aws

管理员指南

Amazon WorkMail

版本 1.0

Amazon WorkMail: 管理员指南

Table of Contents

什么是 Amazon WorkMail？

Amazon WorkMail 是一种安全的托管式企业电子邮件和日历服务，支持用于现有桌面和移动电子邮件客户端。Amazon WorkMail 用户可以使用 Microsoft Outlook、浏览器或本机 iOS 和 Android 电子邮件应用程序访问其电子邮件、联系人和日历。您可以将 Amazon WorkMail 与您现有的企业目录集成，并控制对数据和数据存储位置进行加密的两个密钥。

有关支持的 AWS 区域和端点的列表，请参阅 AWS 区域和端点。

主题

Amazon WorkMail 系统要求

当您的 Amazon WorkMail 管理员邀请您登录 Amazon WorkMail 账户时，您可以使用 Amazon WorkMail Web 客户端进行登录。

Amazon WorkMail 还适用于支持 Exchange ActiveSync 协议的所有主流移动设备和操作系统。这些设备包括 iPad、iPhone、Android 和 Windows Phone。macOS 用户可以将其 Amazon WorkMail 账户添加到其“邮件”、“日历”和“联系人”应用。

Amazon WorkMail 支持以下操作系统版本：

- Windows：Windows 7 SP1 或更高版本
- MacOS：MacOS 10.12（Sierra）或更高版本
- Android：Andriod 5.0 或更高版本
- iPhone：iOS 5 或更高版本
- Windows Phone：Windows 8.1 或更高版本
- Blackberry：Blackberry OS 10.3.3.3216

如果您具有有效的 Microsoft Outlook 许可证，则可以使用以下 Microsoft Outlook 版本访问 Amazon WorkMail：

- Outlook 2013 或更高版本
- Outlook 2013 Click-to-Run 或更高版本
- Outlook for Mac 2016 或更高版本

您可以使用以下浏览器版本访问 Amazon WorkMail Web 客户端：

- Google Chrome：版本 22 或更高版本
- Mozilla Firefox：版本 27 或更高版本
- Safari：版本 7 或更高版本
- Internet Explorer：版本 11
- Microsoft Edge

您还可以将 Amazon WorkMail 与您首选的 IMAP 客户端结合使用。

Amazon WorkMail 概念

下面将介绍便于您了解和使用 Amazon WorkMail 的核心术语和概念。

组织

Amazon WorkMail 的租户设置。

别名

用于标识您的组织的全局唯一名称。别名用于访问 Amazon WorkMail Web 应用程序 (https://*alias*.awsapps.com/mail)。

域

电子邮件地址中 @ 符号后面的 Web 地址。您可以添加一个域来接收邮件并将其发送到您组织中的邮箱。

测试邮件域

在设置过程中会自动配置一个可用于测试 Amazon WorkMail 的域。测试邮件域为 *alias*.awsapps.com。如果您没有配置自己的域，则使用它作为默认域。测试邮件域受不同限制的约束。有关更多信息，请参阅 Amazon WorkMail 配额。

目录

在 AWS Directory Service 中创建的 AWS Simple AD、AWS Managed AD 或 AD Connector。如果您使用 Amazon WorkMail 快速设置功能创建组织，我们会为您创建一个 WorkMail 目录。您无法在 AWS Directory Service 中查看 WorkMail 目录。

用户

在 AWS Directory Service 中创建的用户。可以采用 USER 或 REMOTE_USER 角色创建用户。使用 USER 角色创建并启用用户后，他们将获得自己的邮箱以进行访问。当禁用了用户后，他们将无法访问 Amazon WorkMail.。

使用 REMOTE_USER 角色创建和启用的用户将列在通讯簿中，但在 Amazon WorkMail 中未获得邮箱。REMOTE_USER 可以将邮箱托管在 Amazon WorkMail 外部，但仍将作为在 Amazon WorkMail 通讯簿中拥有邮箱的任何其他用户列出，并且可以相互查找日历以查找忙/闲信息。

组

在 AWS Directory Service 中使用的组。组可用作 Amazon WorkMail 中的通讯组列表或安全组。组没有自己的邮箱。

资源

资源表示可供 Amazon WorkMail 用户预订的会议室或设备资源。

移动设备策略

控制移动设备的安全功能和行为的各种 IT 策略规则。

相关 AWS 服务

以下服务可与 Amazon WorkMail 结合使用：

- AWS Directory Service - 您可以将 Amazon WorkMail 与现有的 AWS Simple AD、AWS Managed AD 或 AD Connector 集成。在 AWS Directory Service 中创建一个目录，然后为此目录启用 Amazon WorkMail。在配置了此集成后，您可以从现有目录中的用户列表中选择要为 Amazon WorkMail 启用的用户，以便这些用户可以使用其现有的 Active Directory 凭证登录。有关更多信息，请参阅 AWS Directory Service 管理指南。
- Amazon Simple Email Service - Amazon WorkMail 使用 Amazon SES 发送所有传出电子邮件。测试邮件域和您的域可用于在 Amazon SES 控制台中进行管理。从 Amazon WorkMail 发送的传出电子邮件不产生任何费用。有关更多信息，请参阅 Amazon Simple Email Service 开发人员指南。

- AWS Identity and Access Management – AWS 管理控制台需要您提供用户名和密码，这样您使用的任何服务才能确定您是否有权访问其资源。我们建议您不要使用 AWS 账户凭证访问 AWS，因为无法使用任何方法来撤销或限制 AWS 账户凭证。相反，我们建议您创建一个 IAM 用户，并将该用户添加到具有管理权限的 IAM 组。然后，您可以使用该 IAM 用户凭证访问控制台。

  如果您已注册 AWS，但尚未为自己创建 IAM 用户，则可以使用 IAM 控制台自行创建。有关更多信息，请参阅《IAM 用户指南》中的创建单个 IAM 用户。
- AWS Key Management Service - Amazon WorkMail 与 AWS KMS 集成以对客户数据进行加密。可以从 AWS KMS 控制台执行密钥管理。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的什么是 AWS Key Management Service。

Amazon WorkMail 定价

Amazon WorkMail 没有预付费用或预先承诺。您只需为活动用户账户付费。有关定价的更多具体信息，请参阅定价。

Amazon WorkMail 资源

下列相关资源在您使用此服务的过程中会有所帮助。

- 课程和研讨会 – 指向基于角色的专业课程和自主进度动手实验室的链接，这些课程和实验室旨在帮助您增强 AWS 技能并获得实践经验。
- AWS 开发人员中心 – 浏览教程、下载工具并了解 AWS 开发人员活动。
- AWS 开发人员工具 – 指向开发人员工具、开发工具包、IDE 工具包和命令行工具的链接，这些资源用于开发和管理 AWS 应用程序。
- 入门资源中心 – 了解如何设置 AWS 账户、加入 AWS 社区和启动您的第一个应用程序。
- 动手实践教程 – 按照分步教程在 AWS 上启动您的第一个应用程序。
- AWS 白皮书 – 指向 AWS 技术白皮书的完整列表的链接，这些资料涵盖了架构、安全性、经济性等主题，由 AWS 解决方案架构师或其他技术专家编写。
- AWS 支持 中心 – 用于创建和管理 AWS 支持 案例的中心。还提供指向其他有用资源的链接，如论坛、技术常见问题、服务运行状况以及AWS Trusted Advisor。
- 支持 – 提供有关 支持 的信息的主要网页，这是一个一对一的快速响应支持渠道，可以帮助您在云中构建和运行应用程序。
- 联系我们 – 用于查询有关 AWS 账单、账户、事件、滥用和其他问题的中央联系点。
- AWS 网站条款：有关我们的版权和商标、您的账户、许可、网站访问和其他主题的详细信息。

先决条件

要充当 Amazon WorkMail 管理员，您需要一个 AWS 账户。如果您尚未注册 AWS，请完成以下任务进行设置。

主题

注册 AWS 账户

如果您还没有 AWS 账户，请完成以下步骤来创建一个。

注册 AWS 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
2. 按照屏幕上的说明操作。

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

   当您注册 AWS 账户 时，系统将会创建一个 AWS 账户根用户。根用户有权访问该账户中的所有 AWS 服务和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

注册过程完成后，AWS 会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册 AWS 账户 后，请保护好您的 AWS 账户根用户，启用 AWS IAM Identity Center，并创建一个管理用户，以避免使用根用户执行日常任务。

保护您的 AWS 账户根用户

1. 选择根用户并输入您的 AWS 账户 电子邮件地址，以账户拥有者身份登录 AWS 管理控制台。在下一页上，输入您的密码。

要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的 Signing in as the root user。

2. 为您的根用户启用多重身份验证（MFA）。

   有关说明，请参阅《IAM 用户指南》中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Enabling AWS IAM Identity Center。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

   有关如何使用 IAM Identity Center 目录 作为身份源的教程，请参阅《AWS IAM Identity Center 用户指南》中的 Configure user access with the default IAM Identity Center 目录。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

  要获取使用 IAM Identity Center 用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的 Signing in to the AWS access portal。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Create a permission set。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Add groups。

向 IAM 用户授予 Amazon WorkMail 的权限

默认情况下，IAM 用户无权管理 Amazon WorkMail 资源。您必须附加 AWS 托管式策略（AmazonWorkMailFullAccess a或 AmazonWorkMailReadOnlyAccess），或者创建客户管理型策略，以明确授予 IAM 用户这些权限。然后，将此策略附加到需要这些权限的 IAM 用户或组。有关更多信息，请参阅 适用于 Amazon WorkMail 的 Identity and Access Management。

Amazon WorkMail 中的安全性

AWS 十分重视云安全性。作为 AWS 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

安全性是 AWS 和您的共同责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS负责保护在AWS云中运行AWS服务的基础架构。AWS还向您提供可安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于 Amazon WorkMail 的合规性计划，请参阅合规性计划范围内的 AWS 服务。
- 云中的安全性：您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档将帮助您了解如何在使用 Amazon WorkMail 时应用责任共担模式。以下主题说明了如何配置 Amazon WorkMail 以实现您的安全性和合规性目标。您还会了解如何使用其它 AWS 服务来帮助您监控和保护 Amazon WorkMail 资源。

主题

Amazon WorkMail 中的数据保护

AWS 责任共担模式适用于 Amazon WorkMail 中的数据保护。如该模式中所述，AWS 负责保护运行所有 AWS 云 的全球基础结构。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

出于数据保护目的，建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management（IAM）设置单个用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与 AWS 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 AWS CloudTrail 设置 API 和用户活动日记账记录。有关使用 CloudTrail 跟踪来捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的使用 CloudTrail 跟踪。
- 使用 AWS 加密解决方案以及 AWS 服务中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括当您使用控制台、API、AWS CLI 或 AWS SDK 使用 Amazon WorkMail 或其他 AWS 服务时。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

Amazon WorkMail 如何使用 AWS KMS

Amazon WorkMail 在将所有 Amazon WorkMail 组织的邮箱中的所有邮件写入磁盘之前会以透明方式对这些邮件进行加密，并在用户访问这些邮件时以透明方式对其进行解密。您不能禁用加密。为了确保用于保护消息的加密密钥的安全，Amazon WorkMail 将与 AWS Key Management Service (AWS KMS) 集成。

Amazon WorkMail 还提供了一个使用户能够发送已签名或加密的电子邮件的选项。此加密功能不使用 AWS KMS。有关更多信息，请参阅 启用已签名或已加密的电子邮件。

主题

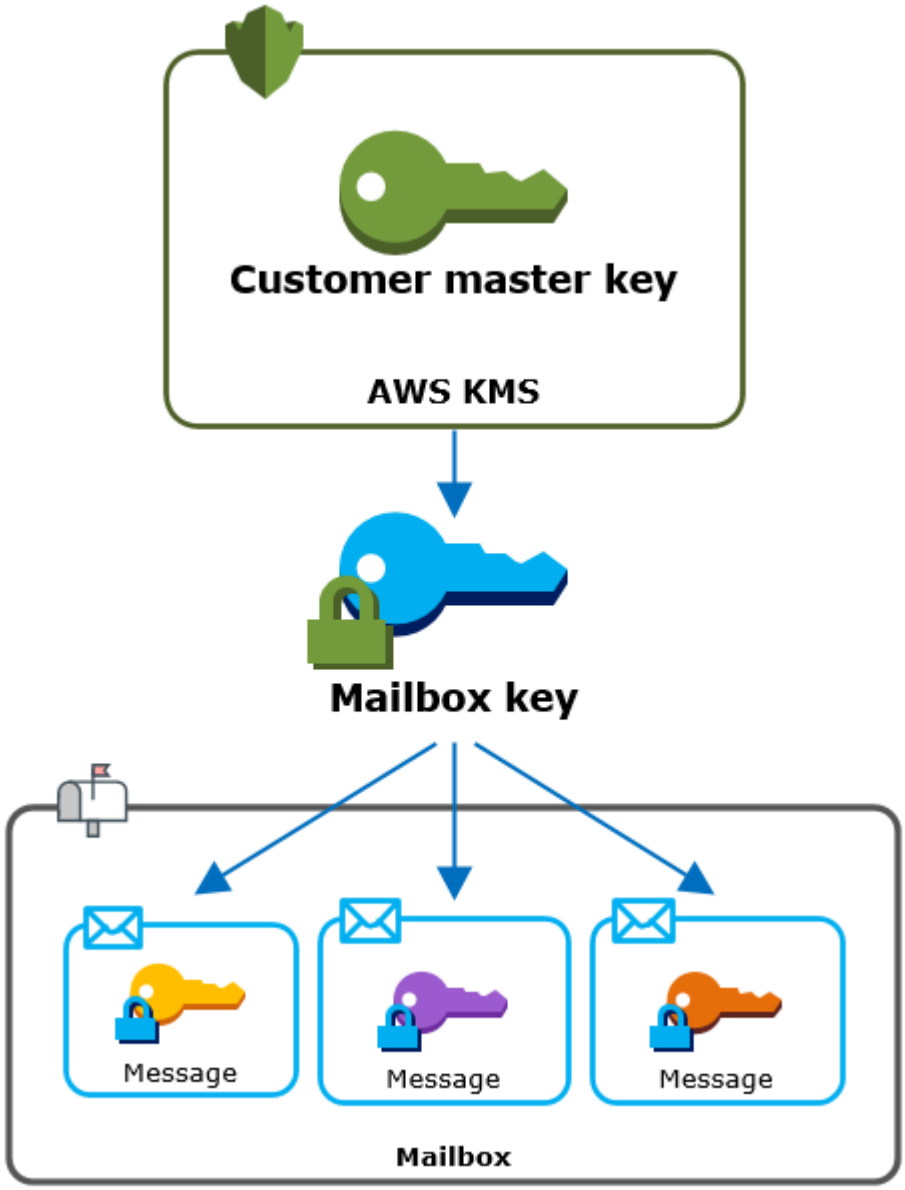
- Amazon WorkMail 加密
- 授权使用 CMK
- Amazon WorkMail 加密上下文
- 监控 Amazon WorkMail 与 AWS KMS 的交互

Amazon WorkMail 加密

在 Amazon WorkMail 中，每个组织可以包含多个邮箱，组织中的每个用户都有一个邮箱。所有消息（包括电子邮件和日历项）都存储在用户的邮箱中。

为了保护 Amazon WorkMail 组织中邮箱的内容，Amazon WorkMail 会在所有邮箱消息写入磁盘之前对其进行加密。任何客户提供的信息均为明文形式存储。

每条消息都使用唯一的数据加密密钥进行加密。邮件密钥受邮箱密钥保护，邮箱密钥是仅用于该邮箱的唯一加密密钥。对于始终对 AWS KMS 加密的组织，使用 AWS KMS 客户主密钥 (CMK) 对邮箱密钥进行加密。下图显示了 AWS KMS 中加密消息、加密消息密钥、加密邮箱密钥和组织中 CMK 之间的关系。



为组织设置 CMK

在创建 Amazon WorkMail 组织时，您可以为组织选择 AWS KMS 客户主密钥 (CMK)。此 CMK 保护该组织中的所有邮箱密钥。

您可以为 Amazon WorkMail 选择默认的 AWS 托管 CMK，也可以选择自己拥有和管理的现有客户托管 CMK。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的客户主密钥 (CMKs)。您可以为每个组织选择相同的 CMK 或不同的 CMK，但一旦选择 CMK，就无法更改它。

> **Important**
>
> Amazon WorkMail 仅支持对称 CMK。您不能使用非对称 CMK。要获取确定 CMK 是对称还是非对称密钥的帮助，请参阅《AWS Key Management Service 开发人员指南》中的识别对称和非对称 CMK。

要查找组织的 CMK，请使用记录对 AWS CloudTrail 的调用的 AWS KMS 日志条目。

每个邮箱的唯一加密密钥

当您创建邮箱时，Amazon WorkMail 会在 AWS KMS 外部为邮箱生成唯一的 256 位高级加密标准 (AES) 对称加密密钥，称为其“邮箱密钥”。Amazon WorkMail 使用邮箱密钥来保护邮箱中每封邮件的加密密钥。

为了保护邮箱密钥，Amazon WorkMail 调用 AWS KMS 来使用组织的 CMK 加密邮箱密钥。然后，它将加密的邮箱密钥存储在邮箱元数据中。

> **Note**
>
> Amazon WorkMail 使用对称邮箱加密密钥来保护消息密钥。以前，Amazon WorkMail 使用非对称密钥对来保护每个邮箱。它使用公有密钥加密每个消息密钥，并使用私有密钥解密该密钥。私有邮箱密钥受组织的 CMK 保护。较旧的邮箱可能使用非对称邮箱密钥对。此更改不会影响邮箱或其消息的安全。

加密每封邮件

当用户将邮件添加到邮箱时，Amazon WorkMail 会在 AWS KMS 外部为邮件生成一个唯一的 256 位 AES 对称加密密钥。它使用这个消息密钥对消息进行加密。Amazon WorkMail 会在邮箱密钥下加密消息密钥，并将加密的消息密钥与消息一起存储。然后，它使用组织的 CMK 加密邮箱密钥。

创建新邮箱

当 Amazon WorkMail 创建邮箱时，它会使用以下过程准备邮箱以保存加密的邮件。

- Amazon WorkMail 会在 AWS KMS 外部为邮箱生成一个唯一的 256 位 AES 对称加密密钥。
- Amazon WorkMail 调用 AWS KMS Encrypt 操作。它为组织传入邮箱密钥和客户主密钥 (CMK) 的标识符。AWS KMS 返回使用 CMK 加密的邮箱密钥的密文。
- Amazon WorkMail 将加密的邮箱密钥与邮箱元数据一起存储。

加密邮箱消息

要加密消息，Amazon WorkMail 使用以下过程。

1. Amazon WorkMail 为消息生成一个唯一的 256 位 AES 对称密钥。它使用明文消息密钥和高级加密标准 (AES) 算法在 AWS KMS 外加密消息。
2. 为保护邮箱密钥下的消息密钥，Amazon WorkMail 需要解密邮箱密钥（它始终以加密形式存储）。

   Amazon WorkMail 调用 AWS KMS Decrypt 操作，并传入加密的邮箱密钥。AWS KMS 使用组织的 CMK 解密邮箱密钥，并将明文邮箱密钥返回到 Amazon WorkMail。
3. Amazon WorkMail 使用明文邮箱密钥和高级加密标准 (AES) 算法在 AWS KMS 外加密消息密钥。
4. Amazon WorkMail 将加密的消息密钥存储在加密消息的元数据中，以便对其进行解密。

解密邮箱消息

要解密消息，Amazon WorkMail 使用以下过程。

1. Amazon WorkMail 调用 AWS KMS Decrypt 操作，并传入加密的邮箱密钥。AWS KMS 使用组织的 CMK 解密邮箱密钥，并将明文邮箱密钥返回到 Amazon WorkMail。
2. Amazon WorkMail 使用明文邮箱密钥和高级加密标准 (AES) 算法在 AWS KMS 外对加密的消息密钥进行解密。
3. Amazon WorkMail 使用明文消息密钥来解密加密的消息。

缓存邮箱密钥

为了提高性能并最大限度地减少对 AWS KMS 的调用，Amazon WorkMail 在本地为每个客户端缓存每个明文邮箱密钥最多 1 分钟。在缓存期结束时，将删除邮箱密钥。如果在缓存期间需要该客户端的邮

箱密钥，则 Amazon WorkMail 可以从缓存中获取它而不是调用 AWS KMS。邮箱密钥在缓存中受保护，并且永远不会以明文形式写入磁盘中。

授权使用 CMK

当 Amazon WorkMail 在加密操作中使用客户主密钥 (CMK) 时，它代表邮箱管理员。

要代表您将 AWS KMS 客户主密钥 (CMK) 用于密钥，管理员必须拥有以下权限。您可以在 IAM 策略或密钥策略中指定这些所需的权限。

- `kms:Encrypt`
- `kms:Decrypt`
- `kms:CreateGrant`

要仅允许将 CMK 用于源自 Amazon WorkMail 的请求，可将 kms:ViaService 条件键与 `workmail.<region>.amazonaws.com` 值结合使用。

您还可以在加密上下文中将密钥或值用作将 CMK 用于加密操作的条件。例如，可在 IAM 或密钥策略文档中使用字符串条件运算符，或在授权中使用授权约束。

AWS 托管 CMK 的密钥策略

仅当 Amazon WorkMail 代表用户发出请求时，用于 Amazon WorkMail 的 AWS 托管 CMK 的密钥策略才向用户授予将 CMK 密钥用于指定操作的权限。密钥策略不允许任何用户直接使用 CMK。

此密钥策略与所有 AWS 托管密钥的策略类似，均由该服务来建立。您无法更改密钥策略，但可以随时查看。有关详细信息，请参阅《AWS Key Management Service 开发人员指南》中的查看密钥策略。

密钥策略中的策略语句具有以下影响：

- 仅当 Amazon WorkMail 代表账户和区域中的用户发出请求时，才允许这些用户使用 CMK 执行加密操作和创建授权。`kms:ViaService` 条件密钥可强制实施此限制。
- 允许 AWS 创建 IAM 策略以允许用户查看 CMK 属性和撤销授权。

下面是用于 Amazon WorkMail 的 AWS 托管 CMK 示例的密钥策略。

JSON

```
{
```

```
 "Version":"2012-10-17",
 "Id" : "auto-workmail-1",
 "Statement" : [ {
   "Sid" : "Allow access through WorkMail for all principals in the account that
 are authorized to use WorkMail",
   "Effect" : "Allow",
   "Principal" : {
     "AWS" : "*"
   },
   "Action" : [ "kms:Decrypt", "kms:CreateGrant", "kms:ReEncrypt*",
"kms:DescribeKey", "kms:Encrypt" ],
   "Resource" : "*",
   "Condition" : {
     "StringEquals" : {
       "kms:ViaService" : "workmail.us-east-1.amazonaws.com",
       "kms:CallerAccount" : "111122223333"
     }
   }
 }, {
   "Sid" : "Allow direct access to key metadata to the account",
   "Effect" : "Allow",
   "Principal" : {
     "AWS" : "arn:aws:iam::111122223333:root"
   },
   "Action" : [ "kms:Describe*", "kms:List*", "kms:Get*", "kms:RevokeGrant" ],
   "Resource" : "*"
 } ]
}
```

使用授权来授权 Amazon WorkMail

除了密钥策略之外，Amazon WorkMail 还使用授权向每个组织的 CMK 添加权限。要查看有关账户中 CMK 的授权，请使用 ListGrants 操作。

Amazon WorkMail 使用授权向组织的 CMK 添加以下权限。

- 添加 `kms:Encrypt` 权限以允许 Amazon WorkMail 加密邮箱密钥。
- 添加 `kms:Decrypt` 权限以允许 Amazon WorkMail 使用 CMK 解密邮箱密钥。Amazon WorkMail 在授予中需要此权限，因为读取邮箱消息的请求使用正在阅读消息的用户的安全上下文。该请求不使用 AWS 账户的凭证。当您选择组织的 CMK 时，Amazon WorkMail 会创建此授权。

为了创建授权，Amazon WorkMail 代表创建组织的用户调用 CreateGrant。用于创建授权的权限来自密钥策略。此策略允许账户用户在 Amazon WorkMail 代表授权用户发出请求时对组织的 CMK 调用 `CreateGrant`。

该密钥策略还允许账户根用户撤销对 AWS 托管密钥的授权。但是，如果您撤销授权，Amazon WorkMail 将无法解密邮箱中的已加密数据。

Amazon WorkMail 加密上下文

加密上下文是一组包含任意非机密数据的键值对。在请求中包含加密上下文以加密数据时，AWS KMS 以加密方式将加密上下文绑定到加密的数据。要解密数据，您必须传入相同的加密上下文。有关更多信息，请参阅 AWS Key Management Service 开发人员指南中的加密内容。

Amazon WorkMail 在所有 AWS KMS 加密操作中使用相同的加密上下文格式。您可以使用加密上下文在审计记录和日志中标识加密操作（例如 AWS CloudTrail），并将加密上下文用作在策略和授权中进行授权的条件。

在其对 AWS KMS 的 Encrypt 和 Decrypt 请求中，Amazon WorkMail 使用加密上下文，其中密钥为 `aws:workmail:arn`，值是组织的 Amazon Resource Name (ARN)。

```
"aws:workmail:arn":"arn:aws:workmail:region:account ID:organization/organization-ID"
```

例如，以下加密上下文将示例组织 ARN 包含在欧洲地区（爱尔兰）(`eu-west-1`) 区域中。

```
"aws:workmail:arn":"arn:aws:workmail:eu-west-1:111122223333:organization/m-
a123b4c5de678fg9h0ij1k2lm234no56"
```

监控 Amazon WorkMail 与 AWS KMS 的交互

您可以使用 AWS CloudTrail 和 Amazon CloudWatch Logs 跟踪 Amazon WorkMail 代表您发送到 AWS KMS 的请求。

Encrypt

当您创建邮箱时，Amazon WorkMail 会生成一个邮箱密钥并调用 AWS KMS 来加密邮箱密钥。Amazon WorkMail 使用明文邮箱密钥和 Amazon WorkMail 组织的 CMK 的标识符将 Encrypt 请求发送到 AWS KMS。

记录 `Encrypt` 操作的事件与以下示例事件类似。该用户是 Amazon WorkMail 服务。参数包含 CMK ID (`keyId`) 和 Amazon WorkMail 组织的加密上下文。Amazon WorkMail 还传入邮箱密钥，而不是将它记录在 CloudTrail 日志中。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-19T10:01:09Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Encrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/
m-a123b4c5de678fg9h0ij1k2lm234no56"
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
    },
    "responseElements": null,
    "requestID": "76e96b96-7e24-4faf-a2d6-08ded2eaf63c",
    "eventID": "d5a59c18-128a-4082-aa5b-729f7734626a",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "d08e60f1-097e-4a00-b7e9-10bc3872d50c"
}
```


Decrypt

当您添加、查看或删除邮箱邮件时，Amazon WorkMail 会要求 AWS KMS 来解密邮箱密钥。Amazon WorkMail 使用加密邮箱密钥和 Amazon WorkMail 组织的 CMK 的标识符将 Decrypt 请求发送到 AWS KMS。

记录 Decrypt 操作的事件与以下示例事件类似。该用户是 Amazon WorkMail 服务。参数包含未记录在日志中的加密邮箱密钥（作为加密文字 blob）和 Amazon WorkMail 组织的加密上下文。AWS KMS 从加密文字派生 CMK 的 ID。


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-20T11:51:10Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/
m-a123b4c5de678fg9h0ij1k2lm234no56"
        }
    },
    "responseElements": null,
    "requestID": "4a32dda1-34d9-4100-9718-674b8e0782c9",
    "eventID": "ea9fd966-98e9-4b7b-b377-6e5a397a71de",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "241e1e5b-ff64-427a-a5b3-7949164d0214"
}
```

适用于 Amazon WorkMail 的 Identity and Access Management

AWS Identity and Access Management（IAM）是一项 AWS 服务，可以帮助管理员安全地控制对 AWS 资源的访问。IAM 管理员控制谁可以通过身份验证（登录）和获得授权（具有权限）来使用 Amazon WorkMail 资源。IAM 是一项无需额外费用即可使用的 AWS 服务。

主题

受众

您使用 AWS Identity and Access Management（IAM）的方式因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅 Amazon WorkMail 身份和访问问题排查）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅 Amazon WorkMail 如何与 IAM 结合使用）
- IAM 管理员：编写用于管理访问权限的策略（请参阅 Amazon WorkMail 基于身份的策略示例）

使用身份进行身份验证

身份验证是您使用身份凭证登录 AWS 的方法。您必须作为 AWS 账户根用户、IAM 用户或通过代入 IAM 角色进行身份验证。

您可以使用来自身份源 [例如 AWS IAM Identity Center（IAM Identity Center）] 的凭证、单点登录身份验证或 Google/Facebook 凭证，以联合身份进行登录。有关登录的更多信息，请参阅《AWS 登录用户指南》中的如何登录您的 AWS 账户。

对于编程访问，AWS 提供了 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的 AWS 签名版本 4。

AWS 账户根用户

当您创建 AWS 账户时，最初使用的是一个对所有 AWS 服务和资源拥有完全访问权限的登录身份（称为 AWS 账户根用户）。强烈建议您不要使用根用户执行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

IAM 用户和群组

IAM 用户是对单个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅《IAM 用户指南》中的要求人类用户使用带有身份提供商的联合身份验证才能使用临时凭证访问 AWS。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户的使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用 AWS CLI 或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon EC2 上运行的应用程序非常有用。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

使用策略管理访问

您将创建策略并将其附加到 AWS 身份或资源，以控制 AWS 中的访问。策略可定义与身份或资源关联时的权限。当主体发出请求时，AWS 将评估这些策略。大多数策略在 AWS 中存储为 JSON 文档。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员可使用策略来指定访问权限，具体做法是定义哪个主体可在何种条件下对哪些资源执行何种操作。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以代入这些角色。IAM 策略定义权限，而不考虑您使用哪种方法来执行操作。

基于身份的策略

基于身份的策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可在何种条件下对哪些资源执行什么操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

基于身份的策略可以是内联策略（直接嵌入到单个身份中）或托管式策略（附加到多个身份的独立策略）。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管式策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。您必须在基于资源的策略中指定主体。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用来自 IAM 的 AWS 托管式策略。

访问控制列表（ACL）

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3、AWS WAF 和 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的访问控制列表（ACL）概览。

其他策略类型

AWS 支持额外的策略类型，这些策略类型可以设置由更常用的策略类型授予的最大权限：

- 权限边界：设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略（SCP）：指定 AWS Organizations 中组织或组织单元的最大权限。有关更多信息，请参阅 AWS Organizations 用户指南中的服务控制策略。
- 资源控制策略（RCP）：设置对账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations User Guide》中的 Resource control policies (RCPs)。
- 会话策略：在为角色或联合用户创建临时会话时，作为参数传递的高级策略。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解 AWS 如何确定在涉及多种策略类型时是否允许请求，请参阅IAM 用户指南中的策略评估逻辑。

Amazon WorkMail 如何与 IAM 结合使用

在使用 IAM 管理对 Amazon WorkMail的访问权限之前，您应该了解哪些 IAM 功能可用于 Amazon WorkMail。要大致了解 Amazon WorkMail 和其他 AWS 服务如何与 IAM 结合使用，请参阅《IAM 用户指南》中的与 IAM 结合使用的 AWS 服务。

主题

- Amazon WorkMail 基于身份的策略
- Amazon WorkMail 基于资源的策略
- 基于 Amazon WorkMail 标签的授权
- Amazon WorkMail IAM 角色

Amazon WorkMail 基于身份的策略

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。Amazon WorkMail 支持特定的操作、资源和条件键。要了解在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》 中的 IAM JSON 策略元素参考。

操作

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。在策略中包含操作以授予执行关联操作的权限。

Amazon WorkMail 中的策略操作在操作前面使用以下前缀：`workmail:`。例如，要授予某人使用 Amazon WorkMail `ListUsers` API 操作检索用户列表的权限，您应在其策略中纳入 `workmail:ListUsers` 操作。策略语句必须包含 `Action` 或 `NotAction` 元素。Amazon WorkMail 定义了一组自己的操作，以描述您可以使用该服务执行的任务。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示：

```
"Action": [
      "workmail:ListUsers",
      "workmail:DeleteUser"
```

您也可以使用通配符（*) 指定多个操作。例如，要指定以单词 `List` 开头的所有操作，包括以下操作：

```
"Action": "workmail:List*"
```

要查看 Amazon WorkMail 操作的列表，请参阅《IAM 用户指南》中的 Amazon WorkMail 定义的操作。

资源

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于不支持资源级权限的操作，请使用通配符（*）来指示此语句应用于所有资源。

```
"Resource": "*"
```

Amazon WorkMail 支持 Amazon WorkMail 组织的资源级权限。

Amazon WorkMail 组织资源具有以下 ARN：

```
arn:aws:workmail:${Region}:${Account}:organization/${OrganizationId}
```

有关 ARN 格式的更多信息，请参阅 Amazon Resource Name (ARN) 和 AWS 服务命名空间。

例如，要在语句中指定 m-n1pq2345678r901st2u3vx45x6789yza 组织，请使用以下 ARN。

```
"Resource": "arn:aws:workmail:us-east-1:111122223333:organization/m-
n1pq2345678r901st2u3vx45x6789yza"
```

要指定属于特定账户的所有组织，请使用通配符 (*)：

```
"Resource": "arn:aws:workmail:us-east-1:111122223333:organization/*"
```

无法对特定资源执行某些 Amazon WorkMail 操作，例如用于创建资源的操作。在这些情况下，您必须使用通配符（*）。

```
"Resource": "*"
```

要查看 Amazon WorkMail 资源类型及其 ARN 的列表，请参阅《IAM 用户指南》中的 Amazon WorkMail 定义的资源。要了解可为每个资源的 ARN 指定哪些操作，请参阅Amazon WorkMail 的操作、资源和条件键。

条件键

Amazon WorkMail 支持以下全局条件键。

- aws:CurrentTime
- aws:EpochTime
- aws:MultiFactorAuthAge
- aws:MultiFactorAuthPresent
- aws:PrincipalOrgID
- aws:PrincipalArn
- aws:RequestedRegion
- aws:SecureTransport
- aws:UserAgent

以下示例策略仅授予来自 eu-west-1 AWS 区域中经过 MFA 身份验证的 IAM 主体对 Amazon WorkMail 控制台的访问权限。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ses:Describe*",
                "ses:Get*",
                "workmail:Describe*",
                "workmail:Get*",
                "workmail:List*",
                "workmail:Search*",
                "lambda:ListFunctions",
                "iam:ListRoles",
                "logs:DescribeLogGroups",
```

```
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": [
                        "eu-west-1"
                    ]
                },
                "Bool": {
                    "aws:MultiFactorAuthPresent": true
                }
            }
        }
    ]
}
```

要查看所有 AWS 全局条件键，请参阅《IAM 用户指南》中的 AWS 全局条件上下文键。

`workmail:ImpersonationRoleId` 是 Amazon WorkMail 支持的特定于服务的唯一条件键。

以下示例策略将 `AssumeImpersonationRole` 操作范围缩小到特定的 WorkMail 组织和模拟角色。

示例

要查看 Amazon WorkMail 基于身份的策略的示例，请参阅 Amazon WorkMail 基于身份的策略示例。

Amazon WorkMail 基于资源的策略

Amazon WorkMail 不支持基于资源的策略。

基于 Amazon WorkMail 标签的授权

您可以将标签附加到 Amazon WorkMail 资源，或者在请求中将标签传递给 Amazon WorkMail。要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。有关为 Amazon WorkMail 资源添加标签的更多信息，请参阅标记组织。

Amazon WorkMail IAM 角色

IAM 角色是 AWS 账户中具有特定权限的实体。

将临时凭证用于 Amazon WorkMail

可以使用临时凭证进行联合身份验证登录，分派 IAM 角色或分派跨账户角色。可以通过调用 AWS STS API 操作（如 AssumeRole 或 GetFederationToken）获得临时安全凭证。

Amazon WorkMail 支持使用临时凭证。

服务相关角色

服务相关角色允许 AWS 服务访问其他服务中的资源以代表您完成操作。服务相关角色显示在 IAM 账户中，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

Amazon WorkMail 支持服务相关角色。有关创建或管理 Amazon WorkMail 服务相关角色的详细信息，请参阅对 Amazon WorkMail 使用服务相关角色。

服务角色

此功能允许服务代表您担任服务角色。此角色允许服务访问其他服务中的资源以代表您完成操作。服务角色显示在 IAM 账户中，并归该账户所有。这意味着，IAM 管理员可以更改该角色的权限。但是，这样做可能会中断服务的功能。

Amazon WorkMail 支持服务角色。

Amazon WorkMail 基于身份的策略示例

默认情况下，IAM 用户和角色无权创建或修改 Amazon WorkMail 资源。它们还无法使用 AWS 管理控制台、AWS CLI 或 AWS API 执行任务。IAM 管理员必须创建 IAM 策略，以便为用户和角色授予权限以对所需的指定资源执行特定的 API 操作。然后，管理员必须将这些策略附加到需要这些权限的 IAM 用户或组。

要了解如何使用这些示例 JSON 策略文档创建 IAM 基于身份的策略，请参阅《IAM 用户指南》中的在 JSON 选项卡上创建策略。

主题

- 策略最佳实践
- 使用 Amazon WorkMail 控制台
- 允许用户查看他们自己的权限
- 允许用户对 Amazon WorkMail 资源进行只读访问

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Amazon WorkMail 资源。这些操作可能会使 AWS 账户 产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- AWS 托管式策略及转向最低权限许可入门 – 要开始向用户和工作负载授予权限，请使用 AWS 托管式策略来为许多常见使用场景授予权限。您可以在 AWS 账户 中找到这些策略。我们建议通过定义特定于您的使用场景的 AWS 客户托管式策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略或工作职能的 AWS 托管式策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果通过特定 AWS 服务（例如 CloudFormation）使用服务操作，您还可以使用条件来授予对服务操作的访问权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证（MFA）：如果您所处的场景要求您的 AWS 账户 中有 IAM 用户或根用户，请启用 MFA 来提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用 Amazon WorkMail 控制台

要访问 Amazon WorkMail 控制台，您必须具有一组最低的权限。这些权限必须允许您列出和查看有关您 AWS 账户中的 Amazon WorkMail 资源的详细信息。如果您创建的基于身份的策略比所需的最低权限更严格，则无法为具有该策略的实体（IAM 用户或角色）正常运行控制台。

要确保这些实体仍可使用 Amazon WorkMail 控制台，也可向实体附加以下 AWS 托管式策略 AmazonWorkMailFullAccess。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

AmazonWorkMailFullAccess 策略授予 IAM 用户对 Amazon WorkMail 资源的完全访问权限。此策略允许用户访问 Amazon WorkMail、AWS Key Management Service、Amazon Simple Email Service

和 AWS Directory Service 操作。其中还包括 Amazon WorkMail 需要代表您执行的多项 Amazon EC2 操作。`logs` 和 `cloudwatch` 权限是电子邮件事件日志记录和在 Amazon WorkMail 控制台中查看指标所必需的。审计日志记录使用 CloudWatch Logs、Amazon S3 和 Amazon Data FireHose 来存储 `logs`。有关更多信息，请参阅 Amazon WorkMail 中的日志记录和监控。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "WorkMailAdministration",
      "Effect": "Allow",
      "Action": [
        "ds:AuthorizeApplication",
        "ds:CheckAlias",
        "ds:CreateAlias",
        "ds:CreateDirectory",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:ListAuthorizedApplications",
        "ds:UnauthorizeApplication",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "kms:DescribeKey",
        "kms:ListAliases",
```

```
        "lambda:ListFunctions",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53:GetHostedZone",
        "route53domains:CheckDomainAvailability",
        "route53domains:ListDomains",
        "ses:*",
        "workmail:*",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:DeleteDeliveryDestination",
        "logs:DeleteDeliveryDestinationPolicy",
        "logs:DescribeDeliveryDestinations",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:PutDeliveryDestination",
        "logs:PutDeliveryDestinationPolicy",
        "logs:CreateDelivery",
        "logs:DeleteDelivery",
        "logs:DescribeDeliveries",
        "logs:GetDelivery",
        "logs:DeleteDeliverySource",
        "logs:DescribeDeliverySources",
        "logs:GetDeliverySource",
        "logs:PutDeliverySource",
        "logs:DescribeResourcePolicies",
        "cloudwatch:GetMetricData",
        "firehose:DescribeDeliveryStream",
        "firehose:ListDeliveryStreams",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
        "Sid": "AuditLogDeliveryThroughCWLogs",
        "Effect": "Allow",
        "Action": [
            "firehose:TagDeliveryStream",
            "logs:PutResourcePolicy",
            "s3:GetBucketPolicy",
            "s3:PutBucketPolicy"
```

```
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:CalledViaLast": "logs.amazonaws.com"
            }
        }
    },
    {
        "Sid": "InboundOutboundEmailEventsLink",
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:AWSServiceName": "events.workmail.amazonaws.com"
            }
        }
    },
    {
        "Sid": "AuditLoggingLink",
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:AWSServiceName": "delivery.logs.amazonaws.com"
            }
        }
    },
    {
        "Sid": "InboundOutboundEmailEventsUnlink",
        "Effect": "Allow",
        "Action": [
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus"
        ],
        "Resource": "arn:aws:iam::*:role/aws-service-role/
events.workmail.amazonaws.com/AWSServiceRoleForAmazonWorkMailEvents*"
    },
    {
        "Sid": "InboundOutboundEmailEventsAuth",
        "Effect": "Allow",
        "Action": "iam:PassRole",
```

```
        "Resource": "arn:aws:iam::*:role/*workmail*",
        "Condition": {
            "StringLike": {
                "iam:PassedToService": "events.workmail.amazonaws.com"
            }
        }
    }
  ]
}
```

对于只需要调用 AWS CLI 或 AWS API 的用户，无需为其提供最低控制台权限。相反，只允许访问与您尝试执行的 API 操作相匹配的操作。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上完成此操作或者以编程方式使用 AWS CLI 或 AWS API 所需的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
```

```
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

允许用户对 Amazon WorkMail 资源进行只读访问

以下策略声明向 IAM 用户授予对 Amazon WorkMail 资源的只读访问权限。此策略可与 AWS 托管式策略 AmazonWorkMailReadOnlyAccess 提供相同级别的访问权限。两个策略均向用户授予对所有 Amazon WorkMail `Describe` 操作的访问权限。需要对 AWS Directory Service `DescribeDirectories` 操作的访问权限才能获取有关您的 Directory Service 目录的信息。需要 Amazon SES 服务的访问权限才能获取有关已配置域的信息。需要 AWS Key Management Service 的访问权限才能获取有关已使用的加密密钥的信息。`logs` 和 `cloudwatch` 权限是电子邮件事件日志记录和在 Amazon WorkMail 控制台中查看指标所必需的。审计日志记录使用 CloudWatch Logs、Amazon S3 和 Amazon Data FireHose 来存储 `logs`。有关更多信息，请参阅 Amazon WorkMail 中的日志记录和监控。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "WorkMailReadOnly",
      "Effect": "Allow",
      "Action": [
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:DescribeDeliveryDestinations",
```

```
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliverySources",
        "logs:GetDelivery",
        "logs:GetDeliverySource",
        "cloudwatch:GetMetricData"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon WorkMail 身份和访问问题排查

您可以使用以下信息，帮助诊断和修正在使用 Amazon WorkMail 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 Amazon WorkMail 中执行操作
- 我无权执行 iam:PassRole
- 我希望允许我的 AWS 账户以外的人员访问我的 Amazon WorkMail 资源

我无权在 Amazon WorkMail 中执行操作

如果AWS 管理控制台告诉您，无权执行某个操作，则必须联系管理员寻求帮助。管理员是指提供用户名和密码的人员。

当不具有 `workmail:DescribeGroup` 权限的 `mateojackson` IAM 用户尝试使用控制台查看有关组的详细信息时，就会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workmail:DescribeGroup on resource: group
```

在这种情况下，Mateo 请求他的管理员更新其策略，以允许他使用 `workmail:DescribeGroup` 操作访问 `group` 资源。

我无权执行 iam:PassRole

如果您收到一个错误，指明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 Amazon WorkMail。

有些 AWS 服务 允许将现有角色传递到该服务，而不是创建新服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 Amazon WorkMail 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系 AWS 管理员。您的管理员是提供登录凭证的人。

我希望允许我的 AWS 账户以外的人员访问我的 Amazon WorkMail 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Amazon WorkMail 是否支持这些功能，请参阅Amazon WorkMail 如何与 IAM 结合使用。
- 要了解如何为您拥有的 AWS 账户中的资源提供访问权限，请参阅《IAM 用户指南》中的为您拥有的另一个 AWS 账户中的 IAM 用户提供访问权限。
- 要了解如何为第三方 AWS 账户 提供您的资源的访问权限，请参阅《IAM 用户指南》中的为第三方拥有的 AWS 账户 提供访问权限。
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

适用于 Amazon WorkMail 的 AWS 托管式策略

要向用户、组和角色添加权限，与自己编写策略相比，使用 AWS 托管式策略更简单。创建仅为团队提供所需权限的 IAM 客户管理型策略需要时间和专业知识。要快速入门，您可以使用我们的 AWS 托管策略。这些策略涵盖常见使用案例，可在您的 AWS 账户 中使用。有关 AWS 托管策略的更多信息，请参阅《IAM 用户指南》中的AWS 托管策略。

AWS 服务负责维护和更新 AWS 托管式策略。您无法更改 AWS 托管式策略中的权限。服务偶尔会向 AWS 托管式策略添加额外权限以支持新特征。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新特征或新操作可用时，服务最有可能会更新 AWS 托管式策略。服务不会从 AWS 托管式策略中删除权限，因此策略更新不会破坏您的现有权限。

此外，AWS 还支持跨多种服务的工作职能的托管式策略。例如，ReadOnlyAccess AWS 托管式策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动新特征时，AWS 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的 AWS 托管式策略。

AWS 托管式策略：AmazonWorkMailFullAccess

您可以将 `AmazonWorkMailFullAccess` 策略附加到 IAM 身份。此策略授予允许对 Amazon WorkMail 进行完全访问的权限。

要查看此策略的权限，请参阅 AWS 管理控制台中的 AmazonWorkMailFullAccess。

AWS 托管式策略：AmazonWorkMailReadOnlyAccess

您可以将 `AmazonWorkMailReadOnlyAccess` 策略附加到 IAM 身份。此策略授予允许对 Amazon WorkMail 进行只读访问的权限。

要查看此策略的权限，请参阅 AWS 管理控制台中的 AmazonWorkMailReadOnlyAccess。

AWS 托管式策略：AmazonWorkMailEventsServiceRolePolicy

此策略附加到名为 AmazonWorkMailEvents 的服务相关角色，以允许访问 Amazon WorkMail 事件使用或管理的 AWS 服务和资源。有关更多信息，请参阅 对 Amazon WorkMail 使用服务相关角色。

AWS 托管式策略的 Amazon WorkMail 更新

查看有关自适用于 Amazon WorkMail 的 AWS 托管式策略开始跟踪这些更改以来的更新的详细信息。

更改	描述	日期
AWS 托管式策略更新 – 对现有策略的更新	Amazon WorkMail 的 `AmazonWorkMailReadOnlyAccess` 和 `AmazonWorkMailFullAccess` 权限已更新，以支持审计日志记录。有关更新的权限的更多信息，请参阅 Amazon WorkMail 基于身份的策略示例；有关审计日志记录的信息，请参阅启用审计日志记录。	2024 年 2 月 14 日
Amazon WorkMail 开启了跟踪更改	Amazon WorkMail 为其 AWS 托管式策略开启了跟踪更改。	2021 年 3 月 1 日

对 Amazon WorkMail 使用服务相关角色

Amazon WorkMail 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特类型的 IAM 角色，它与 Amazon WorkMail 直接关联。服务相关角色由 Amazon WorkMail 预定义，并包含服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色可让您更轻松地设置 Amazon WorkMail，因为您不必手动添加必要的权限。Amazon WorkMail 定义其服务相关角色的权限，除非另有定义，否则仅 Amazon WorkMail 可以代入该角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

只有在先删除相关资源后，才能删除服务相关角色。这将保护您的 Amazon WorkMail 资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参阅与 IAM 结合使用的 AWS 服务，并查找服务相关角色列中显示为是的服务。选择是，可转到查看该服务的服务相关角色文档的链接。

Amazon WorkMail 的服务相关角色权限

Amazon WorkMail 使用名为 AmazonWorkMailEvents 的服务相关角色 – Amazon WorkMail 使用此服务相关角色来启用对 Amazon WorkMail 事件使用或管理的 AWS 服务和资源的访问，例如监控

CloudWatch 记录的电子邮件事件。有关为 Amazon WorkMail 启用电子邮件事件日志记录的更多信息，请参阅启用电子邮件事件日志记录。

AmazonWorkMailEvents 服务相关角色信任以下服务代入该角色：

- `events.workmail.amazonaws.com`

角色权限策略允许 Amazon WorkMail 对指定资源完成以下操作：

- 操作：`logs:CreateLogGroup` 上的 `all AWS resources`
- 操作：`logs:CreateLogStream` 上的 `all AWS resources`
- 操作：`logs:PutLogEvents` 上的 `all AWS resources`

必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为 Amazon WorkMail 创建服务相关角色

您无需手动创建服务相关角色。当您在 Amazon WorkMail 控制台中开启 Amazon WorkMail 事件日志记录并使用默认设置时，Amazon WorkMail 会为您创建服务相关角色。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您开启 Amazon WorkMail 事件日志记录并使用默认设置时，Amazon WorkMail 会再次为您创建服务相关角色。

为 Amazon WorkMail 编辑服务相关角色

Amazon WorkMail 不允许您编辑 AmazonWorkMailEvents 服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

为 Amazon WorkMail 删除服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，必须先清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果在您尝试删除资源时 Amazon WorkMail 服务正在使用该角色，则删除操作可能会失败。如果发生这种情况，请等待几分钟后重试。

删除 AmazonWorkMailEvents 使用的 Amazon WorkMail 资源

1. 关闭 Amazon WorkMail 事件日志记录。
   a. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

      如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
   b. 在导航窗格中，选择组织，然后选择贵组织的名称。
   c. 在导航窗格中，选择组织设置，然后选择监控。
   d. 对于 Log settings (日志设置)，选择 Edit (编辑)。
   e. 将启用邮件事件滑块移动到“关闭”位置。
   f. 选择保存。
2. 删除 Amazon CloudWatch 日志组。
   a. 通过 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
   b. 选择 Logs (日志)。
   c. 对于 Log Groups (日志组)，选择要删除的日志组。
   d. 对于 Actions (操作)，选择 Delete log group (删除日志组)。
   e. 选择是，删除。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台、AWS CLI 或 AWS API 删除 AmazonWorkMailEvents 服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

Amazon WorkMail 服务相关角色支持的区域

Amazon WorkMail 支持在该服务可用的所有区域中使用服务相关角色。有关更多信息，请参阅 Amazon WorkMail 区域和端点。

Amazon WorkMail 中的日志记录和监控

监控和审计电子邮件和日志对于保持 Amazon WorkMail 组织的运行状况非常重要。Amazon WorkMail 支持两种类型的监控：

- 事件日志记录：监控组织的电子邮件发送活动有助于保护您的域声誉。监控还可以帮助您跟踪发送和接收的电子邮件。有关如何启用电子邮件事件日志记录的更多信息，请参阅启用电子邮件事件日志记录。
- 审计日志记录：您可以使用审计日志来捕获有关 Amazon WorkMail 组织使用情况的详细信息，例如监控用户对邮箱的访问、审计是否存在可疑活动，以及调试访问控制和可用性提供商配置。有关更多信息，请参阅 启用审计日志记录。

AWS 提供以下监控工具来监视 Amazon WorkMail、在出现错误时进行报告并在适当的时候采取自动化措施：

- Amazon CloudWatch 实时监控您的 AWS 资源以及在 AWS 上运行的应用程序。例如，当您为 Amazon WorkMail 启用电子邮件事件日志记录时，CloudWatch 可以跟踪为您的组织发送和接收的电子邮件。有关使用 CloudWatch 监控 Amazon WorkMail 的更多信息，请参阅使用 CloudWatch 指标监控 Amazon WorkMail。有关 CloudWatch 的更多信息，请参阅 Amazon CloudWatch 用户指南。
- Amazon CloudWatch Logs 使您能够在 Amazon WorkMail 控制台中启用电子邮件和审计日志记录后，监控、存储和访问 Amazon WorkMail 的电子邮件事件和审计日志。CloudWatch Logs 可以监控日志文件中的信息，并且您可以将日志数据归档在高持久性存储中。有关使用 CloudWatch Logs 跟踪 Amazon WorkMail 邮件的更多信息，请参阅启用电子邮件事件日志记录和启用审计日志记录。有关 CloudWatch Logs 的更多信息，请参阅 Amazon CloudWatch Logs 用户指南。
- AWS CloudTrail 捕获由您的 AWS 账户或代表该账户发出的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以标识哪些用户和账户调用了 AWS、发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 使用 AWS CloudTrail 记录 Amazon WorkMail API 调用。
- Amazon S3 使您能够以经济高效的方式存储和访问 Amazon WorkMail 事件。Amazon S3 提供了用于管理事件数据生命周期的机制，使您能够配置自动删除旧事件，或者配置自动归档到 Amazon S3 Glacier。请注意，传输到 Amazon S3 仅适用于审计日志记录事件。有关 Amazon S3 的更多信息，请参阅 Amazon S3 用户指南。
- Amazon Data Firehose 使您能够将事件数据流式传输到其他 AWS 服务，例如 Amazon Simple Storage Service（Amazon S3）、Amazon Redshift、Amazon OpenSearch Service、Amazon OpenSearch 无服务器、Splunk，以及任何自定义 HTTP 端点或受支持的第三方服务提供商拥有

的 HTTP 端点，包括 Datadog、Dynatrace、LogicMonitor、MongoDB、New Relic、Coralogix 和 Elastic。只有审计日志记录事件支持传输到 Firehose。有关 Firehose 的更多信息，请参阅 Amazon Data Firehose 开发人员指南。

主题

使用 CloudWatch 指标监控 Amazon WorkMail

您可以使用 CloudWatch 监控 Amazon WorkMail，CloudWatch 会收集原始数据并将其处理为可读且近乎实时的指标。这些免费指标会保存 15 个月，以便您可以访问历史信息，查看 Web 应用程序或服务的执行情况。此外，可以设置用于监测特定阈值的警报，并在达到相应阈值时发送通知或执行操作。有关更多信息，请参阅《Amazon CloudWatch 用户指南》。

Amazon WorkMail 的 CloudWatch 指标

Amazon WorkMail 将以下指标和维度信息发送到 CloudWatch。

`AWS/WorkMail` 命名空间包括以下指标。

指标	描述
`OrganizationEmailReceived`	您的 Amazon WorkMail 组织收到的电子邮件数量。如果一封电子邮件发送到您组织中的 10 个收件人，则 `OrganizationEmailReceived` 计数为一。 单位：计数

指标	描述
MailboxEmailDelivered	传送到您的 Amazon WorkMail 组织中各个邮箱的电子邮件数量。如果一封电子邮件成功传送到您组织中的 10 个收件人，则 MailboxEmailDelivered 计数为 10。 单位：计数
IncomingEmailBounced	由于邮箱已满而退回的传入电子邮件数量。针对每个目标收件人计算此指标。例如，如果一封电子邮件发送到您组织中的 10 个收件人，其中两个收件人因邮箱已满导致退回邮件响应，则 IncomingEmailBounced 计数为二。 单位：计数
OutgoingEmailBounced	无法传送的外发电子邮件数量。针对每个目标收件人计算此指标。例如，如果一封电子邮件发送给 10 个收件人，而两封电子邮件无法传送，则 OutgoingEmailBounced 计数为 2。 单位：计数
OutgoingEmailSent	从您的 Amazon WorkMail 组织成功发送的电子邮件数量。针对成功发送的电子邮件的每个收件人计算此指标。例如，如果 1 封电子邮件发送给 10 个收件人，并且该电子邮件已成功传送到其中 8 个收件人，则 OutgoingEmailSent 计数为 8。 单位：计数

指标	描述
AuthenticationFailure	该指标用于统计身份验证尝试的次数。当身份验证成功时，计数为 0；当身份验证不成功时，计数为 1。使用 Sum 统计数据来监控失败的身份验证尝试次数。使用 Sample count 统计数据来监控身份验证事件的总数。使用 Average 统计数据来监控失败和成功的身份验证事件的比率。 单位：计数
AccessDenied	该指标用于统计访问控制评估的次数。当访问控制拒绝操作时，计数为 1；当授权执行操作时，计数为 0。使用 Sum 统计数据来监控被拒绝操作的数量，使用 Sample count 统计数据来监控所尝试操作的总数，并使用 Average 统计数据来监控支持操作和拒绝操作的比率。 单位：计数
ActionDenied	当对邮箱数据进行操作时，就会统计此指标。当拒绝操作时，计数为 1；如果授权执行操作，则计数为 0。使用 Sum 统计数据来监控被拒绝邮箱操作的数量，使用 Sample count 统计数据来监控所尝试邮箱操作的总数，并使用 Average 统计数据来监控支持操作和拒绝操作的比率。 单位：计数
AvailabilityProviderFailure	对于 Amazon WorkMail 为从外部来源检索日历可用性而执行的每个可用性提供商请求，都会统计此指标。有关可用性提供商的更多信息，请参阅《Amazon WorkMail 管理员指南》。

监控 Amazon WorkMail 电子邮件事件日志

当您为 Amazon WorkMail 组织启用电子邮件事件日志记录时，Amazon WorkMail 将使用 CloudWatch 记录电子邮件事件。有关启用电子邮件事件日志记录的更多信息，请参阅启用电子邮件事件日志记录。

下表列明了 Amazon WorkMail 使用 CloudWatch 记录的事件、传输这些事件的时间以及事件字段包含的内容。

ORGANIZATION_EMAIL_RECEIVED

此事件在您的 Amazon WorkMail 组织收到电子邮件时记录。

字段	描述
recipients	邮件的目标收件人。
sender	代表其他用户发送电子邮件的用户的电子邮件地址。仅当代表其他用户发送电子邮件时，才设置此字段。
from	From (发件人) 地址，它通常是发送邮件的用户的电子邮件地址。如果该用户以其他用户名义或代表其他用户发送邮件，则此字段返回代表其发送电子邮件的用户的电子邮件地址，而不是实际发件人的电子邮件地址。
subject	电子邮件主题。
messageId	SMTP 邮件 ID。
spamVerdict	指示邮件是否被 Amazon SES 标记为垃圾邮件。有关更多信息，请参阅《Amazon Simple Email Service 开发人员指南》中的 Amazon SES 电子邮件接收的通知的内容。
dkimVerdict	指示是否已通过域名密钥识别邮件 (DKIM) 检查。有关更多信息，请参阅《Amazon Simple Email Service 开发人员指南》中的 Amazon SES 电子邮件接收的通知的内容。
dmarcVerdict	指示是否已通过基于域的邮件身份验证、报告和合规性（DMARC）检查。有关更多信息，请参阅《Amazon Simple Email Service 开发人员指

字段	描述
	南》中的 Amazon SES 电子邮件接收的通知的内容。
dmarcPolicy	仅当 dmarcVerdict 字段包含“FAIL”时才会显示。表示 DMARC 检查失败时对电子邮件执行的操作（NONE、QUARANTINE 或 REJECT）。它由发送电子邮件域的拥有者设置。
spfVerdict	指示是否已通过发件人策略框架（SPF）检查。有关更多信息，请参阅《Amazon Simple Email Service 开发人员指南》中的 Amazon SES 电子邮件接收的通知的内容。
messageTimestamp	指示收到邮件的时间。

MAILBOX_EMAIL_DELIVERED

此事件在邮件传送到您组织中的邮箱时记录。此事件为邮件传送到的每个邮箱记录一次，因此单个 ORGANIZATION_EMAIL_RECEIVED 事件可能生成多个 MAILBOX_EMAIL_DELIVERED 事件。

字段	描述
recipient	将邮件传送到的邮箱。
folder	放置邮件的邮箱文件夹。

RULE_APPLIED

此事件在传入或传出邮件启动电子邮件流规则时记录。

字段	描述
ruleName	规则的名称。

字段	描述
ruleType	所应用的规则的类型（INBOUND_RULE、OUTBOUND_RULE 或 MAILBOX_RULE）。入站和出站规则适用于您的 Amazon WorkMail 组织。邮箱规则仅适用于指定邮箱。有关更多信息，请参阅 管理电子邮件流。
ruleActions	基于规则执行的操作。不同的邮件收件人可能具有不同的操作，例如电子邮件被退回或电子邮件成功传送。
targetFolder	Move 或 Copy MAILBOX_RULE 的预定目标文件夹。
targetRecipient	Forward 或 Redirect MAILBOX_RULE 的目标收件人。

JOURNALING_INITIATED

此事件在 Amazon WorkMail 向由您的组织管理员指定的日志地址发送电子邮件时记录。仅当为您的组织配置日志后才会传输此事件。有关更多信息，请参阅 在 Amazon WorkMail 中使用电子邮件日志。

字段	描述
journalingAddress	日志邮件发送到的电子邮件地址。

INCOMING_EMAIL_BOUNCED

此事件在传入邮件无法传送到目标收件人时记录。电子邮件退回的原因有很多，例如目标邮箱已满。系统会为导致电子邮件被退回的每个收件人记录一次此事件。例如，如果传入邮件发送给 3 个收件人，其中 2 个收件人的邮箱已满，则会记录 2 个 INCOMING_EMAIL_BOUNCED 事件。

字段	描述
bouncedRecipient	Amazon WorkMail 为其退回邮件的目标收件人。

OUTGOING_EMAIL_SUBMITTED

此事件在您组织中的用户提交要发送的电子邮件时记录。此事件在邮件离开 Amazon WorkMail 时记录，因此它不会指示电子邮件是否成功传送。

字段	描述
recipients	由发件人指定的邮件收件人。包括“收件人”、“抄送”和“密件抄送”行中的所有收件人。
sender	代表其他用户发送电子邮件的用户的电子邮件地址。仅当代表其他用户发送电子邮件时，才设置此字段。
from	From (发件人) 地址，它通常是发送邮件的用户的电子邮件地址。如果该用户以其他用户名义或代表其他用户发送邮件，则此字段返回代表其发送电子邮件的用户的电子邮件地址，而不是实际发件人的电子邮件地址。
subject	电子邮件主题。

OUTGOING_EMAIL_SENT

此事件在传出电子邮件成功传送到目标收件人时记录。此事件为每个成功收件人记录一次，因此单个 OUTGOING_EMAIL_SUBMITTED 可能生成多个 OUTGOING_EMAIL_SENT 条目。

字段	描述
recipient	成功传送的电子邮件的收件人。
sender	代表其他用户发送电子邮件的用户的电子邮件地址。仅当代表其他用户发送电子邮件时，才设置此字段。
from	From (发件人) 地址，它通常是发送邮件的用户的电子邮件地址。如果该用户以其他用户名义或代表其他用户发送邮件，则此字段返回代表其发

字段	描述
	送电子邮件的用户的电子邮件地址，而不是实际发件人的电子邮件地址。
messageId	SMTP 邮件 ID。

OUTGOING_EMAIL_BOUNCED

此事件在传出邮件无法传送到目标收件人时记录。电子邮件退回的原因有很多，例如目标邮箱已满。系统会为导致电子邮件被退回的每个收件人记录一次退回。例如，如果传出邮件发送给 3 个收件人，其中 2 个收件人的邮箱已满，则会记录 2 个 OUTGOING_EMAIL_BOUNCED 事件。

字段	描述
bouncedRecipient	目标邮件服务器为其退回邮件的目标收件人。

DMARC_POLICY_APPLIED

将 DMARC 策略应用于发送给您的组织的电子邮件时，将记录此事件。

字段	描述
from	From (发件人) 地址，它通常是发送邮件的用户的电子邮件地址。如果该用户以其他用户名义或代表其他用户发送邮件，则此字段返回代表其发送电子邮件的用户的电子邮件地址，而不是实际发件人的电子邮件地址。
recipients	邮件的目标收件人。
policy	应用的 DMARC 策略表示当 DMARC 检查失败时要对电子邮件执行的操作（NONE、QUARANTINE 或 REJECT）。这与 ORGANIZATION_EMAIL_RECEIVED 事件中的 dmarcPolicy 字段相同。

监控 Amazon WorkMail 审计日志

您可以使用审计日志来监控对 Amazon WorkMail 组织邮箱的访问情况。Amazon WorkMail 记录五种类型的审计事件，这些事件可发布到 CloudWatch Logs、Amazon S3 或 Amazon Firehouse。您可以使用审计日志来监控用户与组织邮箱的交互、身份验证尝试、访问控制规则评估、对外部系统执行可用性提供商调用，以及使用个人访问令牌监控事件。有关配置审计日志记录的信息，请参阅启用审计日志记录。

以下各节介绍 Amazon WorkMail 记录的审计事件、传输这些事件的时间以及有关事件字段的信息。

邮箱访问日志

邮箱访问事件提供有关对哪个邮箱对象采取（或尝试）了什么操作的信息。对于您尝试对邮箱中的项目或文件夹运行的每个操作，都会生成一个邮箱访问事件。这些事件对于审计对邮箱数据的访问非常有用。

字段	描述
event_timestamp	事件发生的时间，以自 Unix 纪元以来的毫秒数表示。
request_id	唯一标识请求的 ID。
organization_arn	经过身份验证的用户所属的 Amazon WorkMail 组织的 ARN。
user_id	经过身份验证的用户的 ID。
impersonator_id	模拟者的 ID。仅当为请求使用了模拟功能时才显示。
protocol	使用的协议。协议可以是：`AutoDiscover` 、`EWS`、`IMAP`、`WindowsOutlook` 、`ActiveSync` 、`SMTP`、`WebMail`、`IncomingEmail` 或 `OutgoingEmail` 。
source_ip	请求的源 IP 地址。
user_agent	发出请求的用户代理。

字段	描述
action	对对象执行的操作，可以是：read、read_hierarchy 、read_summary 、read_attachment 、read_permissions 、create、update、update_permissions 、update_read_state 、delete、submit_email_for_sending 、abort_sending_email 、move、move_to、copy 或 copy_to。
owner_id	用户的 ID，该用户拥有正在对其执行操作的对象。
object_type	对象类型，可以是：文件夹、邮件或附件。
item_id	用于唯一标识邮件的 ID，该邮件为事件的主题或包含作为事件主题的附件。
folder_path	正在对其执行操作的文件夹的路径，或包含正在对其执行操作的项目的文件夹的路径。
folder_id	用于唯一标识文件夹的 ID，该文件夹为事件的主题或包含作为事件主题的对象。
attachment_path	受影响附件的显示名称路径。
action_allowed	是否支持执行该操作。可以为 true 或 false。

访问控制日志

每当访问控制规则被评估时，就会生成访问控制事件。这些日志对于审计禁止的访问或调试访问控制配置很有用。

字段	描述
event_timestamp	事件发生的时间，以自 Unix 纪元以来的毫秒数表示。
request_id	唯一标识请求的 ID。
organization_arn	经过身份验证的用户所属的 WorkMail 组织的 ARN。
user_id	经过身份验证的用户的 ID。
impersonator_id	模拟者的 ID。仅当为请求使用了模拟功能时才显示。
protocol	使用的协议，可以是：`AutoDiscover` 、`EWS`、`IMAP`、`WindowsOutlook` 、`ActiveSync` 、`SMTP`、`WebMail`、`IncomingEmail` 或 `OutgoingEmail` 。
source_ip	请求的源 IP 地址。
scope	规则的范围，可以是：`AccessControl` 、`DeviceAccessControl` 或 `ImpersonationAccessControl` 。
rule_id	匹配的访问控制规则的 ID。当没有匹配的规则时，rule_id 不可用。
access_granted	是否支持访问。可以为 true 或 false。

身份验证日志

身份验证事件包含有关身份验证尝试的信息。

> **Note**
>
> 不会通过 Amazon WorkMail WebMail 应用程序为身份验证事件生成身份验证事件。

字段	描述
event_timestamp	事件发生的时间，以自 Unix 纪元以来的毫秒数表示。
request_id	唯一标识请求的 ID。
organization_arn	经过身份验证的用户所属的 WorkMail 组织的 ARN。
user_id	经过身份验证的用户的 ID。
用户	尝试进行身份验证时使用的用户名。
protocol	使用的协议，可以是：`AutoDiscover` 、`EWS`、`IMAP`、`WindowsOutlook` 、`ActiveSync` 、`SMTP`、`WebMail`、`IncomingEmail` 或 `OutgoingEmail` 。
source_ip	请求的源 IP 地址。
user_agent	发出请求的用户代理。
方法	身份验证方法。目前仅支持基本身份验证。
auth_successful	身份验证尝试是否成功。可以为 true 或 false。
auth_failed_reason	身份验证失败的原因。仅在身份验证失败时才会出现。
personal_access_token_id	用于身份验证的个人访问令牌的 ID。

个人访问令牌日志

对于每次尝试创建或删除个人访问令牌，都会生成个人访问令牌（PAT）事件。个人访问令牌事件提供有关用户是否成功创建个人访问令牌的信息。个人访问令牌日志对于审计最终用户创建和删除其自己的 PAT 非常有用。用户使用个人访问令牌登录将在现有身份验证日志中生成事件。有关更多信息，请参阅身份验证日志。

字段	描述
event_timestamp	事件发生的时间，以自 Unix 纪元以来的毫秒数表示。
request_id	唯一标识请求的 ID。
organization_arn	经过身份验证的用户所属的 WorkMail 组织的 ARN。
user_id	经过身份验证的用户的 ID。
用户	执行该操作的用户的用户名。
protocol	执行该操作所使用的协议，可以是：webapp
source_ip	请求的源 IP 地址。
user_agent	发出请求的用户代理。
action	个人访问令牌的操作，可以是：创建或删除。
名称	个人访问令牌的名称。
expires_time	个人访问令牌到期的日期。
范围	针对邮箱的个人访问令牌权限的范围。

可用性提供商日志

对于 Amazon WorkMail 代表您向所配置的可用性提供商发出的每个可用性请求，都会生成可用性提供商事件。这些事件对于调试可用性提供商配置很有用。

字段	描述
event_timestamp	事件发生的时间，以自 Unix 纪元以来的毫秒数表示。
request_id	唯一标识请求的 ID。
organization_arn	经过身份验证的用户所属的 WorkMail 组织的 ARN。
user_id	经过身份验证的用户的 ID。
type	正在调用的可用性提供商的类型，可以是：EWS 或 LAMBDA。
域	可用性信息已获取的域。
function_arn	如果类型为 LAMBDA，则为调用的 Lambda 的 ARN。否则，将不显示该字段。
ews_endpoint	EWS 端点的类型为 EWS。否则，将不显示该字段。
error_message	描述失败原因的消息。如果请求成功，则不显示该字段。
availability_event_successful	是否成功处理了可用性请求。

将 CloudWatch Insights 与 Amazon WorkMail 结合使用

如果您已在 Amazon WorkMail 控制台中开启电子邮件事件日志记录，或者启用了向 CloudWatch Logs 传送审计日志，则可以使用 Amazon CloudWatch Logs Insights 来查询事件日志。有关启用电子邮件事件日志记录的更多信息，请参阅启用电子邮件事件日志记录。有关 CloudWatch Logs Insights 的更多信息，请参阅《Amazon CloudWatch Logs 用户指南》中的使用 CloudWatch Logs Insights 分析日志数据。

以下示例演示如何查询 CloudWatch 日志中的常见电子邮件事件。您在 CloudWatch 控制台中运行这些查询。有关如何运行这些查询的说明，请参阅《Amazon CloudWatch Logs 用户指南》中的教程：运行和修改示例查询。

Example 查看为何用户 B 没有收到用户 A 发送的电子邮件。

以下代码示例演示了如何查询用户 A 向用户 B 发送的传出电子邮件（按时间戳排序）。

```
fields @timestamp, traceId

| sort @timestamp asc
| filter (event.from like /(?i)userA@example.com/
and event.eventName = "OUTGOING_EMAIL_SUBMITTED"
and event.recipients.0 like /(?i)userB@example.com/)
```

这将返回已发送的邮件和跟踪 ID。使用以下代码示例中的跟踪 ID 查询已发送邮件的事件日志。

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter traceId = "$TRACEID"
```

这将返回电子邮件 ID 和电子邮件事件。OUTGOING_EMAIL_SENT 表示电子邮件已发送。OUTGOING_EMAIL_BOUNCED 表示电子邮件被退回。要了解是否收到了电子邮件，请使用以下代码示例中的邮件 ID 进行查询。

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter event.messageId like "$MESSAGEID"
```

这还应该返回收到的邮件，因为它具有相同的邮件 ID。使用以下代码示例中的跟踪 ID 可查询送达情况。

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter traceId = "$TRACEID"
```

这将返回传送操作以及任何合适的规则操作。

Example 查看从某个用户或域收到的所有邮件

以下代码示例演示了如何查询从指定用户接收的所有邮件。

```
fields @timestamp, event.eventName
```

```
| sort @timestamp asc
| filter (event.from like /(?i)user@example.com/ and event.eventName =
 "ORGANIZATION_EMAIL_RECEIVED")
```

以下代码示例演示了如何查询从指定域接收的所有邮件。

```
fields @timestamp, event.eventName
| sort @timestamp asc
| filter (event.from like "example.com" and event.eventName =
 "ORGANIZATION_EMAIL_RECEIVED")
```

Example 查看被退回电子邮件的发件人

以下代码示例演示了如何查询被退回的传出电子邮件，并返回了退回的原因。

```
fields @timestamp, event.destination, event.reason
| sort @timestamp desc
| filter event.eventName = "OUTGOING_EMAIL_BOUNCED"
```

以下代码示例演示了如何查询退回的传入电子邮件。它还会返回退回邮件的收件人的电子邮件地址和退回的原因。

```
fields @timestamp, event.bouncedRecipient.emailAddress, event.bouncedRecipient.reason,
 event.bouncedRecipient.status
| sort @timestamp desc
| filter event.eventName = "INCOMING_EMAIL_BOUNCED"
```

Example 查看正在发送垃圾邮件的域

以下代码示例演示了如何查询您组织中正在接收垃圾邮件的收件人。

```
stats count(*) as c by event.recipients.0
| filter (event.eventName = "ORGANIZATION_EMAIL_RECEIVED" and event.spamVerdict =
 "FAIL")
| sort c desc
```

以下代码示例演示了如何查询垃圾电子邮件的发件人。

```
fields @timestamp, event.recipients.0, event.sender, event.from
| sort @timestamp asc
| filter (event.spamVerdict = "FAIL")
```

Example 查看为何电子邮件会发送到收件人的垃圾邮件文件夹

以下代码示例演示了如何查询被认定为垃圾邮件的电子邮件（按主题进行筛选）。

```
fields @timestamp, event.recipients.0, event.spamVerdict, event.spfVerdict,
 event.dkimVerdict, event.dmarcVerdict
| sort @timestamp asc
| filter event.subject like /(?i)$SUBJECT/ and event.eventName =
 "ORGANIZATION_EMAIL_RECEIVED"
```

您还可以通过电子邮件跟踪 ID 进行查询以查看该电子邮件的所有事件。

Example 查看与电子邮件流规则匹配的电子邮件

以下代码示例演示了如何查询与出站电子邮件流规则匹配的电子邮件。

```
fields @timestamp, event.ruleName, event.ruleActions.0.action
| sort @timestamp desc
| filter event.ruleType = "OUTBOUND_RULE"
```

以下代码示例演示了如何查询与入站电子邮件流规则匹配的电子邮件。

```
fields @timestamp, event.ruleName, event.ruleActions.0.action,
 event.ruleActions.0.recipients.0
| sort @timestamp desc
| filter event.ruleType = "INBOUND_RULE"
```

Example 查看您的组织接收或发送的电子邮件数量

以下代码示例演示了如何查询您组织中的每个收件人接收的电子邮件数。

```
stats count(*) as c by event.recipient
| filter event.eventName = "MAILBOX_EMAIL_DELIVERED"
| sort c desc
```

以下代码示例演示了如何查询您组织中的每个发件人发送的电子邮件数。

```
stats count(*) as c by event.from
| filter event.eventName = "OUTGOING_EMAIL_SUBMITTED"
```

```
| sort c desc
```

使用 AWS CloudTrail 记录 Amazon WorkMail API 调用

Amazon WorkMail 与 AWS CloudTrail 集成，后者是一项服务，可用于记录 Amazon WorkMail 中由用户、角色或 AWS 服务所采取的操作。CloudTrail 将对 Amazon WorkMail 的所有 API 调用作为事件捕获，包括来自 Amazon WorkMail 控制台的调用和对 Amazon WorkMail API 的代码调用。如果您创建跟踪，则可以让 CloudTrail 事件持续传送到 Amazon S3 存储桶，包括 Amazon WorkMail 的事件 如果您不配置跟踪，则仍可在 CloudTrail 控制台中的事件历史记录中查看最新事件。使用通过 CloudTrail 收集的信息，您可以确定向 Amazon WorkMail 发出了什么请求、发出请求时使用的 IP 地址、何人发出的请求、请求的发出时间以及其它详细信息。

要了解有关 CloudTrail 的更多信息，请参阅 AWS CloudTrail 用户指南。

CloudTrail 中的 Amazon WorkMail 信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。当 Amazon WorkMail 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 服务事件一同保存在事件历史记录中。您可以在 AWS 账户 中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录 AWS 账户中的事件（包括 Amazon WorkMail 的事件），则必须创建跟踪。通过跟踪记录，CloudTrail 可将日志文件传送至 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

所有 Amazon WorkMail 操作都由 CloudTrail 记录，并记录在 Amazon WorkMail API 参考中。例如，对 `CreateUser`、`CreateAlias` 和 `GetRawMessageContent` API 操作的调用将在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 IAM 用户凭证发出的。

- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 Amazon WorkMail 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。CloudTrail 日志文件包含一个或多个日记账条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

以下示例显示了一个 CloudTrail 日志条目，该条目演示了来自 Amazon WorkMail API 的 `CreateUser` 操作。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T17:49:59Z",
  "eventSource": "workmail.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "name": "janedoe",
    "displayName": "Jane Doe",
    "organizationId": "m-5b1c980000EXAMPLE"
  },
  "responseElements": {
    "userId": "a3a9176d-EXAMPLE"
  },
  "requestID": "dec81e4a-EXAMPLE",
```

```
  "eventID": "9f2f09c5-EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

以下示例显示了一个 CloudTrail 日志条目，该条目演示了来自 Amazon WorkMail API 的 `CreateAlias` 操作。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T18:13:44Z",
  "eventSource": "workmail.amazonaws.com",
  "eventName": "CreateAlias",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "alias": "aliasjamesdoe@testofconsole.awsapps.com",
    "organizationId": "m-5b1c980000EXAMPLE"
    "entityId": "a3a9176d-EXAMPLE"
  },
  "responseElements": null,
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

以下示例显示了一个 CloudTrail 日志条目，该条目演示了来自 Amazon WorkMail Message Flow API 的 `GetRawMessageContent` 操作。

```
{
  "eventVersion": "1.05",
```

```
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T18:13:44Z",
  "eventSource": "workmailMessageFlow.amazonaws.com",
  "eventName": "GetRawMessageContent",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "messageId": "123A4A5A-67B8-90C1-D23E-45FG67H890J1"
  },
  "responseElements": null,
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```


启用电子邮件事件日志记录

您可以在 Amazon WorkMail 控制台中启用电子邮件事件日志记录来跟踪组织的电子邮件。电子邮件事件日志记录使用 AWS Identity and Access Management 服务相关角色（SLR）来授予将电子邮件事件日志发布到 Amazon CloudWatch 的权限。有关 IAM 服务相关角色的更多信息，请参阅对 Amazon WorkMail 使用服务相关角色。

在 CloudWatch 事件日志中，您可以使用 CloudWatch 搜索工具和指标来跟踪邮件和排查电子邮件问题。有关 Amazon WorkMail 发送到 CloudWatch 的事件日志的更多信息，请参阅 监控 Amazon WorkMail 电子邮件事件日志。有关 CloudWatch Logs 的更多信息，请参阅 Amazon CloudWatch Logs 用户指南。

主题

- 关闭电子邮件事件日志记录
- 防止跨服务混淆座席

启用电子邮件事件日志记录

当您使用默认设置开启电子邮件事件日志记录时会发生以下情况，Amazon WorkMail：

- 创建 AWS Identity and Access Management 服务相关角色 – `AmazonWorkMailEvents`。
- 创建 CloudWatch 日志组 – `/aws/workmail/emailevents/`*`organization-alias`*。
- 将 CloudWatch 日志保留期设置为 30 天。

启用电子邮件事件日志记录

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择日志记录设置。
4. 选择电子邮件流日志设置选项卡。
5. 在电子邮件流日志设置部分中，选择编辑。
6. 将启用邮件事件滑块移到开启位置。
7. 请执行以下操作之一：
   - （推荐）选择使用默认设置。
   - （可选）清除使用默认设置，然后从显示的列表中选择目标日志组和 IAM 角色。

   > **Note**
   >
   > 仅当您已使用 AWS CLI 创建日志组和自定义 IAM 角色时，才选择此选项。有关更多信息，请参阅 创建自定义日志组和 IAM 角色以进行电子邮件事件日志记录。
8. 选择我授权 Amazon WorkMail 使用此配置在我的账户中发布日志。
9. 选择保存。

创建自定义日志组和 IAM 角色以进行电子邮件事件日志记录

当为 Amazon WorkMail 启用电子邮件事件日志记录时，我们建议使用默认设置。如果您需要自定义监控配置，您可以使用 AWS CLI 创建专用的日志组和自定义 IAM 角色，以进行电子邮件事件日志记录。

创建自定义日志组和 IAM 角色以进行电子邮件事件日志记录

1. 使用以下 AWS CLI 命令在与 Amazon WorkMail 组织相同的 AWS 区域中创建日志组。有关更多信息，请参阅《AWS CLI 命令参考》中的 create-log-group。

```
aws --region us-east-1 logs create-log-group --log-group-name workmail-monitoring
```

2. 创建一个文件，其中包含以下策略：

   JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "events.workmail.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

3. 使用以下 AWS CLI 命令创建 IAM 角色并将此文件附加为角色策略文档。有关更多信息，请参阅《AWS CLI 命令参考》中的 create-role。

```
aws iam create-role --role-name workmail-monitoring-role --assume-role-policy-
document file://trustpolicyforworkmail.json
```

> **Note**
>
> 如果您是 WorkMailFullAccess 托管式策略用户，您必须在角色名称中包括术语 workmail。此托管策略仅允许您使用名称中带有 workmail 的角色配置电子邮件事件日

志记录。有关更多信息，请参阅 IAM 用户指南中的向用户授予将角色传递给 AWS 服务的权限。

4. 创建一个文件，其中包含您在上一步中创建的 IAM 角色的策略。至少，该策略必须向角色授予权限，使该角色可以创建日志流并将日志事件放入您在第 1 步创建的日志组。
5. 使用以下 AWS CLI 命令将策略文件附加到 IAM 角色。有关更多信息，请参阅《AWS CLI 命令参考》中的 put-role-policy。

```
aws iam put-role-policy --role-name workmail-monitoring-role --policy-
name workmail-permissions --policy-document file://rolepolicy.json
```

关闭电子邮件事件日志记录

从 Amazon WorkMail 控制台关闭电子邮件事件日志记录。如果您不再需要使用电子邮件事件日志记录，我们建议您删除相关的 CloudWatch 日志组和服务相关角色。有关更多信息，请参阅 为 Amazon WorkMail 删除服务相关角色。

关闭电子邮件事件日志记录

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择 Monitoring (监控)。
4. 在日志设置部分中，选择编辑。
5. 将启用邮件事件滑块移动到“关闭”位置。
6. 选择保存。

防止跨服务混淆座席

混淆代理问题是一个安全性问题，即不具有操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在 AWS 中，跨服务模拟可能会导致混淆代理问题。一个服务（呼叫服务）调用另一项服务（所谓的服务）时，可能会发生跨服务模拟。

可以操纵调用服务以使用其权限对另一个客户的资源进行操作（该服务原本不应拥有访问权限）。

为防止这种情况，AWS 提供可帮助您保护所有服务的数据的工具，而这些服务中的服务主体有权限访问账户中的资源。

我们建议在资源策略中使用 aws:SourceArn 和 aws:SourceAccount 全局条件上下文密钥，以限制 CloudWatch Logs 和 Amazon S3 向生成日志的服务授予的权限。如果使用两个全局条件上下文键，在同一策略语句中使用时，这些值必须使用相同的账户 ID。

aws:SourceArn 的值必须是生成日志的传输源的 ARN。

防范混淆代理问题最有效的方法是使用 aws:SourceArn 全局条件上下文键和资源的完整 ARN。如果您不知道资源的完整 ARN，或正在指定多个资源，请针对 ARN 未知部分使用带有通配符 (*) 的 aws:SourceArn 全局上下文条件键。

启用审计日志记录

您可以使用审计日志来捕获有关 Amazon WorkMail 组织使用情况的详细信息。审计日志可用于监控用户对邮箱的访问、审计是否存在可疑活动，以及调试访问控制和可用性提供商配置。

> **Note**
>
> AmazonWorkMailFullAccess 托管式策略并不包括管理日志传输所需的所有权限。如果您使用此策略来管理 WorkMail，请确保用于配置日志传输的主体（例如，代入的角色）也具有所有必需的权限。

Amazon WorkMail 对于审计日志支持三个传输目标：CloudWatch Logs、Amazon S3 和 Amazon Data Firehose。有关更多信息，请参阅 Amazon CloudWatch Logs 用户指南中的需要额外权限 [V2] 的日志记录。

除了需要额外权限 [V2] 的日志记录下列出的权限外，Amazon WorkMail 还需要一项额外的权限来配置日志传输：workmail:AllowVendedLogDeliveryForResource。

工作日志传输由三个元素组成：

- DeliverySource，表示用于发送日志的一个或多个资源的逻辑对象。对于 Amazon WorkMail，它是 Amazon WorkMail 组织。
- DeliveryDestination，这是表示实际传输目标的逻辑对象。
- Delivery，这将传输源连接到传输目标。

要在 Amazon WorkMail 和目标之间配置日志传输，您可以执行以下操作：

- 使用 putDeliverySource 创建传输源。
- 使用 putDeliveryDestination 创建传输目标。
- 如果要跨账户传输日志，则必须在目标账户中使用 PutDeliveryDestinationPolicy 为目标分配 IAM 策略。此策略授权创建从账户 A 中的传输源到账户 B 中的传输目标的传输。
- 通过使用 CreateDelivery 将一个传输源和一个传输目标精确配对来创建传输。

以下各节详细介绍在您登录以便将日志传输设置为每种类型的目标时必须具备的权限。这些权限可以授予您登录时使用的 IAM 角色。

> **Important**
>
> 删除日志生成资源后，您负责移除日志传输资源。

要在删除日志生成资源后移除日志传输资源，请执行以下步骤。

1. 使用 DeleteDelivery 操作删除 Delivery。
2. 使用 DeleteDeliverySource 操作删除 DeliverySource。
3. 如果与您刚删除的 DeliverySource 关联的 DeliveryDestination 仅用于此特定的 DeliverySource，则您可以使用 DeleteDeliveryDestinations 操作将其移除。

使用 Amazon WorkMail 控制台配置审计日志记录

您可以在 Amazon WorkMail 控制台中配置审计日志记录：

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 选择日志记录设置。
4. 选择审计日志设置选项卡。
5. 使用相应的小组件为所需的日志类型配置传输。
6. 选择保存。

发送到 CloudWatch Logs 的日志

用户权限

要启用将日志发送到 CloudWatch Logs，您必须使用以下权限登录。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:delivery:*",
                "arn:aws:logs:us-east-1:111122223333:delivery-source:*",
                "arn:aws:logs:us-east-1:111122223333:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyCWL",
            "Effect": "Allow",
            "Action": [
                "logs:PutResourcePolicy",
                "logs:DescribeResourcePolicies",
                "logs:DescribeLogGroups"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:*"
            ]
        },
        {
            "Sid": "AllowLogDeliveryForWorkMail",
            "Effect": "Allow",
            "Action": [
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource": [
                "arn:aws:workmail:us-
east-1:111122223333:organization/organization-id"
            ]
        }
    ]
}
```

日志组和资源策略

接收日志的日志组必须具有包含特定权限的资源策略。如果日志组当前没有资源策略，而且设置日志记录的用户对日志组具有 `logs:PutResourcePolicy`、`logs:DescribeResourcePolicies` 和 `logs:DescribeLogGroups` 权限，那么当您开始将日志发送到 CloudWatch Logs 日志时，AWS会自动为其创建以下策略。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "AWSLogDeliveryWrite20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "delivery.logs.amazonaws.com"
                ]
            },
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:log-group:my-log-group:log-
stream:*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": [
                        "111122223333"
                    ]
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:logs:us-east-1:111122223333:*"
                    ]
                }
            }
        }
    ]
}
```

日志组资源策略大小限制注意事项

这些服务必须在资源策略中列出它们向其发送日志的每个日志组。CloudWatch Logs 资源策略限制为 5120 个字符。将日志发送到大量日志组的服务可能会遇到此限制。

为了缓解这种情况，CloudWatch Logs 会监控发送日志的服务所使用的资源策略的大小。当 CloudWatch Logs 检测到策略接近 5120 个字符的大小限制时，它将在该服务的资源策略中自动启用 `/aws/vendedlogs/*`。之后，您可以开始将名称以 `/aws/vendedlogs/` 开头的日志组作为这些服务所发送的日志的目标。

发送到 Amazon S3 的日志

用户权限

要启用向 Amazon S3 发送日志，您必须使用以下权限登录。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:delivery:*",
                "arn:aws:logs:us-east-1:111122223333:delivery-source:*",
                "arn:aws:logs:us-east-1:111122223333:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyS3",
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketPolicy",
                "s3:GetBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
        },
        {
            "Sid": "AllowLogDeliveryForWorkMail",
            "Effect": "Allow",
            "Action": [
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource": [
                "arn:aws:workmail:us-
east-1:111122223333:organization/organization-id"
            ]
        }
    ]
}
```

接收日志的 S3 存储桶必须具有包含特定权限的资源策略。如果存储桶当前没有资源策略，而设置日志记录的用户对存储桶具有 S3:GetBucketPolicy 和 S3:PutBucketPolicy 权限，那么当您开始将日志发送到 Amazon S3 时，AWS 会自动为其创建以下策略。

JSON

```
{
    "Version":"2012-10-17",
    "Id": "AWSLogDeliveryWrite20150319",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
```

```
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::my-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": [
                        "account-id"
                    ]
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:logs:us-east-1:111122223333:delivery-source:*"
                    ]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::my-bucket/AWSLogs/111122223333/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": [
                        "account-id"
                    ]
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:logs:us-east-1:111122223333:delivery-source:*"
                    ]
                }
            }
        }
    ]
}
```

在之前的策略中，对于 aws:SourceAccount，请指定将日志传送到此存储桶的账户 ID 列表。对于 aws:SourceArn，请按 arn:aws:logs:*source-region*:*source-account-id*:* 格式指定生成日志的资源 ARN 列表。

如果存储桶具有资源策略，但该策略不包含上一个策略中所示的语句，并且设置日志记录的用户对存储桶具有 S3:GetBucketPolicy 和 S3:PutBucketPolicy 权限，则该语句将附加到存储桶的资源策略中。

> **Note**
>
> 在某些情况下，如果未向 delivery.logs.amazonaws.com 授予 s3:ListBucket 权限，您可能会在 AWS CloudTrail 中看到 AccessDenied 错误。为了避免在 CloudTrail 日志中出现这些错误，您必须向 delivery.logs.amazonaws.com 授予 s3:ListBucket 权限。还必须包含与在前面的存储桶策略中设置的 s3:GetBucketAcl 权限一起显示的 Condition 参数。为简化这一过程，可以直接将 AWSLogDeliveryAclCheck 更新为 “Action”: [“s3:GetBucketAcl”, “s3:ListBucket”]，而不是创建一个新的 Statement。

Amazon S3 存储桶服务器端加密

您可以通过启用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）或具有 AWS KMS 密钥（存储在 AWS Key Management Service 中）的服务器端加密（SSE-KMS）来保护 Amazon S3 存储桶中的数据。有关更多信息，请参阅使用服务器端加密保护数据。

如果选择 SSE-S3，则不需要额外的配置。Amazon S3 处理加密密钥。

> **Warning**
>
> 如果选择 SSE-KMS，则必须使用客户自主管理型密钥，因为此场景不支持使用 AWS 托管式密钥。如果您使用 AWS 托管密钥设置加密，则会以不可读取的格式提供日志。

当您使用客户托管式 AWS KMS 密钥时，您可以在启用存储桶加密时指定客户托管式密钥的Amazon Resource Name (ARN)。将以下内容添加到客户自主管理型密钥的密钥策略（不是 S3 存储桶的存储桶策略）中，以便日志传输账户可以写入 S3 存储桶。

如果选择 SSE-KMS，则必须使用客户自主管理型密钥，因为此场景不支持使用 AWS 托管式密钥。当您使用客户托管式 AWS KMS 密钥时，您可以在启用存储桶加密时指定客户托管式密钥的Amazon

Resource Name (ARN)。将以下内容添加到客户自主管理型密钥的密钥策略（不是 S3 存储桶的存储桶策略）中，以便日志传输账户可以写入 S3 存储桶。

```
{
    "Sid":"Allow Logs Delivery to use the key",
    "Effect":"Allow",
    "Principal":{
        "Service":[
            "delivery.logs.amazonaws.com"
        ]
    },
    "Action":[
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource":"*",
    "Condition":{
        "StringEquals":{
            "aws:SourceAccount":[
                "account-id"
            ]
        },
        "ArnLike":{
            "aws:SourceArn":[
                "arn:aws:logs:region:account-id:delivery-source:*"
            ]
        }
    }
}
```

对于 aws:SourceAccount，请指定将日志传送到此存储桶的账户 ID 列表。对于 aws:SourceArn，请按 arn:aws:logs:*source-region*:*source-account-id*:* 格式指定生成日志的资源 ARN 列表。

日志发送至 Firehose

用户权限

要启用向 Firehose 发送日志，您必须使用以下权限登录。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:delivery:*",
                "arn:aws:logs:us-east-1:111122223333:delivery-source:*",
                "arn:aws:logs:us-east-1:111122223333:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyFH",
            "Effect": "Allow",
            "Action": [
```

```
                "firehose:TagDeliveryStream"
            ],
            "Resource": [
                "arn:aws:firehose:us-east-1:111122223333:deliverystream/*"
            ]
        },
        {
            "Sid": "CreateServiceLinkedRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/aws-service-role/
delivery.logs.amazonaws.com/AWSServiceRoleForLogDelivery"
        },
        {
            "Sid": "AllowLogDeliveryForWorkMail",
            "Effect": "Allow",
            "Action": [
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource": [
                "arn:aws:workmail:us-
east-1:111122223333:organization/organization-id"
            ]
        }
    ]
}
```

用于资源权限的 IAM 角色

由于 Firehose 不使用资源策略，AWS 在将这些日志设置为发送到 Firehose 时会使用 IAM 角色。AWS 创建名为 AWSServiceRoleForLogDelivery 的服务相关角色。此服务相关角色包括以下权限。

此服务相关角色会为将 `LogDeliveryEnabled` 标签设置为 `true` 的所有 Firehose 传输流授予权限。当您设置日志记录时，AWS 会将此标签提供给目标传输流。

此服务相关角色还具有允许 `delivery.logs.amazonaws.com` 服务委托人来代入所需服务相关角色的信任策略。该信任策略如下所示：

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

控制台特定的权限

除了前面各节列出的权限外，如果您使用控制台而不是 API 来设置日志传输，则还需要以下权限：

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111122223333:log-group:*",
                "arn:aws:firehose:us-east-1:111122223333:deliverystream/*",
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "ListAccessForDeliveryDestinations",
            "Effect": "Allow",
```

```
            "Action": [
                "logs:DescribeLogGroups",
                "firehose:ListDeliveryStreams",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon WorkMail 的合规性验证

作为多项 AWS 合规性计划的一部分，第三方审计员将评估 Amazon WorkMail 的安全性和合规性。其中包括 SOC、ISO 和 C5。

有关特定合规性计划范围内的 AWS 服务的列表，请参阅合规性计划范围内的 AWS 服务。有关一般信息，请参阅 AWS合规性计划。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅在 Amazon Artifact 中下载报告。

您使用 Amazon WorkMail 的合规性责任取决于您数据的敏感度、贵公司的合规性目标以及适用的法律法规。AWS 提供以下资源来帮助满足合规性：

- 安全性与合规性快速入门指南 – 这些部署指南讨论了架构注意事项，并提供了在 AWS 上部署基于安全性和合规性的基准环境的步骤。
- AWS 合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- AWS Config – 此 AWS 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- AWS Security Hub CSPM – 此 AWS 服务提供了 AWS 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实操。

Amazon WorkMail 中的故障恢复能力

AWS全球基础架构围绕AWS区域和可用区构建。AWS区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础架构相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅 AWS 全球基础架构。

除了 AWS 全球基础设施之外，Amazon WorkMail 还提供多种功能，以帮助支持您的数据恢复能力和备份需求。

Amazon WorkMail 中的基础设施安全性

> **Note**
>
> Amazon WorkMail 已停止支持传输层安全性协议（TLS）1.0 和 1.1。如果您使用的是 TLS 1.0 或 1.1，则必须将 TLS 版本升级到 1.2。有关更多信息，请参阅 TLS 1.2 to become the minimum TLS protocol level for all AWS API endpoints。

作为一项托管式服务，Amazon WorkMail 受 AWS 全球网络安全保护。有关 AWS 安全服务以及 AWS 如何保护基础设施的信息，请参阅 AWS 云安全性。要按照基础设施安全最佳实践设计您的 AWS 环境，请参阅《安全性支柱 AWS Well-Architected Framework》中的基础设施保护。

您可以使用 AWS 发布的 API 调用通过网络访问 Amazon WorkMail。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

Amazon WorkMail 入门

完成先决条件后，您即可开始使用 Amazon WorkMail. 有关更多信息，请参阅 Amazon WorkMail 入门。

您可以在以下部分中了解有关将现有邮箱迁移到 Amazon WorkMail、与 Microsoft Exchange 之间的互操作性以及 Amazon WorkMail 配额的更多信息。

主题

Amazon WorkMail 入门

无论您是 Amazon WorkMail 的新用户，还是 Amazon WorkSpaces 的现有用户，都可以通过完成以下步骤开始使用 Amazon WorkMail。

> **Note**
>
> 开始使用前先完成先决条件。

主题

步骤 1：登录 Amazon WorkMail 控制台

您必须先登录 Amazon WorkMail 控制台，然后才能添加用户并管理其账户和邮箱。

登录 Amazon WorkMail 控制台

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。
2. 如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关区域的更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

步骤 2：设置 Amazon WorkMail 站点

1. 登录 Amazon WorkMail 控制台后，设置您的组织并添加域。我们建议为您的 Amazon WorkMail 组织使用专用域。有关更多信息，请参阅创建组织和添加域。
2. （可选）您可以选择使用 Amazon WorkMail 提供的免费测试域。如果您选择执行此操作，请跳至步骤 4。

> **Note**
>
> 测试域名使用以下格式：*alias*.awsapps.com。进行操作时，请记住，您只能使用测试域进行测试。不要在生产环境中使用测试域。此外，您的 Amazon WorkMail 组织中必须至少有一个已启用的用户。如果您没有已启用的用户，则该域可供其他客户注册和使用。

3. 如果您使用外部域，请通过向域名系统 (DNS) 服务添加相应的文本 (TXT) 和邮件交换 (MX) 记录来验证该域。TXT 记录允许您在 DNS 中输入注释。MX 记录指定了传入邮件服务器。请务必将您的域设置为贵组织的默认域。有关更多信息，请参阅验证域和选择默认域。
4. 为 Amazon WorkMail 创建新用户或启用您的现有目录用户。有关更多信息，请参阅 添加用户。
5. （可选）如果您有现有的 Microsoft Exchange 邮箱，请将其迁移到 Amazon WorkMail。有关更多信息，请参阅 迁移到 Amazon WorkMail。

在 Amazon WorkMail 站点设置完毕后，您可以使用 Web 应用程序 URL 访问 Amazon WorkMail。

查找 Amazon WorkMail Web 应用程序 URL

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。为此，请打开位于搜索框右侧的选择区域列表，然后选择所需的区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。

   此时将显示组织设置页面，并在用户登录下显示 URL。URL 采用以下形式：https://*alias*.awsapps.com/mail。

步骤 3：设置 Amazon WorkMail 用户访问权限

从以下选项中进行选择来设置 Amazon WorkMail 用户访问权限：

- 使用 Microsoft Outlook 客户端从现有桌面客户端设置用户访问权限。有关更多信息，请参阅将 Microsoft Outlook 连接到您的 Amazon WorkMail 账户。
- 从移动设备（如 Kindle、Android、iPad 或 iPhone）设置用户访问权限。有关更多信息，请参阅开始使用移动设备。
- 要设置用户访问权限，请使用与互联网邮件访问协议 (IMAP) 协议兼容的任何客户端软件。有关更多信息，请参阅将 IMAP 客户端连接到您的 Amazon WorkMail 账户。

更多资源

- 迁移到 Amazon WorkMail
- Amazon WorkMail 与 Microsoft Exchange 之间的互操作性
- Amazon WorkMail 配额

迁移到 Amazon WorkMail

通过与我们的合作伙伴之一合作，您可以从 Microsoft Exchange、Microsoft Office 365、G Suite Basic（以前称为 Google Apps for Work）及其他平台迁移到 Amazon WorkMail。有关我们的合作伙伴的更多信息，请参阅 Amazon WorkMail 功能。

主题

- 第 1 步：在 Amazon WorkMail 中创建或启用用户

第 1 步：在 Amazon WorkMail 中创建或启用用户

在迁移用户之前，您必须先在 Amazon WorkMail 中添加用户以预置其邮箱。有关更多信息，请参阅 添加用户。

第 2 步：迁移到 Amazon WorkMail

您可以与任何 AWS 迁移合作伙伴合作迁移到 Amazon WorkMail。有关这些提供商的信息，请参阅 Amazon WorkMail 功能。

要迁移您的邮箱，请创建专用 Amazon WorkMail 用户来充当迁移管理员。下面的过程向该用户授予访问组织中的所有邮箱的权限。

创建迁移管理员

1. 请执行以下操作之一：
   - 在 Amazon WorkMail 控制台中，创建新用户以充当迁移管理员。有关更多信息，请参阅 添加用户。
   - 在 Active Directory 中，创建一个新用户以充当迁移管理员，并为 Amazon WorkMail 启用该用户。有关更多信息，请参阅 启用用户。
2. 在 Amazon WorkMail 控制台导航窗格中，选择组织，然后选择贵组织的名称。
3. 依次选择组织设置、迁移和编辑。
4. 将已启用迁移滑块移动到“开启”位置。
5. 打开迁移管理员并选择一个用户。
6. 选择保存。

第 3 步：完成到 Amazon WorkMail 的迁移

在将电子邮件账户迁移到 Amazon WorkMail 后，您可以验证 DNS 记录并配置桌面和移动客户端。

完成到 Amazon WorkMail 的迁移

1. 验证是否所有 DNS 记录均已更新并指向 Amazon WorkMail。有关所需 DNS 记录的更多信息，请参见添加域。

   > **Note**
   >
   > DNS 记录更新过程可能需要几小时。如果更改 MX 记录时源邮箱中出现任何新项目，则可在 DNS 记录更新后重新运行迁移工具来迁移新项目。

2. 有关配置桌面或移动客户端以使用 Amazon WorkMail 的更多信息，请参阅《Amazon WorkMail 用户指南》中的将 Microsoft Outlook 连接到您的 Amazon WorkMail 账户。

Amazon WorkMail 与 Microsoft Exchange 之间的互操作性

在您将邮箱迁移到 Amazon WorkMail 或对一部分企业邮箱使用 Amazon WorkMail 时，Amazon WorkMail 与 Microsoft Exchange Server 之间的互操作性可尽可能减少给用户带来的中断。

此互操作性使您可对两种环境中的邮箱使用同一企业域。这样，您的用户可以通过双向共享日历闲/忙状态信息安排会议。

先决条件

在启用与 Microsoft Exchange 的互操作性之前，请执行以下操作：

- 确保为 Amazon WorkMail 启用了至少一个用户。这是配置 Microsoft Exchange 的可用性设置所必需的。要启用用户，请执行为用户启用电子邮件路由中的步骤。
- 设置 Active Directory (AD) Connector。使用本地目录设置 AD Connector 使用户能够继续使用其现有的企业凭证。有关更多信息，请参阅创建 AD Connector 和将 Amazon WorkMail 与您的本地目录集成。
- 设置您的 Amazon WorkMail 组织。创建一个使用您设置的 AD Connector 的 Amazon WorkMail 组织。
- 将您的企业域添加至 Amazon WorkMail 组织并在 Amazon WorkMail 控制台中验证它们。否则，发送至此别名的电子邮件将会退回。有关更多信息，请参阅使用域。
- 将邮箱迁移到 Amazon WorkMail 使用户能够预置邮箱并将其从本地环境迁移到 Amazon WorkMail。有关更多信息，请参阅启用现有用户和迁移到 Amazon WorkMail。

> **Note**
>
> 请勿将 DNS 记录更新为指向 Amazon WorkMail。这样可以确保，只要您愿意两个环境之间具有互操作性，Microsoft Exchange 会一直作为传入电子邮件的主服务器。

- 确保 Active Directory 中的用户主体名称 (UPN) 与用户的主要 SMTP 地址匹配。

Amazon WorkMail 向 Microsoft Exchange 上的 Exchange Web Services (EWS) URL 发出 HTTPS 请求，以获取日历忙/闲信息。

对于基于 EWS 的可用性提供商，Amazon WorkMail 向 Microsoft Exchange 上的 Exchange Web Services (EWS) URL 发出 HTTPS 请求，以获取日历忙/闲信息。因此，以下先决条件仅适用于基于 EWS 的可用性提供商。

- 确保将相关防火墙设置为允许来自 Internet 的访问。用于 HTTPS 请求的默认端口是端口 443。
- 仅当 Microsoft Exchange 环境中提供由有效证书颁发机构 (CA) 签名的证书时，Amazon WorkMail 才能对 Microsoft Exchange 上的 EWS URL 发出成功的 HTTPS 请求。有关更多信息，请参阅 Microsoft Exchange 文档网站上的为证书颁发机构创建 Exchange Server 证书请求。
- 您必须为 Microsoft Exchange 中的 EWS 启用基本身份验证。有关更多信息，请参阅 Microsoft MVP 奖励计划博客上的虚拟目录：Exchange 2013。

添加域并启用邮箱

将您的企业域添加到 Amazon WorkMail，以便可在电子邮件地址中使用它们。确保添加到 Amazon WorkMail 的域已经过验证，然后让用户和组在 Amazon WorkMail 中预置邮箱。在互操作模式下，无法在 Amazon WorkMail 中启用资源，而在禁用互操作模式后，应在 Amazon WorkMail 中重新创建资源。但是，在互操作模式下，仍然可以使用资源来安排会议。来自 Microsoft Exchange 的资源始终显示在 Amazon WorkMail 的用户选项卡中。

- 有关更多信息，请参阅添加域、启用现有用户以及启用现有组。

> **Note**
>
> 为确保与 Microsoft Exchange 之间的互操作性，请勿将 DNS 记录更新为指向 Amazon WorkMail 记录。只要您愿意两个环境之间具有互操作性，Microsoft Exchange 会一直作为传入电子邮件的主服务器。

启用互操作性

如果您尚未创建 Amazon WorkMail 组织，则可以使用公有 API 创建一个启用了互操作模式的新 WorkMail 组织。

如果您已有通过 AD Connector 链接至 Active Directory 的 Amazon WorkMail 组织，并且您还具有 Microsoft Exchange，请联系 AWS Support，以获取为现有 Amazon WorkMail 组织启用 Microsoft Exchange 互操作性的相关帮助。

在 Microsoft Exchange 和 Amazon WorkMail 中创建服务账户

> **Note**
>
> 如果不将 Exchange 用作自定义可用性提供商的后端，则无需在 Exchange 中创建服务账户。

要访问日历闲/忙信息，请在 Microsoft Exchange 和 Amazon WorkMail 中均创建一个服务账户。Microsoft Exchange 服务账户是 Microsoft Exchange 中对其他 Exchange 用户的日历闲/忙信息拥有访问权限的任何用户。默认情况下授予该访问权限；因此无需特殊权限。

类似地，Amazon WorkMail 服务账户是 Amazon WorkMail 中对其他 Amazon WorkMail 用户的日历闲/忙信息拥有访问权限的任何用户。这也是默认情况下授予的。您必须在本地目录中创建 Amazon WorkMail 用户，然后为该用户启用 Amazon WorkMail，才能将 Amazon WorkMail 与 AD Connector 集成到您的目录中。

互操作模式中的限制

当贵组织处于互操作模式时，您必须使用 Exchange 管理中心管理所有用户、组和资源。要启用 Amazon WorkMail 用户和组，请使用 AWS 管理控制台。有关更多信息，请参阅启用现有用户和启用现有组。

在为 Amazon WorkMail 启用用户或组时，您无法编辑这些用户和组的电子邮件地址或别名。这些内容也必须通过 Exchange 管理中心进行配置。Amazon WorkMail 会每 4 小时同步一次目录中的更改。

在互操作模式下，无法在 Amazon WorkMail 中创建或启用资源。但是，您的所有 Exchange 资源都可以在 Amazon WorkMail 通讯簿中找到，并可用于像往常一样安排会议。

在 Amazon WorkMail 上配置可用性设置

在 Amazon WorkMail 上配置可用性设置，以启用查询外部系统、提供日历功能以及获取日历忙/闲信息。Amazon WorkMail 支持两种从远程系统获取忙/闲信息的模式：

- Exchange Web Services (EWS) - 在此配置中，Amazon WorkMail 将使用 EWS 协议查询 Exchange 服务器或其他 WorkMail 组织的可用性信息。这是最简单的配置，但要求 Exchange 服务器的 EWS 端点可通过公共互联网进行访问。
- 自定义可用性提供商 (CAP) - 在此配置中，管理员可以配置 AWS Lambda 函数以获取给定电子邮件域的用户可用性信息。根据您的电子邮件服务器平台，将 CAP 与 Amazon WorkMail 结合使用具有以下优势：
  - 无需为 WorkMail 打开防火墙，即可从内部 EWS 获取用户可用性。
  - 从 Google Workspace（以前称为 G Suite）等非 Exchange 或非 EWS 系统获取用户可用性。

主题

配置基于 EWS 的可用性提供商

要在控制台上配置基于 EWS 的可用性设置，请完成以下过程：

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。为此，请打开位于搜索框右侧的选择区域列表，然后选择所需的区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择组织的名称。
3. 在导航窗格中，选择组织设置，然后选择互操作性选项卡。
4. 选择添加可用性配置，然后输入以下信息：

- 类型 – 选择 EWS。
- 域 – WorkMail 将尝试使用此配置查询其可用性信息的域。
- EWS URL – Amazon WorkMail 将查询指向 EWS 端点的此 URL。请参阅本指南的获取 EWS URL 部分。
- 用户电子邮件地址 – WorkMail 将用来向 EWS 端点进行身份验证的用户的电子邮件地址。
- 密码 – WorkMail 用于向 EWS 端点进行身份验证的密码。

5. 选择保存。

获取 EWS URL

要使用 Microsoft Outlook 获取 Exchange 的 EWS URL，请完成以下过程：

1. 对于 Exchange 环境中的任何用户，登录到 Windows 中的 Microsoft Outlook。
2. 按住 Ctrl 键并在任务栏中的 Microsoft Outlook 图标上打开上下文 (右键单击) 菜单。
3. 选择 Test E-mail AutoConfiguration。
4. 输入 Microsoft Exchange 用户的电子邮件地址和密码，然后选择 Test。
5. 从“Results”窗口中复制 Availability Service URL 的值。

要使用 PowerShell 获取 Exchange 的 EWS URL，请在 PowerShell 提示符下执行以下命令：

```
Get-WebServicesVirtualDirectory |Select name, *url* | fl
```

要获取 Amazon WorkMail 的 EWS URL，请先在 Amazon WorkMail 端点和配额下找到 EWS 域。输入 EWS URL (`https://"EWS domain"/EWS/Exchange.asmx`)，然后将“EWS 域”替换为您的 EWS 域。

配置自定义可用性提供商

要配置自定义可用性提供商 (CAP)，请完成以下过程：

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。为此，请打开位于搜索框右侧的选择区域列表，然后选择所需的区域。
2. 在导航窗格中，选择组织，然后选择组织的名称。
3. 在导航窗格中，选择组织设置，然后选择互操作性。

4. 选择添加可用性配置，然后输入以下信息：

   - 类型 – 选择 CAP Lambda。
   - 域 – WorkMail 将尝试使用此配置查询其可用性信息的域。
   - ARN – 将提供可用性信息的 Lambda 函数的 ARN。

要构建 CAP Lambda 函数，请参阅构建自定义可用性提供商 Lambda 函数。

构建自定义可用性提供商 Lambda 函数

自定义可用性提供商 (CAP) 使用基于 JSON 的请求和响应协议进行配置，该协议以明确定义的 JSON 架构编写。Lambda 函数将解析请求并提供有效的响应。

主题

请求和响应元素

请求元素

以下是用于为 Amazon WorkMail 用户配置 CAP 的示例请求：

```
{
    "requester": {
        "email": "user1@internal.example.com",
        "userName": "user1",
        "organization": "m-0123456789abcdef0123456789abcdef",
        "userId": "S-1-5-18",
        "origin": "127.0.0.1"
    },
    "mailboxes": [
        "user2@external.example.com",
        "unknown@internal.example.com"
    ],
    "window": {
        "startDate": "2021-05-04T00:00:00.000Z",
        "endDate": "2021-05-06T00:00:00.000Z"
```

```
    }
}
```

请求由三个部分组成：requester、mailboxes 和 window。本指南的 请求者、Mailboxes 和 窗口 部分分别介绍了这些内容。

请求者

requester 部分提供了有关向 Amazon WorkMail 发出原始请求的用户的信息。CAP 会使用此信息来更改提供商的行为。例如，此数据可用于模拟后端可用性提供商上的同一用户，或者可以在响应中省略某些详细信息。

字段	描述	必填
`Email`	请求者的主要电子邮件地址。	是
`Username`	请求者的用户名。	是
`Organization`	请求者的组织 ID。	是
`UserID`	请求者 ID。	是
`Origin`	请求的远程地址。	否
`Bearer`	留待将来使用。	否

Mailboxes

mailboxes 部分包含用户的以逗号分隔的电子邮件地址列表，用于请求其可用性信息。

窗口

window 部分包含请求可用性信息的时间窗口。`startDate` 和 `endDate` 均采用 UTC 格式指定，并根据 RFC 3339 设置格式。预计事件不会被截断。换句话说，如果事件在定义的 `StartDate` 之前开始，则将使用原始开始时间。

响应元素

Amazon WorkMail 将等待 25 秒才能收到来自 CAP Lambda 函数的响应。25 秒后，Amazon WorkMail 将假定该函数已失败，并在 EWS GetUserAvailability 响应中为关联的邮箱生成失败。这不会导致整个 getUserAvilability 操作失败。

以下是来自本部分开头定义的配置的响应示例：

```
{
    "mailboxes": [{
        "mailbox": "user2@external.example.com",
        "events": [{
            "startTime": "2021-05-03T23:00:00.000Z",
            "endTime": "2021-05-04T03:00:00.000Z",
            "busyType": "BUSY"|"FREE"|"TENTATIVE",
            "details": {  // optional
                "subject": "Late meeting",
                "location": "Chime",
                "instanceType": "SINGLE_INSTANCE"|"RECURRING_INSTANCE"|"EXCEPTION",
                "isMeeting": true,
                "isReminderSet": true,
                "isPrivate": false
            }
        }],
        "workingHours": {
            "timezone": {
                "name": "W. Europe Standard Time"
                "bias": 60,
                "standardTime": {  // optional (not needed for fixed offsets)
                    "offset": 60,
                    "time": "02:00:00",
                    "month":
 "JAN"|"FEB"|"MAR"|"APR"|"JUN"|"JUL"|"AUG"|"SEP"|"OCT"|"NOV"|"DEC",
                    "week": "FIRST"|"SECOND"|"THIRD"|"FOURTH"|"LAST",
                    "dayOfWeek": "SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"
                },
                "daylightTime": {  // optional (not needed for fixed offsets)
                    "offset": 0,
                    "time": "03:00:00",
                    "month":
 "JAN"|"FEB"|"MAR"|"APR"|"JUN"|"JUL"|"AUG"|"SEP"|"OCT"|"NOV"|"DEC",
                    "week": "FIRST"|"SECOND"|"THIRD"|"FOURTH"|"LAST",
                    "dayOfWeek": "SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"
                },
            },
            "workingPeriods":[{
                "startMinutes": 480,
                "endMinutes": 1040,
                "days": ["SUN"|"MON"|"TUE"|"WED"|"THU"|"FRI"|"SAT"]
            }]
```

```
        }
    },{
        "mailbox": "unknown@internal.example.com",
        "error": "MailboxNotFound"
    }]
}
```

响应由一个 mailboxes 部分组成，该部分包含邮箱列表。成功获取其可用性的每个邮箱均由三个部分组成：mailbox、events 和 workinghours。如果可用性提供商无法获取邮箱的可用性信息，则该部分由两个部分组成：mailbox 和 error。本指南的 Mailbox、事件、Working Hours、时区、Working Periods 和 错误 部分分别介绍了这些内容。

Mailbox

mailbox 部分是在请求的 mailboxes 部分中找到的用户的电子邮件地址。

事件

events 部分是请求的窗口中发生的事件的列表。每个事件都使用以下参数进行定义：

字段	描述	必填
`startTime`	事件的开始时间，采用 UTC 格式，并根据 RFC 3339 设置格式。	是
`endTime`	事件的结束时间，采用 UTC 格式，并根据 RFC 3339 设置格式。	是
`busyType`	事件的忙类型。可以是 `Busy`、`Free` 或 `Tentative`。	是
`details`	事件的详细信息。	否
`details.subject`	事件的主题。	是
`details.location`	事件发生的位置。	是

字段	描述	必填
details.instanceType	事件的实例类型。可以是 Single_Instance 、Recurring_Instance 或 Exception 。	是
details.isMeeting	一个布尔值，用于指示事件是否有参与者。	是
details.isReminderSet	一个布尔值，用于指示事件是否设置了提醒。	是
details.isPrivate	一个布尔值，用于指示事件是否设置为私有。	是

Working Hours

workingHours 部分包含有关邮箱所有者的工作时间的信息。它包含两个部分：timezone 和 workingPeriods。

时区

timezone 子部分说明了邮箱所有者所在的时区。当请求者在不同的时区工作时，正确呈现用户的工作时间非常重要。可用性提供商必须明确描述时区，而不是使用名称。使用标准化时区描述有助于避免时区不匹配。

字段	描述	必填
name	时区的名称。	是
bias	与 GMT 的默认偏移量（以分钟为单位）。	是
standardTime	指定时区标准时间的开始时间。	否
daylightTime	指定时区夏令时的开始时间。	否

必须同时定义 standardTime 和 daylightTime，或者省略两者。standardTime 和 daylightTime 对象中的字段包括：

字段	描述	允许的值
offset	相对于默认偏移量的偏移量（以分钟为单位）。	NA
time	标准时间和夏令时之间发生转换的时间，指定为 hh:mm:ss。	NA
month	标准时间和夏令时之间发生转换所在的月份。	JAN,FEB, MAR, APR, JUN, JUL, AUG, SEP, OCT, NOV, DEC
week	指定月份内标准时间和夏令时之间发生转换所在的周。	FIRST, SECOND, THIRD, FOURTH, LAST
dayOfWeek	指定周内标准时间和夏令时之间发生转换所在的当天。	SUN, MON, TUE, WED, THU, FRI, SAT

Working Periods

workingPeriods 部分包含一个或多个工作周期对象。每个周期定义一天或多天工作日的开始和结束。

字段	描述	允许的值
startMinutes	工作日的开始，从午夜算起（以分钟为单位）。	NA
endMinutes	工作日的结束，从午夜算起（以分钟为单位）。	NA
days	此周期适用的工作日。	SUN, MON, TUE, WED, THU, FRI, SAT

错误

error 字段可以包含任意错误消息。下表列出了已知代码到 EWS 错误代码的映射。所有其他消息都将映射到 ERROR_FREE_BUSY_GENERATION_FAILED。

值	EWS 错误代码	
MailboxNotFound	ERROR_MAIL_RECIPIENT_NOT_FOUND	
ErrorAvailabilityConfigNotFound	ERROR_AVAILABILITY_CONFIG_NOT_FOUND	
ErrorServerBusy	ERROR_SERVER_BUSY	
ErrorTimeoutExpired	ERROR_TIMEOUT_EXPIRED	
ErrorFreeBusyGenerationFailed	ERROR_FREE_BUSY_GENERATION_FAILED	
ErrorResponseSchemaValidation	ERROR_RESPONSE_SCHEMA_VALIDATION	

授予访问权限

从 AWS Command Line Interface (AWS CLI) 运行以下 Lambda 命令。此命令可将资源策略添加到解析 CAP 的 Lambda 函数。此函数允许 Amazon WorkMail 可用性服务调用您的 Lambda 函数。

```
aws lambda add-permission \
    --region LAMBDA_REGION \
    --function-name CAP_FUNCTION_NAME \
    --statement-id AllowWorkMail \
    --action "lambda:InvokeFunction" \
    --principal availability.workmail.WM_REGION.amazonaws.com \
    --source-account WM_ACCOUNT_ID \
    --source-arn arn:aws:workmail:WM_REGION:WM_ACCOUNT_ID:organization/ORGANIZATION_ID
```

在命令中，在指示的位置添加以下参数：

- *LAMBDA_REGION* – 部署 CAP Lambda 的区域的名称。例如 us-east-1。
- *CAP_FUNCTION_NAME* – CAP Lambda 函数的名称。

> **Note**
>
> 这可以是 CAP Lambda 函数的名称、别名或者部分或全部 ARN。

- *WM_REGION* – Amazon WorkMail 组织调用 Lambda 函数所在的区域的名称。

> **Note**
>
> 只有以下区域可与 CAP 结合使用：
>
> - 美国东部（弗吉尼亚州北部）
> - 美国西部（俄勒冈州）
> - 欧洲地区（爱尔兰）

- *WM_ACCOUNT_ID* – 组织账户的 ID。
- *ORGANIZATION_ID* – 调用 CAP Lambda 的组织的 ID。例如，组织 ID：m-934ebb9eb57145d0a6cab566ca81a21f。

> **Note**
>
> 仅当需要跨区域调用时，*LAMBDA_REGION* 和 *WM_REGION* 才会有所不同。如果不需要跨区域调用，则它们将是相同的。

使用 CAP Lambda 函数的 Amazon WorkMail 示例

有关 Amazon WorkMail 使用 CAP Lambda 函数查询 EWS 端点的示例，请参阅适用于 Amazon WorkMail GitHub 存储库的无服务器应用程序中的 AWS 示例应用程序。

在 Microsoft Exchange 中配置可用性设置

要将已启用用户的所有日历闲/忙信息请求都重定向到 Amazon WorkMail，请在 Microsoft Exchange 中设置一个可用性地址空间。

使用以下 PowerShell 命令创建地址空间：

```
$credentials = Get-Credential
```

在提示符处，输入 Amazon WorkMail 服务账户的凭证。应将用户名输入为 **domain\username**（即 ***orgname*.awsapps.com\workmail_service_account_*username***）。其中，***orgname*** 表示 Amazon WorkMail 组织的名称。有关更多信息，请参阅 在 Microsoft Exchange 和 Amazon WorkMail 中创建服务账户。

```
Add-AvailabilityAddressSpace -ForestName orgname.awsapps.com -AccessMethod OrgWideFB -
Credentials $credentials
```

有关更多信息，请参阅 Microsoft Docs 网站上的 Add-AvailabilityAddressSpace。

在 Microsoft Exchange 与 Amazon WorkMail 用户之间启用电子邮件路由

通过 Microsoft Exchange Server 和 Amazon WorkMail 之间的电子邮件路由，用户可以在迁移到 Amazon WorkMail 后保留其现有电子邮件地址。电子邮件路由允许您将 Microsoft Exchange Server 作为组织接收电子邮件的主要简单邮件传输协议 (SMTP) 服务器。

在使用电子邮件路由之前，您需要完成以下先决条件：

- 为组织启用互操作模式。有关更多信息，请参阅 启用互操作性。
- 确保您在 Amazon WorkMail 控制台中看到您的域。
- 验证我们的 Microsoft Exchange Server 是否可以将电子邮件发送到互联网。您可能需要配置“发送”连接器。有关“发送”连接器的更多信息，请参阅 Microsoft 文档中的在 Exchange Server 中创建“发送”连接器以将邮件发送到互联网。

为用户启用电子邮件路由

建议您先对测试用户完成以下步骤，然后再对组织应用任何更改。

1. 启用要迁移到 Amazon WorkMail 的用户账户。有关更多信息，请参阅启用现有用户。
2. 在 Amazon WorkMail 控制台中，确保至少有两个电子邮件地址与已启用的用户关联。
   - <*workmailuser*@*orgname*.awsapps.com>（这是自动添加的，可用于不使用 Microsoft Exchange 时的测试。）

- <*workmailuser*@*yourdomain*.com>（这是自动添加的，是主 Microsoft Exchange 地址。）

  有关更多信息，请参阅编辑用户电子邮件地址。

3. 确保将 Microsoft Exchange 中邮箱内的所有数据都迁移到 Amazon WorkMail 中的邮箱。有关更多信息，请参阅迁移到 Amazon WorkMail。
4. 迁移完所有数据后，在 Microsoft Exchange 上禁用该用户的邮箱。然后，创建一个邮件用户（或已启用邮件的用户），其外部 SMTP 地址指向 Amazon WorkMail。为此，请在 Exchange Management Shell 中使用以下命令：

   > **Important**
   >
   > 以下步骤可擦除邮箱的内容。确保您的数据已迁移到 Amazon WorkMail，然后再尝试启用电子邮件路由。当您运行此命令时，某些邮件客户端无法无缝切换到 Amazon WorkMail。有关更多信息，请参阅 邮件客户端配置。

   ```
   $old_mailbox = Get-Mailbox exchangeuser
   ```

   ```
   Disable-Mailbox $old_mailbox
   ```

   ```
   $new_mailuser = Enable-MailUser $old_mailbox.Identity -
   ExternalEmailAddress workmailuser@orgname.awsapps.com -PrimarySmtpAddress
    $old_mailbox.PrimarySmtpAddress
   ```

   ```
   Set-MailUser $new_mailuser -EmailAddresses $old_mailbox.EmailAddresses -
   HiddenFromAddressListsEnabled $old_mailbox.HiddenFromAddressListsEnabled
   ```

   在上述命令中，*orgname* 表示您的 Amazon WorkMail 组织的名称。有关更多信息，请参阅 Microsoft TechNet 上的禁用邮箱和启用邮件用户。

5. 向用户发送测试电子邮件（在上面的示例中，为 **workmailuser@yourdomain.com**）。如果已正确启用电子邮件路由，用户应该能够登录其 Amazon WorkMail 邮箱并接收电子邮件。

> **Note**
>
> 只要您愿意两个环境之间具有互操作性，Microsoft Exchange 会一直作为传入电子邮件的主服务器。为确保与 Microsoft Exchange 之间的互操作性，DNS 记录不应更新为指向 Amazon WorkMail。

发布设置配置

上述步骤将用户邮箱从 Microsoft Exchange Server 移动到 Amazon WorkMail，同时将该用户作为联系人保留在 Microsoft Exchange 中。由于已迁移用户现在是外部邮件用户，Microsoft Exchange Server 施加了其他约束，完成迁移可能需要满足其他配置要求。

- 默认情况下，该用户可能无法向组发送电子邮件。要启用此功能，必须将用户添加到所有组的安全发件人列表中。有关更多信息，请参见 Microsoft TechNet 上的交付管理。
- 用户可能无法预订资源。要启用此功能，必须设置用户需要访问的所有资源的 `ProcessExternalMeetingMessages`。有关更多信息，请参见 Microsoft TechNet 上的 Set-CalendarProcessing。

邮件客户端配置

某些邮件客户端无法无缝切换到 Amazon WorkMail。这些客户端要求用户执行其他设置步骤。不同邮件客户端需要执行不同操作。

- Windows 上的 Microsoft Outlook – 需要重新启动 Outlook。启动时，您需要选择继续使用旧邮箱还是使用临时邮箱。选择临时邮箱选项。然后重新配置 Microsoft Exchange 邮箱。
- MacOS 上的 Microsoft Outlook – 重新启动 Outlook 时，它会提示以下消息：Outlook 已重定向到 ***orgname***.awsapps.com。是否希望此服务器配置您的设置？接受建议。
- iOS 上的邮件 – 该邮件应用程序将停止接收电子邮件并生成 can't get mail 错误。重新创建并重新配置 Microsoft Exchange 邮箱。

禁用互操作模式并停用邮件服务器

为 Amazon WorkMail 配置 Microsoft Exchange 邮箱后，您即可禁用互操作模式。如果您尚未迁移任何用户或记录，则禁用互操作模式不会影响任何配置。

> **Warning**
>
> 在禁用互操作模式之前，请确保完成所有必需的步骤。否则可能会导致电子邮件被退回或发生意外行为。如果您尚未完成迁移，禁用互操作性可能导致组织中断。您无法撤消此操作。

禁用互操作模式支持

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择您要为其禁用互操作模式的组织。
3. 在组织设置中，选择禁用互操作模式。
4. 在禁用互操作模式对话框中，输入组织的名称并选择禁用互操作模式。

在禁用互操作性支持后，将从通讯簿中删除没有为 Amazon WorkMail 启用的用户和组。您仍然可以使用 Amazon WorkMail 控制台启用任何缺失的用户或组，这些用户或组将添加到通讯簿中。在完成以下步骤之前，无法启用 Microsoft Exchange 中的资源，并且这些资源不会显示在通讯簿中。

- 在 Amazon WorkMail 中创建资源 – 您可以在 Amazon WorkMail 中创建资源，然后为这些资源配置代理和预订选项。有关更多信息，请参阅使用资源。
- 创建自动发现 DNS 记录 – 为组织中的所有邮件域配置自动发现 DNS 记录。这使用户能够从其 Microsoft Outlook 和移动客户端连接到其 Amazon WorkMail 邮箱。有关更多信息，请参阅使用自动发现配置终端节点。
- 将您的 MX DNS 记录切换到至 Amazon WorkMail – 要将所有传入的电子邮件传送到 Amazon WorkMail，您必须将 MX DNS 记录切换至 Amazon WorkMail。对 DNS 记录的更改最多可能需要 72 小时才能传播到所有 DNS 服务器。
- 停用邮件服务器 – 在确认所有电子邮件都直接路由到 Amazon WorkMail 后，如果不打算继续使用邮件服务器，则您可以将其停用。

故障排除

下面列出了最常遇到的 Amazon WorkMail 互操作性和迁移错误的解决方案。

Exchange Web Services (EWS) URL 无效或无法访问 –检查您是否具有正确的 EWS URL。有关更多信息，请参阅 在 Amazon WorkMail 上配置可用性设置。

EWS 验证期间出现连接故障 – 这是常规错误，可能由以下原因引起：

- Microsoft Exchange 中没有互联网连接。
- 您的防火墙未配置为允许来自互联网的访问。确保端口 443 (HTTPS 请求的默认端口) 处于打开状态。

如果您已确认互联网连接和防火墙设置，但错误仍然存在，请联系 AWS Support。

配置 Microsoft Exchange 互操作性时用户名和密码无效 – 这是常规错误，可能由以下原因引起：

- 用户名未使用所需形式。请使用以下模式：

```
DOMAIN\username
```

- 您的 Microsoft Exchange 服务器没有配置为对 EWS 进行基本身份验证。有关更多信息，请参阅 Microsoft MVP 奖励计划博客上的虚拟目录：Exchange 2013。

用户收到包含 winmail.dat 附件的电子邮件 – 在从 Exchange 向 Amazon WorkMail 发送加密的 S/MIME 电子邮件并在 Outlook 2016 for Mac 或 IMAP 客户端中接收时，可能会发生这种情况。解决方案是在 Exchange Management Shell 中运行以下命令：

Set-RemoteDomain -Identity "Default" -TNEFEnabled $false

如果您已确认上述几点，但错误仍然存在，请联系 AWS Support。

Amazon WorkMail 配额

企业客户和小型企业主均可使用 Amazon WorkMail。虽然我们支持大多数使用案例而无需配置对配额的任何更改，但我们也会避免让用户和 Internet 滥用产品。因此，一些客户可能会遇到我们设置的配额。本节介绍这些配额以及如何对其进行更改。

部分配额值可以更改，还有一些硬性配额无法更改。有关请求增加配额的更多信息，请参阅《Amazon Web Services 一般参考》中的AWS 服务限额。

Amazon WorkMail 组织和用户配额

您最多可以向 Amazon WorkMail 组织添加 25 个用户，以获得 30 天的免费试用。在此期限结束后，您将需要为所有活动用户付费，除非删除它们或关闭您的 Amazon WorkMail 账户。

在评估这些配额时，将考虑发送到其他用户的所有消息。这些包括由于规则而自动转发或重定向的电子邮件、会议请求、会议响应、任务请求和消息。

> **Note**
>
> 请求增加特定组织的配额时，必须在请求中包含组织名称。

资源	默认配额	更改请求的上限
每个 AWS 账户的 Amazon WorkMail 组织	100	可以根据组织的目录类型增加。您可以从 AWS Directory Service 控制台查看 Directory Service 配额并请求增加。有关更多信息，请参阅《AWS 一般参考》中的服务配额。
每个 Amazon WorkMail 组织的用户数	1000	可以根据组织的目录类型增加，如下所示： • Amazon WorkMail 目录：最多 1,000 万个用户 • Simple AD 或 AD Connector，大型：最多 5000 个用户* • Simple AD 或 AD Connector，小型：最多 500 个用户* • 由 Directory Service 托管的 Microsoft AD：根据您的设置和配置，最多 1,000 万个用户，

资源	默认配额	更改请求的上限
		*如果您使用的是 Simple AD 或 AD Connector，请参阅 AWS Directory Service 来获取更多信息。
免费试用用户	前 30 天最多 25 个用户	免费试用期仅适用于任何组织中的前 25 个用户。任何其他用户都不包括在免费试用优惠中。
每个 AWS 账户每天向其发送邮件的收件人数	100000 个组织外部收件人，对组织内部收件人数未设硬性配额	无上限。但是，Amazon WorkMail 是企业电子邮件服务，不能用于批量电子邮件服务。有关批量电子邮件服务，请参阅 Amazon SES 或 Amazon Pinpoint。
每个 AWS 账户每天使用任何测试域向其发送邮件的收件人数	200 个收件人，不考虑目的地	测试邮件域不能长期使用。我们建议您添加自己的域并使用它作为默认域。

组的配额是由基础目录设置的。

WorkMail 组织设置配额

资源	默认配额
每个 Amazon WorkMail 组织的域的数量	1000 这是硬性配额，无法更改。
每个规则电子邮件流规则中的发件人模式数量	250 这是硬性配额，无法更改。
每个组织电子邮件流规则中的发件人模式数量	1000

资源	默认配额
	这是硬性配额，无法更改。

每用户配额

在评估这些配额时，将考虑发送到其他用户的所有消息。这些包括由于规则而自动转发或重定向的电子邮件、会议请求、会议响应、任务请求和消息。

资源	默认配额	更改请求的配额上限
邮箱的最大大小	50 GB 这是硬性配额，无法更改。	不适用
每个用户的最大别名数	100 这是硬性配额，无法更改。	不适用
每个用户每天使用您拥有的域向其发送邮件的收件人数	10000 个组织外部收件人，对组织内部收件人数未设硬性配额。	无上限。但是，Amazon WorkMail 是企业电子邮件服务，不能用于批量电子邮件服务。有关批量电子邮件服务，请参阅 Amazon SES 或 Amazon Pinpoint。

消息配额

在评估这些配额时，将考虑发送到其他用户的所有消息。这些包括由于规则而自动转发或重定向的电子邮件、会议请求、会议响应、任务请求和消息。

资源	默认配额
传入邮件的最大大小	29MB 的未编码数据。 以 MIME 格式接收邮件。传入的 MIME 邮件的最大大小为 40MB。

资源	默认配额
	这是硬性配额，无法更改。
传出邮件的最大大小	29MB 的未编码数据。 以 MIME 格式发送邮件。传出的 MIME 邮件的最大大小为 40MB。 这是硬性配额，无法更改。
每封邮件的最大收件人数	500 这是硬性配额，无法更改。
每封邮件的最大附件数	500 这是硬性配额，无法更改。

使用组织

在 Amazon WorkMail 中，组织代表公司中的用户。在 Amazon WorkMail 控制台中，您会看到可用的组织列表。如果您没有任何可用组织，则必须创建一个组织才能使用 Amazon WorkMail。

主题

创建组织

要使用 Amazon WorkMail，您必须先创建一个组织。一个 AWS 账户可以具有多个 Amazon WorkMail 组织。创建组织时，您还可以为组织选择域并设置用户目录和加密设置。

您可以创建一个新的 Amazon WorkMail 目录与 WorkMail 组织结合使用，也可以将 Amazon WorkMail 与现有目录集成。您可以将 Amazon WorkMail 与以下类型的现有目录结合使用：

- 本地 Microsoft Active Directory
- AWS Managed Active Directory（即由 AWS Directory Service 管理的 Microsoft AD）
- Simple AD

通过与本地目录集成，您可以使用 Amazon WorkMail 中现有的用户和组，并且用户可以使用其现有的凭证登录。如果您使用的是本地目录，则必须先在 AWS Directory Service 中设置 AD Connector。AD Connector 将您的用户和组与 Amazon WorkMail 通讯簿同步，并执行用户身份验证请求。有关更多信息，请参阅《Directory Service 管理员指南》中的 Active Directory Connector。

您还可以选择 Amazon WorkMail 用于加密邮箱内容的 AWS KMS key。您可以为 Amazon WorkMail 选择默认的 AWS 托管主密钥，也可以在 AWS Key Management Service (AWS KMS) 中使用现有的 KMS 密钥。有关创建新的 KMS 密钥的信息，请参阅《AWS Key Management Service 开发指南》中的创建密钥。如果您以 AWS Identity and Access Management (IAM) 用户身份登录，请使自己成为

KMS 密钥的密钥管理员。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的启用和禁用密钥。

注意事项

创建 Amazon WorkMail 组织时，请记住以下几点：

- Amazon WorkMail 目前不支持您与多个账户共享的托管 Microsoft Active Directory 服务。
- 如果您有带有 Microsoft Exchange 和 AD Connector 的本地 Active Directory，我们建议您为组织配置互操作性设置。这样，当您将邮箱迁移到 Amazon WorkMail 或对一部分企业邮箱使用 Amazon WorkMail 时，可尽可能减少给用户带来的中断。有关更多信息，请参阅 Amazon WorkMail 与 Microsoft Exchange 之间的互操作性。
- 如果您选择免费测试域选项，则可以开始将 Amazon WorkMail 组织与提供的测试域结合使用。测试域采用以下格式：*example*.awsapps.com。只要在 Amazon WorkMail 组织中维护已启用的用户，您就可以将测试邮件域与 Amazon WorkMail 和其他受支持的 AWS 服务结合使用。但是，不能将测试域用于其他目的。如果您的 Amazon WorkMail 组织维护的已启用的用户不足一个，则测试域可能可以供其他客户注册和使用。
- Amazon WorkMail 不支持多区域目录。
- Amazon WorkMail 每四小时将目录数据与 AWS Managed Active Directory、Simple AD 和 AD Connector 同步一次。

有关使用 AWS Managed Active Directory 的重要更改

Amazon WorkMail 正在更新其针对使用 AWS Managed Active Directory（托管式 AD）的组织的授权模型。此更改会影响 Amazon WorkMail 与目录数据交互的方式，并要求您采取特定的措施以确保功能持续正常运行。

以前，当使用 AWS Managed Active Directory 创建 Amazon WorkMail 组织时，Amazon WorkMail 使用服务级别权限来与托管式 AD 进行交互。为了让客户更灵活地将目录管理和邮箱管理角色分开，WorkMail 的 API 和控制台现在将使用 AWS Directory Service Data（DS-Data）API 来创建或更新 AWS Managed Active Directory 中的用户和组。通过 WorkMail 控制台或 API 执行这些操作的 IAM 主体还需要获得授权，才能对与其 WorkMail 组织关联的托管式 AD 使用等效的 DS-Data 操作，从而提供更精细的控制并更好地与 IAM 策略集成。

无论您是使用托管式 AD 创建新组织，还是具有使用托管式 AD 的现有组织，如果您希望继续能够通过 WorkMail 控制台或 API 创建、更新或删除用户和组，则必须完成其他配置步骤，以确保更新后的授权模型能够正常运行。相关解释，请参阅the section called “托管式 AD 集成”。

主题

创建组织

在 Amazon WorkMail 控制台中创建一个新组织。

创建 组织

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航栏中，选择组织。

   此时将出现组织页面并显示您的组织（如果有）。
3. 选择创建组织。
4. 在电子邮件域下，选择要用于组织中电子邮件地址的域：
   - 现有 Route 53 域：选择您使用 Amazon Route 53 (Route 53) 托管区管理的现有域。
   - 新的 Route 53 域：注册新的 Route 53 域以用于 Amazon WorkMail。
   - 外部域：输入您使用外部域名系统 (DNS) 提供商管理的现有域。
   - 免费测试域：使用 Amazon WorkMail 提供的免费测试域。您可以使用测试域来浏览 Amazon WorkMail，然后再向组织添加域。
5. （可选）如果您的域是通过 Amazon Route 53 进行管理，则对于 Route 53 托管区，请选择您的 Route 53 域。
6. 在别名中，输入组织的唯一别名。
7. 选择高级设置，然后对于用户目录，选择以下选项之一：
   - 创建新的 Amazon WorkMail 目录：创建用于添加和管理用户的新目录。

- 使用现有目录：使用现有目录管理用户，例如本地 Microsoft Active Directory、AWS Managed Active Directory 或 Simple AD。

8. 对于加密，选择以下选项之一：

   - 使用 Amazon WorkMail 托管密钥：在您的账户中创建新的加密密钥。
   - 使用现有 KMS 密钥：使用您已在 AWS KMS 中创建的现有 KMS 密钥。

9. 选择创建组织。

如果您使用一个外部域，请通过向 DNS 服务添加相应的文本 (TXT) 和邮件交换器 (MX) 记录来验证该域。TXT 记录允许您输入有关 DNS 服务的注释。MX 记录指定了传入邮件服务器。

请务必将您的域设置为贵组织的默认域。有关更多信息，请参阅验证域和选择默认域。

当组织处于活动状态时，您可以向其添加用户并设置其电子邮件客户端。有关更多信息，请参阅添加用户和为 Amazon WorkMail 设置电子邮件客户端。

配置 AWS Managed Active Directory 集成

将 AWS Managed Active Directory 与 Amazon WorkMail 组织结合使用时，额外的配置步骤可确保更新后的授权模型能够正常运行。

为新组织配置托管式 AD 集成

1. 在 Directory Service 控制台中，导航到托管式 AD（Microsoft AD），或者从 Amazon WorkMail 控制台中，在左侧导航面板中选择用户或组，然后单击页面顶部备注框中的目录链接。
2. 针对用户和组管理选择启用。默认情况下禁用该设置，但必须启用此设置才能对用户和组执行写操作。
3. 通过附加包含以下操作的策略，确保 IAM 主体拥有所需的权限：

```
ds:AccessDSData
ds:ResetUserPassword
ds-data:CreateGroup
ds-data:DeleteGroup
ds-data:AddGroupMember
ds-data:RemoveGroupMember
ds-data:CreateUser
ds-data:DeleteUser
ds-data:UpdateUser
```

迁移现有的托管式 AD 组织

1. 监控 Amazon WorkMail 控制台中的用户或组页面，以获取迁移通知。
2. 出现通知后，开启启用更新的目录操作以迁移到新的 Directory Service API。
3. 最后，请确保您已在 Directory Service 控制台中启用用户和组管理，并使用上一节中所述的所需 DS-Data 权限更新您的 IAM 策略。

对于所有仍在使用托管式 AD 的 Amazon WorkMail 组织，将启用 AWS Directory Service Data（DS-Data）API 来创建、更新和删除用户（如果之前尚未启用）。

查看组织的详细信息

您的每个 Amazon WorkMail 组织都可以显示组织详细信息页面。该页面会显示有关其组织的信息，包括可与 AWS Command Line Interface结合使用的 ID。页面上的消息还可以显示完成设置和组织所需的任何步骤，例如未经验证的域或缺少用户。这些消息还提供了设置给定电子邮件客户端所遵循的第一步。

查看组织详细信息

1. 在导航栏中，选择组织。

   此时将出现组织页面并显示您的组织。
2. 选择要查看的组织。

集成 WorkSpaces 目录

要将 Amazon WorkMail 与 WorkSpaces 结合使用，请使用以下步骤创建一个兼容目录。

添加兼容的 WorkSpaces 目录

1. 使用 WorkSpaces 创建兼容的目录。有关 Amazon WorkDocs 说明，请参阅《Amazon WorkDocs 管理员指南》中的 Amazon WorkSpaces 快速设置入门。
2. 在 Amazon WorkMail 控制台中，创建 Amazon WorkMail 组织并选择使用现有目录。有关更多信息，请参阅 创建组织。

组织状态和描述

在创建组织之后，它会具有以下状态之一。

状态	描述
活跃	您的组织很正常，可以使用。
Creating	工作流程正在运行以创建您的组织。
失败	无法创建您的组织。
Impaired (受损	您的组织出现故障或检测到问题。
非活动	您的组织处于非活跃状态。
Requested (已请求	您的组织创建请求在队列中，正在等待创建。
正在验证	正在检查组织的所有设置的运行状况。

删除组织

如果您不再希望对组织的电子邮件使用 Amazon WorkMail，可以从 Amazon WorkMail 中删除组织。

> **Note**
>
> 此操作无法撤消。删除组织后，您将无法恢复邮箱数据。

删除组织

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在组织屏幕上的组织列表中，选择要删除的组织，然后选择删除。
3. 对于删除组织，选择是删除还是保留现有用户目录，然后输入组织的名称。
4. 选择删除组织。

> **Note**
>
> 如果您没有为 Amazon WorkMail 提供自己的目录，我们会为您创建目录。如果您在删除组织时保留此现有目录，则除非 Amazon WorkMail、WorkDocs 或 WorkSpaces 正在使用该目录，否则您需要为此付费。有关定价信息，请参阅其他目录类型定价。
> 如要删除目录，则该目录不能包含已启用的任何其他 AWS 应用程序。有关更多信息，请参阅《AWS Directory Service 管理指南》中的删除 Simple AD 目录或删除 AD Connector 目录。

当您尝试删除组织时，您可能会收到无效的 Amazon Simple Email Service (Amazon SES) 规则集集错误消息。如果您收到此错误，请在 Amazon SES 控制台中编辑 Amazon SES 规则并删除无效的规则集。您编辑的规则应在规则名称中包含 Amazon WorkMail 组织 ID。有关更多信息，请参阅《Amazon Simple Email Service 开发人员指南》中的创建接收规则。

如果您需要确定哪个规则集置无效，请先保存规则。此时将为规则集显示错误消息。

查找电子邮件地址

您可以按用户、资源或组查找您的组织中是否使用了某个电子邮件地址。

查找电子邮件地址

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择组织的名称。
3. 在组织页面中，选择查找电子邮件地址。
4. 选择搜索。

使用组织设置

以下部分说明如何使用可用于 Amazon WorkMail 组织的设置。您选择的设置将应用于整个组织。

主题

- 启用邮箱迁移
- 启用日志

- 启用互操作性
- 启用 SMTP 网关
- 管理电子邮件流
- 对传入电子邮件执行 DMARC 策略

启用邮箱迁移

当您想将邮箱从源（如 Microsoft Exchange 或 G Suite Basic）传输到 Amazon WorkMail 时，可以启用邮箱迁移。您可以将迁移作为更大规模迁移过程的一部分来启用。有关更多信息（包括操作步骤），请参阅本指南“入门”部分中的迁移到 Amazon WorkMail。

启用日志

您可以启用日志来记录电子邮件通信。使用日志时，通常使用集成式第三方存档和电子数据展示工具。日志有助于确保您满足数据存储、隐私保护和信息保护的合规性法规。

有关更多信息（包括操作步骤），请参阅本指南“入门”部分中的在 Amazon WorkMail 中使用电子邮件日志。

启用互操作性

互操作性允许您从 Microsoft Exchange 迁移，并将 Amazon WorkMail 用作一部分企业邮箱。有关更多信息（包括操作步骤），请参阅本指南“入门”部分中的在 Amazon WorkMail 上配置可用性设置。

启用 SMTP 网关

您可以启用简单邮件传输协议 (SMTP) 网关以与出站电子邮件流规则结合使用。出站电子邮件流规则可让您通过 SMTP 网关路由从您的 Amazon WorkMail 组织发送的电子邮件。有关更多信息，请参阅 出站电子邮件规则操作。

> **Note**
>
> 为出站电子邮件流规则配置的 SMTP 网关必须使用主要证书颁发机构颁发的证书支持传输层安全性协议 (TLS) 1.2 版。只支持基本身份验证。

配置 SMTP 网关

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

2. 在导航窗格中，选择组织，然后选择组织的名称。
3. 在导航面板中选择组织设置。

   此时将出现组织设置页面并显示一组选项卡。
4. 选择 SMTP 网关选项卡，然后选择创建网关。
5. 输入以下信息：

   - 网关名称：输入唯一名称。
   - 网关地址：输入网关的主机名或 IP 地址。
   - 端口号：输入网关的端口号。
   - 用户名：输入用户名。
   - 密码：输入强密码。
6. 选择创建。

   SMTP 网关可与出站电子邮件流规则结合使用。

将 SMTP 网关配置为与出站邮件流规则一起使用时，出站邮件会尝试将该规则与 SMTP 网关相匹配。与该规则匹配的邮件将路由到相应的 SMTP 网关，然后由该网关处理电子邮件传送的其余部分。

如果 Amazon WorkMail 无法到达 SMTP 网关，系统会将电子邮件退回给发件人。如果发生这种情况，请按照前面的步骤更正网关设置。

管理电子邮件流

要帮助管理电子邮件，您可以设置电子邮件流规则。电子邮件流规则可以根据电子邮件的地址或域对电子邮件执行一项或多项操作。您可以对发件人和收件人的电子邮件地址或域使用电子邮件流规则。

创建电子邮件流规则时，可以指定在指定的规则模式匹配时应用于电子邮件的规则操作。

主题

- 入站电子邮件规则操作
- 出站电子邮件规则操作
- 发件人和收件人模式
- 创建电子邮件流规则

- 编辑电子邮件流规则
- 为 Amazon WorkMail 配置 AWS Lambda
- 管理对 Amazon WorkMail Message Flow API 的访问
- 测试电子邮件流规则
- 删除电子邮件流规则

入站电子邮件规则操作

入站电子邮件流规则有助于阻止不受欢迎的电子邮件到达用户的邮箱。入站电子邮件流规则（也称为规则操作）会自动应用于发送给 Amazon WorkMail 组织内部任何人的所有电子邮件。这与单个邮箱的电子邮件规则不同。

> **Note**
>
> 或者，您可以将规则与 AWS Lambda 函数结合使用，以便在传入电子邮件传送到用户邮箱之前对其进行处理。有关将 Lambda 与 Amazon WorkMail 结合使用的更多信息，请参阅为 Amazon WorkMail 配置 AWS Lambda。有关 Lambda 的更多信息，请参阅 AWS Lambda 开发人员指南。

入站电子邮件流规则（也称为规则操作）会自动应用于发送给 Amazon WorkMail 组织内部任何人的所有电子邮件。这与单个邮箱的电子邮件规则不同。

以下规则操作定义如何处理入站电子邮件。对于每个规则，指定发件人和收件人模式以及以下操作之一。

操作	描述
删除电子邮件	电子邮件将被忽略。它未送达，并且不会通知发件人未送达。
发送退回邮件响应	电子邮件未送达，并且使用退回邮件来通知发件人未送达。
传送到垃圾邮件文件夹	电子邮件被传送到用户的垃圾邮件文件夹，即使 Amazon WorkMail 垃圾邮件检测系统最初没有将它识别为垃圾邮件也是如此。

操作	描述
默认值	电子邮件在经过 Amazon WorkMail 垃圾邮件检测系统检查后发送。垃圾邮件将被发送到垃圾邮件文件夹。所有其他电子邮件将被发送到收件箱。 将忽略其他具有不太明确的发件人模式的电子邮件流规则。要向基于域的电子邮件流规则添加例外，请使用更明确的发件人模式配置默认操作。有关更多信息，请参阅 发件人和收件人模式。
从不传送到垃圾邮件文件夹	电子邮件始终被发送到用户的收件箱，即使 Amazon WorkMail 垃圾邮件检测系统将它识别为垃圾邮件也是如此。 **Important** 如果不使用默认的垃圾邮件检测系统，则会使用户面临来自您指定的地址的高风险内容。
运行 AWS Lambda	在电子邮件被发送到用户的收件箱之前或期间，可将电子邮件传递到 Lambda 函数以进行处理。

Note

入站电子邮件首先被发送到 Amazon SES，然后被发送到 Amazon WorkMail。如果 Amazon SES 阻止入站电子邮件，则规则操作不适用。例如，Amazon SES 会在检测到已知病毒或由于显式 IP 筛选规则而阻止电子邮件。指定规则操作（例如，Default (默认)、Deliver to junk folder (发送到垃圾邮件文件夹) 或 Never deliver to junk folder (从不发送到垃圾邮件文件夹)）不起作用。

出站电子邮件规则操作

您可以使用出站电子邮件流规则通过 SMTP 网关定向电子邮件，或者阻止发件人将电子邮件发送给指定的收件人。有关 SMTP 网关的更多信息，请参阅启用 SMTP 网关。

您还可以使用出站电子邮件流规则将电子邮件发送到 AWS Lambda 函数，以便在发送电子邮件后进行处理。有关 Lambda 的更多信息，请参阅 AWS Lambda 开发人员指南。

以下规则操作定义如何处理出站电子邮件。对于每个规则，指定发件人和收件人模式以及以下操作之一。

操作	描述
默认值	通过正常流程发送电子邮件。
删除电子邮件	电子邮件将被删除。它未发送，并且不会通知发件人未送达。
发送退回邮件响应	电子邮件未发送，向发件人通知管理员阻止了电子邮件的消息。
路由到 SMTP 网关	通过配置的 SMTP 网关发送电子邮件。
运行 Lambda	在发送电子邮件之前或期间，可将电子邮件发送到 Lambda 函数进行处理。

发件人和收件人模式

电子邮件流规则可应用于特定电子邮件地址，或特定域或一组域之下的所有电子邮件地址。定义模式来确定规则所应用于的电子邮件地址。

发件人和收件人模式都采用以下形式之一：

- 电子邮件地址与单个电子邮件地址匹配；例如：

```
mailbox@example.com
```

- 域名与该域之下的所有电子邮件地址匹配；例如：

```
example.com
```

- 通配符域与该域及其所有子域之下的所有电子邮件地址匹配。通配符只出现在域的前面；例如：

```
*.example.com
```

- 星号与任何域之下的任何电子邮件地址匹配。

```
*
```

> **Note**
>
> + 符号在发件人或收件人模式中无效。

可以为一个规则指定多种模式。有关更多信息，请参阅入站电子邮件规则操作和出站电子邮件规则操作。

如果入站电子邮件中的 Sender 或 From 标头与任何模式匹配，则将应用入站电子邮件流规则。如果匹配，将首先匹配 Sender 地址。如果没有 From 标头或 Sender 标头不与任何规则匹配，则匹配 Sender 地址。如果有多个电子邮件收件人与不同的规则匹配，则每个规则应用于所匹配的收件人。

如果出站电子邮件中的收件人和 Sender 或 From 标头与任何模式匹配，则将应用出站电子邮件流规则。如果有多个电子邮件收件人与不同的规则匹配，则每个规则应用于所匹配的收件人。

如果多个规则匹配，则应用最明确的规则的操作。例如，针对特定电子邮件地址的规则的优先级高于针对整个域的规则。如果多个规则具有相同的明确性，则应用最受限制的操作。例如，Drop 操作优先于 Bounce 操作。操作的优先顺序与它们在入站电子邮件规则操作和出站电子邮件规则操作中列出的顺序相同。

> **Note**
>
> 在创建具有重叠的发件人模式以及 Drop 或 Bounce 操作的规则时，应格外小心。意外的优先顺序可能会导致许多入站电子邮件未送达。

创建电子邮件流规则

电子邮件流规则将规则操作应用于传入和传出电子邮件。当邮件与指定模式匹配时，这些操作将适用。新的电子邮件流规则将立即生效。

创建电子邮件流规则

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择组织的名称。
3. 在导航面板中选择组织设置。

   此时将出现组织设置页面并显示一组选项卡。在此页面中，您可以创建入站或出站规则。以下步骤说明了如何创建这两种规则。

   创建入站规则

   1. 选择入站规则选项卡，然后选择创建。
   2. 在规则名称框中，输入唯一的名称。
   3. 在操作下，打开列表并选择一项操作。列表中的每个项目都包含描述，有些还提供了解更多链接。

      > **Note**
      >
      > 如果您选择运行 Lambda 操作，则会显示其他控件。有关使用这些控件的信息，请参阅下一部分：为 Amazon WorkMail 配置 AWS Lambda。

   4. 在发件人域或地址下，输入要应用规则的发件人域或地址。
   5. 在目标域或地址下，输入目标域和电子邮件地址的任意组合。
   6. 选择创建。

   创建出站规则

   1. 选择出站规则选项卡，然后选择创建。
   2. 在规则名称框中，输入唯一的名称。
   3. 在操作下，打开列表并选择一项操作。列表中的每个项目都包含描述，有些还提供了解更多链接。

> **Note**
>
> 如果您选择运行 Lambda 操作，则会显示其他控件。有关使用这些控件的信息，请参阅下一部分“为 Amazon WorkMail 配置 AWS Lambda”。

4. 在发件人域或地址下，输入有效发件人域和电子邮件地址的任意组合。
5. 在目标域或地址下，输入有效目标域和电子邮件地址的任意组合。
6. 选择创建。

您可以测试您创建的新电子邮件流规则。有关更多信息，请参阅 测试电子邮件流规则。

编辑电子邮件流规则

每当您需要更改电子邮件的一项或多项规则操作时，都可以编辑电子邮件流规则。本部分中的步骤适用于传入和传出电子邮件。

编辑电子邮件流规则

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择组织的名称。
3. 在导航面板中选择组织设置。

   此时将出现组织设置页面并显示一组选项卡。
4. 选择入站规则或出站规则选项卡。
5. 选择要更改的规则旁边的单选按钮，然后选择编辑。
6. 根据需要更改规则中的一项或多项操作，然后选择保存。

为 Amazon WorkMail 配置 AWS Lambda

在入站和出站电子邮件流规则中使用运行 Lambda 操作，以将与规则匹配的电子邮件传递到 AWS Lambda 函数进行处理。

从 Amazon WorkMail 中的运行 Lambda 操作的以下配置中进行选择。

同步运行 Lambda 配置

在发送或传送与流规则匹配的电子邮件之前，会先将此电子邮件传递给 Lambda 函数进行处理。使用此配置修改电子邮件内容。您还可以针对不同的使用案例控制入站或出站电子邮件流。例如，传递到 Lambda 函数的规则可以阻止敏感电子邮件的传送、删除附件或添加免责声明。

异步运行 Lambda 配置

在发送或传送与流规则匹配的电子邮件时，会将此电子邮件传递给 Lambda 函数进行处理。此配置不会影响电子邮件传递，并且用于收集入站或出站电子邮件的指标等任务。

无论您选择同步配置还是异步配置，传递到 Lambda 函数的事件对象都包含入站或出站电子邮件事件的元数据。您还可以使用元数据中的邮件 ID 来访问电子邮件的全部内容。有关更多信息，请参阅 使用 AWS Lambda 检索消息内容。有关电子邮件事件的更多信息，请参阅 Lambda 事件数据。

有关入站和出站电子邮件流规则的更多信息，请参阅管理电子邮件流。有关 Lambda 的更多信息，请参阅 AWS Lambda 开发人员指南。

> **Note**
>
> 目前，Lambda 电子邮件流规则仅引用与所配置的 Amazon WorkMail 组织相同的 AWS 区域和 AWS 账户中的 Lambda 函数。

适用于 Amazon WorkMail 的 AWS Lambda 入门

要开始将 AWS Lambda 与 Amazon WorkMail 结合使用，我们建议您将 WorkMail Hello World Lambda 函数从 AWS Serverless Application Repository 部署到您的账户。该函数具有所有必要的资源及为您配置的权限。有关更多示例，请参阅 GitHub 上的 amazon-workmail-lambda-templates 存储库。

如果您选择创建自己的 Lambda 函数，则必须使用 AWS Command Line Interface (AWS CLI) 配置权限。在以下示例命令中，请执行以下操作：

- 将 `MY_FUNCTION_NAME` 替换为您的 Lambda 函数的名称。
- 将 `REGION` 替换为您的 Amazon WorkMail AWS 区域。可用的 Amazon WorkMail 区域包括 `us-east-1` [美国东部（弗吉尼亚州北部）]、`us-west-2` [美国西部（俄勒冈州）] 和 `eu-west-1` [欧洲地区（爱尔兰）]。
- 将 `AWS_ACCOUNT_ID` 替换为您的 12 位 AWS 账户 ID。

- 将 WORKMAIL_ORGANIZATION_ID 替换为您的 Amazon WorkMail 组织 ID。您可以在组织页面上贵组织对应的卡上找到该 ID。

```
aws --region REGION lambda add-permission --function-name MY_FUNCTION_NAME
--statement-id AllowWorkMail
--action "lambda:InvokeFunction"
--principal workmail.REGION.amazonaws.com
--source-arn
 arn:aws:workmail:REGION:AWS_ACCOUNT_ID:organization/WORKMAIL_ORGANIZATION_ID
```

有关使用 AWS CLI 的更多信息，请参阅 AWS Command Line Interface用户指南。

配置同步运行 Lambda 规则

要配置同步运行 Lambda 规则，请使用运行 Lambda 操作创建电子邮件流规则，然后选中同步运行复选框。有关创建邮件流规则的更多信息，请参阅创建电子邮件流规则。

要完成同步规则的创建操作，请添加 Lambda Amazon 资源名称 (ARN) 并配置以下选项。

Fallback action (回退操作

在 Lambda 函数无法运行时 Amazon WorkMail 应用的操作。如果未设置 allRecipients 标志，则此操作也适用于 Lambda 响应中省略的任何收件人。回退操作不能是另一项 Lambda 操作。

Rule timeout (规则超时) (以分钟为单位)

一个时间段，如果 Amazon WorkMail 无法调用 Lambda 函数，则将在该时间段内重试此函数。在此时间段结束时将应用 Fallback action (回退操作)。

> **Note**
>
> 同步运行 Lambda 规则仅支持 * 目标条件。

Lambda 事件数据

使用以下事件数据触发 Lambda 函数。数据的呈现方式会有所不同，具体取决于用于 Lambda 函数的编程语言。

```
{
    "summaryVersion": "2018-10-10",
    "envelope": {
        "mailFrom" : {
            "address" : "from@example.com"
        },
        "recipients" : [
           { "address" : "recipient1@example.com" },
           { "address" : "recipient2@example.com" }
        ]
    },
    "sender" : {
        "address" :  "sender@example.com"
    },
    "subject" : "Hello From Amazon WorkMail!",
    "messageId": "00000000-0000-0000-0000-000000000000",
    "invocationId": "00000000000000000000000000000000",
    "flowDirection": "INBOUND",
    "truncated": false
}
```

事件 JSON 包含以下数据。

summaryVersion

LambdaEventData 的版本号。仅当您在 LambdaEventData 中进行向后不兼容的更改时，此数据才会更新。

envelope

电子邮件的信封，其中包括以下字段：

mailFrom

From (发件人) 地址，它通常是发送电子邮件的用户的电子邮件地址。如果该用户以其他用户名义或代表其他用户发送电子邮件，则 mailFrom 字段返回代表其发送电子邮件的用户的电子邮件地址，而不是实际发件人的电子邮件地址。

recipients

收件人电子邮件地址的列表。Amazon WorkMail 不区分收件人、抄送或密送。

> **Note**
>
> 对于入站电子邮件流规则，此列表包括您在其中创建规则的 Amazon WorkMail 组织内的所有域中的收件人。Lambda 函数会针对发件人的每个 SMTP 会话进行单独调用，并且收件人字段将列出该 SMTP 对话中的收件人。不包括具有外部域的收件人。

sender

代表其他用户发送电子邮件的用户的电子邮件地址。仅在代表其他用户发送电子邮件时设置此字段。

subject

电子邮件主题行。当它超过 256 个字符限制时将被截断。

messageId

使用 Amazon WorkMail Message Flow SDK 时用于访问电子邮件完整内容的唯一 ID。

invocationId

唯一 Lambda 调用的 ID。当为同一 LambdaEventData 多次调用 Lambda 函数时，此 ID 保持不变。用于检测重试并避免重复。

flowDirection

指示电子邮件流的方向，即 INBOUND (入站) 或 OUTBOUND (出站)。

truncated

适用于负载大小，而不是主题行长度。当为 `true` 时，负载大小超过 128 KB 的上限，因此收件人列表会被截断，以便满足限制。

同步运行 Lambda 响应架构

当包含同步运行 Lambda 操作的电子邮件流规则与入站或出站电子邮件匹配时，Amazon WorkMail 将调用配置的 Lambda 函数并等待响应，然后再对电子邮件执行操作。Lambda 函数根据预定义的架构返回响应，该架构列出了操作、操作类型、适用参数以及操作适用的收件人。

以下示例显示了同步运行 Lambda 响应。响应因用于 Lambda 函数的编程语言而异。

```
{
```

```
    "actions": [
      {
        "action" : {
          "type": "string",
          "parameters": { various }
        },
        "recipients": [list of strings],
        "allRecipients": boolean
      }
    ]
}
```

响应 JSON 包含以下数据。

action

要为收件人执行的操作。

type

操作类型。对于异步运行 Lambda 操作，不会返回操作类型。

入站规则操作类型包括 BOUNCE、DROP、DEFAULT、BYPASS_SPAM_CHECK 和 MOVE_TO_JUNK。有关更多信息，请参阅 入站电子邮件规则操作。

出站规则操作类型包括 BOUNCE、DROP 和 DEFAULT。有关更多信息，请参阅 出站电子邮件规则操作。

parameters

其他操作参数。支持 BOUNCE 操作类型作为具有键 bounceMessage 和值 string 的 JSON 对象。此退回邮件用于创建退回电子邮件。

recipients

应对其执行操作的电子邮件地址的列表。可以向响应添加新的收件人，即使这些新收件人未包含在原始收件人列表中也是如此。如果操作的 allRecipients 为 true，则不需要此字段。

> **Note**
>
> 当为入站电子邮件调用 Lambda 操作时，您只能添加来自贵组织的新收件人。新收件人将作为 BCC (密件抄送) 添加到响应中。

allRecipients

如果为 true，则将操作应用于不受 Lambda 响应中的其他特定操作约束的所有收件人。

同步运行 Lambda 操作限制

当 Amazon WorkMail 调用 Lambda 函数进行同步运行 Lambda 操作时，存在以下限制：

- Lambda 函数必须在 15 秒内进行响应，否则将被视为失败的调用。

> **Note**
>
> 系统将按照您指定的规则超时间隔重试调用。

- Lambda 函数响应的最大允许大小为 256 KB。
- 响应最多可包含 10 个唯一操作。10 个以外的操作将受配置的 Fallback action (回退操作) 的约束。
- 出站 Lambda 函数最多允许 500 个收件人。
- Rule timeout (规则超时) 的最大值为 240 分钟。如果配置的最小值为 0，则在 Amazon WorkMail 应用回退操作之前不进行重试。

同步运行 Lambda 操作失败

如果 Amazon WorkMail 由于错误、无效响应或 Lambda 超时而无法调用您的 Lambda 函数，则 Amazon WorkMail 会以指数回退的方式重试调用，这会降低处理速率，直到规则超时时间完成。然后，Fallback action (回退操作) 将应用于电子邮件的所有收件人。有关更多信息，请参阅 配置同步运行 Lambda 规则。

同步运行 Lambda 响应示例

以下示例演示了常见同步运行 Lambda 响应的结构。

Example ：从电子邮件中删除指定的收件人

以下示例演示了用于从电子邮件中删除收件人的同步运行 Lambda 响应的结构。

```
{
    "actions": [
      {
        "action": {
```

```
          "type": "DEFAULT"
        },
        "allRecipients": true
      },
      {
        "action": {
          "type": "DROP"
        },
        "recipients": [
          "drop-recipient@example.com"
        ]
      }
    ]
}
```

Example ：退回自定义电子邮件

以下示例演示了用于退回自定义电子邮件的同步运行 Lambda 响应的结构。

```
{
    "actions" : [
      {
        "action" : {
          "type": 'BOUNCE',
          "parameters": {
            "bounceMessage" : "Email in breach of company policy."
          }
        },
        "allRecipients": true
      }
    ]
}
```

Example ：将收件人添加到电子邮件

以下示例演示了用于将收件人添加到电子邮件的同步运行 Lambda 响应的结构。这不会更新电子邮件的 To (收件人) 或 CC (抄送) 字段。

```
{
    "actions": [
      {
        "action": {
          "type": "DEFAULT"
```

```
        },
        "recipients": [
          "new-recipient@example.com"
         ]
      },
      {
        "action": {
          "type": "DEFAULT"
        },
        "allRecipients": true
      }
    ]
}
```

有关在为运行 Lambda 操作创建 Lambda 函数时要使用的更多代码示例，请参阅 Amazon WorkMail Lambda 模板。

有关将 Lambda 与 Amazon WorkMail 结合使用的更多信息

您还可以访问触发 Lambda 函数的电子邮件的完整内容。有关更多信息，请参阅 使用 AWS Lambda 检索消息内容。

使用 AWS Lambda 检索消息内容

在配置 AWS Lambda 函数以管理 Amazon WorkMail 的电子邮件流后，您可以访问使用 Lambda 处理的电子邮件的完整内容。有关开始使用适用于 Amazon WorkMail 的 Lambda 的更多信息，请参阅为 Amazon WorkMail 配置 AWS Lambda。

要访问电子邮件的完整内容，请使用 Amazon WorkMail Message Flow API 中的 `GetRawMessageContent` 操作。调用时传递给 Lambda 函数的电子邮件 ID 会向该 API 发送请求。然后，该 API 会使用电子邮件的完整 MIME 内容进行响应。有关更多信息，请参阅《Amazon WorkMail API 参考》中的 Amazon WorkMail 电子邮件流。

以下示例显示了使用 Python 运行时环境的 Lambda 函数如何检索完整的邮件内容。

> **Tip**
>
> 如果您首先将 Amazon WorkMail Hello World Lambda 函数从 AWS Serverless Application Repository 部署到您的账户，则系统会在您的账户中创建一个 Lambda 函数，其中包含所有必要的资源和权限。然后，您可以根据使用案例将业务逻辑添加到 lambda 函数。

```
import boto3
import email
import os

def email_handler(event, context):
    workmail = boto3.client('workmailmessageflow',
 region_name=os.environ["AWS_REGION"])
    msg_id = event['messageId']
    raw_msg = workmail.get_raw_message_content(messageId=msg_id)

    parsed_msg = email.message_from_bytes(raw_msg['messageContent'].read())
    print(parsed_msg)
```

有关针对传输中消息内容的分析方法的更多详细示例，请参阅 GitHub 上的 amazon-workmail-lambda-templates 存储库。

> **Note**
>
> 您只能使用 Amazon WorkMail Message Flow API 访问传输中的电子邮件。您只能在邮件发送或接收后 24 小时内访问。要以编程方式访问用户邮箱中的邮件，请使用 Amazon WorkMail 支持的其他协议之一，例如 IMAP 或 Exchange Web Services (EWS)。

使用 AWS Lambda 更新邮件内容

配置同步 AWS Lambda 函数来管理电子邮件流后，您可以使用 Amazon WorkMail Message Flow API 中的 `PutRawMessageContent` 操作来更新传输中的电子邮件内容。有关开始使用适用于 Amazon WorkMail 的 Lambda 函数的更多信息，请参阅配置同步运行 Lambda 规则。有关该 API 的更多信息，请参阅 PutRawMessageContent。

> **Note**
>
> PutRawMessageContent API 需要 boto3 1.17.8，或者您可以向 Lambda 函数添加层。要下载正确的 boto3 版本，请参阅 GitHub 上的 boto 页面。有关添加层的更多信息，请参阅配置函数以使用层。
> 下面是一个示例层："LayerArn":"arn:aws:lambda:${AWS::Region}:489970191081:layer:WorkMailLambdaLayer:2"。在此示例中，将 ${AWS::Region} 替换为适当的 AWS 区域，如 us-east-1。

> **Tip**
>
> 如果您首先将 Amazon WorkMail Hello World Lambda 函数从 AWS Serverless Application Repository 部署到您的账户，则系统会在您的账户中创建一个具有必要资源和权限的 Lambda 函数。然后，您可以根据使用案例将业务逻辑添加到 lambda 函数。

操作时请记住以下几点：

- 使用 GetRawMessageContent API 检索原始邮件内容。有关更多信息，请参阅 使用 AWS Lambda 检索消息内容。
- 获得原始邮件后，请更改 MIME 内容。完成后，将邮件上传到您账户中的 Amazon Simple Storage Service (Amazon S3) 存储桶。确保 S3 存储桶使用与您的 Amazon WorkMail 操作相同的 AWS 账户，并且它使用与您的 API 调用相同的 AWS 区域。
- 要使 Amazon WorkMail 处理请求，您的 S3 存储桶必须具有正确的策略才能访问 S3 对象。有关更多信息，请参阅 Example S3 policy。
- 使用 PutRawMessageContent 将更新后的邮件内容发送回 Amazon WorkMail。

> **Note**
>
> `PutRawMessageContent` API 可确保更新邮件的 MIME 内容符合 RFC 标准以及 RawMessageContent 数据类型中提及的标准。传入 Amazon WorkMail 组织的电子邮件并不总是符合这些标准，因此 `PutRawMessageContent` API 可能会拒绝它们。在这种情况下，您可以查阅返回的错误消息，了解有关如何解决任何问题的更多信息。

Example S3 策略示例

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "workmail.REGION.amazonaws.com"
```

```
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::My-Test-S3-Bucket/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "Bool": {
                    "aws:SecureTransport": "true"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:workmailmessageflow:us-
east-1:111122223333:message/WORKMAIL_ORGANIZATION_ID/*"
                }
            }
        }
    ]
}
```

以下示例显示了 Lambda 函数如何使用 Python 运行时更新传输中电子邮件的主题。

```
    import boto3
    import os
    import uuid
    import email

    def email_handler(event, context):
        workmail = boto3.client('workmailmessageflow',
 region_name=os.environ["AWS_REGION"])
        s3 = boto3.client('s3', region_name=os.environ["AWS_REGION"])

        msg_id = event['messageId']
        raw_msg = workmail.get_raw_message_content(messageId=msg_id)
        parsed_msg = email.message_from_bytes(raw_msg['messageContent'].read())

        # Updating subject. For more examples, see https://github.com/aws-samples/
amazon-workmail-lambda-templates.
        parsed_msg.replace_header('Subject', "New Subject Updated From Lambda")
```

```
        # Store updated email in S3
        key = str(uuid.uuid4());
        s3.put_object(Body=parsed_msg.as_bytes(), Bucket="amzn-s3-demo-bucket",
Key=key)

        # Update the email in WorkMail
        s3_reference = {
            'bucket': "amzn-s3-demo-bucket",
            'key': key
        }
        content = {
            's3Reference': s3_reference
        }
        workmail.put_raw_message_content(messageId=msg_id, content=content)
```

有关分析传输中邮件的内容的方法的更多示例，请参阅 GitHub 上的 amazon-workmail-lambda-templates 存储库。

管理对 Amazon WorkMail Message Flow API 的访问

使用 AWS Identity and Access Management (IAM) 策略管理对 Amazon WorkMail Message Flow API 的访问。

Amazon WorkMail Message Flow API 适用于单一资源类型，即传输中的电子邮件。每封传输中的电子邮件均具有与之关联的唯一 Amazon 资源名称 (ARN)。

以下示例显示了与传输中的电子邮件关联的 ARN 的语法。

```
arn:aws:workmailmessageflow:region:account:message/organization/context/messageID
```

在上述示例中，可更改的字段如下所示：

- 区域：您的 Amazon WorkMail 组织所在的 AWS 区域。
- 账户：您的 Amazon WorkMail 组织的 AWS 账户 ID。
- 组织：您的 Amazon WorkMail 组织 ID。
- 上下文：指示邮件是发往 (`incoming`) 您的组织，还是从您的组织发出 (`outgoing`)。
- 邮件 ID：作为输入传递给 Lambda 函数的唯一电子邮件 ID。

以下示例包括与传输中的传入电子邮件关联的 ARN 的示例 ID。

```
arn:aws:workmailmessageflow:us-east-1:111122223333:message/m-
n1pq2345678r901st2u3vx45x6789yza/incoming/d1234567-8e90-1f23-456g-hjk7lmnop8q9
```

您可以在 IAM 用户的“Resource”部分中将这些 ARN 用作资源，以管理对传输中 Amazon WorkMail 邮件的访问。

针对 Amazon WorkMail 邮件流访问的示例 IAM 策略

以下示例策略向 IAM 实体授予对您的 AWS 账户中每个 Amazon WorkMail 组织的所有入站和出站邮件的完全读取访问权限。

如果您的 AWS 账户中有多个组织，则还可以将访问权限限制到一个或多个组织。如果某些 Lambda 函数应仅用于特定组织，就可以使用此功能。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource": "arn:aws:workmailmessageflow:us-
east-1:111122223333:message/organization/*",
            "Effect": "Allow"
        }
    ]
}
```

您还可以根据消息是发往 (incoming) 您的组织还是从您的组织发出 (outgoing)，选择授予对消息的访问权限。要执行此操作，请在 ARN 中使用限定词 incoming 或 outgoing。

以下示例策略仅授予对发往您的组织的消息的访问权限。

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource": "arn:aws:workmailmessageflow:us-
east-1:111122223333:message/organization/incoming/*",
            "Effect": "Allow"
        }
    ]
}
```

以下示例策略向 IAM 实体授予对您的 AWS 账户中每个 Amazon WorkMail 组织的所有入站和出站邮件的完全读取和更新访问权限。

测试电子邮件流规则

要检查当前规则配置，您可以测试该配置将对特定电子邮件地址采取什么操作。

测试电子邮件流规则

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，依次选择 Organization settings (组织设置) 和 Inbound/Outbound rules (入站/出站规则)。
4. 在 Test configuration (测试配置) 旁边，输入要测试的发件人和收件人的完整电子邮件地址。
5. 选择测试。将显示要为提供的电子邮件地址采取的操作。

删除电子邮件流规则

在您删除电子邮件流规则后，更改立即应用。

删除电子邮件流规则

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，依次选择 Organization settings (组织设置) 和 Inbound/Outbound rules (入站/出站规则)。
4. 选择规则，然后选择 Remove。
5. 在确认提示符下，选择 Remove (删除)。

对传入电子邮件执行 DMARC 策略

电子邮件域使用域名系统 (DNS) 记录来确保安全。它们可以保护您的用户免受常见的攻击，例如欺骗或网络钓鱼。DNS 记录通常包括基于域的邮件身份验证、报告和一致性 (DMARC) 记录，这些记录由发送电子邮件的域所有者设置。DMARC 记录包括用于指定当电子邮件未通过 DMARC 检查时所要执行的操作的策略。您可以选择是否对发送给您的组织的电子邮件执行 DMARC 策略。

默认情况下，新的 Amazon WorkMail 组织会启用 DMARC 执行。

启用 DMARC 执行

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航面板中选择组织设置。此时将出现组织设置页面并显示一组选项卡。
4. 选择 DMARC 选项卡，然后选择编辑。
5. 将 DMARC 执行滑块移动到“开启”位置。
6. 选中我确认，开启 DMARC 执行可能会导致传入电子邮件被删除或隔离，具体取决于发件人的域配置旁边的复选框。
7. 选择保存。

禁用 DMARC 执行

- 按照上一部分中的步骤操作，但将 DMARC 执行滑块移动到“关闭”位置。

使用电子邮件事件日志记录来跟踪 DMARC 执行

启用 DMARC 执行可能会导致入站电子邮件被删除或标记为垃圾邮件，具体取决于发件人如何配置其域。如果发件人将电子邮件域配置错误，您的用户可能会无法接收合法电子邮件。要检查有没有未发送给用户的电子邮件，您可以为 Amazon WorkMail 组织启用电子邮件事件日志记录。然后，可以对根据发件人的 DMARC 策略筛选出的传入电子邮件查询电子邮件事件日志。

在使用电子邮件事件日志记录跟踪 DMARC 执行之前，请在 Amazon WorkMail 控制台中启用电子邮件事件日志记录。为了充分利用日志数据，请在记录电子邮件事件的同时留出一些时间。有关更多信息和说明，请参阅 the section called “启用电子邮件事件日志记录”。

使用电子邮件事件日志记录跟踪 DMARC 执行

1. 在 CloudWatch Insights 控制台的日志下，选择见解。
2. 对于选择日志组，选择 Amazon WorkMail 组织的日志组。例如，/aws/workmail/events/organization-alias。
3. 选择要查询的时间段。
4. 运行以下查询：stats count() by event.dmarcPolicy | filter event.dmarcVerdict == "FAIL"
5. 选择运行查询。

您还可以为这些事件设置自定义指标。有关更多信息，请参阅创建指标筛选器。

标记组织

通过为 Amazon WorkMail 组织资源添加标签，您可以：

- 区分 AWS 账单与成本管理 控制台中的组织。
- 通过将 Amazon WorkMail 组织资源添加到 AWS Identity and Access Management (IAM) 权限策略语句的 `Resource` 元素，控制对这些资源的访问。

有关 Amazon WorkMail 资源级权限的更多信息，请参阅资源。有关基于标签控制访问的更多信息，请参阅基于 Amazon WorkMail 标签的授权。

Amazon WorkMail 管理员可以使用 Amazon WorkMail 控制台为组织添加标签。

向 Amazon WorkMail 组织添加标签

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 选择标签。
4. 对于 Organization tags (组织标签)，请选择 Add new tag (添加新标签)。
5. 在键中，输入标识标签的名称。
6. （可选）对于 Value (值)，输入标签的值。
7. （可选）重复步骤 4-6 以向组织添加更多标签。最多可以添加 50 个标签。
8. 选择 保存 以保存您的更改。

您可以在 Amazon WorkMail 控制台中查看组织标签。

开发人员还可以使用 AWS 开发工具包或 AWS Command Line Interface (AWS CLI) 标记组织。有关更多信息，请参阅 Amazon WorkMail API 参考或 AWS CLI 命令参考中的 `TagResource`、`ListTagsForResource` 和 `UntagResource` 命令。

您可以随时使用 Amazon WorkMail 控制台从组织中删除标签。

从 Amazon WorkMail 组织中删除标签

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 选择标签。
4. 对于 Organization tags (组织标签)，选择要删除的标签旁边的 Remove (删除)。
5. 选择 Submit (提交) 可保存您的更改。

使用访问控制规则

Amazon WorkMail 的访问控制规则允许管理员控制如何向其组织的用户和模拟角色授予对 Amazon WorkMail 的访问权限。每个 Amazon WorkMail 组织均有一个默认访问控制规则，该规则向添加到组织的所有用户和模拟角色授予邮箱访问权限，不管这些用户使用的访问协议或 IP 地址如何。管理员可以编辑默认规则或将其替换为自己的规则、添加新规则或删除规则。

> **Warning**
>
> 如果管理员删除组织的所有访问控制规则，则 Amazon WorkMail 将阻止对组织邮箱的所有访问。

管理员可以应用将根据以下条件允许或拒绝访问的访问控制规则：

- 协议：用于访问邮箱的协议。示例包括 Autodiscover、EWS、IMAP、SMTP、ActiveSync、Windows 版 Outlook 和 Webmail。
- IP 地址：用于访问邮箱的 IPv4 CIDR 范围。
- Amazon WorkMail 用户：贵组织中用于访问邮箱的用户。
- 模拟角色：贵组织中用于访问邮箱的模拟角色。有关更多信息，请参阅 管理模拟角色。

除了用户的邮箱和文件夹权限之外，管理员还会应用访问控制规则。有关更多信息，请参阅《Amazon WorkMail 用户指南》中的使用邮箱权限和共享文件夹和文件夹权限。

> **Note**
>
> - 启用 Windows 版 Outlook 的访问权限时，建议同时启用 Autodiscover 和 EWS 的访问权限。
> - 访问控制规则不适用于 Amazon WorkMail 控制台或 SDK 访问。请改用 AWS Identity and Access Management (IAM) 角色或策略。有关更多信息，请参阅 适用于 Amazon WorkMail 的 Identity and Access Management。

创建访问控制规则

从 Amazon WorkMail 控制台创建新的访问控制规则。

创建新的访问控制规则

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。

3. 选择 Access control rules (访问控制规则)。
4. 选择创建规则。
5. 对于 Description (描述)，输入规则的描述。
6. 对于 Effect (效果)，选择 Allow (允许) 或 Deny (拒绝)。这将根据您在下一步中选择的条件来允许或拒绝访问。
7. 对于此规则应用于符合以下条件的请求...，选择要应用于规则的条件，例如，包含或排除特定的协议、IP 地址、用户或模拟角色。
8. （可选）如果输入 IP 地址范围、用户或模拟角色，请选择添加以将其添加到规则中。
9. 选择创建规则。

编辑访问控制规则

从 Amazon WorkMail 控制台编辑新的和默认的访问控制规则。

编辑访问控制规则

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 选择 Access control rules (访问控制规则)。
4. 选择要编辑的规则。
5. 选择 Edit rule。
6. 根据需要编辑描述、效果和条件。
7. 选择保存更改。

> **Important**
>
> 更改访问规则时，受影响的邮箱可能需要五分钟才能遵循更新的规则。在此期间，访问受影响邮箱的客户端可能会出现不一致的行为。但是，在测试规则时，您会立即看到正确的行为。有关测试规则的更多信息，请参阅下一部分中的相关步骤。

测试访问控制规则

要了解如何应用组织的访问控制规则，请从 Amazon WorkMail 控制台测试规则。

测试组织的访问控制规则

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 选择 Access control rules (访问控制规则)。
4. 选择 Test rules (测试规则)。
5. 对于 Request context (请求上下文)，选择要测试的协议。
6. 对于 Source IP address (源 IP 地址)，输入要测试的 IP 地址。
7. 对于请求执行者，选择要为其测试的用户或模拟角色。
8. 选择要为其测试的用户或模拟角色。
9. 选择测试。

测试结果将显示在 Effect (效果) 下。

删除访问控制规则

从 Amazon WorkMail 控制台中删除不再需要的访问控制规则。

> **Warning**
>
> 如果管理员删除组织的所有访问控制规则，则 Amazon WorkMail 将阻止对组织邮箱的所有访问。

删除访问控制规则

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 选择 Access control rules (访问控制规则)。
4. 选择要删除的规则。
5. 选择 Delete rule (删除规则)。
6. 选择删除。

设置邮箱保留策略

您可以为 Amazon WorkMail 组织设置邮箱保留策略。保留策略会在您选择的时间段后自动从用户邮箱中删除电子邮件。您可以选择要应用保留策略的邮箱文件夹。此外，还可以选择是否为不同的文件夹设置不同的保留策略。邮箱保留策略应用于您的组织中的所有用户邮箱中的选定文件夹。用户不能覆盖保留策略。

设置邮箱保留策略

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 选择 Retention policy (保留策略)。
4. 对于 Folder actions (文件夹操作)，在要包括在策略中的每个邮箱文件夹旁边，选择 Delete (删除)或 Permanently delete (永久删除)。
5. 输入在删除电子邮件之前将电子邮件保留在每个邮箱文件夹中的天数。
6. 选择保存。

留出 48 小时来为组织应用保留策略。如果选择删除文件夹操作，用户可以从 Amazon WorkMail Web 应用程序和支持的客户端恢复已删除的电子邮件。如果选择永久删除文件夹操作，则电子邮件在删除后将无法恢复。

保留策略保留项目的天数基于项目的创建、修改或移动时间。例如，如果保留策略在一年后删除项目，则该策略将从您创建该项目或上次对该项目采取操作之日起计算保留天数。它不受实施保留策略的日期的影响。

使用域

您可以将 Amazon WorkMail 配置为使用自定义域，也可以将域设为组织的默认域，并启用适用于 Microsoft Outlook 的自动发现。

主题

添加域

您最多可以向 Amazon WorkMail 组织添加 100 个域。在添加新域时，Amazon Simple Email Service (Amazon SES) 发送授权策略会自动添加到域身份策略。这使 Amazon WorkMail 可以访问您的域的所有 Amazon SES 发送操作并允许您将电子邮件重定向到您的域。您也可以将电子邮件重定向到外部域。

> **Note**
>
> 作为最佳实践，您应该为所有域添加 <postmaster@> 和 <abuse@> 的别名。如果您希望组织中的特定用户接收发送到这些别名的邮件，则可以为这些别名创建通讯组。

当您使用自定义域配置 Amazon WorkMail 组织时，请记住有关域的 DNS 记录的以下信息：

- 对于 MX 和自动发现 CNAME 记录，我们建议将生存时间 (TTL) 值设置为 3600。减少 TTL 可确保您的邮件服务器不会在您更新 MX 记录或迁移邮箱后使用过时的或无效的 MX 记录。
- 创建用户和通讯组，然后成功迁移邮箱后，您应更新 MX 记录以开始将电子邮件转发到 Amazon WorkMail。对 DNS 记录的更新可能需要长达 48 小时来处理。

- 某些 DNS 提供商会自动将域名附加到 DNS 记录的末尾。添加已包含域名（如 _amazonses.example.com）的记录可能会导致域名重复（如 _amazonses.example.com.example.com）。要避免记录名称中的域名重复，请在 DNS 记录中的域名结尾添加句点。这向您的 DNS 提供商表明，记录名称是完全限定的，不再相对于域名。它还可防止 DNS 提供商追加其他域名。
- 复制的记录名称包含域名。根据您使用的 DNS 服务，域名可能已添加到域的 DNS 记录中。
- 创建 DNS 记录后，选择 Amazon WorkMail 控制台上的刷新图标可查看验证状态和记录值。有关验证域的更多信息，请参阅验证域。
- 我们建议您将域配置为 `MAIL FROM` 域。要为 iOS 设备启用自动发现，您必须将域配置为 `MAIL FROM` 域。您可以在控制台的提高送达率部分中查看 `MAIL FROM` 域的状态。有关更多信息，请参阅配置自定义 MAIL FROM 域。

添加域

1. 登录到 AWS 管理控制台并打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。
2. 如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
3. 在导航窗格中，选择组织，然后选择要向其添加域的组织的名称。
4. 在导航窗格中，选择域，然后选择添加域。
5. 在添加域屏幕上，输入一个域名。域名只能包含基本拉丁语 (ASCII) 字符。

   > **Note**
   >
   > 如果您有一个托管于 Amazon Route 53 公共托管区的域，则可以从输入域名时显示的下拉菜单中选择该域。

6. 选择添加域。

   此时将出现一个页面，其中列出了新域的 DNS 记录。该页面将记录分为以下几个部分：

   - 域所有权
   - WorkMail 配置
   - 提高了安全性
   - 改进了电子邮件传送

其中每个部分都包含一条或多条 DNS 记录，每条记录都显示一个状态值。以下列表显示了记录及其可用状态值。

TXT 所有权

Verified（已验证）– 记录已解析和验证。

Pending（待处理）– 记录尚未验证。

Failed（已失败）– 无法验证所有权。记录不匹配或无法访问。

MX WorkMail 配置

Verified（已验证）– 记录已解析和验证。

Missing（缺失）– 无法解析记录。

Inconsistent（不一致）– 值与预期记录不匹配。

自动发现

Verified（已验证）– 记录已解析和验证。

Missing（缺失）– 无法解析记录。

Inconsistent（不一致）– 值与预期记录不匹配。

> **Note**
>
> 自动发现验证过程还会检查自动发现设置是否正确。该过程会验证每个阶段的配置设置。验证完成后，状态列中的已验证旁边会显示一个绿色复选标记。您可以将鼠标悬停在已验证上，查看流程验证了哪些阶段。有关自动发现阶段的更多信息，请参阅。启用自动发现以配置端点

DKIM CNAME

Verified（已验证）– 记录已解析和验证。

Pending（待处理）– 记录尚未验证。

Failed（已失败）– 无法验证所有权。记录不匹配或无法访问。

有关更多信息，请参阅《Amazon Simple Email Service 开发人员指南》中的在 Amazon SES 中使用 DKIM 对电子邮件进行身份验证。

SPF TXT

Verified（已验证）– 记录已解析和验证。

Missing（缺失）– 无法解析记录。

Inconsistent（不一致）– 值与预期记录不匹配。

有关 SPF 验证的更多信息，请参阅使用 SPF 对电子邮件进行身份验证。

DMARC TXT

Verified（已验证）– 记录已解析和验证。

Missing（缺失）– 无法解析记录。

Inconsistent（不一致）– 值与预期记录不匹配。

有关 Amazon WorkMail 中 DMARC 记录的更多信息，请参阅《Amazon Simple Email Service 开发人员指南》中的使用 Amazon SES 遵守 DMARC。

TXT MAIL FROM 域

Verified（已验证）– 记录已解析和验证。

Pending（待处理）– 记录尚未验证。

Failed（已失败）– 无法验证所有权。记录不匹配或无法访问。

MX MAIL FROM 域

Verified（已验证）– 记录已解析和验证。

Missing（缺失）– 无法解析记录。

Inconsistent（不一致）– 值与预期记录不匹配。

7. 在下一步中，根据您使用的 DNS 提供商选择适当的操作。

如果您使用 Route 53 域

- 在页面顶部，选择在 Route 53 中更新全部。

如果您使用其他 DNS 提供商

- 复制记录并将其粘贴到您的 DNS 提供商中。您可以批量复制记录，也可以逐一复制记录。要批量复制记录，请选择全部复制。这将创建一个文件区域，您可以将其导入到 DNS 提供商中。要逐一复制记录，请选择记录名称旁边的重叠方块，然后将每条记录粘贴到您的 DNS 提供商中。

8. 选择刷新图标更新每条记录的状态。这将验证域所有权以及使用 Amazon WorkMail 的域配置是否正确。

删除域

当您不再需要域时，可以删除它。但是，您必须先删除使用该域作为其电子邮件地址的所有个人或群组。

删除域

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域名称和端点。

2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在域列表中，选中域名旁边的复选框，然后选择删除。
4. 在删除域对话框中，键入要删除的域的名称，然后选择删除。

选择默认域

您可以将与您的组织关联的域设置为该组织中用户和组的默认域。使一个域成为默认域不会更改现有电子邮件地址。

使一个域成为默认域

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域名称和端点。

2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在域列表中，选中要使用的域名旁边的复选框，然后选择设置为默认域。

验证域

在 Amazon WorkMail 控制台中添加域后，您必须对其进行验证。验证域可确认您拥有该域，并将使用 Amazon WorkMail 作为该域的电子邮件服务。

您可以通过在 DNS 服务中向域添加 TXT 和 MX 记录来验证域。TXT 记录允许您向 DNS 服务添加注释。MX 记录指定了传入邮件服务器。

您可以使用 Amazon SES 控制台创建 TXT 和 MX 记录，然后使用 Amazon WorkMail 控制台将这些记录添加到您的 DNS 服务。执行以下步骤。

创建 TXT 和 MX 记录

1. 打开 Amazon SES 控制台，网址为：https://console.aws.amazon.com/ses/。
2. 在导航窗格中，选择域，然后选择验证新域。

   此时将显示验证新域对话框。
3. 在域框中，输入在添加域部分中创建的域的名称。
4. （可选）如果要使用域名密钥标识的邮件（DKIM），请选中生成 DKIM 设置复选框。
5. 选择验证此域。

   此时控制台将显示 TXT 和 MX 记录的列表。
6. 选择位于 TXT 列表下方的将记录集下载为 CSV链接。

   此时将显示另存为对话框。选择下载位置，然后选择保存。
7. 打开下载的 CSV 文件并复制其所有内容。

创建 TXT 和 MX 记录后，即可将其添加到您的 DNS 提供商。以下步骤将使用 Route 53。如果您使用其他 DNS 提供商，但不知道如何添加记录，请查阅提供程序的文档。

1. 登录 AWS 管理控制台，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择托管区。然后，选中要验证的域旁边的单选按钮。
3. 从您的域的 DNS 记录列表中，选择导入区域文件。
4. 在区域文件下，将复制的记录粘贴到文本框中。文件列表将显示在文本框下方。
5. 向下滚动到列表末尾，然后选择导入。

> **Note**
>
> 最多需要 72 小时才能完成验证过程。

使用您的 DNS 服务验证 TXT 记录和 MX 记录

确认用于验证您拥有该域的 TXT 记录已正确地添加到您的 DNS 服务中。此过程使用 nslookup 工具，目前支持的平台有 Windows 和 Linux。在 Linux 上，您也可以使用 dig。

要使用 nslookup 工具，您必须先查找处理您的域的 DNS 服务器。然后，您可以查询这些服务器以查看 TXT 记录。由于 DNS 服务器包含有关您的域的最新信息，因此您可以向这些服务器查询您的域。此信息可能需要一定的时间才会传播到其他 DNS 服务器。

使用 nslookup 验证您的 TXT 记录是否已添加到 DNS 服务

1. 查找域的名称服务器：

   a. 打开命令提示符 (Windows) 或终端 (Linux)。

   b. 运行以下命令以列出所有处理您的域的名称服务器。将 *example.com* 替换为您的域。

   ```
   nslookup -type=NS example.com
   ```

   您将在下一步中查询其中一个名称服务器。

2. 验证是否已正确添加 Amazon WorkMail TXT 记录。

   a. 运行以下命令，将 *example.com* 替换为您的域，并将 *ns1.name-server.net* 替换为第 1 步中的名称服务器。

   ```
   nslookup -type=TXT _amazonses.example.com ns1.name-server.net
   ```

b. 查看 nslookup 的输出中显示的 "text =" 字符串。确认此字符串与 Amazon WorkMail 控制台的已验证发件人列表中您的域的 TXT 值相匹配。

在以下示例中，您想查看值为 fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk= 的 _amazonses.example.com 的 TXT 记录。如果您已正确更新记录，该命令将具有以下输出：

```
_amazonses.example.com text = "fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk="
```

使用 dig 验证您的 TXT 记录是否已添加到 DNS 服务

1. 打开终端会话。
2. 运行以下命令以列出您的域的 TXT 记录。将 *example.com* 替换为您的域。

```
dig +short example.com txt
```

3. 在命令的输出中，验证 TXT 后的字符串是否与您在 Amazon WorkMail 控制台的已验证发件人列表中选择域时看到的 TXT 值相匹配。

使用 nslookup 来验证您的 MX 记录已添加到您的 DNS 服务

1. 查找您的域的名称服务器：

a. 打开命令提示符。

b. 运行以下命令以列出您的域的所有名称服务器。

```
nslookup -type=NS example.com
```

您将在下一步中查询其中一个名称服务器。

2. 验证已正确添加 MX 记录：

a. 运行以下命令，将 *example.com* 替换为您的域，并将 *ns1.name-server.net* 替换为您在上一步中标识的名称服务器之一。

```
nslookup -type=MX example.com ns1.name-server.net
```

b. 在命令输出中，验证 mail exchange = 后的字符串是否与以下值之一匹配：

美国东部（弗吉尼亚州北部）区域 – 10 inbound-smtp.us-east-1.amazonaws.com

美国西部（俄勒冈州）区域 – 10 inbound-smtp.us-west-2.amazonaws.com

欧洲地区（爱尔兰）区域 – 10 inbound-smtp.eu-west-1.amazonaws.com

> **Note**
>
> 10 代表 MX 首选项的数量或优先级。

使用 dig 验证您的 MX 记录已添加到 DNS 服务

1. 打开终端会话。
2. 运行以下命令以列出您的域的 MX 记录。

```
dig +short example.com mx
```

3. 验证 MX 后的字符串是否与以下值之一匹配：

   美国东部（弗吉尼亚州北部）区域 – 10 inbound-smtp.us-east-1.amazonaws.com

   美国西部（俄勒冈州）区域 – 10 inbound-smtp.us-west-2.amazonaws.com

   欧洲地区（爱尔兰）区域 – 10 inbound-smtp.eu-west-1.amazonaws.com

   > **Note**
   >
   > 10 代表 MX 首选项的数量或优先级。

域验证故障排除

要排查域验证的常见问题，请参阅以下建议：

您的 DNS 服务不允许在 TXT 记录名称中使用下划线。

从 TXT 记录名称中省略 _amazonses。

您想要多次验证同一个域，但不能有多个具有相同名称的 TXT 记录

如果您的 DNS 服务不允许您拥有多个具有相同名称的 TXT 记录，请使用以下解决方法之一：

- （推荐）如果 DNS 服务允许，请为 TXT 记录分配多个值。例如，如果您的 DNS 由 Amazon Route 53 管理，您可以为同一 TXT 记录设置多个值，如下所示：
  1. 在 Route 53 控制台中，选择您在验证第一个区域中的域时添加的 _amazonses TXT 记录。
  2. 对于值，在第一个值之后按 Enter。
  3. 添加附加区域的值，然后保存记录集。
- 如果您只需要验证两次域，则可以通过创建名称中含 _amazonses 的 TXT 记录来验证一次，然后创建另一条记录名称中不含 _amazonses 的记录来验证一次。

Amazon WorkMail 控制台报告域验证失败

Amazon WorkMail 找不到您的 DNS 服务所需的 TXT 记录。按照使用您的 DNS 服务验证 TXT 记录和 MX 记录中的过程，验证所需的 TXT 记录是否已正确添加到您的 DNS 服务。

您的 DNS 提供商已将域名附加到 TXT 记录的末尾。

添加已包含域名（如 _amazonses.example.com）的记录可能会导致域名重复（如 _amazonses.example.com.example.com）。要避免记录名称中的域名重复，请在 TXT 记录中的域名结尾添加句点。这向您的 DNS 提供商表明，该记录名称是完全限定的，并且已将该域名包含在 TXT 记录中。

Amazon WorkMail 报告 MX 记录不一致

从现有邮件服务器迁移时，MX 记录可能会返回不一致的状态。更新您的 MX 记录以指向 Amazon WorkMail，而不是指向您以前的邮件服务器。当第三方电子邮件代理与 Amazon WorkMail 一起使用时，MX 记录也会返回为不一致。如果是这种情况，您可以安全地忽略不一致警告。

启用自动发现以配置端点

利用自动发现，您可以通过仅使用电子邮件地址和密码来配置 Microsoft Outlook 和移动客户端。该服务还保持与 Amazon WorkMail 的连接，并在端点或设置发生更改时更新本地设置。此外，自动发现使您的客户端能够使用额外的 Amazon WorkMail 功能，如离线通讯簿、外出助手以及查看日历中的忙/闲时间的功能。

客户端执行以下自动发现阶段来检测服务器端点 URL：

- t第 1 阶段 – 客户端对本地 Active Directory 执行安全复制协议 (SCP) 查找。如果您的客户端未加入域，则自动发现会跳过此步骤。
- 第 2 阶段 – 客户端将请求发送到以下 URL 并验证结果。只能通过 HTTPS 使用这些端点。

- https://*company.tld*/autodiscover/autodiscover.xml
- https://autodiscover.*company.tld*/autodiscover/autodiscover.xml

- 第 3 阶段 – 客户端对 autodiscover.company.tld 执行 DNS 查找并从用户的电子邮件地址向派生的端点发送未经身份验证的 GET 请求。如果服务器返回 302 重定向，则客户端会对返回的 HTTPS 端点重新发送自动发现请求。

如果所有这些阶段都失败，则无法自动配置客户端。有关手动配置移动设备的信息，请参阅手动连接您的设备。

当您将域添加到 Amazon WorkMail 时，系统会提示您将自动发现 DNS 记录添加到您的提供程序。这使客户端能够执行自动发现过程的第 3 阶段。但是，这些步骤并非适用于所有移动设备，如现有的 Android 电子邮件应用程序。因此，您可能需要手动设置自动发现阶段 2。

您可以使用以下方法为域设置自动发现阶段 2：

（推荐）使用 Route 53 和 Amazon CloudFront

> **Note**
>
> 以下步骤说明如何为 https://autodiscover.*company.tld*/autodiscover/autodiscover.xml 创建代理。要为 https://*company.tld*/autodiscover/autodiscover.xml 创建代理，请通过以下步骤从域中删除 `autodiscover.` 前缀。
> 使用 CloudFront 和 Route 53 可能会产生费用。有关定价的更多信息，请参阅 Amazon CloudFront 定价和 Amazon Route 53 定价。

使用 Route 53 和 CloudFront 启用自动发现阶段 2

1. 获取 autodiscover.*company.tld* 的 SSL 证书并将其上传到 AWS Identity and Access Management (IAM) 或 AWS Certificate Manager。有关更多信息，请参阅《IAM 用户指南》中的使用服务器证书或《AWS Certificate Manager 用户指南》中的入门。
2. 创建新的 CloudFront 分配：
    1. 通过 https://console.aws.amazon.com/cloudfront/v4/home 打开 CloudFront 控制台
    2. 在导航窗格中，选择分配。
    3. 选择 Create Distribution（创建分配）。
    4. 在 Web 下，选择开始使用。

5. 在源设置中，输入以下值：
   - 源域名 – 为您的区域输入相应的域名：
     - 美国东部（弗吉尼亚北部）– **autodiscover-service.mail.us-east-1.awsapps.com**
     - 美国西部（俄勒冈）– **autodiscover-service.mail.us-west-2.awsapps.com**
     - 欧洲地区（爱尔兰）– **autodiscover-service.mail.eu-west-1.awsapps.com**
   - 源协议策略 – 所需的策略：**Match Viewer**

     > **Note**
     >
     > 将源路径留空。请勿更改源 ID 的自动填充值。

6. 在默认缓存行为设置中，为列出的设置选择以下值：
   - Viewer Protocol Policy：HTTPS Only
   - Allowed HTTP Methods：GET、HEAD、OPTIONS、PUT、POST、PATCH、DELETE
   - Cache Based on Selected Request Headers (基于选择的请求标头进行缓存)：全部
   - Forward Cookies：All
   - Query String Forwarding and Caching (查询字符串转发和缓存)：无 (改进缓存)
   - Smooth Streaming：No
   - Restrict Viewer Access：No
7. 为 Distribution Settings (分配设置) 选择以下值：
   - Price Class：Use only US, Canada, and Europe
   - 对于备用域名 (CNAME)，输入 **autodiscover.*company.tld*** 或 ***company.tld***，其中 *company.tld* 是您的域名。
   - SSL 证书：自定义 SSL 证书（存储在 IAM 中）
   - Custom SSL Client Support (自定义 SSL 客户端支持)：选择 All Clients (所有客户端) 或 Only Clients that Support Server Name Indication (SNI) (仅支持服务器名称指示 (SNI) 的客户端)。较旧版本的 Android 可能无法使用后一个选项。

> **Note**
>
> 如果您选择 All Clients (所有客户端)，请将 Default Root Object (默认根对象) 设置为空。

- Logging (日志记录)：选择 On (开启) 或 Off (关闭)。开启表示启用日志记录。
- 对于 Comment (注释)，输入 **`AutoDiscover type2 for autodiscover.`*`company.tld`***
- 分配状态：选择已启用。

8. 选择 Create Distribution（创建分配）。

3. 在 Route 53 控制台中，创建一个记录以将发送到您的域名的 Internet 流量路由到您的 CloudFront 分配：

> **Note**
>
> 这些步骤假定 example.com 的 DNS 记录托管在 Route 53 中。如果您不使用 Route 53，请按照 DNS 提供商的管理控制台中的步骤进行操作。

1. 在控制台的导航窗格中，选择托管区，然后选择一个域。
2. 在域列表中，选择要使用的域名。
3. 在记录中，选择创建记录。
4. 在快速创建记录下，设置以下参数：
   - 在记录名称下，为记录输入名称。
   - 在路由策略下，选择简单路由。
   - 选择别名滑块将其打开。处于开启状态时，滑块会变为蓝色。
   - 在记录类型列表中，选择 A – 将流量路由到 IPv4 地址和部分 AWS 资源。
   - 在流量路由至列表中，选择 CloudFront 分配的别名。
   - 此时流量路由至列表下方将出现一个搜索框。在文本框中输入 CloudFront 分配的名称。您也可以从选择搜索框时显示的列表中选择您的分配。
5. 选择创建记录。

使用 Apache Web 服务器

以下步骤说明如何使用 Apache Web 服务器为 https://autodiscover.*company.tld*/autodiscover/autodiscover.xml 创建代理。要为 https://*company.tld*/autodiscover/autodiscover.xml 创建代理，请通过以下步骤 从域中删除“autodiscover.”前缀。

利用 Apache Web 服务器启用自动发现第 2 阶段

1. 在启用了 SSL 的 Apache 服务器上运行以下指令：

```
SSLProxyEngine on ProxyPass /autodiscover/autodiscover.xml https://autodiscover-
service.mail.REGION.awsapps.com/autodiscover/autodiscover.xml
```

2. 根据需要，启用以下 Apache 模块。如果您不了解如何操作，请参阅 Apache 帮助：

   - `proxy`
   - `proxy_http`
   - `socache_shmcb`
   - `ssl`

有关自动发现测试和问题排查的信息，请参阅以下部分。

自动发现第 2 阶段问题排查

为自动发现配置 DNS 提供商后，您即可测试自动发现端点配置。如果您已正确配置端点，它会使用未经授权的请求消息进行响应。

提出基本的未经授权的请求

1. 在终端中，创建一个对自动发现端点的未经身份验证的 POST 请求。

```
$ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
autodiscover.xml
```

   如果您的端点配置正确，它应返回 `401 unauthorized` 消息，如以下示例所示：

```
$ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
autodiscover.xml
...
```

```
HTTP/1.1 401 Unauthorized
```

2. 接下来，测试实际的自动发现请求。创建包含以下 XML 内容的 `request.xml` 文件：

```
<?xml version="1.0" encoding="utf-8"?>

<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
requestschema/2006">
    <Request>
        <EMailAddress>testuser@company.tld</EMailAddress>
        <AcceptableResponseSchema>
            http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
responseschema/2006
        </AcceptableResponseSchema>
    </Request>
</Autodiscover>
```

3. 使用您创建的 `request.xml` 文件，并向端点发出经过身份验证的自动发现请求。请记住将 *`testuser@company.tld`* 替换为有效的电子邮件地址：

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml
```

如果端点配置正确，则响应将类似于以下示例：

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml

Enter host password for user 'testuser@company.tld':
<?xml version="1.0" encoding="UTF-8"?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/
responseschema/2006" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Response xmlns="http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
responseschema/2006">
    <Culture>en:us</Culture>
    <User>
        <DisplayName>User1</DisplayName>
        <EMailAddress>testuser@company.tld</EMailAddress>
    </User>
    <Action>
        <Settings>
```

```
            <Server>
                <Type>MobileSync</Type>
                <Url>https://mobile.mail.us-east-1.awsapps.com/Microsoft-Server-
ActiveSync</Url>
                <Name>https://mobile.mail.us-east-1.awsapps.com/Microsoft-Server-
ActiveSync</Name>
            </Server>
        </Settings>
    </Action>
</Response>
```

编辑域身份策略

域身份策略为电子邮件操作（如重定向电子邮件）指定权限。例如，您可以将电子邮件重定向到 Amazon WorkMail 组织中的任何电子邮件地址。

> **Note**
>
> 自 2022 年 4 月 1 日起，Amazon WorkMail 开始使用服务主体而不是 AWS 账户主体进行授权。如果您在 2022 年 4 月 1 日之前添加了域，则可能有一个使用 AWS 账户主体进行授权的旧策略。如果是，我们建议您更新到最新策略。本部分中的相关步骤将说明如何操作。更新期间，您的组织将继续正常发送电子邮件。

只有在不使用自定义 Amazon SES 策略的情况下，才可以按照这些步骤操作。如果您使用自定义 Amazon SES 策略，则必须自行进行相关更新。有关更多信息，请参阅本主题后面的自定义 Amazon SES 服务主体策略。

> **Important**
>
> 不要删除您的现有域。如果您这样做，将会中断邮件服务。您只需重新输入现有域。

更新域身份策略

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。为此，请打开位于搜索框右侧的选择区域列表，然后选择所需的区域。有关区域的更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在左侧导航窗格中，选择域。
4. 突出显示并复制要重新输入的域的名称，然后选择添加域。

   此时将显示添加域对话框。
5. 将复制的名称粘贴到域名框中，然后选择添加域。
6. 对组织中的其余域重复第 3 步至第 5 步。

自定义 Amazon SES 服务主体策略

如果您使用自定义 Amazon SES 策略，请调整此示例以在您的域中使用。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AuthorizeWorkMail",
            "Effect": "Allow",
            "Principal": {
                "Service": "workmail.REGION.amazonaws.com"
            },
            "Action": [
                "ses:*"
            ],
            "Resource": "arn:aws:ses:us-east-1:111122223333:identity/WORKMAIL-
DOMAIN-NAME",
            "Condition": {
                "ArnEquals": {
                    "aws:SourceArn": "arn:aws:workmail:us-
east-1:111122223333:organization/WORKMAIL_ORGANIZATION_ID"
                }
            }
        }
    ]
}
```

使用 SPF 对电子邮件进行身份验证

发件人策略框架 (SPF) 是一种电子邮件验证标准，旨在打击电子邮件欺骗。欺诈是指使恶意行为者发送的电子邮件看起来像合法用户发送的电子邮件的行为。有关为启用了 Amazon WorkMail 的域配置 SPF 的信息，请参阅在 Amazon SES 中使用 SPF 对电子邮件进行身份验证.

配置自定义 MAIL FROM 域

默认情况下，Amazon WorkMail 使用 amazonses.com 的子域作为传出电子邮件的 `MAIL FROM` 域。如果您的域上的 DMARC 策略仅针对 SPF 设置，这可能会导致传送失败。要解决此问题，请将您自己的域配置为 `MAIL FROM` 域。要了解如何将电子邮件域设置为 `MAIL FROM` 域，请参阅《Amazon Simple Email Service 开发人员指南》中的设置自定义 MAIL FROM 域。

> **Important**
>
> 针对 iOS 设备启用自动发现时，需要自定义 MAIL FROM 域。

有关自定义 `MAIL FROM` 域的更多信息，请参阅 Amazon SES 现支持自定义 MAIL FROM 域。

使用用户

您可以从 Amazon WorkMail 中创建和删除用户。此外，您还可以重置用户的电子邮件密码、管理其邮箱配额和设备访问权限，以及控制其邮箱权限。

主题

查看用户列表

查看用户列表

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择 Users（用户）。
4. 此外，还可以按用户名、显示名称或主要电子邮件地址筛选用户。

> **Note**
>
> 搜索区分大小写。

添加用户

当您添加用户时，Amazon WorkMail 会自动为他们创建邮箱。用户可以从 Amazon WorkMail Web 应用程序、移动设备或者使用 macOS 或 PC 上的 Microsoft Outlook 登录和访问其邮件。

如何添加用户

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择要向其添加用户的组织。
3. 在导航窗格中，选择用户，然后选择添加用户。

   将出现添加用户屏幕。
4. 在用户详细信息下的用户名字段中，输入用户的名称。该名称还会显示在电子邮件地址框中。如果您希望用户的电子邮件地址与其用户名不同，则可以编辑电子邮件地址字段。
5. （可选）在名字和姓氏框中输入用户的名字和姓氏。
6. 在显示名称框中，输入用户的显示名称。
7. 在电子邮件地址框中，接受电子邮件别名或输入其他别名。
8. 默认情况下，用户显示在全球地址列表中。要在全球地址列表中隐藏用户，请清除在全球地址列表中显示复选框。
9. 选择不创建邮箱，以将用户作为远程用户添加到组织。
10. 在密码设置下，在密码和重复密码框中输入用户的密码。
11. 选择添加用户。

启用用户

当您将 Amazon WorkMail 与贵公司的 Active Directory 集成时，或者您的 Simple AD 目录中已有可用的用户时，可以在 Amazon WorkMail 中启用这些用户。您还可以按照以下步骤重新启用其账户被禁用的用户。

启用用户

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

2. 在导航窗格中，选择组织，然后选择要为其启用用户的组织。
3. 在导航窗格中，选择 Users（用户）。

   将显示用户列表。处于启用、禁用和系统用户状态的用户账户显示在该列表中。
4. 从已禁用账户的用户列表中，选中要启用的用户对应的复选框，然后选择启用。

   此时将显示启用用户对话框。
5. 根据需要，查看并更改每个用户的主电子邮件地址，然后选择启用。

管理用户别名

您可以为用户添加或移除电子邮件别名。

向用户添加电子邮件别名

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择要为其添加用户的组织的名称。
3. 在导航窗格中，选择用户，然后选择要向其添加别名的用户的名称。
4. 在用户详细信息部分，选择别名选项卡。
5. 在别名选项卡下，选择添加别名。
6. 在别名框中，输入别名。
7. 为别名选择一个域。
8. 选择添加。

从用户移除电子邮件别名。

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

2. 在导航窗格中，选择组织，然后选择要从中移除用户的组织的名称。
3. 在导航窗格中，选择用户，然后选择要从中移除别名的用户的名称。
4. 在用户详细信息部分，选择别名选项卡。
5. 在别名选项卡下，选中要移除的别名对应的复选框。
6. 验证要移除的别名。
7. 在移除别名窗口中，选择移除。

禁用用户

您可以随时禁用组织中的任何用户。当您禁用某个用户时，该用户会立即变得无法访问。禁用时间超过 30 天的用户将从 Amazon WorkMail 中删除其收件箱。

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择包含要禁用的用户的组织。
3. 在导航窗格中，选择 Users（用户）。

   此时将出现所有用户的列表，其中显示处于启用、禁用和系统用户状态的账户。
4. 从已启用用户的列表中，选中要禁用的账户对应的复选框，然后选择禁用。

   此时将显示禁用用户对话框。
5. 选择 禁用。

编辑用户详细信息

编辑用户详细信息时，您可以更改以下内容：

- 个人数据：姓名、电子邮件地址、电话号码和其他个人详细信息。
- 邮箱配额（大小）：配额范围可以从 1 MB 到 51,200 MB（50 GB）不等。Amazon WorkMail 会在用户达到配额的 90% 时通知用户。此外，更改用户的邮箱配额不会影响定价。有关定价的更多信息，请参阅 Amazon WorkMail 定价。
- 移动设备访问权限：删除和擦除设备，以及查看设备详细信息。
- 邮箱访问权限：授予用户使用邮箱的权限，并向用户授予不同级别的邮箱访问权限。

- 个人访问令牌（IAM Identity Center 已启用时）：查看和删除个人访问令牌。

> **Note**
>
> 如果您将 Amazon WorkMail 与 AD Connector 目录集成，则无法从 AWS 管理控制台 编辑这些详细信息。您必须使用 Active Directory 管理工具编辑它们。当您的组织处于互操作模式时，将适用这些限制。有关更多信息，请参阅 互操作模式中的限制。

编辑用户详细信息

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择要使用的组织。
3. 在导航窗格中，选择用户，然后选择要编辑的用户的名称。

编辑个人数据

1. 在详细信息部分中，选择编辑。
2. 在用户详细信息下，根据需要输入或更改用户的个人信息。
3. 完成后，选择保存更改。

与 IAM Identity Center 用户关联

1. 在用户详细信息下，选择编辑。
2. 输入您要关联的 IAM Identity Center 用户的用户 ID。您可以在 IAM Identity Center 页面或 IAM Identity Center 控制台的分配的用户表下查看此信息。
3. 选择保存更改。

编辑邮箱配额

1. 在用户详细信息下，选择配额选项卡，然后选择编辑。
2. 在更新邮箱配额框中，输入邮箱的大小。您可以输入介于 **1** 到 **51200** 之间的值。

3. 选择保存更改。

管理移动设备数据

> **Note**
>
> 要管理移动设备，您的用户首先需要将其设备连接到您的 Amazon WorkMail 实例。有关连接移动设备的信息，请参阅为 Amazon WorkMail 设置移动设备客户端。

1. 在用户详细信息下，选择移动设备选项卡。
2. 要查看当前的设备列表，请选择刷新。
3. 要查看设备的详细信息，请从设备 ID 列中选择设备名称。
4. 要删除或擦除设备，请选择设备名称旁边的单选按钮，然后根据需要选择删除或擦除。
5. 在随后显示的对话框中，确认删除或擦除操作。请记住，当用户再次将其设备与 Amazon WorkMail 同步时，他们会重新出现。

编辑邮箱权限

1. 选择 Permissions（权限）选项卡。
2. 请执行下列操作之一：

    1. 要添加权限，请选择添加权限。打开添加新权限列表并选择用户或组，选择该用户或组的权限设置，然后选择保存。
    2. 要编辑用户权限，请选择用户名旁边的按钮。选择编辑，选择所需的选项，然后选择保存。

    有关权限选项的更多信息，请参阅使用邮箱权限。
3. 要删除所有权限，请选择删除，然后确认删除。

删除个人访问令牌

> **Note**
>
> 确保任何电子邮件客户端都没有正在使用您要删除的令牌。在令牌被使用时将其删除，将导致使用该令牌的客户端身份验证中断。

1. 选择个人访问令牌选项卡。
2. 从个人访问令牌列表中，选择要删除的个人访问令牌。
3. 选择删除令牌。
4. 在确认文本框中输入类型。

重置用户密码

如果用户忘记密码或在登录 Amazon WorkMail 时遇到问题，您可以为其重置密码。

> **Note**
>
> - 如果您已将 Amazon WorkMail 与 AD Connector 目录集成，则必须在 Active Directory 中重置用户密码。
> - 如果您已将 Amazon WorkMail 与 IAM Identity Center 集成，则可以选择重置用户密码。有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的重置最终用户的 IAM Identity Center 用户密码。

重置用户密码

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择 Users（用户）。
4. 在用户列表中，选中用户名旁边的复选框，然后选择重置密码。
5. 在重置密码对话框中，键入新密码，然后选择重置。

Amazon WorkMail 密码策略问题排查

如果重置密码未成功，请验证新密码是否符合密码策略要求。

密码策略要求取决于您的 Amazon WorkMail 组织使用的目录类型。

Amazon WorkMail 目录和 Simple AD 目录密码策略

默认情况下，Amazon WorkMail 目录或 Simple AD 目录的密码必须：

- 非空
- 至少 8 个字符
- 不超过 64 个字符
- 由基本拉丁字符或 Latin-1 增补字符组成

密码必须包含以下 5 组字符中的 3 组字符：

- 大写字符
- 小写字符
- 数字（0 到 9）
- 特殊字符（例如，<、~ 或 !）
- Latin-1 增补字符（例如，é、ü 或 ñ）

Amazon WorkMail 目录密码策略不能更改。

要更改 Simple AD 密码策略，请在 Simple AD 目录的 Amazon Elastic Compute Cloud (Amazon EC2) Windows 实例上使用 AD 管理工具。有关更多信息，请参阅《AWS Directory Service 管理指南》中的安装 Active Directory 管理工具。

AWS Managed Microsoft AD Directory 密码策略

有关 AWS Managed Microsoft AD 目录的默认密码策略的信息，请参阅《AWS Directory Service 管理指南》中的管理 AWS Managed Microsoft AD 的密码策略。

AD Connector 密码策略

AD Connector 将使用它连接到的 Active Directory 域的密码策略。有关密码策略设置的更多信息，请参阅 Active Directory 域的文档。

使用通知

借助 Amazon WorkMail Push Notifications API，您可以接收有关您的邮箱中的更改的推送通知，包括新电子邮件和日历更新。您必须注册 URL（或推送通知响应程序）才能接收通知。借助此功能，开发

人员可以为 Amazon WorkMail 用户创建快速响应应用程序，以便快速向应用程序通知用户邮箱中的更改。

有关更多信息，请参阅 Exchange 中的通知订阅、邮箱事件和 EWS。

您可以订阅特定文件夹（如“收件箱”或“日历”），也可以订阅邮箱更改事件的所有文件夹（包括“新建邮件”、“已创建”和“已修改”）。

可以使用客户端库（如 EWS Java API 或托管式 EWS C# API）来访问此功能。AWS GitHub 页面上提供了使用 AWS Lambda 和 API Gateway（使用 AWS Serverless 框架）开发的完整推送响应程序示例应用程序。它使用 EWS Java API。

下面是一个示例推送订阅请求：

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:t="http://
schemas.microsoft.com/exchange/services/2006/types">
   <soap:Body>
      <m:Subscribe xmlns:m="http://schemas.microsoft.com/exchange/services/2006/
messages">
         <m:PushSubscriptionRequest>
            <t:FolderIds>
               <t:DistinguishedFolderId Id="inbox" />
            </t:FolderIds>
            <t:EventTypes>
               <t:EventType>NewMailEvent</t:EventType>
               <t:EventType>CopiedEvent</t:EventType>
               <t:EventType>CreatedEvent</t:EventType>
               <t:EventType>DeletedEvent</t:EventType>
               <t:EventType>ModifiedEvent</t:EventType>
               <t:EventType>MovedEvent</t:EventType>
            </t:EventTypes>
            <t:StatusFrequency>1</t:StatusFrequency>
            <t:URL>https://YOUR_PUSH_RESPONDER_URL</t:URL>
         </m:PushSubscriptionRequest>
      </m:Subscribe>
   </soap:Body>
</soap:Envelope>
```

下面是成功的订阅请求结果：

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

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
   <Header xmlns="http://schemas.xmlsoap.org/soap/envelope/">
      <ServerVersionInfo xmlns="http://schemas.microsoft.com/exchange/
services/2006/types" MajorVersion="14" MinorVersion="2" MajorBuildNumber="390"
 Version="Exchange2010_SP2" MinorBuildNumber="3" />
   </Header>
   <soap:Body>
      <m:SubscribeResponse xmlns:m="http://schemas.microsoft.com/exchange/
services/2006/messages" xmlns:t="http://schemas.microsoft.com/exchange/services/2006/
types">
         <m:ResponseMessages>
            <m:SubscribeResponseMessage ResponseClass="Success">
               <m:ResponseCode>NoError</m:ResponseCode>
               <m:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</m:SubscriptionId>
               <m:Watermark>AAAAAAA=</m:Watermark>
            </m:SubscribeResponseMessage>
         </m:ResponseMessages>
      </m:SubscribeResponse>
   </soap:Body>
</soap:Envelope>
```

稍后，通知将发送到在订阅请求中指定的 URL。下面是示例通知：

```
<soap:Envelope
    xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Header>
        <t:RequestServerVersion
            xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
            xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages"
 Version="Exchange2010_SP2">
        </t:RequestServerVersion>
    </soap:Header>
    <soap:Body>
        <m:SendNotification
            xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
            xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
            <m:ResponseMessages>
                <m:SendNotificationResponseMessage ResponseClass="Success">
                    <m:ResponseCode>NoError</m:ResponseCode>
                    <m:Notification>
```

```
                        <t:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB=</
t:SubscriptionId>
                        <t:PreviousWatermark>ygwAAAAAAAA=</t:PreviousWatermark>
                        <t:MoreEvents>false</t:MoreEvents>
                        <t:ModifiedEvent>
                            <t:Watermark>ywwAAAAAAAA=</t:Watermark>
                            <t:TimeStamp>2018-02-02T15:15:14Z</t:TimeStamp>
                            <t:FolderId Id="AAB2L089bS1kNDgxOGYwOGE5OTQ0="></
t:FolderId>
                            <t:ParentFolderId Id="AAB2L089bS1kNDgxOGYwOGE="></
t:ParentFolderId>
                        </t:ModifiedEvent>
                    </m:Notification>
                </m:SendNotificationResponseMessage>
            </m:ResponseMessages>
        </m:SendNotification>
    </soap:Body>
</soap:Envelope>
```

要确认推送通知响应程序已收到通知，它必须回复以下信息：

```
<?xml version="1.0"?>
  <s:Envelope xmlns:s= "http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body>
      <SendNotificationResult xmlns="http://schemas.microsoft.com/exchange/
services/2006/messages">
        <SubscriptionStatus>OK</SubscriptionStatus>
      </SendNotificationResult>
    </s:Body>
  </s:Envelope>
```

要取消订阅接收推送通知，客户必须在 SubscriptionStatus 字段中发送取消订阅响应，类似于下面这样：

```
<?xml version="1.0"?>
  <s:Envelope xmlns:s= "http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body>
      <SendNotificationResult xmlns="http://schemas.microsoft.com/exchange/
services/2006/messages">
        <SubscriptionStatus>Unsubscribe</SubscriptionStatus>
      </SendNotificationResult>
    </s:Body>
```

```
  </s:Envelope>
```

为验证您的推送通知响应程序的运行状况，Amazon WorkMail 会发送一个“检测信号”（也称为 StatusEvent）。发送的频率将由在初始订阅请求中提供的 StatusFrequency 参数确定。例如，如果 StatusFrequency 等于 **1**，则每分钟发送一个 StatusEvent。此值可以介于 1 到 1440 分钟之间。此 StatusEvent 类似于下面这样：

```
<?xml version="1.0 (http://www.w3.org/TR/REC-xml/)" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Header>
    <t:RequestServerVersion xmlns:t="http://schemas.microsoft.com/exchange/
services/2006/types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/
messages" Version="Exchange2010_SP2"/>
</soap:Header>
<soap:Body>
    <m:SendNotification xmlns:t="http://schemas.microsoft.com/exchange/services/2006/
types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
    <m:ResponseMessages>
        <m:SendNotificationResponseMessage ResponseClass="Success">
            <m:ResponseCode>NoError</m:ResponseCode>
            <m:Notification>
                <t:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</t:SubscriptionId>
                <t:PreviousWatermark>AAAAAAAAAAA=</t:PreviousWatermark>
                <t:MoreEvents>false</t:MoreEvents>
                <t:StatusEvent>
                    <t:Watermark>AAAAAAAAAAA=</t:Watermark>
                </t:StatusEvent>
            </m:Notification>
        </m:SendNotificationResponseMessage>
    </m:ResponseMessages>
</m:SendNotification>
</soap:Body>
</soap:Envelope>
```

如果客户端推送通知响应程序未能以与以前相同的 OK 状态进行响应，则最多在 StatusFrequency 分钟内重试通知。例如，如果 StatusFrequency 等于 5，且第一个通知失败，则它最多在 5 分钟内重试，并且在每次重试之间使用指数回退。如果在重试时间到期后未发送通知，则订阅将失效，并且不会发送任何新通知。您必须创建新订阅以继续接收有关邮箱事件的通知。目前，每个邮箱最多可以有 3 个订阅。

启用已签名或已加密的电子邮件

您可以使用 S/MIME 使用户能够在组织内部和外部发送已签名或已加密的电子邮件。

> **Note**
>
> 仅已连接的 Active Directory 设置支持全局地址列表 (GAL) 中的用户证书。

使用户能够发送已签名或已加密的电子邮件

1. 设置 Active Directory (AD) Connector。使用本地目录设置 AD Connector 使用户能够继续使用其现有的企业凭证。
2. 配置证书自动注册以在 Active Directory 中自动颁发和存储用户证书。Amazon WorkMail 会从 Active Directory 接收用户证书并将其发布到 GAL。有关更多信息，请参阅配置证书自动注册。
3. 通过从运行 Microsoft Exchange 的服务器导出生成的证书并发送电子邮件来将这些证书分配给用户。
4. 每个用户将证书安装到其电子邮件程序 (如 Windows Outlook) 和移动设备。

使用组

您可以在 Amazon WorkMail 中使用组作为通讯组列表，用于接收通用电子邮件地址（如 <sales@example.com> 或 <support@example.com>）的电子邮件。您可以为一个组创建多个电子邮件别名。

您也可以将组用作安全组，以便与特定团队分享邮箱或日历。

组没有自己的邮箱，而这会影响您可以向组授予的邮箱权限。有关为组设置邮箱权限的信息，请参阅管理组的邮箱权限。

> **Note**
>
> 新添加的组出现在 Microsoft Outlook 离线通讯录中最多可能需要 2 小时。

主题

查看组列表

查看组列表

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。

3. 在导航窗格中，选择 组。
4. 此外，您可以按组名称或主要电子邮件地址筛选组。

> **Note**
>
> 搜索区分大小写。

添加组

您可以通过 Amazon WorkMail 控制台添加组。

添加组

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择组，然后选择添加组。

   将出现添加组页面。
4. 在组名称下，输入组的名称。
5. 在电子邮件地址下，输入组的主电子邮件地址。
6. 验证组的电子邮件地址，根据需要进行更新。
7. 默认情况下，组将显示在全球地址列表中。要在全球地址列表中隐藏组，请清除在全球地址列表中显示复选框。
8. 选择添加组。

启用组

当您将 Amazon WorkMail 与贵公司 Active Directory 集成时，或者您的 Simple Active Directory 中已有可用的组时，可以在 Amazon WorkMail 中将这些组用作安全组或通讯组列表。

启用现有目录组

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择 组。
4. 选中要启用的组旁边的复选框，然后选择启用。

   此时将出现启用组对话框，要求您确认操作。
5. 根据需要，查看并更改每个组的主要电子邮件地址，然后选择启用。

将成员添加到组

在您创建并启用 Amazon WorkMail 组之后，使用 Amazon WorkMail 控制台将用户添加到该组。

> **Note**
>
> 如果 Amazon WorkMail 与已连接的 Active Directory 服务或 Microsoft Active Directory 集成，您可以使用 Active Directory 管理组成员。但是，更改可能需要更长的时间才能传播到 Amazon WorkMail。

将成员添加到组

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择 组。
4. 选择组的名称。
5. 在组详细信息页面上，选择成员选项卡。
6. 在组或用户下选择要添加的组或用户。
7. 从下拉列表中选择用户或组。
8. 选择保存。

您的更改可能需要几分钟才能传播。

编辑组详细信息

您可以编辑组的详细信息。

编辑组详细信息

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择组，然后选择要编辑的组。
4. 在组详细信息页面上，根据需要更新电子邮件地址。
5. 默认情况下，组显示在全球地址列表中。要在全球地址列表中隐藏组，请清除在全球地址列表中显示复选框。
6. 选择保存更改。

从组中移除成员

使用 Amazon WorkMail 控制台从组中移除成员。

> **Note**
>
> 如果 Amazon WorkMail 与已连接的 Active Directory 或 Microsoft Active Directory 集成，您可以使用 Active Directory 管理组成员。但是，这样做可能会增加将更改传播到 Amazon WorkMail 所需的时间。

从组中移除成员

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择组，然后选择组的名称。

4. 在组详细信息页面上，选择成员选项卡。
5. 选择要从组中移除的成员。
6. 选择移除。

您的更改可能需要几分钟才能传播。

管理组别名

您可以在组中添加或移除电子邮件别名。

向组中添加电子邮件别名。

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择要为其添加别名的组织的名称。
3. 在导航窗格中，选择组，然后选择要向其添加别名的组的名称。
4. 在组详细信息部分，选择别名。
5. 在别名下，选择添加别名。
6. 在别名框中，输入别名。
7. 为别名选择一个域。
8. 选择添加。

从组中移除电子邮件别名。

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择要从中移除别名的组织的名称。
3. 在导航窗格中，选择组，然后选择要从中移除别名的组的名称。
4. 在组详细信息部分，选择别名。
5. 在别名下，选中要移除的别名对应的复选框。

6. 选择移除。
7. 验证要移除的别名。
8. 在移除别名窗口中，选择移除。

禁用组

当您不再需要组时，可以将其禁用。

禁用组

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择 组。
4. 在组名称下，选择要禁用的组，然后选择禁用。
5. 在 Disable group(s) 对话框中，选择 Disable。

删除组

在删除某个组之前，必须先禁用该组。有关禁用组的信息，请参阅禁用组。

删除组

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择 组。
4. 选中要删除的已禁用组旁边的复选框，然后选择删除。

   将显示删除对话框。
5. 在输入组名称以确认删除框中，输入组的名称，然后选择删除。

> **Note**
>
> 要永久删除某个组，请使用 Amazon WorkMail 的 `DeleteGroup` API 操作。有关更多信息，请参阅《Amazon WorkMail API 参考》中的 DeleteGroup。

使用资源

Amazon WorkMail 可以帮助您的用户预留资源。例如，用户可以预订会议室或投影仪、电话或汽车等设备。要预订资源，用户可以将此资源添加到会议邀请中。

主题

查看资源列表

查看资源列表

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择资源。
4. 此外，您可以按资源名称或主要电子邮件地址筛选资源。

> **Note**
>
> 搜索区分大小写。

添加资源

您可以向组织添加新资源，并允许用户预留该资源。

添加资源

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，依次选择资源和添加资源。

   将显示添加资源页面。
4. 在资源名称框中，为资源输入一个名称。
5. 或者，在资源描述框中，为资源输入一条描述。
6. 在资源类型下，选择一个选项。
7. 验证资源的电子邮件地址，根据需要进行更新。
8. 默认情况下，资源显示在全球地址列表中。要在全球地址列表中隐藏资源，请清除在全球地址列表中显示复选框。
9. 选择添加资源。

编辑资源详细信息

您可以编辑资源的一般详细信息，包括名称、描述、类型和电子邮件地址、预订选项和委托。

编辑一般的资源详细信息

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择 Resources，然后选择要编辑的资源。
4. 在资源详细信息选项卡上，根据需要更新资源名称、描述、资源类型或电子邮件地址。
5. 默认情况下，资源显示在全球地址列表中。要在全球地址列表中隐藏资源，请清除在全球地址列表中显示复选框。
6. 选择保存更改。

您可以将资源配置为自动接受或拒绝预订请求。

您可以编辑资源的预订选项。

更改资源的预订选项

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择 Resources，然后选择要编辑的资源。将出现一个页面，其中显示资源详细信息。
4. 在预订选项下，选择编辑。
5. 根据需要，选中或清除选项旁边的复选框以启用或禁用该选项。

> **Note**
>
> 禁用任何自动预订选项时，必须创建委托来处理预订请求。接下来的步骤说明如何创建委托。

您可以添加委托来控制未配置自动预订选项的资源的预订请求。资源委托自动接收所有预订请求的副本并且对资源日历具有完全访问权限。此外，它们必须接受资源的所有预订请求。

添加资源委托

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择资源，然后选择要向其添加委托的资源的名称。
4. （可选）在预订选项选项卡中，选择编辑，清除自动接受所有资源请求复选框，然后选择保存。
5. 选择委托选项卡，然后选择添加委托。

   此时将显示添加委托对话框。

6. 打开搜索委托列表并选择一个委托，然后选择保存。

移除资源委托

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择要从中移除委托的组织的名称。
3. 在导航窗格中，选择资源，然后选择要从中移除委托的资源的名称。
4. 选择委托，然后选择要移除的委托。
5. 选择移除。

管理资源别名

您可以为资源添加或移除电子邮件别名。

向资源添加电子邮件别名

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择要向其添加别名的组织的名称。
3. 在导航窗格中，选择资源，然后选择要向其添加别名的资源的名称。
4. 在资源详细信息部分中，选择别名。
5. 在别名下，选择添加别名。
6. 在别名框中，输入别名。
7. 为别名选择一个域。
8. 选择添加。

从资源中移除电子邮件别名

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

2. 在导航窗格中，选择组织，然后选择要从中移除别名的组织的名称。
3. 在导航窗格中，选择资源，然后选择要从中移除别名的资源的名称。
4. 在资源详细信息部分中，选择别名。
5. 在别名下，选中要移除的别名对应的复选框。
6. 选择移除。
7. 验证要移除的别名。
8. 在移除别名窗口中，选择移除。

启用资源

默认情况下，Amazon WorkMail 会创建资源。如果您或他人禁用了某项资源，您可以在 30 天内重新启用该资源。

禁用资源

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关区域的更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择包含要启用的资源的组织。
3. 在导航窗格中，选择资源。
4. 在资源列表中，选择要启用的资源旁边的按钮，然后选择启用。

   此时将显示启用资源对话框。
5. 请选择启用。

禁用资源

禁用某项资源即表示该资源无法预订。您可以在改造会议室时禁用会议室，然后在会议室可供使用时将其启用。

禁用资源

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关区域的更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择包含要禁用的资源的组织。
3. 在导航窗格中，选择资源。
4. 在资源列表中，选择要禁用的资源旁边的按钮，然后选择禁用。

   此时将显示禁用资源对话框。
5. 选择 禁用。

删除资源

当您不再需要某项资源，可以删除它。但是，您必须先禁用该资源。有关禁用资源的信息，请参阅上一部分中的相关步骤。

删除资源

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关区域的更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择所需的组织。
3. 在导航窗格中，选择资源。
4. 在资源列表中，选择要删除的已禁用资源旁边的按钮，然后选择删除。

   此时将显示删除资源对话框。
5. 在输入资源名称以确认删除框中，输入要删除的资源的名称，然后选择删除资源。

使用 IAM Identity Center

通过将 Amazon WorkMail 用户与 IAM Identity Center 关联，您可以在 Amazon WorkMail 中启用多重身份验证（MFA）。有关更多信息，请参阅什么是 IAM Identity Center。

下表描述了应对不同场景的步骤。

场景	步骤
将 Amazon WorkMail 用户与 IAM Identity Center 关联	1. 在 Amazon WorkMail 中启用 IAM Identity Center 2. 将 IAM Identity Center 用户和组分配给 Amazon WorkMail 应用程序 3. 将 Amazon WorkMail 用户与 IAM Identity Center 用户关联
现有 Amazon WorkMail 用户	1. 使用相同的用户名创建多个 IAM Identity Center 用户，将这些用户分组到一起，然后将该组分配给 Amazon WorkMail 应用程序。 2. 将 Amazon WorkMail 用户与 IAM Identity Center 用户关联。
现有 IAM Identity Center 用户	1. 使用与 IAM Identity Center 用户相同的用户名创建 Amazon WorkMail 用户。 2. 将 IAM Identity Center 用户或组分配给 Amazon WorkMail 应用程序。 3. 将 Amazon WorkMail 用户与 IAM Identity Center 用户关联。
将外部目录连接到 IAM Identity Center	1. 将外部目录用户同步到 IAM Identity Center 组。有关更多信息，请参阅 IAM Identity Center 身份源教程 2. 将 IAM Identity Center 组分配给 Amazon WorkMail 应用程序。 3. 将外部目录连接到 Amazon WorkMail 并确保用户名匹配

场景	步骤
	4. 将 Amazon WorkMail 用户与 IAM Identity Center 用户关联。

完成上述步骤后，您可以在 Amazon WorkMail 控制台的设置下的 IAM Identity Center 下，查看 IAM Identity Center 状态、指向 AWS IAM Identity Center 的用于管理用户和组的链接、启用 MFA 的 Amazon WorkMail Web 应用程序 URL、身份验证模式、个人访问令牌状态和时间表。有关在 IAM Identity Center 控制台中管理 MFA 的更多信息，请参阅 IAM Identity Center 用户的多重身份验证。

> **Note**
>
> 确保 Amazon WorkMail 和 IAM Identity Center 之间的配置经过充分的测试和验证。如果配置不正确和不完整，用户可能会失去对其邮箱的访问权限。

主题

在 Amazon WorkMail 中启用 IAM Identity Center

启用 IAM Identity Center 时，它将充当 Amazon WorkMail 用户的身份验证层。IAM Identity Center 用户是与 Amazon WorkMail 目录分开管理的。建议在 IAM Identity Center 和 Amazon WorkMail 中使用相同的用户名。

> **Note**
>
> 确保在同一区域中设置 Amazon WorkMail 和 IAM Identity Center。

要启用 IAM Identity Center，请按照以下步骤操作。

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择 Identity Center。

   将出现 IAM Identity Center 设置页面。
3. 请选择启用。

   将出现启用 IAM Identity Center 窗口。
4. 请选择启用。

   将出现 Identity Center 设置页面，并显示 Identity Center 状态。
5. 要将 IAM Identity Center 用户和组添加到 Amazon WorkMail 组织，请点击 Identity Center 状态下的链接。有关如何添加用户和组的信息，请参阅在 IAM Identity Center 中管理身份。

将 IAM Identity Center 用户和组分配给 Amazon WorkMail 应用程序

在 Amazon WorkMail 中启用 IAM Identity Center 时，WorkMail 会代表您在 IAM Identity Center 中创建应用程序。默认情况下，IAM Identity Center 用户必须分配给此应用程序或属于分配给该应用程序的组，才能访问 Amazon WorkMail 组织中的邮箱。有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的 AWS 托管式策略。

可以通过以下方式将 IAM Identity Center 用户和组分配给 Amazon WorkMail：

- 通过 IAM Identity Center 用户：您可以将 IAM Identity Center 用户分配给 Amazon WorkMail。
- 通过 IAM Identity Center 组：您可以将 IAM Identity Center 组分配给 Amazon WorkMail。通过添加组，组下的所有用户都将有权访问 Amazon WorkMail。

  有关添加用户和组的更多信息，请参阅 IAM Identity Center 中的用户、组和预置。

> **Note**
>
> 如果您要将现有身份源与 IAM Identity Center 连接，请在更改目录源之前先查看以下内容。
>
> - 您的身份验证由 IAM Identity Center 管理。

- Amazon WorkMail 将保留所有 Amazon WorkMail 用户和组。
- IAM Identity Center 将保留所有 IAM Identity Center 用户、组和分配。
- 您必须在 Amazon WorkMail 控制台中管理 Amazon WorkMail 用户和组。
- 您必须在 IAM Identity Center 中管理 IAM Identity Center 用户和组。
- 没有 IAM Identity Center 分配或用户关联的用户无法访问 Amazon WorkMail。
- 您必须在 IAM Identity Center 中管理 MFA 策略控制。
- 如果您在 IAM Identity Center 中将 IAM Identity Center 源更改为 IAM Identity Center 或反之，则必须禁用 Amazon WorkMail 中的现有 IAM Identity Center 配置，然后重新配置以将 Amazon WorkMail 用户与 IAM Identity Center 关联。

与 IAM Identity Center 目录同步的用户和组可供分配给 Amazon WorkMail 应用程序。有关 IAM Identity Center 用户和组管理的更多信息，请参阅 IAM Identity Center 中的常见任务入门。

要将 IAM Identity Center 用户和组分配给 Amazon WorkMail，请按照以下步骤操作。

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择 Identity Center。

   将出现 IAM Identity Center 设置页面。
3. 选择分配用户和组。

   您可以添加和分配新用户或分配现有用户和组。

   - 分配用户：您可以将各个 IAM Identity Center 用户分配给 Amazon WorkMail。您可以创建新的 IAM Identity Center 用户，也可以搜索现有用户。
   - 分配组：您也可以将 IAM Identity Center 组分配给 Amazon WorkMail。然后，该组的所有成员都将分配给 Amazon WorkMail。

> **Note**
>
> 默认情况下，在 IAM Identity Center 中启用了所有新的 IAM Identity Center 用户。要授予访问 Amazon WorkMail 的权限，您必须在 IAM Identity Center 中设置其密码并将他们分配给 Amazon WorkMail。有关更多信息，请参阅将用户添加到 Identity Center 目录。

将 Amazon WorkMail 用户与 IAM Identity Center 用户关联

当用户使用其 IAM Identity Center 用户凭证登录 Amazon WorkMail Web 客户端时，该客户端将打开关联的 Amazon WorkMail 用户的邮箱。如果 WorkMail 组织中没有用户与 IAM Identity Center 用户相关联，则 WorkMail 将在登录的 IAM Identity Center 用户与使用相同用户名的 WorkMail 用户之间创建关联（如果存在这样的 WorkMail 用户）。否则，客户端会向用户显示一条错误消息。

> **Note**
>
> 建议您在 Amazon WorkMail 和 IAM Identity Center 中为用户使用相同的用户名，因为当用户首次使用其 IAM Identity Center 用户凭证登录 Amazon WorkMail Web 客户端时，WorkMail 将自动创建关联。当用户名不同时，将由您负责创建关联。

要关联用户，请按照以下步骤操作。

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

2. 在导航窗格中，选择 Identity Center。

   将出现 IAM Identity Center 设置页面。

3. 选择关联用户。
4. 在选择 WorkMail 用户下，选择您希望关联的 Amazon WorkMail 用户。
5. 在输入 IAM Identity Center 用户 ID 下，输入您希望关联的 IAM Identity Center 用户的 ID。您可以从 Identity Center 页面上的分配的用户选项卡中复制 ID。

> **Note**
>
> IAM Identity Center 用户必须获得授权，才能访问 Amazon WorkMail 应用程序。

6. 选择关联用户。

   关联成功后，Amazon WorkMail 用户可以使用 MFA IAM Identity Center 凭证登录 Amazon WorkMail。

> **Note**
>
> 还可以在编辑 Amazon WorkMail 用户详细信息时，将 Amazon WorkMail 用户与 IAM Identity Center 用户相关联。有关更多信息，请参阅 编辑用户详细信息。

身份验证模式

您可以使用身份验证模式，来支持用户使用其 Amazon WorkMail 目录凭证、其 IAM Identity Center 凭证登录，或者仅允许使用 IAM Identity Center 凭证登录。

Amazon WorkMail 中有两种身份验证模式可供选择。

> **Note**
>
> 身份验证模式的选择取决于贵组织的安全要求和用户体验偏好。建议使用仅限 IAM Identity Center 模式，因为它通过强制实施 IAM Identity Center 凭证和 MFA 来增强安全性。但是，在从 Amazon WorkMail 目录和 IAM Identity Center 模式切换之前，请务必与所有用户一起测试 MFA 流程，以确保平稳过渡并避免对现有电子邮件客户端访问造成任何影响。

- Amazon WorkMail 目录和 IAM Identity Center（建议用于测试）：这是默认选项，供您在切换到生产模式之前测试 IAM Identity Center 关联。测试模式支持用户同时使用 Amazon WorkMail 目录和 IAM Identity Center 凭证登录 Amazon WorkMail Web 客户端。当您共享组织设置中的 Amazon WorkMail Web 应用程序 URL 时，您的用户可以使用其 Amazon WorkMail 目录凭证登录。当您共享 IAM Identity Center 设置中启用 MFA 的 URL 时，您的用户可以使用其 IAM 凭证登录。
- 仅限 IAM Identity Center（建议用于生产）：此身份验证模式仅支持您使用 IAM Identity Center 凭证登录 Amazon WorkMail 客户端邮箱。对于任何现有 Amazon WorkMail 用户，Amazon WorkMail 目

录凭证对 Amazon WorkMail Web 应用程序和任何现有电子邮件客户端都不再有效。您可以请求个人访问令牌，以使用任何电子邮件客户端来访问邮箱。为避免失去对邮箱的访问权限，请确保为所有 Amazon WorkMail 用户启用 MFA。

要启用身份验证模式，请按照以下步骤操作。

1. 在 Identity Center 设置页面下，选择身份验证模式选项卡。
2. 选择编辑。

   将出现编辑身份验证模式页面。
3. 选择以下选项之一：

   - 仅限 IAM Identity Center
   - Amazon WorkMail 目录和 IAM Identity Center
4. 选择保存。

配置个人访问令牌

您可以启用个人访问令牌，来让 Amazon WorkMail 用户使用桌面和移动电子邮件客户端访问其邮箱。启用 IAM Identity Center 后，默认情况下，个人访问令牌状态设置为活动，有效期为 365 天。启用 IAM Identity Center 后，用户的现有凭证将不再有效，因而无法登录其电子邮件客户端。您的用户可以从 Amazon WorkMail Web 应用程序生成个人访问令牌，并使用它登录任何电子邮件客户端。您可以编辑个人访问令牌到期时间，当令牌到期时，您的用户可以生成新的访问令牌。

> **Note**
>
> - 当您在 Amazon WorkMail 中创建个人访问令牌时，您的用户只能查看和复制一次您的个人访问令牌。如果您丢失个人访问令牌，出于安全考虑，您需要生成新的令牌。
> - 只有当 Amazon WorkMail 用户与获得授权可访问 Amazon WorkMail 应用程序的 IAM Identity Center 用户关联时，Amazon WorkMail 才支持使用个人访问令牌访问邮箱。

下面列出了个人访问令牌配置：

- 活动：当个人访问令牌状态设置为活动时，用户可以从 Amazon WorkMail 生成个人访问令牌，并在令牌的生命周期内使用该令牌登录任何电子邮件客户端。

- 非活动：当个人访问令牌状态设置为非活动时，用户将无法生成或使用个人访问令牌来访问邮箱。
- 令牌生命周期：默认情况下，个人访问令牌的有效期为 365 天。您可以选择更改个人访问令牌生命周期。当您将生命周期设置留空时，令牌的生命周期将为无限期且从不过期。

要配置个人访问令牌，请按照以下步骤操作。

1. 在 Identity Center 设置页面下，选择个人访问令牌配置选项卡。
2. 选择编辑。

   将出现编辑个人令牌配置页面。
3. 在令牌状态下，滑动活动按钮以启用个人访问令牌。
4. 在令牌生命周期（以天为单位）文本框中，输入可以激活个人访问令牌的天数。
5. 选择保存。

禁用 IAM Identity Center

您可以从 Amazon WorkMail 控制台中禁用 IAM Identity Center。禁用后，您将无法使用 IAM Identity Center 凭证或个人访问令牌访问邮箱。建议重置所有用户密码，Amazon WorkMail 用户将恢复为使用 Amazon WorkMail 目录凭证。

> **Note**
>
> 请检查以下事项：
>
> - 禁用 IAM Identity Center 后，Amazon WorkMail 和 IAM Identity Center 用户和组将保持不变。
> - 现有的用户关联将继续存在。
> - 身份验证将恢复为由 Amazon WorkMail 目录管理，而不是由 IAM Identity Center 管理。

要禁用 IAM Identity Center，请按照以下步骤操作。

1. 在 Identity Center 设置页面下，选择禁用。

   将出现禁用 IAM Identity Center 页面。
2. 选择确认。

使用移动设备

本部分中的主题介绍如何管理连接到 Amazon WorkMail 的移动设备。

主题

编辑组织的移动设备策略

您可以编辑组织的移动设备策略以更改移动设备与 Amazon WorkMail 交互的方式。

编辑组织的移动设备策略

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域名称和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择 Mobile Policies (移动策略)，然后在 Mobile policy (移动策略) 屏幕上选择 Edit (编辑)。
4. 根据需要更新以下任意项：

   a. Require encryption on device：对移动设备上的电子邮件数据进行加密。

   b. Require encryption on storage card：对移动设备的可移除存储上的电子邮件数据进行加密。

   c. 需要提供密码：需要密码来解锁移动设备。

   d. 允许简单密码：使用设备的 PIN 作为密码。

   e. 最小密码长度：设置有效密码所需的字符数。

   f. 需要字母数字密码：要求密码由字母和数字组成。

   g. 允许的失败尝试次数：指定在擦除用户的设备之前支持的设备解锁失败尝试次数。擦除设备时，将删除包括个人文件在内的所有数据。

h. Password expiration：指定密码还有多少天过期并必须更改。

i. Enable screen lock：指定必须多少秒没有用户输入才锁定用户的屏幕。

j. Enforce password history：指定在重复相同密码之前可以输入的密码数。

5. 选择保存。

管理移动设备

本部分中的主题说明如何远程擦除移动设备、从组织中删除设备以及查看设备的详细信息。有关编辑组织的移动设备策略的信息，请参阅编辑组织的移动设备策略。

主题

远程擦除移动设备

本部分中的步骤说明如何远程擦除移动设备。请记住以下事项：

- 设备必须处于在线状态并连接到 Amazon WorkMail。如果有人断开了设备的连接，则当用户重新连接设备时，擦除操作将恢复。
- 擦除操作可能需要五分钟才能传播。

> **Important**
>
> 对于大多数移动设备，远程擦除会将设备重置为出厂默认值。在您执行此过程时，会删除包括个人文件在内的所有数据。

远程擦除用户的移动设备

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域名称和端点。

2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择用户，然后在用户列表中选择需要擦除其设备的用户的名称。
4. 选择移动设备选项卡。
5. 在设备列表中，选择相应设备旁边的按钮，然后选择擦除。
6. 查看概述中的状态以查看是否请求擦除。
7. 擦除设备后，将其从设备列表中删除。下一部分中的相关步骤将说明如何操作。

> **Important**
>
> 要将已擦除的设备返回到用户的设备列表中，请务必先将其从设备列表中删除。否则，系统会再次擦除该设备。

从设备列表中删除用户设备

如果有人停止使用特定的移动设备，或者您已远程擦除该设备，则可以将该设备从设备列表中删除。当用户再次配置该设备时，它会显示在列表中。

从设备列表中删除用户的移动设备

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择用户，然后选择用户的名称。
4. 选择移动设备选项卡。
5. 在设备列表中，选择相应设备旁边的按钮，然后选择删除。

查看移动设备详细信息

您可以查看用户的移动设备的详细信息。

> **Note**
>
> 有些设备不会将其所有详细信息发送到服务器。您可能看不到所有可用的设备详细信息。

查看设备详细信息

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改区域。从导航栏中，选择满足您的需求的区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择用户，然后选择移动设备选项卡。
4. 在设备列表中，选择要查看其详细信息的设备的 ID。

   下表列出了设备状态代码。

Status	描述
PROVISIONING_REQUIRED	用户或管理员已请求预配置设备以与 Amazon WorkMail 一起使用。如果在 Amazon WorkMail 控制台中修改了设备的当前策略，则也会将该设备设置为此状态。
PROVISIONING_SUCCEEDED	已成功预配置设备。设备已执行给定策略。
WIPE_REQUIRED	管理员在 Amazon WorkMail 控制台中请求了擦除。
WIPE_SUCCEEDED	已成功擦除设备。

管理移动设备访问规则

适用于 Amazon WorkMail 的移动设备访问规则允许管理员控制邮箱对某些类型的移动设备的访问。默认情况下，每个 Amazon WorkMail 组织均采用授予邮箱对任何设备的访问权限的规则，无论设备的类型、型号、操作系统或用户代理如何。您可以编辑该默认规则或将其替换为您自己的规则。您还可以添加、更改和删除规则。

> **Warning**
>
> 如果您删除组织的所有移动设备访问规则，Amazon WorkMail 将阻止所有移动设备访问。

您可以根据以下设备属性创建允许或拒绝访问的规则：

- 设备类型 -“iPhone”、“iPad”或“Android”。
- 设备型号 -“iPhone10C1”、“iPad5C1”或“HTCOneX”。
- 设备操作系统 -“iOS 12.3.1 16F203”或“Android 8.1.0”。
- 设备用户代理 -“iOS/14.2 (18B92) exchangesyncd/1.0”或“Android-Mail/7.7.16.163886392.release”。

要在 AWS 管理控制台上查看设备属性，请参阅查看移动设备详细信息。

> **Note**
>
> 某些设备和客户端可能不会报告所有字段对应的属性。有关解决这些情况的信息，请参阅Dealing with empty fields

> **Important**
>
> Amazon WorkMail 移动设备访问规则仅适用于使用 Microsoft Exchange ActiveSync 协议的设备。使用其他协议（例如 IMAP）的移动客户端不会报告此处列出的设备属性，因此这些规则将不适用。
> 如果您需要限制使用其他协议的设备的访问权限，则可以创建访问控制规则。有关这些规则的更多信息，请参阅使用访问控制规则。例如，您可以将对其他协议和网络邮件的访问限制为仅限一系列公司 IP 地址，但允许从其他位置访问 Microsoft ActiveSync，然后使用移动设备访问规则进一步限制允许的客户端的类型和版本。

主题

移动设备访问规则的工作原理

移动设备访问规则仅适用于使用 Microsoft Exchange ActiveSync 协议的设备。每个规则都有一组条件，用于指定何时应用规则，以及设备对应的 ALLOW 或 DENY 访问权限。仅当一个规则的所有条件都

与用户移动设备的属性匹配时，该规则才适用于访问请求。无条件的规则适用于所有请求。每个条件均使用不区分大小写的前缀与设备报告的属性进行匹配。

Amazon WorkMail 对规则的评估如下：

- 如果任何 DENY 规则与设备属性匹配，则该策略会阻止该设备访问。DENY 规则优先于 ALLOW 规则。
- 如果至少有一个 ALLOW 规则匹配，并且没有任何 DENY 规则匹配，则该策略允许该设备访问。
- 如果不适用任何规则，则该设备会被阻止。

> **Important**
>
> 移动设备会报告规则用于操作的属性。这些设备会在 Microsoft ActiveSync 设备配置过程中报告其属性。Amazon WorkMail 无法独立验证移动客户端报告的信息是否正确或最新。

管理移动设备访问规则

您可以使用 API 或 AWS 命令行界面 (CLI) 创建和管理移动设备访问规则。有关 AWS CLI 的更多信息，请参阅 AWS 命令行界面用户指南。

> **Important**
>
> 当您更改 Amazon WorkMail 组织的访问规则时，受影响的设备可能需要五分钟才能遵循更新的规则，并且在此期间设备可能会表现出不一致的行为。但是，在测试规则时，您会立即看到正确的行为。有关更多信息，请参阅 Testing mobile device access rules。

列出移动设备访问规则

以下示例演示如何列出移动设备访问规则。

```
aws workmail list-mobile-device-access-rules --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

创建移动设备访问规则

以下示例创建了一个阻止所有 Android 设备访问邮箱的规则。

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name BlockAllAndroid --effect DENY --device-types
 "android"
```

以下示例创建了一个仅允许特定版本的 iOS 的规则。请务必删除默认的 ALLOW-all 规则。

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name AllowLatestiOS --effect ALLOW --device-
operating-systems "iOS 14.3"
```

更新移动设备访问规则

以下示例通过添加标识符来更新设备规则。

```
aws workmail update-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d --
name AllowLatestiOS --effect ALLOW --device-operating-systems "iOS 14.4"
```

删除移动设备访问规则

以下示例删除具有给定标识符的移动设备访问规则。

```
aws workmail delete-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d
```

测试移动设备访问规则

要测试访问规则，您可以使用 GetMobileDeviceAccessEffect API 或 AWS CLI 中的 get-mobile-device-access-effect 命令。有关 AWS CLI 的更多信息，请参阅 AWS 命令行界面用户指南。

测试时，您传入模拟移动设备的属性，然后 API 或 CLI 会返回具有这些属性的实际移动设备将获得的访问权限（ALLOW 或 DENY）。例如，此命令测试运行 iOS 14.2 的 iPhone 以及默认邮件应用程序能否访问邮箱。

```
aws workmail get-mobile-device-access-effect --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --device-type "iPhone" --device-model "iPhone10C1"
 --device-operating-system "iOS 14.2.1 16F203" --device-user-agent "iOS/14.2 (18B92)
 exchangesyncd/1.0"
```

处理空字段

某些移动设备或客户端可能不会报告一个或多个字段的信息，从而将对应值留空。通过在条件中使用特殊值 $NONE，可以将规则与这些设备进行匹配。例如，包含 DeviceTypes=["iphone", "ipad", "$NONE"] 的规则将匹配报告设备类型为 "iphone" 或 "ipad" 的设备或根本不报告设备类型的设备。

NotDeviceTypes 或 NotDeviceUserAgents 等否定条件与这些空值不匹配。例如，包含 NotDeviceTypes=["android"] 的规则将匹配报告设备类型不是 "android" 的设备。但是，该规则不会匹配根本不报告设备类型的设备。

管理移动设备访问覆盖

您可以使用移动设备访问覆盖来覆盖移动设备访问规则的结果。覆盖适用于特定用户和设备，并且会反转默认访问规则。您还可以使用覆盖来创建访问规则的一次性例外，并允许或拒绝特定的用户和设备对。此外，还可以将覆盖与 DefaultDenyAll 移动设备访问规则结合使用。这就将访问决策交给了第三方移动设备管理（MDM）解决方案。有关更多信息，请参阅 管理覆盖 和 与移动设备管理解决方案集成

主题

移动设备访问覆盖的工作原理

您可以为特定用户和设备对创建移动设备访问覆盖。评估给定用户和设备的移动设备访问规则时，覆盖会反转默认访问结果。例如，如果访问规则通常拒绝访问，则访问覆盖允许该用户和设备同步其电子邮件。相反，如果访问规则通常允许访问，则可以创建阻止用户和设备同步其邮件的覆盖。当您删除移动设备访问覆盖时，Amazon WorkMail 在决定是否向该用户和设备授予访问权限时，会再次遵循当前移动设备访问规则的结果。

> **Important**
>
> 当您更改 Amazon WorkMail 组织的移动设备访问覆盖时，受影响的设备可能需要五分钟才能遵循更新的覆盖。

管理覆盖

可以使用 API 或 AWS Command Line Interface创建、更新或删除移动设备访问覆盖。有关 AWS CLI 的更多信息，请参阅 AWS 命令行界面用户指南。

要查找设备 ID，请使用 AWS 管理控制台。有关更多信息，请参阅查看移动设备详细信息。

列出移动设备访问覆盖

此示例演示如何列出指定 Amazon WorkMail 组织的所有移动设备访问覆盖。

```
aws workmail list-mobile-device-access-overrides --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

创建和更新移动设备访问覆盖

这将创建移动设备访问覆盖，以拒绝对指定 Amazon WorkMail 组织、用户和设备 ID 的访问。

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECDO --effect DENY
```

可以修改现有的移动设备访问覆盖以具有不同的权限。这将更新之前创建的移动设备访问覆盖，以允许访问而不是拒绝。

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECDO --effect ALLOW
```

删除移动设备访问覆盖

这将删除指定 Amazon WorkMail 组织、用户和设备 ID 的移动设备访问覆盖。

```
aws workmail delete-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECDO
```

与移动设备管理解决方案集成

Amazon WorkMail 通过移动设备策略和移动设备访问规则支持一些基本的移动设备管理功能。但是，这些功能只能通过 Microsoft Exchange ActiveSync (EAS) 协议与移动设备交互，因此它们自检和实施

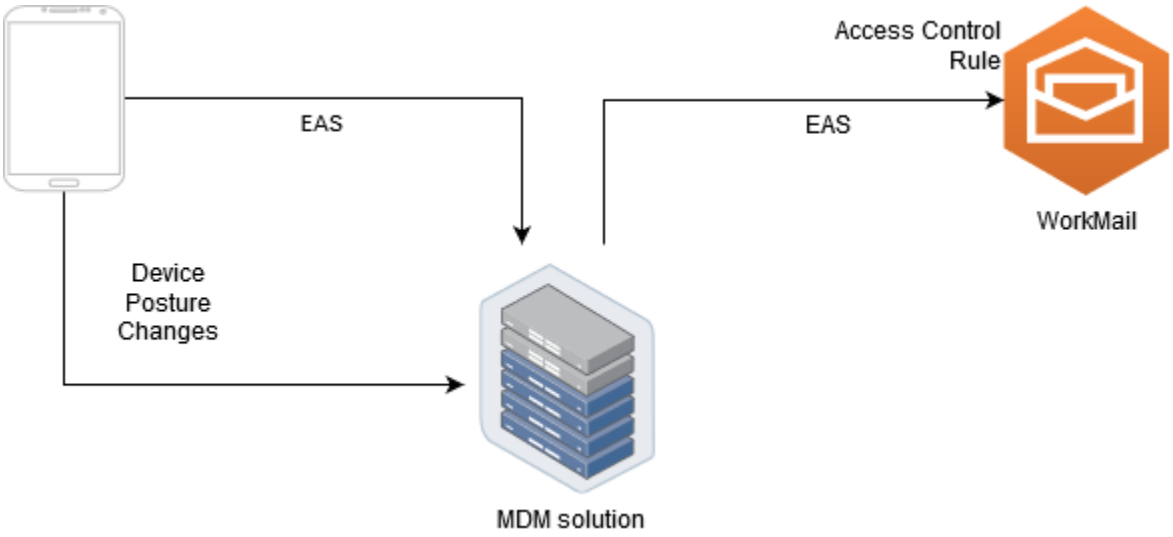
设备安全态势的能力有限。需要更好地控制设备安全性和合规性的管理员可以使用第三方移动设备管理 (MDM) 解决方案。

移动设备管理解决方案概述

您可以在两种模式下配置 MDM 解决方案：“代理”或“直接”。请查阅您的 MDM 文档，了解您的解决方案支持哪些模式。

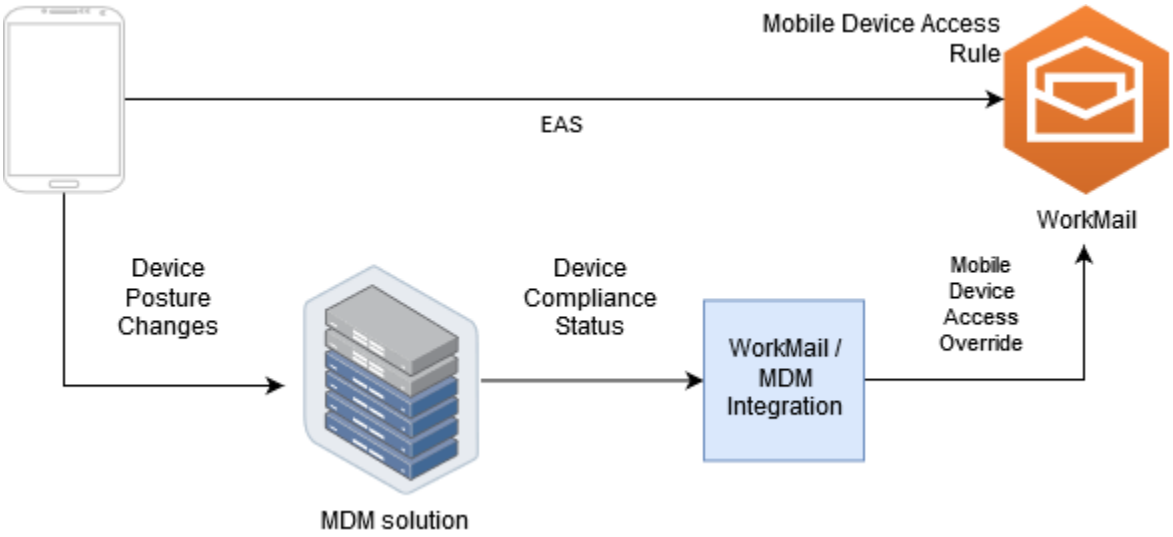
在代理模式下，移动设备通过您的 MDM 解决方案使用 Exchange 活动同步 (EAS) 协议来访问 Amazon WorkMail。MDM 解决方案使用设备状态来允许或拒绝对 Amazon WorkMail 数据的访问。在 Amazon WorkMail 端，请使用一个访问控制规则，该规则仅允许从 MDM 解决方案的一个或多个 IP 地址进行 EAS 访问。有关更多信息，请参阅使用访问控制规则。

下图显示了典型的代理模式配置。



在直接模式下，移动设备使用 EAS 直接访问 Amazon WorkMail。您的 MDM 解决方案会接收设备状态更改，并持续评估每台设备是否满足这些要求。当 MDM 解决方案检测到状态更改（例如设备不合规）时，它可以采取多项操作，并且通常会发出通知或事件。Amazon WorkMail 管理员可以设置一个系统来侦听这些合规性状态事件，并自动创建移动设备访问覆盖，以便在设备符合或不符合 MDM 设备要求时允许或拒绝对设备的访问。

下图显示了典型的直接模式配置。



将 WorkMail 组织配置为在直接模式下与第三方 MDM 解决方案集成

要在直接模式下与第三方移动设备管理 (MDM) 解决方案集成，必须满足以下要求：

- 创建访问控制规则，限制只能通过 ActiveSync 协议访问用户设备。
- 创建默认的“拒绝全部”移动设备访问规则，以确保默认情况下拒绝所有未知或非托管移动设备。
- 采用移动设备管理解决方案，当设备更改安全态势（即设备符合或不符合要求）时，该解决方案会发出自定义通知或事件。
- 创建自定义软件组件以侦听这些通知，并调用 Amazon WorkMail SDK 以创建移动设备访问覆盖。

这些组件可确保所有用户设备在被允许访问其 Amazon WorkMail 邮箱之前均符合其 MDM 合规性要求。

使用访问控制规则限制移动设备对 ActiveSync 的访问

您必须确保所有设备仅使用 ActiveSync 协议，并且您可以使用访问控制规则来执行此操作。例如，您可以仅从公司内部 IP 地址范围内授予对其他邮件协议的访问权限，然后在从公司防火墙外部访问电子邮件时仅允许 ActiveSync。您必须执行此操作，因为只有 ActiveSync 允许您使用设备 ID 标识设备。不能使用互联网邮件访问协议 (IMAP) 或 Exchange Web Services 等协议。有关更多信息，请参阅 使用访问控制规则。

创建默认的“拒绝全部”访问规则

要将所有移动设备访问决策交给第三方移动设备管理解决方案，请创建一个访问规则，该规则会自动拒绝所有设备，除非按用户或按设备进行覆盖。有关更多信息，请参阅管理移动设备访问规则。

此示例显示了“拒绝全部”规则。

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name DefaultDenyAll --effect DENY
```

对设备状态更改做出反应并创建移动设备访问覆盖

您必须将 MDM 解决方案配置为发送有关设备状态更改的通知。这些通知必须由可使用 Amazon WorkMail SDK 创建或更新移动设备访问覆盖的组件来使用。由于本主题前面所示的默认“拒绝全部”移动设备访问规则，默认情况下，Amazon WorkMail 会拒绝访问未托管或新配置的设备。当 MDM 解决方案确定设备符合所有要求并发出指示设备符合要求的通知时，此组件可以通过为指定用户和设备创建具有 ALLOW 权限的移动设备访问覆盖来对此通知做出反应。如果设备之后不符合要求，移动设备管理解决方案会发出另一个通知，并且可能会删除或修改访问覆盖以拒绝该设备的访问。有关更多信息，请参阅 管理移动设备访问覆盖。

有关与 MDM 集成的 Amazon WorkMail 的示例，请参阅此 AWS 示例应用程序。

使用邮箱权限

您可以使用 Amazon WorkMail 中的邮箱权限向用户和组授予在其他用户的邮箱中工作的权利。邮箱权限适用于整个邮箱。它们使多个用户能够访问同一邮箱，而无需共享该邮箱的凭证。具有邮箱权限的用户可以读取和修改邮箱数据并从共享邮箱发送电子邮件。

> **Note**
>
> 对属于全局地址列表中隐藏的用户的邮箱具有权限的用户仍可以访问隐藏用户的邮箱。

以下列表显示了您可以授予的权限：

- 完全访问权限 – 启用对邮箱的完全读取和写入访问权限，包括修改文件夹级权限的权限。

  > **Note**
  >
  > 此选项仅适用于用户。无法向组授予完全访问权限。

- 代表发送 – 可让用户或组代表其他用户发送电子邮件。邮箱所有者显示在 From: (从:) 标头中，发件人显示在 Sender: (发件人:) 标头中。
- 发送为 – 可让用户或组以邮箱所有者身份发送电子邮件，而不显示邮件的实际发件人。邮箱所有者显示在 From: (从:) 标头和 Sender: (发件人:) 标头中。
- 无 – 阻止用户或组发送电子邮件。

> **Note**
>
> 向某个组授予邮箱权限可将这些权限扩展到该组的所有成员，包括嵌套组的成员。

当您授予邮箱权限时，Amazon WorkMail 自动发现服务会为您添加的用户或组自动更新对这些邮箱的访问权限。

对于 Windows 中的 Microsoft Outlook 客户端，具有完全访问权限的用户可以自动访问共享邮箱。最多允许更改传播 60 分钟，然后重新启动 Microsoft Outlook。

对于 Amazon WorkMail Web 应用程序以及在其他电子邮件客户端中，具有完全访问权限的用户可以手动打开共享邮箱。即使在不同会话之间，已打开的邮箱也将保持打开状态，除非用户将其关闭。

主题

关于邮箱和文件夹权限

邮箱权限适用于邮箱内的所有文件夹。这些权限只能由 AWS 账户持有人或有权调用 Amazon WorkMail 管理 API 的 IAM 用户启用。要设置和更改邮箱或整个组的权限，请使用 AWS 管理控制台或 Amazon WorkMail API。您可以从控制台管理多达 100 个邮箱和组权限。要管理更多用户和组的权限，请使用 Amazon WorkMail API。

文件夹权限仅适用于单个文件夹。最终用户可以使用电子邮件客户端或使用 Amazon WorkMail Web 应用程序设置文件夹权限。有关使用 Amazon WorkMail Web 应用程序共享文件夹的更多信息，请参阅《Amazon WorkMail 用户指南》中的共享文件夹和文件夹权限。

管理用户的邮箱权限

您可以使用 Amazon WorkMail 控制台管理用户和组的邮箱权限。以下各部分说明如何管理用户的权限。有关管理组的权限的更多信息，请参阅管理组的邮箱权限。

主题

添加权限

添加权限时，您会向一个用户授予在另一个用户的邮箱中执行一项或多项任务的权利。例如，假设员工 A 需要代表其主管（员工 B）发送邮件。要授予该权限，请转到员工 B 的邮箱设置，并授予员工 A 执行所请求任务的权限。

添加邮箱权限

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改区域。从导航栏中，选择符合您需求的区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

2. 在导航窗格中，选择组织，然后选择要为其管理权限的组织的名称。
3. 在导航窗格中，选择用户，然后选择要为其管理权限的用户的名称。
4. 请选择 Permissions 选项卡，然后选择 Add permissions。

   此时将显示添加权限对话框。
5. 打开添加新权限列表，然后选择需要访问邮箱的用户或组。
6. 在邮箱权限和发送权限下，选择所需的选项。
7. 选择添加。

新权限最多可能需要 5 分钟才能传播到用户。

编辑用户的邮箱权限

编辑用户的邮箱权限时，您会更改其他人对该用户邮箱的访问权限。编辑邮箱权限不会更改邮箱原始用户的访问权限。

编辑邮箱权限

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改区域。从导航栏中，选择符合您需求的区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择要为其管理权限的组织的名称。
3. 在导航窗格中，选择用户，然后选择要编辑其权限的用户的名称。
4. 选择 Permissions（权限）选项卡。

   此时将显示有权访问该邮箱的用户和组的列表。
5. 选择要更改的用户或组旁边的单选按钮，然后执行以下任一操作：

   删除用户的权限

   1. 选择移除。

      此时将显示删除权限对话框。
   2. 在删除权限对话框中，选择删除。

编辑用户的权限

1. 选择编辑。

   此时将显示编辑权限对话框。
2. 根据需要设置权限，然后选择保存。

向其他用户授予对邮箱的权限

1. 选择添加权限。

   此时将显示添加权限对话框。
2. 打开添加新权限列表并选择要添加的用户。
3. 根据需要设置权限，然后选择添加。

对权限的更改最多可能需要 5 分钟才能传播到用户。

管理组的邮箱权限

您可以为 Amazon WorkMail 添加或删除组权限。

> **Note**
>
> 您无法对组应用完全访问权限，因为组没有可访问的邮箱。

管理组权限

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择要为其管理权限的组织的名称。
3. 在导航窗格中，选择组，然后选择要为其设置权限的组的名称。
4. 选择权限选项卡，然后选择添加权限。

此时将显示添加权限对话框。

5. 打开添加新权限列表，然后选择要授予邮箱权限的用户或组。
6. 在邮箱权限和发送权限下，选择所需的选项。
7. 选择添加。

对权限的更改最多可能需要 5 分钟才能传播到用户。

以编程方式访问邮箱

要以编程方式访问 Amazon WorkMail 邮箱，请使用 Exchange Web Services (EWS) 协议。使用 EWS，您可以访问邮箱中的所有项目类型。以下是一些可与 Amazon WorkMail 结合使用的 EWS 库：

- Java – EWS Java API
- .Net – EWS Managed API
- Python – Exchangelib

Amazon WorkMail 还支持 IMAP 和 SMTP 协议，您可以使用这些协议来发送和接收电子邮件。您可以在 Amazon WorkMail 端点和配额下查看 Amazon WorkMail 协议支持的 URL。

使用 EWS 协议时，Amazon WorkMail 支持以下身份验证方法：

- 基本身份验证 – 使用基本身份验证，您需要输入电子邮件地址和密码。
- 模拟角色 – 使用模拟角色，您无需输入用户的凭证即可访问用户的邮箱。

主题

管理模拟角色

使用模拟角色，管理员无需输入用户的凭证即可配置以编程方式访问用户邮箱。服务和工具可以扮演模拟角色，在用户的邮箱中执行操作。只有 EWS 协议支持模拟角色。

模拟角色概述

要允许模拟，管理员必须创建具有以下属性的模拟角色：

- 角色类型 – 选择完全访问或只读。角色类型限制了角色可以执行的操作类型。
- 规则 – 定义模拟角色可以模拟哪些用户的规则列表。

Amazon WorkMail 根据以下条件评估规则：

- 如果任何 DENY 规则匹配，则策略将拒绝模拟。DENY 规则优先于任何 ALLOW 规则。

- 如果至少有一个 ALLOW 规则匹配，并且没有 DENY 规则匹配，则策略允许模拟。
- 如果没有应用规则，则拒绝模拟。

> **Note**
>
> 要允许 Amazon WorkMail 组织中的所有用户进行模拟，请创建一个具有 ALLOW 权限且不带任何条件的规则。

> **Warning**
>
> 您必须创建规则以允许模拟角色模拟用户。如果您未指定规则，则模拟角色无法代入用户的访问权限。

创建模拟角色后，您可以使用它来访问用户的邮箱。有关更多信息，请参阅 使用模拟角色。

安全性注意事项

使用模拟角色可能会在您的 Amazon WorkMail 组织和 AWS 账户中造成安全问题。以下是创建模拟角色时需要考虑的一些潜在问题：

- 传递权限 - 如果用户 A 有权访问用户 B 的邮箱，并且允许模拟角色模拟用户 A，则此模拟角色可以模拟用户 A 的访问权限并访问用户的 B 邮箱。
- 访问控制 – 您可以使用访问控制规则来限制模拟角色的访问权限。有关更多信息，请参阅 使用访问控制规则。
- IAM 策略 – 您可以使用 `workmail:ImpersonationRoleId` 条件将 `AssumeImpersonationRole` 操作分配给特定的 Amazon WorkMail 组织和模拟角色。要查看 IAM 策略示例，请参阅 Amazon WorkMail 如何与 IAM 结合使用。

创建模拟角色

您可以通过 Amazon WorkMail 控制台创建模拟角色。

创建模拟角色

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

如果需要，可以更改区域。从导航栏中，选择符合您需求的区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

2. 在导航窗格中，选择组织，然后选择组织的名称。
3. 选择模拟角色，然后选择创建角色。
4. 此时将显示创建模拟角色对话框。在角色下，输入以下信息：
   - 名称 - 输入模拟角色的唯一名称。
   - （可选）描述 - 输入模拟角色的描述。
   - 角色类型 – 选择只读或完全访问。
5. 在规则下，选择添加规则。
6. 此时将显示添加规则对话框。输入以下信息：
   - 名称 – 输入规则的唯一名称。
   - （可选）描述 – 输入规则的描述。
   - 在权限下，选择允许或拒绝。这将根据您在下一步中选择的条件来允许或拒绝访问。
   - （可选）在此规则：下，选择匹配模拟所选用户的请求以包含特定用户。选择匹配模拟所选用户以外的用户的请求以添加所选用户以外的用户。
7. 选择添加规则。

> **Note**
>
> 只有在保存相应角色时才会保存规则。

8. 选择创建角色。

编辑模拟角色

您可以通过 Amazon WorkMail 控制台编辑模拟角色。

编辑模拟角色

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改区域。从导航栏中，选择符合您需求的区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

2. 在导航窗格中，选择组织，然后选择组织的名称。
3. 选择模拟角色。
4. 选择要编辑的模拟角色名称，然后选择编辑。
5. 此时将显示编辑模拟角色对话框。在角色下，输入以下信息：
   - 名称 - 输入模拟角色的唯一名称。
   - （可选）描述 - 输入模拟角色的描述。
   - 角色类型 - 要授予模拟角色对用户邮箱的只读权限，请选择只读。要授予模拟角色读取和修改用户邮箱中项目的权限，请选择完全访问。
6. 在规则下，选择要编辑的规则，然后选择编辑。
7. 此时将显示编辑规则对话框。输入以下信息：
   - 名称 - 编辑规则的名称。
   - （可选）描述 – 更新或输入规则的描述。
   - 在权限下，选择允许以在满足规则中设置的条件时允许访问。要拒绝访问，请选择拒绝。
   - （可选）在此规则：下，选择匹配模拟所选用户的请求以包含特定用户。选择匹配模拟所选用户以外的用户的请求以添加所选用户以外的用户。
8. 选择保存。
9. 选择保存更改。

> **Important**
>
> 更改模拟规则时，受影响的邮箱最多可能需要五分钟才会更新。在规则更新过程中，您可能会发现邮箱中的行为不一致。但是，如果您测试角色，Amazon WorkMail 会根据更新的规则按预期进行响应。有关更多信息，请参阅 测试模拟角色。

测试模拟角色

您可以通过 Amazon WorkMail 控制台测试模拟角色。

测试模拟角色

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

如果需要，可以更改区域。从导航栏中，选择符合您需求的区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

2. 在导航窗格中，选择组织，然后选择组织的名称。
3. 选择模拟角色。
4. 选择要测试的模拟角色。
5. 选择测试角色。
6. 此时将显示测试模拟角色对话框。在目标用户下，选择要为其测试模拟访问权限的用户。
7. 选择测试。

删除模拟角色

您可以通过 Amazon WorkMail 控制台删除模拟角色。

删除模拟角色

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改区域。从导航栏中，选择符合您需求的区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。
2. 在导航窗格中，选择组织，然后选择组织的名称。
3. 选择模拟角色。
4. 选择要删除的模拟角色名称。
5. 选择删除。
6. 此时将显示删除角色对话框。要确认删除，请在对话框中输入角色的名称，然后选择删除。

使用模拟角色

要访问邮箱数据，请使用 Amazon WorkMail API 操作 `AssumeImpersonationRole`。有关 Amazon WorkMail API 的更多详细信息，请参阅 API 参考。

`AssumeImpersonationRole` 会返回一个 `Token`。此 `Token` 必须在 15 分钟内通过 HTTP 标头 `Authorization` 传递到 EWS 协议。

以下示例演示如何将模拟角色与 EWS 协议结合使用。示例中使用的常量指定了您的组织和账户所特有的以下详细信息：

- *WORKMAIL_ORGANIZATION_ID* – Amazon WorkMail 组织 ID
- *IMPERSONATION_ROLE_ID* – 模拟角色 ID
- *WORKMAIL_EWS_URL* – Amazon WorkMail 端点和配额中提供的 EWS 端点
- *EMAIL_ADDRESS* – 用户邮箱的电子邮件地址

Example Java – EWS Java API

```
import software.amazon.awssdk.services.workmail.WorkMailClient;
import software.amazon.awssdk.services.workmail.model.AssumeImpersonationRoleRequest;
import software.amazon.awssdk.services.workmail.model.AssumeImpersonationRoleResponse;

import microsoft.exchange.webservices.data.core.ExchangeService;
import microsoft.exchange.webservices.data.core.enumeration.misc.ExchangeVersion;
import microsoft.exchange.webservices.data.misc.ImpersonatedUserId;
import microsoft.exchange.webservices.data.core.enumeration.misc.ConnectingIdType;

// ...

AssumeImpersonationRoleResponse response = workMailClient.assumeImpersonationRole(
    AssumeImpersonationRoleRequest.builder()
        .organizationId(WORKMAIL_ORGANIZATION_ID)
        .impersonationRoleId(IMPERSONATION_ROLE_ID)
        .build());

ExchangeService exchangeService = new
 ExchangeService(ExchangeVersion.Exchange2010_SP2);
exchangeService.setUrl(URI.create(WORKMAIL_EWS_URL));
exchangeService.getHttpHeaders().put("Authorization", "Bearer " + response.token());
exchangeService.setImpersonatedUserId(new
 ImpersonatedUserId(ConnectingIdType.SmtpAddress, EMAIL_ADDRESS));
```

Example .Net – EWS Managed API

```
using Amazon.WorkMail;
using Amazon.WorkMail.Model;

using Microsoft.Exchange.WebServices.Data;
```

```
// ...

AssumeImpersonationRoleRequest request = new AssumeImpersonationRoleRequest();
request.OrganizationId = WORKMAIL_ORGANIZATION_ID;
request.ImpersonationRoleId = IMPERSONATION_ROLE_ID;
AssumeImpersonationRoleResponse response =
 workMailClient.AssumeImpersonationRole(request);

ExchangeService service = new ExchangeService(ExchangeVersion.Exchange2010_SP2);
service.Url = new Uri(WORKMAIL_EWS_URL);
service.HttpHeaders.Add("Authorization", "Bearer " + response.Token);
service.ImpersonatedUserId = new
 ImpersonatedUserId(ConnectingIdType.SmtpAddress, EMAIL_ADDRESS);
```

Example Python – Exchangelib

```
import boto3

from requests.auth import AuthBase
from exchangelib.transport import AUTH_TYPE_MAP
from exchangelib import Configuration, Account, Version, IMPERSONATION
from exchangelib.version import EXCHANGE_2010_SP2


work_mail_client = boto3.client("workmail")

class ImpersonationRoleAuth(AuthBase):
    def __init__(self):
         self.token = work_mail_client.assume_impersonation_role(
             OrganizationId=WORKMAIL_ORGANIZATION_ID,
             ImpersonationRoleId=IMPERSONATION_ROLE_ID
        )["Token"]

     def __call__(self, r):
         r.headers["Authorization"] = "Bearer " + self.token
         return r

AUTH_TYPE_MAP["ImpersonationRoleAuth"] = ImpersonationRoleAuth

ews_config = Configuration(
     service_endpoint=WORKMAIL_EWS_URL,
     version=Version(build=EXCHANGE_2010_SP2),
     auth_type="ImpersonationRoleAuth"
```

```
)
ews_account = Account(
     config=ews_config,
     primary_smtp_address=EMAIL_ADDRESS,
     access_type=IMPERSONATION
)
```

导出邮箱内容

使用《Amazon WorkMail API 参考》中的 StartMailboxExportJob API 操作将 Amazon WorkMail 邮箱内容导出到 Amazon Simple Storage Service (Amazon S3) 存储桶。此操作会以 MIME 格式将指定邮箱中的所有电子邮件和日历项目导出到 Amazon S3 存储桶中的一个 `.zip` 文件中。不会导出联系人和任务等其他项目。

完成邮箱导出作业所需的时间取决于邮箱中项目的大小和数量。由于邮箱导出作业会持续一段时间，因此它不代表邮箱内容在单个时间点的快照。要查看导出作业的状态，请使用《Amazon WorkMail API 参考》中的 DescribeMailboxExportJob 或 ListMailboxExportJobs API 操作。

邮箱导出作业完成后，将使用您提供的对称 AWS Key Management Service (AWS KMS) 客户主密钥 (CMK) 对 Amazon S3 存储桶中的 `.zip` 文件进行加密。由于 AWS KMS 加密已与 Amazon S3 集成，因此只要用户有权访问 AWS KMS CMK，下载后即可查看解密后的数据。

先决条件

以下是导出邮箱内容的先决条件：

- 编程能力。
- 一个 Amazon WorkMail 管理员账户。
- 一个不允许公有访问的 Amazon S3 存储桶。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的使用 Amazon S3 屏蔽公共访问权限和 Amazon Simple Storage Service 用户指南。
- 一个对称 AWS KMS CMK。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的入门。
- 一个 AWS Identity and Access Management (IAM) 角色，其策略授予写入 Amazon S3 存储桶并使用 AWS KMS CMK 加密已发送文件的权限。有关更多信息，请参阅 Amazon WorkMail 如何与 IAM 结合使用。

IAM 策略示例和角色创建

以下示例显示了一个 IAM 策略，该策略授予写入 Amazon S3 存储桶并使用 AWS KMS CMK 加密已发送文件的权限。要在以下示例：导出邮箱内容过程中使用此示例策略，请将该策略另存为文件名为 `mailbox-export-policy.json` 的 JSON 文件。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:GetBucketPolicyStatus"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:111122223333:key/KEY-ID"
            ],
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "s3.us-east-1.amazonaws.com"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-
demo-bucket/S3-PREFIX*"
                }
            }
        }
    ]
}
```

以下示例显示了一个附加到您创建的 IAM 角色的 IAM 信任策略。要在以下示例：导出邮箱内容过程中使用此示例策略，请将该策略另存为文件名为 mailbox-export-trust-policy.json 的 JSON 文件。

您不必同时使用 aws:SourceArn 和 aws:SourceAccount 条件。例如，如果您需要使用相同的角色从同一 AWS 账户下的不同 Amazon WorkMail 组织导出消息，则可以从该策略中删除 aws:SourceArn。有关条件键的更多信息，请参阅《AWS Identity and Access Management 用户指南》中的 AWS 全局条件上下文键。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "export.workmail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workmail:us-
east-1:111122223333:organization/m-a123b4c5de678fg9h0ij1k2lm234no56"
        }
      }
    }
  ]
}
```

您可以使用 AWS CLI 通过运行以下命令在您的账户中创建 IAM 角色。

```
aws iam create-role --role-name WorkmailMailboxExportRole --assume-role-policy-
document file://mailbox-export-trust-policy.json --region us-east-1
```

```
aws iam put-role-policy --role-name WorkmailMailboxExportRole --policy-
name MailboxExport --policy-document file://mailbox-export-policy.json
```

有关 AWS CLI 的更多信息，请参阅《AWS Command Line Interface 用户指南》。

示例：导出邮箱内容

在上一部分中创建 IAM 角色和策略后，请完成以下步骤导出邮箱内容。您必须拥有 Amazon WorkMail 组织 ID 和用户 ID（实体 ID），您可以在 Amazon WorkMail 控制台中或通过使用 Amazon WorkMail API 访问它们。

示例：导出邮箱内容

1. 使用 AWS CLI 启动邮箱导出作业。

   ```
   aws workmail start-mailbox-export-job --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56 --entity-
   id S-1-1-11-1111111111-2222222222-3333333333-3333 --kms-key-
   arn arn:aws:kms:us-east-1:111122223333:key/KEY-ID --role-arn
    arn:aws:iam::111122223333:role/WorkmailMailboxExportRole --s3-bucket-name amzn-s3-
   demo-bucket --s3-prefix S3-PREFIX
   ```

2. 使用 AWS CLI 监控您的 Amazon WorkMail 组织的邮箱导出作业的状态。

   ```
   aws workmail list-mailbox-export-jobs --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56
   ```

   或者，使用 **start-mailbox-export-job** 命令生成的作业 ID 仅监控该邮箱导出作业的状态。

   ```
   aws workmail describe-mailbox-export-job --organization-id m-
   a123b4c5de678fg9h0ij1k2lm234no56 --job-id JOB-ID
   ```

当邮箱导出作业状态为已完成时，导出的邮箱项目会以 .zip 文件的形式存在于指定的 Amazon S3 存储桶中。

以下是导出邮箱的输出日志示例：

```
{
```

```
  "totalNonExportableItems" : "13",
  "totalMessages" : "76",
  "sha384Hash" : "4de93a***96a1dd",
  "totalBytes" : "161892",
  "totalFolders" : "15",
  "startTime" : "168***380",
  "endTime" : "168***384"
}
```

> **Note**
>
> totalNonExportableItems 是不受支持的项目，如备注和联系人。

注意事项

导出 Amazon WorkMail 的邮箱作业时，请注意以下事项：

- 对于给定的 Amazon WorkMail 组织，您最多可以同时运行 10 个邮箱导出作业。
- 您可以每隔 24 小时为给定邮箱运行一次邮箱导出作业。
- 以下资源必须全部位于同一 AWS 区域中：
  - Amazon WorkMail 组织
  - AWS KMS CMK
  - Amazon S3 存储桶

故障排除

本节中的主题将介绍如何排查 Amazon WorkMail 中的问题。

主题

查看电子邮件标头

电子邮件标头中的信息可帮助您排查常见的用户电子邮件问题。Amazon WorkMail 允许您查看任何邮件的标头信息。

在 Amazon WorkMail 中查看电子邮件标头

1. 在 Amazon WorkMail Web 应用程序中，双击要打开的电子邮件。
2. 选择位于邮件右上角的发送日期旁边的邮件选项（齿轮和信封图标）。

电子邮件标头显示在 Internet Headers (Internet 标头) 下。

邮件路由

如果用户停止接收电子邮件，则说明您的 Amazon WorkMail 组织可能遇到了邮件路由问题。本节中的步骤说明了解决传送和路由问题的常用方法。

入站邮件问题：

- 检查与您的 Amazon WorkMail 组织关联的域的 MX 记录。`WorkMail` 应是唯一的条目，并且应具有最低的优先级。多条 MX 记录可能会导致错误的服务接收消息。有关 MX 记录的更多信息，请参阅验证域。
- 在 Amazon WorkMail 控制台中检查组织的基于域的消息身份验证、报告和一致性 (DMARC) 设置。DMARC 记录用于防范常见的攻击，例如欺骗或网络钓鱼，这些攻击可能会破坏用户的账户凭证。有关 DMARC 的更多信息，请参阅对传入电子邮件执行 DMARC 策略。
- 检查 Amazon Simple Email Service 入站规则。如果该规则包含 Amazon WorkMail 以外的操作，则这些操作可能会失败并导致 Amazon WorkMail 停止接收邮件。有关 Amazon SES 规则的更多信息，请参阅《Amazon Simple Email Service 开发人员指南》中的“与 Amazon WorkMail 集成”操作。

- 在 Amazon WorkMail 中启用邮件跟踪，然后检查日志中是否存在传送问题。有关邮件跟踪的更多信息，请参阅启用电子邮件事件日志记录。

出站邮件问题

- 确保您的 SPF 记录包括 Amazon SES。检查 Amazon WorkMail 控制台中的域页面进行验证。有关 SPF 的更多信息，请参阅使用 SPF 对电子邮件进行身份验证。
- 确保 Amazon WorkMail 有权使用该域。如果没有，请重新添加该域。本指南中的添加域部分提供了相关操作步骤。

在 Amazon WorkMail 中使用电子邮件日志

您可以设置日记，以使用集成的第三方存档和电子数据展示工具来记录您的电子邮件通信。这样可确保您能够遵循用于隐私保护、数据存储和信息保护的电子邮件存储规范规则。

使用日记

Amazon WorkMail 将记录发送给指定组织内任何用户的所有电子邮件以及由该组织内的用户发送的所有电子邮件。所有电子邮件的副本将以 `journal record` 的格式发送到系统管理员指定的地址。此格式与 Microsoft 电子邮件程序兼容。电子邮件日记不产生任何额外费用。

用于电子邮件日志的电子邮件地址有两个，即日志电子邮件地址和报告电子邮件地址。日记电子邮件地址是与您的帐户集成的专用邮箱或第三方设备的地址，日记报告将发往该地址。报告邮箱地址是系统管理员的地址，有关失败日记报告的通知会发往此地址。

所有日志记录均从自动添加到您的域的电子邮件地址发送，该地址如下所示。

```
amazonjournaling@yourorganization.awsapps.com
```

没有与此地址关联的邮箱，您将无法使用此名称或地址创建一个邮箱。

> **Note**
>
> 请勿从 Amazon Simple Service（Amazon Simple Service）控制台中删除以下域记录，否则电子邮件日志功能将停止运行。
>
> ```
> yourorganization.awsapps.com
> ```

每个传入或传出的电子邮件都会生成一条日志记录，与收件人或用户组的数量无关。无法生成日记记录的电子邮件将生成错误通知，该错误通知会发送至报告电子邮件地址。

启用电子邮件日记

1. 打开 Amazon WorkMail 控制台，网址为：https://console.aws.amazon.com/workmail/。

   如果需要，可以更改 AWS 区域。在控制台窗口顶部的栏中，打开选择区域列表，然后选择一个区域。有关更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。

2. 在导航窗格中，选择组织，然后选择贵组织的名称。
3. 在导航窗格中，选择组织设置，选择日志选项卡，然后选择编辑。
4. 将日志状态滑块移至开启位置。
5. 在日志电子邮件地址框中，输入您的电子邮件日志提供商所提供的电子邮件地址。

> **Note**
>
> 我们建议使用专门的日记提供商。

6. 在报告电子邮件地址中，输入电子邮件管理员的地址。
7. 选择保存。更改将立即生效。

文档历史记录

下表描述了《Amazon WorkMail 管理员指南》每次发布时进行的重要更改。要获得本文档的更新通知，您可以订阅 RSS 源。

变更	说明	日期
审计日志记录支持	审计日志可用于监控用户对邮箱的访问、审计是否存在可疑活动，以及调试访问控制和可用性提供商配置。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的启用审计日志记录和 Amazon WorkMail 中的日志记录和监控。	2024 年 3 月 20 日
传输层安全性协议（TLS）支持	Amazon WorkMail 已停止支持传输层安全性协议（TLS）1.0 和 1.1。如果您使用的是 TLS 1.0 或 1.1，则必须将 TLS 版本升级到 1.2。	2023 年 11 月 2 日
远程用户	远程用户是托管在 Amazon WorkMail 组织之外或托管在其他电子邮件域上的 Amazon WorkMail 用户。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的用户。	2023 年 9 月 18 日
以编程方式访问邮箱	Amazon WorkMail 现提供模拟角色，以授予对邮箱的编程访问权限。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的以编程方式访问邮箱。	2022 年 10 月 4 日

在 Amazon WorkMail 上配置自定义可用性提供程序	Amazon WorkMail 支持使用自定义可用性提供程序 (CAP)。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的配置自定义可用性提供程序。	2022 年 6 月 30 日
用于创建组织的控制台发生更改	用于创建组织的 Amazon WorkMail 控制台体验已更新。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的创建组织。	2020 年 10 月 23 日
导出邮箱内容	使用 `StartMailboxExportJob` API 操作将 Amazon WorkMail 邮箱内容导出到 Amazon Simple Storage Service (Amazon S3) 存储桶。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的导出邮箱内容。	2020 年 9 月 22 日
邮箱保留策略	为您的 Amazon WorkMail 组织设置邮箱保留策略，以便在经过选定的时间段后自动删除电子邮件。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的设置邮箱保留策略。	2020 年 5 月 28 日
同步和异步运行 Lambda 操作	在 Amazon WorkMail 电子邮件流规则中为运行 Lambda 操作选择同步或异步配置。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的为 Amazon WorkMail 配置 AWS Lambda。	2020 年 5 月 11 日

使用访问控制规则	访问控制规则允许 Amazon WorkMail 管理员控制其组织的邮箱的访问方式。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的使用访问控制规则。	2020 年 2 月 12 日
标记组织	标记 Amazon WorkMail 组织以区分 AWS 账单与成本管理控制台中的各个组织，或控制对组织资源的访问。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的标记组织。	2020 年 1 月 23 日
对传入电子邮件执行 DMARC 策略	有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的对传入电子邮件执行 DMARC 策略。	2019 年 10 月 17 日
使用 Lambda 检索消息内容	将 Amazon WorkMail Message Flow API 与 AWS Lambda 结合使用以检索消息内容。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的使用 Lambda 检索消息内容。	2019 年 9 月 12 日
记录 Amazon WorkMail 电子邮件事件	在 Amazon WorkMail 控制台中启用电子邮件事件日志记录以跟踪您组织的电子邮件。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的跟踪电子邮件。	2019 年 5 月 13 日

Route 53 DNS 记录插入	在设置托管于 Route 53 公共托管区的域时，Amazon WorkMail 会自动为您插入 DNS 记录。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的添加域。	2019 年 2 月 13 日
针对入站电子邮件路由规则操作配置 Lambda	Amazon WorkMail 支持配置 Lambda 函数以与入站电子邮件流规则结合使用。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的管理电子邮件流。	2019 年 1 月 24 日
为 Amazon WorkMail 配置 Lambda	Amazon WorkMail 支持配置 Lambda 函数以与出站电子邮件流规则结合使用。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的为 Amazon WorkMail 配置 Lambda。	2018 年 11 月 19 日
SMTP 路由选择	Amazon WorkMail 支持配置 SMTP 网关以与出站电子邮件流规则结合使用。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的配置 SMTP 网关。	2018 年 11 月 1 日
用于自定义域的调试工具	Amazon WorkMail 已添加用于自定义域的调试工具。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的添加域。	2018 年 10 月 15 日

支持 Outlook 2019	Amazon WorkMail 支持 Outlook 2019 for Windows 和 Outlook 2019 for macOS。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的 Amazon WorkMail 系统要求。	2018 年 10 月 1 日
各种更新	主题布局和组织的各种更新。	2018 年 7 月 12 日
邮箱权限	您可以使用 Amazon WorkMail 中的邮箱权限向用户或组授予在其他用户的邮箱中工作的权利。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的使用邮箱权限。	2018 年 4 月 9 日
支持 AWS CloudTrail	Amazon WorkMail 已与 AWS CloudTrail 集成。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的使用 AWS CloudTrail 记录 Amazon WorkMail API 调用。	2017 年 12 月 12 日
支持电子邮件流	您可以设置电子邮件流规则以根据发件人的电子邮件地址或域处理传入电子邮件。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的管理电子邮件流。	2017 年 7 月 5 日
快速设置功能更新	现在，快速设置功能可为您创建一个 Amazon WorkMail 目录。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的使用快速设置功能设置 Amazon WorkMail。	2017 年 5 月 10 日

支持更广泛的电子邮件客户端	现在，您可以将 Amazon WorkMail 与 Microsoft Outlook 2016 for Mac 和 IMAP 电子邮件客户端结合使用。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的 Amazon WorkMail 的系统要求。	2017 年 1 月 9 日
支持 SMTP 日记	您可以设置日记来记录电子邮件通信。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的将电子邮件日记与 Amazon WorkMail 结合使用。	2016 年 11 月 25 日
支持将电子邮件重定向至外部电子邮件地址	可通过更新域的 Amazon SES 身份策略来设置电子邮件重定向规则。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的编辑域身份策略。	2016 年 10 月 26 日
支持互操作性	您可以在 Amazon WorkMail 与 Microsoft Exchange 之间启用互操作性。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的 Amazon WorkMail 与 Microsoft Exchange 之间的互操作性。	2016 年 10 月 25 日
公开发行版	Amazon WorkMail 的公开发行版本。	2016 年 1 月 4 日
支持预留资源	支持预留资源，如会议室和设备。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的使用资源。	2015 年 10 月 19 日

支持电子邮件迁移工具	支持电子邮件迁移工具。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的迁移到 Amazon WorkMail。	2015 年 8 月 16 日
Amazon WorkMail 预览版	Amazon WorkMail 预览版。	2015 年 1 月 28 日