscreen白名单接口

本地 postscreen(8) 服务器 IP 地址列表,非白名单远程 SMTP 客户端可从中获取 postscreen(8) 的临时白名单状态。客户端必须先获取此状态,然后才能与 Postfix SMTP 服务器进程通信。默认情况下,客户端可以在任何本地 postscreen(8) 服务器 IP 地址上获取 postscreen(8) 的白名单状态。

当 postscreen(8) 同时监听主 MX 地址和备份 MX 地址时,可以配置postscreen_whitelist_interfaces

参数,以便仅当客户端连接到主 MX 地址时才提供临时白名单状态。一旦客户端被列入白名单,它就可以与任何地址上的 Postfix SMTP 服务器通信。因此,仅连接到备份 MX 地址的客户端永远不会被列入白名单,也永远不会被允许与 Postfix SMTP 服务器进程通信。

指定网络地址或网络/网络掩码模式的列表,以逗号和/或空格分隔。网络掩码指定主机地址的网络部分的位数。通过在下一行开头使用空格来继续较长的行。

您还可以指定/file/name或type :table模式。/file/name模式由其内容替换;当表条目与查找字符串匹配时,将匹配type:table查找表（查找结果将被忽略）。

该列表从左到右进行匹配,搜索在第一次匹配时停止。指定!pattern可从列表中排除地址或网络块。

必须在postscreen_whitelist_interfaces值的[]内以及用/file/name指定的文件中指定 IPv6 地址信息。6 个地址包含 ":"字符,否则会与type:table模式混淆。

IP版本

例子:

```
/etc/postfix/main.cf:
```

```
# 不要将与备用 IP 地址的连接列入白名单。postscreen_whitelist_interfaces = !168.100.189.8,
static:all
```

- zimbraMtaPostscreenDnsblMinTTL 默认值 = 60s

允许 postscreen(8) 的最短时间（基于 DNS 的信誉测试成功后得出的结果）,之后客户端 IP 地址必须再次通过该测试。如果 DNS 回复指定了更大的 TTL 值,则将使用该值,除非该值大于postscreen_dnsbl_max_ttl。

指定非零时间值（一个整数值加上一个可选的指定时间单位的单字母后缀）。

时间单位:s (秒)、m (分钟)、h (小时)、d (天)、w (星期)。

- zimbraMtaPostscreenDnsblMaxTTL 默认值 = postscreen dnsbl ttl

`postscreen(8)` 使用成功的基于 DNS 的客户端 IP 地址必须再次通过信誉测试。如果 DNS 回复指定了较短的 TTL 值,除非该值小于 `postscreen_dnsbl_min_ttl`,否则将使用该值。
指定非零时间值 (一个整数值加上一个可选的指定时间单位的单字母后缀)。
时间单位:`s` (秒)、`m` (分钟)、`h` (小时)、`d` (天)、`w` (星期)。

请注意,默认设置与 3.1 之前的 Postscreen 版本向后兼容。

启用 Postscreen:

本节中的示例演示了适合中高级别的后屏幕保护。

[Postscreen 4](#) 全局配置示例

```

zmprov mcf zimbraMtaPostscreenAccessList permit_my networks zmprov mcf
zimbraMtaPostscreenBareNewlineAction 忽略 zmprov mcf
zimbraMtaPostscreenBareNewlineEnable 否 zmprov mcf
zimbraMtaPostscreenBareNewlineTTL 30d zmprov mcf
zimbraMtaPostscreenBlacklistAction 忽略 zmprov mcf
zimbraMtaPostscreenCacheCleanupInterval 12h zmprov mcf
zimbraMtaPostscreenCacheRetentionTime 7d zmprov mcf
zimbraMtaPostscreenCommandCountLimit 20 zmprov mcf
zimbraMtaPostscreenDnsblAction 强制执行 zmprov mcf \
zimbraMtaPostscreenDnsblSites b.barracudacentral.org=127.0.0.2_7 \ zimbraMtaPostscreenDnsblSites
dnsbl.inps.de=127.0.0.2*7 \ zimbraMtaPostscreenDnsblSites zen.spamhaus.org=127.0.0.[10;11]*8 \ zimbraMtaPostscreenDnsblSites zen.spamhaus.org=127.0.0.[4..7]*6 \
zimbraMtaPostscreenDnsblSites zen.spamhaus.org=127.0.0.3*4 \ zimbraMtaPostscreenDnsblSites
zen.spamhaus.org=127.0.0.2*3 \ zimbraMtaPostscreenDnsblSites list.dnswl.org=127.0.[0..255].0*-2 \ zimbraMtaPostscreenDnsblSites list.dnswl.org=127.0.[0..255].1*-3 \
zimbraMtaPostscreenDnsblSites list.dnswl.org=127.0.[0..255].2*-4 \
zimbraMtaPostscreenDnsblSites list.dnswl.org=127.0.[0..255].3*-5 \
zimbraMtaPostscreenDnsblSites bl.mailspike.net=127.0.0.2*5 \
zimbraMtaPostscreenDnsblSites bl.mailspike.net=127.0.0.[10;11;12]*4 \ zimbraMtaPostscreenDnsblSites
wl.mailspike.net=127.0.0.[18;19;20]*2 \ zimbraMtaPostscreenDnsblSites
dnsbl.sorbs.net=127.0.0.10*8 \
zimbraMtaPostscreenDnsblSites dnsbl.sorbs.net=127.0.0.5*6 \
zimbraMtaPostscreenDnsblSites dnsbl.sorbs.net=127.0.0.7*3 \
zimbraMtaPostscreenDnsblSites dnsbl.sorbs.net=127.0.0.8*2 \
zimbraMtaPostscreenDnsblSites dnsbl.sorbs.net=127.0.0.6*2 \
zimbraMtaPostscreenDnsblSites dnsbl.sorbs.net=127.0.0.9*2
zmprov mcf zimbraMtaPostscreenDnsblTTL 5m zmprov mcf
zimbraMtaPostscreenDnsblThreshold 8 zmprov mcf
zimbraMtaPostscreenDnsblTimeout 10s zmprov mcf
zimbraMtaPostscreenDnsblWhitelistThreshold 0 zmprov mcf zimbraMtaPostscreenGreetAction
强制执行 zmprov mcf zimbraMtaPostscreenGreetTTL 1d zmprov mcf
zimbraMtaPostscreenNonSmtpCommandAction 删除 zmprov mcf
zimbraMtaPostscreenNonSmtpCommandEnable 否 zmprov mcf
zimbraMtaPostscreenNonSmtpCommandTTL 30d zmprov mcf
zimbraMtaPostscreenPipeliningAction 强制执行 zmprov mcf
zimbraMtaPostscreenPipeliningEnable 否 zmprov mcf zimbraMtaPostscreenPipeliningTTL
30d zmprov mcf zimbraMtaPostscreenWatchdogTimeout 10s zmprov mcf
zimbraMtaPostscreenWhitelistInterfaces 静态:全部

```

测试后筛选：

测试使用 Postscreen 查看结果而不采取任何操作。在测试场景中，您指示 Postscreen 记录电子邮件连接而不对其采取任何操作。对结果满意后，您可以根据需要设置 Postscreen 值以强制执行或丢弃电子邮件。

1. 设置基于 DNS 的黑洞列表 (DNSBL)。

2. 将 Postscreen 设置为忽略。

以下真实示例演示了测试会话期间 Postscreen 返回 550 错误：

3月1日 02:03:26 edge01 postfix/postscreen[23154]: [112.90.37.251] 的 DNSBL 排名为 28:20438

3月1日 02:03:26 edge01 postfix/postscreen[23154]: 从 [10.210.0.161]:58010 连接到 [10.210.0.174]:25

3月1日 02:03:26 edge01 postfix/postscreen[23154]: 白名单 [10.210.0.161]:58010

3月1日 02:03:27 edge01 postfix/postscreen[23154]: NOQUEUE: 拒绝: 来自 [112.90.37.251] 的 RCPT:20438: 550 5.7.1
服务不可用; 客户端 [112.90.37.251] 被阻止使用 zen.spamhaus.org; 来自 = <hfxdgdsoggvfg@gmail.com>, 至 = <support@zimbra.com>, proto =
ESMTP, helo = <gmail.com>

3月1日 02:03:27 edge01 postfix/postscreen[23154]: 断开连接 [112.90.37.251]:20438

接收和发送邮件

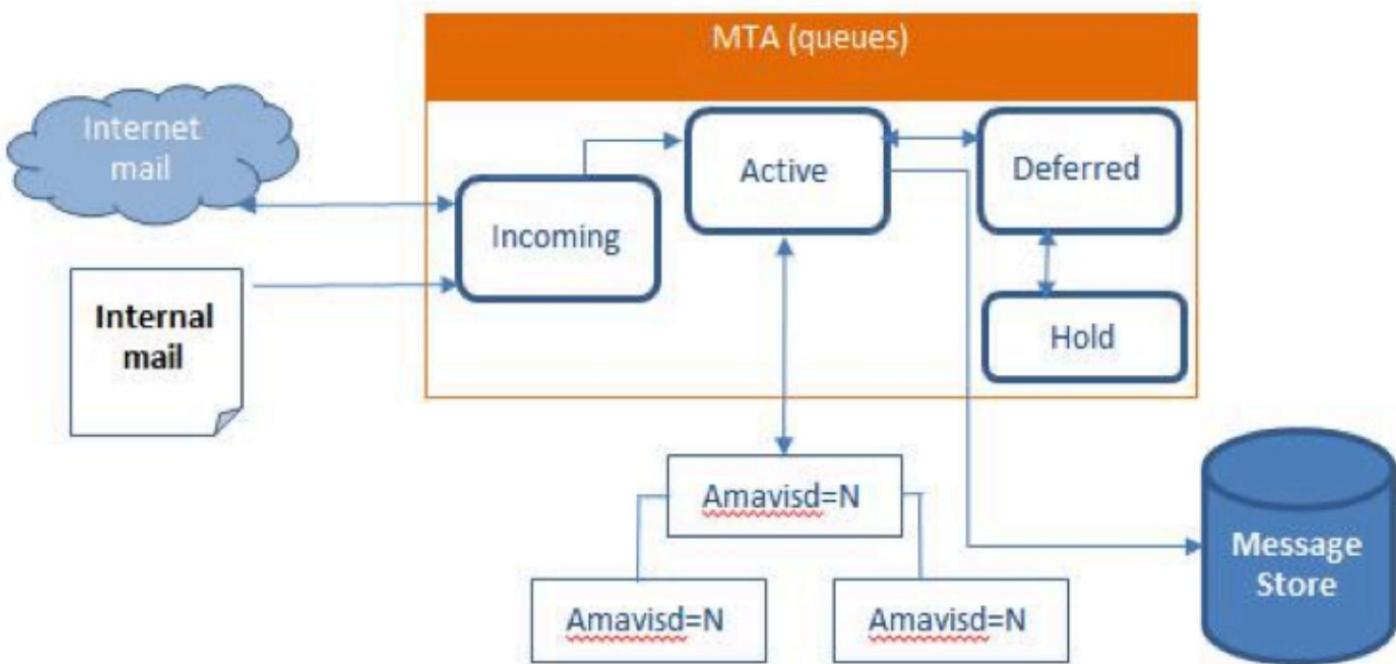
Zimbra MTA 负责传递收件和发件邮件。对于发件邮件,Zimbra MTA 确定收件人地址的目的地。如果目标主机是本地的,则邮件将传递到 Zimbra 服务器进行传递。如果目标主机是远程邮件服务器,则 Zimbra MTA 必须建立通信方法以将邮件传输到远程主机。对于收件邮件,MTA 必须能够接受来自远程邮件服务器的连接请求并接收本地用户的邮件。

要发送和接收电子邮件,必须在 DNS 中为 MTA 配置 A 记录和 MX 记录。要发送邮件,MTA 使用 DNS 来解析主机名和电子邮件路由信息。要接收邮件,必须正确配置 MX 记录以将邮件路由到邮件服务器。

如果您不启用 DNS,则必须配置中继主机。

消息队列

当 Zimbra MTA 收到邮件时,它会通过一系列队列路由邮件以管理传递;传入、活动、延期、保留和损坏。



传入消息队列保存已收到的新邮件。每封邮件都用唯一的文件名标识。当有空间时,邮件将移至活动队列。如果没有问题,邮件会非常快速地通过此队列。

活动邮件队列保存着准备发送的邮件。MTA 设置了活动队列中同时可容纳的邮件数量限制。从这里开始,邮件在被传送到另一个队列之前,会移至防病毒和反垃圾邮件过滤器或从防病毒和反垃圾邮件过滤器移出。

无法投递的邮件将被放入延期队列。投递失败的原因将记录在延期队列的文件中。此队列会频繁扫描以重新发送邮件。如果在设定的投递尝试次数后仍无法发送邮件,则邮件将失败并退回给原始发件人。您可以选择向发件人发送邮件已被延期的通知。

保留邮件队列保留无法处理的邮件。邮件将保留在此队列中,直到管理员将其移动。保留队列中的邮件不会定期尝试投递。

损坏的队列存储了损坏的无法读取的消息。

您可以从管理控制台监控邮件队列的投递问题。请参阅监控 Zimbra 服务器。

来自外部域的邮件的消息横幅

可以为来自外部域的邮件添加邮件中的消息横幅。这将帮助用户识别来自其组织外部的邮件。该功能由 localconfig 属性控制，默认情况下是禁用的。

以下是属性的详细信息：

- zimbra_external_email_warning_enabled - 启用/禁用该功能的属性。
- zimbra_external_email_warning_message - 用于定制邮件中显示的消息的属性。

以下是以 zimbra 用户身份执行的指令：

1. 启用该功能：

```
与 - zimbra
zmlocalconfig -e zimbra_external_email_warning_enabled=true
```

2. 重启邮箱服务：

```
zmmailboxdctl 重启
```

当用户收到来自外部域的邮件时，消息横幅将显示在邮件正文的顶部。

修改消息

外部域的消息也可以修改。

以下是说明：

1. 使用新消息编辑 localconfig 属性 zimbra_external_email_warning_message：

```
zmlocalconfig -e zimbra_external_email_warning_message= 外部域警告已被编辑
```

2. 重启邮箱服务：

```
zmmailboxdctl 重启
```

当用户收到来自外部域的邮件时，编辑的消息横幅将显示在邮件正文的顶部。

Zimbra 代理服务器

Zimbra Proxy 是一个高性能代理服务器,可以配置为 POP3/IMAP/HTTP 代理,用于将 IMAP/POP3 和 HTTP 客户端请求反向代理到一组后端服务器。

Zimbra Proxy 包在 Zimbra Collaboration 安装过程中安装和配置。您可以在邮箱服务器、MTA 服务器或自己的独立服务器上安装此包。安装 Zimbra Proxy 包后,代理功能已启用。在大多数情况下,无需进行任何修改。

使用 Zimbra Proxy 的好处

使用 Zimbra Proxy 的好处包括:

- Zimbra 代理集中访问邮箱服务器
- 负载均衡
- 安全
- 验证
- SSL 终止
- 缓存
- 集中日志记录和审计
- URL 重写
- 严格服务器名称执行 (可选)

有关更多信息,请参阅 wiki 页面[Zimbra_Proxy_Guide](https://wiki.zimbra.com/wiki/Zimbra_Proxy_Guide) (https://wiki.zimbra.com/wiki/Zimbra_Proxy_Guide)。

Zimbra 代理组件

Zimbra Proxy 旨在提供快速、可靠且可扩展的 HTTP/POP/IMAP 代理。Zimbra Proxy 包括以下内容:

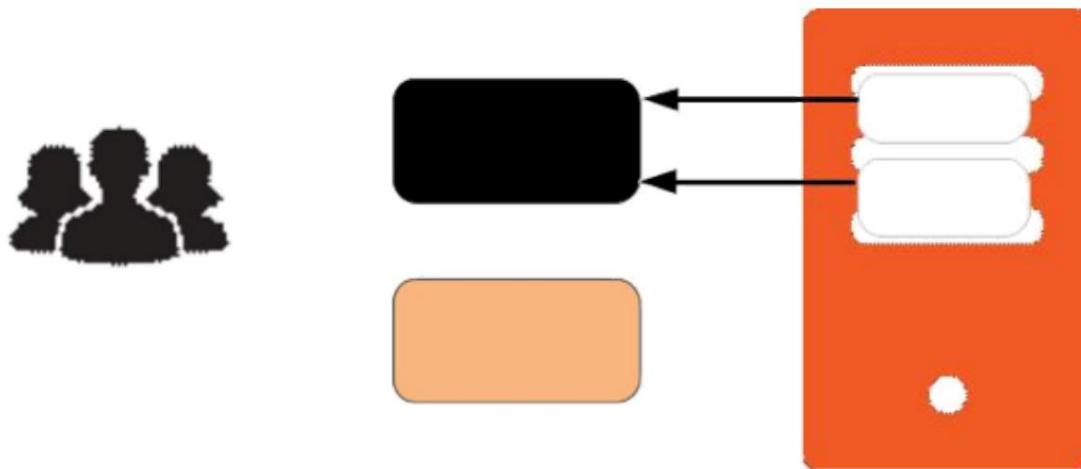
成分	描述
Nginx	高性能 HTTP/IMAP/POP3 代理服务器,可处理所有传入的 HTTP/POP/IMAP 请求。
Memcached	高性能分布式内存对象缓存系统,其中缓存路由信息以提高性能。
Zimbra 代理路由查找 处理程序	Servelet 位于 Zimbra 邮箱服务器上 处理用户帐户路由信息的查询。此路由信息包括用户帐户所在的服务器和端口号。

代理架构和流程

本节介绍 Zimbra 代理的架构和流程顺序。

1. 最终客户端使用 HTTP/HTTPS/POP/IMAP 端口连接到 Zimbra Proxy。

2. 当 Zimbra Collaboration Proxy 收到传入连接时,Nginx 组件会发送 HTTP
向 Zimbra Collaboration Proxy Route Lookup Handler 组件发出请求。



3. Zimbra Collaboration Proxy Route Lookup Handler 找到正在访问的帐户的路由信息并将其返回给 Nginx。
4. Memcached 组件会存储配置的时间段内的路由信息（默认为 1 小时）。Nginx 将使用此路由信息,而不是查询 Zimbra Collaboration Proxy Route Lookup Handler,直到默认时间段到期。
- 5.Nginx 使用路由信息连接到 Zimbra Collaboration Mailbox。
6. Zimbra Collaboration Proxy 连接到 Zimbra Collaboration Mailbox 并启动 Web/邮件代理会话。最终客户端的行为就像直接连接到 Zimbra Collaboration Mailbox 一样。

更改 Zimbra 代理配置

配置 Zimbra 代理时,Zimbra 代理配置会根据需要使用 LDAP 配置和 localconfig 中的值执行关键字替换。

如果在设置 Zimbra Proxy 后需要进行更改,请修改 Zimbra LDAP 属性或 localconfig 值,然后运行 zmconfigd 以生成更新的 Zimbra Proxy 配置。Zimbra Proxy 配置文件位于/opt/zimbra/conf/nginx.conf中。nginx.conf 包括主配置、memcache 配置、邮件配置和 Web 配置文件。

Zimbra Proxy 配置的常见变化是 IMAP/POP 配置从原始默认设置的变化

- HTTP 反向代理配置与原始默认设置不同
- Kerberos 的 GSSAPI 身份验证。在这种情况下,您可以手动识别 Kerberos Keytab 文件的位置,包括 Zimbra Proxy 密码

Zimbra 代理

Zimbra Proxy 允许最终用户使用 Microsoft Outlook、Mozilla Thunderbird 或其他 POP/IMAP 最终客户端软件等客户端访问其 Zimbra Collaboration 帐户。最终用户可以使用 POP3、IMAP、POP3S (安全 POP3)或 IMAPS (安全 IMAP)进行连接。

例如,代理允许用户输入 imap.example.com 作为其 IMAP 服务器。在 imap.example.com 上运行的代理会检查其 IMAP 流量,查找以确定用户邮箱所在的后端邮箱服务器,并透明地将用户 IMAP 客户端的连接代理到正确的邮箱服务器。

Zimbra 代理端口

以下端口由 Zimbra Proxy 或 Zimbra Mailbox 使用（如果未配置代理）。如果您有
在这些端口上运行的任何其他服务，请将其关闭。

最终客户端使用 Zimbra 代理端口直接连接到 Zimbra 代理。Zimbra 代理连接到路由
使用 Zimbra 邮箱端口的查找处理程序或 Zimbra 邮箱。

表 10. 代理端口

Zimbra 代理端口 (Zimbra 外部)	港口
HTTP	80
HTTPS	443
POP3	110
POP3S (安全 POP3)	995
信息访问协议	143
IMAPS (安全 IMAP)	993
Zimbra 邮箱端口 (Zimbra 内部)	港口
路由查找处理程序	7072
HTTP 后端 (如果配置了代理)	8080
HTTPS 后端 (如果配置了代理)	8443
POP3 后端 (如果配置了代理)	7110
POP3S 后端 (如果配置了代理)	7995
IMAP 后端 (如果配置了代理)	7143
IMAPS 后端 (如果配置了代理)	7993

严格执行服务器名称

Zimbra Proxy 能够严格执行客户端传入的 Host 标头中允许的值。

这是 默认启用 在新安装上,但离开
在安装过程中。

可以通过设置 zimbraReverseProxyStrictServerNameEnabled 布尔值来改变功能
配置选项,然后重新启动代理服务器。

- TRUE - 已启用严格服务器名称强制执行
- FALSE - 已禁用严格服务器名称强制执行

`zmprov mcf zimbraReverseProxyStrictServerNameEnabled TRUE`

重击

启用严格服务器名称功能后,可以使用
域级别的 zimbraVirtualHostName 和 zimbraVirtualIPAddress 配置项。

zmprov md example.com zimbraVirtualHostName mail.example.com zimbraVirtualIPAddress 1.2.3.4

重击

每个域只需要一个虚拟 IP 地址,但也可以接受多个。

安装 HTTP 代理后设置 IMAP 和 POP 代理

IMAP 代理随 Zimbra Collaboration 一起安装,并在安装过程中从配置菜单中进行设置。

设置 HTTP 代理,必须在已识别的代理节点上安装代理才能设置 HTTP 代理。否

通常还需要其他配置。

如果需要,请在已安装 HTTP 代理后设置 IMAP/POP 代理,并设置邮箱服务器和代理节点。

您可以运行命令 `zmproxyconfig -r server` 以在 LDAP 主服 ,针对远程主机运行。这需要服务器中进行正确配置。

使用单独的代理节点设置 IMAP/POP 代理

如果您的配置包含单独的代理服务器,请使用本节中的步骤。

1. 在您想要代理的每个 Zimbra 邮箱服务器上,启用 IMAP/POP 代理。

重击

```
/opt/zimbra/libexec/zmproxyconfig -e -m -H 邮箱.节点.服务.主机名
```

这将配置以下内容:

端口属性	环境
zimbraImapBindPort	7143
zimbraImapProxyBindPort	143
zimbraImapSSLBindPort	7993
zimbraImapSSLProxyBindPort	993
zimbraPop3BindPort	7110
zimbraPop3ProxyBindPort	110
zimbraPop3SSLBindPort	7995
zimbraPop3SSLProxyBindPort	995
zimbraImapCleartextLoginEnabled	真的
zimbraReverseProxyLookupTarget	真的
zimbraPop3CleartextLoginEnabled	真的

- 2.重新启动代理服务器和邮箱服务器的服务。

zmcontrol 重启

重击

设置代理节点

在每个安装了代理服务的代理节点上,启用 Web 代理。

/opt/zimbra/libexec/zmproxyconfig -e -m -H 代理.节点.服务.主机名

重击

这将配置以下内容：

端口属性	环境
zimbraImapBindPort	7143
zimbraImapProxyBindPort	143
zimbraImapSSLBindPort	7993
zimbraImapSSLProxyBindPort	993
zimbraPop3BindPort	7110
zimbraPop3ProxyBindPort	110
zimbraPop3SSLBindPort	7995
zimbraPop3SSLProxyBindPort	995
zimbraReverseProxyMailEnabled	真的

设置单个节点

如果 Zimbra 代理与 Zimbra Collaboration 安装在同一台服务器上,请按照本节中的步骤操作。

1. 启用网络代理。

/opt/zimbra/libexec/zmproxyconfig -e -m -H 邮箱.节点.服务.主机名

重击

这将配置以下内容：

端口属性	环境
zimbraImapBindPort	7143
zimbraImapProxyBindPort	143
zimbraImapSSLBindPort	7993
zimbraImapSSLProxyBindPort	993
zimbraPop3BindPort	7110
zimbraPop3ProxyBindPort	110

端口属性	环境
zimbraPop3SSLBBindPort	7995
zimbraPop3SSLProxyBindPort	995
zimbraImapCleartextLoginEnabled	真的
zimbraReverseProxyLookupTarget	真的
zimbraPop3CleartextLoginEnabled	真的
zimbraReverseProxyMailEnabled	真的

2.重新启动代理服务器和邮箱服务器的服务。

zmcontrol 重启

重击

配置 Zimbra HTTP 代理

Zimbra Proxy 还可以将代理 HTTP 请求反向发送至正确的后端服务器。

例如,用户可以使用 Web 浏览器连接到https://mail.example.com处的代理服务器。

来自邮箱位于 mbs1.example.com 的用户的连接由代理代理到 mbs1.example.com

在 mail.example.com 服务器上运行。该代理还支持 REST 和 CalDAV 客户端、Zimbra Connector for Outlook 和 Zimbra Mobile Sync 设备。

HTTP 反向代理按如下方式路由请求：

- 如果可以检查请求 URL 以确定用户名,则请求将被路由到后端 URL 中的用户邮箱服务器。通过此机制。
- 如果请求具有身份验证令牌 cookie (ZM_AUTH_TOKEN),则请求将被路由到后端邮箱已认证用户的服务器。
- 如果上述方法不起作用,则使用 IP 哈希方法在后端对请求进行负载平衡能够处理请求或执行任何必要的内部代理的邮箱服务器。

设置 HTTP 代理

要设置 HTTP 代理,必须在已识别的节点上安装 Zimbra Proxy。

您可以通过/opt/zimbra/libexec/zmproxyconfig -r运行命令
主机。请注意,这需要在 LDAP 主服务器中正确配置服务器。

,对抗远程

将 HTTP 代理设置为单独的代理节点

如果您的配置包含单独的代理服务器,请使用本节中的步骤。

- 在您想要代理的每个 Zimbra 邮箱服务器上,启用 Web 代理。

/opt/zimbra/libexec/zmproxyconfig -e -w -H 邮箱.节点.服务.主机名

重击

这将配置以下内容：

属性	环境
zimbra邮件参考模式	反向代理。
zimbra邮件端口	8080 (避免端口冲突)
zimbraMailSSL端口	8443 (避免端口冲突)
zimbraReverseProxyLookupTarget	真的
zimbra邮件模式	HTTP

2.重新启动代理服务器和邮箱服务器的服务。

zmcontrol 重启

重击

3. 使用公共服务主机名配置每个域,以用于 REST URL、电子邮件和公文包文件夹。

zmprov 修改域 <domain.com> zimbraPublicServiceHostname <hostname.domain.com>

重击

设置代理节点

在每个安装了代理服务的代理节点上,启用 Web 代理。

/opt/zimbra/libexec/zmproxyconfig -e -w -H 代理.节点.服务.主机名

重击

这将配置以下内容：

属性	环境
zimbra邮件参考模式	反向代理。要设置代理服务器邮件模式，在命令中添加 -x 选项,具体如下 模式为 http、https、both、重定向或混合。
zimbraMailProxy端口	80 (以避免端口冲突)。
zimbraMailSSL代理端口	443 (以避免端口冲突)。
zimbraReverseProxyHttpEnabled	TRUE (表示 Web 代理已启用)。
zimbraReverseProxyMailMode	HTTP (默认)

要设置代理服务器邮件模式,请在命令中添加-x选项,并使用特定模式：http、https、both、重定向,混合。

为 HTTP 代理设置单个节点

如果 Zimbra 代理与 Zimbra 一起安装在同一台服务器上,请按照本节中的步骤操作。

1. 在每个想要代理的 zimbra 邮箱服务器上,启用 Web 代理。

/opt/zimbra/libexec/zmproxyconfig -e -w -H 邮箱.节点.服务.主机名

重击

这将配置以下内容：

属性	环境
zimbra邮件参考模式	反向代理。
zimbra邮件端口	8080（避免端口冲突）
zimbraMailSSL端口	8443（避免端口冲突）
zimbraReverseProxyLookupTarget	真的
zimbra邮件模式	HTTP（唯一支持的模式）
zimbraMailProxy端口	80（避免端口冲突）
zimbraMailSSL代理端口	443（避免端口冲突）
zimbraReverseProxyHttpEnabled	TRUE（表示已启用 Web 代理）
zimbraReverseProxyMailMode	HTTP（默认）

要设置代理服务器邮件模式,请在命令中添加-x选项,并使用特定模式： http、 https、 both、重定向,混合。

2.重新启动代理服务器和邮箱服务器的服务。

zmcontrol 重启

重击

使用公共服务主机名配置每个域,以用于 REST URL、电子邮件和公文包文件夹。

zmprov 修改域 <domain.com> zimbraPublicServiceHostname <hostname.domain.com>

重击

设置代理以使用明文进行上行连接

设置代理以使用明文进行上行连接时,请设置

zimbraReverseProxySSLToUpstreamEnabled为 FALSE。

此属性默认为 TRUE。在“现成的”代理设置中,上游通信默认为 SSL。

REST URL 生成

对于 REST URL,您可以全局设置主机名、服务协议和服务端口,也可以针对特定域设置以下属性。

- zimbraPublicServiceHostname
- zimbra公共服务协议
- zimbra公共服务端口

生成 REST URL 时:

- 如果设置了domain.zimbraPublicServiceHostname ,则使用zimbraPublicServiceProtocol + zimbraPublicServiceHostname + zimbraPublicServicePort
- 否则,它将恢复到服务器 (帐户的主服务器)属性:

- 协议是根据server.zimbraMailMode计算得出的
- 主机名是server.zimbraServiceHostname
- 端口是根据协议计算出来的。

关于使用zimbraMailReferMode - 在早期版本中,本地配置变量 zimbra_auth_always_send_refer 决定了当用户的邮箱不在用户登录的服务器上时后端服务器采取的操作。如果用户登录到错误的后端主机,则默认值 FALSE 会重定向用户。

在多服务器 Zimbra 上,如果需要负载平衡名称来创建友好的登录页面,则必须始终重定向用户。在这种情况下, zimbra_auth_always_send_refer设置为 TRUE。

现在有了功能齐全的反向代理,用户无需重定向。本地配置变量zimbraMailReferMode与 nginx 反向代理一起使用。

设置代理信任的 IP 地址

当使用 Zimbra 配置代理时,必须在 LDAP 属性zimbraMailTrustedIP中配置每个代理服务器的 IP 地址,以便在用户通过代理登录时将代理地址标识为受信任。代理 IP 地址将添加到X-Forwarded-For标头信息中,X -Forwarded-For标头会自动添加到 localconfig zimbra_http_originating_ip标头属性中。当用户登录时,此 IP 地址和用户的地址将在 Zimbra 邮箱日志中进行验证。

在属性中设置每个代理 IP 地址。例如,如果您有两个代理服务器:

`zmprov mcf +zimbraMailTrustedIP {nginx-1 的 IP} +zimbraMailTrustedIP {nginx-2 的 IP}`

重击

要验证 X-Forwarded-For 是否已正确添加到 localconfig,请键入

`zmlocalconfig | grep -i http`

重击

你应该看到

`zimbra_http_originating_ip_header = X-Forwarded-For`

重击

配置 Zimbra 代理进行 Kerberos 身份验证

如果您使用 Kerberos5 身份验证机制并想要为 IMAP 和 POP 代理进行配置,请使用本节中的步骤。

确保您的 Kerberos5 身份验证机制配置正确。请参阅Zimbra
LDAP 服务

1. 在每个代理节点上,将 zimbraReverseProxyDefaultRealm 服务器属性设置为与代理服务器对应的域名称。例如:

`zmprov ms [DNS 名称.isp.net] zimbraReverseProxyDefaultRealm [ISP.NET]`

重击

2. 邮件客户端连接的每个代理 IP 地址都必须配置为邮件服务器的 GSSAPI 身份验证
服务器。在每个代理节点上,针对每个代理 IP 地址:

`zmprov mcf +zimbraReverseProxyAdminIPAddress [IP 地址]`

重击

3. 在每个代理服务器上:

`zmprov ms [proxyexample.net] zimbraReverseProxyImapSaslGssapiEnabled TRUE`

重击

`zmprov ms proxyl.isp.net zimbraReverseProxyPop3SaslGssapiEnabled TRUE`

4. 重新启动代理服务器

`zmproxyctl 重启`

重击

Zimbra 管理控制台

Zimbra 管理控制台是一个基于浏览器的用户界面,用于集中管理 Zimbra 服务器和用户帐户。

管理员帐户

当您登录到管理控制台时,您有权执行的任务将显示在导航窗格中。这些任务取决于分配给您的管理员角色的权限。

您可以创建两种类型的管理员帐户来管理 Zimbra Collaboration:

- 全局管理员拥有管理服务器、全局设置、域和帐户以及创建其他管理员的完全权限。软件安装期间会自动创建一个全局管理员帐户。以后可以随时创建其他全局管理员帐户。您可以从管理控制台或命令行执行管理任务。
- 委派管理员由全局管理员授予自定义管理员角色,以便从管理控制台管理不同的任务。有关更多详细信息,请参阅委派管理。

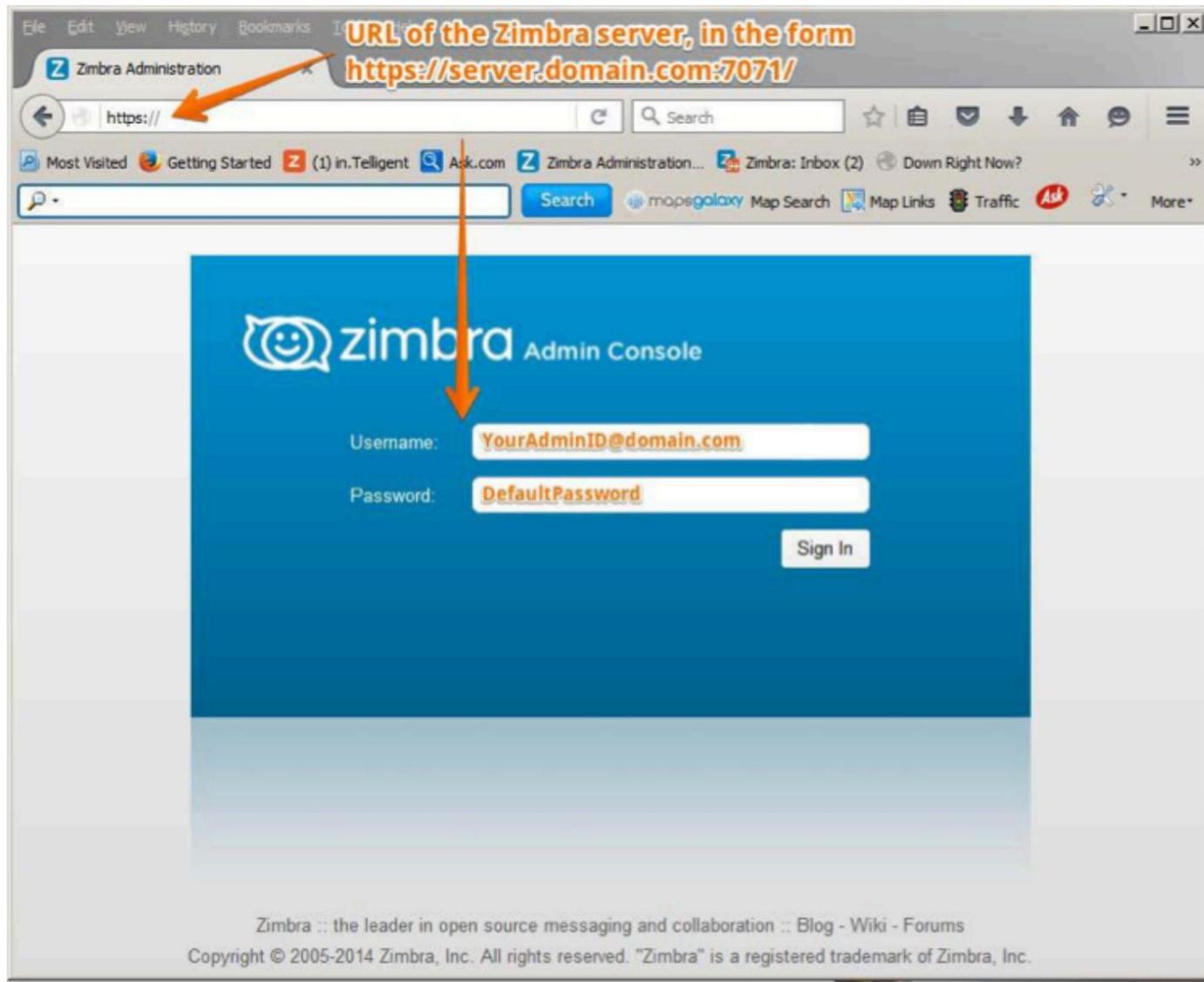
登录管理控制台

- 要在典型安装中启动管理控制台,请使用以下 URL 模式。

<https://server.domain.com:7071/>

范围	描述
服务器.域名.com	Zimbra 服务器名称或 IP 地址。
7071	默认的 HTTP 监听端口。

- 在登录屏幕上,输入完整的管理员地址 (例如admin@domain.com) 和密码
在 Zimbra Collaboration 服务器安装期间对其进行配置。



修改管理员密码

您可以随时从管理控制台或 CLI 更改密码。

在管理控制台中,使用“更改密码”屏幕设置新密码字符串,并定义用户密码修改策略。

管理控制台：

主页→管理→账户

双击选择 用户帐户 或者从齿轮图标中,从弹出菜单中选择更改密码。



zmprov sp adminname@domain.com 密码

重击

自定义登录和注销页面

不同的登录和注销页面可以配置为全局设置或域设置。

指定管理员登录身份验证失败或身份验证已过期时重定向到的 URL:

全球的:

zmprov mcf zimbraAdminConsoleLoginURL <https://example.com>

重击

领域:

zmprov md <域> zimbraAdminConsoleLoginURL <https://example.com>

重击

要指定将管理员重定向到的 URL,以便注销:

全球的:

zmprov mcf zimbraAdminConsoleLogoutURL <https://example.com>

重击

领域:

zmprov md <域> zimbraAdminConsoleLogoutURL <https://example.com>

重击

管理任务

大多数 Zimbra 任务 (例如创建帐户和服务类别、服务器状态监控、域管理、备份计划和会话管理)都可以从管理控制台进行管理。

其他配置和维护任务需要使用 Zimbra CLI,因为您无法在管理控制台中执行这些任务。例如:启动和停止服务以及管理本地服务器配置。

在管理控制台中,如果您需要查看与特定功能相关的属性,您可以单击当前可见配置页面的文本标签以在弹出窗口中打开信息。这些弹出窗口还提供指导文本,如下图所示。

查看属性

这 管理控制台

单击字段标签可以查看属性弹出窗口。

General Information

Most results returned by GAL search:

Default domain:

Maximum number of Attribute Name simultaneous zimbraDefaultDomainName

More

Sleep time before:

Maximum size of a file uploaded from the desktop (KB):

Admin help URL:

Delegated admin help URL:

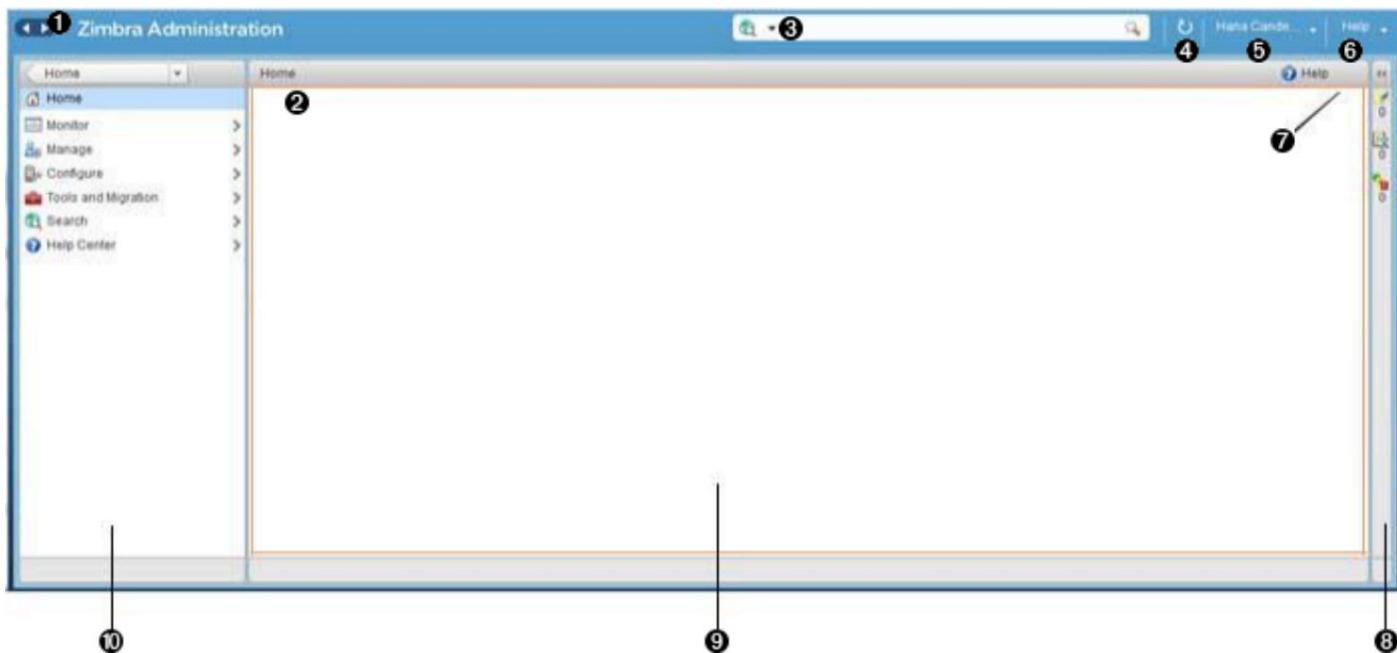
在属性弹出窗口视图中,单击“更多”以查看有关该字段的指导文本。

General Information	
Most results returned by GAL search:	100
Default domain:	jhurley1.us.zimbralab.com
Maximum number of simultaneous Attribute Name	zimbraDefaultDomainName
Sleep time before authentication:	name of the default domain for accounts when authenticating without a domain
Maximum size (KB):	1000
Admin help URL:	
Delegated admin help URL:	

浏览用户界面

Zimbra 协作管理控制台的组织结构可快速导航至与您的登录权限相关的配置和监控工具和视图。它还可以轻松访问各种类型的帮助和屏幕指南文本。

登录管理控制台后,主页提供状态信息和选项,您可以选择导航至本用户指南中描述的配置和查看选项。



- <1> 转至上一页或下一页
- <2> 当前位置/路径
- <3> 搜索
- <4> 屏幕刷新
- <5> 当前用户和注销选项
- <6> 帮助
- <7> 齿轮图标
- <8> 状态窗格
- <9> 查看窗格
- <10> 导航窗格

导航窗格和查看窗格中的显示和选项会根据您的选择而变化。用户界面的其他部分（箭头按钮、搜索字段、屏幕刷新、当前位置/路径、当前登录和帮助）始终保持在视图中。

齿轮图标



与一些屏幕一起显示,以便快速访问与屏幕中提供的功能。有关齿轮图标的更多信息,请参阅使用齿轮图标

主页导航窗格

主页导航窗格中提供的选项归类在主页目录下。一些选项会引导至配置页面;其他选项会引导至包含报告的页面,这些页面与您的选择相关。

右图是导航窗格中当前支持的选项的扩展视图。

视图页面的上方栏始终显示您在层次结构中的当前位置,并且您可以使用多个选项来关闭当前视图:

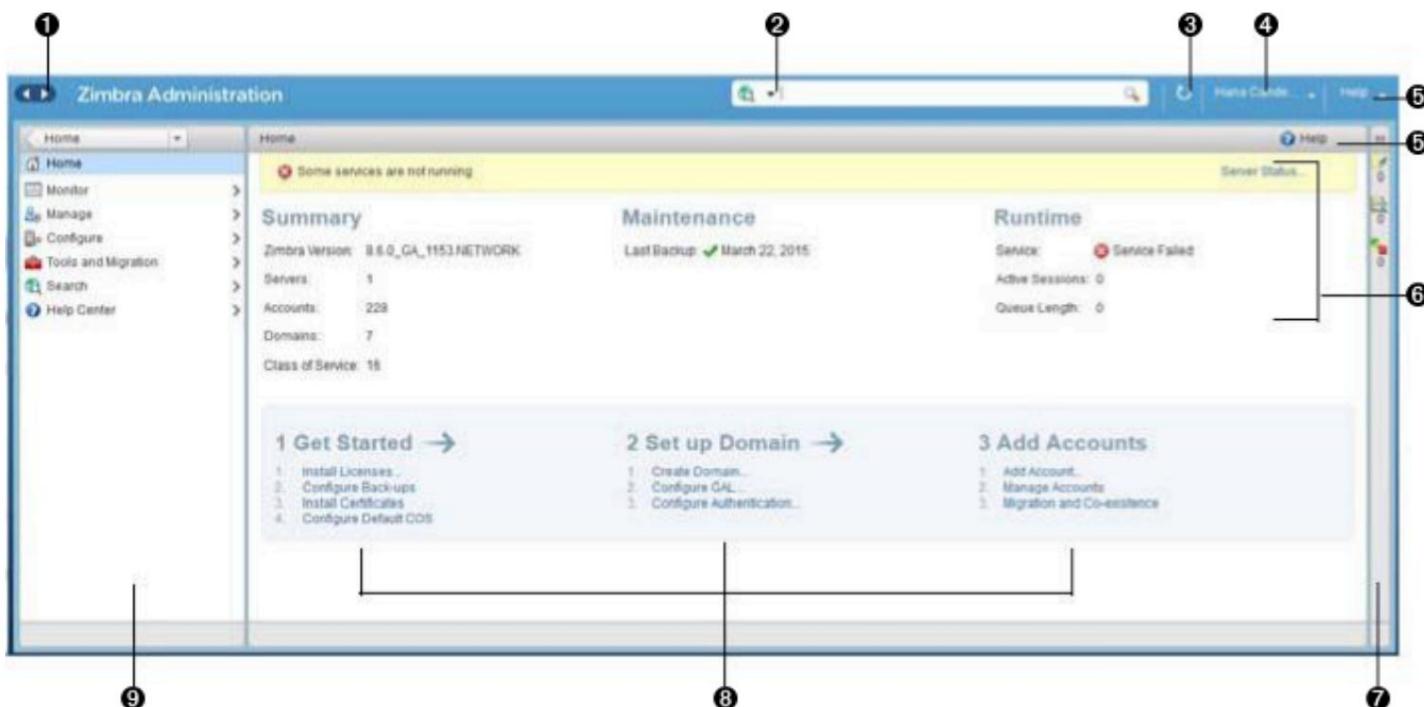
- 要返回上一页或转到下一页,请单击向左或向右箭头。
- 要返回 UI 的特定部分,请从主页下拉菜单中选择一个选项。
- 要直接转到特定选项,请单击导航窗格中的层次结构。

导航窗格选项在以下主题中描述:

- 主页用户界面。
- 监控用户界面。
- 管理用户界面。
- 配置 UI。
- 全局设置用户界面。
- 工具和迁移 UI。
- 搜索用户界面。

主页界面

主页屏幕是默认的登录视图,提供主页导航窗格和主页。此页面提供系统状态的快照视图和一系列用于基本任务的快速访问链接。



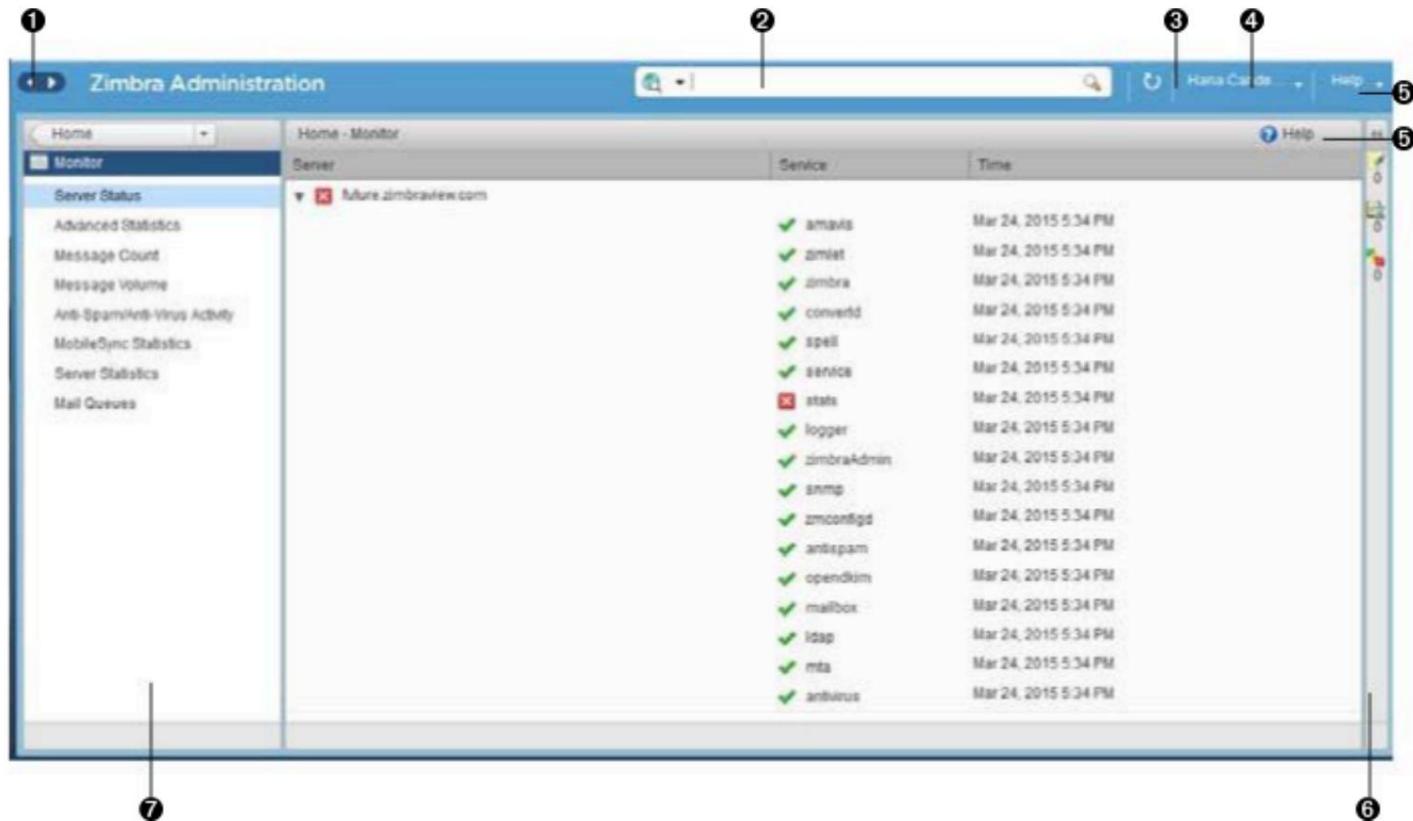
<1> 转至上一页或下一页
 <2> 搜索
 <3> 屏幕刷新
 <4> 当前用户和注销选项
 <5> 帮助
 <6> 系统状态
 <7> 状态窗格
 <8> 快速入门
 <9> 导航窗格

表格主页UI.

话题	描述
概括	显示当前正在运行且可见的 Zimbra Collaboration 版本,以及检测到的相关服务器、账户、域和服务类别的数量与本次会议。
维护	显示最近执行的软件备份。
运行时	显示服务、活动会话和队列长度的运行时统计信息。
1 开始	显示开始使用 Zimbra Collaboration 所必需的步骤操作,并提供此 UI 中功能的快速链接: <ol style="list-style-type: none"> 1. 安装许可证 2. 配置备份 3. 安装证书 4. 配置默认 COS
2 设置域名	显示用于建立由合作者。每个步骤都是此 UI 中功能的链接: <ol style="list-style-type: none"> 1. 创建域 2. 配置 GAL… 3. 配置身份验证
3 添加账户	显示添加帐户以供合作者管理的步骤。每个步骤是此 UI 中功能的链接: <ol style="list-style-type: none"> 1. 添加账户 2. 管理账户 3. 移民与共存

监控界面

监控屏幕提供监控导航窗格和监控页面,显示各种有关合作者监控的服务器的详细说明。



<1> 转至上一页或下一页

<2> 搜索

<3> 屏幕刷新

<4> 当前用户和注销选项

<5>帮助

<6> 状态窗格

<7> 导航窗格

监控导航窗格和页面

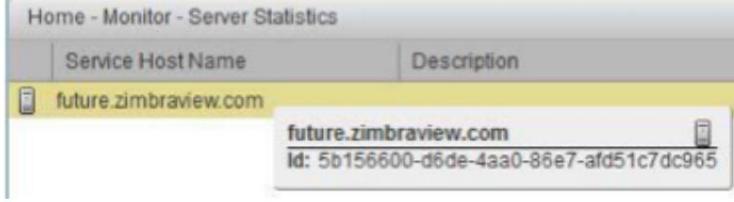
监控页面提供的选项提供了各种方法（动态图表或表格）来查看下表列出的单个或系统范围的监控服务器和服务。

必须激活 Adobe Flash Player 才能查看动态图表。

表监视器101

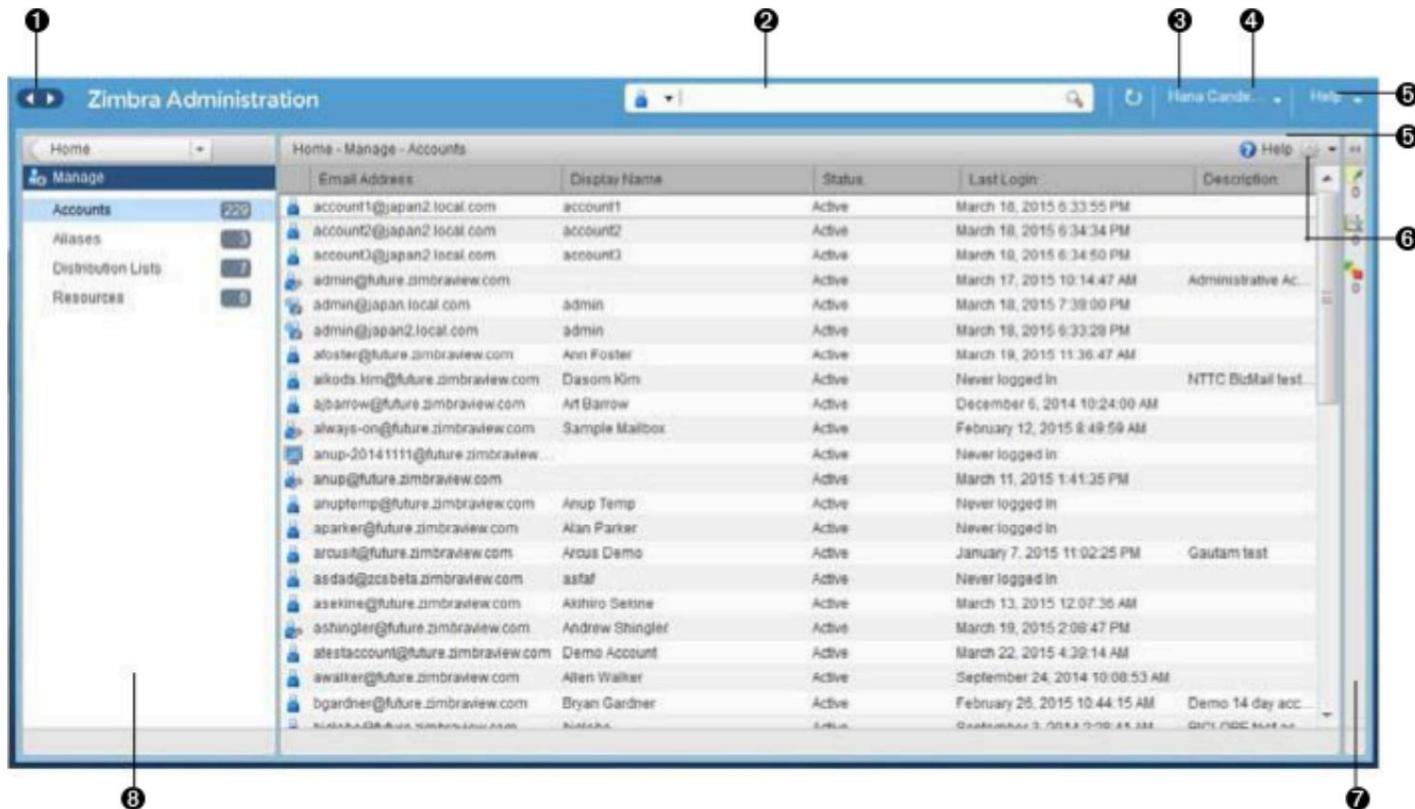
选项	描述
服务器状态	合作者监控的每个服务器的服务器、服务和时间详细信息。

选项	描述
高级统计	<p>系统范围的高级统计信息页面,允许您设置 使用来自选择字段的参数创建新的监控图表 此页面:服务器、组、开始、结束和计数器。</p> <p>在此高级统计页面中,您还可以选择执行以下操作 运营:</p> <ul style="list-style-type: none"> • 隐藏图表设置 • 更新图表 • 移除图表
消息数	<p>系统范围的信息页面,用于消息计数,查看描述 过去 48、30、60 和 365 天的计数。该信息总结了 使用 SMTP 或 LMTP 的邮件收件人数量。轮询间隔 因为计数直接发布在每个图表下方。</p>
留言量	<p>系统范围的信息页面,用于查看消息量图表 使用 SMTP 或 LMTP 的邮件收件人数量,以及相关 邮件大小。这些计数会按过去 48、30、60 和 365 天。计票的投票间隔直接张贴在每个 图表。</p>
反垃圾邮件/反病毒	系统范围的信息页面,用于反垃圾邮件/反病毒
活动	<p>活动,描述 AS/AC 系统处理的唯一消息数量 过去 48、30、60 和 365 天内的统计数据。统计的轮询间隔为 直接发布在每张图表下方。</p>

选项	描述
服务器统计	<p>访问所选服务主机的统计信息。您可以查看选定主机,如下:</p> <ul style="list-style-type: none"> 将光标放在服务主机名上并按住以查看弹出许可证信息。  <ul style="list-style-type: none"> 右键单击服务主机名,然后从弹出窗口中选择“查看”,转到其统计信息页面。您也可以双击服务主机名来访问统计信息页面。  <p>对于选定的服务器,服务器统计信息导航窗格提供了查看磁盘、会话、邮箱配额、消息计数、消息量和反垃圾邮件/反病毒活动的选项。</p>
邮件队列	选项卡页可查看检测到的邮件队列的延迟、传入、活动、保留和损坏统计信息。每个选项卡页均提供摘要过滤信息和消息详细信息。

管理用户界面

管理屏幕提供管理导航窗格和管理页面,其中显示当前由 Collaborator 管理的帐户、别名、分发列表和资源等类别的表格。



<1> 转至上一页或下一页

<2> 搜索

<3> 屏幕刷新

<4> 当前用户和注销选项

<5> 帮助

<6> 齿轮图标

<7> 状态窗格

<8> 导航窗格

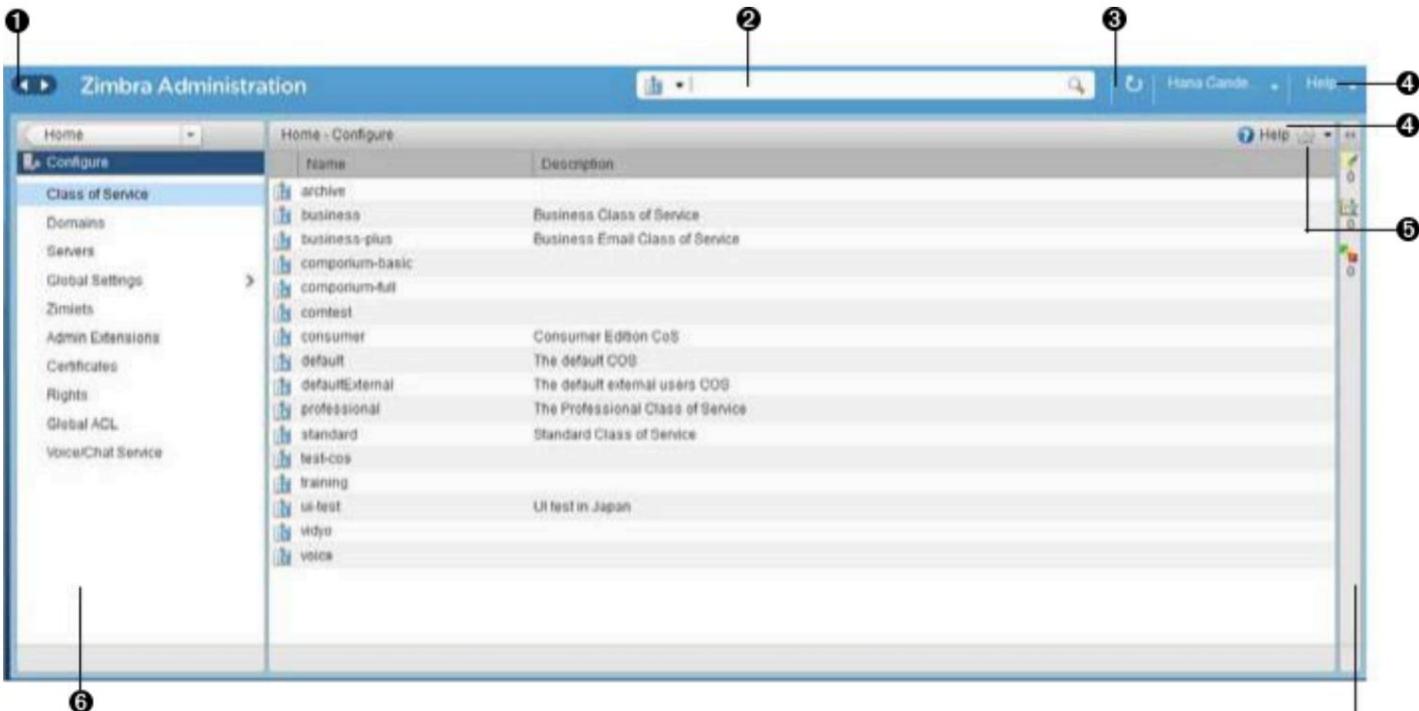
表管理界面

选项	描述
账户 (数量)	<p>合作者管理的帐户表。您可以执行的操作：</p> <ul style="list-style-type: none"> 从弹出窗口查看 ID 信息 :将光标放在帐户上排。 右键单击表格行 ,或使用齿轮图标访问以下内容功能 :删除、编辑、更改密码、新管理员、查看邮件、新建、使会话无效、查看权限、配置授权、移动邮箱、搜索邮件。
别名 (数量)	<p>协作者管理的别名表。每个别名都是一个电子邮件地址，将所有电子邮件转发到指定帐户。</p> <p>您可以执行的操作：</p> <ul style="list-style-type: none"> 在弹出窗口中查看 ID 信息 :将光标悬停在别名行上。 右键单击表格行 ,或使用齿轮图标访问以下内容功能 :删除、编辑、新建管理员、查看邮件、移动别名、新建、使会话无效、查看权限、配置授权、移动邮箱、搜索邮件。

选项	描述
分发列表 (计数)	<p>协作者管理的分发列表表。分发列表是包含在列表中的一组邮件地址,其中包含列表的邮件地址。当您向分发列表发送消息时,您会将其发送给地址出现在列表中的每个人。收件人 :地址行显示分发列表地址。</p> <p style="text-align: right;">隐含地</p> <p>您可以执行的操作:</p> <ul style="list-style-type: none"> 查看 ID 信息 :将光标悬停在分发列表行上。 右键单击表格行,或使用齿轮图标访问以下功能 :删除、编辑、新管理员、查看邮件、新建、查看权限、配置授权、搜索邮件。
资源 (数量)	<p>协作者管理的资源表。资源是支持会议安排的地点或设备。</p> <p>您可以执行的操作:</p> <ul style="list-style-type: none"> 查看 ID 信息 :将光标悬停在资源行上。 右键单击表格行,或使用齿轮图标访问以下功能 :删除、编辑、新管理员、查看邮件、新建、查看权限、配置授权、搜索邮件。

配置 UI

配置屏幕提供了配置导航窗格和配置页面,可用于配置单个或全局组件。



<1> 转至上一页或下一页
 <2> 搜索
 <3> 屏幕刷新
 <4> 帮助
 <5> 齿轮图标
 <6> 状态窗格
 <7> 配置导航窗格

表配置 UI 14.

选项	描述
服务等级	<p>显示从此 AdministrationConsole 管理的 COS。</p> <ul style="list-style-type: none"> 双击表格行可访问所选的配置屏幕 版权, <p>或者</p> 右键单击表格行,或使用齿轮图标访问以下功能:新建、删除、编辑、复制
域	<p>显示从该管理控制台管理的域。</p> <ul style="list-style-type: none"> 双击表格行以访问所选域的配置屏幕, <p>或者</p> 右键单击表格行,或使用齿轮图标访问以下功能:新建、删除、编辑、配置 GAL、配置身份验证、查看账户,添加域别名,配置授权
服务器	<p>显示从该管理控制台管理的服务器。</p> <ul style="list-style-type: none"> 双击表格行可访问所选的配置屏幕 服务器, <p>或者</p> 右键单击表格行,或使用齿轮图标访问以下功能:编辑、清除缓存、启用代理、禁用代理
全局设置	<p>提供对您用来为 Zimbra Collaboration 设置各种全局参数的工具的访问。</p> <p>齿轮图标:保存、下载、更新许可证、激活许可证、手动激活 执照</p>

选项	描述
齐姆莱茨	<p>显示从该管理控制台管理的 Zimlets。</p> <ul style="list-style-type: none"> 双击表格行可访问所选的配置屏幕 齐姆莱特, 或者 右键单击表格行,或使用齿轮图标访问以下功能:部署、取消部署、切换状态
管理扩展	<p>显示从此管理控制台管理的管理扩展。</p> <ul style="list-style-type: none"> 双击表格行可访问所选的配置屏幕 管理扩展, 或者 右键单击表格行,或使用齿轮图标访问以下功能:部署、取消部署
证书	<p>显示从此管理控制台管理的证书。</p> <ul style="list-style-type: none"> 双击表格行可访问 选定的证书, 或者 右键单击表格行,或使用齿轮图标访问以下功能:安装证书、查看证书
权利	<p>显示适用于此管理控制台的各种权利。</p> <ul style="list-style-type: none"> 双击表格行可访问 选择右侧, 或者 右键单击表格行,或使用齿轮图标来访问以下功能: 看法
全局 ACL	<p>显示从此管理控制台管理的全局访问控制列表。</p> <ul style="list-style-type: none"> 双击表格行,访问所选全局的编辑 ACE 屏幕 ACL, 或者 右键单击表格行,或使用齿轮图标访问以下功能:添加、删除、编辑

全局设置用户界面

全局设置定义了服务器、账户、COS 和域的默认全局值。当特定项目的设置中没有特定的值和参数时,将应用这些默认值和参数。

您可以在安装过程中配置全局设置的默认设置。您可以随时更改设置管理控制台上的全局设置。

表全局设置 15.

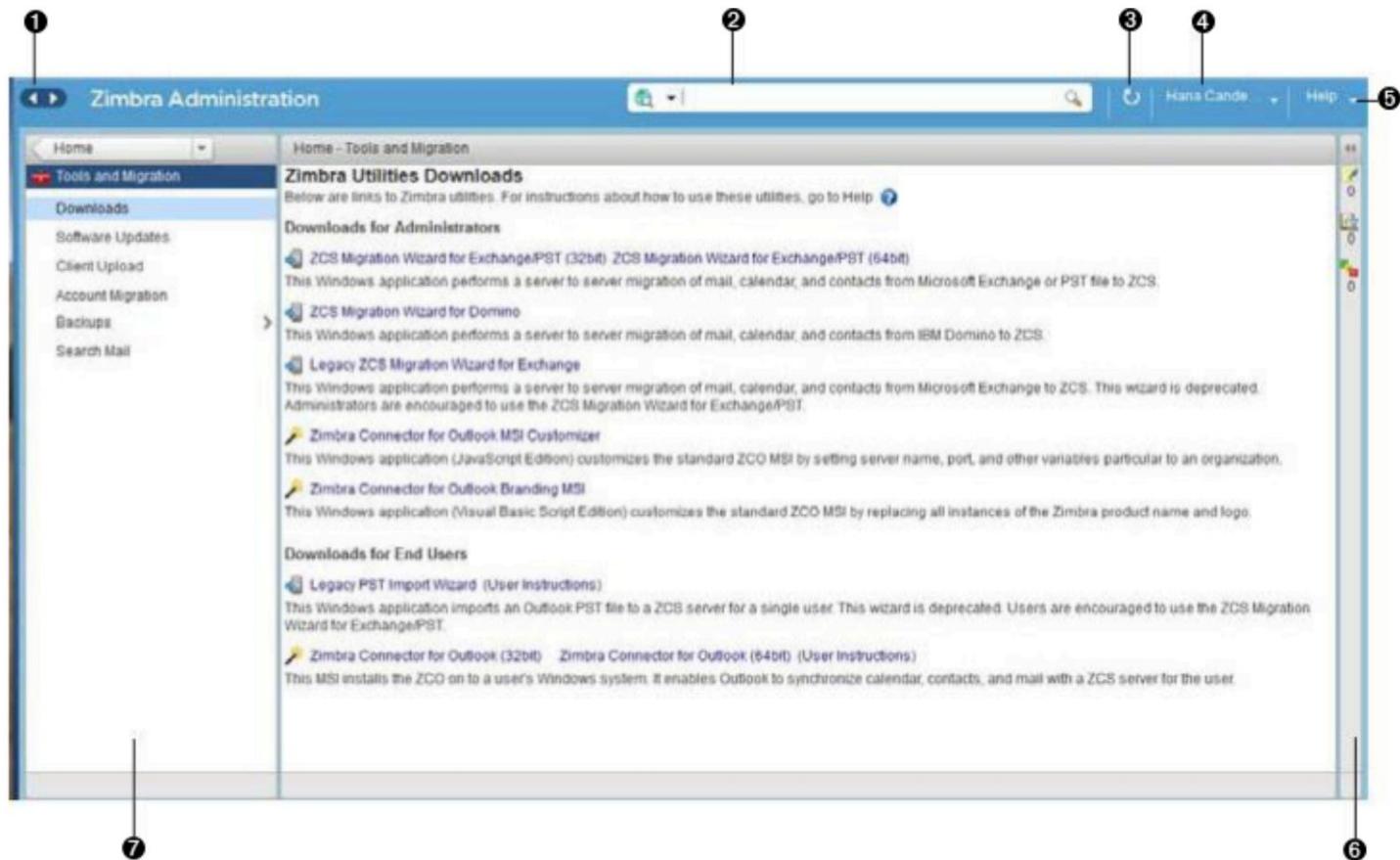
用户界面

选项	描述
一般信息	<ul style="list-style-type: none"> 设置 GAL 搜索的结果数量的全局上限。 定义默认域。 配置可用于从远程数据源。 <p>有关详细信息,请参阅常规信息配置</p>
附件	<ul style="list-style-type: none"> 启用规则以拒绝包含特定扩展名的附件的消息。 禁止读取附件。 将附件转换为 HTML 以供查看。 <p>有关详细信息,请参阅附件配置。</p>
大都会运输署	<ul style="list-style-type: none"> 启用身份验证。 设置最大消息大小。 启用或禁用协议和 DNS 检查。 添加 X-Originating-IP 消息头。 <p>有关更多信息,请参阅MTA 配置。</p>
信息访问协议	启用 IMAP 服务。这些设置的更改只有在服务器重新启动。
流行音乐	启用 POPS3 服务。这些设置的更改只有在服务器重新启动。
开启/关闭	设置反垃圾邮件和反病毒规则。垃圾邮件检查设置的更改不会直到服务器重启才能生效。
主题	<ul style="list-style-type: none"> 自定义现有主题的配色方案 为主题添加徽标。 <p>更改主题设置需要使用以下方法刷新服务器主题缓存 []服务器设置工具栏上的刷新缓存。</p> <p>有关详细信息,请参阅颜色和徽标管理。</p>
先进的	<ul style="list-style-type: none"> 配置在提示中显示的公司名称 <p>用于登录与以下用户共享的“公文包”文件夹的“需要身份验证”对话框 外部嘉宾</p> <ul style="list-style-type: none"> 添加帐户电子邮件验证的正则表达式规则。

选项	描述
保留政策	设置用户文件夹中项目的保留和删除时间阈值。您可以将保留和删除策略配置为全局设置,或配置 COS 级别策略而不是从全局设置继承。
代理人	设置 Web 代理和邮件代理的参数。还提供以下工具： 设置高级代理参数。
邮件/多用途邮件	(安全多用途互联网邮件扩展) :配置 LDAP 设置 S/MIME 选项卡 (如果启用了 S/MIME 功能)。用户可从以下位置检索私钥：LDAP 服务器。
访问控制列表	(访问控制列表) :转到 ACE (访问控制条目)配置以进行委派 授予选定目标的管理权限,以添加、编辑或删除 ACE。
备份/恢复	设置备份参数-标准或自动分组模式。有关更多信息 信息请参阅备份和恢复。
山猫	(存储管理) :配置消息在移至 次要卷。
执照	<ul style="list-style-type: none"> 更新并安装您的 Zimbra 许可证。 查看当前许可证信息。

工具和迁移 UI

工具和迁移屏幕提供工具和迁移导航窗格,用于访问系统软件
管理和系统备份/恢复。管理员可以从以下位置访问和下载特定向导和工具
本页。



- <1> 转至上一页或下一页
- <2> 搜索
- <3> 屏幕刷新
- <4> 当前用户和注销选项
- <5>帮助
- <6> 状态窗格
- <7> _工具和迁移_导航窗格

表 16. 工具和迁移

选项	描述
下载	访问 Zimbra 实用程序,它提供可下载的zip包 - 用于一般管理使用,并同步单个最终用户 - 包含适用于各种平台的迁移向导和 Outlook 连接器。其他可下载的向导和连接器中提供了相关信息。
软件更新	了解您的系统是否需要 Zimbra 服务器更新,并使用此页面来查看与您的软件更新相关的投票和电子邮件联系信息系统。 另请参阅检查 Zimbra 协作软件更新。
账户迁移	查看系统检测到的账户迁移表格详情。这页面列出了总进口量和每项进口量的状态。此页面还提供了名称列出的每个帐户迁移的所有者。另请参阅从 Zimbra 服务器。

选项	描述
客户端上传	使用此页面浏览要上传到系统的最新版本软件。选择映像后,您可以使用此页面上的“上传”完成软件上传。 []
备份	根据最新的系统备份访问当前可用空间和总空间 (MB) 的摘要视图。您还可以从此导航窗格中选择管理员以查看其备份历史记录。历史记录列出了每次备份的标签、开始和结束时间以及成功或失败情况。这些列表中的每一个都与备份目标的相同显示目录路径相关联。备份和恢复部分提供了更多信息。

可下载的向导和连接器

使用工具和迁移屏幕下载选项来获取本节描述的工具。

表管理员工具和迁移选项 17.

Zimbra 协作迁移向导 Exchange/PST (32 位)	获取zip文件以执行来自 Microsoft 的邮件、日历和联系人的服务器到服务器迁移 将 Exchange 或 PST 文件传输至 Zimbra Collaboration 服务器。 此软件包已弃用!我们建议 奥德里加自助服务 迁移解决方案(https://zimbra.audriga.com/) 作为所有帐户迁移的首选方案。
Zimbra 协作迁移向导 (适用于 Domino)	此软件包已弃用!我们推荐使用Audriga 的 自助迁移解决方案 (https://zimbra.audriga.com/) 作为所有帐户迁移的首选方案。
旧版 Zimbra 协作迁移向导 交换	此软件包已弃用!我们推荐使用Audriga 的 自助迁移解决方案 (https://zimbra.audriga.com/) 作为所有帐户迁移的首选替代方案。
Zimbra 连接器 for Outlook MSI 定制器	提供包含可用于自定义标准 ZCO MSI 的函数的文本文件。可以自定义特定于组织的服务器名称、端口和其他变量。

用于 Outlook 品牌推广 MSI 的 Zimbra 连接器

获取 Windows Visual Basic 脚本版本 (VBScript) 使用脚本文件 (Script File) 来定制标准 ZCO MSI。定制替换 Zimbra 的所有实例产品名称和标志。

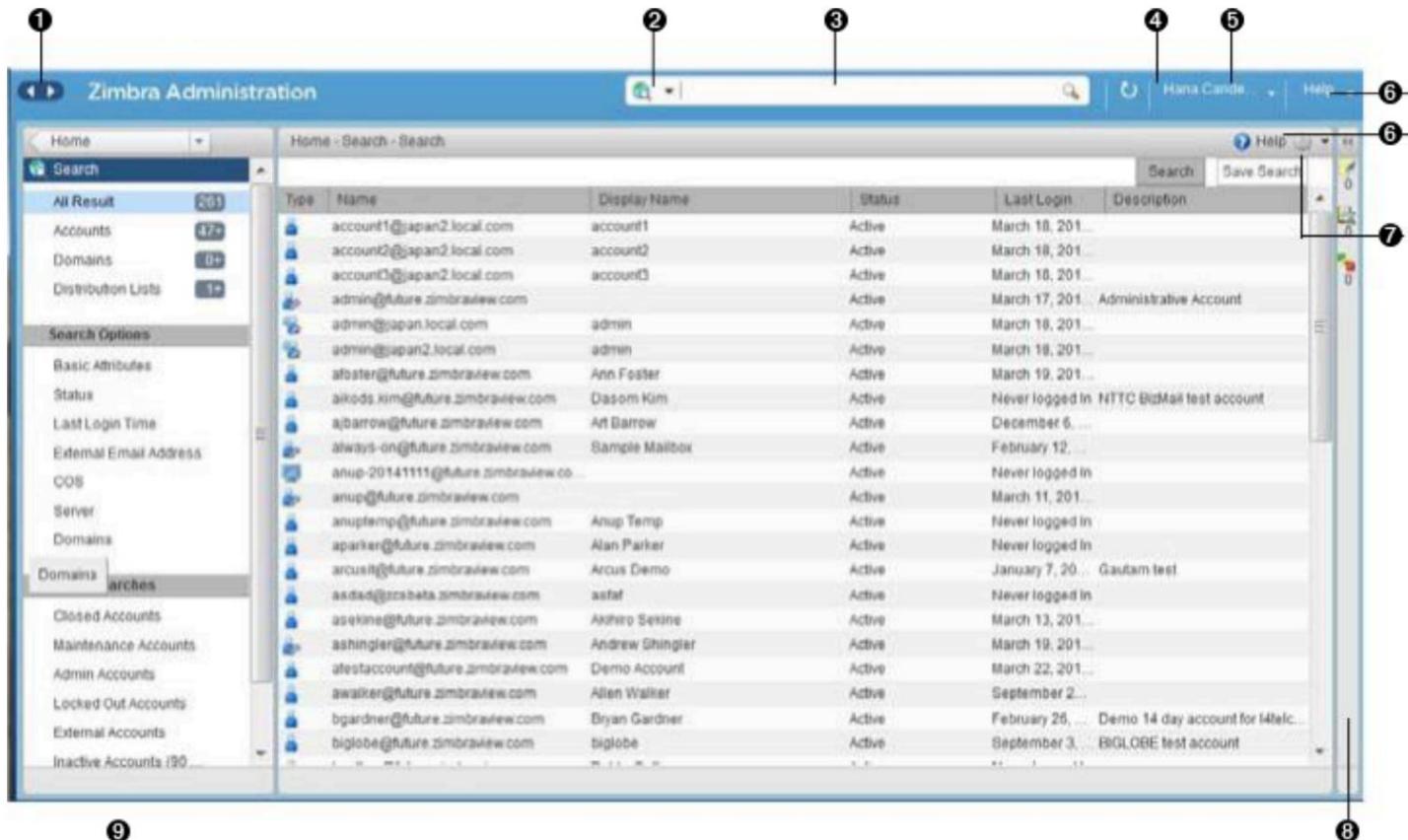
表最终用¹⁸**桌面应用程序和实用程序/迁移和导入工具**

Zimbra 适用于 Outlook 的连接器 (32 位) Zimbra Connector for Outlook (64 位) (用户指示)	此应用程序使 Outlook 能够同步使用 Zimbra 服务器管理日历、联系人和邮件并访问 Zimbra Collaboration 的业务功能。 地址簿、联系人、日历、任务和邮件 直接与 Zimbra Collaboration 同步 服务器。
(旧版)Microsoft Outlook PST 导入工具	此软件包已弃用! 用户应使用普通移民 PST 导入向导。
(旧版)Microsoft Exchange 迁移向导	此软件包已弃用! 我们推荐 Audriga 的 自助服务 迁移解决方案 (https://zimbra.audriga.com/) 作为所有帐户的首选替代方案移动。
通用迁移向导	此工具可导入 Microsoft Exchange 中的数据服务器和 Outlook PST 文件到 Zimbra 服务器。 此包仅支持 PST 文件导入。我们建议 Audriga 的自助迁移解决方案 (https://zimbra.audriga.com/) 作为所有人的首选方案帐户迁移。

搜索用户界面

搜索屏幕显示管理控制台中搜索字段查询的搜索结果
标轴。

- 当您打开此页面而不输入搜索查询时,内容窗格中将显示帐户、域和分发列表。 全部结果 是默认搜索,显示
- 自动完成功能允许您输入部分名称,然后从中选择一个可搜索的名称
显示匹配字符串的列表。
- 您还可以使用 Zimbra 邮箱 ID 号来搜索帐户。但是,要从邮箱 ID,搜索时必须输入完整的ID字符串。



<1> 转至上一页或下一页

<2> 搜索选项

<3> 搜索

<4> 屏幕刷新

<5> 当前用户和注销选项

<6>帮助

<7> 齿轮图标

<8> 状态窗格

<9> 搜索导航窗格

表格搜索¹⁰界面

选项	描述
全部结果	查看所有搜索结果的计数和表格。
帐户	查看帐户查询产生的计数和表格。
域	查看域查询产生的计数和表。
分发列表	查看分发列表查询所得的计数和表格。
基本属性	按名字、姓氏、显示名称或帐户 ID 号搜索用户。您可以 仅可以搜索管理员或委派管理员。
地位	按状态搜索帐户：活跃、已关闭、已锁定、已注销、待处理或 维护。
上次登录时间	按最后登录时间搜索账户。您可以指定日期范围进行搜索。
外部电子邮件地址	搜索具有外部电子邮件地址的帐户。

选项	描述
操作系统	按 COS 搜索对象或未分配 COS 的对象。
服务器	在选定的服务器上搜索帐户。
域	在选定的域中搜索帐户。
已保存的搜索	默认情况下,此部分包含预定义的常见搜索查询。您还可以 创建并保存查询。输入查询语法后,单击“保存搜索” 并为搜索提供名称。然后,该搜索将添加到此“已保存的搜索”中 部分。

设置简单搜索

1. 在“搜索”字段中,使用下拉选择器中的搜索选项定义搜索类型,例如
, 分发列表别名帐户 , , 资源 , 域服务类别 , , 或者 所有对象 。

对于帐户,您可以按显示名称、名字/姓氏、电子邮件地址的第一部分、别名、送货地址或邮箱ID。

2. 在搜索字段中输入搜索字符串。

允许将部分条目作为搜索条件,但基于邮箱 ID 的搜索必须包含完整 ID
细绳。

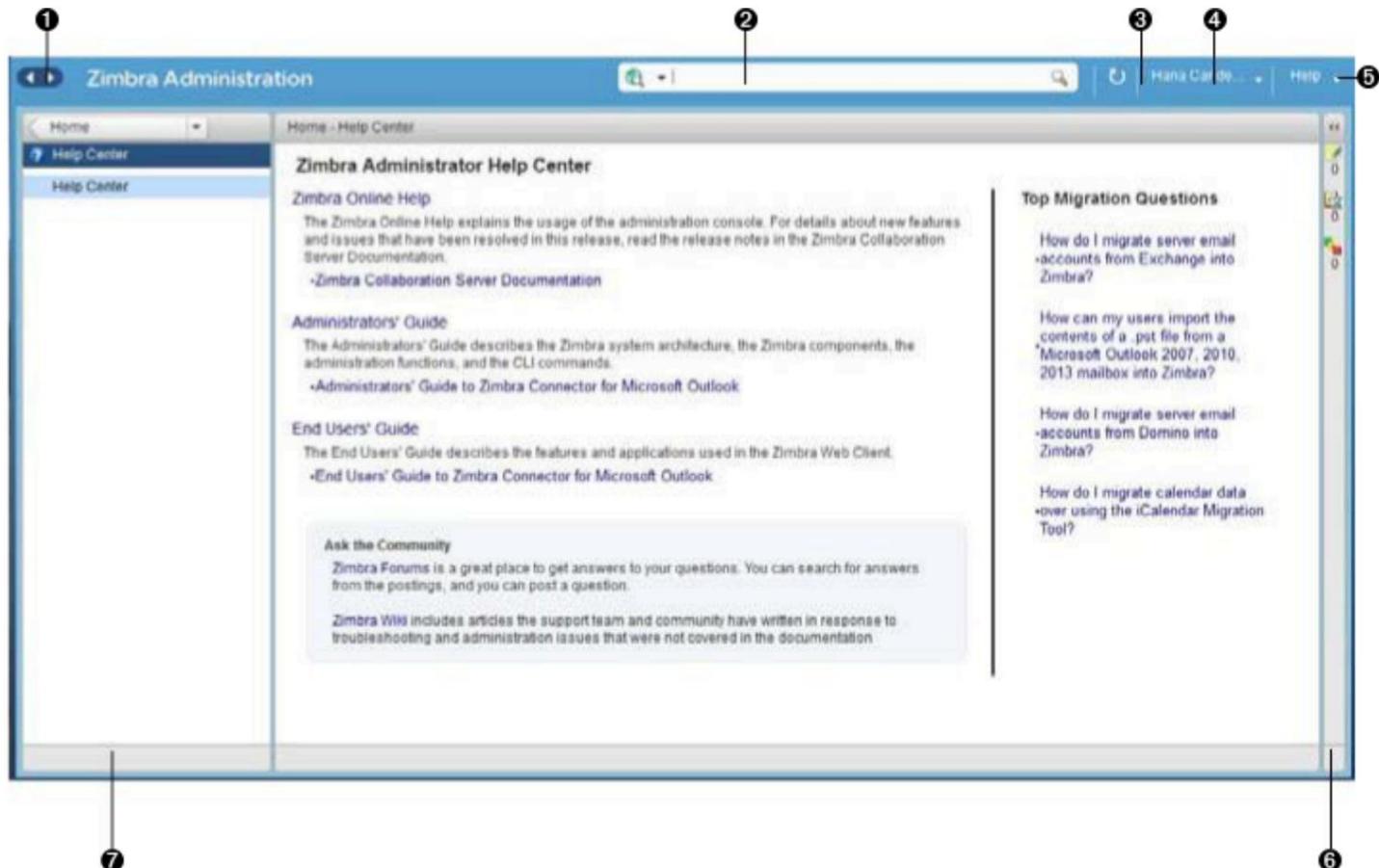
- 3.单击“搜索”。

出现“搜索”页面,其中包含根据您的条件进行的搜索的结果。

4. 在导航窗格中的“搜索">>“所有结果”中查看结果总数。

帮助中心界面

帮助中心是在线帮助和文档中可用资源的参考,您可以
使用帮助中心屏幕提供的链接进行访问。使用此页面还可以访问社区论坛和
查看专家对最热门移民问题的回答。



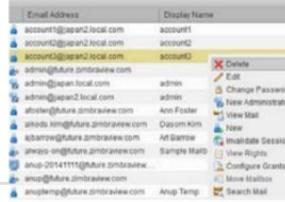
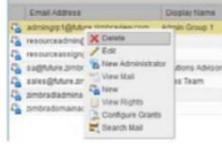
- <1> 转至上一页或下一页
- <2> 搜索
- <3> 屏幕刷新
- <4> 当前用户和注销选项
- <5>帮助
- <6> 状态窗格
- <7> 帮助中心导航窗格

协作者表中的工具

从导航窗格中选择一个类别通常会以表格形式显示所选类别的所有管理对象。所有表格均显示带标签的列,可在其中查看电子邮件地址、显示名称、状态、上次登录和说明 (如果已配置)等信息。

如果您需要更多信息或访问所选表条目的配置,表中的每一行都可以执行操作。

桌上行动 排	结果																
保持光标	显示选择的 ID 详细信息,类似于右侧的示例 (从帐户行调用)。	<table border="1"> <thead> <tr> <th>Email Address</th> <th>Display Name</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>account1@japan2.local.com</td> <td>account1</td> <td>Active</td> </tr> <tr> <td>account2@japan2.local.com</td> <td>account2@japan2.local.com</td> <td></td> </tr> <tr> <td>account3@japan2.local.com</td> <td>Mail Server: future.zimbraview.com</td> <td></td> </tr> <tr> <td>admin@future.zimbraview.com</td> <td></td> <td></td> </tr> </tbody> </table>	Email Address	Display Name	Status	account1@japan2.local.com	account1	Active	account2@japan2.local.com	account2@japan2.local.com		account3@japan2.local.com	Mail Server: future.zimbraview.com		admin@future.zimbraview.com		
Email Address	Display Name	Status															
account1@japan2.local.com	account1	Active															
account2@japan2.local.com	account2@japan2.local.com																
account3@japan2.local.com	Mail Server: future.zimbraview.com																
admin@future.zimbraview.com																	

桌上行动 排	结果	
右键单击	访问所选表格行的弹出菜单。典型表格的弹出菜单可能因行而异,如以下示例所示。	帐户和别名 :Dist 列表和资源:  

每日讯息

全局管理员可以创建管理员在登录管理控制台时查看的消息或每日消息 (MOTD)。

管理登录期间,MOTD 显示在管理控制台的左上角,类似于下面的示例。



该消息可以被关闭、替换或删除。

结束当天的信息

要从视图中删除消息,请单击消息内容旁边的“关闭” []

创建每日讯息

使用zimbraAdminConsoleLoginMessage属性 (按照本节中的指南)创建当天的单条消息,或者创建要显示的多条消息。

使用命令输入创建消息时,请始终在要显示的消息的开头和结尾放置双引号。

创建全局消息或特定域消息。

zmprov md <域> zimbraAdminConsoleLoginMessage “要显示的消息”

重击

创建多条消息显示:

zmprov md <域> +zimbraAdminConsoleLoginMessage “要显示的第二条消息”

重击

删除每日消息

使用zimbraAdminConsoleLoginMessage属性 (按照本节中的指南)删除当天的单条消息或删除多条消息。

使用命令输入删除消息时,请遵循以下准则进行单独或多次删除:

- 在属性前放置减号 (-),并在单个消息 ID 的开头和结尾放置双引号以便删除。
- 使用带有属性的单引号来删除所有消息。

删除特定消息:

zmprov md <域> -zimbraAdminConsoleLoginMessage “要显示的消息”

重击

删除所有消息:

zmprov md <域> zimbraAdminConsoleLoginMessage

重击

功能参考

本节提供了在管理控制台中导航时可以使用的功能的鸟瞰图,主题如下:

- GUI 路线图
- 弹出菜单选项
- 容器

GUI 路线图

下图提供了管理控制台 UI 的高级视图。

高层视角

管理控制台

用户界面

(not applicable)

- Accounts:**
New, New Administrator, Edit, Delete, Change Password, Invalidate Sessions, View Mail, Move Mailbox, View Rights, Configure Grants
- Aliases:**
New, New Administrator, Edit, Delete, Move Alias, Invalidate Sessions, View Mail, Move Mailbox, View rights, Configure Grants
- Distribution Lists:**
New, New Administrator, Edit, Delete, View Mail, View Rights, Configure Grants
- Resources:**
New, New Administrator, Edit, Delete, View Mail, View Rights, Configure Grants
- Class of Service <name>:**
New, Delete, Edit, Duplicate
- Domain:**
New, Delete, Edit, Configure GAL, Configure Authentication, View Accounts, Add a Domain Alias, Configure Grants
- Servers:**
Edit, Flush Cache, Enable Proxy, Disable Proxy
- Global Settings:**
Save, Download, Update License, Activate License, Manually Activate License
- Zimlets:**
Deploy, Undeploy, Toggle Status
- Admin Extensions**
Deploy, Undeploy
- Certificates**
Install Certificate, View Certificate
- Voice/Chat Service:**
New, Delete, Edit, Generate Session ID
- Rights:**
View
- Global ACL:**
Add, Delete, Edit

d (not applicable)

i

- All Results:**
Delete, Edit, Change Password, View Mail, Move Alias, Invalidate Sessions, Move Mailbox, Download
- Accounts:**
Delete, Edit, Change Password, View Mail, Move Alias, Invalidate Sessions, Move Mailbox, Download
- Domains:**
Delete, Edit, Change Password, View Mail, Move Alias, Invalidate Sessions, Move Mailbox, Download
- Distribution Lists:**
Delete, Edit, Change Password, View Mail, Move Alias, Invalidate Sessions, Move Mailbox, Download

iter (not applicable)

弹出菜单选项

您可以从导航窗格中的齿轮图标或主题中选择要对选定实体执行的选项

弹出菜单。

使用齿轮图标

如果与显示页面中的可选项目相关，则齿轮图标始终位于页面视图的右上角。

Class of Service

defaultExternal

ID: f27456a8-0c00-11d9-280a-286d93afea2g
Created: click to view operations you can perform from this page

General Information

Display name: defaultExternal
Description: The default external users COS
Notes:

Voice and Chat

Voice/Chat Service: Not set

要查看可用选项,请在导航窗格或页面视图中突出显示主题:在弹出窗口中,选项

不适用于您的选择的选项将被禁用 其余已启用的选项适用于您的选择。

以下示例演示了基于导航栏主题选择 (而非表格行) 的 Gear 选项

在同一页面视图中输入。

Highlighted selection

Manage

	Email Address	Display Name	Status	Last Login
1	admin@zimbra.com		Active	March 11, 2016 9:37:27 PM
2	anything@zimbra.com	d. sss	Active	Never logged in
3	john@zimbra.com	john	Active	March 2, 2016 10:37:23 PM

Gear options for the selection

Highlighted selection

Manage

	Email Address	Display Name	Status	Last Login
1	admin@zimbra.com		Active	March 11, 2016 9:37:27 PM
2	anything@zimbra.com	d. sss	Active	Never logged in
3	john@zimbra.com	john	Active	March 2, 2016 10:37:23 PM

Gear options for the selection

下表提供了齿轮图标派生的操作的高级视图,具体如下:

特定功能。

表 20. 齿轮图标操作

导航窗格 话题	选择	选项

导航窗格 话题	选择	选项 
家庭监控	服务器统计	看法
	邮件队列	冲洗
管理	帐户	新建、新管理员、编辑、删除、更改密码、使会话无效、查看邮件、移动邮箱、查看权限、配置授权
	别名	新建、新管理员、编辑、删除、移动别名、使无效会话、查看邮件、移动邮箱、查看权限、配置授权
	分发列表	新建、新管理员、编辑、删除、查看邮件、查看权限、配置授权
	资源	新建、新管理员、编辑、删除、查看邮件、查看权限、配置权限
配置	服务等级	新建、删除、编辑、复制
	域	新建、删除、编辑、配置 GAL、配置身份验证、查看账户,添加域别名,配置授权
	服务器	编辑、清除缓存、启用代理、禁用代理
	全局设置	保存、下载、更新许可证、激活许可证、手动激活许可证
	齐姆莱茨	部署、取消部署、切换状态
	管理扩展	部署、取消部署
	证书	安装证书、查看证书
	语音/聊天服务	新建、删除、编辑、生成会话 ID
	权利	看法
	全局 ACL	添加、删除、编辑
工具和 迁移	账户迁移删除任务、刷新、迁移向导	
	软件更新	保存,立即检查
	备份	查看、备份、恢复、配置、刷新

导航窗格	选择	选项
话题		
搜索	全部结果 帐户 别名 域 分发列表	删除、编辑、更改密码、查看邮件、移动别名、使无效 会话、移动邮箱、下载

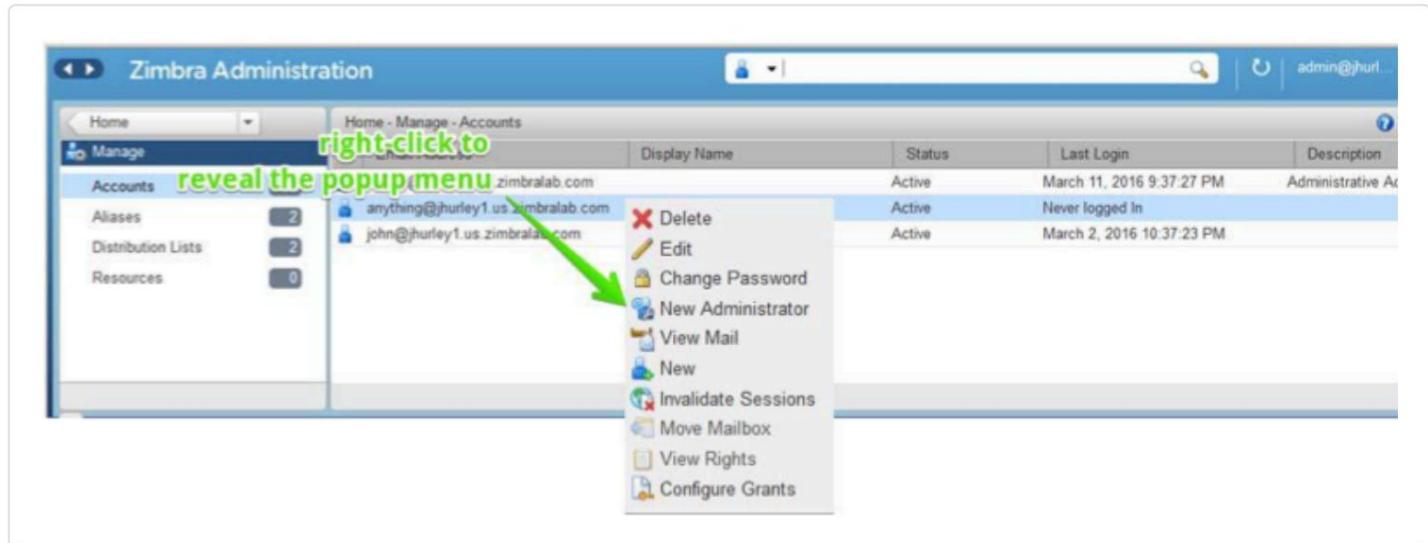
使用主题弹出菜单

您可以选择使用弹出菜单来访问要执行的选项：

导航窗格中没有弹出菜单。

以下示例演示了页面视图中特定选择所提供的弹出选项。

弹出选项示例.



容器

管理控制台按逻辑将各种配置选项分组为。适用于

这些容器内的配置选项列在管理控制台 UI 的高级视图中

容器

默认情况下，页面上的所有容器均处于打开状态（展开）。您可以选择关闭（折叠）容器 - 这可以

[释放页面视图中的额外空间 - 通过单击位于页面左上角的折叠/展开

容器。

]

Configure

Global Settings

General Information

Attachments

MTA

IMAP

POP

AS/AV

Free/Busy Interop

Themes

Advanced

Authentication

Retention Policy

Proxy

Backup/Restore

License

HSM

Home - Configure - Global Settings - MTA

Note: Settings only apply to servers that have the appropriate service(s) installed and enabled. Domains and classes of service override global settings.

▶ Authentication

▶ Network

▶ click to toggle between open | close

▼ Milter Server

Milter server bind port: 7026

Enable milter server

▶ Messages

▶ Policy Service Checks

▶ Protocol checks

▶ DNS checks

container is closed (collapsed)

Open (expanded) container

管理配置

Zimbra 组件在软件初始安装期间进行配置。安装后,您可以从管理控制台或使用 CLI 实用程序管理以下组件。

管理控制台提供了有关如何从管理控制台执行任务的帮助。如果该任务只能从 CLI 执行,请参阅Zimbra CLI 命令以获取有关如何使用 CLI 实用程序的说明。

全局配置

全局设置适用于 Zimbra 服务器中的所有帐户。它们最初在安装期间设置。您可以从管理控制台修改设置。

全局设置中设置的配置定义了以下对象的继承默认值:服务器、账户、COS 和域。如果在服务器中设置了这些属性,则服务器设置会覆盖全局设置。

管理控制台:

要配置全局设置,请导航至:

[主页](#)→[配置](#)→[全局设置](#)

配置的全局设置是:

- 默认域
- GAL 搜索返回的最大结果数。默认值 = 100。
- 不允许用户查看电子邮件附件和附件类型。
- 用于身份验证过程、外部传递的中继 MTA、DNS 查找和协议检查的配置。
- 垃圾邮件检查控制和防病毒选项用于检查收到的消息。
- 跨 Zimbra 协作服务器和第三方电子邮件服务器进行空闲/忙碌安排。
- 主题定制:修改颜色并添加您的徽标。
- 查看共享公文包文件夹时,外部访客登录时的公司名称显示配置。
- 备份默认目录和备份通知信息。
- 全局 SM 计划定义何时应将消息移动到二级存储空间。
- 查看当前 Zimbra 许可证信息、许可证更新,并查看创建的账户数量。

常规信息配置

管理控制台:

[主页](#)→[配置](#)→[全局设置](#)

使用常规信息屏幕可以查看和设置已安装和启用的服务器的全局参数。

服务器上定义的设置将覆盖 “常规信息”屏幕中配置的设置。

Home - Configure - Global Settings Help Save Close

Note: Settings only apply to servers that have the appropriate service(s) installed and enabled. Server settings override global settings.

General Information

Most results returned by GAL search:	100
Default domain:	future.zimbraview.com
Maximum number of scheduled tasks that can run simultaneously:	20
Sleep time between subsequent mailbox purges:	1 minutes
Maximum size of a file uploaded from the desktop (KB):	2504800
Admin help URL:	
Delegated admin help URL:	

1. 根据您的要求修改参数。
2. 从齿轮图标中,选择保存以使用您的设置。

表 一般信息参数

选项	描述
GAL 搜索返回的大多数结果	从 用户搜索。此值可以通过域设置： 域设置覆盖全局设置。 默认值 = 100。
默认域	用于对用户登录进行身份验证的域。
可运行的计划任务数量 同时地	用于从远程获取内容的线程数 数据源。 * 如果设置得太低,用户就无法获得他们的 来自外部来源的邮件经常被拉低。 * 如果设置得太高,服务器可能会被 下载此邮件且不为“主要”用户提供服务 要求。 默认值 = 20
后续邮箱清除之间的休眠时间	服务器应“休息”的时间长度 清除邮箱之间。如果邮件清除 计划设置为 0,则不会清除消息,即使 邮件、垃圾邮件和垃圾邮件的生存时间已设置。 默认 = 邮件清除计划每 1 分钟。

选项	描述
公文包文件上传的最大文件大小 (知识库)	可上传到公文包中的文件的最大大小。
管理员帮助 URL 委派管理员帮助 URL	可发送的电子邮件消息和附件的最大消息大小在主页→配置→全局设置→MTA页面的消息部分中配置。 要使用 Zimbra 协作帮助,您可以指定从管理控制台帮助

附件配置

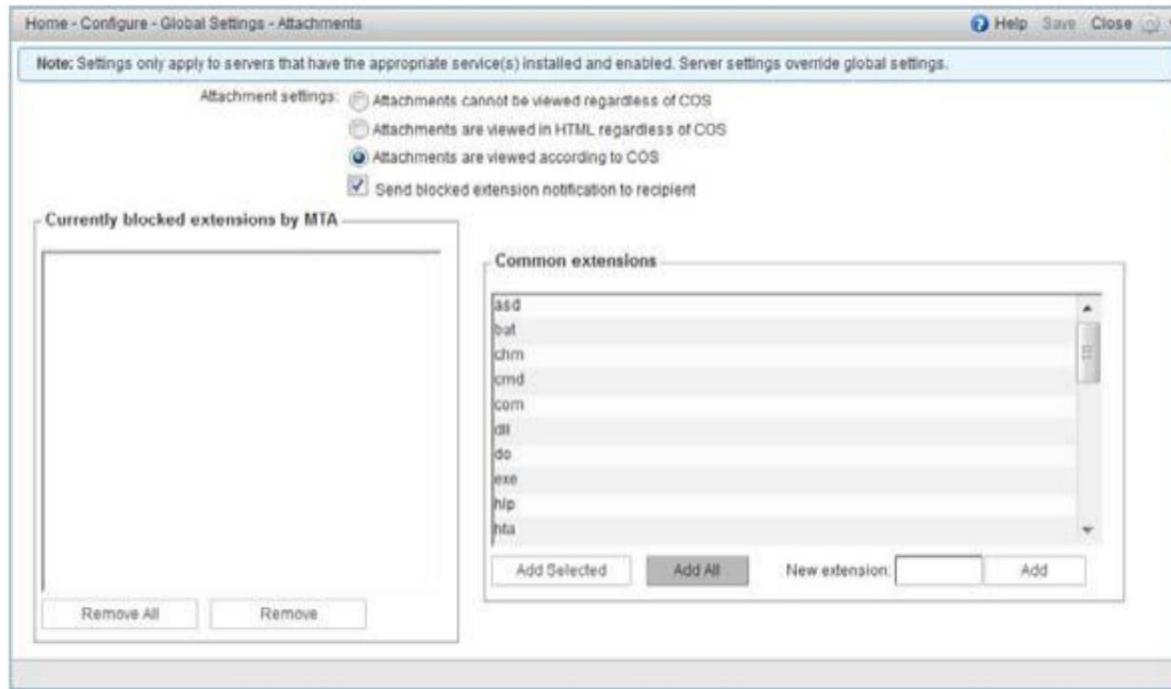
设置电子邮件附件规则

全局电子邮件附件设置允许您指定处理电子邮件附件的全局规则。

您还可以按 COS 和单个账户设置规则。当在全局设置中配置附件设置时,全局规则优先于 COS 和账户设置。

管理控制台:

主页→配置→全局设置→附件



有关此屏幕部分的信息,请参阅按文件类型阻止电子邮件附件。

表全局设置高级22.

选项	描述

选项	描述
无论 COS 如何,都无法查看附件	用户无法查看任何附件。此全局 可以设置防止病毒爆发 附件,因为无法打开任何邮件附件。
无论 COS 如何,附件均以 HTML 格式查看	电子邮件附件只能以 HTML 格式查看。 COS 可能有其他设置,但这个全局设置 覆盖 COS 设置。
附件按照 COS 查看	此全局设置规定 COS 设置以下规则 如何查看电子邮件附件
向收件人发送阻止扩展通知	

按文件类型阻止电子邮件附件

您还可以拒绝带有特定类型文件附件的邮件。您可以选择哪些文件类型是未经授权的
常见扩展列表。您还可以将其他扩展类型添加到列表中。带有这些文件类型的邮件
附件将被拒绝。默认情况下,收件人和发件人都会收到邮件已被阻止的通知。

如果您不想在消息被阻止时向收件人发送通知,您可以禁用此选项。

管理控制台:

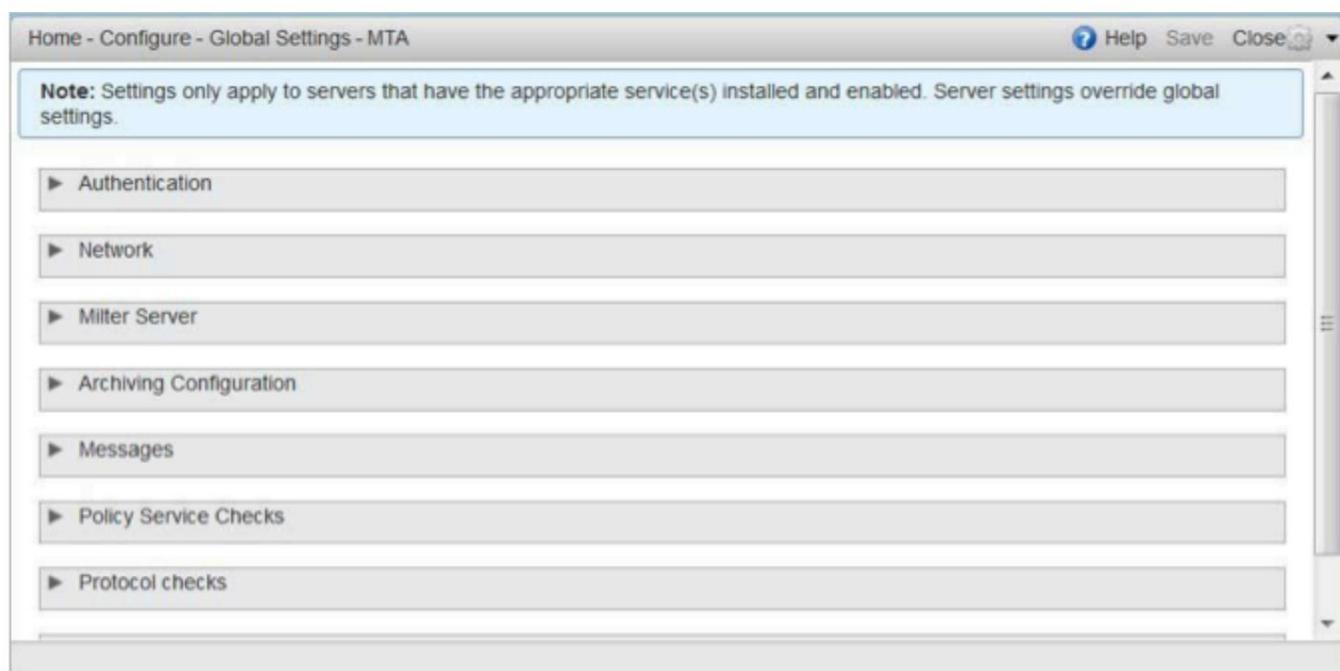
主页→配置→全局设置→附件

MTA 配置

使用 MTA 页面中的选项启用或禁用身份验证并配置中继主机名,最大值
消息大小、启用 DNS 查找、协议检查和 DNS 检查。

管理控制台:

主页→配置→全局设置→MTA



选项	描述
验证	<ul style="list-style-type: none"> 应启用身份验证,以支持移动 SMTP 身份验证用户,以便他们的电子邮件客户端可以与 Zimbra MTA 对话。 TLS 身份验证仅强制所有 SMTP 身份验证使用事务级别安全性以避免以明文形式传递密码。
网络	<ul style="list-style-type: none"> Web 邮件 MTA 主机名和 Web 邮件 MTA 端口。Web 服务器连接的 MTA 发送邮件。默认端口号为25。 外部投递的中继 MTA是中继主机名。这是 Postfix 所要投递到的 Zimbra MTA 中继非本地电子邮件。 如果您的 MX 记录指向垃圾邮件中继或任何其他外部非 Zimbra 服务器,请在入站 SMTP 主机名字段中输入该服务器的名称。此检查将域 MX 设置与 <code>zimbraInboundSmtpHostname</code> 设置 (如果已设置)进行比较。如果未设置此属性,则将域 MX 设置与 <code>zimbraSmtpHostname</code> 进行比较。 MTA 受信任网络。配置允许中继邮件的受信任网络。指定网络地址列表,以逗号和/或空格分隔。
军事服务器	<ul style="list-style-type: none"> 如果选中“启用 DNS 查找”,Zimbra MTA 将对收件人域的 MX 记录进行显式 DNS 查询。如果禁用此选项,请在中继 MTA 中设置中继主机以进行外部传递。 如果允许域管理员检查 MX 管理控制台中的记录已检查,域管理员可以检查 MX 记录他们的域名。
归档	<ul style="list-style-type: none"> 如果选中“启用 Milter 服务器”,则 Milter 将强制执行针对谁可以向分发列表发送电子邮件而设置的规则。
	<ul style="list-style-type: none"> 如果您安装了存档功能,您可以在这里进行配置。

选项	描述
消息	<ul style="list-style-type: none"> 设置可发送的邮件及其附件的最大邮件大小。 <p style="text-align: center;"> 设置 将文件上传至公文包,转到常规信息页面。</p>
	<ul style="list-style-type: none"> 您可以启用邮件的 X-Originating-IP 标头复选框。X-Originating-IP 标头信息指定服务器正在转发的电子邮件消息的原始发送 IP。
政策服务	<ul style="list-style-type: none"> 定制zimbraMtaRestriction (限制拒绝检查一些可疑的 SMTP 客户端)。
协议检查	<ul style="list-style-type: none"> 拒绝未经请求的商业电子邮件 (UCE),以控制垃圾邮件。
DNS 检查	<ul style="list-style-type: none"> 如果客户端的 IP 地址未知、问候语中的主机名未知或发件人的域未知,则拒绝邮件。 将其他电子邮件收件人限制添加到RBL 列表字段。 <p style="text-align: center;">可以从 Zimbra 打开或关闭 RBL (实时黑洞列表) CLI。</p>

全局 IMAP 和 POP 配置

使用 IMAP 和 POP 页面实现全球访问。

管理控制台：

主页→配置→全局设置→IMAP

主页→配置→全局设置→POP

当您更改 IMAP 或 POP 设置时,必须重新启动 Zimbra Collaboration 才能使更改生效。

可以从管理控制台 COS 高级页面设置 IMAP 和 POP3 轮询间隔。

默认 = 无论询问间隔。

如果设置了 IMAP/POP 代理,请确保端口号配置正确。

使用 POP3,用户可以检索存储在 Zimbra 服务器上的邮件并将新邮件下载到计算机。用户在“首选项”→“邮件”页面中的 POP 配置决定了如何下载和保存邮件。

使用域

安装过程中会识别一个域。您可以在安装后添加域。您可以从管理控制台管理以下域功能。

- 全局地址列表
- 验证
- 域的虚拟主机为用户登录建立默认域
- 用于 REST URL 的公共服务主机名,常用于共享。
- 域上可创建的最大帐户数
- 与 Microsoft Exchange 一起使用的空闲/忙碌互操作设置。
- 域名 SSL 证书

可以重命名域,并将所有帐户、分发列表、别名和资源地址更改为新域名。CLI 实用程序用于更改域名。请参阅重命名域。

域设置覆盖全局设置。

域常规信息配置

使用新建域向导设置本节中描述的选项。

管理控制台:

主页→2 设置域名→1. 创建域名…

The screenshot shows the 'New Domain' configuration dialog. On the left, a sidebar lists options: General Information (selected), GAL Mode Settings, SSO, Authentication Mode, Virtual Hosts, Advanced, Feature, Domain Configuration, and Complete. The main area is titled 'General Information' and contains fields for 'Domain name:' (with a required asterisk), 'Public service host name:', 'Public service protocol:' (dropdown menu), and 'Public service port:' (text input). Below these fields is a note: 'If your MX records point to a spam-relay or any other external non-zimbra server, enter the name of that server in "Inbound SMTP host name" field.' This note is enclosed in a light blue box with an info icon. Further down are fields for 'Inbound SMTP host name:', 'Description:', 'Default Class of Service:' (with placeholder 'enter search term'), 'Status:' (dropdown menu set to 'Active'), and 'Notes:' (text input). At the bottom right are buttons: 'Cancel', 'Previous', 'Next', and 'Finish'.

表新域一般信息 24.

选项	描述

选项	描述
域名 公共服务主机名	输入 REST URL 的主机名。这是常用于共享。请参阅设置公共服务主机
公共服务协议	从下拉字段中选择 HTTP 或 HTTPS。
公共服务端口	
入站 SMTP 主机名	如果您的 MX 记录指向垃圾邮件中继或任何其他外部非 Zimbra 服务器,输入服务器在这里。
描述	
默认服务等级	此 COS (针对域)自动分配给如果没有其他 COS,则在域上创建帐户放。

选项	描述
地位	<p>域状态为正常状态 ,用户可以登录并发送邮件。更改状态也会影响域中帐户的状态。</p> <p>域状态显示在域→常规页面。域状态可以设置如下：</p> <ul style="list-style-type: none"> 积极的 <ul style="list-style-type: none"> 活跃是域的正常状态。帐户可以创建并传递邮件。 如果帐户状态不同 设置比域设置 ,帐户状态覆盖 域名状态。 关闭 <ul style="list-style-type: none"> 当域状态标记为已关闭时 ,域上的账户登录将被禁用 ,邮件将被退回。已关闭状态将覆盖个人帐户状态设置。 已锁定 <ul style="list-style-type: none"> 当域名状态被标记为已锁定时 ,用户无法登录查看电子邮件 ,但电子邮件仍会发送到帐户。如果帐户状态被标记为维护或关闭 ,帐户状态将覆盖域状态设置。 环境。 <ul style="list-style-type: none"> 当域状态标记为维护时 ,用户无法登录 ,并且他们的电子邮件将在 MTA 中排队。如果帐户的状态设置标记为关闭 ,则帐户的状态将覆盖域状态设置。 暂停 <ul style="list-style-type: none"> 当域状态被标记为 “暂停”时 ,用户将无法登录 ,其电子邮件将在 MTA 中排队 ,并且无法创建、删除或修改帐户和分发列表。如果帐户的状态设置被标记为 “关闭” ,则帐户的状态将覆盖域状态设置。

设置公共服务主机名

您可以为每个域配置用于 REST URL 的公共服务主机名。这是共享电子邮件文件夹和公文包文件夹以及共享任务列表、地址簿和日历时使用的 URL。

当用户共享 Zimbra Collaboration 文件夹时,默认使用 Zimbra 服务器主机名和 Zimbra 服务主机名创建 URL。显示为https://server.domain.com/service/home/username/sharedfolder。属性生成如下:

- 主机名是 server.zimbraServiceHostname
- 协议由 server.zimbraMailMode 决定
- 端口是根据协议计算出来的

配置公共服务主机名时,将使用此名称代替服务器/服务名称,如https://publicservicename.domain.com/home/username/sharedfolder。要使用的属性为:

- zimbraPublicServiceHostname
- zimbra公共服务协议
- zimbra公共服务端口

您可以使用另一个 FQDN,只要该名称具有正确的 DNS 条目来在内部和外部指向“服务器”。

全局地址列表 (GAL) 模式配置

全局地址列表 (GAL) 是公司范围内的用户列表,可供电子邮件系统的所有用户使用。GAL 是邮件系统中常用的功能,它使用户能够按名字或姓氏查找其他用户的信息,而无需知道完整的电子邮件地址。

GAL 是针对每个域进行配置的。每个域的 GAL 模式设置决定了在何处执行 GAL 查找。

使用GAL 模式设置工具和您的域配置来定义全局地址列表。

管理控制台:

主页→2 设置域→1 创建域… → GAL 模式设置

表新域GAL 模式设置 25。

选项	描述
GAL 模式	<ul style="list-style-type: none"> 内部。Zimbra LDAP 服务器用于目录查找。 外部。外部目录服务器用于 GAL 查找。您可以为 GAL 配置多个外部 LDAP 主机。所有其他目录服务都使用 Zimbra LDAP 服务（配置、邮件路由等）。配置外部 GAL 时，您可以配置不同的搜索设置和同步设置。如果您的 LDAP 环境设置为通过设置 LDAP 缓存服务器来优化 LDAP 搜索，您可能需要配置不同的搜索设置，但用户也需要能够同步到 GAL。 两者皆有。内部和外部目录服务器均用于 GAL 查找。
GAL 搜索返回的大多数结果	<p>可显示的最大搜索结果数 一次 GAL 搜索中返回的结果。如果此值未定义 这里，系统将使用“全局设置”中定义的值。</p> <p>默认 = 100 个结果。</p>
GAL 同步帐户名称*	显示 galsync 名称和关联域的只读字段。
内部 GAL 的数据源名称	显示内部 加尔。
内部 GAL 轮询间隔	定义 GAL 同步帐户与 LDAP 服务器同步的频率（以天、小时、分钟或秒为单位）。首次同步到 LDAP 服务器时，LDAP 中的所有 GAL 联系人都会添加到 galsync 帐户的通讯簿中。在后续同步中，帐户会更新有关新联系人、修改的联系人和删除的联系人的信息。

使用 GAL 同步帐户更快地访问 GAL

创建内部或外部 GAL 时，将为域创建一个 GAL 同步帐户，如果您有多个邮箱服务器，则可以为域中的每个邮箱服务器创建一个 GAL 同步帐户。使用 GAL 同步帐户，用户可以更快地访问 GAL 中的自动完成名称。

当服务器上创建 GAL 同步帐户时，GAL 请求将定向到服务器的 GAL 同步帐户，而不是域的 GAL 同步帐户。GalSyncResponse 包含一个令牌，该令牌对 GAL 同步帐户 ID 和当前更改号进行编码。客户端存储此令牌，然后在下一个 GalSyncRequest 中使用它。用户使用他们最初同步的 GAL 同步帐户执行 GAL 同步。如果由于某种原因 GalSync 帐户不可用，则运行传统的基于 LDAP 的搜索。

GAL 同步帐户是系统帐户 ,不使用 Zimbra 许可证。

配置 GAL 同步帐户时,您将定义 GAL 数据源,联系人数据将从数据源同步到 GAL 同步帐户的通讯录。如果选择 “Both”模式,则会在帐户中为每个 LDAP 数据源创建一个通讯录。

GAL 同步的 GAL 轮询间隔决定了 GALSsync 帐户与 LDAP 服务器同步的频率。

同步间隔可以是 x 天、小时、分钟或秒。轮询间隔是针对每个数据源设置的。

当 GAL 同步帐户同步到 LDAP 目录时,LDAP 中的所有 GAL 联系人都会添加到该 GAL 的通讯簿中。在同步过程中,通讯簿会更新新联系人、修改的联系人和删除的联系人信息。您不应直接修改通讯簿。当 LDAP 将 GAL 同步到通讯簿时,您对通讯簿直接所做的更改将被删除。

您可以从管理控制台创建 GALSsync 帐户。与此功能相关的 CLI 是zmgsutil。

创建其他 GALSsync 帐户

当 Zimbra 配置了多个服务器时,您可以为每个服务器添加一个额外的 GAL 同步帐户。

管理控制台：

主页→配置→域

1. 选择要添加另一个 GAL 同步帐户的域。
2. 在齿轮图标中,选择配置 GAL。
3. 单击添加 GAL 帐户。
4. 在 GAL 同步帐户名称字段中,输入此帐户的名称。请勿使用默认名称。
5. 选择此帐户将适用的邮箱服务器。
6. 输入GAL 数据源名称。如果 GAL 模式为 BOTH,则输入内部和外部数据源名称。
GAL 和外部GAL。
7. 将GAL 轮询间隔设置为 GAL 同步帐户与 LDAP 服务器同步更新的频率。
- 8.单击 “完成” 。

更改 GAL 同步帐户名称

GAL 同步账户默认名称为galsync,配置 GAL 模式时可指定其他名称,GAL 同步账户创建后不可重命名,否则会导致数据同步失败。

要更改帐户名称,请删除现有的 GAL 同步帐户并为域配置新的 GAL。

管理控制台：

主页→配置→域

1. 选择您要更改 GAL 同步帐户名的域。
2. 在齿轮图标中,选择配置 GAL以打开配置向导并将 GAL 模式更改为内部。
请勿配置任何其他字段。单击 “完成” 。
3. 在域的账户内容窗格中,删除域的 galsync 账户。

4. 再次选择域并选择“配置 GAL”以重新配置 GAL。在“GAL 同步帐户名称”字段中，输入帐户名称。完成 GAL 配置并单击“完成”。新帐户将显示在“帐户内容”窗格中。

身份验证模式

身份验证是向目录服务器识别用户或服务器并根据用户登录时提供的用户名和密码信息向合法用户授予访问权限的过程。

根据每个域设置身份验证方法。

管理控制台：

主页→2 设置域→1 创建域…→身份验证模式

表 26. 新域身份验证模式

选项	描述
认证机制	<ul style="list-style-type: none"> 内部。内部身份验证使用 Zimbra 目录服务器用于域上的身份验证。选择“内部”时，无需其他配置。 外部 LDAP。用户名和密码是绑定到目录服务器的操作中提供的身份验证信息。您必须配置 LDAP URL、LDAP 过滤器并使用 DN 密码来绑定到外部服务器。 外部 Active Directory。用户名和密码是提供给 Active Directory 服务器的身份验证信息。您可以识别 Active Directory 域名和 URL。

虚拟主机

虚拟主机允许您在一台服务器上托管多个域名。一般域名配置不变。

当您创建虚拟主机时，它将成为用户登录的默认域；用户无需将域名指定为其用户名的一部分即可登录。

管理控制台：

主页→2 设置域名→1 创建域名…→虚拟主机

表新域虚拟主机 27。

选项	描述
添加虚拟主机	用于标识此域的虚拟主机的字母数字字符串。虚拟主机需要具有 A 记录的有效 DNS 配置。要从域中删除虚拟主机，请单击此向导屏幕中显示的主机名旁边的“删除”。

要打开 Zimbra Classic Web App 登录页面,用户需要输入虚拟主机名作为 URL 地址。例如, <https://mail.company.com>。

当 Zimbra 登录屏幕显示时,用户只需输入用户名和密码。身份验证请求会搜索具有该虚拟主机名的域。找到虚拟主机后,针对该域的身份验证就完成了。

设置账户限制

您可以限制域上可配置的帐户数量。可以在创建域时设置域可配置的最大帐户数量。您还可以编辑域配置来添加或更改该数量。

在管理控制台中,可以在帐户限制页面中为域设置此限制。如果未配置此页面,则不会对域设置任何限制。

资源、垃圾邮件和普通账户不计入此限制。

您不能超出 Zimbra Collaboration 许可证设置的账户限制。

当有多个服务类别 (COS) 可用时,您可以选择可以配置哪些服务类别以及可以将域中的多少个帐户分配给 COS。这在域的“帐户限制”页面中配置。使用的 COS 帐户类型数量会被跟踪。所有 COS 的限制不能超过为域设置的最大帐户数量。

分配给帐户的 COS 数量是可跟踪的。您可以从任何帐户的“常规信息”页面查看已分配的数量/剩余的数量。

重命名域

重命名域时,您实际上是在创建新域,将所有帐户移至新域并删除旧域。所有帐户、别名、分发列表和资源地址都将更改为新域名。LDAP 会更新以反映更改。

重命名域之前

- 确保为新域名在 DNS 中创建 MX 记录
- 确保您拥有该域名的可用且最新的完整备份

域名重命名后

- 将您为旧域名设置的外部引用更新为新域名。这可能包括发送到管理员邮箱的自动生成的电子邮件,例如备份会话通知。立即对新域名进行完整备份:

`zmprov -l rd [旧域名.com] [新域名.com]`

重击

域名重命名流程

当您运行此`zmprov`命令时,域重命名过程将经历以下步骤:

1. 旧域名状态更改为内部关闭状态,域名邮件状态为
 更改为暂停。用户无法登录,其电子邮件被 MTA 退回,并且无法创建、删除或修改帐户、日历资源和分发列表。
- 2.新域名创建 ,状态为关闭,邮件状态为暂停。
3. 帐户、日历资源、分发列表、别名和资源全部复制到新域。
4. LDAP 已更新以反映新的域地址。
- 5.旧域名被删除。
6. 新域名的状态更改为活动状态。新域名可以开始接受电子邮件。

添加域别名

域别名允许不同的域名指向单个域地址。例如,您的域是 ,但您希望用户拥有example.com的地址,您可以创建example.com作为domain.com地址的别名。向user@example.com发送邮件与向user@domain.com发送邮件相同。

域别名就像您的主域名一样,是一个域名。您必须拥有该域名并验证所有权,然后才能将其添加为别名。

管理控制台:

主页→配置→域,从齿轮图标中选择添加域别名。

启用对域免责声明的支持

免责声明是针对每个域设置的。升级时,现有的全局免责声明将转换为每个域上的域特定免责声明,以保留以前版本的行为。

可以使用以下步骤启用每个域免责声明支持:

- 1.创建一个新域 (例如example.com)和帐户 (例如user2@example.com) 。

```
$ zmprov cd example.com cb9a4846-6df1-4c18-8044-4c1d4c21ccc5 $ zmprov ca user2@example.com
test123 95d4caf4-c474-4397-83da-aa21de792b6a $ zmprov -l gaa user1@example.com user2@example.com
```

重击

2. 允许使用免责声明

```
$ zmprov mcf zimbraDomainMandatoryMailSignatureEnabled TRUE $ zmprov gcf
zimbraDomainMandatoryMailSignatureEnabled zimbraDomainMandatoryMailSignatureEnabled:
TRUE
```

重击

3. 为新域名添加免责声明

重击

```
$ zmprov md example.com
zimbraAmavisDomainDisclaimerText "文本免责声明"
zimbraAmavisDomainDisclaimerHTML "HTML 免责声明"

$ zmprov gd example.com zimbraAmavisDomainDisclaimerText zimbraAmavisDomainDisclaimerHTML # 名称 example.com
```

zimbraAmavisDomainDisclaimerHTML:HTML 免责声明
zimbraAmavisDomainDisclaimerText:文本免责声明

```
$ zmprov gd eng.example.com # 名称 eng.example.com
```

zimbraAmavisDomain免责声明文本
zimbraAmavisDomain免责声明HTML

a. 在第一个 MTA 上：

```
/opt/zimbra/libexec/zmaltermimeconfig -e example.com
```

重击

为域启用免责声明 :example.comm 正在为域 example.com 生成免责声明。

b. 在所有其他 MTA 上：

```
/opt/zimbra/libexec/zmaltermimeconfig
```

重击

- 为了进行测试,请从帐户 (例如user2@example.com)以 html 和纯文本格式发送一封电子邮件
- 为了验证,请检查收到的电子邮件是否有正确的 HTML 免责声明和纯文本免责声明。
- 禁用域 example.com

1. 在第一个 MTA 上,作为 Zimbra 用户：

```
/opt/zimbra/libexec/zmaltermimeconfig -d example.com
```

重击

2. 在所有附加 MTA 上：

```
/opt/zimbra/libexec/zmaltermimeconfig
```

重击

禁用域内电子邮件的免责声明

您可以启用同一域中个人之间的电子邮件不附加免责声明的选项。

将属性attachmentzimbraAmavisOutboundDisclaimersOnly设置为TRUE。

为了保持向后兼容性,此属性默认为FALSE。

禁用免责声明功能

通过将相关属性设置为FALSE ,可以完全删除对免责声明的支持。

```
zmprov mcf zimbraDomainMandatoryMailSignatureEnabled FALSE
```

重击

域中的 Zimlets

所有已部署的 Zimlet 都显示在域的 Zimlet 页面中。如果您不想让域中的用户使用所有已部署的 Zimlet,请从列表中选择可用于域的 Zimlet。

这将覆盖 COS 或帐户中的 Zimlet 设置。

管理服务器设置

服务器是安装了一个或多个 Zimbra 服务包的机器。在安装过程中,Zimbra 服务器会自动在 LDAP 服务器上注册。

在管理控制台中,您可以查看所有配置了 Zimbra 软件的服务器的当前状态,并且可以编辑或删除现有服务器记录。您无法将服务器直接添加到 LDAP。必须使用 Zimbra Collaboration 安装程序来添加新服务器,因为安装程序包旨在在安装时注册新主机。

可以从管理控制台的“配置服务器”链接查看特定服务器的服务器设置包括:

- 有关服务主机名、LMTP 公布名称和绑定地址的一般信息,以及可同时处理数据源导入的线程数。
- 已启用服务的列表。您可以禁用或启用这些服务。
- 为服务器启用身份验证类型,设置与全局不同的 Web 邮件 MTA 主机名。设置用于外部传递的中继 MTA,并启用 DNS 查找(如果需要)。启用 Milter 服务器并设置绑定地址。
- 启用 POP 和 IMAP 并设置服务器的端口号。如果设置了 IMAP/POP 代理,请确保端口号配置正确。
- 索引和消息量配置。设置 SM 策略。
- IP 地址绑定。如果服务器有多个 IP 地址,IP 地址绑定允许您指定要绑定到哪个接口。
- 如果配置了代理,则进行代理设置。
- 备份和恢复服务器的配置。当为服务器配置备份和恢复时,这将覆盖全局备份和恢复设置。

如果服务器配置中未设置这些值,则服务器将继承全局设置。可以从全局配置继承的设置包括 MTA、SMTP、IMAP、POP、防病毒和反垃圾邮件配置。

常规服务器设置

常规信息页面包含以下配置信息:

- 服务器显示名称和描述字段
- 服务器主机名
- LMTP 信息包括公布的名称、绑定地址以及可同时处理数据源导入的线程数。

默认 = 20 个线程。

- 清除设置:服务器管理邮件清除计划。您可以从管理控制台、全局设置或服务器设置或常规信息页面配置服务器在清除邮箱之间应“休息”的时间长度。

默认 = 消息清除每分钟运行一次。

安装反向代理时,代理服务器和后端邮箱服务器之间的通信必须以纯文本形式显示。选中“此服务器是反向代理查找目标”会自动设置以下参数:

```
zimbraImapCleartextLoginEnabled TRUE
zimbraReverseProxyLookupTarget 真实
zimbraPop3CleartextLoginEnabled 真
```

注释文本框可用于记录您想要保存的详细信息。

更改 MTA 服务器设置

管理控制台:

主页→配置→服务器→ 服务器 →大都会运输署

MTA 页面显示以下设置:

- 已启用身份验证。

启用 SMTP 客户端身份验证,以便用户可以进行身份验证。只有经过身份验证的用户或来自受信任的用户网络允许中继邮件。启用 TLS 身份验证后,强制所有 SMTP 身份验证使用传输层安全性 (SSL 的后继者)可避免以明文形式传递密码。

- 网络设置,包括 Web 邮件 MTA 主机名、Web 邮件 MTA 超时、外部中继 MTA 传递、MTA 可信网络 ID、以及为服务器启用 DNS 查找的能力。
- 军事服务器。

如果选中“**启用邮件服务器**”,邮件服务器将强制执行为谁可以向服务器上的分发列表。

设置 IP 地址绑定

如果服务器有多个 IP 地址,您可以使用 IP 地址绑定来指定要使用的特定 IP 地址想要绑定到特定服务器。

管理控制台:

主页→配置→服务器→ 服务器 → IP 地址绑定

表 28. IP 地址绑定

选项	描述
Web 客户端服务器 IP 地址	HTTP 服务器监听的接口地址
Web 客户端服务器 SSL IP 地址	HTTPS 服务器监听的接口地址
Web 客户端服务器 SSL 客户端证书 IP 地址	HTTPS 服务器接受的接口地址 客户端证书监听
管理控制台服务器 IP 地址	管理员控制台接口地址 HTTPS 服务器监听

管理 Zimbra 的 SSL 证书

证书是用于不同主机或客户端与服务器之间安全通信的数字身份。

证书用于证明某个站点归您所有。

可以使用两种类型的证书：自签名证书和商业证书。

- 自签名证书是由其创建者自己签名的身份证书。

您可以使用证书安装向导生成新的自签名证书。当您使用自签名证书并想要更改到期日期时，这很有用。自签名证书通常用于测试。

默认值 = 1825 天（5 年）

- 商业证书由证书颁发机构 (CA) 颁发，证明证书中包含的公钥属于证书中注明的组织（服务器）。

安装 Zimbra Collaboration 时，会自动安装自签名证书，可用于测试 Zimbra Collaboration。在生产环境中使用 Zimbra Collaboration 时，应安装商业证书。

自签名环境中的 ZCO 用户将遇到有关连接安全性的警告，除非将根 CA 证书添加到客户端的 Windows 证书存储中。请参阅 Zimbra

[维基百科](https://wiki.zimbra.com/wiki/Main_Page) (https://wiki.zimbra.com/wiki/Main_Page) 文章 [ZCO 连接安全](https://wiki.zimbra.com/wiki/ZCO_Connection_Security) (https://wiki.zimbra.com/wiki/ZCO_Connection_Security) 了解更多信息。

安装证书

要生成证书签名请求 (CSR)，您需要填写包含域、公司和国家/地区详细信息的表单，然后使用 RSA 私钥生成 CSR。您可以将此文件保存到计算机并将其提供给商业证书授权人。

要获得商业签名的证书，请使用管理控制台中的 Zimbra 证书向导生成 RSA 私钥和 CSR。

管理控制台：

主页 → 1 开始 → 2. 安装证书

使用安装证书表中的指南为您的证书设置参数。

表安装证书 29.

选项	描述
通用名称 (CN)	安全访问您的网站时应使用的确切域名。您要使用通配符通用名称吗？如果您想使用单个证书管理服务器上单个域上的多个子域，请选中此框。通用名称字段中添加了一个星号 (*)。
国家名称 (C)	您希望证书显示为我们公司所在地的国家名称
州/省 (ST)	您希望证书显示为公司所在地的州/省。
城市 (左)	您希望证书显示为您的公司所在地的城市。

选项	描述
组织名称 (O)	您的公司名称
组织单位 (OU)	单位名称（如适用）
主题备用名称 (SAN)	<p>如果您要使用 SAN，则输入必须是有效的域名。使用 SAN 时，会将域名与通用名称进行比较，然后与 SAN 进行比较以查找匹配项。您可以创建多个 SAN。在此处输入备用名称时，客户端会忽略通用名称并尝试匹配服务器名称</p> <p>更改为其中一个 SAN 名称。</p>

从 Zimbra 服务器下载 CSR 并将其提交给证书颁发机构，例如 VeriSign 或 GoDaddy。

他们颁发数字签名的证书。

收到证书后，再次使用证书向导在 Zimbra Collaboration 上安装证书。安装证书后，必须重新启动服务器才能应用证书。

查看已安装的证书

您可以查看当前部署的证书的详细信息。详细信息包括证书主体、颁发者、有效期和主体备用名称。

管理控制台：

主页→配置→证书→ zm主机名

显示不同 Zimbra 服务（例如 LDAP、mailboxd、MTA 和代理）的证书。

维护有效证书

保持 SSL 证书有效很重要，以确保客户端和环境正常运行，因为如果证书过期，Zimbra 系统可能会无法运行。您可以从 Zimbra 管理员控制台查看已部署的 SSL 证书，包括其有效期。建议定期检查证书，以便您知道它们何时过期并保持其有效性。

为域安装 SSL 证书

您可以在 Zimbra Collaboration 服务器上为每个域安装 SSL 证书。必须在 Zimbra Collaboration 上安装 Zimbra Proxy 并正确配置以支持多个域。对于每个域，都会使用虚拟域名和 IP 地址配置虚拟主机名和虚拟 IP 地址。

每个域都必须颁发一个签名的商业证书，证明证书中包含的公钥属于该域。

配置 Zimbra 代理虚拟主机名和 IP 地址。

```
zmprov md <域> +zimbraVirtualHostName {domain.example.com} +zimbraVirtualIPAddress {1.2.3.4}
```

BASH

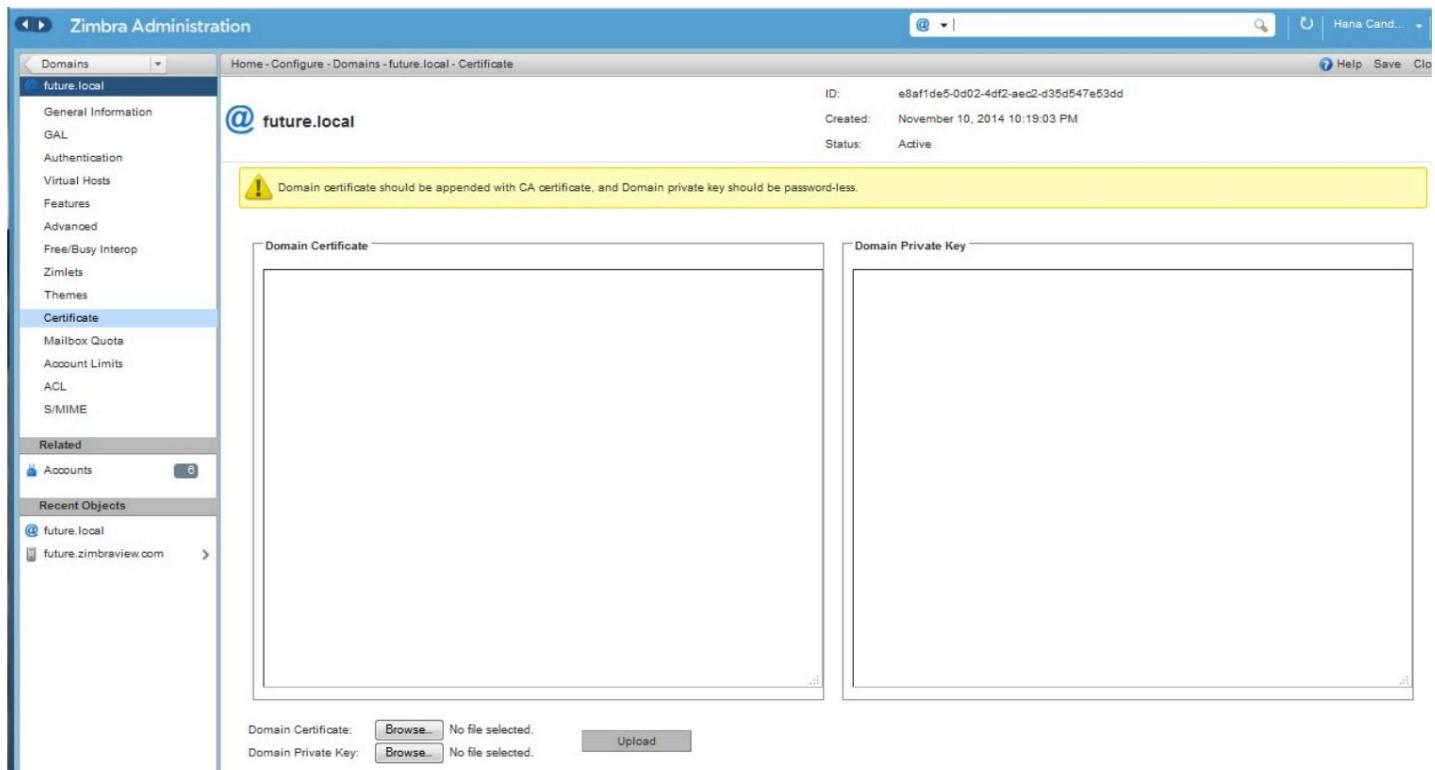
虚拟域名需要具有 A 记录的有效 DNS 配置。

编辑域的证书：

管理控制台：

主页→1开始→2.安装证书

将域名颁发的签名商业证书和私钥文件复制到所选域名的域名证书部分。



1. 从您的域名开始,按降序复制根证书和中间证书
证书。这样就可以验证完整的证书链。

2. 在保存证书之前,从私钥中删除所有密码（密码短语）。

有关如何删除密码的详细信息,请咨询商业证书提供商。

3.单击上传。

域证书部署到/opt/zimbra/conf/domaincerts

使用 DKIM 验证电子邮件消息

域密钥识别邮件 (DKIM) 定义了一种域级身份验证机制,让您的组织负责以收件人可以验证的方式传输电子邮件。您的组织可以是原始发送站点或中介。您的组织的声誉是评估是否信任邮件传递的基础。

您可以将 DKIM 数字签名添加到外发电子邮件中,将邮件与您组织的域名关联。您可以为 Zimbra 托管的任意数量的域启用 DKIM 签名。并非所有域都必须启用 DKIM 签名才能使用此功能。

DKIM 定义了一种电子邮件身份验证机制,使用

- 域名标识符
- 公钥加密
- 基于DNS的公钥发布服务。

DKIM 签名已添加到电子邮件消息头字段。头信息类似于以下内容
例子。

```
DKIM 签名 a=rsa-sha1; q=dns;
d=example.com;
我=用户@eng.example.com;
s=jun2021.eng;c=轻松/简单;
t=1117574938; x=1118006938;
h=从 :至 :主题:日期;
b=zdvyOfAKCdLXdJoc9G2q8LoXSIEniSbav+yuU4zGeeruD00lszzVoG4ZHRNiyzR
```

成功验证 DKIM 签名的接收者可以使用签名者的信息作为程序的一部分来
限制垃圾邮件、欺骗、网络钓鱼或其他不良行为。

配置 Zimbra Collaboration 进行 DKIM 签名

DKIM 对外发邮件的签名是在域级别完成的。

要设置 DKIM,您必须运行 CLI zmdkimkeyutil 来生成 DKIM 密钥和选择器。然后更新
带有选择器 (即公钥) 的 DNS 服务器。

1. 登录 Zimbra 服务器并以 zimbra 身份执行下列操作：

```
/opt/zimbra/libexec/zmdkimkeyutil -a -d <example.com>
```

重击

将显示必须为域添加到 DNS 服务器的公共 DNS 记录数据。公钥
DNS 记录显示为 DNS TXT 记录,必须将其添加到域的 DNS 服务器。

可选。要指定新密钥的位数,请在命令行中包含 -b , -b <#####>不添加-b
,默认设置为 2048 位。

。如果你

DKIM 数据已添加到域 example.com 的 LDAP,选择器为 B534F5FC-EAF5-11E1-A25D-
54A9B1B23156

输入 DNS 的公共签名：

```
B534F5FC-EAF5-11E1-A25D-54A9B1B23156._domainkey IN TXT
"v=DKIM1;k=rsa;
p=MIGfMA0GCSqSIB3DQEBAQUAA4GNADCBiQKBgQC+yChjGL/mJXEVRZnxZL/VqaN/Jk9VllvIOTkKgwLSFtVsKC69kV
aUDDb3zkbJ6qpswjOCO+0eGJZFA4aB4BQjFBHbl97vgNnpJq1sV3QzRfHrN8X/gdhvfKSlwSDFFl3DHewKDWNcCzBkN
f5wHt5ujeavz2XogL8HfeL0bTwIDAQA B ; ----- DKIM B534F5FC-EAF5-11E1-A25D-54A9B1B23156
示例.com
```

生成的 DKIM 数据作为域 LDAP 条目的一部分存储在 LDAP 服务器中。

2. 与您的服务提供商合作,使用 DKIM DNS 文本记录更新域的 DNS。
3. 重新加载 DNS 并验证 DNS 服务器是否返回 DNS 记录。
4. 验证公钥与私钥是否匹配。请参阅-d的标识符表

, -s , 和-x描述。

```
/opt/zimbra/common/sbin/opendkim-testkey -d <example.com> -s <0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB> -x /opt/zimbra/conf/
opendkim.conf
```

重击

表标识符0.

范围	描述
----	----

范围	描述
-d	域名
-s	选择器名称
-x	配置文件名称。

更新域的 DKIM 数据

当 DKIM 密钥更新时,DNS 服务器必须重新加载新的 TXT 记录。

好的做法是将之前的 TXT 记录保留在 DNS 中一段时间,以便之前的电子邮件使用以前的密钥签名的仍然可以被验证。

登录 Zimbra 服务器并以 zimbra 身份执行下列操作:

```
/opt/zimbra/libexec/zmdkimkeyutil -u -d <example.com>
```

重击

可选。要指定新密钥的位数,请在命令行中包含-b , -b <#####>添加-b

。如果你不

,默认设置为 2048 位。

1. 与您的服务提供商合作,使用 DKIM DNS 文本记录更新域的 DNS。

2. 重新加载 DNS 并验证 DNS 服务器是否返回 DNS 记录。

3. 验证公钥是否与私钥匹配:请参阅标识符表中的-d

, -s , 和-x描述。

重击

```
/opt/zimbra/common/sbin/opendkim-testkey -d <example.com> -s <0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB> -x /opt/zimbra/conf/opendkim.conf
```

从 Zimbra 中删除 DKIM 签名

删除 DKIM 签名会从 LDAP 中删除 DKIM 数据,并且新电子邮件将不再签名域。从域中删除 DKIM 时,最好将之前的 TXT 记录保留在 DNS 中以供一段时间,以便仍然可以验证使用先前的密钥签名的电子邮件。

使用以下命令语法删除该文件:

```
/opt/zimbra/libexec/zmdkimkeyutil -r -d example.com
```

重击

检索域的 DKIM 数据

使用以下命令语法查看域、选择器、私钥存储的 DKIM 信息,公开签名及身份:

```
/opt/zimbra/libexec/zmdkimkeyutil -q -d example.com
```

重击

反垃圾邮件设置

Zimbra 使用 SpamAssassin 来控制垃圾邮件。SpamAssassin 使用预定义规则以及贝叶斯数据库来邮件评分。Zimbra 以百分比值来评估垃圾邮件。标记为垃圾邮件的邮件在 33%-75% 之间发送到用户的垃圾邮件文件夹。超过 75% 的邮件不会被发送给用户,而是会被丢弃。