主控台管理指南

AWS re:Post Private

AWS re:Post Private: 主控台管理指南

Table of Contents

什麼是 AWS RE：私人貼文？

AWS RE: 私人貼文是 AWS RE: POST 的私有版本，適用於擁有企業 Support 或企業上線支 Support 計劃的企業。它提供知識和專家的存取權限，以加速雲端採用並提高開發人員生產力。使用組織特定的私有 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存取權。此外，Re: Post Private 可集中受信任的AWS技術內容，並提供私人討論區，以改善團隊在內部和 AWS 的協作方式，以消除技術障礙、加速創新，並在雲端更有效率地擴展規模。

如需詳細資訊，請參閱 AWS RE：私人貼文。

訪問 RE: 私人發布

管理員使用 AWS RE: POST 私有主控台來建立其組織特定的私有 RE: POST。當管理員建立私人 RE: POST 時，他們可以將其專用 Re: POST 命名，並在下定義子網域。`*.private.repost.aws`組織的私人 RE: POST 的管理員可以使用下列其中一個身分識別來源來設定使用AWS IAM Identity Center者存取權限，以進行驗證：身分識別中心目錄、Active Directory 或外部身分識別提供者。設定使用者之後，主控台管理員可以將 Re: Post Private 管理員角色指派給一或多個使用者。Re: Private 管理員可以根據組織品牌和知識需求，自訂其私人 RE: POST 應用程式。熟悉組織架構和工作負載的客AWS戶團隊成員 (例如技術客戶經理) 會自動新增至組織的私人 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、新增標籤以將內容分類，以及為開發人員選取感興趣的主題，以自動填入訓練和技術內容。他們也可以邀請使用者加入他們的私人 Re: POST，以增加協同作業。如需詳細資訊，請參閱 AWS RE：私有管理後指南。

非系統管理使用者會使用 RE: Private 應用程式，使用其管理員設定的認證來登入。登入私人 Re: Post 後，使用者可以瀏覽或搜尋現有內容，包括量身打造的訓練和技術內容，這些內容範圍是根據他們感興趣的主題而定。使用者也可以直接從他們的私人 RE: POST 搜尋AWS公開技術內容，並建立內部討論AWS公開內容的私人討論串。使用者可以透過提出問題、提供回應或發表文章，協同解AWS決技術問題，並從私人 RE: Post 的其他使用者取得技術指引。使用者也可以將討論串轉換成AWS Support案例。使用者可以選擇將來自的回覆新增AWS Support至私人 Re: POST。如需詳細資訊，請參閱 AWS RE：發佈私人使用者指南。

定價

只有擁有企業 Support (ES) 和企業登入 (EOP) Support 計劃的客戶可以訂閱 RE: 私人貼文服務。您可以從兩個可用的定價層中進行選擇：免費方案和標準層。免費方案可讓您在六個月內全面探索和試用標

準方案功能，然後才能順暢地轉換為付費方案。如果您使用標準層，則可以支付每個使用者的每月訂閱費用，以使用 Re: Post Private。如需詳細資訊，請參閱 定價。

如何開始

若要開始使用 Re: 私人貼文，請參閱。先決條件

先決條件

您必須符合下列先決條件，才能在 AWS RE: post 中建立新的私人 RE: POST 或管理現有的私有 Re: post 私人貼文：

- 您必須註冊企業或企業登入支 Support 計劃。
- 您必須AWS IAM Identity Center在您要設定私人 Re: POST 的相同地區啟用。
- 您必須建立具有必要權限的AWS Identity and Access Management角色，才能為您建立、管理和解決AWS Support案例。RE: 私人貼文服務會使用此角色來對其進行 API 呼叫。AWS Support如需詳細資訊，請參閱 在 Re: 私人貼文中管理 AWS Support 案例建立和管理的存取。

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 中的安全性：私人貼文

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同承擔的責任。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：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。若要瞭解適用於 AWS Re: Private 的合規方案，請參閱規範計劃AWS 服務範圍內的計劃)。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用 RE: Post Private 時套用共同的責任模型。下列主題說明如何設定「重新:私人貼文」，以符合您的安全性與合規性目標。您也會學到如何使用其他可協助您監控和保護 RE: Post Private 資源的 AWS 服務。

主題

- Re 中的資料保護AWS:私人貼文
- 如何回復：發布私人工作 IAM
- AWSRe: 私人貼文的符合性驗證
- RE 中的韌性AWS：私人後
- RE 中的基礎結構安全性AWS：私人貼文

Re 中的資料保護AWS:私人貼文

AWS 共用責任模型適用於 AWS Re: Private 中的資料保護。如此模型中所述， AWS 負責保護執行所有 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。如需有關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 安全性GDPR部落格上的AWS 共同責任模型和部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 認證並設定個別使用者。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 資源溝通。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 使用設定API和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 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 AWS 透過命令列介面或存取時需要 FIPS 140-3 驗證的密碼編譯模組API，請使用端點。FIPS 如需有關可用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。這包括當您使用主控台、、API或 AWS 服務 使用 Re: 私人貼文或其他工作時。AWS CLI 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。如果您提供URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

使用加密來保護資料

靜態加密

RE：私有貼文使用 Amazon 簡單儲存服務儲存貯體、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進行靜態加密的 Amazon OpenSearch 服務網域。

傳輸中加密

RE：Post Private 使用該HTTPS協議與您的客戶端應用程序進行通信。它使用HTTPS和 AWS 簽名代表您的應用程序與其他服務進行通信。

金鑰管理

RE：郵政私有集成 AWS Key Management Service 並支持 AWS KMS 密鑰。您可以在建立私人 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。

如何回复：發布私人工作 IAM

在您用IAM來管理「AWS重新:私人貼文」的存取權之前，您必須瞭解哪些IAM功能可用於「重新:私人貼文」。若要取得 Re: Private 和其他 AWS 服務如何使用的高階檢視IAM，請參閱IAM使用者指南IAM中的使用AWS 服務。

RE: 張貼以私人身分識別為基礎的原則

使用以IAM身分為基礎的原則，您可以指定允許或拒絕的動作。Re: 私人貼文支援特定動作。若要瞭解您在JSON策略中使用的元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

動作

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。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策略`Action`元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯 AWS API操作具有相同的名稱。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。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: 私人貼文中的原則動作會在動作之前使用下列前置詞:。`repostspace:`例如，若要授與某人執行 Re: Private (私人貼文) 作業的權限，您可以將`repostspace:CreateSpace`動`CreateSpace`API作包含在他們的原則中。原則陳述式必須包含`Action`或`NotAction`元素。Re: Post Private 會定義它自己的一組動作，用來描述您可以使用此服務執行的工作。

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「重新:張貼私人」動作的清單，請參閱「使用者指南」中的「Re: 私人貼文」所定義的動作。IAM

資源

管理員可以使用 AWS JSON策略來指定誰可以存取什麼內容。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。

ResourceJSON原則元素會指定要套用動作的一或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (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 不提供任何特定於服務的條件密鑰，但它支持使用全局條件密鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《使用指南》中的AWS 全域條件內IAM容索引鍵。

範例

若要檢視 Re: 張貼以私人身分識別為基礎的原則的範例，請參閱。AWSRE: 張貼以私人身分識別為基礎的政策範例

RE: 張貼以私有資源為基礎的政策

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括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。主參與者可以包括帳戶、使用者、角色、同盟使用者或 AWS 服務。資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的策略IAM中使用 AWS 受管政策。

RE: 私人貼文不支援以資源為基礎的政策。

以標籤為基礎的授權

RE：私人郵政支持標記資源或基於標籤控制訪問。如需詳細資訊，請參閱使用標籤控制AWS資源的存取。

RE: 張貼私人角色 IAM

IAM角色是您 AWS 帳戶中具有特定權限的實體。

使用臨時登入資料搭配 Re: 私人貼文

我們強烈建議您使用臨時登入資料來登入同盟、擔任IAM角色或擔任跨帳戶角色。您可以透過呼叫AssumeRole或之類的 AWS STS API作業來取得臨時安全登入資料GetFederationToken。

RE：發布私有支持使用臨時憑據。

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，以便為您完成動作。服務連結角色會顯示在您的IAM帳戶中，且屬於服務所有。IAM管理員可以檢視但無法編輯服務連結角色的權限。

服務角色

此功能可讓服務為您擔任服務角色。此角色可讓服務存取其他服務中的資源，以便為您完成動作。如需詳細資訊，請參閱建立角色以將權限委派給AWS服務。服務角色會顯示在您的IAM帳戶中，且屬於帳戶所有。這表示IAM系統管理員可以變更此角色的權限。不過，這樣可能會破壞此服務的功能。

針對 Re: 私人貼文使用服務連結角色

AWSRE: 發佈私人使用 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: 私人貼文的唯一IAM角色類型。服務連結角色由 Re: Post Private 預先定義，並包含服務代表您呼叫其他 AWS 服務所需的所有權限。

服務連結角色可讓設定「RE: Private」變得更容易，因為您不需要手動新增必要的權限。Re: Private會定義其服務連結角色的權限，除非另有定義，否則只有 Re: Post Private 可以擔任其角色。定義的權限包括信任原則和權限原則，而且該權限原則無法附加至任何其他IAM實體。

如需支援服務連結角色之其他服務的相關資訊，請參閱使用的AWS 服務，IAM並在服務連結角色欄中尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

Re: 私人貼文的服務連結角色權限

Re: 私人貼文會使用名為的服務連結角色AWSServiceRoleForrePostPrivate。Re: Post Private 會使用此服務連結角色將資料發佈至。 CloudWatch

服 AWSServiceRoleForrePostPrivate 務連結角色會信任下列服務擔任該角色：

- `repostspace.amazonaws.com`

名為的角色權限原則AWSrePostPrivateCloudWatchAccess允許 Re: Private Post 在指定資源上完成下列動作：

- 處理行動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使用指南中的服務連結角色權限。

如需詳細資訊，請參閱AWSrePostPrivateCloudWatchAccess。

建立 Re: 私人貼文的服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、或「Re: 私人貼文」中建立第一個私人 Re: Post 時 AWS API，會為您建立服務連結角色。 AWS CLI

> **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「重新:私人貼文」服務，則該服務開始支援服務連結角色時，「重新:私人貼文」會在您的帳戶中建立角色。AWSServiceRoleForrePostPrivate要了解更多信息，請參閱我的一個新角色出現 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。當您建立第一個私人 Re: POST 時，「重新:私人貼文」會再次為您建立服務連結角色。

在 AWS CLI 或中 AWS API，使用repostspace.amazonaws.com服務名稱建立服務連結角色。如需詳細資訊，請參閱IAM使用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: 私人貼文的服務連結角色

RE: 私人貼文不允許您編輯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。但是，您可以使用編輯角色的描述IAM。如需詳細資訊，請參閱IAM使用指南中的編輯服務連結角色。

刪除 Re: 私人貼文的服務連結角色

您不需要手動刪除 AWSServiceRoleForrePostPrivate 角色。當您刪除 AWS Management Console、或「Re: 私人貼文」中的私人 Re: post 時 AWS API，會為您刪除服務連結的角色。 AWS CLI

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

若要使用手動刪除服務連結角色 IAM

使用IAM主控台 AWS CLI、或刪除 AWSServiceRoleForrePostPrivate 服務連結角色。 AWS API如需詳細資訊，請參閱IAM使用指南中的刪除服務連結角色。

RE 支援的區域:貼上私人服務連結角色

RE: 私有貼文支援在提供服務的 AWS 區域中使用服務連結角色。

區域名稱	區域身分	在 RE Support：私人郵政
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	在 RE Support：私人郵政
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

AWSRE: 張貼以私人身分識別為基礎的政策範例

> **Note**
>
> 為了提高安全性，請盡可能建立同盟使用IAM者而非使用者。

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 資源的權限。他們也無法使用 AWS Management Console AWS CLI、或執行工作 AWS API。IAM管理員必須建立IAM政策，授與使用者和角色權限，才能對他們所需的指定資源執行特定API作業。然後，系統管理員必須將這些原則附加到需要這些權限的IAM使用者或群組。

若要瞭解如何使用這些範例原則文件建立以IAM身分識別為基礎的JSON策略，請參閱使用指南中的IAM建立IAM策略。

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

以身分識別為基礎的政策會決定某人是否可以在您的帳戶中建立、存取或刪除 RE: 張貼私人資源。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 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您的使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需詳細資訊，請參閱AWS 《IAM使用指南》中針對工作職能的AWS 受管理策略或受管理的策略。
- 套用最低權限權限 — 當您使用原則設定權限時，IAM只授與執行工作所需的權限。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。如需有關使用套用權限IAM的詳細資訊，請參閱《使用指南》IAM中的IAM《策略與權限》。
- 使用IAM策略中的條件進一步限制存取 — 您可以在策略中新增條件，以限制對動作和資源的存取。例如，您可以撰寫政策條件，以指定必須使用傳送所有要求SSL。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱《IAM使用指南》中的IAMJSON策略元素：條件。
- 使用 IAM Access Analyzer 驗證您的原IAM則，以確保安全和功能性的權限 — IAM Access Analyzer會驗證新的和現有的原則，以便原則遵循IAM原則語言 (JSON) 和IAM最佳做法。IAMAccess Analyzer 提供超過 100 項原則檢查和可採取動作的建議，協助您撰寫安全且功能正常的原則。如需詳細資訊，請參閱IAM使IAM用指南中的存取分析器原則驗證。
- 需要多因素驗證 (MFA) — 如果您的案例需要使IAM用者或 root 使用者 AWS 帳戶，請開啟以取得額外MFA的安全性。若要在呼叫API作業MFA時需要，請在原則中新增MFA條件。如需詳細資訊，請參閱《IAM使用指南》中的 < 設定MFA受保護的API存取 > 。

如需有關中最佳作法的詳細資訊IAM，請參閱《IAM使用指南》IAM中的「安全性最佳作法」。

允許使用者檢視他們自己的許可

此範例顯示如何建立原則，讓使IAM用者檢視附加至其使用者身分識別的內嵌和受管理原則。此原則包含在主控台上或以程式設計方式使用或完成此動作的 AWS CLI 權限 AWS API。

```
{
```

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

內嵌政策

內嵌原則是您建立和管理的原則。您可以將內嵌政策直接內嵌到使用者、群組或角色中。下列原則範例顯示如何指派執行「AWSRE: 私人貼文」動作的權限。如需有關內嵌原則的一般資訊，請參閱AWSIAM使用指南中的管理IAM原則。您可以使用 AWS Management Console、 AWS Command Line Interface (AWSCLI) 或建立和內嵌內嵌政策。 AWS Identity and Access Management API

主題

- Re 的唯讀存取權限：私人張貼
- 對 Re 的完全訪問權限：私人發布

Re 的唯讀存取權限：私人張貼

下列原則會授與使用者IAM身分識別中心和 RE: POST 專用主控台的讀取存取權。此原則可讓使用者執行為唯讀的「重新:私人貼文」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": "*"
        }
    ]
}
```

對 Re 的完全訪問權限：私人發布

下列原則會授與使用者IAM身分識別中心和 RE: POST 專用主控台的完整存取權。此原則可讓使用者執行所有「重新:私人貼文」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 AWSRe: 私人貼文的受管理策略

使用 AWS 受管理的原則可讓新增使用者、群組和角色的權限，比自己撰寫政策更容易。建立IAM客戶管理的政策需要時間和專業知識，以便為您的團隊提供他們所需的權限。使用 AWS 受管理的原則快速開始使用。這些政策涵蓋常見使用案例，並可在您的 AWS 帳戶中使用。如需有關 AWS 受管理策略的詳細資訊，請參閱IAM使用指南中的AWS 受管理策略。

AWS 服務會維護和更新 AWS 受管理的策略。您無法變更 AWS 受管理原則中的權限。服務有時可能會將其他權限新增至 AWS 受管理的策略，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)。當新功能啟動或新作業可用時，服務最有可能更新 AWS 受管理的策略。服務不會從 AWS 受管理的政策移除權限，因此政策更新不會破壞您現有的權限。

此外，還 AWS 支援跨多個服務之工作職能的受管理原則。例如，`ReadOnlyAccess` AWS 受管理的策略提供對所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時，會為新作業和資源新 AWS 增唯讀權限。如需詳細資訊，請參閱IAM使用指南中的AWS 受管理策略。

主題

- AWS 受管理的策略： AWSRepostSpaceSupportOperationsPolicy
- AWS 受管理的策略： AWSrePostPrivateCloudWatchAccess
- AWSRE：將私人更新張貼到受管理的策略 AWS

AWS 受管理的策略： AWSRepostSpaceSupportOperationsPolicy

此原則可讓「AWS重新:私人貼文」服務建立、管理及解決透過「重新:私人貼文」Web 應用程式建立的 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 受管理的策略： AWSrePostPrivateCloudWatchAccess

此原則允許「重新:私人貼文」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"
     ]
    }
   }
  }
 ]
}
```

AWSRE：將私人更新張貼到受管理的策略 AWS

檢視有關 Re: 私人貼文之 AWS 受管理政策更新的詳細資訊，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動警示，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: 私人貼上受管理的策略的重要更新。

變更	描述	日期
新政策-AWSrePostPrivateCloudWatchAccess	用於將資料發佈至的新受管理政策 CloudWatch	2023 年 11 月 26 日
新政策-AWSRepostSpaceSupportOperationsPolicy	AWSRe: 私人貼文中 Sup AWS port 功能的新受管政策	2023 年 11 月 26 日
RE: 發佈私人開始追蹤變更	Re: 私人貼文開始追蹤其受管理政策的 AWS 變更	2023 年 11 月 26 日

疑難排解 AWS RE：張貼私人身分和存取

使用下列資訊可協助您診斷並修正使用 Re: Post Private 和時可能會遇到的常見問題。IAM

主題

- 我沒有授權在 Re：私人貼文中執行動作
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪問我 AWS 帳戶 的 RE：POST 私有資源

我沒有授權在 Re：私人貼文中執行動作

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。

當使用mateojacksonIAM者嘗試使用主控台來檢視虛構*my-example-widget*資源的詳細資料，但沒有虛構的repostPrivate:*GetWidget*權限時，就會發生下列範例錯誤。

```
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 系統管理員。您的管理員提供您的簽署憑證。

我沒有授權執行 iam：PassRole

如果您收到未獲授權執行`iam:PassRole`動作的錯誤訊息，則必須更新您的原則，以允許您將角色傳遞給「Re: Private」。

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。

當名為的使用IAM者`marymajor`嘗試使用主控台執行 Re: Post Private 中的動作時，就會發生下列範例錯誤。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 系統管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪問我 AWS 帳戶 的 RE：POST 私有資源

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。對於支援以資源為基礎的政策或存取控制清單 (ACLs) 的服務，您可以使用這些政策授與人員存取您資源的權限。

如需進一步了解，請參閱以下內容：

- 若要瞭解「重新:私密貼文」是否支援這些功能，請參閱。如何回復：發布私人工作 IAM
- 若要瞭解如何提供您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM使用者指南》中 AWS 帳戶 的〈提供存取權給其他IAM使用者〉。
- 若要瞭解如何將資源存取權提供給第三方 AWS 帳戶，請參閱《IAM使用指南》中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要瞭解如何透過身分聯盟提供存取權，請參閱使用指南中的提供對外部驗證使用IAM者的存取權 (身分聯合)。
- 若要瞭解針對跨帳號存取使用角色與以資源為基礎的政策之間的差異，請參閱《使用IAM者指南》IAM中的〈跨帳號資源存取〉。

AWSRe: 私人貼文的符合性驗證

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、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遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上進行HIPAA安全與合規架構 — 本白皮書說明公司如何使用建立符合資格的應 AWS 用程HIPAA式。

> **Note**
>
> 並非所有 AWS 服務 人都HIPAA符合資格。如需詳細資訊，請參閱合HIPAA格服務參考。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準 AWS 服務 與技術研究所 (NIST)、支付卡產業安全標準委員會 () 和國際標準化組織 ()PCI) 中保護安全控制指引的最佳做法，並將其對應至安全性控制。ISO
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 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 — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求 PCIDSS，例如符合特定合規性架構所要求的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，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。

RE 中的韌性AWS：私人後

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。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 全域基礎結構。

RE 中的基礎結構安全性AWS：私人貼文

AWSRe: Private 是受管理的服務，受到 Amazon Web Services：安 AWS 全程序概觀白皮書中所述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「重新:私人貼文」。用戶端必須支援「傳輸層安全性」(TLS) 1.0 或更新版本。我們建議使用 TLS 1.2 或更高版本。客戶還必須支持具有完美前向保密（ ）的密碼套件，例如（短暫的迪菲-赫爾曼PFS）或DHE（橢圓曲線短暫迪菲-赫爾曼）。ECDHE現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 AWS Identity and Access Management 主體相關聯的秘密存取金鑰來簽署。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复: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
私人回复數：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、設定和自訂您的私人 Re: POST

主題

建立新的私人 Re: 貼文

若要建立新的私人 Re: POST，請依照下列步驟執行：

1. 請在 https://console.aws.amazon.com/repost-private/ 開啟「重新發佈私人張貼」主控台。
2. 在主控台首頁上，選擇 [建立私人 Re: 貼文]。
3. 如果您的帳戶尚未設定 IAM 身分中心，請選擇 [開啟身分中心]。按照 AWS IAM 身分中心使用者指南中的入門指示進行操作。
4. 在「建立私人電子郵件：貼文」頁面上，針對「定價」，根據您的使用案例選取免費方案或標準層。如果您的帳戶已使用免費方案，則無法使用免費方案選項。
5. 在詳細資料下，執行下列操作：

   在「名稱」中，輸入私人 Re: post 的唯一名稱。

   (選擇性) 在說明中，輸入私人 Re: post 的簡短說明。

   在「自訂」子網域中，輸入子網域的自訂名稱。
6. (選擇性) 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，執行下列其中一個動作：

   對於選擇 AWS KMS 金鑰，請選取金 AWS Key Management Service 鑰或 Amazon 資源名稱 (ARN)。

   -或-

   選擇建立 AWS KMS 金鑰。然後，創建 AWS KMS 密鑰。

7. (選擇性) 在 Sup port 案例整合的服務存取權下，選取啟用此 RE: POST 的服務存取。

> **Note**
>
> 您也可以在建立私人 Re: POST 之後開啟此選項。

請在下方選取現有的 IAM 角色，或在 IAM 主控台中建立新角色，請使用搜尋列尋找現有的 IAM 角色。

-或-

選擇在 IAM 主控台中建立新角色。

如果您選擇新建角色，那么請按照中的說明進行操作建立 IAM 角色。

如果您選擇使用現有的服務角色，請在搜尋列中輸入要使用之角色的 ARN。從下拉式清單中選擇角色。

如需詳細資訊，請參閱 在 Re: 私人貼文中管理 AWS Support 案例建立和管理的存取。

8. (選擇性) 在「標籤」下，選擇「新增標籤」。然後輸入以下信息：

在 Key 中，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 [新增標籤]。

9. 選擇「建立此 Re: 過帳」。

確認頁面會讓您知道您的私人 Re: POST 正在建立中。您可以在「狀態」欄位中檢視「私人 Re: 張貼」的狀態。當您的私人 Re: POST 建立時，「狀態」欄位會顯示「建立」。

建立私人 Re: POST 大約需要 30 分鐘。當您的私人 Re: POST 準備就緒時，「狀態」欄位會顯示「線上」。您可以將 AWS 產生的子網域用於「設定」索引標籤下所列的私有 RE: POST，存取您的私有 RE: POST。審核完成後，您可以在「設定」標籤下檢視您私人 Re: Post 的「自訂」子網域。

在 Re: 私人貼文中管理 AWS Support 案例建立和管理的存取

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

- CreateCase
- AddCommunicationToCase
- ResolveCase

建立 IAM 角色後，將 IAM 政策附加到此角色，以便該角色具有完成這些動作所需的許可。當您在 Re: POST 私人主控台中建立私人 Re: post 時，您可以選擇此角色。

私人 RE: POST 中的使用者擁有與您授予 IAM 角色相同的許可。

> **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。

請依照這些程序建立 IAM 角色和政策。

主題

使用受 AWS 管政策或建立客戶管理的政策

若要授與您的角色權限，您可以使用 AWS 受管政策或客戶管理的政策。

> **Tip**
>
> 如果您不想手動建立原則，建議您改用 AWS 受管理的原則，並略過此程序。受管理的策略會自動擁有的必要權限 AWS Support。您不需要手動更新政策。如需詳細資訊，請參閱 AWS 受管理的策略： AWSRepostSpaceSupportOperationsPolicy。

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

若要針對「重新:私人貼文」建立客戶管理的政策

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 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. 請選擇 JSON 標籤。
5. 輸入您的 JSON，然後在編輯器中取代預設 JSON。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 Review policy (檢閱政策) 頁面，輸入 Name (名稱) (例如 *rePostPrivateSupportPolicy*) 和 Description (說明) (選用)。
10. 檢閱 [摘要] 頁面以查看原則允許的權限，然後選擇 [建立原則]。

此政策定義角色可以採取的動作。若需詳細資訊，請參閱《IAM 使用者指南》中的建立 IAM 政策 (主控台)。

IAM 政策範例

可將下列範例政策連接至您的 IAM 角色。此原則允許角色擁有的所有必要動作的完整權限 AWS Support。使用該角色設定私人 Re: post 後，私人 RE: POST 中的任何使用者都擁有相同的權限。

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

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

> **Note**
>
> 如需「重新:私人貼文」的 AWS 受管理原則清單，請參閱。AWS AWSRe: 私人貼文的受管理策略

您可以更新原則以從中移除權限 AWS 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
- 下列項目的動作、資源和條件索引鍵 AWS Identity and Access Management

建立 IAM 角色

建立政策之後，必須建立 IAM 角色，並將政策連接到該角色。當您在重新:POST 私人主控台中建立私人 Re: post 時，您可以選擇此角色。

建立 AWS Support 案例建立和管理的角色

1. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 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. 針對自訂信任原則，輸入下列內容：

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

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

5. 選擇下一步。
6. 在「權限政策」下的搜尋列中，輸入 AWS 受管理的策略或您建立的客戶管理策略，例如*rePostPrivateSupportPolicy*。選取您希望服務具有的權限原則旁邊的核取方塊。
7. 選擇下一步。
8. 在名稱、檢閱和建立頁面上，為角色名稱輸入名稱，例如*rePostPrivateSupportRole*。
9. (選擇性) 在說明中，輸入角色的說明。
10. 檢閱信任原則和權限。
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 IAM 中使用標籤的詳細資訊，請參閱標記 IAM 資源。
12. 選擇建立角色。現在，當您在 Re: POST 私人主控台中設定私人 Re: post 時，可以選擇此角色。請參閱 建立新的私人 Re: 貼文。

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「重新:私人貼文」的存取權。

內容

- 我想限制我的私人 RE 中的特定用戶：從特定操作發布
- 當我設定私有 RE: POST 時，我看不到我建立的 IAM 角色
- 我的 IAM 角色缺少許可
- 錯誤表示我的 IAM 角色無效

我想限制我的私人 RE 中的特定用戶：從特定操作發布

根據預設，私有 Re: POST 中的使用者擁有與您建立的 IAM 角色連接的 IAM 政策中指定的相同許可。這意味著私有 Re: POST 中的任何人都有讀取或寫入權限來創建和管理 AWS Support 案例，無論他們是否擁有 IAM 用戶。 AWS 帳戶

建議遵循下列最佳實務：

- 使用具有的最低必要許可的 AWS Support IAM 政策 請參閱 AWS 受管理的策略：AWSRepostSpaceSupportOperationsPolicy。

當我設定私有 RE: POST 時，我看不到我建立的 IAM 角色

如果您的 IAM 角色沒有出現在 Re: Post Private; 清單的 IAM 角色中，這表示該角色沒有 Re: Post Private 做為受信任的實體，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。

我的 IAM 角色缺少許可

您為私有 RE: post 建立的 IAM 角色需要許可才能執行您想要的動作。例如，如果您希望私人 Re: post 中的使用者建立支援案例，則該角色必須具有`support:CreateCase`權限。Re: Post Private 會假設此角色為您執行這些動作。

如果您收到有關遺失權限的錯誤訊息 AWS Support，請確認附加至您角色的原則具有必要的權限。

請參閱之前的 IAM 政策範例。

錯誤表示我的 IAM 角色無效

確認您為私人 RE: POST 組態選擇了正確的角色。

設定及管理使用者存取權 AWS IAM Identity Center

RE: Post Private 與整合， AWS IAM Identity Center 以便為您組織的員工提供身分聯盟。使用 IAM 身分中心建立或連接組織中的使用者，並集中管理其所有 AWS 帳戶和應用程式的存取權限。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。

自定義您的私人 RE：帖子

您可以在建立私人 Re: Post 後，將一或多個管理員新增至您的私人 Re: Post。系統管理員會使用「重新:私人貼文」應用程式來啟動私人「RE: 張貼」，並管理其中的使用者。他們可以為私人 Re: Post 自訂品牌、新增標籤以分類內容，以及選取感興趣的主題以自動填入內容。如需詳細資訊，請參閱 AWS RE：私有管理後指南。

邀請使用者加入您的私人 Re: 張貼

您可以在建立私人 Re: Post 後，新增一或多個使用者至您的私人 Re: Post。您可以邀請使用者在您的私人 Re: Post 中進行共同作業。使用者可以使用 RE: Post Private 應用程式，使用您設定的認證來登入。登入私人 Re: Post 後，使用者可以瀏覽或搜尋現有內容，包括量身打造的訓練和技術內容，這些內容範圍是根據他們感興趣的主題而定。如需詳細資訊，請參閱 AWS RE：發佈私人使用者指南。

在 Re: POST 私人主控台中管理您的私人 Re: 張貼

本節說明如何在 AWS RE: POST 私有主控台中管理私有 Re: post。

主題

將使用者和群組新增至您的私人 Re: POST

如果您是管理員，則可以將使用者和群組新增至您的私人 Re: Post。

將使用者新增至您的私人 Re: 貼文

1. 請在 https://console.aws.amazon.com/repost-private/ 開啟「重新發佈私人張貼」主控台。
2. 在功能窗格中，選擇 [所有我的私人回覆:貼文]。
3. 選擇您要管理的「私人回覆:貼文」。
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，選取您要新增至私人 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人 Re: POST，並列在「使用者」索引標籤下。

將群組新增至您的私人 Re: POST

1. 請在 https://console.aws.amazon.com/repost-private/ 開啟「重新發佈私人張貼」主控台。
2. 在功能窗格中，選擇 [所有我的私人回覆:貼文]。
3. 選擇您要管理的「私人回覆:貼文」。

4. 選擇 Groups (群組) 標籤。
5. 選擇 [新增使用者和群組]。
6. 從清單中，選取您要新增至私人 Re: POST 的群組。然後，選擇「指派」。

選取的群組會新增至您的私人 Re: POST，並列在「群組」標籤下。

將使用者新增至您的私人 Re: POST 中的群組

使用 IAM 身分中心將新使用者新增至私人 RE: POST 中的現有群組。如需詳細資訊，請參閱 AWS IAM 身分中心使用者指南中的新增使用者至群組。

邀請使用者和群組加入您的私人 Re: POST

請按照以下步驟邀請使用者和群組加入 AWS RE: 私人貼文中的私人 RE: post: 私人貼文：

1. 請在 https://console.aws.amazon.com/repost-private/ 開啟「重新發佈私人張貼」主控台。
2. 在功能窗格中，選擇 [所有我的私人回覆:貼文]。
3. 選擇您要管理的「私人回覆:貼文」。
4. 若要邀請使用者加入您的私人 Re: Post，請選擇「使用者」標籤。

   從清單中，選取您要邀請加入私人 Re: Post 的使用者。然後，選擇內建使用者重新：張貼。
5. 在「使用此私人 RE: 張貼」對話方塊中，輸入下列資訊：

   在 [主旨] 中，輸入您要傳送的電子郵件訊息的主旨。

   在「內文」中，輸入私人 Re: POST 的歡迎訊息。

   選擇發送入職電子郵件。
6. 若要邀請群組加入您的私人 Re: Post，請選擇「群組」分頁。

   從清單中，選取您要邀請加入私人 Re: Post 的群組。然後，選擇要重新發佈的內建群組。
7. 在「此私人 RE: POST 的內建群組」對話方塊中，輸入下列資訊：

   在 [主旨] 中，輸入您要傳送的電子郵件訊息的主旨。

   在「內文」中，輸入私人 Re: POST 的歡迎訊息。

   選擇發送入職電子郵件。

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人 Re: POST 的相關資訊。

在您的私人 RE 中升級使用者：張貼至管理員

若要將私人 RE: 張貼使用者升級為管理員，請依照下列步驟執行：

1. 請在 https://console.aws.amazon.com/repost-private/ 開啟「重新發佈私人張貼」主控台。
2. 在功能窗格中，選擇 [所有我的私人回覆:貼文]。
3. 選擇您要管理的「私人回覆:貼文」。
4. 選擇 Users (使用者) 索引標籤。
5. 選取要升級為管理員的一或多個使用者。
6. 選擇 [編輯角色]，然後選擇 [設為管理員]。

選取的使用者會升級為管理員。在「使用者」標籤下，這些使用者的「角色」會更新為「管理員」。

從您的私人 Re: POST 中移除使用者或群組

如果您是管理員，則可以從私人 Re: Post 中移除使用者或群組。

從您的私人 Re: Post 中移除使用者

1. 請在 https://console.aws.amazon.com/repost-private/ 開啟「重新發佈私人張貼」主控台。
2. 在功能窗格中，選擇 [所有我的私人回覆:貼文]。
3. 選擇您要管理的「私人回覆:貼文」。
4. 在「使用者」下，從清單中選取您要從私人 Re: Post 中移除的使用者。然後，選擇「移除」。

選取的使用者會從您的私人 Re: POST 中移除。已移除使用者的相關資訊不再顯示在 [使用者] 索引標籤下。

從您的私人 Re: POST 中移除群組

1. 請在 https://console.aws.amazon.com/repost-private/ 開啟「重新發佈私人張貼」主控台。
2. 在功能窗格中，選擇 [所有我的私人回覆:貼文]。
3. 選擇您要管理的「私人回覆:貼文」。
4. 選擇 Groups (群組) 標籤。

5. 從清單中，選取您要從私人 Re: POST 移除的群組。然後，選擇「移除」。

選取的群組會從您的私人 Re: POST 中移除。已移除群組的相關資訊不再顯示在「群組」(Groups) 標籤下

從您的私人 Re: Po AWS st 中新增或移除員工

如果您有企業或企業上 Support 計劃，則可以在私人 Re: Post 中新增或移除 AWS 員工。如需詳細資訊，請聯絡禮賓服務 Support 或您的技術客戶經理 (TAM)。

刪除私人 Re: 從 Re: 私人貼文

若要刪除 AWS RE: 私人貼文中的私人 RE: 貼文，請按照下列步驟操作：

1. 請在 https://console.aws.amazon.com/repost-private/ 開啟「重新發佈私人張貼」主控台。
2. 在功能窗格中，選擇 [所有我的私人回覆:貼文]。
3. 選擇您要管理的「私人電子郵件:貼文」，然後選擇「刪除」。
4. 選取所有選項以確認並確認您要永久刪除私人 RE: POST 及與其相關聯的資料。

> **Important**
>
> 當您刪除私人 Re: POST 時，與私人 Re: POST 相關的所有組態資訊都將被刪除。刪除私人 Re: POST 後，您將無法從中還原任何內容。

5. 當系統提示您獲得額外書面同意時，請輸入您的私人 Re: POST 的名稱。再選擇 Delete (刪除)。

刪除您的私人 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复：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AWS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 Priv ate 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AWS 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": "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"
}
```

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

```
{
   "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"
}
```

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

```
 {
    "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"
}
```


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": "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"
    }
}
```

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

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 先決條件。

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 AWSRE: 張貼以私人身分識別為基礎的政策範例。

文件歷史記錄

下表說明 AWS RE：私人貼文的文件發行版本：

變更	描述	日期
更新	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
更新	新增亞太區域 (新加坡) 至支援的區域	2024年3月6日
新資源	已新增 AWS RE: 私有貼文 AWS 受管政策的文件	2023 年 11 月 26 日
初始版本	RE: POST 專用主控台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。