aws

管理指南

Amazon Chime

Amazon Chime: 管理指南

Table of Contents

..... vii
什么是 Amazon Chime？ 1
管理概述 1
如何开始 1
定价 1
资源 1
Amazon Chime 系统管理员的先决条件 3
创建 Amazon Web Services 账户 3
注册获取 AWS 账户 3
创建具有管理访问权限的用户 3
开始使用 5
步骤 1：创建 Amazon Chime 管理员账户 5
步骤 2（可选）：配置账户设置 5
第 3 步：将用户添加到账户 6
（可选）为您的 Amazon Chime 账户设置电话号码 7
管理账户 8
选择团队账户或企业账户 8
申请域 9
将团队账户转换为企业账户 10
重命名账户 11
删除账户 11
管理会议设置 13
会议策略设置 13
会议应用程序设置 13
会议区域设置 13
管理聊天保留策略 14
留存策略如何影响 Amazon Chime 用户 14
打开聊天保留 16
恢复聊天消息 17
删除聊天消息 18
连接到 Active Directory 18
先决条件 19
连接到 Amazon Chime 中的 Active Directory 19
配置多个电子邮件地址 20

连接到 Okta SSO 21
部署适用于 Outlook 的插件 24
设置适用于 Slack 的 Amazon Chime Meetings 应用程序 24
在组织中安装适用于 Slack 的 Amazon Chime Meetings 应用程序 25
在工作区上安装适用于 Slack 的 Amazon Chime Meetings 应用程序 26
将工作区迁入组织 26
将工作区关联至 Amazon Chime 团队账户 26
管理用户 29
添加用户 29
查看用户详细信息 30
管理用户权限和访问权限 32
管理用户权限 32
管理用户访问权限 33
更改个人会议 PIN 35
管理 Pro 试用 35
请求用户附件 36
Amazon Chime 如何管理自动更新 37
将用户迁移到另一个团队账户 37
管理电话号码 39
预置电话号码 39
转网现有电话号码 40
移植号码的先决条件 41
正在移植电话号码 41
提交所需文件 43
查看请求状态 43
分配端口号 44
移植电话号码 44
电话号码转网状态定义 46
分配电话号码 47
取消分配电话号码 47
使用出站呼叫名称 48
删除电话号码 49
还原已删除的电话号码 49
管理全局设置 50
配置呼叫详细信息记录 50
Amazon Chime Business Calling 的呼叫详细信息记录 51

会议室配置 52
加入有人监管的会议 52
兼容的 VTC 设备 53
网络配置和带宽要求 54
查看报告 57
扩展 Amazon Chime 桌面客户端 58
用户管理 58
邀请多个用户 58
下载用户列表 59
注销多个用户 59
更新用户个人 PIN 60
集成聊天机器人 60
将聊天机器人与 Amazon Chime 配合使用 61
发送给聊天机器人的 Amazon Chime 事件 69
创建 Webhook 71
排查 Webhook 错误 72
管理支持 73
安全性 74
Identity and Access Management 75
受众 75
使用身份进行身份验证 75
使用策略管理访问 78
Amazon Chime 如何与 IAM 配合使用 80
Amazon Chime 基于身份的策略 80
资源 81
示例 81
防止跨服务混淆代理 81
Amazon Chime 基于资源的策略 82
基于 Amazon Chime 标签的授权 82
Amazon Chime IAM 角色 82
结合使用临时凭证和 Amazon Chime 82
服务相关角色 83
服务角色 83
基于身份的策略示例 83
策略最佳实践 84
使用 Amazon Chime 控制台 84

允许用户完全访问 Amazon Chime 85
允许用户查看他们自己的权限 86
允许用户访问用户管理操作 87
AWS 托管策略： AmazonChimeVoiceConnectorServiceLinkedRolePolicy 89
Amazon Chime 更新了托管政策 AWS 89
故障排除 90
我无权在 Amazon Chime 中执行操作 90
我无权执行 iam：PassRole 91
我想允许 AWS 账户之外的用户访问我的 Amazon Chime 资源 91
使用服务相关角色 92
将角色与共享设备结合使用 92
使用具有实时转录功能的角色 94
通过媒体管道使用角色 96
日志记录和监控 98
使用 CloudWatch 进行监控 99
使用 EventBridge 自动执行 109
记录服务 API 调用 114
合规性验证 116
弹性 117
基础设施安全性 118
了解 Amazon Chime 自动更新 118
文档历史记录 120

要完成本指南中的步骤，您必须是 Amazon Chime 系统管理员。如需 Amazon Chime 桌面客户端、网络应用程序或移动应用程序方面的帮助，请参阅《Amazon Chime 用户指南》中的获取支持。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。

什么是 Amazon Chime？

Amazon Chime 是一项通信服务，通过安全且全面的应用程序转换在线会议。Amazon Chime 能够无缝接入各种设备，让您时刻保持连接。您可以使用 Amazon Chime 进行在线会议、视频会议、呼叫和聊天。也可以在组织内外部共享内容。Amazon Chime 是一项在 AWS 云上安全运行的完全托管服务，让 IT 部门无需部署和管理复杂的基础设施。

有关更多信息，请参阅 Amazon Chime。

管理概述

作为管理员，您可以使用 Amazon Chime 控制台执行关键任务，例如创建 Amazon Chime 账户以及管理用户和权限。要访问 Amazon Chime 控制台并创建 Amazon Chime 管理员账户，请先创建 AWS 账户。有关更多信息，请参阅Amazon Chime 系统管理员的先决条件。

如何开始

完成 Amazon Chime 系统管理员的先决条件 即可创建并配置 Amazon Chime 管理账户，然后添加用户。为您的用户选择高级或基本权限。

如果您已准备好立即开始使用，请参阅以下教程：

- 开始使用

有关用户访问和权限的更多信息，请参阅管理用户权限和访问权限。有关具有高级和基本权限的用户所能访问功能的更多信息，请参阅方案与定价。

定价

Amazon Chime 提供基于使用率的定价模式。您只需为举办会议的高级权限用户且仅按照所举办会议的天数付费。不向会议参加者和聊天用户收取费用。

具有基本权限的用户不会产生费用。基本用户无法主持会议，但他们可以参加会议并使用聊天。有关定价以及具有高级和基本权限的用户所能访问功能的更多信息，请参阅方案与定价。

资源

有关 Amazon Chime 的更多信息，请参阅以下资源：

- Amazon Chime 帮助中心
- Amazon Chime 培训视频

Amazon Chime 系统管理员的先决条件

您必须拥有一个 AWS 账户才能访问 Amazon Chime 控制台并创建 Amazon Chime 管理员账户。

创建 Amazon Web Services 账户

您必须先创建 AWS 账户，才能创建 Amazon Chime 管理员账户。

主题

- 注册获取 AWS 账户
- 创建具有管理访问权限的用户

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

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

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为安全最佳实践，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。

AWS 注册过程完成后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

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS Management Console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》中的以根用户身份登录。
2. 为您的根用户启用多重身份验证 (MFA)。

   有关说明，请参阅 I A M 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》中的启用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，为用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

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。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

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》中的创建权限集。
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》中的添加组。

有关设置 Amazon Chime 管理员账户的更多信息，请参阅 开始使用。

开始使用

Amazon Chime 入门的最简单方法就是下载支持 30 天免费试用的 Amazon Chime Pro 版本。有关更多信息，请参阅下载 Amazon Chime。

购买 Amazon Chime

如需在 30 天免费试用期结束后继续使用 Amazon Chime Pro 版本，则必须创建 Amazon Chime 管理员账户并添加用户。要开始使用，您必须先完成Amazon Chime 系统管理员的先决条件，其中包括创建 AWS 账户。然后，您可以通过完成以下任务，创建并配置 Amazon Chime 管理员账户并添加用户。

任务

- 步骤 1：创建 Amazon Chime 管理员账户
- 步骤 2（可选）：配置账户设置
- 第 3 步：将用户添加到账户
- （可选）为您的 Amazon Chime 账户设置电话号码

步骤 1：创建 Amazon Chime 管理员账户

完成 Amazon Chime 系统管理员的先决条件 后，即可创建 Amazon Chime 管理员账户。

创建 Amazon Chime 管理员账户

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在账户页面上，选择新建账户。
3. 对于账户名称，输入账户名称，然后选择创建账户。
4. （可选）选择是允许 Amazon Chime 在所有可用区域中选出最佳的 AWS 会议区域，还是仅使用您选择的区域。有关更多信息，请参阅管理会议设置。

步骤 2（可选）：配置账户设置

默认情况下，新账户将作为团队账户创建。如果您选择申请域并连接到自己的身份提供者，或选择使用 Okta SSO，则可以将此账户转换为企业账户。有关团队和企业账户类型的更多信息，请参阅选择使用 Amazon Chime 的团队账户或企业账户。

将团队账户转换为企业账户

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 对于账户，选择账户的名称。
3. 对于 Identity (身份)，选择 Getting Started (开始使用)。
4. 按照控制台中的步骤，申请您的域名。
5. （可选）按照控制台中的步骤设置身份提供程序并配置目录组。

有关申请域的更多信息，请参阅申请域。有关设置身份提供商的更多信息，请参阅 连接到 Active Directory 和 连接到 Okta SSO。

您也可以允许使用或停止使用账户策略选项，例如远程控制共享屏幕和 Amazon Chime 的“给我打电话”特征。

配置账户策略

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在 Accounts (账户) 页面上，选择要配置账户的名称。
3. 对于 Settings (设置)，选择 Meetings (会议)。
4. 对于 Policies (策略)，选择或清除要允许或停止允许的账户策略选项。
5. 选择 Change (更改)。

有关更多信息，请参阅管理会议设置。

第 3 步：将用户添加到账户

创建 Amazon Chime 团队账户之后，邀请您和您的用户加入。如果您要将账户升级到企业账户，则无需邀请用户。而是改为升级到企业账户并申请您的域。有关更多信息，请参阅步骤 2（可选）：配置账户设置。

添加用户到 Amazon Chime 账户

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在 Accounts (账户) 页面上，选择您的账户名称。
3. 在 Users (用户) 页面上，选择 Invite users (邀请用户)。
4. 输入要邀请用户的电子邮件地址（包括您自己），然后选择 Invite users (邀请用户)。

受邀用户会收到一封电子邀请函，邀请其加入您创建的 Amazon Chime 团队账户。在用户注册 Amazon Chime 用户账户时，默认获得高级权限，同时 30 天免费试用期结束。如果用户已使用其工作电子邮件地址注册 Amazon Chime 用户账户，则可以继续使用账户。用户还可以选择下载 Amazon Chime 并登录用户账户，以随时下载 Amazon Chime 客户端应用程序。

您只需为具有高级权限的用户在他们主持会议时支付费用。具有基本权限的用户不会产生费用。基本用户无法主持会议，但他们可以参加会议并使用聊天。有关定价和具有 Pro 版和 Basic 版权限的用户可访问的特征的更多信息，请参阅计划和定价。

更改用户权限

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在 Accounts (账户) 页面上，选择您的账户名称。
3. 在 Users (用户) 页面中，选择要更改权限的用户。
4. 依次选择 User actions (用户操作)、Assign user permission (分配用户权限)。
5. 对于 Permissions (权限)，选择 Pro (高级) 或 Basic (基本)。
6. 选择 Assign (分配)。

您可以向其他用户提供管理员权限，同时控制他们对您账户的 Amazon Chime 控制台的访问权限。有关更多信息，请参阅适用于 Amazon Chime 的身份和访问管理。

（可选）为您的 Amazon Chime 账户设置电话号码

Amazon Chime 管理账户可使用以下电话选项：

Amazon Chime Business Calling

用户可以直接从 Amazon Chime 收发电话和短信。可以在 Amazon Chime 控制台中预置您的电话号码或输入现有电话号码。为 Amazon Chime 用户分配电话号码，并授予其使用 Amazon Chime 收发电话和短信的权限。有关更多信息，请参阅 管理 Amazon Chime 中的电话号码 和 转网现有电话号码：

Amazon Chime Voice Connector

为现有电话系统提供 SIP 中继服务。在 Amazon Chime 控制台中输入现有电话号码或预置新电话号码。有关更多信息，请参阅《Amazon Chime SDK 管理指南》中的管理 Amazon Chime Voice Connector。

管理您的 Amazon Chime 账户

您可以以单个用户或没有管理员的组的身份使用 Amazon Chime。但如需添加管理员功能或购买 Amazon Chime Pro 版本，则必须在 AWS Management Console中创建 Amazon Chime 账户。如需了解 Amazon Chime 管理员账户的创建流程，或了解有关购买 Amazon Chime Pro 版本的更多信息，请参阅 开始使用。

有关不同类型的 Amazon Chime 管理员账户的更多信息，请参阅 选择使用 Amazon Chime 的团队账户或企业账户。有关管理现有管理员账户的更多信息，请参阅以下主题。

主题

- 选择使用 Amazon Chime 的团队账户或企业账户
- 申请域
- 将团队账户转换为企业账户
- 重命名账户
- 删除账户
- 管理会议设置
- 管理聊天保留策略
- 恢复聊天消息
- 删除聊天消息
- 连接到 Active Directory
- 连接到 Okta SSO
- 部署适用于 Outlook 的 Amazon Chime 插件
- 设置适用于 Slack 的 Amazon Chime Meetings 应用程序

选择使用 Amazon Chime 的团队账户或企业账户

创建 Amazon Chime 管理员账户时，您可以选择创建团队账户或企业账户。有关创建 Amazon Chime 管理员账户的更多信息，请参阅 开始使用。

团队账户

如果创建团队账户，您可以邀请用户并授予其使用 Amazon Chime Pro 版本的权限，而无需申请电子邮件域。有关 Pro 版和 Basic 版权限的更多信息，请参阅计划和定价。

您可以邀请来自尚未经过其他组织申请的任何电子邮件域的用户。您只在用户主持会议时为用户付费。团队账户中的用户可以使用 Amazon Chime 应用程序，搜索并联系注册同一账户的其他 Amazon Chime 用户。亚马逊建议您使用团队账户为组织以外的 Pro 版用户付费。

企业账户

如果创建企业账户，您可以更好地控制组织域中的用户。您可以连接自己的身份提供者或 Okta SSO 进行身份验证并分配 Pro 版或 Basic 版的权限。Amazon Chime 还支持 Microsoft Active Directory。

如需创建企业账户，您必须申请至少一个电子邮件域。这样才能确保在您集中管理的 Amazon Chime 账户中，加入通过申请域登录 Amazon Chime 的所有用户。使用支持的目录集成管理用户时，必须使用企业账户。有关更多信息，请参阅 申请域 和 连接到 Active Directory。

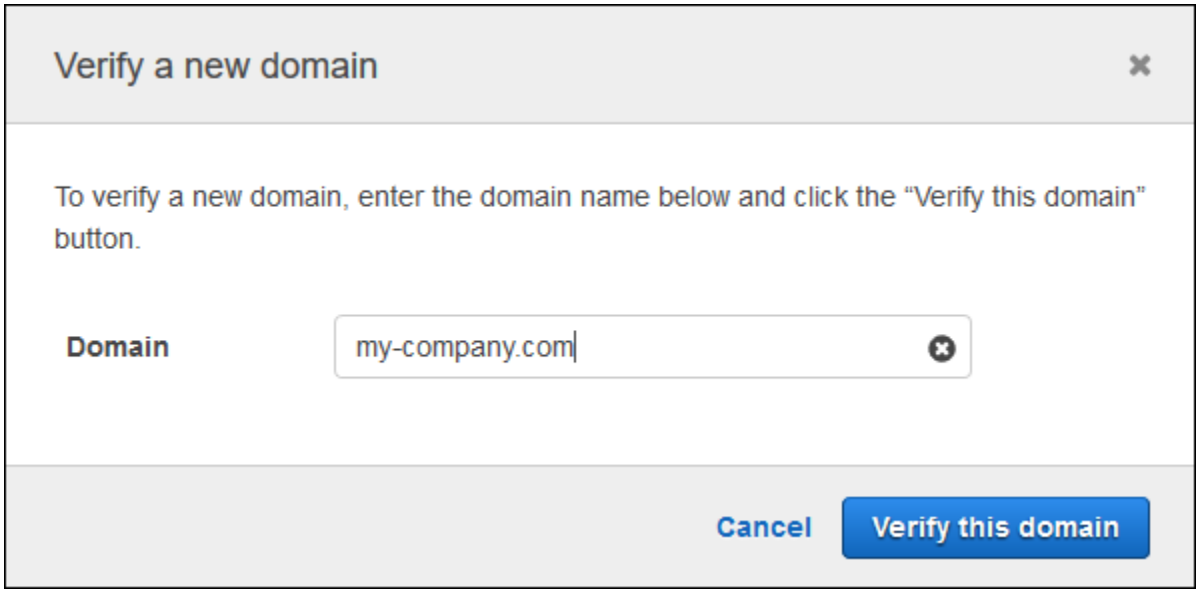
您还可以在企业账户中管理用户激活和暂停操作。有关更多信息，请参阅 管理用户权限和访问权限。

申请域

要创建企业账户并从它提供的对账户和用户的更强控制中受益，您必须至少申请一个电子邮件域。

申请域

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在 Accounts (账户) 页面上，选择团队账户的名称。
3. 在导航窗格中，依次选择 Identity (标识) 和 Domains (域)。
4. 在 Domains (域) 页面上，选择 Claim a new domain (申请新域)。
5. 对于 Domain (域)，键入您的组织用于电子邮件地址的域。选择 Verify this domain (验证此域)。



6. 按照屏幕上的说明将 TXT 记录添加到您的域的 DNS 服务器。此流程一般涉及登录域中的账户、查找域的 DNS 记录，以及使用 Amazon Chime 提供的名称和值添加 TXT 记录。有关更新您的域的 DNS 记录的更多信息，请参阅您的 DNS 提供商或域名注册商的文档。

   Amazon Chime 会检查此记录是否存在，以确认此域属于您。验证域后，其状态会从 Pending verification (等待验证) 更改为 Verified (已验证)。

   > **Note**
   >
   > Amazon Chime 最多可能需要 24 小时才能传播完 DNS 更改和验证。

7. 如果您的组织对电子邮件地址使用其他域或子域，请对每个域重复此过程。

有关域注册疑难解答的更多信息，请参阅 为什么我的域注册请求未获得验证？。

将团队账户转换为企业账户

如需将现有的团队账户转换为企业账户，请在 Amazon Chime 控制台中申请一个或多个电子邮件域。有关团队账户与企业账户差异的更多信息，请参阅 选择使用 Amazon Chime 的团队账户或企业账户。有关申请域的更多信息，请参阅 申请域。

将团队账户转换为企业账户

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 对于账户，选择账户的名称。
3. 对于 Identity (身份)，选择 Getting Started (开始使用)。
4. 按照控制台中的步骤，申请您的域名。
5. （可选）按照控制台中的步骤设置身份提供程序并配置目录组。

将您的账户转换为企业账户后，您可以决定是否通过连接 Active Directory 实例 AWS Directory Service。连接到 Active Directory 实例后，用户可通过 Active Directory 凭证登录 Amazon Chime。有关更多信息，请参阅 连接到 Active Directory。

如果未能连接到 Active Directory 实例，则用户可通过 Login with Amazon (LWA) 或 Amazon.com 账户凭证登录 Amazon Chime。

重命名账户

以下步骤说明了如何重命名您管理的 Amazon Chime 团队和企业账户。您选择的姓名会出现在邀请用户加入 Amazon Chime 的电子邮件中。

重命名账户

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。

   默认情况下会显示 “帐户” 页面。
2. 在账户名称列中，选择要重命名的账户。
3. 在左侧窗格的设置下，选择账户。

   此时显示账户摘要页面。
4. 打开账户操作列表，然后选择重命名账户。

   此时显示重命名账户对话框。
5. 输入新的账户名并选择保存。

删除账户

如果您在中删除 AWS 账户 AWS Management Console，则会自动删除您的 Amazon Chime 账户。或者，您可以在 Amazon Chime 控制台中删除团队账户或企业账户。

> **Note**
>
> 未在团队或企业账户中托管的用户可以运行 Amazon Chime Assistant 的“删除我本人”命令来请求删除。有关更多信息，请参阅使用 Amazon Chime Assistant。

删除团队账户

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在 Account name (账户名称) 列中选择账户，然后在 Settings (设置) 下选择 Account (账户)。
3. 在导航窗格中，Users (用户) 页面将显示。
4. 选择用户，然后依次选择 User actions (用户操作)、Remove user(删除用户)。

5. 在导航窗格中，依次选择 Accounts (账户)、Account actions (账户操作) 和 Delete account (删除账户)。
6. 确认您要删除账户。

Amazon Chime 在您删除账户的同时会删除所有用户数据。这包括终止 AWS 账户、个人 Amazon Chime 账户或非托管的 Amazon Chime 用户。但不包括由 Amazon Chime 生成的有关用户账户和 Amazon Chime 使用情况（客户协议规定的服务属性）的非内容数据。

删除企业账户

1. 删除域。

> **Note**
>
> 删除域时，会发生以下情况：
>
> - 与该域关联的用户会立即从所有设备中注销，并失去对所有联系人、聊天对话和聊天室的访问权限。
> - 此域中的用户安排的会议不再开始。
> - 已暂停的用户在用户和用户详细信息页面上继续显示为已暂停状态，并且无法访问其数据。这些用户不能使用其电子邮件地址新建 Amazon Chime 账户。
> - 注册用户在用户和用户详细信息页面上显示为已释放状态，并且无法访问其数据。这些用户可以使用其电子邮件地址新建 Amazon Chime 账户。
> - 如果您拥有 Active Directory 账户，并删除了与用户主要电子邮件地址关联的域，则 Amazon Chime 将拒绝用户访问并删除相关的配置文件。如果您删除了与用户辅助电子邮件地址关联的域，则用户无法通过此电子邮件地址登录，但仍能访问保留在 Amazon Chime 中的联系人和数据。
> - 如果您拥有 OpenID Connect (OIDC) 企业账户，并删除了与用户主要电子邮件地址关联的域，则 Amazon Chime 将始终拒绝用户访问并删除相关的配置文件。

2. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
3. 在 Accounts (账户) 页面上，选择团队账户的名称。
4. 在导航窗格中，选择 Settings (设置)、Domains (域)。
5. 在 Domains (域) 页面上，选择 Remove domain (删除域)。
6. 在导航窗格中，依次选择 Accounts (账户)、Account actions (账户操作) 和 Delete account (删除账户)。

7. 确认您要删除账户。

Amazon Chime 在您删除账户的同时会删除所有用户数据。这包括终止 AWS 账户、个人 Amazon Chime 账户或非托管的 Amazon Chime 用户。但不包括由 Amazon Chime 生成的有关用户账户和 Amazon Chime 使用情况（客户协议规定的服务属性）的非内容数据。

管理会议设置

在 Amazon Chime 控制台中管理会议设置。

会议策略设置

在 Amazon Chime 控制台的设置和会议项下，管理账户策略。从以下策略选项中进行选择。

在屏幕共享中启用共享控制

选择组织中的用户是否可以在会议期间授予对其计算机的共享控制权。请求对用户计算机进行共享控制的与会者将收到一条错误消息，指示远程控制不可用。

启用出站呼叫以加入会议

开启 Amazon Chime 的“给我打电话”功能。与会者可选择接听来自 Amazon Chime 的电话呼叫，以加入会议。

会议应用程序设置

在 Amazon Chime 控制台的设置和会议项下，管理会议应用程序的访问权限。可以选择以下选项：

允许用户通过适用于 Slack 的 Amazon Chime Meetings 应用程序登录 Amazon Chime

此选项允许组织中的用户通过适用于 Slack 的 Amazon Chime Meetings 应用程序登录 Amazon Chime。有关更多信息，请参阅 设置适用于 Slack 的 Amazon Chime Meetings 应用程序。

会议区域设置

为了提高会议质量和减少延迟，Amazon Chime 在最适合所有参与者的 AWS 区域处理会议。由您决定 Amazon Chime 是从所有可用区域中选择最佳区域还是使用您选择的区域作为会议室。

您可以随时从您账户的 Meetings (会议) 设置更新此设置。在会议设置中，您还可以查看各区域正在召开的 Amazon Chime 会议的百分比。

更新会议区域设置

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在 Accounts (账户) 页面上，选择您的账户名称。
3. 在导航窗格中，选择 Settings (设置)、Meetings (会议)。
4. 对于 Regions (区域)，选择以下选项之一：
   - 使用所有可用区域以确保会议质量：允许 Amazon Chime 优化您的会议质量。
   - 仅使用我选择的区域：允许在下拉菜单中选择区域。
5. 选择保存。

管理聊天保留策略

在管理一个或多个 Amazon Chime 企业账户时，可以为以下内容设置聊天留存策略：

- 仅包含企业账户成员的聊天对话。
- 由企业账户成员创建的聊天室。

保留策略会根据您设置的时间段自动删除消息。您可以将持续时间段设置为一天到 15 年。

> **Note**
>
> Amazon Chime 企业账户的留存期为 90 天。此策略适用于涉及账户用户和非账户用户的对话。
> 保留策略不适用于以下情况：
>
> - 不包括任何 Amazon Chime 企业账户成员的聊天对话
> - 由不属于 Amazon Chime 企业账户的用户创建的聊天室

留存策略如何影响 Amazon Chime 用户

由企业账户管理员设置的留存策略对 Amazon Chime 用户的影响程度不同，具体取决于用户是属于相同的企业账户、不同的企业账户，还是属于团队账户，或者取决于用户是否不属于任何账户。

企业成员聊天对话

下表显示了保留策略如何影响企业账户成员的聊天对话。

如果聊天对话包括...	保留策略是...
仅用户的企业账户的其他成员	由用户的管理员设置
用户的企业账户之外的任何人	自动设置为 90 天

企业会员聊天室

下表显示了保留策略如何影响企业账户成员的聊天室。

如果聊天室的创建人是...	保留策略是...
用户的企业账户的成员	由用户的管理员设置
另一个企业账户的成员	由其他账户的管理员设置
非企业账户成员	不适用

团队成员聊天对话

下表显示了保留策略如何影响团队账户成员的聊天对话。

如果聊天对话包括...	保留策略是...
仅包括不是企业账户成员的用户	不适用
企业账户的至少一个成员	自动设置为 90 天

团队成员聊天室

下表显示了保留策略如何影响团队账户成员的聊天室。

如果聊天室的创建人是...	保留策略是...
团队账户用户	不适用

如果聊天室的创建人是...	保留策略是...
不属于企业账户的任何人	不适用
企业账户的成员	由企业账户的管理员设置

不属于企业账户或团队账户的 Amazon Chime 用户只需遵守适用于企业账户成员创建的聊天室的聊天室留存策略。

与不属于企业或团队账户的接收人进行的聊天对话

下表显示了留存策略如何影响不属于 Amazon Chime 企业账户或团队账户的用户的聊天对话。

如果聊天对话包括...	保留策略是...
仅包括不是企业账户成员的用户	不适用
企业账户的至少一个成员	自动设置为 90 天

由不属于企业或团队账户的用户创建的聊天室

下表显示了留存策略如何影响不属于 Amazon Chime 企业账户或团队账户的用户的聊天室。

如果聊天室的创建人是...	保留策略是...
不属于企业或团队账户的用户	不适用
团队账户用户	不适用
企业账户的成员	由企业账户的管理员设置

打开聊天保留

Amazon Chime 企业账户管理员可以使用 Amazon Chime 控制台，为账户中的聊天对话和聊天室启用聊天留存功能。您也可以随时使用控制台更新聊天保留期或关闭聊天保留。

打开聊天保留

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在 Accounts (账户) 页面上，选择账户的名称。
3. 在导航窗格的 “设置” 下，选择 “保留”。
4. 在 “保留” 页面的 “聊天对话保留” 下，将滑块移至 “开”。
5. 在 “保留期” 下，在第一个框中输入一个数字，然后打开该框旁边的列表并选择 “天”、“周” 或 “年”。
6. 在 “聊天室保留” 下，重复步骤 4-5。完成后，选择保存。

在设置保留期后的一天内，您账户中的用户将无法访问在保留期之外发送的消息。

恢复聊天消息

> **Note**
>
> 要完成这些步骤，您必须是 Amazon Chime Enterprise 账户管理员。

您可以在设置聊天保留期后 30 天内恢复聊天消息。恢复聊天消息时，即恢复您的 Amazon Chime 账户中所有用户发送的所有消息。

在这 30 天内，您可以执行以下任一操作来恢复邮件：

- 使用 Amazon Chime 控制台关闭数据保留。

  -或-

- 延长保留期。

30 天宽限期过后，所有属于保留期的聊天消息都将被永久删除。新的聊天消息一过保留期就会被永久删除。

有关设置或更改保留期的信息打开聊天保留，请参阅本节前面的。

当您或账户成员执行以下任一操作时，聊天消息也会从 Amazon Chime 中永久删除：

- 删除 Amazon Chime 聊天室。有关删除聊天室的更多信息，请参阅 Amazon Chime 用户指南中的删除聊天室。

- 结束有聊天消息的 Amazon Chime 会议。

> **Note**
>
> 根据需要，您可以手动复制和保存会议中的聊天消息，但必须在会议结束前这样做。有关更多信息，请参阅 Amazon Chime 用户指南中的使用会议中聊天。

删除聊天消息

为了遵守数据保留政策，Amazon Chime 会保留所有聊天消息，并防止最终用户删除他们发送的消息。但是，Amazon Chime 系统管理员可以使用两个 API 从对话和聊天室中删除单个消息。消息必须存放在管理员的 Amazon Chime 账户中。

用户可以通过向您发送消息 ID 和相应的对话或聊天室 ID 来请求删除消息。Amazon Chime 用户指南中的使用聊天功能主题说明了如何使用聊天功能。

收到删除请求时，您可以编写代码或使用 AWS CLI 调用以下 API。

删除消息

- 请执行以下操作之一：
  - 对于对话消息-使用 RedactConversationMessageAPI。

    在 CLI 中，运行以下命令：

    ```
    aws chime redact-conversation-message --conversation-id id_string --message-id id_string
    ```
  - 对于聊天室消息-使用 RedactRoomMessageAPI。

    在 CLI 中，运行以下命令：

    ```
    aws chime redact-room-message --room-id id_string --message-id id_string
    ```

连接到 Active Directory

在将 Amazon Chime 管理账户连接到 Active Directory 时，您可以从以下功能中受益：

- Amazon Chime 用户可通过自己的 Active Directory 凭证登录。
- Amazon Chime 管理员可选择要添加的凭证安全功能，包括密码轮换、密码复杂性规则和多重身份验证。
- 用户的 Active Directory 账户和 Amazon Chime 账户会同时删除。
- 您可以指定获得 Amazon Chime Pro 版本权限的 Active Directory 组。
  - 可将多个组配置为接收 Basic 权限或 Pro 权限。
  - 用户必须是任意一组的成员，才能登陆 Amazon Chime。
  - 两个组的用户都会收到 Pro 许可证。

有关管理用户权限的更多信息，请参阅 管理用户权限和访问权限。

先决条件

您必须先满足以下先决条件，才能连接到 Amazon Chime 中的 Active Directory：

- 确保您拥有配置域、活动目录和目录组的正确 AWS Identity and Access Management 权限。有关更多信息，请参阅 适用于 Amazon Chime 的身份和访问管理。
- 使用 AWS Directory Service 在美国东部（弗吉尼亚北部）区域配置的目录创建目录。有关更多信息，请参阅 AWS Directory Service 管理指南。Amazon Chime 可通过 AD Connector、Microsoft AD 或 Simple AD 进行连接。
- 申请域的目的是创建 Amazon Chime 企业账户，或将现有的团队账户转换为企业账户。如果用户在多个域中设有工作电子邮件地址，请务必申请所有这些域。有关更多信息，请参阅 申请域 和 将团队账户转换为企业账户。

连接到 Amazon Chime 中的 Active Directory

在将 Active Directory 连接到 Amazon Chime 后，用户会在使用您在 Amazon Chime 企业账户中申请的域的某个电子邮件地址时，收到需要使用目录凭证登录的提示。

连接到 Amazon Chime 中的 Active Directory

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 对于身份，在导航窗格中选择 Active directory。
3. 对于云端目录 ID，选择要用于 Amazon Chime 的 AWS Directory Service 目录，然后选择 Connect。

> **Note**
>
> 您可以使用 AWS Directory Service 控制台查找目录 ID。

4. 连接目录后，选择添加新组。
5. 对于组，输入组名称。名称必须与目标目录中的 Active Directory 组完全匹配。不支持 Active Directory 组织单位 (OU)。
6. 对于权限，选择 Basic 版或 Pro 版。
7. 选择 Add Group (添加组)。
8. （可选）重复此程序以创建其他目录组。

配置多个电子邮件地址

在连接到 Amazon Chime 中的 Active Directory 后，用户可通过自己的 Active Directory 凭证登录 Amazon Chime。您可以在 Active Directory 中为用户分配多个电子邮件地址。如需允许用户使用其 Active Directory 凭证登录 Amazon Chime，您必须在 Amazon Chime 管理账户中申请每个适用的电子邮件域。有关更多信息，请参阅 申请域。

> **Note**
>
> 如果用户试图通过未经申请的域的电子邮件地址登录，则会收到执行 Login with Amazon 的登录提示。用户使用未经申请的域的电子邮件地址无法登录管理账户。

在 Amazon Chime 控制台中查看用户详细信息时，Amazon Chime 会使用 Active Directory 的 `EmailAddress` 属性中的单独电子邮件地址作为每个用户的主电子邮件地址。在 Amazon Chime 控制台中，您只能看到这一个用户电子邮件地址。但只要您在 Amazon Chime 账户中申请了这些域，用户就可以使用 `ProxyAddress` 属性中列出的其他任意地址登录。

错误配置示例

用户名为 shirley.rodriguez 的用户是 Amazon Chime 账户成员，此账户申请了两个域：example.com 和 example.org。在 Active Directory 中，此用户拥有以下三个电子邮件地址：

- 主电子邮件地址：shirley.rodriguez@example.com
- 代理电子邮件地址 1：shirley.rodriguez@example2.com

- 代理电子邮件地址 2：srodriguez@example.org

此用户可使用 shirley.rodriguez@example.com 或 srodriguez@example.org 及其用户名 shirley.rodriguez 登录 Amazon Chime。尝试通过 shirley.rodriguez@example2.com 登录的用户需要执行 Login with Amazon 操作，且不是您托管账户的成员。因此务必申请所有用户的电子邮件域。

其他 Amazon Chime 用户可使用 shirley.rodriguez@example.com 或 srodriguez@example.org 电子邮件地址，添加此用户为联系人、邀请其加入会议或添加其为代表。

正确配置示例

用户名为 shirley.rodriguez 的用户是 Amazon Chime 账户成员，此账户申请了三个域：example.com、example2.com 和 example.org。在 Active Directory 中，此用户拥有以下三个电子邮件地址：

- 主电子邮件地址：shirley.rodriguez@example.com
- 代理电子邮件地址 1：shirley.rodriguez@example2.com
- 代理电子邮件地址 2：srodriguez@example.org

此用户可以使用其任一工作电子邮件地址登录 Amazon Chime。其他用户也可以使用其任一工作电子邮件地址，添加此用户为联系人、邀请其加入会议或添加其为代表。

连接到 Okta SSO

如果您有企业账户，则可以连接到 Okta SSO 以进行身份验证和分配用户权限。

> **Note**
>
> 如果您需要创建企业账户（这将允许您管理一组指定电子邮件地址域中的所有用户），请参阅申请域。

将 Amazon Chime 连接到 Okta 需要在 Okta 管理控制台中配置两个应用程序。第一个应用程序需要手动配置，然后通过 OpenID Connect 验证用户使用 Amazon Chime 服务的身份。第二个应用程序作为 Amazon Chime SCIM 预置，可以在 Okta Integration Network (OIN) 中使用。经过配置后，此应用程序会向 Amazon Chime 推送有关用户和组更改的更新内容。

连接到 Okta SSO

1. 在 Okta 管理控制台中创建 Amazon Chime 应用程序 (OpenID Connect)：

    1. 登录 Okta 管理控制面板，然后选择 Add Application (添加应用程序)。在 Create New Application (创建新应用程序) 对话框中，依次选择 Web、Next (下一步)。
    2. 配置应用程序设置：
        a. 命名应用程序 **`Amazon Chime`**。
        b. 对于 Login Redirect URI (登录重定向 URI)，请输入以下值：**`https://signin.id.ue1.app.chime.aws/auth/okta/callback`**
        c. 在 Allowed Grant Types (允许的授权类型) 部分中，选择所有选项以启用它们。
        d. 在 Login initiated by (登录发起方) 下拉菜单中，选择 Either (Okta or App) (两者之一 (Okta 或应用程序))，然后选择所有相关选项。
        e. 对于 Initiate Login URI (启动登录 URI)，请输入以下值：**`https://signin.id.ue1.app.chime.aws/auth/okta`**
        f. 选择保存。
        g. 保持此页面打开，因为您将需要 Client ID (客户端 ID)、Client secret (客户端密钥) 和 Issuer URI (发布者 URI) 信息用于步骤 2。
2. 在 Amazon Chime 控制台中，按照以下步骤操作：

    1. 在 Okta single-sign on configuration (Okta single-sign on 配置) 页面的顶部，选择 Set up incoming keys (设置传入密钥)。
    2. 在 Setup incoming Okta keys (设置传入 Okta 密钥) 对话框中：
        a. 粘贴 Okta 应用程序设置页面上的客户端 ID 和客户端密钥信息。
        b. 粘贴 Okta API 页面上的相应的发布者 URI。Issuer URI (颁发者 URI) 必须是 Okta 域，例如 `https://example.okta.com`。
3. 在 Okta 管理控制台中设置 Amazon Chime SCIM 预置应用程序，以便与 Amazon Chime 交换选定的身份和组成员资格信息：

    1. 在 Okta 管理控制台中，依次选择应用程序和添加应用程序，搜索 Amazon Chime SCIM 预置，然后添加此应用程序。

> **Important**
>
> 在初始设置期间，同时选择 Do not display application to users (不向用户显示应用程序) 和 Do not display application icon in the Okta Mobile App (不在 Okta 移动应用程序中显示应用程序图标)，然后选择 Done (完成)。

2. 在 Provisioning (预配置) 选项卡上，选择 Configure API Integration (配置 API 集成)，然后选择 Enable API Integration (启用 API 集成)。保留此页面打开，因为您需要在接下来的步骤中向其复制 API 访问密钥。
3. 在 Amazon Chime 控制台中，选择创建访问密钥以创建 API 访问密钥。将此密钥复制到配置 API 集成对话框中的 Okta API 令牌字段，选择测试集成，然后选择保存。
4. 配置 Okta 将用于更新 Amazon Chime 的操作和属性。在 Provisioning (预配置) 选项卡的 To App (至应用程序) 部分下方，选择 Edit (编辑)，在 Enable Users (启用用户)、Update User Attributes (更新用户属性) 和 Deactivate Users (停用用户) 中选择，然后选择 Save (保存)。
5. 在 Assignments (分配) 选项卡上，授予用户对新 SCIM 应用程序的权限。

> **Important**
>
> 无论有无许可，亚马逊都建议您通过包含所有需要访问 Amazon Chime 的用户的组来授予权限。该组必须是在前面的步骤 1 中，分配面向用户的 OIDC 应用程序时所用的同一个组。否则，最终用户将无法登录。

6. 在推送组选项卡上，配置要同步到 Amazon Chime 的组和成员资格。这些组用于区分基本用户和高级用户。

4. 在 Amazon Chime 中配置目录组：

1. 在 Amazon Chime 控制台中，导航到 Okta 单一登录配置页面。
2. 在 Directory groups (目录组) 下，选择 Add new groups (添加新组)。
3. 输入要添加到 Amazon Chime 的目录组名称。该名称必须与在步骤 3-f 中配置的 Push Groups (推送组) 之一完全相符。
4. 选择此组中的用户应该获取 Basic (基本) 还是 Pro (高级) 功能，然后选择 Save (保存)。重复此过程来配置额外的组。

> **Note**
>
> 如果您收到错误消息，说明找不到该组，则两个系统可能未完成同步。请等待几分钟，然后重新选择 Add new groups (添加新组)。

为目录组用户选择的 Basic 版或 Pro 版功能会影响这些用户在 Amazon Chime 企业账户中的许可证、功能和费用。有关更多信息，请参阅定价。

部署适用于 Outlook 的 Amazon Chime 插件

Amazon Chime 提供两种适用于 Microsoft Outlook 的插件：适用于 Windows Outlook 的 Amazon Chime 插件和适用于 Outlook 的 Amazon Chime 插件。这些插件提供相同的计划功能，但支持不同类型的用户。使用本地 Microsoft Exchange 2013 或更高版本的 Microsoft Office 365 订阅者和组织可以使用适用于 Outlook 的 Amazon Chime 插件。使用运行 Exchange Server 2010 或更早版本的本地 Exchange 服务器的 Windows 用户和 Outlook 2010 用户必须使用适用于 Windows 版 Outlook 的 Amazon Chime 插件。

无权安装适用于 Outlook 的 Amazon Chime 插件的 Windows 用户应选择适用于 Windows 版 Outlook 的 Amazon Chime 插件。

有关哪些插件适合您和您的组织的信息，请参阅 选择合适的 Outlook 插件。

如果为组织选择适用于 Outlook 的 Amazon Chime 插件，则您可以采用集中部署的方式，为用户部署此插件。有关更多信息，请参阅适用于 Outlook 的 Amazon Chime 插件的管理员安装指南。

设置适用于 Slack 的 Amazon Chime Meetings 应用程序

如果您使用 Slack Enterprise Grid 组织，并且拥有或管理 Slack 组织，则可以为组织设置适用于 Slack 的 Amazon Chime Meetings 应用程序。如果您是 Slack 工作区管理员，则可以为工作区设置适用于 Slack 的 Amazon Chime Meetings 应用程序。

以下章节中的步骤说明了如何执行这两种设置，以及如何完成其他任务，如将工作区迁移到组织中。

主题

- 在组织中安装适用于 Slack 的 Amazon Chime Meetings 应用程序
- 在工作区上安装适用于 Slack 的 Amazon Chime Meetings 应用程序

- 将工作区迁入组织
- 将工作区关联至 Amazon Chime 团队账户

在组织中安装适用于 Slack 的 Amazon Chime Meetings 应用程序

在 Slack 组织中安装适用于 Slack 的 Amazon Chime Meetings 应用程序后，用户可以与其中不同工作区的其他用户启动即时会议和呼叫。此操作还能让工作区管理员在新工作区上自动安装适用于 Slack 的 Amazon Chime Meetings 应用程序。操作步骤如下所述。

> **Note**
>
> 以下步骤假设您是组织所有者或管理员，并且可以登录 Slack 管理控制台。

为组织设置适用于 Slack 的 Amazon Chime Meetings 应用程序

1. 在 Slack 管理控制台的左侧窗格中，选择应用程序。

   此时显示应用程序页面，其中列出了组织已安装的应用程序（如果有）。
2. 选择位于页面右上角的管理应用程序，然后选择安装应用程序。

   此时显示查找要安装的应用程序对话框。
3. 搜索 **`Amazon Chime Meetings`** 并在搜索结果中进行选择。

   此时显示将 Amazon Chime Meetings 添加到工作区对话框，其中列出了组织中的工作区。
4. 选择一个或多个工作区，安装适用于 Slack 的 Amazon Chime Meetings 应用程序。
5. 或者，如果您想在所有新工作区中自动安装适用于 Slack 的 Amazon Chime Meetings 应用程序，则选择未来工作区的默认设置，然后选择下一步。

   此时显示查看此应用程序所需的权限对话框，其中会显示适用于 Slack 的 Amazon Chime Meetings 应用程序的权限和操作。
6. 选择下一步。
7. 如果默认在新工作区中安装适用于 Slack 的 Amazon Chime Meetings 应用程序，请选择我准备将此应用程序设为未来工作区的默认设置，然后选择保存。否则，请选择保存。

> **Note**
>
> 您也可以使用 OAuth 在组织中安装应用程序。有关详细信息，请参阅 Slack 帮助中的使用 OAuth 安装。

在工作区上安装适用于 Slack 的 Amazon Chime Meetings 应用程序

在工作区上安装适用于 Slack 的 Amazon Chime Meetings 应用程序后，用户可以与其中的其他用户启动即时会议和呼叫。用户无需 Amazon Chime 用户配置文件，也能使用适用于 Slack 的 Amazon Chime Meetings 应用程序。他们可以随时使用 Slack 用户配置文件登录并启动呼叫或会议。如需启动多人会议，则必须设置 Amazon Chime 团队账户，授予这些用户 Pro 版权限。有关启动 Amazon Chime 呼叫和会议的更多信息，请参阅《Amazon Chime 用户指南》中的使用适用于 Slack 的 Amazon Chime Meetings 应用程序。有关设置 Amazon Chime 团队账户的更多信息，请参阅本指南中的 将工作区关联至 Amazon Chime 团队账户。

为 Slack 工作区安装适用于 Slack 的 Amazon Chime Meetings 应用程序

1. 导航到 Slack 应用程序目录并找到 Amazon Chime Meetings 应用程序。
2. 选择添加到 Slack，从 Slack 应用程序目录中安装适用于 Slack 的 Amazon Chime Meetings 应用程序。
3. 将 Slack 工作区的呼叫设置配置为使用 Amazon Chime 启动 Slack 呼叫。

将工作区迁入组织

如果您是 Slack 组织的所有者，则可以将工作区迁入组织。有关迁移工作区的更多信息，请参阅 Slack 帮助中的将工作区迁入 Enterprise Grid。

将工作区关联至 Amazon Chime 团队账户

将工作区关联至 Amazon Chime 团队账户，以管理用户权限。将会议主机升级为 Amazon Chime Pro 版，即可启动最多容纳 250 名与会者和 25 个视频磁贴的会议，并添加用于拨入音频的电话号码。为用户分配 Amazon Chime 基本权限，以便他们可以开始 one-on-one 会议或加入 Amazon Chime 会议。有关更多信息，请参阅 Amazon Chime 定价。

> **Note**
>
> 如果 Amazon Chime 团队账户与 Slack 工作区关联，则用户可以通过适用于 Slack 的 Amazon Chime Meetings 应用程序，登录 Amazon Chime。您可以随时更改此设置。有关更多信息，请参阅 管理会议设置。

必须先创建一个 AWS 账户，然后才能将 Slack 工作空间与 Amazon Chime Team 账户关联。有关如何创建 AWS 账户的更多信息，请参阅Amazon Chime 系统管理员的先决条件。

在安装适用于 Slack 的 Amazon Chime Meetings 应用程序时，将 Slack 工作区关联到 Amazon Chime 团队账户

1. 在 Slack 工作区中安装适用于 Slack 的 Amazon Chime Meetings 应用程序后马上选择立即升级。
2. 按照提示使用您的 AWS 账户凭证登录 Amazon Chime 控制台。
3. 根据提示，在 Amazon Chime 中新建团队账户或者选择现有账户。
   - 新建账户：新建 Amazon Chime 账户，邀请 Slack 用户加入。输入账户名称，选择是否邀请 Slack 用户，然后选择 Create (创建)。
   - 选择现有账户：选择现有的 Amazon Chime 账户，邀请 Slack 用户加入。选择账户，然后选择 Invite (邀请)。

受邀加入 Amazon Chime 的 Slack 用户会收到一封电子邮件邀请函。接受邀请的用户会自动升级为 Amazon Chime Pro 版用户。

如果在安装适用于 Slack 的 Amazon Chime Meetings 应用程序时，您没有将 Slack 工作区关联到 Amazon Chime 团队账户，则可以在事后使用以下步骤执行此操作。

安装适用于 Slack 的 Amazon Chime Meetings 应用程序后，将 Slack 工作区关联到 Amazon Chime 团队账户

1. 登录您的 AWS 账户。
2. 以管理员身份登录到您的 Slack 工作区。
3. 转到 https://signin.id.ue1.app.chime.aws/auth/slack?purpose=app_authz。
4. 根据提示，在 Amazon Chime 中新建团队账户或选择现有账户。
   - 新建账户：新建 Amazon Chime 账户，邀请 Slack 用户加入。输入账户名称，选择是否邀请 Slack 用户，然后选择 Create (创建)。

- 选择现有账户：选择现有的 Amazon Chime 账户，邀请 Slack 用户加入。选择账户，然后选择 Invite (邀请)。

管理用户

> **Note**
>
> 本节中的步骤假设您有一组用户电子邮件地址，或者您已将管理员帐户关联到 Active Directory。有关更多信息，请参阅本连接到 Active Directory指南中的。

您可以使用 Amazon Chime 控制台，添加并管理用户。还可以通过邀请的方式添加用户。接受邀请的用户会显示在用户项下，其中列出了您账户中的所有用户及其详细信息。有关更多信息，请参阅 查看用户详细信息。

使用 Login with Amazon (LWA) 的账户管理员还可查看权限套餐管理选项和账户用户删除选项。Active Directory 或 Okta 管理上述操作，取决于在配置使用账户时的具体操作。有关更多信息，请参阅 管理用户权限和访问权限。

内容

- 添加用户
- 查看用户详细信息
- 管理用户权限和访问权限
- 更改个人会议 PIN
- 管理 Pro 试用
- 请求用户附件
- Amazon Chime 如何管理自动更新
- 将用户迁移到另一个团队账户

添加用户

您可以通过邀请用户加入 Amazon Chime 账户的方式添加用户。您可以通过 Amazon Chime 控制台向潜在用户发出邀请，操作步骤如下所述。

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。

   此时显示所管理的账户列表。
2. 选择要添加成员的账户，然后选择邀请用户。

此时显示邀请新用户对话框。

3. 输入要邀请的用户的电子邮件地址。使用分号 (;) 分隔每个地址。
4. 选择 Invite users。

此时列表中会显示新用户。在邀请用户加入团队账户时，只会显示接受邀请的用户的详细资料。

查看用户详细信息

您可以在 Amazon Chime 控制台的用户项下，查看账户用户列表以及用户详细信息。通过电子邮件地址搜索特定用户，然后通过用户名称查看其详细信息。您可以在用户详细信息项下，查看用户详细信息并更新用户账户。

下表列出了控制台中显示的用户详细信息。

> **Note**
>
> 只有在用户接受加入团队账户的邀请后，才会显示完整的用户详细信息。

字段	描述	示例
显示名称	Amazon Chime 中显示的用户名称。Login with Amazon (LWA) 用户需要输入全名。Active Directory 用户则会使用 DISPLAY_NAME_ATTRIBUTE。	Major、Mary
电子邮件地址	对于 LWA 用户，用于注册的电子邮件地址。对于 Active Directory 用户，显示 Active Directory 中的主电子邮件地址。	mary.major@example.com
注册	用户的当前注册状态。可能的值在未发送邀请的企业账户与	Registered (已注册)、Unregistered (已取消

字段	描述	示例
	发送邀请的团队账户之间有所不同。	注册)（对于团队账户）或 Suspended (已暂停)（对于企业账户）
权限套餐	默认设置为 Pro 版，以支持用户主持会议。它可更改为 Basic。	Pro、Basic
已邀请	对于团队账户，即为邀请用户加入账户的日期。	01/05/2020
已加入	用户首次登录 Amazon Chime 的日期。对于试用 Pro 版的用户，也可以是开始试用的日期。	01/10/2020
个人 PIN	用户可用于安排会议的个人会议 PIN。	0123456789
隐私设置	用户选择的在线状态设置。	Public (公开) 或 Private (私密)
已参加的会议	用户已参加的会议的数量。	87
已组织的会议	用户已组织的会议的数量。	12
会议满意度	对 end-of-meeting调查给予正面回应的百分比。	92%
上一次活动日期	用户上次处于活动状态的日期。	06/12/2020
已发送的聊天消息	用户已发送的聊天消息条数。	1025
电话号码	分配给用户的电话号码（如果有）。	+12065550100

管理用户权限和访问权限

为 Amazon Chime 用户分配 Pro 版或 Basic 版权限，以管理其访问哪些功能。只有 Basic 版权限的用户无法主持会议，但可以加入会议并使用聊天功能。有关 Pro 版和 Basic 版用户可访问的功能的更多信息，请参阅计划和定价。

通过邀请或暂停的方式，管理可登录 Amazon Chime 管理账户的用户。只有企业账户管理员可以暂停用户。团队账户管理员可以从其账户中删除用户，这样就无需再为其权限付费。但无法暂停用户并阻止其登录。有关团队账户和企业账户差异的更多信息，请参阅 管理您的 Amazon Chime 账户。

管理用户权限

作为 Amazon Chime 管理员，您可以管理 Amazon Chime 账户中具有 Pro 版和 Basic 版权限的用户。

如果您为 Amazon Chime 账户配置了 Active Directory 或 Okta，则可以使用目录组成员资格来管理用户权限。否则，请通过 Amazon Chime 控制台管理用户权限。

团队账户和企业 Login with Amazon

如果您管理的是 Amazon Chime 团队账户或 LWA 企业账户 [用户通过 Login with Amazon (LWA) 账户登录]，则可以在 Amazon Chime 控制台中管理 Pro 版和 Basic 版权限。

管理团队账户和 LWA 企业账户的用户权限

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 对于账户，选择 Amazon Chime 账户名称。
3. 选择用户。
4. 选择用户，然后依次选择操作和分配权限。
5. 选择以下权限之一：
   - Pro 版
   - 基本
6. 选择 Assign (分配)。

配置 Active Directory 或 OpenID Connect (Okta) 的企业账户

对于使用 Active Directory 或 Okta 凭证登录的用户，将其加入具有 Pro 版和 Basic 版权限的目录组，以管理其权限。

如需为用户分配 Pro 版权限，则将其加入具有 Pro 版权限的 Active Directory 或 Okta 组。如需为用户分配 Basic 版权限，则将其加入具有 Basic 版权限的成员组。没有 Pro 版或 Basic 版权限的用户无法登录 Amazon Chime。

管理用户访问权限

如果您是 Amazon Chime 账户的管理员，则可以邀请用户并允许其登录账户。企业账户管理员有权暂停用户的访问权限，以阻止其登录账户。

邀请和删除团队账户用户

如果您是团队账户的管理员，则可以通过 Amazon Chime 控制台邀请来自任何电子邮件域的用户。

> **Note**
>
> 用户将在接受邀请时结束 30 天免费试用期。

邀请用户加入团队账户

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 对于账户，选择团队账户的名称。
3. 依次选择用户和邀请用户。
4. 输入要邀请用户的电子邮件地址，使用分号 (**;**) 进行分隔。
5. 选择 Invite users。

请按照以下流程删除分配给用户的 Pro 版或 Basic 版权限，然后解除用户与团队账户的关联。已删除的用户仍能登录 Amazon Chime，但不再是 Amazon Chime 账户的付费成员。

从团队账户中删除用户

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 对于账户，选择团队账户的名称。
3. 选择用户。
4. 选择要删除的用户，然后依次选择操作和删除用户。

此操作将删除分配给用户的所有 Pro 版或 Basic 版权限。用户无法再使用自动完成功能来查找联系人中的新团队用户。

邀请并暂停企业账户用户

如果您是企业账户的管理员，所有使用您申请域的电子邮件地址注册 Amazon Chime 的用户都将自动成为账户成员。如果您配置了 Active Directory 或 Okta，请务必将用户加入 Amazon Chime 目录组。

邀请用户加入企业账户

- 向组织中的用户发送电子邮件邀请函，并指导其按照 Amazon Chime 用户指南中的创建 Amazon Chime 账户的步骤进行操作。

用户会通过您为账户申请的某个域中的电子邮件地址登录。按步骤创建的 Amazon Chime 用户账户会自动通过 Amazon Chime 控制台显示在企业账户的用户项下。

以下流程会暂停用户使用未配置 Active Directory 或 Okta 的企业账户。用户将无法登录 Amazon Chime。

从企业账户中暂停用户

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 对于账户，选择企业账户的名称。
3. 选择用户。
4. 选择要暂停的用户，然后依次选择操作和暂停用户。
5. 选中相应的复选框，然后选择暂停。

如果您已为企业账户配置了 Active Directory 或 Okta，请按照以下流程暂停用户。

从企业 Active Directory 或 OpenID Connect (Okta) 账户中暂停用户

- 请执行以下操作之一：
  - 通过 Active Directory 或 Okta 管理员控制面板暂停用户或将用户标记为不活跃用户。
  - 从具有 Pro 版或 Basic 版权限的 Active Directory 组中删除用户。

更改个人会议 PIN

个人会议 PIN 是用户注册时生成的一个静态 ID。Amazon Chime 用户可使用 PIN，轻松安排与其他 Amazon Chime 用户的会议。使用个人会议 PIN 意味着会议组织者无需记住他们安排的每个新会议的会议详细信息。

如果用户觉得其个人会议 PIN 已遭盗用，您可以重置其 PIN 并生成新的 ID。在您更新个人会议 PIN 之后，用户必须更新使用旧的个人会议 PIN 安排的所有会议。

更改个人会议 PIN

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在账户页面上，选择 Amazon Chime 账户的名称。
3. 在导航窗格中，选择用户。
4. 搜索需要更改其 PIN 的用户。
5. 要打开 User detail (用户详细信息) 页面，选择用户的名称。
6. 依次选择 User actions (用户操作)、Reset personal PIN (重置个人 PIN)、Confirm (确认)。

管理 Pro 试用

当用户接受 Amazon Chime 团队邀请或成为企业账户成员时，其免费试用期将结束，但可享有 Pro 版权限。这使得他们能够继续主持已安排的会议。将用户的权限套餐更改为“Basic”会阻止其担任会议主持人。

基于 Amazon Chime 使用情况制定的定价模式让您只需为主持会议的用户按照所举办会议的天数付费。不向会议参加者和聊天用户收取费用。

高级用户如果主持了在一个日历日内结束的会议并且至少出现以下情况之一，则视为活动高级用户：

- 已安排会议。
- 会议包含了两个以上的参加者。
- 会议至少有一个记录事件。
- 会议包含了拨入的参加者。
- 会议包含了使用 H.323 或 SIP 的参加者。

有关更多信息，请参阅计划和定价。

请求用户附件

如果您是企业账户的管理员并拥有相应权限，则可以请求并接收用户上传至 Amazon Chime 的附件。您可以获取用户上传到一对一对话和组对话或他们所创建聊天室中的附件。

> **Note**
>
> 如果您是 Amazon Chime 团队账户的管理员，则可以通过申请一个或多个域来升级为企业账户。或者，您也可以删除团队账户中的用户，让这些非托管用户使用 Amazon Chime Assistant 获取其附件。

请求用户附件

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在账户页面上，选择 Amazon Chime 账户的名称。
3. 在 Settings (设置) 下，依次选择 Account (账户)、Account actions (账户操作)、Request attachments (请求附件)。
4. 账户摘要页面会在约 24 小时内提供指向含有预签名 URL 列表的文件链接，您可以使用这些预签名 URL 访问每个附件。
5. 下载该文件。

> **Note**
>
> 请确保对该文件保持适当的访问控制级别。获取该文件的任何用户均可使用提供的 URL 列表下载关联的附件。
> 预签名 URL 将在 6 天后过期。您可以每 7 天提交一次请求。

要使用 AWS Identity and Access Management (IAM) 策略来管理对 Amazon Chime 管理控制台和 “请求附件” 操作的访问权限，请使用其中一个 Amazon Chime 托管策略（ UserManagement、或 ）。 ReadOnly FullAccess或者，您也可以更新自定义策略以包含 `StartDataExport` 操作和 `RetrieveDataExport` 操作。有关此类操作的更多信息，请参阅《IAM 用户指南》中的 Amazon Chime 定义的操作。

Amazon Chime 如何管理自动更新

Amazon Chime 提供了不同的客户端更新方式。根据 Amazon Chime 的运行位置是在浏览器上、桌面上还是移动设备上，方法会有所不同。

Amazon Chime Web 应用程序 (https://app.chime.aws) 始终加载最新功能和安全修复程序。

每当您选择退出或注销时，Amazon Chime 桌面客户端都会检查是否有更新。此操作适用于 Windows 和 macOS 计算机。当运行客户端时，会每三小时检查一次更新。您也可以在 Windows 帮助菜单上选择检查更新，或通过 macOS 的 Amazon Chime 菜单检查更新。

当桌面客户端检测到更新时，Amazon Chime 会提示用户安装更新，除非他们正在参加会议。以下情况说明用户正在参加会议：

- 用户参加会议。
- 用户应邀参加正在进行中的会议。

Amazon Chime 会提示用户安装最新版本，并设置 15 秒倒计时，以便用户推迟安装。用户可以选择稍后再试以推迟更新。

如果用户未加入正在进行的会议却选择推迟更新，则客户端会在三小时后检查更新，并再次提示用户进行安装。倒计时结束时，开始安装。

> **Note**
>
> 在 macOS 计算机上，用户需要选择立即重启才能开始更新。

在移动设备上：Amazon Chime 移动应用程序会通过 App Store 和 Google Play 提供的更新选项，为客户提供 Amazon Chime 最新版客户端。您也可以使用移动设备管理系统来部署更新。

将用户迁移到另一个团队账户

您可以创建并配置目标账户（如果尚不存在），将用户迁移到其他团队账户。然后将用户添加到目标账户。以下步骤介绍了有关完成迁移的信息。

迁移用户

1. 如果您没还没有目标团队账户，则先创建账户。有关更多信息，请参阅 步骤 1：创建 Amazon Chime 管理员账户。

2. 按需配置账户。有关更多信息，请参阅 步骤 2（可选）：配置账户设置。
3. 向账户添加用户。有关更多信息，请参阅 第 3 步：将用户添加到账户。

管理 Amazon Chime 中的电话号码

您可以使用 Amazon Chime 控制台来配置电话号码。当您配置号码时，您可以从 Amazon Chime 管理的号码池中请求这些号码。如果您取消分配并删除号码，则这些号码将返回资源池。当你移植号码时，你可以将它们移入和移出 Amazon Chime。

> **Note**
>
> 当你使用 Amazon Chime 控制台时，你只能预配置 Amazon Chime 商务电话号码。如果您需要国际号码，则可以使用 Amazon Chime 语音连接器和 SIP 媒体应用程序。为此，您必须先创建一个 Amazon Chime 软件开发工具包管理账户。有关更多信息，请参阅《Amazon Chime 软件开发工具包管理员指南》中的以下主题：
>
> - 先决条件
> - 管理电话号码清单
> - 管理语音连接器
> - 管理 SIP 媒体应用程序

以下各节中的主题说明了如何配置和管理 Amazon Chime 电话号码。

内容

- 预置电话号码
- 转网现有电话号码
- 分配 Amazon Chime 商务电话号码
- 取消分配 Amazon Chime 商务电话号码
- 使用出站呼叫名称
- 删除电话号码
- 还原已删除的电话号码

预置电话号码

使用 Amazon Chime 控制台为 Amazon Chime 账户预置电话号码。这些数字均来自 Amazon Chime 托管的资源池。使用 Amazon Chime Business Calling 为现有的 Amazon Chime 用户预置并分配电话号码。

预置完成后，电话号码将显示在您的清单中。随即为不同用户分配电话号码。

预置电话号码

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在导航窗格的呼叫项下，选择电话号码管理。
3. 依次选择 Orders（订单）和 Provision phone numbers（预置电话号码）。
4. 选择业务呼叫，然后选择下一步。
5. 搜索可用电话号码。选择所需的电话号码，然后选择 Provision (预置)。

预置时，电话号码会显示在订单和待处理列表中。

转网现有电话号码

除了配置电话号码外，您还可以将电话运营商的号码移植到库存中。这包括免费电话号码。

> **Note**
>
> 如果您需要移植国际号码、使用 Amazon Chime Voice Connector 或 SIP 媒体应用程序，则必须创建一个 Amazon Chime 软件开发工具包管理员账户并使用 Amazon Chime SDK 控制台。有关执行此操作的更多信息，请参阅 Amazon Chime SDK 管理员指南中的先决条件。

以下各节说明如何移植电话号码。

主题

- 移植号码的先决条件
- 正在移植电话号码
- 提交所需文件
- 查看请求状态
- 分配端口号
- 移植电话号码
- 电话号码转网状态定义

移植号码的先决条件

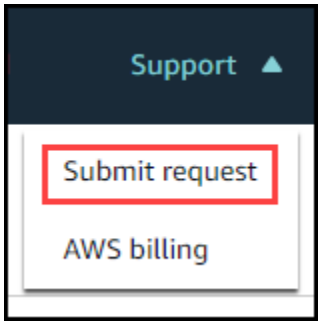
要获得端口号，您必须有代理信 (LOA)。对于国内电话号码，您必须有 LOA。下载代理信 (LOA) 表格并填写。如果您需要移植来自不同运营商的电话号码，请为每个运营商填写单独的 LOA。

正在移植电话号码

您可以创建支持请求以将现有电话号码移入其中。

接入现有电话号码

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在页面顶部的命令栏上，选择 Su pp ort，然后选择提交请求。



这会将你带到 Su AWS pport 控制台。

> **Note**
>
> 您也可以直接进入AWS Support 中心页面。如果这样做，请选择 “创建案例”，然后按照以下步骤操作。

3. 在 “我们如何提供帮助” 下，执行以下操作：
   a. 选择账户和账单。
   b. 从服务列表中选择 Chime SDK（号码管理）。
   c. 从 “类别” 列表中，选择 “电话号码 Port In”。
   d. 选择 Next step: Additional information（下一步：其他信息）。
4. 在 “其他信息” 下，执行以下操作
   a. 在主题下，输入 **`Porting phone numbers in`**。
   b. 在描述下，输入以下信息：

要移植美国号码：

- 账户的账单电话号码 (BTN)。
- 授权人员的姓名。这是当前运营商的账户计费负责人。
- 当前运营商（如果已知）。
- 服务账号（如果当前运营商提供此信息）。
- 服务 PIN（如果可用）。
- 服务地址和客户名称，显示在当前运营商合同中。
- 请求转网的日期和时间。
- （可选）如果要移植账单电话号码 (BTN)，请选择以下选项之一：
  - 我正在移植 BTN，希望使用新 BTN 进行替换。我确认新 BTN 在当前运营商的同一账户上。
  - 我正在转网我的 BTN，我想关闭我的当前运营商的账户。
  - 我正在转网我的 BTN，因为我的账户目前已经设置，以便每个电话号码都是它自己的 BTN。（仅当您以此方式设置当前运营商的账户时，才选择此选项。）
  - 选择选项后，请在申请中附上您的代理信 (LOA)。

要移植国际号码：

- 对于非美国电话号码，您必须使用 SIP 媒体应用程序拨入产品类型。
- 号码类型（本地号码或免费号码）
- 要转入的现有电话号码
- 估算使用量
- Country

c. 从 “电话号码类型” 列表中，选择 “商务呼叫”、“SIP 媒体应用程序拨入” 或 “语音连接器”。

d. 在 “电话号码” 下，至少输入一个电话号码，即使您要移植多个号码。

e. 在移植日期下，输入所需的移植日期。

f. 在 “移植时间” 下，输入所需的时间。

g. 选择下一步：立即解决或联系我们。

5. 在 “立即解决” 或 “联系我们” 下，选择 “联系我们”。
6. 从 “首选联系人语言” 列表中选择一种语言
7. 选择 “Web” 或 “电话”。如果您选择电话，请输入您的电话号码。完成后，选择提交。

AWS Support 让您知道您的电话号码是否可以从现有的电话运营商移植。如果可以，则需要提交所有必需的文件。下一节中的步骤将说明如何提交这些文档。

提交所需文件

在 S AWS upport 表示您可以移植电话号码后，您需要提交所有必需的文件。以下步骤说明了操作方法。

> **Note**
>
> AWS Support 提供了一个安全的 Amazon S3 链接，用于上传所有请求的文档。在收到链接之前，请勿继续。

提交文件

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 登录您的 AWS 账户，然后打开专门为您的账户生成的 Amazon S3 上传链接。

   > **Note**
   >
   > 此链接将于十天后过期。此链接专为案例创建账户生成。该链接需要账户中的授权用户才能执行上传。

3. 选择 “添加文件”，然后选择与您的请求相关的身份证件。
4. 展开权限一节，选择指定单个 ACL 权限。
5. 在访问控制列表 (ACL) 部分的末尾，选择添加被授权者，然后将 Su AWS pport 提供的密钥粘贴到 Grantee 框中。
6. 在 “对象” 下，选中 “读取” 复选框，然后选择 “上传”。

在您提供代理信 (LOA) 后，请向现有的电话运营商 AWS Support 确认委托书上的信息正确无误。如果 LOA 上提供的信息与您的电话运营商存档的信息不匹配， AWS Support 联系您以更新 LOA 上提供的信息。

查看请求状态

以下步骤说明了如何使用 Amazon Chime 控制台查看移植请求的状态。

查看状态

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在导航窗格中，选择电话号码管理。
3. 选择 “订单” 选项卡。

“状态” 列显示您的请求状态。 AWS Support 还会根据需要与您联系以获取最新信息并要求您提供更多信息。有关更多信息，请参阅此部分后面的电话号码转网状态定义。

分配端口号

在您的电话运营商确认 LOA 正确后，他们会审核并批准请求的端口。然后，他们 AWS Support 提供固定订单提交 (FOC) 的日期和时间，以便港口发生。

在 FOC 日期，移植的电话号码已激活以供使用。然后，您必须将号码分配给所需账户中的用户。

分配电话号码

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在导航窗格中，选择电话号码管理。
3. 在库存选项卡上，选中要分配的号码旁边的复选框，然后选择分配。

> **Note**
>
> 一次只能选择一个数字。

4. 在为用户个人资料分配 +1 电话号码页面上，选择该号码的帐户，然后选择下一步。
5. 选择要为其分配号码的用户，然后选择分配。

移植电话号码

您可以向获胜的承运人发起移植请求，将号码移出 Amazon Chime。向获奖运营商提交信息时，请将您的 AWS 账户 ID 作为与要移植的电话号码关联的账户 ID。

移植过程完成并且您的中标承运人拥有号码后，您必须取消分配这些号码并将其从库存中删除。有关更多信息，请参阅本指南中的取消分配 Amazon Chime 商务电话号码和删除电话号码。

> **Important**
>
> - 将号码移出去的能力取决于获胜的运营商接受这些号码的能力。
> - 验证新运营商转出请求的真实性对您电话号码的安全而言至关重要。如果账户详细信息不正确（例如，账户 ID 不匹配），则您的移出请求可能会被拒绝，从而导致延迟，并要求您重新提交请求。

（可选）如何申请 PIN 以保护您的号码

为了提高安全性，您可以联系我们为您的号码设置PIN码。然后，获胜的承运人将使用该PIN码。按照以下步骤进行操作：

索取 PIN

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在导航窗格的 “联系我们” 下，选择 Supp ort。

   这会将你带到 Su AWS pport 控制台。

   > **Note**
   >
   > 您也可以直接进入AWS Support 中心页面。如果这样做，请选择 “创建案例”，然后按照以下步骤操作。

3. 在 “我们如何提供帮助” 下，执行以下操作：
   a. 选择账户和账单。
   b. 从服务列表中选择 Chime SDK（号码管理）。
   c. 从 “类别” 列表中，选择 “电话号码 Port Out”。
   d. 选择 Next step: Additional information（下一步：其他信息）。
4. 在 “其他信息” 下，执行以下操作
   a. 在主题下，输入 **`Porting phone numbers out`**。
   b. 在 “描述” 下，输入以下内容。

I would like to assign a pin to my phone number: Pin: ABCD123 Phone Number: 1234567890

> **Note**
>
> 您必须提供 4-10 个字符的字母数字 PIN。

AWS Support 会将 PIN 与电话号码相关联。向中标承运人申请港口时，请提供您的 AWS 账户 ID 和 PIN。我们将使用该信息来验证收到的有关您的号码的任何端口请求。

电话号码转网状态定义

提交将现有电话号码移植到 Amazon Chime 的请求后，您可以在 Amazon Chime 控制台中的呼叫、电话号码管理和待处理项下查看移植请求状态。

转网状态和定义包括以下内容：

CANCELLED

AWS Support 由于港口出现问题，例如承运人或您的取消请求，取消了港口订单。 AWS Support 与您联系并提供详细信息。

CANCEL_REQUESTED

AWS Support 由于港口问题（例如承运人或您的取消请求），正在处理港口订单的取消。 AWS Support 与您联系并提供详细信息。

CHANGE_REQUESTED

AWS Support 正在处理您的变更申请，承运人正在等待回复。允许额外的处理时间。

COMPLETED

您的移植订单已完成且电话号码已激活。

EXCEPTION

AWS Support 请与您联系以获取完成端口请求所需的其他详细信息。允许额外的处理时间。

FOC

FOC 日期已与承运人确认。 AWS Support 与您联系以确认日期。

PENDING DOCUMENTS

AWS Support 请与您联系以获取完成港口请求所需的其他文件。允许额外的处理时间。

SUBMITTED

您的移植订单已提交，正在等待运营商回复。

分配 Amazon Chime 商务电话号码

使用电话号码管理库存页面为个人用户分配 Amazon Chime 商务电话号码。

要分配 Amazon Chime 商务电话号码

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在导航窗格的呼叫项下，选择电话号码管理。
3. 在 “库存” 选项卡上，选择要分配的电话号码。
4. 选择 Assign (分配)。
5. 选择用户所属的帐户，然后选择下一步。
6. 选择用户，然后选择 “分配”。

当您更改电话号码或电话号码权限时，我们建议向用户提供他们的新信息或权限信息。用户必须先退出 Amazon Chime 账户后重新登录，才能使用新电话号码或权限功能。

取消分配 Amazon Chime 商务电话号码

以下程序取消为 Amazon Chime Business Calling 用户分配电话号码。

取消分配电话号码

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在导航窗格的呼叫项下，选择电话号码管理。
3. 在 “库存” 选项卡上，选择要取消分配的电话号码。
4. 选择 Unassign (取消分配)。
5. 选中相应的复选框，然后选择 Unassign (取消分配)。

您可以查看库存中数字的详细信息。例如，您可以查看是否启用了电话和短信。

查看清单电话号码详细信息

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在导航窗格的呼叫项下，选择电话号码管理。
3. 选择清单选项卡，然后选择要查看的电话号码。
4. 打开操作列表，然后选择查看详细信息。

使用出站呼叫名称

出站呼叫名称充当呼叫者 ID。您可以为清单中的一个或多个电话号码设置默认呼叫名称。您也可以为各个电话号码设置唯一的呼叫名称。然后，这些姓名会显示给使用这些电话号码拨打的外拨电话的收件人。呼叫名称适用于所有电话号码产品类型。您可以每七天更新一次名称。

例如，您可以将该部门的所有电话号码的默认呼叫名称设置为 “部门 5”。您也可以为部门负责人设置一个唯一的名字 Jane Doe。

以下步骤说明了如何设置默认和个人出站呼叫名称。

设置呼叫者姓名

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在导航窗格的呼叫项下，选择电话号码管理。
3. 在 “库存” 选项卡上，执行以下任一操作：选中要更新的电话号码旁边的复选框。
   - 要为多个号码设置默认呼叫名称，请选中这些号码旁边的复选框。
   - 要设置个人呼叫者姓名，请选择所需的号码。
4. 打开操作列表，然后选择更新默认呼叫名称。
5. 默认呼叫名称框中输入名称，最多包含 15 个字符。
6. 选择保存。

系统会在 72 小时内更新默认呼叫名称。

删除电话号码

> **Important**
>
> 只有 Amazon Chime 系统管理员才能完成这些步骤。此外，您必须先取消分配电话号码，才能将其删除。

预置电话号码时，您可以从 Amazon Chime 维护的号码池中进行订购。删除的号码会回到号码池。删除号码时，它首先会进入删除队列并保留 7 天。在此期间，您可以随时将此号码移回清单。7 天后，系统将自动删除保留队列中的号码，并解除它与您账户的关联。这会将数字返回到数字池。如需回收保留队列中已删除的号码，请按照 预置电话号码 中的步骤操作，同时注意此号码可能不可用。

删除未分配的电话号码

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在导航窗格的呼叫项下，选择电话号码管理。
3. 选择清单选项卡，然后选择要删除的电话号码或号码。
4. 打开操作列表，然后选择删除电话号码。
5. 选择复选框，然后选择删除。

删除队列会将已删除的电话号码保留 7 天，然后才从清单中永久删除。

还原已删除的电话号码

您可以从删除队列中还原删除天数未满 7 天的电话号码。还原电话号码是将其移回您的 Inventory（库存）。

还原已删除的电话号码

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 在导航窗格的呼叫项下，选择电话号码管理。
3. 选择删除队列选项卡，然后选择要还原的电话号码或号码。
4. 选择 Move to inventory (移动到清单)。

在 Amazon Chime 中管理全局设置

您可以使用 Amazon Chime 控制台管理呼叫详细信息记录设置。

配置呼叫详细信息记录

必须先创建 Amazon Simple Storage Service 存储桶，才能为 Amazon Chime 管理账户配置呼叫详细信息记录设置。Amazon S3 存储桶将用作记录呼叫详细信息的日志目标。在配置呼叫详细信息记录设置时，为保存和管理数据，您需要为 Amazon Chime 授予读写 Amazon S3存储桶的权限。有关创建 Amazon S3 存储桶的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon Simple Storage Service 入门。

您可以为 Amazon Chime Business Calling 配置呼叫详细信息记录设置。有关 Amazon Chime Business Calling 的更多信息，请参阅 管理 Amazon Chime 中的电话号码。

配置呼叫详细信息记录设置

1. 请根据《Amazon Simple Storage Service 用户指南》中的 Amazon Simple Storage Service 入门所述步骤，创建 Amazon S3 存储桶。
2. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
3. 对于 Global Settings (全局设置)，选择 Call detail records (调用详细信息记录)。
4. 选择业务呼叫配置。
5. 选择 Amazon S3 存储桶作为日志目标。
6. 选择 Save（保存）。

您可以随时停止记录呼叫详细信息。

停止记录呼叫详细信息

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 对于 Global Settings (全局设置)，选择 Call detail records (调用详细信息记录)。
3. 对适用的配置选择 Disable logging (禁用日志记录)。

Amazon Chime Business Calling 的呼叫详细信息记录

您选择接收的 Amazon Chime Business Calling 的呼叫详细信息记录将会发送到 Amazon S3 存储桶。以下示例显示了 Amazon Chime Business Calling 的呼叫详细信息记录名称的通用格式。

```
Amazon-Chime-Business-Calling-CDRs/json/111122223333/2019/03/01/123a4567-
b890-1234-5678-cd90efgh1234_2019-03-01-17.10.00.020_1a234567-89bc-01d2-3456-
e78f9g01234h
```

下面的示例显示了呼叫详细信息记录名称中表示的数据。

```
Amazon-Chime-Business-Calling-CDRs/json/awsAccountID/year/month/
day/conferenceID_connectionDate-callStartTime-callDetailRecordID
```

以下示例显示了 Amazon Chime Business Calling 的呼叫详细信息记录的通用格式。

```
{
    "SchemaVersion": "2.0",
    "CdrId": "1a234567-89bc-01d2-3456-e78f9g01234h",
    "ServiceCode": "AmazonChimeBusinessCalling",
    "ChimeAccountId": "12a3456b-7c89-012d-3456-78901e23fg45",
    "AwsAccountId": "111122223333",
    "ConferenceId": "123a4567-b890-1234-5678-cd90efgh1234",
    "ConferencePin": "XXXXXXXXXX",
    "OrganizerUserId": "1ab2345c-67de-8901-f23g-45h678901j2k",
    "OrganizerEmail": "jdoe@example.com",

    "CallerPhoneNumber": "+12065550100",
    "CallerCountry": "US",

    "DestinationPhoneNumber": "+12065550101",
    "DestinationCountry": "US",

    "ConferenceStartTimeEpochSeconds": "1556009595",
    "ConferenceEndTimeEpochSeconds": "1556009623",
    "StartTimeEpochSeconds": "1556009611",
    "EndTimeEpochSeconds": "1556009623",
    "BillableDurationSeconds": "24",
    "BillableDurationMinutes": ".4",
    "Direction": "Outbound"
}
```

会议室配置

Amazon Chime 可集成至 Cisco、Tandberg、Polycom、Lifesize、Vidyo 或其他使用 SIP 或 H.323 协议的室内视频硬件。

如需使用支持 SIP 的会议室 VTC 设备连接 Amazon Chime，请务必输入以下选项之一：

- **@meet.chime.in**
- **u@meet.chime.in**
- 10 位数会议 ID，后跟 **@meet.chime.in**

使用 **meet.chime.in**，将 SIP 会议室设备连接到最近的 Amazon Chime 区域。要连接到特定区域，请为 SIP 会议室系统使用区域特定的 DNS 条目。有关更多信息，请参阅会话发起协议 (SIP) 会议室系统。

> **Note**
>
> 如果您的 SIP 会议室设备不支持 TLS 并且需要 TCP 连接，请与 AWS Support 联系。

如果您使用的设备仅支持 H.323，则必须拨打以下任一电话：

- **13.248.147.139**
- **76.223.18.152**

如果防火墙正在筛选 VTC 设备与 Amazon Chime 之间的流量，请打开所用协议的端口范围。有关更多信息，请参阅网络配置和带宽要求。

在 Amazon Chime 欢迎画面中输入 10 位数或 13 位数会议 ID，即可加入会议。您可以在 Amazon Chime 客户端或 Web 应用程序中找到 13 位数会议 ID，或选择拨入选项。

加入有人监管的会议

如果会议有人监管且您是监管人或委托人，请输入您的 13 位数会议 ID 以作为监管人加入会议。如果您是监管人，请在拨号盘中输入监管人密码，然后输入井号 (#) 以加入并开始会议。如果您不是主持人、委托人或监管人，则在监管人加入并开始会议后，您将连接到会议。

监管人具有主持人控制权，这意味着他们可以执行其他会议操作。这些操作包括开始和停止记录、锁定和解锁会议、将所有其他与会者静音以及结束会议。有关更多信息，请参阅《Amazon Chime 用户指南》中的监管人使用电话或室内视频系统执行的操作。

> **Note**
>
> 如果您正在使用企业版 Alexa 参加 Amazon Chime 会议，则只有在设备连接到室内视频系统并使用设备的拨号盘拨入时，才能以监管人的身份加入会议。

兼容的 VTC 设备

下表列出了一部分兼容的 VTC 设备列表。

设备	SIP	H.323	注释
Cisco SX20	是	是	音频/视频/屏幕：输入和输出正常
Cisco DX80	是	是	音频/视频/屏幕：输入和输出正常
Lifesize 图标	是	否	音频/视频/屏幕：输入和输出正常
Polycom Debut	是	是	音频/视频/屏幕：输入和输出正常
Polycom RealPresence Desktop	否	是	音频/视频：正常，屏幕：从设备输入正常
Polycom Trio	是	是	音频/视频/屏幕：输入和输出正常
Tandberg C40	是	是	音频/视频/屏幕：输入和输出正常

网络配置和带宽要求

Amazon Chime 需要使用本主题所述目标和端口来支持不同服务。如果阻止了入站或出站流量，则此阻止可能会影响到使用各种服务的能力，包括音频、视频、屏幕共享或聊天。

Amazon Chime 在端口 TCP/443 上使用了 Amazon Elastic Compute Cloud (Amazon EC2) 和其他 AWS 服务。如果防火墙阻止端口 TCP/443 进行访问，请务必在允许列表中添加 `*.amazonaws.com`，或者对于以下服务，将 AWS IP 地址范围添加至 AWS 一般参考：

- Amazon EC2
- 亚马逊 CloudFront
- Amazon Route 53

展开以下部分，了解有关目的地、端口和带宽的更多信息。

所需的目的地和港口

运行 Amazon Chime 需要以下目的地和端口。

目标位置	端口
chime.aws	TCP/443
*.chime.aws	TCP/443
*.amazonaws.com	TCP/443
99.77.128.0/18	TCP/443

会议和电话端口

Amazon Chime 为会议和 Amazon Chime Business Calling 使用以下目标和端口。

目标位置	端口
99.77.128.0/18	UDP/3478

H.323 会议室系统

Amazon Chime 为 H.323 室内视频系统使用以下目标和端口。

目标位置	端口
13.248.147.139	TCP/1720
76.223.18.152	TCP/1720
99.77.128.0/18	TCP/5100:6200
34.212.95.128/25	UDP/5100:6200
34.223.21.0/25	
52.55.62.128/25	
52.55.63.0/25	

会话发起协议 (SIP) 会议室系统

当您在环境中运行适用于 SIP 室内视频系统的 Amazon Chime 时，建议使用以下目标和端口。

AWS 区域	目标位置	端口
全球（最近区域）	99.77.128.0/18	UDP/10000:60000
	34.212.95.128/25	
	34.223.21.0/25	
	52.55.62.128/25	
	52.55.63.0/25	
全局	meet.chime.in	TCP/5061
	13.248.147.139	

AWS 区域	目标位置	端口
	76.223.18.152	
美国东部（弗吉尼亚州北部）	meet.ue1.chime.in	TCP/5061
US West（Oregon）	meet.uw2.chime.in	TCP/5061
亚太地区（新加坡）	meet.as1.chime.in	TCP/5061
亚太地区（悉尼）	meet.as2.chime.in	TCP/5061
亚太地区（东京)	meet.an1.chime.in	TCP/5061
欧洲地区（爱尔兰）	meet.ew1.chime.in	TCP/5061
南美洲（圣保罗）	meet.se1.chime.in	TCP/5061

带宽要求

Amazon Chime 对音频、视频和屏幕共享的带宽要求如下：

- 音频
  - 1:1 呼叫：54 kbps 上行和下行
  - 大规模呼叫：50 名呼叫者需要增加的下行带宽不超过 32 kbps
- 视频
  - 1:1 呼叫：650 kbps 上行和下行
  - HD 模式：1400 kbps 上行和下行
  - 3-4 人：450 kbps 上行和 (N-1)*400 kbps 下行
  - 5-16 人：184 kbps 上行和 (N-1)*134 kbps 下行
  - 上行和下行带宽会根据网络情况而降低
- 屏幕共享
  - 上行 1.2 mbps（呈现时）和下行 1.2 mbps（观看时）以获得高品质。这可根据网络条件自适应为低至 320 kbps。
  - 远程控制：800 kbps 固定

查看报告

为做出更明智的决策和提升组织的工作效率，您可以直接从控制台访问使用情况和反馈数据。报告数据每天更新，不过最多可能会有 48 小时的延迟。

查看使用情况和反馈报告

1. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
2. 依次选择 Reports (报告)、Dashboard (控制面板)。
3. 在 Usage and feedback dashboard report (使用情况和反馈控制面板报告) 页面上，查看以下数据：

> **Note**
>
> 有关可用数据的更多信息，请参阅 Amazon Chime 报告控制面板和用户活动详细信息。

- 日期范围 (UTC)：报告的日期范围。
- 注册用户：已经注册 Amazon Chime 的用户数。
- 活跃用户：已经通过 Amazon Chime 参加会议或发送消息的用户数。
- 已举行会议：已经结束的会议总数。您可以选择特定会议以查看详细信息，包括会议 ID、开始时间、类型、组织者、持续时间和参加者数量。选择特定 Conference ID (会议 ID) 或 Meeting organizer (会议组织者) 值可查看其他详细信息，包括参加者、会议清单事件、客户端类型和会议反馈。
- 会议满意度：在会议结束调查中给出了积极响应的百分比。
- 已发送聊天消息：用户已经发送的聊天消息数。

扩展 Amazon Chime 桌面客户端

您可以通过添加聊天机器人、代理电话会话和 Webhook 来扩展 Amazon Chime 桌面客户端的功能。用户可使用聊天机器人执行任务，如查询内部系统以获取信息。用户可使用代理电话会话在不透露其电话号码的情况下，拨打电话并发送短信。Webhook 可以自动向聊天室发送消息。例如，Webhook 可以向团队同时发送会议提醒和链接。

主题

- 用户管理
- 为 Amazon Chime 桌面客户端集成聊天机器人
- 创建适用于 Amazon Chime 的 Webhook

用户管理

以下代码片段有助于您管理 Amazon Chime 用户。本主题中的所有示例都使用了 Java。

主题

- 邀请多个用户
- 下载用户列表
- 注销多个用户
- 更新用户个人 PIN

邀请多个用户

以下示例显示了如何邀请多用户加入 Amazon Chime Team 账户。

```
List<String> emails = new ArrayList<>();
emails.add("janedoe@example.com");
emails.add("richardroe@example.net");
InviteUsersRequest inviteUsersRequest = new InviteUsersRequest()
    .withAccountId("chimeAccountId")
    .withUserEmailList(emails);

chime.inviteUsers(inviteUsersRequest);
```

下载用户列表

以下示例显示了如何以 .csv 格式，下载与 Amazon Chime 管理账户关联的用户列表。

```
BufferedWriter writer = Files.newBufferedWriter(Paths.get("/path/to/csv"));
CSVPrinter printer = new CSVPrinter(writer, CSVFormat.DEFAULT.withHeader("userId",
 "email"));

ListUsersRequest listUsersRequest = new ListUsersRequest()
    .withAccountId(accountId)
    .withMaxResults(1);

boolean done = false;
while (!done) {
    ListUsersResult listUsersResult = chime.listUsers(listUsersRequest);
    for (User user: listUsersResult.getUsers()) {
        printer.printRecord(user.getUserId(), user.getPrimaryEmail());
    }

    if (listUsersResult.getNextToken() == null) {
        done = true;
    }

    listUsersRequest = new ListUsersRequest()
        .withAccountId(accountId)
        .withNextToken(listUsersResult.getNextToken());
}

printer.close();
```

注销多个用户

以下示例显示了如何注销 Amazon Chime 管理账户中的多个用户。

```
ListUsersRequest listUsersRequest = new ListUsersRequest()
    .withAccountId("chimeAccountId");
ListUsersResult listUsersResult = chime.listUsers(listUsersRequest);

for (User user: listUsersResult.getUsers()) {
    LogoutUserRequest logoutUserRequest = new LogoutUserRequest()
        .withAccountId(user.getAccountId())
        .withUserId(user.getUserId());
```

```
    chime.logoutUser(logoutUserRequest);
}
```

更新用户个人 PIN

以下示例显示了如何重置 Amazon Chime 特定用户的会议个人 PIN 码。

```
ResetPersonalPINRequest request = new ResetPersonalPINRequest()
    .withAccountId("chimeAccountId")
    .withUserId("userId");

ResetPersonalPINResult result = chime.resetPersonalPIN(request);

User user = result.getUser();
user.getPersonalPIN()
```

为 Amazon Chime 桌面客户端集成聊天机器人

您可以使用 AWS Command Line Interface (AWS CLI)、Amazon Chime API 或 AWS SDK，将聊天机器人集成至 Amazon Chime。在聊天机器人的帮助下，您可以利用 Amazon Lex、AWS Lambda 和其他 AWS 服务，通过 Amazon Chime 聊天室用户可用的智能对话界面简化常规任务流程。

如果您是 Amazon Chime 企业账户管理员，则可以使用聊天机器人帮助用户执行以下任务：

- 查询内部系统以获取信息。
- 自动执行任务。
- 接收关键问题的通知。
- 创建支持票证。

有关 Amazon Chime 企业账户的更多信息，请参阅 管理您的 Amazon Chime 账户。

如果您是 Amazon Chime 企业账户管理员，则最多可以创建 10 个聊天机器人以集成至 Amazon Chime。这些聊天机器人仅适用于由您账户成员创建的聊天室。只有聊天室管理员才能为聊天室添加聊天机器人。聊天机器人添加至聊天室后，聊天室成员可以运行由创建者提供的命令与聊天机器人进行交互。有关更多信息，请参阅本主题中的下一节。

Linux 和 macOS 的用户可以构建支持自定义的示例聊天机器人。有关更多信息，请参阅为 Amazon Chime 构建自定义聊天机器人。

内容

- 将聊天机器人与 Amazon Chime 配合使用
- 发送给聊天机器人的 Amazon Chime 事件

将聊天机器人与 Amazon Chime 配合使用

如果您是 Amazon Chime 企业账户管理员，则最多可以创建 10 个聊天机器人以集成至 Amazon Chime。这些聊天机器人仅适用于由您账户成员创建的聊天室。只有聊天室管理员才能为聊天室添加聊天机器人。聊天机器人添加至聊天室后，聊天室成员可以运行由创建者提供的命令与聊天机器人进行交互。有关更多信息，请参阅《Amazon Chime 用户指南》中的使用聊天机器人。

您还可以使用 Amazon Chime API 操作，为 Amazon Chime 账户启用或停用聊天机器人。有关更多信息，请参阅更新聊天机器人。

> **Note**
>
> 您无权删除聊天机器人。如需停用账户中的聊天机器人，请执行《Amazon Chime API 参考》中的 Amazon Chime UpdateBot API 操作。停用聊天机器人时，聊天室管理员只能将其移出聊天室，而无法添加。如果对聊天室中已停用的聊天机器人执行 @mention 操作，用户将会收到错误消息。

先决条件

在启动用于集成聊天机器人与 Amazon Chime 的程序前，请先完成以下先决条件：

- 创建聊天机器人。
- 创建 Amazon Chime 出站端点，向机器人发送事件信息。从 AWS Lambda 函数 ARN 或 HTTPS 端点中选择。有关 Lambda 的更多信息，请参阅 AWS Lambda 开发人员指南。

适用于 HTTPS 端点的 DNS 最佳实践

在为您的 HTTPS 端点分配 DNS 时，我们建议采用以下最佳实践：

- 使用专用于自动程序端点的 DNS 子域。
- 仅使用 A 记录指向自动程序端点。
- 保护您的 DNS 服务器和 DNS 注册商账户，以防止域劫持。

- 使用专用于自动程序端点的公开有效的 TLS 中间证书。
- 在处理机器人消息前，请先对其签名进行加密验证。

创建聊天机器人后，使用 AWS Command Line Interface (AWS CLI) 或执行 Amazon Chime API 操作，完成以下章节所述任务。

任务

- 步骤 1：将聊天机器人集成至 Amazon Chime
- 步骤 2：为 Amazon Chime 聊天机器人配置出站端点
- 步骤 3：为 Amazon Chime 聊天室添加聊天机器人
- 对聊天机器人请求进行身份验证
- 更新聊天机器人

步骤 1：将聊天机器人集成至 Amazon Chime

完成先决条件后，使用 AWS CLI 或 Amazon Chime API，将聊天机器人集成至 Amazon Chime。

> **Note**
>
> 这些流程会为聊天机器人创建姓名和电子邮件地址。聊天机器人的名称和电子邮件地址创建后就无法更改。

AWS CLI

使用 AWS CLI 集成聊天机器人

1. 如需将聊天机器人集成至 Amazon Chime，请运行 AWS CLI 中的 create-bot 命令。

```
aws chime create-bot --account-id 12a3456b-7c89-012d-3456-78901e23fg45 --display-
name exampleBot --domain example.com
```

   a. 请输入聊天机器人的显示名称，最多包含 55 个字母数字或特殊字符（如 +、–、% ）。

   b. 请输入 Amazon Chime 企业账户的注册域名。

2. Amazon Chime 将返回包含机器人 ID 在内的响应结果。

```
"Bot": {
        "CreatedTimestamp": "timeStamp",
        "DisplayName": "exampleBot",
        "Disabled": exampleBotFlag,
        "UserId": "1ab2345c-67de-8901-f23g-45h678901j2k",
        "BotId": "botId",
        "UpdatedTimestamp": "timeStamp",
        "BotType": "ChatBot",
        "SecurityToken": "securityToken",
        "BotEmail": "displayName-chimebot@example.com"
         }
```

3. 请复制并保存机器人 ID 和电子邮件地址，以备如下程序使用。

Amazon Chime API

使用 Amazon Chime API 集成聊天机器人

1. 如需将聊天机器人集成至 Amazon Chime，请在 Amazon Chime API 参考中执行 CreateBot API 操作。
   a. 请输入聊天机器人的显示名称，最多包含 55 个字母数字或特殊字符（如 +、–、%）。
   b. 请输入 Amazon Chime 企业账户的注册域名。
2. Amazon Chime 将返回包含机器人 ID 在内的响应结果。请复制并保存机器人 ID 和电子邮件地址。机器人的电子邮件地址显示为：*exampleBot*-chimebot@*example.com*。

AWS SDK for Java

以下示例代码演示了如何将适用于 Java 的 AWS SDK 用于聊天机器人集成。

```
CreateBotRequest createBotRequest = new CreateBotRequest()
    .withAccountId("chimeAccountId")
    .withDisplayName("exampleBot")
    .withDomain("example.com");

chime.createBot(createBotRequest);
```

Amazon Chime 将返回包含机器人 ID 在内的响应结果。请复制并保存机器人 ID 和电子邮件地址。机器人的电子邮件地址显示为：*exampleBot*-chimebot@*example.com*。

步骤 2：为 Amazon Chime 聊天机器人配置出站端点

为 Amazon Chime 企业账户创建聊天机器人 ID 后，继续配置出站端点，以便 Amazon Chime 向机器人发送消息。此出站端点可以是 AWS Lambda 函数 ARN，也可以是在先决条件中创建的 HTTPS 端点。有关 Lambda 的更多信息，请参阅 AWS Lambda 开发人员指南。

> **Note**
>
> 如果机器人的 HTTPS 出站端点未配置或者为空，则聊天室管理员无法将其加入聊天室。同时，聊天室用户也无法与机器人互动。

AWS CLI

如需为聊天机器人配置出站端点，请运行 AWS CLI 中的 put-events-configuration 命令。配置 Lambda 函数 ARN 或 HTTPS 出站端点。

Lambda ARN

```
aws chime put-events-configuration --account-id 12a3456b-7c89-012d-3456-78901e23fg45
 --bot-id botId --lambda-function-arn arn:aws:lambda:us-
east-1:111122223333:function:function-name
```

HTTPS endpoint

```
aws chime put-events-configuration --account-id 12a3456b-7c89-012d-3456-78901e23fg45
 --bot-id botId --outbound-events-https-endpoint https://example.com:8000
```

Amazon Chime 使用机器人 ID 和 HTTPS 端点进行响应。

```
{
    "EventsConfiguration": {
        "BotId": "BotId",
        "OutboundEventsHTTPSEndpoint": "https://example.com:8000"
    }
```

```
}
```

Amazon Chime API

如需为聊天机器人配置出站端点，请在 Amazon Chime API 参考中执行 Amazon Chime PutEventsConfiguration API 操作。配置 Lambda 函数 ARN 或 HTTPS 出站端点。

- 如需配置 Lambda 函数 ARN：Amazon Chime 调用 Lambda 以添加权限，允许其管理员的 AWS 账户调用提供的 Lambda 函数 ARN。然后实施试运行调用，以验证 Amazon Chime 是否有权调用此函数。如果权限添加失败或者试运行调用失败，则 `PutEventsConfiguration` 请求将返回 HTTP 4xx 错误。
- 如需配置 HTTPS 出站端点：Amazon Chime 使用 Challenge JSON 有效负载，向上一步提供的 HTTPS 出站端点发送 HTTP Post 请求以验证端点。您的出站 HTTPS 端点必须使用 JSON 格式来回应质询参数，从而进行响应。下面的示例显示了请求和有效的响应。

  Request

  ```
  HTTPS POST

  JSON Payload:
  {
     "Challenge":"00000000000000000000",
     "EventType" : "HTTPSEndpointVerification"
  }
  ```

  Response

  ```
  HTTP/1.1 200 OK
  Content-type: application/json

  {
      "Challenge":"00000000000000000000"
  }
  ```

  如果质询握手失败，则 `PutEventsConfiguration` 请求将返回 HTTP 4xx 错误。

AWS SDK for Java

以下示例代码演示了如何使用适用于 Java 的 AWS SDK 进行端点配置。

```
PutEventsConfigurationRequest putEventsConfigurationRequest = new
 PutEventsConfigurationRequest()
     .withAccountId("chimeAccountId")
     .withBotId("botId")
     .withOutboundEventsHTTPSEndpoint("https://www.example.com")
     .withLambdaFunctionArn("arn:aws:lambda:region:account-id:function:function-name");

 chime.putEventsConfiguration(putEventsConfigurationRequest);
```

步骤 3：为 Amazon Chime 聊天室添加聊天机器人

只有聊天室管理员才能为聊天室添加聊天机器人。管理员会使用 步骤 1 中为聊天机器人创建的电子邮件地址。

在聊天室中添加聊天自动程序

1. 打开 Amazon Chime 桌面客户端或 Web 应用程序。
2. 选择右上角的齿轮图标，然后选择管理 Webhook 和机器人。
3. 选择 Add bot (添加自动程序)。
4. 在电子邮件地址中输入您的电子邮件地址。
5. 选择 Add（添加）。

自动程序名称将会出现在聊天室名单中。如果必须执行其他操作后才能为聊天室添加聊天机器人，请向聊天室管理员说明此类操作。

聊天机器人添加至聊天室后，为聊天室用户提供机器人运行命令。完成这项任务的一种方法是设定聊天机器人程序，使其在收到聊天室邀请时向聊天室发送命令帮助。此外，AWS 还建议您为聊天机器人用户创建帮助命令。

对聊天机器人请求进行身份验证

您可以对 Amazon Chime 聊天室向聊天机器人发送的请求进行身份验证。为此，请根据请求计算签名。然后，验证计算得出的签名是否与请求标题中的签名相匹配。Amazon Chime 使用 HMAC SHA256 哈希生成签名。

如果使用 HTTPS 出站端点配置 Amazon Chime 聊天机器人，请采用以下身份验证步骤。

为配有 HTTPS 出站端点的聊天机器人验证 Amazon Chime 签名请求

1. 从 HTTP 请求中获取 Chime-Signature 标头。
2. 获取请求的 Chime-Request-Timestamp 标头和 body (正文)。然后，在这两个元素之间使用竖线作为分隔符以形成一个字符串。
3. 使用 CreateBot 响应中的 SecurityToken 作为 HMAC_SHA_256 的初始键，然后对在第 2 步中创建的字符串进行哈希操作。
4. 使用 Base64 编码器对上述哈希字节编码为一个签名字符串。
5. 将此计算得到的签名与 Chime-Signature 标头中的签名进行比较。

下面的代码示例演示了如何使用 Java 生成签名。

```
       private final String DELIMITER = "|";
       private final String HMAC_SHA_256 = "HmacSHA256";

       private String generateSignature(String securityToken, String requestTime,
String requestBody)
       {
           try {
               final Mac mac = Mac.getInstance(HMAC_SHA_256);
               SecretKeySpec key = new SecretKeySpec(securityToken.getBytes(UTF_8),
HMAC_SHA_256);
               mac.init(key);
               String data = requestTime + DELIMITER + requestBody;
               byte[] rawHmac = mac.doFinal(data.getBytes(UTF_8));

               return Base64.getEncoder().encodeToString(rawHmac);
               }
           catch (Exception e) {
               throw e;
               }
        }
```

HTTPS 出站端点必须在 2 秒内通过 200 OK 响应 Amazon Chime 请求。否则，请求将失败。如果 HTTPS 出站端点（因连接问题或读取超时）超过 2 秒不可用，或如果 Amazon Chime 收到 5xx 响应代码，则 Amazon Chime 会重发两次请求。在初始请求失败 200 毫秒后将发送第一次重试请求。在第

一次重试请求失败 400 毫秒后发送第二次重试请求。如果在第二次重试之后出站 HTTPS 端点仍不可用，则请求失败。

> **Note**
>
> 每当重试请求时，Chime-Request-Timestamp 都会发生更改。

如果使用 Lambda 函数 ARN 配置 Amazon Chime 聊天机器人，请采用以下身份验证步骤。

为配有 Lambda 函数 ARN 的聊天机器人验证 Amazon Chime 签名请求

1. 使用经过 Base64 编码的 JSON 格式，从 Lambda 请求 ClientContext 中获取 Chime-Signature 和 Chime-Request-Timestamp。

   ```
   {
   "Chime-Signature" : "1234567890",
   "Chime-Request-Timestamp" : "2019-04-04T21:30:43.181Z"
   }
   ```

2. 从请求负载中获取请求的 body (正文)。
3. 将 `CreateBot` 响应结果中的 SecurityToken 作为 HMAC_SHA_256 的初始键，然后对已创建的字符串执行哈希操作。
4. 使用 Base64 编码器对上述哈希字节编码为一个签名字符串。
5. 将此计算得到的签名与 Chime-Signature 标头中的签名进行比较。

如果在调用 Lambda 时发生 `com.amazonaws.SdkClientException`，Amazon Chime 会重发两次请求。

更新聊天机器人

作为 Amazon Chime 账户管理员，您可以使用具有 AWS SDK 或 AWS CLI 的 Amazon Chime API 查看聊天机器人的详细信息。您也可以启用或停用账户中的聊天机器人。还可以为聊天机器人重新生成安全令牌。

有关更多信息，请参阅《Amazon Chime API 参考》中的以下主题：

- GetBot：获取聊天机器人的详细信息，如电子邮件地址和机器人类型。
- UpdateBot：启用或停用账户中的聊天机器人。

- RegenerateSecurityToken：为聊天机器人重新生成安全令牌。

您还可以为聊天机器人更改 PutEventsConfiguration。例如，如果聊天机器人在初始配置中可以使用 HTTPS 出站端点，则您可以删除之前的事件配置，重新为 Lambda 函数 ARN 设置事件配置。

有关更多信息，请参阅《Amazon Chime API 参考》中的以下主题：

- DeleteEventsConfiguration
- PutEventsConfiguration

发送给聊天机器人的 Amazon Chime 事件

以下事件均由 Amazon Chime 发送给聊天机器人：

- 邀请：在为 Amazon Chime 聊天室添加聊天机器人时发送的事件
- 提及：在聊天室用户对聊天机器人执行 @mentions 操作时发送的事件
- 移除：在移除 Amazon Chime 聊天室中的聊天机器人时发送的事件

以下示例显示了在发生上述事件时，聊天机器人收到的 JSON 格式的有效负载。

Example ：邀请事件

```
            {
              "Sender": {
                           "SenderId": "user@example.com",
                           "SenderIdType": "EmailId"
                         },
              "Discussion": {
                           "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
                           "DiscussionType": "Room"
                           },
              "EventType": "Invite",
              "InboundHttpsEndpoint": {
                                        "EndpointType": "Persistent",
                                        "Url": "https://
hooks.a.chime.aws/incomingwebhooks/a1b2c34d-5678-90e1-f23g-h45i67j8901k?
token=ABCDefGHiJK1LMnoP2Q3RST4uvwxYZAbC56DeFghIJkLM7N8OP9QRsTuV0WXYZABcdefgHiJ"
                                      },
              "EventTimestamp": "2019-04-04T21:27:52.736Z"
```

```
            }
```

Example ：提及事件

```
            {
                "Sender": {
                            "SenderId": "user@example.com",
                            "SenderIdType": "EmailId"
                          },
                "Discussion": {
                                "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
                                "DiscussionType": "Room"
                              },
                "EventType": "Mention",
                "InboundHttpsEndpoint": {
                                            "EndpointType": "ShortLived",
                                            "Url": "https://
hooks.a.chime.aws/incomingwebhooks/a1b2c34d-5678-90e1-f23g-h45i67j8901k?
token=ABCDefGHiJK1LMnoP2Q3RST4uvwxYZAbC56DeFghIJkLM7N8OP9QRsTuV0WXYZABcdefgHiJ"
                                        },
                "EventTimestamp": "2019-04-04T21:30:43.181Z",
                "Message": "@botDisplayName@example.com Hello Chatbot"
            }
```

> **Note**
>
> 有关提及事件的 InboundHttpsEndpoint URL 将在发送 2 分钟后过期。

Example ：移除事件

```
            {
                "Sender": {
                            "SenderId": "user@example.com",
                            "SenderIdType": "EmailId"
                          },
                "Discussion": {
                                "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
```

```
                        "DiscussionType": "Room"
                    },
        "EventType": "Remove",
        "EventTimestamp": "2019-04-04T21:27:29.626Z"
    }
```

创建适用于 Amazon Chime 的 Webhook

Webhook 允许 Web 应用程序互相进行实时通信。Webhook 通常会在操作时发送通知。例如，假设您运营着一个在线购物网站。当客户为购物车添加商品、为订单付款或发送评论时，您会收到 Webhook 的通知。Webhook 不需要像传统应用程序那样进行大量编程，也不会耗费太多的处理能力。没有 webhook 的程序必须定期轮询才能实时获取数据。具有 webhook 的发送应用程序则可以立即发布数据。

您创建的入站 Webhook 能够以编程方式向 Amazon Chime 聊天室发送消息。例如，Webhook 可以通知客户服务团队有关创建新的高优先级服务单的内容以及在聊天室中添加指向该服务单的链接。

Webhooks 消息可通过 markdown 进行格式设置并且可以包含表情符号。HTTP 链接和电子邮件地址会显示为活跃链接。消息还可以包括 @All 和 @Present 注释以分别提醒聊天室内的所有成员和在线成员。要直接 @ 提及某个聊天室参与者，请使用其别名或完整的电子邮件地址。例如，`@alias` 或 `@alias@domain.com`。

Webhook 只是聊天室中不支持共享的一种功能。Amazon Chime 聊天室管理员可以为每个聊天室添加最多 10 个 Webhook。

根据以下流程，您可以将创建的 Webhook 集成至 Amazon Chime 聊天室。

将 Webhook 集成至聊天室

1. 从聊天室管理员处获取 Webhook URL。有关更多信息，请参阅《Amazon Chime 用户指南》中的将 Webhook 添加到聊天室。
2. 您可以使用脚本或应用程序中创建的 Webhook URL 向聊天室发送消息：

    a. URL 接受 HTTP POST 请求。

    b. Amazon Chime Webhook 接受含有单一密钥内容的 JSON 有效负载。以下是带示例负载的示例 curl 命令：

```
curl -X POST "<Insert your webhook URL here>" -H "Content-Type:application/
json" --data '{"Content":"Message Body emoji test: :) :+1: link test: http://
```

```
sample.com email test: marymajor@example.com All member callout: @All All
 Present member callout: @Present"}'
```

下面是一个针对 Windows 用户的示例 PowerShell 命令：

```
Invoke-WebRequest -Uri '<Insert your webhook URL here>' -Method 'Post' -
ContentType 'application/JSON' -Body '{"Content":"Message Body emoji test: :) :
+1: link test: http://sample.com email test: marymajor@example.com All member
 callout: @All All Present member callout: @Present"}'
```

在外部程序将 HTTP POST 发送到 Webhook URL 之后，服务器会验证 Webhook 是否有效且具有已分配的聊天室。Webhook 出现在聊天室花名册中，其名称旁边带有一个 Webhook 图标。Webhook 发送的聊天室消息出现在 Webhook 名称下的聊天室中，后跟 (Webhook)。

> **Note**
>
> 当前没有为 Webhooks 启用 CORS。

排查 Webhook 错误

以下是与 Webhook 相关的错误的列表：

- 每个 Webhook 的传入 Webhook 速率限制为每个聊天室 1 TPS。限制会导致 HTTP 429 错误。
- 由一个 Webhook 发布的消息必须为 4 KB 或更小。较大的消息负载会导致 HTTP 413 错误。
- 具有 @All 和 @Present 注释的 Webhook 所发布的消息仅适用于具有 50 个或更少成员的聊天室。超过 50 个成员会导致 HTTP 400 错误。
- 如果重新生成 Webhook URL，使用旧的 URL 会导致 HTTP 404 错误。
- 如果删除房间内的 Webhook，使用旧的 URL 会导致 HTTP 404 错误。
- 无效的 Webhook URL 会导致 HTTP 403 错误。
- 如果服务不可用，用户会在响应中收到 HTTP 503 错误。

Amazon Chime 的管理支持

> **Note**
>
> 如需有关亚马逊购物账户的帮助，请前往 amazon.com 上的客户服务。

如果您需要联系 Amazon Chime 的支持人员，请选择以下选项之一：

- 如果您有 AWS 支持帐户，请前往支持中心并提交工单。
- 否则，请打开 AWS Management Console 并依次选择 Amazon Chime、支持和提交请求。

尽可能多地提供以下信息：

- 问题的详细说明。
- 发生问题的时间，包括您的时区。
- 您使用的 Amazon Chime 版本。要查找您的版本号，请执行以下操作：
  - 在 Windows 中，依次选择帮助和关于 Amazon Chime。
  - 在 macOS 中，依次选择 Amazon Chime、About Amazon Chime (关于 Amazon Chime)。
  - 在 iOS 和 Android 中，依次选择 Settings (设置)、About (关于)。
- 日志引用 ID。要查找此 ID，请执行以下操作：
  - 在 Windows 和 macOS 中，依次选择 Help (帮助)、Send Diagnostic Logs (发送诊断日志)。
  - 在 iOS 和 Android 中，依次选择 Settings (设置)、Send Diagnostic Logs (发送诊断日志)。
- 如果您的问题与会议有关，则还需要提供会议 ID。

Amazon Chime 的安全性

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方 AWS 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：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用于 Amazon Chime 的合规性计划，请参阅合规性计划范围内的 AWS 服务。
- 云端安全-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。

此文档帮助您了解如何在使用 Amazon Chime 时应用责任共担模式。以下主题说明了如何配置 Amazon Chime 才能实现安全性和合规性目标。您还将学习如何使用其他 AWS AWS 服务来帮助您监控和保护您的 Amazon Chime 资源。

主题

- 适用于 Amazon Chime 的身份和访问管理
- Amazon Chime 如何与 IAM 配合使用
- 防止跨服务混淆代理
- Amazon Chime 基于资源的策略
- 基于 Amazon Chime 标签的授权
- Amazon Chime IAM 角色
- Amazon Chime 基于身份的策略示例
- Amazon Chime 身份和访问问题排查
- 使用适用于 Amazon Chime 的服务相关角色
- Amazon Chime 的日志记录和监控
- Amazon Chime 的合规性验证
- Amazon Chime 中的恢复能力
- Amazon Chime 中的基础设施安全性
- 了解 Amazon Chime 自动更新

适用于 Amazon Chime 的身份和访问管理

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员负责把控经过身份验证（已登录）且获得授权（具有权限）的用户，允许其使用 Amazon Chime 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 Amazon Chime 中所做的工作。

服务用户：如果您使用 Amazon Chime 执行操作，则管理员会提供所需凭证和权限。随着执行操作需要的 Amazon Chime 功能越来越多，您可能需要获得其他权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果无法使用 Amazon Chime 的功能，请参阅 Amazon Chime 身份和访问问题排查。

服务管理员：如果您负责管理 Amazon Chime 企业资源，则可能对 Amazon Chime 具有完全访问权限。您有义务为服务用户确定可访问的 Amazon Chime 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。有关公司如何结合使用 IAM 与 Amazon Chime 的更多信息，请参阅 Amazon Chime 如何与 IAM 配合使用。

IAM 管理员：如果您是 IAM 管理员，则可能希望了解如何编写策略，才能管理有关 Amazon Chime 访问权限的详细信息。要查看 IAM 支持使用的 Amazon Chime 基于身份的示例策略，请参阅 Amazon Chime 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 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。

当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的 多重身份验证和《IAM 用户指南》中的 在 AWS中使用多重身份验证（MFA）。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关需要您以根用户身份登录的任务的完整列表，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

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的何时创建 IAM 用户（而不是角色）。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或

AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的 权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅 IA M 用户指南中的跨账户资源访问。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service (Amazon S3) 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。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。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM policy，用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的创建 IAM policy。

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。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。基于资源的策略的示例包括 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。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

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 IAM 中的 AWS 托管策略。

AWS Amazon Chime 的托管政策

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。这些策略涵盖常见应用场景，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 服务维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务偶尔会向 AWS 托管策略添加其他权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当推出新功能或有新操作可用时，服务最有可能更新 AWS 托管策略。服务不会从 AWS 托管策略中移除权限，因此策略更新不会破坏您的现有权限。

此外，还 AWS 支持跨多个服务的工作职能的托管策略。例如，ReadOnly访问 AWS 管理策略提供对所有 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 管理型策略。

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 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF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 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，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)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP

限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 SCP 的工作原理。

- 会话策略 – 会话策略是当您以编程方式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。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。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。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

Amazon Chime 如何与 IAM 配合使用

在使用 IAM 管理 Amazon Chime 访问权限之前，应先了解可用于 Amazon Chime 的 IAM 功能。要全面了解 Amazon Chime 和其他 AWS 服务如何与 IAM 配合使用，请参阅 IAM 用户指南中与 IAM 配合使用的AWS 服务。

主题

- Amazon Chime 基于身份的策略
- 资源
- 示例

Amazon Chime 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 Chime 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。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。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

条件键

Amazon Chime 不提供任何服务专用的条件键。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。

资源

Amazon Chime 不支持在策略中指定资源 ARN。

示例

要查看 Amazon Chime 基于身份的策略示例，请参阅 Amazon Chime 基于身份的策略示例。

防止跨服务混淆代理

混淆代理问题属于信息安全问题，当无权执行操作的实体调用权限更高的实体代为执行操作时，就会出现这个问题。恶意行为者会借此机会运行原本无权运行的命令或修改原本无权访问的资源。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的混淆代理问题。

在中 AWS，跨服务模仿可能会导致副手场景混乱。当一项服务（调用服务）调用另一项服务（被调用服务）时，就会发生跨服务模拟。恶意行为者可以使用平时无法获取的权限，利用调用服务改变另一项服务中心的资源。

AWS 为服务委托人提供对您账户中资源的托管访问权限，以帮助您保护资源的安全。亚马逊建议您在资源策略中使用 `aws:SourceAccount` 全局条件上下文键。这些键会限制 Amazon Chime 赋予其他服务访问该资源的权限。

以下示例显示了 S3 存储桶策略，在经过配置的 `CallDetailRecords` S3 存储桶中使用 `aws:SourceAccount` 全局条件上下文键，以免出现混淆代理问题。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonChimeAclCheck668426",
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": "chime.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::your-cdr-bucket"
        },
        {
            "Sid": "AmazonChimeWrite668426",
            "Effect": "Allow",
            "Principal": {
                "Service": "chime.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::your-cdr-bucket/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": "112233446677"
                }
            }
        }
    ]
}
```

Amazon Chime 基于资源的策略

Amazon Chime 不支持基于资源的策略。

基于 Amazon Chime 标签的授权

Amazon Chime 不支持基于标签标记资源或控制访问权限。

Amazon Chime IAM 角色

I AM 角色是您的 AWS 账户中具有特定权限的实体。

结合使用临时凭证和 Amazon Chime

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。您可以通过调用 AWS STS API 操作（例如AssumeRole或GetFederation令牌）来获取临时安全证书。

Amazon Chime 支持使用临时凭证。

服务相关角色

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

Amazon Chime 支持服务相关角色。有关创建或管理 Amazon Chime 服务相关角色的详细信息，请参阅 使用适用于 Amazon Chime 的服务相关角色。

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 Chime 不支持服务角色。

Amazon Chime 基于身份的策略示例

IAM 用户和角色默认无权创建或修改 Amazon Chime 资源。他们也无法使用 AWS Management Console 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 Chime 控制台
- 允许用户完全访问 Amazon Chime
- 允许用户查看他们自己的权限
- 允许用户访问用户管理操作
- AWS 托管策略： AmazonChimeVoiceConnectorServiceLinkedRolePolicy
- Amazon Chime 更新了托管政策 AWS

策略最佳实践

基于身份的策略可确定用户是否有权创建、访问或删除您账户中的 Amazon Chime 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：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管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 托管策略 或 工作职能的AWS 托管策略。
- 应用最低权限 – 在使用 IAM policy 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 policy 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。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。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 policy，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 policy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 IAM Acess Analyzer 策略验证。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。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 配置受 MFA 保护的 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 中的安全最佳实操。

使用 Amazon Chime 控制台

要访问 Amazon Chime 控制台，您必须具有一组最低级别的权限。这些权限必须允许您列出和查看有关您 AWS 账户中的 Amazon Chime 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。

为确保这些实体仍然可以使用 Amazon Chime 控制台，还需要将以下 AWS 托管AmazonChimeReadOnly策略附加到这些实体。有关更多信息，请参阅 IAM 用户指南中的为用户添加权限：

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "chime:List*",
                "chime:Get*",
                "chime:SearchAvailablePhoneNumbers"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与您尝试执行的 API 操作相匹配的操作。

允许用户完全访问 Amazon Chime

以下 AWS 托管AmazonChimeFullAccess策略授予 IAM 用户对 Amazon Chime 资源的完全访问权限。此策略可授予用户对 Amazon Chime 的所有操作以及需要代表您执行的其他操作的访问权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "chime:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketVersioning",
                "s3:GetBucketWebsite"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        },
        {
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:GetLogDelivery",
                "logs:ListLogDeliveries",
                "logs:DescribeResourcePolicies",
                "logs:PutResourcePolicy",
                "logs:CreateLogGroup",
                "logs:DescribeLogGroups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes"
            ],
            "Resource": [
                "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sqs:GetQueueAttributes",
                "sqs:CreateQueue"
            ],
            "Resource": [
                "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
            ]
        }
    ]
}
```

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策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "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": "*"
        }
    ]
}
```

允许用户访问用户管理操作

使用 AWS 托管AmazonChimeUserManagement策略向用户授予在 Amazon Chime 控制台中访问用户管理操作的权限。

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

```
            "Action": [
                "chime:ListAccounts",
                "chime:GetAccount",
                "chime:GetAccountSettings",
                "chime:UpdateAccountSettings",
                "chime:ListUsers",
                "chime:GetUser",
                "chime:GetUserByEmail",
                "chime:InviteUsers",
                "chime:InviteUsersFromProvider",
                "chime:SuspendUsers",
                "chime:ActivateUsers",
                "chime:UpdateUserLicenses",
                "chime:ResetPersonalPIN",
                "chime:LogoutUser",
                "chime:ListDomains",
                "chime:GetDomain",
                "chime:ListDirectories",
                "chime:ListGroups",
                "chime:SubmitSupportRequest",
                "chime:ListDelegates",
                "chime:ListAccountUsageReportData",
                "chime:GetMeetingDetail",
                "chime:ListMeetingEvents",
                "chime:ListMeetingsReportData",
                "chime:GetUserActivityReportData",
                "chime:UpdateUser",
                "chime:BatchUpdateUser",
                "chime:BatchSuspendUser",
                "chime:BatchUnsuspendUser",
                "chime:AssociatePhoneNumberWithUser",
                "chime:DisassociatePhoneNumberFromUser",
                "chime:GetPhoneNumber",
                "chime:ListPhoneNumbers",
                "chime:GetUserSettings",
                "chime:UpdateUserSettings",
                "chime:CreateUser",
                "chime:AssociateSigninDelegateGroupsWithAccount",
                "chime:DisassociateSigninDelegateGroupsFromAccount"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

AWS 托管策略： AmazonChimeVoiceConnectorServiceLinkedRolePolicy

Amazon Chime Voice Connector 可通过 `AmazonChimeVoiceConnectorServiceLinkedRolePolicy` 将媒体流式传输到 Amazon Kinesis Video Streams，从而发送流式传输通知并使用 Amazon Polly 合成语音。此策略授予 Amazon Chime Voice Connector 以下服务权限：访问客户的 Amazon Kinesis Video Streams、向 Amazon Simple Notification Service 和 Amazon Simple Queue Service 发送通知事件，以及在执行 Amazon Chime SDK 语音应用程序的 `Speak` 和 `SpeakAndGetDigits` 操作时使用 Amazon Polly 合成语音。有关更多信息，请参阅《Amazon Chime SDK 管理指南》中的 Amazon Chime SDK 基于身份的策略示例。

Amazon Chime 更新了托管政策 AWS

下表列出并描述了 Amazon Chime IAM 策略的更新内容。

更改	描述	日期
`AmazonChimeVoiceConnectorServiceLinkedRolePolicy` – 对现有策略的更新	Amazon Chime Voice Connector 的新增权限允许您使用 Amazon Polly 合成语音。必须具有这些权限，才能执行 Amazon Chime SDK 语音应用程序的 `Speak` 和 `SpeakAndGetDigits` 操作。	2022 年 3 月 15 日
`AmazonChimeVoiceConnectorServiceLinkedRolePolicy` – 更新了现有策略	Amazon Chime Voice Connector 的新增权限允许您访问 Amazon Kinesis Video Streams 并向 SNS 和 SQS 发送通知事件。Amazon Chime Voice Connector 必须具有这些权限，才能向 Amazon Kinesis Video Streams 流式传输媒体并发送流式通知。	2021 年 12 月 20 日

更改	描述	日期
现有策略更改内容。使用 Chime SDK 策略创建 IAM 用户或角色。	Amazon Chime 的新增操作支持扩展验证。 新增的大量操作允许列出并标记与会者和会议资源，且允许启动和停止会议转录操作。	2021 年 9 月 23 日
Amazon Chime 启动跟踪更改	Amazon Chime 开始跟踪其 AWS 托管政策的变更。	2021 年 9 月 23 日

Amazon Chime 身份和访问问题排查

以下信息有助于您诊断并修复在使用 Amazon Chime 和 IAM 时会遇到的常见问题。

主题

- 我无权在 Amazon Chime 中执行操作
- 我无权执行 iam：PassRole
- 我想允许 AWS 账户之外的用户访问我的 Amazon Chime 资源

我无权在 Amazon Chime 中执行操作

如果您收到错误提示，表明您无权执行某个操作，则您必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 chime:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 chime:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 chime:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到提示自己无权执行 iam:PassRole 操作的错误消息，则必须更新策略以获得向 Amazon Chime 传递角色的权限。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的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 Chime 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，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许 AWS 账户之外的用户访问我的 Amazon Chime 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，可以担任角色。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 Chime 是否支持这些功能，请参阅 Amazon Chime 如何与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（联合身份验证）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的区别，请参阅 IA M 用户指南中的跨账户资源访问。

使用适用于 Amazon Chime 的服务相关角色

Amazon Chime 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种特殊的 IAM 角色类型，直接关联到 Amazon Chime。服务相关角色经过 Amazon Chime 预定义，包含服务代表您调用其他 AWS 服务所需的所有权限。

您不需要手动为服务相关角色添加所需权限，可以更轻松地设置 Amazon Chime。Amazon Chime 负责定义其服务相关角色的权限，除非另有定义，否则只有 Amazon Chime 可以代入此角色。定义的权限包括信任策略和权限策略。不能将该权限策略附加到任何其他 IAM 实体。

只有在首先删除相关资源后，才能删除服务相关角色。这样可以避免误删资源访问权限，保护您的 Amazon Chime 资源。

有关支持服务相关角色的其他服务的信息，请参阅与 IAM 配合使用的 AWS 服务。查找在 Service-Linked Role（服务相关角色）列中具有 Yes（是）值的服务。选择 Yes（是）与查看该服务的服务相关角色文档的链接。

主题

- 通过企业版 Alexa 共享设备使用角色
- 使用具有实时转录功能的角色
- 通过 Amazon Chime SDK 媒体管道使用角色

通过企业版 Alexa 共享设备使用角色

以下章节介绍了如何使用服务相关角色，以及如何授予 Amazon Chime 访问 AWS 账户中企业版 Alexa 资源的权限。

主题

- 适用于 Amazon Chime 的服务相关角色权限
- 为 Amazon Chime 创建服务相关角色
- 为 Amazon Chime 编辑服务相关角色
- 删除适用于 Amazon Chime 的服务相关角色
- Amazon Chime 服务相关角色支持的区域

适用于 Amazon Chime 的服务相关角色权限

Amazon Chime 使用名为 AWSServiceRoleForAmazonChime 的服务相关角色，允许访问由 Amazon Chime 使用或托管的 AWS 服务和资源，如企业版 Alexa 共享设备。

AWSServiceRoleForAmazonChime 服务相关角色信任以下角色代入服务：

- `chime.amazonaws.com`

角色权限策略允许 Amazon Chime 对指定资源执行以下操作：

- 操作：`arn:aws:iam::*:role/aws-service-role/chime.amazonaws.com/AWSServiceRoleForAmazonChime` 上的 `iam:CreateServiceLinkedRole`

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 Chime 创建服务相关角色

无需手动创建服务相关角色。Amazon Chime 会在您为 AWS Management Console、AWS CLI 或 AWS API 中的 Amazon Chime 共享设备启用企业版 Alexa 时，为您创建服务相关角色。

您也可以通过 IAM 控制台，使用 Amazon Chime 用例创建服务相关角色。在 AWS CLI 或 AWS API 中，使用 `chime.amazonaws.com` 服务名称创建服务相关角色。有关更多信息，请参阅《IAM 用户指南》 中的创建服务相关角色。如果您删除了此服务相关角色，则可以使用此相同过程再次创建角色。

为 Amazon Chime 编辑服务相关角色

Amazon Chime 不允许编辑 AWSServiceRoleForAmazonChime 服务相关角色。创建服务相关角色后，将无法更改角色名称，因为可能有多个实体引用该角色。但是可以使用 IAM 编辑角色说明。有关更多信息，请参阅 IAM 用户指南中的编辑服务相关角色。

删除适用于 Amazon Chime 的服务相关角色

如果您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。这样您就没有未被主动监控或维护的未使用实体。但是，您必须先清除您的服务相关角色，然后才能手动删除它。

清除服务相关角色

必须先删除服务相关角色使用的所有资源，然后才能使用 IAM 删除该角色。

> **Note**
>
> 如果 Amazon Chime 在您尝试删除资源时使用角色，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 AWSServiceRoleForAmazonChime（控制台）所用的 Amazon Chime 资源

- 关闭 Amazon Chime 账户中适用于所有共享设备的企业版 Alexa。
  a. 您可以访问 https://chime.aws.amazon.com/，打开 Amazon Chime 控制台。
  b. 选择 Users (用户)、Shared devices (共享设备)。
  c. 选择设备。
  d. 选择 Actions。
  e. 选择禁用企业版 Alexa。

手动删除 服务相关角色

使用 IAM 控制台、AWS CLI 或 AWS API，删除 AWSServiceRoleForAmazonChime 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 Chime 服务相关角色支持的区域

Amazon Chime 支持在所有服务可用区中使用服务相关角色。有关更多信息，请参阅 Amazon Chime 端点和限额。

使用具有实时转录功能的角色

以下章节介绍了如何为 Amazon Chime 实时转录创建并管理服务相关角色。有关实时转录服务的更多信息，请参阅使用 Amazon Chime SDK 实时转录。

主题

- 适用于 Amazon Chime 实时转录的服务相关角色权限
- 为 Amazon Chime 实时转录创建服务相关角色
- 为 Amazon Chime 实时转录编辑服务相关角色
- 删除适用于 Amazon Chime 实时转录的服务相关角色

- Amazon Chime 服务相关角色支持的区域

适用于 Amazon Chime 实时转录的服务相关角色权限

Amazon Chime 实时转录使用名为 AWSServiceRoleForAmazonChimeTranscription 服务相关角色，允许 Amazon Chime 代表您访问 Amazon Transcribe 和 Amazon Transcribe Medical。

AWSServiceRoleForAmazonChimeTranscription 服务相关角色信任以下角色代入服务：

- `transcription.chime.amazonaws.com`

角色权限策略允许 Amazon Chime 对指定资源执行以下操作：

- 操作：`transcribe:StartStreamTranscription` 上的 `all AWS resources`
- 操作：`all AWS resources` 上的 `transcribe:StartMedicalStreamTranscription`

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 Chime 实时转录创建服务相关角色

您可以使用 IAM 控制台为 Chime 转录用例创建服务相关角色。

> **Note**
>
> 必须具有 IAM 管理权限才能完成这些步骤。如果没有，请联系系统管理员。

创建角色

1. 登录 AWS 管理控制台，并通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在 IAM 控制台的导航窗格中，选择角色，然后选择创建角色。
3. 选择 AWS 服务角色类型，然后依次选择 Chime 和 Chime 转录。
4. 选择 Next（下一步）。
5. 选择 Next（下一步）。
6. 按需编辑描述，然后选择创建角色。

您还可以使用 AWS CLI 或 AWS API，创建名为 transcription.chime.amazonaws.com 的服务相关角色。

在 CLI 中，运行以下命令：`aws iam create-service-linked-role --aws-service-name transcription.chime.amazonaws.com`。

有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。如果您删除了此服务相关角色，则可以使用此相同过程再次创建角色。

为 Amazon Chime 实时转录编辑服务相关角色

Amazon Chime 不允许编辑 AWSServiceRoleForAmazonChimeTranscription 服务相关角色。创建服务相关角色后，将无法更改角色名称，因为可能有多个实体引用该角色。但您可以使用 IAM 编辑角色描述。有关更多信息，请参见 IAM 用户指南中的编辑服务相关角色。

删除适用于 Amazon Chime 实时转录的服务相关角色

如果不再需要使用某个需要服务相关角色的特征或服务，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。

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 AWSServiceRoleForAmazonChimeTranscription 服务相关角色。有关更多信息，请参见 IAM 用户指南中的删除服务相关角色。

Amazon Chime 服务相关角色支持的区域

Amazon Chime 支持在所有服务可用区中使用服务相关角色。有关更多信息，请参阅 Amazon Chime 端点和限额和使用 Amazon Chime SDK 媒体区域。

通过 Amazon Chime SDK 媒体管道使用角色

以下章节介绍了如何为 Amazon Chime SDK 媒体管道创建并管理服务相关角色。

主题

- 适用于 Amazon Chime SDK 媒体管道的服务相关角色权限
- 为 Amazon Chime SDK 媒体管道创建服务相关角色
- 为 Amazon Chime SDK 媒体管道编辑服务相关角色
- 删除适用于 Amazon Chime SDK 媒体管道的服务相关角色
- Amazon Chime SDK 媒体管道服务相关角色支持的区域

适用于 Amazon Chime SDK 媒体管道的服务相关角色权限

Amazon Chime 使用名为 AWSServiceRoleForAmazonChimeSDKMediaPipelines 的服务相关角色，允许 Amazon Chime SDK 媒体管道代表您访问 Amazon Chime SDK 会议。

AWSServiceRoleForAmazonChimeSDKMediaPipelines 服务相关角色信任以下角色代入服务：

- `mediapipelines.chime.amazonaws.com`

此角色允许 Amazon Chime 对指定资源执行以下操作：

- 操作：`all AWS resources` 上的 `chime:CreateAttendee`
- 操作：`chime:DeleteAttendee` 上的 `all AWS resources`
- 操作：`chime:GetMeeting` 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 Chime SDK 媒体管道创建服务相关角色

您可以通过 Amazon Chime SDK 媒体管道*用例，使用 IAM 控制台创建服务相关角色。

> **Note**
>
> 必须具有 IAM 管理权限才能完成这些步骤。如果没有，请联系系统管理员。

创建角色

1. 登录 AWS 管理控制台，并通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在 IAM 控制台的导航窗格中，选择角色，然后选择创建角色。
3. 选择 AWS 服务角色类型，然后依次选择 Chime 和 Chime SDK 媒体管道。
4. 选择 Next（下一步）。
5. 选择 Next（下一步）。
6. 按需编辑描述，然后选择创建角色。

您还可以使用 AWS CLI 或 AWS API，创建名为 mediapipelines.chime.amazonaws.com 的服务相关角色。

在 AWS CLI 中，运行以下命令：`aws iam create-service-linked-role --aws-service-name mediapipelines.chime.amazonaws.com`。

有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。如果您删除了此服务相关角色，则可以使用此相同过程再次创建角色。

为 Amazon Chime SDK 媒体管道编辑服务相关角色

Amazon Chime 不允许编辑 AWSServiceRoleForAmazonChimeSDKMediaPipelines 服务相关角色。创建服务相关角色后，将无法更改角色名称，因为可能有多个实体引用该角色。但是可以使用 IAM 编辑角色说明。有关更多信息，请参见 IAM 用户指南中的编辑服务相关角色。

删除适用于 Amazon Chime SDK 媒体管道的服务相关角色

如果不再需要使用某个需要服务相关角色的特征或服务，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。

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 AWSServiceRoleForAmazonChimeSDKMediaPipelines 服务相关角色。有关更多信息，请参见 IAM 用户指南中的删除服务相关角色。

Amazon Chime SDK 媒体管道服务相关角色支持的区域

Amazon Chime SDK 支持在所有服务可用 AWS 区中使用服务相关角色。有关更多信息，请参阅 Amazon Chime 端点和限额。

Amazon Chime 的日志记录和监控

监控是维护 Amazon Chime 和其他 AWS 解决方案的可靠性、可用性和性能的重要手段。AWS 提供以下工具，用于监控 Amazon Chime、报告问题，并适时自动采取措施。

- Amazon CloudWatch 实时监控 AWS 资源以及运行在 AWS 上的应用程序。您可以收集和跟踪指标，创建自定义的控制面板，以及设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。例如，您可以具有 Amazon EC2 实例的 CloudWatch 跟踪 CPU 使用率或其他指标并且在需要时自动启动新实例。有关更多信息，请参阅 Amazon CloudWatch 用户指南。

- Amazon EventBridge 提供近乎实时的系统事件流，这些系统事件描述了 AWS 资源中的更改。EventBridge 支持自动事件驱动型计算。这使您可以编写规则，以监控某些事件和在这些事件发生时在其他 AWS 服务中触发自动操作。有关更多信息，请参阅 Amazon EventBridge 用户指南。
- Amazon CloudWatch Logs 帮助您监控、存储和访问 Amazon EC2 实例、CloudTrail 和其他来源中的日志文件。CloudWatch Logs 可以监控日志文件中的信息，并在达到特定阈值时通知您。您还可以在高持久性存储中检索您的日志数据。有关更多信息，请参阅 Amazon CloudWatch Logs 用户指南。
- AWS CloudTrail 捕获由某个 AWS 账户发出或代表该账户发出的 API 调用和相关事件。然后它将日志文件传送到您指定的 Amazon S3 存储桶。您可以标识哪些用户和账户调用了 AWS、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 AWS CloudTrail 用户指南。

主题

- 使用 Amazon CloudWatch 监控 Amazon Chime
- 使用 EventBridge 自动执行 Amazon Chime
- 使用 AWS CloudTrail 记录 Amazon Chime API 调用

使用 Amazon CloudWatch 监控 Amazon Chime

您可以使用 CloudWatch 监控 Amazon Chime。CloudWatch 会收集原始数据并将其处理为可读且近实时的指标。这些统计数据会保存 15 个月，从而使您能够访问历史信息，并能够更好地了解您的 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。

适用于 Amazon Chime 的 CloudWatch 指标

Amazon Chime 会向 CloudWatch 发送以下指标。

`AWS/ChimeVoiceConnector` 命名空间包括以下指标，其适用于分配给 AWS 账户和 Amazon Chime Voice Connector 的电话号码。

指标	描述
`InboundCallAttempts`	尝试的入站呼叫次数。 单位：计数
`InboundCallFailures`	入站呼叫失败次数。

指标	描述
	单位：计数
InboundCallsAnswered	应答的入站呼叫次数。 单位：计数
InboundCallsActive	当前处于活动状态的入站呼叫次数。 单位：计数
OutboundCallAttempts	尝试进行的出站呼叫次数。 单位：计数
OutboundCallFailures	出站呼叫失败的次数。 单位：计数
OutboundCallsAnswered	应答的出站呼叫次数。 单位：计数
OutboundCallsActive	当前处于活动状态的出站呼叫次数。 单位：计数
Throttles	尝试进行呼叫时，您的账户受到限制的次数。 单位：计数
Sip1xxCodes	具有 1xx 级状态代码的 SIP 消息数。 单位：计数
Sip2xxCodes	具有 2xx 级状态代码的 SIP 消息数。 单位：计数
Sip3xxCodes	具有 3xx 级状态代码的 SIP 消息数。 单位：计数

指标	描述
Sip4xxCodes	具有 4xx 级状态代码的 SIP 消息数。 单位：计数
Sip5xxCodes	具有 5xx 级状态代码的 SIP 消息数。 单位：计数
Sip6xxCodes	具有 6xx 级状态代码的 SIP 消息数。 单位：计数
CustomerToVcRtpPackets	客户发送到 Amazon Chime Voice Connector 基础设施的 RTP 数据包数。 单位：计数
CustomerToVcRtpBytes	客户在 RTP 数据包中发送到 Amazon Chime Voice Connector 基础设施的字节数。 单位：计数
CustomerToVcRtcpPackets	客户发送到 Amazon Chime Voice Connector 基础设施的 RTCP 数据包数。 单位：计数
CustomerToVcRtcpBytes	客户在 RTCP 数据包中发送到 Amazon Chime Voice Connector 基础设施的字节数。 单位：计数
CustomerToVcPacketsLost	客户发送到 Amazon Chime Voice Connector 基础设施的传输过程中丢失的数据包数。 单位：计数

指标	描述
CustomerToVcJitter	客户发送到 Amazon Chime Voice Connector 基础设施的数据包的平均抖动。 单位：微秒
VcToCustomerRtpPackets	Amazon Chime Voice Connector 基础设施发送到客户的 RTP 数据包数。 单位：计数
VcToCustomerRtpBytes	在 RTP 数据包中 Amazon Chime Voice Connector 基础设施发送到客户的字节数。 单位：计数
VcToCustomerRtcpPackets	Amazon Chime Voice Connector 基础设施发送到客户的 RTCP 数据包数。 单位：计数
VcToCustomerRtcpBytes	在 RTCP 数据包中 Amazon Chime Voice Connector 基础设施发送到客户的字节数。 单位：计数
VcToCustomerPacketsLost	Amazon Chime Voice Connector 基础设施发送到客户的传输过程中丢失的数据包数。 单位：计数
VcToCustomerJitter	Amazon Chime Voice Connector 基础设施发送到客户的数据包的平均抖动。 单位：微秒
RTTBetweenVcAndCustomer	客户与 Amazon Chime Voice Connector 基础设施之间的平均往返时间。 单位：微秒

指标	描述
MOSBetweenVcAndCustomer	客户与 Amazon Chime Voice Connector 基础设施之间的语音流关联的估计平均意见得分 (MOS)。 单位：得分，介于 1.0 到 4.4 之间。分数越高表示感知的音频质量越好。
RemoteToVcRtpPackets	远程端发送到 Amazon Chime Voice Connector 基础设施的 RTP 数据包数。 单位：计数
RemoteToVcRtpBytes	在 RTP 数据包中远程端发送到 Amazon Chime Voice Connector 基础设施的字节数。 单位：计数
RemoteToVcRtcpPackets	远程端发送到 Amazon Chime Voice Connector 基础设施的 RTCP 数据包数。 单位：计数
RemoteToVcRtcpBytes	在 RTCP 数据包中远程端发送到 Amazon Chime Voice Connector 基础设施的字节数。 单位：计数
RemoteToVcPacketsLost	远程端发送到 Amazon Chime Voice Connector 基础设施的传输过程中丢失的数据包数。 单位：计数
RemoteToVcJitter	远程端发送到 Amazon Chime Voice Connector 基础设施的数据包的平均抖动。 单位：微秒

指标	描述
VcToRemoteRtpPackets	Amazon Chime Voice Connector 基础设施发送到远程端的 RTP 数据包数。 单位：计数
VcToRemoteRtpBytes	在 RTP 数据包中 Amazon Chime Voice Connector 基础设施发送到远程端的字节数。 单位：计数
VcToRemoteRtcpPackets	Amazon Chime Voice Connector 基础设施发送到远程端的 RTCP 数据包数。 单位：计数
VcToRemoteRtcpBytes	在 RTCP 数据包中 Amazon Chime Voice Connector 基础设施发送到远程端的字节数。 单位：计数
VcToRemotePacketsLost	Amazon Chime Voice Connector 基础设施发送到远程端的传输过程中丢失的数据包数。 单位：计数
VcToRemoteJitter	Amazon Chime Voice Connector 基础设施发送到远程端的数据包的平均抖动。 单位：微秒
RTTBetweenVcAndRemote	远程端与 Amazon Chime Voice Connector 基础设施之间的平均往返时间。 单位：微秒

指标	描述
MOSBetweenVcAndRemote	远程端与 Amazon Chime Voice Connector 基础设施之间的语音流关联的估计平均意见得分 (MOS)。 单位：得分，介于 1.0 到 4.4 之间。分数越高表示感知的音频质量越好。

适用于 Amazon Chime 的 CloudWatch 维度

可与 Amazon Chime 结合使用的 CloudWatch 维度如下所示。

维度	描述
VoiceConnectorId	用于显示指标的 Amazon Chime Voice Connector 标识符。
Region	与事件关联的 AWS 区域。

适用于 Amazon Chime 的 CloudWatch Logs

您可以向 CloudWatch Logs 发送 Amazon Chime Voice Connector 指标。有关更多信息，请参阅《Amazon Chime SDK 管理指南》中的编辑 Amazon Chime Voice Connector 设置。

媒体质量指标日志

您可以选择接受适用于 Amazon Chime Voice Connector 的媒体质量指标日志。此时，Amazon Chime 会将适用于所有 Amazon Chime Voice Connector 调用的每分钟详细指标发送到专为您创建的 CloudWatch Logs 日志组。日志组名称为 `/aws/ChimeVoiceConnectorLogs/${VoiceConnectorID}`。以下字段以 JSON 格式包含在日志中。

字段	描述
voice_connector_id	传送呼叫的 Amazon Chime Voice Connector ID。

字段	描述
event_timestamp	发出指标的时间，以 UTC 时间的 UNIX 纪元（1970 年 1 月 1 日午夜）开始的毫秒为单位。
call_id	对应事务 ID。
from_sip_user	发出呼叫的用户。
from_country	发出呼叫的国家/地区。
to_sip_user	接收呼叫的用户。
to_country	接收呼叫的国家/地区。
endpoint_id	一个不透明标识符，指明呼叫的其他终端节点。配合 CloudWatch Logs Insights 使用。有关更多信息，请参阅《Amazon CloudWatch Logs 用户指南》中的使用 CloudWatch Logs Insights 分析日志数据。
aws_region	呼叫的 AWS 区域。
cust2vc_rtp_packets	客户发送到 Amazon Chime Voice Connector 基础设施的 RTP 数据包数。
cust2vc_rtp_bytes	客户在 RTP 数据包中发送到 Amazon Chime Voice Connector 基础设施的字节数。
cust2vc_rtcp_packets	客户发送到 Amazon Chime Voice Connector 基础设施的 RTCP 数据包数。
cust2vc_rtcp_bytes	客户在 RTCP 数据包中发送到 Amazon Chime Voice Connector 基础设施的字节数。
cust2vc_packets_lost	客户发送到 Amazon Chime Voice Connector 基础设施的传输过程中丢失的数据包数。
cust2vc_jitter	客户发送到 Amazon Chime Voice Connector 基础设施的数据包的平均抖动。

字段	描述
vc2cust_rtp_packets	Amazon Chime Voice Connector 基础设施发送到客户的 RTP 数据包数。
vc2cust_rtp_bytes	在 RTP 数据包中 Amazon Chime Voice Connector 基础设施发送到客户的字节数。
vc2cust_rtcp_packets	Amazon Chime Voice Connector 基础设施发送到客户的 RTCP 数据包数。
vc2cust_rtcp_bytes	在 RTCP 数据包中 Amazon Chime Voice Connector 基础设施发送到客户的字节数。
vc2cust_packets_lost	Amazon Chime Voice Connector 基础设施发送到客户的传输过程中丢失的数据包数。
vc2cust_jitter	Amazon Chime Voice Connector 基础设施发送到客户的数据包的平均抖动。
rtt_btwn_vc_and_cust	客户与 Amazon Chime Voice Connector 基础设施之间的平均往返时间。
mos_btwn_vc_and_cust	客户与 Amazon Chime Voice Connector 基础设施之间的语音流关联的估计平均意见得分 (MOS)。
rem2vc_rtp_packets	远程端发送到 Amazon Chime Voice Connector 基础设施的 RTP 数据包数。
rem2vc_rtp_bytes	在 RTP 数据包中远程端发送到 Amazon Chime Voice Connector 基础设施的字节数。
rem2vc_rtcp_packets	远程端发送到 Amazon Chime Voice Connector 基础设施的 RTCP 数据包数。
rem2vc_rtcp_bytes	在 RTCP 数据包中远程端发送到 Amazon Chime Voice Connector 基础设施的字节数。

字段	描述
rem2vc_packets_lost	远程端发送到 Amazon Chime Voice Connector 基础设施的传输过程中丢失的数据包数。
rem2vc_jitter	远程端发送到 Amazon Chime Voice Connector 基础设施的数据包的平均抖动。
vc2rem_rtp_packets	Amazon Chime Voice Connector 基础设施发送到远程端的 RTP 数据包数。
vc2rem_rtp_bytes	在 RTP 数据包中 Amazon Chime Voice Connector 基础设施发送到远程端的字节数。
vc2rem_rtcp_packets	Amazon Chime Voice Connector 基础设施发送到远程端的 RTCP 数据包数。
vc2rem_rtcp_bytes	在 RTCP 数据包中 Amazon Chime Voice Connector 基础设施发送到远程端的字节数。
vc2rem_packets_lost	Amazon Chime Voice Connector 基础设施发送到远程端的传输过程中丢失的数据包数。
vc2rem_jitter	Amazon Chime Voice Connector 基础设施发送到远程端的数据包的平均抖动。
rtt_btwn_vc_and_rem	远程端与 Amazon Chime Voice Connector 基础设施之间的平均往返时间。
mos_btwn_vc_and_rem	远程端与 Amazon Chime Voice Connector 基础设施之间的语音流关联的估计平均意见得分 (MOS)。

SIP 消息日志

您可以选择接收 Amazon Chime Voice Connector 的 SIP 消息日志。执行此操作时，Amazon Chime 会捕获出入站的 SIP 消息并将其发送到为您创建的 CloudWatch Logs 日志组。日志组名称为 `/aws/ChimeVoiceConnectorSipMessages/${VoiceConnectorID}`。以下字段以 JSON 格式包含在日志中。

字段	描述
voice_connector_id	Amazon Chime Voice Connector ID。
aws_region	与事件关联的 AWS 区域。
event_timestamp	捕获消息的时间，以 UTC 时间的 UNIX 纪元（1970 年 1 月 1 日午夜）开始的毫秒为单位。
call_id	Amazon Chime Voice Connector 调用 ID。
sip_message	捕获的完整 SIP 消息。

使用 EventBridge 自动执行 Amazon Chime

使用 Amazon EventBridge，您可以自动执行 AWS 服务并响应系统事件，如应用程序可用性问题或资源更改。有关会议事件的更多信息，请参阅《Amazon Chime 开发人员指南》中的会议事件。

当 Amazon Chime 生成事件时，它会将事件发送到 EventBridge，以便尽最大努力传送事件，这意味着 Amazon Chime 会尝试将所有事件发送到 EventBridge，但在极少数情况下，可能无法发送事件。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的 AWS 服务事件。

> **Note**
>
> 如需加密数据，则必须使用 Amazon S3 托管密钥。亚马逊不支持使用存储在 AWS Key Management Service 中的客户主密钥进行服务端加密。

使用 EventBridge 自动执行 Amazon Chime Voice Connector

Amazon Chime Voice Connector 可自动触发的操作包括：

- 调用 AWS Lambda 函数
- 启动 Amazon Elastic Container Service 任务
- 将事件中继到 Amazon Kinesis Video Streams
- 激活 AWS Step Functions 状态机
- 通知 Amazon SNS 主题或 Amazon SQS 队列

EventBridge 与 Amazon Chime Voice Connector 配合使用的一些示例包括：

- 激活 Lambda 函数，在结束调用后下载相关音频。
- 启动 Amazon ECS 任务，在开始调用后启用实时转录。

有关更多信息，请参阅 Amazon EventBridge 用户指南。

Amazon Chime Voice Connector 流式处理事件

Amazon Chime Voice Connector 支持在发生本节讨论的事件时，向 EventBridge 发送事件。

Amazon Chime Voice Connector 开启流式处理

Amazon Chime Voice Connector 会在 Kinesis Video Streams 开启媒体流时发送此事件。

Example 事件数据

以下是此事件的示例数据。

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-111122223333",
    "detail-type": "Chime VoiceConnector Streaming Status",
    "source": "aws.chime",
    "account": "111122223333",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "callId": "1112-2222-4333",
        "direction": "Outbound",
        "fromNumber": "+12065550100",
        "inviteHeaders": {
            "from": "\"John\" <sip:+12065550100@10.24.34.0>;tag=abcdefg",
            "to": "<sip:
+13605550199@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws:5060>",
            "call-id": "1112-2222-4333",
            "cseq": "101 INVITE",
            "contact": "<sip:user@10.24.34.0:6090>;",
            "content-type": "application/sdp",
            "content-length": "246"
        },
```

```
        "isCaller": false,
        "mediaType": "audio/L16",
        "sdp": {
            "mediaIndex": 0,
            "mediaLabel": "1"
        },
        "siprecMetadata": "<&xml version=\"1.0\" encoding=\"UTF-8\"&>;\r\n<recording
 xmlns='urn:ietf:params:xml:ns:recording:1'>",
        "startFragmentNumber": "1234567899444",
        "startTime": "yyyy-mm-ddThh:mm:ssZ",
        "streamArn": "arn:aws:kinesisvideo:us-east-1:123456:stream/ChimeVoiceConnector-
abcdef1ghij2klmno3pqr4-111aaa-22bb-33cc-44dd-111222/111122223333",
        "toNumber": "+13605550199",
        "transactionId": "12345678-1234-1234",
        "voiceConnectorId": "abcdef1ghij2klmno3pqr4",
        "streamingStatus": "STARTED",
        "version": "0"
    }
}
```

Amazon Chime Voice Connector 结束流式处理

Amazon Chime Voice Connector 会在 Kinesis Video Streams 结束媒体流时发送此事件。

Example 事件数据

以下是此事件的示例数据。

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-111122223333",
    "detail-type": "Chime VoiceConnector Streaming Status",
    "source": "aws.chime",
    "account": "111122223333",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "streamingStatus": "ENDED",
        "voiceConnectorId": "abcdef1ghij2klmno3pqr4",
        "transactionId": "12345678-1234-1234",
        "callId": "1112-2222-4333",
        "direction": "Inbound",
        "fromNumber": "+12065550100",
```

```
        "inviteHeaders": {
            "from": "\"John\" <sip:+12065550100@10.24.34.0>;tag=abcdefg",
            "to": "<sip:
+13605550199@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws:5060>",
            "call-id": "1112-2222-4333",
            "cseq": "101 INVITE",
            "contact": "<sip:user@10.24.34.0:6090>",
            "content-type": "application/sdp",
            "content-length": "246"
        },
        "isCaller": false,
        "mediaType": "audio/L16",
        "sdp": {
            "mediaIndex": 0,
            "mediaLabel": "1"
        },
        "siprecMetadata": "<&xml version=\"1.0\" encoding=\"UTF-8\"&>\r\n<recording
 xmlns='urn:ietf:params:xml:ns:recording:1'>",
        "startFragmentNumber": "1234567899444",
        "startTime": "yyyy-mm-ddThh:mm:ssZ",
        "endTime": "yyyy-mm-ddThh:mm:ssZ",
        "streamArn": "arn:aws:kinesisvideo:us-east-1:123456:stream/ChimeVoiceConnector-
abcdef1ghij2klmno3pqr4-111aaa-22bb-33cc-44dd-111222/111122223333",
        "toNumber": "+13605550199",
        "version": "0"
    }
}
```

Amazon Chime Voice Connector 更新流式处理

Amazon Chime Voice Connector 会在 Kinesis Video Streams 更新媒体流时发送此事件。

Example 事件数据

以下是此事件的示例数据。

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-111122223333",
    "detail-type": "Chime VoiceConnector Streaming Status",
    "source": "aws.chime",
    "account": "111122223333",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
```

```
    "resources": [],
    "detail": {
        "callId": "1112-2222-4333",
        "updateHeaders": {
            "from": "\"John\" <sip:+12065550100@10.24.34.0>;;tag=abcdefg",
            "to": "<sip:
+13605550199@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws:5060>",
            "call-id": "1112-2222-4333",
            "cseq": "101 INVITE",
            "contact": "<sip:user@10.24.34.0:6090>",
            "content-type": "application/sdp",
            "content-length": "246"
        },
        "siprecMetadata": "<&xml version=\"1.0\" encoding=\"UTF-8\"&>\r\n<recording
 xmlns='urn:ietf:params:xml:ns:recording:1'>",
        "streamingStatus": "UPDATED",
        "transactionId": "12345678-1234-1234",
        "version": "0",
        "voiceConnectorId": "abcdef1ghij2klmno3pqr4"
    }
}
```

Amazon Chime Voice Connector 流式处理失败

Amazon Chime Voice Connector 会在 Kinesis Video Streams 媒体流操作失败时发送此事件。

Example 事件数据

以下是此事件的示例数据。

```
{
  "version": "0",
  "id": "12345678-1234-1234-1234-111122223333",
  "detail-type": "Chime VoiceConnector Streaming Status",
  "source": "aws.chime",
  "account": "111122223333",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [],
  "detail": {
       "streamingStatus":"FAILED",
       "voiceConnectorId":"abcdefghi",
       "transactionId":"12345678-1234-1234",
       "callId":"1112-2222-4333",
```

```
        "direction":"Inbound",
        "failTime":"yyyy-mm-ddThh:mm:ssZ",
        "failureReason": "Internal failure",
        "version":"0"
    }
}
```

使用 AWS CloudTrail 记录 Amazon Chime API 调用

将 Amazon Chime 集成至 AWS CloudTrail 服务，后者记录了用户、角色或 Amazon Chime AWS 服务所执行的操作。CloudTrail 会捕获所有 Amazon Chime API 调用作为事件，其中包括来自 Amazon Chime 控制台的调用以及对 Amazon Chime API 的代码调用。如果您创建了跟踪，则可以持续向 Amazon S3 存储桶传送 CloudTrail 事件，包括 Amazon Chime 事件。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录）中查看最新事件。您可以根据 CloudTrail 收集的信息，确定向 Amazon Chime 发送的请求内容以及发送请求的 IP 地址、对象和时间等详细信息。

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

CloudTrail 中的 Amazon Chime 信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。当 Amazon Chime 控制台调用 API 时，此活动就会和事件历史记录中的其他 AWS 服务事件一起记录在 CloudTrail 事件中。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。

如需持续记录 AWS 账户中的事件，包括 Amazon Chime 事件，请创建跟踪。通过跟踪，CloudTrail 可将日志文件传送至 Amazon S3 桶。默认情况下，在控制台中创建跟踪时，此跟踪应用于所有区域。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，您可以配置其它 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

CloudTrail 会将所有 Amazon Chime 操作记录在 Amazon Chime API 参考中。例如，对 `CreateAccount`、`InviteUsers` 和 `ResetPersonalPIN` 部分的调用将在 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。
- 请求是否由其它 AWS 服务发出。

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

了解 Amazon Chime 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 桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关请求的操作、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。

使用 chime.amazonaws.com 事件源识别 Amazon Chime 条目。

如果您已为 Amazon Chime 账户配置 Active Directory，请参阅使用 CloudTrail 记录 AWS Directory Service API 调用。其中描述了如何监控可能会影响 Amazon Chime 用户登录功能的问题。

以下示例显示了适用于 Amazon Chime 的 CloudTrail 日志条目：

```
{"eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":" AAAAAABBBBBBBBEXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice ",
            "accountId":"0123456789012",
            "accessKeyId":"AAAAAABBBBBBBBEXAMPLE",
            "sessionContext":{
               "attributes":{
                  "mfaAuthenticated":"false",
                  "creationDate":"2017-07-24T17:57:43Z"
               },
               "sessionIssuer":{
                  "type":"Role",
                  "principalId":"AAAAAABBBBBBBBEXAMPLE",
                  "arn":"arn:aws:iam::123456789012:role/Joe",
                  "accountId":"123456789012",
                  "userName":"Joe"
               }
            }
         } ,
```

```
        "eventTime":"2017-07-24T17:58:21Z",
        "eventSource":"chime.amazonaws.com",
        "eventName":"AddDomain",
        "awsRegion":"us-east-1",
        "sourceIPAddress":"72.21.198.64",
        "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36",
        "errorCode":"ConflictException",
        "errorMessage":"Request could not be completed due to a conflict",
        "requestParameters":{
           "domainName":"example.com",
           "accountId":"11aaaaaa1-1a11-1111-1a11-aaadd0a0aa00"
        },
        "responseElements":null,
        "requestID":"be1bee1d-1111-11e1-1eD1-0dc1111f1ac1",
        "eventID":"00fbeee1-123e-111e-93e3-11111bfbfcc1",
        "eventType":"AwsApiCall",
        "recipientAccountId":"123456789012"
     }
```

Amazon Chime 的合规性验证

作为多个合 AWS 规计划（例如 SOC、PCI、FedRAMP 和 HIPAA）的一部分，第三方审计师评估 AWS 服务的安全性和合规性。

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全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，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

Amazon Chime 中的恢复能力

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。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失效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设施相比，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 全球基础设施。

除了 AWS 全球基础设施外，Amazon Chime 还提供不同的功能来帮助支持您的数据弹性和备份需求。有关更多信息，请参阅《Amazon Chime SDK 管理指南》中的管理 Amazon Chime Voice Connector 组和向 Kinesis 流式传输 Amazon Chime Voice Connector 媒体。

Amazon Chime 中的基础设施安全性

作为一项托管服务，Amazon Chime 受到 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络进行访问。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。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

了解 Amazon Chime 自动更新

Amazon Chime 提供了不同的客户端更新方式。这些方式有所不同，具体取决于用户是在浏览器、桌面设备还是移动设备上运行 Amazon Chime。

Amazon Chime Web 应用程序 (https://app.chime.aws) 始终加载最新功能和安全修复程序。

每当用户选择退出或注销时，Amazon Chime 桌面客户端都会检查是否有更新。此操作适用于 Windows 和 macOS 计算机。当用户运行客户端时，会每三小时检查一次更新。用户还可以在 Windows 帮助菜单或 macOS 的 Amazon Chime 菜单上选择检查更新来查看更新。

当桌面客户端检测到更新时，Amazon Chime 会提示用户安装更新，除非他们正在参加会议。在以下场景中，用户正在参加会议：

- 用户正在参加会议。
- 用户应邀参加正在进行中的会议。

Amazon Chime 会提示用户安装最新版本，并设置 15 秒倒计时，以便用户推迟安装。选择稍后再试以推迟更新。

当用户推迟更新且未加入正在进行的会议时，客户端会在三个小时后检查更新并再次提示用户进行安装。倒计时结束时，开始安装。

> **Note**
>
> 在 macOS 计算机上，用户需要选择立即重启才能开始更新。

在移动设备上：Amazon Chime 移动应用程序会使用 App Store 和 Google Play 提供的更新选项来交付 Amazon Chime 最新版客户端。您也可以通过移动设备管理系统发布更新。本主题假定您知道如何操作。

Amazon Chime 文档历史记录

下表介绍了自 2018 年 3 月起对 Amazon Chime 管理员指南做出的一些重要更改。如需有关此文档更新的通知，您可以订阅 RSS 源。

变更	说明	日期
已发布 Amazon Chime SDK 管理指南	Amazon Chime SDK 管理指南现已发布 Amazon Chime SDK 主题。有关信息，请参阅 Amazon Chime SDK 管理指南。	2022 年 3 月 24 日
IAM 策略更新内容	由管理的 IAM 策略的更改 AWS 现在可以在本管理员指南中进行跟踪。请参阅基于 Amazon Chime 身份的策略示例。	2021 年 9 月 23 日
服务相关角色	管理员现在可以为 Amazon Live Transcription 创建服务相关角色，并在 Amazon Chime 实时转录操作开始和结束时查看事件消息。有关更多信息，请参阅使用角色进行实时转录和使用事件自动化 Amazon Ch CloudWatch ime。	2021 年 8 月 12 日
SIP 媒体应用程序和规则	管理员可以创建 SIP 媒体应用程序和规则，以便与 Amazon Chime 语音连接器和 AWS Lambda 功能配合使用。有关更多信息，请参阅 Amazon Chime 管理员指南中的管理 SIP 应用程序和规则。	2020 年 11 月 18 日

Amazon Chime Voice Connector 紧急呼叫路由号码	Amazon Chime 管理员可以为 Amazon Chime Voice Connector 设置紧急呼叫路由号码。有关更多信息，请参阅 Amazon Chime 管理员指南中的 Amazon Chime 语音连接器设置紧急呼叫路由号码。	2020 年 7 月 1 日
杜比语音小会议室上的 Amazon Chime	在杜比语音小会议室的音频和视频会议硬件上，Amazon Chime 提供本机或第一方会议体验。有关更多信息，请参阅《亚马逊 Chime 管理员指南》中的在杜比硬件上设置 Amazon Chime。	2020 年 6 月 3 日
设置聊天保留策略	Amazon Chime 管理员可以为其企业账户设置聊天保留策略。有关更多信息，请参阅 Amazon Chime 管理员指南中的管理聊天保留政策。	2020 年 5 月 21 日
删除聊天消息	如果您有编程能力，则可以使用两个 Amazon Chime API 来删除聊天室中的消息和账户中的对话。有关更多信息，请参阅 Amazon Chime 管理员指南中的删除单条消息。	2020 年 5 月 18 日
CloudWatch Amazon Chime 语音连接器的媒体质量指标	Amazon Chime 支持将您的 Amazon Chime 语音连接器的媒体质量指标发送到。CloudWatch有关更多信息，请参阅《Amazon Chime 管理员指南》中的 “使用 CloudWatch 监控 Amazon Chime”。	2020 年 1 月 23 日

适用于 Slack 的 Amazon Chime Meetings 应用程序	Amazon Chime 支持适用于 Slack 的 Amazon Chime Meetings 应用程序。有关更多信息，请参阅《亚马逊 Chime 管理员指南》中的 “为 Slack 设置亚马逊 Chime 会议应用程序”。	2019 年 12 月 4 日
会议区域设置	Amazon Chime 支持在最佳 AWS 区域为所有参与者处理会议。有关更多信息，请参阅 Amazon Chime 管理员指南中的会议区域设置。	2019 年 12 月 3 日
基于 SIP 的媒体录制 (SIPREC) 兼容性	Amazon Chime Voice Connector 支持将媒体从兼容 SIPREC 的语音基础设施流式传输到 Kinesis Video Streams。有关更多信息，请参阅 Amazon Chime 管理员指南中的基于 SIP 的媒体录制 (SIPREC) 兼容性。	2019 年 11 月 25 日
杜比语音室上的 Amazon Chime	如需改善用户参加会议的便捷体验，Amazon Chime 可在杜比语音室音频和视频会议硬件上提供本机或第一方会议体验。有关更多信息，请参阅《亚马逊 Chime 管理员指南》中的 “在杜比语音室中设置 Amazon Chime”。	2019 年 10 月 29 日

更新出站呼叫名称	设置默认呼叫名称，向使用 Amazon Chime 清单中的电话号码进行出站呼叫的接收人显示。有关更多信息，请参阅 Amazon Chime 管理员指南中的更新出站呼叫姓名。	2019 年 10 月 24 日
将媒体流式传输到 Amazon Kinesis	将电话音频从 Amazon Chime Voice Connector 流式传输到 Kinesis Video Streams，用于分析、机器学习和其他处理目的。有关更多信息，请参阅《亚马逊 Chime 管理员指南》中的 “将 Amazon Chime 语音连接器媒体流式传输到 Kinesis 和使用 Amazon Chime 语音连接器服务相关角色”。	2019 年 10 月 24 日
使用亚马逊监控 Amazon Chime CloudWatch	使用监控 Amazon Chime CloudWatch，它收集原始数据并将其处理为可读的近乎实时的指标。有关更多信息，请参阅《Amazon Chime 管理员指南》中的 “使用 CloudWatch监控 Amazon Chime”。	2019 年 10 月 24 日
Amazon Chime Voice Connector 组	创建一个 Amazon Chime 语音连接器群组，其中包括在不同地区创建的 Amazon Chime 语音连接器。 AWS 这允许入站呼叫跨区域故障转移，从而创建容错机制，以便在出现可用性事件的情况下进行回退。有关更多信息，请参阅《亚马逊 Chime 管理员指南》中的 “使用 Amazon Chime 语音连接器群组”。	2019 年 10 月 24 日

网络配置更新	Amazon Chime 简化了对防火墙的要求。有关更多信息，请参阅 Amazon Chime 管理员指南中的网络配置和带宽要求。	2019 年 9 月 6 日
有人监管的会议	Amazon Chime 支持有人监管的会议。有关更多信息，请参阅 Amazon Chime 管理员指南中的加入主持人会议。	2019 年 7 月 25 日
Amazon Chime 的合规性验证	Amazon Chime 是一项符合 HIPAA 要求的服务。有关更多信息，请参阅 Amazon Chime 管理员指南中的 Amazon Chime 的合规性验证。	2019 年 6 月 11 日
接入免费电话号码	Amazon Chime 支持免费移植美国境内的电话号码，以配合 Amazon Chime Voice Connector 使用。有关更多信息，请参阅 Amazon Chime 管理员指南中的移植现有电话号码。	2019 年 5 月 28 日
管理 Amazon Chime 中的电话号码	使用 Amazon Chime Business Calling 为 Amazon Chime 用户预置并分配电话号码。将 Amazon Chime Voice Connector 与现有电话系统集成。有关更多信息，请参阅 Amazon Chime 管理员指南中的管理 Amazon Chime 中的电话号码。	2019 年 3 月 18 日

适用于 Outlook 的 Amazon Chime 插件	Amazon Chime 提供两种适用于 Microsoft Outlook 的插件：适用于 Windows Outlook 的 Amazon Chime 插件和适用于 Outlook 的 Amazon Chime 插件。这些插件提供相同的计划功能，但支持不同类型的用户。有关更多信息，请参阅 Amazon Chime 管理员指南中的为 Outlook 部署插件。	2019 年 3 月 12 日
各种更新	主题布局和组织的各种更新。	2019 年 2 月 11 日
Amazon Chime 的“给我打电话”功能	管理员可以在会议设置下启用 Amazon Chime 的“给我打电话”功能。有关更多信息，请参阅 Amazon Chime 管理员指南中的管理会议设置。	2018 年 8 月 22 日
连接到 Okta SSO	如果您有企业账户，则可以连接到 Okta SSO 以进行身份验证和分配用户权限。有关更多信息，请参阅 Amazon Chime 管理员指南中的 C onnect 到 Okta SSO。	2018 年 8 月 1 日
请求用户附件	接收用户上传到 Amazon Chime 中的附件。有关更多信息，请参阅 Amazon Chime 管理员指南中的请求用户附件。	2018 年 4 月 23 日
查看其他报告数据	查看其他报告数据。有关更多信息，请参阅 Amazon Chime 管理员指南中的查看报告。	2018 年 3 月 30 日

向用户分配高级或基本权限	向用户分配高级或基本权限。有关更多信息，请参阅 Amazon Chime 管理员指南中的管理用户访问权限和权限。	2018 年 3 月 29 日