



主控台管理指南

# AWS re:Post Private



# AWS re:Post Private: 主控台管理指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

# Table of Contents

什麼是 AWS re : Post Private ? .....	1
存取 re : Post Private .....	1
定價 .....	1
必要條件 .....	2
在船上轉發：私人發布 .....	3
安全 .....	4
資料保護 .....	4
使用加密來保護資料 .....	5
傳輸中加密 .....	5
金鑰管理 .....	5
re : Post Private 如何使用 IAM .....	6
re : Post 私有身分型政策 .....	6
re : Post 私有資源型政策 .....	7
以標籤為基礎的授權 .....	7
re : Post Private IAM角色 .....	8
服務連結角色 .....	8
服務角色 .....	8
使用服務連結角色 .....	8
身分型政策範例 .....	11
內嵌政策 .....	13
AWS 受管政策 .....	16
故障診斷 .....	18
法規遵循驗證 .....	20
恢復能力 .....	21
基礎設施安全性 .....	21
配額 .....	22
Service Quotas .....	22
API 節流限制 .....	22
建立、設定和自訂您的私有 re : Post .....	24
建立新的私有 re : Post .....	24
管理 Support 案例建立和管理 .....	26
使用或建立受管政策 .....	26
範例IAM政策 .....	27
建立 IAM 角色 .....	28

故障診斷 .....	29
設定和管理使用者存取權 .....	30
自訂您的私有 re : Post .....	31
邀請使用者到您的私有 re : Post .....	31
管理您的私有 re : Post .....	32
新增使用者 .....	32
新增群組 .....	33
將使用者新增至群組 .....	33
邀請使用者和群組 .....	33
將角色指派給使用者 .....	34
移除使用者 .....	35
移除群組 .....	35
新增或移除 AWS 員工 .....	35
刪除私有 re : Post .....	36
監督 Re: 私人貼文 .....	37
使用監控 CloudWatch .....	37
記錄 RE: 使用張貼私人 API 呼叫 AWS CloudTrail .....	38
Re: 張貼私人資訊 CloudTrail .....	38
瞭解 RE: 張貼私人記錄檔項目 .....	39
故障診斷 .....	45
無法在特定地區設定我的私人 Re: POST AWS .....	45
無法設定私人 Re: 在我的帳戶中張貼 .....	45
無法管理私人 RE 中的使用者或群組:POST .....	45
文件歷史紀錄 .....	46
.....	xlvii

# 什麼是 AWS re : Post Private ?

AWS re : Post Private 是 AWS re:Post 適用於具有 Enterprise Support 或 Enterprise On-Ramp Support 計劃之企業的私有版本。它可讓您存取知識和專家，以加速雲端採用並提高開發人員生產力。透過組織特定的私有 re : Post，您可以建立組織特定的開發人員社群，以大規模提高效率，並提供寶貴的知識資源。此外，re : Post Private 會集中處理受信任 AWS 的技術內容，並提供私有討論論壇，以改善團隊內部協作和與合作的方式AWS，以消除技術障礙、加速創新，並更有效率地在雲端中擴展。

如需詳細資訊，請參閱 [AWS re : Post Private](#)。

## 存取 re : Post Private

管理員使用 AWS re : Post Private 主控台建立其組織特定的 re : Post。當管理員建立私有 re : Post 時，他們可以為私有 re : Post 命名，並在 下定義子網域\*.private.repost.aws。組織的私有 re : Post 管理員可以使用 設定使用者存取權，AWS IAM Identity Center 並指定下列其中一個身分來源進行身分驗證：Identity Center 目錄、Active Directory 或外部身分提供者。設定使用者後，主控台管理員可以將 re : Post Private admin 角色指派給一或多個使用者。re : Post Private Administrators 可以自訂其私有 re : Post 應用程式，以符合組織品牌和知識需求。熟悉組織架構和工作負載 AWS 的帳戶團隊成員，例如技術客戶經理，會自動新增至組織的私有 re : Post 以進行協同合作。

re : Post Private 應用程式的管理員可以自訂品牌、新增標籤來分類內容，以及選取開發人員感興趣的主題，以自動填入訓練和技術內容。他們也可以邀請使用者加入其私有 re : Post，以提高協同合作。如需詳細資訊，請參閱 [AWS re : Post Private Administration Guide](#)。

非管理使用者使用 re : Post Private 應用程式，使用管理員設定的憑證登入。登入私有 re : Post 後，使用者可以瀏覽或搜尋現有內容，包括為其感興趣的主題範圍量身打造的訓練和技術內容。使用者也可以直接從其私有 re : Post 搜尋 AWS 公有技術內容，並建立私有執行緒以進行 AWS 公有內容的內部討論。使用者可以透過提出問題、提供回應或發佈文章，協同解決 AWS 技術問題並從私有 re : Post 的其他使用者取得技術指導。使用者也可以將討論執行緒轉換為 Support 案例。使用者可以選擇將回應從 Support 新增至私有 re : Post。如需詳細資訊，請參閱 [AWS re : Post Private 使用者指南](#)。

## 定價

只有具備 Enterprise Support ( ES ) 和 Enterprise On-Ramp ( EOP ) Support 計劃的客戶才能訂閱 re : Post Private 服務。您可以從兩個可用的定價層 - 免費層和標準層中進行選擇。免費方案可讓您在

順利轉換至付費方案之前，探索並嘗試完整六個月的標準方案功能。如果您使用 Standard 層，則您可以支付每位使用者每月訂閱費用，以使用 re : Post Private。如需詳細資訊，請參閱 [定價](#)。

## 必要條件

您必須先符合下列先決條件，才能建立新的私有 re : Post 或管理 re : Post Private 中的現有私有 AWS re : Post :

- 您必須註冊 [Enterprise](#) 或 [Enterprise On-Ramp](#) Support Plan。
- 您必須在您要設定私有 re : Post 的相同區域中 [啟用 AWS IAM Identity Center](#)。
- 您必須建立具有為您建立、管理和解決 Support 案例所需許可 AWS Identity and Access Management 的角色。re : Post Private 服務使用此角色對 進行API呼叫 Support。如需詳細資訊，請參閱 [管理 re : Post Private 中 Support 案例建立和管理的存取權](#)。

## 登機重新發佈：透過 IAM 身分中心私人張貼

RE: Post Private 與AWS IAM Identity Center整合，為您的員工提供身分聯盟。透過 IAM 身分中心，使用者會重新導向至其現有的公司目錄，以使用現有的登入資料登入。然後，他們將無縫地登錄到他們的私人 RE: POST。這可確保強制執行密碼原則和雙因素驗證等安全性設定。使用 IAM 身分中心不會影響您現有的 IAM 組態。

如果您沒有現有的使用者目錄或不想要聯合，則 IAM Identity Center 會提供整合的使用者目錄，供您建立 Re: Post Private 的使用者和群組。Re: Private 不支援在私有 RE: POST 中使用 IAM 使用者和角色指派許可。私人 RE: POST 中的使用者權限是由管理員在其私人 Re: POST 應用程式上設定。

如需 IAM 身分中心的詳細資訊，請參閱[什麼是 AWS IAM 身分中心 \(AWS Single Sign-On 的後續產品\)](#)。如需開始使用 IAM 身分中心的詳細資訊，請參閱[入門](#)。若要使用 IAM 身分中心，您還必須為該帳戶AWS Organizations啟用。

### Important

RE：私有貼文僅支援 [IAM 身分中心的組織執行個體](#)。

## re : Post Private 中的安全性

的雲端安全 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了滿足最安全敏感組織的需求而建置。

安全性是 AWS 和 之間的共同責任。[共同責任模型](#)將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。AWS 也提供您可以安全使用的服務。第三方稽核人員會定期測試和驗證我們的安全有效性，這是[AWS 合規計畫](#)的一部分。若要了解適用於 AWS re : Post Private 的合規計畫，請參閱依[AWS 合規計畫在範圍內的合規計畫](#)
- 雲端安全 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您的要求和適用法律和法規。

本文件可協助您了解如何在使用 re : Post Private 時套用共同責任模型。下列主題說明如何設定 re : Post Private 以符合您的安全和合規目標。您也會了解如何使用其他服務 AWS 來協助您監控和保護 re : Post 私有資源。

### 主題

- [AWS re : Post Private 中的資料保護](#)
- [re : Post Private 如何使用 IAM](#)
- [AWS re : Post Private 的合規驗證](#)
- [AWS re : Post Private 中的復原能力](#)
- [AWS re : Post Private 中的基礎設施安全](#)

## AWS re : Post Private 中的資料保護

AWS [共同責任模型](#)適用於 AWS re : Post Private 中的資料保護。如本模型所述，AWS 負責保護執行所有的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱[資料隱私權](#)。[FAQ](#)如需歐洲資料保護的相關資訊，請參閱AWS 安全部落格上的[AWS 共同責任模型和GDPR](#)部落格文章。

為了資料保護目的，我們建議您保護 AWS 帳戶憑證，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management ( ) 設定個別使用者IAM。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 對每個帳戶使用多重要素驗證 ( MFA )。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 和 建議 TLS 1.3。
- 使用 設定 API和使用者活動記錄 AWS CloudTrail。如需使用 CloudTrail 線索擷取 AWS 活動的資訊，請參閱 AWS CloudTrail 使用者指南 中的[使用 CloudTrail 線索](#)。
- 使用 AWS 加密解決方案，以及 中的所有預設安全控制項 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列介面或 FIPS 存取 時需要 140-3 個經過驗證的密碼編譯模組API，請使用 FIPS端點。如需可用FIPS端點的詳細資訊，請參閱[聯邦資訊處理標準 \( FIPS \) 140-3](#)。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 re : Post Private 或其他 AWS 服務 使用主控台API AWS CLI、或 時 AWS SDKs。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您將 URL提供給外部伺服器，強烈建議您在 中不要包含憑證資訊，URL以驗證您對該伺服器的請求。

## 使用加密來保護資料

### 靜態加密

re : Post Private 使用 Amazon Simple Storage Service 儲存貯體、Amazon DynamoDB 資料庫、Amazon Neptune 資料庫，以及使用 Amazon 受管金鑰或客戶受管金鑰靜態加密的 Amazon OpenSearch Service 網域。

### 傳輸中加密

re : Post Private 使用 HTTPS 通訊協定與您的用戶端應用程式通訊。它使用 HTTPS和 AWS 簽章來代表您的應用程式與其他 服務通訊。

### 金鑰管理

re : Post Private 已與 整合 AWS Key Management Service 並支援 AWS KMS 金鑰。您可以在建立私有 re : Post 時自訂資料加密設定。若要這麼做，您可以選擇現有的 AWS KMS 金鑰或[建立新的 AWS KMS 金鑰](#)。

## re : Post Private 如何使用 IAM

使用 IAM 管理 AWS re : Post Private 的存取權之前，您必須了解哪些IAM功能可與 re : Post Private 搭配使用。若要取得 re : Post Private 和其他 AWS 服務如何與 搭配使用的高階檢視IAM，請參閱 IAM 使用者指南 中的[AWS 使用的服務IAM](#)。

### re : Post 私有身分型政策

透過身分IAM型政策，您可以指定允許或拒絕的動作。re : Post Private 支援特定動作。若要了解您在 JSON政策中使用的元素，請參閱 IAM 使用者指南 中的[IAMJSON政策元素參考](#)。

#### 動作

管理員可以使用 AWS JSON政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action元素說明您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API操作相同的名稱。有一些例外狀況，例如沒有相符API操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

re : Post Private 中的政策動作在動作之前使用下列字首：repostspace:。例如，若要授予某人執行 re : Post Private CreateSpaceAPI操作的許可，您可以在其政策中包含 repostspace:CreateSpace動作。政策陳述式必須包含 Action或 NotAction元素。re : Post Private 會定義自己的動作集，描述您可以使用此服務執行的任務。

若要在單一陳述式中指定多個動作，請用逗號分隔，如下所示：

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

您也可以使用萬用字元 (\*) 來指定多個動作。例如，若要指定開頭是 Describe 文字的所有動作，請包含以下動作：

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

若要查看 re : Post Private 動作清單，請參閱 IAM 使用者指南 中的 [re : Post Private 定義的動作](#)。

## 資源

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素會指定動作套用的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 [Amazon Resource Name \( ARN \) 指定資源](#)。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (\*) 來表示陳述式適用於所有資源。

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

## 條件索引鍵

re : Post Private 不提供任何服務特定的條件金鑰，但支援使用全域條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱 IAM 使用者指南 中的 [AWS 全域條件內容索引鍵](#)。

## 範例

若要檢視 re : Post 私有身分型政策的範例，請參閱 [AWS re : Post 私有身分型政策範例](#)。

## re : Post 私有資源型政策

資源型政策是您附加至資源JSON的政策文件。資源型政策的範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中 [指定主體](#)。主體可以包括帳戶、使用者、角色、聯合使用者 AWS 或服務。資源型政策是位於該服務中的內嵌政策。您無法在資源型政策IAM中使用來自的 AWS 受管政策。

re : Post Private 不支援資源型政策。

## 以標籤為基礎的授權

re : Post Private 支援標記資源或根據標籤控制存取權。如需詳細資訊，請參閱 [使用標籤 控制對AWS 資源的存取](#)。

## re : Post Private IAM角色

[IAM 角色](#)是您 AWS 帳戶中具有特定許可的實體。

### 搭配 re : Post Private 使用臨時憑證

我們強烈建議使用臨時憑證來登入聯合、擔任IAM角色或擔任跨帳戶角色。您可以透過呼叫 AWS STS API [AssumeRole](#)或 等操作來取得臨時安全憑證[GetFederationToken](#)。

re : Post Private 支援使用臨時憑證。

## 服務連結角色

[服務連結角色](#)可讓 AWS 服務存取其他服務中的資源，為您完成動作。服務連結角色會顯示在您的帳戶中IAM，並由 服務擁有。IAM 管理員可以檢視但無法編輯服務連結角色的許可。

## 服務角色

此功能可讓 服務為您擔任[服務角色](#)。此角色允許服務存取其他服務中的資源，以為您完成動作。如需詳細資訊，請參閱[建立角色以將許可委派給AWS服務](#)。服務角色會顯示在您的帳戶中IAM，並由 帳戶擁有。這表示IAM管理員可以變更此角色的許可。不過，這樣可能會破壞此服務的功能。

## 使用 re : Post Private 的服務連結角色

AWS re : Post Private 使用 AWS Identity and Access Management ( IAM ) [服務連結角色](#)。服務連結角色是直接連結至 re : Post Private 的唯一IAM角色類型。服務連結角色由 re : Post Private 預先定義，並包含服務 AWS 代表您呼叫其他服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 re : Post Private，因為您不需要手動新增必要的許可。re : Post Private 會定義其服務連結角色的許可，除非另有定義，否則只有 re : Post Private 可以擔任其角色。定義的許可包括信任政策和許可政策，該許可政策無法連接到任何其他IAM實體。

如需有關支援服務連結角色的其他 服務的資訊，請參閱服務連結角色欄中[AWS 使用的服務IAM](#)，並尋找具有是 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

### re : Post Private 的服務連結角色許可

re : Post Private 使用名為 的服務連結角色AWSServiceRoleForrePostPrivate。re : Post Private 使用此服務連結角色將資料發佈至 CloudWatch。

AWSServiceRoleForrePostPrivate 服務連結角色信任下列 服務擔任該角色：

- `repostspace.amazonaws.com`

名為 `re:PostPrivateCloudWatchAccess` 的角色許可政策 `AWSrePostPrivateCloudWatchAccess` 允許 `re:PostPrivate` 對指定的資源完成下列動作：

- 上的動作 `cloudwatch:PutMetricData`

您必須設定許可，以允許您的使用者、群組或角色建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南 中的 [服務連結角色許可](#)。

如需詳細資訊，請參閱 [AWSrePostPrivateCloudWatchAccess](#)。

## 建立 `re:PostPrivate` 的服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、AWS CLI 或 `re:PostPrivate` 中建立第一個私有 `re:Post` 時，AWS API 會為您建立服務連結角色。

### Important

此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。此外，如果您在 2023 年 12 月 1 日之前使用 `re:PostPrivate` 服務，則當其開始支援服務連結角色時，`re:PostPrivate` 會在您的帳戶中建立 `AWSServiceRoleForrePostPrivate` 角色。若要進一步了解，請參閱 [我的 中出現的新角色 AWS 帳戶](#)。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您建立第一個私有 `re:Post` 時，`re:PostPrivate` 會再次為您建立服務連結角色。

在 AWS CLI 或 `re:PostPrivate` 中 AWS API，使用服務名稱建立 `repostspace.amazonaws.com` 服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南 中的 [建立服務連結角色](#)。如果您刪除此服務連結角色，您可以使用此相同的程序以再次建立該角色。

## 編輯 `re:PostPrivate` 的服務連結角色

`re:PostPrivate` 不允許您編輯 `AWSServiceRoleForrePostPrivate` 服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。不過，您可以使用 `re:PostPrivate` 編輯角色的描述 IAM。如需詳細資訊，請參閱 IAM 使用者指南 中的 [編輯服務連結角色](#)。

## 刪除 re : Post Private 的服務連結角色

您不需要手動刪除 `AWSServiceRoleForrePostPrivate` 角色。當您在 AWS Management Console、AWS CLI 或 中刪除私有 re : Post 時 AWS API , re : Post Private 會為您刪除服務連結角色。

您也可以使用 IAM 主控台 AWS CLI、 或 AWS API 手動刪除服務連結角色。

使用 手動刪除服務連結角色 IAM

使用 IAM 主控台 AWS CLI、 或 AWS API 刪除 `AWSServiceRoleForrePostPrivate` 服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南 中的 [刪除服務連結角色](#)。

## re : Post Private Service-linked 角色的支援區域

re : Post Private 支援在提供服務的 AWS 區域中使用服務連結角色。

區域名稱	區域身分	支援 re : Post Private
美國東部 (維吉尼亞北部)	us-east-1	是
美國東部 (俄亥俄)	us-east-2	否
美國西部 (加利佛尼亞北部)	us-west-1	否
美國西部 (奧勒岡)	us-west-2	是
非洲 (開普敦)	af-south-1	否
亞太區域 (香港)	ap-east-1	否
亞太區域 (雅加達)	ap-southeast-3	否
亞太區域 (孟買)	ap-south-1	否
亞太區域 (大阪)	ap-northeast-3	否
亞太區域 (首爾)	ap-northeast-2	否
亞太區域 (新加坡)	ap-southeast-1	是
亞太區域 (雪梨)	ap-southeast-2	是

區域名稱	區域身分	支援 re : Post Private
亞太區域 (東京)	ap-northeast-1	否
加拿大 (中部)	ca-central-1	是
歐洲 (法蘭克福)	eu-central-1	是
歐洲 (愛爾蘭)	eu-west-1	是
歐洲 (倫敦)	eu-west-2	否
歐洲 (米蘭)	eu-south-1	否
歐洲 (巴黎)	eu-west-3	否
歐洲 (斯德哥爾摩)	eu-north-1	否
中東 (巴林)	me-south-1	否
中東 (UAE)	me-central-1	否
南美洲 (聖保羅)	sa-east-1	否

## AWS re : Post 私有身分型政策範例

### Note

為了提高安全性，請盡可能建立聯合使用者，而不是IAM使用者。

根據預設，AWS Identity and Access Management 使用者和角色沒有建立或修改 AWS re : Post Private 資源的許可。他們也無法使用 AWS Management Console AWS CLI、或執行任務 AWS API。IAM 管理員必須建立IAM政策，授予使用者和角色許可，以對所需的指定資源執行特定API操作。然後，管理員必須將這些政策連接到需要這些許可IAM的使用者或群組。

若要了解如何使用這些範例政策文件建立身分IAM型JSON政策，請參閱 IAM 使用者指南 中的[建立IAM政策](#)。

主題

- [政策最佳實務](#)
- [允許使用者檢視他們自己的許可](#)

## 政策最佳實務

身分型政策會決定某人是否可以在帳戶中建立、存取或刪除 re : Post Private 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用受AWS管政策，將許可授予許多常見使用案例。它們可在您的 中使用 AWS 帳戶。建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需詳細資訊，請參閱 IAM 使用者指南 中的 [AWS 受管政策](#) 或 [AWS 受管政策](#)。
- 套用最低權限許可 – 當您使用IAM政策設定許可時，只會授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的詳細資訊，請參閱 IAM 使用者指南 [中的政策和許可IAM](#)。
- 使用IAM政策中的條件來進一步限制存取：您可以將條件新增至政策，以限制對動作和資源的存取。例如，您可以撰寫政策條件來指定所有請求都必須使用 傳送SSL。如果透過特定 使用服務動作，例如 AWS 服務，您也可以使用 條件來授予其存取權 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南 中的 [IAMJSON政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證您的IAM政策，以確保安全且功能許可 – IAM Access Analyzer 會驗證新的和現有的政策，讓政策遵循IAM政策語言（JSON）和IAM最佳實務。IAM Access Analyzer 提供超過 100 個政策檢查和可操作的建議，協助您撰寫安全且實用的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的 [使用 IAM Access Analyzer 驗證政策](#)。
- 需要多因素身分驗證（MFA）– 如果您有需要 IAM使用者或 根使用者的案例 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫API操作MFA時要求，請將MFA條件新增至您的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的 [使用 安全API存取MFA](#)。

如需 中最佳實務的詳細資訊IAM，請參閱 IAM 使用者指南 [中的安全最佳實務IAM](#)。

## 允許使用者檢視他們自己的許可

此範例示範如何建立政策，允許使用者檢視連接至其IAM使用者身分的內嵌和受管政策。此政策包含在 主控台上完成此動作或使用 AWS CLI 或 以程式設計方式完成此動作的許可 AWS API。

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

```
"Statement": [
  {
    "Sid": "ViewOwnUserInfo",
    "Effect": "Allow",
    "Action": [
      "iam:GetUserPolicy",
      "iam:ListGroupsWithUser",
      "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": "*"
  }
]
```

## 內嵌政策

內嵌政策是您建立和管理的政策。您可以直接將內嵌政策內嵌至使用者、群組或角色。下列政策範例示範如何指派執行 AWS re : Post Private 動作的許可。如需內嵌政策的一般資訊，請參閱 AWS IAM 使用者指南 中的 [管理IAM政策](#)。您可以使用 AWS Management Console、AWS Command Line Interface ( AWS CLI ) 或 AWS Identity and Access Management API來建立和內嵌內嵌政策。

### 主題

- [re : Post Private 的唯讀存取權](#)
- [完全存取 re : Post Private](#)

## re : Post Private 的唯讀存取權

下列政策會授予 IAM Identity Center 和 re : Post Private 主控台使用者的讀取存取權。此政策允許使用者執行僅供讀取的 re : Post Private 動作。

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

## 完全存取 re : Post Private

下列政策會將完整存取權授予 IAM Identity Center 和 re : Post Private 主控台的使用者。此政策允許使用者執行所有 re : Post Private 動作。

```
{
  "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 受管政策

使用 AWS 受管政策可讓新增許可給使用者、群組和角色，比自行撰寫政策更輕鬆。建立 [IAM 客戶受管政策](#) 需要時間和專業知識，為您的團隊提供他們所需的許可。使用 AWS 受管政策快速入門。這些政策涵蓋常見的使用案例，可在您的帳戶中使用 AWS。如需 AWS 受管政策的詳細資訊，請參閱 IAM 使用者指南 中的 [AWS 受管政策](#)。

AWS 服務會維護和更新 AWS 受管政策。您無法變更 AWS 受管政策中的許可。服務偶爾可能會將其他許可新增至 AWS 受管政策，以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。啟動新功能或新操作可用時，服務最有可能更新 AWS 受管政策。服務不會從 AWS 受管政策中移除許可，因此政策更新不會破壞現有的許可。

此外，AWS 支援跨多個 服務之任務函數的受管政策。例如，ReadOnlyAccess AWS 受管政策提供所有 AWS 服務和資源的唯讀存取權。服務啟動新功能時，會為新操作和資源 AWS 新增唯讀許可。如需詳細資訊，請參閱 IAM 使用者指南 中的 [AWS 受管政策](#)。

### 主題

- [AWS 受管政策 : AWSRepostSpaceSupportOperationsPolicy](#)
- [AWS 受管政策 : AWSrePostPrivateCloudWatchAccess](#)
- [AWS re : Post Private Update to AWS 受管政策](#)

### AWS 受管政策 : AWSRepostSpaceSupportOperationsPolicy

此政策允許 AWS re : Post Private 服務建立、管理和解決透過 re : Post Private Web 應用程式建立的 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 受管政策：AWSrePostPrivateCloudWatchAccess

此政策允許 re : Post Private 服務將資料發佈至 CloudWatch。

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

## AWS re : Post Private Update to AWS 受管政策

檢視自此服務開始追蹤這些變更以來 re : Post Private 受 AWS 管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱[文件歷史記錄](#)頁面上的RSS摘要。

下表說明自 2023 年 11 月 26 日起 re : Post 私有受管政策的重要更新。

變更	描述	日期
新政策 - <a href="#">AWSrePostPrivateCloudWatchAccess</a>	將資料發佈至 的新受管政策 CloudWatch	2023 年 11 月 26 日
新政策 - <a href="#">AWSRepostSpaceSupportOperationsPolicy</a>	AWS re : Post Private 中AWS 支援功能的新受管政策	2023 年 11 月 26 日
re : Post Private 開始追蹤變更	re : Post Private 開始追蹤其 AWS 受管政策的變更	2023 年 11 月 26 日

## 對 AWS re : Post Private Identity 和 Access 進行故障診斷

使用下列資訊來協助您診斷和修正使用 re : Post Private 和 時可能遇到的常見問題IAM。

### 主題

- [我無權在 re : Post Private 中執行動作](#)
- [我無權執行 iam : PassRole](#)
- [我想要允許 以外的人員 AWS 帳戶 存取我的 re : Post Private 資源](#)

### 我無權在 re : Post Private 中執行動作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

當mateojacksonIAM使用者嘗試使用主控台檢視虛構`my-example-widget`資源的詳細資訊，但沒有虛構`repostPrivate:GetWidget`許可時，會發生下列錯誤範例。

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

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 `repostPrivate:GetWidget` 動作存取 `my-example-widget` 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

## 我無權執行 iam : PassRole

如果您收到錯誤，表示您無權執行iam:PassRole動作，則必須更新政策，才能傳遞角色以重新：張貼私有。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 marymajor IAM的使用者嘗試使用主控台在 re : Post Private 中執行動作時，會發生下列錯誤範例。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

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

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

## 我想要允許 以外的人員 AWS 帳戶 存取我的 re : Post Private 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。對於支援資源型政策或存取控制清單（ACLs）的服務，您可以使用這些政策來授予人員對資源的存取權。

如需進一步了解，請參閱以下內容：

- 若要了解 re : Post Private 是否支援這些功能，請參閱 [re : Post Private 如何使用 IAM](#)。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱 IAM 使用者指南 中的 [在您 AWS 帳戶 擁有的另一個資源中為IAM使用者提供存取權](#)。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱 使用者指南 中的 [提供存取權給第三方 AWS 帳戶 擁有](#)。IAM
- 若要了解如何透過身分聯合提供存取權，請參閱 IAM 使用者指南 中的 [為外部驗證的使用者提供存取權（身分聯合）](#)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 IAM 使用者指南 [中的跨帳戶資源存取IAM](#)。

## AWS re : Post Private 的合規驗證

若要了解 是否 AWS 服務 在特定合規計劃的範圍內，請參閱[AWS 服務 依合規計劃](#)然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 [AWS Compliance Programs](#)。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 [下載報告 AWS Artifact](#)。

您在使用 時的合規責任 AWS 服務 取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源以協助合規：

- [安全與合規快速入門指南](#) – 這些部署指南討論架構考量，並提供以 AWS 安全與合規為重點的基準環境部署步驟。
- [Amazon Web Services 上HIPAA安全與合規架構](#) – 本白皮書說明公司如何使用 AWS 來建立HIPAA 符合 資格的應用程式。

### Note

並非所有 AWS 服務 都HIPAA符合資格。如需詳細資訊，請參閱[HIPAA合格服務參考](#)。

- [AWS 合規資源](#) – 此工作手冊和指南集可能適用於您的產業和位置。
- [AWS 客戶合規指南](#) – 透過合規的角度了解共同的責任模型。本指南摘要說明跨多個架構（包括國家標準和技術研究所（）NIST、支付卡產業安全標準委員會（PCI）和國際標準化組織（ISO））保護指南 AWS 服務 並映射至安全控制的最佳實務。
- AWS Config 開發人員指南中的[使用規則評估資源](#) – AWS Config 服務會評估資源組態是否符合內部實務、產業準則和法規。
- [AWS Security Hub](#) – 這 AWS 服務 提供 內安全狀態的全面檢視 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 [Security Hub controls reference](#)。
- [Amazon GuardDuty](#) – 透過監控您的環境是否有可疑和惡意活動，藉此 AWS 服務 偵測 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可以透過滿足某些合規架構強制要求的入侵偵測需求，協助您解決各種合規要求DSS，例如 PCI。
- [AWS Audit Manager](#) – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

## AWS re : Post Private 中的復原能力

AWS 全域基礎設施是以 AWS 區域 和 可用區域建置。AWS 區域 提供多個實體分隔和隔離的可用區域，這些區域與低延遲、高輸送量和高度冗餘聯網連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和 可用區域的詳細資訊，請參閱[AWS 全域基礎設施](#)。

## AWS re : Post Private 中的基礎設施安全

作為受管服務，AWSre : Post Private 受到 [Amazon Web Services : 安全程序概觀](#) 白皮書中所述 AWS 的全球網路安全程序保護。

您可以使用 AWS 已發佈的API呼叫，透過網路存取 re : Post Private。用戶端必須支援 Transport Layer Security ( TLS ) 1.0 或更新版本。我們建議使用 TLS 1.2 或更新版本。用戶端還必須支援具有完美轉送保密性 ( PFS ) 的密碼套件，例如 DHE ( Ephemeral Diffie-Hellman ) 或 ECDHE ( Elliptic Curve Ephemeral Diffie-Hellman )。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，必須使用與 AWS Identity and Access Management 委託人相關聯的存取金鑰 ID 和秘密存取金鑰來簽署請求。或者，您可以使用 [AWS Security Token Service](#) (AWS STS) 以產生暫時安全憑證以簽署請求。

## RE: 張貼私人配額

AWS RE: 私人貼文提供私有回復:貼文，您可以在指定區域的帳戶中使用這些貼文。AWS當您註冊 Re: 私人貼文時，會針對您可以建立的私人回覆:貼文數量和私人 Re: post 的大小設AWS定預設配額 (先前稱為限制)。

## Service Quotas

以下是您帳戶的「重新:私人貼文」的AWS預設配額。您可以使用「[Service Quotas](#)」[主控台](#)來檢視預設配額。這些配額均不可調整。您無法要求提高配額。

資源	預設	說明	可調整
私人回復數：帖子	3	此帳戶目前區域中私人 Re: 貼文的最大數目。	否
免費私人 RE：郵政大小	10	免費私人 RE 的最大大小 (以 GB 為單位)：POST。	否
標準私人 RE：郵政大小	100	標準私有 RE：POST 的最大大小 (以 GB 為單位)。	否

## API 節流限制

下列節流限制適用於 Re: 私人貼文中每個區域的每個帳戶。這些配額無法增加。

動作	代幣補充率	要求率
CreateSpace	1	1
ListSpaces	10	10
GetSpace	10	10

動作	代幣補充率	要求率	
UpdateSpace	10	10	
DeleteSpace	1	1	
RegisterAdmin	10	100	
DeRegisterAdmin	10	100	
SendInvites	1	1	
TagResource	10	10	
UntagResource	10	10	
ListTagsForResource	10	10	

# 建立、設定和自訂您的私有 re : Post

本節說明如何在 re : Post Private 主控台中建立、設定和自訂私有 AWS re : Post。

## 主題

- [建立新的私有 re : Post](#)
- [管理 re : Post Private 中 Support 案例建立和管理的存取權](#)
- [使用 設定和管理使用者存取權 AWS IAM Identity Center](#)
- [自訂您的私有 re : Post](#)
- [邀請使用者到您的私有 re : Post](#)

## 建立新的私有 re : Post

若要建立新的私有 re : Post，請遵循下列步驟：

1. 在 開啟 re : Post Private 主控台 <https://console.aws.amazon.com/repost-private/>。
2. 在主控台的首頁上，選擇建立私有 re : Post。
3. 如果您尚未為帳戶設定 IAM Identity Center，請選擇 Open Identity Center。請遵循 AWS IAM Identity Center 使用者指南 中的 [入門](#) 中的指示。
4. 在建立私有 re : Post 頁面上，針對定價，根據您的使用案例選取免費層或標準層。如果您已為您的帳戶使用 免費方案，則無法使用 免費方案選項。
5. 在詳細資訊 下，執行下列動作：

針對名稱，輸入私有 re : Post 的唯一名稱。

(選用) 針對描述，輸入私有 re : Post 的簡短描述。

針對自訂子網域，輸入子網域的自訂名稱。

6. (選用) 若要自訂資料加密設定，請在資料加密 下，選取自訂加密設定。然後，執行下列任一動作：

針對選擇AWSKMS金鑰，選取 AWS Key Management Service 金鑰或 Amazon Resource Name (ARN)。

-或-

選擇建立AWSKMS金鑰。然後，[建立 AWS KMS 金鑰](#)。

7. (選用) 在支援案例整合的服務存取權下，選取為此 re : Post 啟用服務存取權。

 Note

您也可以在建建立私有 re : Post 之後開啟此選項。

對於 請在下面選取現有IAM角色，或在IAM主控台 中建立新的角色，請使用搜尋列尋找您的現有IAM角色。

-或-

選擇在IAM主控台 中建立新的角色。

如果您選擇建立新角色，請遵循 中的指示[建立 IAM 角色](#)。

如果您選擇使用現有的服務角色，請在搜尋列中輸入您要使用的角色ARN的。從下拉式清單中選擇角色。

如需詳細資訊，請參閱[管理 re : Post Private 中 Support 案例建立和管理的存取權](#)。

8. (選用) 在標籤下，選擇新增標籤。然後輸入下列資訊：

針對金鑰，輸入您的自訂標籤金鑰。

在值 中，輸入您的自訂標籤值。

若要新增更多標籤，請選擇新增新標籤。

9. 選擇建立此 re : Post 。

確認頁面會通知您正在建立私有 re : Post。您可以在狀態欄位中檢視私有 re : Post 的狀態。建立私有 re : Post 時，狀態欄位會顯示建立。

建立私有 re : Post 大約需要 30 分鐘。當您的私有 re : Post 準備就緒時，狀態欄位會顯示線上。您可以使用在設定索引標籤下列出的私有 re : Post AWS產生的子網域來存取私有 re : Post。您可以在檢閱完成後，在設定索引標籤下檢視私有 re : Post 的自訂子網域。

## 管理 re : Post Private 中 Support 案例建立和管理的存取權

您必須建立 AWS Identity and Access Management ( IAM ) 角色，以管理 AWS re : Post Private 對 Support 案例建立和管理的存取權。此角色會為您執行下列 Support 動作：

- [CreateCase](#)
- [AddCommunicationToCase](#)
- [ResolveCase](#)

建立IAM角色之後，請將IAM政策連接至此角色，讓角色具有完成這些動作所需的許可。您可以在 re : Post Private 主控台中建立私有 re : Post 時選擇此角色。

您私有 re : Post 中的使用者具有您授予IAM角色的相同許可。

### Important

如果您變更IAM角色或IAM政策，則您的變更會套用至您設定的私有 re : Post。

請遵循這些程序來建立您的IAM角色和政策。

### 主題

- [使用 AWS 受管政策或建立客戶受管政策](#)
- [範例IAM政策](#)
- [建立 IAM 角色](#)
- [故障診斷](#)

## 使用 AWS 受管政策或建立客戶受管政策

若要授予角色許可，您可以使用 AWS 受管政策或 客戶受管政策。

### Tip

如果您不想手動建立政策，建議您改用 AWS 受管政策，並略過此程序。受管政策會自動擁有所需的許可 Support。您不需要手動更新政策。如需詳細資訊，請參閱[AWS 受管政策：AWSRepostSpaceSupportOperationsPolicy](#)。

請遵循此程序，為您的角色建立客戶管理政策。此程序使用IAM主控台JSON政策編輯器。

為 re : Post Private 建立客戶受管政策

1. 登入 AWS Management Console 並在 開啟IAM主控台<https://console.aws.amazon.com/iam/>。
2. 在導覽窗格中，選擇政策。
3. 選擇 Create policy (建立政策)。
4. 選擇 JSON 索引標籤。
5. 輸入您的 JSON，然後在編輯器JSON中取代預設值。您可以使用[範例政策](#)。
6. 選擇下一步：標籤。
7. (選用) 您可使用標籤作為金鑰值對，將中繼資料新增至政策。
8. 選擇下一步：檢閱。
9. 在檢閱政策頁面上，輸入名稱，例如 *rePostPrivateSupportPolicy* 和 描述 (選用)。
10. 檢閱摘要頁面以查看政策允許的許可，然後選擇建立政策。

此政策定義角色可以採取的動作。如需詳細資訊，請參閱 IAM 使用者指南 中的[建立IAM政策 \(主控台\)](#)。

## 範例IAM政策

您可以將下列範例政策連接至您的IAM角色。此政策允許角色擁有 所有必要動作的完整許可 Support。使用 角色設定私有 re : Post 後，私有 re : Post 中的任何使用者都有相同的許可。

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

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

### Note

如需 re : Post Private 的 AWS 受管政策清單，請參閱 [AWS AWS re : Post Private 的 受管政策](#)。

您可以更新政策以從 移除許可 Support。

如需每個動作的說明，請參閱《服務授權參考》中的下列主題：

- [適用於 AWS Support的動作、資源及條件金鑰](#)
- [Service Quotas 的動作、資源和條件金鑰](#)
- [的動作、資源和條件索引鍵 AWS Identity and Access Management](#)

## 建立 IAM 角色

建立政策後，您必須建立IAM角色，然後將政策連接至該角色。您可以在 re : Post Private 主控台中建立私有 re : Post 時選擇此角色。

建立 Support 案例建立和管理的角色

1. 登入 AWS Management Console 並在 開啟IAM主控台<https://console.aws.amazon.com/iam/>。
2. 在導覽窗格中，選擇 Roles (角色)，然後選擇 Create role (建立角色)。
3. 對於 Trusted entity type (信任的實體類型)，選擇 Custom trust policy (自訂信任政策)。
4. 針對自訂信任政策，輸入下列內容：

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

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

5. 選擇 Next (下一步)。
6. 在許可政策下，在搜尋列中輸入您建立的 AWS 受管政策或客戶受管政策，例如 *rePostPrivateSupportPolicy*。選取您希望服務擁有的許可政策旁邊的核取方塊。
7. 選擇 Next (下一步)。
8. 在名稱、檢閱和建立頁面上，針對角色名稱輸入名稱，例如 *rePostPrivateSupportRole*。
9. (選用) 針對描述，輸入角色的描述。
10. 檢閱信任政策和許可。
11. (選用) 您可使用標籤作為金鑰值對，將中繼資料新增至角色。如需在中使用標籤的詳細資訊IAM，請參閱[標記IAM資源](#)。
12. 選擇建立角色。您現在可以在 re : Post Private 主控台中設定私有 re : Post 時選擇此角色。請參閱 [建立新的私有 re : Post](#)。

如需詳細資訊，請參閱 IAM 使用者指南 中的 [為 AWS 服務建立角色 \(主控台\)](#)。

## 故障診斷

請參閱下列主題以管理 re : Post Private 的存取權。

### 內容

- [我想要從特定動作限制私有 re : Post 中的特定使用者](#)
- [當我設定私有 re : Post 時，看不到我建立IAM的角色](#)
- [我IAM的角色缺少許可](#)
- [錯誤表示我的IAM角色無效](#)

## 我想要從特定動作限制私有 re : Post 中的特定使用者

依預設，您私有 re : Post 中的使用者具有您連接至您建立IAM之角色IAM的政策中指定的相同許可。這表示私有 re : Post 中的任何人都有讀取或寫入存取權，可建立和管理 Support 案例，無論他們是否有 AWS 帳戶 或 IAM使用者。

建議遵循下列最佳實務：

- 使用對 具有最低必要許可IAM的政策 Support。請參閱 [AWS 受管政策：AWSRepostSpaceSupportOperationsPolicy](#)。

## 當我設定私有 re : Post 時，看不到我建立IAM的角色

如果您的IAM角色未出現在 IAM re : Post Private 的角色中；請列出，這表示該角色沒有 re : Post Private 做為信任的實體，或該角色已刪除。您可以更新現有角色，或建立新角色。請參閱 [建立 IAM 角色](#)。

## 我IAM的角色缺少許可

您為私有 re : Post 建立IAM的角色需要許可才能執行您想要的動作。例如，如果您希望私有 re : Post 中的使用者建立支援案例，該角色必須具有 support:CreateCase 許可。re : Post Private 會擔任此角色，為您執行這些動作。

如果您收到 缺少許可的錯誤 Support，請確認連接至角色的政策具有必要的許可。

請參閱之前的 [範例IAM政策](#)。

## 錯誤表示我的IAM角色無效

確認您已為私有 re : Post 組態選擇正確的角色。

## 使用 設定和管理使用者存取權 AWS IAM Identity Center

re : Post Private 與 整合 AWS IAM Identity Center，為組織的人力資源提供身分聯合。使用 IAM Identity Center 建立或連線您組織中的使用者，並集中管理其所有 AWS 帳戶和應用程式的存取權。如需 IAM Identity Center 的詳細資訊，請參閱[什麼是 AWS IAM Identity Center \( 接續到AWS單一登入 \)](#)。如需開始使用 IAM Identity Center 的詳細資訊，請參閱[入門](#)。若要使用 IAM Identity Center，您還必須為 帳戶 AWS Organizations 啟用。

## 自訂您的私有 re : Post

您可以在建立私有 re : Post 之後，將一或多個管理員新增至私有 re : Post。管理員使用 re : Post Private 應用程式啟動私有 re : Post 並管理其中的使用者。他們可以自訂私有 re : Post 的品牌、新增標籤來分類內容，以及為自動內容群體選取感興趣的主題。如需詳細資訊，請參閱 [AWS re : Post Private Administration Guide](#)。

## 邀請使用者到您的私有 re : Post

您可以在建立私有 re : Post 之後，將一或多個使用者新增至私有 re : Post。您可以邀請使用者在私有 re : Post 中進行協作。使用者使用 re : Post Private 應用程式，使用您設定的憑證登入。登入私有 re : Post 後，使用者可以瀏覽或搜尋現有內容，包括為其感興趣的主題範圍量身打造的訓練和技術內容。如需詳細資訊，請參閱 [AWS re : Post Private 使用者指南](#)。

# 在 re : Post Private 主控台中管理您的私有 re : Post

本節說明如何在 re : Post Private 主控台中管理私有 AWS re : Post。

## 主題

- [將使用者新增至您的私有 re : Post](#)
- [將群組新增至私有 re : Post](#)
- [將使用者新增至私有 re : Post 中的群組](#)
- [邀請使用者和群組到您的私有 re : Post](#)
- [將角色指派給私有 re : Post 中的使用者](#)
- [從私有 re : Post 中移除使用者](#)
- [從私有 re : Post 中移除群組](#)
- [從私有 re : Post 新增或移除 AWS 員工](#)
- [從 re : Post Private 刪除私有 re : Post](#)

## 將使用者新增至您的私有 re : Post

如果您是管理員，您可以將使用者新增至私有 re : Post。

1. 在 開啟 re : Post Private 主控台 <https://console.aws.amazon.com/repost-private/>。
2. 在導覽窗格中，選擇全部我的私有 re : Posts 。
3. 選擇您要管理的私有 re : Post。
4. 選擇 Users (使用者) 索引標籤。
5. 在使用者 下，選擇新增使用者和群組 。
6. 從清單中，選取要新增至私有 re : Post 的使用者。然後，選擇指派 。

選取的使用者會新增至您的私有 re : Post，並列在使用者索引標籤下。

您新增的使用者將收到來自私有 re : Post 的入職電子郵件。您的私有 re : Post 每天會檢閱使用者和群組的清單一次，以確保入職電子郵件已傳送給尚未收到的電子郵件。入職電子郵件包含如何登入私有 re : Post 的資訊。

## 將群組新增至私有 re : Post

如果您是管理員，您可以將群組新增至私有 re : Post。

1. 在 開啟 re : Post Private 主控台<https://console.aws.amazon.com/repost-private/>。
2. 在導覽窗格中，選擇所有我的私有 re : Posts 。
3. 選擇您要管理的私有 re : Post。
4. 選擇 Groups (群組) 標籤。
5. 選擇新增使用者和群組 。
6. 從清單中，選取要新增至私有 re : Post 的群組。然後，選擇指派 。

選取的群組會新增至您的私有 re : Post，並列在群組索引標籤下。

您新增的群組將收到來自私有 re : Post 的入職電子郵件。您的私有 re : Post 每天會檢閱使用者和群組的清單一次，以確保入職電子郵件已傳送給尚未收到的電子郵件。入職電子郵件包含如何登入私有 re : Post 的資訊。

## 將使用者新增至私有 re : Post 中的群組

使用 IAM Identity Center 將新使用者新增至私有 re : Post 中的現有群組。如需詳細資訊，請參閱AWSIAM身分中心使用者指南中的[將使用者新增至群組](#)。

## 邀請使用者和群組到您的私有 re : Post

### Note

邀請使用者和群組加入私有 re : Post 是選用的。您新增的使用者和群組將收到來自私有 re : Post 的入職電子郵件。您的私有 re : Post 每天會檢閱使用者和群組的清單一次，以確保入職電子郵件已傳送給尚未收到的電子郵件。

請依照下列步驟，手動將使用者和群組邀請到您的 re : Post in AWS re : Post Private :

1. 在 開啟 re : Post Private 主控台<https://console.aws.amazon.com/repost-private/>。
2. 在導覽窗格中，選擇所有我的私有 re : Posts 。

3. 選擇您要管理的私有 re : Post。
4. 若要邀請使用者加入私有 re : Post，請選擇使用者索引標籤。

從清單中，選取要邀請至私有 re : Post 的使用者。然後，選擇加入使用者以重新：張貼。

5. 在將使用者加入此私有 re : Post 對話方塊中，輸入下列資訊：

針對主旨，輸入您要傳送之電子郵件訊息的主旨。

針對內文，輸入私有 re : Post 的歡迎訊息。

選擇傳送入職電子郵件。

6. 若要邀請群組加入私有 re : Post，請選擇群組索引標籤。

從清單中，選取要邀請至私有 re : Post 的群組。然後，選擇要 re : Post 的加入群組。

7. 在此私有 re : Post 對話方塊中，輸入下列資訊：

針對主旨，輸入您要傳送之電子郵件訊息的主旨。

針對內文，輸入私有 re : Post 的歡迎訊息。

選擇傳送入職電子郵件。

歡迎訊息會傳送給所有選取的使用者和群組，其中包含如何登入私有 re : Post 的資訊。

## 將角色指派給私有 re : Post 中的使用者

您可以指派私有 re : Post 使用者下列其中一個許可：

- 管理員：具有修改私有 re : Post 組態許可的使用者
- 專家：具有許可可檢閱和驗證社群所提供答案的使用者
- 主持人：可以回應主持佇列中請求的使用者
- 支援請求者：可從其張貼 Support 的問題建立票證的使用者

若要將角色指派給私有 re : Post 使用者，請遵循下列步驟：

1. 在開啟 re : Post Private 主控台 <https://console.aws.amazon.com/repost-private/>。
2. 在導覽窗格中，選擇所有我的私有 re : Posts。

3. 選擇您要管理的私有 re : Post。
4. 選擇 Users (使用者) 索引標籤。
5. 選取您要為其指派角色的一或多個使用者。
6. 選擇 編輯角色 ，然後選擇您要指派給所選使用者的角色。

所選使用者會獲指派您選擇的角色。在使用者索引標籤下，這些使用者的角色會更新為您選擇的角色。

## 從私有 re : Post 中移除使用者

如果您是管理員，則可以從私有 re : Post 中移除使用者。

1. 在 開啟 re : Post Private 主控台 <https://console.aws.amazon.com/repost-private/>。
2. 在導覽窗格中，選擇所有我的私有 re : Posts 。
3. 選擇您要管理的私有 re : Post。
4. 在使用者 下，從清單中選擇您要從私有 re : Post 中移除的使用者。然後，選擇 移除 。

選取的使用者會從私有 re : Post 中移除。移除的使用者的相關資訊不再出現在使用者索引標籤下。

## 從私有 re : Post 中移除群組

如果您是管理員，則可以從私有 re : Post 中移除群組。

1. 在 開啟 re : Post Private 主控台 <https://console.aws.amazon.com/repost-private/>。
2. 在導覽窗格中，選擇所有我的私有 re : Posts 。
3. 選擇您要管理的私有 re : Post。
4. 選擇 Groups (群組) 標籤。
5. 從清單中，選取要從私有 re : Post 中移除的群組。然後，選擇 移除 。

選取的群組會從私有 re : Post 中移除。移除的群組的相關資訊不再出現在群組索引標籤下。

## 從私有 re : Post 新增或移除 AWS 員工

如果您有 Enterprise 或 Enterprise On-Ramp Support Plan，則可以從私有 re : Post 新增或移除 AWS 員工。如需詳細資訊，請聯絡禮賓服務支援或您的技術客戶經理 ( TAM )。

## 從 re : Post Private 刪除私有 re : Post

若要刪除 re : Post Private 中的 AWS re : Post，請遵循下列步驟：

1. 在開啟 re : Post Private 主控台 <https://console.aws.amazon.com/repost-private/>。
2. 在導覽窗格中，選擇所有我的私有 re : Posts。
3. 選擇您要管理的私有 re : Post，然後選擇刪除。
4. 選取所有選項以確認並確認您想要永久刪除私有 re : Post 和與其相關聯的資料。

### Important

當您刪除私有 re : Post 時，所有與私有 re : Post 相關的組態資訊都會遭到刪除。刪除私有 re : Post 後，您無法從中還原任何內容。

5. 在提示取得其他書面同意時，輸入私有 re : Post 的名稱。再選擇 Delete (刪除)。

刪除私有 re : Post 大約需要 30 分鐘。

## 監控 AWS RE：私人貼文

監控是維護 AWS RE: Private 和其AWS他解決方案的可靠性、可用性和效能的重要組成部分。AWS提供下列監控工具來監視 Re: Post Private、在發生錯誤時報告，並在適當時採取自動動作：

- Amazon 會即時 CloudWatch監控您的AWS資源和執行AWS的應用程式。您可以收集和追蹤指標、建立自訂儀表板，以及設定警示，在特定指標達到您指定的閾值時通知您或採取動作。例如，您可以 CloudWatch 追蹤 Amazon EC2 執行個體的 CPU 使用率或其他指標，並在需要時自動啟動新執行個體。如需詳細資訊，請參閱 [Amazon CloudWatch 使用者指南](#)。
- AWS CloudTrail擷取由您或為您發出的 API 呼叫和相關事件，AWS 帳戶並將日誌檔傳遞到您指定的 Amazon S3 儲存貯體。您可以找出哪些使用者和帳戶呼叫 AWS、發出呼叫的來源 IP 地址，以及呼叫的發生時間。如需詳細資訊，請參閱 [AWS CloudTrail 使用者指南](#)。

## 監控 AWS RE：在亞馬遜私有發布 CloudWatch

您可以使用 Amazon 監控 AWS RE: Post Private CloudWatch，這會收集原始資料並將其處理為可讀且接近即時的指標。這些統計數據保留 15 個月，以便您可以訪問歷史信息，並更好地了解 Web 應用程序或服務的性能。您也可以設定留意特定閾值的警示，當滿足這些閾值時傳送通知或採取動作。如需詳細資訊，請參閱 [Amazon CloudWatch 使用者指南](#)。

RE: 私人貼文服務會在命名空間中報告下列量度AWS/rePostPrivate。

指標	說明
NumberOfSpaces	當前帳戶中的私人回復：帖子的數量。 單位：計數
NumberOfUsers	私人 Re: POST 中的使用者數目。此量度使用 SpaceID 作為維度。 單位：計數
ContentSize	私人 Re : POST 中的內容量。此量度使用 SpaceID 作為維度。 單位：位元組

「重新:私人貼文」量度支援下列維度。

維度	說明
spaceId	私人 RE: POST 的唯一識別碼。

## 記錄 AWS RE: 使用發佈私有 API 呼叫 AWS CloudTrail

AWS RE：私有貼文與服務整合在一起AWS CloudTrail，該服務可提供使用者、角色或服務在 RE: 私有貼文中所採取的動作記錄。CloudTrail 擷取 Re: 以私有方式張貼為事件的所有 API 呼叫。擷取的呼叫包括來自 Re: POST 私人主控台的呼叫，以及對 Re: POST 私有 API 作業的程式碼呼叫。如果您建立追蹤，您可以啟用持續傳遞 CloudTrail 事件至 Amazon S3 儲存貯體，包括 Re: Post Private 的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷對 Re: Post Private 提出的要求、提出要求的 IP 位址、提出要求的人員、提出要求的時間以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使[AWS CloudTrail 用者指南](#)。

### Re: 張貼私人資訊 CloudTrail

CloudTrail 在您創建帳戶AWS 帳戶時啟用。當活動在 Re: Post Private 中發生時，該活動會與事件歷史記錄中的其他AWS服務 CloudTrail 事件一起記錄在事件中。您可以檢視、搜尋和下載 AWS 帳戶 的最新事件。如需詳細資訊，請參閱[使用 CloudTrail 事件歷程記錄](#)。

如需您的事件的持續記錄AWS 帳戶，包括 Re: Post Private 的事件，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他AWS服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- [建立 AWS 帳戶的追蹤](#)
- [CloudTrail 支援的服務與整合](#)
- [設定 Amazon SNS 通知 CloudTrail](#)
- [從多個區域接收 CloudTrail 日誌文件和從多個帳戶接收 CloudTrail 日誌文件](#)

所有 RE: 私有貼文動作都會記錄 CloudTrail 並記錄在 [AWS RE: POST 私有 API 參考](#)中。Re: Post Private 支援將下列動作記錄為記錄檔中的事件：CloudTrail

- [CreateSpace](#)

- [DeleteSpace](#)
- [DeregisterAdmin](#)
- [GetSpace](#)
- [ListSpaces](#)
- [ListTagsForResource](#)
- [RegisterAdmin](#)
- [SendInvites](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateSpace](#)

RE: 私人貼文支援將下列Support動作記錄為記錄 CloudTrail 檔中的事件：

- [CreateCase](#)
- [AddCommunicationToCase](#)
- [ResolveCase](#)

每一筆事件或日誌項目都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

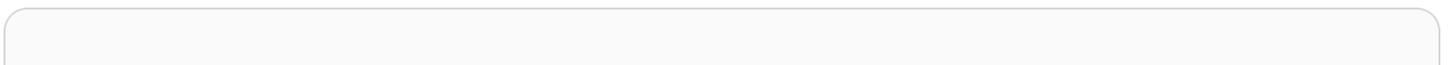
- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務提出。

如需詳細資訊，請參閱 [CloudTrail userIdentity 元素](#)。

## 瞭解 RE: 張貼私人記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範CreateSpace動作的 CloudTrail 記錄項目。



```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ARO AQM47QIR7WLEXAMPLE:user",
    "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
    "accountId": "123456789012",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ARO AQM47QIR7WLEXAMPLE",
        "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"
}
```

下列範例顯示示範RegisterAdmin動作的 CloudTrail 記錄項目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ARO AQM47QIR7WLEXAMPLE:user",
    "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
    "accountId": "123456789012",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ARO AQM47QIR7WLEXAMPLE",
        "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-y1QEmAXpmEXAMPLE"
  },
  "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"
}

```

下列範例顯示示範ListSpaces動作的 CloudTrail 記錄項目。

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ARO AQM47QIR7WLEXAMPLE:user",
    "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
    "accountId": "123456789012",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "ARO AQM47QIR7WLEXAMPLE",
        "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"
}

```

下列範例顯示示範ResolveCase動作的 CloudTrail 記錄項目。您可以使用此記錄項目中的sourceIdentity元素來識別解決案例的使用者。

```

{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "ARO AQM47QIR76DQZ7N5WX: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": "ARO AQM47QIR76DQZ7N5WX",
        "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"
}
}
```

# 疑難排解 RE: 私人貼文

下列資訊可協助您疑難排解 AWS RE: 私有貼文的問題。

## 主題

- [無法在特定地區設定我的私人 Re: POST AWS](#)
- [無法設定私人 Re: 在我的帳戶中張貼](#)
- [無法管理私人 RE 中的使用者或群組:POST](#)

## 無法在特定地區設定我的私人 Re: POST AWS

Re: Private Post Private 僅在美國東部 (維吉尼亞北部)、美國西部 (奧勒岡)、歐洲 (法蘭克福)、亞太區域 (新加坡)、亞太區域 (雪梨)、加拿大 (中部) 和歐洲 (愛爾蘭) 區域提供。請確定您正在以下其中一個區域建立您的私人 Re: Post。

## 無法設定私人 Re: 在我的帳戶中張貼

請確定您的帳戶已啟 AWS IAM Identity Center 用，並在您要建立私有 Re: post 的相同區域中設定 IAM 身分中心。如需詳細資訊，請參閱 [必要條件](#)。

## 無法管理私人 RE 中的使用者或群組:POST

請確定您擁有編輯私人 RE: 張貼和管理私人 Re: post 中的使用者和群組所需的權限。如需更多詳細資訊，請參閱 [AWS re : Post 私有身分型政策範例](#)。

# 文件歷史記錄

下表說明 AWS re : Post Private 的文件版本：

變更	描述	日期
<a href="#">指引結構檢閱和改善</a>	已檢閱指南的結構並進行改進，以改善與尋找特定案例資訊相關的客戶體驗。	2024 年 9 月 24 日
<a href="#">更新</a>	已將美國東部（維吉尼亞北部）、亞太區域（雪梨）、加拿大（中部）和歐洲（愛爾蘭）新增至支援的區域	2024 年 5 月 10 日
<a href="#">更新</a>	已將亞太區域（新加坡）新增至支援的區域	2024 年 3 月 6 日
<a href="#">新資源</a>	新增 <a href="#">AWS AWS re : Post Private 受管政策</a> 的文件	2023 年 11 月 26 日
<a href="#">初始版本</a>	re : Post Private Console 管理指南的初始版本	2023 年 11 月 26 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。