aws

管理員指南

Amazon WorkMail

版本 1.0

Amazon WorkMail: 管理員指南

Table of Contents

什麼是 Amazon WorkMail？

Amazon WorkMail 是安全的受管商業電子郵件與行事曆服務，可支援現有的桌上型電腦及行動裝置電子郵件用戶端。Amazon WorkMail 使用者可以使用 Microsoft Outlook、瀏覽器或其原生 iOS 和 Android 電子郵件應用程式來存取其電子郵件、聯絡人和行事曆。您可以將 Amazon WorkMail 與現有的公司目錄整合，並控制加密資料的金鑰和資料存放位置。

有關支援的 AWS 區域和端點清單，請參閱 AWS 區域與端點。

主題

Amazon WorkMail 系統需求

當您的 Amazon WorkMail 管理員邀請您登入 Amazon WorkMail 帳戶時，您可以使用 Amazon WorkMail Web 用戶端登入。

Amazon WorkMail 也適用於所有支援 Exchange ActiveSync 通訊協定的主要行動裝置和作業系統。這些裝置包含 iPad、iPhone、Android 和 Windows Phone。macOS 使用者可以將其 Amazon WorkMail 帳戶新增至其 Mail、Calendar 和 Contacts 應用程式。

Amazon WorkMail 支援下列作業系統版本：

- Windows – Windows 7 SP1 或更新版本
- MacOS – MacOS 10.12 (Sierra) 或更新版本
- Android – Andriod 5.0 或更新版本
- iPhone – iOS 5 或更新版本
- Windows 電話 – Windows 8.1 或更新版本
- Blackberry – Blackberry 作業系統 10.3.3.3216

如果您有有效的 Microsoft Outlook 授權，您可以使用下列版本的 Microsoft Outlook 存取 Amazon WorkMail：

- Outlook 2013 或更新版本
- Outlook 2013 Click-to-Run 或更新版本
- Outlook for Mac 2016 或更新版本

您可以使用下列瀏覽器版本存取 Amazon WorkMail Web 用戶端：

- Google Chrome – 22 版或更新版本
- Mozilla Firefox – 27 版或更新版本
- Safari – 第 7 版或更新版本
- Internet Explorer – 第 11 版
- Microsoft Edge

您也可以搭配偏好的 IMAP 用戶端使用 Amazon WorkMail。

Amazon WorkMail 概念

以下將說明了解和使用 Amazon WorkMail 的核心術語和概念。

組織

Amazon WorkMail 的租戶設定。

別名

全球唯一識別您組織的名稱。別名用於存取 Amazon WorkMail Web 應用程式 (https：//*alias*.awsapps.com/mail)。

網域

電子郵件地址中 @符號後面的 Web 地址。您可以新增接收和傳送至您組織中的信箱之網域。

測試郵件網域

網域會在設定期間自動設定，可用於測試 Amazon WorkMail。測試郵件網域是## awsapps.com。測試郵件網域需受制於不同的限制。如需詳細資訊，請參閱Amazon WorkMail 配額。

目錄

在 中建立的 AWS Simple AD、 AWS Managed AD 或 AD Connector AWS Directory Service。如果您使用 Amazon WorkMail Quick 設定建立組織，我們會為您建立 WorkMail 目錄。您無法在 中檢視 WorkMail 目錄 AWS Directory Service。

使用者

在 中建立的使用者 AWS Directory Service。您可以在 USER 或 REMOTE_USER 角色中建立使用者。使用 USER 角色建立和啟用使用者時，他們會收到自己的信箱以供存取。當使用者停用時，他們無法存取 Amazon WorkMail。

使用 REMOTE_USER 角色建立和啟用的使用者會列在通訊錄中，但不會在 Amazon WorkMail 中取得信箱。REMOTE_USER 可以將信箱託管在 Amazon WorkMail 之外，但仍會列為 Amazon WorkMail 通訊錄中具有信箱的任何其他使用者，並可查詢其他行事曆以尋找免費或忙碌的資訊。

群組

用於 的群組 AWS Directory Service。群組可以用作 Amazon WorkMail 中的分發清單或安全群組。群組沒有自己的信箱。

資源

資源代表會議室或設備資源，可由 Amazon WorkMail 使用者預訂。

行動裝置政策

控制安全性功能和行動裝置行為的各種 IT 政策規則。

相關 AWS 服務

下列服務會與 Amazon WorkMail 搭配使用：

- AWS Directory Service—您可以將 Amazon WorkMail 與現有的 AWS Simple AD、 AWS Managed AD 或 AD Connector 整合。在 中建立目錄， AWS Directory Service 然後為此目錄啟用 Amazon WorkMail。設定此整合之後，您可以從現有目錄中的使用者清單中選擇要為 Amazon WorkMail 啟用哪些使用者，使用者可以使用其現有的 Active Directory 登入資料登入。如需詳細資訊，請參閱 AWS Directory Service 管理指南。
- Amazon Simple Email Service：Amazon WorkMail 使用 Amazon SES 來傳送所有外寄電子郵件。測試郵件網域和您的網域可在 Amazon SES 主控台中進行管理。從 Amazon WorkMail 傳送的電子郵件無需付費。如需詳細資訊，請參閱 Amazon Simple Email Service 開發人員指南。

- AWS Identity and Access Management— AWS Management Console 需要您的使用者名稱和密碼，以便您使用的任何服務可以判斷您是否具有存取其資源的許可。我們建議您避免使用 AWS 帳戶登入資料進行存取， AWS 因為 AWS 帳戶登入資料無法以任何方式撤銷或限制。反之，我們建議您建立 IAM 使用者，並將使用者新增至具有管理許可的 IAM 群組。然後，您可以使用 IAM 使用者登入資料來存取 主控台。

  如果您已註冊 AWS，但是尚未為自己建立 IAM 使用者，可以使用 IAM 主控台加以建立。如需詳細資訊，請參閱《IAM 使用者指南》中的建立個別 IAM 使用者。
- AWS Key Management Service—Amazon WorkMail 已與 整合， AWS KMS 用於加密客戶資料。您可以從 AWS KMS 主控台執行金鑰管理。如需詳細資訊，請參閱《 AWS Key Management Service 開發人員指南》中的什麼是 AWS Key Management Service。

Amazon WorkMail 定價

使用 Amazon WorkMail，無需預付費用或承諾。您只需為使用中的使用者帳戶付費。如需有關定價的更多特定資訊，請參閱定價。

Amazon WorkMail 資源

以下相關資源可協助您使用此服務。

- 課程和研討會 – 連結至以角色為基礎的特殊課程，以及自主安排進度的實驗室，以協助強化您的 AWS 技能並取得實際經驗。
- AWS 開發人員中心 – 探索教學課程、下載工具，並了解 AWS 開發人員事件。
- AWS 開發人員工具 – 開發人員工具、SDKs、IDE 工具組和命令列工具的連結，用於開發和管理 AWS 應用程式。
- 入門資源中心 – 了解如何設定您的 AWS 帳戶、加入 AWS 社群，以及啟動您的第一個應用程式。
- 實用的教學課程 - 按照逐步教學課程在 AWS上啟動第一個應用程式。
- AWS 白皮書 – 技術 AWS 白皮書的完整清單連結，涵蓋架構、安全和經濟等主題，並由 AWS Solutions Architects 或其他技術專家撰寫。
- AWS 支援 中心 – 建立和管理 AWS 支援 案例的中樞。也包含其他實用資源的連結，例如論壇、技術 FAQs、服務運作狀態和 AWS Trusted Advisor。
- 支援 – 有關one-on-one、快速回應支援管道的資訊主要網頁 支援，可協助您在雲端中建置和執行應用程式。
- 聯絡我們 – 查詢有關 AWS 帳單、帳戶、事件、濫用與其他問題的聯絡中心。

- AWS 網站條款 – 有關我們的著作權和商標、您的帳戶、授權和網站存取，以及其他主題的詳細資訊。

先決條件

若要擔任 Amazon WorkMail 管理員，您需要 AWS 帳戶。如果您尚未註冊 AWS，請完成下列作業以開始進行設定。

主題

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   註冊程序的一部分包括接聽電話或文字訊息，並在電話鍵盤上輸入驗證碼。

   當您註冊 時 AWS 帳戶，AWS 帳戶根使用者會建立 。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理存取權的使用者

註冊 後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center和建立管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

1. 選擇根使用者並輸入 AWS 帳戶 您的電子郵件地址，以帳戶擁有者AWS Management Console身分登入 。在下一頁中，輸入您的密碼。

如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

   如需說明，請參閱《IAM 使用者指南》中的為您的 AWS 帳戶 根使用者 （主控台） 啟用虛擬 MFA 裝置。

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的啟用 AWS IAM Identity Center。

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

   如需使用 IAM Identity Center 目錄 做為身分來源的教學課程，請參閱AWS IAM Identity Center 《 使用者指南》中的使用預設值設定使用者存取 IAM Identity Center 目錄。

以具有管理存取權的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

  如需使用 IAM Identity Center 使用者登入的說明，請參閱AWS 登入 《 使用者指南》中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的新增群組。

授予 Amazon WorkMail 的 IAM 使用者許可

根據預設，IAM 使用者沒有管理 Amazon WorkMail 資源的許可。您必須連接 AWS 受管政策 (AmazonWorkMailFullAccess 或 AmazonWorkMailReadOnlyAccess) 或建立客戶受管政策，明確授予

IAM 使用者這些許可。然後您需要將這些政策連接至需要這些許可的 IAM 使用者或群組。如需詳細資訊，請參閱Amazon WorkMail 的身分和存取管理。

Amazon WorkMail 的安全性

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以從資料中心和網路架構中受益，該架構專為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 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。 AWS 也提供您可以安全使用的服務。在 AWS 合規計畫中，第三方稽核員會定期測試並驗證我們的安全功效。若要了解適用於 Amazon WorkMail 的合規計劃，請參閱AWS 合規計劃範圍內的服務。
- 雲端的安全性 – 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、您公司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 Amazon WorkMail 時套用共同責任模型。下列主題說明如何設定 Amazon WorkMail 以符合您的安全和合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Amazon WorkMail 資源。

主題

Amazon WorkMail 中的資料保護

AWS 共同責任模型適用於 Amazon WorkMail 中的資料保護。如此模型所述， 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，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 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：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 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。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，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 Amazon WorkMail 或其他 AWS 服務 使用主控台 AWS CLI、API 或 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。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

Amazon WorkMail 如何使用 AWS KMS

Amazon WorkMail 會在訊息寫入磁碟之前，對所有 Amazon WorkMail 組織信箱中的所有訊息進行透明加密，並在使用者存取訊息時將其透明解密。您無法停用加密。為了保護保護訊息的加密金鑰，Amazon WorkMail 已與 AWS Key Management Service () 整合AWS KMS。

Amazon WorkMail 還提供一個選項，可讓使用者傳送簽章或加密的電子郵件。此加密功能不使用 AWS KMS。如需詳細資訊，請參閱啟用簽章或加密的電子郵件。

主題

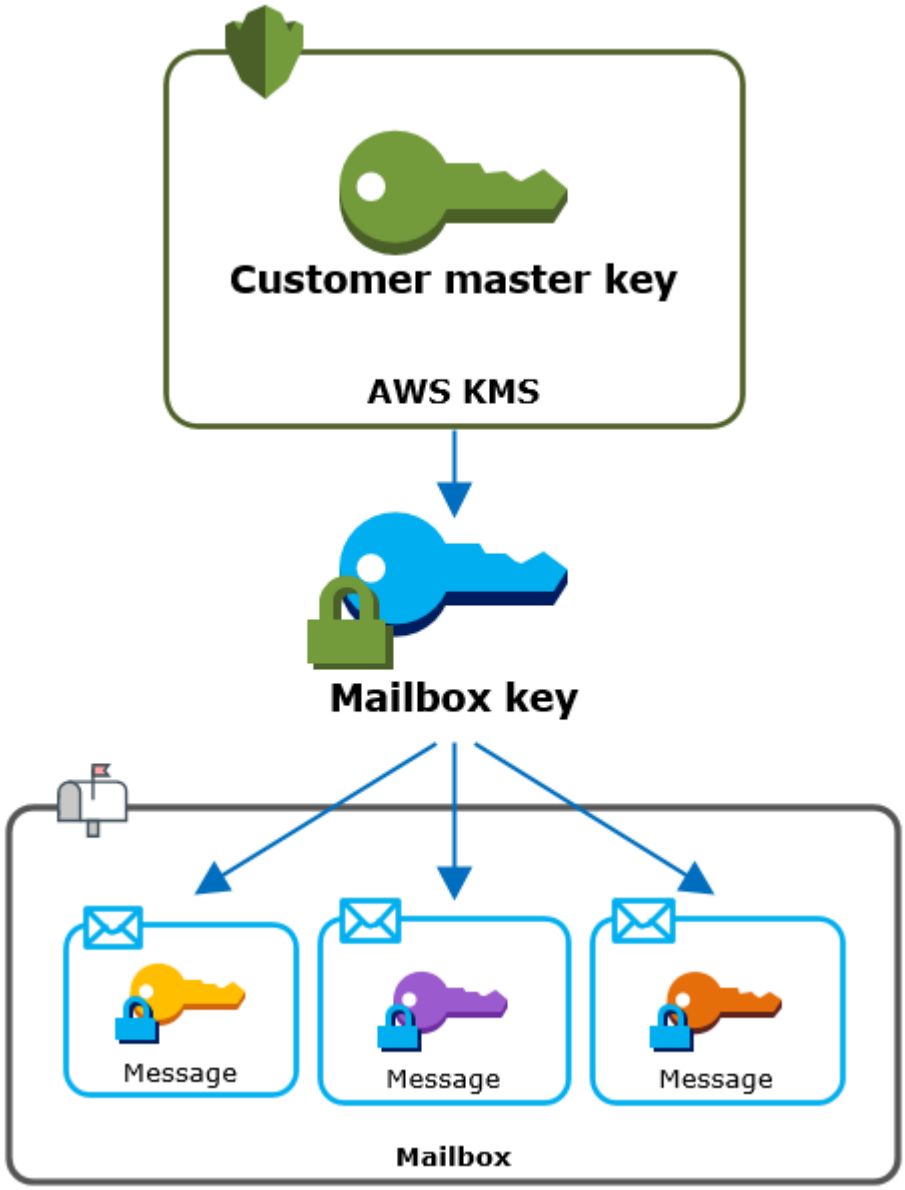
- Amazon WorkMail 加密
- 授權使用 CMK
- Amazon WorkMail 加密內容
- 監控 Amazon WorkMail 與 的互動 AWS KMS

Amazon WorkMail 加密

在 Amazon WorkMail 中，每個組織可以包含多個信箱，各用於組織中的每個使用者。所有訊息 (包括電子郵件和行事曆項目) 都存放在使用者的信箱中。

為了保護 Amazon WorkMail 組織中的信箱的內容，Amazon WorkMail 會在所有信箱訊息寫入磁碟之前加密。客戶提供的資訊都不以純文字形式儲存。

每個訊息都在唯一的資料加密金鑰下加密。訊息金鑰由信箱金鑰加密，這是該信箱專用的唯一加密金鑰。信箱金鑰是在永遠不會 AWS KMS 保持未加密的組織 AWS KMS 的客戶主金鑰 (CMK) 下加密。下圖顯示 AWS KMS中在加密訊息、加密訊息金鑰、加密信箱金鑰及組織 CMK 之間的關係。



設定組織的 CMK

當您建立 Amazon WorkMail 組織時，您可以選擇組織 AWS KMS 的客戶主金鑰 (CMK)。這個 CMK 保護該組織中的所有信箱金鑰。

您可以選取 Amazon WorkMail 的預設 AWS 受管 CMK，也可以選取您擁有和管理的現有客戶受管 CMK。如需詳細資訊，請參閱《 AWS Key Management Service 開發人員指南》中的客戶主金鑰 (CMKs)。您可以為每個組織選取相同的 CMK 或不同的 CMK，但一旦選取 CMK，就無法變更。

> **Important**
>
> Amazon WorkMail 僅支援對稱 CMKs。您不能使用非對稱 CMK。如需協助判斷 CMK 是對稱或非對稱，請參閱《 AWS Key Management Service 開發人員指南》中的識別對稱和非對稱 CMKs。

若要尋找組織的 CMK，請使用記錄對 呼叫的 AWS CloudTrail 日誌項目 AWS KMS。

每個信箱的唯一加密金鑰

當您建立信箱時，Amazon WorkMail 會在外部為信箱產生唯一的 256 位元進階加密標準 (AES) 對稱加密金鑰，稱為其信箱金鑰 AWS KMS。Amazon WorkMail 使用信箱金鑰來保護信箱中每封訊息的加密金鑰。

為了保護信箱金鑰，Amazon WorkMail 會呼叫 AWS KMS 來加密組織 CMK 下的信箱金鑰。然後，它會將加密的信箱金鑰存放在信箱中繼資料。

> **Note**
>
> Amazon WorkMail 使用對稱信箱加密金鑰來保護訊息金鑰。在過去，Amazon WorkMail 使用非對稱金鑰對來保護每個信箱。它使用公有金鑰來加密每個訊息金鑰，並使用私有金鑰來解密金鑰。私有信箱金鑰由組織的 CMK 保護。較舊的信箱可能會使用非對稱信箱金鑰對。此變更不會影響信箱或其訊息的安全性。

加密每個訊息

當使用者將訊息新增至信箱時，Amazon WorkMail 會為外部的訊息產生唯一的 256 位元 AES 對稱加密金鑰 AWS KMS。它會使用此訊息金鑰來加密訊息。Amazon WorkMail 會在信箱金鑰下加密訊息金鑰，並將加密的訊息金鑰存放在訊息中。然後，它在組織的 CMK 下加密信箱金鑰。

建立新信箱

Amazon WorkMail 建立信箱時，會使用下列程序來準備信箱以保留加密的訊息。

- Amazon WorkMail 會為 AWS KMS 外部的信箱產生唯一的 256 位元 AES 對稱加密金鑰。
- Amazon WorkMail 會呼叫 AWS KMS 加密操作。它會傳入 organization. 的信箱金鑰和客戶主金鑰 (CMK) 的識別符。 AWS KMS 會傳回在 CMK 下加密的信箱金鑰的密碼文字。
- Amazon WorkMail 將加密的信箱金鑰存放在信箱中繼資料。

加密信箱訊息

為了加密訊息，Amazon WorkMail 使用以下程序。

1. Amazon WorkMail 為訊息產生唯一的 256 位元 AES 對稱金鑰。它使用純文字訊息金鑰和進階加密標準 (AES) 演算法來加密外部的訊息 AWS KMS。
2. 為了在信箱金鑰下保護訊息，Amazon WorkMail 需要解密一律以加密形式儲存的信箱金鑰。

   Amazon WorkMail 會呼叫 AWS KMS Decrypt 操作，並在加密的信箱金鑰中傳遞。 AWS KMS 會使用 CMK 讓組織解密信箱金鑰，並將純文字信箱金鑰傳回給 Amazon WorkMail。
3. Amazon WorkMail 使用純文字信箱金鑰和進階加密標準 (AES) 演算法來加密外部的訊息金鑰 AWS KMS。
4. Amazon WorkMail 將加密的訊息金鑰存放在中繼資料，以用於解密金鑰。

解密信箱訊息

為了解密訊息，Amazon WorkMail 使用以下程序。

1. Amazon WorkMail 會呼叫 AWS KMS 解密操作，並在加密的信箱金鑰中傳遞。 AWS KMS 會使用 CMK 讓組織解密信箱金鑰，並將純文字信箱金鑰傳回 Amazon WorkMail。
2. Amazon WorkMail 使用純文字信箱金鑰和進階加密標準 (AES) 演算法，在 外部解密加密的訊息金鑰 AWS KMS。
3. Amazon WorkMail 使用純文字訊息金鑰解密已加密的訊息。

快取信箱金鑰

為了改善效能並將對 的呼叫降至最低 AWS KMS，Amazon WorkMail 會在本機快取每個用戶端的每個純文字信箱金鑰最多一分鐘。在快取期間結束時，就會移除信箱金鑰。如果在快取期間需要該用戶端的

信箱金鑰，Amazon WorkMail 可以從快取中取得金鑰，而不需要呼叫 AWS KMS。信箱金鑰放在快取中保護，絕對不會以純文字形式寫入磁碟。

授權使用 CMK

當 Amazon WorkMail 在密碼編譯操作中使用客戶主金鑰 (CMK) 時，它會代表信箱管理員。

若要代表您使用 AWS KMS 客戶主金鑰 (CMK) 做為秘密，管理員必須具有下列許可。您可以在 IAM 政策或金鑰策略中指定這些必要的許可。

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

若要允許 CMK 僅用於源自 Amazon WorkMail 的請求，您可以使用 kms:ViaService 條件索引鍵搭配 `workmail.<region>.amazonaws.com`值。

您也可以使用加密內容中的金鑰或值做為條件金鑰，以將 CMK 用於密碼編譯操作。例如，您可以在 IAM 或金鑰政策文件中使用字串條件運算子，或在授權中使用授權限制。

AWS 受管 CMK 的金鑰政策

Amazon WorkMail 的 AWS 受管 CMK 金鑰政策僅在 Amazon WorkMail 代表使用者提出請求時，才提供使用者使用 CMK 進行指定操作的許可。金鑰政策不允許任何使用者直接使用 CMK。

此金鑰政策與所有 AWS 受管金鑰的政策一樣，都是由服務建立。您無法變更金鑰政策，但您可以隨時檢視。如需詳細資訊，請參閱《 AWS Key Management Service 開發人員指南》中的檢視金鑰政策。

金鑰政策中的政策陳述式具有下列效果：

- 允許帳戶和區域中的使用者使用 CMK 進行密碼編譯操作和建立授予，但僅限於請求來自 Amazon WorkMail 時。`kms:ViaService` 條件金鑰會強制實施此限制。
- 允許 AWS 帳戶建立 IAM 政策，允許使用者檢視 CMK 屬性並撤銷授予。

以下是 Amazon WorkMail AWS 受管 CMK 範例的金鑰政策。

```
{
  "Version" : "2012-10-17",
  "Id" : "auto-workmail-1",
  "Statement" : [ {
```

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

使用授予來授權 Amazon WorkMail

除了金鑰政策之外，Amazon WorkMail 還會使用授予來為每個組織將許可新增至 CMK。若要查看帳戶中的 CMK，請使用 ListGrants 操作。

Amazon WorkMail 使用授予將下列許可新增至組織的 CMK。

- 新增 `kms:Encrypt` 許可，以允許 Amazon WorkMail 加密信箱金鑰。
- 新增允許 Amazon WorkMail 使用 CMK 解密信箱金鑰的`kms:Decrypt`許可。Amazon WorkMail 在授予中需要此許可，因為請求讀取信箱訊息時，將會使用讀取訊息的使用者的安全內容。請求不會使用 AWS 帳戶的登入資料。當您為組織選取 CMK 時，Amazon WorkMail 會建立此授與。

若要建立授予，Amazon WorkMail 會代表建立組織的使用者來呼叫 CreateGrant。建立授與的許可來自金鑰政策。此政策允許帳戶使用者在 Amazon WorkMail 代表授權使用者提出請求時，在組織的 CMK `CreateGrant`上呼叫 。

金鑰政策也允許 帳戶根撤銷 AWS 受管金鑰的授與。不過，如果您撤銷授予，Amazon WorkMail 無法解密信箱中的加密資料。

Amazon WorkMail 加密內容

加密內容是一組金鑰/值對，其中包含任意非私密資料。當您在加密資料的請求中包含加密內容時，AWS KMS 加密會以加密內容繫結至加密的資料。若要解密資料，您必須傳遞相同的加密內容。如需詳細資訊，請參閱 AWS Key Management Service 開發人員指南中的加密內容。

Amazon WorkMail 在所有 AWS KMS 密碼編譯操作中使用相同的加密內容格式。您可以使用加密內容來識別稽核記錄和日誌 (例如 AWS CloudTrail) 中的這些密碼編譯操作，以及在政策和授與中做為授權的條件。

Amazon AWS KMS Amazon WorkMail 在其加密和解密請求中使用加密內容，其中金鑰為 `aws:workmail:arn`，而值為組織的 Amazon Resource Name (ARN)。

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

例如，下列加密內容包含歐洲 （ 愛爾蘭 ） (`eu-west-1`) 區域中的範例組織 ARN。

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

監控 Amazon WorkMail 與 的互動 AWS KMS

您可以使用 AWS CloudTrail 和 Amazon CloudWatch Logs 來追蹤 Amazon WorkMail AWS KMS 代表您傳送到 的請求。

加密

當您建立信箱時，Amazon WorkMail 會產生信箱金鑰並呼叫 AWS KMS 來加密信箱金鑰。Amazon WorkMail 會使用 AWS KMS 純文字信箱金鑰和 Amazon WorkMail 組織的 CMK 識別符，將加密請求傳送至 。

記錄 `Encrypt` 操作的事件類似於以下範例事件。使用者是 Amazon WorkMail 服務。參數包括 Amazon WorkMail 組織的 CMK ID (`keyId`) 和加密內容。Amazon WorkMail 也傳入信箱金鑰，但不會記錄在 CloudTrail 日誌中。

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

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


解密

當您新增、檢視或刪除信箱訊息時，Amazon WorkMail AWS KMS 會要求解密信箱金鑰。Amazon WorkMail 會傳送解密請求至 ， AWS KMS 其中包含加密信箱金鑰和 Amazon WorkMail 組織的 CMK 識別符。

記錄 `Decrypt` 操作的事件類似於以下範例事件。使用者是 Amazon WorkMail 服務。這些參數包括未記錄在日誌中的加密信箱金鑰 （ 做為加密文字 Blob)，以及 Amazon WorkMail 組織的加密內容。 從加密文字 AWS KMS 衍生 CMK 的 ID。

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

Amazon WorkMail 的身分和存取管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （登入） 和授權 （具有許可） 來使用 Amazon WorkMail 資源。IAM 是 AWS 服務 您可以免費使用的 。

主題

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，取決於您在 Amazon WorkMail 中執行的工作。

服務使用者 – 如果您使用 Amazon WorkMail 服務來執行您的任務，您的管理員會為您提供所需的登入資料和許可。當您使用更多 Amazon WorkMail 功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 Amazon WorkMail 中的功能，請參閱 對 Amazon WorkMail 身分和存取進行故障診斷。

服務管理員 – 如果您在公司負責 Amazon WorkMail 資源，您可能可以完整存取 Amazon WorkMail。您的任務是判斷服務使用者應存取哪些 Amazon WorkMail 功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何搭配 Amazon WorkMail 使用 IAM，請參閱Amazon WorkMail 如何與 IAM 搭配使用。

IAM 管理員 – 如果您是 IAM 管理員，建議您了解撰寫政策以管理 Amazon WorkMail 存取的詳細資訊。若要檢視您可以在 IAM 中使用的 Amazon WorkMail 身分型政策範例，請參閱 Amazon WorkMail 身分型政策範例。

使用身分進行驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色身分進行身分驗證 （ 登入 AWS)。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分身分身分登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料，都是聯合身分的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使用聯合 AWS 身分存取 時，您會間接擔任角色。

根據您身分的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱AWS 登入 《 使用者指南》中的如何登入您的 AWS 帳戶 。

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的 登入資料以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的適用於 API 請求的AWS Signature 第 4 版。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來提高帳戶的安全性。如需更多資訊，請參閱《AWS IAM Identity Center 使用者指南》中的多重要素驗證和《IAM 使用者指南》中的 IAM 中的AWS 多重要素驗證。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取 帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 Theroot 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

IAM 使用者和群組

IAM 使用者是 中具有單一人員或應用程式特定許可 AWS 帳戶 的身分。建議您盡可能依賴臨時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在 中擔任 IAM 角色 AWS Management Console，您可以從使用者切換至 IAM 角色 （ 主控台 ）。

您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱《IAM 使用者指南》中的為第三方身分提供者 (聯合) 建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源（而不是使用角色做為代理）。如需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 IAM 中的跨帳戶資源存取。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在 中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。
  - 服務連結角色 – 服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時憑證，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體，並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程

式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式。

使用政策管理存取權

您可以透過建立政策並將其連接到 AWS 身分或資源 AWS 來控制 中的存取。政策是 中的物件， AWS 當與身分或資源建立關聯時， 會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

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。

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console AWS CLI、 或 API AWS 取得角色資訊。

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，請參閱《IAM 使用者指南》中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 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。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 AWS WAF和 Amazon VPC 是支援 ACLs的服務範例。如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。
- 服務控制政策 SCPs) – SCPs是 JSON 政策，可指定 中組織或組織單位 (OU) 的最大許可 AWS Organizations。 AWS Organizations 是用於分組和集中管理您企業擁有 AWS 帳戶 的多個的服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs的詳細資訊，包括支援 RCPs AWS 服務 的 清單，請參閱AWS Organizations 《 使用者指南》中的資源控制政策 RCPs)。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Amazon WorkMail 如何與 IAM 搭配使用

在您使用 IAM 管理 Amazon WorkMail 的存取權之前，您應該了解哪些 IAM 功能可與 Amazon WorkMail 搭配使用。若要深入了解 Amazon WorkMail 和其他 AWS 服務如何與 IAM 搭配使用，請參閱《AWS IAM 使用者指南》中的與 IAM 搭配使用的 服務。

主題

- Amazon WorkMail 身分型政策
- Amazon WorkMail 資源型政策
- 以 Amazon WorkMail 標籤為基礎的授權
- Amazon WorkMail IAM 角色

Amazon WorkMail 身分型政策

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。Amazon WorkMail 支援特定動作、資源和條件索引鍵。若要了解您在 JSON 政策中使用的所有元素，請參閱 IAM 使用者指南中的 JSON 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，哪個主體在什麼条件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述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，例如沒有相符的 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。

Amazon WorkMail 中的政策動作在動作之前使用下列字首：`workmail:`。例如，若要授予某人使用 Amazon WorkMail `ListUsers` API 操作擷取使用者清單的許可，請在其政策中包含 `workmail:ListUsers`動作。政策陳述式必須包含 `Action` 或 `NotAction` 元素。Amazon WorkMail 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": [
      "workmail:ListUsers",
      "workmail:DeleteUser"
```

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 List 文字的所有動作，請包含以下動作：

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

若要查看 Amazon WorkMail 動作清單，請參閱《IAM 使用者指南》中的 Amazon WorkMail 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 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。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": "*"
```

Amazon WorkMail 支援 Amazon WorkMail 組織的資源層級許可。

Amazon WorkMail 組織資源具有下列 ARN：

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

如需 ARNs 格式的詳細資訊，請參閱 Amazon Resource Name (ARNs AWS 和服務命名空間。

例如，若要在陳述式中指定 m-n1pq2345678r901st2u3vx45x6789yza 組織，請使用以下 ARN。

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

若要指定所有屬於特定帳戶的組織，請使用萬用字元 (*)：

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

某些 Amazon WorkMail 動作，例如用於建立資源的動作，無法在特定資源上執行。在這些情況下，您必須使用萬用字元 (*)。

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

若要查看 Amazon WorkMail 資源類型及其 ARNs 的清單，請參閱《IAM 使用者指南》中的 Amazon WorkMail 定義的資源。若要了解您可以為每個資源的 ARN 指定哪些動作，請參閱 Amazon WorkMail 的動作、資源和條件索引鍵。

條件索引鍵

Amazon WorkMail 支援下列全域條件金鑰。

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

下列範例政策僅授予來自 eu-west-1 AWS 區域中 MFA 驗證 IAM 主體的 Amazon WorkMail 主控台存取權。

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

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

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。

`workmail:ImpersonationRoleId` 是 Amazon WorkMail 唯一支援的服務特定條件金鑰。

下列範例政策將`AssumeImpersonationRole`動作範圍縮小至特定 WorkMail 組織和模擬角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workmail:AssumeImpersonationRole"
      ],
      "Resource": "arn:aws:workmail:us-east-1:111122223333:organization/m-
n1pq2345678r901st2u3vx45x6789yza",
      "Condition": {
        "StringEquals": {
          "workmail:ImpersonationRoleId":"12345678-1234-1234-1234-123456789012"
        }
      }
    }
  ]
}
```

範例

若要檢視 Amazon WorkMail 身分型政策的範例，請參閱 Amazon WorkMail 身分型政策範例。

Amazon WorkMail 資源型政策

Amazon WorkMail 不支援以資源為基礎的政策。

以 Amazon WorkMail 標籤為基礎的授權

您可以將標籤連接至 Amazon WorkMail 資源，或在請求中將標籤傳遞至 Amazon WorkMail。如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。如需標記 Amazon WorkMail 資源的詳細資訊，請參閱標記組織。

Amazon WorkMail IAM 角色

IAM 角色是您 AWS 帳戶中具有特定許可的實體。

搭配 Amazon WorkMail 使用臨時憑證

您可以搭配聯合使用暫時憑證、擔任 IAM 角色，或是擔任跨帳戶角色。您可以透過呼叫 AssumeRole 或 GetFederationToken 等 AWS STS API 操作來取得臨時安全登入資料。

Amazon WorkMail 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，以代表您完成 動作。服務連結角色會顯示在您的 IAM 帳戶中，並由該服務所擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

Amazon WorkMail 支援服務連結角色。如需建立或管理 Amazon WorkMail 服務連結角色的詳細資訊，請參閱 使用 Amazon WorkMail 的服務連結角色。

服務角色

此功能可讓服務代表您擔任服務角色。此角色可讓服務存取其他服務中的資源，以代表您完成動作。服務角色會出現在您的 IAM 帳戶中，且由該帳戶所擁有。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。

Amazon WorkMail 支援服務角色。

Amazon WorkMail 身分型政策範例

根據預設，IAM 使用者和角色沒有建立或修改 Amazon WorkMail 資源的許可。他們也無法使用 AWS Management Console AWS CLI或 AWS API 來執行任務。IAM 管理員必須建立 IAM 政策，授予使用

者和角色在指定資源上執行特定 API 作業的所需許可。管理員接著必須將這些政策連接至需要這些許可的 IAM 使用者或群組。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的在 JSON 標籤上建立政策。

主題

- 政策最佳實務
- 使用 Amazon WorkMail 主控台
- 允許使用者檢視他們自己的許可
- 允許使用者唯讀存取 Amazon WorkMail 資源

政策最佳實務

以身分為基礎的政策會判斷是否有人可以在您的帳戶中建立、存取或刪除 Amazon WorkMail 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 AWS 受管政策來授予許多常見使用案例的許可。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，進一步減少許可。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅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 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 使用服務動作，您也可以使用條件來授予存取服務動作的權限 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可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。
- 需要多重要素驗證 (MFA)：如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以增加安全性。如需在呼叫 API 操作時請求 MFA，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》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用 Amazon WorkMail 主控台

若要存取 Amazon WorkMail 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 AWS 帳戶中 Amazon WorkMail 資源的詳細資訊。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (IAM 使用者或角色) 而言，主控台就無法如預期運作。

為了確保這些實體仍可使用 Amazon WorkMail 主控台，也請將下列 AWS 受管政策 AmazonWorkMailFullAccess 連接至實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

AmazonWorkMailFullAccess 政策授予 IAM 使用者對 Amazon WorkMail 資源的完整存取權。此政策可讓使用者存取所有 Amazon WorkMail、 AWS Key Management Service、Amazon Simple Email Service 和 AWS Directory Service 操作。這也包括 Amazon WorkMail 代表您執行所需的數個 Amazon EC2 操作。 Amazon WorkMail 電子郵件事件記錄logs以及在 Amazon WorkMail 主控台中檢視指標時，需要 和 cloudwatch許可。稽核記錄使用 CloudWatch Logs、Amazon S3 和 Amazon Data FireHose 來存放 logs。如需詳細資訊，請參閱在 Amazon WorkMail 中記錄和監控。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WorkMailAdministration",
      "Effect": "Allow",
      "Action": [
        "ds:AuthorizeApplication",
        "ds:CheckAlias",
        "ds:CreateAlias",
        "ds:CreateDirectory",
        "ds:CreateIdentityPoolDirectory",
        "ds:DeleteDirectory",
        "ds:DescribeDirectories",
        "ds:GetDirectoryLimits",
        "ds:ListAuthorizedApplications",
        "ds:UnauthorizeApplication",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
```

```
        "ec2:CreateNetworkInterface",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSubnet",
        "ec2:CreateTags",
        "ec2:CreateVpc",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteSubnet",
        "ec2:DeleteVpc",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "kms:DescribeKey",
        "kms:ListAliases",
        "lambda:ListFunctions",
        "route53:ChangeResourceRecordSets",
        "route53:ListHostedZones",
        "route53:ListResourceRecordSets",
        "route53:GetHostedZone",
        "route53domains:CheckDomainAvailability",
        "route53domains:ListDomains",
        "ses:*",
        "workmail:*",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:DeleteDeliveryDestination",
        "logs:DeleteDeliveryDestinationPolicy",
        "logs:DescribeDeliveryDestinations",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:PutDeliveryDestination",
        "logs:PutDeliveryDestinationPolicy",
        "logs:CreateDelivery",
        "logs:DeleteDelivery",
        "logs:DescribeDeliveries",
        "logs:GetDelivery",
        "logs:DeleteDeliverySource",
        "logs:DescribeDeliverySources",
        "logs:GetDeliverySource",
        "logs:PutDeliverySource",
```

```
            "logs:DescribeResourcePolicies",
            "cloudwatch:GetMetricData",
            "firehose:DescribeDeliveryStream",
            "firehose:ListDeliveryStreams",
            "s3:ListAllMyBuckets"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AuditLogDeliveryThroughCWLogs",
        "Effect": "Allow",
        "Action": [
            "firehose:TagDeliveryStream",
            "logs:PutResourcePolicy",
            "s3:GetBucketPolicy",
            "s3:PutBucketPolicy"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:CalledViaLast": "logs.amazonaws.com"
            }
        }
    },
    {
        "Sid": "InboundOutboundEmailEventsLink",
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:AWSServiceName": "events.workmail.amazonaws.com"
            }
        }
    },
    {
        "Sid": "AuditLoggingLink",
        "Effect": "Allow",
        "Action": "iam:CreateServiceLinkedRole",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "iam:AWSServiceName": "delivery.logs.amazonaws.com"
            }
```

```
        }
    },
    {
        "Sid": "InboundOutboundEmailEventsUnlink",
        "Effect": "Allow",
        "Action": [
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus"
        ],
        "Resource": "arn:aws:iam::*:role/aws-service-role/
events.workmail.amazonaws.com/AWSServiceRoleForAmazonWorkMailEvents*"
    },
    {
        "Sid": "InboundOutboundEmailEventsAuth",
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::*:role/*workmail*",
        "Condition": {
            "StringLike": {
                "iam:PassedToService": "events.workmail.amazonaws.com"
            }
        }
    }
  ]
}
```

對於僅對 AWS CLI 或 AWS API 進行呼叫的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合您嘗試執行之 API 操作的動作就可以了。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此政策包含在主控台上完成此動作的許可，或使用 AWS CLI 或 AWS API 以程式設計方式完成此動作的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

允許使用者唯讀存取 Amazon WorkMail 資源

下列政策陳述式會授予 IAM 使用者對 Amazon WorkMail 資源的唯讀存取權。這個政策與 AWS 受管政策 AmazonWorkMailReadOnlyAccess 提供相同的存取層級。任一政策都提供使用者存取所有 Amazon WorkMail `Describe`操作的權限。需要存取 AWS Directory Service `DescribeDirectories`操作才能取得 AWS Directory Service 目錄的相關資訊。需要存取 Amazon SES 服務，才能取得所設定網域的相關資訊。 AWS Key Management Service 需要存取 ，才能取得使用加密金鑰的相關資訊。Amazon WorkMail 主控台中的電子郵件事件記錄和檢視指標需要 `logs`和 `cloudwatch`許可。稽核記錄使用 CloudWatch Logs、Amazon S3 和 Amazon Data FireHose 來存放 `logs`。如需詳細資訊，請參閱[在 Amazon WorkMail 中記錄和監控]。

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

```
      "Effect": "Allow",
      "Action": [
        "ses:Describe*",
        "ses:Get*",
        "workmail:Describe*",
        "workmail:Get*",
        "workmail:List*",
        "workmail:Search*",
        "lambda:ListFunctions",
        "iam:ListRoles",
        "logs:DescribeLogGroups",
        "logs:DescribeDeliveryDestinations",
        "logs:GetDeliveryDestination",
        "logs:GetDeliveryDestinationPolicy",
        "logs:DescribeDeliveries",
        "logs:DescribeDeliverySources",
        "logs:GetDelivery",
        "logs:GetDeliverySource",
        "cloudwatch:GetMetricData"
      ],
      "Resource": "*"
    }
  ]
}
```

對 Amazon WorkMail 身分和存取進行故障診斷

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

主題

- 我無權在 Amazon WorkMail 中執行動作
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 AWS 帳戶外的人員存取我的 Amazon WorkMail 資源

我無權在 Amazon WorkMail 中執行動作

如果 AWS Management Console 告訴您未獲授權執行 動作，則必須聯絡管理員尋求協助。您的管理員是提供您使用者名稱和密碼的人員。

當 IAM `mateojackson` 使用者嘗試使用主控台檢視群組的詳細資訊，但沒有`workmail:DescribeGroup`許可時，會發生下列範例錯誤。

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

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 `group` 動作存取 `workmail:DescribeGroup` 資源。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，表示您無權執行`iam:PassRole`動作，則必須更新您的政策，以允許您將角色傳遞給 Amazon WorkMail。

有些 AWS 服務 可讓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 IAM `marymajor` 使用者嘗試使用主控台在 Amazon WorkMail 中執行動作時，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 管理員。您的管理員提供您的簽署憑證。

我想要允許 AWS 帳戶外的人員存取我的 Amazon WorkMail 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。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Amazon WorkMail 是否支援這些功能，請參閱 Amazon WorkMail 如何與 IAM 搭配使用。
- 若要了解如何 AWS 帳戶 在您擁有的 資源間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個資源中提供存取權給 IAM 使用者。
- 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《IAM 使用者指南》中的提供存取權給第三方 AWS 帳戶 擁有。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。

- 如需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 IAM 中的跨帳戶資源存取。

AWS Amazon WorkMail 的 受管政策

若要將許可新增至使用者、群組和角色，使用 AWS 受管政策比自行撰寫政策更容易。建立 IAM 客戶受管政策需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可以使用我們的 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中使用。如需受 AWS 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。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。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)。當新功能啟動或新操作可用時，服務很可能會更新 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您現有的許可。

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。當服務啟動新功能時， 會為新操作和資源 AWS 新增唯讀許可。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中有關任務職能的AWS 受管政策。

AWS 受管政策：AmazonWorkMailFullAccess

您可將 `AmazonWorkMailFullAccess` 政策連接到 IAM 身分。此政策會授予許可，以允許完整存取 Amazon WorkMail。

若要檢視此政策的許可，請參閱 中的 AmazonWorkMailFullAccess AWS Management Console。

AWS 受管政策：AmazonWorkMailReadOnlyAccess

您可將 `AmazonWorkMailReadOnlyAccess` 政策連接到 IAM 身分。此政策會授予許可，允許唯讀存取 Amazon WorkMail。

若要檢視此政策的許可，請參閱 中的 AmazonWorkMailReadOnlyAccess AWS Management Console。

AWS 受管政策：AmazonWorkMailEventsServiceRolePolicy

此政策會連接至名為 AmazonWorkMailEvents 的服務連結角色，以允許存取 Amazon WorkMail 事件使用或管理 AWS 的服務和資源。如需詳細資訊，請參閱使用 Amazon WorkMail 的服務連結角色。

AWS 受管政策的 Amazon WorkMail 更新

檢視自此服務開始追蹤這些變更以來，Amazon WorkMail AWS 受管政策更新的詳細資訊。

變更	描述	日期
AWS 受管政策更新 - 現有政策的更新	已更新 `AmazonWorkMailReadOnlyAccess` 和 `AmazonWorkMailFullAccess` 許可，讓 Amazon WorkMail 支援稽核記錄。如需更新許可的詳細資訊，請參閱 Amazon WorkMail 身分型政策範例和 以取得稽核記錄的相關資訊，請參閱 啟用稽核記錄。	2024 年 2 月 14 日
Amazon WorkMail 開始追蹤變更	Amazon WorkMail 開始追蹤其 AWS 受管政策的變更。	2021 年 3 月 1 日

使用 Amazon WorkMail 的服務連結角色

Amazon WorkMail 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 Amazon WorkMail 的唯一 IAM 角色類型。服務連結角色由 Amazon WorkMail 預先定義，並包含服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 Amazon WorkMail，因為您不必手動新增必要的許可。Amazon WorkMail 會定義其服務連結角色的許可，除非另有定義，否則只有 Amazon WorkMail 可以擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

您必須先刪除相關的 資源，才能刪除服務連結角色。這可保護您的 Amazon WorkMail 資源，因為您不會意外移除存取資源的許可。

如需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與 IAM 搭配使用的 AWS 服務，並尋找具有是的服務。選擇具有連結的 Yes (是)，以檢視該服務的服務連結角色文件。

Amazon WorkMail 的服務連結角色許可

Amazon WorkMail 使用名為 AmazonWorkMailEvents 的服務連結角色 – Amazon WorkMail 使用此服務連結角色來啟用存取由 Amazon WorkMail 事件使用或管理 AWS 的服務和資源，例如監控 CloudWatch 記錄的電子郵件事件。如需為 Amazon WorkMail 啟用電子郵件事件記錄的詳細資訊，請參閱 啟用電子郵件事件記錄。

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

- `events.workmail.amazonaws.com`

角色許可政策允許 Amazon WorkMail 對指定的資源完成下列動作：

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

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、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。

為 Amazon WorkMail 建立服務連結角色

您不需要手動建立一個服務連結角色。當您開啟 Amazon WorkMail 事件記錄並使用 Amazon WorkMail 主控台中的預設設定時，Amazon WorkMail 會為您建立服務連結角色。

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。當您開啟 Amazon WorkMail 事件記錄並使用預設設定時，Amazon WorkMail 會再次為您建立服務連結角色。

編輯 Amazon WorkMail 的服務連結角色

Amazon WorkMail 不允許您編輯 AmazonWorkMailEvents 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。然而，您可使用 IAM 來編輯角色描述。如需更多資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除 Amazon WorkMail 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 如果您嘗試刪除資源時，Amazon WorkMail 服務正在使用 角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

刪除 Amazon WorkMail AmazonWorkMailEvents 資源

1. 關閉 Amazon WorkMail 事件記錄。
   a. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

      如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
   b. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
   c. 在導覽窗格中，選擇組織設定，然後選擇監控。
   d. 針對 Log settings (日誌設定)，選擇 Edit (編輯)。
   e. 將啟用郵件事件滑桿移至關閉位置。
   f. 選擇 Save (儲存)。
2. 刪除 Amazon CloudWatch 日誌群組。
   a. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
   b. 選擇 Logs (日誌)。
   c. 針對 Log Groups (日誌群組)，選取要刪除的日誌群組。
   d. 針對 Actions (動作)，選擇 Delete log group (刪除日誌群組)。
   e. 選擇 是，刪除。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI、 或 AWS API 來刪除 AmazonWorkMailEvents 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。

Amazon WorkMail 服務連結角色的支援區域

Amazon WorkMail 支援在提供服務的所有區域中使用服務連結角色。如需詳細資訊，請參閱 Amazon WorkMail 區域和端點。

在 Amazon WorkMail 中記錄和監控

監控和稽核您的電子郵件和日誌對於維護 Amazon WorkMail 組織的運作狀態至關重要。Amazon WorkMail 支援兩種類型的監控：

- 事件記錄 – 監控組織的電子郵件傳送活動有助於保護您的網域評價。監控也可以協助您追蹤傳送和接收的電子郵件。如需有關如何啟用電子郵件事件日誌的詳細資訊，請參閱啟用電子郵件事件記錄。
- 稽核記錄 – 您可以使用稽核日誌來擷取有關 Amazon WorkMail 組織用量的詳細資訊，例如監控使用者對信箱的存取、稽核可疑活動，以及偵錯存取控制和可用性提供者組態。如需詳細資訊，請參閱啟用稽核記錄。

AWS 提供下列監控工具來監看 Amazon WorkMail、在發生錯誤時報告，以及適時採取自動動作：

- Amazon CloudWatch AWS 會即時監控您的 AWS 資源和您在 上執行的應用程式。例如，當您為 Amazon WorkMail 啟用電子郵件事件記錄時，CloudWatch 可以追蹤為組織傳送和接收的電子郵件。如需使用 CloudWatch 監控 Amazon WorkMail 的詳細資訊，請參閱使用 CloudWatch 指標監控 Amazon WorkMail 。如需有關 CloudWatch 的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》。
- 在 Amazon WorkMail 主控台中啟用電子郵件和稽核記錄時，Amazon Amazon CloudWatch Logs 可讓您監控、存放和存取 Amazon WorkMail 的電子郵件事件和稽核日誌。CloudWatch Logs 可以監控日誌檔案中的資訊，而且您可以將日誌資料封存在高度耐用的儲存體中。如需使用 CloudWatch Logs 追蹤 Amazon WorkMail 訊息的詳細資訊，請參閱 啟用電子郵件事件記錄和 啟用稽核記錄。如需 CloudWatch Logs 的詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》。
- AWS CloudTrail 會擷取 API 呼叫和由 或代表您的 發出的相關事件 AWS 帳戶，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 地址，以及呼叫的時間。如需詳細資訊，請參閱使用 記錄 Amazon WorkMail API 呼叫 AWS CloudTrail。
- Amazon S3 可讓您以符合成本效益的方式存放和存取 Amazon WorkMail 事件。Amazon S3 提供管理事件資料生命週期的機制，可讓您設定自動刪除舊事件，或設定自動封存至 Amazon S3 Glacier。請注意，Amazon S3 交付僅適用於稽核記錄事件。如需 Amazon S3 的詳細資訊，請參閱 Amazon S3 使用者指南。
- Amazon Data Firehose 可讓您將事件資料串流至其他 AWS 服務，例如 Amazon Simple Storage Service (Amazon S3)、Amazon Redshift、Amazon OpenSearch Service、Amazon OpenSearch Serverless、Splunk，以及任何由支援的第三方服務提供者擁有的自訂 HTTP 端點或 HTTP 端點，包括 Datadog、Dynatrace、LogicMonitor、MongoDB、New Relic、Coralogix 和 Elastic。交付至 Firehose 僅適用於稽核記錄事件。如需 Firehose 的詳細資訊，請參閱 Amazon Data Firehose 開發人員指南。

主題

使用 CloudWatch 指標監控 Amazon WorkMail

您可以使用 CloudWatch 監控 Amazon WorkMail，這會收集原始資料並將其處理為可讀且近乎即時的指標。不收費指標會儲存 15 個月，讓您可以存取歷史資訊，以了解 Web 應用程式或服務的效能。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。

Amazon WorkMail 的 CloudWatch 指標

Amazon WorkMail 會將下列指標和維度資訊傳送至 CloudWatch。

`AWS/WorkMail` 命名空間包含下列指標。

指標	描述
`OrganizationEmailReceived`	您的 Amazon WorkMail 組織收到的電子郵件數量。如果一封電子郵件已傳送給組織中的 10 個收件人，則`OrganizationEmailReceived` 計數為 1。 單位：計數
`MailboxEmailDelivered`	傳送至 Amazon WorkMail 組織中個別信箱的電子郵件數量。如果一封電子郵件成功交付給組織中的 10 個收件人，則`MailboxEmailDelivered` 計數為 10。 單位：計數

指標	描述
IncomingEmailBounced	由於完整信箱而退信的傳入電子郵件數量。這個指標會將每個預期收件人計入。例如，如果一個電子郵件傳送給組織中的 10 個收件人，而其中兩個收件人有導致退信回應的完整信箱，則 IncomingEmailBounced 計數為 2。 單位：計數
OutgoingEmailBounced	無法傳送的外寄電子郵件數量。這個指標會將每個預期收件人計入。例如，如果傳送一封電子郵件給 10 個收件人，且無法傳送兩封電子郵件，則OutgoingEmailBounced 計數為 2。 單位：計數
OutgoingEmailSent	從您的 Amazon WorkMail 組織成功傳送的電子郵件數量。此指標會將成功傳送電子郵件的每個收件人計入。例如，如果將 1 封電子郵件傳送給 10 個收件人，而電子郵件已成功傳遞給 8 個收件人，則 OutgoingEmailSent 計數為 8。 單位：計數
AuthenticationFailure	此指標會計算身分驗證嘗試的次數。當身分驗證成功時，計數為 0，而身分驗證失敗時，計數為 1。使用 Sum 統計資料來監控失敗的身分驗證嘗試次數。使用 Sample count 統計資料來監控身分驗證事件的總數。使用 Average 統計資料來監控失敗和成功身分驗證事件的比率。 單位：計數

指標	描述
AccessDenied	此指標會計算存取控制評估的數量。當存取控制拒絕動作時，計數為 1，而授予動作時，計數為 0。使用 Sum 統計資料來監控拒絕動作的磁碟區、監控嘗試動作總數的Sample count統計資料，以及監控允許和拒絕動作比率的Average統計資料。 單位：計數
ActionDenied	當信箱資料有動作時，會計算此指標。拒絕動作時，計數為 1，如果授予動作，計數為 0。使用 Sum 統計資料來監控拒絕信箱動作的磁碟區、監控嘗試信箱動作總數的Sample count統計資料，以及監控允許和拒絕動作比率的Average統計資料。 單位：計數
AvailabilityProviderFailure	此指標會計入 Amazon WorkMail 執行的每個可用性提供者請求，以從外部來源擷取行事曆可用性。如需可用性提供者的詳細資訊，請參閱 Amazon WorkMail 管理員指南。

監控 Amazon WorkMail 電子郵件事件日誌

當您開啟 Amazon WorkMail 組織的電子郵件事件記錄時，Amazon WorkMail 會使用 CloudWatch 記錄電子郵件事件。如需啟用電子郵件事件記錄的詳細資訊，請參閱 啟用電子郵件事件記錄。

下表說明 Amazon WorkMail 使用 CloudWatch 記錄的事件、事件傳送的時間，以及事件欄位包含的內容。

ORGANIZATION_EMAIL_RECEIVED

當您的 Amazon WorkMail 組織收到電子郵件訊息時，會記錄此事件。

欄位	描述
recipients	訊息的預期收件人。
寄件者	代表另一位使用者傳送電子郵件訊息的使用者的電子郵件地址。僅在代表其他使用者傳送電子郵件時，才會出現此欄位。
from	From (寄件人) 地址通常是傳送訊息的使用者電子郵件地址。若使用者代表另一位使用者傳送訊息，則此欄位會回傳授權使用者的電子郵件地址，而非實際寄件者的電子郵件地址。
subject	電子郵件訊息主旨。
messageId	SMTP 訊息 ID。
spamVerdict	指示訊息是否由 Amazon SES 標示為垃圾郵件。如需詳細資訊，請參閱《Amazon Simple Email Service 開發人員指南》中的 Amazon SES Email Receiving 通知內容。
dkimVerdict	指出網域金鑰識別郵件 (DKIM) 檢查是否通過。如需詳細資訊，請參閱《Amazon Simple Email Service 開發人員指南》中的 Amazon SES Email Receiving 通知內容。
dmarcVerdict	指出是否通過以網域為基礎的訊息驗證、報告和一致性 (DMARC) 檢查。如需詳細資訊，請參閱《Amazon Simple Email Service 開發人員指南》中的 Amazon SES Email Receiving 通知內容。
dmarcPolicy	只有當 dmarcVerdict 欄位包含「失敗」時才會出現。指示 DMARC 檢查失敗時 (無、隔離或拒絕) 電子郵件要採取的動作。這是由傳送電子郵件網域的擁有者所設定。

欄位	描述
spfVerdict	指出寄件者政策架構 (SPF) 檢查是否通過。如需詳細資訊，請參閱《Amazon SES Email Service 開發人員指南》中的 Amazon SES Email Receiving 通知內容。
messageTimestamp	指出收到訊息的時間。

MAILBOX_EMAIL_DELIVERED

當訊息傳遞到您組織中的信箱時，系統即會記錄此事件。系統會為訊息傳遞目標的每個信箱記錄一次事件，因此，單一的 ORGANIZATION_EMAIL_RECEIVED 事件可能導致多個 MAILBOX_EMAIL_DELIVERED 事件。

欄位	描述
recipient	傳遞訊息的目標信箱。
folder	放置訊息的信箱資料夾。

RULE_APPLIED

當傳入或傳出訊息啟動電子郵件流程規則時，會記錄此事件。

欄位	描述
ruleName	規則的名稱。
ruleType	套用的規則類型 (INBOUND_RULE、OUTBOUND_RULE 或 MAILBOX_RULE)。傳入和傳出規則適用於您的 Amazon WorkMail 組織。信箱規則僅適用指定的信箱。如需詳細資訊，請參閱管理電子郵件流程。

欄位	描述
ruleActions	根據規則採取的動作。訊息的不同收件人可能會有不同的動作，例如退回的電子郵件或成功傳遞的電子郵件。
targetFolder	適用於 Move 或 Copy MAILBOX_RULE 的預期目的地資料夾。
targetRecipient	適用於 Forward 或 Redirect MAILBOX_RULE 的預期收件人。

JOURNALING_INITIATED

當 Amazon WorkMail 傳送電子郵件至您的組織管理員指定的日誌記錄地址時，會記錄此事件。只有在為您的組織設定日誌登載時，才會加以傳輸。如需詳細資訊，請參閱搭配 Amazon WorkMail 使用電子郵件日誌。

欄位	描述
journalingAddress	日誌登載訊息的傳送目標電子郵件地址。

INCOMING_EMAIL_BOUNCED

當傳入訊息無法交付給目標收件人時，會記錄此事件。電子郵件可能會因為多種原因而退信，例如完整目標信箱。系統會為每個收件人記錄此事件一次，導致退信的電子郵件。例如，如果將內送訊息傳送給三個收件人，而其中兩個的信箱已滿載，則會記錄兩個 INCOMING_EMAIL_BOUNCED 事件。

欄位	描述
bouncedRecipient	Amazon WorkMail 退信訊息的目標收件人。

OUTGOING_EMAIL_SUBMITTED

當您組織中的使用者提交要傳送的電子郵件訊息時，系統即會記錄此事件。這會在訊息離開 Amazon WorkMail 之前記錄，因此此事件不會指出電子郵件是否已成功交付。

欄位	描述
recipients	寄件者指定的訊息收件人。包含收件者、副本和密件副本行的所有收件人。
寄件者	代表另一位使用者傳送電子郵件訊息的使用者的電子郵件地址。僅在代表其他使用者傳送電子郵件時，才會出現此欄位。
from	From (寄件人) 地址通常是傳送訊息的使用者電子郵件地址。若使用者代表另一位使用者傳送訊息，則此欄位會回傳授權使用者的電子郵件地址，而非實際寄件者的電子郵件地址。
subject	電子郵件訊息主旨。

OUTGOING_EMAIL_SENT

當系統將外寄電子郵件成功傳遞給目標收件人時，即會記錄這個事件。系統會為每個成功收件人記錄一次事件，因此，單一 OUTGOING_EMAIL_SUBMITTED 可以產生多個 OUTGOING_EMAIL_SENT 項目。

欄位	描述
recipient	成功傳遞電子郵件的收件人。
寄件者	代表另一位使用者傳送電子郵件訊息的使用者的電子郵件地址。僅在代表其他使用者傳送電子郵件時，才會出現此欄位。
from	From (寄件人) 地址通常是傳送訊息的使用者電子郵件地址。若使用者代表另一位使用者傳送訊息，則此欄位會回傳授權使用者的電子郵件地址，而非實際寄件者的電子郵件地址。
messageId	SMTP 訊息 ID。

OUTGOING_EMAIL_BOUNCED

當外寄訊息無法傳遞給目標收件人時，會記錄此事件。電子郵件可能會因為多種原因而退信，例如完整目標信箱。系統會記錄導致退信電子郵件的每個收件人的退信。例如，如果將外寄訊息傳送給三個收件人，而其中兩個的信箱已滿載，則會記錄兩個 OUTGOING_EMAIL_BOUNCED 事件。

欄位	描述
bouncedRecipient	退回訊息的目的地郵件伺服器的預期收件人。

DMARC_POLICY_APPLIED

將 DMARC 政策套用至傳送至組織的電子郵件時，會記錄此事件。

欄位	描述
from	From (寄件人) 地址通常是傳送訊息的使用者電子郵件地址。若使用者代表另一位使用者傳送訊息，則此欄位會回傳授權使用者的電子郵件地址，而非實際寄件者的電子郵件地址。
recipients	訊息的預期收件人。
政策	套用的 DMARC 政策，會指示 DMARC 檢查失敗 (無、隔離或拒絕) 時對電子郵件採取的動作。這與 ORGANIZATION_EMAIL_RECEIVED 事件中 dmarcPolicy 欄位相同。

監控 Amazon WorkMail 稽核日誌

您可以使用稽核日誌來監控對 Amazon WorkMail Organization 信箱的存取。Amazon WorkMail 會記錄五種類型的稽核事件，這些事件可以發佈到 CloudWatch Logs、Amazon S3 或 Amazon Firehouse。您可以使用稽核日誌來監控使用者與組織信箱的互動、身分驗證嘗試、存取控制規則評估，以及對外部系統執行可用性提供者呼叫，並使用個人存取字符監控事件。如需設定稽核記錄的資訊，請參閱 啟用稽核記錄。

下列各節說明 Amazon WorkMail 記錄的稽核事件、事件傳送的時間，以及事件欄位的相關資訊。

信箱存取日誌

信箱存取事件提供有關對哪個信箱物件採取（或嘗試）動作的資訊。針對您嘗試在信箱中的項目或資料夾上執行的每個操作，都會產生信箱存取事件。這些事件對於稽核信箱資料的存取權很有用。

欄位	描述
event_timestamp	當事件發生時，從 Unix epoch 開始，以毫秒為單位。
request_id	唯一識別請求的 ID。
organization_arn	已驗證使用者所屬的 & Amazon WorkMail Organization 的 ARN。
user_id	已驗證使用者的 ID。
impersonator_id	模擬工具的 ID。只有在請求使用模擬功能時才會顯示。
protocol	使用的通訊協定。通訊協定可以是：AutoDiscover 、EWS、IMAP、WindowsOutlook 、ActiveSync 、SMTPWebMail、IncomingEmail 、 或 OutgoingEmail 。
source_ip	請求的來源 IP 位址。
user_agent	提出請求的使用者代理程式。
動作	針對 物件採取的動作可以是：read、read_hierarchy 、read_summary 、read_attachment 、read_permissions create、、update、update_permissions update_read_state 、delete、、submit_email_for_sending 、abort_sen

欄位	描述
	ding_email 、、move、、 move_to copy或 copy_to。
owner_id	擁有要對其採取行動之物件的使用者 ID。
object_type	物件類型，可以是：資料夾、訊息或附件。
item_id	唯一識別訊息的 ID，該訊息是事件的主旨，或包含該事件主旨的附件。
資料夾路徑	要執行動作之資料夾的路徑，或包含要執行動作之項目的資料夾路徑。
folder_id	此 ID 可唯一識別作為事件主體的資料夾，或包含作為事件主體的物件。
attachment_path	受影響附件的顯示名稱路徑。
action_allowed	是否允許 動作。可以是 true 或 false。

存取控制日誌

存取控制事件會在評估存取控制規則時產生。這些日誌適用於稽核禁止存取或偵錯存取控制組態。

欄位	描述
event_timestamp	事件發生時，在 Unix epoch 後的幾毫秒內。
request_id	唯一識別請求的 ID。
organization_arn	已驗證使用者所屬之 WorkMail Organization 的 ARN。
user_id	已驗證使用者的 ID。
impersonator_id	模擬者的 ID。只有在請求使用模擬功能時才會顯示。

欄位	描述
protocol	使用的通訊協定，可以是：AutoDiscover 、EWS、IMAP、WindowsOutlook ActiveSync 、SMTP、、WebMail、IncomingEmail 或 OutgoingEmail 。
source_ip	請求的來源 IP 位址。
scope	規則的範圍，可以是：DeviceAccessControl 、 AccessControl 或 ImpersonationAccessControl 。
rule_id	相符存取控制規則的 ID。沒有相符的規則時，將無法使用 rule_id。
access_granted	是否允許存取。可以是 true 或 false。

身分驗證日誌

身分驗證事件包含身分驗證嘗試的相關資訊。

> **Note**
> 透過 Amazon WorkMail WebMail 應用程式對身分驗證事件不會產生身分驗證事件。

欄位	描述
event_timestamp	事件發生時，在 Unix epoch 後的幾毫秒內。
request_id	唯一識別請求的 ID。
organization_arn	已驗證使用者所屬之 WorkMail Organization 的 ARN。
user_id	已驗證使用者的 ID。

欄位	描述
使用者	嘗試進行身分驗證的使用者名稱。
protocol	使用的通訊協定，可以是：`AutoDiscover` 、EWS、IMAP、`WindowsOutlook ActiveSync` 、SMTP、、WebMail、`IncomingEmail` 或 `OutgoingEmail` 。
source_ip	請求的來源 IP 位址。
user_agent	提出請求的使用者代理程式。
方法	驗證方法。目前僅支援基本 。
auth_successful	驗證嘗試是否成功。可以是 true 或 false。
auth_failed_reason	驗證失敗的原因。只有在驗證失敗時才會顯示。
personal_access_token_id	用於身分驗證之個人存取字符的 ID。

個人存取字符日誌

每次嘗試建立或刪除個人存取權杖時，都會產生個人存取權杖 (PAT) 事件。個人存取字符事件提供有關使用者是否成功建立個人存取字符的資訊。個人存取字符日誌對於稽核建立和刪除自己的 PATs的最終使用者很有用。使用個人存取字符登入的使用者將在現有的身分驗證日誌中產生事件。如需詳細資訊，請參閱身分驗證日誌 。

欄位	描述
event_timestamp	事件發生時，在 Unix epoch 後的幾毫秒內。
request_id	唯一識別請求的 ID。
organization_arn	已驗證使用者所屬之 WorkMail Organization 的 ARN。
user_id	已驗證使用者的 ID。

欄位	描述
使用者	採取此動作之使用者的使用者名稱。
protocol	透過 動作使用的通訊協定已發生，可以是：Webapp
source_ip	請求的來源 IP 位址。
user_agent	提出請求的使用者代理程式。
動作	個人存取字符的動作，可以是：建立或刪除。
name	個人存取字符的名稱。
expires_time	個人存取權杖過期的日期。
範圍	信箱上個人存取權杖許可的範圍。

可用性提供者日誌

每個 Amazon WorkMail 代表您向設定的可用性提供者提出的可用性請求都會產生可用性提供者事件。這些事件有助於偵錯您的可用性提供者組態。

欄位	描述
event_timestamp	事件發生時，在 Unix epoch 後的幾毫秒內。
request_id	唯一識別請求的 ID。
organization_arn	已驗證使用者所屬之 WorkMail Organization 的 ARN。
user_id	已驗證使用者的 ID。
type	要叫用的可用性提供者類型，可以是： `EWS`或 `LAMBDA`。
domain	取得可用性的網域。

欄位	描述
function_arn	如果類型為 LAMBDA，則叫用 Lambda 的 ARN。否則，此欄位不存在。
ews_endpoint	EWS 端點的類型為 EWS。否則，此欄位不存在。
error_message	說明失敗原因的訊息。如果請求成功，則此欄位不存在。
availability_event_successful	是否成功提供可用性請求。

搭配 Amazon WorkMail 使用 CloudWatch Insights

如果您在 Amazon WorkMail 主控台中開啟電子郵件事件記錄，或已啟用稽核日誌傳送至 CloudWatch Logs，您可以使用 Amazon CloudWatch Logs Insights 來查詢您的事件日誌。如需啟用電子郵件事件記錄的詳細資訊，請參閱 啟用電子郵件事件記錄。如需 CloudWatch Logs Insights 的詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的使用 CloudWatch Logs Insights 分析日誌資料。Amazon CloudWatch

下列範例示範如何查詢 CloudWatch Logs 是否有常見的電子郵件事件。您可以在 CloudWatch 主控台中執行這些查詢。如需如何執行這些查詢的說明，請參閱《Amazon CloudWatch Logs 使用者指南》中的教學課程：執行和修改範例查詢。

Example 了解為什麼使用者 B 未收到使用者 A 傳送的電子郵件。

以下程式碼範例示範如何查詢使用者 A 傳送給使用者 B 的外寄電子郵件，依時間戳記排序。

```
fields @timestamp, traceId

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

這會傳回已傳送訊息和追蹤 ID。使用以下程式碼範例中的追蹤 ID 來查詢已傳送訊息的事件日誌。

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

```
| sort @timestamp asc
| filter traceId = "$TRACEID"
```

這會傳回電子郵件訊息 ID 和電子郵件事件。OUTGOING_EMAIL_SENT 指出已傳送電子郵件。OUTGOING_EMAIL_BOUNCED 指出已退回電子郵件。若要查看是否已收到電子郵件，請在以下程式碼範例中使用訊息 ID 來查詢。

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

這應該也會傳回收到的訊息，因為訊息 ID 是一樣的。在以下程式碼範例中使用追蹤 ID 來查詢傳遞。

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

這會傳回傳遞動作和任何適用的規則動作。

Example 查看從使用者或網域收到的所有郵件

以下程式碼範例示範如何查詢從指定使用者收到的所有郵件。

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

以下程式碼範例示範如何查詢從指定網域收到的所有郵件。

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

Example 查看誰傳送了退信電子郵件

以下程式碼範例示範如何查詢退回的外寄電子郵件，同時傳回退回的原因。

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

下列程式碼範例示範如何查詢退信的傳入電子郵件。它也會傳回退信收件人的電子郵件地址，以及跳躍的原因。

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

Example 查看要傳送垃圾郵件的網域

以下程式碼範例示範如何查詢組織中接收垃圾郵件的收件人。

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

以下程式碼範例示範如何查詢垃圾電子郵件的寄件者。

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

Example 了解電子郵件為何傳送至收件人的垃圾郵件資料夾

以下程式碼範例示範如何查詢被識別為垃圾郵件的電子郵件，依主旨篩選。

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

您也可以依電子郵件追蹤 ID 查詢，以查看電子郵件的所有事件。

Example 查看符合電子郵件流程規則的電子郵件

以下程式碼範例示範如何查詢符合傳出電子郵件流程規則的電子郵件。

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

以下程式碼範例示範如何查詢符合傳入電子郵件流程規則的電子郵件。

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

Example 查看您的組織接收或傳送的電子郵件數量

以下程式碼範例示範如何查詢組織中每個收件人接收的電子郵件數量。

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

以下程式碼範例示範如何查詢組織中每個寄件者傳送的電子郵件數量。

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

使用 記錄 Amazon WorkMail API 呼叫 AWS CloudTrail

Amazon WorkMail 已與 整合 AWS CloudTrail，此服務提供 Amazon WorkMail AWS 服務 中使用者、角色或 所採取動作的記錄。CloudTrail 會將 Amazon WorkMail 的所有 API 呼叫擷取為事件，包括來自 Amazon WorkMail 主控台的呼叫，以及來自對 Amazon WorkMail APIs 的程式碼呼叫。如果您建立線索，您可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Amazon WorkMail 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。使用 CloudTrail 收集的資訊，您可以判斷對 Amazon WorkMail 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱「AWS CloudTrail 使用者指南」。

CloudTrail 中的 Amazon WorkMail 資訊

建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當活動在 Amazon WorkMail 中發生時，該活動會記錄於 CloudTrail 事件，以及事件歷史記錄中的其他 AWS 服務 事件。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄檢視事件。

若要持續記錄您 AWS 帳戶中的事件，包括 Amazon WorkMail 的事件，您必須建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 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，您可以設定其他 AWS 服務，以進一步分析 CloudTrail 日誌中收集的事件資料並對其採取行動。如需詳細資訊，請參閱：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案及接收多個帳戶的 CloudTrail 日誌檔案

所有 Amazon WorkMail 動作都會由 CloudTrail 記錄，並記錄在 Amazon WorkMail API 參考中。例如，對 `CreateUser`、 `CreateAlias`和 `GetRawMessageContent` API 操作的呼叫會在 CloudTrail 日誌檔案中產生項目。

每一筆事件或日誌專案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：

- 該請求是否使用根或 IAM 使用者憑證提出。
- 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。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

了解 Amazon WorkMail 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

下列範例顯示 CloudTrail 日誌項目，示範來自 Amazon WorkMail API `CreateUser`的動作。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T17:49:59Z",
  "eventSource": "workmail.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "name": "janedoe",
    "displayName": "Jane Doe",
    "organizationId": "m-5b1c980000EXAMPLE"
  },
  "responseElements": {
    "userId": "a3a9176d-EXAMPLE"
  },
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

下列範例顯示 CloudTrail 日誌項目，示範來自 Amazon WorkMail API `CreateAlias`的動作。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "WMSDK"
  },
```

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

下列範例顯示 CloudTrail 日誌項目，示範來自 Amazon WorkMail 訊息流程 API GetRawMessageContent的動作。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111111111111:user/WMSDK",
    "accountId": "111111111111",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "WMSDK"
  },
  "eventTime": "2017-12-12T18:13:44Z",
  "eventSource": "workmailMessageFlow.amazonaws.com",
  "eventName": "GetRawMessageContent",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "203.0.113.12",
  "userAgent": "aws-sdk-java/1.11.205 Mac_OS_X/10.11.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.151-b12 java/1.8.0_151",
  "requestParameters": {
    "messageId": "123A4A5A-67B8-90C1-D23E-45FG67H890J1"
  },
  "responseElements": null,
```

```
  "requestID": "dec81e4a-EXAMPLE",
  "eventID": "9f2f09c5-EXAMPLE",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "recipientAccountId": "111111111111"
}
```

啟用電子郵件事件記錄

您可以在 Amazon WorkMail 主控台中啟用電子郵件事件記錄，以追蹤組織的電子郵件訊息。電子郵件事件記錄使用 AWS Identity and Access Management 服務連結角色 (SLR) 來授予許可，將電子郵件事件日誌發佈至 Amazon CloudWatch。如需 IAM 服務連結角色的詳細資訊，請參閱使用 Amazon WorkMail 的服務連結角色。

在 CloudWatch 事件日誌中，您可以使用 CloudWatch 搜尋工具和指標來追蹤訊息和疑難排解電子郵件問題。如需 Amazon WorkMail 傳送至 CloudWatch 之事件日誌的詳細資訊，請參閱 監控 Amazon WorkMail 電子郵件事件日誌。如需 CloudWatch Logs 的詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》。

主題

啟用電子郵件事件記錄

當您使用預設設定 Amazon WorkMail 開啟電子郵件事件記錄時，會發生下列情況：

- 建立 AWS Identity and Access Management 服務連結角色 – `AmazonWorkMailEvents`。
- 建立 CloudWatch 日誌群組 – `/aws/workmail/emailevents/`*`organization-alias`*。
- 將 CloudWatch 日誌保留設定為 30 天。

啟用電子郵件事件記錄

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。

2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇記錄設定。
4. 選擇電子郵件流程日誌設定索引標籤。
5. 在電子郵件流程日誌設定區段中，選擇編輯。
6. 將啟用郵件事件滑桿移至開啟位置。
7. 執行以下任意一項：

   - （建議）選擇使用預設設定。
   - （選用）清除使用預設設定，然後從出現的清單中選取目的地日誌群組和 IAM 角色。

   > **Note**
   >
   > 只有在您已使用 建立日誌群組和自訂 IAM 角色時，才選擇此選項 AWS CLI。如需詳細資訊，請參閱建立電子郵件事件記錄的自訂日誌群組和 IAM 角色。

8. 選取我授權 Amazon WorkMail 使用此組態在我的帳戶中發佈日誌。
9. 選擇 Save (儲存)。

建立電子郵件事件記錄的自訂日誌群組和 IAM 角色

為 Amazon WorkMail 啟用電子郵件事件記錄時，建議使用預設設定。如果您需要自訂監控組態，您可以使用 來 AWS CLI 建立專用日誌群組和電子郵件事件記錄的自訂 IAM 角色。

建立電子郵件事件記錄的自訂日誌群組和 IAM 角色

1. 使用下列 AWS CLI 命令，在與您的 Amazon WorkMail 組織相同的 AWS 區域中建立日誌群組。如需詳細資訊，請參閱 AWS CLI 命令參考中的 create-log-group。

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

2. 建立包含以下政策的檔案：

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

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

3. 使用下列 AWS CLI 命令來建立 IAM 角色，並將此檔案附加為角色政策文件。如需詳細資訊，請參閱《AWS CLI 命令參考》中的《create-role》。

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

> **Note**
>
> 如果您是 WorkMailFullAccess 受管政策使用者，您必須在角色名稱workmail中包含術語。此受管政策僅允許您使用名稱中包含 workmail 的角色來設定電子郵件事件日誌。如需詳細資訊，請參閱《IAM 使用者指南》中的授予使用者將角色傳遞至 AWS 服務的許可。

4. 建立檔案，其中包含您在上一個步驟中建立的 IAM 角色政策。此政策至少必須將建立日誌串流的許可授與至該角色，並將日誌事件放到您在步驟 1 中建立的日誌群組。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:us-east-1:111122223333:log-group:workmail-
monitoring*"
        }
    ]
}
```

5. 使用以下 AWS CLI 命令將政策檔案連接至 IAM 角色。如需詳細資訊，請參閱 AWS CLI 命令參考中的 put-role-policy。

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

關閉電子郵件事件日誌

從 Amazon WorkMail 主控台關閉電子郵件事件記錄。如果您不再需要使用電子郵件事件記錄，我們建議您同時刪除相關的 CloudWatch 日誌群組和服務連結角色。如需詳細資訊，請參閱刪除 Amazon WorkMail 的服務連結角色。

關閉電子郵件事件日誌

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 Monitoring (監控)。
4. 在日誌設定區段中，選擇編輯。
5. 將啟用郵件事件滑桿移至關閉位置。
6. 選擇 Save (儲存)。

預防跨服務混淆代理人

混淆代理人問題屬於安全性問題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在 中 AWS，跨服務模擬可能會導致混淆代理人問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。

呼叫服務可以被操縱，以使用其許可來對其他客戶的資源採取行動，否則就沒有存取許可。

為了防止這種情況， AWS 提供工具，協助您保護所有 服務的資料，讓 服務主體能夠存取您帳戶中的資源。

我們建議在資源政策中使用 `aws:SourceArn` 和 `aws:SourceAccount` 全域條件內容金鑰，以限制 CloudWatch Logs 和 Amazon S3 授予給正在產生日誌的服務的許可。如果您使用兩個全域條件內容索引鍵，則值在相同政策陳述式中使用時必須使用相同的帳戶 ID。

aws:SourceArn 的值必須是正在產生日誌之傳遞資源的 ARN。

防範混淆代理人問題的最有效方法是使用 aws:SourceArn 全域條件內容索引鍵，以及資源的完整 ARN。如果不知道資源的完整 ARN，或者如果您指定了多個資源，請使用 aws:SourceArn 全域條件內容索引鍵，同時使用萬用字元 (*) 表示 ARN 的未知部分。

啟用稽核記錄

您可以使用稽核日誌來擷取 Amazon WorkMail 組織用量的詳細資訊。稽核日誌可用來監控使用者對信箱的存取、稽核可疑活動，以及偵錯存取控制和可用性提供者組態。

> **Note**
>
> AmazonWorkMailFullAccess 受管政策不包含管理日誌交付所需的所有必要許可。如果您使用此政策來管理 WorkMail，請確定用於設定日誌交付的委託人（例如，擔任的角色）也具有所有必要的許可。

Amazon WorkMail 支援稽核日誌的三個交付目的地：CloudWatch Logs、Amazon S3 和 Amazon Data Firehose。如需詳細資訊，請參閱《Amazon CloudWatch Logs 使用者指南》中的需要額外許可【V2】的日誌。

除了在需要其他許可【V2】的日誌中列出的許可之外，Amazon WorkMail 還需要額外的許可來設定日誌交付：workmail:AllowVendedLogDeliveryForResource。

工作日誌交付包含三個元素：

- DeliverySource，一種邏輯物件，代表傳送日誌的資源。對於 Amazon WorkMail，它是 Amazon WorkMail Organization。
- DeliveryDestination，這是代表實際交付目的地的邏輯物件。
- 交付，將交付來源連接到交付目的地。

若要設定 Amazon WorkMail 與目的地之間的日誌傳遞，您可以執行下列動作：

- 使用 PutDeliverySource 建立交付來源。
- 使用 PutDeliveryDestination 建立交付目的地。
- 如果您要跨帳戶交付日誌，則必須在目的地帳戶中使用 PutDeliveryDestinationPolicy 將 IAM 政策指派給目的地。此政策授權從帳戶 A 中的交付來源建立交付至帳戶 B 中的交付目的地。

- 使用 CreateDelivery 完全配對一個交付來源和一個交付目的地，以建立交付。

下列各節提供您在登入時必須擁有的許可詳細資訊，以設定將日誌交付到每種類型的目的地。這些許可可以授予您登入的 IAM 角色。

> **Important**
>
> 刪除日誌產生資源後，您有責任移除日誌交付資源。

若要在刪除日誌產生資源後移除日誌交付資源，請遵循下列步驟。

1. 使用 DeleteDelivery 操作刪除交付。
2. 使用 DeliverySource 操作刪除 DeliverySource。 DeleteDeliverySource
3. 如果與您剛刪除的 DeliverySource 相關聯的 DeliveryDestination 僅用於此特定的 DeliverySource，則您可以使用 DeleteDeliveryDestinations 操作將其移除。

使用 Amazon WorkMail 主控台設定稽核記錄

您可以在 Amazon WorkMail 主控台中設定稽核記錄：

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選取區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 選擇記錄設定。
4. 選擇稽核日誌設定索引標籤。
5. 使用適當的小工具設定所需日誌類型的交付。
6. 選擇 Save (儲存)。

傳送至 CloudWatch Logs 的日誌

使用者許可

若要啟用傳送日誌至 CloudWatch Logs，您登入時必須具有以下許可。

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

```
                "logs:DescribeLogGroups"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:*"
            ]
        }
        {
            "Sid":"AllowLogDeliveryForWorkMail",
            "Effect":"Allow",
            "Action":[
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource":[
                "arn:aws:workmail:region:account-id:organization/organization-id"
            ]
        }
    ]
}
```

日誌群組和資源政策

日誌送往的日誌群組必須具有包含特定許可的資源政策。如果日誌群組目前沒有資源政策，且設定日誌的使用者具有日誌群組的 `logs:PutResourcePolicy`、 `logs:DescribeResourcePolicies`和 `logs:DescribeLogGroups`許可，則當您開始將日誌傳送至 CloudWatch Logs 時， AWS 會自動為其建立下列政策。

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"AWSLogDeliveryWrite20150319",
            "Effect":"Allow",
            "Principal":{
                "Service":[
                    "delivery.logs.amazonaws.com"
                ]
            },
            "Action":[
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource":[
                "arn:aws:logs:region:account-id:log-group:my-log-group:log-stream:*"
```

```
            ],
            "Condition":{
                "StringEquals":{
                    "aws:SourceAccount":[
                        "account-id"
                    ]
                },
                "ArnLike":{
                    "aws:SourceArn":[
                        "arn:aws:logs:region:account-id:*"
                    ]
                }
            }
        }
    ]
}
```

日誌群組資源政策大小限制考量

這些服務必須在資源政策中列出其傳送日誌的每個日誌群組。CloudWatch Logs 資源政策限制為 5，120 個字元。傳送日誌至大量日誌群組的服務可能會達到此限制。

為了緩解這種情況，CloudWatch Logs 會監控傳送日誌之服務所使用的資源政策大小。當偵測到政策接近 5，120 個字元的大小限制時，CloudWatch Logs 會在該服務的資源政策/aws/vendedlogs/*中自動啟用 。然後，您就可以開始使用名稱開頭為 /aws/vendedlogs/ 的日誌群組，作為這些服務的日誌目的地。

傳送至 Amazon S3 的日誌

使用者許可

若要啟用傳送日誌至 Amazon S3，您登入時必須具有以下許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
```

```
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:delivery:*",
                "arn:aws:logs:region:account-id:delivery-source:*",
                "arn:aws:logs:region:account-id:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyS3",
            "Effect": "Allow",
            "Action": [
                "s3:PutBucketPolicy",
                "s3:GetBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
        }
          {
            "Sid":"AllowLogDeliveryForWorkMail",
            "Effect":"Allow",
            "Action":[
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource":[
                "arn:aws:workmail:region:account-id:organization/organization-id"
```

```
            ]
        }
    ]
}
```

日誌送往的 S3 儲存貯體必須具有包含特定許可的資源政策。如果儲存貯體目前沒有資源政策，且設定記錄的使用者具有儲存貯體的 S3:GetBucketPolicy和 S3:PutBucketPolicy許可，則 AWS 當您開始將日誌傳送至 Amazon S3 時， 會自動為其建立下列政策。

```
{
    "Version":"2012-10-17",
    "Id":"AWSLogDeliveryWrite20150319",
    "Statement":[
        {
            "Sid":"AWSLogDeliveryAclCheck",
            "Effect":"Allow",
            "Principal":{
                "Service":"delivery.logs.amazonaws.com"
            },
            "Action":"s3:GetBucketAcl",
            "Resource":"arn:aws:s3:::my-bucket",
            "Condition":{
                "StringEquals":{
                    "aws:SourceAccount":[
                        "account-id"
                    ]
                },
                "ArnLike":{
                    "aws:SourceArn":[
                        "arn:aws:logs:region:account-id:delivery-source:*"
                    ]
                }
            }
        },
        {
            "Sid":"AWSLogDeliveryWrite",
            "Effect":"Allow",
            "Principal":{
                "Service":"delivery.logs.amazonaws.com"
            },
            "Action":"s3:PutObject",
            "Resource":"arn:aws:s3:::my-bucket/AWSLogs/account-id/*",
            "Condition":{
```

```
                "StringEquals":{
                    "s3:x-amz-acl":"bucket-owner-full-control",
                    "aws:SourceAccount":[
                        "account-id"
                    ]
                },
                "ArnLike":{
                    "aws:SourceArn":[
                        "arn:aws:logs:region:account-id:delivery-source:*"
                    ]
                }
            }
        }
    ]
}
```

在先前的政策中，針對 aws:SourceAccount，指定要交付至此儲存貯體之日誌的帳戶 IDs 清單。對於 aws:SourceArn，指定產生日誌之資源的 ARN 清單，格式為 arn:aws:logs:*source-region*:*source-account-id*:*。

如果儲存貯體具有資源政策，但該政策不包含先前政策中顯示的陳述式，且設定記錄的使用者具有儲存貯體的 S3:GetBucketPolicy和 S3:PutBucketPolicy許可，則該陳述式會附加到儲存貯體的資源政策。

> **Note**
>
> 在某些情況下， AWS CloudTrail 如果尚未將s3:ListBucket許可授予 ，您可能會在 中看到AccessDenied錯誤delivery.logs.amazonaws.com。若要避免 CloudTrail 日誌中的這些錯誤，您必須將s3:ListBucket許可授予 delivery.logs.amazonaws.com。您還必須在上述儲存貯體政策中包含與s3:GetBucketAcl許可集一起顯示的Condition參數。若要簡化此作業，您可以直接將 更新AWSLogDeliveryAclCheck為 Statement，而不是建立新的 “Action”: [“s3:GetBucketAcl”, “s3:ListBucket”]。

Amazon S3 儲存貯體伺服器端加密

您可以使用 Amazon S3 S3-managed金鑰 (SSE-S3) 啟用伺服器端加密，或使用 AWS Key Management Service (SSE-KMS) 中存放的 AWS KMS 金鑰啟用伺服器端加密，來保護 Amazon S3 儲存貯體中的資料。如需詳細資訊，請參閱使用伺服器端加密保護資料。

如果您選擇 SSE-S3，則不需要其他組態。Amazon S3 會處理加密金鑰。

> **Warning**
>
> 如果您選擇 SSE-KMS，您必須使用客戶受管金鑰，因為此案例 AWS 受管金鑰 不支援使用 。如果您使用 AWS 受管金鑰設定加密，日誌將以無法讀取的格式交付。

當您使用客戶受管 AWS KMS 金鑰時，您可以在啟用儲存貯體加密時指定客戶受管金鑰的 Amazon Resource Name (ARN)。將下列項目新增至客戶受管金鑰的金鑰政策（而非 S3 儲存貯體的儲存貯體政策），讓日誌交付帳戶可以寫入 S3 儲存貯體。

如果您選擇 SSE-KMS，您必須使用客戶受管金鑰，因為此案例不支援使用 AWS 受管金鑰。當您使用客戶受管 AWS KMS 金鑰時，您可以在啟用儲存貯體加密時指定客戶受管金鑰的 Amazon Resource Name (ARN)。將下列項目新增至客戶受管金鑰的金鑰政策（而非 S3 儲存貯體的儲存貯體政策），讓日誌交付帳戶可以寫入 S3 儲存貯體。

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

```
    }
}
```

針對 aws:SourceAccount，指定要交付日誌到此儲存貯體的帳戶 IDs 清單。對於 aws:SourceArn，指定產生日誌之資源的 ARN 清單，格式為 arn:aws:logs:*source-region*:*source-account-id*:*。

傳送至 Firehose 的日誌

使用者許可

若要啟用傳送日誌至 Firehose，您必須使用以下許可登入。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
                "logs:GetDelivery",
                "logs:GetDeliverySource",
                "logs:PutDeliveryDestination",
                "logs:GetDeliveryDestinationPolicy",
                "logs:DeleteDeliverySource",
                "logs:PutDeliveryDestinationPolicy",
                "logs:CreateDelivery",
                "logs:GetDeliveryDestination",
                "logs:PutDeliverySource",
                "logs:DeleteDeliveryDestination",
                "logs:DeleteDeliveryDestinationPolicy",
                "logs:DeleteDelivery"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:delivery:*",
                "arn:aws:logs:region:account-id:delivery-source:*",
                "arn:aws:logs:region:account-id:delivery-destination:*"
            ]
        },
        {
            "Sid": "ListAccessForLogDeliveryActions",
            "Effect": "Allow",
            "Action": [
```

```
                "logs:DescribeDeliveryDestinations",
                "logs:DescribeDeliverySources",
                "logs:DescribeDeliveries",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUpdatesToResourcePolicyFH",
            "Effect": "Allow",
            "Action": [
                "firehose:TagDeliveryStream"
            ],
            "Resource": [
                "arn:aws:firehose:region:account-id:deliverystream/*"
            ]
        },
        {
            "Sid": "CreateServiceLinkedRole",
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "arn:aws:iam::account-id:role/aws-service-role/
delivery.logs.amazonaws.com/AWSServiceRoleForLogDelivery"
        }
           {
            "Sid":"AllowLogDeliveryForWorkMail",
            "Effect":"Allow",
            "Action":[
                "workmail:AllowVendedLogDeliveryForResource"
            ],
            "Resource":[
                "arn:aws:workmail:region:account-id:organization/organization-id"
            ]
        }
    ]
}
```

用於資源許可的 IAM 角色

由於 Firehose 不使用資源政策，因此在設定將這些日誌傳送至 Firehose 時， AWS 會使用 IAM 角色。 會 AWS 建立名為 的服務連結角色AWSServiceRoleForLogDelivery。此服務連結角色包含下列許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "firehose:PutRecord",
                "firehose:PutRecordBatch",
                "firehose:ListTagsForDeliveryStream"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/LogDeliveryEnabled": "true"
                }
            },
            "Effect": "Allow"
        }
    ]
}
```

當您設定記錄時，此服務連結角色會針對LogDeliveryEnabled標籤設為 的所有 Firehose 交付串流授予許可true。將此標籤 AWS 提供給目的地交付串流。

此服務連結角色也有信任政策，以允許 delivery.logs.amazonaws.com 服務委託人擔任所需的服務連結角色。該信任政策如下：

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

主控台特定許可

除了前面各節中列出的許可之外，如果您使用主控台而非 APIs設定日誌交付，您也需要下列許可：

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"AllowLogDeliveryActions",
            "Effect":"Allow",
            "Action":[
                "firehose:DescribeDeliveryStream",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource":[
                "arn:aws:logs:region:account-id:log-group:*",
                "arn:aws:firehose:region:account-id:deliverystream/*",
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid":"ListAccessForDeliveryDestinations",
            "Effect":"Allow",
            "Action":[
                "logs:DescribeLogGroups",
                "firehose:ListDeliveryStreams",
                "s3:ListAllMyBuckets"
            ],
            "Resource":"*"
        }
    ]
}
```

Amazon WorkMail 的合規驗證

第三方稽核人員會在多個合規計畫中評估 Amazon WorkMail 的安全性和 AWS 合規性。其中包括 SOC、ISO 和 C5。

如需特定合規計劃範圍內 AWS 的服務清單，請參閱合規計劃範圍內的 AWS 服務。如需一般資訊，請參閱 AWS 合規計劃。

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 AWS Artifact 中下載報告。

您使用 Amazon WorkMail 時的合規責任取決於資料的敏感度、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，並提供在其中部署以安全與合規為中心之基準環境的步驟 AWS。
- AWS 合規資源 – 此工作手冊和指南的集合可能適用於您的產業和位置。
- AWS Config – AWS 此服務會評估您的資源組態是否符合內部實務、產業準則和法規。
- AWS Security Hub – AWS 此服務提供 內安全狀態的全面檢視 AWS ，可協助您檢查是否符合安全產業標準和最佳實務。

Amazon WorkMail 中的彈性

AWS 全球基礎設施是以 AWS 區域和可用區域為基礎建置。 AWS 區域提供多個實體隔離和隔離的可用區域，這些區域與低延遲、高輸送量和高度備援聯網連接。透過可用區域，您所設計與操作的應用程式和資料庫，就能夠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、容錯能力和擴充能力，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 全球基礎設施。

除了 AWS 全球基礎設施之外，Amazon WorkMail 還提供多種功能，以協助支援您的資料彈性和備份需求。

Amazon WorkMail 中的基礎設施安全性

> **Note**
>
> Amazon WorkMail 已停止對 Transport Layer Security (TLS) 1.0 和 1.1 的支援。如果您使用的是 TLS 1.0 或 1.1，則必須將 TLS 版本升級至 1.2。如需詳細資訊，請參閱 TLS 1.2，以成為所有 AWS API 端點的最低 TLS 通訊協定層級。

Amazon WorkMail 是受管服務，受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及如何 AWS 保護基礎設施的相關資訊，請參閱AWS 雲端安全。若要使用基礎設施安全的最佳實務設計您的 AWS 環境，請參閱 Security Pillar AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 已發佈的 API 呼叫，透過網路存取 Amazon WorkMail。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(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。

Amazon WorkMail 入門

完成 後先決條件，您就可以開始使用 Amazon WorkMail。如需詳細資訊，請參閱Amazon WorkMail 入門。

您可以在以下章節中進一步了解如何將現有信箱遷移至 Amazon WorkMail、與 Microsoft Exchange 的互通性，以及 Amazon WorkMail 配額。

主題

Amazon WorkMail 入門

無論您是新的 Amazon WorkMail 使用者還是 Amazon WorkSpaces 的現有使用者，請完成下列步驟以開始使用 Amazon WorkMail。

> **Note**
>
> 開始使用前，請先完成 先決條件。

主題

步驟 1：登入 Amazon WorkMail 主控台

您必須先登入 Amazon WorkMail 主控台，才能新增使用者和管理其帳戶和信箱。

登入 Amazon WorkMail 主控台

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。
2. 如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需區域的詳細資訊，請參閱《》中的區域和端點Amazon Web Services 一般參考。

步驟 2：設定您的 Amazon WorkMail 網站

1. 登入 Amazon WorkMail 主控台後，您可以設定您的組織並新增網域。建議您為 Amazon WorkMail 組織使用專用網域。如需詳細資訊，請參閱建立組織及新增網域。
2. （選用）您可以選擇使用 Amazon WorkMail 提供的免費測試網域。如果您選擇這樣做，請跳到步驟 4。

   > **Note**
   >
   > 測試網域使用此格式：*alias*.awsapps.com。當您離開時，請記住，您應該只使用測試網域進行測試。請勿將測試網域用於生產環境。此外，您的 Amazon WorkMail 組織中必須至少有一個已啟用的使用者。如果您沒有已啟用的使用者，網域可能會變成可供其他客戶註冊和使用。

3. 如果您使用外部網域，請將適當的文字 (TXT) 和郵件交換 (MX) 記錄新增至您的網域名稱系統 (DNS) 服務，以確認該網域。TXT 記錄可讓您在 DNS 中輸入備註。MX 記錄會指定傳入郵件伺服器。請務必將網域設定為組織的預設值。如需詳細資訊，請參閱驗證網域及選擇預設網域。
4. 為 Amazon WorkMail 建立新使用者或啟用現有的目錄使用者。如需詳細資訊，請參閱新增使用者。
5. （選用）如果您有現有的 Microsoft Exchange 信箱，請將其遷移至 Amazon WorkMail。如需詳細資訊，請參閱遷移至 Amazon WorkMail。

完成設定 Amazon WorkMail 網站後，您可以使用 Web 應用程式 URL 存取 Amazon WorkMail。

尋找您的 Amazon WorkMail Web 應用程式 URL

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。若要這樣做，請開啟搜尋方塊右側的選取區域清單，然後選擇所需的區域。如需詳細資訊，請參閱《》中的區域和端點Amazon Web Services 一般參考。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。

   組織設定頁面隨即出現，並在使用者登入下顯示 URL。URLs 採用此格式：
   https：//*alias*.awsapps.com/mail。

步驟 3：設定 Amazon WorkMail 使用者存取權

從下列選項中選擇，以設定 Amazon WorkMail 使用者存取權：

- 使用 Microsoft Outlook 用戶端從現有桌面用戶端使用設定使用者存取權。如需詳細資訊，請參閱將 Microsoft Outlook 連接至您的 Amazon WorkMail 帳戶。
- 從行動裝置設定使用者存取權，例如 Kindle、Android、iPad 或 iPhone。如需詳細資訊，請參閱行動裝置入門。
- 若要設定使用者存取，請使用與網際網路郵件存取通訊協定 (IMAP) 通訊協定相容的任何用戶端軟體。如需詳細資訊，請參閱將 IMAP 用戶端連線至您的 Amazon WorkMail 帳戶。

其他 資源

- 遷移至 Amazon WorkMail
- Amazon WorkMail 與 Microsoft Exchange 之間的互通性
- Amazon WorkMail 配額

遷移至 Amazon WorkMail

您可以透過與我們的合作夥伴之一合作，從 Microsoft Exchange、Microsoft Office 365、G Suite Basic（先前稱為 Google Apps for Work) 和其他平台遷移至 Amazon WorkMail。如需合作夥伴的詳細資訊，請參閱 Amazon WorkMail 功能。

主題

- 步驟 1：在 Amazon WorkMail 中建立或啟用使用者

步驟 1：在 Amazon WorkMail 中建立或啟用使用者

遷移使用者之前，您必須在 Amazon WorkMail 中新增這些使用者，才能佈建其信箱。如需詳細資訊，請參閱新增使用者。

步驟 2：遷移至 Amazon WorkMail

您可以與任何 AWS 遷移合作夥伴合作，遷移至 Amazon WorkMail。如需這些供應商的資訊，請參閱 Amazon WorkMail 功能。

若要遷移信箱，請建立專用的 Amazon WorkMail 使用者，以擔任遷移管理員。下列程序授予該使用者存取組織中所有信箱的許可。

建立遷移管理員

1. 執行以下任意一項：
   - 在 Amazon WorkMail 主控台中，建立新的使用者以擔任遷移管理員。如需詳細資訊，請參閱新增使用者。
   - 在您的 Active Directory 中，建立新的使用者以擔任遷移管理員，然後啟用 Amazon WorkMail 的使用者。如需詳細資訊，請參閱啟用使用者。
2. 在 Amazon WorkMail 主控台導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 選擇組織設定，選擇遷移，然後選擇編輯。
4. 將啟用遷移的滑桿移至開啟位置。
5. 開啟遷移管理員並選取使用者。
6. 選擇儲存。

步驟 3：完成遷移至 Amazon WorkMail

將電子郵件帳戶遷移至 Amazon WorkMail 後，您可以驗證 DNS 記錄並設定桌面和行動用戶端。

若要完成遷移至 Amazon WorkMail

1. 確認所有 DNS 記錄都已更新，且指向 Amazon WorkMail。如需關於所需的 DNS 記錄的詳細資訊，請參閱新增網域。

   > **Note**
   >
   > DNS 記錄更新程序可能需要幾個小時。如果任何當 MX 記錄正在變更時顯示在來源信箱的新項目，請在 DNS 記錄被更新後，再次執行遷移工具以遷移新項目。

2. 如需設定桌面或行動用戶端以使用 Amazon WorkMail 的詳細資訊，請參閱《Amazon WorkMail 使用者指南》中的將 Microsoft Outlook 連接至 Amazon WorkMail 帳戶。 Amazon WorkMail

Amazon WorkMail 與 Microsoft Exchange 之間的互通性

Amazon WorkMail 和 Microsoft Exchange Server 之間的互通性可讓您在將信箱遷移至 Amazon WorkMail 時，將對使用者的干擾降至最低，或使用 Amazon WorkMail 做為公司信箱的子集。

此互通性可讓您的信箱在跨環境中使用相同的公司網域。如此一來，您的使用者可以透過雙向共用無行事曆/忙碌狀態資訊來排程會議。

先決條件

在啟用與 Microsoft Exchange 的互通性之前，請執行以下事項：

- 請確定您至少已為 Amazon WorkMail 啟用一個使用者 這是設定 Microsoft Exchange 可用性設定的必要項目。要啟用使用者，請依照於 為使用者啟用電子郵件路由 中的步驟。
- 設定 Active Directory (AD) Connector。使用內部部署目錄設定 AD Connector 可讓使用者繼續使用其現有的公司登入資料。如需詳細資訊，請參閱建立 AD Connector 並將 Amazon WorkMail 與您的內部部署目錄整合。
- 設定您的 Amazon WorkMail 組織。建立使用您設定的 AD Connector 的 Amazon WorkMail 組織。
- 將公司網域新增至 Amazon WorkMail 組織，然後在 Amazon WorkMail 主控台中驗證它們。否則，傳送到這個別名的電子郵件將被退信。如需詳細資訊，請參閱使用網域。
- 將信箱遷移至 Amazon WorkMail。讓使用者能夠將信箱從您的現場部署環境佈建和遷移至 Amazon WorkMail。如需詳細資訊，請參閱啟用現有使用者，並參閱遷移至 Amazon WorkMail。

> **Note**
>
> 請勿更新 DNS 記錄以指向 Amazon WorkMail。這可確保 Microsoft Exchange 保留傳入電子郵件的主伺服器，以及您所要的兩個環境間的互通性。

- 確認在 Active Directory 的使用者主體名稱 (UPNs) 符合使用者的主要 SMTP 地址。

Amazon WorkMail 向 Microsoft Exchange 上的 Exchange Web Services (EWS) URL 提出 HTTPS 請求，以取得無行事曆/忙碌的資訊。

對於 EWS 型可用性提供者，Amazon WorkMail 會向 Microsoft Exchange 上的 Exchange Web Services (EWS) URL 提出 HTTPS 請求，以取得無行事曆/忙碌的資訊。因此，下列先決條件僅適用於 EWS 型可用性提供者。

- 確保相關防火牆設定已設定為允許從網際網路存取。HTTPS 請求的預設連接埠是連接埠 443。
- 只有在有效憑證授權機構 (CA) 簽署的憑證可在 Microsoft Exchange 環境中使用時，Amazon WorkMail 才能對 Microsoft Exchange 上的 EWS URL 提出成功的 HTTPS 請求。如需詳細資訊，請參閱 Microsoft Exchange 文件網站上的建立憑證授權機構的 Exchange Server 憑證請求。
- 您必須在 Microsoft Exchange 中啟用 EWS 的基本身分驗證。如需詳細資訊，請參閱 Microsoft MVP Award Program Blog 的虛擬目錄：Exchange 2013。

新增網域和啟用信箱

將公司網域新增至 Amazon WorkMail，以便在電子郵件地址中使用。確保已驗證新增至 Amazon WorkMail 的網域，然後讓使用者和群組在 Amazon WorkMail 上佈建信箱。在互通性模式下，無法在 Amazon WorkMail 中啟用資源，且應在停用互通性模式後，在 Amazon WorkMail 中重新建立資源。不過，您仍可以在互通性模式下繼續使用他們來排程會議。Microsoft Exchange 的資源一律會顯示在 Amazon WorkMail 的使用者索引標籤中。

- 如需詳細資訊，請參閱新增網域、啟用現有的使用者及啟用現有的群組。

> **Note**
>
> 為了確保與 Microsoft Exchange 的互通性，請勿更新 DNS 記錄以指向 Amazon WorkMail 記錄。Microsoft Exchange 會維持內送電子郵件的主伺服器，只要您想要兩個環境之間繼續保有互通性。

啟用互通性

如果您尚未建立 Amazon WorkMail 組織，您可以使用公有 API 在啟用互通性模式的情況下建立新的 WorkMail 組織。

如果您已經有與 Active Directory 連結的 AD Connector 的 Amazon WorkMail 組織，而且您也有 Microsoft Exchange，請聯絡 AWS Support 以取得協助，以啟用現有 Amazon WorkMail 組織的 Microsoft Exchange 互通性。

在 Microsoft Exchange 和 Amazon WorkMail 中建立服務帳戶

> **Note**
>
> 使用 Exchange 做為自訂可用性提供者的後端時，不需要在 Exchange 中建立服務帳戶。

若要存取行事曆免費/忙碌的資訊，請在 Microsoft Exchange 和 Amazon WorkMail 上建立服務帳戶。Microsoft Exchange 服務帳戶是 Microsoft Exchange 上可以存取其他 Exchange 使用者日曆閒置/忙碌行事曆資訊的任何使用者。預設為授予存取，故不需要特殊許可。

同樣地，Amazon WorkMail 服務帳戶是 Amazon WorkMail 上可存取其他 Amazon WorkMail 使用者行事曆免費/忙碌資訊的任何使用者。這也是預設為授予。您必須在內部部署目錄中建立 Amazon WorkMail 使用者，然後啟用該 Amazon WorkMail 使用者，將 Amazon WorkMail 與 AD Connector 整合到您的目錄中。

互通性模式的限制

當您的組織處於互通性模式時，您必須使用 Exchange 管理中心來管理所有使用者、群組和資源。若要啟用 Amazon WorkMail 使用者和群組，請使用 AWS Management Console。如需詳細資訊，請參閱啟用現有的使用者和啟用現有的群組。

為 Amazon WorkMail 啟用使用者或群組時，您無法編輯這些使用者和群組的電子郵件地址或別名。這些也必須透過 Exchange 管理中心設定。Amazon WorkMail 會每四小時同步一次目錄中的變更。

在互通性模式下，無法在 Amazon WorkMail 中建立或啟用資源。不過，Amazon WorkMail 通訊錄中提供所有 Exchange 資源，可用於照常安排會議。

在 Amazon WorkMail 上設定可用性設定

在 Amazon WorkMail 上設定可用性設定，以啟用查詢外部系統、提供行事曆功能，以及取得行事曆免費/忙碌的資訊。Amazon WorkMail 支援兩種從遠端系統取得免費/忙碌資訊的模式：

- Exchange Web Services (EWS) — 在此組態中，Amazon WorkMail 將使用 EWS 通訊協定查詢 Exchange 伺服器或其他 WorkMail 組織，以取得可用性資訊。這是最簡單的組態，但需要 Exchange 伺服器的 EWS 端點才能透過公有網際網路存取。
- 自訂可用性提供者 (CAP) — 在此組態中，管理員可以設定 AWS Lambda 函數，以取得特定電子郵件網域的使用者可用性資訊。根據您的電子郵件伺服器平台，搭配 Amazon WorkMail 使用 CAP 可提供下列優點：
  - 從內部 EWS 取得使用者可用性，而不需要為 WorkMail 開啟防火牆。
  - 從非交換或非 EWS 系統取得使用者可用性，例如 Google Workspace （ 先前稱為 G Suite)。

主題

設定 EWS 型可用性提供者

若要在主控台上設定 EWS 型可用性設定，請完成下列程序：

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。若要這樣做，請開啟搜尋方塊右側的選取區域清單，然後選擇所需的區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇組織設定，然後選擇互通性索引標籤。
4. 選擇新增可用性組態，然後輸入下列資訊：

- 類型 — 選取 EWS。
- 網域 — WorkMail 將嘗試使用此組態查詢可用性資訊的網域。
- EWS URL — Amazon WorkMail 會將此 URL 查詢至 EWS 端點。請參閱本指南的取得 EWS URL 一節。
- 使用者電子郵件地址 — WorkMail 用來向 EWS 端點進行身分驗證之使用者的電子郵件地址。
- 密碼 — WorkMail 用來向 EWS 端點進行身分驗證的密碼。

5. 選擇儲存。

取得 EWS URL

若要使用 Microsoft Outlook 取得適用於 Exchange 的 EWS URL，請完成下列程序：

1. 為在 Exchange 環境的任何使用者在 Windows 登入至 Microsoft Outlook。
2. 按住 Ctrl 鍵並開啟內容 (按一下滑鼠右鍵) 功能表列於任務列上的 Microsoft Outlook 圖示。
3. 選擇 Test E-mail AutoConfiguration (測試電子郵件自動組態)。
4. 鍵入 Microsoft Exchange 使用者的電子郵件地址和密碼，然後選擇 Test (測試)。
5. 從結果視窗複製 Availability Service URL (可用性服務 URL) 的值。

若要使用 PowerShell 取得用於交換的 EWS URL，請在 PowerShell 提示字元中執行下列命令：

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

若要取得 Amazon WorkMail 的 EWS URL，請先在 Amazon WorkMail 端點和配額下尋找 EWS 網域。輸入 EWS URL — `https://"EWS domain"/EWS/Exchange.asmx`並將「EWS 網域」取代為您的 EWS 網域。

設定自訂可用性提供者

若要設定自訂可用性提供者 (CAP)，請完成下列程序：

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。若要這樣做，請開啟搜尋方塊右側的選取區域清單，然後選擇所需的區域。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽面板中，選擇組織設定，然後選擇互通性。

4. 選擇新增可用性組態，然後輸入下列資訊：

   - 類型 — 選取 CAP Lambda。
   - 網域 — WorkMail 將嘗試使用此組態查詢可用性資訊的網域。
   - ARN — 將提供可用性資訊的 Lambda 函數 ARN。

若要建置 CAP Lambda 函數，請參閱 建置自訂可用性提供者 Lambda 函數。

建置自訂可用性提供者 Lambda 函數

自訂可用性提供者 (CAPs) 是使用以 JSON 為基礎的請求和回應通訊協定進行設定，該通訊協定是以明確定義的 JSON 結構描述撰寫。Lambda 函數會剖析請求並提供有效的回應。

主題

- 請求和回應元素
- 授與 存取權
- 使用 CAP Lambda 函數的 Amazon WorkMail 範例

請求和回應元素

請求元素

以下是用於為 Amazon WorkMail 使用者設定 CAP 的範例請求：

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

```
    }
}
```

請求由三個部分組成：申請者、信箱和視窗。這些會在本指南的下列 信箱、 要求者和 視窗章節中說明。

要求者

請求者區段提供向 Amazon WorkMail 提出原始請求之使用者的相關資訊。CAPs會使用此資訊來變更提供者的行為。例如，此資料可用來模擬後端可用性提供者上的相同使用者，或從回應中省略某些詳細資訊。

欄位	描述	必要
`Email`	申請者的主要電子郵件地址。	是
`Username`	請求者的使用者名稱。	是
`Organization`	請求者的組織 ID。	是
`UserID`	請求者 ID。	是
`Origin`	請求的遠端地址。	否
`Bearer`	保留以供日後使用。	否

信箱

信箱區段包含要求可用性資訊之使用者電子郵件地址的逗號分隔清單。

視窗

視窗區段包含請求可用性資訊的時段。`startDate` 和 均以 UTC `endDate`指定，並根據 RFC 3339 格式化。事件預計不會被截斷。換句話說，如果事件在定義的 之前啟動`StartDate`，則會使用原始啟動。

回應元素

Amazon WorkMail 會等待 25 秒，從 CAP Lambda 函數取得回應。25 秒後，Amazon WorkMail 會假設函數失敗，並在 EWS GetUserAvailability 回應中為相關聯的信箱產生失敗。這不會導致整個 GetUserAvailability 操作失敗。

以下是本節開頭所定義組態的範例回應：

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

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

回應由包含信箱清單的單一信箱區段組成。成功取得可用性的每個信箱都由三個部分組成：信箱、事件和工作時間。如果可用性提供者無法取得信箱的可用性資訊，則區段由兩個區段組成：信箱和錯誤。這些會在本指南的下列 信箱、事件、工作期間、、 工作時間 時區和 錯誤章節中說明。

信箱

信箱區段是在請求的信箱區段中找到的使用者電子郵件地址。

事件

事件區段是在請求視窗中發生的事件清單。每個事件都以下列參數定義：

欄位	描述	必要
startTime	事件的開始時間，以 UTC 顯示，並根據 RFC 3339 格式化。	是
endTime	事件的結束時間，以 UTC 顯示，並根據 RFC 3339 格式化。	是
busyType	事件的忙碌類型。可以是 Busy、Free 或 Tentative 。	是
details	事件的詳細資訊。	否
details.subject	事件的主旨。	是
details.location	事件的位置。	是
details.instanceType	事件的執行個體類型。可以是 Single_In	是

欄位	描述	必要
	stance 、Recurring _Instance 或 Exception 。	
details.isMeeting	指出事件是否有出席者的布林值。	是
details.isReminder Set	指出事件是否具有提醒集的布林值。	是
details.isPrivate	指出事件是否設為私有的布林值。	是

工作時間

workingHours 區段包含信箱擁有者工作時間的相關資訊。它包含兩個區段：時區和workingPeriods。

時區

時區子區段說明信箱擁有者的時區。當請求者在不同時區運作時，正確轉譯使用者的工作時數非常重要。可用性提供者需要明確描述時區，而不是使用名稱。使用獨立的時區描述有助於避免時區不相符。

欄位	描述	必要
name	時區的名稱。	是
bias	預設與 GMT 的偏移，以分鐘為單位。	是
standardTime	指定時區的標準時間開始時間。	否
daylightTime	指定時區的日光節約時間開始時間。	否

您必須同時定義 standardTime和 daylightTime，或省略兩者。standardTime 和 daylightTime 物件中的欄位為：

欄位	描述	允許值
offset	相對於預設位移的位移，以分鐘為單位。	NA
time	標準時間與日光節約時間之間發生轉換的時間，指定為 hh:mm:ss。	NA
month	標準時間與日光節約時間之間發生轉換的月份。	JAN,FEB, MAR, APR, JUN, JUL, AUG, SEP, OCT, NOV, DEC
week	在指定月份內的一週，即標準時間和日光節約時間之間的轉換發生。	FIRST, SECOND, THIRD, FOURTH, LAST
dayOfWeek	在指定週內，標準時間與日光節約時間之間的轉換發生的日期。	SUN, MON, TUE, WED, THU, FRI, SAT

工作期間

workingPeriods 區段包含一或多個工作期間物件。每個期間都會定義一天或多天的開始和結束工作日。

欄位	描述	允許值
startMinutes	工作日的開始，從午夜起以分鐘為單位。	NA
endMinutes	工作日結束，從午夜開始以分鐘為單位。	NA
days	此期間適用的天數。	SUN, MON, TUE, WED, THU, FRI, SAT

錯誤

錯誤欄位可以包含任意錯誤訊息。下表列出已知代碼與 EWS 錯誤代碼的映射。所有其他訊息都會映射至 ERROR_FREE_BUSY_GENERATION_FAILED。

Value	EWS 錯誤碼
MailboxNotFound	ERROR_MAIL_RECIPIENT_NOT_FOUND
ErrorAvailabilityConfigNotFound	ERROR_AVAILABILITY_CONFIG_NOT_FOUND
ErrorServerBusy	ERROR_SERVER_BUSY
ErrorTimeoutExpired	ERROR_TIMEOUT_EXPIRED
ErrorFreeBusyGenerationFailed	ERROR_FREE_BUSY_GENERATION_FAILED
ErrorResponseSchemaValidation	ERROR_RESPONSE_SCHEMA_VALIDATION

授與 存取權

從 AWS Command Line Interface () 執行下列 Lambda 命令AWS CLI。此命令會將資源政策新增至剖析 CAP 的 Lambda 函數。此函數允許 Amazon WorkMail 可用性服務調用您的 Lambda 函數。

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

在 命令中，依指示新增下列參數：

- *LAMBDA_REGION* — 部署 CAP Lambda 的區域名稱。例如 us-east-1。
- *CAP_FUNCTION_NAME* — CAP Lambda 函數的名稱。

> **Note**
>
> 這可以是 CAP Lambda 函數的名稱、別名或部分或完整 ARN。

- *WM_REGION* — Amazon WorkMail 組織調用 Lambda 函數的區域名稱。

> **Note**
>
> 只有下列區域可用於 CAP：
>
> - 美國東部 (維吉尼亞北部)
> - 美國西部 (奧勒岡)
> - 歐洲 (愛爾蘭)

- *WM_ACCOUNT_ID* — Organization 帳戶的 ID。
- *ORGANIZATION_ID* — 叫用 CAP Lambda 的組織 ID。例如，組織 ID：m-934ebb9eb57145d0a6cab566ca81a21f。

> **Note**
>
> 只有在需要跨區域呼叫時，*LAMBDA_REGION* 和 *WM_REGION* 才會不同。如果不需要跨區域呼叫，它們將是相同的。

使用 CAP Lambda 函數的 Amazon WorkMail 範例

如需使用 CAP Lambda 函數查詢 EWS 端點的 Amazon WorkMail 範例，請參閱 Amazon WorkMail GitHub 儲存庫的 Serverless 應用程式上的此AWS 範例應用程式。 Amazon WorkMail GitHub

在 Microsoft Exchange 設定可用性設定

若要將已啟用使用者的所有無行事曆/忙碌資訊請求重新導向至 Amazon WorkMail，請在 Microsoft Exchange 中設定可用地址空間。

使用下列 PowerShell 命令來建立地址空間：

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

出現提示時，輸入 Amazon WorkMail 服務帳戶的登入資料。使用者名稱應輸入為 **domain\username**（即 ***orgname*.awsapps.com\workmail_service_account_*username***。在這裡，***orgname***代表 Amazon WorkMail 組織的名稱。如需詳細資訊，請參閱在 Microsoft Exchange 和 Amazon WorkMail 中建立服務帳戶。

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

如需詳細資訊，請參閱 Microsoft 文件上的 Add-AvailabilityAddressSpace。

啟用 Microsoft Exchange 和 Amazon WorkMail 使用者之間的電子郵件路由

透過 Microsoft Exchange Server 和 Amazon WorkMail 之間的電子郵件路由，使用者可以在遷移至 Amazon WorkMail 後保留現有的電子郵件地址。電子郵件路由可讓您將 Microsoft Exchange Server 保留為組織傳入電子郵件的主要簡易郵件傳輸通訊協定 (SMTP) 伺服器。

在使用電子郵件路由之前，您將需要完成下列先決條件：

- 為您的組織啟用互通性模式。如需詳細資訊，請參閱啟用互通性。
- 請確定您在 Amazon WorkMail 主控台中看到您的網域。
- 確認我們的 Microsoft Exchange Server 可以傳送電子郵件到網際網路。您可能需要設定傳送連接器。如需傳送連接器的詳細資訊，請參閱 Microsoft 文件中的在 Exchange Server 中建立傳送連接器以將郵件傳送至網際網路。

為使用者啟用電子郵件路由

建議您先為測試使用者完成下列步驟，再將任何變更套用至您的組織。

1. 啟用您要遷移至 Amazon WorkMail 的使用者帳戶。如需詳細資訊，請參閱啟用現有的使用者。
2. 在 Amazon WorkMail 主控台中，確保至少有兩個電子郵件地址與已啟用的使用者相關聯。
   - <*workmailuser*@*orgname*.awsapps.com>（這是自動新增的，可以在沒有 Microsoft Exchange 的情況下用於測試。）

- <*workmailuser*@*yourdomain*.com>（這會自動新增，且為主要 Microsoft Exchange 地址。）

  如需詳細資訊，請參閱編輯使用者電子郵件地址。

3. 請確定您將所有資料從 Microsoft Exchange 中的信箱遷移至 Amazon WorkMail 中的信箱。如需詳細資訊，請參閱遷移至 Amazon WorkMail。
4. 遷移所有資料後，請在 Microsoft Exchange 上停用使用者的信箱。然後，建立指向 Amazon WorkMail 的外部 SMTP 地址的郵件使用者（或啟用郵件的使用者）。若要這樣做，請在 Exchange Management Shell 中使用下列命令：

   > **Important**
   >
   > 下列步驟會清除信箱的內容。在您嘗試啟用電子郵件路由之前，請確定您的資料已遷移至 Amazon WorkMail。當您執行此命令時，有些郵件用戶端不會無縫切換到 Amazon WorkMail。如需詳細資訊，請參閱郵件使用者組態。

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

   ```
   Disable-Mailbox $old_mailbox
   ```

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

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

   在上述命令中，*orgname* 代表 Amazon WorkMail 組織的名稱。如需詳細資訊，請參閱停用信箱和在 Microsoft TechNet啟動郵件使用者。

5. 傳送測試電子郵件給使用者（在上述範例中為 **workmailuser@yourdomain.com**）。如果電子郵件路由已正確啟用，使用者應該能夠登入其 Amazon WorkMail 信箱並接收電子郵件。

> **Note**
>
> Microsoft Exchange 維持為內送電子郵件的主要伺服器，只要您想要兩個環境之間的互通性繼續保有。為了確保與 Microsoft Exchange 的互通性，DNS 記錄不應更新為指向 Amazon WorkMail，直到稍後為止。

文章設定組態

上述步驟會將使用者信箱從 Microsoft Exchange Server 移至 Amazon WorkMail，同時將 Microsoft Exchange 中的使用者保留為聯絡人。由於遷移的使用者現在是外部郵件使用者，Microsoft Exchange Server 會施加額外的限制。完成遷移可能還有其他組態需求。

- 使用者可能無法以預設傳送電子郵件到群組。若要啟用此功能，您必須將使用者新增至所有群組的安全寄件者清單。如需詳細資訊，請參閱 Microsoft TechNet 上的交付管理。
- 使用者可能無法預訂資源。若要啟用此功能，您必須設定使用者需要存取的所有資源`ProcessExternalMeetingMessages`的 。如需詳細資訊，請參閱 Microsoft TechNet 上的Set-CalendarProcessing。

郵件使用者組態

有些郵件用戶端不會無縫切換到 Amazon WorkMail。這些用戶端需要使用者執行額外的設定步驟。不同郵件用戶端需要採取不同的動作。

- Windows 上的 Microsoft Outlook – 需要重新啟動 Outlook。在啟動時，您必須選擇是否繼續使用舊信箱或使用臨時信箱。選擇暫時信箱選項。然後，重新設定 Microsoft Exchange 信箱。
- MacOS 上的 Microsoft Outlook – 重新啟動 Outlook 時，會提示以下訊息：Outlook 已重新導向至伺服器 ***orgname***.awsapps.com。您希望此伺服器設定您的設定嗎？ 接受建議。
- iOS 上的郵件 – 郵件應用程式停止接收電子郵件，並產生無法收到郵件錯誤。重新建立並重新設定 Microsoft Exchange 信箱。

停用互通性模式並停用您的郵件伺服器

為 Amazon WorkMail 設定 Microsoft Exchange 信箱後，您可以停用互通性模式。如果您尚未遷移任何使用者或記錄，停用互通性模式不會影響您的任何組態。

> **Warning**
>
> 在停用互通性模式之前，請確定您已完成所有必要的步驟。否則可能會導致電子郵件遭到退信或意外行為。如果您尚未完成遷移，停用互通性可能會導致中斷您的組織。您無法復原此操作。

停用互通性模式支援

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇您要停用互通性模式的組織。
3. 在組織設定下，選擇停用互通性模式。
4. 在停用互通性模式對話方塊中，輸入組織的名稱，然後選擇停用互通性模式。

停用互通性支援後，未為 Amazon WorkMail 啟用的使用者和群組會從通訊錄中移除。您仍然可以使用 Amazon WorkMail 主控台啟用任何缺少的使用者或群組，並將他們新增至通訊錄。在完成以下步驟之前，無法啟用來自 Microsoft Exchange 的資源，也不會出現在通訊錄中。

- 在 Amazon WorkMail 中建立資源 – 您可以在 Amazon WorkMail 中建立資源，然後為這些資源設定委派代表和預訂選項。如需詳細資訊，請參閱使用資源。
- 建立 AutoDiscover DNS 記錄 – 為組織中的所有郵件網域設定 AutoDiscover DNS 記錄。這可讓使用者從 Microsoft Outlook 和行動用戶端連線至其 Amazon WorkMail 信箱。如需詳細資訊，請參閱使用 AutoDiscover 設定端點。
- 將 MX DNS 記錄切換到 Amazon WorkMail – 若要將所有傳入電子郵件交付到 Amazon WorkMail，您必須將 MX DNS 記錄切換到 Amazon WorkMail。DNS 記錄的變更最多可能需要 72 小時才能傳播到所有 DNS 伺服器。
- 停用您的郵件伺服器 – 驗證所有電子郵件都直接路由到 Amazon WorkMail 之後，如果您未來不打算使用郵件伺服器，則可以停用您的郵件伺服器。

故障診斷

以下是最常遇到的 Amazon WorkMail 互通性和遷移錯誤的解決方案。

Exchange Web Services (EWS) URL 無效或無法連線 – 檢查您是否擁有正確的 EWS URL。如需詳細資訊，請參閱在 Amazon WorkMail 上設定可用性設定。

EWS 驗證期間的連線失敗 – 這是一般錯誤，可能原因如下：

- Microsoft Exchange 中沒有網際網路連線。
- 您的防火牆未設定為允許從網際網路存取。確認連接埠 443 (HTTPS 請求的預設連接埠) 已開啟。

如果您已確認網際網路連線和防火牆設定，但錯誤仍然存在，請聯絡 AWS Support。

設定 Microsoft Exchange 互通性時的使用者名稱和密碼無效 – 這是一般錯誤，可能原因如下：

- 該使用者名稱不在預期的表單。使用下列模式：

```
DOMAIN\username
```

- 您的 Microsoft Exchange 伺服器並未為 EWS 基本身分驗證設定。如需詳細資訊，請參閱 Microsoft MVP Award Program Blog 的虛擬目錄：Exchange 2013。

使用者收到含有 winmail.dat 連接的電子郵件 – 當加密的 S/MIME 電子郵件從 Exchange 傳送至 Amazon WorkMail，並在適用於 Mac 的 Outlook 2016 或 IMAP 用戶端中收到時，可能會發生這種情況。解決方案是在 Exchange Management Shell 中執行下列命令。

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

如果您已確認上述幾點，但錯誤仍持續出現，請聯絡 AWS Support。

Amazon WorkMail 配額

企業客戶和小型企業擁有者都可以使用 Amazon WorkMail。雖然我們無需在配額內設定任何變化下，支援大多數使用案例，我們還針對產品濫用保護我們的使用者和網際網路。因此，有些客戶可能會碰上我們已設定的配額。本節說明這些配額和其變更方式。

有些配額值可以變更，有些則是無法變更的硬性配額。如需請求提高配額的詳細資訊，請參閱 中的AWS 服務配額Amazon Web Services 一般參考。

Amazon WorkMail 組織和使用者配額

您可以新增最多 25 位使用者到您的 Amazon WorkMail 組織，免費試用 30 天。在此期間結束後，除非您移除或關閉 Amazon WorkMail 帳戶，否則需支付所有作用中使用者的費用。

所有傳送至另一個使用者的訊息在評估這些配額時都會被考量。這些包括電子郵件、會議請求、會議回應、任務請求和因規則而被轉發或自動重新導向的訊息。

> **Note**
>
> 請求提高特定組織的配額時，您必須在請求中包含組織名稱。

資源	預設配額	變更請求上限
每個 AWS 帳戶的 Amazon WorkMail 組織	100	可以根據組織的目錄類型增加。您可以從AWS Directory Service 主控台檢視 AWS Directory Service 配額和請求增加。如需詳細資訊，請參閱《AWS 一般參考》中的服務配額。
每個 Amazon WorkMail 組織的使用者	1,000	可以根據組織的目錄類型增加，如下所示： • Amazon WorkMail 目錄：最多 1，000 萬名使用者 • Simple AD 或 AD Connector，大型：最多 5,000 個使用者 * • Simple AD 或 AD Connector，小型：最多 500 個使用者 * • Microsoft AD，託管者 AWS Directory Service：最多 1，000 萬名使用者，視您的設定和組態而定，

資源	預設配額	變更請求上限
		* 如果您使用 Simple AD 或 AD Connector，更多資訊請參閱 AWS Directory Service。
免費試用使用者	在前 30 天最多 25 個使用者	免費試用期間僅適用於任何組織中的前 25 個使用者。任何其他使用者皆不包含在免費試用優惠。
每天每個 AWS 帳戶的收件人	組織外部的 100,000 個收件人，沒有組織內部的收件人之硬性配額	沒有上限。不過，Amazon WorkMail 是商業電子郵件服務，不適用於大量電子郵件服務。如需大量電子郵件服務，請參閱 Amazon SES 或 Amazon Pinpoint.
每天使用任一測試網域處理每個 AWS 帳戶的收件人	200 個收件人，無論目的地	測試郵件網域不適用於長期使用。我們建議您新增自己的網域，並將其用作預設網域。

對群組的配額係由底層目錄來設定。

WorkMail 組織設定配額

資源	預設配額
每個 Amazon WorkMail 組織的網域數量	1,000 這是硬性配額，無法變更。
每個電子郵件流程規則中的寄件者模式數量	250 這是硬性配額，無法變更。
每個組織的電子郵件流量規則中的寄件者模式數量	1,000 這是硬性配額，無法變更。

每個使用者的配額

所有傳送至另一個使用者的訊息在評估這些配額時都會被考量。這些包括電子郵件、會議請求、會議回應、任務請求和因規則而被轉發或自動重新導向的訊息。

資源	預設配額	變更請求的配額上限
信箱的最大容量	50 GB 這是硬性配額，無法變更。	不適用
每個使用者的別名上限數量	100 這是硬性配額，無法變更。	不適用
收件人使用您擁有的網域每天處理每個使用者	組織外部的 10,000 個收件人，沒有組織內部的收件人之硬性配額限制	沒有上限。不過，Amazon WorkMail 是商業電子郵件服務，不適用於大量電子郵件服務。如需大量電子郵件服務，請參閱 Amazon SES 或 Amazon Pinpoint.

訊息配額

所有傳送至另一個使用者的訊息在評估這些配額時都會被考量。這些包括電子郵件、會議請求、會議回應、任務請求和因規則而被轉發或自動重新導向的訊息。

資源	預設配額
內送訊息的大小上限	29 MB 的未編碼資料。 訊息會以 MIME 格式接收。傳入 MIME 訊息的大小上限為 40 MB。 這是硬性配額，無法變更。
外寄訊息的大小上限	29 MB 的未編碼資料。

資源	預設配額
	訊息會以 MIME 格式傳送。傳出 MIME 訊息的大小上限為 40 MB。 這是硬性配額，無法變更。
每則訊息的最高收件人數量	500 這是硬性配額，無法變更。
每則訊息的附件數量上限	500 這是硬性配額，無法變更。

使用組織

在 Amazon WorkMail 中，您的組織代表您公司的使用者。在 Amazon WorkMail 主控台中，您會看到可用組織的清單。如果您沒有任何可用的組織，您必須建立組織才能使用 Amazon WorkMail。

主題

建立組織

若要使用 Amazon WorkMail，您必須先建立組織。一個 AWS 帳戶可以有多個 Amazon WorkMail 組織。建立組織時，您也可以為組織選取網域，並設定使用者目錄和加密設定。

您可以建立新的使用者目錄，或整合 Amazon WorkMail 與現有的目錄。您可以將 Amazon WorkMail 與內部部署 Microsoft Active Directory、 AWS 受管 Active Directory 或 Simple AD 搭配使用。透過與您的內部部署目錄整合，您可以在 Amazon WorkMail 中使用現有的使用者和群組，使用者可以使用現有的登入資料登入。如果您使用的是內部部署目錄，您必須先在其中設定 AD Connector AWS Directory Service。AD Connector 會將您的使用者和群組與 Amazon WorkMail 通訊錄同步，並執行使用者身分驗證請求。如需詳細資訊，請參閱《 AWS Directory Service 管理指南》中的 Active Directory Connector。

您也可以選擇 AWS KMS key Amazon WorkMail 用來加密信箱內容的 。您可以選取 Amazon WorkMail 的預設 AWS 受管主金鑰，或在 AWS Key Management Service () 中使用現有的 KMS 金鑰 AWS KMS。如需有關建立新的 KMS 金鑰的資訊，請參閱《 AWS Key Management Service 開發人員指南》中的建立金鑰。如果您以 AWS Identity and Access Management (IAM) 使用者身分登入，請讓自己成為 KMS 金鑰的金鑰管理員。如需詳細資訊，請參閱《 AWS Key Management Service 開發人員指南》中的啟用和停用金鑰。

考量事項

建立 Amazon WorkMail 組織時，請記住下列事項：

- Amazon WorkMail 目前不支援您與多個帳戶共用的受管 Microsoft Active Directory 服務。
- 如果您有具有 Microsoft Exchange 和 AD Connector 的內部部署 Active Directory，建議您為組織設定互通性設定。這可讓您在將信箱遷移至 Amazon WorkMail 時將對使用者的干擾降至最低，或使用 Amazon WorkMail 做為公司信箱的子集。如需詳細資訊，請參閱Amazon WorkMail 與 Microsoft Exchange 之間的互通性。
- 如果選取免費測試網域選項，您可以開始將 Amazon WorkMail 組織與提供的測試網域搭配使用。測試網域使用此格式： *example*.awsapps.com。只要您在 Amazon WorkMail 組織中維持已啟用的使用者，您就可以將測試郵件網域與 Amazon WorkMail 和其他支援的 AWS 服務搭配使用。不過，您無法將測試網域用於其他用途。如果您的 Amazon WorkMail 組織未維護至少一個已啟用的使用者，則測試網域可能可供其他客戶註冊和使用。
- Amazon WorkMail 不支援多區域目錄。

主題

建立組織

在 Amazon WorkMail 主控台中建立新組織。

建立組織

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱《》中的區域和端點Amazon Web Services 一般參考。

2. 在導覽列中，選取組織。

   組織頁面隨即出現，如果有的話會顯示您的組織。

3. 選擇建立組織。
4. 在電子郵件網域下，選取要用於組織中電子郵件地址的網域：

- 現有 Route 53 網域 – 選取您使用 Amazon Route 53 (Route 53) 託管區域管理的現有網域。
- 新的 Route 53 網域 – 註冊要與 Amazon WorkMail 搭配使用的新 Route 53 網域名稱。
- 外部網域 – 輸入您使用外部網域名稱系統 (DNS) 供應商管理的現有網域。
- 免費測試網域 – 使用 Amazon WorkMail 提供的免費測試網域。您可以使用測試網域探索 Amazon WorkMail，稍後再將網域新增至您的組織。

5. （選用）如果您的網域是透過 Amazon Route 53 管理，請針對 Route 53 託管區域選取您的 Route 53 網域。
6. 針對別名，輸入組織的唯一別名。
7. 選擇進階設定，然後針對使用者目錄，選取下列其中一個選項：

   - 建立新的 Amazon WorkMail 目錄 – 建立新的目錄以新增和管理使用者。
   - 使用現有目錄 – 使用現有目錄來管理您的使用者，例如內部部署 Microsoft Active Directory、AWS 受管 Active Directory 或 Simple AD。

8. 針對加密，選取下列其中一個選項：

   - 使用 Amazon WorkMail 受管金鑰 – 在帳戶中建立新的加密金鑰。
   - 使用現有的 KMS 金鑰 – 使用您已在其中建立的現有 KMS 金鑰 AWS KMS。

9. 選擇建立組織。

如果您使用外部網域，請將適當的文字 (TXT) 和郵件交換程式 (MX) 記錄新增至 DNS 服務來驗證它。TXT 記錄可讓您輸入有關 DNS 服務的備註。MX 記錄會指定傳入郵件伺服器。

請務必將網域設定為組織的預設值。如需詳細資訊，請參閱驗證網域及選擇預設網域。

當您的組織處於作用中狀態時，您可以將使用者新增至其中，並設定其電子郵件用戶端。如需詳細資訊，請參閱新增使用者和設定 Amazon WorkMail 的電子郵件用戶端。

檢視組織的詳細資訊

每個 Amazon WorkMail 組織都可以顯示組織詳細資訊頁面。此頁面會顯示其組織的相關資訊，包括您可以搭配 IDs AWS Command Line Interface。頁面上的訊息也可以顯示完成設定和組織所需的任何步驟，例如未經驗證的網域或缺少使用者。訊息也提供設定指定電子郵件用戶端時所遵循的第一個步驟。

檢視組織詳細資訊

1. 在導覽列中，選擇組織。

組織頁面隨即出現，並顯示您的組織。

2. 選擇您要檢視的組織。

整合 WorkSpaces 目錄

若要將 Amazon WorkMail 與 WorkSpaces 搭配使用，請使用下列步驟建立相容的目錄。

新增相容的 WorkSpaces 目錄

1. 使用 WorkSpaces 建立相容的目錄。如需 WorkSpaces 說明，請參閱《Amazon WorkSpaces 管理指南》中的開始使用 Amazon WorkSpaces 快速設定。 Amazon WorkSpaces
2. 在 Amazon WorkMail 主控台中，建立您的 Amazon WorkMail 組織，並選擇使用您現有的目錄。如需詳細資訊，請參閱建立組織。

組織狀態和說明

在您建立組織後，它可以有以下其中一個狀態。

州	描述
Active (作用中)	您的組織正常並已做好使用準備。
正在建立	工作流程正在執行以建立您的組織。
失敗	您的組織無法被建立。
Impaired (受損)	您的組織故障或已偵測到問題。
非作用中	您的組織失效。
Requested (已請求)	您的組織在佇列中建立請求並等待建立。
Validating (驗證)	組織的所有設定都被檢查運作狀態。

刪除組織

如果您不想再將 Amazon WorkMail 用於組織的電子郵件，您可以從 Amazon WorkMail 中刪除組織。

> **Note**
>
> 此操作無法復原。刪除組織後，您將無法復原信箱資料。

若要刪除組織

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在組織畫面上的組織清單中，選取要刪除的組織，然後選擇刪除。
3. 針對刪除組織，選擇是否刪除或保留現有的使用者目錄，然後輸入組織的名稱。
4. 選擇刪除組織。

> **Note**
>
> 如果您沒有為 Amazon WorkMail 提供自己的目錄，我們會為您建立一個目錄。如果您在刪除組織時保留此現有目錄，除非 Amazon WorkMail、WorkDocs 或 WorkSpaces 正在使用它，否則您將需要支付費用。如需定價資訊，請參閱其他目錄類型定價。
> 為了刪除目錄，它無法啟用任何其他 AWS 應用程式。如需詳細資訊，請參閱《 AWS Directory Service 管理指南》中的刪除 Simple AD 目錄或刪除 AD Connector 目錄。

當您嘗試刪除組織時，您可能會收到無效的 Amazon Simple Email Service (Amazon SES) 規則集錯誤訊息。如果您收到此錯誤，請在 Amazon SES 主控台中編輯 Amazon SES 規則，並移除無效的規則集。您編輯的規則在規則名稱中應該有您的 Amazon WorkMail 組織 ID。如需編輯 Amazon SES 規則的詳細資訊，請參閱《Amazon Simple Email Service 開發人員指南》中的建立接收規則。

如果您需要找出哪個規則集無效，請先儲存規則。規則集會出現錯誤訊息。

尋找電子郵件地址

您可以查看使用者、資源或群組是否在 Organization 中使用電子郵件地址。

尋找電子郵件地址

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。

2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在組織頁面中，選擇尋找電子郵件地址。
4. 選擇 Search (搜尋)。

使用組織設定

下列各節說明如何使用 Amazon WorkMail 組織可用的設定。您選擇的設定將套用至整個組織。

主題

啟用信箱遷移

當您想要將信箱從 Microsoft Exchange 或 G Suite Basic 等來源轉移到 Amazon WorkMail 時，您可以啟用信箱遷移。您可以在更大的遷移程序中啟用遷移。如需詳細資訊，包括操作步驟，請參閱本指南入門一節遷移至 Amazon WorkMail中的 。

啟用日誌

您可以啟用日誌記錄以記錄您的電子郵件通訊。使用日誌記錄時，您通常會使用整合式第三方封存和 eDiscovery 工具。日誌有助於確保您符合資料儲存、隱私權保護和資訊保護的合規法規。

如需詳細資訊，包括操作步驟，請參閱本指南入門一節搭配 Amazon WorkMail 使用電子郵件日誌中的 。

啟用互通性

互通性可讓您從 Microsoft Exchange 遷移，並使用 Amazon WorkMail 做為公司信箱的子集。如需詳細資訊，包括操作步驟，請參閱本指南入門一節在 Amazon WorkMail 上設定可用性設定中的 。

啟用 SMTP 閘道

您可以啟用 Simple Mail Transfer Protocol (SMTP) 閘道，以與傳出電子郵件流程規則搭配使用。傳出電子郵件流程規則可讓您透過 SMTP 閘道路由從 Amazon WorkMail 組織傳送的電子郵件訊息。如需詳細資訊，請參閱傳出電子郵件規則動作。

> **Note**
>
> 針對傳出電子郵件流程規則設定的 SMTP 閘道，必須使用主要憑證授權單位的憑證來支援 Transport Layer Security (TLS) 1.2 版。僅支援基本身分驗證。

設定 SMTP 閘道

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 Organization settings (組織設定)。

   組織設定頁面隨即出現，並顯示一組索引標籤。
4. 選擇 SMTP 閘道索引標籤，然後選擇建立閘道。
5. 輸入下列資料：

   - 閘道名稱 — 輸入唯一的名稱。
   - 閘道地址 — 輸入閘道的主機名稱或 IP 地址。
   - 連接埠號碼 — 輸入閘道的連接埠號碼。
   - 使用者名稱 — 輸入使用者名稱。
   - 密碼 — 輸入高強度密碼。
6. 選擇建立。

   SMTP 閘道可用於傳出電子郵件流程規則。

當您設定 SMTP 閘道與傳出電子郵件流程規則搭配使用時，傳出訊息會嘗試比對規則與 SMTP 閘道。符合規則的訊息會路由至對應的 SMTP 閘道，然後處理電子郵件交付的其餘部分。

如果 Amazon WorkMail 無法連線到 SMTP 閘道，系統會將電子郵件訊息退回給寄件者。如果發生這種情況，請遵循上述步驟來更正閘道設定。

管理電子郵件流程

若要協助管理電子郵件，您可以設定電子郵件流程規則。電子郵件流程規則可以根據電子郵件訊息的地址或網域，對電子郵件訊息採取一或多個動作。您可以在寄件者和收件人的電子郵件地址或網域上使用電子郵件流程規則。

當您建立電子郵件流程規則時，您可以指定在符合指定規則模式時套用至電子郵件的規則動作。

主題

傳入電子郵件規則動作

傳入電子郵件流程規則可防止不適當的電子郵件寄達您的使用者信箱。傳入電子郵件流程規則也稱為規則動作，會自動套用至傳送給 Amazon WorkMail 組織內任何人的所有電子郵件訊息。這與個別信箱的電子郵件規則不同。

> **Note**
>
> 或者，您可以搭配 AWS Lambda 函數使用規則，在傳入電子郵件傳送到使用者信箱之前進行處理。如需搭配 Amazon WorkMail 使用 Lambda 的詳細資訊，請參閱 AWS Lambda 為

Amazon WorkMail 設定。如需有關 Lambda 的詳細資訊，請參閱 AWS Lambda 開發人員指南。

傳入電子郵件流程規則也稱為規則動作，會自動套用至傳送給 Amazon WorkMail 組織內任何人的所有電子郵件訊息。這與個別信箱的電子郵件規則不同。

下列規則動作定義傳入電子郵件的處理方式。您可為每個規則指定寄件者與收件人模式及下列任一動作。

動作	描述
捨棄電子郵件	電子郵件訊息會被忽略。它不會被傳送且寄件者不會收到未傳遞通知。
傳送退信回應	電子郵件訊息不會傳送，且寄件者會在退信訊息中收到未傳送的通知。
傳遞到垃圾郵件資料夾	電子郵件訊息會傳送到使用者的垃圾郵件或垃圾郵件資料夾，即使 Amazon WorkMail 垃圾郵件偵測系統最初未將其識別為垃圾郵件。
預設	電子郵件訊息會在 Amazon WorkMail 垃圾郵件偵測系統檢查後傳送。垃圾電子郵件會傳送至垃圾郵件資料夾。所有其他電子郵件訊息都會傳送到收件匣。 寄件者模式較不明確的其他電子郵件流程規則會被忽略。若要為網域型電子郵件流程規則新增例外狀況，請採用更明確的寄件者模式來設定預設動作。如需詳細資訊，請參閱寄件者與收件人模式。
永不傳送到垃圾郵件資料夾	電子郵件訊息一律會傳送到使用者的收件匣，即使 Amazon WorkMail 垃圾郵件偵測系統將其識別為垃圾郵件。

動作	描述
	Important 若不使用預設的垃圾郵件偵測系統，您指定的地址可能導致使用者接觸高風險內容。
執行 AWS Lambda	將電子郵件訊息傳遞至 Lambda 函數，以便在交付至使用者的收件匣之前或期間進行處理。

Note

傳入電子郵件會先傳送到 Amazon SES，然後傳送到 Amazon WorkMail。如果 Amazon SES 封鎖傳入電子郵件訊息，則規則動作將不適用。例如，Amazon SES 會在偵測到已知病毒或由於明確的 IP 篩選規則而封鎖電子郵件訊息。此時指定規則動作 (如 Default (預設)、Deliver to junk folder (傳送到垃圾郵件資料夾)或 Never deliver to junk folder (永遠不傳送到垃圾郵件資料夾)) 都不會有作用。

傳出電子郵件規則動作

您可以使用傳出電子郵件流程規則，透過 SMTP 閘道指示電子郵件訊息，或封鎖寄件者傳送電子郵件訊息給指定的收件人。如需 SMTP 閘道的詳細資訊，請參閱 啟用 SMTP 閘道。

您也可以使用傳出電子郵件流程規則，在傳送電子郵件後將電子郵件訊息傳遞至 AWS Lambda 函數進行處理。如需有關 Lambda 的詳細資訊，請參閱 AWS Lambda 開發人員指南。

下列規則動作定義傳出電子郵件的處理方式。您可為每個規則指定寄件者與收件人模式及下列任一動作。

動作	描述
預設	電子郵件訊息會透過正常流程傳送。
捨棄電子郵件	電子郵件訊息已捨棄。該郵件不發送，且寄件者不會收到通知。

動作	描述
傳送退信回應	電子郵件訊息不會傳送，且寄件者會收到訊息通知，告知管理員已封鎖電子郵件訊息。
路由至 SMTP 閘道	電子郵件訊息會透過設定的 SMTP 閘道傳送。
執行 Lambda	在傳送電子郵件之前或期間，將電子郵件訊息傳遞給 Lambda 函數進行處理。

寄件者與收件人模式

電子郵件流程規則可套用到特定電子郵件地址，或是套用到特定的網域或一組網域中的所有電子郵件地址。由您定義模式，以決定要套用規則的電子郵件地址。

寄件者與收件人兩者的模式採用下列任一格式：

- 電子郵件地址符合單一電子郵件地址，例如：

```
mailbox@example.com
```

- 網域名稱符合該網域下的所有電子郵件地址；例如：

```
example.com
```

- 萬用字元網域符合該網域及其所有子網域下的所有電子郵件地址。萬用字元只會顯示於網域的前方，例如：

```
*.example.com
```

- 星號符合任何網域下的任何電子郵件地址。

```
*
```

> **Note**
>
> + 符號在寄件者或收件者模式內無效。

多個模式可被一個規則指定。如需詳細資訊，請參閱傳入電子郵件規則動作及傳出電子郵件規則動作。

如果傳入電子郵件訊息中的 Sender或 From標頭符合任何模式，就會套用傳入電子郵件流程規則。如果存在，Sender 地址會第一個為符合。如果沒有相符的 Sender 標頭或 Sender 標頭不符合任何規則，From 地址為符合。如果電子郵件訊息有多個收件人符合不同的規則，則每個規則適用於相符的收件人。

如果外寄電子郵件訊息中的收件人和 Sender或 From標頭符合任何模式，就會套用外寄電子郵件流程規則。如果電子郵件訊息有多個收件人符合不同的規則，則每個規則適用於相符的收件人。

若多個規則相符，將套用最明確的規則動作。例如，特定電子郵件地址的規則優先於整個網域的規則。若多個規則的明確程度相同，將套用限制最嚴格的動作。例如，Drop (捨棄) 動作的優先順序高於 Bounce (退信) 動作。動作的優先順序與 傳入電子郵件規則動作 和 傳出電子郵件規則動作 所列的順序相同。

> **Note**
>
> 以刪除或彈跳動作建立重疊的寄件者模式規則時請注意。未預期的優先順序排序可能會導致許多傳入電子郵件訊息無法傳遞。

建立電子郵件流程規則

電子郵件流程規則會將規則動作套用至傳入和傳出電子郵件訊息。當訊息符合指定的模式時，就會套用動作。新的電子郵件流程規則會立即生效。

建立電子郵件流程規則

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 Organization settings (組織設定)。

   組織設定頁面隨即出現，並顯示一組索引標籤。從此頁面，您可以建立傳入或傳出規則。下列步驟說明如何建立這兩種類型。

建立傳入規則

1. 選擇傳入規則索引標籤，然後選擇建立。
2. 在規則名稱方塊中，輸入唯一的名稱。
3. 在動作下，開啟清單並選取動作。清單中的每個項目都包含描述，有些則提供進一步了解連結。

> **Note**
>
> 如果您選擇執行 Lambda 動作，則會顯示其他控制項：如需使用這些控制項的相關資訊，請參閱下一節：AWS Lambda 為 Amazon WorkMail 設定。

4. 在寄件者網域或地址下，輸入您要套用規則的寄件者網域或地址。
5. 在目的地網域或地址下，輸入目的地網域和電子郵件地址的任意組合。
6. 選擇建立。

建立傳出規則

1. 選擇傳出規則索引標籤，然後選擇建立。
2. 在規則名稱方塊中，輸入唯一的名稱。
3. 在動作下，開啟清單並選取動作。清單中的每個項目都包含描述，有些則提供進一步了解連結。

> **Note**
>
> 如果您選擇執行 Lambda 動作，則會顯示其他控制項。如需使用這些控制項的詳細資訊，請參閱下一節：AWS Lambda 為 Amazon WorkMail 設定。

4. 在寄件者網域或地址下，輸入有效寄件者網域和電子郵件地址的任意組合。
5. 在目的地網域或地址下，輸入有效目的地網域和電子郵件地址的任意組合。
6. 選擇建立。

您可以測試新建立的電子郵件流程規則。如需詳細資訊，請參閱測試電子郵件流程規則。

編輯電子郵件流程規則

當您需要變更電子郵件訊息的一或多個規則動作時，您可以編輯電子郵件流程規則。本節中的步驟適用於傳入和傳出電子郵件訊息。

編輯電子郵件流程規則

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 Organization settings (組織設定)。

   組織設定頁面隨即出現，並顯示一組索引標籤。
4. 選擇傳入規則或傳出規則索引標籤。
5. 選擇您要變更之規則旁的選項按鈕，然後選擇編輯。
6. 視需要變更規則中的動作，然後選擇儲存。

AWS Lambda 為 Amazon WorkMail 設定

使用傳入和傳出電子郵件流程規則中的執行 Lambda 動作，將符合規則的電子郵件訊息傳遞至 AWS Lambda 函數進行處理。

為 Amazon WorkMail 中的執行 Lambda 動作選擇下列組態。

同步執行 Lambda 組態

符合流程規則的電子郵件訊息會在傳送或交付之前傳遞至 Lambda 函數進行處理。使用此組態來修改電子郵件內容。您也可以控制不同使用案例的傳入或傳出電子郵件流程。例如，傳遞至 Lambda 函數的規則可能會封鎖敏感電子郵件訊息的傳遞、移除附件或新增免責聲明。

非同步 Run Lambda 組態

符合流程規則的電子郵件訊息會在傳送或交付時傳遞至 Lambda 函數進行處理。此組態不會影響電子郵件傳遞，而且可用於收集傳入或傳出電子郵件訊息的指標等任務。

無論您選擇同步或非同步組態，傳遞至 Lambda 函數的事件物件都會包含傳入或傳出電子郵件事件的中繼資料。您也可以使用中繼資料中的訊息 ID，以存取電子郵件訊息的完整內容。如需詳細資訊，請參閱使用 擷取訊息內容 AWS Lambda。如需電子郵件事件的詳細資訊，請參閱 Lambda 事件資料。

如需傳入和傳出電子郵件流程規則的詳細資訊，請參閱管理電子郵件流程。如需有關 Lambda 的詳細資訊，請參閱 AWS Lambda 開發人員指南。

> **Note**
>
> 目前，Lambda 電子郵件流程規則僅參考相同 AWS 區域中和所設定 Amazon WorkMail AWS 帳戶 組織的 Lambda 函數。

適用於 Amazon WorkMail AWS Lambda 的 入門

若要開始使用 AWS Lambda 搭配 Amazon WorkMail，我們建議您將 WorkMail Hello World Lambda 函數從 部署 AWS Serverless Application Repository 到您的帳戶。函數具有所有必要的資源，以及為您設定的許可。如需更多範例，請參閱 GitHub 上的 amazon-workmail-lambda-templates 儲存庫。

如果您選擇建立自己的 Lambda 函數，則必須使用 AWS Command Line Interface () 設定許可AWS CLI。在下列範例命令中，執行下列動作：

- `MY_FUNCTION_NAME` 將 取代為 Lambda 函數的名稱。
- `REGION` 將 取代為您的 Amazon WorkMail AWS 區域。可用的 Amazon WorkMail 區域包括 `us-east-1`（美國東部（維吉尼亞北部））、 `us-west-2`（美國西部（奧勒岡））和 `eu-west-1`（歐洲（愛爾蘭））。
- 將 取代`AWS_ACCOUNT_ID`為您的 12 位數 AWS 帳戶 ID。
- 將 取代`WORKMAIL_ORGANIZATION_ID`為您的 Amazon WorkMail 組織 ID。您可以在 Organizations 頁面上的組織卡片上找到它。

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

如需使用 的詳細資訊 AWS CLI，請參閱 AWS Command Line Interface 使用者指南。

設定同步執行 Lambda 規則

若要設定同步執行 Lambda 規則，請使用執行 Lambda 動作建立電子郵件流程規則，然後選取同步執行核取方塊。如需如何建立郵件流程規則的詳細資訊，請參閱建立電子郵件流程規則。

若要完成建立同步規則，請新增 Lambda Amazon Resource Name (ARN) 並設定下列選項。

Fallback action (備用動作)

如果 Lambda 函數無法執行，Amazon WorkMail 會套用動作。如果未設定 allRecipients 旗標，則此動作也適用於從 Lambda 回應省略的任何收件人。備用動作不能是另一個 Lambda 動作。

Rule timeout (規則逾時) (以分鐘為單位)

如果 Amazon WorkMail 無法叫用 Lambda 函數，則會重試該函數的期間。系統會在此期間結束時套用 Fallback action (備用動作)。

> **Note**
>
> 同步執行 Lambda 規則僅支援*目的地條件。

Lambda 事件資料

使用以下事件資料觸發 Lambda 函數。資料的呈現取決於 Lambda 函數使用的程式設計語言。

```
{
    "summaryVersion": "2018-10-10",
    "envelope": {
        "mailFrom" : {
            "address" : "from@example.com"
        },
        "recipients" : [
           { "address" : "recipient1@example.com" },
           { "address" : "recipient2@example.com" }
        ]
    },
    "sender" : {
        "address" :  "sender@example.com"
```

```
    },
    "subject" : "Hello From Amazon WorkMail!",
    "messageId": "00000000-0000-0000-0000-000000000000",
    "invocationId": "00000000000000000000000000000000",
    "flowDirection": "INBOUND",
    "truncated": false
}
```

事件 JSON 包括下列資料。

summaryVersion

的版本編號LambdaEventData。這只會在您於 中進行回溯不相容的變更時更新LambdaEventData。

envelope

電子郵件訊息的信封，其中包含下列： 欄位。

mailFrom

From (寄件人) 地址通常是傳送電子郵件訊息的使用者電子郵件地址。若使用者以另一位使用者的身分或代表另一位使用者傳送了電子郵件訊息，則 mailFrom (寄件者地址) 欄位會傳回授權使用者傳送電子郵件的電子郵件地址，而非實際寄件者的電子郵件地址。

recipients

收件人電子郵件地址清單。Amazon WorkMail 不會區分 To、CC 或 BCC。

> **Note**
>
> 對於傳入電子郵件流程規則，此清單包含您在其中建立規則的 Amazon WorkMail 組織中所有網域中的收件人。系統會針對來自寄件者的每個 SMTP 對話分別叫用 Lambda 函數，而收件人欄位會列出來自該 SMTP 對話的收件人。使用外部網域的收件人不包含在內。

寄件者

代表另一位使用者傳送電子郵件訊息的使用者的電子郵件地址。只有在代表其他使用者傳送電子郵件訊息時，才會設定此欄位。

subject

電子郵件主旨行。超過 256 個字元限制時就會遭到截斷。

messageId

使用 Amazon WorkMail Message Flow SDK 時，用來存取電子郵件訊息完整內容的唯一 ID。

invocationId

唯一 Lambda 調用的 ID。當針對相同的 LambdaEventData 呼叫 Lambda 函數多次時，此 ID 保持不變。用於偵測重試次數並避免重複。

flowDirection

指出電子郵件流程的方向，即 INBOUND (傳入) 或 OUTBOUND (傳出)。

truncated

適用於承載大小，而不是主旨行長度。若此值為 `true`，則負載大小會超過 128 KB 的限制，因此會截斷收件人清單以符合限制。

同步執行 Lambda 回應結構描述

當具有同步執行 Lambda 動作的電子郵件流程規則符合傳入或傳出電子郵件訊息時，Amazon WorkMail 會呼叫設定的 Lambda 函數，並等待回應，然後再對電子郵件訊息採取動作。Lambda 函數會根據預先定義的結構描述傳回回應，該結構描述會列出動作、動作類型、適用的參數，以及套用動作的收件人。

下列範例顯示同步執行 Lambda 回應。回應會根據用於 Lambda 函數的程式設計語言而有所不同。

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

回應 JSON 包含下列資料。

動作

要為收件人採取的動作。

type

動作類型。非同步 Run Lambda 動作不會傳回動作類型。

傳入規則動作類型包含 BOUNCE (退信)、DROP (捨棄)、DEFAULT (預設)、BYPASS_SPAM_CHECK 和 MOVE_TO_JUNK。如需詳細資訊，請參閱傳入電子郵件規則動作。

輸出規則動作類型包含 BOUNCE (退信)、DROP (捨棄) 和 DEFAULT (預設)。如需詳細資訊，請參閱傳出電子郵件規則動作。

parameters

其他動作參數。支援 BOUNCE 動作類型做為具有金鑰 bounceMessage 和值字串的 JSON 物件。此退信訊息可用來建立退信電子郵件訊息。

recipients

應對其採取動作的電子郵件地址清單。即使原始收件人清單中未包含收件人，您仍可將收件人新增至回應中。如果某個動作的 allRecipients 為 true，此欄位則非必填。

> **Note**
>
> 當對傳入電子郵件呼叫 Lambda 動作時，您只能新增來自您組織的新收件人。新收件人會以 BCC (密件副本) 的形式新增至回應中。

allRecipients

為 true 時， 會將動作套用至 Lambda 回應中不受其他特定動作限制的所有收件人。

同步執行 Lambda 動作限制

當 Amazon WorkMail 針對同步執行 Lambda 動作調用 Lambda 函數時，適用下列限制：

- Lambda 函數必須在 15 秒內回應，或視為失敗的調用。

> **Note**
>
> 系統會針對您指定的規則逾時間隔重試呼叫。

- 允許最多 256 KB 的 Lambda 函數回應。
- 回應中最多可允許 10 個唯一動作。10 個以上都動作會受到設定的 Fallback action (備用動作) 所約束。
- 傳出 Lambda 函數最多允許 500 位收件人。
- Rule timeout (規則逾時) 的最大值為 240 分鐘。如果已設定最小值 0，Amazon WorkMail 套用後援動作之前不會重試。

同步執行 Lambda 動作失敗

如果 Amazon WorkMail 因為錯誤、無效的回應或 Lambda 逾時而無法叫用 Lambda 函數，Amazon WorkMail 會以指數退避重試調用，以降低處理速率，直到規則逾時期間完成為止。接著，Fallback action (備用動作) 會套用至電子郵件訊息的所有收件人。如需詳細資訊，請參閱設定同步執行 Lambda 規則。

同步執行 Lambda 回應範例

下列範例示範常見同步 Run Lambda 回應的結構。

Example ：從電子郵件訊息中移除指定的收件人

下列範例示範從電子郵件訊息中移除收件人的同步 Run Lambda 回應結構。

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

```
        ]
      }
    ]
}
```

Example ：自訂電子郵件訊息的退信

下列範例示範同步 Run Lambda 回應的結構，以便使用自訂電子郵件訊息進行彈跳。

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

Example ：將收件人新增至電子郵件訊息

下列範例示範將收件人新增至電子郵件訊息的同步 Run Lambda 回應結構。這不會更新電子郵件訊息的 To (收件人) 或 CC (副本) 欄位。

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

```
      }
    ]
}
```

如需為執行 Lambda 動作建立 Lambda 函數時要使用的更多程式碼範例，請參閱 Amazon WorkMail Lambda 範本。

搭配 Amazon WorkMail 使用 Lambda 的詳細資訊

您也可以存取觸發 Lambda 函數之電子郵件訊息的完整內容。如需詳細資訊，請參閱使用 擷取訊息內容 AWS Lambda。

使用 擷取訊息內容 AWS Lambda

設定 AWS Lambda 函數以管理 Amazon WorkMail 的電子郵件流程後，您可以存取使用 Lambda 處理之電子郵件訊息的完整內容。如需 Lambda for Amazon WorkMail 入門的詳細資訊，請參閱 AWS Lambda 為 Amazon WorkMail 設定。

若要存取電子郵件訊息的完整內容，請使用 Amazon WorkMail Message Flow API 中的 `GetRawMessageContent`動作。呼叫時傳送到 Lambda 函數的電子郵件訊息 ID 會將請求傳送至 API。接著，API 會以電子郵件訊息的完整 MIME 內容來回應。如需詳細資訊，請參閱《Amazon WorkMail API 參考》中的 Amazon WorkMail 訊息流程。 Amazon WorkMail

下列範例顯示使用 Python 執行時間環境的 Lambda 函數如何擷取完整訊息內容。

> **Tip**
>
> 如果您從 將 Amazon WorkMail Hello World Lambda 函數部署 AWS Serverless Application Repository 到您的帳戶開始，系統會使用所有必要的資源和許可在您的帳戶中建立 Lambda 函數。然後，您可以根據您的使用案例，將商業邏輯新增至 lambda 函數。

```
import boto3
import email
import os

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

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

如需分析傳輸中訊息內容的更詳細範例，請參閱 GitHub 上的 amazon-workmail-lambda-templates 儲存庫。

> **Note**
>
> 您只能使用 Amazon WorkMail Message Flow API 存取傳輸中的電子郵件訊息。您只能在傳送或接收訊息的 24 小時內存取訊息。若要以程式設計方式存取使用者信箱中的訊息，請使用 Amazon WorkMail 支援的其他通訊協定，例如 IMAP 或 Exchange Web Services (EWS)。

使用 AWS Lambda 更新訊息內容

設定同步 AWS Lambda 函數以管理電子郵件流程後，您可以使用 Amazon WorkMail Message Flow API 中的 `PutRawMessageContent`動作來更新傳輸中電子郵件訊息的內容。如需 Amazon WorkMail Lambda 函數入門的詳細資訊，請參閱 設定同步執行 Lambda 規則。如需 API 的詳細資訊，請參閱 PutRawMessageContent。

> **Note**
>
> PutRawMessageContent API 需要 boto3 1.17.8，或者您可以將 layer 新增至 Lambda 函數。若要下載正確的 boto3 版本，請參閱 GitHub 上的 boto 頁面。如需新增層的詳細資訊，請參閱設定函數以使用層。
> 以下是範例 layer：`"LayerArn":"arn:aws:lambda:${AWS::Region}:489970191081:layer:WorkMailLambdaLayer:2"`。在此範例中，`${AWS::Region}`以適當的 aws 區域取代，例如 us-east-1。

> **Tip**
>
> 如果您從將 Amazon WorkMail Hello World Lambda 函數從 AWS Serverless Application Repository 部署到您的帳戶開始，系統會在您的帳戶中建立具有必要資源和許可的 Lambda 函數。然後，您可以根據您的使用案例，將商業邏輯新增至 lambda 函數。

當您離開時，請記住下列事項：

- 使用 GetRawMessageContent API 擷取原始訊息內容。如需更多資訊，請參閱使用 擷取訊息內容 AWS Lambda。
- 收到原始訊息後，請變更 MIME 內容。完成後，將訊息上傳至您帳戶中的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。確保 S3 儲存貯體使用與 Amazon WorkMail 操作 AWS 帳戶 相同的 ，而且它使用與 API 呼叫相同的 AWS 區域。
- 若要讓 Amazon WorkMail 處理請求，您的 S3 儲存貯體必須具有正確的政策，才能存取 S3 物件。如需詳細資訊，請參閱Example S3 policy。
- 使用 PutRawMessageContent API 將更新的訊息內容傳回 Amazon WorkMail。

> **Note**
>
> PutRawMessageContent API 可確保更新訊息的 MIME 內容符合 RFC 標準，以及 RawMessageContent 資料類型中提及的條件。傳入 Amazon WorkMail 組織的電子郵件不一定符合這些標準，因此 PutRawMessageContent API 可能會拒絕它們。在這種情況下，您可以參閱傳回的錯誤訊息，以取得如何修正任何問題的詳細資訊。

Example 範例 S3 政策

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {"Service": "workmail.REGION.amazonaws.com"
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::My-Test-S3-Bucket/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "AWS_ACCOUNT_ID"
                },
                "Bool": {
                    "aws:SecureTransport": "true"
                },
                "ArnLike": {
```

```
                    "aws:SourceArn":
 "arn:aws:workmailmessageflow:REGION:AWS_ACCOUNT_ID:message/WORKMAIL_ORGANIZATION_ID/*"
                }
            }
        }
    ]
}
```

下列範例顯示 Lambda 函數如何使用 Python 執行時間來更新傳輸中電子郵件訊息的主旨。

```
    import boto3
    import os
    import uuid
    import email

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

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

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

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

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

如需更多分析傳輸中訊息內容的方法範例，請參閱 GitHub 上的 amazon-workmail-lambda-templates 儲存庫。

管理對 Amazon WorkMail 訊息流程 API 的存取

使用 AWS Identity and Access Management (IAM) 政策來管理對 Amazon WorkMail 訊息流程 API 的存取。

Amazon WorkMail Message Flow API 適用於單一資源類型，即傳輸中的電子郵件訊息。每個傳輸中的電子郵件都有一個與其關聯的唯一 Amazon Resource Name (ARN)。

以下範例顯示與傳輸中電子郵件訊息關聯的 ARN 語法。

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

上述範例中的可變更欄位包含下列項目：

- 區域 – Amazon WorkMail 組織的 AWS 區域。
- 帳戶 – Amazon WorkMail 組織的 AWS 帳戶 ID。
- 組織 – 您的 Amazon WorkMail 組織 ID。
- 內容 – 指出訊息是`incoming`傳送到您的組織還是`outgoing`來自組織。
- 訊息 ID – 做為輸入傳遞至 Lambda 函數的唯一電子郵件訊息 ID。

以下範例包含與傳輸中傳入電子郵件訊息相關聯的 ARN 範例 ID。

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

您可以使用這些 ARNs 做為 IAM 使用者政策 `Resource`區段中的資源，以管理對傳輸中 Amazon WorkMail 訊息的存取。

Amazon WorkMail 訊息流程存取的 IAM 政策範例

下列範例政策會授予 IAM 實體對 中每個 Amazon WorkMail 組織的所有傳入和傳出訊息的完整讀取存取權 AWS 帳戶。

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

```
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource": "arn:aws:workmailmessageflow:region:account:message/*",
            "Effect": "Allow"
        }
    ]
}
```

如果您的 中有多個組織 AWS 帳戶，您也可以限制對一或多個組織的存取。如果某些 Lambda 函數只應該用於特定組織，這會很有用。

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

您也可以選擇根據訊息是 incoming (傳入) 組織還是從組織 outgoing (傳出)，來授予訊息的存取權。若要執行此作業，請在 ARN 中使用限定詞 incoming 或 outgoing。

以下範例政策僅授予對傳入組織之訊息的存取權。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent"
            ],
            "Resource":
 "arn:aws:workmailmessageflow:region:account:message/organization/incoming/*",
            "Effect": "Allow"
```

```
        }
    ]
}
```

下列範例政策會授予 IAM 實體對 中每個 Amazon WorkMail 組織的所有傳入和傳出訊息的完整讀取和更新存取權 AWS 帳戶。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workmailmessageflow:GetRawMessageContent",
                "workmailmessageflow:PutRawMessageContent"
            ],
            "Resource": "arn:aws:workmailmessageflow:region:account:message/*",
            "Effect": "Allow"
        }
    ]
}
```

測試電子郵件流程規則

若要檢查目前的規則組態，您可以針對特定電子郵件地址測試組態的行為。

測試電子郵件流程規則

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 Organization settings (組織設定)、Inbound/Outbound rules (傳入/傳出規則)。
4. 請在 Test configuration (測試組態) 旁輸入欲測試寄件者和收件人兩者的完整電子郵件地址。
5. 選擇測試。顯示所提供的電子郵件地址會採取的動作。

移除電子郵件流程規則

當您移除電子郵件流程規則時，變更會立即被套用。

移除電子郵件流程規則

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 Organization settings (組織設定)、Inbound/Outbound rules (傳入/傳出規則)。
4. 選取規則然後選擇 Remove (移除)。
5. 在確認提示中，選擇 Remove (移除)。

對內送電子郵件強制執行 DMARC 政策

為了安全起見，電子郵件網域會使用網域名稱系統 (DNS) 記錄。可以保護您的使用者免受常見的攻擊，例如詐騙或網路釣魚。DNS 記錄通常包含網域型訊息驗證、報告和一致性 (DMARC) 記錄，這些記錄是由傳送電子郵件的網域擁有者所設定。DMARC 記錄包含的政策指定當電子郵件未通過 DMARC 檢查時要採取的動作。您可以選擇是否要對傳送至組織的電子郵件強制執行 DMARC 政策。

新的 Amazon WorkMail 組織預設會開啟 DMARC 強制執行。

若要開啟強制執行 DMARC 功能

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 Organization settings (組織設定)。組織設定頁面隨即出現，並顯示一組索引標籤。
4. 選擇 DMARC 索引標籤，然後選擇編輯。
5. 將 DMARC 強制執行滑桿移至開啟位置。
6. 選取我確認開啟 DMARC 強制執行旁的核取方塊，可能會導致根據寄件者的網域組態捨棄或隔離傳入電子郵件。
7. 選擇儲存。

若要關閉 DMARC 強制執行功能

- 遵循上一節中的步驟，但將 DMARC 強制執行滑桿移至關閉位置。

使用電子郵件事件記錄來追蹤 DMARC 的強制執行

開啟 DMARC 強制執行可能會導致內送電子郵件遭到捨棄或標示為垃圾郵件，視寄件者設定其網域的方式而定。如果寄件者設定錯誤的電子郵件網域，您的使用者可能會停止接收合法電子郵件。若要檢查未交付給您使用者的電子郵件，您可以為 Amazon WorkMail 組織啟用電子郵件事件記錄。然後，您可以查詢電子郵件事件日誌，找出根據寄件者的 DMARC 政策篩選掉傳入的電子郵件。

在您使用電子郵件事件記錄來追蹤 DMARC 強制執行之前，請在 Amazon WorkMail 主控台中啟用電子郵件事件記錄。若要充分利用您的日誌資料，請在記錄電子郵件事件的同時等待一些時間。如需詳細資訊和指示，請參閱the section called “啟用電子郵件事件記錄”。

若要使用電子郵件事件記錄來追蹤 DMARC 強制執行

1. 在 CloudWatch Insights 主控台的 Logs (記錄) 下，選擇 Insights (Insights)。
2. 針對選取日誌群組 （選取），選取您 Amazon WorkMail 組織的日誌群組。例如，/aws/workmail/events/organization-alias。
3. 選取要查詢的時間期間。
4. 執行以下查詢：stats count() by event.dmarcPolicy | filter event.dmarcVerdict == "FAIL"
5. 選擇 Run query (執行查詢)。

您也可以為這些事件設定自訂指標。如需詳細資訊，請參閱建立指標篩選器。

標記組織

標記 Amazon WorkMail 組織資源可讓您：

- 在 AWS 帳單與成本管理 主控台中區分組織。
- 將 Amazon WorkMail 組織資源新增至 AWS Identity and Access Management (IAM) 許可政策陳述式的 `Resource`元素，以控制對 Amazon WorkMail 組織資源的存取。

如需 Amazon WorkMail 資源層級許可的詳細資訊，請參閱 資源。如需有關根據標籤控制存取的更多資訊，請參閱以 Amazon WorkMail 標籤為基礎的授權。

Amazon WorkMail 管理員可以使用 Amazon WorkMail 主控台標記組織。

將標籤新增至 Amazon WorkMail 組織

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 選擇標籤。
4. 對於 Organization tags (組織標籤)，選擇 Add New Tag (新增標籤)。
5. 針對金鑰，輸入識別標籤的名稱。
6. (選用) 在 Value (值) 中，輸入標籤的值。
7. (選用) 重複步驟 4-6，將更多標籤新增至您的組織。您最多可新增 50 個標籤。
8. 選擇儲存，以儲存變更。

您可以在 Amazon WorkMail 主控台中檢視您的組織標籤。

開發人員也可以使用 AWS SDK 或 AWS Command Line Interface () 標記組織AWS CLI。如需詳細資訊，請參閱 Amazon WorkMail API `TagResource`參考或 `UntagResource` 命令參考中的 `ListTagsForResource`、 AWS CLI 和 命令。 Amazon WorkMail

您可以隨時使用 Amazon WorkMail 主控台從組織移除標籤。

從 Amazon WorkMail 組織移除標籤

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 選擇標籤。
4. 對於 Organization tags (組織標籤)，選擇要移除之標籤旁邊的 Remove (移除)。
5. 選擇 Submit (提交) 來儲存您的變更。

使用存取控制規則

Amazon WorkMail 的存取控制規則可讓管理員控制組織的使用者和模擬角色如何獲得 Amazon WorkMail 的存取權。每個 Amazon WorkMail 組織都有預設存取控制規則，可將信箱存取權授予新增至組織的所有使用者和模擬角色，無論他們使用哪個存取通訊協定或 IP 地址。管理員可以編輯或使用自己的其中一個規則取代預設規則、新增規則或刪除規則。

> **Warning**
>
> 如果管理員刪除組織的所有存取控制規則，Amazon WorkMail 會封鎖組織信箱的所有存取。

管理員可以根據下列準則套用允許或拒絕存取的存取控制規則：

- 通訊協定 – 用來存取信箱的通訊協定。範例包括 Autodiscover、EWS、IMAP、SMTP、ActiveSync、適用於 Windows 的 Outlook 和 Webmail。
- IP 地址 – 用來存取信箱的 IPv4 CIDR 範圍。
- Amazon WorkMail 使用者 – 組織中用來存取信箱的使用者。
- 模擬角色 – 組織中用來存取信箱的模擬角色。如需詳細資訊，請參閱管理模擬角色。

除了使用者的信箱和資料夾權限之外，管理員還會套用存取控制規則。如需詳細資訊，請參閱《Amazon WorkMail 使用者指南》中的使用信箱許可和共用資料夾和資料夾許可。

> **Note**
>
> - 當您啟用 Outlook for Windows 的存取權時，建議您也啟用 Autodiscover 和 EWS 的存取權。
> - 存取控制規則不適用於 Amazon WorkMail 主控台或 SDK 存取。請改用 AWS Identity and Access Management (IAM) 角色或政策。如需詳細資訊，請參閱Amazon WorkMail 的身分和存取管理。

建立存取控制規則

從 Amazon WorkMail 主控台建立新的存取控制規則。

建立新的存取控制規則

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 選擇 Access Control List (存取控制規則)。
4. 選擇建立規則。
5. 對於 Description (描述)，請輸入規則的描述。
6. 對於 Effect (效果)，請選擇 Allow (允許) 或 Deny (拒絕)。這會根據您在下列步驟中選取的條件允許或拒絕存取。
7. 對於此規則適用於 ... 的請求，請選取要套用至規則的條件，例如是否包含或排除特定通訊協定、IP 地址或使用者，或是模擬角色。
8. （選用）如果您輸入 IP 地址範圍、使用者或模擬角色，請選擇新增以將其新增至規則。
9. 選擇建立規則。

編輯存取控制規則

從 Amazon WorkMail 主控台編輯新的和預設存取控制規則。

編輯存取控制規則

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 選擇 Access Control List (存取控制規則)。
4. 選取要編輯的規則。
5. 選擇編輯規則。
6. 視需要編輯描述、效果和條件。
7. 選擇儲存變更。

> **Important**
>
> 當您變更存取規則時，受影響的信箱可能需要五分鐘的時間才能遵循更新後的規則。存取受影響信箱的用戶端在此期間可能會顯示不一致的行為。不過，當您測試規則時，會立即看到正確的行為。如需測試規則的詳細資訊，請參閱下一節中的步驟。

測試存取控制規則

若要查看如何套用組織的存取控制規則，請從 Amazon WorkMail 主控台測試規則。

測試組織的存取控制規則

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 選擇 Access Control List (存取控制規則)。
4. 選擇測試規則。
5. 在 Request context (要求內容) 中，請選取要測試的通訊協定。
6. 在 Source IP address (來源 IP 地址) 中，輸入要測試的 IP 地址。
7. 針對 執行的請求，選擇要測試的使用者或模擬角色。
8. 選取要測試的使用者或模擬角色。
9. 選擇測試。

測試結果會出現在 Effect (效果) 下。

刪除存取控制規則

從 Amazon WorkMail 主控台刪除不再需要的存取控制規則。

> **Warning**
>
> 如果管理員刪除組織的所有存取控制規則，Amazon WorkMail 會封鎖組織信箱的所有存取。

刪除存取控制規則

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 選擇 Access Control List (存取控制規則)。
4. 選取要刪除的規則。
5. 選擇 Delete rule (刪除規則)。
6. 選擇 刪除。

設定信箱保留政策

您可以為 Amazon WorkMail 組織設定信箱保留政策。保留政策會在您選擇的期間之後，自動從使用者信箱刪除電子郵件訊息。您可以選擇要套用保留政策的信箱資料夾。此外，您可以選擇是否要為不同的資料夾設定不同的保留政策。信箱保留政策會套用至組織中所有使用者信箱中選取的資料夾。使用者無法覆寫保留政策。

設定信箱保留政策

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 選擇 Retention policy (保留政策)。
4. 針對 Folder actions (資料夾動作)，選取要包含在政策中的每個信箱資料夾旁邊的 Delete (刪除) 或 Permanently delete (永久刪除)。
5. 輸入刪除電子郵件訊息之前，將電子郵件訊息保留在每個信箱資料夾中的天數。
6. 選擇儲存。

為您的組織套用保留政策需要 48 小時。如果您選擇刪除資料夾動作，使用者可以從 Amazon WorkMail Web 應用程式和支援的用戶端復原已刪除的電子郵件訊息。如果您選擇永久刪除資料夾動作，電子郵件訊息在刪除後將無法復原。

保留政策保留項目的天數是以建立、修改或移動項目的時間為基礎。例如，如果保留政策在一年後刪除項目，則政策會從您建立或上次對該項目採取動作的日期開始計算保留天數。它不受您實作保留政策的日期影響。

使用網域

您可以設定 Amazon WorkMail 使用自訂網域。您也可以將網域設為組織的預設值，並啟用 AutoDiscover for Microsoft Outlook。

主題

新增網域

您最多可以將 100 個網域新增至 Amazon WorkMail 組織。當您新增網域時，Amazon Simple Email Service (Amazon SES傳送授權政策會自動新增至網域身分政策。這可讓 Amazon WorkMail 存取您網域的所有 Amazon SES 傳送動作，並允許您將電子郵件重新導向至您的網域。您也可以將電子郵件重新導向至外部網域。

> **Note**
>
> 最佳實務是，您應該將 <postmaster@> 和 <abuse@> 的別名新增至所有網域。如果您想要組織中的特定使用者接收傳送到這些別名的郵件，您可以為這些別名建立分發群組。

當您使用自訂網域設定 Amazon WorkMail 組織時，請記住以下有關網域 DNS 記錄的事項：

- 對於 MX 和自動探索 CNAME 記錄，我們建議將存留時間 (TTL) 值設定為 3600。減少 TTL 可確保您的郵件伺服器在您更新這些記錄或遷移信箱之後，不會使用過時或無效的 MX 記錄。
- 在您建立使用者和分發群組，然後成功遷移信箱之後，您應該更新 MX 記錄以開始將電子郵件轉送至 Amazon WorkMail。DNS 記錄的更新至多可能需要 48 小時來處理。

- 有些 DNS 供應商會自動將網域名稱附加到 DNS 記錄的結尾。新增已包含網域名稱的記錄，例如 _amazonses.example.com，可能會導致網域名稱重複，進而產生 _amazonses.example.com.example.com。為了避免網域名稱在記錄名稱內重複，請加入句號 (.) 至 DNS 記錄中的網域名稱結尾處。這會向您的 DNS 供應商指出記錄名稱完全合格，且不再與網域名稱相關。此做法也可防止 DNS 供應商附加額外的網域名稱。
- 複製的記錄名稱包含網域名稱。依據您使用的 DNS 服務，網域名稱可能已經增加至網域的 DNS 記錄。
- 建立 DNS 記錄後，請選擇 Amazon WorkMail 主控台上的重新整理圖示，以查看驗證狀態和記錄值。如需驗證網域的詳細資訊，請參閱驗證網域。
- 建議您將網域設定為MAIL FROM網域。若要為 iOS 裝置啟用 AutoDiscover，您必須將網域設定為MAIL FROM網域。您可以在 主控台的增強可交付性區段中查看MAIL FROM網域的狀態。如需詳細資訊，請參閱設定自訂 MAIL FROM 網域。

新增網域

1. 登入 AWS Management Console ，並在 https://console.aws.amazon.com/workmail/ ：// 開啟 Amazon WorkMail 主控台。
2. 如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
3. 在導覽窗格中，選擇組織，然後選擇您要新增網域的組織名稱。
4. 在導覽窗格中，選擇網域，然後選擇新增網域。
5. 在新增網域畫面上，輸入網域名稱。網域名稱只能包含基本拉丁 (ASCII) 字元。

   > **Note**
   >
   > 如果您有在 Amazon Route 53 公有託管區域中管理的網域，您可以從當您輸入網域名稱時出現的下拉式選單中選擇它。

6. 選擇新增網域。

   頁面隨即出現，並列出新網域的 DNS 記錄。頁面會將記錄分組為下列區段：

   - 網域擁有權
   - WorkMail 組態
   - 改善安全性
   - 改善電子郵件交付

每個區段都包含一或多個 DNS 記錄，且每個記錄都會顯示狀態值。下列清單顯示記錄及其可用的狀態值。

TXT 所有權

已驗證 – 記錄已解析並已驗證。

待處理 – 記錄尚未驗證。

失敗 – 無法驗證所有權。記錄不相符或是無法存取。

MX WorkMail 組態

已驗證 – 記錄已解析並已驗證。

遺失 – 無法解析記錄。

不一致 – 值不符合預期的記錄。

AutoDiscover

已驗證 – 記錄已解析並已驗證。

遺失 – 無法解析記錄。

不一致 – 值不符合預期的記錄。

> **Note**
>
> AutoDiscover 驗證程序也會檢查 AutoDiscover 設定是否正確。程序會驗證每個階段的組態設定。驗證完成時，狀態欄中已驗證旁會出現綠色核取記號。您可以將滑鼠暫留在 Verified 上，查看哪些階段已由程序驗證。如需 AutoDiscover 階段的詳細資訊，請參閱啟用 AutoDiscover 來設定端點。

DKIM CNAME

已驗證 – 記錄已解決並已驗證。

待處理 – 記錄尚未驗證

失敗 – 無法驗證所有權。記錄不相符或是無法存取。

如需 DKIM 簽署的詳細資訊，請參閱《Amazon Simple Email Service 開發人員指南》中的在 Amazon SES 中使用 DKIM 驗證電子郵件。

SPF TXT

已驗證 – 記錄已解析並已驗證。

遺失 – 無法解析記錄。

不一致 – 值不符合預期的記錄。

如需 SPF 驗證的詳細資訊，請參閱以 SPF 驗證您的電子郵件。

DMARC TXT

已驗證 – 記錄已解決並已驗證。

遺失 – 無法解析記錄。

不一致 – 值不符合預期的記錄

如需 Amazon WorkMail 中 DMARC 記錄的詳細資訊，請參閱《Amazon Simple Email Service 開發人員指南》中的使用 Amazon SES 遵守 DMARC。

TXT MAIL FROM 網域

已驗證 – 記錄已解析並已驗證。

待處理 – 記錄尚未驗證。

失敗 – 無法驗證擁有權。記錄不相符或是無法存取。

MX MAIL FROM 網域

已驗證 – 記錄已解析並已驗證。

遺失 – 無法解析記錄。

不一致 – 值不符合預期的記錄。

7. 針對下一個步驟，請根據您使用的 DNS 供應商選擇適當的動作。

如果您使用 Route 53 網域

- 在頁面頂端，選擇在 Route 53 中全部更新。

如果您使用其他 DNS 供應商

- 複製記錄並貼到您的 DNS 供應商。您可以大量複製記錄，或一次複製記錄。若要大量複製記錄，請選擇全部複製。這會建立您可以匯入 DNS 供應商的檔案區域。若要一次複製一個記錄，請選擇記錄名稱旁的重疊方塊，然後將每個方塊貼到您的 DNS 供應商。

8. 選擇重新整理圖示，更新每個記錄的狀態。這會透過 Amazon WorkMail 驗證網域的擁有權和適當的組態。

移除網域

當您不再需要網域時，可以刪除它。不過，您必須先刪除使用網域做為其電子郵件地址的任何個人或群組。

要移除網域

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 中的區域名稱和端點Amazon Web Services 一般參考。

2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在網域清單中，選取網域名稱旁的核取方塊然後選擇 Remove (刪除)。
4. 在移除網域對話方塊中，輸入要移除的網域名稱，然後選擇移除。

選擇預設網域

您可以讓與組織相關聯的網域成為該組織中使用者和群組的預設值。使網域為預設不會變更現有的電子郵件地址。

要讓網域為預設

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 中的區域名稱和端點Amazon Web Services 一般參考。

2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在網域清單中，選取您要使用的網域名稱旁的核取方塊，然後選擇設為預設。

驗證網域

在 Amazon WorkMail 主控台中新增網域之後，您必須驗證網域。驗證網域會確認您擁有網域，並將使用 Amazon WorkMail 做為網域的電子郵件服務。

您可以在 DNS 服務中新增 TXT 和 MX 記錄來驗證網域。TXT 記錄可讓您將備註新增至 DNS 服務。MX 記錄會指定傳入郵件伺服器。

您可以使用 Amazon SES 主控台建立 TXT 和 MX 記錄，然後使用 Amazon WorkMail 主控台將記錄新增至 DNS 服務。請遵循下列步驟。

建立 TXT 和 MX 記錄

1. 開啟 Amazon SES 主控台，網址為 https://console.aws.amazon.com/ses/。
2. 在導覽窗格中，選擇網域，然後選擇驗證新網域。

   隨即出現驗證新網域對話方塊。
3. 在網域方塊中，輸入您在 新增網域區段中建立的網域名稱。
4. （選用）如果您想要使用 DomainKeys 識別郵件 (DKIM)，請選取產生 DKIM 設定核取方塊。
5. 選擇 Verify This Domain (驗證此網域)。

   主控台會顯示 TXT 和 MX 記錄的清單。
6. 選擇位於 TXT 清單下的下載記錄集為 CSV 連結。

   將顯示另存新檔對話方塊。選擇下載的位置，然後選擇儲存。
7. 開啟下載的 CSV 檔案並複製其所有內容。

建立 TXT 和 MX 記錄後，您可以將它們新增至 DNS 供應商。下列步驟使用 Route 53。如果您使用不同的 DNS 提供者，但不知道如何新增記錄，請參閱提供者的文件。

1. 登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/route53/ 開啟 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted Zones (託管區域)。然後，選擇您要驗證之網域旁的選項按鈕。
3. 從網域的 DNS 記錄清單中，選擇匯入區域檔案。
4. 在區域檔案下，將複製的記錄貼到文字方塊中。檔案清單會顯示在文字方塊下方。
5. 向下捲動至清單結尾，然後選擇匯入。

> **Note**
>
> 最多需要 72 小時才能完成驗證程序。

使用 DNS 服務驗證 TXT 記錄和 MX 記錄

確認用來驗證您擁有該網域的 TXT 記錄，已正確新增至您的 DNS 服務。此程序使用 nslookup 工具，適用於 Windows 和 Linux。在 Linux 上，您也可以使用 dig。

若要使用 nslookup工具，您必須先尋找為您的網域提供服務的 DNS 伺服器。然後，您查詢這些伺服器以檢視 TXT 記錄。您可以查詢網域的 DNS 伺服器，因為這些伺服器包含網域up-to-date。這些資訊傳播到其他 DNS 伺服器可能需要一些時間。

使用 nslookup 來驗證您的 TXT 記錄是否已新增至您的 DNS 服務

1. 尋找您網域的名稱伺服器：
   a. 開啟命令提示字元 (Windows) 或終端機 (Linux)。
   b. 執行下列命令，列出為您的網域提供服務的所有名稱伺服器。以您的網域取代 *example.com*。

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

      您將在下一個步驟中查詢其中一個名稱伺服器。
2. 確認已正確新增 Amazon WorkMail TXT 記錄。
   a. 執行下列命令，將 *example.com* 取代為您的網域，並將 *ns1.name-server.net* 取代為步驟 1 的名稱伺服器。

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

b. 檢閱 輸出中顯示的"text ="字串nslookup。確認此字串符合 Amazon WorkMail 主控台中 Verified Senders 清單中網域的 TXT 值。

在下列範例中，您想要查看 _amazonses.example.com 的 TXT 記錄，其值為 fmxqxT/icOYx4aA/bEUrDPMeax9/s3frblS+niixmqk=。如果您正確更新記錄，命令具有下列輸出：

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

使用挖掘確認您的 TXT 記錄已新增至 DNS 服務

1. 開啟終端機工作階段。
2. 執行下列命令來列出您網域的 TXT 記錄。以您的網域取代 *example.com*。

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

3. 確認命令輸出TXT中後續的字串符合您在 Amazon WorkMail 主控台的 Verified Senders 清單中選取網域時看到的 TXT 值。

使用 nslookup 來驗證您的 MX 記錄已新增至您的 DNS 服務

1. 尋找您網域的名稱伺服器：

a. 開啟命令提示。

b. 執行下列命令，列出您網域的所有名稱伺服器。

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

您將在下一個步驟中查詢其中一個名稱伺服器。

2. 確認 MX 記錄已正確新增：

a. 執行下列命令，將 *example.com* 取代為您的網域，並將 *ns1.name-server.net* 取代為您在上一個步驟中識別的其中一個名稱伺服器。

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

b. 在輸出命令中，請確認連接在 `mail exchange =` 後方的字串符合以下其中一個值：

美國東部（維吉尼亞北部）區域 – `10 inbound-smtp.us-east-1.amazonaws.com`

美國西部（奧勒岡）區域 – `10 inbound-smtp.us-west-2.amazonaws.com`

歐洲（愛爾蘭）區域 – `10 inbound-smtp.eu-west-1.amazonaws.com`

> **Note**
>
> 10 代表 MX 偏好數量或優先順序。

使用挖掘來確認您的 MX 記錄已新增至 DNS 服務

1. 開啟終端機工作階段。
2. 執行下列命令來列出您網域的 MX 記錄。

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

3. 請確認連接在 MX 後方的字串符合以下其中一個值：

美國東部（維吉尼亞北部）區域 – `10 inbound-smtp.us-east-1.amazonaws.com`

美國西部（奧勒岡）區域 – `10 inbound-smtp.us-west-2.amazonaws.com`

歐洲（愛爾蘭）區域 – `10 inbound-smtp.eu-west-1.amazonaws.com`

> **Note**
>
> 10 代表 MX 偏好數量或優先順序。

網域驗證故障診斷

若要針對網域驗證的常見問題進行疑難排解，請參閱下列建議：

您的 DNS 服務不允許 TXT 記錄名稱中的底線

_amazonses 從 TXT 記錄名稱省略。

您想要多次驗證相同的網域，但不能有多個具有相同名稱的 TXT 記錄

如果您的 DNS 服務不允許您擁有多個同名的 TXT 記錄，請使用下列其中一個解決方法：

- （建議）如果您的 DNS 服務允許，請將多個值指派給 TXT 記錄。例如，如果您的 DNS 由 Amazon Route 53 管理，您可以為相同的 TXT 記錄設定多個值，如下所示：
  1. 在 Route 53 主控台中，選擇您在第一個區域中驗證網域時新增的 _amazonses TXT 記錄。
  2. 在 Value (值) 中，在第一個值後按 Enter 鍵。
  3. 新增其他區域的值，並儲存記錄集。
- 如果您只需要驗證您的網域兩次，則可以在名稱_amazonses中建立 TXT 記錄，然後在記錄名稱_amazonses中建立另一個記錄，而不建立另一個記錄。

Amazon WorkMail 主控台會回報網域驗證失敗

Amazon WorkMail 找不到 DNS 服務的必要 TXT 記錄。遵循中的程序，確認必要的 TXT 記錄已正確新增至您的 DNS 服務使用 DNS 服務驗證 TXT 記錄和 MX 記錄。

您的 DNS 供應商將網域名稱附加到 TXT 記錄的結尾

新增已包含網域名稱的 TXT 記錄，例如 _amazonses.example.com，可能會導致網域名稱重複，例如 _amazonses.example.com.example.com。為了避免網域名稱在記錄名稱內重複，請加入句號 (.) 至 TXT 記錄中的網域名稱結尾處。這會向您的 DNS 供應商指出記錄名稱完全合格，且 TXT 記錄中已包含網域名稱。

Amazon WorkMail 報告 MX 記錄不一致

從現有的郵件伺服器遷移時，MX 記錄可能會傳回不一致的狀態。更新您的 MX 記錄以指向 Amazon WorkMail，而不是指向先前的郵件伺服器。當第三方電子郵件代理與 Amazon WorkMail 搭配使用時，MX 記錄也會傳回為不一致。如果是這種情況，您可放心忽略不一致警告。

啟用 AutoDiscover 來設定端點

AutoDiscover 可讓您僅使用您的電子郵件地址和密碼來設定 Microsoft Outlook 和行動用戶端。該服務會維持與 Amazon WorkMail 的連線，並在您變更端點或設定時更新本機設定。此外，AutoDiscover 可讓用戶端使用其他 Amazon WorkMail 功能，例如離線通訊錄、Out-of-Office助理，以及檢視行事曆中空閒/忙碌時間的功能。

用戶端執行以下 AutoDiscover 階段以偵測伺服器端點 URL：

- 階段 1 – 用戶端會根據本機 Active Directory 執行安全複製通訊協定 (SCP) 查詢。如果您的用戶端沒有加入的網域，則 AutoDiscover 略過此步驟。
- 第 2 階段 – 用戶端傳送請求至下列 URLs，並驗證結果。這些端點只能使用 HTTPS。
  - https：//*company.tld*/autodiscover/autodiscover.xml
  - https://autodiscover.*company.tld*/autodiscover/autodiscover.xml
- 第 3 階段 – 用戶端執行 DNS 查詢以 autodiscover.company.tld，並從使用者的電子郵件地址傳送未經驗證的 GET 請求至衍生的端點。如果伺服器傳回一個 302 重新導向，用戶端會針對回傳的 HTTPS 端點重新傳送 AutoDiscover 的請求。

如果所有這些階段都失敗，則無法自動設定用戶端。有關手動設定行動裝置的詳細資訊，請參閱手動連接您的裝置。

當您將網域新增至 Amazon WorkMail 時，系統會提示您將 AutoDiscover DNS 記錄新增至您的提供者。這可讓用戶端執行 AutoDiscover 程序的階段 3。不過，這些步驟不適用於所有行動裝置，例如庫存 Android 電子郵件應用程式。因此，您可能需要手動設定 AutoDiscover 階段 2。

您可以使用下列方法來設定網域的 AutoDiscover 階段 2：

（建議）使用 Route 53 和 Amazon CloudFront

> **Note**
>
> 下列步驟說明如何建立 https://autodiscover.*company.tld*/autodiscover/autodiscover.xml 的代理。若要建立 https：//*company.tld*/autodiscover/autodiscover.xml 的代理，請在下列步驟中移除網域的`autodiscover.`字首。
> 使用 CloudFront 和 Route 53 可能會產生費用。如需適用定價的詳細資訊，請參閱 Amazon CloudFront 定價和 Amazon Route 53 定價。

使用 Route 53 和 CloudFront 啟用 AutoDiscover 階段 2

1. 取得 autodiscover.*company.tld* 的 SSL 憑證，並將其上傳至 AWS Identity and Access Management (IAM) 或 AWS Certificate Manager。如需詳細資訊，請參閱 IAM 使用者指南中的使用伺服器憑證，或 AWS Certificate Manager 使用者指南中的入門。
2. 建立新的 CloudFront 分佈：

1. 在 https://console.aws.amazon.com/cloudfront/v4/home 中開啟 CloudFront 主控台。
2. 在導覽窗格中，選擇 Distributions (分佈)。
3. 選擇 Create Distribution (建立分佈)。
4. 在 Web 下，選擇開始使用。
5. 在原始伺服器設定中，輸入下列值：
   - Origin 網域名稱 – 您區域的適當網域名稱：
     - 美國東部（維吉尼亞北部）— **`autodiscover-service.mail.us-east-1.awsapps.com`**
     - 美國西部（奧勒岡）— **`autodiscover-service.mail.us-west-2.awsapps.com`**
     - 歐洲（愛爾蘭）— **`autodiscover-service.mail.eu-west-1.awsapps.com`**
   - 原始通訊協定政策 – 所需的政策： **`Match Viewer`**

     > **Note**
     > 將原始路徑保留空白。請勿變更 Origin ID 的自動填入值。
6. 在預設快取行為設定中，為列出的設定選取下列值：
   - Viewer Protocol Policy (檢視器通訊協定政策)：僅 HTTPS
   - Allowed HTTP Methods (允許的 HTTP 方法)：GET、HEAD、OPTIONS、PUT、POST、PATCH、DELETE
   - Cache Based on Selected Request Headers (根據選取的請求標題快取)：所有
   - Forward Cookies (轉送 Cookies)：所有
   - Query String Forwarding and Caching (轉發和快取查詢字串)：無 (提升快取)
   - Smooth Streaming：否
   - Restrict Viewer Access (限制檢視器存取)：否
7. 請為 Distribution Settings (分佈設定) 填寫以下的值：
   - Price Class (價格分級)：只有使用美國、加拿大和歐洲
   - 對於備用網域名稱 (CNAMEs)，輸入 **`autodiscover.`*`company.tld`*** 或 ***`company.tld`***，其中 *`company.tld`* 是您的網域名稱。
   - SSL 憑證：自訂 SSL 憑證（存放在 IAM 中）

- Custom SSL Client Support (自訂 SSL 用戶端支援)：選擇 All Clients (所有用戶端) 或 Only Clients that Support Server Name Indication (SNI) (只限支援伺服器名稱指示 (SNI) 的用戶端)。舊版 Android 可能不適用於後者選項。

> **Note**
>
> 如果您選擇 All Clients (所有用戶端)，請保留 Default Root Object (預設根物件) 空白。

- Logging (記錄)：選擇 On (開啟) 或 Off (關閉)。在 上啟用記錄。
- 在 Comment (註解) 中，輸入 **`AutoDiscover type2 for autodiscover.`*`company.tld`***
- 分佈狀態：選擇已啟用。

8. 選擇 Create Distribution (建立分佈)。

3. 在 Route 53 主控台中，建立記錄，將網域名稱的網際網路流量路由到您的 CloudFront 分佈。

> **Note**
>
> 這些步驟假設 example.com 的 DNS 記錄託管在 Route 53 上。如果您不使用 Route 53，請遵循 DNS 供應商管理主控台中的程序。

1. 在主控台的導覽窗格中，選擇託管區域。，然後選擇網域。
2. 在網域清單中，選擇您要使用的網域名稱。
3. 在記錄中，選擇建立記錄。
4. 在快速建立記錄下，設定下列參數：
   - 在記錄名稱下，輸入記錄的名稱。
   - 在路由政策下，選取簡易路由。
   - 選擇別名滑桿以將其開啟。當 處於開啟狀態時，滑桿會變成藍色。
   - 在記錄類型清單中，選擇 A - 將流量路由到 IPv4 地址和一些 AWS 資源。
   - 在要列出的路由流量中，選擇 CloudFront 分佈的別名。
   - 搜尋方塊會出現在要列出的路由流量下方。在文字方塊中輸入 CloudFront 分佈的名稱。您也可以從選取搜尋方塊時顯示的清單中選取分佈。
5. 選擇建立記錄。

使用 Apache Web 伺服器

下列步驟說明如何使用 Apache Web 伺服器為 https://autodiscover.*company.tld*/autodiscover/autodiscover.xml 建立代理。若要建立 https：//*company.tld*/autodiscover/autodiscover.xml 的代理，請移除「autodiscover」。字首於網域，依以下步驟。

運用 Apache web 伺服器啟用 AutoDiscover 階段 2

1. 在啟用 SSL 的 Apache 伺服器上執行下列指令：

   ```
   SSLProxyEngine on ProxyPass /autodiscover/autodiscover.xml https://autodiscover-
   service.mail.REGION.awsapps.com/autodiscover/autodiscover.xml
   ```

2. 視需要啟用下列 Apache 模組。如果您不知道如何操作，請參閱 Apache 說明：

   - `proxy`
   - `proxy_http`
   - `socache_shmcb`
   - `ssl`

如需測試和故障診斷 AutoDiscover 的相關資訊，請參閱下一節。

AutoDiscover 階段 2 故障診斷

將 DNS 供應商設定為 AutoDiscover 後，您可以測試 AutoDiscover 端點組態。如果您已正確設定端點，則會以未經授權的請求訊息回應。

進行基本未經授權的請求

1. 從終端機建立未驗證的 POST 請求至 AutoDiscover 端點。

   ```
   $ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
   autodiscover.xml
   ```

   如果您的端點設定正確，應會傳回`401 unauthorized`訊息，如下列範例所示：

   ```
   $ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
   autodiscover.xml
   ...
   ```

```
HTTP/1.1 401 Unauthorized
```

2. 接著，測試真正的 AutoDiscover 請求。使用下列 XML 內容建立`request.xml`檔案：

```
<?xml version="1.0" encoding="utf-8"?>

<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
requestschema/2006">
    <Request>
        <EMailAddress>testuser@company.tld</EMailAddress>
        <AcceptableResponseSchema>
            http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
responseschema/2006
        </AcceptableResponseSchema>
    </Request>
</Autodiscover>
```

3. 使用您建立`request.xml`的檔案，並對端點提出已驗證的 AutoDiscover 請求。請記得將 *`testuser@company.tld`* 取代為有效的電子郵件地址：

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml
```

如果端點設定正確，回應看起來會與下列範例類似：

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml

Enter host password for user 'testuser@company.tld':
<?xml version="1.0" encoding="UTF-8"?>
<Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/
responseschema/2006" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Response xmlns="http://schemas.microsoft.com/exchange/autodiscover/mobilesync/
responseschema/2006">
    <Culture>en:us</Culture>
    <User>
        <DisplayName>User1</DisplayName>
        <EMailAddress>testuser@company.tld</EMailAddress>
    </User>
    <Action>
        <Settings>
```

```
            <Server>
                <Type>MobileSync</Type>
                <Url>https://mobile.mail.us-east-1.awsapps.com/Microsoft-Server-
ActiveSync</Url>
                <Name>https://mobile.mail.us-east-1.awsapps.com/Microsoft-Server-
ActiveSync</Name>
            </Server>
        </Settings>
    </Action>
</Response>
```

編輯網域身分政策

網域身分政策會指定電子郵件動作的許可，例如重新導向電子郵件訊息。例如，您可以將電子郵件重新導向至 Amazon WorkMail 組織中的任何電子郵件地址。

> **Note**
>
> 自 2022 年 4 月 1 日起，Amazon WorkMail 開始使用服務主體進行授權，而非 AWS 帳戶主體。如果您在 2022 年 4 月 1 日之前新增網域，則可能會有使用 AWS 帳戶主體進行授權的舊政策。若是如此，建議您更新至最新的政策。本節中的步驟說明如何進行。您的組織會在更新期間繼續正常傳送電子郵件。

只有在不使用自訂 Amazon SES 政策時，才需要遵循這些步驟。如果您使用自訂 Amazon SES 政策，則必須自行更新。如需詳細資訊，請參閱本主題自訂 Amazon SES 服務原則政策稍後的 。

> **Important**
>
> 請勿移除現有的網域。如果您這麼做，將會中斷郵件服務。您只需重新輸入現有的網域即可。

更新網域身分政策

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。若要這樣做，請開啟搜尋方塊右側的選取區域清單，然後選擇所需的區域。如需區域的詳細資訊，請參閱 中的區域和端點Amazon Web Services 一般參考。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。

3. 在導覽窗格中，選擇網域。
4. 反白顯示並複製您要重新輸入的網域名稱，然後選擇新增網域。

   新增網域對話方塊隨即出現。
5. 將複製的名稱貼到網域名稱方塊中，然後選擇新增網域。
6. 針對組織中剩餘的網域重複步驟 3-5。

自訂 Amazon SES 服務原則政策

如果您使用自訂 Amazon SES 政策，請調整此範例，以便在您的網域中使用。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AuthorizeWorkMail",
      "Effect": "Allow",
      "Principal": {
        "Service": "workmail.REGION.amazonaws.com"
      },
      "Action": [
        "ses:*"
      ],
      "Resource": "arn:aws:ses:REGION:AWS_ACCOUNT_ID:identity/WORKMAIL-DOMAIN-NAME",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn":
 "arn:aws:workmail:REGION:AWS_ACCOUNT_ID:organization/WORKMAIL_ORGANIZATION_ID"
        }
      }
    }
  ]
}
```

以 SPF 驗證您的電子郵件

寄件者政策架構 (SPF) 是一種電子郵件驗證標準，專為打擊電子郵件詐騙而設計。詐騙是讓惡意演員傳送的電子郵件看起來像合法使用者傳送的電子郵件。如需為啟用 Amazon WorkMail 的網域設定 SPF 的資訊，請參閱在 Amazon SES 中使用 SPF 驗證電子郵件。

設定自訂 MAIL FROM 網域

根據預設，Amazon WorkMail 會使用 amazonses.com 的子網域做為外寄電子郵件的MAIL FROM網域。如果網域上的 DMARC 政策僅針對 SPF 設定，這可能會導致交付失敗。若要解決此問題，請將您自己的網域設定為MAIL FROM網域。若要了解如何將電子郵件網域設定為MAIL FROM網域，請參閱《Amazon Simple Email Service 開發人員指南》中的設定自訂「寄件人」網域。

> **Important**
>
> 當您為 iOS 裝置啟用 AutoDiscover 時，需要自訂「寄件人」網域。

如需自訂MAIL FROM網域的詳細資訊，請參閱 Amazon SES 現在支援自訂 MAIL FROM 網域。

使用使用者

您可以從 Amazon WorkMail 建立和移除使用者。此外，您可以重設其電子郵件密碼、管理其信箱配額和裝置存取，以及控制其信箱許可。

主題

檢視使用者清單

檢視使用者清單

1. 在 https://console.aws.amazon.com/workmail/ ：// 開啟 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 中的區域和端點Amazon Web Services 一般參考。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇使用者 。
4. 此外，您可以依使用者名稱、顯示名稱或主要電子郵件地址篩選使用者。

> **Note**
>
> 搜尋區分大小寫。

新增使用者

當您新增使用者時，Amazon WorkMail 會自動為其建立信箱。使用者可以從 Amazon WorkMail Web 應用程式、行動裝置，或在 macOS 或 PC 上使用 Microsoft Outlook 來登入和存取其郵件。

若要新增使用者

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇您要新增使用者的組織。
3. 在導覽窗格中，選擇使用者，然後選擇新增使用者。

   隨即出現新增使用者畫面。
4. 在使用者詳細資訊的使用者名稱欄位中，輸入使用者名稱。名稱也會出現在電子郵件地址方塊中。如果您希望使用者與其使用者名稱有不同的電子郵件地址，您可以編輯電子郵件地址欄位。
5. （選用）在名字和姓氏方塊中輸入使用者的名字和姓氏。
6. 在顯示名稱方塊中，輸入使用者的顯示名稱。
7. 在電子郵件地址方塊中，接受電子郵件別名或輸入另一個別名。
8. 根據預設，使用者會顯示在全域地址清單中。若要從全域地址清單中隱藏使用者，請清除顯示全域地址清單核取方塊。
9. 選取請勿建立信箱，將使用者新增為組織的遠端使用者。
10. 在密碼設定下，在密碼和重複密碼方塊中輸入使用者的密碼。
11. 選擇新增使用者。

啟用使用者

當您將 Amazon WorkMail 與公司 Active Directory 整合時，或您的 Simple AD 目錄中已有可用的使用者時，您可以在 Amazon WorkMail 中啟用這些使用者。您也可以依照下列步驟，重新啟用其帳戶已停用的使用者。

啟用使用者

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。

2. 在導覽窗格中，選擇組織，然後選擇您要啟用使用者的組織。
3. 在導覽窗格中，選擇使用者 。

   使用者清單隨即出現。啟用、停用和系統使用者狀態的使用者帳戶會顯示在清單中。
4. 從具有已停用帳戶的使用者清單中，選取您要啟用之使用者的核取方塊，然後選擇啟用。

   啟用使用者對話方塊隨即出現。
5. 視需要檢閱和變更每個使用者的主要電子郵件地址，然後選擇啟用。

管理使用者別名

您可以新增或移除使用者的電子郵件別名。

將電子郵件別名新增至使用者

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇您要為其新增使用者的組織名稱。
3. 在導覽窗格中，選擇使用者，然後選擇您要新增別名的使用者名稱。
4. 在使用者詳細資訊區段中，選擇別名索引標籤。
5. 在別名索引標籤下，選擇新增別名。
6. 在別名方塊中，輸入別名。
7. 選取別名的網域。
8. 選擇新增。

從使用者移除電子郵件別名

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。

2. 在導覽窗格中，選擇組織，然後選擇您要從中移除使用者的組織名稱。
3. 在導覽窗格中，選擇使用者，然後選擇您要從中移除別名的使用者名稱。
4. 在使用者詳細資訊區段中，選擇別名索引標籤。
5. 在別名索引標籤下，針對您要移除的別名選取核取方塊。
6. 驗證將移除的別名。
7. 在移除別名視窗中，選擇移除。

停用使用者

您可以隨時停用組織中的任何使用者。當您停用使用者時，會立即無法存取該使用者。停用超過 30 天的使用者將從 Amazon WorkMail 中刪除其收件匣。

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇包含您要停用之使用者的組織。
3. 在導覽窗格中，選擇使用者 。

   所有使用者的清單隨即出現，顯示處於已啟用、停用和系統使用者狀態的帳戶。
4. 從已啟用的使用者清單中，選取您要停用之帳戶的核取方塊，然後選擇停用。

   停用使用者對話方塊隨即出現。
5. 選擇停用。

編輯使用者詳細資訊

編輯使用者詳細資訊時，您可以變更下列項目：

- 個人資料 – 名稱、電子郵件地址、電話號碼和其他個人資料。
- 信箱配額 （大小） – 配額範圍可從 1 MB 到 51，200 MB (50 GB)。Amazon WorkMail 會在使用者達到 90% 的配額時通知他們。此外，變更使用者的信箱配額不會影響定價。如需定價的詳細資訊，請參閱 Amazon WorkMail 定價。
- 行動裝置存取 – 移除和清除裝置，並檢視裝置詳細資訊。
- 信箱存取許可 – 授予使用者使用信箱的許可，並授予使用者不同層級的信箱存取。

- 個人存取權杖（啟用 IAM Identity Center 時）– 檢視和刪除個人存取權杖。

> **Note**
>
> 如果您將 Amazon WorkMail 與 AD Connector 目錄整合，則無法從 編輯這些詳細資訊 AWS Management Console。反之，您必須使用您的 Active Directory 管理工具編輯他們。當您的組織處於互通性模式時，則適用於限制。如需詳細資訊，請參閱互通性模式的限制。

編輯使用者詳細資訊

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇您要使用的組織。
3. 在導覽窗格中，選擇使用者，然後選擇要編輯的使用者名稱。

編輯個人資料

1. 在使用者詳細資訊區段中，選擇編輯。
2. 在使用者詳細資訊下，視需要輸入或變更使用者的個人資訊。
3. 完成後，選擇儲存變更。

與 IAM Identity Center 使用者建立關聯

1. 在使用者詳細資訊下，選擇編輯。
2. 輸入您要關聯的 IAM Identity Center 使用者的使用者 ID。您可以在 IAM Identity Center 頁面或 IAM Identity Center 主控台的指派使用者資料表下檢視此資訊。
3. 選擇 Save changes (儲存變更)。

編輯信箱配額

1. 在使用者詳細資訊下，選擇配額索引標籤，然後選擇編輯。
2. 在更新信箱配額方塊中，輸入信箱的大小。您可以將值從 輸入**1**至 **51200**。

3. 選擇 Save changes (儲存變更)。

管理行動裝置資料

> **Note**
>
> 若要管理行動裝置，您的使用者首先需要將其裝置連接到您的 Amazon WorkMail 執行個體。如需有關連接行動裝置的資訊，請參閱為 Amazon WorkMail 設定行動裝置用戶端。

1. 在使用者詳細資訊下，選擇行動裝置索引標籤。
2. 若要查看裝置的最新清單，請選擇重新整理。
3. 若要檢視裝置的詳細資訊，請從裝置 ID 欄選擇裝置名稱。
4. 若要移除或抹除裝置，請選擇裝置名稱旁的選項按鈕，然後視需要選擇移除或抹除。
5. 在出現的對話方塊中，確認移除或清除操作。請記住，當使用者再次將裝置與 Amazon WorkMail 同步時，使用者會重新出現。

編輯信箱許可

1. 選擇許可索引標籤標籤。
2. 執行下列任意一項：

    1. 若要新增許可，請選擇新增許可。開啟新增許可清單，選擇使用者或群組，選擇使用者或群組的許可設定，然後選擇儲存。
    2. 若要編輯使用者許可，請選擇使用者名稱旁的按鈕。選擇編輯，選擇所需的選項，然後選擇儲存。

    如需許可選項的詳細資訊，請參閱使用信箱許可。
3. 若要移除所有許可，請選擇移除，然後確認移除。

刪除個人存取權杖

> **Note**
>
> 請確定您刪除的字符未由任何電子郵件用戶端主動使用。在使用時刪除權杖會中斷用戶端使用權杖的身分驗證。

1. 選擇個人存取字符索引標籤。
2. 從個人存取權杖清單中，選取要刪除的個人存取權杖。
3. 選擇刪除字符。
4. 在確認文字方塊中輸入類型。

重設使用者密碼

如果使用者忘記密碼或無法登入 Amazon WorkMail，您可以重設密碼。

> **Note**
>
> - 如果您已將 Amazon WorkMail 與 AD Connector 目錄整合，則必須在 Active Directory 中重設使用者密碼。
> - 如果您已將 Amazon WorkMail 與 IAM Identity Center 整合，您可以選擇重設使用者密碼。如需詳細資訊，請參閱《 AWS IAM Identity Center 使用者指南》中的重設最終使用者的 IAM Identity Center 使用者密碼。

若要重設使用者密碼

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇使用者 。
4. 在使用者清單中，選取使用者名稱旁的核取方塊，然後選擇重設密碼。

5. 在重設密碼對話方塊中，輸入新密碼，然後選擇重設。

對 Amazon WorkMail 密碼政策進行故障診斷

如果重設密碼失敗，請確認新的密碼符合密碼政策的要求。

密碼政策需求取決於您的 Amazon WorkMail 組織使用的目錄類型。

Amazon WorkMail 目錄和 Simple AD 目錄密碼政策

根據預設，Amazon WorkMail 目錄或 Simple AD 目錄的密碼必須是：

- 非空白
- 至少八個字元
- 少於 64 個字元
- 由基本拉丁或Latin-1 補充字元組成

密碼的字元必須納入下列五種的其中三種：

- 大寫字元
- 小寫字元
- 數字 (0 到 9)
- 特殊字元 (如 <、~ 或!)
- 拉丁文-1 補充字元 (如 é、ü 或 ñ)

Amazon WorkMail 目錄密碼政策無法變更。

若要變更 Simple AD 密碼政策，請在 Simple AD 目錄的 Amazon Elastic Compute Cloud (Amazon EC2) Windows 執行個體上使用 AD 管理工具。如需詳細資訊，請參閱《 管理指南》中的安裝 Active Directory 管理工具。 AWS Directory Service

AWS Managed Microsoft AD 目錄密碼政策

如需 目錄預設密碼政策 AWS Managed Microsoft AD 的相關資訊，請參閱 AWS Directory Service 管理指南中的管理 的密碼政策 AWS Managed Microsoft AD。

AD Connector 密碼政策

AD Connector 會使用其連線之 Active Directory 網域的密碼政策。如需密碼政策設定的詳細資訊，請參閱 Active Directory 網域的文件。

使用通知

使用 Amazon WorkMail 推播通知 API，您可以接收信箱變更的推播通知，包括新的電子郵件和行事曆更新。您必須註冊 URLs（或推送通知回應者）才能接收通知。透過此功能，開發人員可以為 Amazon WorkMail 使用者建立回應式應用程式，因為應用程式會快速收到使用者信箱變更的通知。

如需詳細資訊，請參閱通知訂閱、信箱事件，以及在 Exchange 的 EWS。

您可以訂閱特定資料夾，例如收件匣或行事曆，或訂閱信箱變更事件的所有資料夾（包括新郵件、建立和修改）。

您可以使用用戶端程式庫，例如 EWS Java API 或 Managed EWS C# API 來存取此功能。推送回應程式的完整範例應用程式，使用 AWS Lambda 和 API Gateway 開發（使用 AWS Serverless 架構），可在 AWS GitHub 頁面上取得。它使用 EWS Java API。

以下是推送訂閱請求的範例：

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:t="http://
schemas.microsoft.com/exchange/services/2006/types">
   <soap:Body>
      <m:Subscribe xmlns:m="http://schemas.microsoft.com/exchange/services/2006/
messages">
         <m:PushSubscriptionRequest>
            <t:FolderIds>
               <t:DistinguishedFolderId Id="inbox" />
            </t:FolderIds>
            <t:EventTypes>
               <t:EventType>NewMailEvent</t:EventType>
               <t:EventType>CopiedEvent</t:EventType>
               <t:EventType>CreatedEvent</t:EventType>
               <t:EventType>DeletedEvent</t:EventType>
               <t:EventType>ModifiedEvent</t:EventType>
               <t:EventType>MovedEvent</t:EventType>
            </t:EventTypes>
            <t:StatusFrequency>1</t:StatusFrequency>
            <t:URL>https://YOUR_PUSH_RESPONDER_URL</t:URL>
```

```
         </m:PushSubscriptionRequest>
      </m:Subscribe>
   </soap:Body>
</soap:Envelope>
```

以下是推送訂閱請求成功的結果：

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
   <Header xmlns="http://schemas.xmlsoap.org/soap/envelope/">
      <ServerVersionInfo xmlns="http://schemas.microsoft.com/exchange/
services/2006/types" MajorVersion="14" MinorVersion="2" MajorBuildNumber="390"
 Version="Exchange2010_SP2" MinorBuildNumber="3" />
   </Header>
   <soap:Body>
      <m:SubscribeResponse xmlns:m="http://schemas.microsoft.com/exchange/
services/2006/messages" xmlns:t="http://schemas.microsoft.com/exchange/services/2006/
types">
         <m:ResponseMessages>
            <m:SubscribeResponseMessage ResponseClass="Success">
               <m:ResponseCode>NoError</m:ResponseCode>
               <m:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</m:SubscriptionId>
               <m:Watermark>AAAAAAA=</m:Watermark>
            </m:SubscribeResponseMessage>
         </m:ResponseMessages>
      </m:SubscribeResponse>
   </soap:Body>
</soap:Envelope>
```

如此一來，通知會傳送到訂閱請求中指定的 URL。以下是範例通知：

```
<soap:Envelope
    xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Header>
        <t:RequestServerVersion
            xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
            xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages"
 Version="Exchange2010_SP2">
        </t:RequestServerVersion>
    </soap:Header>
    <soap:Body>
```

```
        <m:SendNotification
            xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
            xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
            <m:ResponseMessages>
                <m:SendNotificationResponseMessage ResponseClass="Success">
                    <m:ResponseCode>NoError</m:ResponseCode>
                    <m:Notification>
                        <t:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</
t:SubscriptionId>
                        <t:PreviousWatermark>ygwAAAAAAAA=</t:PreviousWatermark>
                        <t:MoreEvents>false</t:MoreEvents>
                        <t:ModifiedEvent>
                            <t:Watermark>ywwAAAAAAA=</t:Watermark>
                            <t:TimeStamp>2018-02-02T15:15:14Z</t:TimeStamp>
                            <t:FolderId Id="AAB2L089bS1kNDgxOGYwOGE5OTQ0="></
t:FolderId>
                            <t:ParentFolderId Id="AAB2L089bS1kNDgxOGYwOGE="></
t:ParentFolderId>
                        </t:ModifiedEvent>
                    </m:Notification>
                </m:SendNotificationResponseMessage>
            </m:ResponseMessages>
        </m:SendNotification>
    </soap:Body>
</soap:Envelope>
```

要確認推送通知回應方收到通知，必須回覆如下：

```
<?xml version="1.0"?>
  <s:Envelope xmlns:s= "http://schemas.xmlsoap.org/soap/envelope/">
    <s:Body>
      <SendNotificationResult xmlns="http://schemas.microsoft.com/exchange/
services/2006/messages">
        <SubscriptionStatus>OK</SubscriptionStatus>
      </SendNotificationResult>
    </s:Body>
  </s:Envelope>
```

要取消訂閱接收推送通知，用戶端必須傳送於 SubscriptionStatus 欄位的取消訂閱回應，類似以下：

```
<?xml version="1.0"?>
  <s:Envelope xmlns:s= "http://schemas.xmlsoap.org/soap/envelope/">
```

```
    <s:Body>
      <SendNotificationResult xmlns="http://schemas.microsoft.com/exchange/
services/2006/messages">
        <SubscriptionStatus>Unsubscribe</SubscriptionStatus>
      </SendNotificationResult>
    </s:Body>
  </s:Envelope>
```

若要驗證推播通知回應者的運作狀態，Amazon WorkMail 會傳送「heartbeat」（也稱為 StatusEvent)。傳送的頻率取決於在初始訂閱請求所提供的 StatusFrequency 參數。例如，如果 StatusFrequency等於 **1**，StatusEvent則會每 1 分鐘傳送一次 。這個值的範圍介於 1 和 1440 分鐘之間。此 StatusEvent 看起來類似如下：

```
<?xml version="1.0 (http://www.w3.org/TR/REC-xml/)" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<soap:Header>
    <t:RequestServerVersion xmlns:t="http://schemas.microsoft.com/exchange/
services/2006/types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/
messages" Version="Exchange2010_SP2"/>
</soap:Header>
<soap:Body>
    <m:SendNotification xmlns:t="http://schemas.microsoft.com/exchange/services/2006/
types" xmlns:m="http://schemas.microsoft.com/exchange/services/2006/messages">
    <m:ResponseMessages>
        <m:SendNotificationResponseMessage ResponseClass="Success">
            <m:ResponseCode>NoError</m:ResponseCode>
            <m:Notification>
                <t:SubscriptionId>hKJETtoAdi9PPW0tZDQ4MThmMDoVYB</t:SubscriptionId>
                <t:PreviousWatermark>AAAAAAAAAAA=</t:PreviousWatermark>
                <t:MoreEvents>false</t:MoreEvents>
                <t:StatusEvent>
                    <t:Watermark>AAAAAAAAAAA=</t:Watermark>
                </t:StatusEvent>
            </m:Notification>
        </m:SendNotificationResponseMessage>
    </m:ResponseMessages>
</m:SendNotification>
</soap:Body>
</soap:Envelope>
```

如果用戶端推送通知回應者無法以與之前相同的OK狀態回應，則會重試通知最多 StatusFrequency 分鐘。例如，如果 StatusFrequency 等於 5 且第一個通知失敗，它會重試最多 5 分鐘且在每個重試

中以指數退避。如果在重試時間過後未傳送通知，訂閱會失效，而且不會傳送新的通知。您必須建立新的訂閱以持續收到信箱事件的通知。目前，每個信箱最多可以訂閱三個訂閱。

啟用簽章或加密的電子郵件

您可以使用 S/MIME 讓使用者在組織內部和外部傳送已簽署或加密的電子郵件。

> **Note**
>
> 全球地址清單 (GAL) 的使用者憑證僅於連結的 Active Directory 設定支援。

要讓使用者傳送簽章或加密的電子郵件

1. 設定 Active Directory (AD) Connector。以您的現場部署目錄設定 Active Directory (AD) Connector 讓使用者可以繼續使用他們現有的企業登入資料。
2. 設定 Certificate Autoenrollment 以自動發行和存放 Active Directory 中的使用者憑證。Amazon WorkMail 會從 Active Directory 接收使用者憑證，並將其發佈至 GAL。如需詳細資訊，請參閱設定 Certificate Autoenrollment 。
3. 將產生的憑證從執行 Microsoft Exchange 的伺服器匯出並郵寄給使用者。
4. 每個使用者安裝憑證至他們的電子郵件計劃 (例如 Windows Outlook) 和行動裝置。

使用 群組

您可以使用群組做為 Amazon WorkMail 中的分發清單，以接收一般電子郵件地址的電子郵件，例如 <sales@example.com> 或 <support@example.com>。一個群組可建立多個電子郵件別名。

您也可將群組做為安全群組，藉此與特定團隊共用信箱或行事曆。

群組沒有自己的信箱，這會影響您可以授予群組的信箱許可。如需設定群組信箱許可的資訊，請參閱管理群組的信箱許可。

> **Note**
>
> 在新增的群組出現在您的 Microsoft Outlook 離線通訊錄之前可能要花費長達 2 個小時。

主題

檢視群組清單

檢視群組清單

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 中的區域和端點Amazon Web Services 一般參考。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。

3. 在導覽窗格中，選擇 Groups (AS 安全群組)。
4. 此外，您可以依群組名稱或主要電子郵件地址篩選群組。

> **Note**
>
> 搜尋區分大小寫。

新增群組

您可以從 Amazon WorkMail 主控台新增群組。

新增群組

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域 在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇群組，然後選擇新增群組。

   隨即顯示新增群組頁面。
4. 在群組名稱下，輸入群組的名稱。
5. 在電子郵件地址下，輸入群組的主要電子郵件地址。
6. 驗證群組的電子郵件地址，並視需要更新。
7. 根據預設， 群組會顯示在全域地址清單中。若要從全域地址清單中隱藏群組，請清除顯示全域地址清單核取方塊。
8. 選擇 Add group (新增群組)。

啟用群組

當您將 Amazon WorkMail 與公司 Active Directory 整合時，或您的簡易 Active Directory 中已有可用的群組，您可以使用這些群組做為 Amazon WorkMail 中的安全群組或分發清單。

要啟用現有目錄群組

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。

2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 Groups (AS 安全群組)。
4. 選擇您要啟用的群組旁的核取方塊，然後選擇啟用。

   啟用群組對話方塊隨即出現，並要求您確認操作。
5. 視需要檢閱和變更每個群組的主要電子郵件地址，然後選擇啟用。

將成員新增至群組

建立並啟用 Amazon WorkMail 群組之後，請使用 Amazon WorkMail 主控台將成員新增至該群組。

> **Note**
>
> 如果 Amazon WorkMail 與連線的 Active Directory 服務或 Microsoft Active Directory 整合，您可以使用 Active Directory 來管理您的群組成員。不過，變更可能需要更長的時間才能傳播至 Amazon WorkMail。

將成員新增至群組

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 Groups (AS 安全群組)。
4. 選取群組的名稱。
5. 在群組詳細資訊頁面上，選擇成員索引標籤。
6. 在群組或使用者下選擇要新增的群組或使用者。
7. 從下拉式清單中選取使用者或群組。
8. 選擇 Save (儲存)。

您的變更可能需要幾分鐘的時間才能傳播。

編輯群組詳細資訊

您可以編輯群組的詳細資訊。

編輯群組詳細資訊

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇群組，然後選擇要編輯的群組。
4. 在群組詳細資訊頁面上，視需要更新電子郵件地址。
5. 根據預設， 群組會顯示在全域地址清單中。若要從全域地址清單中隱藏群組，請清除顯示全域地址清單核取方塊。
6. 選擇 Save changes (儲存變更)。

從群組移除成員

使用 Amazon WorkMail 主控台從群組中移除成員。

> **Note**
>
> 如果 Amazon WorkMail 與連線的 Active Directory 或 Microsoft Active Directory 整合，您可以使用 Active Directory 來管理您的群組成員。不過，這樣做可以建立將變更傳播到 Amazon WorkMail 所需的時間。

從群組中移除成員

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇群組，然後選擇群組的名稱。

4. 在群組詳細資訊頁面上，選擇成員索引標籤。
5. 選取要從群組中移除的成員。
6. 選擇移除。

您的變更可能需要幾分鐘的時間才能傳播。

管理群組別名

您可以新增或移除群組的電子郵件別名。

將電子郵件別名新增至群組。

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇您要為其新增別名的組織名稱。
3. 在導覽窗格中，選擇群組，然後選擇您要新增別名的群組名稱。
4. 在群組詳細資訊區段中，選擇別名。
5. 在別名下，選擇新增別名。
6. 在別名方塊中，輸入別名。
7. 選取別名的網域。
8. 選擇新增。

從群組中移除電子郵件別名。

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇您要從中移除別名的組織名稱。
3. 在導覽窗格中，選擇群組，然後選取您要從中移除別名的群組名稱。
4. 在群組詳細資訊區段中，選擇別名。
5. 在別名下，針對您要移除的別名選取核取方塊。

6. 選擇移除。
7. 驗證將移除的別名。
8. 在移除別名視窗中，選擇移除。

停用群組

當您不再需要該群組時，可以停用它。

停用群組

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 Groups (AS 安全群組)。
4. 在群組名稱下，選取要停用的群組，然後選擇停用。
5. 在 Disable group(s) (停用群組) 對話方塊中，選擇 Disable (停用)。

刪除群組

您必須先停用該群組，才能刪除群組。如需停用群組的詳細資訊，請參閱 停用群組。

刪除群組

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 Groups (AS 安全群組)。
4. 選取您要刪除之已停用群組旁的核取方塊，然後選擇刪除。

   刪除對話方塊隨即出現。
5. 在輸入群組名稱以確認刪除方塊中，輸入群組的名稱，然後選擇刪除 。

> **Note**
>
> 若要永久刪除群組，請使用 Amazon WorkMail 的 `DeleteGroup` API 動作。如需詳細資訊，請參閱《Amazon WorkMail API 參考》中的 DeleteGroup。

使用 資源

Amazon WorkMail 可協助您的使用者保留資源。例如，使用者可以預留會議室或設備，例如投影機、電話或汽車。若要預訂資源，使用者會將資源新增至會議邀請。

主題

檢視資源清單

檢視資源清單

1. 在 https://console.aws.amazon.com/workmail/ : // 開啟 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 中的區域和端點Amazon Web Services 一般參考。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 Resources (資源)。
4. 此外，您可以依資源名稱或主要電子郵件地址篩選資源。

> **Note**
>
> 搜尋區分大小寫。

新增資源

您可以將新資源新增至組織，並允許使用者進行保留。

要新增資源

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇資源，然後選擇新增資源。

   隨即顯示新增資源頁面。
4. 在資源名稱方塊中，輸入資源的名稱。
5. 或者，在資源描述方塊中，輸入資源的描述。
6. 在資源類型下，選擇一個選項。
7. 驗證資源的電子郵件地址，並視需要更新。
8. 根據預設，資源會顯示在全域地址清單中。若要從全域地址清單中隱藏資源，請清除顯示全域地址清單核取方塊。
9. 選擇 Add resource (新增資源)。

編輯資源詳細資訊

您可以編輯資源的一般詳細資訊，包括名稱、描述、類型和電子郵件地址、預訂選項和委派。

要編輯一般資源詳細資訊

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 Resources (資源)，然後選擇要編輯的資源。
4. 在資源詳細資訊頁面上，視需要更新資源名稱、描述、資源類型或電子郵件地址。
5. 根據預設，資源會顯示在全域地址清單中。若要從全域地址清單中隱藏資源，請清除顯示全域地址清單核取方塊。
6. 選擇 Save changes (儲存變更)。

您可以設定資源以接受或拒絕自動預訂請求。

您可以編輯資源的預訂選項。

變更資源的預訂選項

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 Resources (資源)，然後選擇要編輯的資源。頁面隨即出現，並顯示資源詳細資訊。
4. 在預訂選項下，選擇編輯。
5. 視需要選取或清除選項旁的核取方塊，以啟用或停用選項。

> **Note**
>
> 當您停用任何自動預訂選項時，您必須建立委派以處理預訂請求。後續步驟說明如何建立委派。

您可以新增委派，以控制未設定自動預訂選項之資源的預訂請求。資源自動委派接收所有預訂請求的副本和完整存取資源行事曆。此外，他們必須接受資源的所有預訂請求。

要新增資源委派代表

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇資源，然後選擇您要新增委派的資源名稱。
4. （選用）在預訂選項索引標籤中，選擇編輯，清除自動接受所有資源請求核取方塊，然後選擇儲存。
5. 選擇委派標籤，然後選擇新增委派。

隨即顯示新增委派對話方塊。

6. 開啟搜尋委派清單，然後選擇委派，然後選擇儲存。

移除資源委派

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。

2. 在導覽窗格中，選擇組織，然後選擇您要從中移除委派者的組織名稱。
3. 在導覽窗格中，選擇資源，然後選擇您要從中移除委派的資源名稱。
4. 選擇委派代表，然後選擇要移除的委派代表。
5. 選擇移除。

管理資源別名

您可以新增或移除資源的電子郵件別名。

將電子郵件別名新增至資源

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。

2. 在導覽窗格中，選擇組織，然後選擇您要新增別名的組織名稱。
3. 在導覽窗格中，選擇資源，然後選擇您要新增別名的資源名稱。
4. 在資源詳細資訊區段中，選擇別名。
5. 在別名下，選擇新增別名。
6. 在別名方塊中，輸入別名。
7. 選取別名的網域。
8. 選擇新增。

從資源中移除電子郵件別名

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇您要從中移除別名的組織名稱。
3. 在導覽窗格中，選擇資源，然後選擇您要從中移除別名的資源名稱。
4. 在資源詳細資訊區段中，選擇別名。
5. 在別名下，針對您要移除的別名選取核取方塊。
6. 選擇移除。
7. 驗證將移除的別名。
8. 在移除別名視窗中，選擇移除。

啟用資源

根據預設，Amazon WorkMail 會建立 資源。如果您或其他人停用資源，您可以在 30 天內重新啟用資源。

啟用資源

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需區域的詳細資訊，請參閱 中的區域和端點Amazon Web Services 一般參考。
2. 在導覽窗格中，選擇組織，然後選擇包含您要啟用之資源的組織。
3. 在導覽窗格中，選擇 Resources (資源)。
4. 在資源清單中，選取您要啟用的資源旁的按鈕，然後選擇啟用。

   啟用資源對話方塊隨即出現。
5. 選擇 啟用 。

停用資源

當您停用資源時，會使其無法進行預訂。例如，您可以在會議室進行重新建模時停用會議室，然後在會議室可供使用時啟用該會議室。

停用資源

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需區域的詳細資訊，請參閱 中的區域和端點Amazon Web Services 一般參考。
2. 在導覽窗格中，選擇組織，然後選擇包含您要停用之資源的組織。
3. 在導覽窗格中，選擇 Resources (資源)。
4. 在資源清單中，選取您要停用的資源旁的按鈕，然後選擇停用。

   停用資源對話方塊隨即出現。
5. 選擇停用。

刪除資源

當您不再需要資源時，您可以將其刪除。不過，您必須先停用資源。如需停用資源的資訊，請參閱上一節中的步驟。

要移除資源

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需區域的詳細資訊，請參閱 中的區域和端點Amazon Web Services 一般參考。
2. 在導覽窗格中，選擇組織，然後選擇所需的組織。
3. 在導覽窗格中，選擇 Resources (資源)。
4. 在資源清單中，選取您要移除的已停用資源旁的按鈕，然後選擇刪除。

   刪除資源對話方塊隨即出現。
5. 在輸入資源名稱以確認刪除方塊中，輸入您要刪除的資源名稱，然後選擇刪除資源。

使用 IAM Identity Center

您可以將 Amazon WorkMail 使用者與 IAM Identity Center 建立關聯，以在 Amazon WorkMail 中啟用多重驗證 (MFA)。如需詳細資訊，請參閱什麼是 IAM Identity Center。

下表說明處理不同案例的步驟。

案例	步驟
將 Amazon WorkMail 使用者與 IAM Identity Center 建立關聯	1. 在 Amazon WorkMail 中啟用 IAM Identity Center 2. 將 IAM Identity Center 使用者和群組指派給 Amazon WorkMail 應用程式 3. 將 Amazon WorkMail 使用者與 IAM Identity Center 使用者建立關聯
現有的 Amazon WorkMail 使用者	1. 使用相同的使用者名稱建立 IAM Identity Center 使用者、將使用者分組在一起，並將群組指派給 Amazon WorkMail 應用程式。 2. 將 Amazon WorkMail 使用者與 IAM Identity Center 使用者建立關聯。
現有的 IAM Identity Center 使用者	1. 使用與 IAM Identity Center 使用者相同的使用者名稱建立 Amazon WorkMail 使用者。 2. 將 IAM Identity Center 使用者或群組指派給 Amazon WorkMail 應用程式。 3. 將 Amazon WorkMail 使用者與 IAM Identity Center 使用者建立關聯。
將外部目錄連線至 IAM Identity Center	1. 將外部目錄使用者同步至 IAM Identity Center 群組。如需詳細資訊，請參閱 IAM Identity Center Identity 來源教學課程 2. 將 IAM Identity Center 群組指派給 Amazon WorkMail 應用程式。 3. 將外部目錄連接至 Amazon WorkMail，並確保使用者名稱相符

案例	步驟
	4. 將 Amazon WorkMail 使用者與 IAM Identity Center 使用者建立關聯。

完成上述步驟後，您可以在 Amazon WorkMail 主控台的設定下，檢視 IAM Identity Center 狀態、連結至 AWS IAM Identity Center 以管理使用者和群組、啟用 MFA 的 Amazon WorkMail Web 應用程式 URL、身分驗證模式、個人存取字符狀態和 IAM Identity Center 下的時間軸。如需在 IAM Identity Center 主控台中管理 MFA 的詳細資訊，請參閱 IAM Identity Center 使用者的多重驗證。

> **Note**
>
> 確定 Amazon WorkMail 和 IAM Identity Center 之間的組態經過良好測試和驗證。當組態不正確且不完整時，使用者可能會失去對其信箱的存取權。

主題

在 Amazon WorkMail 中啟用 IAM Identity Center

當您啟用 IAM Identity Center 時，它會充當 Amazon WorkMail 使用者的身分驗證層。IAM Identity Center 使用者與 Amazon WorkMail 目錄分開管理。建議跨 IAM Identity Center 和 Amazon WorkMail 使用相同的使用者名稱。

> **Note**
>
> 確定 Amazon WorkMail 和 IAM Identity Center 是在相同的區域中設定。

若要啟用 IAM Identity Center，請遵循下列步驟。

1. 開啟 Amazon WorkMail 主控台，網址為 https：//https://console.aws.amazon.com/workmail/.。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱《》中的區域和端點Amazon Web Services 一般參考。

2. 在導覽窗格中，選擇身分中心。

   IAM Identity Center Settings 頁面隨即出現。

3. 選擇 啟用 。

   啟用 IAM Identity Center 視窗隨即出現。

4. 選擇 啟用 。

   身分中心設定頁面會顯示身分中心狀態。

5. 若要將 IAM Identity Center 使用者和群組新增至 Amazon WorkMail Organization，請遵循 Identity Center 狀態下方的連結。如需如何新增使用者和群組的資訊，請參閱在 IAM Identity Center 中管理身分。

將 IAM Identity Center 使用者和群組指派給 Amazon WorkMail 應用程式

當您在 Amazon WorkMail 中啟用 IAM Identity Center 時，WorkMail 會代表您在 IAM Identity Center 中建立應用程式。根據預設，IAM Identity Center 使用者必須指派給此應用程式，或屬於指派給此應用程式的群組，才能存取 Amazon WorkMail 組織中的信箱。如需詳細資訊，請參閱 AWS IAM Identity Center 《 使用者指南》中的AWS 受管應用程式。

您可以透過下列方式將 IAM Identity Center 使用者和群組指派給 Amazon WorkMail：

- 依 IAM Identity Center 使用者 – 您可以將 IAM Identity Center 使用者指派給 Amazon WorkMail。
- 依 IAM Identity Center 群組 – 您可以將 IAM Identity Center 群組指派給 Amazon WorkMail。透過新增群組，群組下的所有使用者都可以存取 Amazon WorkMail。

  如需新增使用者和群組的詳細資訊，請參閱 IAM Identity Center 中的使用者、群組和佈建。

> **Note**
>
> 如果您要將現有身分來源與 IAM Identity Center 連線，請在變更目錄來源之前檢閱以下內容。
>
> - 您的身分驗證是由 IAM Identity Center 管理。
> - Amazon WorkMail 將保留所有 Amazon WorkMail 使用者和群組。
> - IAM Identity Center 將保留所有 IAM Identity Center 使用者、群組和指派。
> - 您必須在 Amazon WorkMail 主控台中管理 Amazon WorkMail 使用者和群組。
> - 您必須在 IAM Identity Center 中管理 IAM Identity Center 使用者和群組。
> - 沒有 IAM Identity Center 指派或使用者關聯的使用者無法存取 Amazon WorkMail。
> - 您必須在 IAM Identity Center 中管理 MFA 政策控制。
> - 當您在 IAM Identity Center 中將 IAM Identity Center 來源變更為管理 Active Directory 或從中變更時，您必須停用 Amazon WorkMail 中現有的 IAM Identity Center 組態，並重新設定以將 Amazon WorkMail 使用者與 IAM Identity Center 建立關聯。

與 IAM Identity Center 目錄同步的使用者和群組可指派給您的 Amazon WorkMail 應用程式。如需 IAM Identity Center 使用者和群組管理的詳細資訊，請參閱 IAM Identity Center 中的常見任務入門。

若要將 IAM Identity Center 使用者和群組指派給 Amazon WorkMail，請遵循下列步驟。

1. 開啟 Amazon WorkMail 主控台，網址為 https：//https://console.aws.amazon.com/workmail/.。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱《》中的區域和端點Amazon Web Services 一般參考。

2. 在導覽窗格中，選擇身分中心。

   IAM Identity Center Settings 頁面隨即出現。

3. 選擇指派使用者和群組。

   您可以新增和指派新使用者，或指派現有的使用者和群組。

   - 指派使用者 – 您可以將個別 IAM Identity Center 使用者指派給 Amazon WorkMail。您可以建立新的 IAM Identity Center 使用者或搜尋現有的使用者。
   - 指派群組 – 您也可以將 IAM Identity Center 群組指派給 Amazon WorkMail。然後，群組的所有成員都會指派給 Amazon WorkMail。

> **Note**
>
> 根據預設，所有新的 IAM Identity Center 使用者都會在 IAM Identity Center 中啟用。若要授予 Amazon WorkMail 的存取權，您必須在 IAM Identity Center 中設定其密碼，並將其指派給 Amazon WorkMail。如需詳細資訊，請參閱將使用者新增至 Identity Center 目錄。

將 Amazon WorkMail 使用者與 IAM Identity Center 使用者建立關聯

當使用者使用其 IAM Identity Center 使用者憑證登入 Amazon WorkMail Web 用戶端時，用戶端將開啟相關聯 Amazon WorkMail 使用者的信箱。如果 WorkMail 組織中沒有使用者與 IAM Identity Center 使用者相關聯，WorkMail 將在 IAM Identity Center 使用者登入與具有相同使用者名稱的 WorkMail 使用者之間建立關聯，如果該 WorkMail 使用者存在。否則，用戶端會顯示錯誤訊息給使用者。

> **Note**
>
> 建議您對 Amazon WorkMail 和 IAM Identity Center 的使用者使用相同的使用者名稱，因為 WorkMail使用者第一次使用其 IAM Identity Center 使用者憑證登入 Amazon WorkMail Web 用戶端時，WorkMail 會自動建立關聯。當使用者名稱不同時，您需負責建立關聯。

若要關聯使用者，請依照下列步驟進行。

1. 開啟 Amazon WorkMail 主控台，網址為 http：//https://console.aws.amazon.com/workmail/。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱《》中的區域和端點Amazon Web Services 一般參考。

2. 在導覽窗格中，選擇身分中心。

   IAM Identity Center Settings 頁面隨即出現。

3. 選擇關聯使用者。
4. 在選取 WorkMail 使用者下，選取您要關聯的 Amazon WorkMail 使用者。
5. 在輸入 IAM Identity Center 使用者 ID 下，輸入您要關聯的 IAM Identity Center 使用者 ID。您可以從 Identity Center 頁面上的指派使用者索引標籤複製 ID。

> **Note**
>
> IAM Identity Center 使用者必須獲得授權才能存取 Amazon WorkMail 應用程式。

6. 選擇關聯使用者。

   一旦關聯成功，Amazon WorkMail 使用者可以使用 MFA IAM Identity Center 憑證登入 Amazon WorkMail。

> **Note**
>
> 當您編輯 Amazon WorkMail 使用者詳細資訊時，也可以將 Amazon WorkMail 使用者與 IAM Identity Center 使用者建立關聯。如需詳細資訊，請參閱編輯使用者詳細資訊。

身分驗證方式

您可以使用身分驗證模式，允許使用者使用其 Amazon WorkMail 目錄登入資料、其 IAM Identity Center 登入資料，或限制僅登入 IAM Identity Center 登入資料。

Amazon WorkMail 提供兩種身分驗證模式。

> **Note**
>
> 身分驗證模式的選擇取決於組織的安全需求和使用者體驗偏好設定。建議您只使用 IAM Identity Center 模式，因為它透過強制執行 IAM Identity Center 憑證和 MFA 來提供增強的安全性。不過，從 Amazon WorkMail Directory 和 IAM Identity Center 模式切換之前，請務必與所有使用者一起測試 MFA 程序，以確保順利轉換，並避免對現有電子郵件用戶端存取造成任何影響。

- Amazon WorkMail Directory 和 IAM Identity Center （建議用於測試） – 這是預設選項，可讓您在切換到生產模式之前測試 IAM Identity Center 關聯。測試模式可讓使用者同時使用 Amazon WorkMail 目錄和 IAM Identity Center 登入資料來登入 Amazon WorkMail Web 用戶端。當您從組織設定共用 Amazon WorkMail Web 應用程式 URL 時，您的使用者可以使用其 Amazon WorkMail 目錄憑證登入。當您從 IAM Identity Center 設定共用已啟用 MFA 的 URL 時，使用者可以使用其 IAM 憑證登入。

- 僅限 IAM Identity Center （建議用於生產） – 此身分驗證模式僅允許您使用 IAM Identity Center 憑證登入 Amazon WorkMail 用戶端信箱。對於任何現有的 Amazon WorkMail 使用者，Amazon WorkMail 目錄憑證不再對 Amazon WorkMail Web 應用程式和任何現有的電子郵件用戶端有效。您可以使用任何電子郵件用戶端請求個人存取字符來存取信箱。為了避免失去信箱的存取權，請確保為所有 Amazon WorkMail 使用者啟用 MFA。

若要啟用身分驗證模式，請遵循下列步驟。

1. 在身分中心設定頁面下，選擇身分驗證模式索引標籤。
2. 選擇編輯。

   編輯身分驗證模式頁面隨即出現。
3. 選擇下列其中之一：

   - 僅限 IAM Identity Center
   - Amazon WorkMail 目錄和 IAM Identity Center
4. 選擇儲存。

設定個人存取字符

您可以啟用個人存取字符，讓 Amazon WorkMail 使用者使用桌面和行動電子郵件用戶端來存取其信箱。啟用 IAM Identity Center 後，依預設，個人存取字符狀態會設為作用中，有效期為 365 天。啟用 IAM Identity Center 之後，您使用者的現有登入資料將不再有效，無法登入其電子郵件用戶端。您的使用者可以從 Amazon WorkMail Web 應用程式產生個人存取字符，並使用它登入任何電子郵件用戶端。您可以編輯個人存取字符過期，當字符過期時，您的使用者可以產生新的字符。

> **Note**
>
> - 當您在 Amazon WorkMail 中建立個人存取權杖時，您的使用者只能檢視和複製一次。如果您遺失個人存取權杖，基於安全考量，您將需要產生新的存取權杖。
> - 當 Amazon WorkMail 使用者與有權存取 Amazon WorkMail 應用程式的 IAM Identity Center 使用者相關聯時，Amazon WorkMail 僅允許信箱存取的個人存取字符。

個人存取字符組態如下所示：

- 作用中 – 當個人存取字符狀態設定為作用中時，您的使用者可以從 Amazon WorkMail 產生個人存取字符，並在字符生命週期內使用該字符登入任何電子郵件用戶端。
- 非作用中 – 當個人存取字符狀態設定為非作用中時，您的使用者將無法產生或使用個人存取字符來存取信箱。
- 權杖生命週期 – 根據預設，個人存取權杖的有效期為 365 天。您可以選擇變更個人存取字符生命週期。當您將生命週期設定保留空白時，字符會有無限的生命週期且永遠不會過期。

若要設定個人存取字符，請遵循下列步驟。

1. 在身分中心設定頁面下，選擇個人存取字符組態索引標籤。
2. 選擇編輯。

   隨即出現編輯個人字符組態頁面。
3. 在字符狀態下，滑動作用中按鈕以啟用個人存取字符。
4. 在字符存留期（以天為單位）文字方塊中，輸入個人存取字符可以啟用的天數。
5. 選擇儲存。

停用 IAM Identity Center

您可以從 Amazon WorkMail 主控台停用 IAM Identity Center。停用後，您就無法使用 IAM Identity Center 登入資料或個人存取字符來存取信箱。建議重設所有使用者密碼，Amazon WorkMail 使用者將使用 Amazon WorkMail Directory 登入資料還原為 。

> **Note**
>
> 請檢查以下內容：
>
> - 停用 IAM Identity Center 後，Amazon WorkMail 和 IAM Identity Center 使用者和群組將保持不變。
> - 現有的使用者關聯將繼續存在。
> - 您的身分驗證將還原為由 Amazon WorkMail 目錄管理，而不是由 IAM Identity Center 管理。

若要停用 IAM Identity Center，請遵循下列步驟。

1. 在身分中心設定頁面下，選擇停用。

   停用 IAM Identity Center 頁面隨即出現。

2. 選擇確認。

使用行動裝置

本節中的主題說明如何管理連線至 Amazon WorkMail 的行動裝置。

主題

編輯您的組織行動裝置政策

您可以編輯組織的行動裝置政策，以變更行動裝置與 Amazon WorkMail 互動的方式。

編輯您的組織的行動裝置政策

1. 在 https://console.aws.amazon.com/workmail/ ：// 開啟 Amazon WorkMail 主控台。

   如有需要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 中的區域名稱和端點Amazon Web Services 一般參考。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中選擇 Mobile Policies (行動政策)，然後在 Mobile policy (行動政策) 畫面中選擇 Edit (編輯)。
4. 根據需求更新任何以下操作：

   a. Require encryption on device (裝置上的加密需求)：加密行動裝置上的電子郵件資料。

   b. Require encryption on storage card (儲存卡上的加密需求)：加密行動裝置上可移除儲存的電子郵件資料。

   c. 需要密碼：需要密碼才能解鎖行動裝置。

   d. 允許簡單的密碼：使用裝置的 PIN 做為密碼。

   e. 密碼長度下限：設定有效密碼所需的字元數。

   f. 需要英數字元密碼：需要由字母和數字組成的密碼。

g. 允許的失敗嘗試次數：指定清除使用者裝置之前允許的失敗裝置解除鎖定嘗試次數。所有資料，包括個人檔案，都會在清除裝置時刪除。

h. Password expiration (密碼過期)：指定密碼過期幾天前必須變更。

i. Enable screen lock (啟用螢幕鎖定)：指定使用者沒有任何輸入並鎖定使用者的畫面前經過的秒數。

j. Enforce password history (強制密碼歷史記錄)：指定輸入的密碼可重複的字數。

5. 選擇 Save (儲存)。

管理行動裝置

本節中的主題說明如何遠端抹除行動裝置、從您的組織中移除裝置，以及檢視裝置的詳細資訊。如需有關編輯您組織行動裝置政策的更多資訊，請參閱 編輯您的組織行動裝置政策。

主題

- 遠端抹除行動裝置
- 從裝置清單移除使用者裝置
- 檢視行動裝置詳細資訊

遠端抹除行動裝置

本節中的步驟說明如何遠端清除行動裝置。請記得以下事項：

- 裝置必須上線並連線至 Amazon WorkMail。如果有人中斷連線裝置，清除操作會在使用者重新連線裝置時繼續。
- 清除操作可能需要五分鐘的時間才能傳播。

> **Important**
>
> 對於大多數行動裝置，遠端抹除會重設裝置為原廠預設值。當執行此程序時，您可以移除所有資料，包括個人檔案。

要從遠端抹除使用者的行動裝置

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

如有需要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 中的區域名稱和端點Amazon Web Services 一般參考。

2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇使用者，然後在使用者清單中，選取您需要清除其裝置的使用者名稱。
4. 選擇行動裝置索引標籤。
5. 在裝置清單中，選擇裝置旁的按鈕，然後選擇清除。
6. 檢查概觀中的狀態，以查看是否請求清除。
7. 清除裝置後，請從裝置清單中移除它。下一節中的步驟說明如何進行。

> **Important**
>
> 若要將清除的裝置傳回使用者的裝置清單，請確定您先將其從裝置清單中移除。否則，系統會再次清除裝置。

從裝置清單移除使用者裝置

如果有人停止使用特定的行動裝置，或者您已遠端抹除裝置，您可以從裝置清單中移除裝置。當使用者再次設定裝置，它會顯示在清單中。

要從裝置清單移除使用者的行動裝置

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有需要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇使用者，然後選擇使用者名稱。
4. 選擇行動裝置索引標籤。
5. 在裝置清單中，選取裝置旁的按鈕，然後選擇移除。

檢視行動裝置詳細資訊

您可以檢視使用者行動裝置的詳細資訊。

> **Note**
>
> 有些裝置不會將所有詳細資訊傳送至伺服器。您可能看不到所有可用的裝置詳細資訊。

要檢視裝置的詳細資訊

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要請變更區域。從導覽列，選取符合您需求的區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中，選擇使用者，然後選擇行動裝置索引標籤。
4. 在裝置清單中，選取您要檢視其詳細資訊的裝置 ID。

   下表列出裝置狀態碼。

狀態	描述
PROVISIONING_REQUIRED	使用者或管理員已請求將裝置佈建為與 Amazon WorkMail 搭配使用。如果在 Amazon WorkMail 主控台中修改該裝置的目前政策，則裝置也會設為此狀態。
PROVISIONING_SUCCEEDED	裝置已成功佈建。裝置已強制執行指定的政策。
WIPE_REQUIRED	管理員在 Amazon WorkMail 主控台中請求清除。
WIPE_SUCCEEDED	裝置已成功被抹除。

管理行動裝置存取規則

Amazon WorkMail 的行動裝置存取規則可讓管理員控制特定類型行動裝置的信箱存取。根據預設，每個 Amazon WorkMail 組織都會使用規則，將信箱存取權授予任何裝置，無論類型、模型、作業系統或

使用者代理程式。您可以編輯該預設規則，或以您自己的規則取代該預設規則。您也可以新增、變更和刪除規則。

> **Warning**
>
> 如果您刪除組織的所有行動裝置存取規則，Amazon WorkMail 會封鎖所有行動裝置存取。

您可以根據下列裝置屬性建立允許或拒絕存取的規則：

- 裝置類型 —「iPhone」、「iPad」或「Android」。
- 裝置模型 —「iPhone10C1」、「iPad5C1」或「HTCOneX."
- 裝置作業系統—"iOS 12.3.1 16F203" 或 "Android 8.1.0"。
- 裝置使用者代理程式—"iOS/14.2 (18B92) exchangesyncd/1.0" 或 "Android-Mail/7.7.16.163886392.release"。

若要在 AWS 管理主控台上檢視裝置屬性，請參閱檢視行動裝置詳細資訊。

> **Note**
>
> 有些裝置和用戶端可能不會報告所有欄位的屬性。如需處理這些案例的資訊，請參閱 Dealing with empty fields

> **Important**
>
> Amazon WorkMail 行動裝置存取規則僅適用於使用 Microsoft Exchange ActiveSync 通訊協定的裝置。使用 IMAP 等不同通訊協定的行動用戶端不會報告此處列出的裝置屬性，因此這些規則不適用。
>
> 如果您需要限制使用其他通訊協定之裝置的存取，您可以建立存取控制規則。如需這些規則的詳細資訊，請參閱使用存取控制規則 。例如，您可以將其他通訊協定和 Webmail 的存取限制為只有一系列的公司 IP 地址，但允許 Microsoft ActiveSync 從其他地方存取，然後使用行動裝置存取規則進一步限制允許的用戶端類型和版本。

主題

行動裝置存取規則的運作方式

行動裝置存取規則僅適用於使用 Microsoft Exchange ActiveSync 通訊協定的裝置。每個規則都有一組條件，指定規則的套用時間，以及裝置的 ALLOW或 DENY 存取效果。只有在規則的所有條件都符合使用者行動裝置的屬性時，規則才會套用至存取請求。沒有條件的規則適用於所有請求。每個條件都會針對裝置回報的屬性使用不區分大小寫的字首比對。

Amazon WorkMail 會評估規則，如下所示：

- 如果任何DENY規則符合裝置屬性，政策會封鎖裝置。 DENY規則優先於ALLOW規則。
- 如果至少有一個ALLOW規則相符，但沒有DENY規則相符，則政策會允許裝置。
- 如果沒有套用規則，則會封鎖裝置。

> **Important**
>
> 行動裝置會報告規則用於操作的屬性。裝置會在 Microsoft ActiveSync 裝置佈建程序期間報告其屬性。Amazon WorkMail 無法獨立驗證行動用戶端是否報告正確或up-to-date資訊。

使用行動裝置存取規則

您可以使用 APIs或 AWS Command Line Interface (CLI) 來建立和管理行動裝置存取規則。如需 的詳細資訊 AWS CLI，請參閱 AWS Command Line Interface 使用者指南。

> **Important**
>
> 當您變更 Amazon WorkMail 組織的存取規則時，受影響的裝置可能需要五分鐘的時間才能遵循更新後的規則，而裝置在此期間可能會顯示不一致的行為。不過，當您測試規則時，會立即看到正確的行為。如需詳細資訊，請參閱Testing mobile device access rules。

列出行動裝置存取規則

下列範例示範如何列出行動裝置存取規則。

```
aws workmail list-mobile-device-access-rules --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

建立行動裝置存取規則

下列範例會建立規則，封鎖所有 Android 裝置存取信箱。

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name BlockAllAndroid --effect DENY --device-types
 "android"
```

下列範例會建立僅允許特定 iOS 版本的規則。請務必移除預設ALLOW-all規則。

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name AllowLatestiOS --effect ALLOW --device-
operating-systems "iOS 14.3"
```

更新行動裝置存取規則

下列範例透過新增識別符來更新裝置規則。

```
aws workmail update-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d --
name AllowLatestiOS --effect ALLOW --device-operating-systems "iOS 14.4"
```

刪除行動裝置存取規則

下列範例會刪除具有指定識別符的行動裝置存取規則。

```
aws workmail delete-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d
```

測試行動裝置存取規則

若要測試存取規則，您可以使用 GetMobileDeviceAccessEffect API 或 中的 get-mobile-device-access-effect 命令 AWS CLI 。如需 的詳細資訊 AWS CLI，請參閱 AWS 命令列界面使用者指南。

當您測試時，您會傳入模擬行動裝置的屬性，而 API 或 CLI 會傳回具有這些屬性的真實行動裝置將收到的存取效果 DENY或ALLOW 。例如，此命令會測試執行 iOS 14.2 的 iPhone 以及預設郵件應用程式是否可以存取信箱。

```
aws workmail get-mobile-device-access-effect --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --device-type "iPhone" --device-model "iPhone10C1"
 --device-operating-system "iOS 14.2.1 16F203" --device-user-agent "iOS/14.2 (18B92)
 exchangesyncd/1.0"
```

處理空白欄位

有些行動裝置或用戶端可能不會報告一或多個欄位的資訊，將值保留空白。規則可以搭配這些裝置，方法是在 條件$NONE中使用特殊值。例如，具有 的規則DeviceTypes=["iphone", "ipad", "$NONE"]會比對報告裝置類型為 "iphone"或 的裝置"ipad"，或完全不報告裝置類型。

負條件，例如 NotDeviceTypes或 NotDeviceUserAgents不符合這些空值。例如，具有 的規則NotDeviceTypes=["android"]會比對報告 以外裝置類型的裝置"android"。不過，規則不會比對完全不報告裝置類型的裝置。

管理行動裝置存取覆寫

您可以使用行動裝置存取覆寫來覆寫行動裝置存取規則的結果。覆寫適用於特定使用者和裝置，並會反轉預設存取規則。您也可以使用覆寫來建立存取規則的一次性例外狀況，並允許或拒絕特定使用者和裝置對。此外，您可以使用覆寫搭配DefaultDenyAll行動裝置存取規則。這會將存取決策延遲到第三方行動裝置管理 (MDM) 解決方案。如需詳細資訊，請參閱 管理覆寫 和 與行動裝置管理解決方案整合

主題

- 行動裝置存取覆寫的運作方式
- 管理覆寫

行動裝置存取覆寫的運作方式

您可以為特定使用者和裝置對建立行動裝置存取覆寫。覆寫會在評估特定使用者和裝置的行動裝置存取規則時，反轉預設存取結果。例如，如果存取規則通常拒絕存取，則存取覆寫允許該使用者和裝置同步其電子郵件。相反地，如果存取規則通常允許存取，您可以建立覆寫，以防止使用者和裝置同步其郵件。當您刪除行動裝置存取覆寫時，Amazon WorkMail 在決定是否授予該使用者和裝置的存取權時，會再次遵守目前的行動裝置存取規則的結果。

> **Important**
>
> 當您變更 Amazon WorkMail 組織的行動裝置存取覆寫時，受影響的裝置可能需要五分鐘的時間才能遵循更新的覆寫。

管理覆寫

您可以使用 API 或 來建立、更新或刪除行動裝置存取覆寫 AWS Command Line Interface。如需 的詳細資訊 AWS CLI，請參閱 AWS Command Line Interface 使用者指南。

若要尋找裝置 ID，請使用 AWS Management Console。如需詳細資訊，請參閱檢視行動裝置詳細資訊。

列出行動裝置存取覆寫

此範例說明如何列出指定 Amazon WorkMail 組織的所有行動裝置存取覆寫。

```
aws workmail list-mobile-device-access-overrides --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56
```

建立和更新行動裝置存取覆寫

這將建立行動裝置存取覆寫，以拒絕存取指定的 Amazon WorkMail 組織、使用者和裝置 ID。

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECDO --effect DENY
```

現有的行動裝置存取覆寫可以修改為具有不同的效果。這將更新先前建立的行動裝置存取覆寫，以允許存取，而不是拒絕。

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECDO --effect ALLOW
```

刪除行動裝置存取覆寫

這將刪除指定 Amazon WorkMail 組織、使用者和裝置 ID 的行動裝置存取覆寫。

```
aws workmail delete-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECDO
```

與行動裝置管理解決方案整合

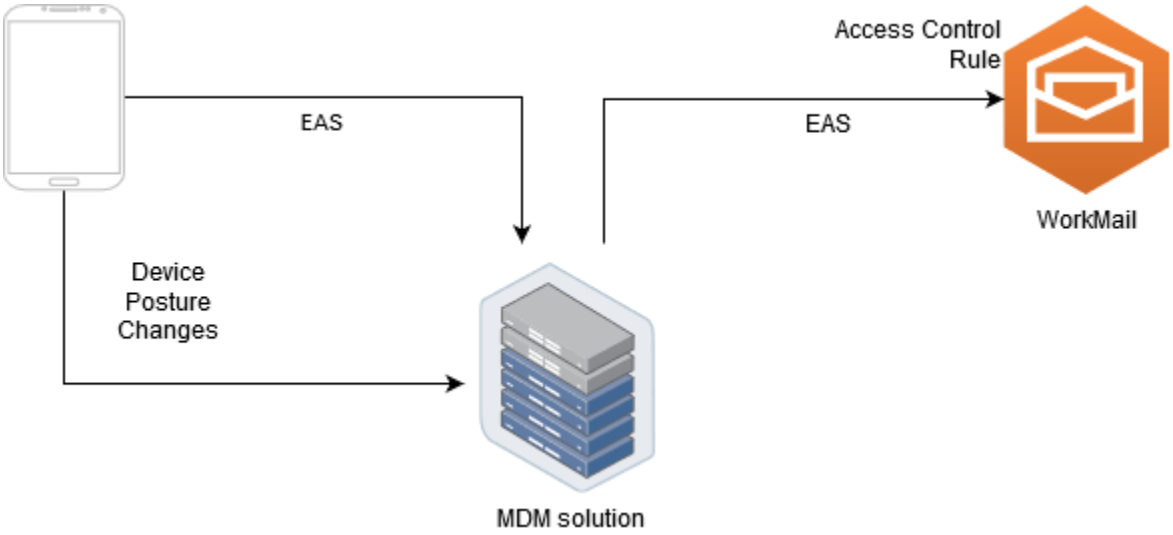
Amazon WorkMail 透過行動裝置政策和行動裝置存取規則支援一些基本的行動裝置管理功能。不過，這些功能只能透過 Microsoft Exchange ActiveSync (EAS) 通訊協定與行動裝置互動，因此它們在導入和強制執行裝置安全狀態的能力有限。需要更充分控制裝置安全和合規的管理員可以使用第三方行動裝置管理 (MDM) 解決方案。

行動裝置管理解決方案概觀

您可以將 MDM 解決方案設定為兩種模式：代理或直接。請參閱您的 MDM 文件，以了解您的解決方案支援哪些模式。

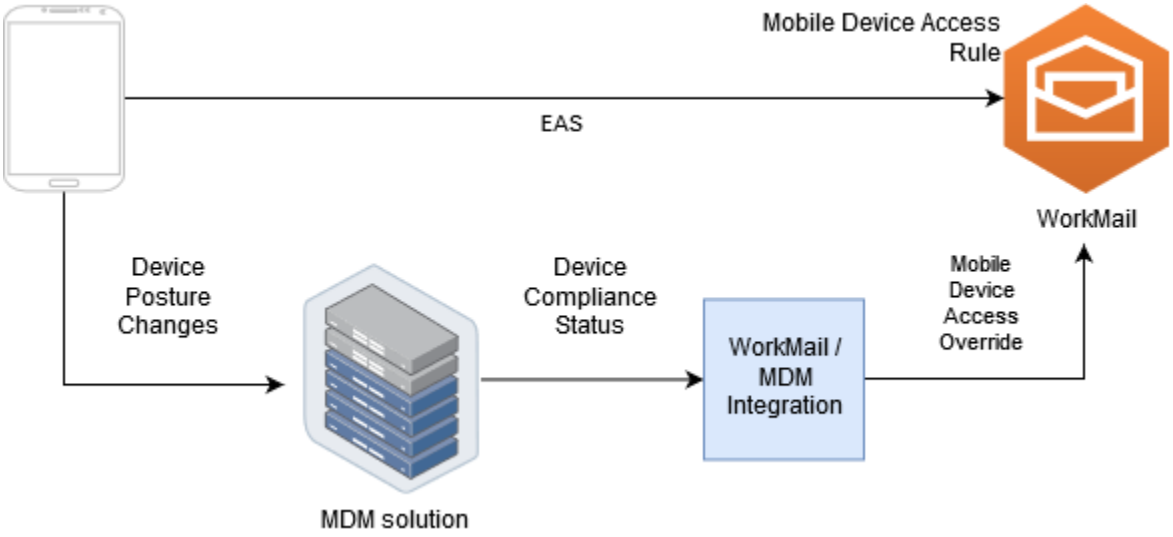
在代理模式中，行動裝置會透過 MDM 解決方案使用 Exchange Active Sync (EAS) 通訊協定來存取 Amazon WorkMail。MDM 解決方案使用裝置狀態來允許或拒絕存取 Amazon WorkMail 資料。在 Amazon WorkMail 端，使用存取控制規則，僅允許從 MDM 解決方案的 IP 地址或地址進行 EAS 存取。如需詳細資訊，請參閱使用存取控制規則。

下圖顯示典型的代理模式組態。



在直接模式下，行動裝置使用 EAS 直接存取 Amazon WorkMail。您的 MDM 解決方案會收到裝置狀態變更，並持續評估每個裝置是否符合這些要求。當 MDM 解決方案偵測到姿勢變更時，例如裝置不合規，它可以採取數個動作，通常發出通知或事件。Amazon WorkMail 管理員可以設定 系統來接聽這些合規狀態事件，並自動建立行動裝置存取覆寫，允許或拒絕存取進出 MDM 裝置要求的裝置。

下圖顯示典型的直接模式組態。



設定 WorkMail 組織以直接模式與第三方 MDM 解決方案整合

若要以直接模式與第三方行動裝置管理 (MDM) 解決方案整合，您必須符合下列要求：

- 建立存取控制規則，將使用者裝置的存取限制為僅限 ActiveSync 通訊協定。
- 建立預設的「deny-to-all」行動裝置存取規則，以確保預設會拒絕所有未知或未受管的行動裝置。
- 採用行動裝置管理解決方案，在裝置變更安全狀態時發出自訂通知或事件，這表示它會進入或不符合規範。
- 建立自訂軟體元件以聆聽這些通知，並呼叫 Amazon WorkMail SDK 以建立行動裝置存取覆寫。

這些元件可確保所有使用者裝置都符合 MDM 合規要求，才能存取其 Amazon WorkMail 信箱。

使用存取控制規則來限制行動裝置對 ActiveSync 的存取

您必須確保所有裝置僅使用 ActiveSync 通訊協定，而且您可以使用存取控制規則來執行此操作。例如，您只能從內部公司 IP 地址範圍授予對其他郵件通訊協定的存取，然後在從公司防火牆外部存取 eamil 時僅允許 ActiveSync。您必須這樣做，因為只有 ActiveSync 允許您使用裝置 ID 來識別裝置。您無法使用網際網路訊息存取通訊協定 (IMAP) 或 Exchange Web Services 等通訊協定。如需詳細資訊，請參閱使用存取控制規則。

建立預設「拒絕所有」存取規則

若要將所有行動裝置存取決策延遲到第三方行動裝置管理解決方案，請建立存取規則，自動拒絕所有裝置，除非依每個使用者或每個裝置覆寫。如需詳細資訊，請參閱 管理行動裝置存取規則。

此範例顯示「拒絕所有」規則。

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name DefaultDenyAll --effect DENY
```

對裝置狀態變更做出反應，並建立行動裝置存取覆寫

您必須設定 MDM 解決方案，以傳送裝置狀態變更的通知。這些通知必須由可以使用 Amazon WorkMail SDK 來建立或更新行動裝置存取覆寫的元件使用。根據預設，Amazon WorkMail 拒絕存取未受管或新佈建的裝置，因為本主題稍早顯示的預設「拒絕所有」行動裝置存取規則。當 MDM 解決方案判斷裝置符合所有需求，並發出通知指出裝置符合規範時，此元件可以透過為指定的使用者和裝置建立具有 效果ALLOW的行動裝置存取覆寫來回應此通知。如果裝置稍後不合規，行動裝置管理解決方案會發出另一個通知，而且可以刪除或修改存取覆寫，以拒絕該裝置的存取。如需詳細資訊，請參閱管理行動裝置存取覆寫。

如需與 MDM 整合的 Amazon WorkMail 範例，請參閱此AWS 範例應用程式。

使用信箱許可

您可以使用 Amazon WorkMail 中的信箱許可，授予使用者和群組在其他使用者的信箱中工作的權利。信箱許可適用於整個信箱。它們可讓多個使用者存取相同的信箱，而無需共用該信箱的憑證。擁有信箱許可的使用者可以讀取和修改信箱資料並自共用信箱傳送電子郵件。

> **Note**
>
> 具有從全域地址清單中隱藏之使用者的信箱許可的使用者，仍然可以存取隱藏使用者的信箱。

以下清單顯示您可被授予的許可：

- 完整存取 – 啟用信箱的完整讀取和寫入存取，包括修改資料夾層級許可的許可。

  > **Note**
  >
  > 此選項僅適用於 使用者。無法授予群組完整存取權。

- 代表傳送 – 讓使用者或群組代表其他使用者傳送電子郵件。信箱擁有者顯示於 From: (寄件者) 標頭中，且寄件者會顯示在 Sender: (寄件者) 標頭。
- 傳送身分 – 讓使用者或群組以信箱擁有者身分傳送電子郵件，而不會顯示訊息的實際寄件者。信箱擁有者同時顯示於 From (寄件人) 和 Sender (寄件者) 標頭。
- 無 – 防止使用者或群組傳送電子郵件。

> **Note**
>
> 授予信箱許可給群組，這些許可會擴展至該群組的所有成員，包括巢狀群組的成員。

當您授予信箱許可時，Amazon WorkMail AutoDiscover 服務會自動為您新增的使用者或群組更新這些信箱的存取權。

於 Windows 的 Microsoft Outlook 用戶端，使用者有完全存取許可可以自動存取共用信箱。最多需要 60 分鐘才能傳播變更，然後重新啟動 Microsoft Outlook。

對於 Amazon WorkMail Web 應用程式和其他電子郵件用戶端，具有完整存取許可的使用者可以手動開啟共用信箱。即使在工作階段之間，開啟的信箱會保持開啟，除非使用者將它關閉。

主題

關於信箱和資料夾許可

信箱許可適用於信箱中的所有資料夾。這些許可只能由 AWS 帳戶持有人或有權呼叫 Amazon WorkMail 管理 API 的 IAM 使用者啟用。若要設定和變更信箱或群組整體的許可，請使用 AWS Management Console 或 Amazon WorkMail API。您可以從主控台管理多達 100 個信箱和群組許可。若要管理更多使用者和群組的許可，請使用 Amazon WorkMail API。

資料夾許可只適用於單一資料夾。最終使用者可以使用電子郵件用戶端或使用 Amazon WorkMail Web 應用程式來設定資料夾許可。如需使用 Amazon WorkMail Web 應用程式共用資料夾的詳細資訊，請參閱《Amazon WorkMail 使用者指南》中的共用資料夾和資料夾許可。

管理使用者的信箱許可

您可以使用 Amazon WorkMail 主控台來管理使用者的信箱許可以及群組。下列各節說明如何管理 使用者的許可。如需有關管理群組許可的資訊，請參閱 管理群組的信箱許可。

主題

新增許可

當您新增許可時，您會授予一位使用者在另一位使用者的信箱中執行一或多個任務的權利。例如，假設員工 A 需要代表他的主管員工 B 傳送訊息。若要授予該許可，請前往員工 B 的信箱設定，並授予員工 A 執行請求任務的許可。

新增信箱許可

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更區域。從導覽列中，選擇符合您需求的區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。

2. 在導覽窗格中，選擇組織，然後選擇您要管理許可的組織名稱。
3. 在導覽窗格中，選擇使用者，然後選擇您要為其管理許可的使用者名稱。
4. 選擇 許可 標籤，然後選擇 新增許可。

   新增許可對話方塊隨即出現。
5. 開啟新增許可清單，然後選取需要存取信箱的使用者或群組。
6. 在信箱許可和傳送許可下，選擇所需的選項。
7. 選擇新增。

新的許可最多可能需要五分鐘才能傳播給使用者。

編輯使用者的信箱許可

當您編輯使用者的信箱許可時，您可以變更其他人對該使用者信箱的存取權。編輯信箱許可不會變更信箱原始使用者的存取權。

編輯信箱許可

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更區域。從導覽列中，選擇符合您需求的區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇您要管理許可的組織名稱。
3. 在導覽窗格中，選擇使用者，然後選擇您要編輯其許可的使用者名稱。
4. 選擇許可索引標籤標籤。

   具有信箱存取權的使用者和群組清單隨即出現。
5. 選取您要變更的使用者或群組旁的選項按鈕，然後執行下列任何動作：

   移除使用者的許可

   1. 選擇移除。

      移除許可對話方塊隨即出現。
   2. 在移除許可對話方塊中，選擇移除。

編輯使用者的許可

1. 選擇編輯。

   編輯許可對話方塊隨即出現。
2. 視需要設定許可，然後選擇儲存。

將其他使用者許可授予信箱

1. 選擇新增許可。

   新增許可對話方塊隨即出現。
2. 開啟新增許可清單，然後選取您要新增的使用者。
3. 視需要設定許可，然後選擇新增。

許可的變更最多可能需要五分鐘的時間才能傳播給使用者。

管理群組的信箱許可

您可以新增或移除 Amazon WorkMail 的群組許可。

> **Note**
>
> 您無法將完整存取許可套用至群組，因為群組沒有信箱可供存取。

管理群組許可

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要，請變更主控台視窗頂端的 AWS 區域 列，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇您要管理許可的組織名稱。
3. 在導覽窗格中，選擇群組，然後選擇您要設定許可的群組名稱。
4. 選擇許可索引標籤，然後選擇新增許可。

新增許可對話方塊隨即出現。

5. 開啟新增許可清單，然後選取要授予信箱許可的使用者或群組。
6. 在信箱許可和傳送許可下，選擇所需的選項。
7. 選擇新增。

許可的變更最多可能需要五分鐘的時間才能傳播給使用者。

信箱的程式設計存取

若要以程式設計方式存取 Amazon WorkMail 信箱，請使用 Exchange Web Services (EWS) 通訊協定。透過 EWS，您可以存取信箱中的所有項目類型。以下是您可以與 Amazon WorkMail 搭配使用的一些 EWS 程式庫：

- Java – EWS Java API
- .Net – EWS 受管 API
- Python – Exchangelib

Amazon WorkMail 也支援 IMAP 和 SMTP 通訊協定，您可以使用這些通訊協定來傳送和接收電子郵件。您可以在 Amazon WorkMail 端點和配額下查看 Amazon WorkMail 通訊協定支援的 URLs。

使用 EWS 通訊協定時，Amazon WorkMail 支援下列身分驗證方法：

- 基本身分驗證 – 使用基本身分驗證，您可以輸入電子郵件地址和密碼。
- 模擬角色 – 使用模擬角色時，您可以存取使用者的信箱，而無需輸入使用者的登入資料。

主題

管理模擬角色

透過模擬角色，管理員可設定使用者信箱的程式設計存取，而無需輸入使用者的登入資料。服務和工具可以擔任模擬角色，在使用者的信箱中執行動作。模擬僅支援 EWS 通訊協定。

模擬角色概觀

若要允許模擬，管理員必須使用下列屬性建立模擬角色：

- 角色類型 – 選擇完整存取或唯讀。角色類型會限制角色可執行的操作類型。
- 規則 – 定義模擬角色可模擬哪些使用者的規則清單。

Amazon WorkMail 會評估下列條件的規則：

- 如果任何 DENY 規則相符，政策會拒絕模擬。DENY 規則優先於任何允許規則。
- 如果至少一個 ALLOW 規則相符，且沒有 DENY 規則相符，則政策允許模擬。
- 如果沒有適用規則，則拒絕模擬。

> **Note**
>
> 若要允許 Amazon WorkMail 組織中的所有使用者模擬，請建立具有 ALLOW 效果且沒有條件的規則。

> **Warning**
>
> 您必須建立規則，以允許模擬角色模擬使用者。如果您未指定規則，模擬角色無法擔任使用者的存取權。

建立模擬角色之後，您可以使用它來存取使用者的信箱。如需詳細資訊，請參閱使用模擬角色。

安全考量

使用模擬角色會在您的 Amazon WorkMail 組織內產生安全問題的可能性 AWS 帳戶。以下是您在建立模擬角色時需要考慮的一些潛在問題：

- 暫時性許可 – 如果使用者 A 有權存取使用者 B 的信箱，且允許模擬角色模擬使用者 A，則此模擬角色可以模擬使用者 A 的存取許可和存取使用者的 B 信箱。
- 存取控制 – 您可以使用存取控制規則來限制模擬角色存取。如需詳細資訊，請參閱使用存取控制規則。
- IAM 政策 – 您可以使用 `workmail:ImpersonationRoleId`條件將`AssumeImpersonationRole`動作指派給特定 Amazon WorkMail 組織和模擬角色。若要查看 IAM 政策範例，請參閱 Amazon WorkMail 如何與 IAM 搭配使用。

建立模擬角色

您可以從 Amazon WorkMail 主控台建立模擬角色。

建立模擬角色

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更區域。從導覽列中，選擇符合您需求的區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 選擇模擬角色，然後選擇建立角色。
4. 隨即出現建立模擬角色對話方塊。在角色下，輸入下列資訊：
   - 名稱 – 輸入模擬角色的唯一名稱。
   - （選用）描述 – 輸入模擬角色的描述。
   - 角色類型 – 選擇唯讀或完整存取。
5. 在規則下，選擇新增規則。
6. 新增規則對話方塊隨即出現。輸入下列資訊：
   - 名稱 – 輸入規則的唯一名稱。
   - （選用）描述 – 輸入規則的描述。
   - 在效果下，選擇允許或拒絕。這會根據您在下列步驟中選取的條件允許或拒絕存取。
   - （選用）在此規則下：，選擇符合模擬所選使用者以包含特定使用者的請求。選擇符合模擬所選使用者以外的使用者的請求，以新增所選使用者以外的使用者。
7. 選擇新增規則。

   > **Note**
   >
   > 只有在您儲存對應的角色時，才會儲存規則。

8. 選擇建立角色。

編輯模擬角色

您可以從 Amazon WorkMail 主控台編輯模擬角色。

編輯模擬角色

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

如有必要請變更區域。從導覽列中，選擇符合您需求的區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。

2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 選擇模擬角色。
4. 選取您要編輯的模擬角色名稱，然後選擇編輯。
5. 隨即出現編輯模擬角色對話方塊。在角色下，輸入下列資訊：
   - 名稱 – 輸入模擬角色的唯一名稱。
   - （選用）描述 – 輸入模擬角色的描述。
   - 角色類型 – 若要提供模擬角色對使用者信箱的唯讀存取權，請選擇唯讀。若要授予模擬角色讀取和修改使用者信箱中項目的權限，請選擇完整存取。
6. 在規則下，選取您要編輯的規則，然後選擇編輯。
7. 編輯規則對話方塊隨即出現。輸入下列資訊：
   - 名稱 – 編輯規則的名稱。
   - （選用）描述 – 更新或輸入規則的描述。
   - 在效果下，選擇允許，以便在符合規則中設定的條件時允許存取。若要拒絕存取，請選擇拒絕。
   - （選用）在此規則下：，選擇符合模擬所選使用者以包含特定使用者的請求。選擇符合模擬所選使用者以外的使用者的請求，以新增所選使用者以外的使用者。
8. 選擇 Save (儲存)。
9. 選擇 Save changes (儲存變更)。

> **Important**
>
> 當您變更模擬規則時，受影響的信箱最多可能需要五分鐘才能更新。在規則更新過程中，您可能會在信箱中觀察到不一致的行為。不過，如果您測試角色，Amazon WorkMail 會根據更新後的規則如預期回應。如需詳細資訊，請參閱測試模擬角色。

測試模擬角色

您可以從 Amazon WorkMail 主控台測試模擬角色。

測試模擬角色

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要請變更區域。從導覽列中，選擇符合您需求的區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 選擇模擬角色。
4. 選取您要測試的模擬角色。
5. 選擇測試角色。

6. 測試模擬角色對話方塊隨即出現。在目標使用者下，選取要測試模擬存取的使用者。
7. 選擇測試。

刪除模擬角色

您可以從 Amazon WorkMail 主控台刪除模擬角色。

刪除模擬角色

1. 開啟位於 https：//https://console.aws.amazon.com/workmail/ 的 Amazon WorkMail 主控台。

   如有必要請變更區域。從導覽列中，選擇符合您需求的區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。
2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 選擇模擬角色。
4. 選取您要刪除的模擬角色名稱。
5. 選擇 刪除 。
6. 刪除角色對話方塊隨即出現。若要確認刪除，請在對話方塊中輸入角色的名稱，然後選擇刪除。

使用模擬角色

若要存取信箱資料，請使用 Amazon WorkMail API 動作 `AssumeImpersonationRole`。如需 Amazon WorkMail APIs的詳細資訊，請參閱 API 參考。

AssumeImpersonationRole 傳回 Token。這Token必須在 15 分鐘內透過 HTTP 標頭 傳遞至 EWS 通訊協定Authorization。

下列範例示範如何搭配 EWS 通訊協定使用模擬角色。範例中使用的常數會指定組織和帳戶獨有的下列詳細資訊：

- *WORKMAIL_ORGANIZATION_ID* – Amazon WorkMail 組織 ID
- *IMPERSONATION_ROLE_ID* – 模擬角色 ID
- *WORKMAIL_EWS_URL* – Amazon WorkMail 端點和配額提供 EWS 端點
- *EMAIL_ADDRESS* – 使用者信箱的電子郵件地址

Example Java – EWS Java API

```
import software.amazon.awssdk.services.workmail.WorkMailClient;
import software.amazon.awssdk.services.workmail.model.AssumeImpersonationRoleRequest;
import software.amazon.awssdk.services.workmail.model.AssumeImpersonationRoleResponse;

import microsoft.exchange.webservices.data.core.ExchangeService;
import microsoft.exchange.webservices.data.core.enumeration.misc.ExchangeVersion;
import microsoft.exchange.webservices.data.misc.ImpersonatedUserId;
import microsoft.exchange.webservices.data.core.enumeration.misc.ConnectingIdType;

// ...

AssumeImpersonationRoleResponse response = workMailClient.assumeImpersonationRole(
    AssumeImpersonationRoleRequest.builder()
        .organizationId(WORKMAIL_ORGANIZATION_ID)
        .impersonationRoleId(IMPERSONATION_ROLE_ID)
        .build());

ExchangeService exchangeService = new
 ExchangeService(ExchangeVersion.Exchange2010_SP2);
exchangeService.setUrl(URI.create(WORKMAIL_EWS_URL));
exchangeService.getHttpHeaders().put("Authorization", "Bearer " + response.token());
exchangeService.setImpersonatedUserId(new
 ImpersonatedUserId(ConnectingIdType.SmtpAddress, EMAIL_ADDRESS));
```

Example .Net – EWS 受管 API

```
using Amazon.WorkMail;
```

```
using Amazon.WorkMail.Model;

using Microsoft.Exchange.WebServices.Data;

// ...

AssumeImpersonationRoleRequest request = new AssumeImpersonationRoleRequest();
request.OrganizationId = WORKMAIL_ORGANIZATION_ID;
request.ImpersonationRoleId = IMPERSONATION_ROLE_ID;
AssumeImpersonationRoleResponse response =
 workMailClient.AssumeImpersonationRole(request);

ExchangeService service = new ExchangeService(ExchangeVersion.Exchange2010_SP2);
service.Url = new Uri(WORKMAIL_EWS_URL);
service.HttpHeaders.Add("Authorization", "Bearer " + response.Token);
service.ImpersonatedUserId = new
 ImpersonatedUserId(ConnectingIdType.SmtpAddress, EMAIL_ADDRESS);
```

Example Python – Exchangelib

```
import boto3

from requests.auth import AuthBase
from exchangelib.transport import AUTH_TYPE_MAP
from exchangelib import Configuration, Account, Version, IMPERSONATION
from exchangelib.version import EXCHANGE_2010_SP2


work_mail_client = boto3.client("workmail")

class ImpersonationRoleAuth(AuthBase):
    def __init__(self):
         self.token = work_mail_client.assume_impersonation_role(
             OrganizationId=WORKMAIL_ORGANIZATION_ID,
             ImpersonationRoleId=IMPERSONATION_ROLE_ID
        )["Token"]

     def __call__(self, r):
         r.headers["Authorization"] = "Bearer " + self.token
         return r

AUTH_TYPE_MAP["ImpersonationRoleAuth"] = ImpersonationRoleAuth
```

```
ews_config = Configuration(
     service_endpoint=WORKMAIL_EWS_URL,
     version=Version(build=EXCHANGE_2010_SP2),
     auth_type="ImpersonationRoleAuth"
)
ews_account = Account(
     config=ews_config,
     primary_smtp_address=EMAIL_ADDRESS,
     access_type=IMPERSONATION
)
```

匯出信箱內容

使用 Amazon WorkMail API 參考中的 StartMailboxExportJob API 動作，將 Amazon WorkMail 信箱內容匯出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體。 Amazon WorkMail 此動作會以 MIME 格式，將所有電子郵件訊息和行事曆項目從指定的信箱匯出至 Amazon S3 儲存貯體中的`.zip`檔案。不會匯出其他項目，例如聯絡人和任務。

信箱匯出任務完成所需的時間取決於信箱中的項目大小和數量。由於信箱匯出任務會在一段時間內進行，因此不代表信箱內容在單一時間點的快照。若要查看匯出任務的狀態，請使用 Amazon WorkMail API 參考中的 DescribeMailboxExportJob 或 ListMailboxExportJobs API 動作。 Amazon WorkMail

信箱匯出任務完成後，Amazon S3 儲存貯體中的`.zip`檔案會使用您提供的對稱 AWS Key Management Service (AWS KMS) 客戶主金鑰 (CMK) 進行加密。因為 AWS KMS 加密已與 Amazon S3 整合，所以下載資料的使用者可以看到解密的資料，只要使用者可以存取 AWS KMS CMK。

先決條件

以下是匯出信箱內容的先決條件：

- 編寫程式的能力。
- Amazon WorkMail 管理員帳戶。
- 不允許公開存取的 Amazon S3 儲存貯體。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》和《Amazon Simple Storage Service 使用者指南》中的使用 Amazon S3 封鎖公開存取。 https://docs.aws.amazon.com/AmazonS3/latest/userguide/
- 對稱 AWS KMS CMK。詳情請參閱 AWS Key Management Service 開發人員指南中的開始使用。
- 具有政策的 AWS Identity and Access Management (IAM) 角色，可授予寫入 Amazon S3 儲存貯體並使用 CMK AWS KMS 加密已傳送檔案的許可。如需詳細資訊，請參閱Amazon WorkMail 如何與 IAM 搭配使用。

IAM 政策範例和角色建立

下列範例顯示 IAM 政策，授予許可，以寫入 Amazon S3 儲存貯體並使用 CMK AWS KMS 加密傳送的檔案。若要在下列範例：匯出信箱內容程序中使用此範例政策，請將政策儲存為檔案名稱為 的 JSON 檔案`mailbox-export-policy.json`。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:GetBucketPolicyStatus"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:111122223333:key/KEY-ID"
            ],
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "s3.us-east-1.amazonaws.com"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-
bucket/S3-PREFIX*"
                }
            }
        }
    ]
}
```

下列範例顯示連接至您建立之 IAM 角色的 IAM 信任政策。若要在下列範例：匯出信箱內容程序中使用此範例政策，請將政策儲存為檔案名稱為 的 JSON 檔案`mailbox-export-trust-policy.json`。

您不需要同時使用 `aws:SourceArn`和 `aws:SourceAccount`條件。例如，如果您需要使用相同的角色從相同 AWS 帳戶下的不同 Amazon WorkMail 組織匯出訊息，您可以從`aws:SourceArn`政策中移除 。如需條件索引鍵的詳細資訊，請參閱 AWS Identity and Access Management 使用者指南中的AWS 全域條件內容索引鍵。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "export.workmail.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workmail:us-east-1:111122223333:organization/m-
a123b4c5de678fg9h0ij1k2lm234no56"
        }
      }
    }
  ]
}
```

您可以使用 執行下列命令 AWS CLI ，在帳戶中建立 IAM 角色。

```
aws iam create-role --role-name WorkmailMailboxExportRole --assume-role-policy-
document file://mailbox-export-trust-policy.json --region us-east-1
```

```
aws iam put-role-policy --role-name WorkmailMailboxExportRole --policy-
name MailboxExport --policy-document file://mailbox-export-policy.json
```

如需 的詳細資訊 AWS CLI，請參閱AWS Command Line Interface 《 使用者指南》。

範例：匯出信箱內容

在上一節中建立 IAM 角色和政策後，請完成下列步驟以匯出信箱內容。您必須擁有可在 Amazon WorkMail 主控台或使用 Amazon WorkMail API 存取的 Amazon WorkMail 組織 ID 和使用者 ID （實體 ID)。

範例：匯出信箱內容

1. 使用 AWS CLI 啟動信箱匯出任務。

```
aws workmail start-mailbox-export-job --organization-id m-
a123b4c5de678fg9h0ij1k2lm234no56 --entity-
id S-1-1-11-1111111111-2222222222-3333333333-3333 --kms-key-
arn arn:aws:kms:us-east-1:111122223333:key/KEY-ID --role-arn
 arn:aws:iam::111122223333:role/WorkmailMailboxExportRole --s3-bucket-name amzn-s3-
demo-bucket --s3-prefix S3-PREFIX
```

2. 使用 AWS CLI 來監控 Amazon WorkMail 組織的信箱匯出任務狀態。

```
aws workmail list-mailbox-export-jobs --organization-id m-
a123b4c5de678fg9h0ij1k2lm234no56
```

或者，使用 **start-mailbox-export-job**命令產生的任務 ID，僅監控該信箱匯出任務的狀態。

```
aws workmail describe-mailbox-export-job --organization-id m-
a123b4c5de678fg9h0ij1k2lm234no56 --job-id JOB-ID
```

當信箱匯出任務狀態為 COMPLETED 時，匯出的信箱項目可在指定 Amazon S3 儲存貯體的.zip檔案中使用。

以下是匯出信箱的輸出日誌範例：

```
{
  "totalNonExportableItems" : "13",
  "totalMessages" : "76",
  "sha384Hash" : "4de93a***96a1dd",
  "totalBytes" : "161892",
  "totalFolders" : "15",
  "startTime" : "168***380",
  "endTime" : "168***384"
}
```

> **Note**
>
> totalNonExportableItems 是不支援的項目，例如備註和聯絡人。

考量事項

匯出 Amazon WorkMail 的信箱任務時，適用下列考量：

- 您可以為指定的 Amazon WorkMail 組織執行最多 10 個並行信箱匯出任務。
- 您可以為指定的信箱執行信箱匯出任務，頻率為每 24 小時一次。
- 下列資源必須全部位於相同的 AWS 區域：
  - Amazon WorkMail 組織
  - AWS KMS CMK
  - Amazon S3 儲存貯體

故障診斷

本節中的主題說明如何對 Amazon WorkMail 中的問題進行疑難排解。

主題

檢視電子郵件標頭

電子郵件標頭中的資訊可協助您疑難排解常見的使用者電子郵件問題。Amazon WorkMail 可讓您檢視任何訊息的標頭資訊。

在 Amazon WorkMail 中檢視電子郵件標頭

1. 在 Amazon WorkMail Web 應用程式中，按兩下電子郵件訊息以開啟。
2. 選擇訊息右上角的訊息選項（齒輪和信封圖示），位於傳送日期旁。

電子郵件標頭會出現在 Internet Headers (網際網路標頭) 下。

郵件路由

如果使用者停止接收電子郵件，您的 Amazon WorkMail 組織可能會遇到郵件路由問題。本節中的步驟說明解決交付和路由問題的常見方法。

傳入郵件問題：

- 檢查與您的 Amazon WorkMail 組織相關聯的網域的 MX 記錄。 `WorkMail` 應該是唯一的項目，並且應該具有最低的優先順序。多個 MX 記錄可能會導致錯誤的服務接收訊息。如需 MX 記錄的詳細資訊，請參閱 驗證網域。
- 在 Amazon WorkMail 主控台中檢查組織的網域型訊息驗證、報告和一致性 (DMARC) 設定。DMARC 記錄用於防範常見攻擊，例如詐騙或網路釣魚，這些攻擊可能會危害使用者的帳戶登入資料。如需 DMARC 的詳細資訊，請參閱 對內送電子郵件強制執行 DMARC 政策。
- 檢查 Amazon Simple Email Service 傳入規則。如果規則包含 Amazon WorkMail 以外的動作，這些動作可能會失敗，並導致 Amazon WorkMail 停止接收郵件。如需 Amazon SES 規則的詳細資訊，請參閱《Amazon Simple Email Service 開發人員指南》中的與 Amazon WorkMail 動作整合。

- 在 Amazon WorkMail 中啟用訊息追蹤，然後檢查日誌是否有交付問題。如需訊息追蹤的詳細資訊，請參閱 啟用電子郵件事件記錄。

傳出郵件問題

- 確保您的 SPF 記錄包含 Amazon SES。檢查 Amazon WorkMail 主控台中的網域頁面以進行驗證。如需 SPF 的詳細資訊，請參閱以 SPF 驗證您的電子郵件。
- 確保 Amazon WorkMail 具有使用網域的許可。如果沒有，請再次新增網域。 本指南新增網域提供操作說明步驟。

搭配 Amazon WorkMail 使用電子郵件日誌

您可以使用整合的第三方封存與 eDiscovery 工具設定日誌登載以記錄您的電子郵件通訊。這可確保電子郵件儲存的隱私保護，資料儲存體和資訊保護皆合規法規。

使用日誌登載

Amazon WorkMail 會記錄傳送到指定組織中任何使用者的所有電子郵件訊息，以及該組織中使用者傳送的所有電子郵件訊息。所有電子郵件訊息的副本都會以稱為 的格式傳送至系統管理員指定的地址`journal record`。此格式與 Microsoft 電子郵件計劃相容。電子郵件日誌登載無需額外收費。

電子郵件日誌使用兩個電子郵件地址：一個日誌電子郵件地址和一個報告電子郵件地址。日誌登載電子郵件地址是專用信箱或與您帳戶整合的第三方裝置的地址，為日誌報告會傳送的地址。報告電子郵件地址是您系統管理員的地址，為錯誤日誌報告通知會傳送的地址。

所有日誌記錄都會從自動新增至網域的電子郵件地址傳送，如下所示。

```
amazonjournaling@yourorganization.awsapps.com
```

沒有與此地址相關聯的信箱，您將無法使用此名稱或地址建立一個信箱。

> **Note**
>
> 請勿從 Amazon Simple Email Service (Amazon SES主控台刪除下列網域記錄，否則電子郵件日誌會停止運作。
>
> ```
> yourorganization.awsapps.com
> ```

每則傳入或傳出電子郵件訊息都會產生一筆日誌記錄，無論收件人或使用者群組數量為何。無法產生日誌記錄的電子郵件，會產生傳送到報告電子郵件地址的錯誤通知。

要啟用電子郵件日誌登載

1. 在 https：//https://console.aws.amazon.com/workmail/ 開啟 Amazon WorkMail 主控台。

   如有必要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟選取區域清單，然後選擇區域。如需詳細資訊，請參閱 Amazon Web Services 一般參考 中的 區域與端點。

2. 在導覽窗格中，選擇組織，然後選擇組織的名稱。
3. 在導覽窗格中的組織設定中，選擇日誌索引標籤，然後選擇編輯。
4. 將日誌記錄狀態滑桿移至開啟位置。
5. 在日誌電子郵件地址方塊中，輸入電子郵件日誌提供者提供的電子郵件地址。

> **Note**
>
> 我們建議您使用專用的日誌登載供應商。

6. 在報告電子郵件地址中，輸入電子郵件管理員的地址。
7. 選擇 Save (儲存)。這些變更會立即套用。

文件歷史紀錄

下表說明 Amazon WorkMail 管理員指南每個版本的重要變更。如需有關此文件更新的通知，您可以訂閱 RSS 訂閱源。

變更	描述	日期
稽核記錄支援	稽核日誌可用來監控使用者對信箱的存取、稽核可疑活動，以及偵錯存取控制和可用性提供者組態。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的在 Amazon WorkMail 中啟用稽核記錄和記錄和監控。 Amazon WorkMail	2024 年 3 月 20 日
Transport Layer Security (TLS) 支援	Amazon WorkMail 已停止對 Transport Layer Security (TLS) 1.0 和 1.1 的支援。如果您使用的是 TLS 1.0 或 1.1，則必須將 TLS 版本升級至 1.2。	2023 年 11 月 2 日
遠端使用者	遠端使用者是託管於 Amazon WorkMail 組織外部的 Amazon WorkMail 使用者，或託管於不同電子郵件網域。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的使用者。	2023 年 9 月 18 日
信箱的程式設計存取	Amazon WorkMail 現在提供模擬角色，以授予信箱的程式設計存取權。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的信箱程式設計存取。	2022 年 10 月 4 日

在 Amazon WorkMail 上設定自訂可用性提供者	Amazon WorkMail 支援使用自訂可用性提供者 (CAPs)。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的設定自訂可用性提供者。	2022 年 6 月 30 日
建立組織的主控台變更	用於建立組織的 Amazon WorkMail 主控台體驗已更新。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的建立組織。	2020 年 10 月 23 日
匯出信箱內容	使用 `StartMailboxExportJob` API 動作將 Amazon WorkMail 信箱內容匯出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的匯出信箱內容。	2020 年 9 月 22 日
信箱保留政策	為您的 Amazon WorkMail 組織設定信箱保留政策，在您選擇的期間之後自動刪除電子郵件訊息。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的設定信箱保留政策。	2020 年 5 月 28 日
同步和非同步 Run Lambda 動作	在 Amazon WorkMail 電子郵件流程規則中選擇執行 Lambda 動作的同步或非同步組態。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的 AWS Lambda 設定 Amazon WorkMail。 Amazon WorkMail	2020 年 5 月 11 日

使用存取控制規則	存取控制規則可讓 Amazon WorkMail 管理員控制存取組織信箱的方式。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的使用存取控制規則。	2020 年 2 月 12 日
標記組織	標記 Amazon WorkMail 組織以區分 AWS 帳單與成本管理 主控台中的組織，或控制對組織資源的存取。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的標記組織。	2020 年 1 月 23 日
對傳入電子郵件強制執行 DMARC 政策	如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的對傳入電子郵件強制執行 DMARC 政策。	2019 年 10 月 17 日
使用 Lambda 擷取訊息內容	搭配 使用 Amazon WorkMail 訊息流程 API AWS Lambda 來擷取訊息內容。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的使用 Lambda 擷取訊息內容。	2019 年 9 月 12 日
記錄 Amazon WorkMail 電子郵件事件	在 Amazon WorkMail 主控台中啟用電子郵件事件記錄，以追蹤您組織的電子郵件訊息。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的追蹤訊息。	2019 年 5 月 13 日

Route 53 DNS 記錄插入	設定在 Route 53 公有託管區域中管理的網域時，Amazon WorkMail 會自動為您插入 DNS 記錄。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的新增網域。	2019 年 2 月 13 日
為傳入電子郵件規則動作設定 Lambda	Amazon WorkMail 支援設定 Lambda 函數以搭配傳入電子郵件流程規則使用。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的管理電子郵件流程。	2019 年 1 月 24 日
為 Amazon WorkMail 設定 Lambda	Amazon WorkMail 支援設定 Lambda 函數以與傳出電子郵件流程規則搭配使用。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的為 Amazon WorkMail 設定 Lambda。 Amazon WorkMail	2018 年 11 月 19 日
SMTP 路由	Amazon WorkMail 支援設定 SMTP 閘道以搭配傳出電子郵件流程規則使用。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的設定 SMTP 閘道。	2018 年 11 月 1 日
自訂網域的偵錯工具	Amazon WorkMail 已新增自訂網域的偵錯工具。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的新增網域。	2018 年 10 月 15 日

支援 Outlook 2019	Amazon WorkMail 支援 Outlook 2019 for Windows 和 macOS。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的 Amazon WorkMail 系統需求。 Amazon WorkMail	2018 年 10 月 1 日
各種更新	主題配置和組織的各種更新。	2018 年 7 月 12 日
信箱許可	您可以使用 Amazon WorkMail 中的信箱許可，授予使用者或群組在其他使用者的信箱中工作的權利。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的使用信箱許可。	2018 年 4 月 9 日
的支援 AWS CloudTrail	Amazon WorkMail 已與 整合 AWS CloudTrail。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的使用 記錄 Amazon WorkMail API 呼叫 AWS CloudTrail。 Amazon WorkMail	2017 年 12 月 12 日
支援電子郵件流程	您可以根據寄件者的電子郵件地址或網域設定處理內送電子郵件的電子郵件流程規則。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的管理電子郵件流程。	2017 年 7 月 5 日
快速設定更新	Quick Setup 現在會為您建立 Amazon WorkMail 目錄。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的使用快速設定設定 Amazon WorkMail。	2017 年 5 月 10 日

支援更廣泛的電子郵件用戶端	您現在可以將 Amazon WorkMail 與 Microsoft Outlook 2016 for Mac 和 IMAP 電子郵件用戶端搭配使用。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的 Amazon WorkMail 的系統需求。	2017 年 1 月 9 日
支援 SMTP 日誌記錄	您可以設定日誌登載以記錄您的電子郵件通訊。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的搭配 Amazon WorkMail 使用電子郵件日誌。	2016 年 11 月 25 日
支援將電子郵件重新導向至外部電子郵件地址	您可以更新網域的 Amazon SES 身分政策來設定電子郵件重新導向規則。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的編輯網域身分政策。	2016 年 10 月 26 日
支援互通性	您可以啟用 Amazon WorkMail 與 Microsoft Exchange 之間的互通性。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的 Amazon WorkMail 與 Microsoft Exchange 之間的互通性。	2016 年 10 月 25 日
一般可用性	Amazon WorkMail 的一般可用性版本。	2016 年 1 月 4 日

支援預留資源	支援保留資源，如會議室和設備。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的使用資源。	2015 年 10 月 19 日
支援電子郵件遷移工具	支援電子郵件遷移工具。如需詳細資訊，請參閱《Amazon WorkMail 管理員指南》中的遷移至 Amazon WorkMail。	2015 年 8 月 16 日
Amazon WorkMail 的預覽版本	Amazon WorkMail 的預覽版本。	2015 年 1 月 28 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。