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和行事曆服務，可支援現有桌面和行動電子郵件用戶端。Amazon 用 WorkMail 戶可以使用 Microsoft Outlook，他們的瀏覽器或原生的 iOS 和 Android 電子郵件應用程序訪問他們的電子郵件，聯繫人和日曆。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的存放位置。

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 系統要求

當您的 Amazon WorkMail 管理員邀請您登錄到您的 Amazon WorkMail 帳戶時，您可以使用 Amazon WorkMail 網絡客戶端登錄。

Amazon WorkMail 也可以與支援 Exchange ActiveSync 通訊協定的所有主要行動裝置和作業系統搭配使用。這些裝置包含 iPad、iPhone、Android 和 Windows Phone。macOS 的用戶可以將其 Amazon WorkMail 帳戶添加到他們的郵件，日曆和聯繫人應用程序中。

Amazon WorkMail 支援下列作業系統版本：

- 視窗 — 視窗 7 SP1 或更高版本
- MacOS-蘋 MacOS 10.12 (塞拉利昂) 或更高版本
- 安卓 — 安卓 5.0 或更高版本
- 蘋果 iPhone — iOS 5 或以上版本
- 視窗手機 — 視窗 8.1 或更高版本
- 黑莓-黑莓手機操作系統 10.3.3.3216

如果你有一個有效的 Microsoft Outlook 許可證，您可以 WorkMail 使用以下版本的 Microsoft Outlook 訪問 Amazon：

- 2013 年或以後展望
- 展望 2013 按一下即可執行或更新版本
- 適用於 Mac 2016 或更新版本的展望

您可以使用下列瀏覽器版本存取 Amazon WorkMail 網路用戶端：

- 谷歌瀏覽器 — 版本 22 或更高版本
- 火狐瀏覽器 — 版本 27 或更高版本
- 野生動物園-版本 7 或更高版
- 互聯網瀏覽器-版本 11
- Microsoft Edge

您也可以將 Amazon WorkMail 與您首選的 IMAP 客戶端一起使用。

Amazon WorkMail 概念

以下描述了您對 Amazon WorkMail 的理解和使用至關重要的術語和概念。

組織

Amazon 的租戶設置 WorkMail。

別名

全球唯一識別您組織的名稱。別名用於訪問 Amazon WorkMail 網絡應用程序（HTTPS：//## .awsapps.com/郵件）。

網域

電子郵件地址中@符號後面的網址。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

網域會在安裝期間自動設定，可用於測試 Amazon WorkMail。測試郵件網域是## .awsapps.com，如果您未設定自己的網域，則會用作預設網域。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 S AWS imple AD、AWS受管理 AD 或 AD 連接器AWS Directory Service。如果您使用 Amazon WorkMail 快速設定建立組織，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 AWS Directory Service 中建立的使用者。使用者可以在使用者或 REMOTE_USER 角色中建立。使用 USER 角色建立並啟用使用者時，他們會收到自己的信箱以供存取。當用戶被禁用時，他們無法訪問 Amazon WorkMail。

使用 REMOTE_USER 角色建立並啟用的使用者會列在通訊錄中，但不會在 Amazon 中取得信箱。WorkMailREMOTE_USER 可以將信箱託管在 Amazon 以外， WorkMail 但仍將列為 Amazon 通 WorkMail 訊錄中具有郵箱的任何其他用戶，並且可以查找彼此的日曆以查找空閒或忙碌的信息。

群組

AWS Directory Service 中使用的群組。一個組可以用作 Amazon 中的分發列表或安全組 WorkMail。群組沒有自己的信箱。

資源

資源代表 Amazon WorkMail 使用者可預訂的會議室或設備資源。

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

以下服務與 Amazon 一起使用 WorkMail：

- AWS Directory Service— 您可以將 Amazon WorkMail 與現有的 S AWS imple AD，AWS託管 AD 或 AD Connector 集成在一起。在中建立目錄，AWS Directory Service然後 WorkMail 為此目錄啟用 Amazon。設定此整合之後，您可以 WorkMail 從現有目錄中的使用者清單中選擇要為 Amazon 啟用的使用者，使用者可以使用現有的 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 簡單電子郵件服務-亞馬遜 WorkMail 使用 Amazon SES 發送所有外發電子郵件。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 發送的傳出電子郵件沒有任何費用 WorkMail。有關詳情，請參閱 Amazon 簡易電子郵件服務開發人員指南。

- AWS Identity and Access ManagementAWS Management Console需要您的使用者名稱和密碼，以便您使用的任何服務都可以判斷您是否具有存取其資源的權限。建議您避免使用 AWS 帳戶登入資料來存取，AWS因為AWS帳戶登入資料無法以任何方式撤銷或限制。相反地，我們建議您建立 IAM 使用者，並將該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— 與 Amazon 集 WorkMail 成，用AWS KMS於對客戶數據進行加密。金鑰管理可以於 AWS KMS 主控台執行。如需詳細資訊，請參閱AWS Key Management Service開發人員指南AWS Key Management Service中的 [什麼是]。

Amazon WorkMail 定價

使用 Amazon WorkMail，沒有預付費用或承諾。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專門課程以及自主進度實驗室，協助加強您的 AWS 技能，並取得實際體驗。
- AWS 開發人員中心 – 研究教學課程、下載工具，以及瞭解 AWS 開發人員活動。
- AWS 開發人員工具 – 連結至開發人員工具、軟體開發套件、IDE 工具組和命令列工具，用來開發及管理 AWS 應用程式。
- 入門資源中心 – 瞭解如何設定 AWS 帳戶、加入 AWS 社群，並啟動您的第一個應用程式。
- 實作教學課程 — 按照 step-by-step 教學課程啟動您的第一個應用程式AWS。
- AWS 白皮書 – 連結至完整的技術 AWS 白皮書清單，其中涵蓋了架構、安全和成本等主題，並由 AWS 解決方案架構師或其他技術專家撰寫。
- AWS Support 中心 – 建立和管理您的 AWS Support 案例的中心。這也包含與其他實用資源的連結，例如論壇、技術常見問答集、服務運作狀態以及 AWS Trusted Advisor。
- AWS Support— 有關資訊的主要網頁 AWS Support one-on-one, 快速回應的支援管道，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 – 我們的著作權與商標；您的帳戶、授權與網站存取；以及其他主題的詳細資訊。

必要條件

要擔任 Amazon WorkMail 管理員，您需要一個 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

如果您還沒有 AWS 帳戶，請完成以下步驟建立新帳戶。

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。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   註冊 AWS 帳戶時，會建立 AWS 帳戶根使用者。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為最佳安全實務，將管理存取權指派給管理使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

註冊程序完成後，AWS 會傳送一封確認電子郵件給您。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。

建立管理使用者

當您註冊 AWS 帳戶 之後，請保護您的 AWS 帳戶根使用者，啟用 AWS IAM Identity Center，並建立管理使用者，讓您可以不使用根使用者處理日常作業。

保護您的 AWS 帳戶根使用者

1. 選擇 根使用者 並輸入您的 AWS 帳戶電子郵件地址，以帳戶擁有者身分登入 AWS Management Console。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)。

   如需指示，請參閱《IAM 使用者指南》中的為 AWS 帳戶根使用者啟用虛擬 MFA 裝置 (主控台)。

建立管理使用者

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，將管理權限授予管理使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的教學課程，請參閱《使用 AWS IAM Identity Center 使用者指南中的以預設 IAM Identity Center 目錄 設定使用者存取權限。

以管理員的身分登入

- 若要使用您的 IAM 身分中心使用者登入，請使用建立 IAM 身分中心使用者時傳送至您電子郵件地址的登入 URL。

  如需有關如何使用 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。

為 Amazon 授予 IAM 使用者許可 WorkMail

依預設，IAM 使用者沒有管理 Amazon WorkMail 資源的許可。您必須附加 AWS 受管政策 (AmazonWorkMailFullAccess或 AmazonWorkMailReadOnlyAccess) 或建立客戶管理政策，以明確授予 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。如需更多詳細資訊，請參閱 Amazon 的身份和訪問管理 WorkMail。

Amazon 的安全性 WorkMail

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同的責任。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 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供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 的合規計劃 WorkMail，請參閱合規計劃適用範圍的AWS 服務。
- 雲端安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 Amazon 時應用共同的責任模型 WorkMail。下列主題說明如何設定 Amazon WorkMail 以符合安全和合規目標。您也會學到如何使用其他 AWS 服務，協助您監控和保護 Amazon WorkMail 資源。

主題

- Amazon 的數據保護 WorkMail
- Amazon 的身份和訪問管理 WorkMail
- AWS Amazon 的受管政策 WorkMail
- 使用 Amazon 的服務連結角色色色色 WorkMail
- Amazon 中的記錄和監控 WorkMail
- Amazon 的合規驗證 WorkMail
- Amazon 的韌性 WorkMail
- Amazon 基礎設施安全 WorkMail

Amazon 的數據保護 WorkMail

AWS 共同責任模型適用於 Amazon 中的資料保護 WorkMail。如此模型所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需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，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。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。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，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) 140-2 概觀。

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。這包括當您使用控制台，API WorkMail 或 AWS SDK 與 Amazon 或其他 AWS 服務 AWS CLI人合作時。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 如何 WorkMail 使用 AWS KMS

在將訊息寫入磁碟之前，Amazon 會 WorkMail 透明地加密所有 Amazon WorkMail 組織信箱中的所有訊息，並在使用者存取訊息時透明地解密訊息。您無法停用加密。為了保護訊息的加密金鑰，Amazon WorkMail 與 AWS Key Management Service (AWS KMS) 整合。

Amazon WorkMail 也提供一個選項，讓使用者能夠傳送已簽署或加密的電子郵件。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

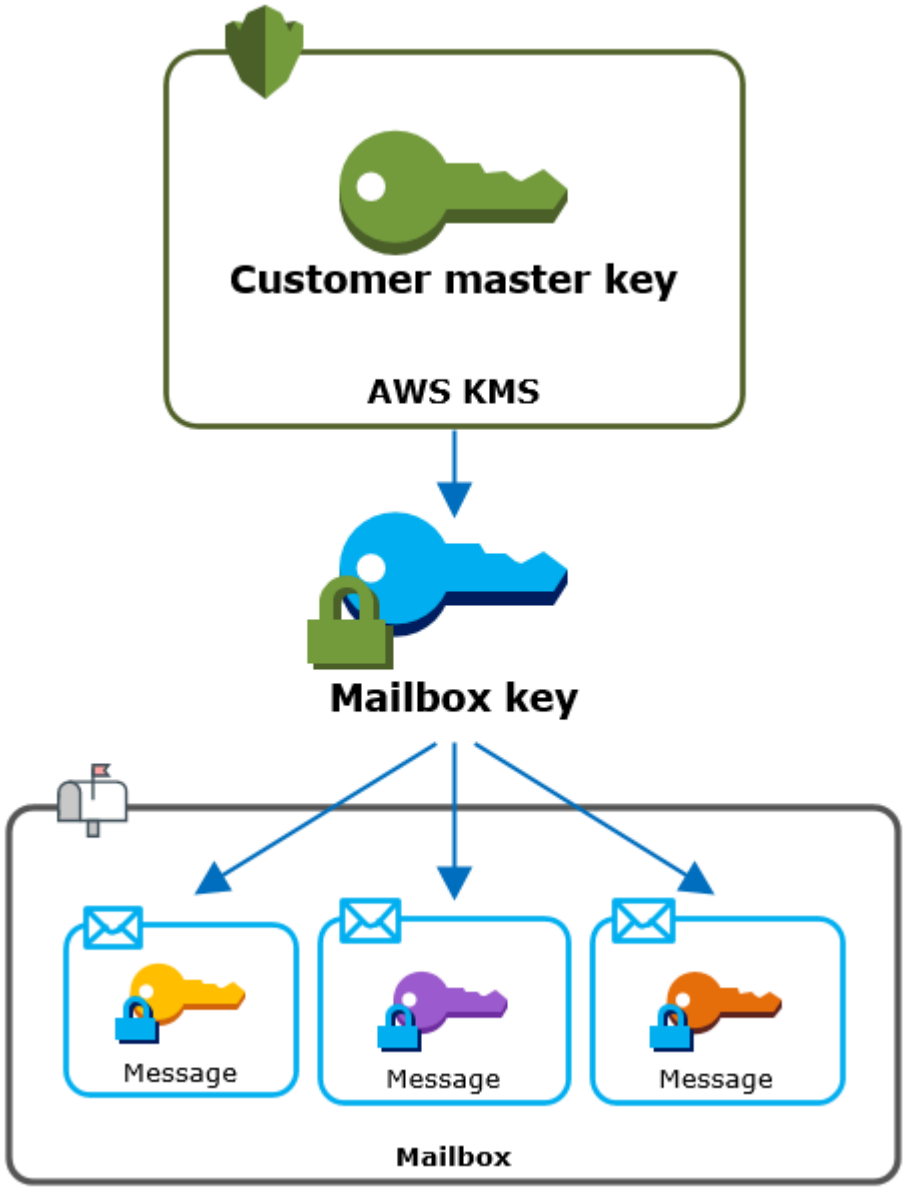
- Amazon WorkMail 加密
- 授權使用 CMK
- Amazon WorkMail 加密環境
- 監控 Amazon WorkMail 互動與 AWS KMS

Amazon WorkMail 加密

在 Amazon 中 WorkMail，每個組織都可以包含多個信箱，組織中的每個使用者一個信箱。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 組織中信箱的內容，Amazon 會在所有信箱訊息寫入磁碟之前先 WorkMail 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。信箱金鑰會根據 AWS KMS 客戶主要金鑰 (CMK) 加密，而組織永遠不會保留 AWS KMS 未加密。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。



為組織設定 CMK

建立 Amazon 組 WorkMail 織時，您可以選擇為組織選取 AWS KMS 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 的預設 AWS 受管 CMK WorkMail，也可以選取您擁有和管理的現有客戶管理 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 (CMK)。您可以為每個組織選取相同的 CMK 或不同的 CMK，但是一旦選取 CMK，就無法變更 CMK。

> **Important**
>
> Amazon 僅 WorkMail 支持對稱 CMK。您無法使用非對稱 CMK。如需確定 CMK 是對稱還是非對稱的說明，請參閱開發人員指南中的識別對稱和非對稱 CMK。AWS Key Management Service

若要尋找組織的 CMK，請使用記錄呼叫的記錄項目。 AWS CloudTrail AWS KMS

每個信箱的唯一加密金鑰

當您建立信箱時，Amazon WorkMail 會為信箱產生唯一的 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個訊息的加密金鑰。

為了保護信箱金鑰，Amazon 會 WorkMail 呼叫 AWS KMS 將組織 CMK 下的信箱金鑰加密。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。之前，Amazon 會使用非對稱 key pair 來 WorkMail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 key pair。此變更不會影響信箱或其訊息的安全性。

加密每封郵件

當使用者將訊息新增至信箱時，Amazon WorkMail 會為其外的訊息產生唯一的 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 會加密信箱金鑰下的訊息金鑰，並將加密的訊息金鑰與訊息一起儲存。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，會使用下列程序準備信箱以保存加密訊息。

- Amazon 為 AWS KMS 之外的信箱 WorkMail 產生唯一的 256 位元 AES 對稱加密金鑰。

- Amazon WorkMail 調用加 AWS KMS 密操作。它會傳遞信箱金鑰和組織的客戶主金鑰 (CMK) 的識別碼。 AWS KMS 傳回以 CMK 加密之信箱金鑰的密文字。
- Amazon 會將加密的信箱金鑰與信箱中繼資料一起 WorkMail 儲存。

加密信箱訊息

要加密消息，Amazon WorkMail 使用以下過程。

1. Amazon 為消息 WorkMail 生成一個唯一的 256 位 AES 對稱密鑰。它會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. 為了保護信箱金鑰下的訊息金鑰，Amazon WorkMail 需要解密信箱金鑰，信箱金鑰一律以其加密形式儲存。

   Amazon WorkMail 呼叫「 AWS KMS 解密」作業，並傳入加密的信箱金鑰。 AWS KMS 使用組織的 CMK 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 會將加密的訊息金鑰 WorkMail 儲存在加密訊息的中繼資料中，以便對其進行解密。

解密信箱訊息

要解密消息，Amazon WorkMail 使用以下過程。

1. Amazon WorkMail 呼叫「 AWS KMS 解密」作業，並傳入加密的信箱金鑰。 AWS KMS 使用組織的 CMK 解密信箱金鑰，並將純文字信箱金鑰傳回給 Amazon。 WorkMail
2. Amazon WorkMail 使用純文字信箱金鑰和進階加密標準 (AES) 演算法來解密外部的加密訊息金鑰。 AWS KMS
3. Amazon WorkMail 使用純文字訊息金鑰來解密加密的訊息。

快取信箱金鑰

為了改善效能並將呼叫減至最少 AWS KMS，Amazon 會在本機 WorkMail 快取每個用戶端的每個純文字信箱金鑰，最長可達一分鐘。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 可以從快取取取得金鑰，而不必呼叫 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 在密碼編譯作業中 WorkMail 使用客戶主金鑰 (CMK) 時，它會代表信箱管理員採取行動。

若要代表您使用 AWS KMS 客戶主要金鑰 (CMK) 做為密碼，管理員必須具備下列權限。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`

要允許 CMK 僅用於源自 Amazon 的請求 WorkMail，您可以使用帶有值的 kms: ViaService 條件鍵。`workmail.<region>.amazonaws.com`

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

適用於 Amazon 的 AWS 受管 CMK 金鑰政策 WorkMail 讓使用者只有在 Amazon 代表使用者 WorkMail 提出要求時，才允許使用者將 CMK 用於指定的作業。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。您無法變更金鑰原則，但可以隨時檢視。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 進行加密操作和建立授權，但只有當請求來自 Amazon WorkMail 代表他們。`kms:ViaService` 條件金鑰會強制實施此限制。
- 允許 AWS 帳戶建立 IAM 政策，讓使用者檢視 CMK 屬性和撤銷授權。

以下是適用於 Amazon WorkMail 的 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" : "*"
  } ]
}
```

使用贈款授權 Amazon WorkMail

除了關鍵政策之外，Amazon 還 WorkMail 使用授權為每個組織新增許可至 CMK。要查看您帳戶中 CMK 上的授予，請使用ListGrants操作。

Amazon WorkMail 使用授權將下列許可新增至組織的 CMK。

- 新增允許 Amazon WorkMail 加密信箱金鑰的`kms:Encrypt`權限。
- 新增允許 Amazon WorkMail 使用 CMK 解密信箱金鑰的`kms:Decrypt`權限。Amazon 在授權中 WorkMail 需要此權限，因為讀取信箱訊息的請求會使用讀取訊息之使用者的安全內容。請求不使用 AWS 帳戶的憑據。Amazon WorkMail 會在您為組織選取 CMK 時建立此授權。

若要建立贈款，Amazon 會代表建立組織的使用者 WorkMail 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`CreateGrant`在 Amazon 代表授權 WorkMail 使用者提出要求時，向組織的 CMK 撥打電話。

金鑰策略也允許帳號根目錄撤銷受 AWS 管理金鑰的授權。不過，如果您撤銷授權，Amazon 就 WorkMail 無法解密信箱中的加密資料。

Amazon WorkMail 加密環境

加密內容是一組金鑰/值對，其中包含任意非私密資料。當您在加密資料的要求中包含加密內容時，AWS KMS 密碼編譯會將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 在所 AWS KMS 有加密操作中 WorkMail 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。

在其加密和解密請求中 AWS KMS，Amazon WorkMail 使用密鑰所在的加密上下文，值是組織的 Amazon 資源名稱（ARN）。`aws:workmail: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 互動與 AWS KMS

您可以使用 AWS CloudTrail 和 Amazon CloudWatch 日誌來跟踪 Amazon 代表您 WorkMail 發送到 AWS KMS 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 以加密信箱金鑰。Amazon WorkMail 會將加密請求傳送到 AWS KMS Amazon 組織的明文信箱金鑰和 CMK 識別碼。 WorkMail

記錄 `Encrypt` 操作的事件類似於以下範例事件。用戶是 Amazon WorkMail 服務。這些參數包括 Amazon WorkMail 組織的 CMK ID (`keyId`) 和加密內容。Amazon WorkMail 也通過在郵箱密鑰，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 會 AWS KMS 要求您解密信箱金鑰。Amazon WorkMail 會將解密請求傳送至，其中 AWS KMS 包含加密信箱金鑰和 Amazon WorkMail 組織 CMK 的識別碼。

記錄 `Decrypt` 操作的事件類似於以下範例事件。用戶是 Amazon WorkMail 服務。這些參數包括未記錄在記錄中的加密信箱金鑰 (做為密文 Blob)，以及 Amazon WorkMail 組織的加密內容。 AWS KMS 從密文中導出 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 的身份和訪問管理 WorkMail

AWS Identity and Access Management (IAM) 可協助管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以通過身份驗證 (登入) 和授權 (具有許可) 來使用 Amazon WorkMail 資源。 您可以使用 IAM AWS 服務 ，無需額外付費。

主題

物件

您的使用方式 AWS Identity and Access Management (IAM) 會有所不同，具體取決於您在 Amazon 所做的工作 WorkMail。

服務使用者 — 如果您使用 Amazon WorkMail 服務執行工作，則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 功能完成工作時，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。如果您無法在 Amazon 中存取某個功能 WorkMail，請參閱疑難排解 Amazon WorkMail 身分和存取。

服務管理員 — 如果您負責公司的 Amazon WorkMail 資源，則可能擁有對 Amazon 的完全訪問權限 WorkMail。判斷服務使用者應存取哪些 Amazon WorkMail 功能和資源是您的工作。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將 IAM 與 Amazon 搭配使用 WorkMail，請參閱Amazon 如何與 IAM 合 WorkMail 作。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要了解如何撰寫政策來管理 Amazon 存取權限的詳細資訊 WorkMail。若要檢視可在 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

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴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識別的範例。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 AWS 用同盟存取時，您會間接擔任角色。

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

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

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) 來增加帳戶的安全性。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 使用者指南中的在 AWS中使用多重要素驗證 (MFA)。

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，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 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 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，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，但角色僅提供暫時憑證。如需進一步了解，請參閱 IAM 使用者指南中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法更多相關資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 – 若要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 (信任的委託人) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取權角色和資源型政策間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源類型政策的差異。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。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。
  - 轉寄存取工作階段 (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 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 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。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。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 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。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 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。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暫時憑證。如需更多資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

若要了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的更多相關資訊，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哪些內容。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。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 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。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

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。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管政策及內嵌政策間選擇，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。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些委託人 (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 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF若要進一步了解 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原則類型。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。如需許可範圍的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 實體許可範圍。
- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。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 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需組織和 SCP 的更多相關資訊，請參閱 AWS Organizations 使用者指南中的 SCP 運作方式。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。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。如需更多資訊，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。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Amazon 如何與 IAM 合 WorkMail 作

在您使用 IAM 管理對 Amazon 的存取權限之前 WorkMail，您應該了解哪些 IAM 功能可用於 Amazon WorkMail。若要深入瞭解 Amazon WorkMail 和其他 AWS 服務如何與 IAM 搭配使用，請參閱 IAM 使用者指南中的與 IAM 搭配使用的AWS 服務。

主題

- Amazon 基於 WorkMail身份的政策
- Amazon WorkMail 資源型政策
- 基於 Amazon WorkMail 標籤的授權
- Amazon WorkMail IAM 角色

Amazon 基於 WorkMail身份的政策

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、資源和條件金鑰。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哪些內容。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。原則動作通常與關聯的 AWS API 作業具有相同的名稱。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 中的政策動作會在動作之前 WorkMail 使用下列前置詞：`workmail:`例如，若要授與某人透過 Amazon WorkMail `ListUsers` API 操作擷取使用者清單的權限，您可以在他們的政策中加入該`workmail:ListUsers`動作。政策陳述式必須包含 `Action` 或 `NotAction` 元素。Amazon WorkMail 定義了自己的一組動作，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 WorkMail中由 Amazon 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哪些內容。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 支持 Amazon 組織的資源級許可。 WorkMail

Amazon 組 WorkMail 織資源具有以下 ARN：

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

如需 ARN 格式的詳細資訊，請參閱 Amazon 資源名稱 (ARN) 和 AWS 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 ARN 的清單，請參閱 IAM 使用者指南 WorkMail中的 Amazon 定義的資源。若要了解可以針對每個資源的 ARN 指定哪些動作，請參閱 Amazon WorkMail 的動作、資源和條件金鑰。

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從 eu-west-1 AWS 區域中經過 MFA 驗證的 IAM 主體存取 Amazon 主 WorkMail 控台的存取權。

```
{
    "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 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

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

下列範例針對特定 WorkMail 組織和模擬角色的政策範圍關閉`AssumeImpersonationRole`動作。

```
{
  "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 不支持以資源為基礎的政策。

基於 Amazon WorkMail 標籤的授權

您可以將標籤附加到 Amazon WorkMail 資源或將請求中的標籤傳遞給 Amazon WorkMail。若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，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。

使用 Amazon 臨時登入資料 WorkMail

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或等 AWS STS API 作業來取得臨時安全登入資料GetFederationToken。

Amazon WorkMail 支援使用臨時登入資料。

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 的服務連結角色色色色 WorkMail。

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 支持服務角色。

Amazon WorkMail 身分型政策範例

依預設，IAM 使用者和角色沒有建立或修改 Amazon WorkMail 資源的權限。他們也無法使用 AWS Management Console AWS CLI、或 AWS API 執行工作。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 控制台
- 允許使用者檢視他們自己的許可
- 允許使用者以唯讀方式存取 Amazon WorkMail 資源

政策最佳實務

以身分識別為基礎的政策決定某人是否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 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。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。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 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。您也可以使用條件來授與對服務動作的存取權 (如透過特定 AWS 服務) 使用 AWS CloudFormation。如需更多資訊，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，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 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 控制台

若要存取 Amazon WorkMail 主控台，您必須擁有最少一組許可。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。

為確保這些實體仍可使用 Amazon WorkMail 主控台，請同時將下列 AWS 受管政策附加到實體。AmazonWorkMailFullAccess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。

該AmazonWorkMailFullAccess政策授予 IAM 使用者對 Amazon WorkMail 資源的完整存取權。此政策使用戶可以訪問所有 Amazon WorkMail AWS Key Management Service，Amazon 簡單電子郵件服務和 AWS Directory Service 操作。這也包括 Amazon 代表您執行 WorkMail 的幾個 Amazon EC2 操作。電子郵件事件記錄logs和在 Amazon WorkMail 主控台中檢視指標需要和cloudwatch許可。稽核記錄會使用 CloudWatch 日誌、Amazon S3 和 Amazon 資料 FireHose 來存放logs。如需詳細資訊，請參閱 Amazon 中的記錄和監控 WorkMail。

```
{
  "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"
            }
        }
    }
  ]
}
```

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。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。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
```

```
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

允許使用者以唯讀方式存取 Amazon WorkMail 資源

以下政策聲明授予 IAM 使用者對 Amazon WorkMail 資源的唯讀存取權限。此政策提供與 AWS 受管政策相同的存取層級AmazonWorkMailReadOnlyAccess。這兩個政策都可讓使用者存取所有 Amazon WorkMail `Describe` 作業。需要訪問該 AWS Directory Service `DescribeDirectories`操作才能獲取有關 AWS Directory Service 目錄的信息。需要存取 Amazon SES 服務，才能取得已設定網域的相關資訊。需要 AWS Key Management Service 存取，才能取得有關所使用加密金鑰的資訊。在 `logs` Amazon WorkMail 主控台中，電子郵件事件記錄和檢視指標需要和`cloudwatch`許可。稽核記錄會使用 CloudWatch 日誌、Amazon S3 和 Amazon 資料 FireHose 來存放`logs`。如需詳細資訊，請參閱 Amazon 中的記錄和監控 WorkMail。

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

疑難排解 Amazon WorkMail 身分和存取

使用下列資訊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

- 我沒有授權在 Amazon 執行操作 WorkMail
- 我沒有授權執行 iam：PassRole
- 我想允許我 AWS 帳戶以外的人訪問我的 Amazon WorkMail 資源

我沒有授權在 Amazon 執行操作 WorkMail

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡您的管理員以尋求協助。您的管理員是提供您使用者名稱和密碼的人員。

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

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 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。

我沒有授權執行 iam：PassRole

如果您收到未獲授權執行`iam:PassRole`動作的錯誤訊息，則必須更新您的政策以允許您將角色傳遞給 Amazon WorkMail。

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

當名為的 IAM 使用者`marymajor`嘗試使用主控台在 Amazon 中執行動作時，會發生下列範例錯誤 WorkMail。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。

我想允許我 AWS 帳戶以外的人訪問我的 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 是否 WorkMail 支援這些功能，請參閱Amazon 如何與 IAM 合 WorkMail 作。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 IAM 使用者指南中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源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第三方 AWS 帳戶 擁有的存取權。
- 若要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)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源型政策的差異。

AWS Amazon 的受管政策 WorkMail

若要新增使用者、群組和角色的權限，使用 AWS 受管理的原則比自己撰寫原則更容易。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 AWS 受管政策的詳細資訊，請參閱 IAM 使用者指南中的AWS 受管政策。

AWS 服務會維護和更新 AWS 受管理的策略。您無法變更 AWS 受管理原則中的權限。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 受管理的政策移除權限，因此政策更新不會破壞您現有的權限。

此外，還 AWS 支援跨多個服務之工作職能的受管理原則。例如，ReadOnlyAccess AWS 受管理的策略提供對所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時，會為新作業和資源新 AWS 增唯讀權限。如需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 受管理的策略： AmazonWorkMailFullAccess

您可將 `AmazonWorkMailFullAccess` 政策連接到 IAM 身分。此政策授予允許完整存取 Amazon 的許可 WorkMail。

若要檢視此原則的權限，請參閱AmazonWorkMailFullAccess中的 AWS Management Console。

AWS 受管理的策略： AmazonWorkMailReadOnlyAccess

您可將 `AmazonWorkMailReadOnlyAccess` 政策連接到 IAM 身分。此政策授予允許 Amazon 唯讀存取權限的許可 WorkMail。

若要檢視此原則的權限，請參閱AmazonWorkMailReadOnlyAccess中的 AWS Management Console。

AWS 受管理的策略： AmazonWorkMailEventsServiceRolePolicy

此政策附加至名為的服務連結角色，AmazonWorkMailEvents以允許存取 Amazon WorkMail 事件所使用或管理的 AWS 服務和資源。如需詳細資訊，請參閱 使用 Amazon 的服務連結角色色色色 WorkMail。

Amazon WorkMail 更新受 AWS 管政策

檢視有關 Amazon AWS 受管政策更新的詳細資訊， WorkMail 因為此服務開始追蹤這些變更。

變更	描述	日期
AWS 受管政策更新-現有政策的更新	Amazon 已更新`AmazonWorkMailReadOnlyAccess` 和`AmazonWorkMailFullAccess` 許可，WorkMail 以支援稽核記錄。如需有關更新權限的詳細資訊，請參閱 Amazon WorkMail 身分型政策範例和如需稽核記錄的資訊，請參閱啟用稽核記錄。	2024年2月14日
Amazon WorkMail 開始跟踪變化	Amazon WorkMail 開始追蹤其 AWS 受管政策的變更。	2021 年 3 月 1 日

使用 Amazon 的服務連結角色色色色 WorkMail

亞馬遜 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 的一種特殊 IAM 角色類型 WorkMail。服務連結角色由 Amazon 預先定義 WorkMail ，內含該服務代您呼叫其他服AWS務所需的所有許可。

服務連結角色可讓設定 Amazon WorkMail 更為簡單，因為您不必手動新增必要的許可。Amazon WorkMail 定義其服務連結角色的許可，除非另有定義，否則僅有 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。如此可保護您的 Amazon WorkMail 資源，避免您不小心移除資源的存取許可。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的 AWS 服務，尋找服務連結角色欄顯示為是的服務。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 的服務連結角色許可許可 WorkMail

Amazon WorkMail 使用名為的服務連結角色 AmazonWorkMailEvents— Amazon WorkMail 使用此服務連結角色來存取 Amazon WorkMail 事件使用或管理的AWS服務和資源，例如監控記錄的電子郵件事件 CloudWatch。如需針對 Amazon 啟用 Amazon 的電子郵件事件日誌的詳細資訊 WorkMail，請參閱啟用電子郵件事件記。

服 AmazonWorkMailEvents 務連結角色信任下列服務以擔任角色：

- `events.workmail.amazonaws.com`

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

- 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。

建立 Amazon 的服務連結角色色色色色色色 WorkMail

您不需要手動建立一個服務連結角色。當您開啟 Amazon WorkMail 事件日誌記錄並且在 Amazon WorkMail 主控台中使用預設設定時，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 事件記錄並且使用預設設定時，Amazon WorkMail 會再次為您建立服務連結角色。

編輯 Amazon 的服務連結角色色色色色色色 WorkMail

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 的服務連結角色色色色色色色 WorkMail

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**
>
> 若 Amazon WorkMail 服務在您試圖刪除資源時正在使用該角色，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。

要刪除亞馬遜 WorkMail 資源使用 AmazonWorkMailEvents

1. 關閉亞馬遜 WorkMail 事件日誌記錄。
   a. 在以下位置打開亞馬遜 WorkMail 控制台 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 [選取地區] 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。
   b. 在導覽窗格中選擇組 Organ izations，然後選擇您組織的名稱。
   c. 在導覽窗格中，選擇組織設定，然後選擇監視。
   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 儲存 。
2. 刪除亞馬遜 CloudWatch 日誌組。
   a. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
   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 支援在所有提供服務的區域中，使用服務連結角色。如需詳細資訊，請參閱「Amazon WorkMail 區域和端點」。

Amazon 中的記錄和監控 WorkMail

監控和稽核您的電子郵件和日誌對於維持 Amazon WorkMail 組織的運作狀態非常重要。Amazon WorkMail 支持兩種類型的監控：

- 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信譽評等。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。
- 稽核記錄 — 您可以使用稽核日誌擷取有關 Amazon WorkMail 組織使用情況的詳細資訊，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 提供以下監控工具來觀看 Amazon WorkMail、在發生錯誤時報告，並在適當時採取自動動作：

- Amazon 會即時 CloudWatch監控您的 AWS 資源和執行 AWS 的應用程式。例如，當您為 Amazon 啟用電子郵件事件記錄時 WorkMail， CloudWatch 可以追蹤組織傳送和接收的電子郵件。如需 WorkMail 使用監控 Amazon 的詳細資訊 CloudWatch，請參閱 WorkMail 使用 CloudWatch 指標監控 Amazon。如需詳細資訊 CloudWatch，請參閱 Amazon CloudWatch 使用者指南。
- Amazon Lo CloudWatch gs 可讓您在 Amazon 主控台中啟用電子郵件和稽核記錄功能 WorkMail 時，監 WorkMail 控、存放和存取 Amazon 的電子郵件事件和稽核日誌。 CloudWatch 日誌可以監控日誌文件中的信息，您可以將日誌數據存檔在高耐久性的存儲中。如需使用 CloudWatch 日誌追蹤 Amazon 訊 WorkMail息的詳細資訊，請參閱啟用電子郵件事件記和啟用稽核記錄。如需有關 CloudWatch 日誌的詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南。
- AWS CloudTrail擷取由您或代表您發出的 API 呼叫和相關事件 AWS 帳戶，並將日誌檔傳送到您指定的 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 位址，以及呼叫發生的時間。如需詳細資訊，請參閱 記錄 Amazon WorkMail API 呼叫 AWS CloudTrail。
- Amazon S3 可讓您以經濟實惠的方式存放和存取 Amazon WorkMail 事件。Amazon S3 提供管理事件資料生命週期的機制，讓您設定自動刪除舊事件，或設定自動存檔至 Amazon S3 Glacier。請注意，Amazon S3 交付僅適用於稽核記錄事件。如需有關 Amazon S3 的詳細資訊，請參閱 Amazon S3 使用者指南。
- Amazon 數據 Firehose 使您可以將事件數據流式傳輸到其他 AWS 服務，例如 Amazon 簡單存儲服務（Amazon S3），Amazon 紅移，亞馬遜服務，亞馬遜 OpenSearch 無 OpenSearch 服務器，Splunk 以及受支持的第三方服務提供商擁有的任何自定義 HTTP 端點或 HTTP 端點，包括數據多，重新發布，新遺物， LogicMonitorCoralogix 和彈性。傳遞至 Firehose 僅適用於稽核記錄事件。如需有關 Firehose 的詳細資訊，請參閱 Amazon 資料 Firehose 開發人員指南。

主題

- WorkMail 使用 CloudWatch 指標監控 Amazon
- 監控 Amazon WorkMail 電子郵件事件日誌
- 監控 Amazon WorkMail 稽核日誌

- 使用 Amazon 的 CloudWatch 洞察 WorkMail
- 記錄 Amazon WorkMail API 呼叫 AWS CloudTrail
- 啟用電子郵件事件記
- 啟用稽核記錄

WorkMail 使用 CloudWatch 指標監控 Amazon

您可以 WorkMail 使用 CloudWatch收集原始資料並將其處理為可讀且接近即時的指標來監控 Amazon。免費指標會儲存 15 個月，以便您存取歷史資訊，以查看 Web 應用程式或服務的執行情況。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。

CloudWatch Amazon 的指標 WorkMail

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。如果一封電子郵件寄給組織中的 10 位收件者，則OrganizationEmailReceived 計數為 1。 單位：計數
MailboxEmailDelivered	傳遞至 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傳遞給組織中的 10 位收件者，則MailboxEmailDelivered 計數為 10。 單位：計數
IncomingEmailBounced	由於信箱已滿而退回的傳入電子郵件數目。這個指標會將每個預期收件人計入。例如，如果一封電子郵件傳送給組織中的 10 位收件者，而其

指標	描述
	中兩位收件者擁有完整信箱，而導致退回回應，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，如果一封電子郵件傳送給 10 位收件者，但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	此測量結果會計算認證嘗試的次數。驗證成功時，計數為 0，當驗證失敗時，計數為 1。使用Sum統計資料來監視失敗的驗證嘗試次數。使用Sample count統計資料來監視驗證事件的總數。使用Average統計資料來監視失敗和成功驗證事件的比率。 單位：計數
AccessDenied	此測量結果會計算存取控制評估的數目。當存取控制拒絕動作時，計數為 1，而當授與動作時，計數為 0。使用Sum統計資料來監視拒絕的動作數量、監督嘗試的動作總數的Sample count統計資料，以及監督允許和拒絕動作比率的Average統計資料。 單位：計數

指標	描述
ActionDenied	當信箱資料有動作時，就會計算此度量。拒絕動作時，計數為 1，如果授與動作，則計數為 0。使用Sum統計資料來監視拒絕信箱動作的數量、監視嘗試信箱動作總數的Sample count統計資料，以及監視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 執行的每個可用性供應商請求，以從外部來源擷取行事曆可用性。如需可用性供應商的詳細資訊，請參閱 Amazon WorkMail 管理員指南。

監控 Amazon WorkMail 電子郵件事件日誌

當您為 Amazon WorkMail 組織開啟電子郵件事件記錄時，Amazon 會使用記 WorkMail 錄電子郵件事件 CloudWatch。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。

下表說明 Amazon WorkMail 記錄的事件 CloudWatch、傳輸事件的時間，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，就會記錄此事件。

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

欄位	描述
	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	指出郵件是否被 Amazon SES 標示為垃圾郵件。如需詳細資訊，請參閱 Amazon 簡易電子郵件服務開發人員指南中的 Amazon SES 電子郵件接收通知內容。
dkimVerdict	指出「 DomainKeys 識別的郵件」(DKIM) 檢查是否通過。如需詳細資訊，請參閱 Amazon 簡易電子郵件服務開發人員指南中的 Amazon SES 電子郵件接收通知內容。
dmarcVerdict	指出以網域為基礎的訊息驗證、報告及一致性 (DMARC) 檢查是否通過。如需詳細資訊，請參閱 Amazon 簡易電子郵件服務開發人員指南中的 Amazon SES 電子郵件接收通知內容。
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。
spfVerdict	指出寄件者原則架構 (SPF) 檢查是否通過。如需詳細資訊，請參閱 Amazon 簡易電子郵件服務開發人員指南中的 Amazon SES 電子郵件接收通知內容。
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

當內送或外寄郵件啟動電子郵件流程規則時，就會記錄此事件。

欄位	描述
ruleName	規則的名稱。
ruleType	套用的規則類型 (「輸入規則」、「輸出規則」或「信箱規則」)。入站和輸出規則適用於您的 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。
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

Amazon WorkMail 將電子郵件傳送至組織管理員指定的日誌地址時，就會記錄此事件。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 使用電子郵件日誌 WorkMail。

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

當內送郵件無法傳遞給目標收件者時，就會記錄此事件。電子郵件可能會因為多種原因而退回，例如完整的目標信箱。系統會針對每個導致退回電子郵件的收件者記錄此事件一次。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 退回該消息的預定收件人。

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。這是在訊息離開 Amazon 之前記錄的 WorkMail，因此此事件不會指出電子郵件是否已成功傳遞。

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。

欄位	描述
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

當外寄郵件無法傳遞給目標收件者時，就會記錄此事件。電子郵件可能會因為多種原因而退回，例如完整的目標信箱。系統會針對每個收件者記錄退回的電子郵件的退信。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 組織信箱的存取。Amazon WorkMail 記錄了四種類型的稽核事件，這些事件可以發佈到 CloudWatch 日誌、Amazon S3 或 Amazon 防火站。您可以使用稽核記錄來監視使用者與組織信箱的互動、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。如需有關配置稽核記錄的資訊，請參閱啟用稽核記錄。

以下各節說明 Amazon 記錄的稽核事件 WorkMail、事件傳輸時間，以及事件欄位的相關資訊。

信箱存取記錄檔

信箱存取事件提供對哪個信箱物件採取 (或嘗試) 動作的相關資訊。會針對您嘗試在信箱中的項目或資料夾上執行的每項作業產生信箱存取事件。這些事件對於稽核信箱資料的存取非常有用。

欄位	描述
event_timestamp	當事件發生時，以毫秒為單位，自 Unix 時代以來。
request_id	唯一識別要求的識別碼。
阿恩组织	已驗證使用者所屬的和 Amazon WorkMail 組織的 ARN。

欄位	描述
user_id	已驗證使用者的識別碼。
模仿者	模擬者的識別碼。僅當使用模擬功能用於請求時才會顯示。
protocol	使用的通訊協定。通訊協定可以是：AutoDiscover EWSIMAP、WindowsOutlook 、ActiveSync 、SMTP、、WebMail、IncomingEmail 、或OutgoingEmail 。
IP 來源	要求的來源 IP 位址。
user_agent	提出要求的使用者代理程式。
動作	對物件執行的動作，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_sending_email 、move、move_to、、copy、或copy_to。
owner_id	擁有所執行動作之物件的使用者識別碼。
object_type	物件類型，可以是：「資料夾」、「訊息」或「附件」。
item_id	唯一識別為事件主旨或包含事件主旨之附件之郵件的 ID。
資料夾路徑	正在處理的資料夾路徑，或包含正在處理之項目的資料夾路徑。

欄位	描述
資料夾識別碼	唯一識別作為事件主旨的資料夾或包含作為事件主旨之物件的識別碼。
附件路徑	受影響附件的顯示名稱路徑。
動作允許 (_)	是否允許動作。可以是真的也可以是假的。

存取控制記錄

每當評估存取控制規則時，就會產生存取控制事件。這些記錄檔對於稽核禁止存取或偵錯存取控制組態非常有用。

欄位	描述
event_timestamp	當事件發生時，以毫秒為單位，自 Unix 時代以來。
request_id	唯一識別要求的識別碼。
阿恩组织	已驗證使用者所屬之 WorkMail 組織的 ARN。
user_id	已驗證使用者的識別碼。
模仿者	模擬者的識別碼。僅當使用模擬功能用於請求時才會顯示。
protocol	使用的通訊協定，可以是：`AutoDiscover` `EWS` `IMAP`、`WindowsOutlook` 、`ActiveSync` 、`SMTP`、`WebMail`、、`IncomingEmail` 、或`OutgoingEmail` 。
IP 來源	要求的來源 IP 位址。
scope	規則的範圍，可以是：`AccessControl` `DeviceAccessControl` 、或`ImpersonationAccessControl` 。

欄位	描述
規則識別碼	相符存取控制規則的識別碼。如果沒有符合的規則，rule_id 就無法使用。
授予訪問	是否允許存取。可以是真的也可以是假的。

驗證記錄

驗證事件包含驗證嘗試的相關資訊。

> **Note**
>
> 不會透過 Amazon WorkMail WebMail 應用程式為身份驗證事件產生身份驗證事件。

欄位	描述
event_timestamp	當事件發生時，以毫秒為單位，自 Unix 時代以來。
request_id	唯一識別要求的識別碼。
阿恩组织	已驗證使用者所屬之 WorkMail 組織的 ARN。
user_id	已驗證使用者的識別碼。
使用者	嘗試使用驗證的使用者名稱。
protocol	使用的通訊協定，可以是：`AutoDiscover` `EWS`、`IMAP`、`WindowsOutlook` 、`ActiveSync` 、`SMTP`、`WebMail`、、`IncomingEmail` 、或`OutgoingEmail` 。
IP 來源	要求的來源 IP 位址。
user_agent	提出要求的使用者代理程式。

欄位	描述
方法	身份驗證方法。目前，僅支援基本版本。
成功	無論是驗證嘗試成功。可以是真的也可以是假的。
失敗原因	身份驗證失敗的原因。僅在身份驗證失敗時出現。

可用性提供程式

Amazon 代表您向設定的可用性供應商 WorkMail執行的每個可用性請求產生可用性提供者事件。這些事件對於偵錯可用性提供者組態非常有用。

欄位	描述
event_timestamp	當事件發生時，以毫秒為單位，自 Unix 時代以來。
request_id	唯一識別要求的識別碼。
阿恩组织	已驗證使用者所屬之 WorkMail 組織的 ARN。
user_id	已驗證使用者的識別碼。
type	要呼叫的可用性提供者類型，可以是：EWS或LAMBDA。
domain	取得可用性的網域。
函數	被調用的 Lambda 的 ARN，如果類型是 LAMBDA。否則，此欄位不存在。
ews 端點	EWS 端點的類型是 EWS。否則，此欄位不存在。
error_message	描述失敗原因的訊息。如果請求成功，則此欄位不存在。

欄位	描述
可用性 _ 事件 _ 成功	是否已成功提供可用性要求。

使用 Amazon 的 CloudWatch 洞察 WorkMail

如果您在 Amazon WorkMail 主控台中開啟電子郵件事件記錄功能，或啟用了將稽核 CloudWatch 日誌交付到日誌，則可以使用 Amazon CloudWatch 日誌洞察來查詢事件日誌。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。如需有關 CloudWatch 日誌洞見的詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南中的使用日誌洞察分析 CloudWatch 日誌資料。

下列範例示範如何查詢常見電子郵件事件的 CloudWatch 記錄檔。您可以在 CloudWatch 主控台中執行這些查詢。如需有關如何執行這些查詢的指示，請參閱 Amazon CloudWatch Logs 使用者指南中的教學課程：執行和修改查詢範例。

Example 瞭解使用者 B 為何沒有收到使用者 A 所傳送的電子郵件。

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 查看誰發送了退回的電子郵件

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"
```

下列程式碼範例會示範如何查詢已退回的傳入電子郵件。它還會返回退回的收件人的電子郵件地址以及彈跳的原因。

```
fields @timestamp, event.bouncedRecipient.emailAddress, event.bouncedRecipient.reason,
 event.bouncedRecipient.status
| sort @timestamp desc
```

```
| filter event.eventName = "INCOMING_EMAIL_BOUNCED"
```

Example 查看哪些網域傳送垃圾郵件

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 瞭解電子郵件傳送至收件者的垃圾郵件資料夾的原因

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郵

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了多少封電子郵件

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
```

記錄 Amazon WorkMail API 呼叫 AWS CloudTrail

Amazon 集 WorkMail 成了一種服務 AWS CloudTrail，該服務可提供用戶，角色或 AWS 服務 在 Amazon 中採取的操作記錄 WorkMail。 CloudTrail 以事件 WorkMail形式擷取 Amazon 的所有 API 呼叫，包括來自 Amazon WorkMail 主控台的呼叫，以及從程式碼呼叫到 Amazon WorkMail API 的呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 Amazon 的事件 WorkMail。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷向 Amazon 發出的請求 WorkMail、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，請參閱使AWS CloudTrail 用者指南。

Amazon WorkMail 信息 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。在 Amazon 中發生活動時 WorkMail，該活動會與事件歷史記錄中的其他 CloudTrail AWS 服務 事件一起記錄在事件中。您可以查看，搜索和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

如需 AWS 帳戶中持續記錄事件 (包括 Amazon 的事件) WorkMail，您必須建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套

用至所有的 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件和從多個帳戶接收 CloudTrail 日誌文件

所有 Amazon WorkMail 動作都會記錄下來， CloudTrail 並記錄在 Amazon WorkMail API 參考中。例如，對`CreateUser`、`CreateAlias`、和 `GetRawMessageContent` API 作業的呼叫會在 CloudTrail記錄檔中產生項目。

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使 userIdentity 元素。

了解 Amazon WorkMail 日誌文件條目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。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 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

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

```
{
  "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"
}
```

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

```
{
  "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"
}
```

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

```
{
  "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

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) 來授與將電子郵件事件日誌發佈到 Amazon 的許可。 CloudWatch如需 IAM 服務連結角色的詳細資訊，請參閱使用 Amazon 的服務連結角色色色色 WorkMail。

在 CloudWatch 事件記錄檔中，您可以使用 CloudWatch 搜尋工具和指標來追蹤郵件並疑難排解電子郵件問題。如需 Amazon WorkMail 傳送至之事件日誌的詳細資訊 CloudWatch，請參閱監控 Amazon WorkMail 電子郵件事件日誌。如需有關 CloudWatch 日誌的詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南。

主題

啟用電子郵件事件記錄

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

- 建立 AWS Identity and Access Management 服務連結角色 — `AmazonWorkMailEvents`。
- 建立 CloudWatch 記錄群組 — `/aws/workmail/emailevents/`*`organization-alias`*。
- 將 CloudWatch 記錄保留設定為 30 天。

啟用電子郵件事件記錄

1. 在 https://console.aws.amazon.com/workmail/ 打開 Amazon WorkMail 控制台。

   如有必要，請變更「 AWS 區域」。在主控台視窗頂端的列中，開啟 [選取地區] 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 Organ izations」，然後選擇組織的名稱。
3. 在功能窗格中，選擇 [記錄設定]。
4. 選擇電子郵件流程記錄設定索引標籤。

5. 在電子郵件流程記錄設定區段中，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) 選擇 [使用預設設定]。
   - (選擇性) 清除 [使用預設設定]，然後從顯示的清單中選取 [目的地記錄群組] 和 [IAM 角色]。

   > **Note**
   >
   > 僅當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 建立用於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. 選擇儲存。

建立用於電子郵件事件記錄的自訂日誌群組和 IAM 角色

我們建議在啟用 Amazon 的電子郵件事件記錄時使用預設設定 WorkMail。如果您需要自訂監控設定，可以使用建立專 AWS CLI 用的日誌群組和自訂 IAM 角色以進行電子郵件事件記錄。

建立用於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 Amazon WorkMail 組織所在的相同 AWS 區域中建立日誌群組。若要取得更多資訊，請參閱《指AWS CLI 令參考》create-log-group中的。

```
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受管原則使用者，則必須在角色名稱workmail中包含該字詞。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》中的授與使用者將角色傳遞給 AWS 服務的權限。

4. 建立包含您在上一個步驟中建立的 IAM 角色政策的檔案。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. 使用下列 AWS CLI 命令將政策檔附加至 IAM 角色。若要取得更多資訊，請參閱《指AWS CLI 令參考》put-role-policy中的。

```
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，建議您也刪除相關的記 CloudWatch 錄群組和服務連結角色。如需詳細資訊，請參閱 刪除 Amazon 的服務連結角色色色色色色色 WorkMail。

關閉電子郵件事件日誌

1. 在 https://console.aws.amazon.com/workmail/ 打開 Amazon WorkMail 控制台。

   如有必要，請變更「 AWS 區域」。在主控台視窗頂端的列中，開啟 [選取地區] 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 Organ izations」，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 Monitoring (監控)。
4. 在「記錄設定」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的副問題。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。

調用服務可以被操縱以使用其權限來處理另一個客戶的資源，否則它將無法訪問。

為了防止這種情況發生， AWS 提供的工具可協助您透過已授予您帳戶中資源存取權的服務主體來保護所有服務的資料。

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 提供給產生日誌之服務的許可。如果您同時使用全域條件內容索引鍵，則在相同政策陳述式中使用時，這些值必須使用相同的帳號 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擷取有關 Amazon WorkMail 組織使用情況的詳細資訊。稽核記錄檔可用來監視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受管理的策略不包括管理日誌傳遞的所有必要權限。如果您使用此原則來管理 WorkMail，請確定用來設定記錄傳送的主參與者 (例如，假設的角色) 也具有所有必要的權限。

Amazon WorkMail 支援稽核日誌的三個交付目的地： CloudWatch 日誌、Amazon S3 和 Amazon 資料 Firehose。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南中的需要其他許可的記錄 [V2]。

除了需要額外許可 [V2] 的記錄下列出的許可外，Amazon 還 WorkMail 需要額外的權限才能設定日誌傳遞：`workmail:AllowVendedLogDeliveryForResource`。

工作記錄傳送包含三個元素：

- DeliverySource，代表傳送記錄的資源或資源的邏輯物件。對於 Amazon 來說 WorkMail，這是 Amazon WorkMail 組織。
- A DeliveryDestination，這是代表實際傳遞目的地的邏輯物件。
- 傳送，將傳送來源連接至傳送目的地。

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

- 使用建立傳送來源PutDeliverySource。
- 使用建立傳送目的地PutDeliveryDestination。
- 如果您要跨帳戶交付記錄，則必須PutDeliveryDestinationPolicy在目標帳戶中使用，將 IAM 政策指派給目的地。此原則授權從帳戶 A 中的傳遞來源建立傳遞至帳戶 B 中的傳送目的地。
- 使用將一個傳送來源和一個傳送目的地完全配對，以建立傳送CreateDelivery。

以下各節提供登入時必須擁有的權限詳細資料，以便設定每種目的地類型的記錄傳遞。您可以將這些權限授與您登入的 IAM 角色。

> **Important**
>
> 您有責任在刪除記錄產生資源之後移除記錄傳遞資源。

若要在刪除記錄產生資源之後移除記錄傳遞資源，請依照下列步驟執行。

1. 使用DeleteDelivery作業刪除傳送。
2. 使用DeliverySource作DeleteDeliverySource業刪除。
3. 如果DeliveryDestination與您剛剛刪除的DeliverySource相關聯僅用於此特定內容 DeliverySource，則可以使用該DeleteDeliveryDestinations操作將其刪除。

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://console.aws.amazon.com/workmail/ 打開 Amazon WorkMail 控制台。

   如有必要，請變更「 AWS 區域」。在主控台視窗頂端的列中，開啟 [選取地區] 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 Organ izations」，然後選擇組織的名稱。
3. 選擇 [記錄設定]。
4. 選擇 [稽核記錄設定] 索引標籤。
5. 使用適當的 Widget 設定所需記錄類型的傳送。
6. 選擇儲存。

傳送至記錄 CloudWatch 檔的記錄

使用者許可

若要啟用將記錄檔傳送至 CloudWatch 記錄檔，您必須使用下列權限登入。

```
{
    "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": "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。如果記錄群組目前沒有資源原則，而且設定記錄的使用者具有記錄群組的logs:PutResourcePolicylogs:DescribeResourcePolicies、和logs:DescribeLogGroups權限，則當您開始將記錄檔傳送至記 CloudWatch 錄檔時，會 AWS 自動為其建立下列原則。

```
{
    "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原則中列出要傳送記錄檔的每個記錄群組。 CloudWatch 記錄檔資源策略的長度限制為 5,120 個字元。將記錄檔傳送至大量記錄群組的服務可能會遇到此限制。

為了減輕此問題， CloudWatch Logs 會監視傳送記錄檔之服務所使用的資源策略大小。當偵測到原則接近 5,120 個字元的大小限制時， CloudWatch 記錄檔會自動/aws/vendedlogs/*在該服務的資源原則中啟用。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，則當您開始將日誌傳送到 Amazon S3 時， AWS 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:*"
                    ]
                }
            }
        }
    ]
}
```

在先前的策略中aws:SourceAccount，針對指定要傳送至此儲存貯體的記錄檔之帳號 ID 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*:*。

如果值區具有資源策略，但該政策未包含先前政策中顯示的陳述式，且設定記錄的使用者擁有值區的S3:GetBucketPolicy和S3:PutBucketPolicy權限，則該陳述式會附加至值區的資源策略。

> **Note**
>
> 在某些情況下， AWS CloudTrail 如果未授予s3:ListBucket權限，您可能會在中看到AccessDenied錯誤訊息delivery.logs.amazonaws.com。若要避免 CloudTrail記錄中出現這些錯誤，您必須將s3:ListBucket權限授與delivery.logs.amazonaws.com。此外，您還必須包含與上述儲存貯體策略中設定s3:GetBucketAcl權限一起顯示的Condition參數。為了簡化此操作，您可以直接將其更新AWSLogDeliveryAclCheck為Statement，而不是創建新的“Action”: [“s3:GetBucketAcl”, “s3:ListBucket”]。

Amazon S3 儲存貯體伺服器端加密

您可以使用 Amazon S3 受管金鑰 (SSE-S3) 啟用伺服器端加密，或使用存放在 (SSE-KMS) 的伺服器端加密來保護 Amazon S3 儲存貯體中的資 AWS Key Management Service 料。 AWS KMS 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，則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 受管理金鑰設定加密，記錄檔將會以無法讀取的格式傳遞。

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 資源名稱 (ARN)。將以下內容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)，以便日誌交付帳戶可以寫入 S3 儲存貯體。

如果您選擇 SSE-KMS，則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。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 資源名稱 (ARN)。將以下內容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)，以便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，指定要傳送記錄至此儲存貯體的帳號 ID 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*:*。

原木已傳送至 Firehose

使用者許可

若要啟用將記錄檔傳送至 Firehose，您必須使用下列權限登入。

```
{
    "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， AWS 因此在設定這些記錄檔以傳送至 Firehose 時，會使用 IAM 角色。 AWS 會建立名為AWSServiceRoleForLogDelivery的服務連結角色。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"
        }
    ]
}
```

此服務連結角色會授予LogDeliveryEnabled標籤設定為的所有 Firehose 傳遞串流的權限。`true` AWS 當您設定記錄時，將此標記提供給目的地傳遞串流。

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"
    }
  ]
}
```

主機特定權限

除了上一節所列的權限之外，如果您要使用主控台而非 API 來設定記錄傳遞，您還需要下列權限：

```
{
    "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 的合規驗證 WorkMail

第三方稽核員會在多個合規計劃中評估 Amazon WorkMail 的安全性和合 AWS 規性。其中包括 SOC、ISO 和 C5。

如需特定合規計劃範圍內的 AWS 服務清單，請參閱合規計劃的 AWS 服務範圍。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。

使用 Amazon 時的合規責任取決 WorkMail 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遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供在上部署以安全性和法規遵循為重點的基準環境的步驟。 AWS
- AWS 合規資源 — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS Config— 此 AWS 服務評估您的資源配置是否符合內部實踐，行業準則和法規。
- AWS Security Hub— 此 AWS 服務提供安全狀態的全面檢視，協助您檢查您 AWS 是否符合安全性產業標準和最佳做法。

Amazon 的韌性 WorkMail

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

如需區域和可用區域的相關 AWS 資訊，請參閱AWS 全域基礎結構。

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

Amazon 基礎設施安全 WorkMail

> **Note**
>
> Amazon WorkMail 停止了對傳輸層安全性（TLS）1.0 和 1.1 的支持。如果您使用 TLS 1.0 或 1.1，您必須將 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 協定層級。

作為一項受管服務，Amazon WorkMail 受到 AWS 全球網路安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫 WorkMail 透過網路存取 Amazon。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。

開始使用 Amazon WorkMail

完成後必要條件，您就可以開始使用 Amazon 了 WorkMail。如需詳細資訊，請參閱 開始使用 Amazon WorkMail。

您可以在以下各節中進一步了解如何將現有信箱遷移到 Amazon WorkMail、與 Microsoft Exchange 的互通性以及 Amazon WorkMail 配額的相關資訊。

主題

開始使用 Amazon WorkMail

無論您是 Amazon 的新 WorkMail 用戶還是 Amazon WorkDocs 或 Amazon 的現有用戶 WorkSpaces，都可以 WorkMail 通過完成以下步驟開始使用 Amazon。

> **Note**
>
> 開始使用前，請先完成 必要條件。

主題

步驟 1：登錄到 Amazon 控 WorkMail 制台

您必須先登入 Amazon 主 WorkMail 控台，才能新增使用者並管理其帳戶和信箱。

登錄到 Amazon 控 WorkMail 制台

1. 在以下位置打開 Amazon WorkMail 控制台 https://console.aws.amazon.com/workmail/。
2. 如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟 [選取地區] 清單，然後選擇 [區域]。如需有關區域的詳細資訊，請參閱中的區域和端點Amazon Web Services 一般參考。

第 2 步：設置您的 Amazon WorkMail 網站

1. 登入 Amazon WorkMail 主控台後，您可以設定組織並新增網域。我們建議您為 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. （可選）您可以選擇使用 Amazon 提供的免費測試域 WorkMail。如果您選擇這樣做，請跳至步驟 4。

> **Note**
>
> 測試網域使用以下格式：## .awsapps.com。當您進行時，請記住，您應該只使用測試域進行測試。請勿在生產環境中使用測試網域。此外，您的 Amazon WorkMail 組織中必須至少有一個啟用使用者。如果您沒有啟用的使用者，則該網域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 記錄允許您在 DNS 中輸入備註。MX 記錄會指定內送郵件伺服器。請務必將您的網域設定為組織的預設網域。如需詳細資訊，請參閱 驗證網域 及 選擇預設網域。
4. 為 Amazon 建立新使用者或啟用現有的目錄使用者 WorkMail。如需詳細資訊，請參閱 新增使用者。
5. (選擇性) 如果您有現有的 Microsoft Exchange 信箱，請將它們遷移到 Amazon WorkMail。如需詳細資訊，請參閱 遷移到 Amazon WorkMail。

完成設置 Amazon 網 WorkMail 站後，您可以使用 Web 應 WorkMail 用程序 URL 訪問 Amazon。

找到您的 Amazon WorkMail 網絡應用程序 URL

1. 在以下位置打開 Amazon WorkMail 控制台 https://console.aws.amazon.com/workmail/。

   如有必要請變更 AWS 區域。若要這麼做，請開啟位於搜尋方塊右側的 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，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。這些網址採用這種形式：HTTPS://## .awsapps.com /郵件。

步驟 3：設置 Amazon WorkMail 用戶訪問

從下列選項中選擇以設定 Amazon WorkMail 使用者存取權限：

- 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 Connect 到您的 Amazon WorkMail 帳戶。
- 從移動設備（例如 Kindle，安卓，iPad 或 iPhone）設置用戶訪問權限。如需詳細資訊，請參閱行動裝置入門。
- 若要設定使用者存取權，請使用任何與網際網路郵件存取通訊協定 (IMAP) 通訊協定相容的用戶端軟體。如需詳細資訊，請參閱將 IMAP 用戶端連線到您的 Amazon WorkMail 帳戶。

其他 資源

- 遷移到 Amazon WorkMail
- Amazon WorkMail 和 Microsoft 交易所的互操作
- Amazon WorkMail 配額

遷移到 Amazon WorkMail

您可以遷移到 Amazon WorkMail 從 Microsoft 交換, Microsoft 辦公室 365, G 套房基本 (原谷歌企業應用套件工作), 和其他平台與我們的合作夥伴之一的工作. 如需有關合作夥伴的詳細資訊，請參閱 Amazon WorkMail 功能。

主題

步驟 1：在 Amazon 中創建或啟用用戶 WorkMail

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

第 2 步：遷移到 Amazon WorkMail

您可以與任何AWS遷移合作夥伴合作遷移到 Amazon WorkMail。如需這些供應商的相關資訊，請參閱 Amazon WorkMail 功能。

若要遷移信箱，請建立專屬的 Amazon WorkMail 使用者以擔任遷移管理員。下列程序會授與該使用者存取組織中所有信箱的權限。

建立遷移管理員

1. 執行以下任意一項：
   - 在 Amazon 主 WorkMail 控台中，建立新使用者以擔任移轉管理員。如需詳細資訊，請參閱 新增使用者。
   - 在您的活動目錄中，創建一個新的用戶作為遷移管理員，然後為 Amazon 啟用該用戶 WorkMail。如需詳細資訊，請參閱 啟用使用者。
2. 在 Amazon 主 WorkMail 控台導覽窗格中，選擇「組 Organ izations」，然後選擇組織的名稱。
3. 依序選擇 [組織設定]、[移轉] 和 [編輯]。
4. 將已啟用移轉的滑桿移至開啟位置。
5. 開啟移轉管理員並選取使用者。
6. 選擇儲存。

步驟 3：完成遷移到 Amazon WorkMail

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

完成遷移到 Amazon WorkMail

1. 驗證所有 DNS 記錄都已更新，並且它們指向 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數小時。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. 有關將桌面或移動客戶端配置為使用 Amazon 的更多信息 WorkMail，請參閱 Amazon 用戶指南中的將 Microsoft Outlook Connect 到您的 Amazon WorkMail 帳 WorkMail 戶。

Amazon WorkMail 和 Microsoft 交易所的互操作

Amazon WorkMail 和 Microsoft Exchange 服務器之間的互操作性允許您將郵箱遷移到 Amazon 或將 Amazon 用於企業郵箱的子集時 WorkMail，將 WorkMail 對用戶的干擾降到最低。

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，您的使用者就可以透過雙向共用行事曆空閒/忙碌狀態資訊來排定會議。

必要條件

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

- 請確定您至少有一個使用者啟用 Amazon WorkMail 這是設定 Microsoft Exchange 的可用性設定所需的。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認證。如需詳細資訊，請參閱建立 AD Connector 並將 Amazon WorkMail 與現場部署目錄整合。
- 設置您的 Amazon WorkMail 組織。建立使用您設定的 AD Connector 的 Amazon WorkMail 組織。
- 將您的公司網域新增至您的 Amazon WorkMail 組織，然後在 Amazon WorkMail 主控台中進行驗證。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。
- 將信箱遷移到 Amazon WorkMail。讓使用者能夠從現場部署環境佈建和遷移信箱到 Amazon WorkMail。如需詳細資訊，請參閱啟用現有使用者並參閱遷移到 Amazon WorkMail。

> **Note**
>
> 不要更新 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 交易所網絡服務（EWS）網址發出 HTTPS 請求，以獲取日曆空閒/忙碌信息。

對於基於 EWS 的可用性提供商，Amazon WorkMail 向 Microsoft Exchange 上的交換網絡服務（EWS）URL 發出 HTTPS 請求，以獲取日曆空閒/忙碌信息。因此，下列先決條件僅適用於以 EWS 為基礎的可用性提供者。

- 確定相關的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。
- 只有當您的 Microsoft Exchange 環境中有一個有效的憑證授權單位 (CA) 簽署的憑證時，Amazon 才 WorkMail 能成功地向 Microsoft Exchange 上的 EWS URL 發出 HTTPS 請求。如需詳細資訊，請參閱在 Microsoft Exchange 文件網站上建立憑證授權單位的憑證要求。
- 您必須在 Microsoft 交易所中啟用 EWS 的基本驗證。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

將您的公司網域新增至 Amazon，以 WorkMail 便在電子郵件地址中使用這些網域。確保已驗證新增至 Amazon WorkMail 的網域，然後讓使用者和群組在 Amazon 上佈建信箱 WorkMail。在互操作性模式下，Amazon 無法啟用資源，應 WorkMail 在停用互通性模式 WorkMail 後在 Amazon 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。來自 Microsoft Exchange 的資源始終顯示在 Amazon 的用戶選項卡中 WorkMail。

- 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 交換互操作性，請不要更新 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，可以使用公有 API 建立啟用互通性模式的新 WorkMail 組織。

如果您已經有一個 Amazon WorkMail 組織的 AD 連接器連接到活動目錄，並且您也有 Microsoft 交換，請聯繫 AWS Support 以獲取有關啟用現有 Amazon WorkMail 組織 Microsoft Exchange 互操作性的協助。

在 Microsoft 交易所和 Amazon 創建服務帳戶 WorkMail

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

若要存取行事曆空閒/忙碌資訊，請在 Microsoft Exchange 和 Amazon 上建立服務帳戶。WorkMailMicrosoft 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，Amazon WorkMail 服務帳戶是 Amazon 上的任何用戶，可以訪問其他 Amazon WorkMail WorkMail 用戶的日曆空閒/忙碌信息。這也是預設為授予。您必須在現場部署目錄中建立 Amazon WorkMail 使用者，然後為 Amazon 啟用該使用者 WorkMail，才能將 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 系統管理中心來管理所有使用者、群組和資源。若要啟用 Amazon 使用 WorkMail 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 啟用使用者或群組時 WorkMail，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 系統管理中心進行設定。Amazon 每四個小時 WorkMail 會同步處理您目錄中的變更。

處於互通性模式 WorkMail 時，無法在 Amazon 中建立或啟用資源。但是，您所有的 Exchange 資源都可以在 Amazon 通 WorkMail 訊錄中使用，並且可以像往常一樣用於排程會議。

在 Amazon 上設定可用性設定 WorkMail

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

- 交換網路服務 (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 端點才能透過公用網際網路存取。
- 自訂可用性供應商 (CAP) — 在此組態中，管理員可以設定 AWS Lambda 函數，以取得指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，將 CAP 與 Amazon 搭配使用可 WorkMail 提供以下優點：
  - 從內部 EWS 取得使用者可用性，無需為其開啟防火牆。 WorkMail
  - 從非交換或非 EWS 系統取得使用者可用性，例如 Google 工作區 (舊稱為 G Suite)。

主題

設定以 EWS 為基礎的可用性提供者

若要在主控台上設定以 EWS 為基礎的可用性設定，請完成下列程序：

1. 在以下位置打開 Amazon WorkMail 控制台 https://console.aws.amazon.com/workmail/。

   如有必要請變更 AWS 區域。若要這麼做，請開啟位於搜尋方塊右側的 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，然後選擇組織的名稱。
3. 在瀏覽窗格中，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 網址 — Amazon WorkMail 將向 EWS 端點查詢此 URL。請參閱本指南的〈取得 EWS URL〉一節。
   - 使用者電子郵件地址 — WorkMail 將用來向 EWS 端點進行驗證的使用者電子郵件地址。
   - 密碼 — WorkMail 將用於向 EWS 端點進行驗證的密碼。
5. 選擇儲存。

取得 EWS 網址

若要使用 Microsoft Outlook 取得交換的 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. 選擇測試電子郵件 AutoConfiguration。
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。

若要使用取得 EWS URL 以進行交換 PowerShell，請在 PowerShell 提示下執行下列命令：

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

要獲取 Amazon 的 EWS 網址 WorkMail，首先，在 Amazon WorkMail 端點和配額下找到 EWS 域。輸入 EWS 網址 — `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. 在以下位置打開 Amazon WorkMail 控制台 https://console.aws.amazon.com/workmail/。

   如有必要請變更 AWS 區域。若要這麼做，請開啟位於搜尋方塊右側的 「選取地區」清單，然後選擇所需的「區域」。

2. 在瀏覽窗格中，選擇 [組 Organ izations]，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 [上限 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 函數的 ARN。

若要建置 CAP Lambda 函數，請參閱建立自訂可用性供應商 Lambda 函數。

建立自訂可用性供應商 Lambda 函數

自訂可用性提供者 (CAP) 是以 JSON 為基礎的要求和回應通訊協定配置，該要求和回應通訊協定是以明確定義的 JSON 結構定義。Lambda 函數將解析請求並提供有效的響應。

主題

- 請求和響應元素
- 授與 存取權
- WorkMail 使用 CAP Lambda 函數的 Amazon 示例

請求和響應元素

請求元素

以下是用於為 Amazon 使用 WorkMail 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"
    }
}
```

要求由三個區段組成：要求者、信箱和視窗。本指南的以下要求者、信箱和視窗各節將對這些內容進行了說明。

要求者

請求者部分提供有關向 Amazon WorkMail 發出原始請求的使用者的資訊。CAP 會使用此資訊來變更提供者的行為。例如，此資料可用於在後端可用性提供者上模擬相同的使用者，或者可以從回應中省略某些詳細資料。

欄位	描述	必要
Email	請求者的主要電子郵件地址。	是
Username	請求者的使用者名稱。	是
Organization	請求者的組織識別碼。	是
UserID	請求者識別碼。	是
Origin	要求的遠端位址。	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的電子郵件地址清單 (逗號分隔)。

視窗

視窗段落包含要求使用狀態資訊的時間範圍。startDate和endDate均以世界標準時間指定，並根據 RFC 33 39 進行格式化。事件預期不會被截斷。換句話說，如果事件在定義之前開始StartDate，則會使用原始開始。

回應元素

Amazon WorkMail 將等待 25 秒，以獲得來自 CAP Lambda 函數的響應。25 秒後，Amazon WorkMail 會假設該功能已失敗，並在 EWS GetUserAvailability 回應中為相關聯的信箱產生故障。這不會導致整個 GetUserAvailability 操作失敗。

以下是本節開頭所定義之組態的範例回應：

```
{
    "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"
    }]
}
```

回應是由包含信箱清單的單一信箱區段所組成。成功取得可用性的每個信箱都是由三個區段組成：信箱、事件和工作區。如果可用性提供者無法取得信箱的可用性資訊，則此區段包含兩個區段：信箱和錯誤。本指南的下列信箱、、、事件工作時間時區、工作期和錯誤各節將對這些內容進行了說明。

信箱

信箱區段是在要求的信箱區段中找到的使用者的電子郵件地址。

事件

「事件」部分是發生在請求窗口中的事件列表。每個事件都使用下列參數定義：

欄位	描述	必要
`startTime`	以世界標準時間為單位的事件開始時間，並根據 RFC 33 39 進行格式化。	是
`endTime`	以世界標準時間為單位的事件結束時間，並根據 RFC 33 39 進行格式化。	是
`busyType`	事件的忙碌類型。可以是 `Busy`、`Free` 或 `Tentative`。	是
`details`	活動的詳細信息。	否

欄位	描述	必要
details.subject	事件的主旨。	是
details.location	事件的地點。	是
details.instanceType	事件的執行個體類型。可以是 Single_Instance 、Recurring_Instance 或 Exception 。	是
details.isMeeting	一個布爾值，用於指示事件是否有與會者。	是
details.isReminderSet	布林值，指示事件是否已設定提醒。	是
details.isPrivate	布爾值，用於指示事件是否設置為私有。	是

工作時間

WorkHours 區段包含信箱擁有者工作時數的相關資訊。它包含兩個部分：時區和工作週期。

時區

時區子區段說明信箱擁有者的時區。當請求者在不同的時區工作時，正確顯示使用者的工作時間是很重要的。可用性提供者需要明確描述時區，而不是使用名稱。使用標準化的時區說明有助於避免時區不匹配。

欄位	描述	必要
name	時區的名稱。	是
bias	從 GMT 的預設偏移量 (以分鐘為單位)。	是
standardTime	指定時區的標準時間開始。	否

欄位	描述	必要
daylightTime	指定時區的夏令時開始。	否

您必須同時定義standardTime和daylightTime，或同時忽略兩者。standardTime和daylightTime物件中的欄位包括：

欄位	描述	允許值
offset	相對於預設偏移量的偏移量 (以分鐘為單位)。	NA
time	標準時間與日光節約時間之間轉換的時間，指定為hh:mm:ss。	NA
month	標準時間和夏令時間之間的轉換發生的月份。	JAN,FEB, MAR, APR, JUN, JUL, AUG, SEP, OCT, NOV, DEC
week	標準時間和夏令時間之間的轉換發生的指定月份內的一周。	FIRST, SECOND, THIRD, FOURTH, LAST
dayOfWeek	標準時間和夏令時間之間的轉換發生的指定週內的日期。	SUN, MON, TUE, WED, THU, FRI, SAT

工作期

「工作期間」區段包含一或多個工作期間物件。每個期間定義一或多天的工作日的開始和結束時間。

欄位	描述	允許值
startMinutes	從午夜開始工作日的幾分鐘。	NA
endMinutes	工作日從午夜幾分鐘結束。	NA
days	此期間適用的日期。	SUN, MON, TUE, WED, THU, FRI, SAT

錯誤

錯誤欄位可以包含任意錯誤訊息。下表列出眾所周知的代碼與 EWS 錯誤代碼的映射。所有其他訊息都會對應至ERROR_FREE_BUSY_GENERATION_FAILED。

值	EWS 錯誤代碼	
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 (AWS CLI) 執行下列 Lambda 命令。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
```

在指令中，在指示的位置新增下列參數：

- *#####* — 部署 CAP Lambda 所在地區的名稱。例如 `us-east-1`。
- *####-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 組織叫用 Lambda 函數的區域名稱。

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

- 帳戶 *ID – ######*別碼。
- 組*# ID – ## CAP L* ambda 的組織識別碼。例如，組織識別碼：公司識別碼：

> **Note**
>
> 只有在需要跨*######LAMBDA ### WM_REGION* 才會有所不同。如果沒有必要跨區域呼叫，它們將是相同的。

WorkMail 使用 CAP Lambda 函數的 Amazon 示例

如需 WorkMail 使用 CAP Lambda 函數查詢 EWS 端點的 Amazon 範例，請參閱 Amazon WorkMail GitHub 儲存庫無伺服器應用程式上的此AWS範例應用程式。

在 Microsoft Exchange 設定可用性設定

若要將啟用使用者的所有行事曆空閒/忙碌資訊請求重新導向至 Amazon WorkMail，請在 Microsoft Exchange 中設定可用性位址空間。

使用下列 PowerShell 命令建立位址空間：

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

在提示符下，輸入 Amazon WorkMail 服務帳戶的憑據。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 交易所和 Amazon 創建服務帳戶 WorkMail。

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

如需詳細資訊，請參閱新增 Microsoft 文件。AvailabilityAddressSpace

啟用 Microsoft 交換和 Amazon WorkMail 用戶之間的電子郵件

通過 Microsoft Exchange 服務器和 Amazon 之間的電子郵件路由 WorkMail，用戶可以在遷移到 Amazon 後保留其現有的電子郵件地址 WorkMail。電子郵件路由可讓您將 Microsoft Exchange 伺服器保留為組織內送電子郵件的主要簡易郵件傳送通訊協定 (SMTP) 伺服器。

使用電子郵件路由之前，您必須先完成下列先決條件：

- 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。
- 確保您在 Amazon WorkMail 主控台中看到您的網域。
- 驗證我們的 Microsoft Exchange 服務器可以發送電子郵件到互聯網。您可能需要設定傳送連接器。如需傳送連接器的相關資訊，請參閱 Microsoft 說明文件中的在 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，然後再將任何變更套用至組織。

1. 啟用您要遷移到 Amazon 的用戶帳戶 WorkMail。如需詳細資訊，請參閱啟用現有的使用者。
2. 在 Amazon 主 WorkMail 控台中，確保至少有兩個電子郵件地址與啟用的使用者相關聯。
   - <###### @### .awsapps.com>（這是自動添加的，並且可以用於測試沒有您的 Microsoft 交易所。）
   - <###### @ ### .com>（這是自動添加的，並且是主要的 Microsoft 交換地址。）

     如需詳細資訊，請參閱編輯使用者電子郵件地址。

3. 請務必將所有資料從 Microsoft Exchange 中的信箱遷移到 Amazon 中的信箱 WorkMail。如需詳細資訊，請參閱移轉至 Amazon WorkMail。
4. 遷移所有資料之後，請在 Microsoft Exchange 上停用該使用者的信箱。然後，建立具有外部 SMTP 地址指向 Amazon WorkMail 的郵件使用者 (或擁有郵件功能的使用者)。若要這麼做，請在 Exchange 管理命令介面中使用下列命令：

   > **Important**
   >
   > 下列步驟會清除信箱的內容。在嘗試啟用電子郵件路由 WorkMail 之前，請確保您的資料已遷移到 Amazon。執行此命令 WorkMail 時，有些郵件用戶端無縫切換至 Amazon。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
   ```

   在上面的命令中，組###代表您的 Amazon WorkMail 組織的名稱。如需詳細資訊，請參閱停用信箱和啟用 Microsoft 上的郵件使用者 TechNet。
5. 傳送測試電子郵件給使用者 (在上面的範例中**workmailuser@yourdomain.com**)。如果已正確啟用電子郵件路由，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 交換互操作性，DNS 記錄不應更新以指向 Amazon， WorkMail 直到以後。

文章設定組態

上述步驟將用戶郵箱從 Microsoft Exchange 服務器移動到 Amazon WorkMail，同時保持用戶在 Microsoft Exchange 作為聯繫人。由於已遷移的使用者現在是外部郵件使用者，因此 Microsoft Exchange 伺服器會強制執行其他條件約束。也可能需要其他組態需求才能完成移轉。

- 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 上的傳遞管理 TechNet。
- 使用者可能無法預訂資源。若要啟用此功能，您必須設定`ProcessExternalMeetingMessages`使用者需要存取的所有資源。如需詳細資訊，請參閱CalendarProcessing在 Microsoft 上設定 TechNet。

郵件使用者組態

有些郵件客戶端不能無縫切換到 Amazon WorkMail。這些用戶端會要求使用者執行其他設定步驟。不同郵件用戶端需要採取不同的動作。

- Microsoft 展望視窗 — 需要重新啟動展望. 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，重新配置 Microsoft 交換郵箱。
- Microsoft 展望在 MacOS 上 — 當展望重新啟動時，它會提示以下消息:展望被重定向到服務*#####*. awsapps.com. 您希望此伺服器配置您的設定嗎？ 接受建議。
- iOS 上的郵件 — 郵件應用程序停止接收電子郵件，並生成無法收到郵件錯誤。重新建立並重新設定 Microsoft 交換信箱。

停用互通性模式並停用郵件伺服器

在您設定適用於 Amazon 的 Microsoft Exchange 信箱之後 WorkMail，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，停用互通性模式並不會影響您的任何設定。

> **Warning**
>
> 停用互通性模式之前，請確定您已完成所有必要步驟。不這樣做可能會導致退回的電子郵件或意外行為。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。

若要停用互通性模式支援

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，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，未啟用 Amazon 的使用者和群組 WorkMail 會從通訊錄中移除。您仍然可以使用 Amazon WorkMail 主控台啟用任何遺失的使用者或群組，並將這些使用者或群組新增至通訊錄。在您完成下列步驟之前，無法啟用 Microsoft Exchange 的資源，也不會顯示在通訊錄中。

- 在 Amazon 中建立資源 WorkMail — 您可以在 Amazon 中建立資源， WorkMail 然後為這些資源設定委派和預約選項。如需詳細資訊，請參閱使用資源。
- 建立 AutoDiscover DNS 記錄 — 設定組織中所有郵件網域的 AutoDiscover DNS 記錄。這使用戶能夠從他們的 Microsoft Outlook 和移動客戶端連接到他們的 Amazon WorkMail 郵箱。如需詳細資訊，請參閱用 AutoDiscover 來設定端點。
- 將您的 MX DNS 記錄切換到 Amazon WorkMail — 若要將所有傳入的電子郵件傳送到 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。
- 取消委任您的郵件伺服器 — 驗證所有電子郵件都直接路由到 Amazon 之後 WorkMail，如果您不打算繼續使用郵件伺服器，則可以取消委任郵件伺服器。

故障診斷

下面列出了最常遇到的 Amazon WorkMail 互操作性和遷移錯誤的解決方案。

交換網路服務 (EWS) URL 無效或無法連線 — 檢查您擁有正確的 EWS URL。如需詳細資訊，請參閱在 Amazon 上設定可用性設定 WorkMail。

EWS 驗證期間的連線失敗 — 這是一般錯誤，可能由下列原因造成：

- Microsoft 交換中沒有互聯網連接。
- 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，可能由下列原因造成：

- 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 附件的電子郵件 — 當加密的 S/MIME 電子郵件從交換傳送到 Amazon，WorkMail並在 Mac 版或 IMAP 用戶端的 Outlook 2016 中接收時，可能會發生這種情況。解決方案是在 Exchange 管理命令介面中執行下列命令。

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

Amazon WorkMail 可供企業客戶和小型企業主使用。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，有些是無法變更的硬配額。如需有關要求增加配額的詳細資AWS訊，請參閱 Amazon Web Services 一般參考.

Amazon WorkMail 組織和使用者配額

您最多可以將 25 個使用者新增至您的 Amazon WorkMail 組織，享受 30 天的免費試用期。在此期限結束後，除非您將其移除或關閉 Amazon WorkMail 帳戶，否則我們會向您收取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**
>
> 要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
Amazon WorkMail 組織每個 AWS帳戶	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配額和要求增加。如需詳細資訊，請參閱《AWS 一般參考》中的服務配額。
Amazon WorkMail 組織的用戶	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 1000 萬用戶 • 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，由託管AWS Directory Service：最多 1000 萬用戶，具體取決於您的設置和配置， * 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。

資源	預設配額	變更請求上限
每個AWS帳戶每天所收到的收件者	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。但是，Amazon WorkMail 是一種商業電子郵件服務，不打算用於批量電子郵件服務。如需大量電子郵件服務，請參閱 Amazon SES 或 Amazon Pinpoint.
每個AWS帳戶每天使用任何測試網域所收到的收件者	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 組織的域數	1,000 這是一個硬配額，無法更改。
每個電子郵件流程規則中的寄件者模式數量	250 這是一個硬配額，無法更改。
每個組織的電子郵件流量規則中的寄件者模式數量	1,000 這是一個硬配額，無法更改。

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 這是一個硬配額，無法更改。	不適用
每個使用者的別名上限數量	100 這是一個硬配額，無法更改。	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。但是，Amazon WorkMail 是一種商業電子郵件服務，不打算用於批量電子郵件服務。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。 郵件會以 MIME 格式接收。內送 MIME 郵件的大小上限為 40 MB。 這是一個硬配額，無法更改。
外寄訊息的大小上限	29 MB 的未編碼資料。 郵件會以 MIME 格式傳送。外寄 MIME 郵件的大小上限為 40 MB。 這是一個硬配額，無法更改。
每則訊息的最高收件人數量	500

資源	預設配額
	這是一個硬配額，無法更改。
每封郵件的附件數目上限	500 這是一個硬配額，無法更改。

使用組織

在 Amazon 中 WorkMail，您的組織代表公司中的使用者。在 Amazon 主 WorkMail 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，則必須創建一個組織才能使用 Amazon WorkMail。

主題

建立組織

要使用 Amazon WorkMail，您必須首先創建一個組織。一個AWS帳戶可以有多個 Amazon WorkMail 組織。建立組織時，您也可以選取組織的網域，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，或將 Amazon WorkMail 與現有目錄整合。您可以使用 Amazon WorkMail 與現場部署 Microsoft 活動目錄，AWS管理活動目錄，或 Simple AD。透過與現場部署目錄整合，您可以使用 Amazon WorkMail 中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，則必須先在中設定 AD Connector AWS Directory Service。AD Connector 會將您的使用者和群組與 Amazon 通 WorkMail 訊錄同步，並執行使用者身份驗證請求。如需詳細資訊，請參閱《AWS Directory Service管理指南》中的使用中目錄連接器。

您也可以選擇 Amazon WorkMail 用來加密信箱內容的選項。 AWS KMS key您可以選取 Amazon 的預設AWS受管主金鑰 WorkMail，或使用 AWS Key Management Service (AWS KMS) 中的現有 KMS 金鑰。如需建立新 KMS 金鑰的詳細資訊，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，請記住以下事項：

- Amazon 目前 WorkMail 不支持您與多個帳戶共享的託管 Microsoft 活動目錄服務。
- 如果您有內部部署作用中目錄與 Microsoft Exchange 和 AD Connector，我們建議您設定組織的互通性設定。這可讓您在將信箱遷移到 Amazon 時，將使用者的干擾降到最低 WorkMail，或將 Amazon 用 WorkMail 於企業信箱的子集。如需詳細資訊，請參閱 Amazon WorkMail 和 Microsoft 交易所的互操作。
- 如果您選擇免費測試網域選項，則可以開始使用提供的測試網域的 Amazon WorkMail 組織。測試網域會使用這種格式：## .awsapps.com。只要您在 Amazon WorkMail 組織中維護已啟用的使用者，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，則測試網域可供其他客戶註冊和使用。
- Amazon WorkMail 不支持多區域目錄。

主題

建立組織

在 Amazon WorkMail 控制台中創建一個新的組織。

建立組織

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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」。

   「Organ izations」頁面隨即出現，並顯示您的組織 (如果有)。
3. 選擇 [建立組織]。
4. 在 [電子郵件網域] 底下，選取要用於組織中電子郵件地址的網域：

   - 現有的路由 53 網域 — 選取您使用 Amazon Route 53 (路線 53) 託管區域管理的現有網域。

- 新的路線 53 網域 — 註冊一個新的 Route 53 網域名稱，以便與 Amazon 搭配使用 WorkMail。
- 外部網域 — 輸入您使用外部網域名稱系統 (DNS) 提供者管理的現有網域。
- 免費測試域 — 使用 Amazon 提供的免費測試域 WorkMail。您可以 WorkMail 使用測試網域探索 Amazon，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 進行管理，對於 Route 53 託管區域，請選取您的路線 53 網域。
6. 在「別名」中，輸入組織的唯一別名。
7. 選擇 [進階設定]，並針對 [使用者目錄] 選取下列其中一個選項：
   - 建立新的 Amazon WorkMail 目錄 — 建立用於新增和管理使用者的新目錄。
   - 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受管理的使用中目錄或 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 — 在您的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) 記錄新增至您的 DNS 服務，以進行驗證。TXT 記錄可讓您輸入有關 DNS 服務的備註。MX 記錄會指定內送郵件伺服器。

請務必將您的網域設定為組織的預設網域。如需詳細資訊，請參閱 驗證網域 及 選擇預設網域。

當您的組織處於使用中狀態時，您可以在其中新增使用者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 的電子郵件用戶端 WorkMail。

檢視組織的詳細資訊

您的每個 Amazon 組 WorkMail 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，包括您可以搭配使用的 ID AWS Command Line Interface。頁面上的訊息也會顯示完成設定和組織所需的任何步驟，例如未驗證的網域或缺少使用者。這些訊息也會提供您設定指定電子郵件用戶端所遵循的第一個步驟。

若要檢視組織明細

1. 在導覽列中，選擇「組織」。

「Organ izations」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 Amazon WorkDocs 或 WorkSpaces 目錄

若要將 Amazon WorkMail 與 Amazon 搭配使用 WorkSpaces， WorkDocs 或使用以下步驟建立相容的目錄。

添加兼容的 Amazon WorkDocs 或 WorkSpaces 目錄

1. 使用 Amazon WorkDocs 或創建一個兼容的目錄 WorkSpaces。
   a. 如需 Amazon WorkDocs 指示，請參閱 Amazon WorkDocs 管理指南中的快速入門。
   b. 如需 WorkSpaces 指示，請參閱 Amazon WorkSpaces 管理指南中的開始使用 Amazon WorkSpaces 快速設定。
2. 在 Amazon 主 WorkMail 控台中，建立您的 Amazon WorkMail 組織，然後選擇使用現有的目錄。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 用 WorkMail 於組織的電子郵件，則可以從 Amazon 刪除組織 WorkMail。

> **Note**
>
> 此作業無法復原。刪除組織之後，您將無法復原信箱資料。

若要刪除組織

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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 Organ izations」畫面的組織清單中，選取要刪除的組織，然後選擇「刪除」。
3. 在 [刪除組織] 中，選擇要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 提供自己的目錄 WorkMail，我們將為您創建一個目錄。如果您在刪除組織時保留此現有目錄，則除非 Amazon、Amazon 或正在使用該目錄 WorkMail，否則將向您收取費用 WorkSpaces。 WorkDocs如需定價資訊，請參閱其他目錄類型定價。
> 為了刪除目錄，它不能啟用任何其他AWS應用程序。如需詳細資訊，請參閱《AWS Directory Service管理指南》中的刪除 S imple AD 目錄或刪除 AD 連接器目錄。

嘗試刪除組織時，您可能會收到無效的 Amazon 簡易電子郵件服務 (Amazon SES) 規則集錯誤訊息。如果收到此錯誤訊息，請在 Amazon SES 主控台中編輯 Amazon SES 規則，並移除無效的規則集。您編輯的規則應該在規則名稱中包含您的 Amazon WorkMail 組織 ID。如需有關編輯 Amazon SES 規則的詳細資訊，請參閱 Amazon 簡易電子郵件服務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。此時會顯示規則集的錯誤訊息。

尋找電子郵件地址

您可以根據使用者、資源或群組，找出您的組織中是否使用了電子郵件地址。

尋找電子郵件地址

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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 Organ izations」，然後選擇組織的名稱。
3. 在 [組織] 頁面中，選擇 [尋找電郵地址]。
4. 選擇 Search (搜尋)。

使用組織設定

以下各節說明如何使用適用於 Amazon WorkMail 組織的設定。您選擇的設定將套用至整個組織。

主題

- 啟用信箱遷移
- 啟用日誌記錄
- 啟用互通性
- 啟用 SMTP 閘道
- 管理電子郵件流程
- 對內送電子郵件強制執行 DMARC 政策

啟用信箱遷移

當您想要將信箱從來源（例如 Microsoft Exchange 或 G Suite 基本版）傳輸到 Amazon 時，可以啟用信箱遷移 WorkMail。您可以在較大的移轉程序中啟用移轉。如需詳細資訊，包括操作步驟，請參閱本指南的「入門」一節遷移到 Amazon WorkMail中的。

啟用日誌記錄

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協力廠商封存和 eDiscovery 工具。日誌記錄有助於確保您符合資料儲存、隱私權保護和資訊保護方面的法規遵循法規。

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

啟用互通性

互通性可讓您從 Microsoft Exchange 遷移，並將 Amazon 用 WorkMail 作企業信箱的子集。如需詳細資訊，包括操作步驟，請參閱本指南的「入門」一節在 Amazon 上設定可用性設定 WorkMail中的。

啟用 SMTP 閘道

您可以啟用簡易郵件傳送通訊協定 (SMTP) 閘道以搭配輸出電子郵件流程規則使用。輸出電子郵件流程規則可讓您透過 SMTP 閘道路由傳送從 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**
>
> 針對輸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傳輸層安全性 (TLS) v1.2。僅支援基本身分驗證。

設定 SMTP 閘道

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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 Organ izations」，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 — 輸入唯一名稱。
   - 閘道位址 — 輸入閘道的主機名稱或 IP 位址。
   - 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 — 輸入強式密碼。
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 閘道與輸出電子郵件流程規則搭配使用時，輸出郵件會嘗試將該規則與 SMTP 閘道相符。符合規則的郵件會路由傳送至對應的 SMTP 閘道，接著會處理其餘的電子郵件傳遞。

如果 Amazon WorkMail 無法連接 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，請按照上述步驟更正閘道設定。

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的地址或網域對電子郵件採取一或多個動作。您可以對寄件者和收件者的電子郵件地址或網域使用電子郵件流程規則。

建立電子郵件流程規則時，您可以指定在符合指定的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。輸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，您可以使用具有AWS Lambda功能的規則，在內送電子郵件傳遞至使用者的信箱之前處理內送電子郵件。如需將 Lambda 搭配 Amazon 使用的詳細資訊 WorkMail，請參閱AWS

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

輸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	系統會忽略電子郵件訊息。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遞，而寄件者會收到退回郵件中未傳遞的通知。
傳遞到垃圾郵件資料夾	電子郵件會傳遞至使用者的垃圾郵件或垃圾郵件資料夾，即使 Amazon 垃圾郵件偵測系統最初未將其識別為垃圾郵 WorkMail 件。
預設	Amazon WorkMail 垃圾郵件偵測系統檢查後，會傳送電子郵件訊息。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至收件匣。 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	即使 Amazon 垃圾郵件偵測系統將電子郵件識別為垃圾郵件，電子郵件也一律會傳送到使用者的收 WorkMail 件匣。

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，以便在傳送至使用者的收件匣之前或之後進行處理。

Note

輸入電子郵件會先傳送至 Amazon SES，然後傳送至 Amazon WorkMail。如果 Amazon SES 封鎖傳入的電子郵件訊息，則不會套用規則動作。例如，Amazon SES 會在偵測到已知病毒或因為明確的 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

您可以使用輸出電子郵件流程規則，透過 SMTP 閘道引導電子郵件訊息，或封鎖寄件者傳送電子郵件給指定的收件者。如需 SMTP 閘道的詳細資訊，請參閱啟用 SMTP 閘道。

您也可以使用輸出電子郵件流程規則，將電子郵件訊息傳遞至電子郵件傳送後處理的AWS Lambda函數。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	電子郵件訊息會遭到捨棄。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	不會傳送電子郵件訊息，寄件者會收到系統管理員封鎖電子郵件訊息的訊息通知寄件者。
路由至 SMTP 閘道	電子郵件訊息是透過設定的 SMTP 閘道傳送。
執行 Lambda	在傳送電子郵件訊息之前或傳送期間，將電子郵件訊息傳遞至 Lambda 函數以進行處理。

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：

- 電子郵件地址與單一電子郵件地址相符；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
```

- 萬用字元網域會比對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。

如果輸入電子郵件訊息中的Sender或From標頭符合任何模式，則會套用輸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符合不同規則的收件者，則每個規則都會套用至符合的收件者。

如果收件者和輸出電子郵件中的Sender或From標頭符合任何模式，則會套用輸出電子郵件流程規則。如果電子郵件訊息有多個符合不同規則的收件者，則每個規則都會套用至符合的收件者。

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。意外的優先順序排序可能會導致許多輸入電子郵件訊息無法傳遞。

建立電郵流程規則

電子郵件流程規則會將規則動作套用至內送和外寄電子郵件。這些動作會在郵件符合指定的模式時套用。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. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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 Organ izations」，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。您可以在此頁面建立輸入或輸出規則。下列步驟說明如何建立這兩種類型。

若要建立輸入規則

1. 選擇入站規則選項卡，然後選擇創建。
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，有些則提供了解更多連結。

> **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 配置 WorkMail。

4. 在 [寄件者網域或地址] 底下，輸入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。

若要建立輸出規則

1. 選擇輸出規則索引標籤，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，有些則提供了解更多連結。

> **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 配置 WorkMail。

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何組合。
5. 在 [目的地網域或地址] 下，輸入任何有效目的地網域和電子郵件地址的組合。
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。

編輯電郵流程規則

每當您需要變更電子郵件訊息的一或多個規則動作時，都可以編輯電子郵件流程規則。本節中的步驟適用於內送和外寄電子郵件訊息。

編輯電子郵件流程規則

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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 Organ izations」，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. 選擇輸入規則或輸出規則索引標籤。
5. 選擇您要變更的規則旁邊的圓鈕，然後選擇 「編輯」。
6. 視需要變更規則中的一或多個動作，然後選擇「儲存」。

AWS Lambda為 Amazon 配置 WorkMail

在輸入和輸出電子郵件流程規則中使用「執行 Lambda」動作，將符合規則的電子郵件訊息傳遞至 AWS Lambda函數以進行處理。

請從下列組態中進行選擇，以便在 Amazon 中執行 Lambda 動作 WorkMail。

同步執行 Lambda 組態

符合流程規則的電子郵件訊息會傳送至 Lambda 函數進行處理，然後再傳送或傳送。使用此設定可修改電子郵件內容。您也可以針對不同的使用案例控制輸入或輸出電子郵件流程。例如，傳遞至 Lambda 函數的規則可以封鎖敏感電子郵件訊息的傳遞、移除附件或新增免責聲明。

非同步執 Lambda 組態

符合流程規則的電子郵件訊息會傳送至 Lambda 函數，以便在傳送或交付時進行處理。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 函數的事件物件都包含輸入或輸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 AWS Lambda 擷取訊息內容。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 區域和AWS 帳戶所設定之 Amazon WorkMail 組織中的 Lambda 函數。

開始使AWS Lambda用 Amazon WorkMail

若要開AWS Lambda始使用 Amazon WorkMail，我們建議您將 WorkMail Hello World Lambda 函數從您的帳戶部署AWS Serverless Application Repository到您的帳戶。該功能具有所有必要的資源，以及為您配置的權限。有關更多示例，請參閱（詳見）的amazon-workmail-lambda-templates存儲庫 GitHub。

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

- `MY_FUNCTION_NAME`以 Lambda 函數的名稱取代。
- 替換`REGION`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))。
- 替換為您`AWS_ACCOUNT_ID`的 12 位數 AWS 帳戶 ID。
- 替換`WORKMAIL_ORGANIZATION_ID`為您的 Amazon WorkMail 組織 ID。您可以在組織的卡片上找到該組織的「組 Organ izations」頁面。

```
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 AWS CLI 的詳細資訊，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 L amb da」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，請參閱建立電郵流程規則。

若要完成同步規則的建立，請新增 Lambda Amazon 資源名稱 (ARN) 並設定下列選項。

Fallback action (備用動作)

如果 Lambda 函數無法運行，Amazon WorkMail 適用的操作。如果未設定所有收件者旗標，則此動作也適用於 Lambda 回應中省略的任何收件者。後援動作不能是另一個 Lambda 動作。

Rule timeout (規則逾時) (以分鐘為單位)

如果 Amazon WorkMail 無法調用 Lambda 函數，則重試該函數的期間。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*目標條件。

Lambda 事件資料

Lambda 函數會使用下列事件資料觸發。資料的呈現方式視 Lambda 函數所使用的程式設計語言而有所不同。

```
{
    "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

的版本號碼LambdaEventData。這只會在您在中進行向後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 沒有區分收件人，抄送或密件抄送。

> **Note**
>
> 對於輸入電子郵件流程規則，此清單包括您在其中建立規則之 Amazon WorkMail 組織中所有網域中的收件者。Lambda 函數會針對來自寄件者的每個 SMTP 交談個別叫用，而收件者欄位會列出來自該 SMTP 交談的收件者。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 訊息流程開發套件時，用來存取電子郵件訊息完整內容的唯一 ID。

叫用識別碼

唯一 Lambda 叫用的識別碼。當 Lambda 函數被多次呼叫相同時，此 ID 會保持不變LambdaEventData。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 回應架構

當具有同步執行 Lambda 動作的電子郵件流程規則與輸入或輸出電子郵件訊息相符時，Amazon 會 WorkMail 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，該結構描述會列出適用動作的動作、動作類型、適用參數和收件者。

下列範例顯示同步執行 Lambda 回應。回應會根據 Lambda 函數所使用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。非同步執行 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 BOUN CE 動作類型做為 JSON 物件，且具有鍵值訊息和值字串。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**
>
> 針對輸入電子郵件呼叫 Lambda 動作時，您只能新增來自組織的新收件者。新收件人會以 BCC (密件副本) 的形式新增至回應中。

allRecipients

當為 true 時，會將動作套用至不受 Lambda 回應中其他特定動作約束的所有收件者。

同步執行 Lambda 動作限制

當 Amazon 為同步執行 Lambda 動作 WorkMail 叫用 Lambda 函數時，會套用下列限制：

- Lambda 函數必須在 15 秒內回應，或被視為失敗的叫用。

> **Note**
>
> 系統會根據您指定的「規則」逾時間隔重試呼叫。

- 允許最大 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。
- 輸出 Lambda 函數最多允許 500 個收件者使用。
- Rule timeout (規則逾時) 的最大值為 240 分鐘。如果設定的最小值為 0，則在 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 因為錯誤、無效回應或 Lambda 逾時而無法叫用 Lambda 函數，Amazon 會 WorkMail 以指數輪詢 WorkMail 重試呼叫，從而降低處理速率，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。

範例同步執行 Lambda 回應

下列範例示範常見同步執行 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者的同步執行 Lambda 回應的結構。

```
{
    "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

下列範例示範使用自訂電子郵件訊息彈回的同步執行 Lambda 回應的結構。

```
{
    "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者新增至電子郵件訊息的同步執行 Lambda 回應的結構。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
      }
    ]
}
```

如需建立 Lambda 函數以執行 Lambda 動作時使用的更多程式碼範例，請參閱 Amazon WorkMail Lambda 範本。

有關在 Amazon 上使用 Lambda 的更多 WorkMail

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 AWS Lambda 擷取訊息內容。

使用 AWS Lambda 擷取訊息內容

設定管理 Amazon 電子郵件流程的AWS Lambda函數後 WorkMail，您可以存取使用 Lambda 處理的電子郵件訊息的完整內容。如需開始使用適用於 Amazon 的 Lambda 的詳細資訊 WorkMail，請參閱AWS Lambda為 Amazon 配置 WorkMail。

若要存取電子郵件的完整內容，請使用 Amazon WorkMail 訊息流程 API 中的`GetRawMessageContent`動作。呼叫時傳遞至 Lambda 函數的電子郵件訊息 ID 會傳送要求至 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 參考資料中的 Amazon 訊 WorkMail 息流程。

下列範例顯示使用 Python 執行階段環境的 Lambda 函數如何擷取完整的訊息內容。

> **Tip**
>
> 如果您先從帳戶部署 Amazon WorkMail Hello World Lambda 函數，系統會在您的帳戶中建立具有所有必要資源和許可的 Lambda 函數。AWS Serverless Application Repository然後，您可以根據您的用例將業務邏輯添加到 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)
```

有關分析傳輸中郵件內容的方法的更多詳細示例，請參閱（amazon-workmail-lambda-templates詳見） GitHub。

> **Note**
>
> 您只能使用 Amazon WorkMail 訊息流程 API 存取傳輸中的電子郵件訊息。您只能在發送或接收後的 24 小時內訪問消息。若要以程式設計方式存取使用者信箱中的訊息，請使用 Amazon 支援的其他協定之一 WorkMail，例如 IMAP 或交換網路服務 (EWS)。

使用 AWS Lambda 更新訊息內容

設定同步AWS Lambda功能以管理電子郵件流程後，您可以使用 Amazon M WorkMail essage 流程 API 中的`PutRawMessageContent`動作來更新傳輸中電子郵件訊息的內容。如需開始使用 Amazon Lambda 函數的詳細資訊 WorkMail，請參閱設定同步執行 Lambda 規則。如需 API (匯入 API) 的詳細資訊，請參閱「 PutRawMessageContent」。

> **Note**
>
> 該 PutRawMessageContent API 需要 boto3 1.17.8，或者您可以在 Lambda 函數中添加一個圖層。要下載正確的 boto3 版本，請參閱上的 boto 頁面。 GitHub如需有關新增圖層的詳細資訊，請參閱設定使用圖層的函數。
> 這是一個示例層：`"LayerArn":"arn:aws:lambda:${AWS::Region}:489970191081:layer:WorkMailLambdaLayer:2"`。在此範例中，請以適當`${AWS::Region}`的 AWS 區域取代，例如 us-east-1。

> **Tip**
>
> 如果您先將 Amazon WorkMail Hello World Lambda 函數從 AWS Serverless Application Repository 部署到您的帳戶，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，將商務邏輯新增至 lambda 函數。

當你去, 記住以下幾點:

- 使用 GetRawMessageContentAPI 擷取原始訊息內容。如需更多資訊，請參閱 使用 AWS Lambda 擷取訊息內容。

- 取得原始郵件後，請變更 MIME 內容。完成後，將訊息上傳到您帳戶中的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。確保 S3 儲存貯體使用與您的 Amazon WorkMail 操AWS 帳戶作相同，並且使用與您的 API 呼叫相同的 AWS 區域。
- WorkMail 若要讓 Amazon 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 PutRawMessageContentAPI 將更新的訊息內容傳送回 Amazon WorkMail。

> **Note**
>
> PutRawMessageContentAPI 可確保更新郵件的 MIME 內容符合 RFC 標準，與RawMessageContent資料類型中提到的準則一樣。傳入 Amazon WorkMail 組織的電子郵件並不總是符合這些標準，因此 PutRawMessageContent API 可能會拒絕這些標準。在這種情況下，您可以查閱返回的錯誤消息，以獲取有關如何修復任何問題的更多信息。

Example S3 政策範例

```
{
    "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 執行階段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="Your-S3-Bucket", Key=key)

        # Update the email in WorkMail
        s3_reference = {
            'bucket': "Your-S3-Bucket",
            'key': key
        }
        content = {
            's3Reference': s3_reference
        }
        workmail.put_raw_message_content(messageId=msg_id, content=content)
```

有關 GitHub分析傳輸中消息內容的方法的更多示例，請參閱（詳見）的 amazon-workmail-lambda-templates存儲庫。

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 訊息流程 API 可與單一資源類型 (傳輸中的電子郵件訊息) 搭配使用。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 — 適用於您 Amazon WorkMail 組織的 AWS 區域。
- 帳戶 — 您 Amazon WorkMail 組織的 AWS 帳戶 ID。
- 組織 — 您的 Amazon WorkMail 組織 ID。
- 前後關聯 — 指出訊息是傳送`incoming`給您的組織，還是傳送給您`outgoing`的組織。
- 訊息 ID — 作為輸入傳送至 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
```

您可以在 IAM 使用者政策的`Resource`部分使用這些 ARN 做為資源，以便管理傳輸中 Amazon WorkMail 訊息的存取。

Amazon WorkMail 訊息流程存取權管理政策範例

以下範例政策授予 IAM 實體對您中每個 Amazon WorkMail 組織的所有輸入和輸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，您也可以限制對一個或多個組織的存取。如果某些 Lambda 函數只應用於特定組織，則此功能非常有用。

```
{
    "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"
        }
    ]
}
```

下列範例政策授予 IAM 實體完整讀取和更新存取權限，以讀取和更新您的每個 Amazon WorkMail 組織的所有輸入和輸出訊息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. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，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. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，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

電子郵件網域使用網域名稱系統 (DNS) 記錄來確保安全性。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 記錄通常包括以網域為基礎的訊息驗證、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 記錄包括指定電子郵件未通過 DMARC 檢查時要採取的動作的策略。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。

根據預設，新的 Amazon WorkMail 組織已開啟 DMARC 強制功能。

若要開啟強制執行 DMARC 功能

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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 Organ izations」，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 標籤頁，然後選擇「編輯」。
5. 將 DMARC 強制滑桿移至開啟位置。
6. 選取 [我確認] 旁邊的核取方塊，開啟 DMARC 強制可能會導致根據寄件者的網域組態捨棄或隔離輸入電子郵件。
7. 選擇儲存。

若要關閉 DMARC 強制執行功能

- 請依照上一節中的步驟進行，但是將 DMARC 強制滑桿移至關閉位置。

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。若要檢查是否有未傳送給使用者的電子郵件，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追蹤 DMARC 強制執行之前，請先在 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 見解] 主控台的 [記錄] 下，選擇 [深入解析]
2. 對於選取日誌群組，請選取 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 組 WorkMail 織資源可讓您：

- 在 AWS Billing and Cost Management 主控台中區分組織。
- 透過將資源新增到 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 資 WorkMail 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，請參閱基於 Amazon WorkMail 標籤的授權。

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

若要新增標籤至 Amazon WorkMail 組織

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，然後選擇組織的名稱。
3. 選擇 Tags (標籤)。
4. 對於 Organization tags (組織標籤)，選擇 Add New Tag (新增標籤)。
5. 在「金鑰」中，輸入可識別標籤的名稱。
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 (AWS CLI) 標記組織。如需詳細資訊，請參閱 Amazon WorkMail API 參考或命`UntagResource`令參考中的`ListTagsForResource`、和AWS CLI命令。`TagResource`

您可以隨時使用 Amazon WorkMail 主控台從組織移除標籤。

若要從 Amazon WorkMail 組織移除標籤

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，然後選擇組織的名稱。
3. 選擇 Tags (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 的存取控制規則可 WorkMail 讓管理員控制其組織的使用者和模擬角色授與 Amazon 存取權的方式。 WorkMail每個 Amazon WorkMail 組織都有一個預設存取控制規則，無論使用者使用何種存取通訊協定或 IP 地址，都會授與新增至組織的所有使用者和模擬角色的信箱存取權。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 會 WorkMail 封鎖對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 [自動探索]、[EWS]、[IMAP]、[SMTP] ActiveSync、[視窗版 Outlook] 和 [網路郵件]。
- IP 位址 — 用來存取信箱的 IPv4 CIDR 範圍。
- Amazon 使用 WorkMail 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 Windows 版 Outlook 的存取權時，建議您同時啟用自動探索和 EWS 的存取權。
> - 存取控制規則不適用於 Amazon WorkMail 主控台或開發套件存取。請改用 AWS Identity and Access Management (IAM) 角色或政策。如需詳細資訊，請參閱 Amazon 的身份和訪問管理 WorkMail。

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. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，然後選擇組織的名稱。

3. 選擇 Access Control List (存取控制規則)。
4. 選擇 Create rule (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. 對於此規則適用於請求... 中，選取要套用至規則的條件，例如要包含或排除特定通訊協定、IP 位址或使用者，或是模擬角色。
8. (選擇性) 如果您輸入 IP 位址範圍、使用者或模擬角色，請選擇 [新增] 將其新增至規則。
9. 選擇 Create rule (建立規則)。

編輯存取控制規則

從 Amazon WorkMail 主控台編輯新的預設存取控制規則。

編輯存取控制規則

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，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才能遵循更新的規則。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。但是，當您測試規則時，您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

若要查看組織的存取控制規則的套用方式，請從 Amazon WorkMail 主控台測試規則。

測試組織的存取控制規則

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，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. 對於執行者的要求，請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 會 WorkMail 封鎖對組織信箱的所有存取。

刪除存取控制規則

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，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。保留原則會在您選擇的期間後，自動刪除使用者信箱中的電子郵件。您可以選擇要套用保留原則的信箱資料夾。此外，您也可以選擇是否要為不同的資料夾設定不同的保留原則。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原則。

設定信箱保留政策

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，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. 輸入在刪除電子郵件之前保留在每個信箱資料夾中的天數。
6. 選擇儲存。

請允許 48 小時為您的組織套用保留原則。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就無法復原。

保留政策保留項目的天數是根據項目的建立、修改或移動時間而定。例如，如果保留原則在一年後刪除項目，則政策會從您建立的日期或上次對該項目採取動作開始計算保留天數。它不會受到您實施保留原則的日期影響。

使用網域

您可以 WorkMail 將 Amazon 配置為使用自定義域。您也可以將網域設為組織的預設值，並 AutoDiscover 為 Microsoft Outlook 啟用。

主題

新增網域

您最多可以為您的 Amazon WorkMail 組織新增 100 個網域。當您新增網域時，Amazon SES Simple Email Service (Amazon SES) 傳送授權政策會自動新增至網域身分識別政策。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**
>
> 最佳做法是，您應該在所有網域中新增<##### @> 和<## @> 的別名。如果您希望組織中的特定使用者接收傳送至這些別名的郵件，您可以為這些別名建立通訊群組。

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更新這些記錄或遷移信箱之後，不會使用過期或無效的 MX 記錄。
- 建立使用者和通訊群組，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寄到 Amazon WorkMail。DNS 記錄的更新至多可能需要 48 小時來處理。

- 有些 DNS 提供者會自動將網域名稱附加到 DNS 記錄的末端。新增已包含網域名稱的記錄，例如，可能會導致網域名稱重複，進而導致系統產生。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 提供者表示該記錄名稱是完整的，而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，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網MAIL FROM域。若要 AutoDiscover 為 iOS 裝置啟用，您必須將網域設定為MAIL FROM網域。您可以在主控台的 [增強交付能力] 區段中查看MAIL FROM網域的狀態。如需詳細資訊，請參閱 設定自訂郵件寄件者網域。

新增網域

1. 登錄到AWS Management Console並打開 Amazon WorkMail 控制台 https://console.aws.amazon.com/workmail/.
2. 如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟 [選取地區] 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. 在瀏覽窗格中，選擇 [組織]，然後選擇您要新增網域的組織名稱。
4. 在功能窗格中，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文 (ASCII) 字元。

   > **Note**
   >
   > 如果您有在 Amazon Route 53 公共託管區域中管理的網域，則可以從輸入網域名稱時顯示的下拉式功能表中選擇該網域。

6. 選擇新增網域。

   會出現一個頁面，並列出新網域的 DNS 記錄。此頁面會將記錄群組為下列段落：

   - 網域擁有權
   - WorkMail 配置
   - 提高安全性
   - 改善電郵傳送

這些區段中的每一個都包含一或多個 DNS 記錄，而每筆記錄都會顯示「狀態」值。下列清單顯示記錄及其可用狀態值。

TXT 擁有權

已驗證 — 記錄已解決並驗證。

擱置中 — 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 WorkMail 組態設定

已驗證 — 記錄已解決並驗證。

遺失 — 無法解析記錄。

不一致 — 值與預期的記錄不符。

AutoDiscover

已驗證 — 記錄已解決並驗證。

遺失 — 無法解析記錄。

不一致 — 值與預期的記錄不符。

> **Note**
>
> AutoDiscover 驗證程序也會檢查 AutoDiscover 設定是否正確。此程序會驗證每個階段的組態設定。驗證完成後，「狀態」欄中的「已驗證」旁邊會出現綠色核取記號。您可以將游標暫留在「已驗證」上，然後查看程序驗證了哪些階段。若要取得有關 AutoDiscover 階段的更多資訊，請參閱啟用 AutoDiscover 以設定端點。

DKIM 名稱

已驗證 — 記錄已解決並驗證。

擱置中 — 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。

如需 DKIM 簽署的詳細資訊，請參閱 Amazon 簡單電子郵件服務開發人員指南中的 Amazon SES 使用 DKIM 驗證電子郵件。

文本文件

已驗證 — 記錄已解決並驗證。

遺失 — 無法解析記錄。

不一致 — 值與預期的記錄不符。

如需 SPF 驗證的詳細資訊，請參閱以 SPF 驗證您的電子郵件。

德馬克 TXT

已驗證 — 記錄已解決並驗證。

遺失 — 無法解析記錄。

不一致 — 值與預期的記錄不符

如需 Amazon 中 DMARC 記錄的詳細資訊 WorkMail，請參閱 Amazon 簡單電子郵件服務開發人員指南中的使用 Amazon SES 遵守 DMARC。

來自域的 TXT 郵件

已驗證 — 記錄已解決並驗證。

擱置中 — 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 郵件來自域

已驗證 — 記錄已解決並驗證。

遺失 — 無法解析記錄。

不一致 — 值與預期的記錄不符。

7. 對於下一個步驟，請根據您使用的 DNS 提供者選擇適當的動作。

如果您使用路線 53 網域

- 在頁面頂端，選擇路線 53 中的全部更新。

如果您使用其他 DNS 供應商

- 複製記錄並將其粘貼到您的 DNS 提供商中。您可以大量複製記錄，也可以一次複製一筆記錄。若要大量複製記錄，請選擇「全部複製」。這將創建一個文件區域，您可以將其導入到 DNS 提供商中。若要一次複製一筆記錄，請選擇記錄名稱旁的重疊方塊，然後將每個記錄貼到 DNS 提供者中。

8. 選擇重新整理圖示，更新每筆記錄的「狀態」。這會驗證 Amazon WorkMail 的網域擁有權和網域的正確組態。

移除網域

當您不再需要網域時，可以刪除它。不過，您必須先刪除任何使用該網域作為其電子郵件地址的個人或群組。

要移除網域

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，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

您可以將與組織關聯的網域設為該組織中使用者和群組的預設網域。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. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，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邊的核取方塊，然後選擇 [設為預設值]。

驗證網域

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

您可以在 DNS 服務中將 TXT 和 MX 記錄新增至網域來驗證網域。TXT 記錄可讓您將備註新增至 DNS 服務。MX 記錄會指定內送郵件伺服器。

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。

若要建立 TXT 和 MX 記錄

1. 開啟 Amazon SES 主控台，網址為 https://console.aws.amazon.com/ses/。
2. 在功能窗格中，選擇 [網域]，然後選擇 [驗證新網域]。

   驗證新網域] 對話方塊隨即出現。
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. (選擇性) 如果您想要使用 DomainKeys 識別的郵件 (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 清單下方的「下載記錄集為 CSV」連結。

   這時系統顯示「另存為」對話框。選擇下載位置，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，您就可以將它們新增至 DNS 提供者。以下步驟使用 53 號路線。如果您使用不同的 DNS 提供者，但不知道如何新增記錄，請參閱供應商的說明文件。

1. 登入 AWS Management Console 並開啟位於 https://console.aws.amazon.com/route53/ 的 Route 53 主控台。
2. 在導覽窗格中，選擇 Hosted Zones (託管區域)。然後，選擇您要驗證的網域旁邊的選項按鈕。
3. 從您網域的 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 小時才能完成驗證過程。

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。

若要使用此nslookup工具，您必須先找到為您的網域提供服務的 DNS 伺服器。然後，您可以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您網域的最多 up-to-date 資訊。這些資訊傳播到其他 DNS 伺服器可能需要一些時間。

請使用核對您的 TXT 記錄是否已新增至您的 DNS 服務

1. 尋找您的網域名稱伺服器：
   a. 開啟命令提示字元 (視窗) 或終端機 (Linux)。
   b. 執行下列命令以列出為您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，並使用步驟 1 中的名*###### ns1.name-###*。

      ```
      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「已驗證的寄件者」清單中您網域的 TXT 值。

在下列範例中，您想要查看值為的 _Amazonses.example.com 的 TXT 記錄。fmxqxT/ic0Yx4aA/bEUrDPMeax9/s3frblS+niixmqk=如果您正確更新記錄，命令會有下列輸出：

```
_amazonses.example.com text = "fmxqxT/ic0Yx4aA/bEUrDPMeax9/s3frblS+niixmqk="
```

使用挖掘來驗證您的 TXT 記錄是否已新增至 DNS 服務

1. 開啟終端機工作階段。
2. 執行下列命令以列出您網域的 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中後面的字串與您在 Amazon WorkMail 主控台的「已驗證的寄件者」清單中選取網域時看到的 TXT 值相符。

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. 執行下列命令以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，並以您在上一個步驟中識別的其中一個名稱伺服器取代 *ns1.name-server.net*。

```
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 dig 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. 執行下列命令以列出網域的 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

若要疑難排解網域驗證的常見問題，請參閱下列建議：

您的 DNS 服務不允許在 TXT 記錄名稱中加上底線

`_amazonses`從 TXT 記錄名稱中省略。

您想要多次驗證同一個域，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具有相同名稱的 TXT 記錄，請使用下列其中一種因應措施：

- (建議) 如果您的 DNS 服務允許，請為 TXT 記錄指派多個值。例如，如果您的 DNS 是由 Amazon 路線 53 管理，您可以為相同的 TXT 記錄設置多個值，如下所示：
  1. 在 Route 53 主控台中，選擇您在第一個區域驗證網域時新增的 _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。
- 如果您只需要驗證網域兩次，您可以透過建立名稱_amazonses中的 TXT 記錄來驗證網域一次，然後建立另一筆不含記錄名稱_amazonses的記錄。

Amazon 主 WorkMail 控台報告網域驗證失敗

Amazon WorkMail 無法為您的 DNS 服務找到必要的 TXT 記錄。請遵循中的程序，確認所需的 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 提供商將域名附加到 TXT 記錄的末尾

新增已包含網域名稱的 TXT 記錄，例如網域名稱可能會導致網域名稱重複，例如網域名稱重複。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 提供者表示該記錄名稱是完整的，而且 TXT 記錄中已包含網域名稱。

Amazon WorkMail 報告 MX 記錄不一致

從現有郵件伺服器遷移時，MX 記錄可能會傳回 [不一致] 狀態。將 MX 記錄更新為指向 Amazon，WorkMail 而不是指向先前的郵件伺服器。將第三方電子郵件代理伺服器與 Amazon 搭配使用時，MX 記錄也會傳回為「不一致」 WorkMail。如果是這種情況，您可放心忽略不一致警告。

啟用 AutoDiscover 以設定端點

AutoDiscover 可讓您只使用您的電子郵件地址和密碼來設定 Microsoft Outlook 和行動用戶端。此服務會維持 WorkMail 與 Amazon 的連線，並在您變更端點或設定時更新本機設定。此外，您的用戶端 AutoDiscover 可以使用其他 Amazon WorkMail 功能，例如離線通訊錄、辦公室外助理，以及在行事曆中檢視空閒/忙碌時間的功能。

用戶端會執行下列 AutoDiscover 階段來偵測伺服器端點 URL：

- 階段 1 — 用戶端會針對本機 Active Directory 執行安全複製通訊協定 (SCP) 查詢。如果您的用戶端未加入網域，則會 AutoDiscover 略過此步驟。

- 階段 2 — 用戶端傳送要求至下列 URL 並驗證結果。這些端點只能使用 HTTPS。
  - HTTPS://*#### /autodiscover/autodiscover.xml*
  - https://autodiscover. *##. #*級 /autodiscover/autodiscover.xml
- 階段 3 — 用戶端對自動探索 .company.tld 執行 DNS 查詢，並從使用者的電子郵件地址將未經驗證的 GET 要求傳送至衍生端點。如果伺服器傳回 302 重新導向，用戶端會針對傳回的 HTTPS 端點重新傳送 AutoDiscover 要求。

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。

將網域新增至 Amazon 時，系統會提示您將 AutoDiscover DNS 記錄新增至供應商 WorkMail。這可讓用戶端執行 AutoDiscover 程序的階段 3。但是，這些步驟並不適用於所有移動設備，例如庫存的 Android 電子郵件應用程序。因此，您可能需要手動設定 AutoDiscover 階段 2。

您可以使用下列方法為網域設定 AutoDiscover 階段 2：

（推薦）使用 53 號路線和 Amazon CloudFront

> **Note**
>
> 下列步驟說明如何為 https://autodiscover 建立代理伺服器。 *## .tld /####/####.* 若要為 https://*## .tld* /autodiscover/autodiscover.xml 建立代理伺服器，請依照下列步驟從網域移除`autodiscover.`前置詞。
> 使用 CloudFront 和 53 號路線可能會損害費用。如需有關適用定價的詳細資訊，請參閱 Amazon CloudFront 定價和 Amazon Route 53 定價。

啟用 AutoDiscover 第二階段設有 53 號幹線及 CloudFront

1. 取得用於自動探索的 SSL 憑證。 *## .tld* 並將其上傳到AWS Identity and Access Management（IAM）或。AWS Certificate Manager如需詳細資訊，請參閱 IAM 使用指南中的使用伺服器憑證或使AWS Certificate Manager用者指南中的入門。
2. 建立新的 CloudFront 發行版：
   1. 在開啟 CloudFront 主控台https://console.aws.amazon.com/cloudfront/v4/home。
   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 「原點設定」 中，輸入下列值：
   - 原始網域名稱 — 適合您所在地區的網域名稱：
     - 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`**
   - 原始協議策略 — 所需的策略：**`Match Viewer`**

     > **Note**
     > 將原點路徑保留空白。請勿變更原始 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
   - 對於替代網域名稱 (CNAME)，請輸入**`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 (儲存在 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)。開啟啟用記錄功能。
- 在 Comment (註解) 中，輸入 **`AutoDiscover type2 for autodiscover.`*`company.tld`***
- 分配狀態：選擇「啟用」。

8. 選擇 Create Distribution (建立分佈)。

3. 在 Route 53 主控台中，建立一個記錄，將您網域名稱的網際網路流量路由到您的 CloudFront 發行版本。

> **Note**
>
> 這些步驟假設例如 .com 的 DNS 記錄託管在路線 53 上。如果您不使用 Route 53，請依照 DNS 提供者管理主控台中的程序執行。

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。
   - 在路由原則下，選取簡單路由。
   - 選擇別名滑桿將其開啟。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 地址和部分 AWS 資源。
   - 在 [將流量路由到] 清單中，選擇 [要 CloudFront散佈的別名]。
   - 一個搜索框將出現在路由流量列表下。在文字方塊中輸入您的 CloudFront發行版名稱。您也可以從選取搜尋方塊時出現的清單中選取您的分發。
5. 選擇建立記錄。

使用阿帕奇網頁伺服器

以下步驟說明如何使用 Apache 網頁伺服器來建立 https://autodiscover 的代理伺服器。 *## .tld /####/####.* 若要為 HTTPS://*## .tld* /autodiscover/autodiscover.xml 建立代理伺服器，請移除「自動探索」。字首於網域，依以下步驟。

若要透過 Apache 網頁伺服器啟用 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 幫助：

   - `proxy`
   - `proxy_http`
   - `socache_shmcb`
   - `ssl`

如需測試和疑難排解的相關資訊，請參閱下一節 AutoDiscover。

AutoDiscover 階段 2 疑難排解

設定 DNS 提供者之後 AutoDiscover，您就可以測試 AutoDiscover 端點組態。如果您已正確設定端點，則會以未經授權的要求訊息回應。

進行基本未經授權的請求

1. 從終端機，向 AutoDiscover 端點建立未經驗證的 POST 要求。

```
$ curl -X POST -v https://autodiscover.''company.tld''/autodiscover/
autodiscover.xml
```

   如果您的端點設定正確，它應該會傳回`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. 接下來，測試一個真正的 AutoDiscover 請求。創建具有以下 XML 內容的`request.xml`文件：

```
<?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. 使用您建立的`request.xml`檔案，並向端點發出驗證的 AutoDiscover 要求。請記住以有效的電子郵件地址取代 *`testuser@company.tld`*：

```
$ curl -d @request.xml -u testuser@company.tld -v https://autodiscover.company.tld/
autodiscover/autodiscover.xml
```

如果端點設定正確，回應看起來會類似下列範例：

```
$ 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

網域識別原則會指定電子郵件動作的權限，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，而不是AWS帳戶主體。如果您在 2022 年 4 月 1 日之前新增網域，則可能有較舊的政策使用AWS帳戶主體進行授權。如果是這樣，我們建議您更新為最新政策。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。

只有在未使用自訂 Amazon SES 政策時，才需遵循下列步驟。如果您使用自訂的 Amazon SES 政策，則必須自行更新。若要取得更多資訊自訂 Amazon SES 服務主要政策，請參閱本主題稍後的〈〉。

> **Important**
>
> 請勿移除您現有的網域。如果這樣做，您將中斷郵件服務。您需要做的就是重新輸入現有域名。

更新網域身分識別原則

1. 在以下位置打開 Amazon WorkMail 控制台 https://console.aws.amazon.com/workmail/。

如有必要請變更 AWS 區域。若要這麼做，請開啟位於搜尋方塊右側的 [選取地區] 清單，然後選擇所需的區域。如需有關區域的詳細資訊，請參閱中的區域和端點Amazon Web Services 一般參考。

2. 在瀏覽窗格中，選擇 [組 Organ izations]，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]。

   這時系統顯示「添加域」對話框。
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. 針對組織中的其餘網域重複步驟 3-5。

自訂 Amazon SES 服務主要政策

如果您使用自訂 Amazon SES 政策，請調整此範例以在您的網域中使用。

```
{
  "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。欺騙是指使惡意行為者發送的電子郵件看起來像合法用戶發送的電子郵件的行為。如需為 WorkMail已啟用 Amazon 的網域設定 SPF 的相關資訊，請參閱在 Amazon SES 中使用 SPF 驗證電子郵件。

設定自訂郵件寄件者網域

默認情況下，Amazon WorkMail 使用 amazonses.com 的子域作為您的外發電子郵件的MAIL FROM域。如果您網域上的 DMARC 原則僅針對 SPF 設定，這可能會導致傳遞失敗。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網MAIL FROM域，請參閱 Amazon 簡易電子郵件服務開發人員指南中的設定自訂 MAIL FROM 網域。

> **Important**
>
> 當您啟用 AutoDiscover iOS 裝置時，需要自訂「郵件寄件者」網域。

如需有關自訂MAIL FROM網域的詳細資訊，請參閱 Amazon SES 現在支援自訂郵件來源網域。

使用使用者

您可以從 Amazon 創建和刪除用戶 WorkMail。此外，您可以重設他們的電子郵件密碼、管理其信箱配額和裝置存取，以及控制其信箱權限。

主題

檢視使用者清單

若要檢視使用者清單

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，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來篩選使用者。

> **Note**
>
> 搜尋是區分大小寫的。

新增使用者

當您新增使用者時，Amazon WorkMail 會自動為使用者建立信箱。用戶可以登錄和訪問他們的郵件從 Amazon WorkMail 網絡應用程序，他們的移動設備，或通過使用 Microsoft Outlook 在 macOS 或 PC 上。

若要新增使用者

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組織]，然後選擇要新增使用者的組織。
3. 在功能窗格中，選擇 [使用者]，然後選擇 [新增使用者]。

   會出現「新增使用者」畫面。
4. 在「使用者詳細資訊」下的「使用者名稱」欄位中，輸入使用者的名稱。名稱也會顯示在 [電子郵件地址] 方塊中。如果您希望使用者的電子郵件地址與其使用者名稱不同，您可以編輯 [電子郵件地址] 欄位。
5. (選擇性) 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其他別名。
8. 依預設，使用者會顯示在全域通訊清單中。若要隱藏全域通訊清單中的使用者，請清除 [在全域通訊清單中顯示] 核取方塊。
9. 選取 [遠端使用者] 以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

當您整合 Amazon WorkMail 與您的企業活動目錄，或者你已經有用戶可用在您的 Simple AD 目錄，您可以在 Amazon 啟用這些用戶 WorkMail。您也可以依照下列步驟重新啟用帳戶已停用的使用者。

啟用使用者

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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」，然後選擇您要啟用其使用者的組織。
3. 在導覽窗格中，選擇使用者 。

   這時系統顯示用戶列表。處於已啟用、已停用和系統使用者狀態的使用者帳戶會顯示在清單中。
4. 從已停用帳號的使用者清單中，選取要啟用之使用者的核取方塊，然後選擇 [啟用]。

   將顯示 [啟用使用者] 對話方塊。
5. 視需要檢閱並變更每位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。

新增電子郵件別名至使用者

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，然後選擇您要新增使用者的組織名稱。
3. 在導覽窗格中，選擇 [使用者]，然後選取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」標籤。
5. 在「別名」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。

移除使用者的電子郵件別名

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，然後選擇要從中移除使用者的組織名稱。
3. 在瀏覽窗格中，選擇 [使用者]，然後選取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」標籤。
5. 在「別名」標籤下，針對您要移除的別名選取核取方塊。
6. 確認要移除的別名。
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，它會立即變得無法存取。停用超過 30 天的使用者將會從 Amazon 刪除其收件匣 WorkMail。

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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 。

   會顯示所有使用者的清單，其中顯示處於 [已啟用]、[已停用] 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]。

   這時系統顯示「禁用用戶」對話框
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 — 姓名、電子郵件地址、電話號碼和其他個人詳細資料。
- 信箱配額 (大小) — 配額範圍可從 1 MB 到 51,200 MB (50 GB) 之間。Amazon WorkMail 會在使用者達到其配額的 90% 時通知使用者。此外，變更使用者的信箱配額也不會影響定價。如需有關定價的詳細資訊，請參閱 Amazon WorkMail 定價。
- 行動裝置存取 — 移除和清除裝置，以及檢視裝置詳細資料。
- 信箱存取權限 — 授與使用者使用信箱的權限，以及授與使用者不同層級的信箱存取權限。

> **Note**
>
> 如果您將 Amazon WorkMail 與 AD Connector 目錄整合，則無法從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。

若要編輯使用者詳細資訊

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在使用者詳細資料區段中，選擇編輯。
2. 在 [使用者詳細資訊] 底下，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]。

編輯信箱配額

1. 在 [使用者詳細資料] 底下，選擇 [配額] 索引標籤，然後選擇 [
2. 在 [更新信箱配額] 方塊中，輸入信箱的大小。您可以輸入**1**到的值**51200**。
3. 選擇儲存變更。

管理行動裝置資料

> **Note**
>
> 要管理移動設備，您的用戶首先需要將其設備連接到您的 Amazon 實例 WorkMail。如需連接行動裝置的相關資訊，請參閱為 Amazon 設定行動裝置用戶端 WorkMail。

1. 在 [使用者詳細資料] 下方，選擇 [行動裝置]
2. 若要查看目前的裝置清單，請選擇「重新整理」。
3. 若要檢視裝置的詳細資料，請從「裝置 ID」欄中選擇裝置名稱。
4. 若要移除或清除裝置，請選擇裝置名稱旁的選項按鈕，然後視需要選擇 [移除] 或 [清除]。
5. 在出現的對話方塊中，確認移除或清除作業。請記住，當用戶 WorkMail 再次將其設備與 Amazon 同步時，將重新出現。

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. 若要新增權限，請選擇 [新增權限]。開啟 [新增權限] 清單並選擇使用者或群組，選擇使用者或群組的權限設定，然後選擇 [儲存]。
    2. 若要編輯使用者權限，請選擇使用者名稱旁邊的按鈕。選擇 [編輯]，選取想要的選項，然後選擇 [儲存]。

    如需有關權限選項的詳細資訊，請參閱使用信箱許可。
3. 如要移除所有權限，請選擇「移除」，然後確認移除。

重設使用者密碼

如果使用者忘記密碼或登入 Amazon 時遇到問題 WorkMail，您可以重設他們的密碼。

> **Note**
>
> 如果您已將 Amazon WorkMail 與 AD Connector 目錄集成，則必須在活動目錄中重置用戶密碼。

若要重設使用者密碼

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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 Organ izations」，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，選取使用者名稱旁邊的核取方塊，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]。

Amazon WorkMail 密碼政策故障

如果重設密碼失敗，請確認新的密碼符合密碼政策的要求。

密碼政策要求取決於 Amazon WorkMail 組織使用的目錄類型。

Amazon WorkMail 目錄和 Simple AD 目錄密碼策略

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
- 由基本拉丁文或拉丁文 -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 目錄密碼政策無法更改。

若要變更 Simple AD 密碼政策，請在簡單 AD 目錄的亞馬遜彈性運算雲端 (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 AWS Directory Service 管理工具。

AWS Managed Microsoft AD 目錄密碼政策

如需有關AWS Managed Microsoft AD目錄預設密碼原則的資訊，請參閱《管理指南》AWS Managed Microsoft AD中的〈管理密碼原則〉。AWS Directory Service

AD Connector 密碼原則

AD Connector 會使用它所連線的使用中目錄網域的密碼原則。如需有關密碼原則設定的詳細資訊，請參閱 Active Directory 網域的文件。

使用通知

使用 Amazon WorkMail 推送通知 API，您可以接收有關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 URL（或推送通知回應者）才能接收通知。使用此功能，開發人員可以為 Amazon 使 WorkMail 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 [新增郵件]、[已建立] 及 [已修改])。

您可以使用用戶端程式庫，例如 EWS Java API 或受管理的 EWS C# API 來存取此功能。此頁面提供使用 AWS Lambda 和 API Gateway (使用 AWS 無伺服器架構) 開發的推播回應程式的完整範例應用程式AWS GitHub。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>ywwAAAAAAAA=</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>
```

為了驗證推送通知回應者的運作狀態，Amazon WorkMail 會傳送「心跳訊號」(也稱為 aStatusEvent)。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>
```

如果用戶端推播通知回應程式無法以與之前相同的OKStatusFrequency狀態回應，則會重試通知最多幾分鐘。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。如果在重試時間過期後仍未傳遞通知，則訂閱會失效，且不會傳遞新的通知。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 來讓使用者在組織內外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. 設定憑證自動註冊，以便自動發行使用者憑證並將其儲存在 Active Directory 中。Amazon 從活動目錄 WorkMail接收用戶證書，並將其發佈到 GAL。如需詳細資訊，請參閱設定 Certificate Autoenrollment 。
3. 透過從執行 Microsoft Exchange 的伺服器匯出憑證並將其郵寄給使用者，藉此將產生的憑證散發給使用者。
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

您可以在 Amazon WorkMail 中使用群組做為通訊群組清單，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，而且會影響您可以授與群組的信箱權限。如需為群組設定信箱權限的相關資訊，請參閱管理群組的信箱權限。

> **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

若要檢視群組清單

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，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**
>
> 搜尋是區分大小寫的。

新增群組

您可以從 Amazon WorkMail 主控台新增群組。

新增群組

1. 在以下位置打開 Amazon WorkMail 控制台 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] 清單並選擇區域。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 Organ izations」，然後選擇組織的名稱。
3. 在功能窗格中，選擇 [群組]，然後選擇 [新增群組]。

   便會顯示「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] 底下，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，視需要更新。
7. 依預設，群組會顯示在全域通訊清單中。若要從全域通訊清單中隱藏群組，請清除 [在全域通訊清單中顯示] 核取方塊。
8. 選擇 Add group (新增群組)。

啟用群組

當您將 Amazon WorkMail 與您的企業活動目錄集成，或者您已經在簡單的活動目錄中使用組時，您可以將這些組用作 Amazon 中的安全組或分發列表 WorkMail。

要啟用現有目錄群組

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，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邊的核取方塊，然後選擇 [啟用]。

   這時系統顯示「啟用組」對話框，要求您確認操作。
5. 視需要檢閱並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 群組後，請使用 Amazon 主 WorkMail 控台將成員新增至該群組。

> **Note**
>
> 如果 Amazon WorkMail 與連接的活動目錄服務或 Microsoft 活動目錄集成，您可以使用活動目錄來管理您的組成員。但是，更改可能需要更長的時間才能傳播到 Amazon WorkMail。

若要將成員新增至群組

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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 Organ izations」，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」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. 選擇儲存。

您的變更可能需要幾分鐘的時間來傳播。

編輯群組詳情

您可以編輯群組的詳細資訊。

編輯群組詳細資訊

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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 Organ izations」，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 [群組]，然後選取要編輯的群組。
4. 在 [群組詳細資料] 頁面上，視需要更新電子郵件地址。
5. 依預設，群組會顯示在全域通訊清單中。若要從全域通訊清單中隱藏群組，請清除 [在全域通訊清單中顯示] 核取方塊。
6. 選擇儲存變更。

從群組中移除成員

使用 Amazon WorkMail 主控台從群組中移除成員。

> **Note**
>
> 如果 Amazon WorkMail 與連接的活動目錄或 Microsoft 活動目錄集成，您可以使用活動目錄來管理您的組成員。但是，這樣做可能會創造將更改傳播到 Amazon WorkMail 所需的時間。

若要從群組中移除成員

1. 在 https://console.aws.amazon.com/workmail/ 打開 Amazon WorkMail 控制台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟 [選取地區] 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 Organ izations」，然後選擇組織的名稱。
3. 在導覽窗格中，選擇「群組」，然後選擇群組名稱。

4. 在「群組詳細資訊」頁面上，選擇「成員」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來傳播。

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. 在 https://console.aws.amazon.com/workmail/ 打開 Amazon WorkMail 控制台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟 [選取地區] 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. 在瀏覽窗格中，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 [群組]，然後選取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://console.aws.amazon.com/workmail/ 打開 Amazon WorkMail 控制台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟 [選取地區] 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. 在瀏覽窗格中，選擇 [組織]，然後選擇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. 確認將要移除的別名。
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://console.aws.amazon.com/workmail/ 打開 Amazon WorkMail 控制台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟 [選取地區] 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 Organ izations」，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] 底下，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。如需關於停用群組的資訊，請參閱停用群組。

刪除群組

1. 在 https://console.aws.amazon.com/workmail/ 打開 Amazon WorkMail 控制台。

   如有必要請變更 AWS 區域。在主控台視窗頂端的列中，開啟 [選取地區] 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 Organ izations」，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. 選取您要刪除的停用群組旁邊的核取方塊，然後選擇 [刪除]。

   這時系統顯示刪除對話框。
5. 在「輸入要確認刪除的群組名稱」方塊中，輸入群組名稱，然後選擇「刪除」。

> **Note**
>
> 若要永久刪除群組，請使用適用於 Amazon 的 `DeleteGroup` API 動作 WorkMail。如需詳細資訊，請DeleteGroup參閱 Amazon WorkMail API 參考中的。

使用 資源

Amazon WorkMail 可以幫助您的用戶保留資源。例如，使用者可以預約會議室或投影機、電話或汽車等設備。若要預約資源，使用者會將資源新增至會議邀請。

主題

檢視資源清單

若要檢視資源清單

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，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**
>
> 搜尋是區分大小寫的。

新增資源

您可以將新資源新增至組織，並允許您的使用者保留該資源。

要新增資源

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，然後選擇組織的名稱。
3. 在導覽窗格中，選擇 [資源]，然後選取 [新增資源]。

   將會顯示 [新增資源] 頁面。
4. 在 [資源名稱] 方塊中，輸入資源的名稱。
5. 選擇性地在 [資源描述] 方塊中，輸入資源的說明。
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，視需要更新。
8. 根據預設，資源會顯示在全域通訊清單中。若要隱藏全域通訊清單中的資源，請清除 [在全域通訊清單中顯示] 核取方塊。
9. 選擇 Add resource (新增資源)。

編輯資源詳情

您可以編輯資源的一般詳細資料，包括名稱、描述、類型和電子郵件地址、預約選項和代理人。

要編輯一般資源詳細資訊

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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 Organ izations」，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 [資源詳細資料] 頁面上，視需要更新資源名稱、說明、資源類型或電子郵件地址。
5. 根據預設，資源會顯示在全域通訊清單中。若要隱藏全域通訊清單中的資源，請清除 [在全域通訊清單中顯示] 核取方塊。
6. 選擇儲存變更。

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約選項。

若要變更資源的預約選項

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，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。隨即出現頁面，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，以啟用或停用該選項。

> **Note**
>
> 當您停用任何自動預訂選項時，您必須建立一個代理人來處理預訂請求。接下來的步驟說明如何創建委託。

您可以新增委派，以控制未設定自動預約選項的資源的預約請求。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. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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 Organ izations」，然後選擇組織的名稱。
3. 在瀏覽窗格中，選擇 [資源]，然後選取要新增委派的資源名稱。
4. (選擇性) 在 [預約選項] 索引標籤中，選擇 [編輯]，清除 [自動接受所有資源要求] 核取方塊，然後選擇 [儲存]。
5. 選擇 [委派] 索引標籤，然後選擇 [新增委派]。

[新增委派] 對話方塊隨即出現。

6. 開啟 [搜尋委派] 清單並選擇委派，然後選擇 [儲存]。

若要移除資源委派

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，然後選擇您要從中移除委派的組織名稱。
3. 在瀏覽窗格中，選擇 [資源]，然後選取要從中移除委派的資源名稱。
4. 選擇 [委派]，然後選擇要移除的委派。
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。

若要將電子郵件別名新增至資源

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組織]，然後選擇要新增別名的組織名稱。
3. 在導覽窗格中，選擇 [資源]，然後選取要新增別名的資源名稱。
4. 在「資源詳細資訊」段落中，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。

若要從資源中移除電子郵件別名

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，然後選擇您要從中移除別名的組織名稱。
3. 在瀏覽窗格中，選擇 [資源]，然後選取要從中移除別名的資源名稱。
4. 在「資源詳細資訊」段落中，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. 確認要移除的別名。
8. 在「移除別名」視窗中，選擇「移除」。

啟用資源

默認情況下，Amazon WorkMail 創建一個資源。如果您或其他人停用了資源，您可以在 30 天內重新啟用資源。

若要啟用資源

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 清單，然後選擇 [區域]。如需有關區域的詳細資訊，請參閱中的區域和端點Amazon Web Services 一般參考。
2. 在瀏覽窗格中，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邊的按鈕，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

當您停用某個資源時，您會使其無法進行預約。例如，您可以在會議室進行重新整理時停用該會議室，然後在會議室可供使用時啟用該會議室。

若要停用資源

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 清單，然後選擇 [區域]。如需有關區域的詳細資訊，請參閱中的區域和端點Amazon Web Services 一般參考。
2. 在瀏覽窗格中，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邊的按鈕，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，可以將其刪除。但是，您必須先停用資源。如需停用資源的相關資訊，請參閱上一節中的步驟。

要移除資源

1. 在以下位置打開 Amazon WorkMail 控制台 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 [選取地區] 清單，然後選擇 [區域]。如需有關區域的詳細資訊，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 Organ izations」，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，選取您要移除的停用資源旁邊的按鈕，然後選擇 [刪除]。

   [刪除資源] 對話方塊隨即出現。
5. 在 [輸入要確認刪除的資源名稱] 方塊中，輸入要刪除的資源名稱，然後選擇 [刪除資源]。

使用行動裝置

本節中的主題說明如何管理連接到 Amazon 的行動裝置 WorkMail。

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 互動的方式 WorkMail。

編輯您的組織的行動裝置政策

1. 在以下位置打開 Amazon WorkMail 控制台 https://console.aws.amazon.com/workmail/。

   如有需要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，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：解除鎖定行動裝置時需要密碼。

   d. 允許簡單密碼：使用設備的 PIN 作為密碼。

   e. 最小密碼長度：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：指定在清除使用者裝置之前，允許嘗試失敗的裝置解除鎖定嘗試次數。擦除設備時，所有數據（包括個人文件）都將被刪除。

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. 選擇儲存。

管理行動裝置

本節中的主題說明如何遠端清除行動裝置、從組織移除裝置，以及檢視裝置的詳細資料。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：

- 設備必須在線並連接到 Amazon WorkMail。如果有人中斷裝置的連線，抹除作業會在使用者重新連線裝置時繼續。
- 抹除作業可能需要五分鐘的時間來傳播。

> **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. 在以下位置打開 Amazon WorkMail 控制台 https://console.aws.amazon.com/workmail/。

如有需要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，然後選擇組織的名稱。
3. 在瀏覽窗格中，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，選擇裝置旁邊的按鈕，然後選擇 [清除]。
6. 檢查概觀中的狀態，以查看是否要求清除。
7. 清除裝置後，將其從裝置清單中移除。下一節中的步驟說明如何進行。

> **Important**
>
> 若要將已清除的裝置還原至使用者的裝置清單，請務必先將其從裝置清單中移除。否則，系統將再次擦除設備。

從裝置清單移除使用者裝置

如果某人停止使用特定的行動裝置，或者您已從遠端清除裝置資料，您可以從裝置清單中移除該裝置。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. 在以下位置打開 Amazon WorkMail 控制台 https://console.aws.amazon.com/workmail/。

   如有需要，請變更 AWS 區域。在主控台視窗頂端的列中，開啟 [選取地區] 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. 在瀏覽窗格中，選擇 [組 Organ izations]，然後選擇組織的名稱。
3. 在功能窗格中，選擇 [使用者]，然後選取使用者的名稱。
4. 選擇 [行動裝置] 索引標籤。
5. 在裝置清單中，選取裝置旁邊的按鈕，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料。

> **Note**
>
> 某些設備不會將所有詳細信息發送到服務器。您可能看不到所有可用的裝置詳細資料。

要檢視裝置的詳細資訊

1. 在以下位置打開 Amazon WorkMail 控制台 https://console.aws.amazon.com/workmail/。

   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. 在瀏覽窗格中，選擇 [組 Organ izations]，然後選擇組織的名稱。
3. 在功能窗格中，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料之裝置的 ID。

   下表列出裝置狀態碼。

狀態	描述
PROVISIONING_REQUIRED	使用者或管理員已要求將裝置佈建為與 Amazon 搭配使用 WorkMail。如果在 Amazon WorkMail 主控台中修改了該裝置的目前政策，裝置也會設定為此狀態。
PROVISIONING_SUCCEEDED	已成功佈建裝置。設備已強制執行指定的策略。
WIPE_REQUIRED	管理員要求在 Amazon WorkMail 主控台進行清除。
WIPE_SUCCEEDED	裝置已成功被抹除。

管理移動設備訪問規則

亞馬遜移動設備訪問規則 WorkMail 允許管理員控制某些類型的移動設備的郵箱訪問。默認情況下，每個亞馬遜 WorkMail 組織使用的規則授予郵箱訪問任何設備（無論類型、型號、操作系統或用户代理）的訪問權限。您可以用自己的規則編輯或替換該默認規則。您也可以添加、變更和刪除規則。

> **Warning**
>
> 如果您刪除組織的所有移動設備訪問規則，亞馬遜 WorkMail 會阻止所有移動設備訪問。

您可以根據下列裝置屬性來建立允許或拒絕存取的規則：

- 裝置類型-「iPhone」、「iPad」或「安卓」。
- 裝置模型-「iPhone10C1"，「IPAD5C1」，或者「HtConex」。
- 裝置作業系統—「安卓系統」或「安卓系統」
- 裝置用户代理程式—「安卓信件交換器」或「安卓信件」。18B92

若要在AWS管理主控台，請參檢視行動裝置詳細資訊。

> **Note**
>
> 某些設備和客户端可能不會報告所有字段的屬性。如需解決這些情況的詳細資訊，請參Dealing with empty fields

> **Important**
>
> 亞馬遜 WorkMail 移動設備訪問規則僅適用於使用 ActiveSync 通訊協定。使用其他協議（如 IMAP）的移動客户端不報告此處列出的設備屬性，因此這些規則將不適用。
> 如果需要限制使用其他協議的設備的訪問權限，則可以創建訪問控制規則。如需的詳細資訊，請參使用存取控制規則。例如，您可以將對其他協議和 Web 郵件的訪問限製為僅限於一系列企業 IP 地址，但允許 Microsoft ActiveSync ，然後使用移動設備訪問規則進一步限制允許的客户端的類型和版本。

主題

- 移動裝置存取規則如何工作
- 使用移動設備訪問規則

移動裝置存取規則如何工作

移動設備訪問規則僅適用於使用微軟交換的設備 ActiveSync 通訊協定。每個規則都有一組條件，用於指定應用規則的時間，以及ALLOW或者DENY作為裝置。僅當規則的所有條件與用户移動設備的屬性匹配時，才適用於訪問請求。沒有任何條件的規則適用於所有請求。每個條件都使用與設備報告的屬性不區分大小寫的前綴匹配。

亞馬遜 WorkMail 評估規則，如下所示：

- 如果存在DENY規則與設備屬性匹配時，策略將阻止該設備。DENY規則優先於ALLOW規則。
- 如果至少有一個ALLOW規則匹配，且沒有DENY規則匹配時，策略允許設備。
- 如果不適用任何規則，則設備將被阻止。

> **Important**
>
> 移動設備報告規則用於操作的屬性。設備在微軟期間報告其屬性 ActiveSync 設備配置過程。亞馬遜 WorkMail 無法獨立驗證移動客户端報告正確或 up-to-date 資訊。

使用移動設備訪問規則

您可以使用 API 或 AWS 命令列界面 (CLI) 來建立和管理移動裝置存取規則。如需的詳細資訊AWS CLI，請參AWS 命令列界面使用者指南。

> **Important**
>
> 當您更改亞馬遜的訪問規則 WorkMail 組織中，受影響的設備可能需要五分鐘才能遵循更新的規則，設備在此期間可能會顯示不一致的行為。但是，當您測試規則時，您會立即看到正確的行為。如需詳細資訊，請參閱 Testing mobile device access rules。

列出移動設備訪問規則

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
```

創建移動設備訪問規則

以下示例創建阻止所有 Android 設備訪問郵箱的規則。

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name BlockAllAndroid --effect DENY --device-types
 "android"
```

以下示例創建一個僅允許特定版本的 iOS 的規則。請務必刪除默認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"
```

更新移動設備訪問規則

以下示例通過添加標識符來更新設備規則。

```
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

以下示例刪除具有給定標識符的移動設備訪問規則。

```
aws workmail delete-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --mobile-device-access-rule-id 1a2b3c4d
```

測試移動設備訪問規則

要測試訪問規則，您可以使用獲取移動設備訪問API，或移動設備訪問效果命令AWS CLI。如需的詳細資訊AWS CLI，請參AWS命令列界面使用者指南。

測試時，您將傳入模擬移動設備的屬性，並且 API 或 CLI 返回訪問效果-ALLOW或者DENY-具有這些屬性的真正移動設備將接收到這些信息。例如，此命令測試運行 iOS 14.2 的 iPhone 以及默認郵件應用程序是否可以訪問郵箱。

```
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"
```

處理空字段

某些移動設備或客户端可能不會報告一個或多個字段的信息，這些值留空。規則可以與這些設備匹配，方法是使用特殊值$NONE在條件下。例如，一個帶有DeviceTypes=["iphone", "ipad", "$NONE"]將匹配報告設備類型為"iphone"或者"ipad"，或者根本不報告設備類型。

負面條件，如NotDeviceTypes或者NotDeviceUserAgents不匹配這些空值。例如，一個帶有NotDeviceTypes=["android"]將匹配報告設備類型"android"。但是，該規則與根本不報告設備類型的設備不匹配。

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。覆寫會套用至特定使用者和裝置，而且會反轉預設存取規則。您也可以使用覆寫建立一次性例外來存取規則，以及允許或拒絕特定使用者和裝置配對。此外，您可以將覆寫與DefaultDenyAll行動裝置存取規則搭配使用。這會將存取決策延遲至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 整合行動裝置管理解決方案

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配對建立行動裝置存取覆寫。在評估指定使用者和裝置的行動裝置存取規則時，覆寫會反轉預設存取結果。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處理其電子郵件。相反地，如果存取規則通常允許存取，您可以建立覆寫，防止使用者和裝置同步處理其郵件。刪除行動裝置存取覆寫時，Amazon 在決定是否授予該使用者和裝置存取權時， WorkMail 再次遵守目前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。如需有關的詳細資訊 AWS CLI，請參閱 AWS 命令列界面使用者指南。

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料。

列出行動裝置存取覆寫

此範例顯示如何列出指定 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，以拒絕對指定 Amazon WorkMail 組織、使用者和裝置 ID 的存取。

```
aws workmail put-mobile-device-access-override --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --user-id user1@domain.com --device-
id 6APMEKPHCP2ND42VIJ4BR8ECDO --effect DENY
```

您可以修改現有的行動裝置存取取代，以產生不同的效果。這將更新先前創建的移動設備訪問覆蓋以允許訪問而不是拒絕。

```
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
```

整合行動裝置管理解決方案

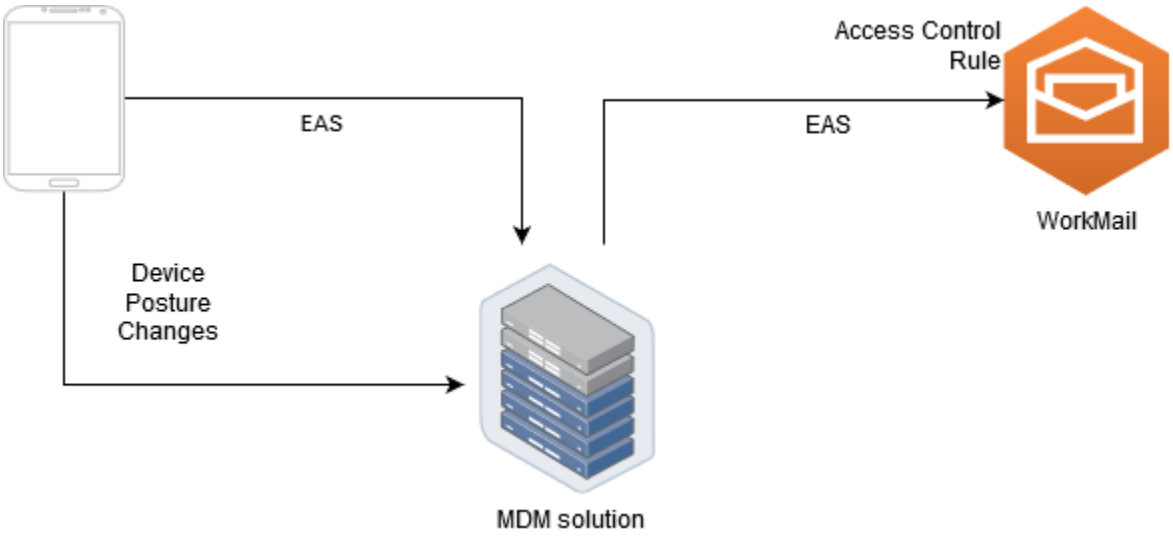
Amazon 透過行動裝置政策和行動裝置存取規則 WorkMail 支援某些基本的行動裝置管理功能。不過，這些功能只能透過 Microsoft Exchange ActiveSync (EAS) 通訊協定與行動裝置互動，因此它們的內部檢查和強制執行裝置安全性狀態的能力有限。需要更好地控制裝置安全性和合規性的管理員可以使用第三方流動裝置管理 (MDM) 解決方案。

行動裝置管理解決方案概

您可以使用代理伺服器或直接兩種模式來設定 MDM 解決方案。請參閱 MDM 文件，以瞭解您的解決方案支援哪些模式。

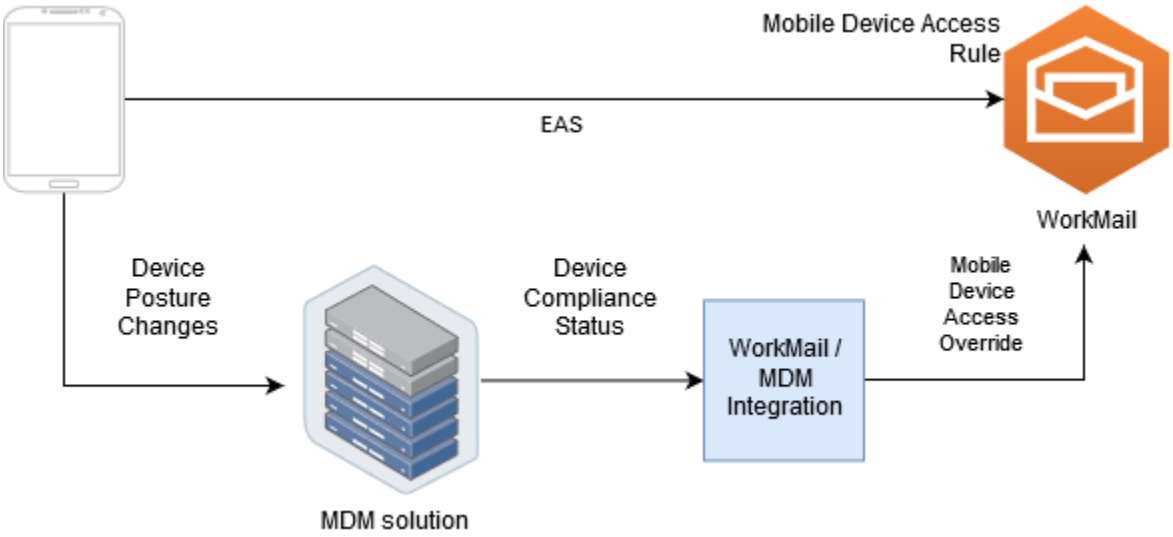
在代理模式下，移動設備通過 MDM 解決方案使用交換活動同步（EAS）協議訪問 Amazon。WorkMailMDM 解決方案會使用裝置狀態來允許或拒絕存取 Amazon WorkMail 資料。在 Amazon 方 WorkMail 面，請使用存取控制規則，該規則僅允許從 MDM 解決方案的一或多個 IP 地址存取 EAS。如需詳細資訊，請參閱使用存取控制規則。

下圖顯示了典型的代理模式配置。



在直 WorkMail 接模式下，移動設備使用 EAS 直接訪問 Amazon。您的 MDM 解決方案會接收裝置姿勢變更，並持續評估每部裝置是否符合這些需求。當 MDM 解決方案偵測到狀態變更時，例如裝置不符合規定，它可以採取數個動作，而且通常會發出通知或事件。Amazon WorkMail 管理員可以設定系統來監聽這些合規狀態事件，並自動建立行動裝置存取覆寫，以便在裝置進入或不符合 MDM 裝置要求時允許或拒絕存取裝置。

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，您必須符合下列需求：

- 建立存取控制規則，將使用者裝置的存取限制為只有 ActiveSync通訊協定。
- 建立預設的 "deny-to-all" 行動裝置存取規則，以確保預設拒絕所有未知或未受管理的行動裝置。
- 採用行動裝置管理解決方案，當裝置變更安全狀態時，就會發出自訂通知或事件，表示裝置符合規定。
- 建立自訂軟體元件以監聽這些通知，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在允許存取其 Amazon WorkMail 信箱之前都符合其 MDM 合規要求。

使用存取控制規則限制行動裝置存取 ActiveSync

您必須確保所有裝置都只使用 ActiveSync 通訊協定，而且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 位址範圍授與其他郵件通訊協定的存取權，然後僅在從公司防火牆外部存取 eamil ActiveSync 時允許。您必須這麼做，因為僅 ActiveSync 允許您使用裝置 ID 識別裝置。您無法使用諸如網際網路訊息存取通訊協定 (IMAP) 或交換網頁服務之類的通訊協定。如需詳細資訊，請參閱 使用存取控制規則。

建立預設的「拒絕所有人」存取規則

若要將所有行動裝置存取決策延遲至第三方行動裝置管理解決方案，請建立自動拒絕所有裝置的存取規則，除非針對個別使用者或每個裝置進行覆寫。如需詳細資訊，請參閱 管理移動設備訪問規則。

此範例顯示「拒絕所有人」規則。

```
aws workmail create-mobile-device-access-rule --organization-id
 m-a123b4c5de678fg9h0ij1k2lm234no56 --name DefaultDenyAll --effect DENY
```

回應裝置姿勢變更並建立行動裝置存取覆寫

您必須將 MDM 解決方案設定為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 建立或更新行動裝置存取覆寫的元件使用。根據預設，由於本主題稍早顯示的預設「拒絕所有」行動裝置存取規則，Amazon WorkMail 拒絕存取未受管或新佈建的裝置。當 MDM 解決方案判定裝置符合所有需求，並發出通知，指出裝置符合規定時，此元件便可ALLOW針對指定的使用者和裝置建立行動裝置存取覆寫，以回應此通知。如果裝置稍後不符合規範，行動裝置管理解決方案會發出另一個通知，並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 Amazon 與 MDM WorkMail 整合的範例，請參閱此AWS 範例應用程式。

使用信箱許可

您可以使用 Amazon 中的信箱許可授與 WorkMail 使用者和群組在其他使用者信箱中工作的權限。信箱權限會套用至整個信箱。它們可讓多位使用者存取相同的信箱，而不需共用該信箱的認證。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**
>
> 擁有隱藏在全域通訊清單中之使用者之信箱權限的使用者，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：

- 完整存取權 — 啟用信箱的完整讀取和寫入存取權限，包括修改資料夾層級權限的權限。

  > **Note**
  >
  > 此選項僅適用於使用者。無法授與群組完整存取權限。

- 代理傳送者 — 可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。
- 以下列傳送 — 可讓使用者或群組以信箱擁有者的身分傳送電子郵件，而不顯示郵件的實際寄件者。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。

當您授與信箱權限時，Amazon WorkMail AutoDiscover 服務會自動為您新增的使用者或群組更新對這些信箱的存取。

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。請在 60 分鐘內傳播變更，然後重新啟動 Outlook。

對於 Amazon WorkMail Web 應用程式和其他電子郵件用戶端，具有完整存取權限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

關於信箱和資料夾權限

信箱權限會套用至信箱內的所有資料夾。這些許可只能由AWS帳戶持有人或授權呼叫 Amazon WorkMail 管理 API 的 IAM 使用者啟用。若要設定和變更信箱或整個群組的許可，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。如需有關使用 Amazon WorkMail Web 應用程式共用資料夾的詳細資訊，請參閱 Amazon 使用 WorkMail 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 主控台管理使用者和群組的信箱許可。以下各節說明如何管理使用者的許可。如需管理群組許可的詳細資訊，請參閱管理群組的信箱權限。

主題

新增許可

當您新增權限時，您會授與一位使用者在其他使用者信箱中執行一或多項工作的權限。例如，假設員工 A 需要代表他的主管員工 B 傳送郵件。若要授與該權限，您可以前往員工 B 的信箱設定，並授與員工 A 執行要求工作的權限。

新增信箱權限

1. 在以下位置打開亞馬遜 WorkMail 控制台 https://console.aws.amazon.com/workmail/。

   如有必要請變更區域。請在導覽列中，選擇符合您需求的區域。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 Organ izations，然後選擇您要管理其許可的組織名稱。
3. 在導覽窗格中，選取使用者名稱，然後選取您要管理其許可的使用者名稱。
4. 選擇 許可 標籤，然後選擇 新增許可。

   [新增權限] 對話方塊隨即出現。
5. 開啟 [新增權限] 清單，然後選取需要存取信箱的使用者或群組。
6. 在 [信箱權限] 和 [傳送權限] 底下，選擇所需的選項。
7. 選擇 Add (新增)。

新許可的傳播可能需要 5 分鐘。

編輯使用者的信箱權限

當您編輯使用者的信箱權限時，您會變更其他人對該使用者信箱所擁有的存取權。編輯信箱權限並不會變更信箱原始使用者的存取權。

編輯信箱許可

1. 在以下位置打開亞馬遜 WorkMail 控制台 https://console.aws.amazon.com/workmail/。

   如有必要請變更區域。請在導覽列中，選擇符合您需求的區域。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 Organ izations，然後選擇您要管理其許可的組織名稱。
3. 在導覽窗格中，選擇使用者名稱，然後選取您要編輯其許可的使用者名稱。
4. 選擇 許可 標籤。

   會出現具有信箱存取權的使用者和群組清單。
5. 選取您要變更的使用者或群組旁的選項按鈕，然後執行以下任一項作業：

   若要移除使用者的權限

   1. 選擇 Remove (移除)。

      [移除權限] 對話方塊隨即出現。
   2. 在 [移除權限] 對話方塊中，選擇 [移除]。

若要編輯使用者的權限

1. 選擇 編輯 。

   [編輯權限] 對話方塊隨即出現。
2. 視需要設定許可，然後選擇儲存。

授與其他使用者權限給信箱

1. 選擇 Add permissions (新增許可)。

   [新增權限] 對話方塊隨即出現。
2. 開啟 [新增權限] 清單，然後選取您要新增的使用者。
3. 視需要設定權限，然後選擇 [新增]。

對許可的變更可能需要 5 分鐘才會傳播給使用者。

管理群組的信箱權限

您可以新增或移除 Amazon 的群組許可 WorkMail。

> **Note**
>
> 您無法將完整存取權限套用至群組，因為群組沒有信箱可供存取。

管理群組許可

1. 在以下位置打開亞馬遜 WorkMail 控制台 https://console.aws.amazon.com/workmail/。

   如有必要，請變更主控台視窗頂端的列AWS 區域中，開啟 [選取區域] 清單並選擇 [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 Organ izations，然後選擇您要管理其許可的組織名稱。
3. 在導覽窗格中，選取群組，然後選取您要為其設定許可的群組名稱。
4. 選擇「權限」標籤頁，然後選擇「新增權限」。

[新增權限] 對話方塊隨即出現。

5. 開啟 [新增權限] 清單，然後選取要授與信箱權限的使用者或群組。
6. 在 [信箱權限] 和 [傳送權限] 底下，選擇所需的選項。
7. 選擇 Add (新增)。

對許可的變更可能需要 5 分鐘才會傳播給使用者。

以程式設計方式存取信箱

若要以程式設計方式存取 Amazon WorkMail 信箱，請使用交換網路服務 (EWS) 通訊協定。使用 EWS，您可以存取信箱中的所有項目類型。以下是您可以與亞馬遜一起使用的一些 EWS 庫 WorkMail：

- 爪哇 — EWS 爪哇 API
- 。淨-EWS 託管的 API。
- 蟒蛇-交換

Amazon WorkMail 也支援 IMAP 和 SMTP 協定，您可以用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 協定支援的網址。

使用 EWS 通訊協定時，Amazon WorkMail 支援下列身份驗證方法：

- 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，您可以存取使用者的信箱，而無需輸入使用者的認證。

主題

管理模擬角色

透過模擬角色，系統管理員可設定使用者信箱的程式設計存取，而不需要輸入使用者的認證。服務和工具可以假設模擬角色，在使用者的信箱中執行動作。僅 EWS 通訊協定支援模擬。

模擬角色概觀

若要允許模擬，系統管理員必須建立具備下列屬性的模擬角色：

- 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作業類型。
- Rules — 定義模擬角色可模擬哪些使用者的規則清單。

亞馬遜 WorkMail 根據以下條件評估規則：

- 如果任何 D ENY 規則相符，則策略會拒絕模擬。DENY 規則的優先順序高於任何允許規則。
- 如果至少一個允許規則符合，且沒有符合 DENY 規則，則原則會允許模擬。
- 如果沒有規則適用，則會拒絕模擬。

> **Note**
>
> 若要允許 Amazon WorkMail 組織中的所有使用者模擬，請建立具有「允許」效果且無條件的規則。

> **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，模擬角色就無法承擔使用者的存取權限。

建立模擬角色之後，您可以使用它來取得使用者信箱的存取權。如需詳細資訊，請參閱使用模擬角色。

安全考量

使用模擬角色可以在 Amazon WorkMail 組織和AWS 帳戶. 以下是建立模擬角色時需要考量的一些潛在問題：

- 轉移權限 — 如果使用者 A 具有使用者 B 信箱的存取權，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 的存取權限，並存取使用者 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 如何與 IAM 合 WorkMail 作。

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. 在以下位置打開亞馬遜 WorkMail 控制台 https://console.aws.amazon.com/workmail/。

   如有必要請變更區域。請在導覽列中選擇符合您需求的區域。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 Organ izations，然後選擇組織名稱。
3. 選擇模擬角色，然後選擇 [建立角色]。
4. 這時系統顯示「創建模擬角色」對話框。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) 說明 — 輸入模擬角色的說明。
   - 角色類型 — 選擇 [唯讀] 或 [完整存取權]。
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) 說明 — 輸入規則的描述。
   - 在效果下，選擇允許或拒絕。這會根據您在以下步驟中選取的條件來允許或拒絕存取。
   - (選擇性) 在此規則下：，選擇比對模擬所選使用者的要求以包含特定使用者。選擇比對模擬所選使用者以外之使用者的請求，以新增所選使用者以外的使用者。
7. 選擇 Add rule (新增規則)。

   > **Note**
   >
   > 只有當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。

若要編輯模擬角色

1. 在以下位置打開亞馬遜 WorkMail 控制台 https://console.aws.amazon.com/workmail/。

如有必要請變更區域。請在導覽列中選擇符合您需求的區域。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 Organ izations，然後選擇組織名稱。
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. [編輯模擬角色] 對話方塊隨即出現。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) 說明 — 輸入模擬角色的說明。
   - 角色類型 — 若要授與模擬角色對使用者信箱的唯讀存取權，請選擇 [唯讀]。若要授與模擬角色讀取和修改使用者信箱中項目的權限，請選擇 [完整存取權]。
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 — 編輯規則名稱。
   - (選用) 說明 — 更新或輸入規則的描述。
   - 在「效果」下，選擇「允許」以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]。
   - (選擇性) 在此規則下：，選擇比對模擬所選使用者的要求以包含特定使用者。選擇比對模擬所選使用者以外之使用者的請求，以新增所選使用者以外的使用者。
8. 選擇 儲存 。
9. 選擇 Save changes (儲存變更)。

> **Important**
>
> 變更模擬規則時，受影響的信箱可能需要 5 分鐘才會更新。在規則更新程序期間，您可能會發現信箱中不一致的行為。但是，如果您測試角色，Amazon WorkMail 會根據更新的規則如預期回應。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。

若要測試模擬角色

1. 在以下位置打開亞馬遜 WorkMail 控制台 https://console.aws.amazon.com/workmail/。

   如有必要請變更區域。請在導覽列中選擇符合您需求的區域。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 Organ izations，然後選擇組織名稱。
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，選取您要測試模擬存取權的使用者。
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。

若要刪除模擬角色

1. 在以下位置打開亞馬遜 WorkMail 控制台 https://console.aws.amazon.com/workmail/。

   如有必要請變更區域。請在導覽列中選擇符合您需求的區域。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 Organ izations，然後選擇組織名稱。
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`。如需有關亞馬遜 WorkMail API 的詳細資訊，請參閱 API 參考資料。

AssumeImpersonationRole返回一個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下列組織與帳戶專屬的詳細資訊：

- *WORKMAIL_ORGANIZATION_ID*— 亞馬遜 WorkMail 組織 ID
- *IMPERSONATION_ROLE_ID*— 模擬角色 ID
- *WORKMAIL_EWS_URL*— 可在亞馬遜端點和配額上使用的 EWS WorkMail 端點
- *EMAIL_ADDRESS*— 使用者信箱的電子郵件地址

Example 爪哇 — EWS 爪哇 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 。淨-EWS 託管的 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 蟒蛇-交換

```
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 StartMailboxExportJobAPI 參考中的 WorkMail API 動作，將 Amazon WorkMail 信箱內容匯出至亞馬遜 Simple Storage Service (Amazon S3) 儲存貯體。此動作會以 MIME 格式將指定信箱中的所有電子郵.zip件和行事曆項目匯出至 Amazon S3 儲存貯體中的檔案。不會匯出其他項目，例如連絡人和工作。

完成信箱匯出工作所需的時間取決於信箱中的項目大小和數目。由於信箱匯出工作會在一段時間內進行，因此不代表單一時間點的信箱內容快照。若要查看匯出任務的狀態，請使用 Amazon ListMailboxExportJobsAPI 參考中的DescribeMailboxExportJob或 WorkMail API 動作。

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) 加密。由於AWS KMS加密已與 Amazon S3 整合，因此只要使用者能夠存取AWS KMS CMK，下載資料的使用者就可以看到解密的資料。

先決條件

下列是匯出信箱內容的先決條件：

- 編程的能力。
- 亞馬遜 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 簡單儲存服務使用者指南中的使用 Amazon S3 區塊公開存取和 Amazon 簡單儲存服務使用者指南。
- 一個對稱的AWS KMS CMK。如需詳細資訊，請參閱開AWS Key Management Service發人員指南中的入門。
- 具有政策的AWS Identity and Access Management (IAM) 角色，授予寫入 Amazon S3 儲存貯體和使用AWS KMS CMK 加密傳送檔案的權限。如需詳細資訊，請參閱Amazon 如何與 IAM 合 WorkMail 作。

IAM 政策範例和角色建立

以下範例顯示 IAM 政策，該政策授予寫入 Amazon S3 儲存貯體以及使用AWS KMS CMK 加密傳送檔案的權限。若要在下列範例：匯出信箱內容程序中使用此範例原則，請將原則另存為具有檔案名稱的 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:::AWSDOC-EXAMPLE-BUCKET",
                "arn:aws:s3:::AWSDOC-EXAMPLE-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:::AWSDOC-EXAMPLE-
BUCKET/S3-PREFIX*"
                }
            }
        }
    ]
}
```

以下範例顯示連接到您建立的 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原則，請將原則另存為具有檔案名稱的 JSON 檔案`mailbox-export-trust-policy.json`。

您不必同時使用`aws:SourceArn`和`aws:SourceAccount`條件。例如，如果您需要使用相同角色`aws:SourceArn`從同一AWS帳戶下的不同 Amazon WorkMail 組織匯出訊息，則可以從政策中移

除。如需有關條件索引鍵的詳細資訊，請參閱 AWSIdentity 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"
        }
      }
    }
  ]
}
```

您可以執AWS CLI行下列命令，使用在帳戶中建立 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 AWS CLI 的詳細資訊，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 角色和政策之後，請完成下列步驟以匯出信箱內容。您必須擁有您的 Amazon WorkMail 組織 ID 和使用者 ID (實體 ID)，您可以在 Amazon WorkMail 主控台或使用 Amazon WorkMail API 存取這些 ID。

範例：若要匯出信箱內容

1. 使用啟AWS CLI動信箱匯出工作。

```
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 AWSDOC-
EXAMPLE-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，您也可以使用**start-mailbox-export-job**命令產生的工作識別碼，僅監視該信箱匯出工作的狀態。

```
aws workmail describe-mailbox-export-job --organization-id m-
a123b4c5de678fg9h0ij1k2lm234no56 --job-id JOB-ID
```

當信箱匯出任務狀態為「已完成」時，匯出的信箱項目可在指定 Amazon S3 儲存貯體中的.zip檔案中使用。

下列是匯出信箱的輸出記錄檔：

```
{
  "totalNonExportableItems" : "13",
  "totalMessages" : "76",
  "sha384Hash" : "4de93a***96a1dd",
  "totalBytes" : "161892",
  "totalFolders" : "15",
  "startTime" : "168***380",
  "endTime" : "168***384"
}
```

> **Note**
>
> totalNonExportable項目是不受支持的項目，如備忘錄和聯繫人

考量事項

匯出 Amazon 的信箱任務時要注意下列事項 WorkMail：

- 您最多可以為指定的 Amazon WorkMail 組織執行 10 個並行信箱匯出任務。
- 您可以每 24 小時為指定信箱執行一次信箱匯出工作。
- 下列資源必須全部位於相同的AWS區域：
  - 亞馬遜 WorkMail 組織
  - AWS KMSCMK
  - Amazon S3 儲存貯體

故障診斷

本節中的主題說明如何疑難排解 Amazon 中的問題 WorkMail。

主題

檢視電子郵件標頭

電子郵件標頭中的資訊可協助您排解常見的使用者電子郵件問題。Amazon WorkMail 允許您查看任何消息的標題信息。

在 Amazon 中查看電子郵件標題 WorkMail

1. 在 Amazon WorkMail Web 應用程式中，按兩下要開啟的電子郵件訊息。
2. 選擇郵件右上角「傳送日期」旁邊的「訊息」選項 (齒輪和信封圖示)。

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 組織可能遇到郵件路由問題。本節中的步驟說明解決傳送與路由問題的常見方法。

入站郵件問題：

- 查看與您的 Amazon WorkMail 組織相關聯之網域的 MX 記錄。 `WorkMail`應該是唯一的條目，並應具有最低的優先級。多個 MX 記錄可能會導致錯誤的服務接收郵件。如需 MX 記錄的詳細資訊，請參閱驗證網域。
- 在 Amazon 主控台中檢查組織的網域型訊息身份驗證、報告和一致性 (DMARC) 設定。 WorkMail DMARC 記錄可用來防範可能危及使用者帳戶憑證的常見攻擊 (例如詐騙或網路釣魚)。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 簡易電子郵件服務輸入規則。如果規則包含 Amazon 以外的動作 WorkMail，則這些動作可能會失敗，並導 WorkMail 致 Amazon 停止接收郵件。如需 Amazon SES 規則的詳細資訊，請參閱 Amazon 簡單電子郵件服務開發人員指南中的「與 Amazon 整合」 WorkMail 動作。

- 在 Amazon 中啟用訊息追蹤 WorkMail，然後檢查日誌是否有交付問題。如需郵件追蹤的詳細資訊，請參閱啟用電子郵件事件記。

輸出郵件問題

- 確保您的 SPF 記錄包括 Amazon SES。檢查 Amazon WorkMail 主控台中的網域頁面以進行驗證。若要取得有關 SPF 的更多資訊，請參閱以 SPF 驗證您的電子郵件。
- 確保 Amazon WorkMail 擁有使用該域的許可。如果沒有，請再次新增網域。 新增網域本指南中提供了操作步驟。

搭配 Amazon 使用電子郵件日誌 WorkMail

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 會 WorkMail 記錄傳送給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會傳送至系統管理員指定的地址，格式稱為`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。

兩個電子郵件地址用於電子郵件日誌：日誌電子郵件地址和報告電子郵件地址。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。

所有日誌記錄都是從自動新增至您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，您也無法使用此名稱或地址建立信箱。

> **Note**
>
> 請勿從 Amazon Simple Email Service (Amazon SES) 開始，不要從 Amazon Simple Email Service (Amazon SES) 開始，不然，
>
> ```
> yourorganization.awsapps.com
> ```

無論收件者或使用者群組的數目為何，每封內送或寄出的電子郵件都會產生一個日誌記錄。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. 在以下位置打開亞馬遜 WorkMail 控制台 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 [選取地區] 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 Organ izations，然後選擇您的組織的名稱。
3. 在功能窗格的 [組織] 設定中，選擇 [日誌記錄] 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 [日誌記錄電子郵件地址] 方塊中，輸入電子郵件日誌提供者所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 儲存 。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中的重要變更。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	稽核記錄檔可用來監視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 管理員指南中的啟用稽核記錄以及 Amazon WorkMail 中的記錄和監控。	2024年3月20日
傳輸層安全性 (TLS) 支援	Amazon WorkMail 停止了對傳輸層安全性（TLS）1.0 和 1.1 的支持。如果您使用的是 TLS 1.0 或 1.1，您必須將 TLS 版本升級至 1.2。	2023 年 11 月 2 日
遠端使用者	遠端使用者是在 Amazon WorkMail 組織外部託管或託管在不同電子郵件網域上的 Amazon WorkMail 使用者。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
以程式設計方式存取信箱	Amazon WorkMail 現在提供模擬角色，以授與信箱的程式設計存取權限。如需詳細資訊，請參閱 Amazon WorkMail 管理員指南中的信箱以程式設計方式存取。	2022 年 10 月 4 日

在 Amazon 上設定自訂可用性供應商 WorkMail	Amazon WorkMail 支持使用自定義可用性提供商（CAP）。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
用於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 動作可將 Amazon WorkMail 信箱內容匯出至亞馬遜簡易儲存服務 (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
信箱保留原則	為您的 Amazon WorkMail 組織設定信箱保留政策，以便在您選擇的時間段後自動刪除電子郵件。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
同步和非同步執行 Lambda 動作	為在 Amazon WorkMail 電子郵件流程規則中執行 Lambda 動作選擇同步或非同步組態。如需詳細資訊，請參閱 Amazon WorkMail 管理員指南 WorkMail中的 AWS Lambda 為 Amazon 設定。	2020 年 5 月 11 日

使用存取控制規則	存取控制規則可讓 Amazon WorkMail 管理員控制其組織信箱的存取方式。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 組 WorkMail 織以區分 AWS Billing and Cost Management 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
對內送電子郵件強制執行 DMARC 政策	如需詳細資訊，請參閱 Amazon WorkMail 管理員指南中的對內送電子郵件執行 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

路線 53 DNS 記錄插入	設置在 Route 53 公共託管區域中管理的域時，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
為輸入電子郵件規則動作設定 Lambda	Amazon WorkMail 支援設定 Lambda 函數以搭配輸入電子郵件流程規則使用。如需詳細資訊，請參閱 Amazon 管理 WorkMail 員指南中的管理電子郵件流程。	2019 年 1 月 24 日
為 Amazon 配置 Lambda WorkMail	Amazon WorkMail 支援設定 Lambda 函數以搭配輸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 WorkMail中的為 Amazon 設定 Lambda。	2018 年 11 月 19 日
SMTP 路由	Amazon WorkMail 支援設定 SMTP 閘道以搭配輸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 已經為自定義域添加了調試工具。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

對 2019 年展望的 Support	Amazon WorkMail 支持展望 2019 的視窗和 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。	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
信箱權限	您可以使用 Amazon 中的信箱許可授與 WorkMail 使用者或群組在其他使用者信箱中工作的權限。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
Support AWS CloudTrail	Amazon WorkMail 集成 AWS CloudTrail. 如需詳細資訊，請參閱 Amazon WorkMail 管理員指南 AWS CloudTrail中的使用記錄 Amazon WorkMail API 呼叫。	2017 年 12 月 12 日
Support 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 管理 WorkMail 員指南中的管理電子郵件流程。	2017 年 7 月 5 日
快速設定的更新	快速設置現在為您創建一個 Amazon WorkMail 目錄。如需詳細資訊，請參閱 Amazon WorkMail 管理員指南中的 WorkMail 使用快速設定設定 Amazon。	2017 年 5 月 10 日

Support 更廣泛的電子郵件客戶端	您現在可以使用 Amazon WorkMail 與 Microsoft 展望 2016 年的 Mac 和 IMAP 電子郵件客戶端。如需詳細資訊，請參閱 Amazon WorkMail 管理員指南 WorkMail中的 Amazon 系統要求。	2017 年 1 月 9 日
Support 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 WorkMail中的搭配 Amazon 使用電子郵件日誌。	2016 年 11 月 25 日
Support 電子郵件重新導向至外部電子郵件	您可以透過更新網域的 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
Support 互通性	您可以啟用 Amazon WorkMail 和 Microsoft 交換之間的互操作性。如需詳細資訊，請參閱 Amazon WorkMail 管理員指南中的 Amazon WorkMail 和 Microsoft Exchange 之間的互通性。	2016 年 10 月 25 日
一般可用性	Amazon 的正式發行版本 WorkMail。	2016 年 1 月 4 日
Support 保留資源	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

Support 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 WorkMail中的移轉到 Amazon。	2015 年 8 月 16 日
Amazon 的預覽版 WorkMail	Amazon 的預覽版本 WorkMail。	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。