

| 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。

您可以更改反垃圾邮件设置。

管理控制台

主页→配置→全局设置→AS/AV

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

Spam checking Settings

Note: Changes to settings require amavisd restart in order to take effect.

| | |
|-----------------|----|
| Kill percent: | 75 |
| Tag percent: | 33 |
| Subject prefix: | |

Antivirus Settings

| | |
|--------------------------------|-------------------------------------|
| Definition update frequency: | 2h |
| Block encrypted archives | <input checked="" type="checkbox"/> |
| Send notification to recipient | <input checked="" type="checkbox"/> |

1. 在反垃圾邮件字段中,根据您的要求输入适当的参数。

2. 从齿轮图标中,选择保存以使用您的设置。

表 反垃圾邮件 31.

| 选项 | 描述 |
|-------|---|
| 击杀率 | 被视为垃圾邮件并因此无法投递的邮件百分比。 默认值 = 75% |
| 标签百分比 | 将邮件视为垃圾邮件 (应被递送到垃圾邮件文件夹) 的百分比。 默认值 = 33% |
| 主题前缀 | 添加到标记为垃圾邮件的邮件主题行的文本字符串。 |

当邮件被标记为垃圾邮件时,该邮件将被递送到收件人的垃圾文件夹。用户可以查看垃圾文件夹中未读邮件的数量,并可以打开垃圾文件夹查看标记为垃圾邮件的邮件。如果您启用了反垃圾邮件训练过滤器,当用户在垃圾文件夹中添加或删除邮件时,他们的操作有助于训练垃圾邮件过滤器。

可以从 Zimbra CLI 在 SpamAssassin 中打开或关闭 RBL (实时黑洞列表)。

反垃圾邮件训练过滤器

默认启用自动垃圾邮件训练过滤器,并创建两个反馈系统邮箱用于接收邮件通知。

- 垃圾邮件培训用户,针对未被标记为垃圾邮件但应该被标记为垃圾邮件的邮件。
- 非垃圾邮件 (称为普通邮件) 培训用户处理那些被标记为垃圾邮件但不应该被标记为垃圾邮件的邮件。

这些培训帐户的邮箱配额和附件索引已禁用。禁用配额可防止邮箱已满时邮件被退回。

反垃圾邮件过滤器的运作效果取决于识别哪些邮件被视为垃圾邮件。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。

安装 Zimbra 后，仅在第一个 MTA 上配置垃圾邮件/非正常邮件清理过滤器。Zimbra 垃圾邮件训练工具 zmtrainsa 配置为自动检索这些邮件并训练垃圾邮件过滤器。zmtrainsa 脚本通过 crontab 作业启用，以将邮件提供给 SpamAssassin 应用程序，从而使 SpamAssassin 能够“了解”哪些迹象可能意味着垃圾邮件或非正常邮件。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。

在新的 MTA 服务器上进行此项设置

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

重击

禁用垃圾邮件训练邮箱

Zimbra 默认所有用户在垃圾邮件文件夹中添加或删除项目时都可以提供反馈。

如果您不希望用户训练垃圾邮件过滤器，您可以禁用此功能。

1. 修改全局配置属性 ZimbraSpamIsSpamAccount 和 ZimbraSpamIsNotSpamAccount

2. 从属性中删除账户地址。

```
zmprov mcf ZimbraSpamIsSpamAccount    zmprov mcf  
ZimbraSpamIsNotSpamAccount
```

重击

修改这些属性时，标记为垃圾邮件或非垃圾邮件的邮件不会被复制到垃圾邮件训练邮箱。

手动训练垃圾邮件过滤器

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、单词或垃圾邮件中常见的短字符序列的数据库。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，这些消息用于训练垃圾邮件过滤器。请确保添加足够多的消息样本以获得准确的分数。要确定是否将消息标记为垃圾邮件，必须至少识别 200 条已知垃圾邮件和 200 条已知正常邮件。

保护别名域免受反向散射垃圾邮件的侵害

为了降低反向散射垃圾邮件的风险，您可以运行运行 Zimbra 访问策略守护进程的服务，该服务专门针对别名域验证 RCPT To : 内容。

有关创建域别名的信息,请参阅Zimbra wiki (<https://wiki.zimbra.com>)文章管理域 (https://wiki.zimbra.com/wiki/Managing_Domains)。

1.设置后缀LC键。

`zmlocalconfig -e postfix_enable_smtpd_policyd=yes`

重击

2. 定义 MTA 限制。

`zmprov mcf +zimbraMtaRestriction "check_policy_service unix:private/policy"`

重击

设置postfix_policy_time_limit键是因为默认情况下 Postfix spawn(8) 守护进程会在 1000 秒后终止其子进程。对于只要 SMTP 客户端连接到 SMTP 进程就可能运行的策略守护进程而言,这个时间太短了。

禁用 Postfix 策略守护进程

禁用 SMTPD 策略。

`zmlocalconfig -e postfix_enable_smtpd_policyd=no`

重击

管理控制台：

主页→配置→全局设置→ MTA

定义策略限制。设置电子邮件收件人限制可以在 MTA 中打开或关闭实时黑洞列表和实时右侧阻止/黑名单。

对于协议检查,可以启用以下三种 RBL:

- 姓名
- 客户端必须使用完全限定的主机名进行欢迎 - `rejection_non_fqdn_hostname`
- 发件人地址必须完全合格 - `rejection_non_fqdn_sender`

问候语中的主机名违反了 RFC - `Reject_invalid_host`

`zmprov mcf -zimbraMtaRestriction "check_policy_service unix:private/policy"`

重击

还可以设置以下 RBL。

- `rejection_rbl_client cbl.abuseat.org`
- `拒绝_rbl_client bl.spamcop.net`
- `拒绝_rbl_client dnsbl.sorbs.net`
- `拒绝_rbl_client`

作为收件人限制的一部分,您还可以使用`rejection_rbl_client <rbl hostname>`选项。

管理控制台：

主页→配置→全局设置→ MTA → DNS 检查

使用 MTA 配置中的 DNS 工具来定义限制列表。

| ▼ DNS checks | |
|---|--------------------------|
| Client's IP address (reject_unknown_client_hostname) | <input type="checkbox"/> |
| Hostname in greeting (reject_unknown_reverse_client_hostname) | <input type="checkbox"/> |
| Sender's domain (reject_unknown_sender_domain) | <input type="checkbox"/> |
| Client must greet with a resolving hostname (reject_unknown_helo_hostname) | <input type="checkbox"/> |
| List of Client RBLs: | <input type="text"/> |
| | Add |
| List of Client RHSBLs: | <input type="text"/> |
| | Add |
| List of Reverse Client RHSBLs: | <input type="text"/> |
| | Add |
| List of Sender RHSBLs: | <input type="text"/> |
| | Add |

有关当前 RBL 的列表,请参阅DNS 黑名单比较 (https://en.wikipedia.org/wiki/Comparison_of_DNS_blacklists)文章。

使用 CLI 添加 RBL

1. 查看当前的RBL。

```
zmprov gacf zimbraMta限制
```

重击

2. 添加新的 RBL:在同一命令条目中列出现有 RBL 和新添加的 RBL。对于 2 个单词的 RBL 名称,在条目中用引号将名称括起来。

```
zmprov mcf zimbraMtaRestriction [RBL 类型]
```

重击

示例 6. 添加所有可能的限制

```
zmprov mcf \
zimbraMtaRestriction 拒绝_无效_主机名 \ zimbraMtaRestriction 拒绝_非-
fqdn_主机名 \ zimbraMtaRestriction 拒绝_非_fqdn_发送者 \
zimbraMtaRestriction “拒绝_rbl_客户端 cbl.abuseat.org” \
zimbraMtaRestriction “拒绝_rbl_客户端 bl.spamcop.net” \ zimbraMtaRestriction “拒绝_rbl_
客户端 dnsbl.sorbs.net” \ zimbraMtaRestriction “拒绝_rbl_客户端 sbl.spamhaus.org”
```

重击

为标记为垃圾邮件和白名单的邮件设置全局规则

当您使用第三方应用程序在 Zimbra 接收邮件之前过滤垃圾邮件时,Zimbra 全局规则是将所有被第三方标记为垃圾邮件的邮件发送到垃圾邮件文件夹。这包括被识别为垃圾邮件且被识别为白名单的邮件。

如果您不希望被标识为白名单的邮件被发送到垃圾邮件文件夹,您可以配置zimbraSpamWhitelistHeader和zimbraSpamWhitelistHeaderValue以将这些邮件传递到用户的邮箱。此全局规则与 Zimbra MTA 垃圾邮件过滤规则无关。邮件仍会通过用户的过滤规则。

要在邮件中搜索白名单标头：

zmprov mcf zimbraSpamWhitelistHeader <X-Whitelist-Flag>

重击

要设置值：

zmprov mcf zimbraSpamWhitelistHeaderValue <第三方白名单消息值>

重击

防病毒设置

安装 Zimbra 软件后,每台服务器都会启用防病毒保护。防病毒软件配置为将已识别为带有病毒的邮件发送到病毒隔离邮箱。将向收件人发送电子邮件通知,告知他们邮件已被隔离。隔离邮箱邮件有效期设置为 7 天。

从管理控制台,您可以指定在 Zimbra Collaboration 中要如何积极地过滤垃圾邮件。

管理控制台：

主页→配置→全局设置→AS/AV

Home - Configure - Global Settings - AS/AV

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

Spam checking Settings

Note: Changes to settings requires amavisd restart in order to take effect.

| | |
|-----------------|----|
| Kill percent: | 75 |
| Tag percent: | 33 |
| Subject prefix: | |

Antivirus Settings

| | |
|--------------------------------|-------------------------------------|
| Definition update frequency: | 2h |
| Block encrypted archives | <input checked="" type="checkbox"/> |
| Send notification to recipient | <input checked="" type="checkbox"/> |

1. 在防病毒字段中,根据您的要求输入适当的参数。

2. 从齿轮图标中,选择保存以使用您的设置。

表防病毒 32。

| 选项 | 描述 |
|----|----|
| | |

| 选项 | 描述 |
|----------|--|
| 定义更新频率 | 默认情况下,Zimbra MTA 每两小时检查一次 ClamAV 是否有新的防病毒更新。频率可以设置为 1 到 24 小时之间。 |
| 阻止加密档案 | 限制加密文件,例如受密码保护的压缩文件。 |
| 发送通知给收件人 | 警告邮件内容含有病毒且无法送达。 |

在 Zimbra Collaboration 安装期间,会配置防病毒警报的管理员通知地址。默认设置是设置管理员帐户来接收通知。当发现病毒时,会自动向该地址发送通知。

通过 HTTP 从 ClamAV 网站获取更新。

Zimbra 空闲/忙碌日历安排

空闲/忙碌功能允许用户查看彼此的日历,以便高效地安排会议。您可以在 Zimbra 和 Microsoft Exchange 服务器上设置空闲/忙碌安排。

Zimbra 可以在支持的 Microsoft Exchange 服务器上查询用户的空闲/忙碌时间表,也可以将 Zimbra 用户的空闲/忙碌时间表传播到 Exchange 服务器。

要设置忙/闲互操作性,必须按照 Exchange 设置要求部分所述设置 Exchange 系统,并且必须配置 Zimbra Collaboration 全局配置、域、COS 和帐户设置。配置 Zimbra Collaboration 最简单的方法是从管理控制台进行配置。

Exchange 设置要求

设置忙/闲功能需要以下条件:

- 系统中必须有一个 Active Directory (AD) 或者必须有全局目录可用。
- Zimbra 协作服务器必须能够访问至少一个 Exchange 上的 IIS 的 HTTP(S) 端口服务器。
- 需要通过 IIS 提供 Exchange 公用文件夹的 Web 界面。(<http://server/public/>)
- 必须使用每个邮件域的相同管理组将 Zimbra Collaboration 用户配置为 AD 上的联系人。这仅适用于 Zimbra 到 Exchange 的忙/闲复制。
- 对于 Zimbra Collaboration 到 Exchange 的忙/闲复制,必须在所有 Zimbra Collaboration 用户的帐户属性zimbra-ForeignPrincipal中配置 Exchange 用户电子邮件地址。

在 Zimbra Collaboration 上配置空闲/忙碌

要从管理控制台设置空闲/忙碌互操作性,必须按照此处的说明配置全局配置、域、COS 和帐户设置。

- 配置 Exchange 服务器设置 (全局或每个域) 。
 - Microsoft Exchange 服务器 URL。这是 Exchange 的 Web 界面。
 - Microsoft Exchange 身份验证方案,可以是基本身份验证方案,也可以是表单身份验证方案。
 - Basic 是通过 HTTP 基本身份验证对 Exchange 进行身份验证。

- 表单是对 Exchange 的身份验证,作为基于 HTML 表单的身份验证。
- Microsoft Exchange 服务器类型, WebDav或ews
- 选择 WebDAV 来支持 Exchange 2003 或 Exchange 2007 的忙/闲功能。

这仅供参考,因为这些版本的 Exchange 不再受支持。

- 选择 ews (Exchange Web 服务) 来支持 Exchange 2010 SP1 及更新版本的忙/闲功能。
- 包括 Microsoft Exchange 用户名和密码。这是 Active Directory 中有权访问公共文件夹的帐户名称和密码。这些用于在 REST 和 WebDAV 接口上对 Exchange 服务进行身份验证。
- 在全局配置忙/闲互操作页面、域忙/闲互操作页面或服务类别 (COS) 高级页面上,添加在 Exchange 的legacyExchangeDN属性中配置的o和ou值。在全局级别设置,这适用于与 Exchange 通信的所有帐户。
- 在帐户的“空闲/忙碌互操作”页面中,配置帐户的外部主要电子邮件地址。这将设置从 Zimbra 协作帐户到 AD 中相应用对象的映射。

要在 Exchange 服务器上找到这些设置,您可以运行 Exchange ADSI 编辑工具并在legacyExchangeDN属性中搜索o=和cn=设置。, 或=, ,

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

您可以在 Zimbra 服务器之间设置空闲/忙碌互操作性。空闲/忙碌互操作性在每个服务器上配置服务器。

每台服务器必须运行 Zimbra Collaboration 8.0.x 或更高版本。

1.输入服务器主机名和端口。

`zmprov mcf zimbraFreebusyExternalZimbraURL http[s]://[用户:密码@]主机:端口`

重击

如果未包含用户:密码,服务器将运行匿名忙/闲查找。

2.重新启动服务器。

`zmcontrol 重启`

重击

3. 在所有其他服务器上重复这些步骤。

设置 S/MIME

S/MIME 是发送安全电子邮件的标准。S/MIME 消息使用数字签名来验证和加密消息。

目前,有两种不同的方法可以提供 S/MIME 功能

1. 旧的基于客户端的解决方案需要在客户端机器上部署 Java 1.6 SE
2. 新的基于服务器的解决方案不需要客户端计算机上安装 Java。服务器执行所有加密操作。(推荐)

此功能仅在经典 Web 应用程序中受支持。

使用基于客户端的解决方案设置使用 S/MIME 功能

先决条件

- 要使用 S/MIME, 用户必须拥有 PKI 证书和私钥。私钥必须安装在 Windows 和 Apple Mac 上的用户本地证书存储中, 如果使用 Firefox 浏览器, 则必须安装在浏览器证书存储中。请参阅相应的计算机或浏览器文档以了解如何安装证书。
- 用户可以使用以下任意一种浏览器:
 - Mozilla Firefox 4 或更高版本
 - Internet Explorer 8、9
 - Chrome 12 或更高版本
- 用户计算机必须部署 Java 1.6 SE 才能使用 S/MIME。如果没有, 用户将看到要求他们安装的错误。

S/MIME 许可证

您必须拥有启用 S/MIME 的 Zimbra 许可证。

启用 S/MIME 功能

管理控制台:

| | |
|-------------|-----------|
| 主页→配置→服务等级→ | 操作系统 → 特点 |
| 主页→管理→账户→ | 帐户 → 特点 |

可以从 COS 或账户功能选项卡启用 S/MIME 功能。

- 选择需要编辑的 COS 或账户。
- 在“功能”选项卡的 S/MIME 功能部分中, 选中启用 S/MIME。
- 单击保存。

导入 S/MIME 证书

如果用户将收件人的公钥证书存储在以下任一位置, 则可以向收件人发送加密消息:

- 收件人地址簿中的联系页面。
- 本地操作系统或浏览器密钥库。
- 外部 LDAP 目录。

证书应发布到 LDAP 目录中, 以便可以从 GAL 中检索它们。S/MIME 证书的格式必须是 X.509 Base64 编码的 DER。

配置证书的外部 LDAP 查找

如果您使用外部 LDAP 来存储证书, 则可以配置 Zimbra 服务器以代表客户端从外部 LDAP 查找和检索证书。

管理控制台:

主页→配置→全局设置→S/MIME

主页→配置→域→→S/MIME

领域

您可以从全局设置→S/MIME选项卡或域→S/MIME选项卡配置外部 LDAP 服务器设置。

全局设置覆盖域设置

1. 编辑全局设置页面或选择要编辑的域。打开S/MIME选项卡。
2. 在配置名称字段中,输入一个名称来标识外部 LDAP 服务器。例如, companyLDAP_1
3. 在LDAP URL字段中,输入 LDAP 服务器的 URL。例如, ldap://host.domain:3268
4. 要使用 DN 绑定到外部服务器,请在S/MIME LDAP 绑定 DN字段中输入绑定 DN。例如, administrator@domain

如果您想使用匿名绑定,请将绑定 ND 和绑定密码字段留空。

5. 在S/MIME Ldap 搜索基础字段中,输入要搜索的 LDAP 服务器的特定分支
找到证书。

例如, ou=Common Users,DC=host,DC=domain

或者,勾选“自动发现搜索库”以自动发现搜索库 DN。要使此功能有效,S/MIME 搜索库字段必须为空。

6. 在S/MIME Ldap 过滤器字段中,输入搜索的过滤器模板。过滤器模板可以包含
以下为扩展的转换变量:
 - %n - 带有@的搜索键 (如果没有指定@,则不带有@)
 - %u -删除@ (例如, mail=%n)

7. 在S/MIME Ldap 属性字段中,输入外部 LDAP 服务器中包含用户 S/MIME 的属性
证书。多个属性可以用逗号(,)分隔。

例如,“userSMIMECertificate,UserCertificate”

8.单击保存。

要设置另一个外部 LDAP 服务器,请单击添加配置。

使用基于服务器的解决方案设置使用 S/MIME 功能

先决条件

与基于客户端的 S/MIME 解决方案相同,只是客户端机器上不需要 Java。私钥也不需要位于客户端机器的本地/浏览器证书存储中。

S/MIME 许可证

与基于客户端的 S/MIME 解决方案相同

启用 S/MIME 功能

与基于客户端的 S/MIME 解决方案相同

导入 S/MIME 证书

与基于客户端的 S/MIME 解决方案相同,只是收件人的公钥证书不再需要存储在本地操作系统或浏览器密钥库中。证书可以发布到以前的 S/MIME 版本中提到的所有其他地方。

为支持基于服务器的 S/MIME 解决方案而引入的 LDAP 属性列表

1. zimbraSmimeOCSPEnabled

- 服务器在验证用户和公共证书时使用
- 如果为TRUE , 证书验证期间将执行吊销检查
- 如果为FALSE , 证书验证期间不会执行吊销检查

2. zimbraSmimePublicCertificateExtensions

- 支持的公共证书文件扩展名以逗号分隔
- 包含userCertificate LDAP 属性支持的格式列表
- 默认值: cer , 韩規 , , , p7b , p7r , 海表温度 , 我是佩姆
- Zimbra Classic Web App 检索上传公共证书所支持的文件格式或扩展名从服务器

3. zimbraSmimeUserCertificateExtensions

- 支持的公共证书文件扩展名以逗号分隔
- 包含 userSmimeCertificate LDAP 属性支持的格式列表
- 默认值: p12 , PFX
- Zimbra Classic Web App 检索上传公共证书所支持的文件格式或扩展名从服务器

将 CA 证书添加到 S/MIME 邮箱信任库的过程

S/MIME 使用在 localconfig.xml 中定义的邮箱信任存储路径及其密码

关键名称为：

- mailboxd_truststore
- mailboxd_truststore_密码

如果 localconfig.xml 中未定义 mailboxd_truststore 键,则默认 mailboxd_truststore 的值为：

- <zimbra_java_home>/jre/lib/security/cacerts

可以通过执行以下命令将 CA 证书导入到邮箱信任存储：

```
keytool -import -alias -keystore <mailboxd_truststore 路径> -trustcacerts -file <CA_Cert>
```

重击

电子邮件保留管理

您可以为用户帐户的电子邮件、垃圾箱和垃圾文件夹配置保留策略。基本电子邮件保留策略是在 COS 中或为个人帐户设置电子邮件、垃圾邮件和垃圾邮件的生存期。

您可以设置特定的保留策略,用户可以为其邮箱中的收件箱和其他电子邮件文件夹启用这些策略。帐户。用户还可以创建自己的保留策略。

您可以启用垃圾箱功能来保存从垃圾箱中删除的邮件。当邮件到达根据电子邮件生存期规则或删除策略,邮件保留生存期结束时,将移动到垃圾箱。用户可以从垃圾箱中恢复已删除的项目,直到达到可见性中设置的阈值垃圾箱中的使用寿命供最终用户设置。

如果未启用垃圾箱,则当达到电子邮件保留期限时,消息将从服务器中清除。

您还可以对帐户设置合法保留,以防止邮件被删除。

配置电子邮件生命周期规则

您可以配置何时从帐户文件夹以及垃圾箱和垃圾文件夹中删除电子邮件由 COS 或个人账户提供。

表格电子邮件生命周期选项

| 电子邮件终身选项 | 描述 |
|-------------|---|
| 电子邮件消息的生命周期 | 邮件在被清除之前可以在文件夹中保留的天数。这包括 RSS 文件夹中的数据。 默认值 = 0 最短 = 30 天 |
| 已删除邮件的生存期 | 邮件在被清除之前保留在“垃圾箱”文件夹中的天数。 默认 = 30 天。 |
| 垃圾邮件的生命周期 | 邮件在被归类为垃圾邮件之前可以保留在垃圾邮件文件夹中的天数清除。 默认 = 30 天。 |

清除电子邮件

默认情况下,服务器每分钟清除超过其有效期的电子邮件。您可以更改服务器在清除邮箱之间应“休息”的时间长度。

使用全局休眠时间设置来定义邮箱清除之间的持续时间（以分钟为单位）。

管理控制台：

主页→配置→全局设置→常规信息

The screenshot shows the 'General Information' section of the global settings. Key settings include:

- 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: (empty)
- Delegated admin help URL: (empty)

A note at the top states: "Note: Settings only apply to servers that have the appropriate service(s) installed and enabled. Server settings override global settings."

例如,如果清除间隔设置为 1 分钟,则服务器清除邮箱 1后开始清除邮箱 2。

,等待 1 分钟,然后

如果将邮件清除计划设置为 0,则即使邮件、垃圾邮件和垃圾邮件寿命已设定。

由于用户无法查看消息生存期设置,因此您需要告知他们您的清除策略。

配置消息保留和删除策略

保留和删除策略可以配置为全局设置或 COS 设置。用户可以选择这些策略应用于其帐户中的邮件文件夹。他们还可以设置自己的保留和删除策略。用户可以启用您设置的策略,也可以从文件夹的“编辑属性”对话框中创建自己的策略。

全球保留政策

可以从管理控制台管理系统范围的保留和删除策略。

使用全局保留策略页面来设置全局保留或删除策略。

管理控制台:

主页→配置→全局设置→保留策略

| Policy Name | Retention Range |
|-------------|-----------------|
| | |

COS 保留政策

使用 COS 保留策略页面为所选 COS 设置保留或删除。

管理控制台:

主页→配置→服务等级→

操作系统→保留政策

Home - Configure - Class of Service - standard - Retention Policy

ID: df02cdbf-4b43-4ccd-a238-0c70e64e85c6
Created: August 28, 2014 11:44:23 AM

Enable COS-level policies instead of inheriting from the policy defined in Global Settings.

▼ Retention Policies

| Policy Name | Retention Range |
|-------------|-----------------|
| | |

Delete Edit Add

► Disposal Policies

确保启用 COS 级别策略而不是从全局设置中定义的策略继承。

保留策略不会自动在文件夹中强制执行。如果用户在未达到保留策略阈值的文件夹中选择项目，则会显示以下消息，您正在删除处于文件夹保留期内的邮件。是否要删除该邮件？

当达到删除策略的阈值时，项目将从帐户中删除。它们不会被发送到垃圾箱文件夹。如果启用了垃圾箱功能，它们将被发送到垃圾箱，如果未启用，它们将从服务器中清除。

生命周期和保留/删除策略如何协同工作

如果将电子邮件消息生存期设置为非零 (0) 的值，则此设置将与文件夹的处置或保留策略值一起应用。例如：

电子邮件消息有效期设置为 120 天

- 文件夹 A 的策略规定处理期限为 360 天。文件夹 a 中的邮件将在 120 天内处理完毕。
- 文件夹 B 的策略为 90 天的处置阈值。文件夹 B 中的邮件将在 90 天内处置。
- 文件夹 C 的策略保留期限为 150 天。文件夹 C 中的邮件将在 120 天内处理完毕。

管理垃圾箱

如果启用了此功能，当邮件、垃圾或垃圾邮件达到有效期时，邮件将被移至垃圾箱。当用户右键单击“垃圾箱”时，他们可以单击“恢复已删除的项目”以从垃圾箱中检索过去 x 天内删除的项目。此阈值基于“垃圾箱中最终用户的可见性有效期”设置。

清除前垃圾箱中的保留期限设置设置垃圾箱中项目的保留期限。垃圾箱中超过阈值的项目将被清除，并且无法检索。

管理员可以访问单个垃圾箱的内容,包括垃圾邮件,并且可以在达到邮件生存期之前随时删除数据。

在垃圾箱文件夹中搜索项目

```
zmmailbox -z -m <user@example.com> search --dumpster -l <#> --types <消息,联系人,文档> <搜索字段>
```

BASH

搜索字段可以是日期范围：“之前 :mm/dd/yyyy 和之后 :mm/dd/yyyy”或来自或发送给特定人的电子邮件：“来自 :Joe”等。

删除垃圾箱文件夹中的项目

可以使用 CLI 或管理控制台删除 dumpster 文件夹中的项目：

```
zmmailbox -z -m <user@example.com> -A dumpsterDeleteItem <项目 ID>
```

重击

管理控制台：

主页→配置→服务等级→ 操作系统 →特点→一般特点

1. 启用 (选中)垃圾箱文件夹复选框。
2. 要为最终用户设置垃圾箱中的可见性生命周期,请转到COS 的“高级”页面上的“超时策略”部分
3. 要在清除之前设置垃圾箱中的保留期限,请转到 COS 的高级页面,电子邮件保留策略部分。

配置帐户的合法保留

如果启用了垃圾箱文件夹功能,您可以设置合法保留以保留用户帐户中的所有项目。

启用垃圾箱后,可清除垃圾箱文件夹也会启用。禁用此功能会关闭清除用户垃圾箱中的项目。这可以在 COS 或个人帐户上设置。启用可清除垃圾箱文件夹后,将忽略帐户文件夹上设置的任何删除策略。

配置合法保留：

管理控制台：

| | |
|-------------|----------|
| 主页→配置→服务等级→ | 操作系统 →特点 |
| 主页→管理→账户→ | 帐户 →特点 |

在功能页面上取消选择可以清除垃圾文件夹。

定制管理扩展

开发人员可以创建并向 Zimbra 管理控制台用户界面添加自定义模块,以提供新视图、管理新数据对象、使用新属性扩展现有对象以及自定义现有视图。

有关如何创建扩展管理控制台 UI 模块的最新、最全面的信息,请转至 Zimbra wiki 扩展管理 UI 文章,网址为Extending_Admin_UI (https://wiki.zimbra.com/wiki/Extending_Admin_UI) 。

当前在管理控制台 UI 中包含的所有 Zimbra 扩展均在内容窗格中列为仅供查看。

只有您创建的模块才可以被删除（另请参阅删除管理扩展模块）。

部署新的管理控制台 UI 模块

管理控制台：

主页→配置→管理扩展

将模块zip文件保存到您用于访问管理控制台的计算机。

1. 从齿轮图标中,选择部署以显示部署 Zimlet 或扩展对话框。
2. 浏览到您需要上传的自定义模块zip文件。
- 3.单击部署。

文件已上传并且扩展立即部署在服务器上。

删除管理扩展模块

删除管理扩展会导致所选扩展及其所有相关文件被移除。此操作不会删除原始zip文件。

管理控制台：

主页→配置→管理扩展

使用本部分中的步骤删除自定义管理扩展。

1. 选择要删除的模块,然后从齿轮图标中选择取消部署。系统会显示确认询问。
2. 在确认询问时,单击“是”继续。

短暂数据

Zimbra Collaboration 正常运行期间,LDAP 中存储了 3 种主要类型的临时数据。

- 上次登录时间戳 (zimbraLastLogonTimestamp)
- 身份验证令牌 (zimbraAuthTokens)
- CSRF 令牌 (zimbraCsrfTokenData)

在小型系统中,这些类型的临时数据存储可以在 LDAP 服务器中完成。但是,邮件研究发现,拥有大量活跃用户的系统会导致 LDAP 在短期数据存储方面超负荷。因此,首选方案是使用外部服务器存储这些短暂的数据。

本文档未介绍如何安装和维护临时存储服务器。

通过以下 LDAP 属性配置临时数据的存储位置:

| 属性 | 格式 | 描述 |
|---------------------------|-------------|-------------|
| zimbraEphemeralBackendURL | [后端名称]:[参数] | 临时后端 URL 配置 |

当前支持的两个临时数据后端是:

| 后端 | 格式 | 描述 |
|---------|----------------------|-------------|
| LDAP | ldap://默认 | 默认配置 |
| 固态硬盘数据库 | 固态数据库:127.0.0.1:8888 | SSDB 服务器和端口 |

频繁的身份验证请求会给临时数据存储后端带来很高的负载。请参阅以下 Zimbra 基于身份验证的负载测试结果的 Wiki 页面:

- LDAP 身份验证负载测试
(<https://github.com/Zimbra/zm-ssdb-ephemeral-store/wiki/Zimbra-and-LDAP-Authentication-Load-Tests>)
- SSDB 身份验证负载测试
(<https://github.com/Zimbra/zm-ssdb-ephemeral-store/wiki/Zimbra-and-SSDB-Authentication-Load-Tests>)

配置正在运行的 Zimbra 协作以使用 SSDB

配置已运行的 Zimbra Collaboration 安装以利用SSDB而不是LDAP进行短暂数据存储通过以下过程完成:

- 安装SSDB ,并记下配置的 IP 地址和端口 ,因为接下来的步骤需要这些数据。请参阅
请参阅配置选项概述以了解更多信息。
- 使用`/opt/zimbra/bin/zmmigrateattrs`命令将任何现有的短期数据迁移到SSDB 。
- 配置 Zimbra Collaboration 以使用SSDB 。

迁移程序

1. 在安装中的其中一台机器上访问命令提示符。
2. 使用zmmigrateattrs实用程序将现有的临时数据迁移到SSDB后端

须藤苏-津布拉

```
/opt/zimbra/bin/zmmigrateattrs ssdb:<ip address>|hostname>:port # 替换您的服务器值
```

您可以使用 IP 地址或主机名作为目标 URL 的主机部分。无论哪种方式，您都需要确保它解析为集群中所有机器上的正确 IP 地址。如果提供的 SSDB 地址未解析为正常运行的后端，则迁移过程将终止。

3. 配置 Zimbra Collaboration 以使用SSDB：

须藤苏-津布拉

```
zmprov mcf zimbraEphemeralBackendURL ssdb:<ip address>|hostname>:port # 替换您的服务器值
```

与迁移一样，主机和端口必须解析为正常运行的 SSDB 后端。否则， zimbraEphemeralBackendURL 的值将不会改变。

迁移详情

移民信息

可以通过运行命令zmmigrateattrs 查看最新迁移过程的信息

地位。 如果迁移目前正在运行，则可能必须从新终端窗口运行此命令。

该命令会输出三条信息：

1. 迁移状态:IN_PROGRESS、COMPLETED 或 FAILED 之一
2. 作为目标的 SSDB 后端的 URL
3. 启动迁移过程的时间戳

可以使用命令zmmigrateattrs --clear重置迁移信息。仅当状态不反映系统的真实状态时才应执行此操作。

更改临时后端 URL

当zimbraEphemeralBackendURL的值被修改时，Zimbra Collaboration 会检查上次已知迁移的状态。这可能导致以下几种情况之一：

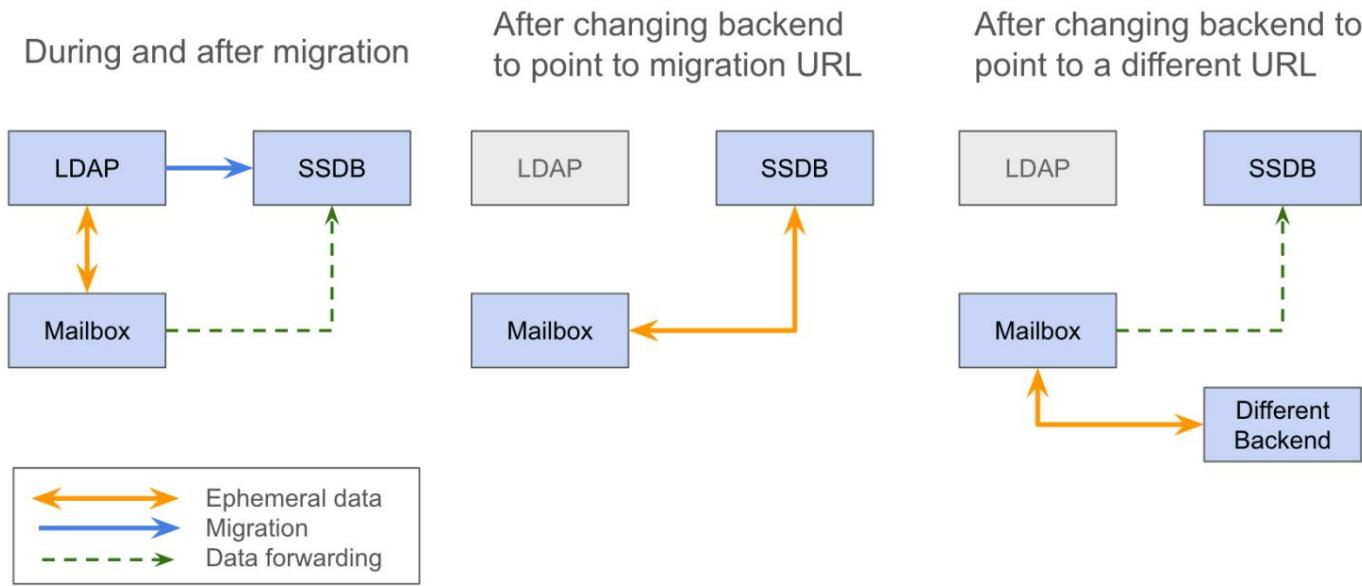
1. 如果迁移已完成，并且此迁移的 URL 与新提供的值匹配，
zimbraEphemeralBackendURL已更改为新值，迁移信息已重置。这是预期的
用例。
2. 如果当前正在进行迁移， zimbraEphemeralBackendURL将不会改变。
3. 如果没有可用的迁移信息，迁移失败，或者新的 URL 与迁移 URL 不匹配，则zimbraEphemeralBackendURL将被更改；但是，将记
录一条警告，指出不能保证数据已迁移。

转发短暂数据

在迁移过程中,直到后端 URL 发生更改,Zimbra Collaboration 都会将新的临时数据存储在 LDAP 和SSDB中;这可防止两个后端不同步。如果zimbraEphemeralBackendURL的新值更改为与迁移 URL 匹配,则会重置迁移信息并关闭转发机制。如果值不匹配,则不会重置迁移信息,并且转发保持不变。

请注意,这意味着迁移只需运行一次,即使初始迁移和 URL 更改之间存在间隔。只要目标后端从未脱机,它就会保持最新状态。但是,如果SSDB在迁移结束和后端 URL 更改之间脱机,则需要重新运行迁移。

这些场景如下所示:



高级迁移选项

zmmigrateattrs工具提供了几个迁移选项,请谨慎使用:

- -r或--dry-run选项将每个帐户要做的更改输出到控制台,而无需实际执行迁移。
- -n或--num-threads选项指定迁移将使用多少个线程。省略此选项将导致迁移同步进行。
- -a或--account选项允许迁移以逗号分隔的特定帐户列表。这仅应用于测试或调试。
- -d或--debug选项启用调试日志记录。

如果没有明确传递属性名称作为参数,则所有已知的临时属性都会发生迁移,如上例所示。

迁移限制

临时数据迁移是一个单向过程。zmmigrateattrs脚本不支持将数据从SSDB迁移到 LDAP,也不支持在不同的SSDB实例之间迁移数据。这意味着,如果在迁移后将zimbraEphemeralBackendURL的值恢复为 LDAP,则之前的身份验证数据将无法访问,并且所有用户会话都将失效。如果需要迁移到新的SSDB后端,则应在更改 的值之前将数据复制到新位置

zimbraEphemeralBackendURL。

有一个例外：在切换到SSDB后，可以立即安全地将后端恢复为 LDAP，并且数据丢失最少。这是因为在迁移期间原始值保留在 LDAP 中；将后端切换到SSDB会在切换时在 LDAP 中留下临时数据的“快照”。迁移实用程序目前不提供删除此数据以释放空间的方法；但是，它允许恢复后端。初始更改和恢复之间的时间越长，LDAP 快照反映的临时数据的真实状态就越少。

对 zmprov 的更改

由于多值临时数据存储方式的变化，属性 zimbraAuthTokens 和 zimbraCsrfTokenData 不再作为 zmprov ga <account> 响应的一部分返回。zimbraLastLogonTimestamp 的值与以前一样返回，但只有在未使用 -l 标志的情况下才会返回，因为添加 -l 标志将限制服务仅访问 LDAP 中的属性。无论临时后端如何，仍然可以使用 zmprov ma <account> 命令修改这些属性。为了做到这一点，提供的属性值必须与其 LDAP 格式匹配：对于身份验证令牌，为 tokenId|expiration|serverVersion；对于 CSRF 令牌，为 data:crumb:expiration。

迁移 CSV 输出

每次运行 zmmigrateattrs 都会在 /opt/zimbra/data/tmp/ 文件夹中生成一个 CSV 文件。该文件包含每个迁移帐户的迁移信息，例如迁移的属性数量。请注意，这个数字可能为零，如果帐户的所有临时数据都已存在于目标存储中，则可能会发生这种情况。

如果任何迁移失败，还会在同一目录中创建一个仅详细说明错误的精简版 CSV 文件报告。文件的名称将在运行结束时记录。

账户删除行为

SSDB 和 LDAP 后端之间的临时数据删除行为略有不同。使用 SSDB 作为后端，帐户删除会导致 zimbraLastLogonTimestamp 属性从 SSDB 中明确删除。然而，当令牌生存期到期时， zimbraAuthTokens 和 zimbraCsrfTokenData 会被 SSDB 保留为过期状态

达到（默认为 2 天）。相反，LDAP 中的临时数据将在帐户删除过程中立即被清除。

SSDB 安装和配置

安装

Zimbra Collaboration 软件包不包括 SSDB 服务器,Zimbra Collaboration 安装和配置实用程序不会更改 SSDB 配置。要安装最新版本的 SSDB,请按照SSDB 安装文档(<http://ssdb.io/docs/install.html>) 中 SSDB 开发人员社区提供的说明进行操作。请注意,Zimbra Collaboration 已使用 SSDB 版本 1.9.5 进行了测试。要安装 SSDB 1.9.5,请下载[stable-1.9.5.zip](https://github.com/ideawu/ssdb/tree/stable-1.9.5) (<https://github.com/ideawu/ssdb/tree/stable-1.9.5>)而不是[master.zip](https://github.com/ideawu/ssdb/archive/master.zip) (<https://github.com/ideawu/ssdb/archive/master.zip>)按照SSDB 安装说明进行操作 (<http://ssdb.io/docs/install.html>) 。

SSDB 不支持加密连接身份验证,这意味着你必须保护访问

配置选项概述

本指南的目的是讨论SSDB的一些可用选项,特别是关于:

- 通过主从复制实现高可用性
- 通过主-主复制实现高可用性
- 通过多主配置实现水平扩展,具有高可用性。

本指南并非旨在详尽介绍该主题。此外,截至撰写本文时,系统管理员必须在更新zimbraEphemeralBackendURL和迁移属性之前安装和配置SSDB及任何相关软件包。

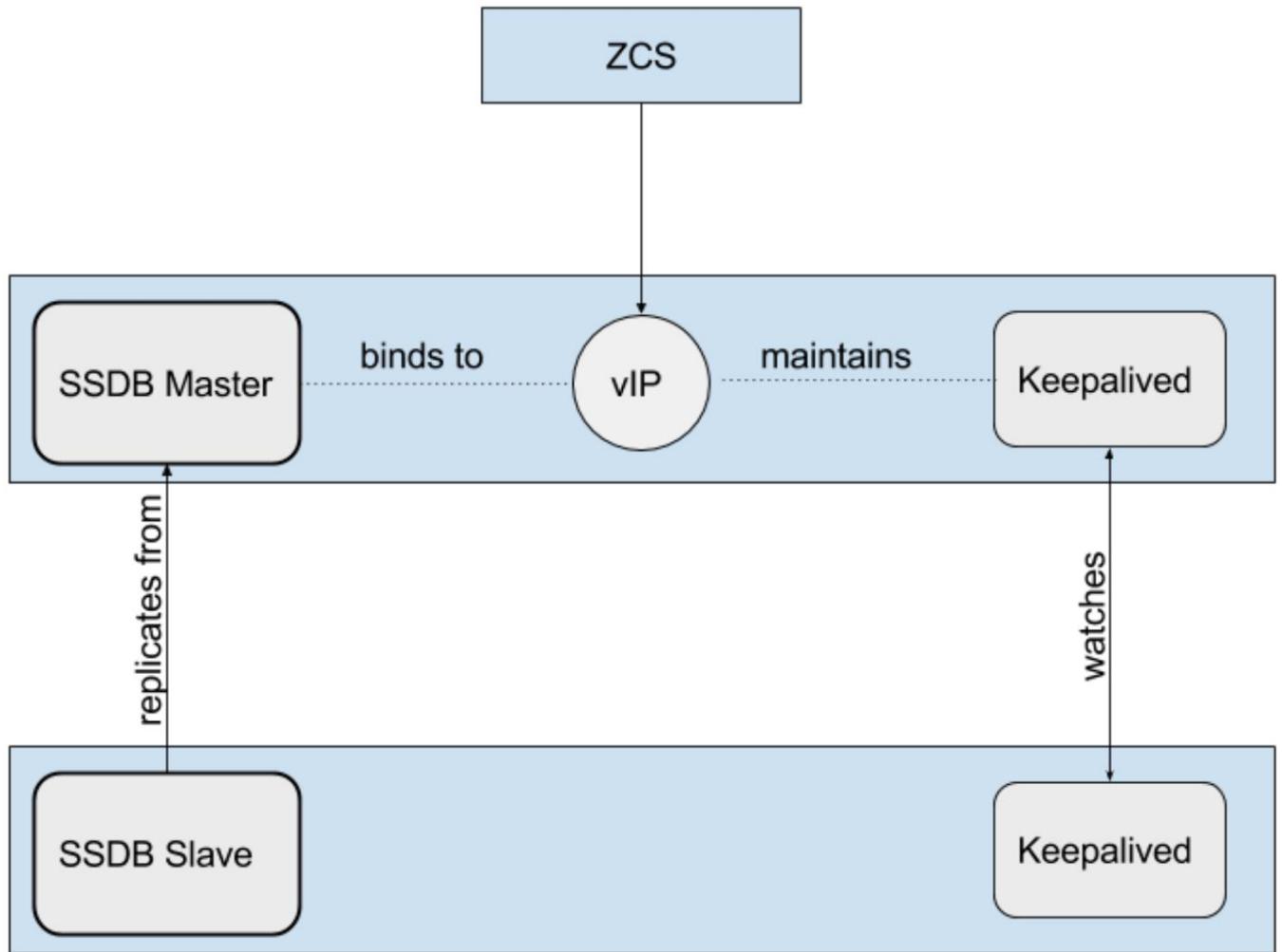
SSDB与Redis兼容 (<https://redis.io/>)客户端和 Zimbra Collaboration 当前使用Redis兼容客户端与SSDB Redis后端进行通信。

,本文描述的许多概念都适用于

通过主从复制实现高可用性

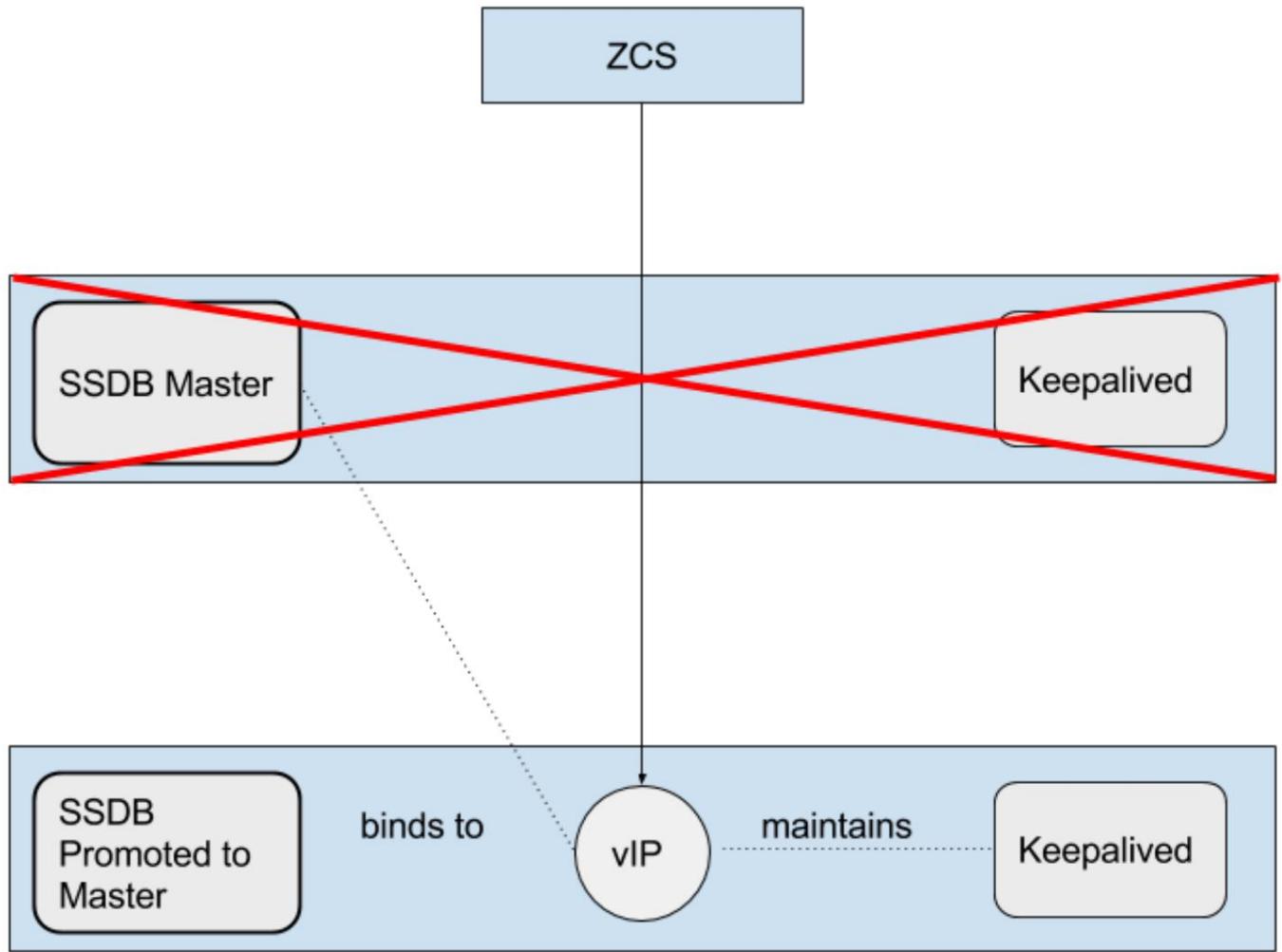
正常运行

本文档介绍的实现主从复制的方法利用了Keepalived (<http://www.keepalived.org/>)维护与主SSDB实例绑定的配置虚拟IP 地址
在正常情况下。



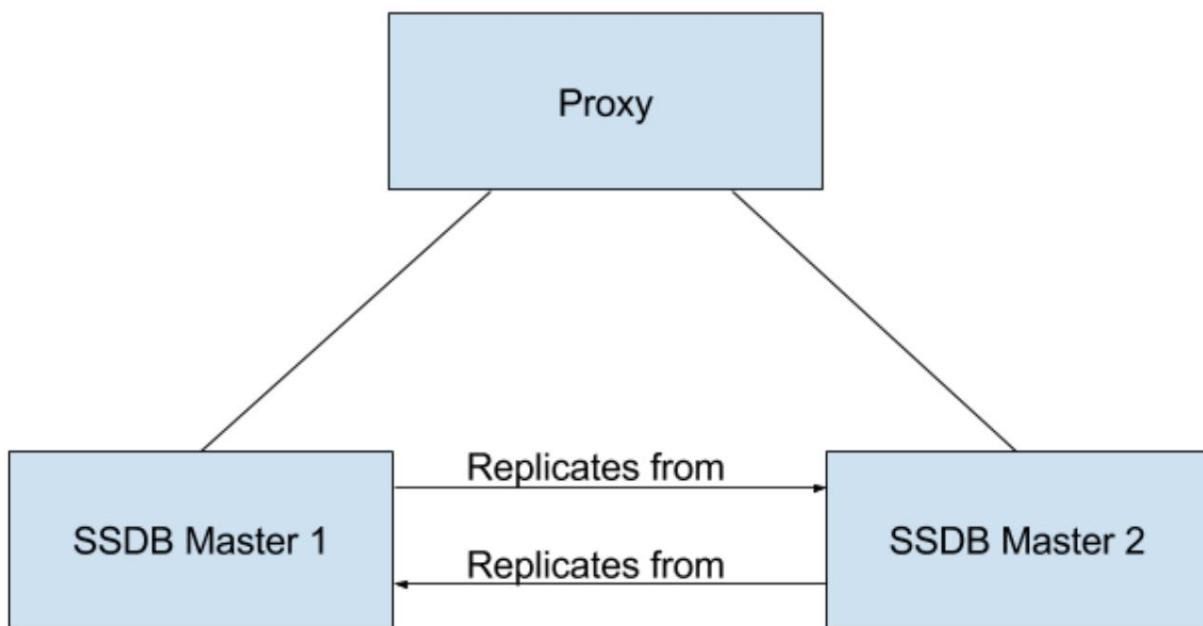
故障转移

如果Keepalived检测到主实例故障，则通过将虚拟 IP 地址重新绑定到备份实例，将备份实例提升为主实例。



通过主-主复制实现高可用性

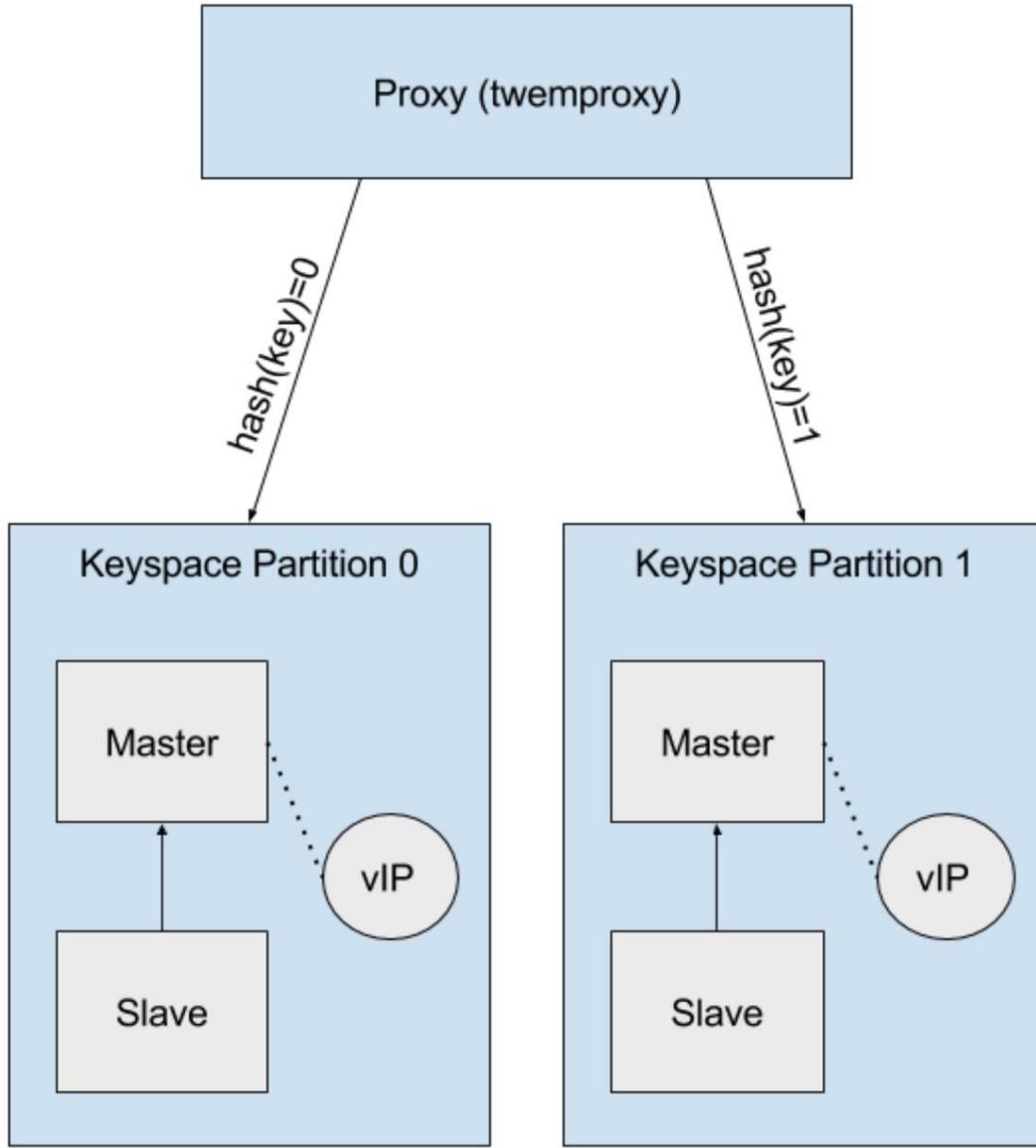
这与主从复制不同,因为两个SSDB实例都处于在线状态且可访问。每个实例都从另一个实例复制更改。在后面描述的示例设置中,我们使用HAProxy (<http://www.haproxy.org/>)作为前端。请记住,对于生产,您必须使用本身具有高可用性的代理服务。



通过多主配置进行水平扩展

通常，SSDB和Redis都在单个实例中包含整个键空间。可以使用twemproxy (<https://github.com/twitter/twemproxy>) 等服务来前端多个实例。它支持各种哈希模式，这样与特定键相关的数据始终存储在同一台服务器上。这允许在非常大的安装中进行水平扩展。

通过以主从配置来配置每个SSDB实例，您可以获得水平扩展和高可用性。



主从复制

确保SSDB保持高可用性的一种方法是设置主从复制并配置一个系统，以便在主实例发生故障时允许备份SSDB实例自动接管。本文档将介绍一种实现该目标的技术。

概述

SSDB将安装在两台服务器上。其中一台服务器将配置为指定的主服务器，另一台服务器将配置为指定的从服务器或备份服务器，该服务器将不断从主服务器复制更改。

Keepalived也将安装在这两台服务器上。每个Keepalived实例都将监视另一个实例。如果主服务器发生故障，Keepalived将检测到该故障并将从属或备份服务器提升为主服务器。Keepalived将维护一个虚拟 IP 地址(https://en.wikipedia.org/wiki/Virtual_IP_address)

绑定到当前主服务器。

Zimbra Collaboration 将被配置为使得zimbraEphemeralBackendURL绑定到由Keepalived维护的。
虚拟的
地址

安装和配置完成后,按照Ephemeral Data中的说明相 两个都SSDB主从设置和 Zimbra 协作已
应地更新zimbraEphemeralBackendURL 。

此处记录的示例是在运行Ubuntu 16.04 (<http://releases.ubuntu.com/16.04/>)的服务器上完成的。

所需软件包

- [SSDB](http://ssdb.io/) (<http://ssdb.io/>)
- [Keepalived](http://www.keepalived.org/) (<http://www.keepalived.org/>)

先决条件

按照Linux系统的步骤在两台服务器上安装SSDB和Keepalived
您正在使用的发行版。

配置

以下配置步骤假设您已将SSDB安装到/var/lib/ssdb ,并且所有SSDB
配置文件位于同一目录中。它进一步假设内部主机地址位于
192.168.56/24网络。

- 192.168.56.111-这是初始主SSDB服务器的 IP 地址
- 192.168.56.112-这是初始从属SSDB服务器的 IP 地址
- 192.168.56.120 这是Keepalived将维护的虚拟 IP 地址。

SSDB 配置,指定 (初始)主服务器

该机器的IP地址是192.168.56.111 。

/var/lib/ssdb/ssdb_master.conf

以下块中的关键配置项为：

- server/ip - 绑定到所有可用的 IP 地址
- server/port - 绑定到标准SSDB端口
- 服务器/拒绝 ， 服务器/允许-限制SSDB对本地主机和内部 (主机)地址的访问。

这里只展示主从复制相关的配置项。

```
# ssdb-server config # 必须用 TAB  
缩进!  
  
# 相对于此文件的路径,目录必须存在 work_dir = ./var pidfile = ./var/ssdb.pid
```

服务器:

ip:0.0.0.0 端口:

8888 拒绝:全部

允许:127.0.0.1

允许:192.168.56

复制:binlog:是

```
# 将同步速度限制为 *MB/s, -1:无限制 sync_speed: -1
```

从属:

```
# sync|mirror,默认为同步 #type: sync
```

/var/lib/ssdb/ssdb_slave.conf

以下块中的关键配置项为:

- server/ip - 绑定到本地主机
- server/port - 绑定到标准SSDB端口
- slaveof/ type-同步
- slaveof/host - 192.168.56.112是另一个SSDB服务器
- slaveof/port - 8888 - 标准SSDB端口

再次,仅显示与主从复制相关的配置项。

```
# ssdb 服务器配置

# 相对于此文件的路径,必须存在 work_dir = ./var_slave pidfile = ./var_slave/ssdb.pid
```

服务器:

IP:127.0.0.1 端口:
8888

复制:binlog:是

将同步速度限制为 *MB/s, -1:无限制 sync_speed: -1

从属:

```
# sync|mirror,默认为同步
类型:同步
# 可以使用主机:<hostname> 和 SSDB 1.9.2 或更新版本
IP:192.168.56.112 端口:  
8888
```

SSDB 配置,指定 (初始)从属

该机器的IP地址是192.168.56.112。

ssdb_master.conf文件与指定的主服务器的文件相同。

ssdb_slave.conf文件与指定主服务器的几乎相同。只有以下几项不同;

- slaveof/ip (或主机) - 192.168.56.111是另一个SSDB服务器

Keepalived 配置,指定 (初始)主服务器

/etc/keepalived/keepalived.conf

需要注意的关键配置项是:

- state -指定 (初始)主服务器和备份服务器的状态设置**两个都UP**。在此情况下,优先级用于协商哪个服务器将首先承担MASTER状态。
- nopreempt - 如果主服务器发生故障,备份服务器被提升为主服务器,此配置指令将阻止原始主服务器在自动恢复在线时收回该角色。这是必需的,因为它可能会过时。在这种情况下,当它恢复时,它将保持备份模式并开始从新主服务器复制信息。需要将发生故障的主服务器重新投入使用。

笔记 :可能存在人为干预

- 接口- 在此示例中, enp0s8是将为其定义虚拟 IP 地址的接口标识符。您将选择适合您的安装的值。
- priority 指定的初始主服务器必须比指定的初始备份服务器具有更高的优先级。
- advert_int - 出于本文档的目的,使用默认值 1 秒。如果您安装Keepalived 1.2.21或更新版本,则可以在此处指定浮点值;例如0.1 (秒)。这将允许Keepalived更快地检测到主故障。
- 通知- 这是状态转换时调用的脚本的路径。脚本的完整内容如下所示

- virtual_ipaddress - 这是Keepalived维护的虚拟 IP 地址。

```
vrrp_instance VRRP1 { 状态备份

    nopreempt 接
    口 enp0s8 virtual_router_id
    41 优先级 200 advert_int 1 通知 /
    var/lib/ssdb/notify.sh

    身份验证 { auth_type PASS
        auth_pass 1234

    }

    虚拟 IP 地址 { 192.168.56.120 dev
        enp0s8 标签 enp0s8:vip
    }

}

/var/lib/ssdb/notify.sh
```

这是Keepalived在状态转换期间调用的脚本。请注意，分配给USER 的值应该是拥有SSDB进程的用户名。

重击

```
#!/bin/bash # 这必须
以 root 身份运行。
```

```
最终状态=$3
名称=$2
类型=$1
```

```
LOG=/var/log/keepalived-state-transition.log LOG_ERROR=0
LOG_WARNING=1
LOG_INFO=2
LOG_DEBUG=3
```

```
LOG_LEVEL=$LOG_INFO
```

```
KPCFG=/etc/keepalived/keepalived.conf
USER=<SSDB 用户名>
PREFIX=/var/lib/ssdb
```

```
函数日志 { lvl=$1
msg= $2
如果 [ $lvl -le
$LOG_LEVEL ]
然后
现在=$(日期) echo
$now[$lvl]$msg >> $LOG
是
}
```

```
函数 log_error { 日志 $LOG_ERROR
$1
}
函数日志警告 {
日志 $LOG_WARNING $1
}
函数 log_info { 日志 $LOG_INFO
$1
}
函数 log_debug { 日志 $LOG_DEBUG
$1
}
```

```
功能备份 { log_info “转换到备
份状态” runuser -l $USER -c “${PREFIX}/ssdb-server ${PREFIX}/ssdb.conf
-s stop” runuser -l $USER -c “cp ${PREFIX}/ssdb_slave.conf ${PREFIX}/ssdb.conf” runuser -l $USER -c “${PREFIX}/ssdb-server
-d ${PREFIX}/ssdb.conf”
```

```
}
```

```
函数故障{log_error “keepalived
处于故障状态”
}
```

```
函数 master { log_info 转换到
MASTER 状态 runuser -l $USER -c ${PREFIX}/ssdb-server ${PREFIX}/
ssdb.conf -s stop runuser -l $USER -c cp ${PREFIX}/ssdb_master.conf ${PREFIX}/ssdb.conf
```

```
运行用户-l $USER-c “${PREFIX}/ssdb-server-d ${PREFIX}/ssdb.conf”
}
```

```
案例 ${ENDSTATE}
BACKUP )# 执行操作以转换到 BACKUP 状态
备份
退出 0
;
“FAULT” )# 执行转换为 FAULT 状态的操作
过错
退出 0
;
“MASTER” )#执行转换为MASTER状态的操作
掌握
退出 0
;
*) echo VRRP ${TYPE} ${NAME} 的未知状态 ${ENDSTATE}
出口 1
;
埃萨克
```

Keepalived 配置,指定 (初始)备份

/etc/keepalived/keepalived.conf

该文件与主节点上的同一文件几乎完全相同。例外情况：

- 优先级 赋予其较低的初始优先级。
- 它不包含nopreempt选项。一旦备份服务器由于原始主服务器故障而成为主服务器,系统应允许一些人为干预,然后再将原始服务器恢复为主状态。

```
vrrp_instance VRRP1 { 状态备份
    接口 enp0s8
    virtual_router_id 41 优先级 100
    advert_int 1 通知 /
    var/lib/ssdb/
    notify.sh

    身份验证 { auth_type PASS
        auth_pass 1234
    }

    虚拟 IP 地址 { 192.168.56.120
        dev enp0s8 标签 enp0s8:vip
    }
}
```

备份服务器的 /var/lib/ssdb/notify.sh与主服务器相同。

主-主复制

[概述](#)

确保SSDB保持高可用性的另一种方法是设置主主复制，并在两个SSDB服务器前配置一个理解Redis协议的代理。代理负责监控两个服务器的运行状况，并从后端移除故障服务器。

以下简化的示例在两个SSDB服务器前使用单个HAProxy实例。

所需软件包

- [SSDB](http://ssdb.io/) (<http://ssdb.io/>) 。在下面显示的示例中，假设安装了1.9.2或更新版本。
- [HAProxy](http://www.haproxy.org/) (<http://www.haproxy.org/>)

先决条件

根据您使用的 Linux 发行版的适用步骤在两台服务器上安装SSDB。在另一台服务器上安装HAProxy。请注意，Keepalived (<http://www.keepalived.org/>)可用于配置高可用性HAProxy服务器池。

配置

SSDB 配置,第一个 Master

笔记：

- 仅显示与主-主复制相关的配置。

```
# ssdb-server config ## ssdb-server
config 必须通过 TAB 缩进!
```

```
# 相对于此文件的路径,目录必须存在 work_dir = ./var pidfile = ./var/ssdb.pid
```

服务器：

```
ip:0.0.0.0 端口:8888
```

```
拒绝:全部 允许:
```

```
127.0.0.1
```

```
# 例如,192.168.56 允许:<ip 地址前缀
```

```
>
```

复制:binlog:是

```
# 将同步速度限制为 *MB/s, -1:无限制 sync_speed: -1
```

从属：

```
id:svc_2 类型:镜
```

```
像
```

```
主机:<其他主主机的主机名>
```

```
端口:8888
```

SSDB 配置 ,Second Master

笔记：

- 仅显示与主-主复制相关的配置。

```
# ssdb-server config # 必须用 TAB 缩进!
# 相对于此文件的路径,目录必须存在 work_dir = ./var pidfile = ./var/ssdb.pid
```

服务器:

ip:0.0.0.0 端口:

8888 拒绝:全部

允许:127.0.0.1

例如,192.168.56 允许:<ip 地址前

缀>

复制:binlog 是

```
# 将同步速度限制为 *MB/s, -1:无限制 sync_speed: -1
```

从属:

id:svc_1 类型:镜

像

主机:<其他主主机的主机名>

端口:8888

HAProxy 配置

笔记:

- 仅显示与SSDB相关的配置。
- SSDB支持Redis网络协议,可以使用Redis客户端连接SSDB服务器并对其进行操作,Zimbra Collaboration 就是这么做的。

默认 REDIS

模式 tcp 超时连
接 4s

服务器超时30秒
客户端超时 30s

```
前端 ft_redis bind <已发布的 ip 地  
址>:8888 名称 redis default_backend bk_redis
```

后端 bk_redis 选项 tcp-check

服务器 R1 <first-master-ip-
address>:8888 检查 inter 1s 服务器 R2 <second-master-ip-address>:8888 检查 inter 1s

多主扩展/复制

概述

本文档不会介绍多主配置的详细信息。实际上,您将使用上述说明安装和配置多个独立的SSDB主从对。每对将负责存储总键空间的一个子集。

与主-主配置一样，SSDB服务器池中的所有对都将由了解Redis协议的代理服务进行前端处理。它还必须能够一致地对呈现的数据密钥进行哈希处理，以便与特定密钥相关的所有请求始终路由到相同的主-从对。

其中一个产品是twemproxy (<https://github.com/twitter/twemproxy>)来自Twitter (<https://github.com/twitter>)。

LDAP 属性

SSDB 后端使用资源池来管理对SSDB服务器的访问;尝试进行短暂数据操作的线程必须首先从此池中获取资源。为此,引入了两个 LDAP 属性来控制池配置。

`zimbraSSDBResourcePoolSize`控制池的大小。这决定了有多少个客户端线程可以同时执行临时 API 操作。默认情况下,此值设置为 0,这会导致池大小不受限制。

`zimbraSSDBResourcePoolTimeout`控制线程在抛出异常之前等待资源的时间。默认值为 0,表示不超时。当池大小为 0 时,此属性无效,因为线程永远不必等待资源释放即可执行临时数据操作。

当池大小有限时,建议使用非零超时值。否则,丢失的SSDB连接可能会导致 `mailboxed` 线程无限期地处于阻塞状态,即使在重新建立连接之后也是如此。通常,资源池的大小应使邮箱服务器不会缺乏资源。

使所有用户会话无效

根据您的环境,运行此命令将需要一些时间,不会显示进度指示。使用 `cd` 命令切换到 SSDB 安装目录:

```
./ssdb-cli -h 127.0.0.1 -p 8888 flushdb
```

SSDB 复制可能会受到影响,因此最好先中断复制,并在 SSDB 的单个主机上运行此命令,然后恢复 SSDB 复制。

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

影响 SSDB 服务器负载的 Zimbra Collaboration 生产负载的主要特征是 Zimbra Collaboration Web Client 和第三方 SOAP 客户端发送的身份验证请求频率和 SOAP 请求频率。每个身份验证请求都会导致 SSDB 执行 2 或 3 次写入操作。写入操作会更新 `zimbraLastLogonTimestamp`、`zimbraAuthTokens` 和 `zimbraCsrfTokenData` 值。请注意,只有在使用支持 CSRF 的 SOAP 客户端 (如 Zimbra Collaboration Web Client) 时才会更新 `zimbraCsrfTokenData`。每个经过身份验证的 SOAP 请求都会导致 SSDB 执行 2 次读取操作。

最低推荐 SSDB 配置

我们建议您的 SSDB 服务器至少配备 2GB RAM 和 1 个 CPU。如果您计划在 SSDB 服务器上运行其他工具 (例如监控和配置管理),请考虑增加内存并添加一个 CPU 核心以容纳其他软件。查看Zimbra 和 SSDB 身份验证负载测试

(<https://github.com/Zimbra/zm-ssdb-ephemeral-store/wiki/Zimbra-and-SSDB-Authentication-Load-Tests>)更多
信息。

结论

对于临时数据存储需求可放在单个实例中的安装,简单的主从复制是最容易实现的,并且需要的资源最少。主从复制确实允许请求在两个主服务器之间进行负载平衡;但是,每个主服务器也会不断地从另一个主服务器进行复制,因此SSDB必须做额外的工作来保持一致性。

服务等级和账户

分配给帐户的服务等级 (COS) 决定了用户帐户的默认属性以及要启用或拒绝的功能。每个帐户都分配有一个 COS。COS 控制邮箱配额、邮件生存期、密码限制、附件阻止和服务器池使用情况。

COS 是一个全局对象，不限于特定的域或域集。

您可以从管理控制台创建和编辑服务类别：

管理控制台：

主页→配置→服务等级→ 操作系统

使用 COS 管理功能和设置

安装 Zimbra Collaboration 时会创建一个默认 COS。您可以修改默认 COS 并创建新的个。

从 COS,您可以管理以下功能：

- 用户可以访问的功能和偏好设置。
- 用户可以访问的主题和 Zimlet。
- 高级设置包括附件设置、配额和密码登录策略。
- Web 应用程序版本（现代 Web 应用程序和经典 Web 应用程序）。
- Web 服务和桌面客户端（EWS、MAPI 等）。
- 离线模式。
- 保留政策。

例如,您可以创建一个高管 COS,配置为启用所有功能、提供无限邮箱配额并且永不清除邮件。还可以创建另一个普通员工 COS,它仅启用邮件功能、设置邮箱配额并且每 60 天清除一次邮件。将帐户分组到特定 COS 允许您批量更新或更改帐户功能。因此,当 COS 更改时,分配给该 COS 的所有帐户都会更改。

如果没有为新帐户明确设置 COS,或者分配给用户的 COS 不再存在,则会自动分配默认COS。

您可以创建一个 COS,并将其指定为该域中创建的所有账户的默认 COS。您可以创建不同的 COS,并指定哪些 COS 可用于该域。如果域未定义 COS,并且您未指定 COS,则在创建账户时会自动分配原始默认 COS。

某些 COS 设置可以被全局设置或用户设置覆盖。例如：

- 可以从 Zimbra Classic Web App 中的用户偏好设置中更改是否将发出的消息保存到“已发送”消息。
- 附件阻止设置为全局设置可以覆盖 COS 设置。

分配给帐户的某些 COS 设置不会强制用于 IMAP 客户端。

选择功能和首选项

COS 的所有可用功能均显示在“功能”页面中。从那里，您可以选择或取消选择您不想包含在 COS 中的功能。

在帐户级别所做的更改将覆盖分配给该帐户的 COS 中的规则。

您可以在“首选项”页面中定义用于保存和查看消息的初始首选项。您还可以为经典 Web 应用程序和现代 Web 应用程序选择特定的语言环境。如果未指定语言环境，则浏览器语言环境为默认语言环境。

要了解功能和首选项的描述，请参阅自定义帐户。

禁用偏好设置

默认情况下，“首选项”处于启用状态，用户可以修改为其配置的默认首选项帐户。

作为管理员，您可以禁用“首选项”。这样，“首选项”页面将不会显示在用户邮箱中：因此，他们无法修改为其帐户设置的默认功能配置。

用户可以在“设置”下的现代 Web 应用程序中更改其首选项。禁用首选项不会对现代 Web 应用程序产生任何影响。

设置默认时区

当使用经典 Web 应用程序或现代 Web 应用程序时，计算机上的时区设置将用作显示收到的消息和日历活动的时间戳。

日历设置中的时区值仅用于识别工作时间的开始和结束时间，以及它们在空闲/忙碌信息中的显示方式。

使用服务器池

在具有多个邮箱服务器的环境中，COS 用于将新帐户分配给邮箱服务器。

配置 COS 时，您可以选择要添加到服务器池的服务器。在每个服务器池中，随机算法会将新邮箱分配给任何可用的服务器。

在新建帐户向导的服务器字段中创建帐户时，您可以将帐户分配给特定的邮箱服务器。取消选中自动并在服务器字段中输入邮箱服务器。

设置账户配额

帐户配额是帐户允许的存储限制。电子邮件、通讯簿、日历、任务和公文包文件都会影响配额。帐户配额可从管理控制台为 COS 或单个帐户设置。

如果将配额设置为 0，则帐户没有配额。

查看账户配额

若要查看域中所有账户的账户配额：

管理控制台：

主页→配置→域→

领域 → 邮箱配额

接近最大配额时通知用户

可以通知用户其邮箱已接近配额。可以设置配额百分比并修改警告消息文本：转到指定服务类的配额容器：

管理控制台：

主页→配置→服务等级→

操作系统 → 高级 → 配额

当达到显示/配置的阈值时，会向用户发送配额警告消息。

在域中设置配额

您可以为域名设置最大邮箱配额。域名邮箱配额的默认设置是无限制的。域名配额是域名内所有邮箱可使用的最大存储量。

您还可以设置总配额。域中所有帐户的配额总和可以超过总配额的大小。

可以设置总计配额策略，用于处理在达到总计配额后发送或接收的消息。策略选项包括：

- 继续允许照常发送和接收消息。
- 不允许发送消息。
- 不允许发送或接收消息。

当配额在配置的总配额百分比范围内时，可以自动发送通知。cron tab 作业每天运行以检查总配额百分比，如果已达到该百分比，则发送配额警告电子邮件。

当设置了域配额时，帐户的有效配额是域或帐户的最小配额设置。

要配置域配额，请转到指定域的域配额设置容器：

管理控制台：

主页→配置→域→

领域 → 高级 → 域名配额设置

管理超额配额

您可以设置当用户的邮箱超出配置的配额时如何处理邮件传递。默认行为是 MTA 暂时将邮件发送到延迟队列。当邮箱有足够的空间时，邮件将被传递。您可以更改此行为，让邮件退回给发件人，而不是先发送到延迟队列，或者您可以配置即使超出配额也会将邮件发送到邮箱。

要退回消息而不是将其发送到延迟队列：

```
zmprov mcf zimbraLmtpPermanentFailureWhenOverQuota TRUE
```

重击

即使超出配额也要将消息发送到邮箱：

```
zmprov mc {cos-name} zimbraMailAllowReceiveButNotSendWhenOverQuota TRUE
```

重击

当此属性设置为 TRUE 时,超出配额的邮箱仍可接收新邮件和日历邀请。此配额绕过仅适用于邮件。所有其他邮件项目仍受配额影响。

管理密码

如果您使用内部身份验证,您可以从帐户工具栏快速更改帐户密码。必须告知用户新密码才能登录。

如果使用 Microsoft Active Directory (AD) 进行用户身份验证,则必须禁用 COS 中的更改密码功能。AD 密码策略不由 Zimbra 管理。

如果您想确保用户更改您创建的密码,您可以为该帐户启用“必须更改密码”。用户下次登录时必须更改密码。

密码限制可以在 COS 级别或帐户级别设置。您可以配置设置以要求用户创建强密码并定期更改密码,还可以设置参数以在输入错误密码时锁定帐户。

将用户引导至您的“更改密码”页面

如果身份验证配置为外部身份验证,您可以配置 Zimbra Collaboration,以便在用户更改密码时将用户引导至您的密码更改页面。您可以将此 URL 设置为全局设置或每个域的设置。

将zimbraChangePasswordURL属性设置为您的密码更改页面的 URL。

在经典 Web 应用程序中,首选项→常规下的更改密码链接到此 URL,当密码过期时,用户将被发送到此页面。在现代 Web 应用程序中,更改密码显示在帐户头像菜单下,它也会链接到提供的 URL。

修改域的密码:

```
zmprov md example.com zimbraChangePasswordURL https://auth.example.com
```

重击

配置密码策略

如果为域配置了内部身份验证,您可以要求用户创建强密码,以防范简单的密码窃取攻击。如果用户在配置的最大尝试次数后仍未登录,则可能会被锁定其帐户。

要设置密码策略,请使用指定服务类的密码容器:

管理控制台:

主页→配置→服务等级→ 操作系统→高级→密码

可以配置的密码设置如下所列。

表密码选项 34.

| 密码选项 | 描述 |
|------|----|
| | |

| 密码选项 | 描述 |
|-------------|---|
| 最小/最大密码长度 | 指定密码所需的长度。 默认最小值和最大值分别为 6 和 64 字符。 |
| 密码最短/最长使用期限 | 配置密码过期日期。用户可以 随时更改密码 最小值和最大值。他们必须在以下情况下更改它： 已达到密码最长使用期限。 |

以下设置要求用户增加密码的复杂性。

| | |
|---------------|--|
| 最小大写字符数 | 大写字母 A - Z |
| 最少小写字符数 | 小写 a - z |
| 最少标点符号 | 非字母数字,例如 !、\$、#、&、% |
| 最小数字字符数 | 十进制数字 0 - 9 |
| 最少数字字符或标点符号 | 非字母数字和数字的组合 |
| 唯一密码历史记录的最小数量 | 用户必须输入的唯一新密码数量 在重新使用旧密码之前先创建。 |
| 密码最短使用期限 (天) | 密码更改间隔的最少天数 |
| 密码最长使用期限 (天) | 密码更改间隔的最长天数 |
| 密码已锁定 | 用户不能更改密码。这应该是 如果身份验证是外部的,则设置。 |
| 必须更改密码 | 用户首次登录时必须更改密码。 |
| 更改密码 | 启用后,用户可以随时更改密码 密码年龄设置内的时间 帐户偏好设置选项卡。 |

阻止常用密码

阻止常用密码功能使组织能够限制常用密码的使用

创建用户时。常用密码列表保存在服务器上,当创建用户时会引用该列表

管理员尝试创建一个具有常用密码的用户。

该功能由本地配置属性zimbra_block_common_passwords_enabled和默认
值设置为FALSE。

启用此功能后,它还将阻止最终用户将其密码设置为常用的
密码可通过以下选项:

- 个人资料→在右上角的现代 Web 应用程序中更改密码。
- 登录页面上的“忘记密码”选项。(如果为用户启用了“忘记密码”功能)。

启用阻止常用密码功能

1.以zimbra用户身份登录：

与 - zimbra

1. 将 localconfig zimbra_block_common_passwords_enabled 值设置为TRUE：

```
zmlocalconfig -e zimbra_block_common_passwords_enabled=TRUE
```

1.重启邮箱服务：

zmmailboxdctl 重启

启用此功能后,如果您尝试创建用户,则创建。

密码无效

显示错误,并且用户无法

管理登录策略

您可以设置指定锁定期限内账户被锁定前的最大登录尝试失败次数
时间。此类策略用于防止密码攻击。

要设置用户登录策略,请使用指定服务类的归档登录策略容器：

管理控制台：

主页→配置→服务等级→

操作系统→高级→登录失败策略

表登录策略选项

| 登录策略选项 | 描述 |
|-----------------------|--|
| 启用登录失败锁定 | 这将启用“登录失败锁定”功能。您可以配置以下设置。 |
| 允许连续登录失败的次数 | 账户登录失败的次数 锁定。默认值为 10。如果设置为 0,则帐户从未被锁定。 |
| 锁定帐户的时间 | 帐户被锁定的时间。如果设置了 为 0,帐户将被锁定,直到正确的 输入密码,或管理员手动 更改帐户状态并创建新的 密码保留时间。默认为1小时。 |
| 登录失败必须发生的时间窗口 锁定账户 | 持续时间,之后的次数 连续失败的登录尝试将被清除 日志。如果设置为 0,用户可以继续尝试 验证身份,无论连续失败多少次 发生登录尝试的时间间隔。默认值为 1 小时。 |

[关于双重身份验证](#)

借助双因素身份验证 (FA) 功能,您可以向 COS 和/或用户应用额外的安全策略帐户,以便在尝试访问系统时提供另一层身份验证。此功能必须是在管理控制台中启用或禁用,以管理适用于用户邮箱的 2FA 功能。



有关更多信息,请参阅双因素身份验证 (https://wiki.zimbra.com/wiki/Zimbra_Two-factor_authentication) 。

管理会话超时策略

您可以根据各种条件设置分配给用户会话的时间段。

要设置会话超时策略,请使用指定服务类的超时策略容器:

管理控制台:

主页→配置→服务等级→ 操作系统 →高级→超时策略

表会话超时策略选项

| 会话超时策略选项 | 描述 |
|----------------|--|
| 管理控制台身份验证令牌有效期 | 设置包含管理员身份验证令牌的浏览器 cookie。管理员可以打开管理控制台,而无需再次登录,直到身份验证令牌过期。默认为 12 小时。 |
| 身份验证令牌有效期 | 设置包含 Web 应用身份验证令牌的浏览器 cookie。用户可以无需登录即可打开经典 Web 应用程序或现代 Web 应用程序直到身份验证令牌过期为止。默认值为 2 天。到期后,显示登录页面,用户必须登录才能继续。 |
| 会话空闲生存期 | 如果没有活动发生,用户会话保持活动状态的时间长度。活动包括任何可点击的鼠标操作,例如查看文件夹内容或单击按钮。默认为无限制。 |

[您可以通过管理控制台的“过期会话”链接手动使用户的 Web 客户端会话过期。这强制帐户的当前会话立即过期。]

管理默认外部 COS

默认外部COS分配给外部虚拟账户,这些虚拟账户在外部用户接受Zimbra 邀请用户分享他们的日历或公文包内容。

此帐户未在服务器上配置,但外部用户可以登录经典 Web 应用程序,创建显示名称并设置密码以查看共享项目。唯一可用的文件夹是他们拥有的内容
访问。

默认的外部COS配置了以下常规功能:更改密码、更改 UI 主题、HTML 编写、导出和搜索。未配置任何主要功能。

现代 Web App 目前不支持外部用户登录。

自定义帐户

本章介绍可以从指定的 COS 或个人帐户配置的帐户功能和用户偏好。

已为 Zimbra Classic Web App 用户启用邮箱功能。使用 IMAP 或 POP 客户端时,用户可能无法使用这些功能。

以下部分中提到的某些功能可能目前不适用于现代 Web 应用程序。

对于经典 Web 应用程序,Chrome 85 及更高版本不再支持离线模式。

用户仍可继续使用以前版本的浏览器的离线模式。

消息传递和协作应用程序

您的 COS 配置和将 COS 分配给帐户决定了帐户功能的默认设置以及应用于帐户组的限制。各个帐户可以进行不同的配置,并且您所做的任何更改都会覆盖 COS 设置。当您更新 COS 时,更改不会反映在具有 COS 覆盖的帐户中。

电子邮件消息功能

您可以配置启用哪些电子邮件消息传递功能。然后,用户可以将许多已启用的功能作为首选项进行管理。

默认情况下,用户管理自己的偏好设置,但您可以通过管理选择不允许用户修改其帐户偏好设置。目前支持的 Web 应用程序电子邮件消息传递功能在以下位置列出并描述:

电子邮件功能。

表格电子邮件功能 37.

| 电子邮件消息功能描述 | |
|------------|--|
| 邮件 | <p>启用电子邮件应用程序。默认启用。</p> <p>看 操作系统 → 功能 → 管理控制台中的主要功能容器。</p> |
| 对话 | <p>消息可以按照共同线索分组到对话中。默认是通过引用标头将消息分组到对话中。如果没有引用标头,则使用主题来确定对话线索。</p> <p>要更改默认值,请从 COS 或个人帐户更新属性 <code>zimbraMailThreadingAlgorithm</code>。请参阅 更改对话线程默认值。</p> <p>如果启用此功能,对话视图将是默认视图。您可以在 COS 首选项页面更改默认视图。用户也可以更改默认视图。</p> <p>看 操作系统 管理控制台中的 → 功能 → 邮件功能容器。</p> |

| 电子邮件消息功能描述 | |
|----------------|---|
| HTML 撰写 | <p>用户可以使用 HTML 编辑器撰写电子邮件。他们可以指定默认字体设置作为首选项。</p> <p>看 操作系统 → 首选项 → 在管理控制台中撰写邮件容器。</p> |
| 草稿自动保存间隔 | <p>保存草稿消息的频率。默认为每 30 秒。用户无法改变频率，但他们可以关闭保存草稿功能。</p> <p>看 操作系统 → 首选项 → 在管理控制台中撰写邮件容器。</p> |
| 邮件稍后发送 | <p>启用后，用户可以选择“稍后发送”以稍后发送消息。用户配置发送日期和时间。消息保存在草稿箱中文件夹。</p> <p>看 操作系统 管理控制台中的 → 功能 → 邮件功能容器。</p> |
| 消息优先级 | <p>启用后，用户可以设置消息的优先级。收件人查看来自 Web 应用程序会看到优先级标志是高还是低。</p> <p>看 操作系统 管理控制台中的 → 功能 → 邮件功能容器。</p> |
| 启用附件 索引 | <p>附件已编入索引。编入索引的附件可供搜索。</p> <p>看 操作系统 → 管理控制台中的高级 → 附件设置容器。</p> |
| 允许用户指定 转寄地址 | <p>您可以指定用户可以使用的默认转发地址。用户可以从其帐户的“首选项”选项卡中更改转发地址。</p> <p>您还可以指定对用户隐藏的转发地址。 发送到该帐户的消息将立即转发到指定转寄地址。</p> <p>看 操作系统 管理控制台中的 → 功能 → 邮件功能容器。</p> |
| 外出回复 | <p>用户可以创建电子邮件消息，自动回复收到的消息。默认情况下，每七天仅向每个收件人发送一次消息，无论该人向该地址发送了多少封邮件。此设置可以在 COS 首选项页面的“外出办公缓存有效期”字段中进行更改。</p> <p>看 操作系统 管理控制台中的 → 功能 → 邮件功能容器。</p> |
| 新邮件通知 | <p>允许用户指定接收新邮件通知的地址。他们可以打开或关闭此功能并从帐户偏好设置中指定一个地址选项卡。</p> <p>请参阅自定义通知电子邮件，了解更改电子邮件模板。</p> <p>看 操作系统 管理控制台中的 → 功能 → 邮件功能容器。</p> |

电子邮件消息功能描述

| | |
|------------------------|---|
| 人 | <p>启用后,用户可以创建其他帐户名来管理不同的角色。可以选择账户别名作为从该账户发送的邮件的发件人姓名。可以为个人账户设置一个专属签名。可以创建的角色数量可以根据您的要求。最小值为 0,默认值为 20 (<code>zimbraIdentityMaxNumEntries</code>)。</p> <p style="text-align: center;">此功能仅在经典 Web 应用程序中受支持。</p> <p>看 操作系统 管理控制台中的→功能→邮件功能容器。</p> |
| 邮件最大长度 签名 | <p>签名的最大字符数。默认为 1024 人物。</p> <p>用户可以创建的签名数量配置在 <code>zimbraSignatureMaxNumEntries</code>。</p> <p>看 操作系统 →首选项→在管理控制台中撰写邮件容器。</p> |
| 高级搜索 | <p>允许用户按日期、域、状态、标签、大小构建复杂的搜索，附件、Zimlets 和文件夹。</p> <p>看 操作系统 →功能→管理控制台中的搜索功能容器。</p> |
| 已保存的搜索 | <p>用户可以保存他们之前执行或构建的搜索。</p> <p>看 操作系统 →功能→管理控制台中的搜索功能容器。</p> |
| 初始搜索偏好 启用后,可以更改默认搜索邮箱。 | <p>看 操作系统 →管理控制台中的功能→常规选项容器。</p> |
| 外部 POP 访问 | <p>启用后,用户可以直接从他们的 Zimbra 帐户。他们将外部帐户地址添加到他们的帐户设置。</p> <p>看 操作系统 管理控制台中的→功能→邮件功能容器。</p> |
| 外部 IMAP 访问 | <p>启用后,用户可以直接检索其 IMAP 帐户的电子邮件从他们的 Zimbra 帐户。他们可以将外部帐户地址添加到他们的帐户设定。</p> <p>看 操作系统 管理控制台中的→功能→邮件功能容器。</p> |
| 此帐户的别名 | 您可以为该帐户创建别名。用户无法更改此设置。 |

电子邮件消息功能描述

| | |
|---|---|
| 邮件过滤器 | <p>用户可以定义一组规则和相应的操作来应用于传入和发送邮件和日历约会。当收到电子邮件消息时匹配过滤规则的条件，则执行与适用该规则。</p> <p>在用户收到邮件之前，垃圾邮件检查已经完成 邮件过滤器运行。被识别为垃圾邮件的邮件被移至垃圾邮件文件夹。为了避免邮件被错误地标记为垃圾邮件，用户可以从偏好设置邮件中创建垃圾邮件白名单文件夹来标识不应标记为的电子邮件地址 垃圾邮件。</p> |
| | <p>看 操作系统 管理控制台中的→功能→邮件功能容器。</p> |
| 标记 | <p>用户可以创建标记并将其分配给公文包中的邮件、联系人和文件文件夹。（此功能仅在经典 Web 应用程序中受支持。）</p> <p>看 操作系统 管理控制台中的→功能→邮件功能容器。</p> |
| 启用键盘快捷方式 | <p>用户可以在邮箱中使用键盘快捷键。快捷键列表可以从用户名下拉菜单中查看经典 Web 应用程序。</p> <p>键盘快捷键在现代 Web 应用中始终可用。快捷键列表可以通过输入来查看 。</p> <p>看 操作系统 →管理控制台中的首选项→常规选项容器。</p> |
| 全局地址列表 (GAL) 使用权 | <p>用户可以访问公司目录来查找其电子邮件名称。</p> <p>看 操作系统 →功能→管理控制台中的常规功能容器。</p> |
| GAL 自动完成 启用后，用户可在撰写邮件标题和姓名时输入几个字母， GAL 按使用情况排序显示。另请参阅自动完成排名名称。 | <p>看 操作系统 →功能→管理控制台中的常规功能容器。</p> |
| Web 离线支持 应用程序 | <p>启用后，用户可以使用离线模式在没有网络的情况下访问他们的数据使用 Zimbra Modern Web App 时的连接。另请参阅离线模式。</p> <p>看 操作系统 →功能→管理控制台中的常规功能容器。</p> |
| IMAP 访问 | <p>用户可以使用第三方邮件应用程序通过 IMAP 访问自己的邮箱协议。</p> <p>您可以从 COS 或帐户高级页面、数据来源→ IMAP 轮询间隔部分。默认情况下未设置轮询间隔。</p> <p>看 操作系统 管理控制台中的→功能→邮件功能容器。</p> |

电子邮件消息功能描述

| |
|--|
| <p>POP3 访问</p> <p>用户可以使用第三方邮件应用程序通过 POP 协议访问邮箱。当他们检索 POP 电子邮件消息时,消息和附件将保存在 Zimbra 服务器上。</p> <p>用户可以从“首选项”→“邮件”页面进行配置</p> <ul style="list-style-type: none"> • 如何下载消息。 • 是否包含他们的垃圾邮件。垃圾邮件将下载到他们的收件箱中。 • 如何从 POP 帐户中删除消息。 <p>您可以从 COS 或帐户高级页面的数据源→ POP3 轮询间隔部分设置轮询间隔。默认情况下不设置轮询间隔。</p> <p>看 操作系统管理控制台中的→功能→邮件功能容器。</p> |
|--|

自动完成排名名称

自动完成功能会按顺序显示姓名,最常回忆的联系人会列在最顶部。如果最先出现的联系人姓名不应列在最顶部,用户可以点击“忘记”,然后重新对联系人姓名进行排名。(仅限经典 Web 应用程序。)

用户管理的电子邮件偏好设置

本节列出的许多首选项的默认行为都可以从 COS 或帐户首选项页面进行设置。用户可以从中帐户首选项或经典 Web 应用程序或现代 Web 应用程序中的设置中修改以下邮件首选项。

- Web 客户端检查新消息的频率(以分钟为单位)：
 - 每隔...检查一次新邮件
- 设置或更改电子邮件消息提醒。可以设置提醒以播放声音、在收到消息时突出显示邮件选项卡以及闪烁浏览器(具体取决于他们使用的 Web 应用程序)。
- 设置经典 Web 应用和现代 Web 应用的显示语言。如果 Zimbra Collaboration 上安装了多个语言区域,用户可以选择与浏览器语言设置不同的区域。

现代 Web 应用程序当前支持经典 Web 应用程序中可用的部分语言,如果用户的语言区域设置尚不受支持,则会恢复为美国英语。

- 是否将发出的邮件副本保存到“已发送”文件夹。
- 是否保存转发邮件的本地副本或将它们从邮箱中删除。(目前只有经典 Web 应用程序可以管理此设置。)
- 是否在单独的窗口中撰写消息。(此功能仅在经典 Web 应用程序中受支持。)
- 对于包含 HTML 的消息,是否以 HTML 格式查看邮件,还是以纯文本格式查看消息。(此功能仅在传统 Web 应用程序中受支持。)
- 当请求时是否发送已读回执。

- 调整打印消息的默认字体大小。默认值为 12 点。(此功能仅在经典 Web 应用程序中受支持。)
- 用户可以设置自己的垃圾邮件选项,即白名单和黑名单电子邮件地址,用于过滤来自“首选项邮件”文件夹的传入邮件。每个列表上的白名单和黑名单地址的最大数量为 100。可以使用 CLI zmprov 更改帐户和 COS 的此值。属性为 zimbraMailWhitelistMaxNumEntries 和 zimbraMailBlacklistMaxNumEntries。
- 用户可以在“签名”下修改以下邮件首选项:
 - 是否自动将签名附加到发出的邮件中。
 - 关于如何将签名应用于回复或转发的消息的首选项。

使用导入和导出保存用户数据

从经典 Web 应用程序中的“首选项导入/导出”页面或现代 Web 应用程序中的“帐户→主帐户”下,用户可以导出其所有帐户数据,包括邮件、联系人、日历和任务。通过选择导出选项,他们可以导出帐户中的特定项目并将数据保存到计算机。

帐户数据保存为 tar-gzipped (.tgz) 存档文件,以便可以导入来恢复其帐户。

个人联系人将保存为.csv文件,个人日历文件将保存为.ics文件。数据将被复制,但不会从用户帐户中删除。

可以使用存档程序(例如从同一页导入他们的帐户)查看导出的帐户数据文件。

压缩包 . 任何这些文件都可以

您可以从COS或帐户功能页面的常规功能部分关闭导入/导出功能。

设置 RSS 轮询间隔

用户可以订阅提供 RSS 和播客源的网站,并将更新信息直接发送到邮箱。最多可返回 50 个源。RSS 源计入用户帐户配额。

默认每 12 小时更新一次 RSS 数据。用户可以右键单击 RSS 源文件夹来手动加载新源。

您可以从管理控制台的 COS 或帐户高级页面的数据源→ RSS 轮询间隔部分更改轮询间隔。

联系人功能

Zimbra Contacts 允许用户创建多个联系人列表,并在收到或发送邮件时自动添加联系人姓名。用户可以将联系人导入到他们的通讯录中。

要允许用户共享其邮件文件夹、地址簿和日历,请在
容器的一般特征:

主页→配置→服务等级→

操作系统→特点→一般特点

表 38. 地址簿功能

| 特征 | 描述 | COS/账户标签 |
|----|----|----------|
| | | |

| 特征 | 描述 | COS/账户标签 |
|---------|---|----------|
| 地址簿 | 用户可以创建个人联系人列表。默认情况下，“联系人”列表和“电子邮件联系人”列表是创建。 | 特征 |
| 地址簿大小限制 | 用户总共可以拥有的最大联系人数量 地址簿。0表示无限制。 | 先进的 |

用户可以从其帐户首选项地址簿页面修改以下地址簿首选项。

设置默认行为：

管理控制台：

主页→配置→服务等级→
操作系统 →偏好设置
主页→管理→账户→
帐户 →偏好设置

- 启用自动添加联系人功能,当联系人发送电子邮件至新地址。
- 启用使用联系人选择器查找姓名时使用全局访问列表的功能。
- 启用使用自动完成功能时在共享地址簿中包含 GAL 地址和名称的选项发送消息。

日历功能

Zimbra 日历让用户可以安排约会和会议、建立重复活动、创建多个日历、与他人共享日历以及委派经理访问其日历。他们可以订阅外部日历，并从 Zimbra Classic Web App 或 Modern Web App 查看其日历信息。它们还可以使用日历中的搜索功能来查找约会。

要允许用户共享日历、地址簿和公文包文件,请在一般特征容器。

管理控制台：

主页→配置→服务等级→
操作系统 →特点→一般特点

桌历功能39.

| 日历功能 | 描述 | COS/账户标签 |
|------|---|----------|
| 日历 | 让用户维护自己的日历、安排会议、委托他人访问他们的日历,创建多个个人日历等等。 | 特征 |

| 日历功能 | 描述 | COS/账户标签 |
|----------------|--|----------|
| 团体日历 | <p>未选中“群组日历”时,用户只能创建个人约会和接受会议邀请。不显示“查找与会者”、“日程安排”和“查找资源”选项卡。</p> <p style="text-align: right;">群组日历功能在现代 Web 应用程序中始终可用。</p> | 特征 |
| 嵌套日历 | <p>日历可以嵌套在 Zimbra 文件夹中,例如邮件、联系人和日历文件夹。管理员使用 CLI 创建嵌套日历列表。也可以通过迁移导入嵌套日历分组。请参阅下面的示例。</p> <p style="text-align: right;">此功能仅在经典 Web 应用程序中受支持。</p> | |
| 时区 | <p>设置日历安排使用的时区。 域管理员在“帐户”、“常规信息”页面中进行此项设置。</p> | 偏好设置 |
| 前进日历 邀请特定地址 | <p>您可以指定电子邮件地址来转发用户的日历邀请。用户还可以从“首选项”日历文件夹中指定转发地址。</p> <p style="text-align: right;">此功能仅在经典 Web 应用程序中受支持。</p> <p>接收邀请的账户必须具有共享日历的管理员权限来回复邀请。</p> | 账户转发 |

创建嵌套在“日历名称”文件夹下的日历：

```
zmmailbox -z -m user1 cf -V appointment /日历名称/子日历
```

重击

解决日历约会问题

使用zmcalchk命令检查不同用户对同一会议的日历之间的差异,并发送有关差异的电子邮件通知。

当约会不同步时,您还可以使用此命令通知组织者和/或所有与会者。

更改远程日历更新间隔

远程日历默认每 12 小时更新一次。可以在管理控制台上修改频率。

要在管理控制台中修改日历更新频率,请转到所需的 COS 或帐户高级页面,数据源→日历轮询间隔字段。

禁止与会者编辑约会

与会者可以编辑其日历中的约会,但他们的更改不会影响其他任何人。如果约会组织者进行更改,这些更改将覆盖与会者的编辑。您可以修改 COS 属性 zimbraPrefCalendarApptAllowAttendeeEdit 以阻止与会者编辑其日历中的约会。

```
zmprov mc <角色名称> zimbraPrefCalendarApptAllowAttendeeEdit FALSE
```

重击

此功能仅在经典 Web 应用程序中受支持。

设置其他用户日历首选项

用户可以修改日历首选项表中列出的日历首选项。您可以在 COS 或帐户首选项页面中设置默认行为。

| 日历偏好 | 描述 |
|---------------------------|---|
| 时区 | 用户首选项中显示的时区。请参阅设置默认时区。如果在 COS 中配置了时区,则将忽略域中配置的时区。 |
| 发生 预约显示提醒 | 设置会议纪要之前发送提醒通知。 |
| 初始日历视图 | 设置默认视图。选项包括“日”、“工作周”、“7 天周”、“月”、“列表”或“时间表”。 |
| 一周的第一天 | 设置用户工作周的默认第一天。 |
| 默认预约可见性 | 选项为公开或私人。设置新约会页面上的默认可见性选项。 默认为公开,其他人可以查看预约详情。 当默认值为“私人”时,所有传入的日历邀请都会在用户的日历上标记为私人,并且在共享日历时会隐藏详细信息。 |
| 使用 iCal 委派模型来共享 CalDAV 日历 | 可以配置 Apple iCal 使用 CalDAV 协议访问用户的日历。启用后,共享日历将显示在用户的 iCal 帐户的“委派”选项卡中,并且用户可以委派他人访问他们的日历。 对于自动轮询,可以在 COS 或账户高级页面的数据源→CalDAV 轮询间隔字段中设置轮询间隔。 |
| 启用逾期提醒 | 用户登录 Classic Web App 或 Modern Web App 时,系统会弹出过去两周未关闭的会议提醒的提醒通知。禁用此功能后,Zimbra Collaboration 会默默关闭旧提醒。 |

| 日历偏好 | 描述 |
|--------------------------|---|
| 启用新消息的通知 日历事件 | 当收到新的日历事件时,经典 Web 应用程序中会显示一个弹出窗口。 此功能仅在经典 Web 应用程序中受支持。 |
| 允许向组织者发送取消电子邮件 | 当用户收到无法在预定时间参加的邀请时,他们可以选择点击“建议新时间”并选择其他时间。会议组织者将收到一封包含建议时间的电子邮件。 此功能仅在经典 Web 应用程序中受支持。 |
| 自动添加邀请 PUBLISH 方法 | 日历邀请电子邮件应在日历对象中包含method=REQUEST,但某些第三方电子邮件客户端错误地设置了method=PUBLISH。默认情况下,这些电子邮件不会作为邀请处理。您可以通过启用此选项来放宽规则。 |
| 自动将转发的邀请添加到日历 | 已转发给用户的邀请会自动添加到转发收件人的日历中。 |
| 约会提醒器上的 Flash 浏览器标题 | 当约会提醒弹出时,浏览器会闪烁,直到用户关闭弹出窗口。 此功能仅在经典 Web 应用程序中受支持。 |
| 启用声音预约通知 | 当约会提醒弹出时,用户可以通过电脑上的蜂鸣声得到通知。用户必须安装 QuickTime 或 Windows Media。 此功能仅在经典 Web 应用程序中受支持。 |
| 自动拒绝用户的邀请 被拒绝邀请 用户 | 用户可以配置谁可以向他们发送日历邀请。启用后,将向这些用户发送自动回复消息,让他们知道他们无权邀请该用户。 此功能仅在经典 Web 应用程序中受支持。 |
| 收到邀请后自动添加约会 | 启用后,约会会自动添加到用户的主日历中。 现代 Web 应用程序中不提供此设置。 |

| 日历偏好 | 描述 |
|-----------------------|--|
| 显示拒绝的会议 | <p>启用后,拒绝的约会将以褪色视图显示在经典 Web 应用程序日历上。</p> <p>此设置仅影响 Zimbra Classic Web App。 在现代 Web 应用程序、第三方日历应用程序和移动设备中查看约会的用户可能看不到被拒绝的事件。</p> |
| 通过委托访问通知所做的更改 | <p>委托其日历的用户将收到委托访问权限获得者对约会所做更改的通知。</p> <p>现代 Web 应用程序中不提供此设置。</p> |
| 始终显示迷你日历 | <p>迷你日历会自动显示在日历视图中。</p> <p>现代 Web 应用程序中不提供此设置。</p> |
| 创建新约会时使用 QuickAdd 对话框 | <p>启用后,当用户双击或拖动 Zimbra Classic Web App 中的日历时,将显示 QuickAdd 对话框。</p> <p>QuickAdd 在现代 Web 应用程序中始终可用。</p> |
| 显示时区列表 预约视图 | <p>启用后,时区列表将与事件时间一起显示在事件编辑器中,让他们有机会在预约时更改时区。</p> |

设置 Zimbra 任务

Zimbra Tasks 允许用户创建待办事项列表并管理任务直至完成。

要允许用户共享其任务列表,请在功能页面中启用共享。任务列表可以与个人、群组和公众共享。

此功能仅在经典 Web 应用程序中受支持。

要启用或禁用任务功能:

管理控制台:

| | |
|-------------|-----------|
| 主页→配置→服务等级→ | 操作系统 → 特点 |
| 主页→管理→账户→ | 帐户 → 特点 |

Zimbra Classic Web 应用程序用户界面主题

Zimbra Classic Web App 用户界面的外观可以更改。Zimbra 包含许多 Zimbra 主题,您可以创建其他主题。您可以选择一个主题作为默认主题,也可以选择用户可自定义其用户体验的主题。要开发主题,请参阅颜色和徽标管理。

此功能仅在经典 Web 应用程序中受支持。

以下主题使用选项可以从 COS 或个人帐户进行配置。

- 限制用户只能使用一个主题

在“功能”页面上,取消选中“更改 UI 主题”。经典 Web 应用主题是“主题”页面上“当前 UI 主题”字段中列出的主题。

- 让用户访问任何已安装的 Zimbra 主题

如果选中“更改 UI 主题”,则用户可以访问“可用 UI 主题”列表中列出的任何主题。

两因素认证

双重身份验证(2FA)功能允许您配置一组第二组安全要求,这些要求可能适用于环境中的任何或所有关键邮箱或用户。您可以为用户帐户和/或服务类别设置2FA。

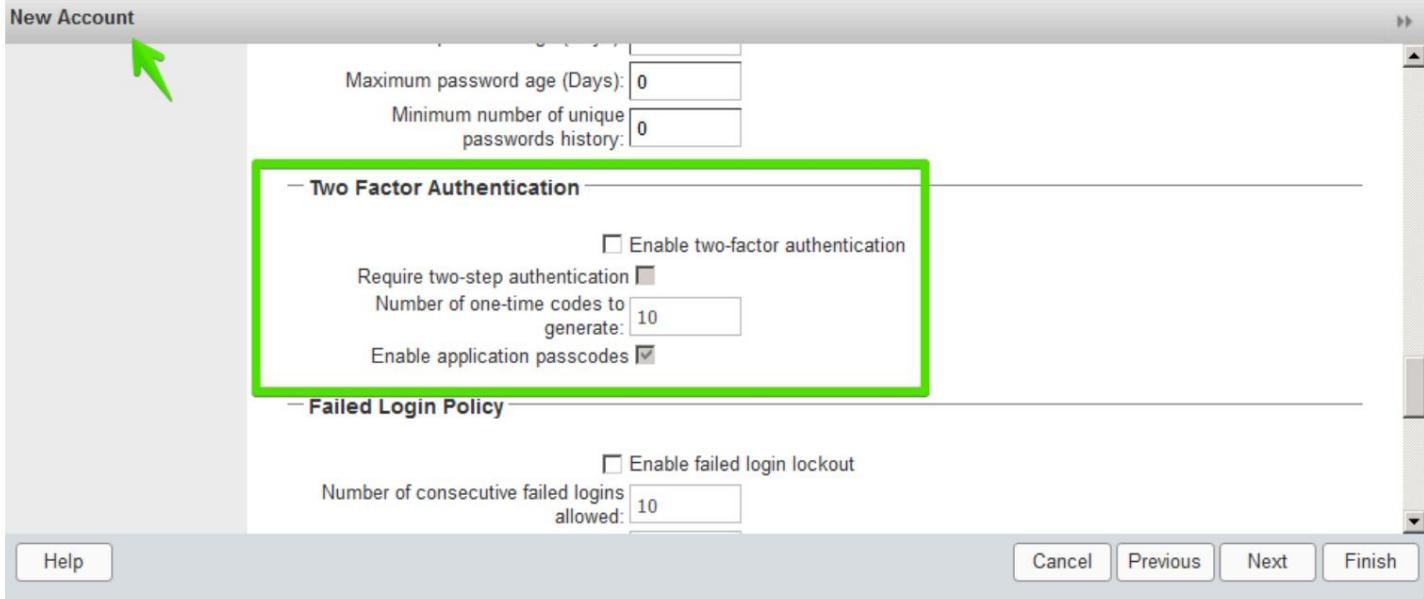
新用户帐户双重认证

在新用户帐户的向导设置中,您将找到2FA的设置和其他高级选项。

管理控制台:

首页→3 添加账户→1. 添加账户

下一个直到“高级”,向下滚动到“双重身份验证”



有关参数描述,请参阅双因素身份验证参数。

现有用户帐户的双重身份验证

对于现有用户帐户,您可以从高级选项中应用2FA设置。

管理控制台:

主页→管理→账户

在帐户的可编辑配置中找到双重身份验证容器:

1. 选择 帐户 从帐户列表中。

2. 从齿轮图标中选择编辑。

一般信息

帐户 现已显示。

3. 从左侧面板中选择高级。

4. 向下滚动到主面板中的双重身份验证容器。

The screenshot shows the Zimbra Administration interface. The left sidebar has a tree view with nodes like 'Accounts', 'General Information', 'Contact Information', etc., under 'anything@jhurley1.us.zimbra.com'. A green arrow points to the 'Advanced' node in the sidebar. The main content area shows account details for 'd.d.sss' (Email: anything@jhurley1.us.zimbralab.com, Quota: 0 MB of unlimited). Below this are several expandable sections: 'Attachment Settings', 'Quotas', 'Data Source', 'Proxy Allowed Domains', 'Password', and 'Two Factor Authentication'. The 'Two Factor Authentication' section is highlighted with a green box. It contains the following settings:

- Enable two-factor authentication:
- Active:
- Require two-step authentication:
- Number of one-time codes to generate:
- Enable application passcodes:

有关参数描述,请参阅双因素身份验证参数。

服务等级双重认证

您可以用来为服务类设置 2FA 的参数包含在其他高级功能中。

要将 2FA 应用于某一类服务,请使用双因素身份验证容器来设置参数。

管理控制台:

主页→配置→服务等级→

操作系统→高级→双因素身份验证

The screenshot shows the Zimbra Administration interface. On the left, there's a sidebar with a tree view of account settings. The 'default' account is selected. Under 'default', the 'Advanced' tab is highlighted with a green arrow. In the main content area, the 'Two Factor Authentication' section is also highlighted with a green border. This section contains four configuration options: 'Enable two-factor authentication' (checked), 'Require two-step authentication' (unchecked), 'Number of one-time codes to generate:' (set to 10), and 'Enable application passcodes' (checked).

有关参数描述,请参阅双因素身份验证参数。

表双因素身份验证参数 40.

| 参数 | 描述 |
|----------------|--|
| 启用双因素身份验证 | 为选定的 COS 启用 (选中)或禁用 (取消选中)此功能帐户。 |
| 需要两步验证 | 对所选 COS 帐户启用 (选中)或禁用 (取消选中)强制使用此功能。 |
| 一次性代码的数量 产生 | 指定帐户尝试访问系统时可查看/使用的 6 位密码的最大数量。初始登录凭据被接受后,密码将提供给帐户。 每个密码的生命周期为 15 秒。 |
| 启用应用程序密码 | 用户可以为不支持双因素身份验证的旧版应用程序生成异常代码。 |

电子邮件作为双因素身份验证的附加因素

电子邮件作为双重身份验证中的附加因素功能允许用户使用其恢复电子邮件作为附加身份验证因素。此功能通过添加额外的验证层来增强帐户安全性。

特征

- 电子邮件作为 2FA 设置:用户可以配置他们的恢复电子邮件作为身份验证的附加因素。
- 验证过程:即使已经验证过,系统也会提示用户验证其恢复电子邮件。
- 后备选项:如果用户无法访问他们的恢复电子邮件,他们可以使用其他 2FA 方法。
- 偏好选择:用户可以在电子邮件和身份验证器应用之间选择他们喜欢的 2FA 方法。

- 管理控制:管理员可以查看和管理用户的 2FA 偏好设置,并在需要时重置 2FA 设置。

将电子邮件配置为 2FA

要将电子邮件配置为 2FA 方法:

1. 导航至安全设置:

- 转到 Zimbra 管理控制台。
- 访问用户或服务等级 (COS) 的安全设置。

2. 启用电子邮件作为 2FA:

- 确保已设置并验证恢复电子邮件字段。如果没有,请提示用户配置并验证其恢复电子邮件。
- 启用电子邮件选项作为有效的 2FA 方法。

当“密码重置功能状态”(zimbraFeatureResetPasswordStatus)未启用时,用户可以直接配置“电子邮件作为2FA”。设置过程中会要求用户输入电子邮件地址(恢复地址)。

管理员可以通过以下方式访问此功能:管理控制台中的帐户或 COS 设置 > 功能 > “密码重置功能状态”。

验证流程

系统会向用户的恢复电子邮件发送验证码。验证后,电子邮件将成为有效的 2FA 方法。每次配置“电子邮件作为 2FA”时,用户都需要验证恢复地址。

后备选项

如果用户无法访问他们的恢复电子邮件,他们可以使用其他配置的 2FA 方法,例如身份验证器应用程序。

管理用户偏好

- 查看用户 2FA 偏好设置:
 - 在管理控制台中,导航到用户的帐户设置。
 - 查看活动的 2FA 方法和用户的首选方法。
- 覆盖用户 2FA 偏好设置:
 - 管理员可以为用户重置或覆盖 2FA 设置。这在出现安全漏洞或出于管理目的时非常有用。

使用命令行选项

- 为用户启用电子邮件作为 2FA:

```
zmprov ma user@example.com zimbraTwoFactorAuthEnabled TRUE zimbraTwoFactorAuthMethodAllowed  
电子邮件  
'zmprov ma user@example.com zimbraTwoFactorAuthEnabled TRUE zimbraTwoFactorAuthMethodAllowed 应用程序'
```

如果尚未配置 2FA 方法且尚未生成用户的内部秘密数据,则命令“zmprov ma zimbraTwoFactorAuthEnabled TRUE”不起作用。

- 相关属性：
 - zimbraFeatureTwoFactorAuthAvailable – 控制用户是否可以配置和使用 2FA。
 - zimbraTwoFactorAuthEnabled 控制用户是否启用了 2FA（应用程序和/或电子邮件方法）。
 - zimbraTwoFactorAuthMethodAllowed 控制哪些方法可作为用户的 2FA 方法。
 - zimbraTwoFactorAuthMethodEnabled – 控制用户（应用程序和/或电子邮件）启用（配置）的方法。

强制实施特定的 2FA 方法

管理员可以使用服务等级 (COS) 设置为用户组强制使用特定的 2FA 方法：

1. 导航到管理控制台中的 COS 设置。
2. 更新 2FA 设置：
 - 启用特定的 2FA 方法（电子邮件或身份验证器应用程序）。
 - 保存更改。

升级时

- 如果升级前使用了使用身份验证器应用程序的 2FA，则升级后 zimbraTwoFactorAuthMethodAllowed 必须具有“app”。空值被视为“app”。
- 如果在升级之前使用了使用身份验证器应用程序的 2FA，并且管理员希望允许用户同时使用应用程序和电子邮件方法，则 zimbraTwoFactorAuthMethodAllowed 必须同时具有“应用程序”和“电子邮件”。
- 如果在升级之前使用了使用身份验证器应用程序的 2FA，并且管理员希望仅允许用户使用电子邮件方法：
 1. 所有帐户都需要禁用 2FA。
 2. 然后 zimbraTwoFactorAuthMethodAllowed 必须设置为“email”。

账户的其他配置设置

启用共享

启用共享功能后，用户可以共享他们的任何文件夹，包括邮件文件夹、日历、地址簿、任务列表和公文包文件夹。

用户指定授予被授予者的访问权限类型。他们可以与内部用户共享，内部用户被授予完全管理员访问权限，外部访客必须使用密码才能查看文件夹内容，以及与公共访问权限，这样任何拥有 URL 的人都可以查看文件夹的内容。

当内部用户共享邮件文件夹时，共享文件夹的副本将放在“概览”窗格上的受让人文件夹列表中。用户可以从其经典 Web 应用程序首选项共享页面管理其共享文件夹。

目前，现代 Web 应用程序仅支持从文件夹和日历上下文菜单进行共享管理。

配置短信通知

经典 Web 应用程序首选项 → 通知页面允许用户配置电子邮件地址或短信提醒，以便向其移动设备接收日历上的任务或会议提醒消息。默认情况下，短信通知处于禁用状态。

短信通知可按域、COS 或单个帐户配置。COS 中设置的短信通知将覆盖域中设置的短信通知。在管理控制台中，此项可在域、COS 或帐户的功能页面上设置。

用户在设置短信提醒时选择地区和运营商。短信/电子邮件网关列表位于 ZmSMS.properties 中。您可以自定义此列表以添加未列出的短信/电子邮件网关。

此功能仅在经典 Web 应用程序中受支持。

配置附件查看

您可以将附件查看规则设置为全局设置、按 COS 设置或针对特定账户。全局设置优先于 COS 和账户设置。您可以从四个选项中选择。

现代 Web 应用程序始终提供高清附件预览，无需用户设置。

表格附件查看功能 41.

| 特征名称 | 描述 | COS/账户标签 |
|------------------------------|----------------------------------|----------|
| 禁用附件 | 无法查看附件。这也可设置为 | 先进的 |
| 从 Web 邮件 UI 查看 | 一个全球性的环境。 | |
| 附件可以是 仅以 HTML 格式查看 | 以其他格式收到的附件将以 HTML 视图。 | 先进的 |
| 附件可以是 仅以原始格式查看 | 用户可能无法打开需要其计算机上没有的 特定应用程序的附件。 | 先进的 |
| 附件可以是 以 HTML 格式查看 原始格式 | 用户可以选择以原始格式打开 或 HTML。 | 先进的 |

当用户尝试离开时显示警告

用户可以点击浏览器中的后退和前进箭头，或关闭浏览器而不退出帐户。

- 如果选中此首选项，则会要求用户确认他们是否要离开他们的帐户。
- 如果未选中此选项，则不会询问该问题。

现代 Web 应用程序中不提供此设置。

启用 Web 客户端的复选框

如果启用了“显示选择复选框以在列表视图中选择电子邮件、联系人、语音邮件项目以进行批量操作”，则当用户在“内容”窗格中查看电子邮件、联系人和任务列表时，每个项目都会显示一个复选框。用户可以选择项目，然后执行操作，例如标记为已读/未读、移动到特定

文件夹,拖放到文件夹,删除并标记所有选定的项目。

现代 Web 应用程序上默认启用复选框。

偏好导入/导出

从经典 Web 应用程序中的“首选项导入/导出”页面或现代 Web 应用程序中的“帐户→主帐户”下,用户可以导出其所有帐户数据,包括邮件、联系人、日历和任务。通过选择导出选项,他们可以导出帐户中的特定项目并将数据保存到计算机。

帐户数据保存为 tar-gzipped (.tgz) 存档文件,以便可以导入来恢复其帐户。

个人联系人将保存为.csv文件,个人日历文件将保存为.ics文件。数据将被复制,但不会从用户帐户中删除。

可以使用存档程序(例如从同一页面导入他们的帐户)查看导出的帐户数据文件。**压缩包** . 任何这些文件都可以

您可以从COS或帐户功能页面的常规功能部分关闭导入/导出功能。

将单词添加到拼写词典

如果 Classic Web App 用户经常使用在 Classic Web App 拼写检查期间被标记为拼写错误的单词、缩写或首字母缩略词,则您可以使用在运行拼写检查时应忽略的单词更新 COS 或域属性zimbraPrefSpellIgnoreWord。

要配置域中要忽略的单词:

```
zmprov md example.com +zimbraPrefSpellIgnoreWord <word> +zimbraPrefSpellIgnoreWord <word2>
```

重击

此功能仅在经典 Web 应用程序中受支持。

Zimbra 中的分层地址簿 (HAB)

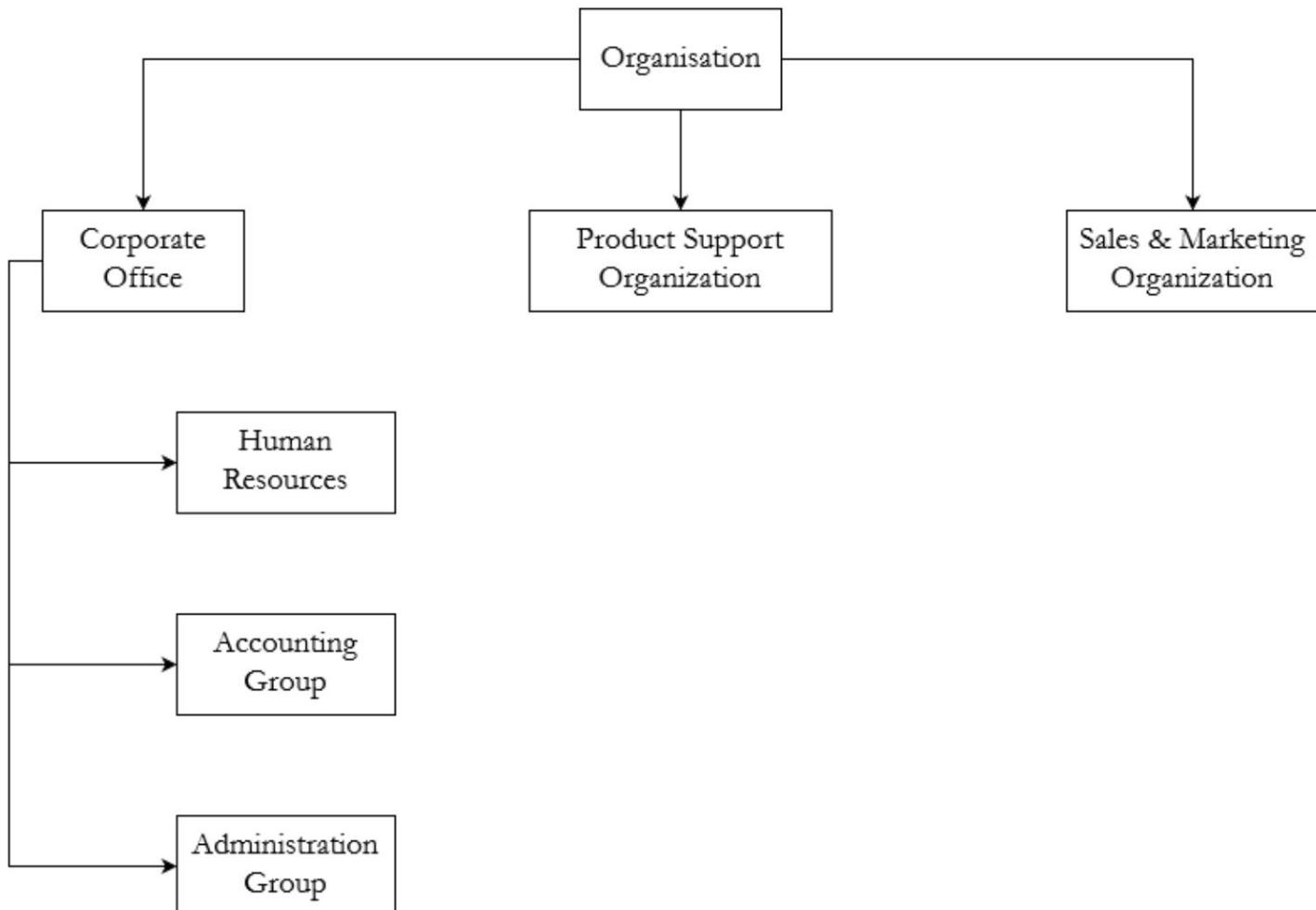
什么是 HAB?

分层地址簿 (HAB) 允许用户使用组织层次结构在其地址簿中查找收件人。通常,用户只能看到默认的全局地址列表 (GAL),其结构无法帮助了解谁向谁报告或识别某个 John Doe 与另一个 John Doe。能够自定义 HAB (映射到您组织独特的业务结构)可为您的用户提供一种查找内部收件人的有效方法。

使用分层地址簿

在分层地址簿 (HAB) 中,您的根组织 (例如 Zimbra) 是顶层。在此顶层下,您可以添加多个子层,以创建按部门、部门或您想要指定的任何其他组织级别细分的自定义 HAB。下图说明了 Zimbra 的 HAB,其结构如下:

- 顶层代表根组织 Zimbra。
- 第二级子层代表 Zimbra 内的业务部门 - 公司办公室、工程、产品支持以及销售和营销。
- 第三级子层代表公司办公室部门内的部门 人力资源、会计和行政。



图示例层次结构 1。

资历指数

资历指数在层次结构中提供了额外的级别。创建 HAB 时,使用此参数按这些组织层级内的资历对个人或组织组进行排名。此排名指定 HAB 显示收件人或组的顺序。较高的资历指数可确保用户或组出现在资历指数较低的用户或组之上。

- 100为副总统
- 行政运营经理50
- 25适用于企业管理员

如果未设置资历指数参数,或者两个或多个用户的资历指数参数相等,则 HAB 排序顺序将按字母升序列出用户和组。

配置分层地址簿

创建组织单位 (OU)

格式

```
zmprov createHABOrgUnit <OU 的域名> <OU 名称>
```

例子

```
zmprov createHABOrgUnit example.com ZimbraOU
```

解释

ZimbraOU 作为一个组织单位创建。

在此 OU 内创建组

您必须创建一个组并为每个部门分配一个电子邮件地址。

格式

```
zmprov createHABGroup <组名称> <OU 名称> <组电子邮件地址>
```

例子

在该系列命令中,我们根据示例层次结构创建了8个HAB 组。

```
zmprov createHABGroup Zimbra ZimbraOU zimbra@example.com
```

```
zmprov createHABGroup CorporateOffice ZimbraOU CorpOffice@example.com
```

```
zmprov createHABGroup 工程 ZimbraOU eng@example.com
```

```
zmprov createHABGroup ProdSupport ZimbraOU prodsupport@example.com
```

```
zmprov createHABGroup SalesAndMarketing ZimbraOU sales-mark@example.com
```

```
zmprov createHABGroup 人力资源 ZimbraOU hr@example.com
```

```
zmprov 创建HABGroup 帐户 ZimbraOU accounts@example.com
```

```
zmprov createHABGroup 管理 ZimbraOU Administration@example.com
```

创建层次结构

每个组 (Zimbra 除外)都需要分配一个父组来创建层次结构。

格式

```
zmprov addHABGroupMember 父组电子邮件地址 子组电子邮件地址
```

在这一系列命令中,我们根据图中示例层次结构中的层次结构指定了7个HAB组 (Zimbra 除外,因为它是根) 。

为此,我们向公司办公室添加了人力资源、会计和行政部门;向Zimbra添加了公司办公室、工程、产品支持和销售与营销部门。

```
zmprov addHABGroupMember CorpOffice@example.com hr@example.com
```

```
zmprov addHABGroupMember CorpOffice@example.com accounts@example.com
```

```
zmprov addHABGroupMember CorpOffice@example.com Administration@example.com
```

```
zmprov addHABGroupMember zimbra@example.com CorpOffice@example.com
```

```
zmprov 添加HABGroupMember zimbra@example.com eng@example.com
```

```
zmprov 添加HABGroupMember zimbra@example.com prodsupport@example.com
```

```
zmprov addHABGroupMember zimbra@example.com sales-mark@example.com
```

获取 Zimbra ID

zimbraId是与电子邮件地址关联的唯一标识符。它用于将用户分配到组并指定以 root 身份加入组。

对于此示例以及其他地方,我们都使用了zimbraId的占位符 (xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx) 。

格式

```
zmprov gdl <群组电子邮件地址> zimbraId
```

例子

```
zmprov gdl zimbra@example.com zimbraId
```

示例输出

```
# 分发列表 zimbra@example.com 成员数=4  
zimbraId:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

解释

zimbra@example.com 是即将成为根用户的组的电子邮件地址。

将用户添加到组

此示例添加用户现有成员。 简 多伊 和 约翰 史密斯 到名为 公司办公室 在不影响其他

格式

```
zmprov addHABGroupMember <群组邮箱地址> <用户邮箱地址>
```

例子

```
zmprov addHABGroupMember hr@example.com jane.doe@example.com
```

```
zmprov addHABGroupMember accounts@example.com john.smith@example.com
```

设置排序顺序

配置 HAB 中群组的排序顺序。资历指数较高的群组显示在资历指数较低的群组之上
资历指数。

格式

```
zmprov modifiedHABGroupSeniority <zimbra ID> <资历指数>
```

例子

拥有 工程 出现在上方 公司办公室 无论其名称和字母顺序如何,都获得
Zimbra ID,用数字代替SeniorityIndexNumber ,并运行以下命令。

分配 公司办公室 资历指数为 90

```
zmprov 修改HABGroupSeniority xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx 90
```

分配 工程 资历指数为 100

```
zmprov 修改HABGroupSeniority xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx 100
```

用于设置群组资历指数的命令也用于设置用户的资历指数。

指定 HAB 的根组织

需要将某个组指定为 root,以便其他组可以作为子组添加,以符合组织层次结构。运行以下命令以使 zimbra@example.com 以 root 身份运行。

格式

```
zmprov md <域名> zimbraHierarchicalAddressBookRoot <要创建的组的 ZimbraID  
根>
```

例子

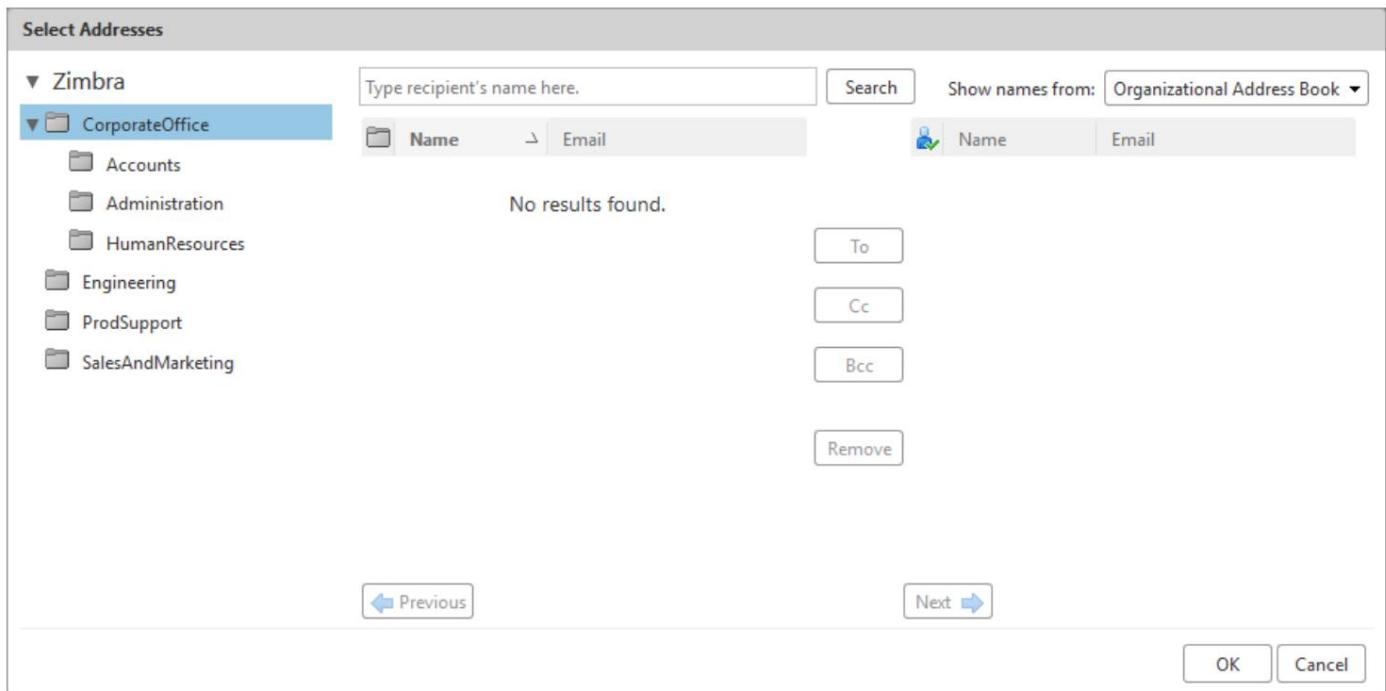
```
zmprov md example.com zimbraHierarchicalAddressBookRoot xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

示例输出

```
# 分发列表 zimbra@example.com 成员数=4  
zimbralid:xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

它有效吗?

1. 登录Zimbra客户端。
2. 单击“新消息”。
3. 在撰写窗口中,单击收件人字段。
4. 在“选择地址”窗口中,找到右上角的“显示名称来自:”下拉菜单。
5. 选择组织通讯簿。
6. 左侧窗格中将显示分层格式的地址簿。



7. 单击任意组以查看并选择该组的用户。

管理组织单位 (OU)

列出组织单位 (OU)

一个域中可以有多个组织单位。此命令列出指定域中的所有 OU。

格式

```
zmprov listHABOrgUnit <OU 的域名>
```

例子

```
zmprov listHABOrgUnit example.com ZimbraOU
```

解释

所有 OU 位于 example.com 列出。

重命名组织单位 (OU)

此命令重命名域中指定的 OU。

格式

```
zmprov renameHABOrgUnit <OU 的域名> <OU 名称> <OU 的新名称>
```

例子

```
zmprov renameHABOrgUnit example.com ZimbraOU ZMXOU
```

解释

ZimbraOU 重命名为 ZMXOU。

重命名组织单位 (OU)

此命令删除域中的指定 OU。

格式

```
zmprov renameHABOrgUnit <OU 的域名> <OU 名称>
```

例子

```
zmprov renameHABOrgUnit example.com ZimbraOU
```

解释

ZimbraOU 已删除。

配置用户帐户

配置帐户时,您可以创建邮箱、分配主帐户电子邮件地址并分配服务类 (COS) 以启用 Zimbra Collaboration 应用程序和功能。

您可以一次配置一个帐户,也可以从服务器迁移多个现有帐户。

创建单个用户帐户

在添加用户帐户之前,请确定应分配哪些功能和访问权限。您可以在创建帐户时分配启用了功能的服务类别 (COS),也可以为各个帐户配置功能。有关功能的描述,请参阅服务类别和帐户。

如果您分配的 COS 具有适合该帐户的正确功能,则无需执行任何其他配置。

创建帐户会在 Zimbra LDAP 目录服务器上设置相应的条目。当用户首次登录或电子邮件发送到用户帐户时,邮箱服务器上会创建邮箱。

基本用户帐户设置:

管理控制台:

首页→3 添加账户→1. 添加账户

1. 在账户名称部分,至少输入账户名称和姓氏,以配置帐户。

默认 COS 已分配给该帐户。

2. 单击“完成”创建帐户。

您可以继续为个人帐户配置特性和功能。您对帐户所做的更改将覆盖分配给该帐户的 COS。

迁移账户并导入账户邮箱

Zimbra Admin UI 中的 Zimbra 协作帐户迁移不再受支持,技术指导结束日期定于 2019 年 12 月 17 日。我们推荐 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。

您可以使用管理控制台中的帐户迁移向导一次性配置多个帐户。您可以从通用 IMAP 服务器或其他 Zimbra 服务器导入帐户。

只有 Zimbra Collaboration 7.2 或更高版本上的帐户可以迁移到 Zimbra Collaboration 8。

您还可以从您创建的 XML 文件中导入要配置的帐户名称。

您可以运行一次迁移向导来配置帐户并导入数据,或者您可以第一次运行迁移向导来配置帐户,然后再次运行该向导来导入已配置帐户的数据。

无论您从 LDAP 目录获取帐户记录还是使用 XML 文件,您都需要为新配置的帐户设置密码要求。选项是让 Zimbra 为每个帐户随机创建密码或为每个帐户设置相同的密码。您可以选择强制用户在首次登录时更改密码。

配置完成后,向导会生成一个.csv文件,其中包含新帐户列表。这包括生成的密码。您应该下载此文件以供将来参考。选择一个安全的位置来存储该文件,因为它可能包含您配置的用户帐户的密码信息。

如果您正在运行拆分域配置,则可以在向导中设置 SMTP 主机和端口。有关拆分域的更多信息,请参阅有关拆分域的 wiki 文章 https://wiki.zimbra.com/wiki/Split_Domain。

从 Zimbra 服务器迁移账户

将账户从运行 Zimbra Collaboration 7.2 或更高版本的服务器迁移到 Zimbra Collaboration 8。

管理控制台:

首页→ 3 添加账户→ 3. 迁移与共存

1. 在邮件服务器类型字段中,选择Zimbra Collaboration。
2. 如果您正在配置帐户,请选择“是”以导入帐户记录。如果您不打算导入此时的数据,在是否要导入邮件中选择否。
3. 单击下一步。
4. 在概述对话框中,选择从另一个 Zimbra LDAP 目录导入。单击下一步。
5. 在批量配置选项页面上,选择是否生成随机密码或分配相同的密码每个帐户的密码。

表批量配置功能 42.

| 批量配置功能 | 描述 |
|-----------------|--|
| 生成随机密码 | <p>如果选择为每个帐户生成随机密码,请设置密码长度。密码长度可以为 6 到 64 个字符。</p> <p>默认值 = 8 个字符</p> <p>如果您选择生成随机密码,则必须下载创建的.csv文件,以便可以向每个用户提供密码信息。</p> |
| 使用相同的密码 | 如果您选择对所有新帐户使用相同的密码,请输入要使用的密码。 |
| 要求用户在首次登录后更改密码 | 建议选中此项以强制用户在第一次登录时更改密码。 |
| SMTP 主机/SMTP 端口 | 对于拆分域配置,设置 SMTP 主机名和端口。 |

6. 单击下一步。

7. 在目录连接对话框中输入连接到服务器的信息。

表目录连接选项 43.

| 目录连接选项 | 描述 |
|----------------------------|---|
| 自动创建缺失的域 | <p>启用此选项可在导入账户但其所在的域尚未创建时创建域。</p> <p>如果不启用此选项,则不会创建服务器上不存在的域的帐户。禁用此选项可轻松导入预先创建的特定域中的帐户。</p> |
| 获取的最大记录数 | 输入一次导入的最大账户数。默认值为 0,表示不设置限制。 |
| 服务器名称、LDAP URL、端口和 SSL 的使用 | <ul style="list-style-type: none"> ◦ LDAP URL 输入如下： ldap://<ldapdirectory.example.com> ◦ 默认端口是 389,但您可以更改它。 ◦ 如果使用了 SSL,请检查。 |
| 绑定 DN | Zimbra 的默认设置如下： uid=zimbra,cn=管理员,cn=zimbra |
| 绑定密码 | 输入服务器的密码。 |
| LDAP 过滤器 | <p>在此字段中输入要运行的 LDAP 搜索过滤器。在这里您可以定义搜索条件来收集要导入的帐户信息类型。字段中的默认过滤器是(objectclass=zimbraAccount)。</p> <p>此过滤器包括电子邮件地址、帐户 ID 和帐户属性。</p> |
| LDAP 搜索基础 | 配置 LDAP 林的子部分以进行搜索。 |

8.单击下一步。

帐户迁移向导连接到目录服务器并生成一份报告,其中显示找到的域数量、服务器上找到的帐户数量以及其中有多少帐户已在 Zimbra 上创建。此对话框还显示您配置的密码选项。

9. 查看生成的报告,然后单击下一步。这些帐户已在 Zimbra Collaboration 上配置
服务器。

10. 下载列出已配置帐户及其密码的.csv文件。以下情况下会删除.csv文件：
关闭向导。如果不下载文件,以后将无法访问该报告。

从通用 IMAP 服务器迁移帐户

使用本节中的步骤在 Zimbra 服务器上配置帐户。

管理控制台：

首页→3 添加账户→3. 迁移与共存

1. 在邮件服务器类型字段中,选择通用 IMAP 服务器。

2. 如果您正在配置帐户,请选择“是”以导入帐户记录。如果您不打算导入
此时的数据,在是否要导入邮件中选择否。

3.单击下一步。

4. 在“概览”对话框中,选择“从另一个 LDAP 目录导入”。单击“下一步”。

5. 在批量配置选项页面上,选择是否生成随机密码或分配相同的密码

每个帐户的密码。

表批量配置功能

| 批量配置功能 | 描述 |
|-------------------|---|
| 生成随机密码 | <p>如果您选择为每个账户生成随机密码,请设置密码长度。密码长度可以为 6 到 64 个字符。 默认值 = 8 个字符</p> <p>如果您选择生成随机密码,则必须下载创建的.csv文件,以便您提供密码信息对每个用户。</p> |
| 使用相同的密码 | 如果您选择对所有新帐户使用相同的密码,请输入使用的密码。 |
| 要求用户更改密码 首次登录后 | 建议选中此项以强制用户更改其首次登录时输入密码。 |
| SMTP 主机/SMTP 端口 | 对于拆分域配置,设置 SMTPHost 名称和端口。 |

6.单击下一步。

7. 在目录连接对话框中输入连接到服务器的信息。

表目录连接选项

| 目录连接选项 | 描述 |
|----------------------------|---|
| 自动创建缺失域 | <p>启用此选项可在导入账户时创建域,他们所在的域尚未创建。</p> <p>如果不启用此功能,则来自不存在的域的帐户不会创建服务器。禁用此选项可轻松导入来自预先创建的特定域的帐户。</p> |
| 获取的最大记录数 | <p>输入一次导入的最大帐户数。</p> <p>默认值为 0,表示不设置限制。</p> |
| 服务器名称、LDAP URL、端口和 SSL 的使用 | <ul style="list-style-type: none"> ◦ LDAP URL 输入如下: ldap://<ldapdirectory.example.com> ◦ 默认端口是 389,但您可以更改它。 ◦ 如果使用了 SSL,请检查。 |
| 绑定 DN | Zimbra 的默认设置如下: uid=zimbra,cn=管理员,cn=zimbra |
| 绑定密码 | 输入服务器的密码。 |
| LDAP 过滤器 | <p>在此字段中输入要运行的 LDAP 搜索过滤器。您可以在此处定义搜索条件来收集您想要的帐户信息类型导入。该字段的默认过滤器是(objectclass=zimbraAccount)。</p> <p>此过滤器包括电子邮件地址、帐户 ID 和以下属性该帐户。</p> |

| 目录连接选项 | 描述 |
|-----------|---------------------|
| LDAP 搜索基础 | 配置 LDAP 林的子部分以进行搜索。 |

8.单击下一步。

迁移向导连接到目录服务器并生成一份报告,显示找到的域数量、在服务器上找到的帐户数量以及其中有多少个帐户已在 Zimbra 上创建。

该对话框还显示您配置的密码选项。

9. 查看生成的报告,然后单击下一步。这些帐户已在 Zimbra Collaboration 上配置
服务器。

10. 下载列出已配置帐户及其密码的.csv文件。以下情况下会删除.csv文件：
关闭向导。如果不下载文件,以后将无法访问该报告。

使用 XML 文件迁移账户

使用本部分中的步骤创建包含帐户信息的 XML 文件,并将其保存到您可以
使用权。

管理控制台：

首页→3 添加账户→3. 迁移与共存

1. 在邮件服务器类型字段中,选择您要从中迁移的服务器类型。
2. 如果您正在配置帐户,请选择“是”以导入帐户记录。如果您不打算导入
此时的数据,在是否要导入邮件中选择否。

3.单击下一步。

4. 在概述对话框中,选择从 XML文件导入。

5.单击下一步。

6.审查选项对话框显示域数量、账户数量和密码选项
在 XML 文件中配置。

7. 如果此信息正确,请单击下一步。如果此信息不正确,请先修复 XML 文件,然后再继续。

如果单击“下一步”,则会在 Zimbra 协作服务器上配置帐户。

8. 下载列出已配置帐户及其密码的.csv文件。以下情况下会删除.csv文件：
关闭向导。如果不下载文件,以后将无法访问该报告。

为选定账户导入电子邮件

使用本节中的步骤来指定要导入邮件的帐户列表,方法是选择要导入数据的帐户或使用 XML 文件来选择帐户。

在尝试此过程之前,请确保在 Zimbra 服务器上已配置帐户。

管理控制台：

首页→3 添加账户→3. 迁移与共存

1. 在邮件服务器类型字段中,选择要从中导入数据的服务器类型。
2. 在您想导入帐户记录菜单中,选择否。
3. 在您想要导入邮件吗菜单中,选择是。

4.单击下一步。

5.在导入选项对话框中,选择要指定要导入邮件的账户的方式

进口。

6.单击下一步。

如果您正在选择帐户,请转至步骤 7。如果您正在使用 XML 文件,请转至步骤 9。

7.如果您正在选择要导入的帐户,请在“选定帐户”对话框中搜索要添加的帐户。

您可以按域名或用户名进行搜索。如果您单击“搜索”而不输入文本,则会返回所有帐户。

将帐户添加到用于数据导入的帐户列中。

8.单击下一步。

9.如果您使用列出帐户的 XML 文件,请浏览到要使用的 XML 文件。

10.单击下一步。

11.在 IMAP 连接详细信息对话框中,输入连接到导出服务器的必要信息

IMAP,这包括 IMAP 主机名、端口和管理员登录信息。

12.单击下一步。

13.检查数据导入选项。如果信息正确,请单击下一步。

XML 文件示例

本节包含用于配置帐户和导入数据的 XML 文件结构的三个示例。

[使用 7 的示例。](#)

[XML 到 文件提供帐户](#)

以下示例显示了用于配置多个电子邮件帐户而无需导入的 XML 文件

邮件:

XML

```
<?xml version= "1.0" encoding= "UTF-8" ?>
<ZCSImport>
<导入用户>
<用户>
<sn>示例</sn>
<给定名称>山姆</给定名称>
<displayName>山姆样品</displayName>
<RemoteEmailAddress>ssample@example.com</RemoteEmailAddress>
<密码>test123</密码>
<zimbraPasswordMustChange>真</zimbraPasswordMustChange>
</用户>
<用户>
<sn>扎克瑞</sn>
<givenName>扎克</givenName>
<displayName>扎克·扎克瑞</displayName>
<RemoteEmailAddress>zzackry@example.com</RemoteEmailAddress>
<密码>test123</密码>
<zimbraPasswordMustChange>真</zimbraPasswordMustChange>
</用户>
</导入用户>
</ZCSImport>
```

以下示例显示了一个 XML 文件,用于为外部托管域配置多个电子邮件帐户而无需导入邮件。

在这个例子中,新配置的帐户的zimbraMailTransport属性将被设置为指向外部 SMTP 服务器而不是 Zimbra 服务器。

```
<?xml version= 1.0 encoding= UTF-8 ?><ZCSImport>

<SMTPHost>smtp.example.com</SMTPHost><SMTPPort>25</
SMTPPort> <ImportUsers> <User>

<sn>示例</sn>
<givenName>Sam</givenName>
<displayName>Sam示例</displayName>
<RemoteEmailAddress>sam@example.com</RemoteEmailAddress> </User>

<用户>
<sn>Zackry</sn>
<givenName>Zak</givenName> <displayName>Zak
Zackry</displayName> <RemoteEmailAddress>zzackry@example.com</
RemoteEmailAddress> </User> </ImportUsers> </ZCSImport>
```

XML

使用 9 的示例。

XML 文件导入电子邮件到

以下示例显示了一个 XML 文件,该文件用于通过 IMAP 从 Gmail 帐户导入一个帐户的电子邮件,而无需在 Zimbra 中配置电子邮件帐户。在运行此类 XML 文件之前,必须在 Zimbra 上配置该帐户。

```
<?xml version= 1.0 encoding= UTF-8 ?><ZCSImport>

<IMAPHost>imap.gmail.com</IMAPHost><IMAPPort>993</
IMAPPort> <ConnectionType>ssl</
ConnectionType> <UseAdminLogin>0</UseAdminLogin>
<ImportUsers>

<用户>
<sn>示例</sn>
<givenName>Sam</givenName>
<displayName>Sam示例</displayName>
<RemoteEmailAddress>sam@example.com</RemoteEmailAddress> <RemoteIMAPLogin>sam@example.com</
RemoteIMAPLogin> <remoteIMAPPASSWORD>test123</remoteIMAPPASSWORD> </User> </
ImportUsers> </ZCSImport>
```

XML

从外部 LDAP 自动配置新帐户

支持通过 CLI 从外部 LDAP 自动配置新帐户。本节介绍支持的 CLI 属性和自动配置方法。

概述

当为 Zimbra 域配置了外部 LDAP 身份验证机制（例如外部 LDAP 身份验证、预身份验证或 SPNEGO）时，您可以设置 Zimbra 以在 Zimbra 上自动创建用户帐户。主电子邮件地址和帐户属性从外部目录映射。您可以配置如何以及何时从外部目录数据创建新帐户。

自动配置支持三种模式。

| 模式 | 描述 |
|-----|--|
| 渴望的 | Zimbra 轮询外部目录以查找要自动配置的帐户。对于此模式，您可以配置轮询外部目录以查找新用户的频率、每个间隔要处理的最大用户数以及在指定服务器上安排哪些域进行帐户自动配置。 在 Eager Mode Configuration 中提供了指南。 |
| 懒惰的 | 如果用户首次通过支持自动配置的身份验证机制之一登录经典 Web 应用程序，并且如果该用户不存在于 Zimbra 目录中，则会在 Zimbra 中自动为该用户创建一个新帐户。 在 惰性模式配置 中提供了指南。 |
| 手动的 | 不会发生自动配置：相反，管理员从配置的外部自动配置 LDAP 源中手动搜索，并从搜索结果中选择一个条目来为外部条目创建相应的 Zimbra 帐户。 在 手动模式配置 中提供了指南。 |

创建帐户时，帐户名称（由 @ 符号旁边的字符组成）将从您在 `zimbraAutoProvAccountNameMap` 中定义的外部目录中的用户属性映射而来。其他帐户信息（例如名字和姓氏、电话号码和地址）将从基于 `zimbraAutoProvAttrMap` 的外部目录映射的属性中填充。您可以查看外部目录的属性以确定应映射到 Zimbra 属性的属性。

自动配置帐户的 COS 分配方式与手动配置帐户的 COS 确定方式相同：

- 如果为域定义了 COS，则该 COS 将分配给创建的账户。
- 如果未定义域 COS，则分配 Zimbra 默认 COS。

您可以配置一封欢迎电子邮件，发送给新创建的帐户。此电子邮件的主题和正文可以使用域上的 `AutoProvNotification` 属性进行配置。

自动配置属性

本节列出的属性可与 `zmprov` 命令一起使用，以配置使用外部 LDAP 目录的新帐户的自动配置。

zimbraAutoProvMode

将自动配置模式设置为 EAGER、LAZY 和/或 MANUAL。可以在一个域上启用多种自动配置模式。

zimbraAutoProvAuthMech

设置身份验证机制的类型 - 为 LDAP、PREAUTH、KRB5 或 SPNEGO - 以启用 LAZY 模式。

一旦用户通过指定的身份验证机制进行身份验证，并且如果用户帐户尚不存在于 Zimbra 目录中，则会在 Zimbra 目录中自动创建一个帐户。

zimbraAutoProvLdapURL

设置用于自动配置的外部 LDAP 源的 LDAP URL

zimbraAutoProvLdapStartTlsEnabled

访问外部 LDAP 服务器进行自动配置时启用 (TRUE) 或禁用 (FALSE) StartTLS 协议。

默认 = FALSE。

zimbraAutoProvLdapAdminBindDn

定义自动配置的 LDAP 搜索绑定 DN。

zimbraAutoProvLdapAdminBindPassword

为自动配置设置 LDAP 搜索管理员绑定密码。

zimbraAutoProvLdapSearchBase

设置自动配置的 LDAP 搜索基础，与 zimbra zimbraAutoProvLdapSearchFilter 结合使用。

如果未设置，则将使用 LDAP 根 DSE。

zimbraAutoProvLdapSearchFilter

定义用于帐户自动配置的 LDAP 搜索过滤器模板。对于 LAZY 模式，必须设置 zimbraAutoProvLdapSearchFilter 或 zimbraAutoProvLdapBindDn。

如果两者都设置， zimbraAutoProvLdapSearchFilter 将优先。请参阅占位符以了解支持的占位符。

zimbraAutoProvLdapBindDn

定义用于帐户自动配置的 LDAP 外部 DN 模板。对于 LAZY 模式，必须设置 zimbraAutoProvLdapSearchFilter 或 zimbraAutoProvLdapBindDn。

如果两者都设置， zimbraAutoProvLdapSearchFilter 将优先。请参阅占位符以了解支持的占位符。

zimbraAutoProvAccountNameMap

定义外部目录中包含帐户名本地部分的属性名称。这是用于创建 Zimbra 帐户的名称。如果未指定，则帐户名的本地部分是用于向 Zimbra 进行身份验证的主要用户名。

zimbraAutoProvAttrMap

定义属性映射,用于将属性值从外部条目映射到 Zimbra 帐户属性。

值的格式为{外部属性}={zimbra 属性}。

任何属性。

如果未设置,Zimbra 帐户中将不会填充外部目录的

映射配置无效将导致帐户创建失败。错误的映射可能由以下情况造成：

- 外部属性名称无效。
- Zimbra 属性名称无效。
- 外部属性包含多个值;Zimbra 属性只包含一个值。
- 语法违规 (例如外部属性=字符串,但 Zimbra 属性=整数)。

zimbraAutoProvNotificationFromAddress

定义要放入发送给新创建帐户的欢迎电子邮件发件人标题中的电子邮件地址。如果未设置,则不会向新创建帐户发送通知电子邮件。

zimbraAutoProvNotificationSubject

用于构建在用户帐户自动配置时发送给用户的 notification 消息主题的模板。

支持的变量： \${ACCOUNT_ADDRESS}、 \${ACCOUNT_DISPLAY_NAME}

zimbraAutoProvNotificationBody

用于构建在用户帐户自动配置时发送给用户的 notification 消息正文的模板。

支持的变量： \${ACCOUNT_ADDRESS}、 \${ACCOUNT_DISPLAY_NAME}

zimbraAutoProvListenerClass

域设置用于定义自动配置侦听器的类名。该类必须实现com.zimbra.cs.account.Account.AutoProvisionListener接口。在 Zimbra 中自动创建每个帐户后,将调用单例侦听器实例。侦听器可以作为服务器扩展插入,以处理诸如在外部 LDAP 目录中更新帐户自动配置状态等任务。

在每个紧急配置间隔,Zimbra 都会根据zimbraAutoProvLdapSearchFilter中配置的值进行 LDAP 搜索。此搜索返回的条目是此批次中自动配置的候选条目。zimbraAutoProvLdapSearchFilter应包含一个断言,该断言只会命中尚未在 Zimbra 中配置的外部目录中的条目,否则很可能相同的条目会被重复拉入 Zimbra。在Zimbra中自动配置帐户后,

自动配置框架将调用com.zimbra.cs.account.Account.AutoProvisionListener.postCreate (Domain domain, Account acct, String external DN)。客户可以在 Zimbra 服务器扩展中实现 AutoProvisionListener 接口,并调用其AutoProvisionListener.postCreate()。客户的后期创建方法的实现可以是,例如,在 Zimbra 中刚刚配置的帐户的外部目录中设置属性。该属性可以作为条件包含在下一个间隔中 LDAP 搜索再次返回的zimbraAutoProvLdapSearchFilter中。

,所以入口不会

zimbraAutoProvBatchSize

域 | 全局设置,用于定义 EAGER 自动在每个间隔内处理的最大帐户数
条款。

zimbraAutoProvScheduledDomains

列出在此服务器上计划进行 EAGER 自动配置的域的服务器属性。计划的域
必须在zimbraAutoProvMode中启用 EAGER 模式。可以在服务器上安排多个域
EAGER 自动配置。此外,可以在多台服务器上安排一个域以实现 EAGER 自动配置。

zimbraAutoProvPollingInterval

域 | 全局设置,用于定义 EAGER 中连续轮询和配置帐户之间的间隔
模式。实际间隔可能会更长,因为它可能受到其他两个因素的影响:
zimbraAutoProvBatchSize和zimbraAutoProvScheduledDomains中配置的域数量。

在每个间隔,自动配置线程都会遍历zimbraAutoProvScheduledDomains中的所有域
并自动创建最大为domain.zimbraAutoProvBatchSize的账户。如果该过程耗时超过
zimbraAutoProvPollingInterval比下一次迭代立即开始,而不是等待
zimbraAutoProvPollingInterval的时间量。

- 如果在服务器启动时设置为 0,则自动配置线程将不会启动。
- 如果在服务器运行时将非 0 值更改为 0,则自动配置线程将关闭。
- 如果在服务器运行时将其从 0 更改为非 0 值,则将启动自动配置线程。

占位符

表 46. 与自动配置属性一起使用的占位符

| 标签 | 描述 | 结果 |
|-----|------------|------------------------|
| %/n | 用户名和@符号 | 这将返回 user1@example.com |
| %在 | 不包含@符号的用户名 | 这将返回 用户1。 |
| %日 | 领域 | 这将返回 示例.com |
| %D | 域为 dc | 这将返回 例如,dc=com |

Eager 模式配置

使用 Eager 模式,Zimbra 会轮询外部目录以查找要自动配置的帐户。您可以配置轮询的频率
外部目录轮询新用户、每个间隔处理的最大用户数以及
在指定的服务器上安排帐户自动配置的域。

1. 以 zimbra 身份登录 Zimbra 服务器,并在命令提示符下输入zmprov。

兹姆普罗夫

重击

2. 在域上启用 EAGER 模式。

md <example.com> zimbraAutoProvMode EAGER

重击

3. 设置每个间隔内要处理的最大账户数

md <example.com> zimbraAutoProvBatchSize <#>

重击

4. 配置轮询和配置帐户之间的间隔（以分钟为单位）。必须将其设置为非 0
自动配置线程启动的值。默认值 = 15 分钟。

```
ms <server.com> zimbraAutoProvPollingInterval <x 分钟>
```

重击

5. 选择要安排自动配置的域。服务器上可以安排多个域。

一个域名可以调度在多台服务器上。

```
ms <服务器.com> +zimbraAutoProvScheduledDomains <域1.com> \ +zimbraAutoProvScheduledDomains <域2.com>
```

重击

6. 配置外部 LDAP 设置：

a. LDAP URL

```
md <example.com> zimbraAutoProvLdapURL "ldap://xxx.xxx.xxx.xxx:<端口>"
```

重击

LDAP 端口通常为 389。

b. (可选)启用 StartTls。

```
md <example.com> zimbraAutoProvLdapStartTlsEnabled TRUE
```

重击

c. LDAP 管理员绑定 DN 进行自动配置：

```
md <example.com> zimbraAutoProvLdapAdminBindDn cn=admin,dc=autoprov,dc=company,dc=com
```

BASH

d. 管理员的 LDAP 搜索绑定密码以进行自动配置。

```
md <example.com> zimbraAutoProvLdapAdminBindPassword <密码>
```

重击

e. 搜索要自动配置的用户时使用的搜索模板。

使用 LDAP 搜索过滤器的示例：

```
md <example.com> zimbraAutoProvLdapSearchFilter "(uid=<%placeholder>)"
```

重击

请参阅占位符以了解支持的占位符。

f. 自动配置的 LDAP 搜索库

这是目录中 LDAP 搜索开始的位置。它与起点一起使用。

`zimbraAutoProvLdapSearchFilter`。如果未设置，则 LDAP 目录根，`rootDSE`

,

```
md <example.com> zimbraAutoProvLdapSearchBase "dc=autoprov,dc=company,dc=com" md <example.com>
zimbraAutoProvLdapBindDn <"placeholder1">
```

重击

请参阅占位符以了解支持的占位符。

7. (可选)定义映射到外部帐户名称本地部分的属性名称

目录。这用于定义 Zimbra 上的帐户名称。如果未指定，则帐户名称的本地部分是用于向 Zimbra 进行身份验证的主要用户名。

重击

```
md <example.com> zimbraAutoProvAccountNameMap <值>
```

8. (可选)将外部条目中的属性值映射到 Zimbra 帐户属性。如果未设置

启动后,Zimbra 目录中不会填充任何来自外部目录的属性。该值以{外部属性}={zimbra 属性}的形式映射。

映射配置无效将导致创建账户失败。

要将外部条目上的“sn”值映射到 Zimbra 帐户上的“displayName” ,并将外部条目上的描述值映射到 Zimbra 帐户上的描述,请键入

```
md <example.com> +zimbraAutoProvAttrMap sn=显示名称 +zimbraAutoProvAttrMap 描述=描述
```

重击

9. (可选)如果您想向新帐户发送欢迎电子邮件,请输入

从 发起者的地址。

```
md <example.com> zimbraAutoProvNotificationFromAddress <name@example.com>
```

重击

10. 要退出 zmprov,请输入

出口

重击

懒惰模式配置

在用户通过外部身份验证机制 (LDAP、预认证、Kerberos 5 和/或 SPNEGO)进行身份验证后,惰性模式自动配置会自动创建一个新帐户。

1. 以 zimbra 身份登录 Zimbra 服务器,并在命令提示符下输入zmprov。

2. 启用 LAZY 模式,

```
md <example.com> zimbraAutoProvMode LAZY
```

重击

3. 选择 LAZY 模式的外部身份验证机制:LDAP、PREAUTH、KRB5、SPNEGO。您可以指定多种身份验证机制。

```
md <example.com> zimbraAutoProvAuthMech <类型> +zimbraAutoProvAuthMech <类型2>
```

重击

4.配置外部 LDAP 设置

a.LDAP URL:

```
md <example.com> zimbraAutoProvLdapURL “ldap://xxx.xxx.xxx.xxx:<端口>”
```

重击

LDAP 端口通常为 389。

b. (可选)启用 StartTls

```
md <example.com> zimbraAutoProvLdapStartTlsEnabled TRUE
```

重击

c. LDAP 管理员绑定 DN 以自动配置格式cn=<LDAPadmin_name>, dc=autoprov, dc=<公司名称>, dc=<com>

重击

```
md <example.com> zimbraAutoProvLdapAdminBindDn <“绑定DN”>
```

例如，“cn=admin, dc=autoprov, dc=company, dc=com” d. 管理员的 LDAP
搜索绑定密码,用于自动配置。

```
md <example.com> zimbraAutoProvLdapAdminBindPassword <密码>
```

重击

e. (可选)搜索要自动配置的用户时使用的搜索模板。

示例:使用 LDAP 搜索过滤器:

```
md <example.com> zimbraAutoProvLdapSearchFilter <“占位符”>
```

重击

请参阅占位符以了解支持的占位符。

必须为 LAZY 模式配置 zimbraAutoProvLdapSearchFilter 或 zimbraAutoProvLdapBindDn。

f. 自动配置的 LDAP 搜索基础。这是目录中 LDAP 搜索开始的位置。

这与zimbraAutoProvLdapSearchFilter一起使用。

如果未设置,则 LDAP 目录根, rootDSE 为起点。

, 是

```
md <example.com> zimbraAutoProvLdapSearchBase <“位置”>
```

重击

例如, “dc=autoprov,dc=company,dc=com”

g. (可选)定义用于帐户配置的 LDAP 外部 DN 模板。

```
md <example.com> zimbraAutoProvLdapBindDn “uid=%<占位符1>, %<占位符2>”
```

重击

请参阅占位符以了解支持的占位符。

5. (可选)在外部条目中标识包含要在 Zimbra 中配置的帐户名称的本地部分的属性名称。如果未指定,则帐户名称的本地部分是用于向 Zimbra 进行身份验证的主要用户。

```
md <example.com> zimbraAutoProvAccountNameMap <值>
```

重击

6. (可选)将外部条目中的属性值映射到 Zimbra 帐户属性。如果未设置,则 Zimbra 目录中不会填充任何来自外部目录的属性。值的形式为

{外部属性} = {zimbra 属性}。

要将外部条目上的sn值映射到 Zimbra 帐户上的displayName ,并将外部条目上的 description 值映射到 Zimbra 帐户上的 description,请键入

```
md <example.com> +zimbraAutoProvAttrMap sn=显示名称 +zimbraAutoProvAttrMap 描述=描述
```

重击

7. (可选)如果您想向新账户发送欢迎电子邮件,请输入

从 发起者的地址。

```
md <example.com> zimbraAutoProvNotificationFromAddress <name@example.com>
```

重击

8.退出 zmprov,输入exit。

手动模式配置

使用手动模式设置可禁用外部 LDAP 服务器的自动配置。

1. 以 zimbra 身份登录 Zimbra 服务器,并在命令提示符下输入zmprov。

2. 启用手动模式:

```
md <example.com> zimbraAutoProvMode 手动
```

重击

管理资源

资源是可以安排会议的地点或设备。每个会议室位置和其他非特定位置的资源（如 AV 设备）都设置为资源帐户。管理控制台中的“管理→资源”部分显示为 Zimbra Collaboration 配置的所有资源。

具有日历功能的用户帐户可以为他们的会议选择这些资源。资源帐户会根据可用性自动接受或拒绝邀请。

管理员不需要定期监控这些邮箱。资源邮箱的内容将根据邮件清除策略进行清除。

资源向导将指导您完成资源配置。您可以使用以下有关资源的详细信息配置帐户：

- 资源类型,位置或设备
- 调度策略
- 用于接收邀请副本的转发地址
- 资源描述
- 联系信息,如有问题可以联系此人
- 位置信息,包括房间名称、具体建筑位置（包括建筑物和地址）以及房间容量

- 自定义自动回复消息和签名以用于回复电子邮件

当您创建资源帐户时,会在 LDAP 服务器中创建一个目录帐户。

要安排资源,用户需要邀请设备资源和/或位置参加会议。当他们选择资源时,他们可以查看资源的描述、联系信息和资源的空闲/忙碌状态（如果已设置）。

发送会议邀请后,会向资源帐户发送电子邮件,并且根据调度策略,如果资源空闲,则会议会自动输入到资源的日历中,并且资源会显示为忙碌。

设置调度策略

调度策略确定如何维护资源的日历。可以设置以下资源调度值：

- 自动拒绝所有定期约会 当资源一次只能安排一次会议时启用此值。无法为此资源安排定期约会。

- 可用时自动接受,冲突时自动拒绝 选择此选项后,资源帐户将自动接受约会,除非资源已安排。可以查看空闲/忙碌时间。您可以修改自动拒绝规则以接受一些冲突的会议。
- 手动接受,冲突时自动拒绝 选择此选项后,资源帐户将自动拒绝所有有冲突的约会。不冲突的约会请求在资源日历中标记为暂定,必须手动接受。如果您设置了此选项,请配置转发地址,以便将邀请副本发送到可以手动接受邀请的帐户。您可以修改自动拒绝规则以接受一些有冲突的会议。
- 始终自动接受 资源帐户自动接受所有安排的约会。在这种情况下,不会维护空闲/忙碌信息,因此多个会议可以同时安排资源。由于资源始终接受邀请,因此建议将此策略用于经常使用的场外位置,您希望将位置地址包含在对与会者的邀请中。
- 不自动接受或拒绝 资源帐户是手动管理的。委派用户必须登录资源帐户并接受或拒绝所有请求。

冲突规则 对于包含自动拒绝冲突值的帐户,您可以设置一个阈值,可以是冲突的数量,也可以是所有定期预约的百分比,以部分接受定期预约。

允许的最大冲突数量和/或允许的最大冲突百分比被配置为允许安排重复资源,即使在所有请求的重复预约日期都不可用的情况下。

即使存在冲突,资源也会接受预约,直到冲突数量达到允许的最大值或允许的最大冲突百分比。为了使部分接受一系列预约能够正常工作,必须将两个字段都设置为非零值。

管理资源帐户

您可以登录资源帐户并设置资源的首选项。可以配置资源帐户首选项→日历,让用户管理资源的日历。您可以配置以下选项来管理资源。

- 转发邀请的地址。如果在配置帐户时设置了转发地址,您可以更改该地址
- 谁可以使用此资源。在权限部分的邀请中,选择仅允许以下内部用户邀请我参加会议,并将相应用户的电子邮件地址添加到列表中。

您可以与用户共享资源日历并授予该用户管理员权限。被委派为管理员的用户对该日历拥有完全的管理权限。他们可以查看、编辑、添加、删除、接受或拒绝邀请。

管理用户帐户

用户帐户状态

管理控制台：

主页→管理→账户

帐户状态决定用户是否可以登录并接收邮件。帐户状态显示在管理控制台的“帐户”窗格。

表 47. 状态 - 用户帐户

| 地位 | 描述 |
|-----|--|
| 积极的 | 邮箱帐户的正常状态。邮件已送达,用户可以登录客户端界面。 |
| 维护 | 日志记录已禁用,任何发往该帐户的邮件都会在 MTA 排队。 请注意,在备份期间或以下情况下,此状态会自动设置为帐户: 导入/导出/恢复账户。 |
| 待办的 | 当帐户已创建但尚未准备好激活时,对其进行分配。 待处理,登录将被禁用并且消息将被退回。 |
| 已锁定 | 用户无法登录,但邮件会继续发送到帐户。锁定状态可以 如果您怀疑邮件帐户已被泄露(用于未经授权的方式)。 |
| 关闭 | 登录被禁用且邮件被退回。此状态用于软删除帐户 然后再从服务器中删除。关闭帐户不会更改帐户许可证。 |
| 闭锁 | 当用户尝试使用错误密码登录时发生的自动状态。 锁定不能由管理员指定,但会在用户数量达到 尝试次数超出配置的允许尝试次数。锁定持续时间为 也可配置。 管理员可以随时解除锁定状态。 |

删除账户

管理控制台：

主页→管理→账户

您可以从管理控制台删除帐户。这将从服务器中删除帐户,删除
消息存储中的消息,并更改许可证中使用的帐户数量。



在删除帐户之前,请对该帐户进行完整备份以保存帐户信息。
另请参阅备份和恢复。

查看账户邮箱

您可以从管理控制台查看选定帐户的邮箱内容,包括所有文件夹、日历条目和标签。

管理控制台：

主页→管理→账户→ 帐户

选择 帐户 ,从齿轮图标中选择查看邮件。用户的 Zimbra 帐户将在新浏览器窗口中打开。

此功能可用于帮助遇到邮件帐户问题的用户,因为您和帐户用户可以同时登录该帐户。

任何访问帐户的查看邮件操作都会记录到audit.log文件中。

使用电子邮件别名

电子邮件别名是将所有邮件重定向到指定邮件帐户的电子邮件地址。别名不是电子邮件帐户。

每个帐户可以拥有无限数量的别名。

当您从“管理别名”导航窗格中选择“别名”时,内容窗格中将显示已配置的所有别名。您可以创建别名、查看特定别名的帐户信息、将别名从一个帐户移动到另一个帐户以及删除别名。

隐藏 GAL 中的别名

从 10.1.1 版本开始,您可以在 GAL 中隐藏别名。一旦隐藏,它们将不会在撰写邮件或搜索收件箱时出现在自动完成中。

该功能可在账户级别进行控制。默认情况下,该功能处于禁用状态。

该功能可以通过以下方式控制:

- 管理控制台

1. 登录管理控制台。
2. 前往主页→管理→账户→<account_name>→常规信息→账户名称→隐藏 GAL 中的别名
3. 可以使用复选框来启用/禁用该功能。

- 命令行

添加了一个新的 LDAP 属性zimbraHideAliasesInGal来控制该功能。

1. 作为zimbra用户,执行以下命令为帐户启用该功能:

```
zmprov ma <帐户名称> zimbraHideAliasesInGal TRUE
```

重击

2. 以zimbra用户身份执行以下命令强制同步更改并使更改生效:

```
zmgsautl forceSync -a <galsync@domain.com> -n InternalGAL
```

重击

使用分发列表

分发列表是包含在具有共同电子邮件地址的列表中的一组电子邮件地址。当用户向分发列表发送邮件时,他们会将邮件发送给地址包含在列表中的每个人。地址行显示分发列表地址;无法查看单个收件人地址。

您可以创建需要管理员管理成员列表的分发列表,也可以创建自动管理列表中成员添加和删除的动态分发列表。有关动态分发列表的详细信息,请参阅使用动态分发列表。

您可以从用户帐户的“成员”页面查看用户是哪些分发列表的成员。当 Zimbra 用户的电子邮件地址添加到分发列表时,用户帐户的“成员”页面将使用分发列表名称进行更新。当删除分发列表时,分发列表名称将自动从帐户的“成员”页面中删除。

设置分发列表的订阅策略

可以设置订阅策略来管理分发列表的成员资格。列表所有者从分发列表的“属性”页面管理订阅策略。

| 分配选项 | 描述 |
|--------|---|
| 新订阅请求 | <ul style="list-style-type: none"> 自动接受 任何订阅者均可成为会员。 需要列表所有者批准 要订阅,用户需要向分发列表的所有者发送电子邮件,然后所有者回复此电子邮件请求。 自动拒绝 无法将任何人添加到此分发列表。 |
| 取消订阅请求 | <ul style="list-style-type: none"> 自动接受 任何人都可以从列表中删除自己的名字。 需要列表所有者批准 要从通讯组列表中删除,用户需要向所有者发送电子邮件。所有者必须接受电子邮件请求才能删除该名称。 自动拒绝 用户不能将自己从列表中删除。 |

分发列表所有者的管理选项

您可以将所有者添加到分发列表,然后他们可以从 Zimbra 帐户的通讯簿、分发列表文件夹中管理列表。列表所有者可以右键单击分发列表,然后单击编辑组链接来编辑列表。

除了添加和删除成员外,所有者可以配置的分发列表属性包括:

- 将列表标记为私人,以便隐藏在全局地址列表中
- 管理谁可以向列表发送消息
- 设置会员订阅政策
- 添加其他所有者

创建分发列表

使用本节中的步骤创建通讯组列表:

管理控制台:

主页→管理→分发列表

1. 从齿轮图标上,单击新建。
2. 在 “成员”页面上,添加分发列表名称。请勿使用空格。其他字段是可选的。
3. 在右栏中找到要添加到通讯组列表的成员。选择要添加的成员,然后单击 “添加”
已选择。如果要添加页面上的所有地址,请单击添加此页面。如果要添加不在公司列表中的成员,请在或在下面输入地址部分中输入完整的邮件地址。
- 4.单击下一步,配置属性页面。

表 48. 分布属性选项

| 分布特性 选项 | 描述 |
|-------------|---|
| 可以接收邮件 | 默认启用。如果此分发列表不应接收邮件,请选择此框。 |
| 在 GAL 中隐藏用户 | 启用此功能可创建不显示在全局地址列表 (GAL) 中的分发列表。您可以使用此功能将分发列表的显示限制为仅知道地址的人。 |
| 邮件服务器 | 默认设置为自动。要选择特定邮件服务器,请取消选中自动并从列表中选择特定服务器。 |
| 动态组 | <p>如果选中此框,则会显示 “成员 URL”字段,并且您可以创建动态分发列表。</p> <p>请参阅创建动态分发列表。</p> |
| 新订阅 请求 | <p>请选择：</p> <ul style="list-style-type: none"> <input type="radio"/> 自动接受 <input type="radio"/> 需要列表所有者批准 <input type="radio"/> 自动拒绝 |
| 取消订阅 请求 | <p>请选择：</p> <ul style="list-style-type: none"> <input type="radio"/> 自动接受 <input type="radio"/> 需要列表所有者批准 <input type="radio"/> 自动拒绝 |

5. 在 “成员”页面中,选择应为该列表的直接或间接成员的分发列表。
6. 如果分发列表应该有别名,请创建它。
7. 如果此分发列表可由其他用户管理,请在所有者页面中输入这些电子邮件地址。
8. 设置如何回复分发列表中收到的消息。
9. 单击 “完成” 。分发列表已启用,URL 也已创建。

管理分发列表的访问

创建分发列表后,您可以管理谁可以查看分发列表的成员以及谁可以向分发列表发送消息。默认所有用户都有权访问所有分发列表。本节介绍如何使用 CLI 管理访问权限。

要限制谁可以访问分发列表,请向域中的单个用户授予权限,或者如果您只希望域成员访问分发列表,您可以授予域上的权限。当您授予域上的权限时,域上的所有分发列表都会继承此授予。

您可以授予单个分发列表的权限并配置允许访问分发列表的特定用户。

您可以通过 CLI zmprov grantRight (grr) 命令限制对分发列表的访问。

有关如何授予权限的详细信息,请参阅委派管理。

[谁可以查看通讯组列表的成员](#)

默认情况下,所有用户都可以查看分发列表中的成员地址。分发列表地址在地址气泡中显示一个+。用户可以单击此按钮以展开分发列表。将显示分发列表中的地址列表。用户可以从展开的列表中选择单个地址。

将可以查看分发列表中地址的人员限制为个人或域:

- 对于个人用户:

zmprov grr domain <域名> usr <user1@example.com> viewDistList

重击

- 对于域中的所有用户:

zmprov grr domain <域名> dom <example.com> viewDistList

重击

- 要授予分发列表的权限并允许特定用户查看列表:

zmprov grr dl <dl_name@example.com> usr <user1@example.com>

重击

[谁可以发送至分发列表](#)

默认情况下,所有用户都可以向所有分发列表发送消息。您可以向分发列表或域授予权限,以定义谁可以向分发列表发送消息。当用户尝试向他们无权使用的分发列表发送消息时,系统会发送一条消息,指出他们无权向收件人分发列表发送消息。

必须从主页→配置→全局设置→MTA启用Milter服务器。

限制谁可以向分发列表发送邮件到个人或域:

- 授予域中的单个用户向所有分发列表发送消息的权限。

zmprov grr domain <域名> usr <user1@example.com> sendToDistList

重击

- 授予域中的所有用户向所有分发列表发送消息的权限。

zmprov grr domain <域名> dom <example.com> sendToDistList

重击

限制访问并删除对不同用户类型的单独分发列表的限制。

- 特定内部用户的访问权限：

```
zmprov grr dl <dlname@example.com> usr <username@example.com> sendToDistList
```

重击

撤销访问权限

```
zmprov rvr dl <dlname@example.com> usr <username@example.com> sendToDistList
```

重击

- 仅限分发列表的成员访问：

```
zmprov grr dl <dlname@example.com> grp <dlname2@example.com> sendToDistList
```

重击

撤销访问权限

```
zmprov rvr dl <dlname@example.com> grp <dlname2@example.com> sendToDistList
```

重击

- 仅限域内所有用户访问：

```
zmprov grr dl <dlname@example.com> dom <example.com> sendToDistList
```

重击

撤销访问权限

```
zmprov rvr dl <dlname@example.com> dom <example.com> sendToDistList
```

重击

- 仅限外部域中的所有用户访问：

```
zmprov grr dl <dlname@example.com> edom <example.com> sendToDistList
```

重击

撤销访问权限

```
zmprov rvr dl <dlname@example.com> edom <example.com> sendToDistList
```

重击

- 仅限内部用户访问：

```
zmprov grr dl <dlname@example.com> 全部 sendToDistList
```

重击

撤销访问权限

```
zmprov rvr dl <dlname@example.com> 全部 sendToDistList
```

重击

- 仅访问所有公共电子邮件地址：

```
zmprov grr dl <dlname@example.com> pub sendToDistList
```

重击

撤销访问权限

```
zmprov rvr dl <dlname@example.com> pub sendToDistList
```

重击

- 仅访问特定的外部电子邮件地址：

```
zmprov grr dl <dlname@example.com> gst <someone@foo.com>      sendToDistList
```

重击

撤销访问权限

```
zmprov rvr dl <dlname@example.com> gst <someone@foo.com>      sendToDistList
```

重击

启用 AD 账户分发列表成员视图

要查看消息或地址簿中的 Active Directory 分发列表成员,必须在每个 Active Directory 的 Zimbra GALsync 帐户中配置 Active Directory 的 GAL 组处理程序。

使用本部分中的步骤更新每个 Active Directory 的 GALsync 帐户。此配置要求您知道 GALsync 帐户名称以及该 GALsync 帐户上的所有数据源。

1. 显示 GAL 同步账户的 Zimbra ID:

```
zmprov gd {域} zimbraGalAccountId
```

重击

查找名称:

```
zmprov ga {zimbraId-of-the-GAL-sync-account} 名称
```

重击

2. 显示 GALsync 帐户的数据源:

```
zmprov gds {域的 gal-sync 帐户名称}
```

重击

3. 启用 Active Directory 的组处理程序:

```
zmprov mds {gal-sync-account-name-for-domain} {AD-data-source-name} \
zimbraGalLdapGroupHandler类 com.zimbra.cs.gal.ADGalGroupHandler
```

重击

使用动态分发列表

动态分发列表会自动管理其成员资格。用户会自动从分发列表中添加和删除。创建动态分发列表时,会指定成员 URL。此成员 URL 用于标识谁应成为列表的成员。您可以从管理控制台分发列表的“属性”页面查看此 URL。

您可以从管理控制台或 CLI 创建动态分发列表。在 URL 中,您可以指定特定的对象类,以标识要添加到动态分发列表中的用户类型。例如,您可以配置一个对象类为 zimbraAccount 的动态分发列表。在这种情况下,当配置帐户或删除帐户时,动态分发列表会更新。

您可以为所有移动用户或 POP/IMAP 用户创建动态分发列表。

您可以修改分发列表以更改过滤规则。修改分发列表时,列表中的成员会更改以反映新规则。

创建动态分发列表

您可以使用管理控制台或 CLI 创建动态分发列表,如本节所述。

管理控制台:

主页→管理→分发列表。

1. 从齿轮图标上,单击新建。
2. 在“成员”页面上,添加动态通讯组列表名称。请勿使用空格。请勿将成员添加到列表。
- 3.单击下一步,配置属性页面。

表格49 分发列表选项

| 选项 | 描述 |
|--|---|
| 可以接收邮件 | 默认启用。如果此分发列表不应接收邮件,请选择此框。 |
| 在 GAL 中隐藏用户启用以创建不显示在全局地址列表中的分发列表 (GAL) | 。您可以使用此功能将分发列表的显示限制为仅那些知道地址的人。 |
| 邮件服务器 | 默认情况下,此项设置为自动。要选择特定邮件服务器,请取消选中“自动”,然后选择列表中的特定服务器。 |
| 动态组 | 勾选此框。 |
| 可用于正确的管理 | 取消选中此框。 |

| 选项 | 描述 |
|--------|--|
| 会员网址 | <p>成员 URL 是 LDAP 类型的 URL, 它定义了一个过滤器, 用于确定哪些用户被添加到列表中或从列表中删除。</p> <p>键入此列表的 URL。在命令中, ldap://??sub?是 URL。您可以添加任意组合过滤器来创建不同类型的动态分布列表。</p> <p>例子 全部和垃圾邮件/普通邮件帐户列表</p> <pre>ldap:///??sub?(objectClass=zimbraAccount)</pre> |
| | <p>委派管理员列表示例</p> <pre>ldap:///??sub?(&(objectClass=zimbraAccount) (zimbraIsDelegatedAdminAccount=TRUE))</pre> |
| | <p>示例 所有活跃帐户</p> <pre>ldap:///??sub?(&(objectClass=zimbraAccount) (ZimbraAccountStatus=active))</pre> |
| | <p>示例 头衔为 13. 经理的所有用户</p> <p>头衔取自账户的联系信息职位字段。在此 例如, 此字段将设置为“经理”。</p> <pre>ldap:///??sub?(&(objectClass=zimbraAccount)(title=经理))</pre> |
| 新订阅请求 | 选择自动拒绝。 |
| 取消订阅请求 | 选择自动拒绝。 |

4. 如果动态分发列表应该有别名, 请创建它。
5. 如果此动态分发列表可由其他用户管理, 请在所有者中输入这些电子邮件地址页。
6. 如果您想设置回复地址, 请在此处输入。对此分发列表的所有回复都将发送到此地址。
7. 单击“完成”。动态分发列表已创建。

根据您指定的过滤器, 系统会自动将用户添加到列表中。如果您添加或删除用户, 列表将已更新。

如果您使用 CLI 修改最初在管理中创建的动态分发列表
控制台 ,您必须为该动态分发列表设置zimbralsACLGroup FALSE 。

使用 CLI zmprov 命令管理动态分发列表。命令中的ldap:///?sub?是 URL。

您可以添加任意过滤器组合来创建不同类型的动态分发列表。

1. 创建所有新账户和现有账户的动态分发列表

包括所有用户、GAL 帐户名以及垃圾邮件/普通垃圾邮件帐户名。删除用户帐户时，
他们就被从名单上除名了。

```
zmprov cddl <all@domain.com> zimbralsACLGroup FALSE \
成员 URL 'ldap:///?sub?(objectClass=zimbraAccount)'
```

重击

2. 创建 COS 并分配用户

如果您创建 COS 并根据特定标准（例如所有经理）将用户分配给 COS,您可以快速
修改动态分发列表以用于特定 COS。

示例 包含 14 个用户中所有活跃账户的动态分发列表

具体的

操作系统

```
zmprov cddl <allusers@domain.com> zimbralsACLGroup FALSE \
memberURL ldap:///?sub?(&(objectClass=zimbraAccount) (zimbraCOSId=513e02e-9abc-4acf-
863a-6dccf38252e3) (zimbraAccountStatus=active))
```

重击

示例 A15。

包含所有用户的动态分发列表

在 职务名称

要使用此功能,帐户的联系信息职位字段必须包含职位。在此示例中,它
将被设置为“经理”。

```
zmprov cddl <allmanagers@domain.com> zimbralsACLGroup FALSE \
memberURL ldap:///?sub?(&(objectClass=zimbraAccount) (zimbraCOSId=513e02e-9abc-4acf-
863a-6dccf38252e3) (头衔=经理))
```

重击

示例 16. 所有委派管理员的动态分发列表

```
zmprov cddl <alldelgateadmins@domain.com> zimbralsACLGroup FALSE \
memberURL ldap:///?sub?(&(objectClass=zimbraAccount) (zimbraCOSId=513e02e-9abc-4acf-
863a-6dccf38252e3) (zimbralsDelegatedADminAccount=TRUE))
```

重击

移动邮箱

邮箱可以在共享同一 LDAP 服务器的 Zimbra 服务器之间移动。

您可以从管理控制台移动邮箱,也可以使用 CLI 命令zmmboxmove重新定位
将邮箱从一台服务器迁移到另一台服务器,而无需关闭服务器。

目标服务器管理邮箱移动过程。移动过程在后台运行,帐户保持活动模式,直到大部分数据移动完毕。帐户短暂锁定以移动最后的数据,然后返回活动模式。

邮箱移动过程经过以下步骤:

- 邮箱 blob 已移动到新服务器
- 当大部分内容被移动后,帐户将进入维护模式
- 数据库表、索引目录和任何更改的 blob 都会被移动
- 帐户重新进入活动模式

邮箱移至新服务器后,旧服务器上仍会保留一份副本,但旧邮箱的状态为关闭。用户无法登录,邮件也无法送达。在清除旧邮箱之前,请检查所有邮箱内容是否已成功移动。

- 将邮箱移动到新服务器

```
zmmboxmove -a <email@address> --from <服务器名称> --to <服务器名称>
```

重击

- 从旧服务器清除邮箱

```
zmpurgeoldmbox -a <电子邮件@地址> -s <服务器名称>
```

重击

移动邮箱的全局配置选项

可以设置移动邮箱的全局配置选项,以在移动邮箱时排除搜索索引、blob 和 SM blob。可以在导出服务器或目标服务器上设置以下配置选项:

- zimbraMailboxMoveSkipSearchIndex 如果不包含搜索索引数据,则邮箱必须移动后重新编制索引。
- zimbraMailboxMoveSkipBlobs 排除与邮箱相关的 Blob,包括主卷和辅助卷 (SM)。
- zimbraMailboxMoveSkipHsmBlobs 当正在移动的邮箱中已经存在 SM blob 时,此功能很有用。如果未配置zimbraMailboxMoveSkipBlobs ,但您想要跳过 SM 卷上的 blob,请设置此项。

监控 Zimbra 服务器

Zimbra Collaboration (Zimbra) 包括以下内容,可帮助您监控 Zimbra 服务器、使用情况和邮件流:

- Zimbra Logger 包用于捕获和显示服务器统计数据和服务器状态,并创建夜间报告
- 邮箱配额监控
- MTA邮件队列监控
- 日志文件

此外,选定的错误消息会生成 SNMP 陷阱,可以使用 SNMP 工具进行监控。

检查整个系统的整体健康状况超出了本文档的范围。

Zimbra 记录器

Logger 包含用于系统日志聚合和报告的工具。安装 Logger 是可选的,但如果不安装,则不会捕获服务器统计信息和服务器状态信息。

在具有多个 Zimbra Collaboration 服务器的环境中,仅在一个邮箱服务器上启用 Logger。

此服务器被指定为监控主机。Zimbra Collaboration 监控主机负责检查所有其他 Zimbra Collaboration 服务器的状态,并在 Zimbra 管理控制台上显示此信息。可以显示实时服务状态、MTA、垃圾邮件、病毒流量和性能统计信息。记录器会创建有关邮件活动的每日报告,例如邮件数量、平均投递延迟和生成的错误。

在多服务器安装中,您必须在每台服务器上设置 syslog 配置文件,以使 Logger 能够在管理控制台上显示服务器统计信息,并且必须启用 Logger 主机。如果您在安装 Zimbra Collaboration 时没有配置此项,请执行此操作

现在。

启用服务器统计

启用服务器统计信息以显示有关过去 48 小时、30 天、60 天和过去一年内处理的消息的入站消息量、入站消息计数、反垃圾邮件/反病毒活动和磁盘使用情况的系统范围和服务器特定数据。

1. 在每个服务器上,以 root 身份输入`/opt/zimbra/libexec/zmsyslogsetup`。这将更新 syslog 配置以启用收集服务器统计信息。
2. 在记录器监控主机上,您必须配置syslog以接受来自远程计算机的 syslog 消息。请参阅
<https://wiki.zimbra.com/wiki/Configuring-Logger-Host>了解详情。

对于单节点安装,这些步骤不是必需的。

查看服务器状态

管理控制台:

首页→监控

服务器状态页面列出了所有服务器和服务、它们的状态以及上次检查服务器状态的时间。服务器包括 MTA、LDAP 和邮箱服务器。服务包括 MTA、LDAP、邮箱、SNMP、反垃圾邮件、反病毒、拼写检查器和记录器。

如果服务器未运行,请使用zmcontrol CLI 命令来启动它。您可以从管理控制台停止和启动服务。

启用或禁用服务器服务

管理控制台：

主页→配置→服务器→服务器

服务器服务可在服务器→服务器页面。在导航窗格中选择服务,然后选择启用或禁用服务。

查看服务器性能统计信息

如果在 Zimbra 邮箱服务器上安装了 Logger 包,则服务器统计信息将显示邮件计数、邮件量、反垃圾邮件和反病毒活动的条形图。显示的信息为过去 48 小时、30 天、60 天和 365 天。

在导航窗格中选择“服务器统计信息”时,将显示所有邮箱服务器的综合统计信息。在扩展视图中选择特定服务器将仅显示该服务器的统计信息。服务器特定信息还包括磁盘使用情况、会话信息和邮箱配额详细信息。

以下显示系统范围的信息：

- 消息计数 计算消息事务。事务定义为每个人通过 SMTP 收到的消息 (由 Postfix 接收) 或每个人通过 LMTP 发送的消息 (由 mailboxd 发送)。例如,如果向三个人发送了一条消息,则显示六项事务。SMTP 到 Postfix 的事务为三项,LMTP 到 mailboxd 的事务为三项。消息计数增加六项。

- 消息量 显示每小时和每天发送和接收的交易的总大小 (以字节为单位)。
图表显示了按字节计算的总入站数据量。
- 反垃圾邮件/反病毒活动 显示已检查垃圾邮件或病毒的邮件数量以及被标记为垃圾邮件或被认为包含病毒的邮件数量。每扫描一封邮件,AS/AV 计数就会增加一。发送给三个人的一封邮件仅算作一封由 AS/AV 处理的邮件。

邮件计数和反垃圾邮件/防病毒活动图表显示不同的邮件计数,因为：

- 出站消息可能不会经过 Amavisd 过滤器,因为系统架构可能不需要检查出站消息。
- Amavisd 接收邮件并检查邮件中是否含有垃圾邮件和病毒,然后才将其发送给邮件中的所有收件人。邮件计数显示收到邮件的收件人数量。

服务器特定的统计信息还包括以下详细信息：

- 磁盘 显示所选服务器的已用磁盘和可用磁盘空间。显示最近一小时、一天、一月和一年的信息。
- 会话 显示有关活动 Web 客户端、管理员和 IMAP 会话的信息。您可以查看打开了多少个活动会话、谁登录了、会话创建时间以及上次访问会话的时间。

- 邮箱配额 按邮箱大小降序显示每个帐户的信息。请参阅监控邮箱配额。

配置记录器邮件报告

记录器每天晚上 11:30 生成有关邮件活动的报告并将其发送到管理员的电子邮件地址。

您可以配置报告中要包含的账户数量。默认为 25 个发件人和 25 个收件人帐户。

- 更改要添加到报告中的收件人数量：

`zmlocalconfig -e zimbra_mtareport_max_recipients=<数字>`

重击

- 更改要添加到报告中的发件人数量：

`zmlocalconfig -e zimbra_mtareport_max_senders=<数量>`

重击

配置磁盘空间通知

您应该定期检查磁盘容量，当磁盘已满时，请采取预防措施来维护服务。当磁盘空间不足时，会向管理员帐户发送警告电子邮件通知。

默认当阈值达到 85% 时发出警告警报，当阈值达到 95% 时发出严重警报。

您可以更改这些值。使用`zmlocalconfig`配置磁盘警告阈值。

- 警告警报

警告阈值

重击

- 严重警报：

磁盘日志临界值

重击

当启动`zmcontrol`启动服务时，您应该清理磁盘以释放空间，如果超过阈值，则会在服务启动前显示警告。

监控服务器

Zimbra 协作服务器收集许多与性能相关的统计数据，可以帮助您诊断问题和负载问题。

管理控制台：

主页→监控→高级统计

高级统计页面包括高级图形选项，可让您根据 CPU、IO、mailboxd、MTA 队列、MariaDB 和其他组件的统计信息生成各种图表。

要绘制高级统计中的图表，请选择其中一个组，然后从特定计数器列表中选择要显示的信息类型。

这些信息涵盖了广泛的数据：

- cpu.csv CPU 使用率。此组包含用于跟踪 CPU 使用率 (iowait、空闲、系统、用户、时间等) 的计数器。可以在服务器级别和进程级别跟踪 CPU 信息。
- df.csv 捕获磁盘使用情况。跟踪每个磁盘分区的磁盘利用率。
- fd.csv 文件描述符计数。跟踪系统文件描述符随时间变化的使用情况。这主要用于跟踪“文件描述符不足”错误。
- mailboxd.csv Zimbra 协作服务器和 JVM 统计信息。Mailboxd 几乎将所有统计信息都存储在此处。
需要跟踪的有趣数字是 heap_used、heap_free、imap_conn、soap_sessions、pop_conn 和 db_conn_count。
- mtaqueue.csv Postfix 队列。此文件测量邮件队列的大小（以邮件数量和字节为单位）。
- proc.csv Zimbra 进程的进程统计信息。例如 mailboxd/java、MariaDB、OpenLDAP 等)
- soap.csv SOAP 请求处理时间。
- threads.csv JVM 线程计数。计算具有通用名称前缀的线程数。
- vm.csv Linux VM 统计信息（来自 vmstat 命令）。
- io-x.csv 和 io.csv 存储来自 iostat(1) 命令（带有 iostat -x 的 io-x.csv）的数据。

配置拒绝服务过滤器参数

拒绝服务过滤器 (DoSFilter) 限制通过 HTTP/HTTPS 发送的请求泛滥。DoSFilter 会限制在短时间内发送大量请求的客户端。

DoSFilter 仅适用于 HTTP 和 HTTPS 请求，换句话说，它不会影响任何其他协议（如 POP3、IMAP 或 SMTP）的请求。您可以修改配置以满足您的特定环境需求。Zimbra 默认启用 DoSFilter。不建议禁用 DoSFilter。有关防止多次登录失败的信息，请参阅密码策略。

识别误报

有时 Zimbra Connector for Outlook (ZCO)、移动 ActiveSync 客户端或运行某些 zmprov 命令会触发 DoSFilter。发生这种情况时，Zimbra 邮箱服务不可用。您可以查看以下日志以查看是否应用了 DoSFilter。

- 请参阅 /opt/zimbra/log/sync.log。

例 17. 同步日志 条目显示 拒绝服务过滤

| 2021-01-15 15:52:20,426 警告 [qtp1635701107-91:https://xxxx/ Microsoft-Server-ActiveSync? User=zsupport2&DeviceId=Appl5dddd3NR&DeviceType=iPhone&Cmd=FolderSync] |
|--|
| [name=zsupport2@domain.com;mid=64;ip=10.1.2.3;Cmd=FolderSync;DeviceID=Appl5K0113UN3NR;Version=12.1;] 同步 - 服务异常 com.zimbra.common.service.ServiceException:代理请求到目标服务器时出错:HTTP/1.1 503 服务不可用ExceptionId:qtp1635701107-91:https://10.10.0.54:443/Microsoft-Server-ActiveSync? |
| 用户 = zsupport2&DeviceId=Appl5K0113UN3NR&DeviceType=iPhone&Cmd=FolderSync:1358286740426:c5ca 7f36bb0a038f 代码: service.PROXY_ERROR Arg:(url,STR, "http://mail.domain.com:80/ service/soap/SyncRequest") |
| • /opt/zimbra/log/zmmailboxd.out |

例子

18. 邮箱地址

条目显示

拒绝服务过滤

```
2021-01-15 15:57:32.537:WARN:oejs.DoSFilter:DOS ALERT :ip=127.0.0.1,session=null,user=null
```

自定义 DoSFilter 配置

以下属性与zmprov一起使用来配置 DoSFilter。这些属性可以配置为全局设置和服务器设置。如果在服务器中设置了这些属性，则服务器设置将覆盖全局设置。

您可以修改这些设置，但建议采用默认配置。

| 属性 | 描述 |
|--|--|
| DoSFilter 延迟 zimbraHttpDosFilterDelay-Millis | <p>所有超过速率限制的请求在被考虑之前的延迟时间。默认值为 -1。</p> <ul style="list-style-type: none"> -1 = 拒绝请求 0 = 无延迟 任何其他值 = 延迟以毫秒为单位 <p>zmprov mcf zimbraHttpDosFilterDelayMillis {x}</p> <p style="text-align: right;">重击</p> |
| DoSFilter 每秒最大请求数 zimbraHttpDosFilterMaxRequestsPerSec | <p>每秒来自一个连接的最大请求数。</p> <p>超出此数量的请求将受到限制。默认值为 30，最小值为 1。</p> <p>zmprov mcf zimbraHttpDosFilterMaxRequestsPerSec {x}</p> <p style="text-align: right;">BASH</p> |
| DoSFilter IP 地址白名单 zmprov mcf zimbraHttpThrottleSafeIPs {xxxx,192.168.xx} | <p>应用 DosFilter 时要忽略的 IP 地址。此属性没有默认值，但以下环回 IP 默认列入白名单。</p> <ul style="list-style-type: none"> 127.0.0.1 ::1 <p>IP 地址应该用逗号分隔。</p> <p>zmprov mcf zimbraHttpThrottleSafeIPs {地址}</p> <p style="text-align: right;">重击</p> |

修改这些属性后需要重新启动邮箱服务器。输入：

zmmailboxdctl 重启

重击

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

- Zimbra 成员服务器 单个 masterLDAP 服务器控制下的 Zimbra 服务器会根据 IP 地址自动列入白名单。这些主机是使用 GetAllServersRequest 发现的。输入为 zmprov gas。

- 外部配置主机/SOAP API 可以将外部配置主机添加到 IP 白名单中,以确保 DoSFilter 不会阻止某些请求。例如,邮箱重新索引可能会每秒进行几次调用,从而触发 DoSFilter。

使用邮件队列

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,邮件在被传递到另一个队列之前,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迟队列。投递失败的原因记录在延迟队列的文件中。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,则邮件失败。邮件将被退回给原始发件人。退回队列的默认有效期为五天。

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。

更改退回队列生命周期

- MTA 服务器的退回队列生存期设置为五天。要更改默认队列生存期设置

```
zmlocalconfig -e bounce_queue_lifetime={#}
```

重击

- 将邮件永久退回给发件人,而不是先发送到延迟队列

```
zmlocalconfig -e zimbraLmtpPermanentFailureWhenOverQuota=TRUE
```

重击

通知发件人邮件被退回

在退回队列生存期将消息发回给发件人之前,可以通知发件人他们发送的消息在延迟队列中并且尚未送达。

配置以下属性以向发件人发送警告消息。

- 配置发件人收到仍在排队的电子邮件的消息头的时间。

```
zmlocalconfig -c postfix_delay_warning_time=0h
```

重击

- 使用 MTA 未传送的邮件的消息头配置邮政局长通知的收件人。

```
zmlocalconfig -c postfix_bounce_notice_recipient=邮政局长
```

重击

- 配置报告给邮政局长的错误类列表。

重击

```
zmlocalconfig -c postfix_notify_classes=资源,软件
```

有关这些 Postfix 属性更改的影响的详细信息,请参阅 Postfix 文档。

您可以从管理控制台监控邮件队列中的传递问题。

查看邮件队列

管理控制台：

[主页](#)→[监控](#)→[邮件队列](#)

如果您在邮件传递方面遇到问题,您可以在管理控制台中的邮件队列页面查看邮件队列,看看是否可以修复邮件传递问题。打开邮件队列时,可以查看当时的延迟、传入、活动、保留和损坏队列的内容。您可以查看邮件数量以及邮件的来源和目的地。

对于每个队列,“摘要”窗格按接收方域、原始 IP、发送方域、接收方地址、发送方地址以及延迟队列的错误类型显示邮件摘要。您可以选择任何摘要以在“邮件”窗格中按邮件查看详细的信封信息。

消息窗格显示从摘要中选择的搜索过滤器的单个消息信封信息
有。

可以对队列中的所有消息执行以下邮箱队列功能：

- 保留以选择要保留的一组邮件。传入、活动、延迟和损坏的邮件可以移动到保留队列。邮件将保留在此队列中,直到管理员将其移动。
- 释放可从保留队列中删除所有消息。消息将移至延期队列。
- 重新排队正在查看的队列中的所有消息。重新排队消息可用于发送由于已修复的配置问题而被推迟的消息。重新评估消息并忘记先前的惩罚。
- 删除正在查看的队列中的所有消息。

Zimbra MTA、Postfix 队列文件 ID 被重复使用。如果您重新排队或删除邮件,请注意邮件信封信息,而不是队列 ID。当您刷新邮件队列时,队列 ID 可能会用于不同的邮件。

刷新消息队列

您可以清除服务器上的所有邮件。单击邮件队列工具栏上的“清除”时,将立即尝试传送“延迟”、“传入”和“活动”队列中的所有邮件。

监控邮箱配额

邮箱配额适用于用户帐户中的电子邮件、附件、日历约会和任务。达到帐户配额时,所有邮件都将被拒绝。用户必须从其帐户中删除邮件才能使其低于配额限制 - 这包括清空他们的垃圾箱,或者您可以增加他们的配额。

观看限额

您可以从管理控制台上的服务器统计信息中检查各个帐户的邮箱配额。

邮箱配额让您即时查看每个帐户的邮箱大小和已用配额信息。

管理控制台：

首页→监控→服务器统计

1. 选择 服务器 您想要查看其统计信息。

2. 在导航窗格中,选择邮箱配额。邮箱配额页面显示以下信息：

- 配额列显示分配给账户的邮箱配额。配额可以在 COS 中配置,也可以按账户配置。
- 邮箱大小列显示使用的磁盘空间。
- 配额已用列显示已使用配额的百分比。

增加或减少配额

您可以从 COS 或帐户配置配额阈值,当达到该阈值时,会发送一条消息提醒用户他们即将达到其邮箱配额。

管理控制台：

主页→配置→服务等级→ 操作系统 →高级
主页→管理→账户→ →高级 帐户

1. 向下滚动到配额部分。

2.修改配额设置。

3.单击保存。

查看 MobileSync 统计数据

管理控制台中监控部分的MobileSync 统计信息页面显示 Zimbra 协作系统上当前连接的 ActiveSync 设备的数量。

监控身份验证失败

为了防范基于字典和分布式攻击,您可以配置zmauditwatch 。该脚本尝试通过查看身份验证失败的来源以及 Zimbra 邮箱服务器上所有帐户发生身份验证失败的频率来检测更高级的攻击,并向管理员的邮箱发送电子邮件警报。

检查的身份验证失败类型包括:

- IP/帐户哈希校验 如果在 60 秒内某个 IP/帐户组合发生 10 次身份验证失败,则默认发送电子邮件警报。
- 帐户检查 默认设置是,如果任何 IP 地址在 60 秒内发生 15 次身份验证失败,则发送电子邮件警报。此检查尝试检测针对单个帐户的分布式劫持攻击。
- IP 检查 默认情况下,如果在 60 秒内任何帐户的身份验证失败 20 次,则发送电子邮件警报。此检查尝试检测跨多个帐户的单个主机攻击。
- 全部身份验证失败检查 默认设置是,如果在 60 秒内从任何 IP 地址到任何帐户发生 1000 次身份验证失败,则发送电子邮件警报。应将默认值修改为邮箱服务器上活动帐户的 1%。

触发电子邮件警报的默认值在以下zmlocalconfig参数中发生更改:

- IP/账户值,更改zimbra_swatches_ipacct_threshold

- 账户检查,更改zimbra_swatches_acct_threshold
- IP检查,更改zimbra_swatches_ip_threshold
- 总体身份验证失败检查,更改zimbra_swatches_total_threshold 使用应接收警报的电子邮件地址配置 zimbra_swatches_notice_user。

查看日志文件

Zimbra Collaboration 通过 syslog 守护程序将其活动和错误记录到系统日志组合中,以及本地文件系统上的 Zimbra 特定日志中。下面描述的日志是用于分析和故障排除的主要日志。

包含 Zimbra Collaboration 活动的本地日志位于/opt/zimbra/log 目录中。

- audit.log 此日志包含用户和管理员的身份验证活动以及登录失败。此外,它还记录管理员活动,以便能够跟踪配置更改。
- clamd.log 此日志包含来自防病毒应用程序 clamd 的活动。
- freshclam.log 此日志包含与更新 clamd 病毒定义相关的信息。
- mailbox.log 此日志是 mailboxd log4j 服务器日志,包含来自邮箱服务器的日志。这包括邮箱存储、LMTP 服务器、IMAP 和 POP 服务器以及索引服务器。
- mysqld.log 此慢查询日志包含邮箱服务器中执行时间超过long_query_time 秒的所有 SQL 语句。

long_query_time 在 /opt/zimbra/conf/my.cnf 中定义。

- spamtrain.log 此日志包含 zmtrainsa 在定期执行期间的输出
计划任务。
- sync.log 此日志包含有关 Zimbra Collaboration mobilesync 操作的信息。

其他日志包括:

- /opt/zimbra/jetty/logs/ 这是记录 Jetty 特定活动的地方。
- /opt/zimbra/db/data/<hostname>.err 这是消息存储数据库错误日志。
- /opt/zimbra/logger/db/data/<hostname>.err 这是 Logger 数据库错误日志。

Zimbra 协作活动记录到系统 syslog

- /var/log/zimbra.log Zimbra 系统日志详细记录了 Zimbra MTA (Postfix、amavisd、反垃圾邮件、反病毒)、记录器、身份验证 (cyrus-sasl) 和目录 (OpenLDAP) 的活动。默认情况下,LDAP 活动记录到 zimbra.log 中。

系统日志

Zimbra Collaboration 修改了系统 syslog 守护程序,以便将邮件和本地 syslog 设施中的数据捕获到 /var/log/zimbra.log 中。这样 syslogd 就可以捕获多个 Zimbra Collaboration 组件中的数据,包括 Postfix、Amavis、ClamAV、mailboxd、zmconfigd 和 logger。SNMP 模块使用日志文件中的数据来生成严重错误的陷阱。zmlogger 守护程序还会收集此文件中的数据子集,以便通过管理控制台提供有关 Zimbra Collaboration 使用情况的统计信息。

默认情况下,mailboxd 配置为将其输出记录到/opt/zimbra/log/mailbox.log。您可以启用 mailboxd 来通过全局或服务器启用下列功能来利用集中式 syslogd 基础架构:

`zmprov mcf zimbraLogToSysLog TRUE`

重击

使用 log4j 配置日志记录

Zimbra 协作服务器使用log4j协作服务器已配置log4j , Java 日志包作为日志管理器。默认情况下,Zimbra 以记录到本地文件系统。您可以配置log4j以直接输出到另一个位置。转到Log4j 网站(<https://logging.apache.org/log4j/2.x/>)有关使用的信息

log4j 是一个日志工具。

Zimbra 不检查 log4j 更改。要删除所有帐户记录器并重新加载 /opt/zimbra/conf/log4j.properties , 使用`zmprov resetAllLoggers`命令。

日志级别

默认日志记录级别设置为包含针对 INFO、WARNING、ERROR 和 FATAL 生成的日志。当问题开始出现,您可以打开 DEBUG 或 TRACE 日志级别。

要更改日志记录级别,请编辑log4j属性`log4j.properties` , 请参阅 `log4j.logger.zimbra`。

启用 DEBUG 时,您可以指定要调试的特定类别。例如,要查看 POP 的调试详细信息,请执行以下操作:活动,您可以输入`logger.zimbra.pop=DEBUG`。

log4j中预定义了以下类别:

| | |
|----------------------------|-----------|
| <code>zimbra.账户</code> | 帐户操作 |
| <code>zimbra.acl</code> | ACL操作 |
| <code>zimbra.备份</code> | 备份和恢复 |
| <code>zimbra.缓存</code> | 内存缓存操作 |
| <code>zimbra.日历</code> | 日历操作 |
| <code>zimbra.dav</code> | DAV 操作 |
| <code>zimbra.dbconn</code> | 数据库连接跟踪 |
| <code>zimbra.扩展</code> | 服务器扩展加载 |
| <code>zimbra.过滤器</code> | 邮件过滤 |
| <code>zimbra.gal</code> | GAL 操作 |
| <code>zimbra.库</code> | IMAP 协议操作 |
| <code>zimbra.索引</code> | 索引操作 |
| <code>zimbra.io</code> | 文件系统操作 |
| <code>zimbra.ldap</code> | LDAP 操作 |

| | |
|-----------------|---------------|
| zimbra.lmtp | LMTP 操作（传入邮件） |
| zimbra.邮箱 | 常规邮箱操作 |
| zimbra.misc | 各种各样的 |
| zimbra.on | 邮箱状态更改 |
| zimbra.pop | POP 协议操作 |
| zimbra.redolog | 重做日志操作 |
| zimbra.安全 | 安全事件 |
| zimbra.会话 | 用户会话追踪 |
| zimbra.smtp | SMTP 操作（外发邮件） |
| zimbra.soap | SOAP 协议 |
| zimbra.sqltrace | SQL 跟踪 |
| zimbra.store | 邮件存储磁盘操作 |
| zimbra.sync | 同步客户端操作 |
| zimbra.系统 | 启动/关闭和其他系统消息 |
| zimbra.wiki | Wiki 操作 |
| zimbra.zimlet | Zimlet 操作 |

日志级别的更改会立即生效。

表日志事件50.

| 等级 | 当地的？ | 系统日志 | SNMP 陷阱 | 使用时 |
|-----|------|------|------------|--|
| 致命和 | | 和 | 和 | 指定应用程序要中止的非常严重的错误事件或影响大量用户。例如，无法联系 MariaDB 数据库。 |
| 错误和 | | 和 | 否 | 指定可能仍允许应用程序执行的错误事件继续运行或影响单个用户。例如，单个邮箱索引损坏或无法删除来自邮箱的消息。 |
| 警告并 | | 否 | 否 | 表示有潜在危害的情况，但通常可恢复或可忽略。例如，用户登录失败。 |

| 等级 | 当地的? | 系统日志 SNMP | | 使用时 |
|-----|------|-----------|---|--|
| | | 陷阱 | | |
| 信息和 | | 否 | 否 | 指定突出显示应用程序进度的信息消息、基本事务级日志记录。例如,服务器启动、邮箱创建/删除、帐户创建。 |
| 调试 | | 否 | 否 | 这些事件通常有助于帮助客户调试问题。 |

(*) 一些非关键消息 (例如服务启动消息) 将生成陷阱。

协议追踪

协议跟踪可在以下日志记录类别中使用：

```
zimbra.smtp
zimbra.lmtp
zimbra.soap
zimbra imap
zimbra imap-客户端
zimbra.pop
zimbra.pop-客户端
```

查看 mailbox.log 记录

mailbox.log文件包含邮箱服务器上执行的所有操作,包括身份验证会话、LMTP、POP3 和 IMAP 服务器以及索引服务器。查看mailbox.log以查找有关服务器运行状况的信息并帮助识别问题。

mailbox.log记录有效和无效的登录尝试、帐户活动（例如打开电子邮件、删除项目、创建项目、索引新邮件）、服务器活动（包括启动和停止）。邮件服务器上活动的进度记录为 INFO。如果活动的预期结果失败并发生错误,则会将异常写入日志。

您可以为单个帐户设置日志选项,以便跟踪一个用户的帐户活动,而无需用无关帐户的日志消息填充 mailbox.log。请参阅命令行实用程序, zmprov 杂项部分。

日志模式

默认情况下, mailbox.log中的日志条目具有以下 Log4j 模式:

```
%d%-5p [%t] [%z]%c {1} - %m%n
```

该模式由 6 个数据块组成:

- 日期和时间 (例如: 2021-01-22 19:23:07,100)
- 日志级别 (例如INFO)
- 线程名称 (例如[qtp1043351526-等)

547:https:https://localhost:7071/service/admin/soap/DeleteAccountRequest] , [Index-9] ,

- Zimbra 协作环境
- 成分名称（例如肥皂、邮箱，mbxmgr，ETC。）
- 日志消息。注意：日志消息部分可能跨越多行。当日志消息包含异常，堆栈跟踪将始终从错误消息下方的新行开始。

您可以在Log4j PatternLayout 文档中阅读有关 Log4j 模式的更多信息
[\(https://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html\)](https://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html)。

mailbox.log 中的线程名称

mailbox.log 中的线程名称带有前缀，用于标识内部组件。大多数线程都具有以下之一命名约定：“{线程前缀}-{线程号}”或“{线程前缀}-{线程号}:{url}”。

Zimbra Collaboration 中当前使用以下{thread prefix}值作为线程名称：btpool，水池，流控协议服务器，映射服务器，ImapSSL服务器，Pop3服务器，Pop3SSL服务器，计划任务，计时器，匿名lo服务，CloudRoutingReaderThread，气泡，套接字接受器，线，qtp。

前缀为qtp 的线程由 Jetty QueuedThreadPool 创建，具有以下命名约定：

“qtp[hash code]-{thread number}:{url}”，其中[hash code]是实例的哈希码值

拥有该线程的QueuedThreadPool（参见Object::hashCode_____）

[https://docs.oracle.com/javase/8/docs/api/java/lang/Object.html#hashCode\(\)](https://docs.oracle.com/javase/8/docs/api/java/lang/Object.html#hashCode())在 Java 平台文档中）。

线程名称中的{线程编号}是在每个线程工厂内单调增加的整数。线程

当mailboxd进程停止或重新启动时，数字会被重置。

为 SOAP 请求提供服务的线程报告的日志记录通常包含正在处理的请求的 URL

线程名称的[url]部分，如下例所示：

Log messages reported by threads serving HTTP/S requests also contain request URL



2017-10-25 00:00:04,365 INFO [qtp649734728-21794:<http://server1.mydomain.com/service/soap/SearchRequest>] [name=user1@mydomain.com;mid=443;oip=129.113.231.190;port=56632;ua=ZimbraWebClient - FF56 (Win)/8.8.3_GA_1872;] soap - SearchRequest elapsed=2

由于 Zimbra Collaboration 中存在已知错误，线程名称的[url]部分可能包含重复协议

标识符，如下例所示：

[qtp1043351526-547:<https://localhost:7071/service/admin/soap/DeleteAccountRequest>]

mailbox.log 中的 Zimbra 协作上下文

日志模式中的[%z]部分描述了 Zimbra 协作上下文，并由以下键值对组成：

格式为key=value，以分号 (;) 分隔。如果值包含分号，则分号为

用双分号 (;;) 替代。例如，浏览器 UserAgent 字符串通常包含分号，例如这个

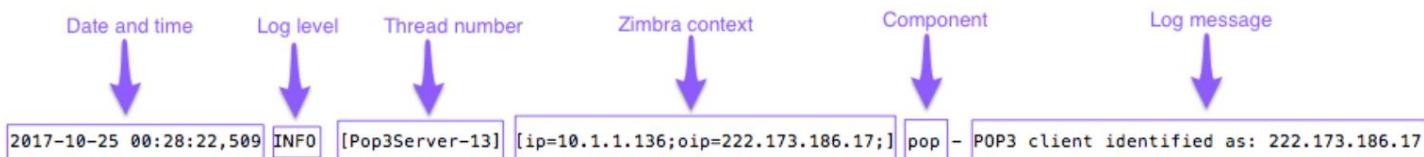
“Mozilla/5.0 (Windows NT 10.0; Win64;x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36”。在mailbox.log中，这个UserAgent字符串会以如下形式出现：

double ";" inside "ua" value

目前支持以下键值对，并且可以以任何顺序和任何组合记录在日志条目中：

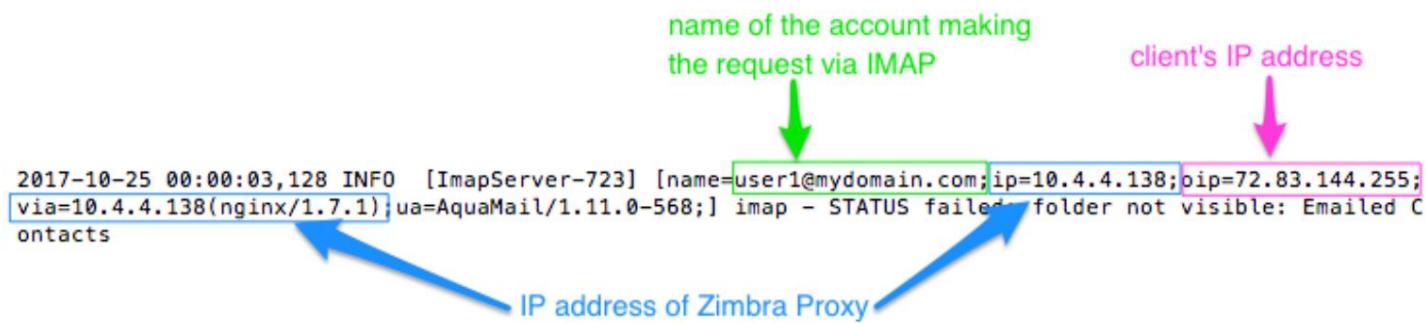
- ip 发出请求的 TCP/IP 客户端的 IP
 - oip 原始 IP 地址。当通过 NGINX 代理发出请求时,此值将包含客户端应用程序的 IP 地址,而 ip 值将包含代理服务器的 IP 地址
 - cid 单调递增的服务器连接 ID - 适用于跟踪单个连接
 - id 目标账户的 ID
 - name 目标账户的名称 (电子邮件地址)
 - aid 已认证账户的 ID。仅当目标账户与已认证账户不同时才存在
 - auname 已验证帐户的名称。仅当目标帐户与已验证帐户不同时才存在
帐户
 - mid 请求邮箱的 ID。仅当请求处理邮箱时才存在
 - ua 客户端应用程序的名称 (即用户代理)
 - via 请求的代理链的 IP 地址和用户代理列表
 - soapId 分配给 SOAP 请求的 ID,用于跟踪特定请求的代理跳转
 - msgid 正在操作的消息的 Message-ID 标头的值
 - ds 正在操作的数据源的名称
 - port 客户端连接的服务器端口
 - oport 请求的发起端口号
 - oproto 请求的发起协议。这可以由代表用户发出 SOAP 请求的内部组件传递 (例如 MTA)

下面的示例是一条记录,显示 2021 年 10 月 25 日午夜 28 分钟,IP 地址为 222.173.186.17 的 POP3 客户端已联系 Zimbra Collaboration 服务器,并且该请求通过 IP 为 10.1.1.136 的本地代理服务器进行代理。



以下示例显示了user1@mydomain.com使用 AquaMail 移动应用发送的失败IMAP STATUS请求的记录。用户设备的 IP 地址为 72.83.144.255（如`oip`字段中报告的那样）。该请求通过 Zimbra Collaboration nginx 代理发送到 IMAP 服务器，该代理的 IP 地址为10.4.4.138（如`ip`字段中报告的那样）

和通过字段)。



以下示例显示了 LMTP 服务器传递消息的记录。此日志消息中的 IP 地址最有可能属于在本地网络上运行的 Zimbra Collaboration MTA。

```
2017-10-25 00:00:03,646 INFO [LmtpServer-726] [ip=10.0.1.17;] lmtp - Delivering message: size=4096 bytes, nrcpts=1, sender=us
er4@mydomain.com, msgid=<421926844.25781.2504914800041.JavaMail.zimbra@mydomain.com>
```

下一个示例显示了 MailboxPurge 线程清除 ID 为 462 的消息的记录，该消息来自以下邮箱：

test@mydomain.net。此日志消息没有 ip 内部进程，而是来自外部请求。, 奥伊普 , 端口或通过字段, 因为它源自

```
2017-10-25 00:00:05,234 INFO [MailboxPurge] [name=test@mydomain.net;mid=462;] purge - Purging messages.
```

处理程序异常和堆栈跟踪

如果在活动进行过程中发生错误，则会在日志记录末尾添加处理程序异常，以通知您在流程执行过程中发生了中断正常流程的事件。这表示检测到某种类型的错误。

处理程序异常示例

```
007-06-25 00:00:10,379 信息 [btppool0-1064]
[name=nriess@example.com;mid=228;ip=10.2.3.4;ua=zimbra Desktop/0.38;] SoapEngine -处理程序
例外
```

有时，异常通知后会显示堆栈跟踪。堆栈跟踪报告线程和 Zimbra 的 mailboxd 服务中的监视器。此信息有助于调试，因为跟踪显示了发生错误。堆栈中的最后几个条目通常表明问题的根源。当由描述符包含在日志行中，这是错误的根源。在下面的示例中，错误是由 501 引起的，错误的地址语法。

例子 20. 堆栈跟踪

```

com.example.cs.mailbox.MailServiceException:无效地址： Jon R at
com.example.cs.mailbox.MailServiceException.internal_SEND_FAILURE (MailServiceException.java:412)at
com.example.cs.mailbox.MailServiceException.SEND_ABORTED_ADDRESS_FAILURE MailServiceException.java:416)

...
在 org.mortbay.thread.BoundedThreadPool$PoolThread.run(BoundedThreadPool.java:442)

原因： com.example.cs.mailbox.MailSender$SafeSendFailedException:501 地址语法错误 ;链接异常为 :com.sun.mail.smtp.SMTPAddressFailedException:
501 地址语法错误

在 com.sun.mail.smtp.SMTPTransport.rcptTo(SMTPTransport.java:1196) 在
com.sun.mail.smtp.SMTPTransport.sendMessage(SMTPTransport.java:584) 在
javax.mail.Transport.send0(Transport.java:169) 在
javax.mail.Transport.send(Transport.java:98) 在
com.example.cs.mailbox.MailSender.sendMessage(MailSender.java:409) 在
com.example.cs.mailbox.MailSender.sendMimeMessage(MailSender.java:262)
... 另外 30

```

邮箱日志文件

mailbox.log文件每日轮换。邮箱日志文件保存在/opt/zimbra/log中。以前的mailbox.log文件名包括文件的创建日期。没有日期的日志是当前日志文件。您可以备份和删除这些文件。

解决邮件问题

要检查mailbox.log中的错误,请搜索出现问题的电子邮件地址或服务。

另外,搜索WARN或ERROR日志级别,阅读消息文本。找到错误后,查看记录,追踪问题记录之前发生的事件。

系统崩溃

当您的系统崩溃时,找到启动消息,然后查找启动消息日期之前的错误。

此示例显示 2021 年 6 月 17 日发生内存不足错误。

[示例启动消息 21](#)

```
2021-06-25 01:56:18,725 INFO [main] [] soap - Servlet SoapServlet 正在启动
```

在启动消息之前查找错误。

例子 22. 错误信息

```
2021-06-17 20:11:34,194 FATAL [btpool0-3335]
[name=samd@example.com;aname=abcadmin@example.com;mid=142;ip=10.3.4.5;ua=zimbraConnectorFor BES/5.0.207;] 系统 - 处理程序异常
java.lang.OutOfMemoryError:PermGen 空间
```

邮件投递问题

找到“LmtpServer”服务。此示例包含一个堆栈跟踪报告,其中说明收件人地址被拒绝,因为该地址必须是完全合格的地址。

[示例邮件传递问题 23。](#)

```
2021-06-25 10:47:43,008 INFO [LmtpServer-250]
[name=bigen@example.com;mid=30;msgid=
<1291804360.35481182793659172.JavaMail.root@example.com>;] lmtp - 拒绝消息 bigen@example.com:发生异常com.zimbra.cs.mailbox.MailServiceException:
重定向到也失败 at
com.zimbra.cs.mailbox.MailServiceException.internal_SEND_FAILURE (MailServiceException.java:412) at
com.zimbra.cs.mailbox.MailServiceException.SEND_FAILURE(MailServiceException.java:424) at
com.zimbra.cs.filter.zimbraMailAdapter.executeActions
(zimbraMailAdapter.java:286)在 org.apache.jsieve.SieveFactory.evaluate (SieveFactory.java:151)在 com.zimbra.cs.filter.RuleManager.applyRules
(RuleManager.java:177)
```

在

```
com.zimbra.cs.lmtpserver.zimbraLmtpBackend.deliverMessageToLocalMailboxes(zimbraLmtpBackend .java:325) at

com.zimbra.cs.lmtpserver.zimbraLmtpBackend.deliver(zimbraLmtpBackend.java:140) at com.zimbra.cs.lmtpserver.LmtpHandler.doDATA(LmtpHandler.java:441)
at com.zimbra.cs.lmtpserver.LmtpHandler.processCommand(LmtpHandler.java:205) at
com.zimbra.cs.tcpserver.ProtocolHandler.processConnection(ProtocolHandler.java:231) at
com.zimbra.cs.tcpserver.ProtocolHandler.run(ProtocolHandler.java:198) at EDU.oswego.cs.dl.util.concurrent.PooledExecutor$Worker.run (未知来源)位于
java.lang.Thread.run (Thread.java:619)
```

原因：

```
com.zimbra.cs.mailbox.MailSender$SafeSendFailedException: 504 <too>: 收件人地址被拒绝:需要完全合格的地址;链式异常为：
com.sun.mail.smtp.SMTPAddressFailedException:504 <too>:收件人地址被
拒绝:需要完全合格的地址,位于 com.sun.mail.smtp.SMTPTransport.rcptTo (SMTPTransport.java:1196) ,位于 com.sun.mail.smtp.SMTPTransport.sendMessage
(SMTPTransport.java:584) ,位于 javax.mail.Transport.send0 (Transport.java:169) ,
位于 javax.mail.Transport.send (Transport.java:120) ,位于 com.zimbra.cs.filter.zimbraMailAdapter.executeActions
(zimbraMailAdapter.java:281)
```

... 还有 10

账户错误 - 登录错误

mailbox.log记录来自 IMAP、POP3 或 ZWC 的任何成功或失败的登录尝试。当您查找登录错误时,请先查找“Auth”。此示例显示来自 IP 地址 10.4.5.6 的某人试图使用 Windows 操作系统中的 Firefox 以管理员身份登录 Zimbra Classic Web App。由于它不是管理员帐户,因此权限被拒绝。

[示例帐户错误 - 登录 24。](#)

错误

```
2021-06-25 09:16:11,483 信息 [btpool0-251] [ip=10.4.5.6;ua=zimbraWebClient - FFX.X (Win);]
SoapEngine - 处理程序异常
com.zimbra.common.service.ServiceException:权限被拒绝:不是管理员帐户,位于 com.zimbra.common.service.ServiceException.PERM_DENIED
(ServiceException.java:205) ,位于 com.zimbra.cs.service.admin.Auth.handle (Auth.java:103)
```

账户错误 - IMAP 或 POP 相关

当您因为 IMAP 或 POP 问题而查找日志时,请查找“ImapServer/Pop3Server”。此示例显示尝试连接sires@example.com 时发生了致命的 IMAP 服务器错误。

示例帐户错误 - IMAP 错误 25。

```
mailbox.log.2021-06-19:2021-06-19 15:33:56,832 FATAL [ImapServer-2444]
[name=sires@example.com;ip=127.0.0.1;] 系统 - 处理时发生致命错误
联系
```

读取邮件头

每封电子邮件都包含一个标题,显示电子邮件从原点到目的地的路径。当邮件出现问题时,此信息用于跟踪邮件的路由。可以从 Zimbra Classic Web App 消息视图中查看 Zimbra 电子邮件消息标题。右键单击邮件并选择显示原始邮件。

邮件头中包含以下几行:

- 日期 发送消息的日期和时间。指定时间时,可以通过添加开始和停止时间来指定范围以搜索消息。
- 发件人 发件人姓名和电子邮件地址
- 收件人 收件人的姓名和电子邮件地址。表示主要收件人。
- 消息 ID 用于跟踪邮件路由的唯一编号
- 回复 - 回复消息的消息 ID。用于将相关消息链接在一起。
- 已接收:发件人 发送邮件的名称和 IP 地址。标题显示从 MTA 到 LMTP 以及从本地主机的已接收:发件人信息。

修复损坏的邮箱索引

在将邮件存入邮箱之前,系统会自动对邮件消息和附件进行索引。每个邮箱都有一个与之关联的索引文件。此索引文件是从邮箱中检索搜索结果所必需的。

如果邮箱的索引文件损坏或被意外删除,您可以从管理控制台重新索引邮箱中的邮件。

当索引损坏时,对帐户的文本搜索可能会失败并出现错误。您不能指望用户报告失败的文本搜索来确定索引已损坏。您必须监视索引日志中有关损坏索引的消息。如果服务器检测到损坏的索引,则会在 WARN 日志记录级别将一条消息记录到 Zimbra mailbox.log 中。该消息以“可能损坏的索引”开头。显示此消息时,管理员必须纠正问题。在许多情况下,纠正问题可能意味着重新索引邮箱。

重新索引邮箱内容可能需要一些时间,具体取决于邮箱中的邮件数量。重新索引期间,用户仍可访问邮箱,但由于搜索无法返回未索引邮件的结果,因此搜索可能无法找到所有结果。

检查索引损坏

使用zmprov verifyIndex命令对特定邮箱索引运行健全性检查。

```
zmprov verifyIndex <user@example.com>
```

重击

如果检测到问题,则返回故障状态并可对索引进行修复。

修复并重新索引损坏的索引

使用reIndexMailbox命令修复并重新索引损坏的索引。

```
zmprov reIndexMailbox <user@example.com> 开始
```

重击

这将返回 **开始**。

SNMP 监控和配置

SNMP 监控工具

您可能需要实施服务器监控软件来监控系统日志、CPU 和磁盘使用情况以及其他运行时信息。

Zimbra Collaboration 使用 swatch 监视系统日志输出以生成 SNMP 陷阱。

SNMP 配置

Zimbra Collaboration 包含一个带有 SNMP 监控的安装程序包。此包应在 Zimbra Collaboration 配置中的每台服务器 (Zimbra Collaboration、OpenLDAP 和 Postfix)上运行。

唯一的 SNMP 配置是应发送陷阱的目标主机。

生成 SNMP 陷阱的错误

当服务停止或启动时,Zimbra Collaboration 错误消息会生成 SNMP 陷阱。您可以使用第三方 SNMP 监控软件捕获这些消息,并将选定的消息发送到寻呼机或其他警报系统。

检查 MariaDB

MariaDB 数据库每周都会自动检查一次,以验证数据库的健康状况。此检查大约需要一个小时。如果发现任何错误,则会向管理员帐户发送报告。运行 MariaDB 检查的报告名称为zmbintegrityreport,并且 crontab 自动配置为每周运行一次此报告。

检查 MariaDB 数据库时,运行此报告会消耗大量 I/O。这应该不会造成问题,但如果您发现运行此报告确实会影响您的操作,则可以更改 zmbintegrityreport 的运行频率。请参阅Zimbra Crontab 作业。

检查 Zimbra 协作软件更新

安装 Zimbra Collaboration 后,Zimbra Collaboration 软件更新实用程序会自动配置为每天检查一次最新的 Zimbra Collaboration 版本,如果有更新,则向管理控制台的服务器更新中配置的地址发送通知。

Zimbra Collaboration 检查更新的日期和时间将保存到“更新”选项卡,并且会发送电子邮件通知,直到您更新 Zimbra 版本。如果您不想收到更新的电子邮件通知,请禁用“有更新时发送通知电子邮件”。

您可以配置以下内容：

- 检查更新的服务器 列出可用的服务器，并且只配置一个服务器。选定的服务器会检查更新，来自 www.zimbra.com 的更新响应结果会存储在 LDAP 中。
- 每 x 检查一次更新 默认为每天检查一次。您可以将频率间隔更改为每 x 小时、分钟或秒检查一次。配置了 cron 作业来检查新更新。如果频率间隔小于 2 小时，则必须修改 crontab 文件。
- 更新URL 此地址是服务器检查更新时连接的 URL。当 Zimbra Collaboration 服务器检查更新时，它会将其版本、平台和内部版本号传输给 Zimbra。
通常情况下，此 URL 不会改变。
- 要接收更新通知，请选中“有更新时发送通知电子邮件”，然后输入发送地址和发件人地址。默认地址是管理员的地址。
- 创建通用电子邮件。电子邮件的主题和内容可以更改。
- 当服务器轮询指定的 URL 时，将显示响应。

更新 Zimbra Connector for Microsoft Outlook

Zimbra Connector for Microsoft Outlook (ZCO) msi 文件可从管理控制台上的 Zimbra Utilities Downloads 页面获取。当新版本的 ZCO 在新版本的 Zimbra 之前发布时，您可以从管理控制台将新版本的 ZCO msi 文件上传到 Zimbra 服务器。该文件将上传到 /opt/zimbra/jetty/webapps/zimbra/downloads 文件夹。

管理控制台：

主页 → 工具和迁移 → 客户端上传

1. 将新的 ZCO 文件下载到您可以从管理中的客户端上传访问的计算机
安慰
2. 单击浏览以找到要上传的 ZCO 文件。
3. 重新启动 Zimbra：

`zmcontrol 重启`

重击

或者运行

`/opt/zimbra/libexec/zmupdatedownload`

重击

downloads/index.html 文件已更新为最新的 ZCO 客户端版本。可以从管理控制台主页 → 工具和迁移 → 下载页面上的 ZCO 链接下载此新文件。

如果不重新启动服务器，Zimbra Utilities 下载页面上的 ZCO 下载链接不会选择要下载的较新版本。

Zimbra Collaboration 发送的通知和警报

服务状态变更通知

当服务停止或重新启动时发送此通知。

服务器启动通知消息

主题:服务 <service_name> 已在 <zimbra_host> 上启动

服务状态改变 :<zimbra_host> <service>由停止变为运行

服务器停止通知消息

主题:服务 <service_name> 已在 <zimbra_host> 上停止

服务状态改变 :<zimbra_host> <service>由运行状态变为停止状态

磁盘使用情况通知

磁盘空间不足时 ,会向管理员帐户发送警告警报电子邮件通知。默认认为当阈值达到 85% 时发送警告警报,当阈值达到 95% 时发送严重警报

主题:磁盘 <volume>,位于 <zimbra_host> 上的 ##%

磁盘警告 :<zimbra_host> <volume> 位于设备 <device_name> 上 ##%

重复的 mysqld 进程运行通知

执行脚本来查看 mysqld 进程是否正在运行,以检测可能导致损坏的情况。如果发现有超过 1 个 mysqld 进程正在运行,则会生成一封电子邮件。

主题:ZCS:检测到重复的 mysqld 进程!

PID:\$pid PPID:\$ppid PGRP:\$pgrp

命令:\$cmdline

超过 \$maxcnt 个 mysqld 进程正在运行,父进程包括:\$procs 应立即调查此问题,因为它可能会导致数据库损坏

SSL 证书到期通知

每月 1 号都会生成一份报告,警告证书将在接下来的 30 天内到期。

主题:ZCS:SSL 证书即将过期!

管理控制台和 CLI 证书工具指南提供了有关如何替换自签名或商业证书的说明。

https://wiki.zimbra.com/index.php?title=Administration_Console_and_CLI_Certificate_Tools 使用 <zimbra_host> 上的 \$0 检查 SSL 证书是否过期。

每日报告通知

安装 logger 包后,crontab 中会自动安排每日邮件报告。报告每天发送到管理员的邮箱。

主题:<day> 的每日邮件报告

<每日报告数据>

数据库完整性检查通知

可以通过运行 crontab 中每周自动安排运行的 zmdbintegrityreport 来检查 MariaDB 数据库。报告将发送到管理员的邮箱。

主题:<zimbra_host> 的数据库完整性检查报告

生成报告无法运行\$cmd: \$!

发现数据库错误。

\$cmd --密码=XXXXXXXX

<命令输出>

未发现错误

命令失败\$!

备份完成通知

配置应运行的备份类型时,您可以设置接收有关备份会话结果的通知。

主题:ZCS 备份报告:成功

服务器:<服务器>

类型:增量

状态:已完成

开始时间:2021/07/13 星期五 01:00:05.488 PDT

结束时间:2021/07/13 星期五 01:10:09.842 PDT

重做日志序列范围:2 .. 2

账户数量:500

归档和发现

Zimbra 归档和发现是一项可选功能,可以归档传递给或由 Zimbra Collaboration 发送的消息并进行跨邮箱搜索。

归档功能的安装提供了 Zimbra 协作发现工具 (也称为跨邮箱搜索) 并设置允许在 Zimbra MTA 上启用归档的属性。

归档是按帐户配置的。每个启用归档的帐户都需要 Zimbra 归档许可证。当为帐户启用归档时,来自或发送到该帐户的所有电子邮件的副本都会在 MTA 处分叉,并且邮件的副本会发送到预定义的归档邮箱。归档过程对用户透明

帳戶用戶。

通过 Discovery,您可以在实时和存档邮箱中搜索电子邮件,并将结果复制到指定邮箱。

归档的工作原理

当用户发送或接收邮件时,邮件始终通过 Postfix MTA 路由。Postfix MTA 允许集成软件,该软件可以对正在传输的邮件执行操作。当为邮件的发件人或收件人启用存档时,Zimbra Archiving 会与 MTA 钩子和 Amavisd-New 实用程序集成以分叉邮件的副本。

“收件人或发件人是否启用了存档”检查是在 SMTP 标准信封上执行的,而不是在发件人或收件人/抄送标头上执行的。由于检查是在信封上执行的,因此可以捕获密件抄送副本和发送到分发列表的邮件。

例 26. 发送启用存档的邮件

例如,如果用户 A 向用户 B 发送一封邮件,并且用户 B 启用了存档功能,则 MTA 会递送两封邮件 一封到用户 B 的邮箱,一封到用户 B 的存档邮箱。用户 B 的邮箱中收到的邮件看起来正常,如下例所示:

```
已收到:来自 localhost (localhost.localdomain [127.0.0.1]) ...
发件人:userA@example.com 收件人:
userB@example.com 主题:新许
可证密钥 消息 ID:
<015f01c717fe$70f042d1$b1d6f61d@thom> 日期:2021 年 11 月 4 日星期一
23:48:18 -0000
```

嗨,B,

您可以再次将该软件的许可证密钥发送给我吗?

谢谢,A

用户 B 的存档邮箱中收到的邮件包含额外的X-Envelope-From和X-Envelope-To标头。这些标头显示了邮件发出的真实电子邮件地址以及邮件发送到的每个电子邮件地址。

已收到:来自 localhost (localhost.localdomain [127.0.0.1]) ...
发件人 :userA@example.com 收件人:
userB@example.com 主题:新许
可证密钥 消息 ID:
<015f01c717fe\$70f042d1\$b1d6f61d@thom> X-Envelope-发件人:
userA@example.com X-Envelope-收件人:
userB@example.com 日期:2021 年 11 月 4 日星期一
23:48:18 -0000

嗨,B,

您可以再次将该软件的许可证密钥发送给我吗?

谢谢,A

可以设置 Zimbra 归档来创建在 Zimbra Collaboration 内维护的归档帐户,或与第三方归档系统配合使用,使用 SMTP 转发将消息发送到第三方归档服务器。

对于第三方归档,Zimbra Collaboration 被配置为充当转发代理。

发现的工作原理

归档和发现的发现功能用于在实时和归档邮箱中搜索电子邮件和附件。可以从管理控制台运行^{*}发现工具,并将结果复制到您指定的目标邮箱。

^{*} 实时邮箱是系统上除存档帐户和系统帐户之外的帐户。

您可以按日期、发件人、收件人、抄送、主题、关键字和附件搜索发送和接收的电子邮件。您还可以创建查询以按名称、日期和时间范围、分发列表、别名进行搜索。

搜索结果放置在目标邮箱中。您可以通过创建不同的目标邮箱或在目标邮箱中为您运行的每个搜索创建单独的文件夹来组织搜索结果。X -zimbra-Source 标头信息会添加到复制到目标邮箱的每个邮件标头中。此标头标签包括帐户 ID、帐户名称以及帐户所在的服务器。

您可以通过登录目标邮箱地址来查看搜索结果。

安装归档包

您可以在现有的单服务器部署或多服务器部署上安装存档包。

如果邮箱服务器和 MTA 服务器位于同一节点,则您可以将归档配置和启用作为单个过程。如果您的邮箱服务器和 MTA 服务器位于不同的节点,则首先在至少一个邮箱服务器上安装 zimbra-archive 包,然后在部署中的每个 MTA 上启用归档组件。

在单服务器环境中安装 zimbra-archiving

以下场景假设 LDAP、MTA、邮件存储和归档服务器位于同一节点上。

1. 参考 Zimbra Collaboration 单服务器安装指南,打开与 Zimbra Collaboration 服务器的 SSH 连接。以 root 身份登录服务器并运行 ./install.sh 命令开始升级
过程。
2. 接受许可协议并输入 “Yes” 以运行升级。
3. 当出现要安装的软件包时,对 zimbra-archiving 键入 Yes。

升级过程开始，并安装存档包。此时，发现功能已安装并可使用。

要启用存档，请切换到zimbra用户并在 MTA 服务器上启用存档。

`zmprov ms <zimbrahostname> +zimbraServiceEnabled 存档`

重击

重新启动服务器。

`zmcontrol 重启`

重击

在多服务器环境中安装zimbra-archiving

以下升级场景是向您的 Zimbra Collaboration 环境添加一个专用于存档服务器的新服务器。

在开始安装过程之前，请记录以下信息。安装存档服务器时需要此信息。运行`zmlocalconfig -s`命令以查找该信息。

| | |
|------------|-------|
| LDAP 管理员密码 | _____ |
| LDAP 主机名 | _____ |
| LDAP 端口 | _____ |

有关安装软件包的详细步骤，请参阅 Zimbra Collaboration 多服务器安装指南中的多服务器安装章节。

1. 打开与正在配置用于归档的邮箱服务器的 SSH 连接。以root 身份登录服务器并解压 Zimbra 软件。运行`./install.sh`命令开始安装过程。

2. 输入y并按Enter 键安装以下软件包：

- zimbra 商店
- zimbra 归档

默认情况下安装zimbra-core包。

3. 输入y并按Enter键修改系统。

4. 主菜单显示您正在安装的 Zimbra 组件的默认条目。要展开菜单，

输入x并按Enter。

5.选择常用配置菜单，配置LDAP主机名、LDAP密码、LDAP端口。

6.选择zimbra-store菜单，配置管理员密码和许可证文件位置。

按照多服务器安装指南中安装 Zimbra 邮箱服务器的步骤完成安装过程。

此时，Discovery功能已安装完毕并可使用。

从管理控制台管理归档

安装存档后，您可以从管理控制台设置存档并对其进行管理。

启用存档

管理控制台：

主页→配置→全局设置→ MTA,从归档配置检查启用归档

从命令行重新启动 Zimbra

zmcontrol 重启

重击

创建专用存档 COS

您可以在 COS 中配置属性来设置邮箱功能、配额和密码、关闭垃圾邮件和病毒检查以及对 GAL 隐藏存档帐户。

管理控制台：

主页→配置→服务等级,从齿轮图标中选择新建

1. 根据归档 COS 的要求更改功能和首选项。
2. 如果您有专用存档服务器,请在服务器池页面中从列表中取消选择存档服务器。在具有专用存档服务器的多服务器部署中,应将该服务器从 COS 服务器池中移除,以便存档服务器不会随机分配给新帐户。

这些从服务器池中删除服务器的步骤不是在单服务器部署中完成的。创建专用的归档 COS 是一个好主意,因为这可以轻松创建配置相同的归档邮箱。

3. 如果需要,修改高级页面上的选项。
4. 在存档页面中,选中启用存档框,使此 COS 成为存档 cos。
5. 如果要更改存档帐户的命名方案格式,请修改两个模板字段。
请参阅设置存档帐户名称部分以了解更多信息。
6. 单击“完成”。

设置存档帐户名

您可以使用属性来创建和管理存档帐户的命名方案。您可以按 COS 或帐户设置这些属性。对于 COS,可以从管理控制台、COS 或个人帐户的存档页面更改这些属性。

- 帐户日期模板。设置名称模板中使用的日期格式。默认值为`yyyyMMdd`。将日期添加到帐户名称中可以更轻松地将旧数据从系统中转出到备份中。
- 帐户名称模板。设置如何创建存档邮箱名称。默认值为 `${USER} ${DATE}@${DOMAIN}.archive`。

档案帐户地址类似于以下示例：

`user-20210510@example.com.archive`

如果更改默认值,则必须使用创建有效电子邮件地址的语法。我们建议您将`.archive`添加到所有存档帐户,以在不可路由的域中创建存档邮箱,以防止欺骗
档案。

当基于`zimbraArchiveAccountDateTemplate`属性的模板设置后,运行`zmconfigarchive`时
`amavisArchiveQuarantineAccount`会更新为新的模板名称。

管理存档服务器

amavisd-new服务器进程控制帐户存档以及防病毒和反垃圾邮件进程。zmarchivectl命令可用于启动、停止、重新启动或获取控制帐户存档的amavisd-new服务器进程的状态。启动或停止存档进程时应小心谨慎,因为它是存档、防病毒和反垃圾邮件进程之间的共享服务器进程。对其中任何一个执行操作都会影响部署中可能启用的任何其他服务。

如果要禁用存档但不禁用防病毒或反垃圾邮件服务,请通过 CLI 或管理控制台禁用相应的服务。

设置用户邮箱存档

有四个属性与帐户的存档功能相关。两个用于配置邮箱,两个用于构建存档帐户名称的模板属性。

要设置邮箱存档,需要在主用户的邮箱上配置两个属性。一个属性用于启用存档,另一个属性用于显示邮件存档的位置。

- **当前存档至** 当前存档地址。存档至单个帐户。如果未设置,则不启用存档。
- **已归档账户** 此邮箱归档到的任何以前和当前的归档地址。包含给定账户已归档的所有账户。

存档邮箱

您可以创建具有或不具有指定 COS 的存档邮箱。您还可以将存档电子邮件转发给第三方。

启用存档功能的帐户将计入为存档功能购买的 Zimbra 许可证数量。存档邮箱与实时帐户一起列在管理控制台中。要查看当前许可证信息,请转到管理控制台:主页→配置→全局设置→许可证。

创建存档邮箱并分配 COS

存档账户是根据 Zimbra 存档名称模板创建的。

- 属性zimbralsSystemResource被添加到档案帐户并设置为 TRUE。
- 存档帐户显示在管理控制台中。
- 当启用了存档的邮箱收到一封邮件时,该邮件的副本将被发送到存档邮箱。

以zimbra身份登录,并使用zmarchiveconfig命令:

`zmarchiveconfig 启用 <account@example.com> archive-cos <archive>`

重击

创建没有 COS 或密码的存档邮箱

如果存档账户未分配 COS,则默认设置以下设置。

- 邮箱配额设置为0,无限制配额。
- 垃圾邮件和病毒检查已被禁用。

- 已启用在 GAL 中隐藏用户,因此存档帐户不会显示在 GAL 中并使用zmarchiveconfig命令:
以zimbra身份登录 ,

zmarchiveconfig 启用 <user@example.com>

重击

启用存档转发到第三方存档服务器

如果 Zimbra Collaboration 中没有维护存档账户,则无需设置密码、COS 或其他属性。

以zimbra身份登录 ,并使用zmarchiveconfig命令:

zmarchiveconfig 启用 <account@example.com> \ 存档地址 account-archive@offsite.com
\ 存档创建 false

重击

跨邮箱搜索

安装存档和发现功能后,您可以从管理控制台或通过命令行界面搜索邮箱。

您不需要配置任何存档邮箱来跨邮箱搜索,但必须安装存档包。

您可以通过创建具有访问邮箱搜索工具权限的委派管理员来指定用户从管理控制台运行邮箱搜索。

从管理控制台进行跨邮箱搜索

添加归档包后,发现工具“搜索邮件”将添加到导航窗格上的“工具和迁移”中。要设置跨邮箱搜索,请配置以下信息。

管理控制台:

主页→工具和迁移→搜索邮件,从齿轮图标中选择新建

- 服务器名称。要搜索的服务器名称。
- 目标邮箱和文件夹。系统会自动创建一个目标邮箱和文件夹。您可以将此邮箱用于所有搜索结果,并为每个搜索创建新文件夹,也可以为每个单独的搜索创建一个新的目标邮箱。

目标邮箱与任何其他邮箱一样,可以具有 COS 或帐户定义的任何功能或首选项。目标邮箱列在管理控制台帐户列表中。您可能希望为目标邮箱指定帐户名称,以将其标识为跨邮箱搜索的目标邮箱,并为目标邮箱配置特定的 COS 以便能够管理访问权限。

- 限制搜索返回的消息数量。默认为 500 条结果。
- 您可以选择在搜索完成后发送电子邮件通知。电子邮件通知的主题行中包含搜索任务 ID 和状态,您可以指定要包含在邮件中的信息类型,例如找到的邮件数量、搜索得到的地址列表以及使用的搜索查询。
- 选择要搜索的邮箱。选中“选择要搜索的账户”时,您可以选择要搜索的账户地址。

- 创建搜索查询。您可以按日期、发件人、收件人、抄送、主题、关键字和附件搜索发送和接收的电子邮件。高级功能可用于快速创建查询,按姓名、日期和时间范围、分发列表、别名进行搜索。

搜索存档消息时,您可以使用envfrom和envto查询语言扩展按信封地址进行搜索。

搜索运行时,“搜索邮箱内容”窗格会列出搜索和状态。单击“刷新”以更新此页。

搜索任务完成后删除,因为它占用服务器内存。服务器重启时,过去的搜索将被删除。

当您使用管理控制台中的发现功能时,该工具会复制您创建的目标邮箱中的邮件。这些邮件会占用服务器空间,从而增加服务器的大小。当不再需要这些邮件时,您可能希望从目标邮箱中删除它们。

法律信息请求

合法拦截功能会复制目标账户发送、接收或保存为草稿的电子邮件，并将这些邮件发送到指定的“影子”电子邮件地址。

法律拦截可配置为发送邮件的完整内容或仅发送标题信息。当目标帐户发送、接收或保存草稿邮件时，会自动创建拦截邮件，以将邮件副本作为附件转发到指定的电子邮件地址。

合法拦截设置

可以为服务类别或单个帐户配置合法拦截功能。此功能通过 CLI 使用 zmprov 进行配置。

设置合法拦截所需的唯一配置是在目标账户或 COS 上启用功能 zimbraInterceptAddress。

您可以启用属性 zimbraInterceptSendHeadersOnly 仅发送电子邮件消息的标题信息，而不是发送完整的消息。

设置合法拦截

指定拦截地址，接收拦截的消息。

- 如果启用 COS 拦截：

```
zmprov mc <cosname> zimbraInterceptAddress <account@intercept.example.com>
```

重击

- 如果为帐户启用拦截：

```
zmprov ma <accountname@example.com> zimbraInterceptAddress <account@intercept.example.com>
```

BASH

如果您要使用默认拦截消息模板和发件人地址（ postmaster@<yourdomain.com>`），则会设置合法拦截。

设置合法拦截以转发邮件头

要转发标题信息而不是帐户的完整消息：

```
zmprov ma <accountname@example.com> zimbraInterceptSendHeadersOnly TRUE
```

重击

修改拦截封面电子邮件信息

系统会自动创建一封电子邮件，以附件形式转发拦截邮件的副本。默认邮件内容包括：

- 发件人地址为“postmaster@<yourdomain.com>”
- 主题行“拦截<account@yourdomain.com>的消息<拦截消息主题>”
- 消息“拦截 <account@yourdomain.com> 的消息。
操作 = <消息类型>,文件夹 = <文件夹名称>,文件夹 ID = <#>”。

封面电子邮件信息可以修改。使用以下参数修改电子邮件信息。

| | |
|--------|---------------------------------|
| 帐户域 | 被拦截的账户域名。 |
| 帐户地址 | 被拦截的地址 |
| 消息主题 | 被拦截的消息的主题。 |
| 手术 | 用户正在执行的操作，“添加消息”，“发送消息”或“保存草稿”。 |
| 文件夹名称 | 保存消息的文件夹的名称。 |
| 文件夹 ID | 保存消息的文件夹的 ID。 |
| 换行 | 用于格式化多行消息正文。 |

使用本节中的步骤更改发件人姓名、主题行或邮件正文中的文本：

- 更改发件人姓名：

```
zmprov ma <accountname@example.com> zimbraInterceptFrom <newname@example.com>
```

重击

- 要更改主题行的文本：

```
zmprov ma <accountname@example.com> zimbraInterceptSubject \
<拦截消息主题文本> 参数 <文本> 参数
```

重击

- 要更改邮件正文中的文本：

```
zmprov ma <accountname@example.com> zimbraInterceptBody \
<拦截的消息文本> 参数
<text> 参数
```

重击

要通过 COS 修改,请输入 zmprov mc {cosname} …。

创建邮箱快照以进行法律调查

您可以使用 REST URL 格式为用户的邮箱创建查询,以搜索特定类型的电子邮件和附件,并将这些邮件压缩并保存到您的计算机中。此zip文件可以转发给请求的执法机构。

电子邮件消息在主题行后显示为.eml文件名。附件将以发送时的格式保存。

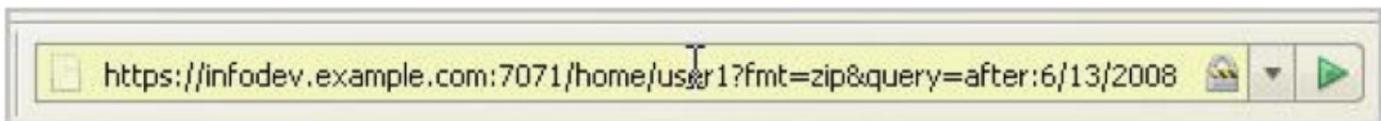
创建邮箱快照zip文件

您必须登录 Zimbra 管理控制台才能创建zip文件。您可以为一个一次只处理一个帐户。

1. 在浏览器的管理控制台地址栏中,在端口号7071/后输入:

home/<用户名>?fmt=zip&query=<搜索查询字符串>

例如:



在上面的例子中,搜索查询请求名为user1的所有帐户的zip文件。

您可以使用 Zimbra 中支持的任何搜索运算符进行搜索。例如,您可以按文件夹 (`in:folder_name`)、发件人姓名 (`from:<someone>`) 进行搜索,还可以使用多个搜索词。请参阅搜索提示 wiki 页面以获取关键字示例, https://wiki.zimbra.com/wiki/Search_Tips。

2. 按Enter或箭头创建 zip。系统会显示一个确认框,询问您是否要离开此页。
3. 单击确定。
4. 选择要保存zip文件的位置。此zip文件已准备好交付。

颜色和徽标管理

您可以更改 Zimbra Classic Web App 主题的徽标和基本颜色,而无需自定义单个 Zimbra Collaboration 主题。这可以从管理控制台或 CLI 完成。

更改 Zimbra Classic Web 应用程序上的主题颜色和徽标

本节介绍与经典 Web 应用相关的自定义。有关与现代 Web 应用相关的自定义,请参阅自定义现代 Web 应用

主题的基本颜色和自定义徽标可以配置为全局设置或域设置。

- 当全局设置发生更改时,更改将应用于所有服务器上的主题。
- 当域设置发生变化时,域上主题的基本颜色和徽标也会发生变化。

如果主题基色或徽标的全局设置和域级设置不一致,则会显示域的域值。

如果在多域 Zimbra Collaboration 环境中自定义徽标和基色,则必须设置虚拟主机作为基色:徽标属性根据浏览器发送的主机标头显示。

Zimbra Collaboration 包含各种主题。其中一些主题 - 例如

lemongrass、Hot Rod 和 Waves 等主题的图形或颜色代码在修改基色时不会发生变化。您可能希望从用户的主题偏好设置选项中禁用这些主题。

自定义基本主题颜色

Zimbra Classic Web App 主题中的以下基本颜色可以更改:

- 客户端中显示的主要背景颜色。此颜色是页面的背景。颜色的变体用于按钮、内容和窗格的背景颜色、选项卡和选择突出显示。在下图中,背景颜色与徽标一起显示,背景颜色的变体显示在登录区域中。
- 次要颜色是用于工具栏的颜色。
- 选择颜色是针对所选项目 (例如消息或概览窗格中的项目) 显示的颜色。
- 前景色是显示的文字颜色,默认文字颜色为黑色,文字颜色一般不需要改变。

更换经典 Web 应用程序徽标

您可以在全局或每个域中将徽标替换为您公司的徽标。

要替换的图形

以下徽标文件可以更改。您的徽标必须与此处指定的大小相同,否则图像可能无法正确显示。这些图形文件可以保存在另一台服务器上,也可以保存在 Zimbra Collaboration 升级时不会被覆盖的目录中。

- Zimbra Classic Web App 和 Zimbra Collaboration 管理控制台的登录和启动屏幕上显示的公司徽标。图形的尺寸必须正好是 300 x 30。
- Zimbra Classic Web App 应用程序和管理控制台左上角的小公司徽标。图形的尺寸必须正好是 170 x 35。
- 通过公司徽标链接的公司网址。

图形未更换

目前无法更改高级搜索工具栏中显示的图标和URL 浏览器地址栏中显示的favicon.ico。

使用管理控制台修改主题颜色和徽标

在管理控制台上,全局设置和域设置包含一个主题页面,可以配置该页面以自定义配色方案并添加公司徽标和徽标 URL。您可以上传公司徽标以在 Zimbra Classic Web App 和管理控制台页面上使用。

更改基本主题颜色

您可以从预定义颜色的弹出视图中选择颜色,也可以输入六位十六进制颜色值进行精确颜色匹配,以设置以下类别的主题颜色:

- 前景,即文本颜色。
- 背景,即客户端中显示的主要背景颜色。
- 次要颜色,用于窗格中的工具栏和选择标题的颜色。
- 选择,即为所选项目(例如消息、右键单击或下拉菜单选择)显示的颜色。

更改主题设置需要刷新服务器主题缓存。要刷新服务器,请转到主页→配置→服务器以获取服务器列表。右键单击服务器并从弹出菜单中选择刷新缓存。

使用自定义主题颜色容器为您的主题类别设置颜色:

管理控制台:

主页→配置→全局设置→主题或
主页→配置→域名→ →主题 领域

1. 点击要修改的主题类别旁边的字段,然后使用弹出的颜色选择器定义颜色供您选择。

您可以直接点击颜色,也可以使用输入字段输入颜色的十六进制值。无论哪种方式,您的选择都会显示在字段中。如果您选择退出颜色选择,请单击重置所有主题颜色以放弃您的设置。

2. 离开此页面将导致查询设置保存。

单击“是”(保存)或“否”(放弃您的设置)。

添加您的徽标

您可以从相应的主题页面全局或按域将 Zimbra Collaboration 徽标替换为您公司的徽标。您的徽标必须与“要替换的图形”部分中指定的大小相同,否则图像可能无法正确显示。图形文件保存在另一台服务器上或非

当 Zimbra Collaboration 升级时会被覆盖。

在全局设置→中配置自定义主题徽标部分时
主题页,必须填写此部分的所有字段才能正确显示图形。

高级搜索工具栏中显示的 Zimlet 图标和 URL 浏览器中显示的 favicon.ico
地址字段没有改变。

使用自定义主题容器的徽标来添加与主题相符的徽标:

管理控制台:

主页→配置→全局设置→主题或
主页→配置→域名→ →主题 领域

桌徽设置1.

| 选项 | 描述 |
|---------------------|--|
| 主题的 Logo URL | 与徽标相连接的公司网址。 |
| 应用程序徽标横幅主题的 URL | 登录时显示的公司徽标和 Zimbra Classic Web App 的启动画面和 管理控制台。图形的尺寸必须是 正好是 450x100。 |
| 应用程序徽标横幅预览 (200x35) | Zimbra 左上角的公司徽标 经典 Web App 应用程序和管理 控制台。图形的尺寸必须完全 120x35。 |
| 登录徽标横幅主题的 URL | |
| 登录徽标横幅预览 (440x60) | |

使用 CLI 更改主题颜色和徽标

要更改 Zimbra Classic Web App 主题基本颜色和徽标,请使用 zmprov 命令。以下属性可以配置为全局配置设置或域设置。颜色值以六位十六进制代码的形式输入。

表格颜色属性

| 属性 | 描述 |
|---------------------------|----------------------------------|
| zimbraSkinBackgroundColor | 主要背景颜色的十六进制颜色值 显示在客户端。 |
| zimbraSkinSecondaryColor | 工具栏和选定选项卡的十六进制颜色值。 |
| zimbraSkinSelectionColor | 所选项目颜色的十六进制颜色值。 |
| zimbraSkinForegroundColor | 文本的十六进制颜色值。这通常不 需要更改,因为默认是黑色。 |

更改主题的基本颜色

开始之前,请确定要更改的各个元素的六位十六进制基本颜色值。
您将在命令条目中使用这些。

全局设置

```
zmprov modifyConfig <属性名称> [ "#HEX_6digit_colorcode" ]
```

重击

域名设置

```
zmprov modifiedDomain <域> <属性名称> [ "#HEX_6digit_colorcode" ]
```

重击

修改域

本节中的示例演示如何更改为以下基色：

- 背景颜色 = 珊瑚色,#FF7F50
- 次要颜色 = 绿松石色,#ADEAEA
- 选择颜色 = 黄色,#FFFF00

1、指定皮肤颜色：以zimbra用户登录，使用zmprov修改域：

```
zmprov 修改域 example.com\
  zimbraSkinBackgroundColor #FF7F50 \
  zimbraSkinSecondaryColor #ADEAEA \
  zimbraSkinSelectionColor #FFFF00
```

重击

引号 “” 是必需的，因此使用#符号不会注释掉后面的文本。

2. 使用 zmmailboxdctl 命令通过重新启动邮箱服务器进程来应用更改：

```
zmmailboxdctl 重启
```

重新加载经典 Web 应用程序，该域的 Zimbra 协作主题现在应该显示这些颜色。

添加您的徽标

您可以通过修改以下徽标属性来添加公司徽标信息和 URL：

桌標標設定 53.

| 属性 | 描述 |
|-------------------------|--|
| zimbraSkinLogoURL | 您想要与徽标链接的公司网址。 |
| zimbra皮肤徽标登录横幅 | 在 Classic Web App 和 Zimbra Collaboration 管理控制台的登录和启动屏幕上显示的公司徽标文件名。 |
| zimbraSkinLogoAppBanner | 经典 Web App 应用程序和管理控制台左上角图形的徽标图形文件名。 |

为域添加徽标

如果徽标文件保存在 Zimbra 协作服务器中,则它们必须位于 /opt/zimbra/jetty/webapps/zimbra 的子目录中。

如果徽标托管在另一台机器上,请在识别徽标时输入完整的 URL。

使用本部分中的步骤更新域上显示的徽标:

1.更改URL链接:

```
zmprov 修改域 zimbraSkinLogoURL https://url.example.com/
```

2.修改logo显示:

要更改登录屏幕和启动屏幕中显示的徽标:

```
zmprov 修改域 zimbraSkinLogoLoginBanner /zimbra/loginlogo.png
```

要更改 Zimbra Classic Web App 主页上显示的徽标:

```
zmprov 修改域 zimbraSkinLogoAppBanner /zimbra/applogo.png
```

3.停止/启动服务器:

```
zmcontrol 重启
```

不是 目前支持: Zimbra Classic Web App 的徽标修改。

定制现代 Web 应用程序

本节仅适用于现代 Web 应用程序。

在本节中,我们将指导您自定义现代 Web 应用并部署您的自定义内容。我们将通过覆盖动态布局来解决自定义问题。

查看您所在组织的品牌指南,了解在 Zimbra 的现代 Web 应用程序中使用的图标和颜色。

可以定制哪些内容

一般来说,您可以在品牌框架内自定义以下内容:

- 徽标
- 各种小部件 (如按钮、链接和选项卡) 的颜色和边框
- 文本字体、颜色和大小
- 现代 Web 应用的基本外观

哪些不能定制

现代 Web 应用用户界面的多个部分需要大量 JavaScript 编码才能更改。自定义这些部分超出了本文档的范围:

- 改变某些事物的行为 (例如按钮)
- 应用程序选项卡的顺序
- 工具栏按钮的顺序
- 添加新的工具栏按钮
- 将搜索位置添加到搜索工具栏

设置

在开始定制现代 Web 应用程序之前,我们需要创建一个空的现代 Web 应用程序包。

您还应具备以下知识和技能:

- 熟悉 Linux 终端和命令的使用
- 熟悉基本的 HTML 和 CSS 概念和相关术语
- 熟悉字体、字体大小和行高等术语
- 熟悉徽标、图像、颜色代码和其他样式元素
- 熟悉组织的品牌指导方针

创建空 Bundle

我们首先在本地创建一个空文件夹及其内容。完成后,我们将该文件夹复制到 Zimbra 服务器。

文件夹名称

命名文件夹是至关重要的第一步。

- 保持文件夹名称与主机名相同,自定义会反映在这些域上的帐户上。

所有域名 并且,推而广之,所有

- 如果文件夹名称与域名相同,则自定义项将显示在
- 如果有虚拟主机设置,文件夹名称必须是您配置的域名
虚拟主机。

所有域名账户

。

例如,考虑一个名为example.com的域名,它有一个虚拟主机mail.example.com ;在这种情况下
在这种情况下,您必须创建一个文件夹mail.example.com。

查找主机名

- 使用ssh登录到您的 Zimbra 服务器。

2.切换到用户zimbra 。

与 - zimbra

3. 运行此命令以获取主机名。

zm主机名

查找域名

- 使用ssh登录到您的 Zimbra 服务器。

2.切换到用户zimbra 。

与 - zimbra

3. 运行此命令以获取域名。

zmprov gad

对于本文档,我们将mail.example.com视为文件夹名称。

文件夹内容

该文件夹 (在我们的例子中为mail.example.com)必须具有以下层次结构和内容。



使用mkdir创建新目录,使用 touch创建新文件。

[文件和](#) [文件夹层次结构](#)

```
mail.example.com
| 配置文件.json
| ...
| 调色板.css
资产
| favicon.ico
| —图标.png
| —图标.svg
| —登录页面背景.png
标志.svg
重量
| 清单.json
| —图标
    — icon_300x300.svg
    — ios
        | —图标_180x180.png
    — 非ios
        | 图标_16x16.png
        | 图标_32x32.png
        | 图标_36x36.png
        | 图标_48x48.png
        | 图标_72x72.png
        | 图标_96x96.png
        | 图标_144x144.png
        | 图标_150x150.png
        | 图标_192x192.png
        | 图标_256x256.png
        | 图标_512x512.png
```

自定义徽标

除非您指定辅助徽标,否则 Zimbra 的现代 Web 应用程序将使用您组织的主要徽标。

1. 将主徽标保存为logo.svg。
 2. 将辅助徽标保存为secondarylogo.svg。

除了徽标之外,您还需要组织的徽章作为图标使用。

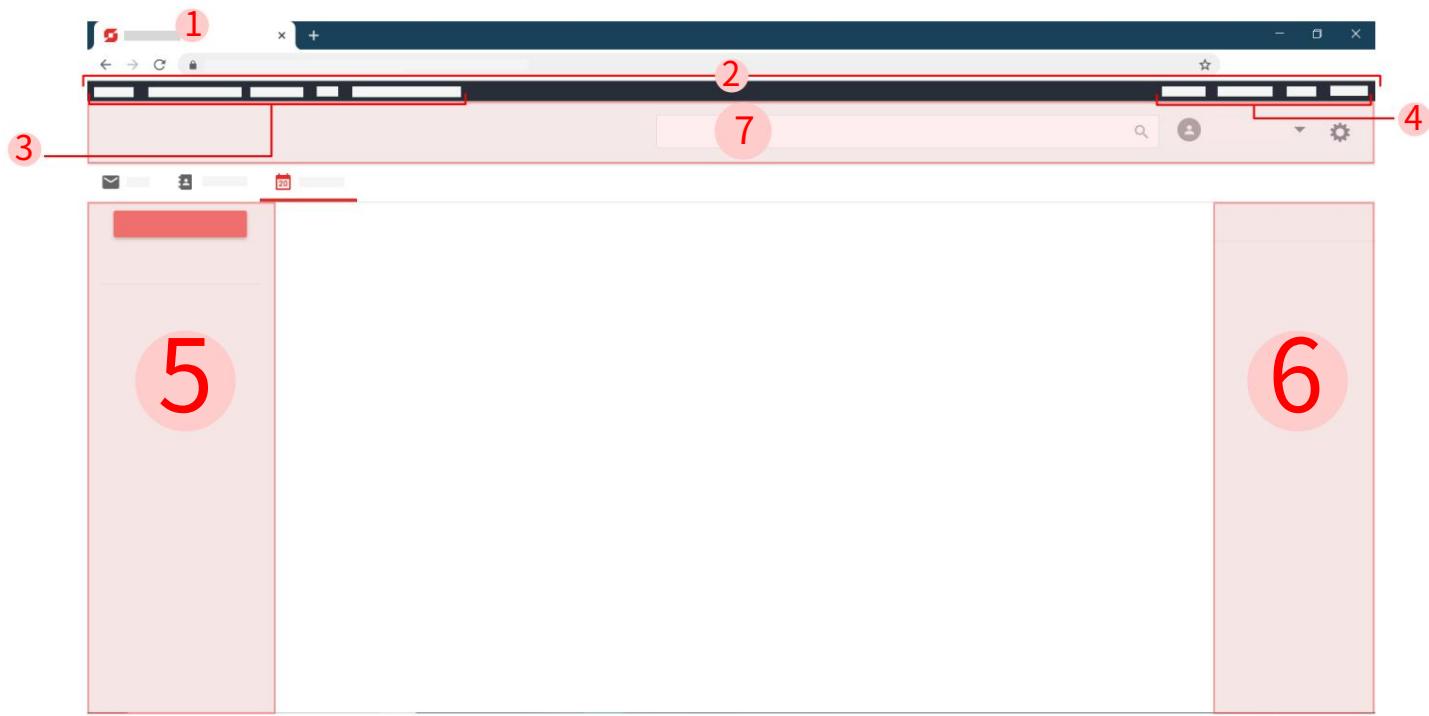
使用此徽标创建多个不同大小的图标。请参阅下表了解文件名、大小和每个图标的目的地。

| 图标文件名 | 图标大小（单位:px） | 目标文件夹 |
|--------|-------------|--------------------------|
| 图标.ico | 48x48 | /mail.example.com/assets |
| 图标.png | 512x512 | /mail.example.com/assets |
| 图标.svg | 那 | /mail.example.com/assets |
| 标志.svg | 那 | /mail.example.com/assets |

| 图标文件名 | 图标大小（单位:px） | 目标文件夹 |
|----------------|-------------|-------------------------------------|
| 次要徽标.svg | 那 | /mail.example.com/assets |
| 图标_16x16.png | 16x16x | /mail.example.com/pwa/icons/ios |
| 图标_32x32.png | 32x32x | /mail.example.com/pwa/icons/ios |
| 图标_57x57.png | 57x57 | /mail.example.com/pwa/icons/ios |
| 图标_72x72.png | 72x72 | /mail.example.com/pwa/icons/ios |
| 图标_114x114.png | 114x114 | /mail.example.com/pwa/icons/ios |
| 图标_180x180.png | 180x180 | /mail.example.com/pwa/icons/ios |
| 图标_16x16.png | 16x16x | /mail.example.com/pwa/icons/non-ios |
| 图标_32x32.png | 32x32x | /mail.example.com/pwa/icons/non-ios |
| 图标_36x36.png | 36x36 | /mail.example.com/pwa/icons/non-ios |
| 图标_48x48.png | 48x48 | /mail.example.com/pwa/icons/non-ios |
| 图标_72x72.png | 72x72 | /mail.example.com/pwa/icons/non-ios |
| 图标_96x96.png | 96x96 | /mail.example.com/pwa/icons/non-ios |
| 图标_144x144.png | 144x144 | /mail.example.com/pwa/icons/non-ios |
| 图标_150x150.png | 150x150 | /mail.example.com/pwa/icons/non-ios |
| 图标_192x192.png | 192x192 | /mail.example.com/pwa/icons/non-ios |
| 图标_256x256.png | 256x256 | /mail.example.com/pwa/icons/non-ios |
| 图标_512x512.png | 512x512 | /mail.example.com/pwa/icons/non-ios |

可定制的细分

请考虑下面的 Zimbra 的现代 Web 应用程序屏幕截图。



图可定制组件2。

此标记的屏幕截图显示了现代 Web 应用程序的可定制部分。

1. 标题
2. 包含链接的导航栏
3. 导航栏左侧链接
4. 导航栏右侧链接
5. 左侧边栏
6. 右侧边栏
7. 标题

标记为1、2、3和4的项目是文本和链接。更改它们的说明位于自定义文本和链接部分。

标记为5、6和7 的项目的颜色可自定义。更改这些颜色和其他颜色的说明位于自定义颜色和尺寸。

自定义文本和链接

1. 复制并粘贴示例 config.json 到 mail.example.com/config.json
2. 要更改标题文本（在可自定义组件中标记为1），请编辑示例中“标题”的值配置.json。
3. 在整个应用程序中将文本 Zimbra 替换为您组织的名称（本例中为“示例”），在示例 config.json 中更改“clientName”的值。
4. 要隐藏和删除忘记密码链接，请在示例 config.json 中将“disableForgotPassword”设置为“true”。
5. 要在导航栏中插入链接和超文本(2),请编辑示例中“nav”下的“left” (3)和“right” (4) 配置.json。
 - 要完全删除导航栏,请删除以下代码片段:

```
“导航”：
{
  .
  .
  .
}
```

示例 config.json

```
{
  title : “示例邮件”， version : 1 ,
  clientName : “示例”，
  userHelpPath : “https://
www.example.com/userguide/”， nav :{ left :[{

    “name” : “示例链接 1”， “href” :
    “https://www.example.com/1”
},{

    “name” : “示例链接 2”， “href” :
    “https://www.example.com/2”
}

], “正确的”：
[{
    “name” : “示例链接 1”， “href” :
    “https://www.example.com/1”
},{

    “name” : “示例链接 2”， “href” :
    “https://www.example.com/2”
}
]
}
}
```

定制颜色和尺寸

此部分处理字体、徽标和侧边栏的颜色和大小等。

调色板.css

该文件可帮助您创建在整个应用程序中使用的调色板。

1. 导航到调色板生成器 (<https://zm-x-theme-generator.netlify.com/>) 并输入十六进制代码 (https://en.wikipedia.org/wiki/Web_colors) 针对原色、间色和三次色。
2. 指定与成功、信息、警告和危险消息相关的颜色的十六进制代码。
3. 单击生成。
4. 出现带有颜色代码的现成样式模板。
5. 单击复制。
6. 将生成的内容粘贴到 mail.example.com/palette.css 中。

索引.css

复制以下片段并按原样粘贴到 mail.example.com/index.css 文件中。更改值以更改现代 Web 应用程序向用户呈现的各个方面。

CSS

```
:根{
    --侧边栏背景颜色: var (--gray-lightest) ;
    --rightbar-bg-color: var (--gray-lightest) ;
    -行高基准: 1.42857143;
    -链接颜色: var (--brand-primary-500) ;
    -link-hover-color: var (--brand-primary-800) ;
    -link-hover-decoration:下划线;
    -徽标高度: 32px;
    -徽标最大宽度: 200px;
    -header-bg: var (--gray-lightest) ;
    -header-fg: var(--gray-darker);
    -外部标头背景: var (--brand-tertiary-700) ;
    -外部标头-fg: #FFFFFF;
}
```

所使用的各种变量名称是不言自明的。不过，下表提供了简要说明。

针对一些变量的数字，参考图可定制的组件。

表 54. 索引.css 选项

| 参数 | 描述 |
|-------------------------|---------------------------------|
| --侧边栏背景颜色(5) | 更改列出电子邮件和联系人的窗格的背景颜色文件夹。 |
| --rightbar-背景颜色(6) | 更改右侧边栏的背景颜色。 |
| --line-height-base | 改变基线高度，改变所有地方的行高应用程序。 |
| --链接颜色 | 更改链接颜色。 |
| --link-hover-color | 更改链接颜色 鼠标悬停。 |
| --link-hover-decoration | 更改链接的行为方式（下划线、上划线或删除线） 鼠标悬停。 |
| --logo 高度 | 更改徽标高度。此值不能超过 72px。 |
| --logo 最大宽度 | 更改徽标的最大宽度。 |
| --header-bg (7) | 更改标题背景颜色。 |
| --header-fg | 更改标题的文本颜色。 |
| --外部标题-背景 | 更改导航栏的背景颜色。 |
| --外部标头-fg | 更改导航栏的文本颜色。 |



在 index.css 中而不是在 palette.css 中进行所有颜色自定义（覆盖），以避免调色板覆盖。

自定义 PWA

本部分可帮助您自定义渐进式 Web 应用 (PWA) 的某些方面。有关 PWA 的更多信息,请参阅什么是渐进式 Web 应用 (https://developer.mozilla.org/en-US/docs/Web/Progressive_web_apps/)。

Introduction#What_is_a_Progressive_Web_App)。

示例 manifest.json

```
{
  "图标": [
    {
      "源码": "/pwa/图标/图标_300x_300x300.svg",
      "尺寸": "300",
      "类型": "图像/svg+xml"
    },
    {
      "源码": "/pwa/图标/非-ios/图标_512x512.png",
      "尺寸": "512x512",
      "类型": "图片/png"
    },
    {
      "源码": "/pwa/图标/非-ios/图标_256x256.png",
      "尺寸": "256x256",
      "类型": "图片/png"
    },
    {
      "源码": "/pwa/图标/非-ios/图标_192x192_192x192.png",
      "尺寸": "192x192",
      "类型": "图片/png"
    },
    {
      "源码": "/pwa/图标/非-ios/图标_150x150_150x150.png",
      "尺寸": "150x150",
      "类型": "图片/png"
    },
    {
      "源码": "/pwa/图标/非-ios/图标_144x144.png",
      "尺寸": "144x144",
      "类型": "图片/png"
    },
    {
      "源码": "/pwa/图标/非-ios/图标_96x96.png",
      "尺寸": "96x96",
      "类型": "图片/png"
    },
    {
      "源码": "/pwa/图标/非-ios/图标_72x72.png",
      "尺寸": "72x72",
      "类型": "图片/png"
    },
    {
      "源码": "/pwa/图标/非-ios/图标_48x48.png",
      "尺寸": "48x48",
      "类型": "图片/png"
    },
    {
      "源码": "/pwa/图标/非-ios/图标_36x36.png",
      "尺寸": "36x36",
      "类型": "图片/png"
    },
    {
      "源码": "/pwa/图标/非-ios/图标_32x32.png",
      "尺寸": "32x32",
      "类型": "图片/png"
    }
  ]
}
```

```

    "src" : "/pwa/icons/non-ios/icon_16x16.png" , "sizes" :
    "16x16" , "type" :
    "image/png"
},{

    "src" : "/pwa/icons/ios/icon_180x180.png" , "sizes" :
    "180x180" , "type" :
    "image/png"
},{

    "src" : "/pwa/icons/ios/icon_114x114.png" , "sizes" :
    "114x114" ,
    "type" : "图像/png"
},{

    "src" : "/pwa/icons/ios/icon_72x72.png" , "sizes" :
    "72x72" , "type" :
    "image/png"
},{

    "src" : "/pwa/icons/ios/icon_57x57.png" , "sizes" :
    "57x57" , "type" :
    "image/png"
},{

    "src" : "/pwa/icons/ios/icon_32x32.png" , "sizes" :
    "32x32" , "type" :
    "image/png"
},{

    "src" : "/pwa/icons/ios/icon_16x16.png" , "sizes" :
    "16x16" ,
    "type" : "图像/png"
}
],{
    name : "示例邮件" ,
    short_name : "示例邮件" , orientation :
    portrait , display : standalone ,
    start_url : "/" ,
    background_color :
    "#ffffff" , theme_color : "#e92d28
}
}
```

1. 将示例 manifest.json 复制并粘贴到 mail.example.com/pwa/manifest.json 中。
2. 将 mail.example.com 的所有实例编辑为文件夹名称部分中决定的文件夹名称。
3. 编辑“name”和“short_name”，使其与示例 config.json 中的“title”具有相同的值。
 - “name”代表 Web 应用程序在移动应用程序列表中向用户显示的名称。
 - 如果没有足够的空间显示“name”，则“short_name”表示 Web 应用程序向用户显示的名称
4. 在 Palette.css 中将“background_color”设置为 background-color。
5. 将“theme_color”设置为与 Palette.css 中的主色相同的值。

不要改变“orientation”的值

，“display”和“start_url”。

自定义登录页面

本节帮助您更改 Zimbra Modern Web App 登录页面向用户显示的方式。

在开始登录（或ssh）Zimbra 服务器之前。

更改背景图像

1. 将背景图像复制到

/opt/zimbra/jetty_base/webapps/zimbra/img/

2. 打开并编辑

/opt/zimbra/jetty_base/webapps/zimbra/skins/_base/base3/skin.properties

3. 找到条目LoginScreen。

4. 将new-back-ground-image.png替换为您刚刚复制的图像的文件名。

更改徽标

现代 Web 应用程序使用的徽标来源于：

/opt/zimbra/jetty_base/webapps/zimbra/img/new-logo.png

您必须用您喜欢的徽标覆盖此文件。



为了保留恢复为默认徽标的规则,请重命名上述文件（在文件名中添加.old）。

1. 将您组织的徽标重命名为new-logo.png。

2. 将此文件复制到：

/opt/zimbra/jetty_base/webapps/zimbra/img/

部署说明

1. 导航到mail.example.com文件夹并打开。
2. 编辑config.json以更改版本。请勿使用以前使用过的值。
 - 输入一个唯一的正数。
 - 每次使用新值进行自定义以反映用户的现代 Web 应用程序。
 - 将文本括在引号中。
3. 保存文件。

所有mail.example.com实例都应替换为文件夹名称部分中确定的文件夹名称。

4. 将 mail.example.com 复制到 Zimbra 服务器上的 /opt/zimbra/jetty/webapps/zimbra/modern/clients/。

重启 Zimbra 邮箱服务器

要应用所做的更改，请重新启动 Zimbra 的邮箱服务器。

1. 以 root 身份登录到您的 Zimbra 安装。

2. 切换到用户 zimbra。

与 - zimbra

3. 重新启动 Zimbra 的邮箱服务器。

zmmailboxdctl 重启

4. 刷新 Zimbra 的 Modern Web App 登录页面以查看更改

如果没有出现更改，您可能需要清除缓存。

存储管理

存储管理 (SM) 功能可用于配置用于主要、次要数据存储和索引的存储卷。SM 支持以下提供商的本地和外部存储（Amazon S3、Ceph、EMC、Netapp StorageGrid、Scality、OpenIO）。SM 通过调度程序还能够根据计划时间的年限将旧数据从成本较高的主要存储移动到成本较低的次要存储。在大多数情况下，最终用户在访问存储在外部存储上的数据时不会遇到任何性能差异。

存储管理可以在全局和服务器级别的管理员 UI 中或通过命令行进行管理。

统一存储

从 Daffodil 10.0.5 Patch 开始，存储管理模块中添加了对统一存储的支持。

统一存储旨在通过将来自多个邮箱服务器的数据整合到单个 S3 存储桶中的同一目录结构下来简化数据管理。这种方法简化了存储、增强了可访问性并降低了操作复杂性。

如果符合以下条件，统一存储功能适合您：

1. 您的环境是多服务器环境，有超过 1 台邮箱服务器。
2. 您的组织有大量的数据存储和访问需求，可从集中式、可扩展的方法。

结构

在以下示例中，邮箱服务器 - Mailbox-1、Mailbox-2、Mailbox-3 在外部存储上使用相同的存储桶。用户 - d8bd3037-38d0-4c45-ade4-a6866f2912bd、91fee523-4841-400f-9dc9-0d1e41f4c61b 和 a8bd3037-4841-400f-ade4-bf1e41f4c61h 使用相同的目录结构，无论账户托管在哪个邮箱服务器上。

重击

```

|-- 邮箱-1
|-- 邮箱-2
|-- 邮箱-3
 \
|-- /存储桶名称/目标路径/前缀/
 \
|-- -d8bd3037-38d0-4c45-ade4-a6866f2912bd
 \
|-- D3S78JHDD8BD303738D04C45ADE4A6866F2912BD000001BD
|-- AD87H7YD8BD303738D04C45ADE4A6866F2912BD000001BD |-
91fee523-4841-400f-9dc9-0d1e41f4c61b
 \
|-- 5D5D494CD8BD303738D04C45ADE4A6866F2912BD000001BD
|-- 2BF41B87D8BD303738D04C45ADE4A6866F2912BD000001BD
|-- 1CC67854D8BD303738D04C45ADE4A6866F2912BD000001BD
|-- 90AA2503D8BD303738D04C45ADE4A6866F2912BD000001BD
|-- 73AC6101D8BD303738D04C45ADE4A6866F2912BD000001BD
|-- a8bd3037-4841-400f-ade4-bf1e41f4c61h
 \
|-- F3545DA7D8BD303738D04C45ADE4A6866F2912BD000001BD
|-- DB88EE7BD8BD303738D04C45ADE4A6866F2912BD000001BD
|-- 4CC67854D8BD303738D04C45ADE4A6866F2912BD000001BD
|-- 2D5D494CD8BD303738D04C45ADE4A6866F2912BD000001BD
|-- 1D5D494CD8BD303738D04C45ADE4A6866F2912BD000001BD
|-- 3CC67854D8BD303738D04C45ADE4A6866F2912BD000001BD

```

使用统一存储的优势

以下是使用统一存储的一些优点：

- 邮箱移动**:由于多个邮箱服务器的数据都存储在单个 S3 存储桶下,因此可以更轻松地将用户的邮箱从一台服务器移动到另一台服务器,而无需移动存储在 S3 中的数据。
- 简化数据管理**:统一存储消除了管理邮箱服务器多个存储位置的需要。所有数据都整合到单个 S3 存储桶中,更易于管理和维护。
- 可扩展性**:统一的方法可以随着组织的发展更轻松地进行扩展,从而降低数据扩展的复杂性。

使用统一存储的局限性

- 仅支持 S3 提供商**:统一存储仅在 S3 提供商上受支持。
- 消息重复**:当数据移动到外部 S3 时,消息重复会丢失并且不受支持。

如何设置统一存储

可以通过管理员 UI 或 CLI 创建基于统一存储的卷。

为了优化该功能的利用率,在使用 S3 创建外部卷时,必须确保在所有邮箱服务器上一致设置相同的卷路径 (相同的 volumePrefix)。

管理员界面

通过主页→配置→服务器→存储管理→管理卷→添加创建卷时,选择统一存储复选框,这将启用统一存储功能。

有关通过管理员 UI 创建卷的详细步骤,请参阅外部存储类型部分。

[命令行界面](#)

可以将选项`--unified`或`-un`与`zmvolume`命令一起使用来启用统一存储功能。

有关通过 CLI 创建 S3 卷的详细步骤,请参阅S3 的外部卷部分

卷管理

在服务器的存储管理页面上,您可以管理每个 Zimbra 邮箱服务器上的存储卷:

主页→配置→服务器→存储管理

[重击](#)

安装 Zimbra Collaboration Server 时,每个邮箱服务器上都会配置一个索引卷和一个消息卷。

- 索引卷是 `/opt/zimbra/index`
- 消息卷是`/opt/zimbra/store`

在存储管理位置中,您可以添加新卷、设置卷类型并设置压缩阈值。

指数成交量

每个 Zimbra 邮箱服务器都配置有一个当前索引卷。每个邮箱都分配到当前索引卷上的永久目录。创建帐户时,会自动为该帐户定义当前索引卷。您无法更改分配给帐户的索引卷。

当卷已满时,您可以为新帐户创建新的当前索引卷。您可以添加新卷、设置卷类型并设置压缩阈值。

未标记为当前的索引卷仍被分配给它们的帐户使用。任何被邮箱引用为其索引卷的索引卷都无法被删除。

留言量

当有新消息被发送或创建时,该消息将保存在当前消息卷中。可以创建消息卷,但只能将一个卷配置为存储新消息的当前卷。当卷已满时,您可以配置新的当前消息卷。当前消息卷接收所有新消息。新消息永远不会存储在之前的卷中。

无法删除当前卷,也无法删除包含引用该卷的消息的消息卷。

管理控制台 :存储管理页面

存储管理页面包含五个部分:

- 管理卷部分显示所有配置,并允许管理员创建、编辑和删除卷。
 - 卷名是分配给每个卷的名称。初始卷名为 `index1` 和 `message1`。
 - 卷根路径是文件系统中存储卷数据的位置。

- 卷类型定义创建卷时设置的卷类型。可设置为索引、主卷或辅助卷，一旦设置，则不可更改。
- 压缩 Blob 选中此框后，大小超过压缩阈值的消息 Blob 将被压缩。如果启用 Blob 压缩，则使用的磁盘空间会减少。注意：启用 Blob 压缩也会增加服务器的内存需求。
- 压缩阈值。大于该阈值的消息将被压缩。默认阈值为 4096 字节。
- 分配当前卷部分是您设置哪个卷当前将用于主要消息、次要消息或索引卷的位置。
 - 当前主消息卷当前主卷名称。新消息保存在此当前消息卷中。
 - 当前辅助消息卷当前辅助消息卷名称。较旧的数据存储在辅助消息卷中。
 - 当前索引卷。当前索引卷名称。当卷已满时，您可以为新账户创建新的当前索引卷
- 存储管理政策部分：
 - SM 会话计划使管理员能够启用和安排 SM 策略每天发生的时间。
 - 管理 SM 会话使管理员能够手动执行存储管理策略。
- 要移动的项目部分定义了用于管理数据从主存储迁移到辅助存储时的 SM 策略。SM 策略可以在全局或每个邮箱服务器上设置。
 - 要移动的项目类型。您可以选择要从主卷移动到当前辅助卷的消息、任务、约会、联系人和公文包项目。

如果您使用外部存储提供商作为辅助存储，请排除 [政策文件在移至外部存储后出现乱码](#)。

- 移动超过以下时间的项目。默认全局 SM 策略是将超过 30 天的邮件和文件移动到辅助卷。要移动的项目的时间可以用天数、月数、周数、小时数或分钟数来指定。
- 策略字符串。您可以使用搜索查询语言来设置其他 SM 策略。例如，如果您希望所有标记为垃圾邮件的邮件都包含在移动到当前辅助卷的邮件中，则可以将以下内容添加到策略中： message:in:junk before:-[x] days。

卷的类型

Zimbra 提供两种类型的卷，可以配置和链接用于数据存储。

1. 内部

2. 外部

内部存储类型

内部存储类型是位于 zimbra 服务器上的存储。

要添加内部存储卷，请按照以下步骤操作：

1. 进入主页→配置→服务器→存储管理
2. 滚动到管理卷,然后单击添加按钮。
3. 选择卷为内部。单击下一步。
4. 选择适当的卷类型,即主卷、辅助卷或索引卷。
5. 输入卷名称和卷根路径。
6. 如果要压缩 Blob,请选中“压缩 Blob”并设置“压缩阈值”。
7. 使用自定义商店经理是可选字段。如果您想使用默认的,请不要单击启用复选框 zimbra 商店经理。
8. 压缩 Blob:选中此框时,大小超过压缩阈值的消息 Blob 将已压缩。如果启用了 blob 压缩,则使用的磁盘空间会减少。

转向 在 blob 压缩将增加服务器的内存要求。

9. 压缩阈值:超过定义阈值的消息将被压缩。默认阈值为 4096 字节。

10. 单击“完成”。

外部存储类型

外部存储类型是可在本地访问但由邮箱服务器外部托管的存储。

目前 Zimbra 支持以下提供商:

1. 亚马逊S3。
2. 头孢。
3. 自定义 S3 创建任何不受支持的外部存储的选项。
4. 电磁兼容。
5. NetApp 存储网格。
6. 开放IO。
7. 可扩展性。

[亚马逊S3](#)

以下是添加 Amazon S3 存储的步骤:

1. 转到主页→配置→服务器。
2. 选择服务器,右键单击并选择编辑。
3. 转到存储管理→管理卷页面,然后单击添加按钮。
4. 选择提供商Amazon S3。单击下一步。
5. 选择卷类型。即主卷或次卷。

不支持外部存储上的索引卷。

6. 输入卷名称、卷前缀。
7. 添加与 S3 兼容的存储桶。单击“创建新存储桶”。

a. 输入Bucket 名称、访问密钥、Secret、目标路径和 URL

使用访问密钥 ID 和密钥访问 AWS 服务。这些可通过 AWS 管理控制台获取。

b. 选择适当的区域并单击下一步。

必须正确填写上述所有字段才能验证存储桶。在正确输入所有凭据之前，“下一步”按钮将被禁用。单击“下一步”按钮后，将验证存储桶凭据。如果凭据出现任何错误，将显示错误。

c. 验证成功后，将创建存储桶。

8. 从S3 兼容存储桶下拉菜单中选择已创建的存储桶。

9. 使用自定义商店经理是可选字段。如果您想使用默认的，请不要单击启用复选框 zimbra 商店经理。

10. 选中复选框以启用“不频繁访问”。输入不频繁访问的阈值。您也可以选择可以选中复选框来启用智能分层。

不频繁访问： S3 Standard-IA 适用于访问频率不高但在需要时需要快速访问的数据。

不频繁访问阈值：此阈值用于设置任何大于此存储类的不频繁访问阈值的文件。

智能分层：这将在卷的所有文件上设置适当的智能分层标志。

[有关不频繁访问的官方 Amazon S3 文档](#)

(https://aws.amazon.com/s3/storage-classes/#Infrequent_access) 和智能分层 (https://aws.amazon.com/s3/storage-classes/#Unknown_or_changing_access/)。

要在此卷上启用统一存储支持，请选中统一存储复选框。

11. 单击完成以添加Amazon S3存储类型。

笔记：

头孢

以下是添加 Ceph 存储的步骤：

1. 转到主页→配置→服务器。

2. 选择服务器，右键单击并选择编辑。

3. 转到存储管理→管理卷页面，然后单击添加按钮。

4. 选择提供商Ceph。单击下一步。

5. 选择卷类型。即主卷或次卷

6. 输入卷名称、卷前缀。

7. 添加与 S3 兼容的存储桶。单击“创建新存储桶”。

a. 输入Bucket 名称、访问密钥、Secret、目标路径和 URL

b. 单击“下一步”。

- c. 验证成功后,将创建存储桶。
- 8. 从S3 兼容存储桶下拉菜单中选择已创建的存储桶。
- 9. 使用自定义商店经理是可选字段。如果您想使用默认的,请不要单击启用复选框 zimbra 商店经理。

要在此卷上启用统一存储支持,请选中统一存储复选框。

10.单击完成添加Ceph存储。

[定制 S3](#)

以下是添加自定义 S3 存储的步骤：

1. 转到主页→配置→服务器。
2. 选择服务器,右键单击并选择编辑。
3. 转到存储管理→管理卷页面,然后单击添加按钮。
4. 选择提供商Custom S3。单击下一步。
5. 选择卷类型。即主卷或次卷
6. 输入卷名称、卷前缀。
7. 添加与 S3 兼容的存储桶。单击“创建新存储桶”。
 - a. 输入Bucket 名称、访问密钥、Secret、目标路径和 URL
 - b.单击“下一步”。
 - c. 验证成功后,将创建存储桶。
8. 从S3 兼容存储桶下拉菜单中选择已创建的存储桶。
9. 使用自定义商店经理是可选字段。如果您想使用默认的,请不要单击启用复选框 zimbra 商店经理。

要在此卷上启用统一存储支持,请选中统一存储复选框。

10.单击完成以添加自定义 S3存储。

[电磁兼容 \(EMC\)](#)

以下是添加 EMC 存储的步骤：

1. 转到主页→配置→服务器。
2. 选择服务器,右键单击并选择编辑。
3. 转到存储管理→管理卷页面,然后单击添加按钮。
4. 选择提供商EMC。单击“下一步”。
5. 选择卷类型。即主卷或次卷
6. 输入卷名称、卷前缀。
7. 添加与 S3 兼容的存储桶。单击“创建新存储桶”。
 - a. 输入Bucket 名称、访问密钥、Secret、目标路径和 URL
 - b.单击“下一步”。

- c. 验证成功后,将创建存储桶。
8. 从S3 兼容存储桶下拉菜单中选择已创建的存储桶。
9. 使用自定义商店经理是可选字段。如果您想使用默认的,请不要单击启用复选框 zimbra 商店经理。

要在此卷上启用统一存储支持,请选中统一存储复选框。

10. 单击“完成”添加EMC存储。

NetApp 存储网格

以下是添加 NetApp StorageGrid 的步骤:

1. 转到主页→配置→服务器。
2. 选择服务器,右键单击并选择编辑。
3. 转到存储管理→管理卷页面,然后单击添加按钮。
4. 选择提供商NetApp StorageGrid。单击“下一步”。
5. 选择卷类型。即主卷或次卷
6. 输入卷名称、卷前缀。
7. 添加与 S3 兼容的存储桶。单击“创建新存储桶”。
 - a. 输入Bucket 名称、访问密钥、Secret、目标路径和 URL
 - b. 单击“下一步”。
 - c. 验证成功后,将创建存储桶。
8. 从S3 兼容存储桶下拉菜单中选择已创建的存储桶。
9. 使用自定义商店经理是可选字段。如果您想使用默认的,请不要单击启用复选框 zimbra 商店经理。

要在此卷上启用统一存储支持,请选中统一存储复选框。

10. 单击“完成”以添加NetApp StorageGrid存储。

开放IO

OpenIO 提供程序不支持统一存储。

以下是添加 OpenIO 存储的步骤:

1. 转到主页→配置→服务器。
2. 选择服务器,右键单击并选择编辑。
3. 转到存储管理→管理卷页面,然后单击添加按钮。
4. 选择“卷类型”为“OpenIO”。单击“下一步”。
5. 选择卷类型。即主卷或次卷
6. 输入卷名称、URL、帐户、命名空间、代理端口和帐户端口。

7. 使用自定义商店经理是可选字段。如果您想使用默认的,请不要单击启用复选框 zimbra 商店经理。

8. 单击完成以添加OpenIO存储。

规模

以下是添加 Scality 存储的步骤：

1. 转到主页→配置→服务器。
2. 选择服务器,右键单击并选择编辑。
3. 转到存储管理→管理卷页面,然后单击添加按钮。
4. 选择提供商Scality。单击“下一步”。
5. 选择卷类型。即主卷或次卷
6. 输入卷名称、卷前缀。
7. 添加与 S3 兼容的存储桶。单击“创建新存储桶”。
 - a. 输入Bucket 名称、访问密钥、Secret、目标路径和 URL
 - b. 单击“下一步”。
 - c. 验证成功后,将创建存储桶。
8. 从S3 兼容存储桶下拉菜单中选择已创建的存储桶。

9. 使用自定义商店经理是可选字段。如果您想使用默认的,请不要单击启用复选框 zimbra 商店经理。

要在此卷上启用统一存储支持,请选中统一存储复选框。

10. 单击“完成”添加Scality存储。

如何将卷分配为辅助卷

在分配 SM 卷之前,该卷必须存在。请参阅向服务器添加新存储卷以了解添加卷的概述。创建卷后,请按照以下步骤操作:

1. 进入主页→配置→服务器→存储管理
2. 滚动至分配当前卷部分
3. 单击当前次要消息量的下拉列表并选择适当的量。
4. 单击保存。
5. 所选卷现已配置为辅助消息卷。

将新卷设置为辅助消息卷后,消息将根据 SM 策略移动到辅助存储卷。

向服务器添加新的存储卷

每个 Zimbra 邮箱服务器都配置有一个主消息卷和一个索引卷。有关更多详细信息,请参阅卷管理部分。此外,Zimbra 数据存储配置允许创建新的主存储、辅助存储和索引存储。

要访问音量页面,请按照以下步骤操作。