

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。

1. 进入主页→配置→服务器→存储管理
2. 默认情况下,配置索引和主数据卷。

## 存储管理策略

存储管理策略是将旧数据移动到辅助存储设备的过程。要管理您的电子邮件存储资源,您可以实施 SM 策略,定义要移动哪些项目以及应在什么时间移动它们。根据邮件的年龄,邮件和附件会从主卷移动到当前的辅助卷。邮件仍然可以访问。用户不会察觉任何变化,打开已移动的旧项目时也不会看到任何明显的差异。

您可以全局或在服务器级别实施 SM 策略。

主页→配置→全局设置→存储管理  
主页→配置→服务器→存储管理

重击

在单个服务器中配置的策略将覆盖全局策略。

默认的全局 SM 策略会将消息和公文包文件 (自收到之日起超过 30 天) 移动到辅助卷。此外,您还可以手动移动任务、约会、联系人和便笺。

您可以将 30 天期限策略更改为特定月份、星期、小时或分钟期限。

## 设置或编辑 SM 策略

在全局或服务器级别的存储管理窗口中,滚动到要移动的项目,然后通过以下方式编辑或创建新规则:

1. 选择现有规则,然后单击“编辑”或“添加”。
2. 选择或修改您想要分配的策略。
3. 点击保存

以下是创建或编辑策略规则时可以配置的规则。

选项	描述
要搬运的物品类型	默认移动邮件公文包文件,但您可以选择其他项目
选项	如果您想要将项目包含在垃圾邮件和废纸文件夹中,请选中此框。
移动早于	选择时间范围来移动较旧的项目。
策略字符串	这显示您已配置的策略字符串。

## 删除现有策略

删除现有策略将从 SM 会话的未来运行中删除该规则。

1. 要删除现有策略,请选择要删除的策略。
2. 单击删除按钮。

3. 选择“是”。

如果意外删除了规则，则重新创建规则将应用于定义配置中的所有数据

下一个 SM 会话。如果手动启动 SM 会话，请注意服务器和 IO 负载可能会更高。

## 存储管理 CLI 实用程序

### 使用zms3config CLI管理全局 S3 配置

zms3config是用于管理可在邮件存储节点之间共享的全局 S3 存储桶的 CLI 实用程序。

可以从任何节点创建存储桶配置，并且可在所有节点之间使用。

可以从管理控制台主页→配置→  
全局设置→存储管理。

以下是 S3 全局配置的一些重要方面：

- 存储桶名称在提供商内应该是唯一的。
- 同一个 bucket 可以用于多个卷，只需遵循不同的路径（检查卷前缀选项为每个卷使用.zmvolume命令。）
- 支持以下提供商：Amazon AWS、Ceph、Custom S3、EMC、NetApp-StorageGrid、OpenIO 和规模

### 句法：

`zms3config {-a | -d | -l | -h} <选项>`

重击

### 选项

运营	长名称	简称	描述
显示帮助	- 帮助	-h	显示帮助
添加新的 S3 配置	- 添加	-a	创建新的 S3 存储桶并提供更多选择。
	--storeProvider	-t	要添加的商店提供商 s3BucketConfig，有效值为：AWS_S3，CEPH_S3、CUSTOM_S3、EMC_S3，存储网格S3，规模:S3。
	--存储桶名称	-bn	存储桶的名称
	--访问密钥	-k	访问密钥
	--秘密密钥	-sk	密钥
	--目标路径	-dp	目标路径，根 S3 存储桶中的路径存储体积数据。

运营	长名称	简称	描述
	- 地区	-r	S3 存储桶区域
	--url	-url	S3 的端点 URL 桶
删除 S3 存储桶	- 删除	-d	删除 S3 存储桶
	--存储桶ID	-出价	bucket 的 ID,即 用于删除 S3 桶。
列表桶	- 列表	-l	列出所有存储桶

## 添加 S3 配置

- 要创建具有长选项名称的 AWS 存储桶配置,请使用以下命令:

```
zms3config --add --storeProvider AWS_S3 --bucketName <bucket_name> --accessKey <secret_key> -  
-destPath <目标路径> -region <有效aws区域> --url <aws有效端点url>
```

重击

- 要使用短选项名称创建 Ceph 存储桶配置,请使用以下命令:

```
zms3config -a -t CEPH_S3 -bn <存储桶名称> -ak <密钥> -dp <目标路径> --url  
<有效端点网址>
```

重击

- 要使用短选项名称创建自定义 S3 存储桶配置,请使用以下命令:

```
zms3config -a -t CUSTOM_S3 -bn <存储桶名称> -ak <密钥> -dp <目标路径> --url  
<有效端点网址>
```

重击

- 要创建具有短选项名称的 EMC 存储区配置,请使用以下命令:

```
zms3config -a -t EMC_S3 -bn <存储桶名称> -ak <密钥> -dp <目标路径> --url  
<有效端点网址>
```

重击

- 要创建具有短选项名称的 StorageGrid 存储桶配置,请使用以下命令:

```
zms3config -a -t STORAGE_GRID_S3 -bn <存储桶名称> -ak <密钥> -dp <目标路径> --  
url <有效端点网址>
```

重击

- 要创建具有短选项名称的 Scality 存储桶配置,请使用以下命令:

```
zms3config -a -t SCALITY_S3 -bn <存储桶名称> -ak <密钥> -dp <目标路径> --url  
<有效端点网址>
```

重击

## 列出 S3 存储桶配置

列出设置中配置的所有 S3 存储桶。

```
zms3config-l
```

重击

## 删除 S3 配置

执行此操作时要小心,因为存储桶是在全局级别使用的,并且可以在节点间的多个卷中引用。

`zms3config -d -bid <存储桶唯一 ID>`

重击

## 使用zmvolume CLI 管理内部和外部卷

zmvolume命令用于创建、编辑和删除存储卷。它支持创建内部和外部卷。内部卷是默认存储,位于服务器目录中,而外部卷使用外部存储提供商提供的 S3 存储桶/OpenIO 设置。

### 句法:

`zmvolume {-a|-d|-l|-e|-dc|-sc} [选项]`

重击

### 描述

手术	长名称	简称	描述
添加新卷	- 添加	一个	添加卷。
	- 帐户	-acc	<arg> 账户名称 对于 OpenIO 卷。
	--帐户端口	-ap	<arg> 帐户端口 OpenIO 卷。它应该 是一个数值。
	--存储桶ID	-出价	<arg> S3 存储桶 ID。注意 桶应该是 <b>在全球范围内创建</b> 使用获取 zms3config。
	- 压缩	-C	<arg> 压缩 BLOB 值是 true 或 false。默认值为 错误的。
	--压缩阈值	-ct	<arg> 压缩 阈值。默认 值为4KB。
	- 姓名	-n	<arg> 卷名称。它 仅可包含 字母数字字符, _ (下划线)、- (连字符)和 . (句号) 但可以从开始开始 以字母或数字表示。

手术	长名称	简称	描述
	--名称空间	-ns	<arg> 命名空间 OpenIO 卷。
	- 小路	-p	<arg> 根路径。
	--代理端口	-页	<arg> 代理端口 开放IO 卷http://port.it[.] 它 应该是数字 价值。
	--存储类型	-stp	<arg> 商店名称 提供商 (S3,开放)
	--商店类型	-英石	<arg> 存储类型 :内部 或外部
	--storeManager类	SMC	<arg> 可选 要指定的参数 非默认商店 经理 classpath.仅可用 对于 S3 提供商。
	- 类型	-t	<arg> 卷类型 (主要信息, secondaryMessage,或 指数)
	--url	-url	<arg> 端点 URL OpenIO 卷。
	--使用智能分层	-出去	<arg> 使用智能 仅限分层存储类 适用于 AWS。默认 值为假。
	--useInFrequentAccess	- 粉末	<arg> 不经常使用 仅访问存储类 适用于 AWS。
	-- useInFrequentAccThreshold	- 胖的	<arg> 不经常使用 访问存储类 blob 尺寸阈值。 默认值为64KB。

手术	长名称	简称	描述
	--volumePrefix	副总裁	<arg> 卷前缀。它必须以“/”开头并且不能包含其他特殊字符除外“-”和“/”。
	- 统一	-和	<arg> 参数启用统一存储支持音量。如果未指定，默认值为假。
删除卷	- 删除	-d	删除卷。提供卷 ID。
	- ID	-ID	<arg> 卷 ID。
显示当前音量--displayCurrent		-直流	显示当前体积。
编辑卷	- 编辑	-和	编辑卷 wrt 提供的卷 ID (-id)。列出的任何选项在“-a”下也可以指定其值针对卷类型进行了修改内部。请注意，只有卷名称可以是编辑为外部卷。
帮助选项	- 帮助	-h	显示此的使用选项工具。
列表卷	- 列表	-l	列出所有卷。
	- 服务器	-S	<arg> 邮件服务器主机名。默认值为本地主机。
将音量设置为当前体积	--设置当前	-SC	设置当前音量。
关闭辅助体积	--turnOffSecondary	-ts	关闭当前次要信息体积。

[添加新卷](#)[内容积](#)

要创建内部卷,必需的参数是-n、-t和-p,可选参数是-c、-ct和  
-英石。

```
zmvolume -a -n <卷名称> -t <存储类型> -p <卷路径>
```

重击

## OpenIO 的外部卷

要创建主或辅助 OpenIO 卷,请执行以下命令:

```
zmvolume -a -n <卷名称> -t <存储类型> -vp <卷前缀> -st external -stp OPENIO -pp <代理端口> -ap <帐户端口> -url <URL> -acc <帐户名称> -ns <名称空间>
```

重击

## S3 的外部音量

要创建主或辅助 S3 (Amazon S3、NetApp StorageGrid、Ceph)卷,请执行以下命令:

```
zmvolume -a -n <卷名称> -t <存储类型> -vp <卷前缀> -st external -stp S3 -bid <存储桶ID>
```

重击

要创建具有统一存储支持的主或辅助 S3 (Amazon S3、NetApp StorageGrid、Ceph)卷,请执行以下命令:

```
zmvolume -a -n <卷名称> -t <存储类型> -vp <卷前缀> -st external -stp S3 -bid <存储桶ID> -un true
```

重击

## 编辑卷

### 内容积

管理员可以编辑创建时使用的内部卷的所有参数:

```
zmvolume -e -id <卷ID> -n <卷名称> -p <卷路径> -t <类型> -c <压缩> -ct <压缩阈值>
```

重击

## 外部音量

仅可以编辑外部卷的名称:

```
zmvolume -e -id <卷 ID> -n <卷名称>
```

重击

## 列表卷

列出所有创建的卷:

```
zm卷-l
```

重击

## 删除卷

删除卷时请务必小心,否则可能会导致数据丢失:

```
zmvolume -d -id <卷 ID>
```

重击

## 设置当前音量

将卷 ID 设置为当前卷,按照配置的卷类型使用:

`zmvolume -sc -id <卷Id>`

重击

## 显示当前音量:

显示设置为当前的主卷和辅助卷详细信息:

`zmvolume-dc`

重击

## 关闭辅助

要禁用辅助卷:

`音量-ts`

重击

## 帮助部分

要显示帮助部分:

`zmvolume-h`

重击

## 使用zmschedulesmpolicy CLI管理策略的调度

`zmschedulesmpolicy`命令用于安排存储管理策略的执行。要跟踪 SM 会话的进度,请使用`zmhsms -u`命令。

- 调度程序支持单个 SM 会话,该会话可包含一个或多个策略。如果调度了新的 SM 会话,它将覆盖现有会话 (如果存在)。
- 计划的 SM 策略会在预定的时间每天执行一次,并且每天都会执行,直到被删除。
- 安排会话的时间格式为 24 小时制。安排 SM 会话时不能指定分钟。
- 即使管理员没有定义任何策略,在手动启动 SM 会话时也会执行默认全局策略,即消息、document:before:-30days。

## 句法

`zmschedulesmpolicy [-l|-h|-f|-e { <小时:00> }]`

重击

## 选项

运营	长名称	简称	描述
帮助	- 帮助	-h	获取有关 <code>zmschedulesmpolicy</code> (默 认命令)的帮助。
列出时间表	- 列表	-l	打印现有的预定 SM 策略。

运营	长名称	简称	描述
清除/取消计划	--刷新	-f	移除当前时间表 (取消所有预定的 SM政策执行)
添加/编辑时间表	- 编辑	-和	编辑当前计划 时间。如果没有 现有的预定策略,那么它将安排 新的 SM 政策 时间。

## 帮助 - zm schedulesmpolicy

打印帮助页面：

```
zm schedulesmpolicy --help  
zm schedulesmpolicy -h
```

重击

## 列表 - 打印当前计划的 SM 策略

列出计划的 SM 策略执行。如果没有关于计划的 SM 策略的输出,则表示当前没有计划 SM 策略。

```
zm schedulesmpolicy --列表  
zm schedulesmpolicy -l
```

重击

## 清除/取消-删除当前安排的 SM 策略

如果可用,则取消当前安排的 SM 策略。

```
zm schedulesmpolicy --刷新  
zm schedulesmpolicy -f
```

重击

## 添加/编辑 - 在指定时间安排 SM 策略

它接受 24 小时格式的时间作为参数,这是安排 SM 策略的时间。

如果没有计划的策略执行,则此选项将安排新的 SM 策略或编辑现有计划。

```
zm schedulesmpolicy --编辑 15:00  
zm schedulesmpolicy -e 15:00
```

重击

## 使用zmhsm CLI管理 SM 会话

zmhsm命令用于启动、停止、中止和查看 SM 会话的状态。SM 会话在为特定服务器创建的 SM 策略上执行,并开始将 blob 从主卷移动到当前辅助卷。

## 句法

zmhsms {中止|启动|状态} {服务器} &lt;服务器名称&gt;

重击

## 描述

长名称	简称	描述
--中止	-一个	中止当前 SM 会话但 不是立即完成的。首先,它完成 正在进行的邮箱并停止 处理该诉讼 邮箱,然后中止 当前 SM 会话。已处理的 邮箱将不会被回滚。
- 帮助	-h	显示使用帮助 zmhsms 的选项。
- 服务器	-s	<arg> 邮件服务器主机名。 默认情况下是 localhost [args]。
- 开始	-t	启动 SM 进程。
- 地位	-在	SM会话的状态为 显示。

例子：

- 启动 SM 会话

要启动 SM 会话,请执行以下命令：

zmhsms-t-s 本地主机

重击

- 中止 SM 会话

要启动 SM 中止序列,请执行以下命令：

zmhsms-a-s 本地主机

重击

- SM 会话状态

要查看 SM 状态,请执行以下命令：

zmhsms -u -s 本地主机

重击

它仅显示最后一个 SM 会话状态。以下是一些示例：

示例 1:

开始时间:2022 年 9 月 8 日星期四 01:57:04 EDT

结束时间:2022 年 9 月 8 日星期四 01:57:04 EDT

查询:之前: -1分钟

目前未运行。

已将 1 个 blob 移动到卷 12。

已处理邮箱:7 个 (共 7 个)。

示例 2:

上次 SM 会话统计信息

开始时间:2022 年 8 月 16 日星期二 07:32:16 EDT

查询:before:-1minute 是:任何地方

目前正在运行。

已将 0 个 blob 移动到卷 3。

已处理邮箱:0 个 (共 61 个)。

## 管理存储管理策略

存储管理 (SM) 策略是一组规则,当触发zmhsm命令时,这些规则将用于定义哪些项目将从主存储移动到辅助存储 (无论是手动还是通过调度zmchandlesmpolicy)。

SM 策略可以在全局和服务器级别进行配置,因为它存储在全局和服务器 LDAP 属性zimbraHSMPolicy 中。

### 在全球级别配置 (默认策略)

向属性添加多个策略时,在zimbraHSMPolicy属性中使用+前缀。

zmprov mcf +zimbraHSMPolicy ‘消息:之前: -1天,在:垃圾箱中’ zmprov mcf +zimbraHSMPolicy ‘消息,文档:之前: -5天,在:任何地方,有:附件,大于:5m,在:已读’

重击

当需要多个值时,也可以在单个配置命令中多次指定该属性。

zmprov mcf zimbraHSMPolicy 消息:之前: -129600分钟 zimbraHSMPolicy 文档,wiki:之前: -10080分钟

重击

在单个配置命令中指定单个属性值将在运行命令之前清除该值的其他实例。在设置值之前,请务必检索当前配置以查看存在哪些值。

```
zmprov gcf zimbraHSMPolicy
```

重击

## 服务器级别策略

类似的格式也可以用来在服务器级别设置策略。

```
zmprov ms `zmhostname` zimbraHSMPolicy 消息:之前: -129600分钟 zmprov gs `zmhostname`  
zimbraHSMPolicy
```

重击

## 自定义存储管理器

### 概述

Zimbra StoreManager SDK 用于将 Zimbra 连接到存储管理功能中不可用的外部数据存储。默认情况下,Zimbra 使用 StoreManager 实现将文件写入本地磁盘。

使用此 SDK 可以将文件写入云数据存储提供商、远程数据库或任何其他存储技术。

源代码示例仅供说明之用。它们不适用于直接在生产环境中使用。

代码示例已精简,以便于阅读。导入、包声明和其他与 StoreManager 扩展不直接相关的细节已被省略。完整代码可在 Zimbra 源代码管理中找到。

### 配置

#### zimbra\_class\_store

zimbra\_class\_store zmlocalconfig 选项配置用于 StoreManager 的类。默认的 StoreManager 类是基于标准文件系统的 blob 存储:

默认:

```
zimbra_class_store = com.zimbra.cs.store.file.FileBlobStore
```

重击

可以用自定义类替换此类,以将消息 blob 写入所选的 Store Manager。

例子:

```
zmlocalconfig -e zimbra_class_store=com.zimbra.examples.extns.storemanager.MyStoreManager
```

重击

#### zmlocalconfig 选项

```
external_store_delete_max_ioexceptions = 25  
external_store_local_cache_max_bytes = 1073741824  
external_store_local_cache_max_files = 10000  
external_store_local_cache_min_lifetime = 60000
```

重击

### 配置示例

1. 将zimbra-extns-storemanager.jar复制到/opt/zimbra/lib/ext/storemanager目录

2. 执行：

```
zmlocalconfig-
e zimbra_class_store=com.zimbra.examples.extns.storemanager.ExampleStoreManager
```

重击

3. 重启服务器

4. 执行任何写入操作,如发送邮件、上传文件等。Blob 应该写入

```
/tmp/examplestore/blobs
```

## 基本集成

集成的最少代码需要重写 ExternalStoreManager 并实现 ExternalBlobIO。

该接口包含写入数据,读取数据,删除数据的方法。

```
/*
 * 最简单的 blob 存储集成接口
 * 实现者必须提供读取、写入和删除 blob 的功能
 */
公共接口 ExternalBlobIO {
    /**
     * 将数据写入 blob 存储
     * @param in:包含要写入的数据的InputStream
     * @param actualSize:流中的数据大小,如果大小未知则为 -1。由
    尽可能进行优化的实施者
     * @param mbox:包含 blob 的邮箱。存储可以选择使用它来
    分割
     * @return 存储 blob 的定位器字符串,由存储协议创建的唯一标识符
     * @throws IOException
     * @throws 服务异常
    */
    String writeStreamToStore(InputStream in, long actualSize, Mailbox mbox) 抛出 IOException,
    服务异常;

    /**
     * 创建一个输入流以从 Blob 存储中读取数据
     * @param locator:写入操作返回的 blob 标识符字符串
     * @param mbox:包含 blob 的邮箱。存储可以选择使用它来
    分割
     * @return 包含数据的 InputStream
     * @throws IOException
    */
    InputStream readStreamFromStore(String locator,Mailbox mbox) 抛出 IOException;

    /**
     * 从存储中删除一个 blob
     * @param locator:blob 的标识符字符串
     * @param mbox:包含 blob 的邮箱。存储可以选择使用它来
    分割
     * @return true 表示成功,false 表示失败
     * @throws IOException
    */
    boolean deleteFromStore(String locator, Mailbox mbox) 抛出 IOException;
}
```

以下是一个极简 StoreManager 实现的示例,它使用 java.io.File 和相关类写入本地磁盘。为简洁起见,省略了 getNewFile() 的细节,通常涉及在预定义目录中创建一个新的空文件。

此类还重写了 ExternalStoreManager 中的三个方法

- `startup()` - 在初始化期间调用,可用于设置商店实现所需的任何路径、后台线程或其他资源。必须调用 `super.startup()` 来初始化父资源
- `shutdown()` - 在应用程序关闭期间调用,可用于清理任何临时资源并终止后台线程。必须调用 `super.shutdown()` 来清理父资源
- `isCentralized()` - 用于多服务器配置的布尔值。如果为 `true`,则存储是全局的,并且一个 Zimbra 服务器的定位器可以从另一个 Zimbra 服务器访问,否则定位器仅在创建它们的服务器内有效。集中式存储的示例是云文件存储系统,非集中式存储的示例是本地文件系统

```

公共类 SimpleStoreManager 扩展了 ExternalStoreManager {

    @Override
    public void startup() 抛出 IOException、ServiceException {
        super.startup(); //初始化
        任何本地资源,如存储目录
    }

    @Override
    public void shutdown()
    { super.shutdown(); //清理
    所有资源和后台线程
    }

    @Override
    protected boolean isCentralized() { //此存储写入本地磁盘,
        因此无法从其他 Zimbra 服务器访问 blob return false;

    }

    私有文件 getNewFile(Mailbox mbox) 抛出 IOException {
        //在磁盘上生成一个新文件
    }

    @Override
    public String writeStreamToStore(InputStream in, long actualSize, Mailbox mbox) 抛出
    IO异常 {
        文件目标文件 = getNewFile(mbox); FileUtil.copy(in,
        false, 目标文件); 返回目标文件.getCanonicalPath();

    }

    @Override
    public InputStream readStreamFromStore(String locator, Mailbox mbox) 抛出 IOException { 返回新的 FileInputStream(locator);

    }

    @Override
    public boolean deleteFromStore(String locator, Mailbox mbox) 抛出 IOException {
        文件 deleteFile = new File(locator); 返回 deleteFile.delete();

    }
}

```

## HTTP 存储

另一个常见用例是写入外部 HTTP API,即云文件存储。如果 HTTP API 允许匿名上传,则可以通过扩展 HttpStoreManager 来实现。实现者只需提供定义用于 POST 新内容的 URL、从 POST 响应中提取 HTTP 服务器唯一标识符的过程以及用于获取和删除先前存储的内容的 URL 的方法代码。Zimbra Mailbox 对象可供可选使用;根据 HTTP API 语义,它可用于构造 URL 的一部分,也可以忽略它。getLocator() 方法中提供了大小、SHA-256 摘要和 Mailbox 对象,Apache Commons HttpClient PostMethod 也可用于提取响应标头和响应正文。有关 HttpClient 的完整详细信息,请参阅<http://hc.apache.org/httpclient-3.x/>

受保护的抽象字符串 getPostUrl (邮箱 mbox) ;受保护的抽象字符串 getGetUrl (邮箱 mbox,字符串定位器) ;受保护的抽象字符串 getDeleteUrl (邮箱 mbox,字符串定位器) ;受保护的抽象字符串 getLocator (PostMethod post,字符串 postDigest,长 postSize,邮箱mbox)抛出ServiceException、IOException；

HttpStoreManager 的完整列表如下。请注意, isCentralized() 返回 true, 因为通常只有一个 HTTP 存储, 所有 Zimbra 服务器都连接到该存储。该存储必须生成全局唯一的定位器, 可从任何 Zimbra 服务器访问。

```

公共抽象类 HttpStoreManager 扩展了 ExternalStoreManager {

    受保护的抽象字符串 getPostUrl (邮箱 mbox) ;受保护的抽象字符串 getGetUrl (邮
    箱 mbox,字符串定位器) ;受保护的抽象字符串 getDeleteUrl (邮箱 mbox,字符串定位器) ;受保护的抽象字符
    字符串 getLocator (PostMethod post,字符串 postDigest,长 postSize,
    邮箱mbox)抛出ServiceException、IOException;

    @Override
    public String writeStreamToStore(InputStream in, long actualSize, Mailbox mbox) 抛出
    IO异常,
        ServiceException
    { MessageDigest 摘要;尝试 { 摘要
        =
        MessageDigest.getInstance( SHA-256 );} catch (NoSuchAlgorithmException
        e) { 抛出 ServiceException.FAILURE( 未找到 SHA-256 摘
        要 ,e);
    }
    ByteUtil.PositionInputStream pin = new ByteUtil.PositionInputStream(new DigestInputStream(in, digest));

    HttpClient 客户端 =
ZimbraHttpConnectionManager.getInternalHttpConnMgr().newHttpClient();
    PostMethod post = new PostMethod(getPostUrl(mbox));尝试

    { HttpClientUtil.addInputStreamToHttpMethod(post, pin, actualSize, application/octet-
    溪流” ) ;
        int statusCode = HttpClientUtil.executeMethod(client,post); 如果 (statusCode ==
        HttpStatus.SC_OK || statusCode == HttpStatus.SC_CREATED || statusCode == HttpStatus.SC_NO_CONTENT) {

            返回 getLocator(post, ByteUtil.encodeFSSafeBase64(digest.digest())),
            pin.getPosition(), mbox);} else { 抛出
                ServiceException.FAILURE( 错误 POSTing blob: + post.getStatusText(),
                无效的) ;

            } } 最后 {
                发布.释放连接();
            }
    }

    @Override
    public InputStream readStreamFromStore(String locator,Mailbox mbox) 抛出 IOException {

        HttpClient 客户端 =
ZimbraHttpConnectionManager.getInternalHttpConnMgr().newHttpClient();
        GetMethod get = new GetMethod(getGetUrl(mbox, locator)); int statusCode =
        HttpClientUtil.executeMethod(client, get); if (statusCode == HttpStatus.SC_OK) { return
        new UserServlet.HttpInputStream(get); } else
            { get.releaseConnection(); 抛出新的 IOException ( “blob GET 期间出
            现意外的返回
            代码: ”
            +
            获取.getStatusText());
        }
    }

    @Override

```

```

公共布尔值deleteFromStore (字符串定位器,邮箱mbox)
    抛出 IOException {
        HttpClient 客户端 =
ZimbraHttpConnectionManager.getInternalHttpConnMgr().newHttpClient();
        DeleteMethod delete = new DeleteMethod(getDeleteUrl(mbox, locator)); 尝试 { int statusCode =
            HttpClientUtil.executeMethod(client, delete); 如果 (statusCode == HttpStatus.SC_OK || statusCode ==
                HttpStatus.SC_NO_CONTENT) {
                    返回 true;
                } else if (statusCode == HttpStatus.SC_NOT_FOUND) { return false; } else { throw
                    new IOException( 在
                    blob DELETE
                    期间出现意外的返回代码:
删除.getText()); } } 最后 { 删
+}

除.releaseConnection();
}
}

}

```

## 基于内容的存储

某些外部存储系统可能会根据数据内容维护标识符。例如，商店可能会使用 SHA-256 或其他哈希作为存储对象的主键。ContentAddressableStoreManager 抽象类可用作与此类商店集成的起点。

实施者必须提供代码来生成 byte[] 哈希和字符串定位器。

```

/**
 * 使用来自远程存储的哈希算法为 blob 生成内容哈希 @param blob - 已在本地构建的 Blob @return byte[] 表示 blob 内容 @throws
 * ServiceException @throws IOException */
*
*
*

公共抽象字节[] getHash(Blob blob) 抛出 ServiceException,IOException;

/**
 * 根据 blob 的内容生成定位器字符串 @param blob - 已在本地构建的 Blob @return 表示 blob 内
 * 容的字符串,例如十六进制编码的哈希 @throws ServiceException @throws IOException */
*
*
*

受保护的抽象 String getLocator(Blob blob) 抛出 ServiceException,IOException;

/**
 * 通过十六进制编码或商店要求的其他类似编码返回内容哈希的定位器字符串
 *
 * @param hash: byte[] 包含内容哈希 @return 定位器字符串
*/
公共抽象字符串 getLocator (byte[] hash) ;

```

这是一个示例实现，它使用 SHA-256 作为哈希并附加 .blob 来生成定位器。

```
@Override  
protected String getLocator(Blob blob) 抛出 ServiceException, IOException {  
    返回 getLocator(getHash(blob));  
}  
  
@Override  
public String getLocator(byte[] hash) {  
    返回 Hex.encodeHexString(hash).toUpperCase() + ".blob" ;  
}  
  
@Override  
public byte[] getHash(Blob blob) 抛出 ServiceException, IOException {  
    MessageDigest digest = MessageDigest.getInstance("SHA-256"); DigestInputStream dis  
    = new DigestInputStream(blob.getInputStream(), digest); while (dis.read() >= 0) {} return digest.digest();  
}  
}
```

ContentAddressableStoreManager 的完整列表如下。ExternalStoreManager 中的几种方法已被覆盖，因此内容定位器可以包含在上游写入请求中。

```

/**
 * StoreManager 实现的抽象框架,需要内容哈希或其他
基于内容的定位器
 * 这里的基本实现处理了更常见的情况,即 blob 在本地缓存
storeIncoming 然后在阶段操作期间推送到远程存储
 */
公共抽象类 ContentAddressableStoreManager 扩展了 ExternalStoreManager {

    @Override
    公共字符串 writeStreamToStore (InputStream 输入,长实际大小,
                                    邮箱 mbox) 抛出 IOException, ServiceException {
        //下面阶段的覆盖绝不应该允许达到此代码
        抛出 ServiceException.FAILURE(“不允许匿名写入,出现错误”,
        无效的) ;
    }

    /**
     * 使用来自远程存储的哈希算法为 blob 生成内容哈希
     * @param blob - 本地构建的 Blob
     * @return byte[] 表示 blob 内容
     * @throws 服务异常
     * @throws IOException
     */
    公共抽象字节[] getHash(Blob blob) 抛出 ServiceException,IOException;

    /**
     * 根据 blob 的内容生成定位器字符串
     * @param blob - 本地构建的 Blob
     * @return 表示 blob 内容的字符串,例如十六进制编码的哈希值
     * @throws 服务异常
     * @throws IOException
     */
    受保护的抽象 String getLocator(Blob blob) 抛出 ServiceException,IOException;

    /**
     * 通过十六进制编码或其他类似编码返回内容哈希的定位器字符串
商店要求
     * @param hash: byte[] 包含内容哈希
     * @return 定位器字符串
     */
    公共抽象字符串 getLocator (byte[] hash) ;

    /**
     * 使用先前生成的 blob 定位器将数据写入 blob 存储
     * @param in:包含要写入的数据的InputStream
     * @param actualSize:流中的数据大小,如果大小未知则为 -1。由
尽可能进行优化的实施者
     * @param getLocator() 返回的 blob 的定位器字符串
     * @param mbox:包含 blob 的邮箱。存储可以选择使用它来
分割
     * @throws IOException
     * @throws 服务异常
     */
    protected abstract void writeStreamToStore(InputStream in, long actualSize, Mailbox mbox,
字符串定位器抛出IOException,ServiceException);

    @Override
    public StagedBlob stage(Blob blob,Mailbox mbox) 抛出 IOException,ServiceException {

```

```

        如果 (支持 (StoreFeature.RESUMABLE_UPLOAD) && blob 实例 ExternalUploadedBlob &&
blob.getRawSize() > 0)
            { ZimbraLog.store.debug( blob 已上传,只需提交 ); String locator = ((ExternalResumableUpload)
this).finishUpload((ExternalUploadedBlob) blob);
ZimbraLog.store.debug( 暂存到定位器 %s , locator);
            localCache.put(locator, getContent(blob)); return new ExternalStagedBlob(mbox,
blob.getDigest(), blob.getRawSize(), locator); } else { InputStream
is = getContent(blob); String locator = getLocator(blob); try { StagedBlob staged = stage(is, blob.getRawSize(), mbox, locator);
if (staged !=
        null) { ZimbraLog.store.debug( 暂存到定位器 %s ,
staged.getLocator()); localCache.put (staged.getLocator
(),
getContent (blob) );
}
        }
    }
}

@Override
public StagedBlob stage(InputStream in, long actualSize, Mailbox mbox) 抛出
服务异常,IO异常{
    Blob blob = storeIncoming(in); 尝试 { 返回
stage(blob, mbox); } 最后 { quietDelete(blob);
}

}
}

受保护的 StagedBlob 阶段 (InputStream 输入、长实际大小、邮箱 mbox、字符串定位器)
抛出 ServiceException { MessageDigest
摘要;尝试 { 摘要 =
MessageDigest.getInstance( SHA-256 ); } 捕获 (NoSuchAlgorithmException
e) { 抛出 ServiceException.FAILURE( 未找到 SHA-256 摘
要 , e);
}
ByteUtil.PositionInputStream pin = new ByteUtil.PositionInputStream(new DigestInputStream(in, digest));
}

尝试
{writeStreamToStore (pin,actualSize,mbox,locator) ;返回新的ExternalStagedBlob
(mbox,ByteUtil.encodeFSSafeBase64 (digest.digest () ) ,
pin.getPosition(), locator); } catch
(IOException e) { 抛出
ServiceException.FAILURE( 无法暂存 blob ,e);
}
}

续传上传 (只限八达通)

```

在 Octopus REST API 中,客户端可以部分上传文档,然后稍后恢复。使用默认的 ExternalStoreManager 实现,blob 会暂存在 Octopus 服务器中,并且只有在完全上传后才会发送到外部存储。这可能会导致客户端在上传完成后出现不必要的延迟。

为了优化这个过程,集成商可以实现 ExternalResumableUpload 接口,然后提供以可恢复的方式与商店交互的 ExternalResumableIncomingBlob 和 ExternalResumableOutputStream 实现。

```

公共接口 ExternalResumableUpload {
    /**
     * 创建一个新的 ExternalResumableIncomingBlob 实例来处理单个对象的上传。实现应在上传过程中计算所有远程元数据,例如远程 ID、
     * 大小和内容哈希,以便 finishUpload() 无需再次遍历数据

     *
     *
     * @param id:本地上传 ID。内部使用;必须传递给超级构造函数@param ctxt:本地上传上下文。内部使用;必须传递给超级构造函数@return
     * 已初始化的 ExternalResumableIncomingBlob 实例,准备接受新数据
     */

    上传
    *
    * @throws IOException
    * @throws ServiceException */

    公共 ExternalResumableIncomingBlob newIncomingBlob (String id, Object ctxt) 抛出
    IO异常,服务异常;

    /**
     * 完成上传。根据存储语义,这可能涉及 * 提交、校验和其他类似操作。

     *
     * @param blob: 已将数据写入的 ExternalUploadedBlob @return 上传数据的永久存储位置的字符串标识符 (定位器)
     */

    内容
    *
    * @throws IOException
    * @throws ServiceException
    */
    公共字符串 finishUpload (ExternalUploadedBlob blob) 抛出 IOException, ServiceException;
}

/**
 *
 * IncomingBlob 实现,在上传过程中将数据直接传输到外部存储
 * 商店必须支持断点续传,否则应使用默认
BufferingIncomingBlob 实现
*/

公共抽象类 ExternalResumableIncomingBlob 扩展了 BufferingIncomingBlob {

    公共 ExternalResumableIncomingBlob (String id, BlobBuilder blobBuilder, Object ctxt) 抛出
    ServiceException, IOException { 超级 (id,
        blobBuilder, ctxt) ;

    }

    @Override
    public OutputStream getAppendingOutputStream() 抛出 IOException {
        lastAccessTime = System.currentTimeMillis () ; 返回
        getAppendingOutputStream (blobBuilder) ;
    }

    @Override
    public long getCurrentSize() throws IOException { long internalSize =
        super.getCurrentSize(); long remoteSize = getRemoteSize(); if
        (remoteSize != internalSize) { throw new
        IOException( 本地 ( + internalSize + ) 和远程
        ( + remoteSize + ) 内容大小不匹配。客户端必须重新启动上传 , null); } else {
            +
        }
    }
}

```

```

        返回内部尺寸;
    }

}

@Override
public Blob getBlob() 抛出 IOException、ServiceException {
    返回新的ExternalUploadedBlob (blobBuilder.finish (),id) ;
}

/**
 * 检索可用于将数据写入远程上传位置的 OutputStream
 * @param blobBuilder:用于在上传时创建本地 Blob 实例。必须传递
到超级构造函数
 * @return ExternalResumableOutputStream 实例,可以将数据写入上传
此 IncomingBlob 实例封装的会话/位置
 * @抛出 IOException */

受保护的抽象 ExternalResumableOutputStream getAppendingOutputStream (BlobBuilder)
blobBuilder ) 抛出 IOException;

/* */
    查询远程存储中迄今为止收到的上传大小。用于在恢复期间进行一致性检查 @return:已远程存储的字节数。@throws IOException @throws ServiceException
*/
 *
 *
 *
 *

受保护的抽象长 getRemoteSize() 抛出 IOException;
}

/* */
    OutputStream 用于在可恢复上传期间写入外部存储器。
*
*/
公共抽象类 ExternalResumableOutputStream 扩展了 BlobBuilderOutputStream {

受保护的 ExternalResumableOutputStream (BlobBuilder blobBuilder){
    超级 (blobBuilder) ;
}

@Override
public void write(byte[] b, int off, int len) 抛出 IOException { writeToExternal(b, off, len); super.write(b,
    off, len);

}

/* */
    将数据附加到远程上传位置@param b:保存要上传的数据的字节数
    组@param off:开始上传的偏移量@param len:要从字节数组复制的数据的长度
    * @throws IOException */
    *

受保护的抽象 void writeToExternal(byte[] b, int off, int len) 抛出 IOException;
}

```

以下示例说明了续传上传所涉及的关键功能。该示例有意随意设置，并使用本地磁盘存储。

公共类 SimpleStreamingStoreManager 扩展了 SimpleStoreManager 实现

外部可恢复上传 {

字符串上传目录 = “/tmp/simplestore/uploads” ;

@Override

public void startup() 抛出 IOException、ServiceException {

超级.startup () ;

FileUtil.mkdirs (新文件 (uploadDirectory) ) ;

}

@Override

public String finishUpload(ExternalUploadedBlob blob) 抛出 IOException，

服务异常 {

ZimbraLog.store.info( 完成上传至 +blob.getUploadId()); return blob.getUploadId();

}

@Override

public ExternalResumableIncomingBlob newIncomingBlob(String id, Object ctxt) 抛出

IOException、ServiceException {返回新的

SimpleStreamingIncomingBlob (id, getBlobBuilder () , ctxt) ;

}

私有类 SimpleStreamingIncomingBlob 扩展了 ExternalResumableIncomingBlob {

私人最终文件文件；

公共 SimpleStreamingIncomingBlob (字符串 id, BlobBuilder blobBuilder,

对象 ctxt) 抛出 ServiceException, IOException {

超级 (id, blobBuilder, ctxt) ;

String baseName = uploadDirectory+ /upload- +id;

字符串名称 = 基本名称；

同步 (此){ int count = 1; File upFile

= new File (name+

“.upl” ) ; while (upFile.exists () ){ name = baseName+

“\_”+count++; upFile = new File (name+

“.upl” ) ;

}

如果 (upFile.createNewFile () ){

ZimbraLog.store.debug( 写入新文件 %s , upFile.getName()); file = upFile; } else { throw new

IOException( 无法创

建新文件 );

}

}

@Override

protected ExternalResumableOutputStream getAppendingOutputStream(BlobBuilder blobBuilder) 抛出 IOException {

返回新的 SimpleStreamingOutputStream (blobBuilder, 文件) ;

}

@Override

protected long getRemoteSize() 抛出 IOException {

```
    返回文件.长度 () ;  
}  
  
@Override  
public Blob getBlob() 抛出 IOException,ServiceException {  
    返回新的 ExternalUploadedBlob (blobBuilder.finish (),file.getCanonicalPath ()) ;  
}  
}  
  
私有类 SimpleStreamingOutputStream 扩展了 ExternalResumableOutputStream {  
  
    私有最终 FileOutputStream fos;  
  
    公共 SimpleStreamingOutputStream(BlobBuilder blobBuilder,File file) 抛出  
IO异常 {  
    超级 (blobBuilder) ;  
    this.fos = 新的 FileOutputStream (文件, true) ;  
}  
  
    @Override  
    protected void writeToExternal(byte[] b, int off, int len)  
        抛出 IOException { fos.write(b,  
            off, len);  
    }  
}
```

## Zimbra 移动同步

Zimbra Mobile Sync 提供移动设备和邮箱服务器账户之间的邮件、联系人、日历和任务数据的无线同步以及设备安全策略实施。

Active Sync 是微软定义的同步协议,用于配置和同步 Zimbra 邮箱服务器与用户设备上使用的本机客户端。

Zimbra Mobile Sync 与 iPhone、iPod Touch、Android、Outlook (Mac 和 Windows) 以及许多其他支持 ActiveSync™ 协议的手机兼容。

以下是 Zimbra ActiveSync 的亮点：

1. 支持协议版本 12.1、14.1、16.1。
2. 完全同步支持草稿、邮件、日历和联系人。
3. 支持允许阻止隔离设备 (又名 ABQ)。
4. 支持移动设备管理 (又名 MDM)。
5. 支持配置用户级 ActiveSync 协议版本。

日历功能：

1. 支持同步在 Android、iOS 上创建的约会 (更改邀请人、日期/时间等)。
2. 支持重复约会 (修改例外、整个系列)。
3. 对于共享日历, 支持修改, 权限等。

共享功能：

邮件、日历和联系人文件夹均支持共享。默认情况下, 共享处于禁用状态。以下是启用共享的属性：

`zimbraMobileShareMailEnabled` : 用于启用邮件文件夹共享的属性。在 cos 和账户级别受支持。`zimbraMobileShareCalendarEnabled` : 用于启用日历共享的属性。在 cos 和账户级别受支持。`zimbraMobileShareContactEnabled` : 用于启用联系人文件夹共享的属性。在 cos 和账户级别受支持。

由于 Exchange ActiveSync 协议的限制, 不支持实现只读共享。因此不建议共享只读文件夹/日历, 因为这会导致客户端和服务器的数据不一致。

以下是启用共享的命令：

- 邮件文件夹共享：

1. 为用户启用：

```
zmprov ma <user@domain.com> zimbraMobileShareMailEnabled TRUE
```

重击

2. 启用 cos：

重击

`zmprov mc <cos_name> zimbraMobileShareMailEnabled TRUE`

- 日历文件夹共享：

1. 为用户启用：

重击

`zmprov ma <user@domain.com> zimbraMobileShareCalendarEnabled TRUE`

2. 启用 cos：

重击

`zmprov mc <cos_name> zimbraMobileShareCalendarEnabled TRUE`

- 联系人文件夹共享：

1. 为用户启用：

重击

`zmprov ma <user@domain.com> zimbraMobileShareContactEnabled TRUE`

2. 启用 cos：

重击

`zmprov mc <cos_name> zimbraMobileShareContactEnabled TRUE`

目前，共享功能仅可通过 CLI 启用。未来版本将添加管理控制台中的支持。

## 设置 ActiveSync 协议版本

管理员可以通过在用户、cos 和域级别配置来限制用户对特定 ActiveSync 协议版本的访问。多值 LDAP 属性 `zimbraActiveSyncVersion` 用于配置协议版本。默认情况下，此属性未设置协议版本。此属性的任何版本更新都将覆盖本地配置属性 `zimbra_activesync_versions`。它支持根据用户代理、设备 ID 或设备类型应用版本。

## 语法

以下是指定版本的格式的详细信息：

- `android:14.1` - Android 设备将通过 14.1 版本连接。
- `iphone:16.1` - iPhone 设备将通过 16.1 版本连接。
- `14.1` - 所有设备类型都将通过 14.1 版本连接。
- `DeviceID:14.1` - 将 DeviceID 替换为实际设备 ID。指定的设备 ID 将通过 14.1 版本进行连接。
- `WindowsMail:14.0` - 对于以 WindowsMail 形式发送用户代理的应用程序，它将通过 14.0 版本进行连接。

## 设置协议版本的示例：

1. 要限制使用 Android 设备的用户使用版本 14.1：

重击

`zmprov ma <user@domain.com> +zimbraActiveSyncVersion android:14.1`

2. 要通过设备 ID 将用户限制为版本 16.0：

重击

`zmprov ma <user@domain.com> +zimbraActiveSyncVersion <设备 ID>:16.0`

3. 将 cos 中使用 Android 设备的用户限制为版本 14.1:

重击

`zmprov mc <cos_name> +zimbraActiveSyncVersion android:14.1`

4. 要将域中使用 iPhone 设备的用户限制为版本 16.0:

重击

`zmprov md <域名> +zimbraActiveSyncVersion iphone:16.0`

5. 要将域中使用任意设备的所有用户限制为版本 16.0:

重击

`zmprov md <域名> +zimbraActiveSyncVersion 16.0`

## 移动设备安全策略

管理员可以配置移动安全策略,以在与 Zimbra Collaboration 帐户同步的兼容移动设备上强制执行安全规则。

可以配置以下功能来增强移动设备的安全性。

- 如果移动设备丢失或被盗,远程擦除将删除设备上的所有数据。
- 设备密码策略用于设置强密码执行,包括最小密码长度、不活动时间、强制密码历史记录以及在配置的登录尝试失败后擦除设备消息。
- S/MIME 加密策略用于启用 S/MIME 使用并设置发送和签名加密的策略消息。

此外,您还可以管理以下设备使用选项:

- 同步过去日历和电子邮件项目、邮件大小和格式的设置
- 可以禁用设备设置,例如摄像头、桌面同步、蓝牙、可移动存储的使用。

## 在 Zimbra 中设置移动策略

您可以从管理控制台将移动设备策略作为服务类别或单个服务进行管理帐户。

重击

主页→配置→服务等级→(COS)→移动接入→常规

主页→管理→账户→(账户)→移动访问→常规

个人账户上配置的策略将覆盖 COS 策略。

1. 要从 COS 设置移动策略,请转到配置→服务类别,然后双击要配置。
2. 为了让移动设备同步到 Zimbra,请检查移动→常规→启用移动同步。
3. 选中启用移动策略以设置强制执行安全规则的移动安全策略。
4. 为了支持不支持部分或全部设备安全策略的旧设备,请选择允许不可配置设备。

5. 如果设备不确认或支持所有分配的策略,但您想允许设备下载消息中,选中允许在设备上实施部分策略。
6. 设备默认策略刷新的刷新间隔为24小时。
7. 在其他部分配置适当的策略。有关可配置设置的描述,请参阅移动设备安全策略属性。管理移动设备
8. 单击保存。

## 移动设备安全策略属性

可以从管理控制台配置以下属性来建立移动策略。

### 常规设置

成分	弃用声明
启用移动同步	为了使移动设备能够同步到 Zimbra Collaboration Server,必须选中“启用移动同步”。用户可以通过无线方式在移动设备和 Zimbra 服务器之间双向同步邮件、联系人和日历数据。
启用移动策略	选中此框可设置在兼容移动设备上强制执行安全规则的移动安全策略。您可以强制执行包括密码规则在内的一般安全策略,并在兼容设备上设置本地擦除功能。设置移动策略后,下次移动设备向服务器发送请求时,能够强制执行安全策略的移动设备会自动设置您实施的规则并立即执行这些规则。
允许不可配置的设备	如果启用此功能,不支持设备安全策略实施的旧设备仍然可以访问服务器。
允许在设备上实施部分策略	如果设备没有确认所有已下载的策略,Zimbra 仍然允许设备继续下载消息。
刷新间隔 (小时) :	指定 Zimbra 通过向同步请求发送“449 预配后重试”响应来强制在设备上刷新策略之前的时间(以分钟为单位)。默认值为 24 小时。

### 密码设置

成分	弃用声明
需要密码	用户必须在移动设备上创建密码。
最小密码长度	密码的最小字符数。默认为 4。 最大长度为 16 个字符。
需要字母数字密码	要求密码包含数字和字母字符。

成分	弃用声明
所需复杂字符数最少	必须包含的最少复杂字符数 密码。这是任何非字母的字符。默认值为 0 (没有任何)
允许简单密码	可以创建简单密码。简单设备密码是 具有特定模式的密码，例如 2468、1111。不 默认启用。
启用密码恢复	设备密码存储在服务器中，可以恢复。 默认启用。
允许设备加密	如果启用，则在手机上启用设备加密。 默认启用；
要求设备加密	如果启用，则必须在设备上实施加密，以 与服务器同步。默认情况下不启用。
不活动后需要重新输入密码 (分钟)	密码输入前设备保持不活动状态的时间长度 必须输入才能重新激活设备。默认为 15 分钟。
允许失败尝试	指定在登录设备之前尝试登录失败的次数 设备会自动启动本地擦除。设备不会 需要联系服务器才能实现此操作。默认值为 4。
有效期 (天)	密码可使用的天数。在此之后 天数，则必须创建新密码。默认值为 0， 密码未过期。
存储密码以防止重复使用	用户在旧密码之前必须创建的唯一密码数量 可以使用密码。默认为 8。

## S/MIME 设置

成分	弃用声明
启用 S/MIME 公钥加密并 签署	为了在移动设备上使用 S/MIME 加密，必须 已勾选。还必须在 COS 中启用 S/MIME 功能 功能页面。
要求设备发送签名消息	设备必须发送签名的 S/MIME 消息。未启用 默认。
需要 S/MIME 算法进行签名	签署消息时必须使用算法。未启用 默认。
要求设备发送加密消息 指定 S/MIME 消息是否必须加密。不 默认启用。	
要求使用 S/MIME 算法进行加密 签署消息时必须使用必需的算法。不 默认启用。	

成分	弃用声明
算法协商	设备上的消息应用程序如何协商 如果收件人的证书不支持加密算法 指定的加密算法。从“块协商”中选择； 仅限强算法，或允许任何算法。默认为允许 任何算法。
允许 S/MIME 软件证书	允许 S/MIME 软件证书。默认为允许。

## 同步设置

成分	弃用声明
已同步过去的日历项目	可同步到的最大日历天数范围 设备。默认为两周。
已同步过去的电子邮件项目	同步电子邮件项目的最长天数 设备。默认为 3 天。
限制纯文本消息大小 (KB)	电子邮件被截断的最大大小 同步到设备。默认不设置最大大小。
允许漫游时直接推送	移动设备在漫游时必须手动同步。默认 不是。
允许 HTML 格式的消息	在设备上启用 HTML 电子邮件。如果禁用此功能，则所有电子邮件都将 在同步之前转换为纯文本。默认为 启用 HTML 格式。
限制 HTML 邮件大小 (KB)	HTML 格式的电子邮件的最大大小 同步到设备。该值以 KB 为单位。默认值为 不设置最大尺寸。

## 设备设置

成分	弃用声明
允许可移动存储	移动设备可以访问存储在存储卡上的信息。 默认为 TRUE。
允许相机	指定可以使用设备上的摄像头。默认为 真的。
允许 Wi-Fi	指定设备允许无线访问互联网。 默认为 TRUE。
允许红外线	指定设备允许红外连接。 默认为 TRUE。
允许共享	指定移动设备可以用作调制解调器来 将计算机连接到互联网。默认为 TRUE。

成分	弃用声明
允许远程桌面	指定移动设备可以启动远程桌面连接。默认值为 TRUE。
允许桌面同步	指定移动设备可以与桌面同步通过电缆连接到计算机。默认值为 TRUE。
允许蓝牙	默认情况下，设备允许使用蓝牙功能。选择从允许、禁用到仅限免提。

## 设备应用

成分	弃用声明
允许浏览器	移动设备上允许使用 Microsoft® Pocket Internet Explorer 设备默认启用此功能。这不会影响第三方浏览器。
允许消费者邮件	用户可以在手机上配置个人电子邮件账户 设备。此参数不控制使用 第三方移动设备电子邮件程序。
允许 POP 或 IMAP 邮件	用户可以在设备上配置 POP3 或 IMAP4 电子邮件帐户。 此参数不控制第三方电子邮件的访问 程序。
允许短信	允许用户在设备上使用短信。
允许未签名的应用程序	允许在设备上使用未签名的应用程序。
允许安装未签名的包	允许在设备上安装未签名的包。

## 已获批准的申请清单

成分	弃用声明
已批准的申请	此设置存储了可以运行的已批准应用程序列表 在移动设备上。
阻止的应用程序	此设置指定了不能运行的应用程序列表。

## 移动设备管理

设置移动策略后，下次移动设备向服务器发送请求时，  
能够自动执行安全策略，设置规则并立即执行。

例如，如果设备上没有设置密码，或者密码强度不符合安全机构的要求，  
移动策略，用户必须在与服务器同步之前修复密码。一旦服务器确认  
该策略在移动设备上强制执行，设备可以同步。

如果移动设备丢失或被盗，该设备将受到以下策略规则的保护：

- 当配置了“不活动后需要重新输入密码（分钟）”时，在配置的分钟数之后，设备将被锁定。要解锁设备，用户必须重新输入密码。
- 当配置了允许失败尝试次数时，如果密码输入错误次数超过指定次数，则将执行本地（由设备生成）启动的设备擦除。这将擦除设备上的所有数据。

除了从管理控制台设置的执行本地设备擦除的规则之外，用户还可以从他们的 ZWC 帐户启动远程擦除，以清除丢失、被盗或退役设备上的所有数据。

Zimbra 移动设备管理（又名 MDM）功能也可以在管理控制台中找到，可以在全局、COS、域和帐户级别管理移动设备：

配置→全局设置→移动  
 配置→COS→移动  
 配置→域→移动  
 配置→管理→账户→（用户）→移动

重击

- 移动策略和注册设备管理设置位于 COS 和帐户内。
- 仅已注册的设备管理设置在全局和域部分可用。

## 移动设备管理允许/阻止规则 (ABQ)

设备管理允许/阻止规则支持正则表达式规则，可以创建这些规则以允许或阻止设备连接到 Zimbra Collaboration 服务器。这些规则使用命令行应用，可以使用 `zimbraMobileAllowedDevices` 和 `zimbraMobileBlockedDevices` 多值属性在全局或域级别创建。这些属性可以在全局或域级别设置。

### `zimbraMobileAllowedDevices`

只有与 `zimbraMobileAllowedDevices` 中配置的设备相匹配的设备才允许使用 ActiveSync 协议进行同步，所有其他设备都将被阻止。例如，如果配置了 iPhone\*，则只有报告为 iPhone~ 的设备才允许同步。

### `zimbraMobileBlockedDevices`

只有与 `zimbraMobileBlockedDevices` 中配置的设备相匹配的设备才允许连接。例如，如果添加了 iPhone\*，则所有报告为 iPhone~，所有其他设备的设备都将被阻止，而所有其他设备（例如 Android 和 Windows）将被允许同步。

## 命令行示例

以下是如何在 Global 和域级别：

由于这些是多值属性，因此在添加或删除规则时需要使用 + 或 -。如果两者都未使用，则所有当前配置都将替换为当前执行的规则。

- 仅阻止 iPhone 设备：

全球的  
`zmprov mcf +zimbraMobileBlockedDevices *iPhone*`

重击

重击

领域

`zmprov md 域名 +zimbraMobileBlockedDevices *iPhone*`

- 仅允许 iPhone 设备：

重击

全球的

`zmprov mcf +zimbraMobileAllowedDevices *iPhone*`

重击

领域

`zmprov md 域名 +zimbraMobileAllowedDevices *iPhone*`

- 列出全局级别所有现有的允许或阻止规则：

重击

全球的

`zmprov gcf zimbraMobileAllowedDevices zmprov gcf  
zimbraMobileBlockedDevices`

重击

领域

`zmprov gd 域名 zimbraMobileAllowedDevices zmprov gd 域名  
zimbraMobileBlockedDevices`

## 隔离通知

可以为所有新隔离设备配置特定时间间隔的隔离通知。这需要在每个邮箱服务器上使用`zmlocalconfig`命令进行配置。

以下是用于配置通知电子邮件正文和主题的属性：

- `zimbra_mobile_mdm_notification_email_body` :用于自定义通知电子邮件正文的属性。如果未设置,将使用默认正文。
- `zimbra_mobile_mdm_notification_email_subject` :用于自定义通知电子邮件主题的属性。如果未设置,将使用默认正文。

要查看电子邮件正文,请执行：

`zmlocalconfig zimbra_mobile_mdm_notification_email_body`

重击

要更改通知电子邮件正文,请执行：

`zmlocalconfig -e zimbra_mobile_mdm_notification_email_body “新通知正文”`

重击

要查看通知电子邮件主题,请执行：

`zmlocalconfig zimbra_mobile_mdm_notification_email_subject`

重击

要更改通知电子邮件主题,请执行：

`zmlocalconfig -e zimbra_mobile_mdm_notification_email_subject “新通知主题”`

重击

## 设置隔离通知间隔

`zmmdmmailschedule`命令用于设置通知间隔。默认情况下，没有通知间隔设定。

### 句法

`zmmdmmailschedule [-l|-h|-f|-e]`

重击

### 选项：

长名称	简称	描述
<code>-l</code>	列表	打印现有的时间表。
<code>-h</code>	帮助	获取有关 <code>zmmdmmailschedule</code> (默认命令)。
<code>-f</code>	冲洗	删除当前时间表 (取消所有 Zimbra MDM 设备电子邮件安排政策)。
<code>-e</code>	编辑	使用 指定的时间表。

### 编辑通知间隔的语法：

`zmmdmmailschedule -e {<45m | 6h | 1d | 0>} 管理员电子邮件`

重击

### 设置通知间隔的 CLI 示例：

- 分钟 : 设置要发送到 `admin@domain.com` 的隔离通知每 45 分钟执行一次  
以下命令：

`zmmdmmailschedule -e 45m admin@domain.com`

重击

管理员电子邮件是可选输入。如果没有提供管理员电子邮件地址，则电子邮件将每 45 分钟发送给所有配置的管理员。例如：`zmmdmmailschedule -e 45m`。

- 小时 : 设置发送至 `admin@domain.com` 的隔离通知每 6 小时执行一次

以下命令：

`zmmdmmailschedule -e 6h admin@domain.com`

重击

- 天 : 设置发送隔离通知至 `admin@domain.com` 每 3 天执行以下操作  
命令：

`zmmdmmailschedule -e 3d admin@domain.com`

重击

- 零:要禁用隔离通知,请执行以下命令:

```
zmmdmmailschedule -e 0 admin@domain.com
```

重击

- flush:要删除隔离通知计划,请执行以下命令:

```
zmmdmmailschedule -f
```

重击

## 注册设备

注册设备部分使管理员能够为用户采取各种操作。

以下是支持的操作

动作名称	描述	操作执行后的状态
断开	断开设备与帐户的连接。	正在等待设备
暂停同步	暂停设备。新消息将无法同步到设备。但旧版消息将可供访问。	暂停
恢复同步	恢复与移动设备的同步。	等待设备。连接后成功并恢复同步后,状态更改为“活动”。
擦除设备	重置移动设备。  请谨慎使用 使用此操作,因为它将删除所有数据 从设备中。	清除待处理。一旦操作完成 已成功完成,状态为 更改为擦除完成。
取消 擦除	取消擦除设备操作。  此举将只 允许,直到状态为 擦除待处理的 设备。	等待设备
堵塞	阻止设备并删除同步的 来自设备的消息。	已阻止
删除帐户	从手机中删除该帐户	删除待处理帐户。一旦 账号删除成功,状态 更改为帐户已移除。

动作名称	描述	操作执行后的状态
取消 移除 帐户	<p>取消删除帐户操作。</p> <p>此次行动将 允许,直到状态为 删除帐户 等待设备。</p>	一旦设备连接并同步电子邮件,状态就会更改 为“活动”。

## 支持自动发现

Zimbra 支持自动发现服务,因此用户无需了解服务器设置即可为其 Zimbra 帐户配置移动设备。用户输入电子邮件地址和密码后,自动发现将返回所需的服务器设置。

自动发现功能默认启用。要使自动发现功能正常工作,您必须配置来自证书颁发机构的有效 SSL 证书。

建议使用的证书类型是统一通信证书或 UCC。此证书允许您在主题备用名称字段中添加多个主机名。要使自动发现正常工作,主题备用名称字段必须包含用户要连接的主机名。

您必须拥有autodiscover.<domain>.com 的有效域名服务 (DNS SRV 记录),以便客户端设备可以定位并连接到自动发现服务。

使用管理控制台上的“安装证书”向导生成证书签名请求,并在收到签名证书后安装该证书。许多证书颁发机构都可以颁发统一通信证书。

完成请求后,您必须拥有有效的域名服务 (DNS SRV 记录)才能进行自动发现。<domain>.com。使用您使用的有效域名配置主题备用名称 (SAN) 字段。备用名称应包括域 autodiscover.<company>.com。在主题备用名称字段中包含您的环境所需的所有域名。

确保 Web 服务器模式为 https、两者、重定向或混合,因为自动发现和来自设备的其他通信是 HTTPS。

## 为用户帐户设置移动同步

移动同步可在帐户的 COS 配置文件中或个人帐户中启用。在大多数情况下,不需要额外的插件。

如果用户没有自动发现功能,则可能需要在移动设备上配置以下内容以同步到他们的 Zimbra 帐户。

- 服务器名称 (地址) :输入用户的 Zimbra Collaboration 邮箱服务器的完全限定主机名。
- 用户名 :输入用户的主要 Zimbra 协作帐户名。
- 域:输入用户的 Zimbra Collaboration 域名 (DNS)。
- 如果在自签名认证中使用 SSL,则可能必须将服务器的SSL 证书作为受信任的证书添加到设备中。

用户可以将 Zimbra 帐户同步到移动设备。他们可以发送电子邮件、创建约会并将联系人添加到地址簿。

有关特定设备设置的详细信息,请参阅 Zimbra Wiki 上的移动设备设置页面。

## 更改移动设备密码策略

如果移动设备被 Zimbra Collaboration 移动密码策略锁定,则必须删除 PIN 要求才能重新同步该设备。

主页→管理→账户→账户→移动

重击

1. 在管理控制台中,打开要修改的用户账户。
2. 在移动页面上,取消选中“强制在设备上输入密码”。禁用密码策略后,用户必须重新同步设备。

## 用户移动设备自助功能

用户可以直接管理以下设备功能。

- 远程擦除设备。如果移动设备丢失、被盗或不再使用,用户可以从其 ZWC 帐户启动远程擦除,以清除移动设备上的所有数据。设备将恢复到其原始出厂设置。
- 暂停从移动设备发起的同步并恢复到设备的同步。
- 从列表中删除设备。如果从列表中删除设备后,设备尝试同步,则服务器会强制设备在下次同步时再次获取策略。

## 备份和恢复

Zimbra Collaboration 包含一个可配置的备份管理器,它驻留在每个 Zimbra Collaboration 服务器上,并执行备份和恢复功能。您无需停止 Zimbra Collaboration 服务器即可运行备份过程。

本章介绍如何备份和恢复数据,以及如何使用管理员用户界面 (管理控制台) 和 CLI 工具备份或恢复 Zimbra Collaboration 邮箱服务器。此外,本章还提供了灾难恢复的信息和一般准则。

对于备份和恢复功能,Zimbra Collaboration Daffodil (M10) 目前不支持。  
将备份文件存储在 S3 外部存储上或从 S3 外部存储恢复备份。

### 备份邮箱服务器

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

目前不支持使用外部存储 (如 S3 外部存储) 进行备份和恢复。

### 重做日志

每个 Zimbra 邮箱服务器都会生成重做日志,其中包含自上次增量备份以来消息存储服务器处理的当前事务和存档事务。

当服务器恢复时,在备份文件完全恢复后,将重播存档中的所有重做日志和当前正在使用的重做日志,以使系统恢复到故障之前的状态。

当当前重做日志文件大小达到 100MB 时,当前重做日志将滚动到存档目录。此时,服务器将启动新的重做日志。上一个重做日志中所有未提交的事务都会被保留。如果发生崩溃,服务器重新启动时,将读取当前重做日志以重新应用任何未提交的事务。

运行增量备份时,重做日志会从存档移动到备份目录。

## 备份方法

有两种备份方法可用:

- 标准备份方法是默认方法,适合希望在同一天备份所有帐户的客户
- 自动分组备份方法是每天备份一部分账户的方法。

### 备份方法概述

自动分组和标准备份将执行完整的备份过程,备份恢复邮箱所需的所有信息,包括每个邮箱的 LDAP 目录服务器、数据库、索引目录和消息目录。

LDAP 目录作为完整或增量备份过程的一部分进行备份。所有帐户、域、服务器、COS 和其他数据均会备份。

每个邮箱服务器都会生成重做日志，其中包含该服务器处理的每个事务。如果服务器发生意外关闭，重做日志将用于以下操作：

- 为了确保没有未提交的事务，服务器在启动时读取当前重做日志并重新执行和完成任何未提交的事务。
- 在服务器发生故障时恢复自上次完整备份以来写入的数据。

当服务器恢复时，在备份文件完全恢复后，将重播存档中的所有重做日志和当前正在使用的重做日志，以使系统恢复到故障之前的状态。

备份共享消息时，如果代表消息的文件已经存在于每日备份中，它会将该对象标记为此类并且不会再次复制其内容。

如果自动分组或增量备份过程发现某个邮箱没有以前的完整备份，则会对该邮箱执行完整备份。

自动分组备份结合了完整备份和增量备份功能，无需增量备份。

自动分组和增量备份会将重做日志移至备份目录。重做日志记录了发生的每项活动。它们包含已发送的所有消息的完整副本，以及标签、联系人和对话等元数据。

这些备份文件可用于恢复完整的邮箱服务器或单个邮箱，以便完全恢复帐户和消息数据。

Zimbra MTA 没有备份，因为数据仅在服务器上保留很短的时间。

自定义配置（例如 mailboxd 的 `jetty/etc/\*.xml`）未备份。

## 自动分组备份方法

自动分组备份方法对不同的邮箱组运行完整备份，然后收集每个邮箱服务器上剩余帐户的重做日志。不建议手动运行自动分组备份，因为它们是从 CLI 安排的，并在安排的时间自动运行。

## 标准备份

标准备份方法每周对每个邮箱服务器进行一次完整备份，然后在计划程序中定义的剩余天数进行增量备份。此方法适用于 400 个用户以下的小型安装。

## 备份通知

执行完整备份和增量备份时，会向管理员邮箱发送备份报告。此报告显示备份成功或失败，并包含有关备份开始和结束时间、备份的帐户数量以及重做日志序列范围的信息。

如果备份失败，则会包含额外的错误信息。

## 备份文件的目录结构

备份目的地称为备份目标。对于备份系统来说，它是邮件服务器文件系统中的路径。Zimbra 默认备份目录是 /opt/zimbra/backup。

标准备份过程创建的备份目录结构显示在标准备份目录中  
结构。您可以定期将备份运行到同一目标区域,而无需覆盖以前的备份  
会话。

accounts.xml文件列出了所有备份中的所有帐户。对于每个帐户,此文件显示  
账户 ID、电子邮件地址以及该账户最新完整备份的标签。如果您保存了备份  
会话保存到另一个位置,您还必须将最新的 accounts.xml 文件保存到该位置.accounts.xml 文件  
用于在恢复期间查找帐户的最新完整备份。如果 accounts.xml 文件丢失,则必须  
指定要从中恢复的备份标签。

重做日志目录位于 /opt/zimbra/redolog redo.log 。当当前重做日志文件大小达到  
100MB,当前重做日志滚动到存档目录 /opt/zimbra/redolog/archive 。此时  
服务器启动一个新的重做日志。所有来自前一个重做日志的未提交事务都会被保留。在  
崩溃,当服务器重新启动时,将读取当前重做日志以重新应用任何未提交的事务。

重做操作对时间至关重要,因此执行目录移动而不是复制然后删除功能。  
仅当源路径和目标路径位于同一文件系统卷上时,才可执行此目录移动。  
换句话说,重做日志和重做归档日志必须位于同一文件系统卷上,因为归档  
文件是重做日志文件系统的子目录。

所有增量和自动分组备份会话必须保存到与所有重做日志相同的目录中  
在同一备份目标中找到。标准完整备份会话可以使用不同的目标目录。

**表 标准备份目录结构**

/opt/zimbra/备份	备份的默认根目录
账户.xml/	所有帐户的列表,每个帐户都有电子邮件文件地址、Zimbra ID 和最新完整备份 标签.accounts.xml 维护电子邮件地址与其当前 zimbraIds 以及每个帐户的最新完整备份。
会议/	备份会话的根。
完整-<时间戳>/	完整备份目录。会话的时间戳是备份开始时间 GMT,包括毫秒。使用 GMT 而不是当地时间是为了保持视觉 在夏令时转换期间进行排序。
会话.xml	有关完整或增量会话的此备份标签的元数据,例如开始和 停止时间。
共享_blobs/	包含此备份中的账户之间共享的消息文件。
系统/	全局数据库表和本地配置。
数据库架构.xml	全局表的数据库架构信息。每个表转储文件都有一个 “.csv” 格式。
本地配置文件	备份时复制 /opt/zimbra/conf/localconfig.xml 。
<表名>.dat	数据库表数据转储。
LDAP/ldap.bak	LDAP 转储。
账户/	每个帐户的数据都保存在该目录的一个子目录中。

<.../zimbraID>/	每个帐户的根。
元文件	有关此帐户备份的元数据。
ldap.xml	帐户的 LDAP 信息,包括别名、身份、数据源、分发列表等
ldap_latest.xml	如果存在,此文件将链接到最新增量备份的 ldap.xml。
分贝/	特定于帐户的数据库表转储。
数据库架构.xml	此帐户表的数据库架构信息。
<表名>.dat	数据库表数据转储。
斑点/	包含 blob 文件。
指数/	包含 Lucene 索引文件。
增加<时间戳>	增量备份目录。此目录类似于完整备份目录模式并包含这些元文件。
会话.xml	
系统/db_schema.xml	
账户/...<zimbraID>/ldap.xml	incr-<timestamp>不包括accounts/.../<zimbraID>/db/db_schema.xml 因为增量备份不会转储帐户表。

对于自动分组备份,目录结构将重做日志文件保存到完整备份会话。没有增量备份会话。

## 使用管理控制台进行备份和恢复

许多备份和恢复任务可以直接从管理控制台运行。您可以配置它们在全局或服务器级别,服务器级别配置将覆盖全局设置。管理员备份和恢复位置位于:

全局备份配置

配置→全局设置→备份/恢复

服务器备份配置

配置→服务器→(服务器)→备份/恢复

备份管理和恢复

工具和迁移→备份→(服务器)

## 从管理控制台配置备份/恢复

可以从管理控制台将备份配置为全局设置配置或服务器特定配置。服务器设置覆盖全局设置。全局设置默认适用于每个服务器,直到被服务器覆盖。

## 备份/恢复

- 启用备份 - 设置为TRUE 时,启用全局备份并初始化当前全局和服务器配置以创建和管理备份。
  - LDAP 属性 - zimbraGlobalBackupEnabled
  - 默认值-TRUE
- 备份类型 - 自动分组或标准备份
  - LDAP 属性 - zimbraBackupMode
  - 默认值 - 自动分组
- 保留完整备份的天数 - 备份将保留的天数。备份计划程序将删除早于设定值的备份。
  - LDAP 属性 - zimbraBackupRetentionDays
  - 默认值 - 8
- 限制自动备份 - 自动分组备份方法会在安排下一次备份时自动备份从未备份过的邮箱。每次需要对所有邮箱进行完整备份时（例如在大量邮箱迁移后或重大升级后）,这可能不是最佳选择。启用此选项会将每日备份中的邮箱数量限制为 T/N。这打破了在 N 天内备份所有邮箱的限制,但有助于在非工作时间完成备份。

当所有邮箱至少备份一次时,禁用限制:

```
zmprov mcf zimbraBackupAutoGroupedThrottled TRUE
```

重击

- 安排时间- 每日备份开始时间,可使用小时和分钟进行配置。
  - LDAP 属性 - zimbraBackupStartTime
  - 默认值 - 01:00
- 默认备份目标 - 存储创建的备份的默认路径。
  - LDAP 属性 - zimbraBackupTarget
  - 默认值-/opt/zimbra/backup
- 通知电子邮件主题的前缀 - 备份通知电子邮件中使用的主题。
  - LDAP 属性 - zimbraBackupReportEmailSubjectPrefix
- 备份最小可用空间 - 配置zimbraBackupMinFreeSpace属性可帮助您通过通知来管理正在运行的备份会话。将属性zimbraBackupMinFreeSpace的值设置为运行备份会话之前备份目标磁盘上所需的可用空间量。如果磁盘空间小于属性中设置的值,则备份会话将不会运行,并向管理员发送电子邮件通知。

如果您还要备份 MariaDB 数据库,请确保将值设置得足够大,以包含mysqldump文件大小。此属性的值可以指定为总磁盘空间的百分比,例如25%等。默认值为0 ,表示禁用检查,并且始终允许启动备份。

, 或者以字节数表示,例如300MB , 50GB ,

- LDAP 属性 - zimbraBackupMinFreeSpace

## 通知

在全局设置中,您可以配置电子邮件地址以接收有关备份结果的通知。

默认是将通知发送到管理员账户。

- LDAP 属性

- zimbraMailReportEnabled
- zimbra备份报告电子邮件发送者
- zimbra备份报告电子邮件收件人

## 选项

您可以配置这些备份选项,以便在完整备份会话期间不备份搜索索引、blob 和 SM blob。

- 排除 blob - 如果将其设置为TRUE,则不会备份 blob。当 blob 驻留在容错存储中时,这可能有助于更快地备份数据库数据。此配置适用于所有 blob,包括主卷和辅助 (SM) 卷上的 blob。
  - LDAP 属性 - zimbraBackupSkipBlobs
  - 默认值-FALSE
- 排除 SM 卷上的 blob - 如果将其设置为TRUE,则不会备份 SM 卷上的 blob。如果zimbraBackupSkipBlobs为FALSE但您想要跳过 SM 卷上的 blob,请设置此项。
  - LDAP 属性 - zimbraBackupSkipHsmBlobs
  - 默认值-FALSE
- 以 zip 格式压缩 Blob - 备份中的 Blob 默认以 zip 格式压缩。
  - zip - 将 blob 备份到带有压缩的 zip 文件中 (默认) 。
  - zipStore - 将 Blob 备份到 zip 文件中,无需压缩。
  - noZip-将 blob 作为单独的文件而不是 zip 文件进行备份。
  - LDAP 属性 - zimbraBackupBlobsCompressType
  - 默认 - zip
- 排除搜索索引 - 设置为TRUE 时,所有帐户的搜索索引都将从备份中排除。如果恢复帐户,则需要重新创建索引。从没有搜索索引的备份恢复后。
  - LDAP 属性 - zimbraBackupSkipSearchIndex
  - 默认值-FALSE

## 选择要备份的用户

选择要备份的用户部分提供了备份一个或多个 COS、域或所有帐户的功能。以下是需要了解的关键事项：

- 此配置将应用于所有邮箱存储,但可以通过命令行覆盖。
- 可以将帐户标记为在 COS 和域内备份,但只能备份一次。
- 启用“域和 COS”时,zimbraBackupObjectLevelEnabled 将设置为 TRUE,从而在 zmschedulebackup 命令中的 useBackupConfig 中启用域、COS、帐户备份。选择“所有用户”时,zimbraBackupObjectLevelEnabled 设置为 FALSE,zmschedulebackup 将设置为所有用户。

- 至少需要选择一个 COS 或域来
- Zimbra 继承将遵循

## 使用存储卷的建议

- 对于内部存储,建议使用 with-blob 备份/恢复
- 对于外部存储,建议使用无 blob 备份/恢复
- 在设置内部主存储和外部辅助存储时,建议对主存储使用带 blob 的备份/恢复,对外部辅助存储使用无 blob 的备份/恢复
- 应使用与备份相同的 blob skip 配置进行还原
- 对于每个无 blob 备份,Blob 的备份责任由 S3 存储提供商承担
- 此版本不支持主存储为外部存储、辅助存储为内部存储的配置

## 邮件恢复设置

消息恢复是使用垃圾箱功能构建的,该功能现在是备份和恢复配置的一部分。

使用消息恢复时,您需要注意:

- 消息恢复和垃圾箱共享配置,并且在任一位置内启用、禁用或修改配置都将应用于另一个位置。
- 消息恢复是恢复已删除消息、日历约会、联系人和任务的推荐方法。
- 可以在管理员的所有账户或一个或多个域和/或 COS 上设置启用消息恢复
- 要禁用消息恢复,请选择域和 COS,并将服务等级和域留空。
- 域和 COS 配置需要至少一个域或 COS 才能启用该功能。
- 启用消息恢复时,zimbraDumpsterEnabled 属性将设置为 TRUE,它是一个全局、COS、域和用户属性。
- Zimbra 继承将遵循

相关的 LDAP 属性有:

- zimbraMailDumpsterLifetimetype - 垃圾箱中消息的保留期限。0 表示所有消息都将被保留。
  - 默认 - 30d
- zimbraDumpsterUserVisibleAge - 根据放入垃圾箱后的时间限制最终用户可以查看多少垃圾箱数据
  - 默认 - 30d
- zimbraDumpsterPurgeEnabled - 设置为 FALSE 时禁用从垃圾箱清除
  - 默认值-FALSE

## 使用命令行界面备份和恢复

Zimbra 备份和恢复过程可以作为 CLI 命令运行。

提供以下实用程序来创建备份计划、执行完整和增量备份、恢复邮件服务器或恢复 LDAP 服务器。

- **zmschedulebackup** 此命令用于安排完整备份、增量备份和删除旧备份。
  
- **zmbackup** 此命令执行 Zimbra Collaboration 邮箱服务器的完整或增量备份。  
此命令在实时服务器上运行,同时mailboxd进程和邮箱服务器正在运行。此命令还有一个选项,可以在不再需要旧备份时手动删除它们。
  
- **zmbackupabort** 此命令停止正在进行的完整备份。
- **zmbackupabort -r** 此命令停止正在进行的恢复。
- **zmbackupquery** 此命令列出有关正在进行和已完成的备份的信息,包括标签和日期。
  
- **zmrestore** 此命令将备份恢复到正在运行的 Zimbra Collaboration 邮箱服务器。
- **zmrestoreoffline** 此命令在mailboxd  
进程停止。
- **zmrestoreldap** 此命令恢复完整的 LDAP 目录服务器,包括帐户、域、服务器、COS 和其他数据。

有关每个命令的用法和定义,请参阅附录 A:命令行实用程序。

## 使用标准方法备份

启动备份时,您可以从正在备份的同一服务器发出命令,远程运行该命令并在命令行上指定目标服务器,或者使用管理控制台启动备份会话。

### 安排标准备份

当将标准备份配置为备份方法时,完整备份和增量备份条目将添加到 crontab 中。根据默认计划,完整备份计划于每周六凌晨 1:00 进行。增量备份计划于每周日至周五凌晨 1:00 进行。

默认情况下,超过一个月的备份将于每天晚上 12 点删除。

您可以使用zmschedulebackup命令或从管理 UI更改备份计划。

按如下方式指定字段,每个字段用空格分隔:

- 分钟 - 0 至 59
- 小时 - 0 至 23
- 月份中的日期 - 1 至 31
- 月 - 1 至 12
- 星期几 - 0 到 7 (0 或 7 表示星期日,或使用名称)

在未使用的字段中键入星号 (\*)。

## 例 27.

备份

选项

- 替换现有的完整备份、增量备份和删除备份计划。使用-R时,完整备份计划将被替换。如果使用此命令,请记住设置删除计划,如果  
您希望安排备份会话自动删除。此示例将替换现有的  
计划在周日凌晨 1 点运行完整备份,在周一至周五运行增量备份  
星期六凌晨 1 点,每天凌晨 12 点删除旧备份。

`zmschedulebackup -Rf "0 1 * * 7" i "0 1 * * 1-6" d 1m "0 0 * * *"`

重击

- 在当前计划中添加额外的完整备份时间。此示例在周四添加完整备份  
凌晨 1 点

`zmschedulebackup -Af 0 1 * * 4`

重击

- 检查您的备份计划。计划随即显示。

`zmschedulebackup -q`

重击

- 将计划命令保存到文本文件。这样,您可以在计划完成后轻松重新创建相同的计划。  
重新安装或升级

`zmschedulebackup -s`

重击

要将备份恢复到默认计划,请使用命令`zmschedulebackup -D`。

## 默认标准备份计划

默认备份计划的显示类似于以下示例:

### 默认备份计划<sup>28</sup>示例

0 1 \* \* 6 /opt/zimbra/bin/zmbbackup -f - 全部  
0 1 \* \* 0-5 /opt/zimbra/bin/zmbbackup -i  
0 0 \* \* \* /opt/zimbra/bin/zmbbackup -del 1m

重击

内容如下:

完整备份运行 上午 1 星期六

`0 1 * * 6 /opt/zimbra/bin/zmbbackup -f - 全部`

重击

增量备份从周日到周五运行 在 1

`0 1 * * 0-5 /opt/zimbra/bin/zmbbackup -i`

重击

备份会话 它们是在创建后一个月的午夜被删除的。

`0 0 * * * /opt/zimbra/bin/zmbbackup -del 1m`

重击

## 如何阅读 crontab

每个 crontab 条目包含六个字段,按以下顺序显示:

场地					
1	2	3	4	5	6
0	1	*	*	6	/opt/zimbra/bin/zmbackup -f -all

1. 分钟 (允许 0-59)
2. 小时 (0-23)
3. 月份中的日期 (1-31)
4. 月份 (1-12或名称)
5. 星期几 (0-7 或允许使用名称,其中 0 和 7 均代表星期日)
6. 要执行的字符串

星号字符起通配符的作用,代表字段的每次出现  
价值。

管理控制台:

主页→配置→全局设置→备份/恢复

您可以在管理控制台中添加其他收件人地址或更改通知电子邮件地址。

## 完整备份过程

完整备份过程通过以下步骤来备份邮箱、数据库、索引和

LDAP 目录:

1. 备份全局系统数据,包括系统表和localconfig.xml。
2. 遍历每个要备份的帐户并备份这些帐户的 LDAP 条目。
3. 将账户的邮箱置于维护模式,以暂时阻止邮件传递和用户对该邮箱的访问  
邮箱。
4. 备份邮箱。
  - a. 为与该邮箱相关的所有数据创建 MariaDB 转储。
  - b. 备份该邮箱的消息目录。
  - c. 创建该邮箱的索引目录的备份。
5. 将该帐户的邮箱返回到活动模式并转到下一个。
6. 备份LDAP目录。

完整备份通常是异步运行的。当您开始完整备份时,正在进行的备份的标签  
进程会立即显示。备份在后台继续。您可以使用zmbackupquery  
命令随时检查正在运行的备份的状态。

备份文件将保存为zip文件,无需压缩。要更改默认zip选项,请参阅附录 A:命令行实用程序, zmbbackup 部分。

## 增量备份过程

增量备份使用 CLI 命令 zmbbackup 运行。增量备份的过程如下:

1. 备份全局系统数据,包括系统表和localconfig.xml。
2. 遍历每个要备份的帐户并备份这些帐户的 LDAP 条目。
3. 将自上次备份以来创建的存档重做日志移动到<backup\_target>/redologs文件夹。

增量备份时少于一小时的归档日志将被复制到备份中,并且不会被删除。这些重做日志将在备份一小时后删除。间隔由localconfig键 backup\_archived\_redolog\_keep\_time设置。默认值为 3600 秒。

如果未找到此帐户的完整备份,则备份过程将对该帐户执行完整备份,即使只指定了增量备份。

4. 备份LDAP目录。

## 执行手动备份

使用zmbbackup命令执行以下备份操作:

- 对服务器 <1> 上的所有邮箱执行手动备份:

```
zmbbackup -f -s server1.domain.com -a all
```

- 自上次完整备份以来,对server1上的所有邮箱执行手动增量备份

```
zmbbackup -i -s server1.domain.com -a all
```

- 在server1上仅对user1 的邮箱执行手动完整备份

```
zmbbackup -f -s server1.domain.com -a user1@domain.com
```

## 删除备份会话

您可以按标签或日期删除备份会话。

- 按标签删除将删除该会话以及该会话之前的所有备份会话。
- 按日期删除会删除指定日期之前的所有备份会话。

例如, zmbbackup -del 7d删除超过 7 天的备份。您可以指定日 ( d )、月 ( m ) 或年 ( y )。

## 查找特定备份

每次完整备份或增量备份都是一个备份会话。

每个备份会话都标有日期和时间。例如,标签full-20210712.155951.123表示这是 2021 年 7 月 12 日 3:59:51.123 的备份。

会话标签中设置的时间为 GMT ,而非当地时间。使用 GMT 而非当地时间是为了在夏令时转换期间保持视觉顺序。

使用zmbackupquery命令查找完整备份会话。

- 要查找特定的完整备份会话：

```
zmbackupquery -lb full-20210712.155951.123
```

- 要查找自特定日期以来的完整备份会话：

```
zmbackupquery --type full --来自 2021/01/01 12:45:45
```

- 要在备份目录中查找所有完整备份会话：

```
zmbackupquery --type full
```

- 要找到恢复帐户的最佳时间点,请指定时间窗口

```
zmbackupquery -a user1@example.com --type full --从 “2021/07/05 12:01:15” --到 “2021/07/12 17:01:45”
```

如果备份会话在备份过程中因服务器崩溃而中断（未中止）,则中断的备份会话将保存为临时会话。临时备份会话放在<backup\_target>/sessions\_tmp文件夹中。您可以使用rm命令删除该目录。

## 中止正在进行的完整备份

- 在中止备份之前,您必须知道备份会话标签。此标签在zmbackup时显示首先启动。如果您不知道完整备份标签,请使用zmbackupquery查找标签。
- 使用zmbackupabort命令停止正在进行的备份。备份将立即停止,并且成为部分成功的备份。
  - 如果您知道标签名称,请停止备份

```
zmbackupabort -lb full-20210712.155951.123 -s server1
```

- 如果您不知道标签,请停止备份

```
zmbackupquery  
zmbackupabort -s server1 -lb full-20210712.155951.123
```

## 使用自动分组方法备份

自动分组备份方法可以从管理控制台或 CLI 配置。

管理控制台：

主页→配置→全局设置→备份/恢复

主页→配置→服务器→备份/恢复

服务器

## 从 CLI 配置自动分组备份

在全局配置中设置备份方法,如果您不希望特定服务器使用自动分组备份方法,则可以基于每个服务器覆盖配置。

要设置自动分组备份,可以使用 zmprov 命令修改 LDAP 属性:

```
zmprov mcf {ldap_attribute} {参数}
```

重击

您还可以使用zmprov ms {server\_name} {attribute}在服务器级别设置属性。

修改了以下 LDAP 属性:

- zimbraBackupMode 设置为自动分组。默认为自动分组。
- zimbraBackupAutoGroupedInterval 将其设置为备份会话应为组运行的间隔(以天或周为单位)。默认值为8d。备份间隔可以是1天或多天,输入为xd(例如1d);也可以是1周或多周,输入为xw(例如1w)。
- zimbraBackupAutoGroupedNumGroups 这是要分散邮箱的组数。默认值为7组。

## 安排自动组备份

自动组备份计划设置为默认模式,可以在管理 UI 或命令行中进行配置。

运行zmschedulebackup -D根据您的zimbraBackupAutoGroupedInterval设置设置自动分组备份的默认计划。

每个间隔备份一组。自动分组备份会根据服务器上邮箱数量的变化自动进行调整。每个备份会话都会备份以下内容:

- 所有从未备份过的邮箱。这些是新配置的邮箱。
- 所有未在计划备份天数内备份的邮箱。例如,如果计划备份运行超过六天,则将备份过去五天未备份的邮箱。
- 邮箱越多,越先备份最旧的邮箱。这样做是为了平衡每日自动分组备份负载。

例如,如果您将自动分组备份间隔配置为每日(1d),并将组数配置为7,则首次运行自动分组备份时,将备份所有帐户。初始备份后,第二天将再次运行自动分组备份。这次将再次备份新配置的帐户和接近总数七分之一的帐户百分比。首先备份日期最早的帐户。备份将继续备份新配置的帐户和七天内每天备份的大约七分之一的帐户。

备份共享消息时,如果代表消息的文件已经存在于备份中,它会将该对象标记为此类并且不会再次复制其内容。

备份文件将保存为zip文件,无需压缩。要更改默认zip选项,请参阅附录 A:命令行实用程序, zmbbackup部分。

这些备份文件可用于恢复整个 Zimbra Collaboration 系统或单个邮箱,以便完全恢复帐户和消息数据。存档的重做日志将作为完整备份的一部分移动到备份会话。当从自动分组备份恢复服务器时,将重播重做日志以使系统恢复到故障前的状态。

## 备份选项

可以配置备份过程以有选择地备份内容并备份 MariaDB 数据库。

### 备份内容选项

您可以配置这些备份选项,以便在完整备份会话期间不备份搜索索引、blob 和 SM blob。

- `zimbraBackupSkipSearchIndex` 默认值为FALSE。如果设置为TRUE,则不会备份搜索索引。从没有搜索索引的备份中恢复后,必须重新索引邮箱。
- `zimbraBackupSkipBlobs` 默认值为FALSE。如果将其设置为TRUE,则不会备份 blob。当 blob 驻留在容错存储中时,这可能有助于更快地备份数据库数据。此配置适用于所有 blob,包括主卷和辅助 (SM) 卷上的 blob。
- `zimbraBackupSkipHsmBlobs` 默认值为FALSE。如果设置为TRUE,则不会备份 SM 卷上的 blob。  
如果`zimbraBackupSkipBlobs`为FALSE但您想要跳过 SM 卷上的 blob,则设置此项。

## 备份MariaDB数据库

您可以配置 Zimbra Collaboration 备份以运行mysqldump来在备份会话期间备份您的 MariaDB 数据库。启用此功能后,mysqldump备份将随每次完整、增量和自动分组备份一起运行。

mysqldump是 MariaDB 数据库在特定时间的备份。转储文件之后发生的数据更改将写入二进制日志。要恢复到特定时间点,必须启用二进制日志记录。请参阅 Zimbra wiki 文章 MariaDB 备份和恢复,网址为[https://wiki.zimbra.com/wiki/MySQL\\_Backup\\_and\\_Restore](https://wiki.zimbra.com/wiki/MySQL_Backup_and_Restore)。

MariaDB 转储文件被压缩并放置在备份目标目录中,或者指定的/opt/zimbra/backup目录中。

,如果没有

这些文件可能非常大。请确保每个保存的 MariaDB 数据库备份文件的可用磁盘空间至少比实际 MariaDB 数据库文件大三倍。

- 启用mysqldump以使用备份自动运行,输入

```
zmlocalconfig mysql_backup_retention=<N>
```

N是保留的 MariaDB 数据库备份的副本数。

要恢复 MariaDB 数据库,请联系 Zimbra 支持寻求帮助。

## 管理备份的磁盘空间

如果目标磁盘空间不足,备份会话将失败。备份会话中备份的所有数据都将被丢弃和删除。

您可以选择在磁盘空间不足时接收通知来完成备份

配置zimbraBackupMinFreeSpace属性可通过通知您来帮助您管理正在运行的备份会话。

将属性zimbraBackupMinFreeSpace的值设置为运行备份会话之前备份目标磁盘上所需的可用空间量。如果磁盘空间小于属性中设置的值，则备份会话将不会运行，并向管理员发送电子邮件通知。

如果您还要备份 MariaDB 数据库,请确保将值设置得足够大以包含myslqdump文件大小。

该属性的值可以指定为总磁盘空间的百分比,例如25%的字节,例如允许启动300MB。

, 50GB , 等等。默认值为0 ,表示禁用检查,并且始终备份

, 或者作为数字

该属性可以全局设置或由服务器设置。

- 作为全球:

```
zmprov mcf zimbraBackupMinFreeSpace <值>
```

- 按服务器:

```
zmprov ms <zimbrahostname> zimbraBackupMinFreeSpace <值>
```

如果可用磁盘空间至少等于您设置的值,则备份会话将运行。如果备份文件大于该值,则备份会话将失败。您应该监视备份文件的大小,如果备份所需的空间大于配置的值,则调整属性值。

## 恢复数据

可以运行三种类型的恢复过程:

- zmrestore命令用于在 Zimbra Collaboration 邮箱服务器处于跑步。
- zmrestoreoffline命令用于在mailboxd进程刚刚停止时恢复邮箱服务器。此命令用于灾难恢复。
- zmrestoredap命令用于恢复LDAP目录服务器的内容。

恢复过程允许指定所有帐户或单个帐户。

### 恢复过程

zmrestore过程经过以下步骤来恢复邮箱、数据库、索引和 LDAP 目录。

- 1.检索要恢复的指定账户,或指定全部已备份的账户。

2. 遍历每个邮箱:

- a. 删除服务器上的邮箱以清除所有现有数据
- b. 恢复该 MariaDB 数据、索引目录和消息目录的最后一次完整备份邮箱

c. 重放自上次完整备份以来的所有增量备份中的重做日志

d. 从邮箱服务器上的重做日志存档区域重播该邮箱的所有存档重做日志

e. 重放当前重做日志

即使帐户超出配额,帐户也会恢复。下次用户执行  
影响配额的行动,他们会收到已超出配额的警告。

使用 Zimbra Connector for Microsoft Outlook 的用户必须在  
Zimbra 服务器恢复后登录时 Outlook 客户端。

## 示例

### 示例执行 29。

[→ 已满所有恢复帐户 server1](#) 在

包括上次完整备份以及自上次完整备份以来的任何增量备份

zmrestore -a 全部

重击

### 示例执行 30.a

单账户恢复server1

在

zmrestore -a account@company.com

重击

### 示例恢复到 31.a

具体时间点

(坑)

以下恢复选项会影响重做日志重放。如果您未指定其中一个选项,则所有重做日志

因为您要恢复的完整备份会被重播

执行以下任何时间点还原后,应立即运行  
对这些帐户进行完整的备份,以避免将来恢复这些帐户时出现问题。

使用以下任一选项运行的还原都是时间点还原:

- `-restoreToTime <arg>` - 重播重做日志直到指定的时间。
- `-restoreToIncrLabel <arg>` - 重播重做日志直至此增量备份并包括此增量备份。
- `-restoreToRedoSeq <arg>` - 重播至此重做日志序列并包括该序列。
- `-br` - 仅重放备份中的重做日志,因此不包括存档的和当前的重做日志  
系统。
- `-rf` - 仅恢复到完整备份。这根本不包括任何增量备份。

### 示例指定 32。

精确

增量备份标签、时间、

或者 要恢复到的重做日志顺序

如果指定了多个时间点还原选项,则还原将在最早的可能时间点停止。

zmrestore -a account@company.com-restoreToTime <arg>

重击

编写 <timearg> 的两种常见方式是

- “YYYY/MM/DD 时:分:秒”
- YYYYMMDD.hhmmss

示例 仅执行最[后完整备份的增量恢复,不包括此后的增量备份](#),至

zmrestore -rf -a 全部

[重击](#)

示例 恢复 34. 帐户的邮箱和 LDAP 数据

一个

zmrestore -ra -a account@company.com

[重击](#)

示例恢复到 35.a

新目标帐户

在原始帐户名称前添加前缀

zmrestore -ca -a account@company.com -pre 恢复

[重击](#)

上述示例的结果将是一个名为 restoreaccount@company.com 的帐户。

例 36.

恢复数据库 (db) 中的系统表和

本地配置文件

zmrestore-sys

[重击](#)

例如包括 37. 遇到。

--continueOnError

(-c )[恢复进程继续的命令,如果](#)

zmrestore -a 全部-c

[重击](#)

当指定-c时,在恢复过程中将显示无法恢复的帐户  
完全的。

例 38.

恢复

特定帐户

也可用于恢复已删除的帐户

zmrestore -a account@company.com

[重击](#)

示例 避免恢复[39](#)删除的帐户

[重击](#)`zmrestore -a account@company.com -skipDeletedAccounts`[示例恢复 40. a](#)[邮箱,但排除所有删除操作](#)[在 重做日志重放](#)

邮箱恢复后,它将包含已删除的邮件。如果用户使用 POP 和从服务器中删除消息

[重击](#)`zmrestore -a account@company.com --skipDeletes`

当请求最新的时间点时,不要添加备份标签 (-lb)。如果没有指定标签,请求点之前的最新完整备份将自动用作起点。

## 停止恢复过程

`zmbbackupabort -r`命令中断正在进行的恢复。恢复过程在当前帐户恢复完成。该命令会显示一条消息,显示哪些帐户未恢复。

要停止还原类型:

`zmbbackupabort -r`[重击](#)

## 当邮件服务器瘫痪时恢复邮箱

离线恢复过程只能在\$1`mailboxd`服务器未运行时运行。一般情况下,离线恢复在以下情况下运行:

- Zimbra 服务器的某些组件已损坏,服务器无法启动。例如,数据 LDAP 或数据库中的内容已损坏。
- 发生灾难时需要在服务器上重新安装 Zimbra 软件。

必须在启动 Zimbra Collaboration 邮箱存储服务器之前运行脱机还原,以保留重做按顺序记录。

在灾难恢复中,当重新安装 Zimbra 软件时,如果在备份文件之前启动了`mailboxd`恢复后,邮件服务器将开始接受电子邮件并执行其他活动,并在这个过程中。由于灾难发生前的数据还没有恢复到服务器,重做日志将会丢失序列。一旦`mailboxd`运行,恢复灾难前的数据就太晚了。

离线恢复过程经过以下步骤。

1. 检索要恢复的指定账户。如果命令行未指定任何邮箱地址,则从 Zimbra LDAP 目录服务器检索指定邮件主机上的所有邮箱列表。
2. 遍历每个邮箱:
  - a. 删除服务器上的邮箱以清除所有现有数据
  - b. 恢复该 MariaDB 数据、索引目录和消息目录的最后一次完整备份邮箱

c. 重放自上次完整备份以来的所有增量备份中的重做日志

d. 从邮箱服务器上的重做日志存档区域重播该邮箱的所有存档重做日志

e. 重放当前重做日志

### 恢复所有帐户

1. 当mailboxd停止时恢复server1上的所有账户

`zmrestoreoffline -a 全部`

重击

2. 离线恢复完成后启动mailboxd

`zmcontrol 启动`

重击

### 在实时系统上恢复个人账户

使用`zmrestore`命令恢复一个或多个选定的帐户。如果用户的邮箱出现已损坏,您可能需要从上次完整备份和增量备份集中恢复该用户。

1. 对于每个需要恢复的帐户,请将帐户置于维护模式

`zmprov ma <账户> zimbraAccountStatus 维护`

重击

维护模式可防止在恢复期间发送新电子邮件。否则,电子邮件将在恢复过程中被覆盖。

2. 运行`zmrestore`命令恢复账户

`zmrestore -a account@abc.com`

重击

3. 对于每个已恢复的帐户,将其重新置于活动模式

`zmprov ma <账户> zimbraAccountStatus 活动`

重击

如果用户帐户恢复后,分配给该帐户的 COS 不再存在,则会为该帐户分配默认 COS。

### 从还原中排除项目

从完整备份恢复时,您可以排除搜索索引和 blob。

- 搜索索引 如果不恢复搜索索引数据,则在恢复。

`zmrestore -a <全部帐户> --exclude-search-index`

重击

- Blobs当正在恢复的邮箱的所有 blob 都已存在时,这是一个有用的选项。

`zmrestore <全部或帐户>|--exclude-blobs`

重击

- HSM-blobs当正在恢复的邮箱的所有 SM blob 都已存在时,这很有用。

```
zmrestore <全部或帐户> --exclude-hsm-blobs
```

重击

## 恢复 LDAP 服务器

在需要恢复整个系统的灾难恢复中,请首先恢复 LDAP 目录服务器。

zmrestoredap命令可恢复全局 LDAP 数据,包括 COS、分发列表等。您可以恢复完整的 LDAP 服务器,这将重新创建整个架构,或者您可以恢复特定的帐户。您可以指定要恢复的会话。必须在要恢复的 LDAP 服务器上运行恢复命令。

### 示例

#### 示例 查找 LDAP 会话标签

[恢复默认设置](#)

重击

#### 完整 LDAP 服务器恢复示例

```
zmrestoredap -lb full20211130135236
```

重击

#### 示例 恢复特定账户的 LDAP 数据

```
zmrestoredap -lb full20211130135236 -a tac@abc.com jane@abc.com
```

重击

## 灾难恢复的一般步骤

使用以下步骤在涉及多台计算机的一般灾难场景中恢复邮箱存储服务器。

### 准备

1. 在对邮箱存储服务器进行任何操作之前,将 LDAP 目录服务器恢复到已知的良好状态。
2. 将所有邮箱置于维护模式,以在恢复邮箱时阻止邮件投递和用户登录。
3. 如果邮箱存储服务器正在运行,请停止它。

### 恢复

1. 如有必要,在邮箱服务器上重新安装 Zimbra Collaboration 软件。
2. 恢复邮箱。
3. 启动 Zimbra 协作服务器。
4. 将所有 Zimbra Collaboration 邮箱重新置于活动模式。
5. 运行服务器的完整备份。

### 崩溃恢复服务器启动

当系统意外停止并在启动时重新启动时,服务器会在重做日志中搜索未提交的事务并重放它发现的任何事务。重放重做日志使系统达到一致的状态。

## 恢复 Zimbra 协作

如果发生整台机器故障,请按照以下步骤恢复到新服务器。

您在新服务器上安装的 Zimbra Collaboration 版本必须与旧服务器上安装的版本相同。服务器可以有不同的操作系统。

新服务器硬件必须满足 Zimbra Collaboration 单服务器安装指南的安装前提条件部分中所述的要求。安装新操作系统,并按照安装指南中的说明进行任何必要的操作系统配置修改。

您可以执行以下操作来还原到新服务器:

1. 准备新服务器。
2. 使用防火墙规则阻止客户端访问旧服务器的 IP 地址。
3. 安装旧服务器上正在使用的所有卷。
4. 删除在 Zimbra Collaboration 初始安装中设置的 MariaDB 数据。
5. 将备份文件复制到新服务器。
6. 运行 `zmrestoredap` 恢复全局 LDAP 数据。
7. 运行 `zmrestoreoffline` 从备份会话中恢复帐户数据。
8. 准备并运行新的备份。

## 旧服务器状态

灾难恢复的两种情况是服务器已死,无法访问 Zimbra Collaboration 文件,或者 Zimbra Collaboration 仍在运行,但需要更换服务器硬件。

如果服务器未运行:

1. 使用防火墙规则阻止客户端访问服务器IP地址。
2. 找到要使用的最新完整 Zimbra Collaboration 备份会话。

如果服务器仍在运行,准备迁移到新服务器:

1. 使用防火墙规则阻止客户端访问服务器的 IP 地址。
2. 对旧服务进行完整备份,或者如果备份是最近的,则运行增量备份以获得最大当前增量备份会话。
3. 最后一次增量备份运行后应该,停止 Zimbra Collaboration。为了恢复到最新状态,没有新邮件会收到运行 `zmcontrol stop` 的消息。
4. 将旧服务器上的主机名和 IP 地址更改为其他内容。不要关闭服务器。

## 在新服务器上安装 Zimbra

开始之前,请确保新服务器已正确配置 IP 地址和主机名,并且 Zimbra Collaboration 已安装并配置了与旧服务器相同的域、主机名、密码等。有关准备服务器的更多信息,请参阅 Zimbra Collaboration 安装指南。在开始安装 Zimbra Collaboration 之前,请记下您需要从旧服务器获取的信息,包括管理员帐户名和密码、LDAP、Amavis 和 Postfix 密码、垃圾邮件培训和非垃圾邮件培训用户帐户名、确切域名以及全局文档帐户名。

确保计算机时间设置为与旧服务器相同的时间。验证旧主机名和 MX DNS 记录是否解析到新服务器。

1. 将 Zimbra Collaboration License.xml 文件复制到新服务器上的目录中。您无法完成  
如果许可证不在新服务器上，则安装 Zimbra Collaboration。
2. 运行./install.sh 并按照安装指南中的说明安装 Zimbra Collaboration。确保配置与旧服务器相同的域、主机名和密码。在 Zimbra Collaboration 安装期间，必须更改以下设置以匹配原始服务器设置：
  - a. Zimbra LDAP 服务器 对于要创建的域，请标识与旧服务器上相同的默认域。
  - b. Zimbra 邮箱服务器 自动创建管理员帐户。
    - 确保管理员用户创建的帐户名与原始服务器上的名称相同。
    - 将管理员密码设置为与旧服务器相同。
    - 将 LDAP 密码设置为与旧服务器上的密码相同。
    - 将 Postfix 用户和 Amavis 用户密码设置为与旧服务器上的相同
    - 将垃圾邮件训练用户和非垃圾邮件（HAM）训练用户帐户名更改为与旧服务器上的垃圾邮件帐户名相同。
  - c. 更改新服务器上的任何其他设置以匹配原始服务器上的配置。
  - d. 在主菜单中，设置默认备份计划和备份完成后服务器的自动启动  
配置完成就到 NO。

## 将备份还原到新服务器

### 1. 停止新服务器

zmcontrol 停止

重击

2. 如果旧服务器配置了额外的存储卷，请立即安装额外的卷。
3. 删除 MariaDB 数据并重新初始化一个空的数据目录。如果不这样做， zmrestoreoffline 将出现错误。以 zimbra 身份输入：

rm -rf /opt/zimbra/db/data/\* /opt/zimbra/libexec/zmmyinit

重击

MariaDB 服务现已运行。

4. 将 /backup 文件夹中的所有文件从旧服务器或存档位置复制到 /opt/zimbra/backup。
5. 恢复 LDAP。

zmrestoredap -lb <最新标签>

重击

如果要恢复大量帐户，您可以运行诸如 UNIX 命令 nohup 之类的命令，以便会话不会在恢复完成之前终止。

,

要查找要恢复的 LDAP 会话标签,请键入`zmrestoreldap -lbs`。

#### 6. 在尝试执行`zmrestoreoffline`之前,请确保以下服务正在运行。

- `mysqld` (MariaDB)
- `slapd` (OpenLDAP)

`zmcontrol start`

重击

#### 7. 在尝试执行`zmrestoreoffline`之前,请确保以下服务已停止。

- 邮箱

`zmmailboxdctl stop`

重击

由于此时某些 Zimbra Collaboration 服务正在运行,请输入`zmconvertctl start`。运行`zmrestoreoffline`之前必须执行此操作。

#### 1. 将您的 LDAP 密码从备份目录同步到新的生产服务器 LDAP 配置。

`zmlocalconfig -f -e zimbra_ldap_password=<密码>`

重击

#### 2. 停止`mailboxd`后开始离线恢复。

`zmmailboxdctl stop`  
`zmrestoreoffline -sys -a 全部 -c -br`

重击

您也可以在此处运行`nohup`等命令。要查看进度,请 `tail /opt/zimbra/log/mailbox.log`。

在命令行上使用`-c`以便恢复帐户,即使某些帐户在离线恢复过程中遇到错误。

#### 3. 由于此时某些 Zimbra Collaboration 服务正在运行,因此键入`zmcontrol stop`来停止所有服务。

#### 4. 删除所有旧的备份会话,因为这些会话不再有效。

`rm -rf /opt/zimbra/redolog/* /opt/zimbra/backup/*`

重击

#### 5. 启动 Zimbra 协作。

`zmcontrol start`

重击

#### 6. 运行完整备份。

`zmbackup-f-a全部`

重击

#### 7. 删除防火墙规则并允许客户端访问新服务器。

### 从不同的故障场景中恢复

对于您可能遇到的大多数服务器故障,恢复步骤都是相似的。如果发生故障,请查看灾难恢复部分以了解流程,然后按照以下步骤针对具体类型的故障进行操作。

## LDAP 损坏时恢复

1. 重新安装 LDAP 服务器。请参阅 Zimbra Collaboration 安装指南。
2. 找到要恢复的 LDAP 会话的标签。运行 `zmrestoredap -lb <label>` 命令, 不带  
用于恢复 LDAP 服务器的所有帐户、域、服务器、COS 等的参数。
3. 确保所有帐户都处于活动模式。在命令行中, 输入 `zmprov ma zimbraAccountStatus`  
积极的

## 替换损坏的分区后恢复

1. 如果分区损坏, 请更换故障磁盘。
2. 要恢复最新的完整和增量备份文件, 请运行

`zmrestore-a 全部`

重击

`zmrestore` 进程会自动检索从备份日期起指定邮件主机上的所有邮箱列表, 并遍历每个邮箱以将邮箱恢复到最后已知的良好状态。

## 重做日志损坏或无法读取后恢复

如果重做日志变得不可读, `mailboxd` 服务将停止并且无法重新启动。如果发生这种情况, 请检查硬件和软件以找出问题的根源, 然后再继续。

如果没有最新的重做日志, Zimbra 邮箱服务器就无法恢复到最新状态。Zimbra 邮箱数据可以恢复到最新的存档重做日志状态。Zimbra 邮箱服务器恢复后, 会为当前事务创建新的重做日志。

在开始之前, `mailboxd` 服务不能正在运行, 并且所有帐户必须处于维护模式。

1. 将所有帐户置于维护模式。

`zmprov md <域> zimbraDomainStatus 维护`

重击

2. 在 `mailboxd` 服务未运行时, 输入

恢复离线

重击

离线恢复过程首先从备份中检索指定邮件主机上的所有邮箱列表。

脱机还原将遍历每个邮箱以执行以下操作:

- 删除服务器上的邮箱
- 从备份区域恢复上次完整备份
- 按顺序恢复该邮箱自上次完整备份以来的所有增量备份。这涉及从备份目标区域重放重做日志
- 重放所有存档重做日志

由于当前事务的重做日志不可用, 邮箱服务器将返回到上次存档重做日志的状态。

3. 离线恢复完成后, 启动 Zimbra Collaboration 服务器。

重击

zmcontrol 启动

4. 当 Zimbra 邮箱服务器启动时,运行 Zimbra 服务器的完整备份。必须运行完整备份

立即备份最新的数据,因为最新的重做日志不可用。

## 恢复 Zimbra 后更改本地配置文件

localconfig.xml文件位于/opt/zimbra/conf文件夹中,包含核心 Zimbra 服务器配置,例如路径和密码。此文件以完整备份和增量备份的形式进行备份。运行增量或完整恢复时,localconfig.xml 的备份版本将重命名为localconfig.xml.restore ,并复制到/opt/zimbra/conf目录。

如果自上次备份以来进行了更改,则可能需要用恢复的副本替换localconfig.xml文件。比较这些文件,如果.restore文件具有最新的本地配置数据,则删除localconfig.xml文件并将带有.restore扩展名的文件重命名为localconfig.xml 。

## 使用快照备份和恢复

您可以使用存储层提供的快照功能来备份和恢复服务器,而不是使用 Zimbra 的备份和恢复功能。使用快照,您可以维护备用站点,并在主站点发生故障时将用户重新路由到备用站点以保持操作正常运行。

所有数据卷都会拍摄快照并定期传输到备用站点。使用快照备份的数据卷包括 MariaDB、blob、Lucene 索引和重做日志。

当主站点关闭时, zmplayredo命令用于使快照保持一致性并重新应用数据中的任何更改,以最大限度地减少卷间数据丢失

数据有四卷:

- 玛拉雅数据库
- 斑点
- Lucene 索引
- 红学家

每小时拍摄一组快照并将其传输到远程备用站点。但是,并不是所有快照都在同一时刻拍摄,而且可能相隔一秒到一分钟。此外,重做日志的快照拍摄频率可能更高。事件顺序可能如下所示:

8:00:00 - 快照 mysql 8:00:01 - 快照

blob 8:00:02 - 快照索引 8:00:03 - 快

照重做日志 8:05:00 - 将快照集传输到远

程站点已完成

...

8:15:00 - 快照重做日志 8:15:05 - 将重做日

志快照传输到远程站点已完成

...

8:30:00 - 快照重做日志 8:30:05 - 已完成将

重做日志快照传输到远程站点

...

8:35:00 - 主站点发生故障

在远程站点上,有来自 8:00 数据集的快照以及重做日志的后续快照。

必须将它们全部整合在一起,以便用户重新路由到备用站点后,可以在备用站点上获取最新的信息。

您现在可以运行zmplayredo命令来重播从 8:00:00 开始的更改。

`zmplayredo --fromTime 2021/10/17 08:00:00:000`

重击

所有数据都已调至当前时间,备用站点已设置并运行。8:30:00 至 8:35:00 之间的数据已丢失,但这是恢复过程中的预期结果。

## 关于短暂数据的说明

从 Zimbra Collaboration 8.8 开始,备份过程中不会备份临时数据。由于身份验证令牌是临时属性,这意味着在删除后恢复帐户的客户端将需要重新进行身份验证;备份之前生成的身份验证令牌将不再起作用。

## 临时存储 SSDB 后端

### 在 SSDB 中备份临时数据

如果使用 SSDB 作为临时后端,则备份将不包含任何临时属性。

注意:本节不详细介绍如何部署和管理 SSDB 服务器。有关该信息,请参阅SSDB 配置选项部分。

备份存储在 SSDB 中的数据 (如果这样配置)按如下方式进行:

`ssdb-dump -h localhost -p 8888 -o /tmp/ephemeral-backup-<日期>`

重击

注意:如果在主/从配置中运行,则ssdb-dump应该在主服务器上运行。

### 示例备份

重击

ssdb-dump - SSDB 备份命令版权所有 (c) 2012-2015

ssdb.io

接收开始... 已接收 1 个  
 条目 已接收 10 个条目 已接收 100  
 个条目 已接收 1000 个条目 已接收  
 10000 个条目 已接收 100000 个条目  
 已接收 200000 个条目 已接收 300000  
 个条目 已接收 400000 个条目 已接收  
 400021 个条目

接收结束

共转储 400021 条

压缩

级别 文件大小(MB) 时间(秒) 读取(MB) 写入(MB)

-----  
2 1 7 0 0 7

压缩数据...

压缩

级别 文件大小(MB) 时间(秒) 读取(MB) 写入(MB)

-----  
2 2 10 0 0 10

已备份至文件夹：/tmp/ephemeral-backup-&lt;date&gt;

## 将临时数据恢复到 SSDB

只能使用来自 SSDB 服务器的备份才能将临时数据从备份恢复到 SSDB。

可以通过以下两种方式之一进行恢复：

- 导入到正在运行的服务器
- 覆盖现有数据

## 导入到正在运行的服务器

使用SSDB 软件提供的leveldb-import命令可以将使用ssdb-dump命令创建的备份导入到正在运行的 SSDB 服务器中。

重击

leveldb-import localhost 8888 /tmp/ephemeral-backup-&lt;date&gt;/data

## 数据覆盖

- 停止 SSDB 服务器。
- 将之前使用ssdb-dump命令创建的目录复制到已知位置。
- 更新ssdb.conf配置文件,将work\_dir选项更新为正确的路径。
- 启动 SSDB 服务器并验证以前工作的登录是否仍然有效。

## 使用 LDAP 后端备份

如果临时后端是 LDAP，则备份将不包含身份验证令牌或 CSRF 令牌，但将包含上次登录时间戳。帐户恢复后，管理控制台中相应的“上次登录”值将被恢复。

## 从备份恢复到 Zimbra 10

NG 备份恢复实用程序将对已升级到 Zimbra 10 的客户有所帮助，Zimbra 10 现在具有原生备份和恢复功能。此实用程序可以读取现有的 NG 备份并恢复它们，为以前使用过 NG 备份的客户提供了一个有用的选项。

要使用 NG 备份恢复实用程序恢复备份，应在需要恢复备份的服务器上触发该实用程序。但是，在恢复备份之前，管理员应手动将备份文件夹从 NG 服务器上传到执行恢复的服务器。上传备份文件夹后，即可执行 NG 备份恢复实用程序来恢复备份数据。

“zmrestorengbackup”是一个单独的包，只能通过命令行访问。可以使用指令“apt-get install zimbra-restore-ngbackup”进行安装

### 迁移的目的

请注意，这不是用于恢复旧 NG 备份的通用恢复实用程序。此实用程序仅用于帮助组织进行审计和 BCP 测试。

不建议从旧的 NG 备份进行恢复以进行灾难恢复。

我们建议在 Zimbra Daffodil (v10) 安装完成后立即使用 Zimbra 备份功能进行完整备份。然后在灾难恢复时使用此完整备份（结合增量或自动分组备份）。

该实用程序可用于以下客户无法避免处理旧 NG 备份的用例：

- 大型组织、金融机构和政府客户有与备份旧电子邮件数据相关的合规性要求。这些要求来自进行法务会计的审计师。
- 许多中大型组织需要制定业务连续性计划 (BCP)。在 BCP 测试期间，根据适用于该公司的规定，可能需要恢复旧备份以检查电子邮件数据是否可访问。

请注意，恢复发生在单独的环境中（而不是生产环境中）。

### 句法

```
zmrestorengbackup --ngbkdir=文件名 [-itemstorecover={all|
{DOCUMENT MESSAGE}]} [--account={all|ACCOUNTS}] [--prefix=PREFIX]
```

重击

表 56. 选项

选项	简称	描述
目录	你	指定 NG Backup 解压目录的路径。此选项是必需的。

选项	简称	描述
itemstorecover itr		指定要从备份中恢复的项目。有效选项为“DOCUMENT”、“MESSAGE”或“ALL”。此选项是必需的。如果指定“ALL”，则将恢复“DOCUMENT”和“MESSAGE”。
帐户	-a	指定要恢复的帐户的电子邮件地址。可以提供多个电子邮件地址，以空格分隔。使用“all”可恢复所有帐户。此选项是必需的。
前缀	前	恢复到新的目标帐户。原始帐户名前面会添加前缀。例如：abc@test.com将恢复为<prefix>_abc@test.com这是可选的。如果没有指定，则将恢复原始帐户。

## 使用示例

- 恢复帐户a@test.com的电子邮件和文档以帐户名restore\_abc@test.com为前缀

```
`zmrestorengbackup -a abc@test.com -pre restore -itr 消息文档 -dir /opt/zimbra/mybackup/`
```

- 恢复帐户a@test.com的文档

```
`zmrestorengbackup -a abc@test.com -itr DOCUMENT -dir /opt/zimbra/mybackup/`
```

- 恢复帐户a@test.com 的电子邮件和文档（目前为全部 - 电子邮件、文档）以帐户名sample\_abc@test.com为前缀

```
`zmrestorengbackup -a abc@test.com -pre sample -itr all -dir /opt/zimbra/mybackup/`
```

## 先决条件

以下是执行迁移之前应满足的模块先决条件。请注意，这些先决条件可能不全面，并且可能需要根据特定服务器配置执行其他步骤

- 必须在 NG 服务器上对需要迁移的模块/数据进行备份。
- 必须手动将备份文件夹迁移/复制到将恢复备份的服务器。
- 备份文件夹必须设置正确的权限，以便恢复过程能够访问和读取备份文件。 - 恢复过程必须在安装模块并需要迁移的 Z10 服务器上执行。

## 迁移顺序

迁移需要遵循以下顺序：

- 需要在 Z10 服务器上安装恢复备份所需的实用程序。
- NG 服务器上进行的备份需要手动传输到 Z10 服务器。

- 备份文件夹应位于 Z10 服务器上 Zimbra 用户可以访问的目录中。备份文件夹的理想位置是 “/opt/zimbra/zxbackup”。
- 正在恢复的帐户的域应该存在于 Z10 服务器上。

## 委派管理

全局管理员可以创建不同的委派管理员角色。

委派管理员角色可以很简单,例如拥有管理一个或多个分发列表的权限,或者为一个或多个用户重置忘记的密码,使其拥有一个或多个域的域管理权限。

两个经常使用的委派管理员角色,域管理员和分发列表管理员,是已定义。您可以将管理员添加到这些预定义角色,无需进行其他配置。

## 授予管理权限的目标类型

委托管理提供了一种定义目标访问控制限制并授予权限的方法管理员对目标执行任务。

目标是可以授予权限的 Zimbra Collaboration 对象。每个目标都与一个目标类型相关联它标识您可以在目标上授予的访问控制条目的类型。

选择目标的目标类型时,请考虑以下几点:

- 目标**:您要向哪个特定目标授予权限?例如,如果您选择的目标类型是“域”,您指的是哪个域名?您指定一个特定域名(目标名称 = example.com)。访问控制条目(ACE)在该目标上被授予。ACE 存储在目标条目的 LDAP 属性中。
- 您要授予的权限是否适用于所选目标类型?权限只能应用于相关目标类型。例如,创建帐户只能应用于域目标类型,而设置密码只能应用于帐户和日历资源目标类型。如果在未授予权限的目标上授予权限,则适用于目标,则该授权将被忽略。
- 在定义权限时,需要考虑授予的权限有效的目标范围。例如例如,设置密码的权限仅适用于帐户和日历资源,但如果此权限包含在域目标权限列表中,对域内所有帐户或日历资源均有效。

### 权利目标57.

目标类型	目标范围描述
帐户	账户条目(特定用户)
日历资源	日历资源条目
操作系统	COS 入口
分发列表	包括分发列表以及此分发列表下的所有分发列表。  如果权限适用于帐户和日历资源,则所有帐户和作为此分发列表的直接或间接成员的日历资源。
领域	适用于特定域,不适用于任何子域。  子域必须明确标记为目标。  当域为目标时,将授予所有帐户、日历的权限域中的资源和分发列表。

目标类型	目标范围描述
配置	特定于全局配置的授权
全局 ACL	目标类型中所有条目的管理员权限。例如,您可以将 ACE 添加到全局访问控制列表 (ACL),以授予在域上创建帐户的权限。  被授予此权限的委派管理员帐户可以在系统中的所有域中创建帐户。
服务器	服务器入口
齐姆莱特	齐姆莱特入口

## 权利

权限是委派管理员可以或不可以对指定目标执行的功能。权限是系统定义的或在属性级别授予的。

### 系统定义的权利

系统定义的权利类型包括：

- 预设权限 (preset) 。例如createAccount创建一个账户； renameDomain , 重命名域。  
预设权限与固定目标类型相关联。例如， createAccount是仅在域上具有的权限； renameAccount是仅在帐户上具有的权限； getServer是仅在服务器上具有的权限  
不需要其他权利来管理对目标的操作。  
预设权限可能涉及访问多个目标。被授予者需要对所有相关目标拥有足够的权限。例如,要为帐户创建别名,被授予者必须拥有向帐户添加别名和在域上创建别名的权限。

### 属性权

在属性级别授予权限允许委派管理员/管理员组修改或查看（或者不修改或查看）目标上的特定属性。

属性权利的类型包括：

- 属性 ( setAttrs ) 权限允许域管理员修改和查看属性值。例如， modifyAccount权限允许域管理员修改帐户的所有属性。
- 获取属性权限 ( getAttrs ) 允许域管理员查看属性值。例如， getAccount权限显示用户帐户的所有属性。

在目标上配置授予的特定属性，并指定权限类型,读取（获取）或写入（设置）。

属性权限可以以任意属性组合的形式授予,以授予积极或消极权限。这可让您否定授予中的某些属性。

### 组合权利

连击权限可分配给任何目标类型,包括预设权限和属性权限。您可以使用连击权限快速授予目标多项属性权限。

## 消极权利

权利有积极权利和消极权利之分。消极权利是明确拒绝授予受让人的权利。

- 当向管理组授予负面权限时,该组内的所有管理员都无法对被授予该权限的目标和子目标行使该权限。
- 当向可能属于或不属于管理组的管理员授予负面权限时,特定管理员将被拒绝对被授予权限的目标和子目标行使该权限。

管理员组被授予域管理员权限,包括在 Domain1 上创建帐户的权限。

AdminA 属于此管理员组,但您希望 AdminA 拥有除创建帐户权限之外的所有域管理员权限。您可以在目标 Domain1 上向 AdminA 授予负面的createAccount权限。

对于同级别的授权,负面权限始终优先。例如,AdminGroup1 被授予查看域中帐户的正面权限;AdminGroup2 被授予查看同一域中帐户的负面权限。AdminA 是两个管理员组的成员。由于负面权限优先,因此 AdminA 无法查看此域中的任何帐户。

对于不同级别的授权,最具体的授权优先。例如,AdminA 被授予查看 GroupDistributionList1 中帐户的负面权限,User1 是该列表的成员。AdminA 还被授予直接查看 User1 帐户的正面权限。在这种情况下,AdminA 可以查看 User1 的帐户,因为帐户目标上的授权比分发列表上的授权更具体。

## 使用权限列表

系统权限在管理控制台概述窗格中的权限文件夹中列出并描述。您可以使用权限文件夹来帮助您定义要授予委派管理员哪些系统定义的权限。此文件夹显示权限的名称、与该权限相关的目标类型、权限类型和简要说明。

当您在页面上选择权限并点击时,另一个页面会显示更多信息:

- 对于组合权限,列出了与组合权限相关的权限列表。
- 对于其他系统权限,列出了与权限相关的属性列表

您可以使用zmprov命令来查看组合权限。

- 组合权利的直接子权利

```
zmprov gr adminConsoleDLRights
```

重击

- 组合的二级子权限

```
zmprov gr adminConsoleDLRights -e
```

重击

查看系统定义的权限列表

您可以使用zmprov命令查看系统为特定主题定义的权限:

使用 [zmprov 58 的表格](#)查看组合权限。

查看此内容	使用此zmprov命令
-------	-------------

查看此内容	使用此zmprov命令	
帐户	zmprov gar -t 帐户	重击
日历资源	zmprov gar -t calresource	重击
操作系统	zmprov gar -t cos	重击
分发列表[1]	zmprov gar -t dl	重击
1. 帐户和日历资源的所有权限也可授予分发列表目标。在分发列表上授予这些权限时，ACE 会将该权限应用于分发列表的所有直接或间接帐户或日历资源成员。		
领域	zmprov gar -t 域	重击
全局配置 [2]	zmprov gar -t config	重击
2. 还可以在域目标上授予所有帐户和日历资源的权限。还可以在域目标上授予所有分发列表的权限。在域上授予权限时,ACE 将权限应用于域中所有直接或间接帐户日历资源以及分发列表的成员。		
全球资助[3]	zmprov gar -t 全局	重击
3. 还可以在全局目标上授予所有其他目标的所有权限。在全局授权条目上授予任何权限,ACE 会将该权限应用于系统上的所有条目。例如,如果您在全局授权条目上向 AdminA 授予 createAccount (这是域权限),则 AdminA 可以在系统上的所有域中创建帐户。		
服务器	zmprov gar -t 服务器	重击
齐姆莱茨	zmprov gar -t zimlet	重击

## 实施委派管理

在创建委派管理员并授予权限之前,请定义角色以及要分配给管理员将管理的目标的权限。

为了更有效地管理委派管理员,请创建管理员组并将各个管理员帐户添加到该组。管理员组允许您创建基于角色的访问控制。

可以将具有相同或几乎相同职责的管理员分组到管理组中。

可以通过下列方法之一设置委派管理权限：

- 使用管理员向导创建管理员或管理员组并授予该帐户权限。
- 配置现有管理员帐户的授权。为现有委派管理员或管理员组帐户添加新权限或修改权限。
- 直接在目标的访问控制列表页面中添加、修改和删除权限。

## 管理员组和管理员

管理员和组管理员帐户是在管理控制台中创建的。

使用管理向导

1. 创建一个管理组或一个管理帐户。

a. 管理员组是已启用管理员组的分发列表 (DL), 将其标记为委派

管理员 DL。创建管理组管理员并配置其权限和管理视图后, 您可以将管理员用户帐户添加到管理组。

b. 管理员帐户是已在帐户上启用管理员权限的用户帐户。

2. 配置帐户的管理员视图。从直接分配的管理员视图列表中选择视图。管理员视图代表委派管理员登录管理控制台时看到的项目。

直接分配的管理员视图是在管理员帐户上设置的视图。继承的管理员视图是在帐户所属的管理员组上设置的视图。

3. 配置授权。授权对话框显示授权所需的列表, 以显示您在

直接分配的视图列。您可以接受这些权限并添加其他权限, 跳过此页面不配置这些权限, 或者单击“完成”接受这些权限并退出向导。

## 配置管理员帐户或管理员组的授权

您可以通过帐户工具栏上的“配置授权”链接管理授予管理员或管理员组的权限。单击“管理帐户地址”工具栏上的“配置授权”时, “内容”窗格将显示直接和继承的授权列表。您可以授予权限、修改权限或删除现有管理员帐户的权限。

## 向目标授予 ACL

当您想在目标上添加特定被授予者或特定权限时, 您可以直接编辑目标。每个目标都有一个 ACL 页面, 其中列出了授予的 ACL。您可以添加、编辑或删除目标的授予。管理帐户 (被授予者)会更新以反映更改。

## 撤销权利

全局管理员可以撤销授予管理员的任何权利。

主页→管理→账户

重击

打开所需的管理员帐户并单击配置授权。

1. 选择正确的撤销并点击删除。
2. 当对话框询问是否确定时, 单击“是”。

如果创建权限时启用了“可以授予其他管理员权限”,则委派管理员可以撤销权限。

### 暂时撤销委派的管理员权限

要暂时撤销委派管理员帐户的权限,您可以编辑管理员帐户并删除管理员字段旁边的复选标记。ACL 不会从帐户中删除。

## 查看授予管理员的权限

管理员帐户或管理员组帐户工具栏上的“查看权限”链接显示与特定目标相关的授予的权限、可读属性和可修改属性。单击选项卡可查看不同目标的权限。

## 授予预定义权限

可以为委派管理员分配常见任务的预定义权限。一个常见示例是创建只能重置密码的帮助台管理员。

主页→管理→账户→委派管理员

重击

以下常用权限已被预定义,并且计划在未来添加更多权限。

### 域管理员

当管理员被分配了域管理员预定义权限时,管理员可以访问管理域的管理员所需的所有常用功能。将此权限分配给用户相当于分配以下权限和视图:

- 指定的权利
  - 域名管理员权限
  - 获取域配额使用情况
- 指定视图
  - 账户列表视图
  - 下载查看
  - DLL列表视图
  - 别名ListView
  - resourceListView
  - domainListView
  - 证书查看
  - 保存搜索

### 重置密码

当管理员被分配了“重置密码”预定义权限时,管理员可以访问重置组织密码所需的所有常用功能。将此权限分配给用户相当于分配以下权限和视图:

- 指定的权利
  - 列表域

- 列出帐户
- 计数帐户
- 计数别名
- countCalendarResource
- 计数分发列表
- 列表分发列表
- 列表别名
- 更改账户密码
- 指定视图
  - 账户列表视图
  - 下载查看
  - DLL列表视图
  - 别名ListView
  - resourceListView
  - 保存搜索

### 编辑联系信息

当管理员被分配了“编辑联系信息”预定义权限时，管理员可以访问需要编辑用户联系信息的管理员所需的所有常用功能。将此权限分配给用户相当于分配以下权限和视图：

- 指定的权利
  - 列表域
  - 列出帐户
  - 计数帐户
  - 计数别名
  - countCalendarResource
  - 计数分发列表
  - 列表分发列表
  - 列表别名
  - 获取账户信息
  - 域名管理员控制台帐户联系标签权利
- 指定视图
  - 账户列表视图
  - 下载查看
  - DLL列表视图
  - 别名ListView
  - resourceListView

- 保存搜索

## 预定义委派管理员角色

将自动创建以下预配置的管理员组。您可以将管理员帐户分配给这些组。

### 域管理组

zimbradomainadmins委派管理组授予支持 Zimbra Collaboration 域管理（包括帐户、别名、分发列表和资源）所需的所有权利。

属于zimbradomainadmins组的管理员可以创建和管理账户，包括设置其域中的账户配额、别名、分发列表和资源账户。

当域管理员登录管理控制台时，只有他们被授权管理的功能才会显示在控制台的导航窗格上。

### 创建从 Zimbra Classic Web App 帐户到管理控制台的链接

对于域管理员，所有任务都从管理控制台执行。为了方便登录，当创建委派管理员帐户时，他们的 Classic Web App 帐户可以链接到管理控制台。

该链接是从zmprov CLI创建的

```
zmprov md {server.example.com} zimbraWebClientAdminReference {https://server.example.com:7071/}
```

BASH

此功能仅在经典 Web 应用程序中受支持。

### 分发列表管理组

zimbradadmin委派管理组授予登录管理控制台和管理分发列表所需的所有权限。

属于该组的管理员可以

- 查看账户列表
- 创建新的分发列表和删除分发列表
- 添加、编辑和删除通讯组列表中的成员

## 创建委派管理员角色

### 管理多个域

若要让一个域管理员管理多个域，请将管理各个域的权限分配给管理员帐户或管理员组。

例如，设置domainadministrator1@example.com管理 domainexample1.com 和 domainexample2.com。在要管理的其中一个域上创建一个新的管理员帐户。

1. 在要管理的其中一个域 (domainexample1.com) 上创建管理员账户

2. 选择域管理员管理域所需的视图。选择视图后,权限与这些视图相关的内容会自动显示在“配置授权”对话框中。
3. 如果此域的授权与您选择的视图相关的授权不同,请配置此域的授权。
4. 添加另一个需要管理的域 (domainexample2.com)。
  - 在配置资助页面上,单击添加
  - 选择目标类型为域
  - 输入目标的域名 (domainexample2.com)
  - 对于权利类型,选择系统定义的权利
  - 对于权限名称类型,应选择 adminConsoleAccountRights。应选择“是肯定权限”。
  - 单击“添加”和“更多”
  - 再次显示“添加 ACE”页面,其中“权限名称”字段为空。输入adminConsoleDLRights并单击添加及更多。
  - 继续添加以下正确名称:
    - adminConsoleAlias权限
    - 管理员控制台资源权限
    - 管理员控制台已保存搜索权限
    - 管理员控制台域权限
  - 完成最后一项权限后,单击“添加”和“完成”。配置授权对话框将显示与以下权限相关的权限目标域。如果您要添加另一个域进行管理,请单击添加和更多。重复步骤 4。如果如果不是,请单击完成。

## 管理分发列表

要分配用户来管理分发列表,请创建分发列表并启用管理员组,选择查看、授予分发列表权限、将用户添加到列表并使该用户成为管理员。

1. 创建新的分发列表:
  - 检查管理员组
  - 将将成为管理员的用户添加为 DL 的成员。
  - 转到管理员视图页面并检查分发列表视图,以便管理员可以查看分发列表。
  - 单击保存。
2. 在配置授权页面中,添加以下权限。

### 桌位权和9.

正确名称	目标类型	目标	正确的类型
以下权限允许管理员管理分发列表。			
列表分发列表	DL 电子邮件地址	DL 电子邮件地址	SD 右
添加分发列表别名	DL 电子邮件地址	DL 电子邮件地址	SD 右
添加分发列表成员	DL 电子邮件地址	DL 电子邮件地址	SD 右

正确名称	目标类型	目标	正确的类型
修改分发列表	DL 分发列表	DL 电子邮件地址	SD 右
获取分发列表成员		DL 电子邮件地址	SD 右
删除分发列表成员		DL 电子邮件地址	SD 右
此域权限显示用户帐户列表，管理员可以从中选择以添加到分发列表。			
列出帐户	领域	DL 电子邮件地址	SD 右

## 更改密码

要创建仅更改密码的委派管理员，请创建管理员或管理员组，选择并授予设置账号密码组合权限。

### 1. 选择以下视图

- 帐户列表视图可以选择要更改密码的帐户
- 别名列表视图可以找到使用别名而不是帐户名的用户。

### 2. 配置授权页面显示针对您选择的视图的推荐授权。对于更改密码权限，不要配置这些授权。选择跳过。单击添加以添加以下权限：

正确名称	目标类型	目标	正确的类型
设置账号密码	领域	域名	SD 右

## 查看邮件访问权限

可以授予帐户、域和分发列表上的查看邮件访问权限。

正确名称	目标类型	目标	正确的类型
管理员登录方式	帐户、域、dl	帐户、域或分发列表地址	SD 右[4]  4. 拒绝查看邮件 正中目标，勾选是 <b>否定权利（拒绝）</b>

为了防止管理员查看具有域或分发列表的帐户，请分配“为否定权限”到帐户。

## 管理分配给用户的权限类别

您可以扩展域管理员角色，以便查看和更改分配给域的服务类别 (COS)。

用户。若要添加管理域 COS 的权限，请为域管理员添加以下权限帐户或域管理员管理组。

为域中的每个 COS 添加系统定义的权限。

表 60. COS 的系统定义权限

正确名称	目标类型	目标	正确的类型
列表Cos	余弦	COS 名称	SD 右
获取Cos	余弦	COS 名称	SD 右
分配Cos	余弦	COS 名称	SD 右

该域权限在用户账户的常规信息页面中显示 COS 信息。

zimbraCOSid	领域	域名	属性权 动词:写 AR 目标:帐户
-------------	----	----	-------------------------

## 管理跨邮箱搜索

此角色创建一个委派管理员角色,可以运行“搜索邮件”工具来搜索邮件存档或实时帐户的邮件。这还允许管理员创建、中止、删除、清除或获取跨邮箱的状态搜索请求。

必须安装存档和发现功能才能使用此功能。

正确名称	目标类型	目标	正确的类型
adminConsoleCrossMailboxSearchRights (组合)		服务器名称 交叉邮箱 可以运行搜索	SD 右

为了实现完整功能,此角色包括创建新帐户的能力,以便管理员可以创建目标邮箱接收搜索结果。如果您不希望此角色具有创建帐户的能力,请授予同样遵循负面权利。

正确名称	目标类型	目标	正确的类型
创建账户	领域	域名	SD 右[5]  5. 否认创造 帐户权利 目标,勾选复选框 是否为负数 (否定)

如果您希望此管理员也能查看目标邮箱和跨邮箱搜索的结果,请授予权限仅查看该邮箱。

正确名称	目标类型	目标	正确的类型
管理员登录方式	帐户	跨邮箱搜索 目标帐户名	SD 右[6]  6. 拒绝查看邮件 正中目标， 勾选是 否定权利（拒绝）

## 管理 Zimlets

该角色创建一个委派管理员角色,可以创建、部署和查看 Zimlets。

正确名称	目标类型	目标	正确的类型
adminConsoleZimlet权利	服务器、域	服务器名称或 域名	SD 右
adminConsoleAccountsZimletsTabRights	服务器、域	服务器名称或 域名	SD 右

## 管理资源

此角色创建一个可以创建和管理资源的委派管理员。

正确名称	目标类型	目标	正确的类型
adminConsoleResourceRights组合		服务器名称或域 姓名	SD 右

## 访问已保存的搜索

此角色创建一个委派管理员,该管理员可以访问管理控制台中保存的所有搜索  
导航窗格,搜索部分。

正确名称	目标类型	目标	正确的类型
adminConsoleSavedSearchRights组合		服务器名称或域 姓名	SD 右

## 访问服务器状态页面

此角色可创建可访问服务器状态页面的委派管理员。除了授予此权限外，  
您还必须选择管理视图、全局服务器状态视图。

正确名称	目标类型	目标	正确的类型
adminConsoleServerStatusRights全局			SD 右

配置为全局管理员帐户的帐户无法被授予 ACL。全局管理员帐户自动拥有 Zimbra Collaboration 的全部权限。如果将 ACL 添加到全局管理员帐户，则会忽略该 ACL。如果将委派管理员帐户更改为全局管理员帐户，则会忽略与该帐户关联的任何 ACL。

## 聊天和视频

聊天和视频提供了一个一体化的集中式协作平台,具有高性能、低延迟和最低的管理员成本。

请注意,聊天和视频功能目前严格在云端运行。这些服务的任何数据都不会保存在本地;它们都存储在云服务器上。我们正在开发聊天和视频的本地版本。

## 安装

详细安装步骤请参考安装指南 ([https://zimbra.github.io/documentation/zimbra-10/single-server-install.html#\\_zimbra\\_chat\\_and\\_video](https://zimbra.github.io/documentation/zimbra-10/single-server-install.html#_zimbra_chat_and_video))。

## 聊天和视频云权限

完成所有安装和配置步骤后,将为您的默认域设置用户对聊天和视频 zimlet 的访问权限。访问管理也可以在服务等级 (COS) 和帐户级别进行。

请注意,由于聊天和视频 zimlet 在经典和现代 UI 中是分开存在的,因此需要对两个客户端分别采取管理步骤。

在 Zimbra 管理控制台中,Zimbra 聊天和视频 zimlet 可以像 COS 或帐户级别的任何其他 zimlet 一样进行管理。

## 聊天和视频许可

聊天和视频是网络版许可功能,需要有效的 Zimbra 许可证。它使用为

许可证属性 ZTalkAccountsLimit 限制访问此功能的用户数量。例如,如果在有效的 Zimbra 许可证中将 ZTalkAccountsLimit 的值设置为 50,则只有 50 个特定用户可以使用聊天和视频功能。管理员可以将帐户的 zimbraFeatureModernChatEnabled 属性设置为 TRUE

需要启用聊天和视频。

## 为用户启用聊天和视频

要为用户启用聊天和视频:

- 将用户帐户或 COS 或域的 zimbraFeatureModernChatEnabled 设置为 TRUE。请注意  
属性 zimbraFeatureModernChatEnabled 目前只能通过 CLI 访问。
- 要在经典 Web 应用中启用聊天和视频 UI,请为用户帐户或 COS 或域启用 zimlet com\_zimbra\_chat\_video (在管理控制台中)
- 要在现代 Web 应用中启用聊天和视频 UI,请启用 zimlet zimbra-zimlet-chat-video (在管理员中  
控制台)用于用户账户或 COS 或域

## 通过用户界面设置权限

首先使用您的管理员帐户登录 Zimbra 管理控制台 (ZAC)。

### 通过服务等级设置权限

1. 转到主页→配置→服务等级。
2. 从列表窗格中选择服务等级。
3. 从菜单栏中选择Zimlets。
4. 现在,您可以启用或禁用com\_zimbra\_chat\_video zimlet for Classic UI和/zimbra-zimlet-chat-video适用于现代 UI 的视频zimlet。

## 通过用户账户设置权限

1. 转到主页→管理→帐户。
- 2.从列表窗格中选择用户帐户。
- 3.从菜单栏中选择Zimlets。
4. 用户未默认设置为他们的COS,请选择限制此用户可用的 Zimlets 为：。
5. 然后,您可以启用或禁用com\_zimbra\_chat\_video` zimlet for Classic UI和/或zimbra-zimlet-适合现代用户界面的聊天视频zimlet。

## 通过命令行界面设置权限

您可以使用以下命令更改服务等级并查看 Zimlet 使用情况。

- 查看用法：

```
兹姆齐姆莱特特尔  
重击  
韋姆齐姆萊特克爾 acl
```

- COS 级别的权限

1. 首先,使用以下命令查看哪些 Zimlet 在哪些 COS 上可用：

```
zmzimletctl listZimlets  
重击
```

2. 使用以下内容向 COS 授予权限,将 “testcos”替换为适合 Classic UI 的值：

```
zmzimletctl acl com_zimbra_chat_video testcos 授予 zmprov fc cos zmzimletctl listZimlets  
重击
```

3. 使用以下内容向 COS 授予权限,将 “testcos”替换为 Modern UI 的适当值：

```
zmzimletctl acl zimbra-zimlet-chat-video testcos 授予 zmprov fc cos  
重击  
zmzimletctl listZimlets
```

4. 使用以下命令撤销 COS 的权限,同样将 “testcos”替换为适当的值

经典用户界面：

```
zmzimletctl acl com_zimbra_chat_video testcos 拒绝 zmprov fc cos zmzimletctl listZimlets  
重击
```

5. 使用以下命令撤销 COS 的权限,同样将 “testcos”替换为适当的值

现代用户界面：

```
zmzimletctl acl zimbra-zimlet-chat-video testcos 拒绝 zmprov fc cos  
重击  
zmzimletctl listZimlets
```

6. 请注意,对于上述两个步骤 ,zmprov fc cos 步骤都将刷新缓存。这可能会导致重新加载工作

您的实例,因此请在采取此步骤之前考虑性能需求和时间。

## 免费一对聊天

新的 1:1 聊天功能适用于所有 Zimbra Daffodil 客户。此功能允许无限数量的用户可以访问托管聊天，并可根据 Zimbra 的免费套餐许可进行聊天和视频。

## 入门

要使用 1:1 聊天功能，请确保您的域中启用了经典 (com\_zimbra\_chat\_video) 和现代 (Zimbra-zimlet-chat-video) zimlet，并且已正确配置 config.domains.json 和 config.properties（后配置）。域中至少应有两个用户具有聊天访问权限，并且在聊天 > 公司联系人下可见。

以下是与新的 1:1 聊天功能相关的 LDAP 属性：

- ZTalkAccountsLimit：此属性决定可以创建的聊天账户的最大数量。
- zimbraFeatureModernChatEnabled：此属性决定是否启用现代聊天功能。

	ZTalk 帐户限制 = 0	ZTalkAccountsLimit > 聊天用户数量	ZTalkAccountsLimit < 聊天用户数量
zimbraFeatureModernChatEnabled = 假	用户将看不到 聊天和视频选项	用户将看不到 聊天和视频选项	不适用
zimbraFeatureModernChatEnabled = 真	用户可以访问 免费 1:1 聊天，但不提供高级 功能	用户可以访问 全套聊天和 视频功能	用户可以访问 免费 1:1 聊天，但不提供高级 功能

## 聊天座位转移

如果 zimbraFeatureModernChatEnabled 设置为 TRUE (COS、域、帐户) 并且聊天用户数量等于 ZTalkAccountsLimit，那么当删除以前使用过聊天功能的用户的聊天帐户时，添加到域的新帐户将能够在登录网络邮件时看到具有完整功能的聊天和视频选项。

请注意，应正确配置这些属性以确保聊天功能正确运行。

## 特征

### 1:1 私人聊天

借助新的 1:1 聊天功能，您可以与同一域中的任何其他用户进行私人聊天。要开始聊天：

1. 登录您的 Zimbra 帐户。
2. 导航至聊天垂直部分。
3. 在联系人下，选择您想要与之聊天的用户。
4. 在右侧聊天窗格中，在文本输入字段中输入您的消息并发送。

### 在聊天中搜索

1:1 聊天功能允许您在选定的聊天中搜索。当您需要从聊天记录中查找特定信息时，此功能特别有用。要使用此功能：

1. 选择您要搜索的聊天记录。
2. 单击选定聊天标题中的放大镜图标。

3. 输入要搜索的字符串。

## 限制

请注意,在免费套餐许可下,存在一些限制:

- 网络上的 1:1 聊天视频会议被阻止:这意味着用户无法在 1:1 聊天期间开始视频会议。
- 网络上的群聊创建被阻止:用户无法创建新的群聊。
- 网络上的群聊访问被阻止:用户无法加入或访问群聊。
- 网络上的所有聊天搜索均被阻止:用户无法一次搜索所有聊天。
- 操作日志被阻止:您无法从管理视图查看操作日志。
- 不允许消息审核:用户无法执行消息审核。
- 存储 - 在免费套餐许可下,域的存储空间总计限制为 1GB。这包括在聊天中共享的所有文件。即使用完了 1GB 限制,用户仍可以继续使用聊天,但无法发送任何附件。
- 如果一家公司有 100 名员工,并决定购买 20 个高级聊天和视频许可证,那么登录电子邮件的前 20 名用户将自动启用高级功能。接下来的 80 名用户只能访问免费的 1:1 聊天。

包括::chat-video-on-prem.adoc[]

## 齐姆莱茨

Zimlets 是一种将 Zimbra 与不同的第三方应用程序集成的机制,旨在增强 Zimbra Classic Web App 的用户体验。借助 Zimlets,用户可以在电子邮件中查看信息并与第三方应用程序交互。通过修改服务类别 (COS),可以从 Zimbra Classic Web App 概览窗格向用户提供 Zimlets。

**经典 Web 应用程序仅列出经典的 zimlets。**

Zimbra 包含几个预定义的 Zimlet。您还可以创建 Zimlet 或从 Zimbra 网站上的 Zimlet Gallery 下载它们。

在管理控制台 → 主页 → 配置 → Zimlets 中,为现代 Web 应用开发的 zimlets 在描述中有(Modern)。

## 经典 Web 应用程序中的默认 zimlets

**经典 Web 应用程序仅列出**

启用预定义的 Zimlets 后,用户可以在 Classic Web App 中预览以下内容:

- 将鼠标悬停在日期或时间上,查看日历中的内容。
- 将鼠标悬停在姓名或电子邮件地址上即可查看该姓名的通讯簿详细信息。
- 右键单击电话号码即可使用软电话拨打电话。
- 右键单击日期即可安排会议。
- 右键单击姓名、地址或电话号码即可更新地址簿信息。

## 从管理控制台管理 Zimlets

以下 Zimlet 管理任务可从 Zimbra 管理控制台执行。

- 部署 Zimlet,在 LDAP 服务器中创建 Zimlet 条目,在服务器上安装 Zimlet 文件,启用 Zimlet 并使其可供默认 COS 的成员使用。
- 根据 COS 或帐户设置 Zimlet 可用或不可用。
- 强制使用 Zimlet。
- 禁用 Zimlet,将其留在服务器上,但 Zimlet 不会被使用。
- 取消部署 Zimlet,将其从 COS 列表和 Zimlets 列表中删除,但不会从服务器上卸载 Zimlet。

您无法从管理控制台卸载 Zimlet。

## 部署定制 Zimlets

您可以从 Zimbra 网站上的 Zimlet Gallery 下载和部署自定义 Zimlet。部署 Zimlet 后,默认 COS 中的每个人都可以立即使用它。如果 Zimlet 未直接部署到另一个 COS,COS 会显示 Zimlet,但不会启用它们。

管理控制台:

主页→配置→ Zimlets,从齿轮图标中选择部署

### 1. 浏览到您想要部署的 Zimlet,然后单击部署。

Zimlet 部署到服务器。系统会显示一个对话框,指示部署 Zimlet 的服务器名称,以及部署状态。

### 2.单击 “完成” 。

通过查看 Zimlets 页面来验证 Zimlet 是否已启用。

## 启用、禁用或强制使用 Zimlets

您可以启用、禁用或强制使用 Zimlets。您还可以使用切换功能选择是否安装 Zimlet 将提供给用户选择。

管理控制台：

主页→配置→服务等级→

操作系统 →齐姆莱茨

表 61. Zimlet 运行状态设置。

环境	描述
强制的	Zimlet 将始终在用户帐户中启用。用户不会在其 Zimlet 页面。
已禁用	Zimlet 不会立即供相关 COS 中的用户使用。
已启用	所有已部署的 Zimlets 都将被启用。

用户可以从其帐户的“首选项” → “Zimlets”页面启用或禁用可选的 Zimlets。如果您选择 Zimlet 作为强制性要求,用户无法禁用它。

## 取消部署 Zimlet

当 Zimlet 取消部署时,它会从所有 COS 中删除,然后从 LDAP 中删除。

管理控制台：

主页→配置→ Zimlets

### 1. 选择 齐姆莱特 取消部署。

### 2. 从齿轮图标菜单中选择取消部署。

### 3. 单击 “是”确认。

## 将允许代理的域添加到 Zimlet

代理允许域可让您配置哪些外部域可以通过 Zimlet 访问。对于 Zimbra 中包含的 Zimlet 已配置允许代理的域。如果您下载并部署其他 Zimlets,您可以添加额外的代理域名。

管理控制台：

主页→配置→服务等级

### 1. 选择 操作系统 进行编辑。

### 2. 在高级页面中,向下滚动到代理允许域部分。

3.单击添加域以添加域。

4.单击保存。

## 升级 Zimlet

使用与部署新 Zimlet 相同的步骤来升级自定义 Zimlet。新 Zimlet zip文件应与现有 Zimlet zip文件同名。

管理控制台：

主页→配置→Zimlets,从齿轮图标中选择部署

1. 勾选刷新 Zimlet 缓存,以便使用升级后的 zimlet。

2. 浏览至 齐姆莱特 您想要升级,然后单击部署。

3.单击“完成”。

## 从命令行界面管理 Zimlets

以下 Zimlet 管理任务可从命令行界面执行。

### 部署 Zimlets

当部署 Zimlet 时,它会立即供默认 COS 中的每个人使用。如果 Zimlet 未直接部署到另一个 COS,则 COS 会显示 Zimlet,但不会启用它们。

使用 CLI 部署 Zimlet,包括在部署之前修改 COS。

1. 选择一个 Zimlet 并将 Zimlet zip文件复制到Zimbra 服务器上的/tmp文件夹。

2. 以 zimbra 用户身份登录su - zimbra

3. 部署 Zimlet

zmzimletctl 部署 /tmp/<zimlet>.zip

重击

### 将代理允许域添加到 Zimlet

部署 Zimlet 时, Zimlet 可能会调用COS 属性zimbraProxyAllowedDomains来获取信息。必须为域名地址设置

要设置zimbraProxyAllowedDomains属性,请输入:

zmprov mc <COs 名称> +zimbraProxyAllowedDomains \*.example.com

重击

必须在 example.com之前添加\*。

这必须应用于所有启用了 Zimlet 的 COS。

### 部署 Zimlet 并授予 COS 访问权限

使用本节中的步骤将 Zimlet 部署到默认 COS 以外的一个或多个 COS:

1. 以 zimbra 用户身份登录:su - zimbra

2. 将 Zimlet 文件从 Gallery 复制到/tmp文件夹。

3. 将 Zimlet 安装到默认 COS:

重击

`zmzimletctl 部署 /tmp/<zimlet>.zip`

#### 4. 要将 zimlet 部署到其他 COS,请运行:

`zmzimletctl acl <zimletname> <cosname1> 授予`

重击

这将授予cosname1权限。您还可以在同一命令行上授予对多个 COS 的访问权限:

`zmzimletctl acl <zimletname> <cosname1> grant <cosname2> grant`

重击

#### 5. 要允许此 zimlet 使用允许的代理域,请在每个 COS 上运行以下命令并添加允许的域。

```
zmprov mc <CO$ 名称 1> +zimbraProxyAllowedDomains *.example.com
zmprov mc <CO$ 名称 2>
+zimbraProxyAllowedDomains *.example.com
```

重击

### 查看已安装的 Zimlet

使用`zmzimletctl`命令查看当前安装的 Zimlets:

`zmzimletctl listZimlets all`

重击

此命令的输出显示服务器上安装的、LDAP 中安装的以及 COS 可用的 Zimlet。

### 更改 Zimlet 配置

某些 Zimlets 在部署后可能需要额外的配置。

Zimlet 配置模板允许您在配置模板上进行更改,然后在 Zimbra 服务器上安装新的配置文件。

使用本节中的步骤更改 Zimlet 配置:

1. 提取配置模板:

`zmzimletctl getConfigTemplate <zimlet.zip>`

重击

2. 在模板中进行必要的更改,注意只更改所需的区域,然后保存文件。

如果您有多个自定义 Zimlet,请在更新 LDAP 中的配置之前重命名配置 `template.xml` 文件,以免文件被覆盖。

3. 使用`zmzimletctl`命令更新 LDAP 中的配置。如果您更改了配置模板,用新名称替换`config_template.xml`。

`zmzimletctl 配置 config_template.xml`

重击

### 升级 Zimlet

升级定制的 Zimlet 的步骤与部署新 Zimlet 的步骤相同。

新的 Zimlet zip文件的名称应与现有的 Zimlet zip文件的名称相同。

使用本节中的步骤升级 Zimlet:

1. 将 Zimlet zip文件复制到/opt/zimbra/zimlets-extra文件夹,替换旧版本。
2. 部署 Zimlet

`zmzimletctl deploy <zimlet.zip 文件名>`

重击

Zimlet 被复制到/opt/zimbra/zimlets-deployed文件夹。如果您的 Zimlet 包含.jsp文件,则.jsp文件也会被复制到/opt/zimbra/jetty/webapps/zimlet/<zimletnamefolder>。

3. 为了确保新版本的可用性,请刷新缓存:

`zmprov 刷新缓存 zimlet`

重击

## 使用 Zimbra 图库

您可以从 Zimbra 网站上的 Zimlet Gallery 下载并部署 Zimlets。请访问<https://www.zimbra.org/extend/>并从 Zimbra Gallery 部分滚动浏览扩展。

## 开发定制 Zimlets

要开发您自己的自定义 Zimlet,请参阅 Zimbra Wiki 上的 Zimlet 开发人员指南 (网址:<https://wiki.zimbra.com>)。

## 为现代 Web 应用配置 Zimlets

Zimlets 是增强 Modern Web App 功能的插件。您需要先配置和授权 Zimlets，然后才能将其与 Modern Web App 一起使用。

现代 Web 应用程序仅列出了现代 zimlets。

### 现代 Web 应用中的默认 zimlets

适用于现代 Web 应用程序的默认 Zimlets 允许用户执行以下任务：

- 从以前的备份中恢复联系人
- 为回复、转发或新电子邮件添加其他签名
- 从给定的内容中检测日期并在鼠标悬停时提供当天的事件列表
- 使用 Zimbra 作为渐进式 Web 应用程序 ([https://en.wikipedia.org/wiki/Progressive\\_web\\_application](https://en.wikipedia.org/wiki/Progressive_web_application))
- 订阅外部日历源
- 在设置中添加选项以更改 Zimbra 中的默认客户端



为现代 Web 应用开发的 Zimlets 在描述中有 (现代) 字样。

## 配置 LDAP

本节是配置 zm-oauth-social 所需 LDAP 属性的基本指南。假设您具有基本的 Zimbra Collaboration CLI 知识。

以下示例可作为配置所需 LDAP 属性的起点，以启用 zm-oauth 服务。

作为 Zimbra Collaboration 用户，这些属性可以像以下示例一样全局应用，或应用于特定域。

### 基本信息

#### 用户 OAuth 令牌配置的基本模板

zimbraOAuthConsumerRedirectUri 是应用程序在 oauth 流程中的中继（即社交媒体网站将向用户发送一次性使用代码以继续 oauth 流程）。LDAP 值的左侧部分必须与应用程序的白名单匹配。

```
zmprov mcf +zimbraOAuthConsumerRedirectUri https://<zimbra 主机名>:<端口>/service/extension/oauth2/
authenticate/<客户端>:<客户端>
```

zimbraOAuthConsumerCredentials 是应用程序的凭证，由社交媒体应用程序设置提供。除 Zoom 之外，所有客户端都可以省略 verify\_token。这些凭证将 oauth 流程与特定应用程序绑定。最终用户使用 clientId 来请求 oauth 代码，然后 Zimbra Collaboration 服务器同时使用 clientId + clientSecret 将该代码交换为 access\_token。

```
zmprov mcf +zimbraOAuthConsumerCredentials <客户端Id>:<客户端秘密>[:<验证令牌>]:
<客户端>
```

zimbraOAuthConsumerAPIScope 是应用程序针对指定的身份验证类型 (caldav、contact、noop) 所需的范围。这些范围决定了在 oauth 流程的社交媒体网站阶段向授权用户请求哪些权限。

```
zmprov mcf +zimbraOAuthConsumerAPIScope <范围><分隔符><范围><分隔符>。。。:<客户端>_<类型>
```

## 客户端示例

### Dropbox 示例

以下是 Dropbox 所需的配置。

```
zmprov mcf +zimbraOAuthConsumerRedirectUri https://  
your.mail.server.host.here/service/extension/oauth2/authenticate/dropbox:dropbox zmprov mcf  
+zimbraOAuthConsumerCredentials yourDropboxClientIdHere:yourDropboxClientSecretHere:dropbox
```

有关获取客户端 ID 和客户端密钥的说明,请参阅设置 Dropbox。

### Google 示例

以下是所需的基本谷歌配置。

```
zmprov mcf +zimbraOAuthConsumerRedirectUri https://  
your.mail.server.host.here/service/extension/oauth2/authenticate/google:google zmprov mcf +zimbraOAuthConsumerCredentials  
yourGoogleClientIdHere:yourGoogleClientSecretHere:google  
zmprov mcf +zimbraOAuthConsumerAPIScope https://www.googleapis.com/auth/  
drive:google_noop
```

有关获取客户端 ID 和客户端密钥的说明,请参阅设置 Google Drive。

### 微软示例

以下是所需的基本微软配置。

```
zmprov mcf +zimbraOAuthConsumerRedirectUri https://  
your.mail.server.host.here/service/extension/oauth2/authenticate/outlook:outlook zmprov mcf +zimbraOAuthConsumerCredentials  
yourMSClientIdHere:yourMSClientSecretHere:outlook zmprov mcf +zimbraOAuthConsumerAPIScope  
profile+User.Read+Files.ReadWrite.All:outlook_noop
```

请参阅设置 OneDrive 以获取有关获取客户端 ID 和客户端密钥的说明。

### Slack 示例

以下是 slack 所需的配置。仅当对 noop 范围执行授权时才应用范围。

```

zmprov mcf +zimbraOAuthConsumerRedirectUri https://
your.mail.server.host.here/service/extension/oauth2/authenticate/slack:slack zmprov mcf

+zimbraOAuthConsumerCredentials yourSlackClientIdHere:yourSlackClientSecretHere:slack
zmprov mcf
+zimbraOAuthConsumerAPIScope groups:write,team:read,users:read,users:read.email,chat:write,mpim:write:slack_noop

```

有关获取客户端 ID 和客户端密钥的说明,请参阅设置 Slack。

## 缩放示例

以下是 zoom 所需的配置。仅当对 noop 范围执行授权时才应用范围。

```

zmprov mcf +zimbraOAuthConsumerRedirectUri https://
your.mail.server.host.here/service/extension/oauth2/authenticate/zoom:zoom zmprov mcf

+zimbraOAuthConsumerCredentials yourZoomClientIdHere:yourZoomClientSecretHere:yourZoomVerificationTokenHere:zoom
zmprov mcf +zimbraOAuthConsumerAPIScope meeting:write:zoom_noop zmprov mc default
+zimbraProxyAllowedDomains api.zoom.us

```

上述代码块的最后一行允许 Zimbra Collaboration 代表默认服务类别 Zimbra Collaboration 帐户向 Zoom API 执行 Zoom zimlet 的代理请求。这对于 Zoom Zimlet 的基本操作是必要的。如果其他服务类别的用户应该有访问权限,则也可以将其应用于这些用户。

有关获取客户端 ID、客户端密钥和验证令牌的说明,请参阅设置 Zoom。

## 域配置

### 细节

配置单个域的凭据将覆盖从该域的全局配置继承的凭据。因此,如果全局和域应用之间的这些配置都应相同,则可以仅配置凭据,并允许域继承重定向 uri 和范围。

## Dropbox 示例

以下是在 Zimbra Collaboration 域 example.zimbra.com 上应用 Dropbox 应用程序凭据的示例,该凭据没有其他范围要求:

```

zmprov md example.zimbra.com +zimbraOAuthConsumerRedirectUri https://
your.mail.server.host.here/service/extension/oauth2/authenticate/dropbox:dropbox zmprov md example.zimbra.com
+zimbraOAuthConsumerCredentials
yourDropboxClientIdHere:yourDropboxClientSecretHere:dropbox

```

## 设置Dropbox

### 创建 Dropbox 应用程序

1. 访问 [Dropbox App Console](https://www.dropbox.com/developers/apps/) (<https://www.dropbox.com/developers/apps/>)
2. 选择创建应用程序。
3. 选择具有完全 Dropbox 访问权限的 Dropbox API,命名您的应用,然后单击创建应用。

4. 在 OAuth 2 部分中调整并配置以下重定向 URL:

- a. https://<主机名>/service/extension/oauth2/authenticate/dropbox
- b. https://<主机名>/@zimbra/service/extension/oauth2/authenticate/dropbox

5. 在选择器/保存器域部分调整并配置相关主机名。

6. 填写申请中的品牌信息和说明。

7. 单击启用其他用户,以便其他人可以授权该应用程序。

在 Zimbra Collaboration 1 中配置新的应用程序凭据。从“设置”选项卡获取应

用程序密钥和应用程序机密。

2. 请参阅配置 LDAP。

## 设置Google云端硬盘

创建 Google API 应用程序

1. 访问Google API 控制台 (<https://console.developers.google.com/>)。

2. 从顶部导航栏的项目下拉菜单中选择选择一个项目。

3.选择新项目。

4. 配置项目名称(以及可选的组织位置)。

5.选择 + 启用 API 和服务

6. 搜索 Google Drive,然后选择 Google Drive API。

7.选择启用。

8.选择 Google API 以返回 API 和服务菜单。

9.通过左侧导航菜单导航到 API 和服务部分:OAuth 同意屏幕。

10. 选择内部或外部应用类型,然后配置基本应用信息。

11. 选择添加范围,然后启用所有与 Google Drive 相关的范围。

12. 将您的邮件服务器主机添加为授权域。

13.选择保存。

14.通过左侧导航菜单导航到 API 和服务部分:凭证。

15.选择 + 创建凭证,然后选择 OAuth 客户端 ID。

16. 选择 Web 应用程序作为应用程序类型。

17.配置应用程序名称。

18. 在授权 JavaScript 来源下选择 + 添加 URI,然后调整并添加您的邮件服务器的主机名

(将“hostname”替换为您的 Zimbra Collaboration 服务器的公共主机名):

a. https://<主机名>

19. 在授权重定向 URI 下,选择 + 添加 URI,然后调整并添加以下重定向 URI (将“<hostname>”替换为您的 Zimbra 协作服务器的公共主机名):

a. https://<主机名>/service/extension/oauth2/authenticate/google

b. https://<主机名>/@zimbra/service/extension/oauth2/authenticate/google

20. 选择创建,然后复制客户端 ID 和客户端密钥。

在 Zimbra Collaboration 1 中配置新的应用程序凭据。从“设置”选项卡获取应用程序密钥和应用程序机密。

2. 请参阅配置 LDAP。

## 设置OneDrive

创建 Microsoft Azure 应用程序

1. 访问 Azure 门户 (<https://portal.azure.com/>)。
2. 搜索并选择应用程序注册。
3. 选择新注册。
4. 配置应用名称。
5. 在支持的帐户类型下,选择任何组织目录中的帐户和个人 Microsoft 帐户。
6. 调整并添加以下重定向 URL (将“<hostname>”替换为您的 Zimbra 的公共主机名协作服务器):
  - a. https://<主机名>/service/extension/oauth2/authenticate/outlook
7. 选择注册。
8. 通过左侧导航菜单导航到管理部分:身份验证。
9. 选择“添加 URI”,然后调整并添加以下重定向 URL (将“<hostname>”替换为公共 Zimbra 协作服务器的主机名),然后单击保存:
  - a. https://<主机名>/%40zimbra/service/extension/oauth2/authenticate/outlook
10. 通过左侧导航菜单导航到管理部分:API 权限。
11. 添加所需的 Microsoft Graph 委派权限,然后单击保存:
  - a. 电子邮件
  - b. offline\_access
  - c. openid
  - d. 简介

例如 Files.ReadWrite.All

  - f. 用户.读取
12. 通过左侧导航菜单导航到管理部分:证书和机密。
13. 选择新客户端密钥,添加描述,并且不设置过期时间。
14. 重复此任务,删除先前创建的条目,直到创建不带:的值(秘密不得出于兼容性原因,请包含冒号),然后单击“保存”。

在 Zimbra 中配置新的应用程序凭据

15. 通过左侧导航菜单的概述获取应用程序(客户端)ID,并通过左侧导航菜单的管理部分:证书和机密获取客户端机密。

在 Zimbra Collaboration 中配置新的应用程序凭据

1. 从“设置”选项卡获取App key和App Secret。
2. 请参阅配置 LDAP。

## 设置 Slack

创建 Slack 应用程序

1. 访问Slack 应用管理 (<https://api.slack.com/apps>)
2. 创建应用程序后,配置基本信息部分。
3. 通过左侧导航菜单导航到功能部分:OAuth 和权限。
4. 添加所需的机器人令牌范围:
  - a. 聊天:写
5. 添加所需的用户令牌范围:
  - a. 聊天:写
  - b. 群组:写入
  - c. mpim:写入
  - d. 团队:阅读
  - e. 用户:阅读
  - f. 用户:read.email
6. 调整并添加以下重定向 URL (将 “<hostname>” 替换为您的 Zimbra 协作服务器):
  - a. <https://<hostname>/service/extension/oauth2/authenticate/slack>
  - b. <https://<hostname>/@zimbra/service/extension/oauth2/authenticate/slack>
7. 在功能部分配置机器人名称:App Home。

在 Zimbra Collaboration 1 中配置新的应用程序凭据。从“设置”选项卡获取应用程序密钥和应用程序机密。

2. 请参阅配置 LDAP。

## 设置 Zoom

Zoom 应用市场最近已禁用 Zimbra 的 Zoom 集成。我们正在进一步评估此事,并将根据评估结论更新文档。

为了使 Zoom 与 Zimbra Collaboration 配合使用,服务器必须配置临时存储 (<https://wiki.zimbra.com/wiki/Ssdb>)。

创建 Zoom 应用程序

1. 以组织所有者或具有开发人员角色的组织账户的身份登录 Zoom。
2. 访问Zoom 应用管理 (<https://marketplace.zoom.us/user/build>)
3. 选择开发→构建应用→ OAuth → 创建
4. 配置应用程序名称,开启用户管理应用程序,保留发布意向,然后点击创建。
5. 通过左侧导航菜单导航到应用程序凭据部分。
6. 将以下重定向 URL 添加到生产部分 (将 “<hostname>” 替换为公共主机名您的 Zimbra 协作服务器):
  - a. <https://<hostname>/service/extension/oauth2/authenticate/slack>
  - b. <https://<hostname>/@zimbra/service/extension/oauth2/authenticate/slack>

a. `https://<hostname>/service/extension/oauth2/authenticate/zoom` 7. 添加以下白名单 URL (将“`<hostname>`”替换为您的 Zimbra 协作服务器的公共主机名) :

a. `https://<主机名>/service/extension/oauth2/authenticate/zoom`

b. `https://<主机名>/@zimbra/service/extension/oauth2/authenticate/zoom`

8. 通过左侧导航菜单导航到信息部分。

9. 配置取消授权通知端点 URL (将“`<hostname>`”替换为公共主机名您的 Zimbra 协作服务器):

a. `https://<主机名>/service/extension/oauth2/deauthorization/zoom`

10. 通过左侧导航菜单导航到范围部分。

11. 添加所需的范围:

a. 会议:写

b. 用户:阅读

12. 通过左侧导航菜单导航到提交部分。

13. 生成可发布的 URL,然后离开提交页面 (如果用于单个 Zoom 组织帐户,请不要提交该应用程序)。

在 Zimbra Collaboration 1 中配置新的应用程序凭据。从“设置”选项卡获取应用程序密钥和应用程序机密。

2. 请参阅配置 LDAP。

## 设置 NextCloud

为了便于理解这些步骤,我们将在整个部分中引用以下示例:

NextCloud 服务器 - `nextcloud.server.com`

Zimbra 服务器 - `myzimbra.server.com`

域名 - `example.com`

如果您已经设置了 NextCloud 服务器,则可以跳过步骤 1。

1. 按照此视频设置 NextCloud 服务器 - <https://www.youtube.com/watch?v=QXfsi0pwgYw>

2. 在 Zimbra Server 上安装 NextCloud zimlet 及其依赖项:

a. 要在 Red Hat 和 CentOS 上安装,请运行:

```
yum 安装 zimbra-zimlet-nextcloud
```

b. 要在 Ubuntu 上安装,请运行:

```
apt-get 安装 zimbra-zimlet-nextcloud
```

c. 重启zmmailbox服务器:

与 - zimbra  
zmmailboxdctl 重启

3. 在 NextCloud 服务器上,更新/etc/httpd/conf.d/nextcloud-ssl.conf中的以下配置

RewriteEngine 在  
RewriteCond %{HTTP:Authorization} ^(.\*)  
重写规则 .\* - [e=HTTP\_AUTHORIZATION:%1]

4. 登录 NextCloud 服务器网址https://nextcloud.server.com并导航至设置→管理→安全。

- a. 在暴力破解 IP 白名单部分,指定 Zimbra 服务器的 IP 范围。
- b. 在OAuth 2.0 客户端部分,指定 Zimbra 服务器的名称和重定向 URL。例如:

指定名称 我的 Zimbra 服务器

指定重定向 URL - https://myzimbra.server.com/service/extension/oauth2/authenticate/nextcloud

- c. 复制上面输入的客户端的客户端标识符和客户端密钥字段。这将用于更新 LDAP相关配置在下一步。

5. 为域启用 NextCloud                   示例.com       ,通过执行以下命令为其添加 LDAP 条目:

```
zmprov md example.com zimbraOAuthConsumerCredentials <客户端标识符>:<客户端  
秘密>:nextcloud  
zmprov md example.com zimbraOAuthConsumerRedirectUri https://  
myzimbra.server.com/service/extension/oauth2/authenticate/nextcloud:nextcloud zmprov md example.com zimbraOAuthConsumerAPIScope  
https://nextcloud.server.com/nextcloud/index.php:nextcloud_noop
```

zimbraOAuthConsumerAPIScope保存了 Nextcloud 实例的 URL,在我们的示例中,我们在 nextcloud.server.com 上的文件夹 /nextcloud 中设置了 Nextcloud。如果您的 Nextcloud 直接安装在域的根目录中,请确保使用

[https://nextcloud.server.com/index.php:nextcloud\\_noop](https://nextcloud.server.com/index.php:nextcloud_noop)

作为zimbraOAuthConsumerAPIScope。

如果您的 Zimbra 和 Nextcloud 位于不同的域上,例如zimbra.example.com和nextcloud.example.org,那么您必须禁用同一站点的 cookie 限制。执行以下命令:

```
zmlocalconfig -e zimbra_same_site_cookie=  
zmmailboxdctl 重启
```

在禁用同一站点 cookie 之前,请检查您组织的安全策略。

您的浏览器将缓存之前的 Cookie 设置。因此,请删除您的 Cookie 和站点数据,然后尝试再次访问 NextCloud。

## 设置 Jitsi 视频会议解决方案

Jitsi 是一种完全加密、100% 开源的视频会议解决方案。Jitsi 集成功能可在 Modern Web App 中使用,让最终用户直接在日历中设置视频会议;即只需单击按钮即可将 Jitsi 链接添加到会议邀请中,然后启动该视频会议。

管理员必须安装/启用 zimlet 并定义他们计划使用的视频服务器实例。

管理员可以部署自己的 Jitsi 视频服务器实例。即使管理员尚未设置 Jitsi 服务器实例,Jitsi 集成 zimlet 也可以使用 Jitsi 公开提供的免费视频会议解决方案为最终用户安排会议。

如果使用 Jitsi 公开提供的免费视频会议解决方案来设置活动,则无需更改配置。

1.在 Zimbra Server 上安装 Jitsi zimlet 及其依赖项:

a. 要在 Red Hat 或 CentOS 上安装,请运行:

百胜安装 zimbra-zimlet-jitsi

b. 要在 Ubuntu 上安装,请运行:

apt-get 安装 zimbra-zimlet-jitsi

c. 重启zmmailbox服务器:

与 - zimbra  
zmmailboxdctl 重启

## 为组织设置单独的 Jitsi 服务器

如果组织不打算使用 Jitsi 公开提供的免费视频会议解决方案,并希望设置自己的 Jitsi 服务器,则可以参考此设置指南 (<https://jitsi.github.io/handbook/docs/devops-guide/devops-guide-start>)\_\_\_\_\_

一旦设置了 Jitsi 服务器,就需要在 Zimbra 服务器上进行配置更改以更新组织的 Jitsi 服务器 URL。

在此示例中,我们将假定您组织的 Jitsi 服务器 URL 为<https://my-org-jitsi-server.com>。

1. 以下 CLI 命令需要以 zimbra 用户身份运行。

与 - zimbra

2. 转到/opt/zimbra/zimlets-deployed/zimbra-zimlet-jitsi。

3. 编辑config\_template.xml并更改 吉特网址 参数至<https://my-org-jitsi-server.com>。

4. 更新后文件中全局块的示例。

```
<zimletConfig 名称= zimbra-zimlet-jitsi 版本= 0.0.1 >
<全局> <属性
    名称= "jitsiUrl"> https://my-org-jitsi-server.com </属性> </全局> </zimletConfig>
```

5. 执行以下命令以应用更改:

```
zmzimletctl 配置 config_template.xml zmprov fc 全部
```

对于已经登录的用户,他们必须重新加载现代 UI 才能应用配置更改。

- 有关如何使用 Jitsi 集成 zimlet 的最终用户指南 - [https://zimbra.github.io/userguide/zcloud/userguide-zcloud.html#\\_jitsi](https://zimbra.github.io/userguide/zcloud/userguide-zcloud.html#_jitsi)

## 设置签名模板

签名模板 Zimlet 提供全局配置的电子邮件签名模板,用户可以使用它来配置自己的电子邮件签名。这样,组织中的所有用户都可以拥有统一的签名。

管理员必须安装 zimlet 并为用户启用它。

如果图像是 HTML,则它们应该位于不变的公共 URL 上,因为收件人会获取该 URL。

- 以下 CLI 命令需要以 zimbra 用户身份运行。

与 - zimbra

- 复制并粘贴以下配置文件至 /tmp/zimbra-zimlet-signature-template.xml :

```
<zimletConfig 名称= zimbra-zimlet-签名模板 版本= 0.0.1 >
<全局>
<属性
name= htmlTemplate >PGRpdj48c3BhbiBzdHlsZT0iY29sb3I6ICNlMDNlMmQ7lj48c3Ryb25nPk5BTUU8L3N0cm9uZ
z48L3NwYW4+PC9kaXY+PGRpdj48ZW0+PHNwYW4gc3R5bGU9ImNvbG95b mFjb3ltbG9nby0yMDE2LXJnYi5wbmcnPjwvaW1nPjwvZGl2Pgo=</属性>
```

```
</全局> </
zimletConfig>
```

- 使用base64解码器解码htmlTemplate值。

- 在htmlTemplate块中进行必要的更改。重新编码并将其粘贴到 /tmp/zimbra-zimlet-  
签名模板.xml

- 部署更改:

```
zmzimletctl 配置 /tmp/zimbra-zimlet-signature-template.xml
```

## 预防外出警报

Zimbra 中的预防性外出警报功能允许管理员配置组织内外出通知的可见性。默认情况下,该功能对同一域内的用户启用,但可以根据组织需求配置跨域可见性。

### 如何配置预防外出警报

#### 启用跨域可见性 (可选)

默认情况下,外出提醒功能仅限于同一域内的用户。要启用外出状态的跨域可见性,必须调整以下本地配置设置:

- 本地配置密钥: `get_out_of_office_cross_domains`
- 设置为true时 ,系统将允许用户检查其他域中收件人的外出状态 ,只要权限允许。

## 管理外部 OOO 通知

以下现有属性允许您控制如何处理外部域的外出通知:

- `zimbraPrefOutOfOfficeSuppressExternalReply` :设置为TRUE可防止将外出消息发送到外部域。设置为FALSE可将 OOO 消息发送到外部域,除非受到其他属性的限制。
- `zimbraInternalSendersDomain` :添加应被视为收件人“内部”的域。来自这些域的用户将显示外出通知。
- `zimbraPrefOutOfOfficeSpecificDomains` :指定哪些域可以接收外出回复。
- `zimbraPrefExternalSendersType` :控制哪些外部发件人接收外出回复。
- ALL :所有外部域。
- ALLNOTINAB :不在收件人地址簿中的外部用户。
- INAB :仅限收件人地址簿中的用户。
- INSD :特定领域。

## 自定义字体

自定义字体功能允许用户和管理员通过向自定义字体列表添加特定字体名称来个性化其电子邮件内容。此功能支持整个组织的一致品牌,同时允许各个用户使用他们喜欢的字体,前提是这些字体已安装在他们的系统本地。

### 自定义字体列表 (管理员)

- 管理员可以将特定字体的名称添加到 Zimbra 网络应用程序中的“自定义字体”列表中。
- 必须在每个用户的本地系统上安装这些字体才能在电子邮件编辑器中正确呈现。
- 如果用户系统上未安装自定义字体,它将以默认的字体呈现。

### 个人字体列表 (用户)

- 用户可以通过 Modern
- 列出的字体必须安装在用户的本地系统上才能在电子邮件编辑器中使用。
- 用户可以使用提供的输入字段输入字体名称并将其添加到他们的个人字体列表中。

### 在 Composer 中选择字体

- “自定义字体”和“我的个人字体”下列出的字体将出现在电子邮件中的字体选择菜单中作曲家。
- 如果用户的机器上没有安装字体,字体名称将出现在列表中,但将使用默认字体呈现。

- 用户可以使用添加到列表中的自定义字体创建电子邮件签名。

### 默认作曲家字体

- 用户可以通过导航至“设置”>“撰写电子邮件”>“撰写器”将自定义字体设置为电子邮件撰写器的默认字体。

### 已知限制

- 名称与 TinyMCE 默认字体匹配的字体可能会导致冲突。例如,如果自定义字体名称为“Mycustom == Roboto”,则在工具栏中选择“Mycustom”可能会错误地从字体菜单中选择“Roboto”。此行为与 TinyMCE 有关,并且超出了 Zimbra 的控制范围。

### 自定义字体配置

本节提供有关在 Zimbra Modern UI 中配置和使用自定义字体的说明。

### 如何在服务器上配置管理员定义的自定义字体

1. 使用 SSH 连接到 Zimbra 服务器。
2. 切换到 Zimbra 用户。
3. 导航到 /opt/zimbra/zimlets-deployed/zimbra-zimlet-custom-fonts 并打开 config\_template.xml 在编辑器中。
4. 按照 config\_template.xml 中提供的说明在 customFontsList 中设置自定义字体属性。根据需要修改 allowPersonalFonts 属性。如果将此属性设置为 false, 用户将不会在自定义字体设置中看到“我的个人字体”部分。
5. 对 config\_template.xml 进行更改后 , 运行以下命令：
  - a. zmzimletctl 配置 config\_template.xml
  - b. zmmailboxdctl 重启

## 附录 A:命令行实用程序

命令行界面 (CLI) 可用于创建、修改和删除 Zimbra Collaboration 的某些特性和功能。管理控制台是维护 Zimbra Collaboration 的主要工具,但某些功能只能通过 CLI 实用程序进行更改。

CLI 实用程序可用于以下目的：

- 配置帐户
- 备份和恢复
- 启动和停止服务
- 移动邮箱
- 跨邮箱搜索
- 安装自签名证书
- 本地配置

一般来说,应该从管理控制台执行帐户的配置和管理。

### 常规工具信息

Zimbra Collaboration 命令行实用程序遵循标准 UNIX 命令行约定。使用

遵循 CLI 的一般准则：

- CLI 命令以 zimbra 用户身份运行：  
与 - zimbra
- CLI 命令区分大小写。必须以小写形式输入。
- 键入命令后按ENTER。
- 要显示有关命令的使用信息,请键入带有-h的 CLI 命令。  
例如： zmprov -h列出zmprov实用程序可用的所有选项。
- 每个操作都通过命令行选项调用。许多操作都有长名称和短名称。例如,这两个命令是等效的：

zmprov 创建帐户 joe@domain.com test123

重击

zmprov 作为 joe@domain.com test123

### 语法约定

在演示每个工具的语法时,以下约定表示必需、可选和替代值：

- 大括号内的{ attribute } 是必填信息。
- 方括号中的[属性] 是可选参数或信息。
- { a|b|c } 或 [ a|b|c ] 选项由管道字符|分隔,表示 “a”或 “b”或 “c”
- 对于可能包含空格的属性名称,请用双引号将名称括起来。

## 命令行实用程序的位置

管理员可用的命令行工具都位于Zimbra 上的/opt/zimbra/bin文件夹中  
协作服务器。

## Zimbra CLI 命令

```
[zimbra@192.168.1.1 ~]$ cd /opt/zimbra/bin/
[zimbra@192.168.1.1 bin]$ ls
antispam-mysql      zmbackupquery    zmhostname        zmmetadump      zmschedulebackup
antispam-mysql.server zblobchk       zmhsms           zmmigrateattrs  zmschedulesmpolicy
antispam-mysqladmin  zmcaldebug     zmminnotop       zmmfilterctl   zmshutil
ldap                 zmcbadmin       zmitemdatafile  zmmtactl       zmskindeploy
mysql                zmcbpolicydctl zmjava           zmmypasswd    zmsoap
mysql.server         zmcertmgr      zmjavaext       zmmysqlstatus  zmspellctl
mysqladmin           zmclamdctl    zmldapasswd     zmmytop       zmsshkeygen
postconf             zmconfigdctl  zmldapupgrade   zmonlyofficectl zmstat-chart
postfix              zmcontactbackup zmlicense       zmopenkimctl  zmstat-chart-config
qshape               zmcontrol      zmlocalconfig  zmplayredo   zmstatctl
zmaccts              zmconvertctl  zmloggerctl    zmproxyconf   zmstorectl
zmamavisdctl        zmdedupe      zmlogerhostmap zmproxyctl    zmswatchctl
zmantispamctl       zmdevicesstats zmloginject    zmpurgeoldbox zmthrdump
zmantispamdbpasswd  zmdhparam     zmlogswatchctl zmpython      zmtlsctl
zmantivirusctl      zmdnscachectl zmdumpenv       zmmailbox     zmrabbitmqctl
zmapachectl          zmfixcalendtime zmfixcalprio   zmmailboxmove zmredodump
zmarchiveconfig      zmfreshclamctl zmgdutil       zmmailboxmovequery zmrestore
zmarchivectl         zmfixcalprio  zmmsearch      zmmailboxsearch zmrestoreoffline
zmarchivesearch      zmfreshclamctl zmmailschedule zmmdmmailschedule zms3config
zmauditswatchctl    zmgsautil     zmmemcachedctl zmsaslauthdctl zmvolume
zmbackup              zmactl       zmmemcachedctl zmsaslauthdctl zmzimletctl
```

下表列出了/opt/zimbra/bin中的 CLI 命令。

命令行界面	描述
反垃圾邮件-mysqladmin	反垃圾邮件 SQL 服务器管理实用程序
反垃圾邮件-mysql	反垃圾邮件 SQL 客户端
antispam-mysql.server启动、停止反垃圾邮件 SQL 实例	
LDAP 目录服务	
ldap搜索	启动、停止或查找 Zimbra LDAP 的状态
登录mysql管理员	在 LDAP 服务器上执行搜索
mysql	发送mysqladmin命令到记录器SQL实例
mysql.服务器	进入邮箱 SQL 实例的交互式命令行
mysql管理员	启动、停止邮箱SQL实例
后置配置	向邮箱 SQL 实例发送管理命令
后缀	Postfix 命令查看或修改 postfix 配置
形	启动、停止、重新加载、刷新、检查、升级-Postfix 的配置
	检查与时间和发送者/接收者域相关的后缀队列

命令行界面	描述
韓國	列出账户并提供域上的账户状态
茲马马维斯德特尔	启动、停止、重新启动或查找 Amavis-D New 的状态
密码	启动、停止、重新加载反垃圾邮件服务的状态
zmantivirusctl	启动、停止、重新加载、防病毒服务的状态
密码保护	更改反垃圾邮件 SQL 数据库密码
映射	启动、停止、重新加载或检查 Apache 服务的状态（进行拼写检查）
归档配置	查看、修改或配置存档的命令
归档	开始、停止、重新加载、存档状态
归档搜索	搜索帐户中的档案
审计工具	启动、停止、重新启动、重新加载审计监视的状态
备份	对指定邮件主机执行完整备份和增量备份。
备份失败	停止正在进行的备份。
zm备份查询	查找特定的完整备份集
茲姆布洛布克	检查 Zimbra blob 存储的一致性
计算校验	检查 Zimbra 日历中的约会和与会者的一致性
zmcbpolicydctl	如果已启用，则启动、停止和重新启动 cluebringer policyd 服务
配置dctl	MTA 配置守护进程的启动、停止、终止、重新启动状态。
管理中心	管理自签名证书和商业证书
韓國語言學家	启动、停止或查看 Clam AV 的状态
zmcleaniplanetics	清理 iPlanet ICS 日历文件
控制	启动、停止、重启 Zimbra 服务器的状态。还可以用来查找 Zimbra 安装版本
转换	启动、停止转换服务器或查找转换附件的状态 转换/索引
zmdevicesstats	每台服务器的唯一 ActiveSync 设备 ID 数量
工具	(获取设备数量)提供系统范围内的设备总数，无需指定单个服务器。
转储	显示有关服务器环境的一般信息

命令行界面	描述
zmgsutil	全局地址簿 (GAL) 同步实用程序。创建、删除 GAL 同步帐户并启动手动同步。
zm主机名	查找 Zimbra 服务器的主机名
韓國	SM 会话的开始、停止和状态。
数据文件	提取并打包Zimbra 用于 REST 导入/导出的tgz文件
龙	使用 Zimbra 特定的环境设置执行 Java
javaext	执行 Java 和 Zimbra 特定的环境设置,包括基于扩展的罐子。
zmldapppasswd	更改 LDAP 密码
许可协议	查看并安装您的 Zimbra 许可证
注射	测试工具
本地配置	用于设置或获取 Zimbra 服务器的本地配置
日志记录器	启动、停止、重新加载或查找 Zimbra 记录器服务的状态
zmloggerhostmap	用于手动将 DNS 主机名映射到 zmhostname。
日志记录器	启动、停止、监控日志记录的样本的状态。
邮箱	执行邮箱管理任务
邮箱邮箱dctl	启动、停止、重新加载或查找邮箱组件的状态 (zmmailboxd、MariaDB,转换)
搜尋工具	(跨邮箱搜索)跨邮箱搜索邮件和附件
zmmbox移动	7.1.3 及更高版本。用于将选定的邮箱从一个 Zimbra 服务器移动到另一个服务器。
zmmbox移动查询	7.1.3 及更高版本。用于查询服务器上正在进行的邮箱移动
zmpurgeoldmbox	7.1.3 及更高版本。邮箱移动后从旧服务器清除邮箱
韋姆克希德克	启动、停止和重新启动
元数据转储	以人类可读的形式转储项目元数据的支持工具
韋特克特	启动、停止和重新启动 Zimbra milter 服务器 (如果已启用)
韋姆塔配置dctl	从 Zimbra Collaboration 7.0 开始,不再使用此命令。使用 zmconfigdctl。
茲姆塔克特尔	启动、停止或查找 MTA 的状态
密码	更改 SQL 密码

命令行界面	描述
mysql状态	邮箱 SQL 实例的状态
nginxconf 配置文件	输出反向代理配置
zmnginxctl	启动、停止和重新启动 Zimbra 反向代理
zmplayredo	使用定期备份的快照执行数据恢复。使用快照备份和从备用站点恢复其信息使用此命令。
兹姆普罗夫	执行 Zimbra LDAP 中的所有配置任务,包括创建帐户、域、分发列表和别名
代理服务器	生成 nginx 代理的配置
zmproxyctl	启动、停止、重新启动和查找 IMAP 代理服务的状态
代理服务器	从一个或多个 memcached 服务器中清除 POP/IMAP 路由信息
python-1.1.1	能够编写访问 Zimbra Java 库的 Python 脚本。它设置 Zimbra 类路径并启动 Jython 解释器。
脏转储	用于转储重做日志文件内容以供调试的支持工具
校长	对指定邮件主机执行完全恢复和增量恢复
恢复ldap	从 LDAP 备份恢复帐户
恢复离线	(离线恢复)当 Zimbra 服务器 (即mailboxd 进程)已关闭
兹姆萨斯劳斯迪特尔	启动、停止或查看 saslauthd (身份验证) 的状态
备份	安排备份并将命令添加到你的 cron 表中
他把事情弄得一团糟	用于其他 zm 脚本,请勿使用
部署	部署皮肤
皂化物	以 SOAP 格式打印邮件、帐户和管理信息
拼写检查	启动、停止或查找拼写检查服务器的状态
密钥生成器	生成 Zimbra 的 SSH 加密密钥
zmstat 图表	根据目录中收集的 zmstat 数据生成图表
zmstat-图表配置	输出描述所收集数据当前状态的 XML 配置 从 zmstat-chart 生成管理控制台上的图表。
zmstatctl	启动、停止、检查状态或轮换 zmstat 数据收集器的日志
zmstorectl	启动、停止或查找 Zimbra 存储服务的状态

命令行界面	描述
zmwatchctl	启动、停止或查看 Swatch 进程的状态 ,用于监控
zmsyncreverseproxy	当详细模式开启时 ,解码同步请求/响应并记录它们在。
转储	启动线程转储并将数据保存到带有时间戳的文件中
兹米特斯特尔	将 Web 服务器模式设置为通信协议选项 :HTTP、HTTPS 或混合
兹姆特兰萨	用于训练反垃圾邮件过滤器识别垃圾邮件和普通邮件
更新	提供处理时区变化的机制
更新验证密钥	用于获取由zmsshkeygen创建的 ssh 加密密钥
体积	管理 Zimbra 邮箱服务器上的存储卷
兹姆齐姆莱特特尔	部署并配置 Zimlets
许可协议	管理 LDS 的各种操作。

## 在 CLI 中使用非 ASCII 字符

如果在 CLI 中使用非 ASCII 字符,为了使字符正确显示,必须更改此

在运行 CLI 命令之前,请将设置更改为所需的 UTF-8。要更改此设置,请键入

导出 LC\_All=<UTF\_locale>

zimbra 用户系统帐户的默认语言环境为 LANG=C。此设置对于启动 Zimbra 服务。更改默认 LANG=C 设置可能会导致性能问题使用 amavisd-new。

## zmprov (配置)

zmprov 工具执行 Zimbra LDAP 中的所有配置任务,包括创建帐户、别名、域、

COS、分发列表和日历资源。每个操作都通过命令行选项调用,每个选项

它有一个长名和一个短名。

语法是zmprov [cmd] [参数]。

修改的语法可以包含前缀 “+” 或 “-”,以便您可以更改受影响的属性,并

不需要重新输入未改变的属性。

- 使用+添加指定属性名称的新实例而不更改任何现有属性。

- 使用-删除属性的特定实例。

以下示例将向用户 1 添加值为 “blue”的属性zimbraZimletUserProperties ,并且

不会改变该属性的任何其他实例的值。

zmprov ma 用户 1 +zimbraZimletUserProperties “com\_company\_testing\_favoriteColor:blue”

重击

输入zmprov -h时,将列出 zmprov 可以使用的任务的属性。任务区域分为

以下部分:

长名称	简称	语法、示例和注释
- 帮助	-h	显示用法
- 文件	-f	使用文件作为输入流
- 服务器	-s	{host}[:{port}] 服务器主机名和可选端口
--ldap	-l	通过 LDAP 而不是 SOAP 进行配置
--logproperty文件	-L	log4j 属性文件,仅对-l有效
- 帐户名称]	-a	授权账户名
--密码 {密码}	-p	账户密码
--passfile {文件}	-P	从文件读取密码
--zadmin	-z	使用来自 localconfig 的 Zimbra 管理员名称/密码 管理员/密码
--authtoken {验证令牌}	-t	使用身份验证令牌字符串 (必须是 JSON 格式) 命令行
--authtoken文件 {authtoken 文件}	-T	使用来自 文件
--详细	-v	详细模式 (转储完整的异常堆栈跟踪)
- 调试	-d	调试模式 (转储 SOAP 消息)
- 掌握	-m	使用 LDAP 主控。这仅在使用-l时有效
- 代替	-r	允许替换安全保护的多值 localconfig 键中配置的属性 zmprov_saveguardedAttrs

这些命令按以下主题进行分类并简要描述:

- 账户配置命令
- 日历资源配置命令
- 空闲忙碌命令
- 域配置命令
- COS 配置命令
- 服务器配置命令
- 配置配置命令
- 分发列表配置命令

- 邮箱命令
- 日志命令
- 搜索命令
- 共享配置命令
- 统一通信服务命令
- IMAP/POP 代理命令

## 账户配置命令

表 62. 兹姆普罗夫 帐户配置命令

命令	句法	示例/注释
addAccountAlias( aaa ) { 名称@域名   编号   管理员名称 } { 别名@域名 }		zmprov aaa joe@domain.com joe.smith@engr.domain.com
检查密码强度 (cps)	{名称@域   ID} {密码}	zmprov cps joe@domain.com test123
		此命令不 检查密码使用期限或历 史。
创建帐户 (如) (光碟)	{名称@域} {密码} [属性1 值1]…	zmprov ca joe@domain.com test123 显示名称 JSmith
创建数据源 (光碟)	{名称@域} {ds 类型} {ds 名称} zimbraDataSourceEnabled {TRUE   FALSE} zimbraDataSourceFolderId {文件夹 ID} [属性 1 值 1 [属性 2 值 2]…]	
createIdentity (cid) {名称@域} {身份名称} [属性1 值1 [属性2 值2]…]		
创建签名 (蜗牛)	{名称@域名} {签名名称} [属性1 值1 [属性2 值2]…]	
删除账户 (da)	{名称@域名   id   管理员名称}	zmprov da joe@domain.com
删除数据源 (DDS)	{名称@域   id} {ds-名称   ds- ID}	
deleteIdentity (did) {名称@域名   id} {身份名称}		
删除签名 (签名)	{名称@域名   id} {签名名称}	
获取账户 (ga)	{名称@域名   id   管理员名称}	zmprov ga joe@domain.com

命令	句法	示例/注释
获取账户成员 (克)	{名称@域名 id}	
获取所有帐户 (gaa)	[ -v ] [ 域 ]	必须包含-l / --ldap  zmprov -l gaa zmprov -l gaa -v 域名.com  重击
获取所有管理员帐户 (充足的)		zmprov gaaa  重击
getDataSources (gds) {名称@域 id} [arg1 [arg2]…]		
获取身份 (gid)	{名称@域名 id} [参数1 [参数2]…]	
getSignatures (gsig) {名称@域 id} [arg1 [arg2]…]		
修改账户 (ma)	{名称@域名   id   管理员名称} [属性1 值1]…	zmprov ma joe@domain.com zimbraAccountStatus 维护  重击
修改数据源 (多发性硬化症)	{名称@域   id} {ds-名称   ds-id} [属性1 值1 [属性2 值2]…]	
修改身份 (mid) {名称@域   id} {身份名称}	[属性1 值1 [属性2 值2]…]	
修改签名 (消息)	{名称@域名   id} {签名名称}   签名 ID} [属性 1 值 1 [属性2 值2]…]	
删除账户别名 (RAA)	{名称@域名   id   管理员名称} {别名@域名}	zmprov 原始 joe@domain.com joe.smith@engr.domain.com  重击
重命名帐户 (ra)	{名称@域名   id} {新名称@域名}	zmprov ra joe@domain.com joe23@domain.com  重命名帐户后,您应该对该帐户运行完整备份  帐户。  BASH zmbackup -f -s <服务器名称.com> - a <新帐户名称@服务器名称.com>
setAccountCOS (sac)	{名称@域名   id   管理员名称} {cos 名称   cos id}	zmprov 包 joe@domain.com 现场技术员  重击

命令	句法	示例/注释
设置密码 (sp)	{名称@域名   id   管理员名称} {密码}	zmprov sp joe@domain.com test321  重击  密码不能 包括重音 字符串中的字符。 重音符号示例 不能的字符 使用:ã、é、í、ú、ü、ñ。

## 日历资源配置命令

表 63. 兹姆普罗夫 日历资源配置命令

命令	句法
创建日历资源 (ccr)	{名称@域} [属性1 值1 [属性2 值2]…]
删除日历资源 (dcr)	{名称@域名 id}
获取所有日历资源 (gacr)	[-v] [域]
获取日历资源 (gcr)	{名称@域名 id}
修改日历资源 (mcr)	{名称@域名   id} [属性1 值1 {属性2 值2}…]
purgeAccountCalendarCache (pacc)	{名称@域名} […]
重命名日历资源 (rcr)	{名称@域名   id} {新名称@域名}

## 空闲忙碌命令

表 64. 兹姆普罗夫 -自由的 忙碌的命令

命令	句法
获取所有Fbp (gafbp)	[-在]
获取空闲忙碌队列信息 (gfbqi)	[{提供商名称}]
推送空闲忙碌 (pfb)	{域名   账户 ID} [账户 ID…]
pushFreebusyDomain (pfbd)	{领域}
purgeFreebusyQueue (pfbg)	[{提供商名称}]

## 域配置命令

表 65. 兹姆普罗夫 域配置命令

命令	句法	示例/注释
计数帐户 (呼叫转移)	{域名 ID}	这列出了每个 COS、COS ID 和 分配给每个 COS 的账户数量

命令	句法	示例/注释
创建别名域 (计算机辅助设计)	{别名域名} {本地域- 名称   id} [属性1 值1 [属性2 值2]…]	
createDomain (cd) {域} [属性1 值1]…		zmprov cd mktng.domain.com zimbraAuthMech zimbra 重击
deleteDomain (dd) {域   id}		zmprov dd mktng.domain.com 重击
获取域名 (gd) (GDI)	{域名 ID}	zmprov gd mktng.domain.com 重击
获取域名信息 (哈德)	名称   ID   虚拟主机名 {值} [属性 1 [属性 2]…]	
获取所有域名 (哈德)	[在]	
修改域 (md) {域   id} [属性1 值1]…		zmprov md domain.com zimbraGalMax结果 500  请勿修改 zimbraDomainRenameInfo 手动。当域名  已重命名。
renameDomain (rd) {域   id} {新域}		renameDomain只能与zmprov 一起使 用 - 目录/-ldap

## COS 配置命令

表 66. 兹姆普罗夫 COS 配置命令

命令	句法	示例/注释
复制成本 (cpc)	{源 cos 名称   id} {目标 cos 名称}	
创建Cos (cc)	{名称} [属性1 值1]…	zmprov cc 执行官 zimbraAttachmentsBlocked FALSE zimbraAuthTokenLifetime 60 分钟 zimbraMailQuota 100M zimbraMailMessageLifetime 0 重击
删除Cos (dc)	{名称 ID}	zmprov dc 执行官 重击
获取Cos (gc)	{名称 ID}	zmprov gc 执行官 重击

命令	句法	示例/注释
获取所有 Cos (gac)	[ - 在]	zmprov gac-v 重击
修改Cos (mc)	{名称 id} [属性1 值1]…	zmprov mc 执行官 zimbraAttachmentsBlocked TRUE 重击
重命名Cos (rc)	{名称 id} {新名称}	zmprov rc 行政商务 重击

## 服务器配置命令

表 67. 兹姆普罗夫 服务器配置命令

命令	句法	示例/注释
创建服务器 (cs)	{名称} [属性1 值1]…	
删除服务器 (ds)	{名称 ID}	zmprov ds 域名.com 重击
获取服务器(gs)	{名称 ID}	zmprov gs 域名.com 重击
获取所有服务器 (来宾)	[ - 在]	锌矿气体 重击
修改服务器 (毫秒)	{名称 id} [属性1 值1]…	zmprov ms domain.com zimbra病毒定义更新频率 2小时 重击
获取所有 MtaAuthURL (步骤)		用于发布到saslauthd.conf中的内容 服务器应该用于saslauthd.conf MTA 认证
获取所有Memcached服务器 (游戏)		用于列出 memcached 服务器（用于 nginx 使用）。

## 配置配置命令

表 68. 兹姆普罗夫 配置配置命令

命令	句法	示例/注释
getAllConfig (gacf) [-v]		显示所有 LDAP 设置
获取配置 (gcf)	{姓名}	
修改配置 (mcf)	属性1 值1	修改 LDAP 设置。
创建XMPP组件 (csc)	{短名称} {域} {服务器} {类别名称} {类别} {类型} [属性1 值1 [属性2 值2]…]	
删除XMPP组件 (直方图)	{xmpp 组件名称}	
获取XMPP组件 (gxc)	{名称@域名} [属性1 [属性2]…]	

命令	句法	示例/注释
修改XMPP组件 (MXC)	{名称@域} [属性1 值1 [属性2 值2]…]	

**分发列表配置命令****表 69.** 兹姆普罗夫 -分配      **列表 配置命令**

命令	句法	示例/注释
createDistributionList (cdl) {列表@域}		zmprov cdl Needlepoint-list@domain.com 重击
添加分发列表成员 (Adm)	{列表@域名 id} {成员@域名}	zmprov adlm Needlepoint-list@domain.com songsh23@mail.free.net 重击
移除分发列表成员 (已读)	{列表@域名 id}	发送 rdlm Needlepoint-list@domain.com songsh23@mail.free.net 重击
获取所有分发列表 (加德尔)	[~在]	
获取分发列表成员 (GDL)	{名称@域名 id}	gdlm无法 用于体操 团体,作为动态 团体不能 嵌套。
获取分布列表 (gdl)	{列表@域名 id}	zmprov gdl list@domain.com 重击
修改分发列表 (mdl) {list@domain   id} attr1 值1 [属性2 值2]…		zmprov md list@domain.com 重击
deleteDistributionList (ddl) {list@domain   id}		
添加分发列表别名 (姓名)	{列表@域名 id} {别名@域名}	
删除分发列表别名 (rdla)	{列表@域名 id} {别名@域名}	
renameDistributionList (rdl) {list@domain   id}	{新名称@域名}	

**邮箱命令****表 70.** 兹姆普罗夫 邮箱命令

命令	句法	示例/注释
获取邮箱信息 (gmi)	{帐户}	

命令	句法	示例/注释
获取配额使用情况 (gqu)	{服务器}	
重新计算邮箱数量 (RMC)	{名称@域名   id}	当未读消息数和配额 使用情况与数据不同步 邮箱, 使用此命令 立即重新计算邮箱 配额使用情况和未读消息 数数。
reIndexMailbox (rim)	{名称@域名   id} {开始 状态   取消} [类型   id]…	重新计算信箱 配额使用情况和 消息计数应该 计划运行 非高峰时段和 在一个邮箱上使用 一次。
紧凑索引邮箱 (象征)	{名称@域名   id} {开始  地位}	
验证索引 (vi)	{名称@域名   id}	
获取索引统计信息 (gis)	{名称@域名   id}	
选择邮箱 (sm)	{account-name} [{zmmailbox 命令}]	
解锁邮箱 (ulm)	{名称@域名   id} [主机名]	仅指定主机名参数 在解锁邮箱失败后 移动试图。

## 其他配置命令

表 71. 兹姆普罗夫 其他配置命令

命令	句法	示例/注释
计数对象 (cto)	{类型} [-d {域   id}]	countObjects只能与 zmprov -l/-ldap
创建批量帐户 (散装)	{域} {名称掩码} {数量 要创建的帐户}	
描述 (描述)	[[-v] [-ni] [[条目类型]]]   [-一个 {属性名称}]	打印所有属性名称（帐户、 域名、COS、服务器等）。

命令	句法	示例/注释
刷新缓存 (fc)	<pre>[ -a ] {acl   区域设置  皮肤  uistrings   许可证   全部   帐户   配置   glo   balgrant   cos   域   galgroup   组   mime   服务器   zimlet   &lt;扩展缓存- 类型&gt;} [名称1   id1 [名称2   id2]…]</pre>	刷新某个类型的缓存 LDAP 条目。请参阅 Zimbra LDAP 服务。
生成域预授权密钥 (gdpak)	{域名 ID}	生成预认证密钥,以使受信任的第三方能够进行认证,从而实现单点登录。  与...结合使用 生成域预授权。
生成域预授权 (国内生产总值)	<pre>{域名 ID} {名称} {名称 ID} foreignPrincipal} {时间戳   0} {到期   0}</pre>	生成 preAuth 值以供比较。
同步加尔 (生病)	{域} [{令牌}]	
获取账户登录器 (加仑)	<pre>[ -s /--服务器主机名] {名称@域名 id}</pre>	

## 日志命令

表 72. 兹姆普罗夫 日志命令

命令	句法	示例/注释
添加账户记录器 (阿尔)	<pre>{名称@域名 id} {logging- 类别} {调试 信息 警告  错误}</pre>	为单个创建自定义日志帐户。
获取账户记录器 (加仑)	<pre>[ -s /--服务器主机名] {名称@域}   id} {日志类别} {调试  信息   警告   错误}</pre>	
获取所有帐户记录器 (加尔)	[ -s /--服务器主机名]	显示所有单独的自定义记录器帐户。
删除AccountLogger (拉尔)	<pre>[ -s /--服务器主机名] {名称@域名   id} {日志类别}</pre>	当指定 name@domain 时,删除为该帐户创建的自定义记录器,否则删除所有帐户系统中的帐户记录器。
resetAllLoggers (rlog)	[ -s /--服务器主机名]	此命令删除所有帐户记录器并重新加载/opt/zimbra/conf/log4j.properties。

请参阅zmprov 日志类别以获取日志类别列表。

## 搜索命令

**表 73.** 兹姆普罗夫 搜索命令

命令	句法	示例/注释
searchGAL (新加坡)	{域名}	zmprov sg joe
autoCompleteGal (acg)	{域名}	
搜索帐户 (位于)	[-v] {ldap 查询} [限制] [偏移] [按{属性}排序] [排序升序 0   1] [域 {领域}]	
搜索日历资源 (斯克尔)	[-v] 域 {属性操作值} [属性 关于价值]...	

**共享配置命令****表 74.** 兹姆普罗夫 共享配置命令

命令	句法	示例/注释
获取共享信息 (全球标准化协会)	{所有者名称   所有者 ID}	

**统一通信服务命令****表 75.** 兹姆普罗夫 统一通信服务命令

命令	句法	示例/注释
创建UCService (蠕虫)	{名称} [属性1 值1 [属性2 值2]…]	
删除UCService (公爵)	{名称 ID}	
获取所有 UC 服务 (高斯)	[在]	
获取UCService (胆量)	[e] {名称   ID} [属性1 [属性2]…]	
修改UCService (粘液)	{名称   id} [属性1 值1 [属性2 值2]…]	
重命名UCService (驴)	{名称 id} {新名称}	

**IMAP/POP 代理命令****表 76.** 兹姆普罗夫 IMAP/POP 代理命令

命令	示例/注释

命令	示例/注释
getAllReverseProxyURLs (garpu)用于将用于反向代理的服务器发布到 nginx.conf 中 代理查找。	
getAllReverseProxy 后端 (外衣)	返回具有 zimbraReverseProxyLookupTarget=TRUE。  指示邮箱服务器是否可用于查找来自 代理。
获取所有反向代理域 (加普德)	返回使用ZimbraSSLCertificate配置的所有域的列表 zimbraVirtualHostname和zimbraVirtualIPAddress已配置。这 允许代理配置要服务的域列表 定制/域名证书。

## 示例 使用 zmprov

示例创建 44。	带有 a 的帐户	默认密码为	操作系统
	zmprov ca 名称@域.com 密码		重击

示例创建 45。	带有 a 的帐户	分配给	指定的	操作系统
您必须知道 COS ID 号。要查找 COS ID：				
	zmprov gc <CO\$ 名称>			重击
	zmprov ca name@domain.com 密码 zimbraCOS cosIDnumberstring			

例 46.	创建	一个 密码内部验证时	不是
	zmprov as name@domain.com		重击

空的单引号是必需的，表示没有本地密码。

使用 47 的示例。	~批量创建账户
请参阅配置用户帐户以了解具体过程。	

批量配置示例 48.
请参阅 Zimbra 维基页面 <u>Bulk_Provisioning</u> ( <a href="https://wiki.zimbra.com/wiki/Bulk_Provisioning">https://wiki.zimbra.com/wiki/Bulk_Provisioning</a> ) 。

例如 49。	一个 帐户别名	一个

`zmprov aaa 帐户名称@域名.com 别名名称@域名.com`

重击

示例创建 50。

[分发列表](#)

`zmprov cdl listname@domain.com`

重击

返回分发列表的 ID。

例如加 51。

[aa会员分发列表至](#)

`zmprov adlm listname@domain.com member@domain.com`

重击



您可以从管理控制台将多个成员添加到列表中。

示例更改 52。

[管理员密码](#)

使用此命令可以更改任意密码。输入要更改密码的地址。

`zmprov sp admin@domain.com 密码`

重击

示例创建 53。

[根据 Zimbra LDAP 进行身份验证的域](#)

`zmprov cd marketing.domain.com zimbraAuthMech zimbra`

重击

默认域示例

[设置 54。](#)

`zmprov mcf zimbraDefaultDomain domain1.com`

重击

示例 列出所有及其属性值

[COS](#)

`zmprov gac-v`

重击

例 56.

[列出所有用户帐户](#)

[域名 \(domain.com\)](#)

`zmprov gaa domain.com`

重击

示例 列出所有及其配置

[用户账户 57.](#)

zmprov gaa -v 域名.com

重击

示例启用记录器 58。

在 **单身的** 服务器

zmprov ms server.com +zimbraServiceEnabled 记录器

重击

然后输入 zmloggerctl start,启动记录器。

示例查询 59。

**氨基多值属性的值**

zmprov gs server.com 属性=值

重击

例如, zmprov gs example.com zimbraServiceEnabled=ldap用于查明 ldap 服务是否启用。

例 60. **修改清除间隔**

要修改清除间隔,请将zimbraMailPurgeSleepInterval设置为服务器  
应该在每两个邮箱之间“休眠”。

zmprov ms server.com zimbraMailPurgeSleepInterval <Xm>

重击

X是邮箱清除的时间间隔; m代表分钟。您也可以将<xh>设置为小时。

例子 **61. 定制** **通知邮件**

修改zimbraNewMailNotification自定义通知邮件模板,发送默认邮件  
来自 Postmaster 通知用户他们已在另一个邮箱中收到邮件。要更改模板,  
修改接收邮箱账户。变量包括

- \${发件人地址}
- \${RECIPIENT\_ADDRESS}
- \${RECIPIENT\_DOMAIN}
- \${通知地址}
- \${主题}
- \${NEWLINE}

您可以指定上述哪些变量出现在电子邮件的主题、发件人或正文中。以下内容

例如,更改在以下位置收到的通知电子邮件正文中的消息的外观:

name@domain.com。您还可以更改服务类中的模板,使用zmprov mc 。命令为  
写在一行上。

重击

```
zmprov ma name@domain.com zimbraNewMailNotificationBody 来自的重要消息
${SENDER_ADDRESS}.${NEWLINE}主题:${SUBJECT}
```

例 62.

通过 COS 账户或

领域

重击

```
zmprov mc <默认> zimbraFeatureCalendarReminderDeviceEmailEnabled TRUE
zmprov ma <用户1> zimbraFeatureCalendarReminderDeviceEmailEnabled TRUE
zmprov md <域> zimbraFeatureCalendarReminderDeviceEmailEnabled TRUE
```

例 63.

启用活动流功能

COS 设置 a 或 的 用户

重击

```
zmprov mc <默认> zimbraFeaturePriorityInboxEnabled TRUE
zmprov ma <用户1> zimbraFeaturePriorityInboxEnabled TRUE
```

## 从 CLI 配置自动分组备份

在全局配置中设置备份方法，并且可以根据每个服务器覆盖配置，如果  
您不希望服务器使用自动分组备份方法。

要设置自动分组备份，可以使用 zmprov CLI 修改 LDAP 属性。输入以下命令：

```
zmprov mcf <ldap_attribute> <参数>
```

重击

您还可以使用 zmprov ms 在服务器级别设置属性。

修改了以下 LDAP 属性：

- zimbraBackupMode 设置为 Auto-Grouped。默认为 Standard。
- zimbraBackupAutoGroupedInterval 将其设置为备份间隔（以天或周为单位）  
会话应该为一个组运行。默认值为 `1d`。备份间隔可以是 1 天或多天，输入为 `xd`  
(`1d`)；或者 1 周或多周，输入为 `xw` (`1w`)。
- zimbraBackupAutoGroupedNumGroups 这是要分散邮箱的组数。默认值为 7  
组。

## 更改对话主题默认设置

消息可以按照共同线索分组到对话中。默认是将消息按线索分组到  
对话由参考标题决定。如果没有参考标题，则使用主题来确定  
对话线程。可以从 COS 或个人帐户更改默认选项。

```
zmprov mc [角色名称] zimbraMailThreadingAlgorithm [类型]
```

重击

类型包括：

- none 不执行任何对话线程。
- 主题 邮件将仅根据其规范化的主题进行线程化。

- **严格** 仅限线程消息标头（参考、回复、消息 ID 和重新发送消息 ID）  
用于关联消息。不执行规范化主题的检查。
- **引用** 与“严格”的逻辑相同，但约束略有改变，以便在线程消息时考虑非标准的线程索引标头，并且缺少引用和回复标头的回复消息将回退到使用基于主题的线程。
- **subjrefs** 与“引用”逻辑相同，但需要注意的是，规范化主题的更改将  
将线折成两半。

## 检测损坏的索引

运行 zmprov verifyIndex 作为指定邮箱索引的健全性检查。诊断信息写入 stdout。如果检测到问题，则返回失败状态。

verifyIndex 在运行时锁定索引，并检查索引中的每个字节。因此，它不是建议定期运行此命令，例如在 cron 作业中。应使用 zmprov verifyIndex 命令仅当需要做出诊断时才需要这样做。

`zmprov verifyIndex <user@example.com>`

重击

如果 verifyIndex 报告索引已损坏，您可以通过运行 reIndexMailbox 来修复邮箱索引（边缘）。

`zmprov rim <user@example.com> 开始`

重击

表 77. 兹姆普罗夫 日志类别

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

## 韓國

使用zmaccts运行一份报告,列出所有账户、其状态、创建时间以及上次创建时间  
任何登录的人。域摘要显示帐户总数及其状态。

## 句法

韓國

重击

## 归档配置

使用zmarchiveconfig配置存档邮箱。它有使用短命令或完整命令的选项  
导致执行相同功能的命令的名称。

## 句法

zmarchiveconfig [参数] [cmd] [cmd 参数]...

重击

## 描述

长名称	简称	描述
-帮助	-h	显示此命令的使用选项

长名称	简称	描述
- 服务器	-s	(主机)[:(端口)] 显示服务器主机名和可选端口
- 帐户	-一个	(name) 返回要设置的账户名的值已授权
--ldap	-l	允许通过 LDAP 提供存档功能
- 密码	-p	(pass)返回身份验证账户的密码
--密码文件	-P	(文件)允许从文件中读取密码
--zadmin	-和	允许从本地使用 Zimbra 管理员/密码
- 调试	-d	激活调试模式 (转储 SOAP 消息)
命令	...	
启用<帐户>		[存档地址 <aaddr> [存档 cos <cos>] [存档创建 <TRUE/FALSE>] [存档密码 <pa [zimbraAccountAttrName <存档属性值>]+
禁用<帐户>		

## 归档

使用zmarchivectl启动、停止、重新加载或检查 Zimbra 帐户存档的状态。

## 句法

zmarchivectl 开始|停止|重新加载|状态

重击

## 归档搜索

使用zmarchivesearch搜索帐户档案。您可以搜索符合特定条件的档案并将其保存到目录中。

## 句法

zmarchivesearch {-m <user@domain.com>} {-q <查询字符串>} {-o <偏移量>} [-l <限制>] [-d  
<输出目录>]

重击

## 描述

长名称	简称	描述
- 你	-d	<arg>写入消息的文件夹。如果没有指定，则只获取标题。文件名以RESULTNUM_ACCOUNT-ID_MAILITEMID形式生成
- 帮助	-h	显示帮助信息

长名称	简称	描述
-限制	-l	<arg>设置返回结果的数量限制。 默认值为 25
--mbox	-m	<arg>要搜索的存档帐户的名称
-抵消	-这	<arg>指定命中列表的开始位置。 默认为 0
-询问	-q	<arg>档案搜索的查询字符串
-服务器	-s	<arg>邮件服务器主机名。默认为 localhost
--详细	-v	允许在搜索过程中打印状态消息 正在被处决

示例搜索档案 64。

在 指定服务器并放置

→ 档案副本

指定目录

重击

zmarchivesearch -m user1@yourdomain.com -q in:sent -o 0 -l 30 -d /var/tmp

## 备份

使用zmbackup对指定邮件主机进行完整备份和增量备份。

此实用程序有短选项名称和全名。短选项前面有一个破折号,而全名选项前面带有双破折号。例如， -f与--fullBackup相同。

## 句法

-f之一 , -我 , 或必须指定-del 。

zmbackup {-f | -i | del} {-a &lt;参数&gt;} [选项]

重击

## 描述

长名称	简称	描述
-帐户	-一个	<arg>账户电子邮件地址,以白色分隔 空间或全部用于所有帐户。此选项不 自系统以来,已指定用于自动分组备份 知道每晚要备份哪些帐户。
-调试	-d	显示诊断信息以用于调试目的。
-删除	-的	<arg>删除包括以下备份以及之前的备份 指定标签、日期 (YYYY/MM/DD[-hh:mm:ss]) 或 周期 (nn(d   m   y))。
--排除斑点		从完整备份中排除 blob。如果未指定,请使用 服务器配置

长名称	简称	描述
--排除HsmBlobs		从完整备份中排除 SM 卷上的 blob;如果未指定,使用服务器配置
--排除搜索索引		从完整备份中排除搜索索引;如果未指定,使用服务器配置
--fullBackup	-f	开始完整备份。在自动分组备份模式下,此选项还会复制自上次备份 (这是增量备份的主要功能备份)。
- 帮助	-h	显示此命令的使用选项。
--增量备份	-i	启动增量备份。此选项不在自动分组备份模式下可用。
--includeBlobs		在完整备份中包含 blob。如果未指定,则使用服务器配置。
--includeHsmBlobs		在完整备份中包含 SM 卷上的 blob。如果这是未指定,则使用服务器配置。
--includeSearchIndex		在完整备份中包含搜索索引。如果未指定,则使用服务器配置。
--无Zip		将 blob 备份为单个文件,而不是zip 文件文件。
- 服务器	-s	<arg>邮件服务器主机名。格式可以使用以下任一方式普通主机名或 server.domain.com 名称。默认值为本地主机名。
--同步	-同步	同步运行完整备份。
- 目标	-t	<arg>指定目标备份位置。 默认是/opt/zimbra/backup。
- 拉链	-和	备份压缩的zip文件中的 blob。如果--,则忽略已指定zipStore。
--zipStore		备份zip文件中的 blob,无需压缩。 (默认)

## 示例

在这些示例中,服务器 (-s) 为server1.domain.com。如果目标是默认的,则不需要( -t )目录, (/opt/zimbra/backup)。

例 65.

履行

↑所有邮箱的完整备份

在 服务器1

```
zmbbackup -f -a all -s server1.domain.com
```

重击

例子 66. 执行所有邮箱的增量备份

server1自

上次完整备份

```
zmbbackup -i -a all -s server1.domain.com
```

重击

例 67. 仅对user1的邮箱server1进行完整备份。

在

```
zmbbackup -f -a 用户1@domain.com -s 服务器1
```

重击

如果使用帐户,主机名不需要完整的域。

例 68. 对user1的邮箱server1进行增量备份

在

```
zmbbackup -i -a user1@domain.com -s server1
```

重击

## 兹姆布洛布克

使用zmblobchk检查 Zimbra blob 存储 ( /opt/zimbra/store ) 的一致性。此命令检查并记录没有匹配数据库元数据的文件的注释。它还会检查以确保大小信息正确的文件。

### 句法

```
zmblobchk [选项] 开始
```

重击

需要使用 start 命令来避免意外运行 blob 检查。ID 值以逗号。

### 描述

长名称	简称	描述
--导出目录		<path> 数据库导出文件的目标目录。
- 帮助	-h	显示帮助信息
--邮箱	-m	<mailbox-ids> 指定要检查的邮箱。如果未指定,检查所有邮箱。
--缺失的 blob 删除-物品		删除所有缺少 blob 的项目。
--无出口		删除项目而不导出
--跳过大小检查		跳过 blob 大小检查

长名称	简称	描述
--意外的 blob 列表		<path> 将任何意外 blob 的路径写入文件
--详细	-v	显示详细输出;显示错误堆栈跟踪
--volumes		<volume-ids> 指定要检查的卷。如果没有指定,检查所有卷

## 计算校验

使用zmcalchk检查 Zimbra 日历上的约会一致性并发送电子邮件通知

解决不一致问题。例如,它会检查日历上活动的所有参与者和组织者是否同意会议的开始/结束时间和发生情况。

有关时间规格的详细信息,请参阅zmmailbox help appointment的输出。

## 句法

zmcalchk [-d] [-n <类型>] <用户> <开始时间规范> <结束时间规范>

重击

## 描述

简称	描述
-d	调试详细信息
-m	允许用户指定要检查的最大与会者人数。默认值为 50。
-n	<p>-n 无   用户   组织者   与会者   全部</p> <p>如果选定用户与预约不同步,则向其发送电子邮件通知</p>

## 备份

使用zmschedulebackup安排备份并将命令添加到您的 cron 表。

默认时间表如下:

- 完整备份,每周六凌晨 1:00 ( 0 1 \* \* 6 )
- 增量备份,周日至周五凌晨 1:00 ( 0 1 \* \* 0-5 )

每个 crontab 条目都是一行,由五个字段组成,每个字段之间用空格分隔。按如下方式指定字段:

- 分钟 - 0 至 59
- 小时 - 0 至 23
- 月日 - 1 至 31
- 月 - 1 至 12
- (星期几)0 到 7 (0 或 7 表示星期日,或使用名称)

在未使用的字段中键入星号 (\*)。

此命令自动将计划写入 crontab。

## 句法

```
zmschedulebackup {-q|-s|-A|-R|-F|-D}[f|d] [ 计划 ]
```

重击

## 描述

姓名	命令名称	描述
帮助	-h	显示此命令的使用选项。
询问	-q	默认命令。显示现有的 Zimbra 備份計劃。
节省	-s	保存时间表。允许您保存时间表命令到文本文件,以便您可以快速当系统恢復。
冲洗	-F	删除当前计划并取消所有預定備份。
附加	一个	在当前备份中添加额外的指定备份日程。
代替	-R	用指定的计划替换当前计划日程。
默认	-D	用默认计划替换当前计划日程。
将传递给 zmbackup 的选项		
无压缩	-n	将 blob 备份为单个文件,而不是zip 文件文件
压缩	-和	备份压缩的zip文件中的 blob。如果--,则忽略已指定zipStore。
--zipStore		备份zip文件中的 blob (无需压缩)。
目标	-t	只能用于指定后卫目标位置。默认为/opt/zimbra/backup。  您不能指定目标增量备份。如果目标 (-t )位置被添加用于增量计划的备份,则会被忽略。
帐户	一个	特定于帐户。默认为所有帐户。
--邮件报告		向管理员用户发送电子邮件报告。

姓名	命令名称	描述
- 服务器		server - 邮件服务器主机名。默认为 localhost。
--同步		同步运行完整备份。
--排除Blob		从完整备份中排除 blob。如果未指定，服务器使用了配置。
--includeBlobs		在完整备份中包含 blob。如果未指定，则服务器使用了配置。
--excludeHsmBlobs		从完整备份中排除 SM 卷上的 blob。如果未指定，则使用服务器配置。
--includeHsmBlobs		在完整备份中包含 SM 卷上的 blob。如果未指定，则使用服务器配置。
--排除搜索索引		从完整备份中排除搜索索引。如果未指定，使用服务器配置。
--includeSearchIndex		在完整备份中包含搜索索引。如果未指定，则使用服务器配置。

Cron 计划- 备份类型:&lt;i | f | d arg&gt;

增量备份	i	<时间说明符>增量备份。 增量备份不与自动分组一起使用 备份模式。
完整备份	f	完整备份
删除	d <参数>	删除备份。<arg>是n(d   m   y)

## 备份计划示例

例 69. 安排默认完整备份和增量备份

```
zmschedulebackup -D
```

重击

示例 将现有的时间表替换为 70。

→ 新时间表

```
zmschedulebackup -R f[ 计划 ]
```

重击

例如添加 71。

一个额外的完整备份

到 现有时间表

```
zmschedulebackup -Af[ 计划 ]
```

重击

[例如添加 72。](#)[一个额外的增量备份](#)[到现有时间表](#)

zmschedulebackup -A i [ 计划 ]

重击

[示例 显示现有的时间表](#)

zmschedulebackup -q

重击

[示例显示计划 74。](#)[— 线](#)

将计划以命令的形式显示在一行上,以便可以将其复制到文本文件中并保存以供使用该应用程序需要恢复。

zmschedulebackup -s

重击

## 备份失败

使用zmbbackupabort停止备份过程。在中止帐户之前,您必须知道其备份标签。这标签会在您启动备份程序后显示。如果您不知道标签,请使用zmbbackupquery查找标签名称。

要停止恢复过程:

`zmbbackupabort -r`中断正在进行的恢复。当前帐户被已恢复。该命令将显示消息,表明哪些帐户未恢复。

## 句法

zmbbackupabort [选项]

重击

## 描述

长名称	简称	描述
- 调试	-d	显示诊断信息以进行调试
- 帮助	-h	显示此命令的使用选项
- 标签	-磅	<arg>要中止的完整备份的标签。 使用zmbbackupquery,查找标签名称。
- 恢复	-r	中止正在进行的恢复
- 服务器	-s	<arg>邮件服务器主机名。格式可以使用以下任一方式普通主机名或 server.domain.com 名称。 默认值为本地主机名。

长名称	简称	描述
- 目标	-t	<arg>指定目标备份位置。 默认是/opt/zimbra/backup。

## zm备份查询

使用zmbackupquery查找完整备份集。该命令可用于查找特定的完整备份集或完整自特定日期以来的备份集，或备份目录中的所有备份集。

要找出最佳完整备份作为帐户时间点还原的基础，请运行以下命令这：

```
zmbackupquery -a <账户邮箱> --type full --to <恢复时间>
```

重击

## 句法

```
zmbackupquery [选项]
```

重击

## 描述

长名称	简称	描述
- 帐户	-a	<arg>账户电子邮件地址，以白色分隔空间或全部用于所有帐户
- 调试	-d	显示诊断信息以进行调试
- 帮助	-h	显示此命令的使用选项
- 从		<arg>列出开始日期/时间等于或晚于的备份 此处指定的日期/时间。
- 标签	-l	<arg>要查询的完整备份会话的标签。 标签示例是backup202107121559510。
- 服务器	-s	<arg>邮件服务器主机名。格式可以使用以下任一方式 普通主机名或 server.domain.com 名称。 默认值为本地主机名。
- 目标	-t	<arg>指定备份目标位置（ 默认是/opt/zimbra/backup。）
- 到		<arg>列出开始日期/时间为或的备份 在此指定的日期/时间之前。
- 类型		<arg>要查询的备份集类型。“full”或 “增量”，如果未指定，则查询两者。
--详细	-v	返回详细的状态信息

采用以下格式之一指定日期/时间：

2021/12/16 12:19:23
2021/12/16 12:19:23 257
2021/12/16 12:19:23.257
2021/12/16-12:19:23-257
2021/12/16-12:19:23
20211216.121923.257
20211216.121923
20211216121923257
20211216121923

指定年、月、日、时、分、秒以及可选的毫秒。

月/日/时/分/秒以 0 填充为 2 位数字,毫秒以 0 填充为 3 位数字。

小时必须以 24 小时格式指定,并且时间是当地时区。

## 校长

使用zmrestore对指定邮件主机执行完整恢复和增量恢复。您可以指定指定账户,或者,如果没有指定账户,则恢复备份中的所有账户。此外,您还可以恢复到特定的时间点。

此应用程序具有短选项名称和全名。短选项前面有一个破折号,全选项是以双破折号开头。例如, -rf与--restorefullBackupOnly相同。

## 句法

zmrestore [选项]

重击

## 描述

长名称	简称	描述
-帐户	一个	<arg>指定账户电子邮件地址。单独用空格隔开,或者输入 all 来恢复所有帐户。
--backedupRedlogs	-br	仅在备份中重放重做日志,仅不包括系统的存档和当前重做日志。
--continueOnError	-c	出现错误时继续恢复其他帐户发生。

长名称	简称	描述
- 创建账户	-n	将账户恢复到名称为 加上前缀。  (只能在使用-pre 选项。)
- 调试	-d	显示诊断信息以用于调试目的。
--排除Blob		不恢复 blob (无论是否为 SM)。
--排除HsmBlobs		不要恢复 SM blob。
--排除搜索索引		不恢复搜索索引。
- 帮助	-h	显示此命令的使用选项。
- 标签	-l	<arg>要恢复的完整备份的标签。恢复 如果省略,则为最新的完整备份。
--前缀	-p	<arg>添加到原始帐户的前缀 名字。
--恢复帐户	-r	恢复目录服务中的帐户。
--restoreToIncrLabel		<arg>重放重做日志直至并包括此日志 增量备份
--restoreToRedoSeq		<arg>重放直至并包括此重做日志 顺序。
--恢复时间		<arg>重播重做日志直到此时间。
-- 仅恢复完整备份	-f	仅恢复到完整备份,而不是任何增量备份 自该备份以来的备份。
- 服务器	-s	<arg>邮件服务器主机名。格式可以使用以下任一方式 普通主机名或 server.domain.com 名称。 默认值为本地主机名。
--跳过删除		如果为 true,则在重做日志期间不执行删除操作 重播。
--skipDeletedAccounts		如果指定帐户已被删除或 备份时不存在。(此选项始终 使用-a all启用)
--系统数据	-sys	恢复全局表和本地配置。
- 目标	-t	<arg>指定备份目标位置。 默认是/opt/zimbra/backup。

## 示例

示例 执行对server1 上所有 75 个帐户的完全恢复

在

对 server1上的所有帐户执行完整恢复,包括上次完整备份和任何增量备份  
自上次完整备份以来。

zmrestore -a all -s server1.domain.com

重击

**例 76. 仅执行恢复上次完整备份 到**

仅对所有账户执行上次完整备份的恢复,不包括此后的增量备份  
服务器1。

zmrestore -rf -a all -s server1.domain.com

重击

创建 77 的新帐户示例.aa

**目标账户的备份**

新帐户的名称将是new\_user1@domain.com。

zmrestore -a user1@domain.com -ca -pre new\_

重击

**zmrestoreoffline (离线恢复)**

zmrestoreoffline要求满足以下条件:

- mailboxd未运行
- SQL 数据库正在运行
- LDAP 目录正在运行

先决条件

**句法**

zmrestoreoffline [选项]

重击

**描述**

长名称	简称	描述
-帐户	-一个	<arg>指定账户电子邮件地址。单独 带有空白空间或状态全部用于恢复的帐户 所有帐户。必填。
--backedupRedologsOnly -br		仅在备份中重放重做日志,不包括 系统的存档和当前重做日志。
--continueOnError	-c	出现错误时继续恢复其他帐户 发生。

长名称	简称	描述
- 创建账户	-n	将账户恢复到新的目标账户 ,其名称前面带有前缀。
- 调试	-d	显示诊断信息以用于调试目的。
- 帮助	-h	显示此命令的使用选项。
--ignoreRedoErrors		如果为真,则忽略重做日志重放期间的所有错误。
- 标签	-l	<arg>要恢复的完整备份的标签。输入此标签来指定除最新文件之外的其他备份文件。
--前缀	-p	<prefix>添加到原始内容前的前缀帐户名。
--恢复帐户	-a	恢复目录服务中的帐户。
--restoreToIncrLabel		<arg>重放重做日志直至并包括此日志增量备份。
--restoreToRedoSeq		<arg>重放直至并包括此重做日志顺序。
--恢复时间		<arg>重播重做日志直到此时间。
-- 仅恢复完整备份	-f	仅恢复到完整备份,而不是任何增量备份自该备份以来的备份。
- 服务器	-s	<arg>邮件服务器主机名。格式可以使用以下任一方式普通主机名或 server.domain.com 名称。默认值为本地主机名。如果指定了 -s ,这必须是本地主机。
--skipDeletedAccounts	-skipDeletedAccounts	如果指定帐户已被删除或备份时不存在。(此选项始终使用-a all启用)
--系统数据	-sys	恢复全局表和本地配置。
- 目标	-t	<arg>指定备份目标位置。 默认是 /opt/zimbra/backup 。

## 示例

开始zmrestoreoffline之前 , LDAP 目录服务器必须正在运行。

示例执行 78.a

完全恢复所有帐户server1

在

对 server1上的所有帐户执行完整恢复,包括上次完整备份和任何增量备份  
自上次完整备份以来。

zmrestoreoffline -s server1.domain.com

重击

## 恢复ldap

使用zmrestoreldap从 LDAP 备份中恢复帐户。

### 句法

zmrestoreldap {-lb &lt;参数&gt;} {-t &lt;参数&gt;} [选项]

重击

### 描述

简称	描述
-磅	<arg>要从中恢复的会话标签。例如，full202112291821113。
-t	<arg>指定备份目标位置。默认为/opt/zimbra/backup。
-磅	列出备份中的所有会话标签。
-l	列出文件中的帐户。
一个	<arg>恢复命名的帐户。列出以空格分隔的帐户名称。

## zmcontrol (启动/停止/重启服务)

由于许可证守护程序服务是一项关键且重要的服务,因此它不通过  
zmcontrol命令。zmcontrol命令显示状态,但您无法  
启动/停止/重启 LDS。使用zmlicensectl执行启动/停止/重启操作  
摩门教。

使用zmcontrol启动、停止或重新启动服务。您还可以找到 Zimbra Collaboration 的哪个版本已安装。

### 句法

zmcontrol [-v -h] 命令 [参数]

重击

### 描述

长名称	简称	描述
	-v	显示 Zimbra 软件版本。
	-h	显示此命令的使用选项。
	-H	主机名 (localhost)。
指挥…		
维护		切换维护模式。
重启		重新启动此主机上的所有服务和管理器。

长名称	简称	描述
关闭		关闭此主机上的所有服务和管理器。 当管理器关闭时,您无法查询 那个状态。
开始		启动管理器和此主机上的所有服务。
启动		启动管理器和此主机上的所有服务。
地位		返回指定主机的服务信息。
停止		停止所有服务但保留管理器 跑步。

## zmmboxsearch (跨邮箱搜索)

使用zmmboxsearch进行跨邮箱搜索。您可以跨邮箱搜索以查找邮件和符合特定标准的附件并将这些邮件的副本保存到目录中。

### 句法

`zmmboxsearch {-m <arg>} {-q <arg>} [-o <arg>] [-l <arg>] [-d <arg>] [选项]`

重击

### 描述

长名称	简称	描述
- 你	-d	<arg>写入消息的文件夹。如果没有指定,则只获取标题。文件名称以RESULTNUM_ACCOUNT-ID_MAILITEMID的形式生成。
- 帮助	-h	显示帮助信息。
- 限制	-l	设置返回结果数量的限制。 默认值为 25。
--mbox	-m	<arg>要搜索的邮箱的逗号分隔列表。 UID 或电子邮件地址或/SERVER/MAILBOXID或*。
- 抵消	-这	<arg>指定命中列表的开始位置。 默认值为 0。
- 询问	-q	<arg>搜索的查询字符串。
- 服务器	-s	<arg>邮件服务器主机名。默认为 localhost
--详细	-v	要求在搜索时打印状态消息 正在执行。

### 例子

以下示例在两个不同邮箱的收件箱文件夹中执行跨邮箱搜索  
指定的服务器并将找到的消息的副本放入指定的目录中。

## 示例 跨邮箱搜索

```
zmmboxsearch -m user1@yourdomain.com,user2@yourdomain.com -q in:inbox -d /var/tmp
```

重击

## zmmbox移动

使用zmmboxmove移动邮箱。目标服务器管理整个移动过程。使用zmmboxmove命令显著减少了账户锁定时间。

CLI 命令zmmboxmove用于将邮箱从一个 Zimbra 服务器移动到另一个服务器。邮箱可以在共享同一 LDAP 服务器的 Zimbra 服务器之间移动。所有文件都复制到新服务器，并且 LDAP 已更新。将邮箱移至新服务器后，旧服务器上仍会保留一份副本，但状态旧邮箱已关闭。用户无法登录，邮件也无法送达。您应该检查所有在清除旧邮箱之前，邮箱内容已成功移动。

## 句法

```
zmmboxmove -a <电子邮件> --来自 <源> --到 <目标> [--sync]
```

重击

## 描述

长名称	简称	描述
- 帐户	–a	<arg>要移动的帐户的电子邮件地址。
- 帮助	-h	显示此命令的使用选项。
- 从	-f	<arg>邮件服务器主机名。服务器所在位置--帐户邮箱所在。
- 到	-t	<arg>目标服务器。
--同步	-同步	同步运行

## zmmbox移动查询

使用zmmboxmovequery查询服务器上正在进行的邮箱移动，包括移入和移出。

## 句法

```
zmmboxmovequery -a <帐户电子邮件> [-s <要查询的服务器>]
```

重击

## zmpurgeoldmbox

邮箱移动后，使用zmpurgeoldmbox从旧服务器清除邮箱。

## 句法

```
zmpurgeoldmbox -a <帐户电子邮件> [-s <要清除的服务器>]
```

重击

## 描述

长名称	简称	描述
-帐户	-a	<arg>要清除的帐户的电子邮件地址。
-帮助	-h	显示此命令的使用选项
-服务器	-s	<arg>邮件服务器主机名。 帐户已存在

## zmgsutil

使用zmgsutil创建或删除 GAL 同步帐户，并强制将 LDAP 数据同步到 GAL 同步帐户。

在域上配置 GAL 时，会创建一个 GAL 同步帐户。创建此帐户后，轮询执行完全同步的间隔由管理控制台管理。

要查看 GAL 同步帐户的属性和设置，请针对该帐户运行zmprov gds。

长名称	描述
创建账户	<p>创建 GAL 同步帐户。这应该从管理控制台。</p> <p>参数“服务器”是必需的。</p> <pre>-a {帐户名称} -n {数据源名称} --domain {域名} -t zimbraldap -s {服务器} [-f {文件夹名称}] [-p {轮询间隔}]</pre>
添加数据源	<p>为服务器配置数据源时，请指定其他文件夹名称而不是/Contacts。数据源文件夹名称必须是唯一的。</p> <pre>-a {帐户名称} -n {数据源名称} --domain {域名} -t zimbraldap [-f {文件夹名称}] [-p {轮询间隔}]</pre>
删除账户	<p>删除 GAL 同步帐户和对 LDAP 服务器的引用。也可以从管理控制台中删除帐户。</p> <pre>deleteAccount [-a {galsyncaccountname}] [-i {account-id}]</pre>
trickleSync	<p>这仅同步新的和更新的联系人数据。</p> <pre>[-a {galsync帐户名}] [-i {帐户ID}] [-d {数据源 ID}] [-n {数据源名称}]</pre> <p>数据源 ID LDAP 数据源 ID。数据源名称是为同步而创建的 GAL 帐户中的地址簿（文件夹）的名称 LDAP 到。</p> <p>可以设置一个 cron 作业来运行trickleSync。</p>

长名称	描述
全同步	<p>这将同步所有 LDAP 联系人数据。您也可以从管理控制台。</p> <p><code>[-a {galsync帐户名} -i {帐户ID}] [-d {数据源 ID}] [-n {数据源名称}]</code></p>
forceSync	<p>如果过滤器发生变化,应使用此方法重新加载整个 GAL,属性映射或 LDAP 服务器参数。</p> <p><code>[-a {galsync帐户名} -i {帐户ID}] [-d {数据源 ID}] [-n {数据源名称}]</code></p>

## zmldappasswd

使用zmldappasswd更改本地服务器上的 LDAP 密码。在多节点环境中,此命令必须仅在 LDAP 主服务器上运行。

此 CLI 命令与选项一起使用可更改其他密码。

为了更好的安全性和审计跟踪,Zimbra 中生成了以下密码:

- LDAP 管理员密码。这是主 LDAP 密码。
- LDAP Root 密码。用于内部 LDAP 操作。
- LDAP Postfix 密码。这是Postfix用户用来向 LDAP 服务器标识自己的密码,并且必须在 MTA 服务器上配置为与 LDAP 主服务器上的密码相同。
- LDAP Amavis 密码。这是amavis用户用来向 LDAP 服务器标识自己的密码,并且必须在MTA服务器上配置为与LDAP服务器上的密码相同。
- LDAP 复制密码。这是LDAPreplication用户用来向 LDAP 主服务器,必须与 LDAP 主服务器上的密码相同。

## 句法

`zmldappasswd [-h] [-r] [-p] [-l] 新密码`

重击

## 描述

姓名	语法、示例、注释
-h	显示帮助。
-r	更改ldap_amavis 密码。
-b	更改ldap_bes_searcher_password。
-l	更改ldap_replication_password。
-p	更改ldap_postfix_password。
-n	更改ldap_nginx_password。

姓名	语法、示例、注释
-r	更改ldap_root_passwd。
-c	更新副本上配置数据库中的密码。必须与-1和 在主服务器上更改密码后，必须在副本服务器上运行。
只有一个 ， 对， 或r可以指定。如果不包含选项，则zimbra_ldap_password 已改变。	

## 本地配置

使用zmlocalconfig设置或获取 Zimbra 服务器的本地配置。使用zmlocalconfig -i查看管理员可以配置支持的属性。

### 句法

zmlocalconfig [选项]

重击

要查看本地配置类型zmlocalconfig。

### 描述

长名称	简称	描述
--配置	-c	<arg>存储配置的文件。
- 默认	-d	显示[args] 中列出的键的默认值。
- 编辑	-e	编辑配置文件，更改键和值 指定。 [args]采用key=value形式。
- 力量	-f	编辑那些已知可能改变的键 危险的。
- 帮助	-h	显示此工具的使用选项的帮助。
- 信息	-i	显示支持的属性列表。
- 格式	-m	<arg>以下列格式之一显示值： plain (默认) 、 xml ， 壳 ， 不可以。
--已更改	-n	仅显示列出的键的值 [args]的默认值已发生改变。
- 小路	-p	显示将使用哪个配置文件。
- 安静的	-q	抑制日志记录。
- 随机的	-r	该选项与 edit 选项一起使用。指定键 设置为随机密码字符串。
- 展示	-s	强制显示密码字符串。

长名称	简称	描述
--取消设置	-z	删除配置键。如果这是带有编译的默认值,将其值设置为空字符串。
- 扩张	-x	扩大价值观。
--zimbraAmavisMaxServers		允许控制 Amavisd 的并发性（默认 10）。
--zimbraClamAVMaxThreads		允许控制 ClamAV 的并发性（默认 10）。

## 邮箱

使用zmmailbox进行邮箱管理。该命令可以帮助管理员配置新邮箱以及使用帐户、调试邮箱问题以及帮助迁移。

您可以从zmprov命令中调用zmmailbox命令。您可以在其中输入selectMailbox

zmprov访问与指定邮箱连接的 zmmailbox 命令。然后您可以输入zmmailbox命令,直到您输入 exit。退出后会返回到zmprov。这在您想要创建帐户时很有用,并且同时预先创建一些文件夹、标签或已保存的搜索。

## 句法

zmmailbox [参数] [cmd] [cmd 参数]...

重击

## 描述

简称	长名称	语法、示例和注释
-h	- 帮助	显示使用情况。
-f	- 文件	使用文件作为输入流。
-z	--url	http[s]://[host][:{port}]服务器主机名和可选端口。必须使用带有-z / -a的管理端口。
-一个	- 帐户	要授权的帐户名为{name}。
-和	--zadmin	使用 localconfig 中的 zimbra 管理员名称/密码用于管理员/密码。
-和	--authtoken {验证令牌}	使用 authtoken 字符串（必须是 JSON 格式）命令行。
-和	--authtoken {authtoken 文件}	使用来自文件。
-m	-邮箱 {名称}	要打开的邮箱。可以用作身份验证并且是有针对性的,除非指定其他选项。
	--auth {名称}	授权的账户名。默认为--mailbox除非使用--admin-priv。

简称	长名称	语法、示例和注释
-a	--管理员权限	以管理员权限执行请求。
-p	-密码 {密码}	管理员帐户和/或邮箱的密码。
-P	--passfile {文件}	从文件读取密码。
-t	- 暂停	超时（以秒为单位）。
-v	--详细	详细模式（转储完整的异常堆栈跟踪）
-d	- 调试	调试模式（转储 SOAP 消息）

邮箱的不同组件有特定的 CLI 工具。用法在以下 CLI 帮助中描述：

下列的。

zmmailbox 帮助管理员	有关管理相关命令的帮助。
zmmailbox 帮助命令	有关所有zmmailbox命令的帮助。
zmmailbox帮助预约	有关约会相关命令的帮助。
zmmailbox 帮助 联系	有关联系人相关命令（地址簿）的帮助。
zmmailbox 帮助对话	有关对话相关命令的帮助。
zmmailbox 帮助过滤器	有关过滤器相关命令的帮助。
zmmailbox 帮助文件夹	有关文件夹相关命令的帮助。
zmmailbox 帮助项	有关项目相关命令的帮助。
zmmailbox帮助消息	有关消息相关命令的帮助。
zmmailbox 帮助 杂项	有关杂项命令的帮助。
zmmailbox帮助吧	关于正确命令的帮助。
zmmailbox 帮助搜索	有关搜索命令的帮助。
zmmailbox 帮助标签	标签相关命令的帮助。

## 示例

### 示例和文件夹 80. 创建标签

创建帐户时，您可能希望预先创建一些标签和文件夹。您可以调用zmmailbox  
在zmprov内部使用selectMailbox(sm)。

[重击](#)

```
$zmprov
prov> 作为 user10@domain.example.com test123
9a993516-aa49-4fa5-bc0d-f740a474f7a8
prov> sm user10@domain.example.com
邮箱:user10@domain.example.com,大小:0 B,消息:0,未读:0
mbox user10@domain.example.com> 创建文件夹/存档
257
mbox user10@domain.example.com> createTag TODO
64
mbox user10@domain.example.com> createSearchFolder /unread “is:unread”
258
mbox user10@domain.example.com>退出
省>
```

例子

查找 81 号的邮箱。

一个 帐户

[重击](#)

```
zmmailbox-zm user@example.com gms
```

示例 使用管理员身份验证令牌发送请求邮箱

使用命令emptyDumpster时需要此权限。使用--admin-priv跳过委托身份验证,因为  
目标信箱。

[重击](#)

```
zmmailbox -z --admin-priv -m foo@example.com emptyDumpster
```

例 83.

使用 --管理员权限

使用选择邮箱命令

[重击](#)

```
zm邮箱-z
mbox> sm --admin-priv foo@domain.com
```

示例验证 84。

作为 委派管理员用户

这允许一个用户登录另一个用户的邮箱。进行身份验证的用户必须是委派管理员  
帐户,并且必须在目标邮箱上拥有adminLoginAs权限。此身份验证选项使用非管理员  
身份验证令牌。使用--auth选项指定身份验证帐户。要以用户bar身份登录并打开  
邮箱foo :

[重击](#)

```
$ zmmailbox --auth bar@example.com -p 密码 -m foo@example.com
```

示例 查找 85 的邮箱大小。

一个 帐户

[重击](#)

```
zmmailbox-z-m user@example.com gms
```

例 86.

备份邮箱内容

拉链 文件

当您使用zmmailbox备份个人邮箱时,您可以将文件保存为zip文件或tgz文件。这些格式保存的信息的默认设置是不同的。

文件	TGZ	拉链
公文包	+	+
日历		+
对话		+
联系方式	+	+
已删除的邮件	+	+
电子邮件联系人		+
收件箱	+	+
发送	+	+
已发送消息	+	+
任务		+

要将所有邮箱内容包含在zip文件中,您必须启用元数据。输入如下:

```
zmmailbox -z -m user@example.com gru ?fmt=zip&meta=1 > <filename.zip>
```

重击

## 兹米特斯特尔

使用zmtlsctl将 Web 服务器zimbraMailMode设置为通信协议选项:HTTP、HTTPS、混合、两者和重定向。默认设置为 HTTPS。

zmtlsctl设置还会影响 ZCO 的使用安全连接设置。自签名环境中的 ZCO 用户将遇到有关连接安全性的警告,除非根 CA

证书已添加到 Windows 证书存储中。请参阅 Zimbra Wiki 文章ZCO 连接  
安全性 ([https://wiki.zimbra.com/wiki/ZCO\\_Connection\\_Security](https://wiki.zimbra.com/wiki/ZCO_Connection_Security))了解更多信息。

- HTTP。仅限 HTTP,用户将浏览至http://zimbra.domain.com。
- HTTPS。仅 HTTPS (默认) ,用户将浏览https://zimbra.domain.com 。http://被拒绝。
- 混合如果用户访问http://,它将切换到https://仅用于登录,然后将恢复为http://  
正常会话流量。如果用户浏览https://  
,那么用户将停留在https://
- 用户都可以访问http://或https://,并且在整个会话期间保持该模式。
- 重定向就像混合一样,如果用户转到http://,它将切换到https://,但他们将保留https://  
整个会话。

所有模式均使用 TLS 加密来处理后端管理流量。

只有zimbraMailMode HTTPS可以确保 HTTP/端口 80 上没有可用的侦听器、没有客户端应用程序会尝试通过 HTTP 进行身份验证、并且与客户端应用程序交换的所有数据都将被加密。

请注意，必须停止并重新启动mailboxd 才能使更改生效。

如果切换到 HTTPS，则可以使用 Zimbra 安装期间在 /opt/zimbra/ssl/zimbra/server/server.crt 中生成的自签名证书。对于 ZCO 用户，除非将根 CA 证书部署到服务器，否则安全的 ZCO 配置文件将显示证书信任对话框。有关 ZCO 证书的更多信息，请参阅 Zimbra Wiki 页面 ZCO 连接安全 ([https://wiki.zimbra.com/wiki/ZCO\\_Connection\\_Security](https://wiki.zimbra.com/wiki/ZCO_Connection_Security))。

## 句法

`zmtrlsctl [模式]`

重击

模式= http , https , 混合 , 两个都 , 重定向

## 运行步骤

1. 输入 `zmtrlsctl [mode]` 并按ENTER。
2. 输入 `zmmailboxdctl stop` 并按ENTER。
3. 当 `mailboxd` 停止时，键入 `zmmailboxdctl start` 并按ENTER。

## 使用重定向的限制

- 许多客户端应用程序在初始 HTTP 请求中向服务器发送身份验证请求（“盲身份验证”）。这意味着在将客户端应用程序重定向到 HTTPS 之前，此身份验证请求以明文/未加密形式发送。
- 重定向模式允许进行中间人攻击、国际/无意重定向到无效服务器，或者用户错误输入服务器名称且不具有基于证书的服务器有效性的可能性。
- 在许多客户端应用程序中，用户无法判断他们是否已被重定向（例如，ActiveSync），因此即使身份验证请求未加密发送，用户也会继续使用 HTTP。

## 韓國

使用 `zmhsms` 启动、停止（中止）和查看 SM 会话的状态。从管理控制台的服务器 → 卷页面配置将消息移动到存储卷的阈值。

## 句法

`zmhsms {中止|启动|状态} {服务器} <名称>`

重击

## 描述

长名称	简称	描述
--中止	-一个	中止当前 SM 会话。如果正在处理的邮箱在您之前没有被移动单击“中止”后,该邮箱中不会再有消息从主卷移出。 已完成移动到辅助卷不会移回主卷体积。
- 帮助	-h	显示此工具的使用选项的帮助。
- 服务器	-s	<arg>邮件服务器主机名。默认为本地主机[参数]。
- 开始	-t	手动启动 SM 进程。
- 地位	- 在	显示最后一个 SM 会话的状态。

## 许可协议

使用zmlicense查看和安装您的 Zimbra 许可证。可以从管理控制台,全局设置→许可证页面。

## 句法

zmlicense [选项]

重击

## 描述

长名称	简称	描述
- 查看	-c	检查是否安装了有效的许可证。
- 帮助	-h	显示此工具的使用选项的帮助。
- 安装	-我	<arg>安装指定的许可证文件。
--ldap	-l	仅在 LDAP 上安装。
- 打印	-p	显示许可证信息。

## 元数据转储

zmmetadump命令是一个支持工具,它以人类可读的形式转储项目元数据的内容形式。

## 句法

zmmetadump -m <邮箱 ID/电子邮件> -i <项目 ID>

重击

或者

zmmetadump -f <包含编码元数据的文件>

重击

## 密码

使用zmmypasswd更改zimbra\_mysql\_password。如果指定了--root选项,则mysql\_root\_passwd为更改。在这两种情况下,MariaDB都会使用新密码进行更新。请参阅 MariaDB 文档以了解如何临时启动 MariaDB 服务器以跳过授权表并覆盖 root 密码。

需要重新启动才能使更改生效。

## 句法

`zmmypasswd [--root] <新密码>`

重击

## zmplayredo

使用存储层快照功能维护备份和恢复机制的用户使用  
zmplayredo恢复备份数据。此命令将所有备份数据恢复到当前状态,以便  
恢复过程中不会丢失信息。

## 句法

`zmplayredo <选项>`

重击

## 描述

长名称	简称	描述
--fromSeq		<arg>从指定的重做日志重放快照顺序。
--来自时间		<arg>从指定时间重播快照。
- 帮助	-h	显示该命令的帮助信息。
--日志文件		<arg>按顺序重播指定的日志文件。
--邮箱ID		<arg>重播指定邮箱的快照。
--队列容量		<arg>用于指定每个队列的容量播放器线程。默认值为 100。
--stopOnError		发生任何错误时停止重播。
--线程		<arg>指定并行重做线程的数量。 默认值为 50。
--toSeq		<arg>将快照重播到指定的重做日志顺序。
--toTime		<arg>重播指定时间的快照。

时间以当地时区指定。年、月、日、时、分、秒以及可选的毫秒  
应指定。月/日/时/分/秒用 0 填充为 2 位数字,毫秒用 0 填充为 3 位数字。小时  
必须以 24 小时格式指定。

## 代理服务器

使用zmproxyconfgen生成 Nginx 代理配置文件。它读取 LDAP 设置来替换模板变量并生成最终的 Nginx 配置。

### 句法

ProxyConfGen [选项]

重击

### 描述

长名称	简称	描述
--配置	-c	<arg>覆盖配置变量。<arg>格式应为name=value。要查看名称列表,请使用-d或-D。
--默认值	-d	打印默认变量图。
--定义	-D	加载 LDAP 后打印定义变量映射配置和处理覆盖。
- 帮助	-h	显示帮助信息。
--include 目录	-I	<arg>显示目录路径（相对于\$workdir/conf）,其中包含配置文件被写入。
--dry-run	-n	指定不写入配置,仅显示将要写入的文件。
--前缀	-p	<arg>显示配置文件前缀。默认值是nginx.conf
--模板前缀	-P	<arg>显示模板文件前缀。默认值为\$prefix。
- 服务器	-s	<arg>指定有效的服务器对象。配置是根据指定服务器的属性生成。默认是基于全局配置值。
--模板目录	-t	<arg>指定代理模板目录。默认值是\$workdir/conf/nginx/templates。
--详细	-v	显示详细数据。
--工作目录	-w	<arg>指定代理工作目录。默认值是/opt/zimbra。

## 代理服务器

使用zmproxypurge从一个或多个 memcached 服务器中清除 POP/IMAP 代理路由信息。可用memcached 服务器由zmprov gamcs函数发现。如有必要,可以使用服务器端口。

## 句法

ProxyPurgeUtil [-v] [-i] -a 帐户 [-L 帐户列表] [缓存1] [缓存2]...]

重击

## 描述

长名称	简称	描述
- 帮助	-h	显示此工具的使用选项的帮助。
--详细	-v	显示详细数据。
- 信息	-i	显示帐户路由信息。
- 帐户	-a	显示帐户名称。
- 列表	-L	显示包含帐户列表的文件,每行一个。
- 输出	-o	指定打印路由使用的格式 信息。显示的字段 默认 <ul style="list-style-type: none"> <li>• 缓存服务器</li> <li>• 帐户名称</li> <li>• 路线信息</li> </ul>
缓存N		(可选命令)指定额外的 memcache 服务器形式为服务器:端口。

## 脏转储

使用zmredodump进行调试并转储重做日志文件的内容。当用户调试问题,Zimbra 支持可能会要求他们使用特定选项运行zmredodump。

可以指定多个日志文件/目录,每个目录下的所有重做日志文件按升序排列订购并处理。

## 句法

zmredodump [选项] <redolog 文件/目录> [...]

重击

## 描述

长名称	简称	描述
- 帮助	-h	显示帮助信息。
	-m	指定以逗号或 空格。如果 使用空格作为分隔符。  要转储所有重做日志文件的内容,请忽略此 选项。

长名称	简称	描述
--无偏移		指定每个重做日志转储的文件偏移量和大小不应显示。
- 安静的	-q	激活安静模式。用于仅打印日志文件名和错误（如果有）。用于验证以最少的输出保证重做日志的完整性。
--显示斑点		显示 blob 内容。指定项目的 blob 是打印有<START OF BLOB>和<END OF BLOB>标记 blob 的开始和结束。

## 部署

使用zmskindeploy简化部署 Classic Web App 皮肤的过程。此工具处理可用的皮肤,为 Zimbra 部署的所有用户启用它们,然后重新启动 Web 服务器,以便识别新皮肤。

## 句法

zmskindeploy <路径/到/皮肤/目录/或/zip文件>

重击

## 皂化物

使用zmsoap以 SOAP 格式打印邮件、帐户和管理信息。

## 句法

zmsoap [选项] {路径1} [路径2]...

重击

## 描述

长名称	简称	描述
- 帮助	-h	打印使用信息。
- 邮箱	-m	<name>显示邮箱账户名。邮件和帐户请求将发送到此帐户。此如果-a和-z,则属性也用于身份验证没有指定。
- 目标		<name>显示要绑定的目标账户名请求已发送。仅用于非管理员会话。
--管理员名称	一个	<name>显示管理员帐户名称验证为。
--zadmin	-和	显示 Zimbra 管理员名称和密码验证为。
- 密码	-p	<pass>显示账户密码。
--密码文件	-P	<path>从文件读取密码。

长名称	简称	描述
-元素	-e	<path>显示根元素路径。如果指定,则所有不以斜杠 (/) 开头的路径参数是相对于该元素。
-类型	-t	<type>显示 SOAP 请求类型。可以是邮件, 帐户, 或admin。
--url	-u	<http[s]://...>显示服务器主机名和可选端口值。
--详细	-v	打印 SOAP 请求和其他状态信息。
小路		<[路径]...>显示元素或属性路径,并值。大致遵循 XPath 语法: [/元素1/[元素2][@属性]=[值]]。

## zmstat 图表

使用zmstat-chart收集 CPU、IO、 mailboxd、MTAqueue、MariaDB 等的统计信息组件并在 csv 文件上运行脚本以在各种图表中显示使用情况详细信息。这些 csv 文件是保存到/opt/zimbra/zmstat/。

您必须启用zmstat来收集性能图表数据:

1.输入zmprov ms {主机名} zimbraServerEnable stats

。

2.重启服务器,输入:

zmcontrol 停止  
zmcontrol 启动

重击

## 句法

zmstat-chart -s <参数> -d <参数> [选项]

重击

## 描述

长名称	简称	描述
--aggregate-end-at		<arg>如果指定了,则聚合计算结束于此时间戳。用法为MM/dd/yyyy 时:分:秒。
--aggregate-start-at		<arg>如果指定了,则聚合计算从此时间戳开始。用法是MM/dd/yyyy 时:分:秒。
-结束于		<arg>如果指定了该参数,则指定的时间戳将被忽略。用法是MM/dd/yyyy 时:分:秒。

长名称	简称	描述
--开始于		<arg>如果指定,则此之前的所有样本时间戳被忽略。
- 标题		<arg>这为图表提供了显示的标题。默认值到srcdir的最后一个目录名。
--无摘要		不包括摘要数据生成。
--conf	-c	<arg>图表配置 xml 文件。
- 可用的	-d	<arg>生成的图表文件所在的目录已保存。
--srcdir		csv 文件所在的一个或多个目录。 csv 文件被移动到按日期列出的目录中在zmstat/ 下。

## zmstat-图表配置

使用zmstat-chart-config从模板生成 xml 文件/opt/zimbra/conf/zmstat-chart.xml ,  
考虑服务器设置 (包括LDAP节点和运行的进程)以及其他规范。

## zmstatctl

使用zmstatctl运行用于检查zmstat数据收集器的控制脚本。此指令启动或停止  
监控进程并检查状态或轮换日志。

## 句法

zmstatctl 开始|停止|状态|旋转

重击

## 转储

使用zmthrdump在 Zimbra 服务器进程中调用线程转储并打印输出文件。此命令还  
提供将线程转储保存到文件的选项,并在日志文件中插入时间戳。

## 句法

zmthrdump [-h] [-i] [-t <超时秒数>] [-p <pid 文件>] [-f <文件>] [-o <输出文件>]

重击

## 描述

简称	描述
-h	显示帮助信息。
-i	在调用 SIGQUIT 之前将时间戳附加到 LOGFILE。
-p	返回发送 SIGQUIT 的 PID。默认值可以在 邮箱服务器
-f	指定保存线程转储输出的 LOGFILE。默认值为 zmmailbox.out。

简称	描述
-这	指定线程转储的输出文件。默认值为 stdout。
-t	指定进程变为 无响应。默认值为 30 秒。

## 兹姆特兰萨

使用zmtrainsa训练反垃圾邮件过滤器。此命令每晚都会自动运行,以训练 SpamAssassin 会过滤用户邮箱中标记为“垃圾邮件” / “非垃圾邮件”的邮件。请参阅SpamAssassin 的 sa-update 工具,该工具包含在 SpamAssassin 中。此工具会从 SA 组织更新 SpamAssassin 规则。该工具安装到/opt/zimbra/common/bin。

可以手动运行zmtrainsa命令,将任意邮箱中的任意文件夹转发到垃圾邮件训练邮箱。如果您在为帐户手动运行zmtrainsa时没有输入文件夹名称,则对于垃圾邮件,默认文件夹是垃圾邮件。对于普通邮件,默认文件夹是收件箱。

## 句法

zmtrainsa <用户> <垃圾邮件|ham> [文件夹]

重击

## 更新

使用zmtzupdate更新特定用户或所有用户的现有约会中的时区变化。.ics规则应首先创建文件以使用此命令运行。规则文件列出了一系列规则,以匹配时区和替换时区定义。有关此命令的更多信息,请访问:  
[https://wiki.zimbra.com/wiki/Changing\\_ZCS\\_Time\\_Zones](https://wiki.zimbra.com/wiki/Changing_ZCS_Time_Zones)。

## 句法

zmtzupdate --rulefile <规则文件> -a <“全部”或特定电子邮件地址列表> [--sync] [--  
<日期/时间戳>之后]

重击

## 描述

长名称*	简称	描述
-帐户	一个	<arg>个帐户的电子邮件地址,中间用白色空格隔开空格。使用“全部”表示所有帐户均要更新。
-后		<arg>指定时间之后发生的约会 此字段中的日期/时间已更新。默认截止时间 时间是2008年1月1日。
-帮助	-h	显示帮助信息。
--规则文件		指定应该使用的.ics XML 文件 更新时区定义。
-服务器	-s	<arg>指定邮件服务器主机名。默认 值是 localhost。

长名称*	简称	描述
--同步		如果指定,此选项会导致zmtzupdate命令阻塞直到服务器处理完所有请求的帐户。默认值为 no。

## 体积

使用zmvolume从 CLI 管理存储卷。请注意,可以从管理控制台,服务器 → 卷页面。

### 句法

```
zmvolume {-a|-d|-l|-e|-dc|-sc} [选项]
```

重击

### 描述

长名称	简称	描述
- 添加	-a	添加卷。
- 压缩	-c	<arg>压缩 BLOB; “true”或 “false”。
--压缩阈值-ct		压缩阈值;默认 4KB。
- 删除	-d	删除卷。
--显示当前	-l	显示当前音量。
- 编辑	-e	编辑卷。
- 帮助	-h	显示此工具的使用选项的帮助。
- ID	-ID	<arg>卷 ID。
- 列表	-l	列出卷。
- 姓名	-n	<arg>卷名称。
- 小路	-p	<arg>根路径。
- 服务器	-s	<arg>邮件服务器主机名。默认为 localhost。
--设置当前	-sc	设置当前音量。
- 类型	-t	<arg>卷类型 (primaryMessage, secondaryMessage,或索引)
--turnOffSecondary	-ts	关闭当前的辅助消息音量。

## 兹姆齐姆莱特特尔

使用zmzimletctl管理 Zimlets 并列出服务器上的所有 Zimlets。更多信息请参见 Zimlets。大多数 Zimlet 部署都可以通过 Zimbra 管理控制台完成。

### 句法

zmzimletctl [-l] {命令} [&lt;zimlet.zip&gt;|&lt;config.xml&gt;|&lt;zimlet&gt;]

重击

## 描述

长名称	描述
部署	<zimlet.zip>在 LDAP 服务器中创建 Zimlet 条目,安装服务器上的 zimlet 文件,授予对默认成员的访问权限 COS,并打开 Zimlet。
取消部署	<zimlet>从 Zimbra 服务器上卸载 zimlet。
安装	<zimlet.zip>在主机上安装 Zimlet 文件。
ldap部署	<zimlet>将 Zimlet 条目添加到 LDAP。
使能够	<zimlet>启用 Zimlet。
禁用	<zimlet>禁用 Zimlet。
访问控制列表	<zimlet> <cos1> {授予   拒绝}   [<cos2> {授予 拒绝}…] 将访问控制 grant deny 设置为 COS。
列表访问权限	<zimlet>列出 Zimlet 的 ACL。
列表Zimlet	查看服务器上所有 Zimlet 的详细信息。
获取配置模板	<zimlet.zip>从 Zimlet.zip 中提取配置模板文件。
配置	<config.xml>安装配置。
列表优先级	显示当前 Zimlet 优先级 (0 为高,9 为低)
设置优先级	<zimlet>设置 Zimlet 优先级。

## 代理配置

使用zmproxyconfig管理 Zimbra 代理,仅当必须对 Zimbra 进行更改时才应使用代理服务器。请参阅Zimbra 代理服务器。

在 Zimbra Collaboration 6.0 之前,此命令被称为zmproxyinit。

## 句法

```
/opt/zimbra/libexec/zmproxyconfig [-h] [-o] [-m] [-w] [-d [-r] [-s] [-a w1:w2:w3:w4] [-i p1:p2:p3:p4] [-p p1:p2:p3:p4] [-x 邮件模式]] [-e [-a w1:w2:w3:w4] [-i p1:p2:p3:p4] [-p p1:p2:p3:p4] [-x 邮件模式]] [-f] -H 主机名
```

重击

## 描述

简称	描述
-h	显示帮助信息。
-H	启用/禁用代理功能的服务器的主机名。
-一个	要使用的 Web 端口的冒号分隔列表。格式：HTTP-STORE:HTTP-PROXY:HTTPS-STORE:HTTPS-PROXY（例如：8080:80:8443:443）
-d	禁用代理。
-和	启用代理。
-f	完全重置 memcached 端口和搜索查询以及 POP/IMAP 限制。
-我	要使用的 IMAP 端口的冒号分隔列表。格式：IMAP-STORE:IMAP-PROXY:IMAPS-STORE:IMAPS-PROXY（例如：7143:143:7993:993）
-m	切换邮件代理部分。
-这	覆盖已启用的检查。
-p	要使用的 POP 端口的冒号分隔列表。格式：POP-STORE:POP-PROXY:POPS-STORE:POPS-PROXY（例如：7110:110:7995:995）
-r	针对远程主机运行。请注意，这需要服务器正确在 LDAP 主服务器中配置。
-s	禁用时将 Cleartext 设置为 FALSE（安全模式）。
-t	禁用商店服务器的反向代理查找目标。仅与-d一起使用时有效。 确保您打算禁用服务器的所有代理功能。
-在	切换 Web 代理部分。
-x	禁用时使用的zimbraMailMode（默认为 HTTP）

hostname是正在修改的服务器的zimbra\_server\_hostname LC 键的值。

所需选项是-f本身,或者-f与-d或-e一起。

#### 注意

- -d或-e需要-m和-w中的一个或两个。
- -i或-p需要-m。
- -a需要-w。
- -x需要-w和-d进行存储。
- -x需要-w作为代理。

以下是-a的默认值

, -我 , -p ,如果它们没有作为选项提供,则为-x。

-一个	默认启用 :8080:80:8443:443	禁用默认 :80:0:443:0
-----	------------------------	------------------

-我	默认启用:7143:143:7993:993	默认禁用:143:7143:993:7993
-p	默认启用:7110:110:7995:995	默认禁用:110:7110:995:7995
-x	商店禁用默认设置:http	默认启用/禁用代理:http

## zmsyncreverseproxy

使用zmsyncreverseproxy在源服务器和转发服务器之间反向代理移动同步 HTTP 流量，并端口。打开详细模式时，解码同步请求/响应并记录它们。

### 句法

```
zmsyncreverseproxy [-v] [-d] [-L log4j.properties] -p <端口号> -fs <转发服务器> -fp <转发端口> [-sv 同步版本]
```

重击

### 描述

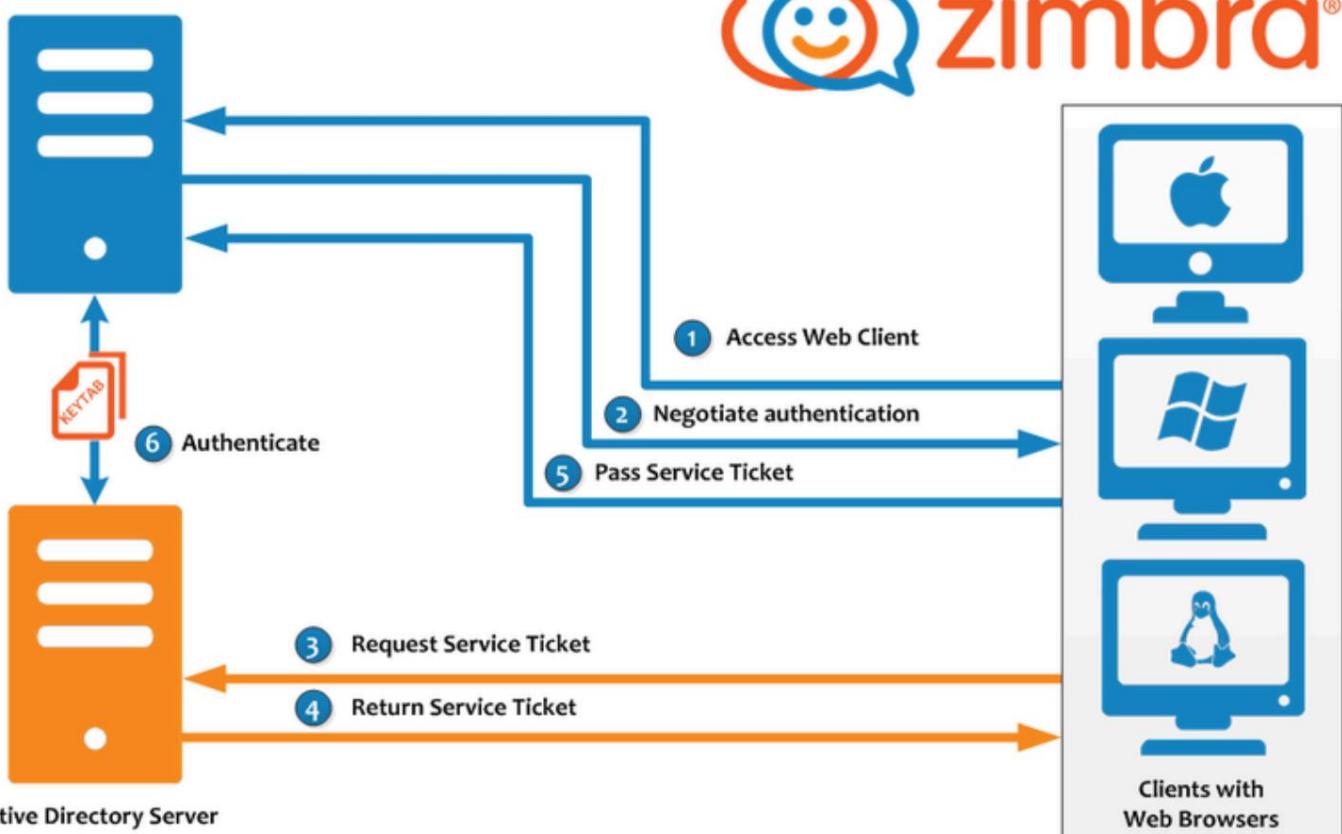
长名称	短的	描述
-帮助	-h	显示帮助。
--详细	-v	详细模式，转储完整的异常堆栈跟踪。
-调试	-d	调试模式，转储解码的同步消息。
-港口	-p	此服务监听的端口。
--转发服务器	-fs	将请求转发到的服务器主机。
--转发端口	-fp	转发请求到的服务器端口。
--同步版本	-sv	支持主动同步版本。
--logproperty文件	-L	log4j属性文件，仅对-l有效。

## 附录 B:配置 SPNEGO 单点登录

可以在 Zimbra 上配置 SPNEGO 协议机制,以便对 Zimbra Classic Web App、Modern Web App 和 Zimbra Connector for Outlook (ZCO) 进行单点登录身份验证。有关 ZCO 配置,请参阅为 ZCO 设置单点登录选项。

当用户通过 Active Directory 对其 Intranet 进行身份验证后,他们可以使用 Classic Web App 或 Modern Web App 进入他们的 Zimbra 邮箱,而无需重新进行身份验证。

Zimbra Collaboration Server



Zimbra 服务器配置会将尝试登录 Classic Web App 或 Modern Web App 的用户重定向到受 SPNEGO 保护的 URL。服务器通过 SPNEGO 要求使用 Kerberos 进行身份验证,并将用户重定向到他们的 Zimbra 邮箱。当用户注销时,他们会被重定向到显示 [启动按钮] 的注销 URL。当用户单击它时,他们会被定向到 Zimbra 登录页面。

]

当用户从登录他们的 Zimbra 帐户时,他们必须输入他们的 Zimbra 密码才能 互联网 , Zimbra 登录页面显示 登录。

在域上启用 SPNEGO SSO 后,相应的浏览器配置至关重要。请参阅配置您的浏览器。配置不当的浏览器可能会通过打开身份验证对话框绕过 SPNEGO,从而允许用户通过输入正确的 AD 域用户名/密码登录 Zimbra 邮箱。在这种情况下,某些其他浏览器可能会显示“401 未授权”错误。

## 配置流程

1. 创建 Kerberos 密钥表文件。

- 创建 Active Directory 服务帐户。您将使用此帐户生成 Kerberos 密钥表文件。
- 为 Active Directory 服务帐户添加服务主体名称 (SPN) 目录属性。
- 创建密钥表文件。

2. 在 Zimbra 服务器上启用并配置 SPNEGO 协议。

3. 配置浏览器

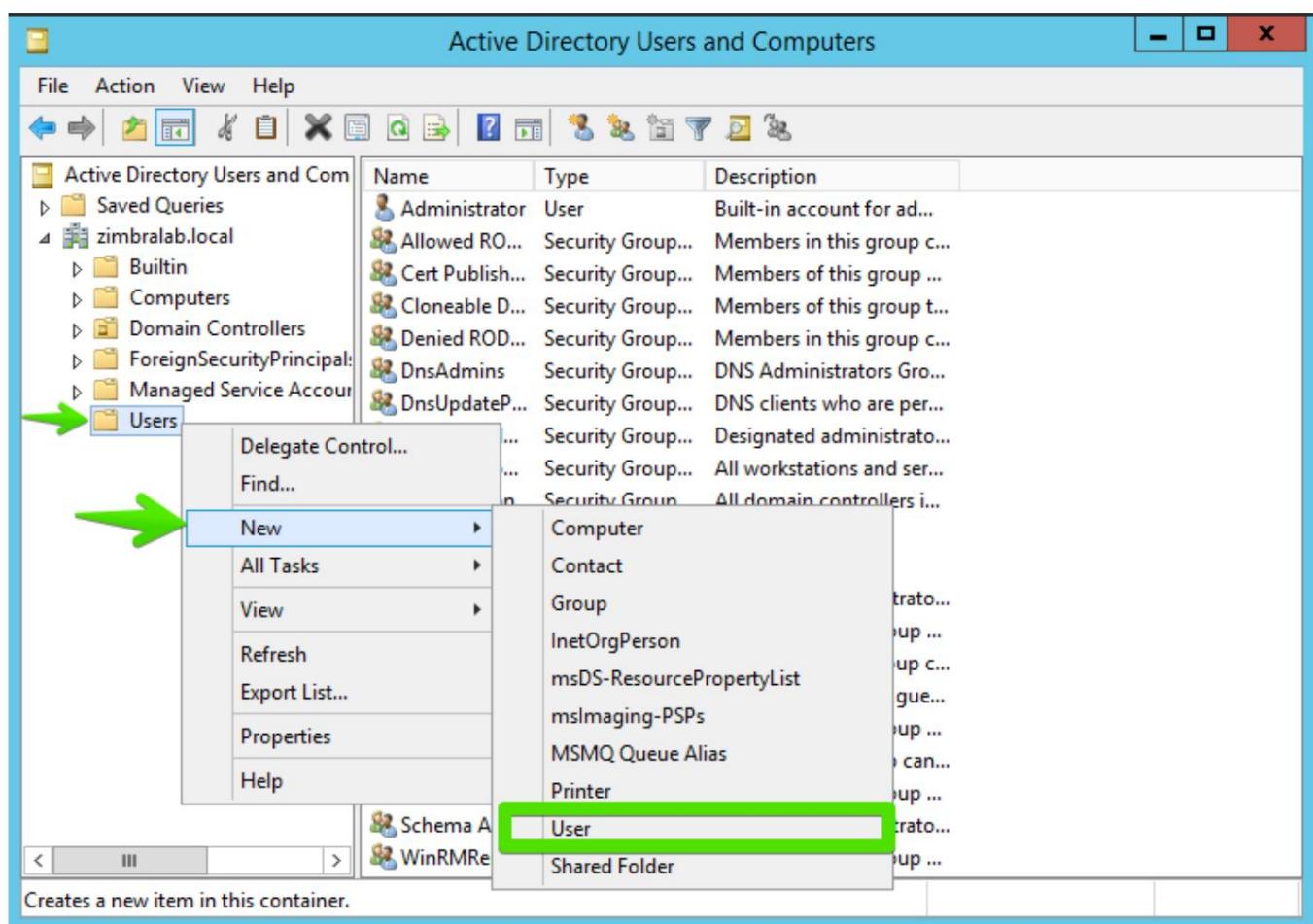
## 创建 Kerberos Keytab 文件

为每个邮件存储服务器创建一个 Active Directory 服务域帐户。

1. 创建 Active Directory 服务帐户。您可以使用此帐户生成要添加到的 Kerberos keytab 文件 Zimbra 服务器。

a. 转到 Active Directory 开始→程序→管理工具→Active Directory 用户和计算机 安慰。

b. 要创建服务帐户,请单击 AD 域名,然后在展开的内容中右键单击用户 并选择新建→用户。完成新对象 – 用户对话框。



- 全名: 输入 AD 服务帐户的用户显示名称。我们建议使用 Zimbra 邮箱服务器名称作为全名。

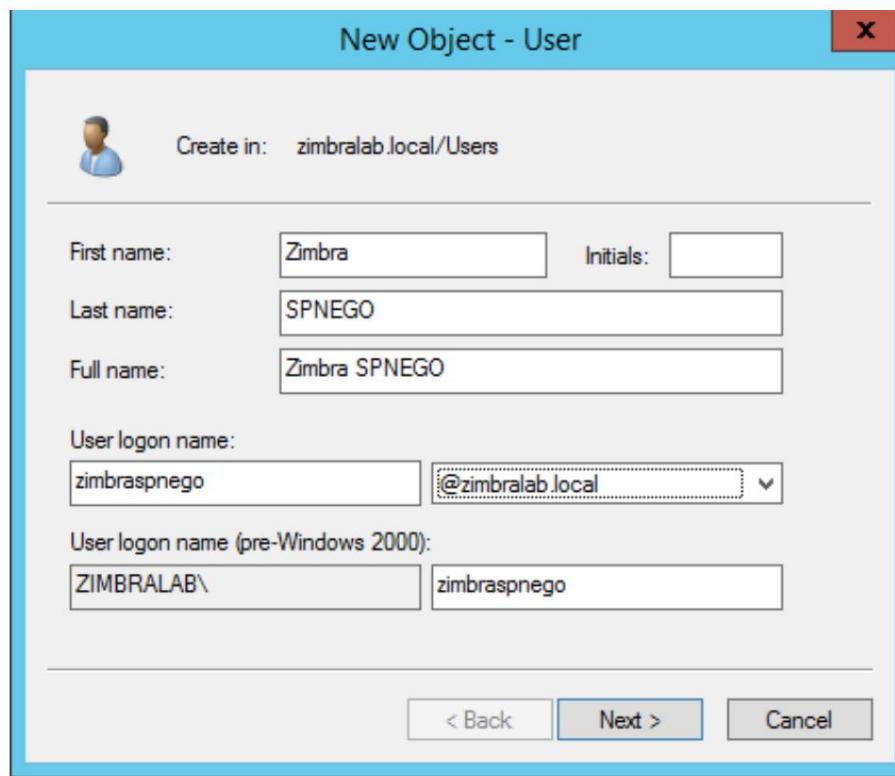
例如: Zimbra SPNEGO。

- 用户名: 此名称是 LDAP 中 zimbraSpnegoAuthTargetName 服务器属性设置的值。请记下来。

例如: zimbraspnego/zimbralab.local。

- 用户登录名（Windows2000 之前）：此名称用于setspn中的–mapUser参数和ktpass命令。

例如：ZIMBRALAB\zimbraspnego。



■ 单击“下一步”。

- 输入并确认ktpass命令中–pass {AD-user-password}参数的密码，配置如下。

- 勾选“密码永不过期”和“用户不能更改密码”，单击“下一步”。

[ ]

- 单击“完成”创建用户。服务帐户名称显示在用户目录中。

## 2. 使用setspn命令将邮箱服务器名称映射到用户帐户作为服务主体名称

(SPN)。SPN 的功能是客户端与托管服务的服务器之间的相互身份验证过程特定服务。

- 在命令提示符下,键入setspn –a {userlogonname} {serviceaccountname}

示例邮箱服务器名称87。

服务主体名称到用户帐户

```
setspn -a HTTP/mail1.example.com mail1
```

重击

- 要验证 SPN 是否已注册,请键入C:\>setspn –l {accountname} 显示已注册的 SPN 列表。

## 3. 创建登录 Kerberos 域时使用的 keytab 文件。使用Windows 中的ktpass工具用于创建 Kerberos 密钥表的服务器工具包。

Kerberos 密钥表文件包含与用户密码类似的密钥列表。限制并监控您创建的任何 keytab 文件的权限。

输入的命令如下：

```
ktpass -out {keytab-file-to-produce} -princ {服务主体名称}@{the-kerberos-realm} -mapUser {AD 用户} -mapOp set -pass {AD 用户密码} -crypto RC4-HMAC-NT -pType
```

### KRB5\_NT\_PRINCIPAL

ktpass-输出	该密钥被写入该输出文件。 输入目录位置和keytab文件名, keytab文件名为jetty.keytab。  例如, C:\Temp\spengo\jetty.keytab。
-王子	主体名称。 输入创建 Kerberos Keytab 文件第 2 步中使用的服务主体名称。  例如, HTTP/mail1.example.com@MY_COMPANY.COM。
-mapUser	将-princ参数中的主体名称映射到此用户帐户。 输入先前在创建 Kerberos Keytab 文件的步骤 1.b 中设置为用户登录名 (Windows2000 之前) 的 AD 服务帐户的名称。
-mapOp	此选项设置映射。此参数的值已设置。
-经过	指定与-princ帐户一起使用的密码。 输入在创建 Kerberos Keytab 文件的步骤 1.c 中设置的用户登录名 (Windows2000 之前) 中输入的密码。
-加密	要使用的密码系统。 输入RC4-HMAC-NT。
-p类型	输入KRB5_NT_PRINCIPAL。 为了避免工具包出现警告消息,请输入此值。

### 4. 使用ktpass创建jetty.keytab文件

```
ktpass -out C:\Temp\spengo\jetty.keytab -princ HTTP/mail1.example.com@MY_COMPANY.COM -mapUser mail1 -mapOp set -pass password123 -crypto RC4-HMAC-NT -pType KRB5_NT_PRINCIPAL
```

BASH

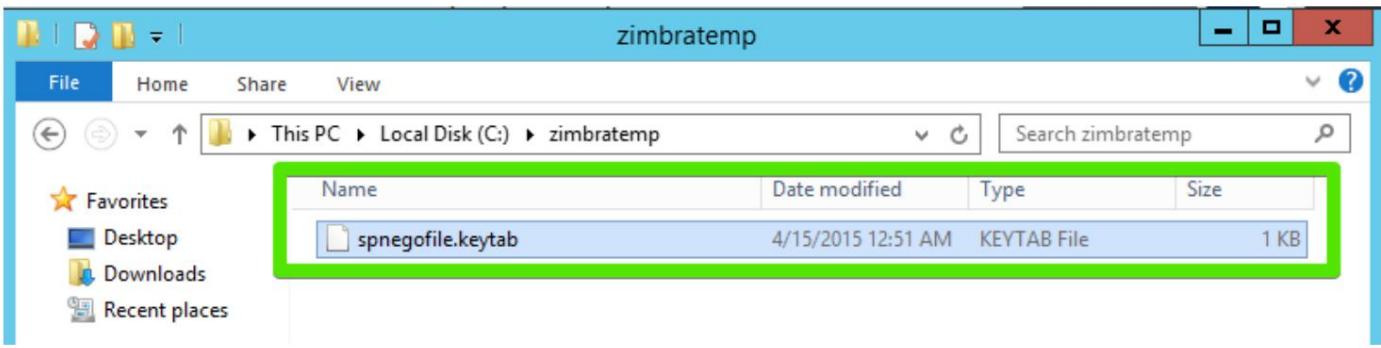
命令确认附带与以下示例类似的内容。

针对域控制器:

...

使用传统的密码设置方法成功将 HTTP/mail1.example.com 映射到 mail1。  
密钥已创建。  
将 keytab 输出到 c:\Temp\spengo\jetty.keytab:Keytab 版本:0x502

```
密钥大小 71 HTTP HTTP/mail1.example.com@MY_COMPANY.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno3 etype 0x17 (RC4-HMAC) 密钥长度 16 (0xc383f6a25f1e195d5aef495c980c2bfe)
```



5. 将 keytab 文件 (jetty.keytab) 传输到 Zimbra 服务器。将步骤 3 中创建的文件复制到以下 Zimbra 服务器位置：/opt/zimbra/data/mailboxd/spnego/jetty.keytab。

不要重命名 jetty.keytab 文件。许多配置文件都引用此文件名。

重复步骤 1 到 4 为每个 Zimbra 邮件存储服务器创建密钥表文件 (jetty.keytab)。

## 配置 Zimbra

SPNEGO 属性在 Global Config 和每个 Zimbra 服务器上配置，并为域配置域预身份验证。使用 zmprov 命令修改 Zimbra 服务器。

Zimbra 安装可能只支持一个 Kerberos REALM。

1. 使用 zmprov mcf 命令修改以下全局配置属性。

zimbraSpnegoAuthEnabled	设置为 TRUE。
zimbraSpnegoAuthErrorURL	此值是 SPNEGO 身份验证失败时用户重定向到的 URL。将其设置为 /zimbra/?ignoreLoginURL=1 会将用户重定向到常规 Zimbra 登录页面，用户可在该页面输入其 Zimbra 用户名和密码。
zimbraSpnegoAuthRealm	域控制器中的 Kerberos 领域；Active Directory 中的域名。 (MY_COMPANY.COM)

要修改全局配置属性，请输入：

- a. zmprov mcf zimbraSpnegoAuthEnabled TRUE
- b. zmprov mcf zimbraSpnegoAuthErrorURL /zimbra/?ignoreLoginURL=1
- c. zmprov mcf zimbraSpnegoAuthRealm <MY\_COMPANY.COM>

2. 在每个 Zimbra 服务器上，使用 zmprov ms 命令修改以下全局配置属性。

zimbraSpnegoAuth目标名称	这是步骤 1B (用户名) 中的用户名。
zimbraSpnegoAuthPrincipal	输入 zimbraSpnegoAuthTargetName 中设置的用户名和全局配置 zimbraSpnegoAuthRealm 中设置的地址。  输入为 zimbraSpnegoAuthTargetName@zimbraSpnegoAuthRealm。  例如，HTTP/mail1.example.com@MY_COMPANY.COM。

要修改服务器全局配置属性，请输入：

a. zmprov ms mail1.example.com zimbraSpnegoAuthTargetName HTTP/mail1.example.com

b. zmprov ms mail1.example.com zimbraSpnegoAuthPrincipal HTTP/mail1.example.com@MY\_COMPANY.COM 3. 为域设置以下内容。

- Kerberos 域
- 虚拟主机
- Web 客户端登录 URL 和 UA
- Web 客户端注销 URL 和 UA

a. 将域的 Kerberos 域设置为与全局配置属性中设置的域相同的域

zimbraSpnegoAuthRealm . 键入zmprov md {domain} zimbraAuthKerberos5Realm {kerberosrealm} 。

b. 设置域的虚拟主机。Virtual-hostname-\* 是您可以浏览 Zimbra Classic Web App UI 的主机名。输入：

zmprov md {域} +zimbraVirtualHostname {虚拟主机名-1} +zimbraVirtualHostname {虚拟主机名-2}

BASH

...

c. 设置 Web 客户端登录 URL 以及域上允许登录 URL 的 UA。

- 设置登录 URL。登录 URL 是 Zimbra 身份验证令牌过期时将用户重定向到的 URL。zmprov md {domain} zimbraWebClientLoginURL .. /service/spnego 。
- 仅尊重支持的平台和浏览器。

zimbraWebClientLoginURLAllowedUA是一个多值属性,值是正则表达式。如果未设置,则允许所有 UA。如果设置了多个值,则只要匹配其中任何一个值,就允许 UA。

zmprov md {域} +zimbraWebClientLoginURLAllowedUA {UA-regex-1} +zimbraWebClientLoginURLAllowedUA {UA-regex-2} ...

重击

例如,为了仅在运行 Windows 的计算机上的 Firefox、Internet Explorer、Chrome 和 Safari 以及 Apple Mac 计算机上的 Safari 中遵守 zimbraWebClientLoginURL ,请键入以下命令。

zmprov md {域} +zimbraWebClientLoginURLAllowedUA \_Windows\_Firefox/3.\* zmprov md {域} +zimbraWebClientLoginURLAllowedUA \_MSIE\_Windows.\* zmprov md {域} +zimbraWebClientLoginURLAllowedUA \_Windows\_Chrome.\* zmprov md {域} +zimbraWebClientLoginURLAllowedUA \_Windows\_Safari.\* zmprov md {域} +zimbraWebClientLoginURLAllowedUA \_Macintosh\_Safari.\*

重击

d. 设置 Web 客户端注销 URL 以及域上允许注销 URL 的 UA。

- 设置注销 URL。注销 URL 是用户点击“注销”时重定向到的 URL 。

[ ]

zmprov md {域} zimbraWebClientLogoutURL ../?sso=1

重击

- 仅遵守受支持的平台和浏览器。zimbraWebClientLogoutURLAllowedUA是一个多值属性,其中接受的值是正则表达式。如果此属性没有设置值,则允许所有 UA。当它有多个值时,只要 UA 与任何一个值匹配,就允许 UA。

重击

```
zmprov md {域} +zimbraWebClientLogoutURLAllowedUA {UA-regex-1} +zimbraWebClientLogoutURLAllowedUA
{UA-regex-2} ...
```

例如,为了仅在运行 Windows 的计算机上对 Firefox、Internet Explorer、Chrome 和 Safari 以及在 Apple Mac 计算机上对 Safari 遵守 zimbraWebClientLogoutURL,请键入以下命令。

重击

```
zmprov md {域} +zimbraWebClientLogoutURLAllowedUA ._Windows._Firefox/3.* zmprov md {域}
+zimbraWebClientLogoutURLAllowedUA ._MSIE._Windows.* zmprov md {域}
+zimbraWebClientLogoutURLAllowedUA ._Windows._Chrome.* zmprov md {域}
+zimbraWebClientLogoutURLAllowedUA ._Windows._Safari.*
```

## 配置您的浏览器

在您的域上启用 SPNEGO SSO 功能后,您必须配置用户的浏览器以使用其身份验证机制。配置不当的浏览器会根据浏览器表现出不同的行为。

支持以下浏览器:

- 对于运行 Windows 的计算机:Edge、Firefox 52 或更高版本、Chrome、Safari
- Apple Mac 电脑:Safari

配置步骤:

### 1.适用于运行 Windows 的计算机的 Firefox 浏览器

a. 在 Firefox 浏览器地址栏中输入about:config。警告 这可能会使您的保修失效,  
现在显示。

b. 点击我会小心的,我保证! [ ]

c. 在过滤器中搜索,输入network.n。输入以逗号分隔的受信任域或 URL 列表。

双击network.negotiate-auth.delegation-uris。输入http://,https://。

双击network.negotiate-auth.trusted-uris。输入http://,https://。

或者,设置 特定 URL,

双击network.negotiate-auth.delegation-uris。输入域地址。例如,  
http://mail1.example.com,https://mail2.example.com。

双击network.negotiate-auth.trusted-uris。输入域地址。例如,  
http://mail1.example.com,https://mail2.example.com。

### 2. 适用于运行 Windows 的计算机的 Internet Explorer、Chrome 和 Safari

a. 在这些浏览器中,转到“工具” → “Internet 选项” → “安全” → “本地 Intranet”>“站点”。在“站点”对话框中,检查所有项目。

b. 选择“高级”。添加域服务器(主机名)URL, http://和https://。

[ c. 单击“确定”关闭文件。

d. 转到工具→选项→高级→安全。找到并选中启用集成 Windows 身份验证。

[ e. 单击“确定”并关闭浏览器。

### 3. Safari 适用于 Apple Mac 电脑。无需配置。

## 测试您的设置

- 在 Windows 计算机或 Apple Mac 计算机上,以域用户身份登录计算机。

您的域用户令牌将保存在计算机上。该令牌由支持 SPNEGO 的浏览器获取,并通过授权标头发送到 Zimbra 服务器。

- 浏览 Zimbra Classic Web App 登录页面。您应该会被重定向到您的收件箱,而不会提示您输入用户名和密码。

如果 SPNEGO 身份验证失败,用户将被重定向到错误 URL。

## 故障排除设置

确保下列内容属实。

- 浏览器位于 Intranet 区域。
- 用户使用主机名而不是 IP 地址访问服务器。
- 集成 Windows 身份验证已在 Internet Explorer 中启用,并且主机已在火狐。
- 该服务器不是浏览器本地的。
- 客户端的 Kerberos 系统已向域控制器进行身份验证。
- 如果浏览器显示“401 未授权”,则很可能是因为浏览器没有发送另一个带有授权的请求来响应 401,或者在未使用 GSS-API/SPNEGO 方案的情况下发送了授权。

检查您的浏览器设置并确保它是受支持的浏览器/平台之一。

- 如果您被重定向到zimbraSpnegoAuthErrorURL中指定的错误 URL,则身份验证序列不起作用。这意味着 SPNEGO

进行网络跟踪,确保浏览器在响应401时发送了 Authorization 标头。确保 Negotiate 使用的是 GSS-API/ SPNEGO,而不是 NTLM (使用网络数据包解码器,如 Wireshark )。

验证浏览器发送了正确的协商后,如果仍然不起作用,请打开以下调试并检查 Zimbra 日志:

- 将-DDEBUG=true -Dsun.security.spnego.debug=all添加 (不要替换)到本地配置键  
请参阅 spnego\_java\_options。

- 在log4j中添加log4j.logger.org.mortbay.log=DEBUG。

然后重新启动邮箱服务器。

浏览到调试监听页面 ([http://\[server\]:\[port\]/spnego/snoop.jsp](http://[server]:[port]/spnego/snoop.jsp))。查看是否可以访问snoop.jsp。

检查zmmailboxd.out和mailox.log以获取调试输出。

- 此阶段的一个错误可能是由于 Jetty 服务器上的时钟偏差造成的。如果是这种情况,它应该显示在zmmailboxd.out中。  
修复时钟偏差并重试。

## 使用 SPNEGO Auth 配置 Kerberos Auth

Kerberos 身份验证和 SPNEGO 可以在域中共存。在此用例中,当用户无法通过 SPNEGO 进入时,您将使用 Kerberos 作为根据 KDC 验证用户主体/密码的机制,而不是使用本机 Zimbra LDAP。

在正确配置的浏览器中,当 SPNEGO 身份验证失败时,用户将被重定向到 Zimbra 登录页面。用户可以在登录页面上输入其 Zimbra 用户名和密码以手动登录。域属性 zimbraAuthMech 控制密码验证机制。如果 zimbraAuthMech 为“kerberos5”,则首先使用输入的用户名来识别有效的 Zimbra 用户（用户必须出现在 Zimbra LDAP 中）。Zimbra 用户将映射到 Kerberos 主体,然后根据 KDC 验证 Kerberos 主体 + 密码。此 KDC 可能与 Active Directory 域控制器（用于 SPNEGO 身份验证）使用的 KDC 不同,也可能相同。

每个 Microsoft Active Directory 域控制器都充当 Kerberos KDC。对于 SPNEGO 身份验证,邮箱服务器不会联系 KDC。从授权 HTTP 标头发送的 Kerberos 令牌以及 jetty 的 keytab 文件可以识别/验证用户。

对于 Kerberos 身份验证 (zimbraAuthMech\*=kerberos5),邮箱服务器需要联系 KDC 来验证主体+密码。对于 java Kerberos 客户端（即 Zimbra 邮箱服务器）,默认领域和该领域的 KDC 在 Kerberos 配置文件中指定。在可选 JVM 参数中指定此配置文件的位置,如果未指定,则默认为/etc/krb5.conf。当 SPNEGO 在java.security.krb5.conf中启用时。

Zimbra,邮箱服务器的java.security.krb5.conf设置为/opt/zimbra/jetty/etc/krb5.ini。因此,这是配置 Kerberos 身份验证的活动文件。

请注意,每次邮箱服务器重新启动时, /opt/zimbra/jetty/etc/krb5.ini都会从/opt/zimbra/jetty/etc/krb5.ini.in重写。因此,为了持久配置,您需要修改/opt/zimbra/jetty/etc/krb5.ini.in文件,而不是/opt/zimbra/jetty/etc/krb5.ini。

在 [realms] 部分下,KDC 和 admin\_server 未设置 SPNEGO 身份验证,但 Kerberos 身份验证需要它们。

配置方法:

1. 编辑/opt/zimbra/jetty/etc/krb5.ini.in。

2. 变更:

```
[领域] %
%zimbraSpnegoAuthRealm%% = {默认域 = %
%zimbraSpnegoAuthRealm%% }
```

到

```
%%zimbraSpnegoAuthRealm%% = {
    kdc = 您的 KDC
    admin_server = 您的管理员服务器 default_domain =
    %%zimbraSpnegoAuthRealm%% }
}
```

3. 将 YOUR-KDC 和 YOUR-ADMIN-SERVER 替换为 Kerberos 的 kdc/admin\_server 所在的主机名  
auth 正在运行。

4. 保存文件并重新启动邮箱服务器。

一个重要的限制是 SPNEGO 和 Kerberos 身份验证的领域必须相同。对于 SPNEGO 身份验证,授权标头中的 Kerberos 主体会映射到唯一的 Zimbra 帐户。对于 Kerberos 身份验证,Zimbra 帐户会映射到唯一的 Kerberos 主体。映射（按域属性

zimbraAuthKerberos5Realm )对于两者来说是相同的。

## 为 ZCO 设置单点登录选项

要使用 SSO ,必须在 Zimbra 服务器上配置 SPNEGO 才能使用此选项。

单点登录选项适用于特定服务器。ZCO 配置文件中使用的服务器名称必须与 SPNEGO 配置中的服务器名称匹配。确保在安装之前将服务器名称合并到.msi文件中。

要在.msi自定义脚本中设置单一登录选项：

- 1.将服务器名称设置为为 SPNEGO 配置的服务器名称,输入-sn <spnegoserver.example.com>。
- 2.设置密码规则,输入-pw 0 。

```
cscript ZmCustomizeMsi.js <路径/msi 文件名> -sn <spnegoserver.example.com> -pw 0
```

重击

## 附录 C:Zimbra Crontab 作业

crontab 用于安排在 Zimbra 服务器上定期执行的命令。

### 如何读取 crontab

crontab 文件中的每个条目由六个字段组成,按以下顺序指定:分钟、小时、天、月、星期几、命令

字段之间由空格或制表符分隔。

场地	描述
分钟	0 至 59
小时	0 至 23
月 1 日至 31 日	
月	1 至 12
(星期几)	0 到 7 (0 或 7 表示星期日,1 表示星期一等,或使用名称)
命令	这是该作业要执行的完整命令序列

当显示星号 (\*) 时,表示该字段的所有可能值。例如,小时时间字段中的星号相当于“每小时”。

### Zimbra Cron 作业

您可以通过以 zimbra 身份登录并输入crontab -l来查看 Zimbra crontab。

### 预定作业

计划为 Zimbra 运行以下 cron 作业:

#### 日志修剪

日志修剪会从/opt/zimbra/log中删除超过 8 天的日志。该作业于凌晨 2:30 运行

#### 状态记录

zmstatuslog调用zmcontrol status并将其数据输出到 syslog。

这主要是为了使得记录器可以读取数据并使管理控制台状态保持最新。

状态记录作业每 2 分钟运行一次。

#### 备份

完整备份和增量备份将根据zmschedulebackup命令定义的计划运行。默认情况下,完整备份计划于每周六凌晨 1:00 运行。增量备份计划于周日至周五凌晨 1:00 运行。

默认情况下,超过一个月的备份将于每月第一天凌晨 12 点删除

#### crontab.store 的职位

## 日志修剪

日志修剪会从 /opt/zimbra/mailboxd/logs 中删除超过八天的日志。该作业于 2:30 运行  
是

## 清理隔离目录

被识别为病毒或垃圾邮件的邮件不会立即被删除,而是被隔离。超过七天的邮件每天凌晨 1:00 会被删除。

## 桌子保养

ANALYZE TABLE 语句在数据库中的所有表上运行,以更新所有索引的统计信息。这样做是为了确保 SQL 查询优化器在执行 SQL 语句时选择正确的索引。此脚本于周日凌晨 1:30 运行。

## 报告任何数据库不一致的情况

zmdbintegrityreport 每周运行一次,检查 SQL 数据库是否损坏,如果发现任何损坏,将通知管理员。运行此操作时,可能会消耗大量 I/O。如果您发现这是一个问题,您可能需要通过编辑 Zimbra crontab 条目来更改 zmdbintegrityreport 的运行频率。此报告于周日晚上 11:00 运行。

大型网站可以通过设置来禁用此功能:

`zmlocalconfig -e zmdbintegrityreport_disabled=TRUE`

重击

如果您选择禁用此功能,建议在正常维护时段内以及运行任何 Zimbra 升级之前手动运行完整性报告。

## 监视多个 mysqld 以防止损坏

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。该脚本每 5 分钟运行一次。

## crontab.logger 的任务

### 进程日志

zmlogprocess 每 10 分钟运行一次,以解析日志并生成 MTA 指标 (as/av、volume、count 等)。

### 每日报告

安装 logger 包后,crontab 中会自动安排每日邮件报告。报告每天上午 11:30 运行并发送到管理员的电子邮件地址。

### crontab.mta 的职位

## 队列日志记录

通过系统日志查看 zmqueue 报告状态。这是记录器数据。状态每 10 分钟更新一次。

## 垃圾邮件培训

启用 zmtrainsa 脚本可将已分类为垃圾邮件或非垃圾邮件的邮件提供给 SpamAssassin 应用程序。SpamAssassin 会了解哪些迹象可能表示垃圾邮件或非垃圾邮件。此作业应仅在一个 Zimbra MTA 上运行。作业于晚上 11:00 运行

## 垃圾邮件培训清理

zmtrainsa 每天清空垃圾邮件和正常邮件邮箱。该任务于晚上 11:45 运行

## 垃圾邮件贝叶斯自动过期

Spam Bayes 自动过期维护 SpamAssassin Bayes 数据库。这使数据库保持可管理的大小，确保垃圾邮件处理尽可能快。该服务每天晚上 11:20 运行。

## 清理 amavisd/tmp

此作业用于清理 amavisd 临时文件。它于上午 5:15 和晚上 8:15 运行。

## 单服务器 Crontab -l 示例

88 的示例。      输出      crontab -l

```

# ZIMBRASTART 请勿编辑此行和 ZIMBRAEND 之间的任何内容
#
# 日志修剪
#
30 2 * * * 查找 /opt/zimbra/log/-type f -name *.log* -mtime +8 -exec rm {} \; > /dev/null 2>&1

35 2 * * * find /opt/zimbra/log/ -type f -name *.out.?????????? -mtime +8 -exec rm {} \; > /dev/null 2>&1

#
# 状态记录
#
*/2 * * * * /opt/zimbra/libexec/zmstatuslog
#
# 备份
#
# 备份开始
# 备份结束
#
# crontab.ldap
#
#
#
# crontab.store
#
# 日志修剪
#
30 2 * * * 查找 /opt/zimbra/mailboxd/logs/ -type f -name \*log\* -mtime +8 -exec rm {} \; > /dev/null 2>&1 30 2 * * * 查找 /opt/zimbra/log/ -type f -name stacktrace.* -mtime
+8 -exec rm {} \; > /dev/null 2>&1

#
# 表维护
#
30 1 * * 7 /opt/zimbra/libexec/zmmaintainables >> /dev/null 2>&1
#

## 报告任何数据库不一致的情况
#
0 23 * * 7 /opt/zimbra/libexec/zmdbintegrityreport -m
#
# 监控多个 mysqld 以防止损坏

*/5 * * * * /opt/zimbra/libexec/zmcheckduplicatemySQL -e > /dev/null 2>&1
#
# crontab.logger
#
# 进程日志
#
00,10,20,30,40,50* * * * * /opt/zimbra/libexec/zmlogprocess > /tmp/logprocess.out 2>&1
#
# 图生成
#
10 * * * * * /opt/zimbra/libexec/zmgengraphs >> /tmp/gengraphs.out 2>&1
#
# 每日报 10 1 * * * /opt/
zimbra/libexec/zmdailyreport -m
#

```

```

#
crontab 脚本
#
#
# 队列日志
#
0,10,20,30,40,50* * * * * /opt/zimbra/libexec/zmqueueuelog
#
# 垃圾邮件训练 0 23 * * * /opt/
zimbra/bin/zmtrainsa >> /opt/zimbra/log/spamtrain.log 2>&1
#
# 垃圾邮件训练清理
#
45 23 * * * /opt/zimbra/bin/zmtrainsa --cleanup >> /opt/zimbra/log/spamtrain.log 2>&1
#
# Dspam 清理
#
0 1 * * * [ -d /opt/zimbra/data/dspam/data/z/i/zimbra/zimbra.sig ] && 查找
/opt/zimbra/dspam/var/dspam/data/z/i/zimbra/zimbra.sig/ -type f -name \*sig -mtime +7 -exec rm {} \; > /dev/null 2>&1 8 4 * * *
[ -f /opt/zimbra/data/dspam/system.log ] && /opt/zimbra/dspam/bin/dspam_logrotate -a 60 -l /opt/zimbra/data/dspam/system.log 8 8 * * * [ -f /opt/
zimbra/data/dspam/data/z/i/zimbra/zimbra.log ] &&
/opt/zimbra/dspam/bin/dspam_logrotate -a 60 -l /opt/zimbra/data/dspam/data/z/i/
zimbra/zimbra.log
#
# 垃圾邮件贝叶斯自动过期
#
20 23 * * * /opt/zimbra/libexec/sa-learn -p /opt/zimbra/conf/salocal.cf --dbpath /opt/zimbra/data/amavisd/.spamassassin --siteconfigpath /opt/zimbra/
conf/spamassassin -- force-expire --sync > /dev/null 2>&1

#
# 清理 amavisd/tmp
#
15 5,20 * * * 查找 /opt/zimbra/data/amavisd/tmp -maxdepth 1 -type d -name amavis-* -mtime +1 -exec rm -rf {} \; > /dev/null 2>&1

#
# 清理隔离目录
#
0 1 * * * 查找 /opt/zimbra/data/amavisd/quarantine -type f -mtime +7 -exec rm -f {} \; > /dev/null 2>&1

```

ZIMBRAEND 请勿编辑此行和 ZIMBRASTART 之间的任何内容

## 使用 SimpleSAMLphp 和 SAML 进行 Zimbra 单点登录

您知道 Zimbra 支持 SAML 单点登录吗?SAML 是一种开放标准,允许您为组织中的所有应用程序提供单一登录页面。SAML 是 Zimbra 网络版功能。设置 SAML 门户后,您可以轻松添加 [多因素身份验证] (多因素身份验证)。

### 在 SimpleSAMLphp 中设置 Zimbra SP

在 SAML 术语中,应用程序称为服务提供商或 SP。提供用户数据库并负责身份验证的服务在 SAML 术语中称为身份提供商或 IDP。通常,您只有一个 IDP,而 SP 的数量与应用程序的数量相同。在此示例中,我们将 Zimbra 设置为 SAML SP,并使用 SimpleSAMLphp 作为 IDP。这是 SimpleSAMLphp 上所需的配置 (位于/etc/simplesamlphp/metadata/saml20-sp-remote.php中) :

```
$元数据[ https://zimbra.example.com/service/extension/samlreceiver ] = [
    simpleaml.attributes          => 正确,
    metadata-set      => saml20-sp-remote , debug
    => TRUE,
    AssertionConsumerService   = [
        [
            Binding  => urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST , Location =>; https://
            zimbra.example.com/service/extension/samlreceiver , index => 0, isDefault => true,
        ],
    ],
    单一注销服务  => [
        [
            Binding  => urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect , Location => https://
            zimbra.example.com/service/extension/samlLogout ,
        ],
    ],
    NameIDFormat  => urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress , authproc => array( 10 =>
        array( class =>
            saml:AttributeNameID , identifyingAttribute =>
                mail , Format =>
                    urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress ,
            ),
        )
    );
];
```

您还需要获取用于从 IDP 向 Zimbra 签署 SAML 请求的 X.509 公共证书。您需要下载它并将其保存在您的 Zimbra 服务器上。本指南假设您将证书存储在/tmp/idpcert.pem SimpleSAMLphp 设置指南中,您可以在/etc/simplesamlphp/cert/server.crt找到该证书。

, 不要忘记chown zimbra:zimbra /tmp/idpcert.pem。

如果你遵循

### 设置 Zimbra

添加文件/opt/zimbra/conf/saml/saml-config.properties以在 Zimbra 中配置 SAML,添加内容:

```

# 发行人
saml_sp_entity_id=https://zimbra.example.com/service/extension/samlreceiver # 服务提供商的登录接收器 saml_acs=https://
zimbra.example.com/service/extension/samlreceiver # IDP 在 SAMLResponse
中使用的名称 ID 格式 saml_name_id_format=urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

# 发行日期格式
saml_date_format_instant=yyyy-MM-dd T HH:mm:ss Z
# 身份提供者登录端点的重定向方法

saml_redirect_login_destination=https://saml.example.tk/simplesaml/saml2/idp/SSOService.php?spentityid=https://zimbra.example.com/service/extension/samlreceiver
# POST 方法的身份提供者登录端点 saml_post_login_destination= # 重定向方法的身份提供者注销端点

saml_redirect_logout_destination=https://saml.example.tk/simplesaml/saml2/idp/SingleLogoutService.php # POST 方法的身份提供者注销端点 saml_post_logout_destination= #
如果我们
是登录页面注销端点,则注销重定向页面 saml_landing_logout_redirect_url=/ # 禁用受众路径检查
saml_skip_audience_restriction=true # 向用户发送带
有 error_code,error_msg 查询参数的 URL。默认结果为 HTTP

错误代码页面。
saml_error_redirect_url= # SAML 注销文档编
码和 SAML 登录接收器参数编码。saml_document_encoding=ASCII # 设置为 true 以禁用受众路径检查。saml_skip_audience_restriction=false

# 如果用户的 Zimbra 帐户未处于活动状态,则向用户发送重定向位置。
saml_inactive_account_redirect_url

```

以root用户身份从命令行复制samlextn.jar并设置 IDP 证书：

```

mkdir /opt/zimbra/lib/ext/saml cp /opt/zimbra/
extensions-network-extra/saml/samlextn.jar /opt/zimbra/lib/ext/saml/ su - zimbra

cat /tmp/idpcert.pem |xargs -0 zmprov md exampledomain.com zimbraMyoneloginSamlSigningCert zmprov mcf zimbraCsrfRefererCheckEnabled FALSE zmmailboxdctl 重启

```

## 创建用户

您的用户帐户必须在 Zimbra 中手动创建,并且可在 IDP 用户数据库中使用。重要的是,您的 IDP 中的电子邮件属性必须与 Zimbra 帐户名完全相同。否则用户将无法登录。如果不起作用,请在执行身份验证请求时运行tail -f /opt/zimbra/log/\* ,然后深入研究日志以找出问题所在。要 grep 的关键字:SAML、受众和断言。

## saml-config.properties中的可配置属性

samlextn.jar 使用位于以下位置的属性文件： \${zimbra\_home}/conf/saml/saml-config.properties。

支持以下属性：

钥匙	描述	默认	选修的
saml_sp_entity_id	发行人		
saml_acs	登录接收器 对于 服务 提供者		
saml_redirect_login_destination	身份 提供商登录 终点 重定向 方法		
saml_redirect_logout_destination	身份 提供者 登出 终点 重定向 方法		
saml_post_login_destination	身份 提供商登录 终点 POST 方法 (未使用)		✓
saml_post_logout_destination	身份 提供者 登出 终点 POST 方法 (未使用)		✓
saml_name_id_格式	姓名 ID 格式 国内流离失所者 使用在 SAML响应	urn:oasis:names:tc:SAML:1.1:nameid- 格式:未指定	✓
saml_date_format_instant	日期格式 针对问题 立即的	yyyy-MM-dd T HH:mm:ss Z	✓

钥匙	描述	默认	选修的
saml_error_redirect_url	发送网址 用户 我错误代码， 错误消息 查询参数。 默认 结果是 HTTP 错误 代码页。		✓
saml_landing_logout_redirect_url	登出 重定向 登陆页面 如果我们是 上次注销 服务。	/	✓
saml_document_encoding	SAML 登出 文档 编码,以及 <b>SAML 登录</b> 接收者 范围 编码。	ASCII	✓
saml_skip_audience_restriction	设置为 true 禁用 观众路径 查看。	错误的	✓
saml_inactive_account_redirect_url 重定向	位置至 发送用户 如果他们的 Zimbra 帐户 未处于活动状态。	/服务/扩展/samllogout	✓

## SLO 端点

如果您需要支持从 IDP 发起的 SLO,则需要 SLO URL: <https://zimbra.example.com/service/extension/samlslslo>

此外,如果您想在用户点击 Zimbra 中的注销时触发 IDP 注销,您必须将 Zimbra 配置为使用此注销 URL: <https://zimbra.example.com/service/extension/samllogout>。

## CsrfRefererCheck

在大多数情况下,在 Zimbra 9 上,您需要禁用 SAML 的 CsrfRefererCheck 并重新启动邮箱服务才能工作。

与 - zimbra

```
zmprov mcf zimbraCsrfRefererCheckEnabled FALSE zmmailboxdctl 重启
```

## 词汇表

术语表列出了本文档中使用的术语和首字母缩略词,包括行业术语和特定应用术语。如果产品中以特定方式实施了一般行业概念或实践,也会注明。

### 记录

A (代表“地址”)记录将主机名映射到数字 IP 地址。对于 Zimbra,A 记录是 Zimbra 服务器的 IP 地址。

### ABQ

允许/阻止/隔离功能使系统管理员可以控制哪些设备可以通过 ActiveSync 同步。

### Zimbra 管理控制台

中显示的帐户策略服务类别。

### 广告

Microsoft Active Directory 服务器。在 Zimbra Collaboration 中用作身份验证和 GAL 的可选选择,与 OpenLDAP 一起用于所有其他 Zimbra Collaboration 功能。

### 别名

“也称为”电子邮件地址,应路由到其他电子邮件地址的用户。

### 属性

包含目录服务器条目的对象相关数据。属性存储服务器主机名或电子邮件转发地址等信息。

### 验证

使用用户提供的登录信息来验证用户进入系统的权限的过程。

### 黑名单

反垃圾邮件术语,表示已知的恶意 IP 地址。这可能是被垃圾邮件发送者劫持的 IP 地址,也可能是来自维护不善但合法的网站,允许未经授权的人员转发邮件。

### 大对象

二进制大对象。

### 服务等级 (COS)

描述 Zimbra Collaboration LDAP 数据架构中的对象,其中包含用户邮件配额等设置。每个 Zimbra Collaboration 帐户都包含一个 COS,帐户会从所选 COS 继承所有设置。

### 命令行界面

命令行界面。用于指代 Zimbra Collaboration 命令行工具的集合,例如作为zmprov。

### 簇

一种高可用性网络配置,使用服务器(节点)集群。如果一台服务器发生故障或脱离网络,备用服务器将接管。

## 联系方式

在 Zimbra Collaboration 中,联系人是一个用户界面功能,列出了用户个人收集的地址和联系信息。

## 对话

在 Zimbra Collaboration 中,对话是一种用户界面功能,可将电子邮件线程(具有相同主题行的电子邮件)显示为单个对话列表。用户可以展开对话以查看其中的所有电子邮件。

## 动态HTML

动态 HTML。Zimbra Classic Web App 中采用的一项技术。

## DNS

域名系统是一种 Internet 目录服务。DNS 是将域名转换为 IP 地址的方式,DNS 还控制电子邮件传递。正确配置 DNS 是 Postfix 将消息路由到远程目的地所必需的

## Edge MTA通

用术语,用于指代作为处理传入电子邮件流量第一道防线的任何邮件传输代理。Edge MTA 上可能出现的功能包括垃圾邮件过滤。

## 入口

目录服务器中的项目,例如帐户或邮件主机。

## 短暂数据

本质上短暂存在或快速变化的数据。登录时间戳、身份验证令牌等。

## 故障转移

接管过程,其中备用服务器检测到主服务器不可用,并且备用服务器接管该服务器的处理。

## 完整限定域名 (FQDN)

完全限定域名。主机名和主机路径。例如, www.zimbra.com是一个完全限定域名,其中www是主机, zimbra是二级域名, .com是顶级域名。

## 加拉帕戈斯

全局地址列表,即 Outlook 版的公司目录。列出组织内所有员工的联系信息,包括电子邮件地址。

## 全局配置

Zimbra 协作对象包含服务器和服务类别的默认设置。

## 高可用性

高可用性,缩写为 HA,是指计算机系统中的组件发生故障时,系统中资源的可用性。

## HTTP

超文本传输协议,与 SOAP 一起用于 UI 集成。

## 信息访问协议

互联网消息访问协议是一种像本地用户一样从远程消息存储库访问邮件的方法。

## 店铺

在 Zimbra Collaboration 中,有一个目录区域,用于存储特定邮箱服务器上邮件消息的所有索引信息。

## 索引解析传

入电子邮件消息中的搜索词的过程。

## Java

Java 是一种行业标准的面向对象编程语言。用于核心 Zimbra Collaboration 应用服务器。

## JavaScript脚

本主要由 Netscape 开发,可以与 HTML 源代码交互。Zimbra Classic Web App 中使用的技术。

## LDAP

轻量级目录访问协议,一种用于身份验证的行业标准协议。

## 低密度聚乙烯

本地邮件传输协议,用于将消息从 Postfix MTA 传输到 Zimbra 协作服务器进行最终传递。

## 邮箱服务器

Zimbra 协作服务器的替代术语。

## 映射接口

消息应用程序编程接口。Microsoft Windows 内置的一个系统,用于使不同的电子邮件应用程序能够协同工作。

## 消息存储

在 Zimbra Collaboration 中,有一个目录区域,用于存储特定邮箱服务器上的邮件消息。

## 丙二醛

邮件传递代理,有时也称为邮件主机。Zimbra 协作服务器充当 MDA。

## 元数据

描述其他数据 (而非实际内容)的数据。在 Zimbra Collaboration 中,元数据包括用户文件夹、线程、消息标题和标签以及指针。

## 哑剧

多用途互联网邮件扩展,一种格式化非 ASCII 互联网消息内容 (如图像文件)的规范。用于在消息存储中存储消息的格式。

大都会运输署

消息传输代理。MTA 是一个在机器之间传递和传输邮件的程序。Zimbra Collaboration 部署假定 Postfix MTA 和边缘 MTA。

## MX 记录

邮件交换。MX 记录是域名数据库中的条目，用于标识负责处理该域名电子邮件的邮件服务器。电子邮件系统依靠 DNS MX 记录在域之间传输电子邮件。处理邮件时，先检查 MX 记录，然后再检查目标地址的 A 记录。

## 真相

“不在办公室”的常用简写，用于发送休假信息。

## 开源

指由用户群体创建的用于非商业分发的软件，其中源代码是公开的而不是专有的。

## 你

操作系统，例如 Linux、UNIX 或 Microsoft Windows。

流行音乐

邮局协议用于通过 TCP/IP 从远程服务器检索电子邮件并将其保存到本地计算机。

## 配置创建帐户或其

他数据的过程，通常以批量或自动的方式。

## RBH

实时黑洞。通常指作为公共服务提供已知不良 IP 地址列表的网站，这些地址的邮件应被阻止，因为这些服务器要么是已知的垃圾邮件发送者，要么是不安全的并且被垃圾邮件发送者利用。

## 响应式（网络应用程序）

这种设计方法可确保应用程序在各种设备和窗口或屏幕尺寸上都能正常显示和运行。现代 Web 应用程序是一种响应式 Web 应用程序，可实现一致的用户体验  
在任何屏幕上。

## 重做日志

Zimbra 协作服务器的详细事务日志，用于重放和复制。

存储区域网络

存储阵列网络。高可用性数据存储区域。

## 架构

描述特定组织站点的目录服务所使用的数据结构。

邮件传输协议

简单邮件传输协议。用于 Edge MTA 和 Postfix 之间的 Zimbra Collaboration 部署

大都会运输署。

简单网络管理协议

简单网络监控协议。监控软件使用它从系统日志中找出严重错误。

## 肥皂

简单对象访问协议,一种基于 XML 的消息传递协议,用于发送 Web 服务请求。

Zimbra Collaboration 服务器使用 SOAP 接收和处理请求,这些请求可以来自 Zimbra Collaboration 命令行工具或 Zimbra Collaboration 用户界面。

## 垃圾邮件

未经请求的商业电子邮件。垃圾邮件发送者将其输出称为“批量商业电子邮件”。

## SQL

结构化查询语言,用于查找消息存储中的消息。

## SSL

安全套接字层。

## 标签

Zimbra Classic Web App 的一项功能。用户可以定义标签并将其应用于邮件消息以供搜索。

## 总拥有成本

总拥有成本。Zimbra Collaboration 通过减少对服务器硬件、操作系统许可费用、支持应用程序许可费用、磁盘存储要求和人员 (IT、服务台、咨询) 的要求来降低总拥有成本 (TCO)。

## TLS

传输层安全性。

## 高等教育委员会

未经请求的商业电子邮件,也称为垃圾邮件。

## 虚拟别名

Postfix MTA 中识别的一种邮件别名。

## 白名单

反垃圾邮件术语,指已知的优质邮件或 IP 地址。来自此类地址的邮件可能会被“自动信任”。

## XML

扩展标记语言。

## Zimbra 管理控制台

Zimbra Collaboration 管理员界面。

## Zimbra Web 客户端

指作为 Zimbra 服务器的一部分通过 Web 提供的任何最终用户界面。

最后更新时间 2024-08-27 13:03:53 +0530