aws

控制台管理指南

AWS re: Post 私有化

AWS re: Post 私有化: 控制台管理指南

Table of Contents

什么是 AWS re: Post Private？

AWS re: Post Private 是 AWS re: Post 的私有版本，适用于拥有企业支持或企业入门级支持计划的企业。它提供了获取知识和专家的机会，以加快云的采用并提高开发人员的工作效率。借助组织特定的私有 re: Post，您可以建立一个特定于组织的开发者社区，该社区可以大规模提高效率并提供对宝贵知识资源的访问权限。此外，re: Post Private 集中了值得信赖AWS的技术内容，并提供私密讨论论坛，以改善您的团队内部协作以及与 AWS 的协作方式，从而消除技术障碍、加快创新并在云中更高效地扩展。

有关更多信息，请参阅 AWS re: Post Pri vate。

访问 re: Post Privat

管理员使用 AWS re: Post 私有控制台来创建其组织特定的私有 re: Post。当管理员创建私有 re: post 时，他们可以将自己的私有 re: post 命名并在下定义一个子域。`*.private.repost.aws`组织私有 re: Post 的管理员可以使用以下身份源配置用户访问权限AWS IAM Identity Center并指定身份源之一进行身份验证：Identity Center 目录、Active Directory 或外部身份提供商。配置用户后，控制台管理员可以为一个或多个用户分配 re: Post Private 管理员角色。re: Post Private 管理员可以根据组织品牌和知识需求自定义其私有 re: Post 应用程序。熟悉组织架构和工作负载的AWS客户团队成员（例如技术客户经理）会自动添加到组织的私人 re: Post 中进行协作。

re: Post Private 应用程序的管理员可以自定义品牌，添加标签以对内容进行分类，以及为开发人员选择感兴趣的话题以自动填充培训和技术内容。他们还可以邀请用户加入他们的私人 re: Post 以加强协作。有关更多信息，请参阅 AWS re: Post 私有管理指南。

非管理员用户使用 re: Post Private 应用程序使用管理员配置的凭据进行登录。登录私人 re: Post 后，用户可以浏览或搜索现有内容，包括针对其感兴趣主题的量身定制的培训和技术内容。用户还可以直接从其私人 re: Post 中搜索AWS公共技术内容，并创建私人话题以供内部讨论AWS公开内容。用户可以通过提问、提供回复或发表文章来协作解决AWS技术问题，并从私有 re: Post 的其他用户那里获得技术指导。用户还可以将讨论话题转换为AWS Support案例。用户可以选择将来自AWS Support的回复添加到私密的 re: Post 中。有关更多信息，请参阅 AWS re: Post 私有用户指南。

定价

只有拥有企业支持 (ES) 和企业入门 (EOP) 支持计划的客户才能订阅 re: Post Private 服务。您可以从两个可用的定价套餐中进行选择：免费套餐和标准套餐。免费套餐使您能够在六个月内全面探索和试用

标准套餐功能，然后才能无缝过渡到付费套餐。如果您使用标准套餐，则可以按每位用户支付月度订阅费用来使用 re: Post Private。有关更多信息，请参阅定价。

如何开始

要开始使用 re: Post Private，请参阅。先决条件

先决条件

您必须满足以下先决条件，然后才能在 AWS re: Post Private 中创建新的私有 re: post 或管理现有的私有 re: post：post：

- 您必须注册企业或企业 On -Ramp Suppor t 计划。
- 您必须在要设置私人 re: Post 的同一个区域AWS IAM Identity Center中启用。
- 您必须创建一个具有创建、管理和解决AWS Support案例所需权限的AWS Identity and Access Management角色。re: Post Private 服务使用此角色对 API 进行调用。AWS Support有关更多信息，请参阅 在 re: Post Private 中管理对 AWS Support 案例创建和管理的访问权限。

通过 IAM 身份中心登录 re: Post Private

re: Post Private AWS IAM Identity Center 与集成，为您的员工提供身份联合。通过 IAM Identity Center，用户将被重定向到其现有公司名录，以便使用其现有证书登录。然后，他们就可以无缝登录自己的私人 re: Post。这样可以确保强制执行诸如密码策略和双重身份验证之类的安全设置。使用 IAM 身份中心不会影响您现有的 IAM 配置。

如果您没有现有的用户目录或不想联合，那么 IAM Identity Center 会提供一个集成的用户目录，您可以使用该目录为 re: Post Private 创建用户和群组。re: Post Private 不支持使用 IAM 用户和角色在私有 re: Post 中分配权限。私有 re: post 中的用户权限由管理员在其私有 re: Post 应用程序上配置。

有关 IAM 身份中心的更多信息，请参阅什么是 AWS IAM 身份中心（AWS Single Sign-On 的继任者）。有关 IAM Identity Center 入门的更多信息，请参阅入门。要使用 IAM 身份中心，您还必须为该账户AWS Organizations激活。

> **Important**
>
> re: post Private 仅支持 IAM 身份中心的组织实例。

re: Post Private 中的安全

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。

安全是双方共同承担 AWS 的责任。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 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。 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 AWS re: Post Private 的合规计划，请参阅按合规计划划分的范围内 AWS 服务按合规计划。
- 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。

本文档可帮助您了解在使用 re: Post Private 时如何应用分担责任模型。以下主题向您展示了如何配置 re: Post Private 以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 re: Post Private 资源。

主题

AWS re: Post Private 中的数据保护

分担责任模型 AWS 分担责任模型适用于 AWS re: Post Private 中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础架构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

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

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

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

利用加密来保护数据

静态加密

re: Post Private 使用亚马逊简单存储服务存储桶、亚马逊 DynamoDB 数据库、Amazon Neptune 数据库 OpenSearch 和使用亚马逊托管密钥或客户托管密钥进行静态加密的亚马逊服务域。

传输中加密

re: Post Private 使用 HTTPS 协议与您的客户端应用程序通信。它使用 HTTPS 和 AWS 签名代表您的应用程序与其他服务进行通信。

密钥管理

re: post Private 与密钥集成 AWS Key Management Service 并支持 AWS KMS 密钥。您可以在创建私人 re: Post 时为其自定义数据加密设置。为此，您可以选择现有 AWS KMS 密钥或创建新 AWS KMS 密钥。

re: Post Private 如何与 IAM 配

在使用 IAM 管理对 AWS re: Post Private 的访问权限之前，您必须了解哪些 IAM 功能可用于 re: Post Private。要全面了解 re: Post Private 和其他 AWS 服务如何与 IAM 配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

re: post 基于私有身份的策略

使用基于 IAM 身份的策略，您可以指定允许或拒绝的操作。re: Post Private 支持特定的操作。要了解您在 JSON 策略中使用的元素，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。

re: Post Private 中的策略操作在操作前使用以下前缀：。`repostspace:`例如，要向某人授予运行 re: Post Private `CreateSpace` API 操作的权限，您需要将该`repostspace:CreateSpace`操作包含在他们的策略中。策略声明必须包含`Action`或`NotAction`元素。re: Post Private 定义了自己的一组操作，这些操作描述了您可以使用此服务执行的任务。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示：

```
"Action": [
      "repostspace:CreateSpace",
      "repostspace:DeleteSpace"
```

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

```
"Action": "repostspace:Describe*"
```

要查看 re: Post 私有操作列表，请参阅 IAM 用户指南中的 re: Post Private 定义的操作。

资源

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

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称 (ARN) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

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

条件键

re: post Private 不提供任何特定于服务的条件密钥，但它支持使用全局条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

示例

要查看基于 re: Post 私有身份的策略示例，请参阅。AWS re: Post 基于私有身份的策略示例

re: post 基于私有资源的政策

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。

re: post Private 不支持基于资源的策略。

基于标签的授权

re: post Private 支持标记资源或根据标签控制访问权限。有关更多信息，请参阅使用标签控制 AWS 资源的访问权限。

重发:发布私有 IAM 角色

I AM 角色是您的 AWS 账户中具有特定权限的实体。

在 re: Post Private 中使用临时证书

强烈建议使用临时凭证进行联合身份登录，担任 IAM 角色或担任跨账户角色。您可以通过调用AssumeRole或之类的 AWS STS API 操作来获取临时安全证书GetFederationToken。

re: post Private 支持使用临时证书。

服务相关角色

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

服务角色

此功能允许服务为您扮演服务角色。此角色允许服务访问其他服务中的资源以为您完成操作。有关更多信息，请参阅创建向 AWS 服务委派权限的角色。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。

在 re: Post Private 中使用服务相关角色

AWS re: Post 私有用途 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特的 IAM 角色，直接链接到 re: Post Private。服务相关角色由 re: Post Private 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色可以更轻松地设置 re: Post Private，因为您不必手动添加必要的权限。re: Post Private 定义了其服务相关角色的权限，除非另有定义，否则只有 re: Post Private 可以担任其角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

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，并查找 Service-linked roles（服务相关角色）列中显示为 Yes（是）的服务。选择是和链接，查看该服务的服务相关角色文档。

re: Post Private 的服务相关角色权限

re: post Private 使用名为的服务相关角色AWSServiceRoleForrePostPrivate。re: Post Private 使用此服务相关角色向其发布数据。 CloudWatch

AWSServiceRoleForrePostPrivate 服务相关角色信任以下服务来代入该角色：

- `repostspace.amazonaws.com`

名为的角色权限策略`AWSrePostPrivateCloudWatchAccess`允许 re: Post Private 对指定资源完成以下操作：

- 对`cloudwatch`以下内容采取行动：`PutMetricData`

您必须配置允许用户、组或角色创建、编辑或删除服务相关角色的权限。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

有关更多信息，请参阅 AWSrePostPrivateCloudWatchAccess。

为 re: Post Private 创建服务相关角色

您无需手动创建服务相关角色。当你在、或 AWS API 中创建第一个私有 re: Post 时 AWS Management Console AWS CLI，re: Post Private 会为你创建服务相关角色。

> **Important**
>
> 如果您在其他使用此角色支持的功能的服务中完成某个操作，此服务相关角色可以出现在您的账户中。另外，如果你在 2023 年 12 月 1 日开始支持服务相关角色之前使用 re: Post Private 服务，那么 re: Post Private 会在你的账户中创建该`AWSServiceRoleForrePostPrivate`角色。要了解更多信息，请参阅 “我的” 中出现了一个新角色 AWS 账户。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当你创建第一个私有 re: Post 时，re: Post Private 会再次为你创建服务相关角色。

在 AWS CLI 或 AWS API 中，使用服务名称创建服务相关角色。`repostspace.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，可以使用同样的过程再次创建角色。

编辑 re: Post Private 的服务相关角色

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

删除 re: Post Private 的服务相关角色

无需手动删除 `AWSServiceRoleForrePostPrivate` 角色。当你在 AWS Management Console、或 AWS API 中删除你的私有 re: post 时 AWS CLI，re: Post Private 会为你删除服务相关角色。

您也可以使用 IAM 控制台 AWS CLI、或 AWS API 手动删除服务相关角色。

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 AWSServiceRoleForrePostPrivate 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。

re: Post 私有服务相关角色支持的区域

re: Post Private 支持在提供服务的 AWS 地区使用服务相关角色。

区域名称	区域标识	re: Post Private 中的支持
美国东部（弗吉尼亚州北部）	us-east-1	是
美国东部（俄亥俄州）	us-east-2	否
美国西部（加利福尼亚北部）	us-west-1	否
美国西部（俄勒冈州）	us-west-2	是
非洲（开普敦）	af-south-1	否
亚太地区（香港）	ap-east-1	否
亚太地区（雅加达）	ap-southeast-3	否
亚太地区（孟买）	ap-south-1	否
Asia Pacific (Osaka)	ap-northeast-3	否
Asia Pacific (Seoul)	ap-northeast-2	否
亚太地区（新加坡）	ap-southeast-1	是
亚太地区（悉尼）	ap-southeast-2	是

区域名称	区域标识	re: Post Private 中的支持
Asia Pacific (Tokyo)	ap-northeast-1	否
加拿大（中部）	ca-central-1	是
欧洲（法兰克福）	eu-central-1	是
欧洲地区（爱尔兰）	eu-west-1	是
欧洲地区（伦敦）	eu-west-2	否
欧洲地区（米兰）	eu-south-1	否
欧洲地区（巴黎）	eu-west-3	否
欧洲地区（斯德哥尔摩）	eu-north-1	否
中东（巴林）	me-south-1	否
中东（阿联酋）	me-central-1	否
South America（São Paulo）	sa-east-1	否

AWS re: Post 基于私有身份的策略示例

> **Note**
>
> 为了提高安全性，请尽可能创建联合用户而不是 IAM 用户。

默认情况下， AWS Identity and Access Management 用户和角色无权创建或修改 AWS re: Post 私有资源。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 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的创建 IAM policy。

主题

- 策略最佳实践
- 允许用户查看他们自己的权限

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 re: Post Private 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 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果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 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 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。

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": "*"
        }
    ]
}
```

内联策略

内联策略是您创建和管理的策略。您可以将内联策略直接嵌入到用户、群组或角色中。以下策略示例说明如何分配权限以执行 AWS re: Post Private 操作。有关内联策略的一般信息，请参阅 A WS IAM 用户指南中的管理 IAM 策略。您可以使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS Identity and Access Management API 来创建和嵌入内联策略。

主题

- re: Post Private 的只读权限
- 完全访问 re: Post Private

re: Post Private 的只读权限

以下策略向用户授予 IAM Identity Center 和 re: Post 私有控制台的读取权限。此策略允许用户执行只读的 re: Post Private 操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",

                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "sso:GetSSOStatus",
                "sso:GetManagedApplicationInstance",
                "sso:ListProfiles",
                "sso:GetProfile",
                "sso:ListProfileAssociations",

                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups",

                "repostspace:GetSpace",
                "repostspace:ListSpaces",
                "repostspace:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

完全访问 re: Post Private

以下策略向用户授予 IAM 身份中心和 re: Post 私有控制台的完全访问权限。此政策允许用户执行所有 re: Post Private 操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",

                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "sso:GetSSOStatus",
                "sso:GetManagedApplicationInstance",
                "sso:ListProfiles",
                "sso:GetProfile",
                "sso:ListProfileAssociations",

                "sso:CreateManagedApplicationInstance",
                "sso:DeleteManagedApplicationInstance",
                "sso:AssociateProfile",
                "sso:DisassociateProfile",

                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups",

                "kms:ListAliases",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:RetireGrant",

                "repostspace:*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS AWS re: Post Private 的托管策略

与自己编写策略相比，使用 AWS 托管策略可以更轻松地向用户、群组和角色添加权限。创建仅为团队提供所需权限的 IAM 客户托管策略需要时间和专业知识。使用 AWS 托管策略快速入门。这些政策涵盖常见用例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅 IAM 用户指南中的AWS 托管策略。

AWS 服务维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务偶尔可能会向 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，`ReadOnlyAccess` AWS 托管策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动一项新功能时， AWS 会为新操作和资源添加只读权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

主题

- AWS 托管策略： AWSRepostSpaceSupportOperationsPolicy
- AWS 托管策略： AWSrePostPrivateCloudWatchAccess
- AWS re: 发布托管策略的私有 AWS 更新

AWS 托管策略： AWSRepostSpaceSupportOperationsPolicy

此策略允许 AWS re: Post 私有服务创建、管理和解决通过 re: Post 私有网络应用程序创建的 AWS Support 案例。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "RepostSpaceSupportOperations",
   "Effect": "Allow",
   "Action": [
    "support:AddAttachmentsToSet",
    "support:AddCommunicationToCase",
    "support:CreateCase",
    "support:DescribeCases",
    "support:DescribeCommunications",
    "support:ResolveCase"
```

```
    ],
    "Resource": "*"
   }
  ]
}
```

AWS 托管策略： AWSrePostPrivateCloudWatchAccess

此政策允许 re: Post Private 服务向发布数据。 CloudWatch

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CloudWatchPublishMetrics",
   "Effect": "Allow",
   "Action": [
    "cloudwatch:PutMetricData"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "cloudwatch:namespace": [
      "AWS/rePostPrivate",
      "AWS/Usage"
     ]
    }
   }
  }
 ]
}
```

AWS re: 发布托管策略的私有 AWS 更新

查看 re: Post Private AWS 托管策略自该服务开始跟踪这些更改以来这些更新的详细信息。要获得有关此页面更改的自动提示，请订阅 文档历史记录 页面上的 RSS 源。

下表描述了 re: Post Private 托管策略自 2023 年 11 月 26 日以来的重要更新。

更改	描述	日期
新政策-AWSrePostPrivateCloudWatchAccess	用于将数据发布到的新托管策略 CloudWatch	2023 年 11 月 26 日
新政策-AWSRepostSpaceSupportOperationsPolicy	AWS re: Post Private 中 AWS Support 功能的新托管策略	2023 年 11 月 26 日
re: Post Private 开始追踪更改	re: Post Private 开始跟踪其 AWS 托管策略的更改	2023 年 11 月 26 日

AWS re: Post 私有身份和访问权限疑难解答

使用以下信息来帮助您诊断和修复在使用 re: Post Private 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 re: Post Private 中执行任何操作
- 我无权执行 iam：PassRole
- 我想允许我以外的人访问我的 r AWS 账户 e: Post 私有资源

我无权在 re: Post Private 中执行任何操作

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 repostPrivate:*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:
 repostPrivate: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 repostPrivate:*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

如果您收到错误消息，提示您无权执行`iam:PassRole`操作，则必须更新您的策略以允许您将角色传递给 re: Post Private。

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。

当名为的 IAM 用户`marymajor`尝试使用控制台在 re: Post Private 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。

我想允许我以外的人访问我的 r AWS 账户 e: Post 私有资源

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 re: Post Private 是否支持这些功能，请参阅。re: Post Private 如何与 IAM 配
- 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之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

AWS re: Post Private 的合规性验证

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，并提供了部署以安全性和合规性为重点 AWS 的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规性 — 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。

AWS re: Post Private 中的弹性

AWS 全球基础设施是围绕 AWS 区域 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连接。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。

AWS 中的基础设施安全 re: Post Private

作为一项托管服务，AWS re: Post Private 受亚马逊网络服务：安全流程概述白皮书中描述的 AWS 全球网络安全程序的保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 re: Post Private。客户端必须支持传输层安全性协议 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 DHE (Ephemeral Diffie-Hellman) 或 ECDHE (Elliptic Curve Ephemeral 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 AWS Identity and Access Management 委托人关联的私有访问密钥对请求进行签名。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。

re: post 私有配额

AWS re: Post Private 提供私有 re: Post，您可以在给定区域的账户中使用这些帖子。AWS当你注册 re: Post Private 时，会对你可以创建的私人 re: Posts 的数量和私人 re: Posts 的大小AWS设置默认配额（以前称为限制）。

Service Quotas

以下是您账户的 re: Post Private AWS 的默认配额。您可以使用 S ervice Quotas 控制台查看默认配额。这些配额均不可调整。您不能申请增加配额。

资源	默认值	描述	可调整
私人 re: Posts 数量	3	当前区域中该账户中私人 re: Posts 的最大数量。	否
免费私人 re: post 大小	10	免费专用 re: Post 的最大大小（以 GB 为单位）。	否
标准私密回复:帖子大小	100	标准私有 re: Post 的最大大小（以 GB 为单位）。	否

API 限流限制

在 re: Post Private 中，以下限制适用于每个账户、每个区域。这些配额不能提高。

操作	代币充值率	请求速率	
CreateSpace	1	1	
ListSpaces	10	10	
GetSpace	10	10	

操作	代币充值率	请求速率	
UpdateSpace	10	10	
DeleteSpace	1	1	
RegisterAdmin	10	100	
DeRegisterAdmin	10	100	
SendInvites	1	1	
TagResource	10	10	
UnTagResource	10	10	
ListTagsForResource	10	10	

创建、配置和自定义您的私人 re: Post

主题

创建新的私人 re: Post

要创建新的私有 re: Post，请按照以下步骤操作：

1. 打开 re: Post Private 主机，网址为 https://console.aws.amazon.com/repost-private/。
2. 在主机主页上，选择创建私有 re: Post。
3. 如果您尚未为账户配置 IAM 身份中心，请选择开放身份中心。按照 AWS IAM 身份中心用户指南中的入门说明进行操作。
4. 在 “创建私有 re: Post” 页面上，在 “定价” 中，根据您的用例选择免费套餐或标准套餐。如果您已经为账户使用了免费套餐，则无法使用免费套餐选项。
5. 在 “详细信息” 下，执行以下操作：

   在 “姓名” 中，为您的私人 re: Post 输入一个唯一的名称。

   （可选）在描述中，输入您的私人 re: Post 的简短描述。

   在自定义子域名中，输入子域名的自定义名称。
6. （可选）要自定义您的数据加密设置，请在数据加密下选择自定义加密设置。然后，执行以下任一操作：

   在选择 AWS KMS 密钥中，选择 AWS Key Management Service 密钥或亚马逊资源名称 (ARN)。

   –或者–

   选择创建 AWS KMS 密钥。然后，创建密 AWS KMS 钥。
7. （可选）在 “支持案例集成的服务访问权限” 下，选择 “为此 re: Post 启用服务访问权限”。

> **Note**
>
> 您也可以在创建私有 re: Post 后启用此选项。

对于请选择下面的现有 IAM 角色或在 IAM 控制台中创建新角色，请使用搜索栏查找您的现有 IAM 角色。

–或者–

选择在 IAM 控制台中创建新角色。

如果您选择创建新角色，请按照中的说明进行操作创建 IAM 角色。

如果您选择使用现有服务角色，请在搜索栏中输入要使用的角色的 ARN。从下拉列表中选择角色。

有关更多信息，请参阅 在 re: Post Private 中管理对 AWS Support 案例创建和管理的访问权限。

8. （可选）在 “标签” 下，选择 “添加新标签”。然后输入以下信息：

   在 Key 中，输入您的自定义标签密钥。

   在 “值” 中，输入您的自定义标签值。

   要添加更多标签，请选择添加新标签。

9. 选择 “创建这个 re: Post”。

确认页面将告知您的私人 re: Post 正在创建中。您可以在 “状态” 字段中查看私人 re: Post 的状态。创建您的私人 re: Post 后，状态字段将显示正在创建。

创建私人 re: Post 大约需要 30 分钟。当您的私人 re: Post 准备就绪后，“状态” 字段将显示在线。您可以将 AWS 生成的子域用于列在 “设置” 选项卡下的私有 re: Post 来访问您的私有 re: Post。审核完成后，您可以在 “设置” 选项卡下查看私人 re: Post 的自定义子域名。

在 re: Post Private 中管理对 AWS Support 案例创建和管理的访问权限

您必须创建一个 AWS Identity and Access Management (IAM) 角色才能管理从 AWS re: Post Private 访问 AWS Support 案例创建和管理权限。此角色将为您执行以下 AWS Support 操作：

- CreateCase
- AddCommunicationToCase
- ResolveCase

创建 IAM 角色后，向该角色附加一个 IAM 策略，以便该角色拥有完成这些操作所需的权限。当你在 re: Post Private 控制台中创建私人 re: Post 时，你可以选择这个角色。

您的私有 re: Post 中的用户拥有的权限与您授予 IAM 角色的权限相同。

> **Important**
>
> 如果您更改了 IAM 角色或 IAM 策略，则您的更改将应用于您配置的私有 re: Post。

按照以下步骤创建您的 IAM 角色和策略。

主题

使用 AWS 托管策略或创建客户托管策略

要授予角色权限，您可以使用 AWS 托管策略或客户托管策略。

> **Tip**
>
> 如果您不想手动创建策略，那么我们建议您改用 AWS 托管策略并跳过此过程。托管策略会自动拥有所需的权限 AWS Support。您无需手动更新策略。有关更多信息，请参阅 AWS 托管策略： AWSRepostSpaceSupportOperationsPolicy。

按照此步骤为您的角色创建客户管理型策略。此过程使用 IAM 控制台中的 JSON 策略编辑器。

为 re: Post Private 创建客户托管策略

1. 登录 AWS Management Console 并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择策略。
3. 选择创建策略。
4. 选择 JSON 选项卡。
5. 输入您的 JSON，然后在编辑器中替换默认 JSON。您可以使用示例策略。
6. 选择下一步：标签。
7. （可选）您可以使用标签作为键值对将元数据添加到策略。
8. 选择 下一步: 审核。
9. 在查看策略页面，输入 Name（名称），例如 *rePostPrivateSupportPolicy* 和 Description（描述）（可选）。
10. 查看摘要页面以查看该策略允许的权限，然后选择创建策略。

此策略定义角色可以执行的操作。有关更多信息，请参阅《IAM 用户指南》中的创建 IAM policy（控制台）。

示例 IAM policy

您可以将下列示例策略附加到 IAM 角色。此策略允许该角色拥有执行所有必需操作的完全权限 AWS Support。使用该角色配置私有 re: post 后，您的私人 re: post 中的任何用户都具有相同的权限。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "RepostSpaceSupportOperations",
   "Effect": "Allow",
   "Action": [
    "support:AddAttachmentsToSet",
    "support:AddCommunicationToCase",
    "support:CreateCase",
    "support:DescribeCases",
    "support:DescribeCommunications",
    "support:ResolveCase"
   ],
```

```
    "Resource": "*"
   }
  ]
}
```

> **Note**
>
> 有关 re: Post Private 的 AWS 托管策略列表，请参阅。AWS AWS re: Post Private 的托管策略

您可以更新策略以从中移除权限 AWS Support。

有关每项操作的描述，请参阅《服务授权参考》中的以下主题：

- AWS Support的操作、资源和条件键
- 服务限额的操作、资源和条件键
- 的操作、资源和条件键 AWS Identity and Access Management

创建 IAM 角色

创建策略后，您必须创建 IAM 角色，并将策略附加到此角色。当你在 re: Post Private 控制台中创建私人 re: Post 时，你可以选择这个角色。

创建用于创建和管理 AWS Support 案例的角色

1. 登录 AWS Management Console 并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 Roles（角色），然后选择 Create role（创建角色）。
3. 对于 Trusted entity type（可信实体类型），选择 Custom trust policy（自定义信任策略）。
4. 在“自定义信任策略”中，输入以下内容：

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

```
    "Service": "repostspace.amazonaws.com"
   },
   "Action": [
    "sts:AssumeRole",
    "sts:SetSourceIdentity"
   ]
  }
 ]
}
```

5. 选择下一步。
6. 在权限策略下的搜索栏中，输入您创建的 AWS 托管策略或客户托管策略，例如*rePostPrivateSupportPolicy*。选中您希望服务拥有的权限策略旁边的复选框。
7. 选择下一步。
8. 在 “名称、查看和创建” 页面上，在 “角色名称” 中输入一个名称，例如*rePostPrivateSupportRole*。
9. （可选）对于描述，输入角色的描述。
10. 查看信任策略和权限。
11. （可选）您可以使用标签作为键值对将元数据添加到角色。有关将在 IAM 中使用标签的更多信息，请参阅 Tagging IAM resources（标记 IAM 资源）。
12. 选择 创建角色。现在，当你在 re: Post Private 控制台中配置私人 re: post 时，你可以选择这个角色。请参阅 创建新的私人 re: Post。

有关更多信息，请参阅 IAM 用户指南中的为 AWS 服务（控制台）创建角色。

故障排除

要管理 re: Post Private 的访问权限，请参阅以下主题。

目录

我想限制私人 re: Post 中的特定用户执行特定操作

默认情况下，您的私有 re: post 中的用户拥有在 IAM 策略中指定的权限与您附加到您创建的 IAM 角色的权限相同。这意味着私有 re: post 中的任何人都有创建和管理 AWS Support 案例的读取或写入权限，无论他们是否拥有还是 IAM 用户。 AWS 账户

我们建议您遵循以下最佳实操：

- 使用具有所需最低权限的 IAM 策略 AWS Support。请参阅 AWS 托管策略：AWSRepostSpaceSupportOperationsPolicy。

当我配置私有 re: post 时，我看不到我创建的 IAM 角色

如果您的 IAM 角色未出现在 re: Post Private; 列表的 IAM 角色中，则意味着该角色没有 re: post Private 作为可信实体，或者该角色已被删除。您可以更新现有角色或创建一个新角色。请参阅 创建 IAM 角色。

我的 IAM 角色缺少权限

您为私有 re: Post 创建的 IAM 角色需要权限才能执行您想要的操作。例如，如果您想让私人 re: post 中的用户创建支持案例，则该角色必须具有`support:CreateCase`权限。re: post Private 担任此角色来为您执行这些操作。

如果您收到有关缺少权限的错误消息 AWS Support，请验证附加到您的角色的策略是否具有所需的权限。

请参阅前面的 示例 IAM policy。

错误提示我的 IAM 角色无效

确认您为私有 re: post 配置选择了正确的角色。

使用设置和管理用户访问权限 AWS IAM Identity Center

re: Post Private AWS IAM Identity Center 与集成，为您的组织员工提供身份联盟。使用 IAM Identity Center 创建或连接组织中的用户，并集中管理他们对所有 AWS 账户和应用程序的访问权限。有关 IAM 身份中心的更多信息，请参阅什么是 AWS IAM 身份中心（AWS Single Sign-On 的继任者）。有关 IAM Identity Center 入门的更多信息，请参阅入门。要使用 IAM 身份中心，您还必须为该账户 AWS Organizations 激活。

自定义您的私人 re: Post

创建私人 re: Post 后，您可以为其添加一个或多个管理员。管理员使用 re: Post Private 应用程序启动私有 re: Post 并管理其中的用户。他们可以为私人 re: Post 自定义品牌，添加标签对内容进行分类，并选择感兴趣的话题以自动填充内容。有关更多信息，请参阅 AWS re: Post 私有管理指南。

邀请用户收看你的私人 re: Post

创建私人 re: Post 后，您可以将一个或多个用户添加到该私人 re: Post。你可以邀请用户在你的私人 re: Post 中进行协作。用户使用 re: Post Private 应用程序使用您配置的凭据登录。登录私人 re: Post 后，用户可以浏览或搜索现有内容，包括针对其感兴趣主题的量身定制的培训和技术内容。有关更多信息，请参阅 AWS re: Post 私有用户指南。

在 re: Post Private 控制台中管理你的私人 re: post

本节介绍如何在 AWS re: Post 私有控制台中管理您的私有 re: Post。

主题

将用户和群组添加到您的私人 re: Post

如果您是管理员，则可以将用户和群组添加到您的私人 re: Post 中。

将用户添加到您的私人 re: Post

1. 打开 re: Post Private 主机，网址为 https://console.aws.amazon.com/repost-private/。
2. 在导航窗格中，选择我的所有私人 re: Posts。
3. 选择你要管理的私人 re: Post。
4. 选择 Users（用户）选项卡。
5. 在 “用户” 下，选择 “添加用户和群组”。
6. 从列表中，选择要添加到私人 re: Post 中的用户。然后，选择 “分配”。

所选用户将添加到您的私人 re: Post 中，并列在 “用户” 选项卡下。

将群组添加到您的私人 re: Post

1. 打开 re: Post Private 主机，网址为 https://console.aws.amazon.com/repost-private/。
2. 在导航窗格中，选择我的所有私人 re: Posts。
3. 选择你要管理的私人 re: Post。

4. 选择 Groups (组) 选项卡。
5. 选择添加用户和群组。
6. 从列表中，选择要添加到私人 re: Post 中的群组。然后，选择 “分配”。

所选群组将添加到您的私人 re: Post 中，并列在 “群组” 选项卡下。

在你的私人 re: Post 中将用户添加到群组

使用 IAM Identity Center 将新用户添加到您的私有 re: Post 中的现有群组。有关更多信息，请参阅 AWS IAM 身份中心用户指南中的向群组添加用户。

邀请用户和群组加入您的私人 re: Post

请按照以下步骤邀请用户和群组加入 AWS re: Post Private 中的私有 re: Post：

1. 打开 re: Post Private 主机，网址为 https://console.aws.amazon.com/repost-private/。
2. 在导航窗格中，选择我的所有私人 re: Posts。
3. 选择你要管理的私人 re: Post。
4. 要邀请用户加入您的私人 re: Post，请选择 “用户” 选项卡。

   从列表中，选择要邀请其加入私人 re: Post 的用户。然后，选择要重发:Post 的 Onboard 用户。
5. 在 “将用户加入此私密 re: Post” 对话框中，输入以下信息：

   在 “主题” 中，输入您要发送的电子邮件的主题。

   在 B ody 中，为您的私人 re: Post 输入欢迎消息。

   选择 “发送入职电子邮件”。
6. 要邀请群组加入您的私人 re: Post，请选择群组选项卡。

   从列表中，选择要邀请加入私人 re: Post 的群组。然后，选择加入群组以重发:Post。
7. 在 “将群组加入到此私人 re: Post” 对话框中，输入以下信息：

   在 “主题” 中，输入您要发送的电子邮件的主题。

   在 B ody 中，为您的私人 re: Post 输入欢迎消息。

   选择 “发送入职电子邮件”。

欢迎消息将发送给所有选定的用户和群组，其中包含有关如何登录您的私人 re: Post 的信息。

在你的私密回复中将用户推荐给管理员

要将私人 re: Post 用户提升为管理员，请执行以下步骤：

1. 打开 re: Post Private 主机，网址为 https://console.aws.amazon.com/repost-private/。
2. 在导航窗格中，选择我的所有私人 re: Posts。
3. 选择你要管理的私人 re: Post。
4. 选择 Users（用户）选项卡。
5. 选择要提升为管理员的一个或多个用户。
6. 选择 “编辑角色”，然后选择 “设为管理员”。

选定的用户将被提升为管理员。在 “用户” 选项卡下，这些用户的角色更新为 “管理员”。

从您的私人 re: Post 中移除用户或群组

如果您是管理员，则可以将用户或群组从您的私人 re: Post 中移除。

将用户从您的私人 re: Post 中移除

1. 打开 re: Post Private 主机，网址为 https://console.aws.amazon.com/repost-private/。
2. 在导航窗格中，选择我的所有私人 re: Posts。
3. 选择你要管理的私人 re: Post。
4. 在 “用户” 下，从列表中选择要从私人 re: Post 中删除的用户。然后，选择 “删除”。

所选用户将从您的私人 re: Post 中移除。有关已删除用户的信息不再显示在 “用户” 选项卡下。

从你的私人 re: Post 中移除群组

1. 打开 re: Post Private 主机，网址为 https://console.aws.amazon.com/repost-private/。
2. 在导航窗格中，选择我的所有私人 re: Posts。
3. 选择你要管理的私人 re: Post。
4. 选择 Groups (组) 选项卡。
5. 从列表中，选择要从私人 re: Post 中删除的群组。然后，选择 “删除”。

所选群组将从您的私人 re: Post 中移除。有关已删除群组的信息不再显示在 “群组” 选项卡下。

在您的私人 re: P AWS ost 中添加或删除员工

如果您有企业或企业 On-Ramp Support 计划，则可以在您的私人 re: Post 中添加或删除 AWS 员工。如需更多信息，请联系 Concierge Support 或您的技术客户经理 (TAM)。

从 re: Post Private 中删除私人 re: post

要在 AWS re: Post Private 中删除私有 re: Post，请按照以下步骤操作：

1. 打开 re: Post Private 主机，网址为 https://console.aws.amazon.com/repost-private/。
2. 在导航窗格中，选择我的所有私人 re: Posts。
3. 选择要管理的私人 re: Post，然后选择 “删除”。
4. 选择所有选项以确认并确认您要永久删除私人 re: Post 和与之相关的数据。

> **Important**
>
> 当你删除私有 re: post 时，与私有 re: post 相关的所有配置信息都将被删除。私人 re: post 被删除后，您将无法从中恢复任何内容。

5. 当系统提示您提供额外的书面同意时，请输入您的私人 re: Post 的名称。然后选择删除。

删除您的私人 re: Post 大约需要 30 分钟。

监控 AWS re: Post 私有版

监控是维护 AWS re: Post Private 和其他AWS解决方案的可靠性、可用性和性能的重要组成部分。AWS提供了以下监控工具，用于监视 re: Post Private，在出现问题时进行报告，并在适当时自动采取措施：

- 亚马逊会实时 CloudWatch监控您的AWS资源和您运行AWS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 CloudWatch 跟踪您的 Amazon EC2 实例的 CPU 使用率或其他指标，并在需要时自动启动新实例。有关更多信息，请参阅亚马逊 CloudWatch 用户指南。
- AWS CloudTrail捕获由您或为您发起的 API 调用AWS 账户和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以标识哪些用户和账户调用了 AWS、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。

通过亚马逊监控 AWS re: Post Private CloudWatch

您可以使用 Amazon 监控 AWS re: Post Private CloudWatch，亚马逊会收集原始数据并将其处理成可读的近乎实时的指标。这些统计数据会保存 15 个月，这样您就可以访问历史信息并更好地了解您的 Web 应用程序或服务的性能。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，请参阅亚马逊 CloudWatch 用户指南。

re: post Private 服务报告命名空间中的以下`AWS/rePostPrivate`指标。

指标	描述
`NumberOfSpaces`	当前账户中私人 re: Posts 的数量。 单位：计数
`NumberOfUsers`	私人 re: Post 中的用户数量。此指标使用 SpaceID 作为维度。 单位：计数
`ContentSize`	私人 re: Post 中的内容量。此指标使用 SpaceID 作为维度。 单位：字节

re: Post Private 指标支持以下维度。

维度	描述
spaceId	私人 re: post 的唯一标识符。

使用记录 AWS re: Post 私有 API 调用 AWS CloudTrail

AWS re: Post Private 与AWS CloudTrail一项服务集成，该服务提供用户、角色或服务在 re: Post Pri AWS vate 中采取的操作的记录。 CloudTrail 将 re: Post Private 的所有 API 调用捕获为事件。捕获的调用包括来自 re: Post Private 控制台的调用和对 re: Post Private API 操作的代码调用。如果您创建跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 re: Post Private 的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向 re: Post Private 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

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

re: 在中发布私人信息 CloudTrail

CloudTrail 在您创建账户AWS 账户时已在您的账户上启用。当 re: Post Private 中发生活动时，该活动会与其他AWS服务 CloudTrail 事件一起记录在事件历史记录中。您可以在 AWS 账户 中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录。

要持续记录您的事件AWS 账户，包括 re: Post Private 的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）桶。此外，您可以配置其他AWS服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 为您的 AWS 账户创建跟踪
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

所有 re: Post Private 操作均由 AWS re: Post 私有 API 参考记录 CloudTrail 并记录在 AWS re: Post Private 参考中。re: Post Private 支持将以下操作作为事件记录在日志文件中： CloudTrail

- CreateSpace
- DeleteSpace
- DeregisterAdmin
- GetSpace
- ListSpaces
- ListTagsForResource
- RegisterAdmin
- SendInvites
- TagResource
- UntagResource
- UpdateSpace

re: post Private 支持将以下AWS Support操作作为事件记录在 CloudTrail 日志文件中：

- CreateCase
- AddCommunicationToCase
- ResolveCase

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 AWS Identity and Access Management（IAM）用户凭证发出。
- 请求是使用角色还是联合身份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 re: Post 私有日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了演示该`CreateSpace`操作的 CloudTrail 日志条目。

```
{
   "eventVersion": "1.08",
   "userIdentity": {
       "type": "AssumedRole",
       "principalId": "AROAQM47QIR7WLEXAMPLE:user",
       "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
       "accountId": "123456789012",
       "accessKeyId": "EXAMPLE_KEY_ID",
       "sessionContext": {
           "sessionIssuer": {
               "type": "Role",
               "principalId": "AROAQM47QIR7WLEXAMPLE",
               "arn": "arn:aws:iam::123456789012:role/User",
               "accountId": "123456789012",
               "userName": "User"
           },
           "webIdFederationData": {},
           "attributes": {
               "creationDate": "2023-11-06T19:24:39Z",
               "mfaAuthenticated": "false"
           }
       }
   },
   "eventTime": "2023-11-06T21:37:44Z",
   "eventSource": "repostspace.amazonaws.com",
   "eventName": "CreateSpace",
   "awsRegion": "us-west-2",
   "sourceIPAddress": "205.251.233.176",
   "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36",
   "requestParameters": {
       "spaceName": "Test space name",
       "spaceSubdomain": "customsubdomain",
       "tagSet": {},
       "tier": "2000",
       "roleArn": "",
       "spaceDescription": "Test space description"
   },
   "responseElements": {
       "spaceId": "SPLPWvQmv9SIWYF30EXAMPLE",
       "Access-Control-Expose-Headers": "x-amzn-errortype, x-amzn-requestid, x-amzn-
errormessage, x-amzn-trace-id, x-amz-apigw-id, date"
```

```
    },
    "requestID": "71d815e0-6632-4ec9-9fac-92af3e4a86dc",
    "eventID": "30a6c3da-ce2e-4931-ba5d-b3cc7cf16ec8",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

以下示例显示了演示该RegisterAdmin操作的 CloudTrail 日志条目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAQM47QIR7WLEXAMPLE:user",
        "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR7WLEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/User",
                "accountId": "123456789012",
                "userName": "User"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-07T21:17:19Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-07T21:24:23Z",
    "eventSource": "repostspace.amazonaws.com",
    "eventName": "RegisterAdmin",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
```

```
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36",
    "requestParameters": {
        "adminId": "08612310-a0f1-7063-3e54-fb2960444dd1",
        "spaceId": "SPlYNZE-ylQEmAXpmEXAMPLE"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-errortype, x-amzn-requestid, x-amzn-
errormessage, x-amzn-trace-id, x-amz-apigw-id, date"
    },
    "requestID": "9939ebbe-8599-4f9a-827b-4995e3006001",
    "eventID": "e1873b18-f80c-4934-9ff2-bf5b35c78031",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

以下示例显示了演示该ListSpaces操作的 CloudTrail 日志条目。

```
 {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAQM47QIR7WLEXAMPLE:user",
        "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR7WLEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/User",
                "accountId": "123456789012",
                "userName": "User"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-09T22:28:23Z",
                "mfaAuthenticated": "false"
```

```
            }
        }
    },
    "eventTime": "2023-11-09T22:38:34Z",
    "eventSource": "repostspace.amazonaws.com",
    "eventName": "ListSpaces",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "95be587b-c04f-4eb0-9269-12fee33ae2e3",
    "eventID": "9777da32-545f-44c4-af0b-1d9109b8cbc3",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

以下示例显示了演示该ResolveCase操作的 CloudTrail 日志条目。您可以使用此日志条目中的sourceIdentity元素来识别解决该案例的用户。

```
 {
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAQM47QIR76DQZ7N5WX:create-support-case-
Uk1iHNTWQEOLmR2BR1FDJQ",
        "arn": "arn:aws:sts::123456789012:assumed-role/AWSRepostSpaceRole/create-
support-case-Uk1iHNTWQEOLmR2BR1FDJQ",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR76DQZ7N5WX",
                "arn": "arn:aws:iam::123456789012:role/AWSRepostSpaceRole",
                "accountId": "123456789012",
                "userName": "AWSRepostSpaceRole"
            },
```

```
            "attributes": {
                "creationDate": "2023-11-17T21:46:42Z",
                "mfaAuthenticated": "false"
            },
            "sourceIdentity": "28e17330-10f1-705d-7cba-3a62a6b10e2e"
        }
    },
    "eventTime": "2023-11-17T21:46:44Z",
    "eventSource": "support.amazonaws.com",
    "eventName": "ResolveCase",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.68.27.29",
    "userAgent": "aws-sdk-nodejs/2.1363.0 linux/v16.20.2 exec-env/AWS_ECS_FARGATE
 promise",
    "requestParameters": {
        "caseId": "case-123456789012-muen-2023-75d2c35481b96357"
    },
    "responseElements": {
        "initialCaseStatus": "unassigned",
        "finalCaseStatus": "resolved"
    },
    "requestID": "594b91c6-df1c-47e4-a834-d67d67f34b9d",
    "eventID": "7fc9cbe4-c8d5-4d61-a016-e076de272fff",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "support.us-west-2.amazonaws.com"
    }
}
```

re: Post Private

以下信息可以帮助您解决 AWS re: Post Private 的问题。

主题

无法在特定区域设置我的私人 re: post AWS

re: Post Private 仅在美国东部（弗吉尼亚北部）、美国西部（俄勒冈）、欧洲（法兰克福）、亚太地区（新加坡）、亚太地区（悉尼）、加拿大（中部）和欧洲（爱尔兰）地区可用。请务必在其中一个区域创建自己的私人 re: Post。

无法在我的账户中设置私人 re: Post

请确保您的账户已启 AWS IAM Identity Center 用，并在要创建私有 re: Post 的同一个区域中设置 IAM 身份中心。有关更多信息，请参阅 先决条件。

无法在私密的 re: Post 中管理用户或群组

请确保您拥有编辑私人 re: Post 以及管理私人 re: Post 中的用户和群组所需的权限。有关更多信息，请参阅 AWS re: Post 基于私有身份的策略示例。

文档历史记录

下表描述了 AWS re: Post Private 的文档版本：

变更	说明	日期
更新	将美国东部（弗吉尼亚北部）、亚太地区（悉尼）、加拿大（中部）和欧洲（爱尔兰）添加到支持的区域	2024年5月10日
更新	将亚太地区（新加坡）添加到支持的区域	2024 年 3 月 6 日
新资源	添加了适用于 AWS re: Post Private 的 AWS 托管策略的文档	2023 年 11 月 26 日
初始版本	re: Post 私有控制台管理指南的初始版本	2023 年 11 月 26 日

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。