aws

管理指南

Amazon WorkDocs

Amazon WorkDocs: 管理指南

Table of Contents

您必須是 Amazon 系 WorkDocs 統管理員才能完成本指南中的步驟。如果您需要使用 Amazon 的協助 WorkDocs，請參閱 Amazon 使用 WorkDocs 者指南 WorkDocs中的 Amazon 入門。

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。

什麼是 Amazon WorkDocs？

Amazon WorkDocs 是全受管、安全的企業儲存和共用服務，具有強大的管理控制和意見反應功能，可提高使用者生產力。檔案會存放在雲端，安全無虞。使用者的檔案只有他們能看見，而他們可以指定參與者和檢視者。除非他們特別授與存取，否則組織中其他成員無法存取其他使用者的任何檔案。

使用者可以與組織的其他成員共用檔案，以執行協同合作或檢閱。Amazon 用 WorkDocs 戶端應用程式可用來檢視許多不同類型的檔案，具體取決於檔案的網際網路媒體類型。Amazon WorkDocs 支持所有常見的文檔和圖像格式，並不斷添加對其他媒體類型的支持。

有關更多信息，請參閱 Amazon WorkDocs。

訪問 Amazon WorkDocs

管理員使用 Amazon WorkDocs 主控台建立和停用 Amazon WorkDocs 網站。透過管理控制面板，他們可管理使用者、儲存與安全性設定。如需詳細資訊，請參閱 WorkDocs 從網站管理控制面板管理 Amazon 及 邀請和管理亞馬遜 WorkDocs 用戶。

非管理使用者使用用戶端應用程式來存取其檔案。他們從不使用 Amazon WorkDocs 主控台或管理儀表板。Amazon WorkDocs 提供數種不同的用戶端應用程式和公用程

- 用來文件管理和檢閱的 web 應用程式。
- 用來文件檢閱的行動裝置原生應用程式。
- Amazon WorkDocs 雲端硬盤，一個應用程序，可將 macOS 或 Windows 桌面上的文件夾與 Amazon WorkDocs 文件同步。

如需使用者如何下載 Amazon 用 WorkDocs 戶端、編輯檔案和使用資料夾的詳細資訊，請參閱 Amazon 使用 WorkDocs 者指南中的以下主題：

- 開始使用 Amazon WorkDocs
- 使用檔案
- 使用資料夾

定價

使用 Amazon WorkDocs，沒有預付費用或承諾。您只需為使用中的使用者帳戶和使用的儲存空間付費。 如需詳細資訊，請參閱定價。

如何開始

要開始使用 Amazon WorkDocs，請參閱創建一個 Amazon WorkDocs 網站。

Amazon 先決條件 WorkDocs

若要設定新的 Amazon WorkDocs 網站或管理現有網站，您必須完成以下任務。

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。

Amazon 中的安全 WorkDocs

雲端安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足組織最為敏感的安全要求。

安全是 AWS 與您共同的責任。共同的責任模型 將此描述為雲端 本身 的安全和雲端內部的安全：

- 雲端本身的安全 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也提供您可安全使用的服務。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 WorkDocs，請參閱合規計劃適用範圍的AWS服務。
- 雲端中的安全性 — 您使用的AWS服務決定了您的責任。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。本節中的主題可協助您了解如何在使用 Amazon 時套用共同的責任模型 WorkDocs。

> **Note**
>
> WorkDocs 組織中的使用者可以傳送檔案的連結或邀請，與該組織外部的使用者共同作業。不過，這只適用於使用作用中目錄連接器的站台。查看您網站的分享連結設定，然後選取最符合貴公司需求的選項。

下列主題說明如何設定 Amazon WorkDocs 以符合安全和合規目標。您也會學到如何使用其他可AWS協助您監控和保護 Amazon WorkDocs 資源的服務。

主題

- Amazon 的身份和訪問管理 WorkDocs
- Amazon 中的記錄和監控 WorkDocs
- Amazon 的合規驗證 WorkDocs
- Amazon 的韌性 WorkDocs
- Amazon 基礎設施安全 WorkDocs

Amazon 的身份和訪問管理 WorkDocs

AWS Identity and Access Management (IAM) 是一種 AWS 服務，讓管理員能夠安全地控制對 AWS 資源的存取權。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 WorkDocs 資源。IAM 是一種您可以免費使用的 AWS 服務。

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 WorkDocs。

服務使用者 — 如果您使用 Amazon WorkDocs 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 WorkDocs 功能完成工作時，您可能需要額外的許可。瞭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 WorkDocs，請參閱疑難排解 Amazon WorkDocs 身分和存取。

服務管理員 — 如果您負責公司的 Amazon WorkDocs 資源，則可能擁有對 Amazon 的完全訪問權限 WorkDocs。判斷服務使用者應存取哪些 Amazon WorkDocs 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 WorkDocs，請參閱Amazon 如何與 IAM 合 WorkDocs 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 WorkDocs。若要檢視可在 IAM 中使用的 Amazon WorkDocs 身分型政策範例，請參閱。Amazon WorkDocs 基於身份的政策示例

使用身分驗證

身分驗證是使用身分憑證登入 AWS 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者身分，或擔任 IAM 角色進行 驗證 (登入至 AWS)。

您可以使用透過身分來源 AWS IAM Identity Center 提供的憑證，以聯合身分登入 AWS。(IAM Identity Center) 使用者、貴公司的單一登入身分驗證和您的 Google 或 Facebook 憑證都是聯合身分的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。您 AWS 藉由使用聯合進行存取時，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。如需有關登入至 AWS 的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

如果您是以程式設計的方式存取 AWS，AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以便使用您的憑證透過密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，您必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的簽署 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) 以提高帳戶的安全。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)。

IAM 使用者和群組

IAM 使用者是您 AWS 帳戶 中的一種身分，具備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。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#rotate-credentials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。您無法以群組身分登入。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過程變得更為容易。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 中的一種身分，具備特定許可。它類似 IAM 使用者，但不與特定的人員相關聯。您可以在 AWS Management Console 中透過切換角色來暫時取得 IAM 角色。您可以透過呼叫

AWS CLI 或 AWS API 操作，或是使用自訂 URL 來取得角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的使用 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 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並取得由角色定義的許可。如需有關聯合角色的詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-idp.html中的為第三方身分供應商建立角色。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。
- 跨帳户存取權 – 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。角色是授予跨帳户存取權的主要方式。但是，針對某些 AWS 服務，您可以將政策直接連接到資源 (而非使用角色作為代理)。如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源類型政策的差異。
- 跨服務存取 – 有些 AWS 服務 會使用其他 AWS 服務 中的功能。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。
  - 轉發存取工作階段 (FAS)：當您使用 IAM 使用者或角色在 AWS 中執行動作時，系統會將您視為主體。當您使用某些服務時，您可能會執行一個動作，而該動作之後會在不同的服務中啟動另一個動作。FAS 使用主體的許可呼叫 AWS 服務，搭配請求 AWS 服務 以向下游服務發出請求。只有在服務收到需要與其他 AWS 服務 或資源互動才能完成的請求之後，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色：服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務 服務。
  - 服務連結角色 – 服務連結角色是一種連結到 AWS 服務 的服務角色類型。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 AWS 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。
- 在 Amazon EC2 上執行的應用程式 – 針對在 EC2 執行個體上執行並提出 AWS CLI 和 AWS API 請求的應用程式，您可以使用 IAM 角色來管理暫時憑證。這是在 EC2 執行個體內儲存存取金鑰的較好方式。如需指派 AWS 角色給 EC2 執行個體並提供其所有應用程式使用，您可以建立連接到執行個

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。如需詳細資訊，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。

如需了解是否要使用 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

您可以透過建立政策並將其附加到 AWS 身分或資源，在 AWS 中控制存取。政策是 AWS 中的一個物件，當其和身分或資源建立關聯時，便可定義其許可。AWS 會在主體 (使用者、根使用者或角色工作階段) 發出請求時評估這些政策。政策中的許可，決定是否允許或拒絕請求。大部分政策以 JSON 文件形式儲存在 AWS 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。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。若要授與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。具備該政策的使用者便可以從 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。受管政策則是獨立的政策，您可以將這些政策附加到 AWS 帳戶 中的多個使用者、群組和角色。受管政策包含 AWS 管理政策和客戶管理政策。如需瞭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。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主體可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

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

存取控制清單

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 Simple Storage Service (Amazon S3)、AWS WAF 和 Amazon VPC 是支援 ACL 的服務範例。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 支援其他較少見的政策類型。這些政策類型可設定較常見政策類型授與您的最大許可。

- 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。
- 服務控制政策 (SCP) – SCP 是 JSON 政策，可指定 AWS Organizations 中組織或組織單位 (OU) 的最大許可。AWS Organizations 服務可用來分組和集中管理您企業所擁有的多個 AWS 帳戶。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個 AWS 帳戶根使用者。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。

> **Note**
>
> Amazon WorkDocs 不支援 Slack Organizations 的服務控制政策。

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。如需瞭解 AWS 在涉及多種政策類型時如何判斷是否允許一項請求，請參閱 IAM 使用者指南中的政策評估邏輯。

Amazon 如何與 IAM 合 WorkDocs 作

在您使用 IAM 管理對 Amazon 的存取權限之前 WorkDocs，您需要了解哪些 IAM 功能可以與 Amazon 搭配使用 WorkDocs。若要深入瞭解 Amazon WorkDocs 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 WorkDocs身份的政策
- Amazon WorkDocs 資源型政策
- 基於 Amazon WorkDocs 標籤的授權
- Amazon WorkDocs IAM 角色

Amazon 基於 WorkDocs身份的政策

使用 IAM 身分型原則，您可以指定允許或拒絕的動作。Amazon WorkDocs 支持特定的操作。若要了解 JSON 政策中使用的所有元素，請參閱 IAM 使用者指南中的 IAM 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，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。政策動作的名稱通常會和相關聯的 AWS API 操作相同。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些操作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與執行相關聯操作的許可。

Amazon 中的政策動作會在動作之前 WorkDocs 使用下列前置詞：`workdocs:`例如，若要授予某人執行 Amazon WorkDocs `DescribeUsers` API 操作的權限，您可以在他們的政策中包含該`workdocs:DescribeUsers`動作。政策陳述式必須包含 `Action` 或 `NotAction` 元素。Amazon WorkDocs 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": [
      "workdocs:DescribeUsers",
      "workdocs:CreateUser"
```

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

```
"Action": "workdocs:Describe*"
```

> **Note**
>
> 若要確保回溯相容性，請包括zocalo動作。例如：
>
> ```
> "Action": [
> "zocalo:*",
> "workdocs:*"
> ],
> ```

若要查看 Amazon WorkDocs 動作清單，請參閱 IAM 使用者指南 WorkDocs中由 Amazon 定義的動作。

資源

Amazon WorkDocs 不支持在政策中指定資源 ARN。

條件索引鍵

Amazon WorkDocs 不提供任何服務特定的條件金鑰，但確實支援使用某些全域條件金鑰。若要查看 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的 AWS 全域條件內容索引鍵。

範例

若要檢視 Amazon WorkDocs 身分型政策的範例，請參閱。Amazon WorkDocs 基於身份的政策示例

Amazon WorkDocs 資源型政策

Amazon WorkDocs 不支持以資源為基礎的政策。

基於 Amazon WorkDocs 標籤的授權

Amazon WorkDocs 不支援標記資源或根據標籤控制存取。

Amazon WorkDocs IAM 角色

IAM 角色是您 AWS 帳戶中具備特定許可的實體。

使用 Amazon 臨時登入資料 WorkDocs

我們強烈建議您使用臨時登入資料來登入聯盟、擔任 IAM 角色或擔任跨帳戶角色。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 WorkDocs 支持使用臨時登入資料

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 WorkDocs 不支援服務連結角色。

服務角色

此功能可讓服務代表您擔任服務角色。此角色可讓服務存取其他服務中的資源，以代表您完成動作。服務角色會出現在您的 IAM 帳戶中，且由該帳戶所擁有。這表示 IAM 管理員可以變更此角色的許可。不過，這樣可能會破壞此服務的功能。

Amazon WorkDocs 不支持服務角色。

Amazon WorkDocs 基於身份的政策示例

> **Note**
>
> 為了獲得更高的安全性，請盡可能建立聯合身分使用者而非 IAM 使用者。

依預設，IAM 使用者和角色沒有建立或修改 Amazon WorkDocs 資源的權限。他們也無法使用 AWS Management Console、AWS CLI 或 AWS API 執行任務。IAM 管理員必須建立 IAM 政策，授予使用者和角色在指定資源上執行特定 API 操作的所需許可。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。

> **Note**
>
> 若要確保回溯相容性，請在您的政策中加入zocalo動作。例如：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
            "zocalo:*",
            "workdocs:*"
            ],
            "Resource": "*"
        }
    ]
}
```

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 WorkDocs 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 WorkDocs 資源
- 更多 Amazon WorkDocs 身分識別政策範例

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 WorkDocs 資源。這些動作可能會讓您的 AWS 帳戶 產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並朝向最低權限許可的目標邁進：如需開始授予許可給使用者和工作負載，請使用 AWS 受管政策，這些政策會授予許可給許多常用案例。它們可在您的 AWS 帳戶 中使用。我

們建議您定義特定於使用案例的 AWS 客戶管理政策，以便進一步減少許可。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的 AWS 受管政策。

- 套用最低許可許可 – 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予對服務動作的存取權，前提是透過特定AWS 服務 (例如 AWS CloudFormation)使用條件。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。
- 需要多重要素驗證 (MFA)：如果存在需要 AWS 帳戶中 IAM 使用者或根使用者的情況，請開啟 MFA 提供額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

有關 IAM 中最佳實務的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 最佳安全實務。

使用 Amazon WorkDocs 控制台

若要存取 Amazon WorkDocs 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查看AWS帳戶中 Amazon WorkDocs 資源的詳細信息。如果您建立的身分型政策限制比最低所需權限更嚴格，則主控台將無法如 IAM 使用者或角色實體的預期運作。

為確保這些實體可以使用 Amazon WorkDocs 主控台，請同時將下列AWS受管政策附加到實體。如需附加政策的詳細資訊，請參閱 IAM 使用者指南中的新增許可至使用者。

- AmazonWorkDocsFullAccess
- AWSDirectoryServiceFullAccess
- 亚马逊 FullAccess

這些政策授予使用者對 Amazon WorkDocs 資源、AWS Directory Service 操作和 Amazon EC2 操作的完整存取權，以便使用 WorkDocs 者能夠正常運作。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許其最基本主控台許可。反之，只需允許存取符合您嘗試執行之 API 操作的動作就可以了。

允許使用者檢視他們自己的許可

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

允許使用者以唯讀方式存取 Amazon WorkDocs 資源

下列AWS受管AmazonWorkDocsReadOnlyAccess政策授予 IAM 使用者對 Amazon WorkDocs 資源的唯讀存取權。該政策使用戶可以訪問所有 Amazon WorkDocs `Describe` 操作。必須存取兩個

Amazon EC2 作業，因此 Amazon 才 WorkDocs 能取得 VPC 和子網路的清單。存取 AWS Directory Service `DescribeDirectories` 操作是必要的，如此才能取得有關您的 AWS Directory Service 目錄的資訊。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workdocs:Describe*",
                "ds:DescribeDirectories",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

更多 Amazon WorkDocs 身分識別政策範例

IAM 管理員可以建立其他政策，以允許 IAM 角色或使用者存取 Amazon WorkDocs API。如需詳細資訊，請參閱 Amazon WorkDocs 開發人員指南中的管理應用程式的身份驗證和存取控制。

疑難排解 Amazon WorkDocs 身分和存取

使用下列資訊協助您診斷和修正使用 Amazon WorkDocs 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 WorkDocs
- 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 WorkDocs 資源

我沒有授權在 Amazon 執行操作 WorkDocs

若 AWS Management Console 告知您並未獲得執行動作的授權，您必須聯絡您的管理員以取得協助。您的管理員是提供您使用者名稱和密碼的人員。

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 WorkDocs。

有些 AWS 服務 允許您傳遞現有的角色至該服務，而無須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 WorkDocs。但是，該動作要求服務具備服務角色授與的許可。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。

如需任何協助，請聯絡您的 AWS 管理員。您的管理員提供您的登入憑證。

我想允許我AWS帳戶以外的人訪問我的 Amazon WorkDocs 資源

您可以建立一個角色，讓其他帳戶中的使用者或您的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 WorkDocs 支援這些功能，請參閱Amazon 如何與 IAM 合 WorkDocs 作。
- 如需了解如何存取您擁有的所有 AWS 帳戶 所提供的資源，請參閱《IAM 使用者指南》中的將存取權提供給您所擁有的另一個 AWS 帳戶 中的 IAM 使用者。
- 如需了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方擁有的 AWS 帳戶。
- 如需了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源型政策的差異。

Amazon 中的記錄和監控 WorkDocs

Amazon WorkDocs 網站管理員可以檢視和匯出整個網站的活動摘要。他們也可以用AWS CloudTrail來從 Amazon WorkDocs 主控台擷取事件。

主題

匯出整個網站的活動摘要

管理員可檢視並匯出整個站台的活動意見回饋。若要使用此功能，您必須先安裝 Amazon WorkDocs 小幫手。要安裝 Amazon WorkDocs 配套，請參閱 Amazon 的應用程序和集成 WorkDocs。

檢視並匯出整個站台的活動意見回饋

1. 在 Web 應用程式中，選擇 [活動]。
2. 選擇「篩選」，然後移動整個網站的活動滑桿來開啟篩選器。
3. 選擇 Activity Type (活動類型) 篩選條件，然後視需要選擇 Date Modified (修改的日期) 設定，然後選擇 Apply (套用)。
4. 當篩選過的活動意見回饋結果顯示時，以檔案、資料夾或使用者名稱進行搜尋以縮小您的結果。您也可以視需要新增或移除篩選條件。
5. 選擇 Export (匯出) 以匯出活動意見回饋為 `.csv` 與 `.json` 檔案至您的桌面。系統會將檔案匯出至下列其中一個位置：

   - 視窗 — 您電腦的 WorkDocsDownloads[下載] 資料夾中的資料夾
   - macOS – `/users/username/WorkDocsDownloads/folder`

   匯出的檔案會反映您套用的任何篩選器。

> **Note**
>
> 非管理員的使用者僅能檢視並匯出他們自己內容的活動意見回饋。如需詳細資訊，請參閱 Amazon WorkDocs 使用者指南中的檢視活動摘要。

用AWS CloudTrail來記錄 Amazon WorkDocs API 呼叫

您可以使用AWS CloudTrail; 記錄 Amazon WorkDocs API 調用。 CloudTrail 提供 Amazon 中使用者、角色或AWS服務所採取的動作記錄 WorkDocs。 CloudTrail 以事件 WorkDocs 形式擷取 Amazon 的所有 API 呼叫，包括來自 Amazon WorkDocs 主控台的呼叫，以及從程式碼呼叫到 Amazon WorkDocs 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 WorkDocs。如果您不建立追蹤，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。

所收集的資訊 CloudTrail 包括要求、提出要求的 IP 位址、提出要求的使用者，以及要求日期。

若要取得有關的更多資訊 CloudTrail，請參閱AWS CloudTrail使用者指南。

Amazon WorkDocs 信息 CloudTrail

CloudTrail 在您創建AWS帳戶時，您的帳戶已啟用。在 Amazon 中發生活動時 WorkDocs，該活動會與事件歷史記錄中的其他AWS服務 CloudTrail 事件一起記錄在事件中。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

如需AWS帳戶中持續記錄事件 (包括 Amazon 的活動) WorkDocs，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。根據預設，當您在主控台建立權杖時，權杖會套用到所有區域。線索會記錄來自 AWS 分割區中所有區域的事件，然後將所有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 WorkDocs 動作都由記錄下來， CloudTrail 並記錄在 Amazon WorkDocs API 參考中。例如，呼叫`CreateFolder`、`DeactivateUser`和`UpdateDocument`區段會在 CloudTrail 記錄檔中產生項目。

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

- 該請求是否使用根或 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。
- 該請求是否由另一項 AWS 服務提出。

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

了解 Amazon WorkDocs 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。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

Amazon WorkDocs 會產生不同類型的 CloudTrail 項目，這些項目來自控制平面，以及來自資料平面的項目。兩者之間的重要區別在於控制平面項目的使用者身分識別是 IAM 使用者。資料平面項目的使用者身分是 Amazon 目 WorkDocs 錄使用者。

> **Note**
>
> 為了獲得更高的安全性，請盡可能建立聯合身分使用者而非 IAM 使用者。

像密碼、身分驗證字符、檔案評論及檔案內容這類敏感資訊是在日誌項目中修訂。這些在日誌中顯示為隱藏 _ 到安全 _ 原因。 CloudTrail 這些在日誌中顯示為隱藏 _ 到安全 _ 原因。 CloudTrail

下列範例顯示 Amazon 的兩個記 CloudTrail 錄項目 WorkDocs：第一筆記錄用於控制平面動作，第二個記錄用於資料平面動作。

```
{
  Records : [
    {
      "eventVersion" : "1.01",
      "userIdentity" :
      {
        "type" : "IAMUser",
        "principalId" : "user_id",
        "arn" : "user_arn",
        "accountId" : "account_id",
        "accessKeyId" : "access_key_id",
        "userName" : "user_name"
      },
      "eventTime" : "event_time",
```

```
      "eventSource" : "workdocs.amazonaws.com",
      "eventName" : "RemoveUserFromGroup",
      "awsRegion" : "region",
      "sourceIPAddress" : "ip_address",
      "userAgent" : "user_agent",
      "requestParameters" :
      {
        "directoryId" : "directory_id",
        "userSid" : "user_sid",
        "group" : "group"
      },
      "responseElements" : null,
      "requestID" : "request_id",
      "eventID" : "event_id"
    },
    {
      "eventVersion" : "1.01",
      "userIdentity" :
      {
        "type" : "Unknown",
        "principalId" : "user_id",
        "accountId" : "account_id",
        "userName" : "user_name"
      },
      "eventTime" : "event_time",
      "eventSource" : "workdocs.amazonaws.com",
      "awsRegion" : "region",
      "sourceIPAddress" : "ip_address",
      "userAgent" : "user_agent",
      "requestParameters" :
      {
        "AuthenticationToken" : "**-redacted-**"
      },
      "responseElements" : null,
      "requestID" : "request_id",
      "eventID" : "event_id"
    }
  ]
}
```

Amazon 的合規驗證 WorkDocs

要了解 AWS 服務 是否在特定法規遵循方案範圍內，請參閱法規遵循方案範圍內的 AWS 服務，並選擇您感興趣的法規遵循方案。如需一般資訊，請參閱 AWS 法規遵循方案。

您可使用 AWS Artifact 下載第三方稽核報告。如需詳細資訊，請參閱 AWS Artifact 中的下載報告。

您使用 AWS 服務 時的法規遵循責任取決於資料的敏感度、您的公司的合規目標，以及適用的法律和法規。AWS 提供以下資源協助您處理法規遵循事宜：

- 安全與合規快速入門指南 – 這些部署指南討論在 AWS 上部署以安全及合規為重心的基準環境的架構考量和步驟。
- Amazon Web Services 的 HIPAA 安全與法規遵循架構：本白皮書說明公司可如何運用 AWS 來建立符合 HIPAA 規定的應用程式。

> **Note**
>
> 並非全部的 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源：這組手冊和指南可能適用於您的產業和位置。
- AWS 客戶合規指南：透過合規的角度了解共同的責任模式。這份指南橫跨多個架構 (包含國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準組織 (ISO))，總結保護 AWS 服務的最佳實務並將指導方針對應至安全控制。
- AWS Config 開發人員指南中的使用規則評估資源：AWS Config 服務可評估您的資源組態對於內部實務、業界準則和法規的合規狀態。
- AWS Security Hub – 此 AWS 服務 可供您全面檢視 AWS 中的安全狀態。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- AWS Audit Manager – 此 AWS 服務 可協助您持續稽核 AWS 使用情況，以簡化管理風險與法規與業界標準的法規遵循方式。

Amazon 的韌性 WorkDocs

AWS 全球基礎設施是以 AWS 區域與可用區域為中心建置的。AWS區域提供多個分開且隔離的實際可用區域，它們以低延遲、高輸送量和高度備援聯網功能相互連結。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。

如需有關 AWS 區域與可用區域的更多相關資訊，請參閱 AWS 全球基礎設施。

Amazon 基礎設施安全 WorkDocs

作為受管服務，Amazon WorkDocs 受到AWS全球網路安全程序的保護。如需詳細資訊，請參閱 IAM 使用者指南中的 AWS Identity and Access Management 中的基礎設施安全和AWS架構中有關安全、身分和合規的最佳實務。

您可以使用AWS已發佈的 API 呼叫 WorkDocs 透過網路存取 Amazon。用戶端必須支援傳輸層安全性 (TLS) 1.2，我們建議您使用 TLS 1.3。客戶還必須支持具有完美前向保密的密碼套件，例如短暫的迪菲-赫爾曼或橢圓曲線短暫迪菲-赫爾曼。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 以產生暫時安全憑證以簽署請求。

開始使用 Amazon WorkDocs

Amazon WorkDocs 使用目錄來存放和管理使用者及其文件的組織資訊。反過來，當您佈建該網站時，您可以將目錄附加到網站。執行此操作時，名為 Auto enable 的 Amazon WorkDocs 功能會將目錄中的使用者以受管使用者的身分新增到網站，這表示他們不需要單獨的登入資料即可登入您的網站，而且他們可以在檔案上共用和協作。每個用戶都有 1 TB 的存儲空間，除非他們購買更多。

您不再需要手動新增和啟用使用者，但您仍然可以。您也可以隨時變更使用者角色和權限。有關這樣做的更多信息邀請和管理亞馬遜 WorkDocs 用戶，請參閱本指南後面的。

如果您需要建立目錄，您可以：

- 建立 Simple AD 目錄。
- 建立 AD Connector 目錄以連線到您的內部部署目錄。
- 使 Amazon WorkDocs 能夠與現有的AWS目錄一起工作。
- 讓 Amazon 為您 WorkDocs 創建一個目錄。

您也可以建立 AD 目錄與 AWS Managed Microsoft AD 目錄之間的信任關係。

> **Note**
>
> 如果您屬於符合性計劃 (例如 PCI、FedRAMP 或 DoD)，則必須設定AWS Managed Microsoft AD目錄以符合法規要求。本節中的步驟說明如何使用現有的 Microsoft AD 目錄。如需建立 Microsoft AD 目錄的相關資訊，請參閱《Direc AWStory Service 管理指南》中的 AWS 受管 Microsoft AD。

目錄

創建一個 Amazon WorkDocs 網站

以下各節中的步驟說明如何設定新的 Amazon WorkDocs 網站。

任務

開始之前

在創建 Amazon WorkDocs 網站之前，您必須具備以下物品。

- 一個用於創建和管理 Amazon WorkDocs 網站的AWS帳戶。但是，用戶不需要AWS帳戶即可連接和使用 Amazon WorkDocs。如需詳細資訊，請參閱 Amazon 先決條件 WorkDocs。
- 如果您打算使用 Simple AD，就必須符合《AWS Directory Service管理指南》中的 S imple AD 先決條件中指定的先決條件。
- 一個AWS Managed Microsoft AD目錄 (如果您屬於 PCI、FedRAMP 或 DoD 等合規性計畫)。本節中的步驟說明如何使用現有的 Microsoft AD 目錄。如需建立 Microsoft AD 目錄的相關資訊，請參閱《Direc AWStory Service 管理指南》中的 AWS 受管 Microsoft AD。
- 管理員的設定檔資訊，包括名字和姓氏，以及電子郵件地址。

創建一個 Amazon WorkDocs 網站

請按照以下步驟在幾分鐘內創建一個 Amazon WorkDocs 網站。

要創建 Amazon WorkDocs 網站

1. 在以下位置打開 Amazon WorkDocs 控制台 https://console.aws.amazon.com/zocalo/。
2. 在主控台首頁的 [建立 WorkDocs 網站] 底下，選擇 [立即開始使用]。

   -或是-

   在瀏覽窗格中，選擇 [我的網站]，然後在 [管理您的網 WorkDocs 站] 頁面上選擇 [建立 WorkDocs 網站]。

   接下來會發生什麼取決於您是否有目錄。

   - 如果您有目錄，則會顯示 [選取目錄] 頁面，讓您選擇現有的目錄或建立目錄。
   - 如果您沒有目錄，[設定目錄類型] 頁面隨即顯示，讓您建立簡易 AD 或 AD Connector 目錄

   下列步驟說明如何執行這兩項工作。

若要使用現有的目錄

1. 開啟「可用目錄」清單，然後選擇您要使用的目錄。
2. 選擇 Enable directory (啟用目錄)。

建立 目錄

1. 重複上述步驟 1 和 2。

   在這一點上，您做什麼取決於您是要使用 Simple AD 還是創建 AD Connector。

   使用 Simple AD

   a. 選擇 S imple AD，然後選擇「下一步」。

      [建立 Simple AD 網站] 頁面隨即出現。

   b. 在 [存取點] 下的 [網站 URL] 方塊中，輸入網站的 URL。
   c. 在 [設定 WorkDocs 管理員] 底下，輸入管理員的電子郵件地址、名字和姓氏。
   d. 視需要完成 [目錄詳細資料] 和 [VPC 組態] 下的選項。
   e. 選擇創建 Simple AD 網站。

   建立 AD 連接器目錄

   a. 選擇 AD Connector，然後選擇「下一步」。

      [建立 AD Connector 網站] 頁面隨即出現。

   b. 完成「目錄詳細資訊」下的所有欄位。
   c. 在 [存取點] 下方的 [網站 URL] 方塊中，輸入您網站的 URL。
   d. 視需要完成 VPC 組態下的選用欄位。
   e. 選擇 [建立 AD Connector 網站]。

Amazon 執 WorkDocs 行以下操作：

- 如果您在上面的步驟 4 中選擇了代表我設定 VPC，Amazon WorkDocs 會為您建立 VPC。VPC 中的目錄會儲存使用者和 Amazon WorkDocs 網站資訊。

- 如果您使用 Simple AD，Amazon WorkDocs 會建立一個目錄使用者，並將該使用者設定為 Amazon WorkDocs 管理員。如果您建立 AD Connector 目錄，Amazon 會 WorkDocs 設定您以 WorkDocs 管理員身分提供的現有目錄使用者。
- 如果您使用現有的目錄，Amazon WorkDocs 會提示您輸入 Amazon WorkDocs 管理員的使用者名稱。使用者必須是目錄的成員。

> **Note**
>
> Amazon WorkDocs 不會通知用戶有關新網站的信息。您需要將 URL 傳達給他們，並讓他們知道他們不需要單獨的登錄即可使用該網站。

啟用單一登入

AWS Directory Service允許用戶 WorkDocs 從加入 Amazon 註冊的同一目錄的計算機訪問 Amazon WorkDocs ，而無需單獨輸入憑據。Amazon WorkDocs 管理員可以使用AWS Directory Service主控台啟用單一登入。如需詳細資訊，請參閱《AWS Directory Service管理指南》中的單一登入。

Amazon WorkDocs 管理員啟用單一登入後，Amazon 網 WorkDocs 站使用者可能還需要修改其網頁瀏覽器設定，以允許單一登入。如需詳細資訊，請參閱《AWS Directory Service管理指南》中的 IE 和 Chrome 的單一登入以及 Firefox 的單一登入。

啟用多重因素認證

您可以使用AWS目錄服務主控台 https://console.aws.amazon.com/directoryservicev2/，為 AD Connector 目錄啟用多重要素驗證。若要啟用 MFA，您必須擁有本身是一種遠端驗證撥號使用者服務 (RADIUS) 伺服器的 MFA 解決方案，或者擁有已在您的內部部署基礎設施上實作之 RADIUS 伺服器的 MFA 外掛程式。您的 MFA 解決方案必須實作使用者從硬體裝置，或是手機等裝置上執行的軟體所取得的一次性密碼 (OTP)。

RADIUS 是業界標準的用戶端/伺服器通訊協定，提供驗證、授權和帳戶管理，讓使用者能夠連線到網路服務。AWS 受管 Microsoft AD 包含一個 RADIUS 用戶端，可連接到您實作 MFA 解決方案的 RADIUS 伺服器。您的 RADIUS 伺服器驗證使用者名稱和 OTP 代碼。如果您的 RADIUS 伺服器成功驗證使用者，則 AWS 受管 Microsoft AD 會根據 AD 對使用者進行驗證。AD 驗證成功後，使用者就可以存取 AWS 應用程式。AWS 受管 Microsoft AD RADIUS 用戶端與 RADIUS 伺服器之間的通訊需要您設定 AWS 安全群組，以便透過連接埠 1812 進行通訊。

如需詳細資訊，請參閱 AWSDirectory Service 管理指南中的為 AWS 受管 Microsoft AD 啟用多因素身份驗證。

> **Note**
>
> Simple AD 目錄無法使用多重要素驗證。

將使用者提升為管理員

您可以使用 Amazon WorkDocs 主控台將使用者升級為管理員。請遵循下列步驟。

將使用者提升為管理員

1. 在以下位置打開 Amazon WorkDocs 控制台 https://console.aws.amazon.com/zocalo/。
2. 在導覽窗格中，選擇 [我的網站]。

   「管理您的 WorkDocs 網站」頁面隨即出現。
3. 選取所需網站旁邊的按鈕，選擇「動作」，然後選擇「設定管理員」。

   設定 WorkDocs 管理員] 對話方塊隨即出現。
4. 在「使用者名稱」方塊中，輸入您要升級之人員的使用者名稱，然後選擇「設定管理員」。

您也可以使用 Amazon WorkDocs 網站管理員控制台降級管理員。如需更多詳細資訊，請參閱 編輯使用者。

WorkDocs 從AWS控制台管理 Amazon

您可以使用這些工具來管理您的 Amazon WorkDocs 網站：

- 控AWS制台位於 https://console.aws.amazon.com/zocalo/。
- 網站管理員控制面板，適用於所有 Amazon 網 WorkDocs 站的管理員。

這些工具中的每一個都提供了一組不同的動作，本節中的主題說明AWS控制台提供的動作。如需有關網站管理員控制台的資訊，請參閱 WorkDocs 從網站管理控制面板管理 Amazon。

設定網站管理員

如果您是系統管理員，您可以授與使用者存取網站控制台及其提供的動作。

若要設定管理員

1. 在 https://console.aws.amazon.com/zocalo/ 打開 Amazon WorkDocs 控制台。
2. 在導覽窗格中，選擇 [我的網站]。

   [管理您的 WorkDocs 網站] 頁面隨即出現，並顯示您的網站清單。
3. 選擇您要為其設定管理員的網站旁邊的按鈕。
4. 開啟 [動作] 清單，然後選擇 [設定管理員]。

   設定 WorkDocs 管理員] 對話方塊隨即出現。
5. 在「使用者名稱」方塊中，輸入新管理員的名稱，然後選擇「設定管理員」。

重新傳送邀請電郵

您可以隨時重新傳送邀請電子郵件。

重新傳送邀請電子郵件

1. 在 https://console.aws.amazon.com/zocalo/ 打開 Amazon WorkDocs 控制台。
2. 在導覽窗格中，選擇 [我的網站]。

   [管理您的 WorkDocs 網站] 頁面隨即出現，並顯示您的網站清單。

3. 選擇您要重新傳送電子郵件的網站旁邊的按鈕。
4. 開啟 [動作] 清單，然後選擇 [重新傳送邀請電

   頁面頂端會顯示綠色橫幅中的成功訊息。

管理多重要素驗證

您可以在建立 Amazon WorkDocs 網站後啟用多因素身份驗證。如需身分驗證的相關詳細資訊，請參閱 啟用多重因素認證。

設定網站網址

> **Note**
>
> 如果您遵循中的網站建立程序開始使用 Amazon WorkDocs，則輸入了網站 URL。因此，Amazon WorkDocs 使設置站點 URL 命令不可用，因為您只能設置一次 URL。只有在部署 Amazon WorkSpaces 並將其與 Amazon 集成時，才需要執行以下步驟 WorkDocs。Amazon WorkSpaces 集成過程讓您輸入序列號而不是站點 URL，因此您必須在完成集成後輸入 URL。有關整合 Amazon WorkSpaces 和 Amazon 的更多信息， WorkDocs 請參閱 Amazon 用 WorkSpaces 戶指南 WorkDocs中的「與集成」。

若要設定網站 URL

1. 在 https://console.aws.amazon.com/zocalo/ 打開 Amazon WorkDocs 控制台。
2. 在導覽窗格中，選擇 [我的網站]。

   [管理您的 WorkDocs 網站] 頁面隨即出現，並顯示您的網站清單。
3. 選擇您與 Amazon 集成的網站 WorkSpaces。網址包含 Amazon WorkSpaces 執行個體的目錄 ID，例如 https://{directory_id}.awsapps.com。
4. 選擇該 URL 旁邊的按鈕，開啟「動作」 清單，然後選擇「設定網站 URL」。

   這時系統顯示「設置站點 URL」對話框。
5. 在「網站 URL」方塊中，輸入網站的 URL，然後選擇「設定網站 URL」。
6. 在 [管理您的 WorkDocs 網站] 頁面上，選擇 [重新整理] 以查看新的 URL。

管理通知

> **Note**
>
> 為了獲得更高的安全性，請盡可能建立聯合身分使用者而非 IAM 使用者。

通知可讓 IAM 使用者或角色呼叫 CreateNotificationSubscriptionAPI，您可以使用這些 API 來設定自己的端點，以處理 WorkDocs 傳送的 SNS 訊息。如需有關通知的詳細資訊，請參閱 Amazon WorkDocs 開發人員指南中的設定 IAM 使用者或角色的通知。

您可以建立和刪除通知，下列步驟說明如何執行這兩項工作。

> **Note**
>
> 若要建立通知，您必須具有 IAM 或角色 ARN。若要尋找您的 IAM ARN，請執行下列動作：
>
> 1. 開啟位於 https://console.aws.amazon.com/iam/ 的 IAM 主控台。
> 2. 在導覽列中，選取 [使用者]。
> 3. 選取您的使用者名稱。
> 4. 在「摘要」下，複製您的 ARN。

若要建立通知

1. 在 https://console.aws.amazon.com/zocalo/ 打開 Amazon WorkDocs 控制台。
2. 在導覽窗格中，選擇 [我的網站]。

   [管理您的 WorkDocs 網站] 頁面隨即出現，並顯示您的網站清單。
3. 選擇所需網站旁邊的按鈕。
4. 開啟 [動作] 清單並選擇 [管理通知]。

   「管理通知」頁面隨即出現。
5. 選擇 Create notification (建立通知)。
6. 在 [新增通知] 對話方塊中，輸入您的 IAM 或角色 ARN，然後選擇 [建立通知]。

刪除通知

1. 在 https://console.aws.amazon.com/zocalo/ 打開 Amazon WorkDocs 控制台。
2. 在導覽窗格中，選擇 [我的網站]。

   [管理您的 WorkDocs 網站] 頁面隨即出現，並顯示您的網站清單。
3. 選擇具有您要刪除之通知的網站旁邊的按鈕。
4. 開啟 [動作] 清單並選擇 [管理通知]。
5. 在「管理通知」頁面上，選擇您要刪除的通知旁邊的按鈕，然後選擇「刪除通知」。

刪除網站

您可以使用 Amazon WorkDocs 控制台刪除網站。

> **Warning**
>
> 刪除網站時會遺失所有檔案。若您確定已不再需要此資訊，始可刪除網站。

若要刪除網站

1. 在 https://console.aws.amazon.com/zocalo/ 打開 Amazon WorkDocs 控制台。
2. 在導覽列中，選擇 [我的網站]。

   [管理您的 WorkDocs 網站] 頁面隨即出現。
3. 選擇您要刪除的網站旁邊的按鈕，然後選擇「刪除」。

   這時系統顯示「刪除站點 URL」對話框。
4. 選擇性地選擇「同時刪除使用者目錄」。

   > **Important**
   >
   > 如果您沒有為 Amazon 提供自己的目錄 WorkDocs，我們會為您創建一個目錄。刪除 Amazon WorkDocs 網站時，除非您刪除該目錄或將其用於其他 AWS 應用程式，否則我們建立的目錄需支付費用。如需定價資訊，請參閱 AWS Directory Service 定價。
5. 在「網站 URL」方塊中，輸入網站 URL，然後選擇「刪除」。

該網站將會立即刪除且再也無法使用。

WorkDocs 從網站管理控制面板管理 Amazon

您可以使用這些工具來管理您的 Amazon WorkDocs 網站：

- 網站管理員控制面板，可供所有 Amazon 網 WorkDocs 站的管理員使用，並在以下主題中進行說明。
- 控 AWS 制台位於 https://console.aws.amazon.com/zocalo/。

這些工具中的每一個都提供了一組不同的操作。本節中的主題說明網站管理員控制台提供的動作。如需控制台中可用工作的相關資訊，請參閱 WorkDocs 從AWS控制台管理 Amazon。

偏好的語言設定

您可以指定電子郵件通知的語言。

若要變更語言設定

1. 在 My Account (我的帳戶) 中選擇 Open admin control panel (開啟管理員控制面板)。
2. 在 Preferred Language Settings (偏好語言設定)，請選擇您偏好使用的語言。

Hancom Online Editing 和 Office Online

從管理控制面板啟用或禁用 Hancom 在線編輯和 Office 在線設置。如需詳細資訊，請參閱 啟用協作編輯。

儲存

指定新使用者接收的儲存量。

若要變更儲存設定

1. 在 My Account (我的帳戶) 中選擇 Open admin control panel (開啟管理員控制面板)。
2. 針對 Storage (儲存)，選擇 Change (變更)。
3. 在 Storage Limit (儲存限制) 對話框中，選擇給予新使用者有限或無限的儲存。
4. 選擇 Save Changes (儲存變更)。

變更儲存設定僅會影響設定變更後新增的使用者。它並不會變更配置給現有使用者的儲存量。若要為現有使用者變更儲存限制，請參閱 編輯使用者。

IP 允許清單

Amazon WorkDocs 網站管理員可以新增 IP 允許清單設定，將網站存取限制在允許的 IP 位址範圍內。每個網站最多可以新增 500 個 IP 允許清單設定。

> **Note**
>
> IP Allow List (IP 允許清單) 目前僅適用於 IPv4 地址。目前不支援 IP 位址拒絕清單。

將 IP 範圍加入至 IP Allow List (IP 允許清單)

1. 在 My Account (我的帳戶) 中選擇 Open admin control panel (開啟管理員控制面板)。
2. 針對 IP Allow List (IP 允許清單)，選擇 Change (變更)。
3. 在輸入 CIDR 值中，輸入 IP 位址範圍的無類別網域間路由 (CIDR) 區塊，然後選擇新增。
   - 若要允許從單一 IP 地址存取，請指定 /32 做為 CIDR 字首。
4. 選擇 Save Changes (儲存變更)。
5. 使用者若從 IP Allow List (IP 允許清單) 所列的 IP 地址連線至您的網站，即會獲得允許存取。凡是嘗試從未經授權的 IP 地址連線至您網站的使用者都將收到未經授權的回應。

> **Warning**
>
> 如果您所輸入的 CIDR 值令您無法使用目前的 IP 地址存取網站，便會出現警告訊息。您若選擇繼續保持目前的 CIDR 值，則將無法使用目前的 IP 地址存取網站。欲復原此動作必須聯絡 AWS Support 尋求協助。

安全性 — 簡單的 ActiveDirectory網站

本主題說明簡易 ActiveDirectory網站的各種安全性設定。如果您管理使用 ActiveDirectory 連接器的網站，請參閱下一節。

使用安全性設定

1. 選擇用戶 WorkDocs 端右上角的設定檔圖示。

2. 在管理員下，選擇打開管理控制面板。
3. 向下捲動至「安全性」並選擇「變更」

[原則設定] 對話方塊隨即出現。下表列出簡單 ActiveDirectory 網站的安全性設定。

設定	Description
在「選擇可分享連結的設定」下方，選取下列其中一項：	
不允許整個網站或公開可分享的連結	停用所有使用者的連結共用。
允許用戶創建站點範圍內的可共享鏈接，但不允許他們創建公共可共享的鏈接	限制只有網站成員的連結共用。受管理的使用者可以建立這種類型的連結。
允許用戶創建站點範圍內的可共享鏈接，但只有高級用戶可以創建公共可共享的鏈接	受管理的使用者可以建立整個網站的連結，但只有進階使用者可以建立公開連結 公共鏈接允許訪問互聯網上的任何人。
所有受管理的使用者都可以建立整個網站且可公開共用的	受管理的使用者可建立公開連結。
在「自動啟用」下，選取或清除核取方塊。	
允許您目錄中的所有使用者在首次登入您的 WorkDocs 網站時自動啟用。	當使用者第一次登入您的網站時，會自動啟用他們。
在「應允許誰邀請新使用者到您的 WorkDocs 網站」下，選取下列其中一項：	
只有管理員可以邀請新使用者。	只有管理員可以邀請新使用者。
用戶可以通過與他們共享文件或文件夾從任何地方邀請新用戶。	允許使用者透過與這些使用者共用檔案或資料夾來邀請新使用者。

設定	Description
使用者可以透過與他們共用檔案或資料夾，邀請來自幾個特定網域的新使用者。	使用者可與來自特定領域的新人員分享檔案與資料夾來邀請他們。
在「為新使用者設定角色」下，選取或清除核取方塊。	
您目錄中的新使用者將是受管理的使用者 (預設為來賓使用者)	自動將目錄中的新使用者轉換為受管理的使用者。

4. 完成後，選擇「儲存變更」。

安全性 — ActiveDirectory 連接器網站

本主題說明 ActiveDirectory 連接器站台的各種安全性設定。如果您管理使用 Simple 的網站 ActiveDirectory，請參閱上一節。

使用安全性設定

1. 選擇用戶 WorkDocs 端右上角的設定檔圖示。

2. 在管理員下，選擇打開管理控制面板。
3. 向下捲動至「安全性」並選擇「變更」

[原則設定] 對話方塊隨即出現。下表列出並說明 ActiveDirectory連接器站台的安全性設定。

設定	Description
在「選擇可分享連結的設定」下方，選取下列其中一項：	
不允許整個網站或公開可分享的連結	選取此選項後，會停用所有使用者的連結共用。
允許用戶創建站點範圍內的可共享鏈接，但不允許他們創建公共可共享的鏈接	限制只有網站成員的連結共用。受管理的使用者可以建立這種類型的連結。

設定	Description
允許用戶創建站點範圍內的可共享鏈接，但只有高級用戶可以創建公共可共享的鏈接	受管理的使用者可以建立整個網站的連結，但只有進階使用者可以建立公開連結 公共鏈接 允許訪問互聯網上的任何人。
所有受管理的使用者都可以建立整個網站且可公開共用的	受管理的使用者可建立公開連結。

在「自動啟用」下，選取或清除核取方塊。

允許您目錄中的所有使用者在首次登入您的 WorkDocs 網站時自動啟用。	當使用者第一次登入您的網站時，會自動啟用他們。

在「誰應該被允許激活您 WorkDocs 站點中的目錄用戶？ 中，選取下列其中一項：

只有管理員可以從您的目錄啟動新使用者。	只允許管理員啟動新的目錄使用者。
用戶可以通過與他們共享文件或文件夾從您的目錄激活新用戶。	允許使用者透過與目錄使用者共用檔案或資料夾來啟動目錄使用者。
用戶可以通過與他們共享文件或文件夾來激活來自一些特定域的新用戶。	使用者只能共用特定網域中使用者的檔案或資料夾。當您選擇此選項時，您必須輸入網域。

在「誰應該被允許邀請新使用者到您的 WorkDocs 網站？ 中，選取下列其中一項：

Share with external users (與外部使用者共享) **Note** 下列選項只會在您選擇此設定後顯示。	Enables administrators and users to invite new external users to your Amazon WorkDocs site.
Only administrators can invite new external users (只有管理員可以邀請新外部使用者)	只有管理員可以邀請外部使用者。
所有受管理使用者皆可邀請新使用	可讓受管理的使用者邀請外部使用者。
只有進階使用者可以邀請新的外部使用者。	僅允許進階使用者邀請新的外部使用者。

設定	Description
在為新使用者設定角色下，選取一個或兩個選項。	
您目錄中的新使用者將是受管理的使用者 (預設為來賓使用者)	自動將目錄中的新使用者轉換為受管理的使用者。
New external users will be Managed users (they are Guest users by default) (新外部使用者將會是「受控」使用者 (依預設，他們會是訪客使用者))	自動將新外部使用者轉換為受管理使用者。

4. 完成後，選擇「儲存變更」。

復原筒保留

當使用者刪除檔案時，Amazon 會將檔案 WorkDocs 儲存在使用者的資源回收筒中 30 天。之後，Amazon 會將檔案 WorkDocs 移至暫存回復資料匣 60 天，然後將其永久刪除。只有系統管理員才能看到暫存復原資料匣。透過變更網站範圍的資料保留原則，網站管理員可以將復原 Bin 保留期限變更為至少為零天且最多 365 天。

若要變更復原筒保留期限

1. 在 My Account (我的帳戶) 中選擇 Open admin control panel (開啟管理員控制面板)。
2. 在 Recovery bin retention (復原筒保留期限) 旁，選擇 Change (變更)。
3. 輸入在復原筒中保留檔案的天數，然後選擇 [儲存]。

> **Note**
>
> 預設保留期間為 60 天。您可以使用 0-365 天的時間。

管理員可以在 Amazon 永久 WorkDocs 刪除使用者檔案之前，從復原筒還原檔案。

若要還原使用者檔案

1. 在 My Account (我的帳戶) 中選擇 Open admin control panel (開啟管理員控制面板)。
2. 在 Manage Users (管理使用者) 下，選擇使用者資料夾圖示。

3. 在 Recovery bin (復原筒) 下，選取要還原的檔案，然後選擇 Recover (復原) 圖示。
4. 針對 Restore file (還原檔案)，選擇欲還原檔案的位置，然後選擇 Restore (還原)。

管理使用者設定

您可為使用者管理設定，包括變更使用者角色與邀請、啟用或停用使用者。如需更多詳細資訊，請參閱邀請和管理亞馬遜 WorkDocs 用戶。

將 Amazon WorkDocs 驅動器部署到多台計算機

如果您有加入網域之機器隊列，則可使用組原則物件 (GPO) 或 System Center Configuration Manager (SCCM) 來安裝 Amazon WorkDocs Drive 客户端。您可以從https://amazonworkdocs.com/en/clients。

隨着您的需要，Amazon WorkDocs Drive 需要在 443 連接埠上為所有 AWS IP 地址提供 HTTPS 存取權限。您還需要確認您的目標系統符合 Amazon WorkDocs 驅動器的安裝要求。如需詳細資訊，請參閱「」安裝 Amazon WorkDocs Drive中的Amazon WorkDocs User Guide。

> **Note**
>
> 作為使用 GPO 或 SCCM 時的最佳做法，請在用户登錄後安裝 Amazon WorkDocs 硬盤客户端。

Amazon WorkDocs Drive 的 MSI 安裝程式支援下列選用安裝參數：

- **SITEID**— 在註冊期間為使用者預先填入 Amazon WorkDocs 網站資訊。例如：`SITEID=####`。
- **DefaultDriveLetter**— 預先填入要用於掛載 Amazon WorkDocs Drive 的磁碟機代號。例如：`DefaultDriveLetter=W`。 請記住，每個用户必須具有不同的驅動器號。此外，用户可以在首次啟動 Amazon WorkDocs 驅動器後更改驅動器名稱，但不能更改驅動器號。

以下示例在沒有用户界面和不重新啟動的情況下部署 Amazon WorkDocs 驅動器。請注意，它使用 MSI 文件的默認名稱：

```
msiexec /i "AWSWorkDocsDriveClient.msi" SITEID=###### _ ## _ ID
DefaultDriveLetter=#######REBOOT=REALLYSUPPRESS /norestart /qn
```

邀請和管理亞馬遜 WorkDocs 用戶

根據預設，當您在網站建立期間附 WorkDocs 加目錄時，Amazon 中的自動啟用功能會將該目錄中的所有使用者以受管使用者的身分新增到新網站。

在中 WorkDocs，受管理的使用者不需要使用個別的認證登入。他們可以在文件上共享和協作，並且自動擁有 1 TB 的存儲空間。不過，如果您只想在目錄中新增部分使用者，則可以關閉自動啟用，接下來章節中的步驟會說明如何執行此操作。

此外，您還可以邀請、啟用或停用使用者，以及變更使用者角色和設定。您也可以將使用者提升為管理員。如需提升使用者的詳細資訊，請參閱將使用者提升為管理員。

您可以在 Amazon WorkDocs Web 用戶端的管理控制台中執行這些任務，以下各節中的步驟將說明如何進行。但是，如果您是 Amazon 的新手 WorkDocs，請花幾分鐘時間瞭解各種使用者角色，然後再深入研究管理任務。

內容

使用者角色概觀

Amazon WorkDocs 定義了下列使用者角色。您可以透過編輯使用者設定檔來變更使用者的角色。如需詳細資訊，請參閱編輯使用者。

- Admin (管理員)：擁有整個網站管理許可的付費使用者，包括使用者管理與網站設定組態。如需有關如何將使用者提升為管理員的詳細資訊，請參閱將使用者提升為管理員。

- 進階使用者：具有管理員特殊權限集的付費使用者。如需如何為進階使用者設定權限的詳細資訊，請參閱安全性 — 簡單的 ActiveDirectory網站和安全性 — ActiveDirectory 連接器網站。
- 使用者：可以在 Amazon WorkDocs 網站中儲存檔案並與其他人共同作業的付費使用者。
- Guest user (訪客使用者)：非付費使用者，只能檢視檔案。您可以將來賓使用者升級為使用者、進階使用者或系統管理員角色。

> **Note**
>
> 當您變更訪客使用者的角色時，您會執行無法回復的單次動作。

亞馬遜 WorkDocs 還定義了這些額外的用戶類型。

WS 使用者

具有指派的使用者 WorkSpaces WorkSpace。

- 訪問所有亞馬遜 WorkDocs 功能
- 50 GB 預設儲存空間 (可付費升級為 1 TB)
- 無每月費用

已升級的 WS 使用者

具有指派 WorkSpaces WorkSpace 及升級儲存裝置的使用者。

- 訪問所有亞馬遜 WorkDocs 功能
- 預設儲存空間為 1 TB (pay-as-you-go依據可提供額外儲存空間)
- 需支付每月費用

亞馬遜 WorkDocs 用戶

沒有分配的活躍亞馬遜 WorkDocs 用戶 WorkSpaces WorkSpace。

- 訪問所有亞馬遜 WorkDocs 功能
- 預設儲存空間為 1 TB (pay-as-you-go依據可提供額外儲存空間)
- 需支付每月費用

啟動管理控制面板

您可以使用 Amazon WorkDocs Web 用戶端中的管理控制台來關閉和開啟自動啟用，以及變更使用者角色和設定。

要打開管理控制面板

1. 選擇用戶 WorkDocs 端右上角的設定檔案圖示。

2. 在管理員下，選擇打開管理控制面板。

> **Note**
>
> 某些控制面板選項在雲目錄和連接的目錄之間有所不同。

停用自動啟用

當您不想將目錄中的所有使用者新增至新網站，以及想要為邀請到新網站的使用者設定不同的權限和角色時，請關閉 [自動啟用]。當您關閉自動啟用時，您也可以決定誰有權邀請新使用者加入網站，包括目前使用者、進階使用者或管理員。這些步驟介紹如何執行這兩項工作。

停用自動啟用

1. 選擇用戶 WorkDocs 端右上角的設定檔案圖示。

2. 在管理員下，選擇打開管理控制面板。
3. 向下捲動至「安全性」並選擇「變更」

   [原則設定] 對話方塊隨即出現。
4. 在 [自動啟用] 下，清除 [允許目錄中的所有使用者在首次登入您的 WorkDocs 網站時自動啟用] 旁邊的核取方塊。

在 [應允許誰啟動您網站中的目錄使用者] 下 WorkDocs 方的選項會變更。您可以讓目前的使用者邀請新使用者，也可以將這項功能授予進階使用者或其他管理員。

5. 選取選項，然後選擇「儲存變更」。

重複步驟 1-4 以重新啟用自動啟用。

管理連結共用

本主題介紹如何管理連結共用。Amazon WorkDocs 用戶可以通過共享鏈接來共享他們的文件和文件夾。他們可以在組織內外共用檔案連結，但只能在內部共用資料夾連結。身為管理員，您可以管理誰可以分享連結。

啟用連結分享

1. 選擇用戶 WorkDocs 端右上角的設定檔案圖示。

2. 在管理員下，選擇打開管理控制面板。
3. 向下捲動至「安全性」並選擇「變更」

   [原則設定] 對話方塊隨即出現。
4. 在「選擇可分享連結的設定」下方，選取一個選項：

   - [不允許整個網站] 或 [公開可共用的連結] — 停用所有使用者的連結共用。
   - 允許用戶創建站點範圍內的可共享鏈接，但不允許他們創建公共可共享的鏈接-將鏈接共享限制為只有網站成員。受管理的使用者可以建立這種類型的連結。
   - 允許使用者建立整個網站的可共用連結，但只有進階使用者才能建立公開可共用的連結 — 受管理的使用者可以建立整個網站的連結，但只有進階使用者可以建立公開連結。公用連結允許存取任何人。
   - 所有受管理的使用者都可以建立整個網站且可公開共用的連結 — 受管理的使用者可以建立公開
5. 選擇 Save Changes (儲存變更)。

在啟用自動啟用的情況下控制使用

當您啟用自動啟用時，請記住，它預設為開啟，您可以讓使用者邀請其他使用者。您可將權限授與下列其中一個：

- 所有使用者
- 進階使用者
- 管理員。

您也可以完全停用權限，而這些步驟會說明如何進行。

設定邀請權限

1. 選擇用戶 WorkDocs 端右上角的設定檔案圖示。

2. 在管理員下，選擇打開管理控制面板。
3. 向下捲動至「安全性」並選擇「變更」

   [原則設定] 對話方塊隨即出現。
4. 在「應允許誰啟用您 WorkDocs網站中的目錄使用者」下方，選取「與外部使用者共用」核取方塊，選取核取方塊下方的其中一個選項，然後選擇「儲存變更」。

   -或是-

   如果您不想讓任何人邀請新使用者，請清除核取方塊，然後選擇「儲存變更」。

邀請新使用者

您可以邀請新使用者加入目錄。您也可以讓現有使用者邀請新使用者。如需詳細資訊，請參閱本指南安全性 — ActiveDirectory 連接器網站中的安全性 — 簡單的 ActiveDirectory網站和。

若要邀請新使用者

1. 選擇用戶 WorkDocs 端右上角的設定檔案圖示。

2. 在管理員下，選擇打開管理控制面板。
3. 在 Manage Users (管理使用者) 下，選擇Invite Users (邀請使用者)。
4. 在 [邀請使用者] 對話方塊中，針對您要邀請誰？ 」下方，輸入受邀者的電子郵件地址，然後選擇「傳送」。為每個邀請重複上述步驟。

Amazon WorkDocs 會向每位收件者傳送邀請電子郵件。該郵件包含有關如何創建亞馬遜 WorkDocs 帳戶的鏈接和說明。邀請連結會在 30 天後到期。

編輯使用者

您可以變更使用者資訊和設定。

編輯使用者

1. 選擇用戶 WorkDocs 端右上角的設定檔案圖示。

2. 在管理員下，選擇打開管理控制面板。
3. 在 Manage Users (管理使用者) 底下，選擇使用者名稱旁邊的鉛筆圖示 (✎)。
4. 在 Edit User (編輯使用者) 對話方塊中，您可以編輯以下選項：

   First Name (名字) (僅限 Cloud Directory)

   使用者的名字。

   Last Name (姓氏) (僅限 Cloud Directory)

   使用者的姓氏。

   狀態

   指定使用者為「作用中」或「非作用中」。如需詳細資訊，請參閱停用使用者。

Role

指定某人是使用者還是管理員。您也可以升級或降級已 WorkSpaces WorkSpace指派給他們的使用者。如需詳細資訊，請參閱使用者角色概觀。

儲存

指定現有使用者的儲存限制。

5. 選擇 Save Changes (儲存變更)。

停用使用者

您可以將使用者的狀態變更為「非作用中」來停用其存取權。

將使用者狀態變更為 Inactive (非作用中)

1. 選擇用戶 WorkDocs 端右上角的設定檔案圖示。

2. 在管理員下，選擇打開管理控制面板。
3. 在 Manage Users (管理使用者) 底下，選擇使用者名稱旁邊的鉛筆圖示 ( )。
4. 選擇 Inactive (非作用中)，然後選擇 Save Changes (儲存變更)。

停用的使用者無法存取您的 Amazon WorkDocs 網站。

> **Note**
>
> 將使用者變更為非作用中狀態並不會從您的 Amazon WorkDocs 網站刪除其檔案、資料夾或意見反應。不過，您可以將非作用中使用者的檔案和資料夾傳輸給作用中的使用者。如需詳細資訊，請參閱轉移文件所有權。

刪除待處理用戶

您可以刪除處於擱置中狀態的 Simple AD、AWS受管理的 Microsoft 和 AD Connector 使用者。若要刪除其中一位使用者，請選擇使用者名稱旁邊的垃圾桶圖示 (🗑)。

您的 Amazon WorkDocs 網站必須始終至少有一個活躍用戶，該用戶不是來賓用戶。如果您需要刪除所有使用者，請刪除整個網站。

不建議您刪除已註冊的使用者。相反，您應該將用戶從活動狀態切換為非活動狀態，以防止他們訪問您的 Amazon WorkDocs 網站。

轉移文件所有權

您可以將作用中使用者的檔案與資料夾轉移至作用中的使用者。如需如何停用使用者的詳細資訊，請參閱停用使用者。

> ⚠ Warning
>
> 您無法復原此動作。

轉移文件所有權

1. 選擇用戶 WorkDocs 端右上角的設定檔案圖示。

2. 在管理員下，選擇打開管理控制面板。
3. 在 Manage Users (管理使用者) 底下，搜尋非作用中的使用者。
4. 在非使用中使用者名稱旁，選擇鉛筆圖示 (✎)。
5. 選擇轉移文件所有權，然後輸入新擁有者的電子郵件地址。
6. 選擇 Save Changes (儲存變更)。

下載使用者清單

若要從管理員控制台下載使用者清單，您必須安裝 Amazon WorkDocs 小幫手。要安裝亞馬遜 WorkDocs 配套，請參閱亞馬遜的應用程序和集成 WorkDocs。

下載使用者清單

1. 選擇用戶 WorkDocs 端右上角的設定檔案圖示。

2. 在管理員下，選擇打開管理控制面板。
3. 在 Manage Users (管理使用者) 底下，選擇Download user (下載使用者)。
4. 對於 Download user (下載使用者)，使用下列選項之一以匯出使用者清單 `.json` 檔案至您的桌面：

   - 所有使用者
   - 訪客使用者
   - WS 使用者
   - 使用者
   - 進階使用者
   - 管理員
5. WorkDocs 將檔案儲存到下列其中一個位置：

   - Windows – `Downloads/WorkDocsDownloads`
   - macOS – *`hard drive`*`/users/`*`username`*`/WorkDocsDownloads/folder`

> **Note**
>
> 下載可能需要一點時間。此外，下載的文件不會降落在您的文件/~users夾中。

如需這些使用者角色的詳細資訊，請參閱 使用者角色概觀。

分享及協同合作

您的用戶可以通過發送鏈接或邀請來共享內容。如果您啟用外部共用，使用者也可以與外部使用者共同作業。

Amazon 通過使用許可來 WorkDocs 控制對文件夾和文件的訪問。系統會根據使用者的角色套用權限。

目錄

分享連結

使用者可以選擇 [共用連結]，快速複製和共用 Amazon WorkDocs 內容的超連結給組織內外的同事和外部使用者。當使用者分享連結時，可以將其設定為允許下列其中一個存取選項：

- Amazon WorkDocs 網站的所有成員都可以搜尋、檢視和評論檔案。
- 任何擁有連結的人，即使是不是 Amazon WorkDocs 網站成員的人，都可以檢視檔案。此連結選項會將權限限制為僅供檢視。

擁有檢視權限的收件人僅能檢視檔案。註解權限讓使用者能夠註解和執行更新或刪除操作，例如上傳新檔案或刪除現有文件。

依據預設，所有受管使用者皆可建立公有連結。若要變更此設定，請從您的管理員控制面板更新 Security (安全性) 設定。如需詳細資訊，請參閱 WorkDocs 從網站管理控制面板管理 Amazon。

以邀請進行共用

當您啟用邀請分享時，您的網站使用者可以透過傳送邀請電子郵件與個別使用者或群組共用檔案或資料夾。邀請包含分享內容的連結，受邀者可以開啟共享的檔案或資料夾。受邀者也可以與其他網站成員以及外部使用者共用這些檔案或資料夾。

您可以為每個受邀使用者設定權限等級。您也可以建立團隊資料夾，以邀請方式與您建立的目錄群組分享。

> **Note**
>
> 共用邀請不包含巢狀群組的成員。若要加入這些成員，您必須將他們新增至「透過邀請分享」清單。

如需詳細資訊，請參閱 WorkDocs 從網站管理控制面板管理 Amazon。

外部分享

外部共用可讓 Amazon WorkDocs 網站的受管使用者共用檔案和資料夾，並與外部使用者協同合作，而不會產生額外成本。網站使用者可以與外部使用者共用檔案和資料夾，而不需要收件者是 Amazon WorkDocs 網站的付費使用者。當您啟用外部共用時，使用者可以輸入他們想要共用的外部使用者的電子郵件地址，並設定適當的檢視者共用權限。新增外部使用者時，權限會限制為僅限檢視者，而其他權限則無法使用。外部使用者將收到電子郵件通知，內含分享檔案或資料夾的連結。選擇連結會將外部使用者導向該網站，在該網站中輸入他們的登入資料以登入 Amazon WorkDocs。他們可以在 Shared with me (與我共享) 檢視畫面中看到分享的檔案或資料夾。

檔案擁有者可隨時針對檔案或資料夾，修改其外部使用者的分享權限或移除存取權限。網站管理員必須啟用網站的外部分享，受管使用者才能與外部使用者分享內容。Guest users (訪客使用者) 若要成為作者群或共同擁有者，必須由網站管理員將其升級為 User (使用者) 層級。如需詳細資訊，請參閱 使用者角色概觀。

根據預設，外部分享是開啟的，所有使用者皆可邀請外部使用者。若要變更此設定，請從您的管理員控制面板更新 Security (安全性) 設定。如需詳細資訊，請參閱 WorkDocs 從網站管理控制面板管理 Amazon。

許可

亞馬遜WorkDocs使用權限來控制對資料夾和檔案的存取。權限是根據使用者角色來套用。

目錄

- 不在共享文件夾中的文件的權限

使用者角色

用戶角色控制文件夾和文件權限。您可以在資料夾層級套用下列使用者角色：

- 資料夾擁有— 資料夾或檔案的擁有者。
- 資料夾共同擁有— 擁有者指定為資料夾或檔案共同擁有者的使用者或群組。
- 文件夾貢獻者— 擁有無限制訪問文件夾的人。
- 資料夾檢視— 對資料夾具有有限存取權限 (唯讀權限) 的人員。

您可以在個別檔案層級套用下列使用者角色：

- 擁有者— 檔案的擁有者。
- 共同擁有者— 擁有者指定為檔案共同擁有者的使用者或群組。
- 撰稿人— 有人允許對文件提供反饋。
- 檢視器— 對檔案具有有限存取權限 (唯讀權限) 的人員。
- 匿名查看器— 組織外的未註冊使用者，可檢視已使用外部檢視連結共用的檔案。除非特別指出，否則匿名檢視者的許可會與檢視者相同。

已分享資料夾的許可

下列權限適用於共用資料夾的使用者角色：

> **Note**
>
> 套用至資料夾的權限也會套用至該資料夾中的子資料夾和檔案。

- 檢視— 檢視共用資料夾的內容。
- 檢視子資料夾— 檢視子資料夾。
- 查看股票— 檢視共用資料夾的其他使用者。
- 下載資料夾— 下載一個文件夾.
- 新增子資料夾— 新增子資料夾。
- 分享— 與其他使用者共用頂層資料夾。

- 撤銷股份— 撤銷頂級文件夾的共享。
- 刪除子資料夾— 刪除子資料夾。
- 刪除頂層資料夾— 刪除頂層共用資料夾。

	檢視	檢視子資料夾	查看股票	下載資料夾	新增子資料夾	Share (分享)	撤銷股份	刪除子資料夾	刪除頂層資料夾
資料夾擁有	✓	✓	✓	✓	✓	✓	✓	✓	✓
資料夾共同擁有	✓	✓	✓	✓	✓	✓	✓	✓	✓
文件夾貢獻者	✓	✓	✓	✓	✓				
資料夾檢視	✓	✓	✓	✓					

共享資料夾中檔案的權限

下列權限適用於共用資料夾中檔案的使用者角色：

- 註解— 將反饋添加到文件中。
- 刪除— 刪除共享資料夾中的檔案。
- 重命名— 重命名文件。
- 上传— 上傳檔案的新版本。
- 下載— 下載一個文件. 這是預設許可。您可以使用檔案屬性來允許或拒絕下載共用檔案的功能。
- 防止下載— 防止下載檔案。

> **Note**
>
> - 當您選取此選項時，使用者檢視權限仍然可以下載文件。若要避免這種情況發生，請開啟共用資料夾並清除允許下載您不希望這些用戶下載的每個文件的設置。

- 當 MP4 檔案的擁有者或共同擁有者不允許下載該檔案時，貢獻者和檢視者將無法在 Amazon 上播放該檔案WorkDocs網頁用戶端。

- 分享— 與其他使用者共用檔案。
- 撤銷分享— 撤銷文件的共享。
- 檢視— 查看共享文件夾中的文件。
- 查看股票— 檢視檔案共用的其他使用者。
- 檢視註解— 查看其他用戶的反饋。
- 檢視活動— 查看文件的活動歷史記錄。
- 檢視版本— 檢視檔案的先前版本。
- 刪除版本— 刪除檔案的一個或多個版本。
- 復原版本— 恢復文件的一個或多個已刪除版本。
- 查看所有私人評論— 擁有者/共同擁有者可以看到文件的所有私人註解，即使他們並未回覆其註解。

	標註	Delete	重新命名	上傳	下載	防止下載	Share (分享)	撤銷股份	檢視	查看股票	檢視註解	檢視活動	檢視版本	刪除版本	復原版本	檢視所有私人評論**
檔案擁有者*	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
資料夾	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	標註	Delete	重新命名	上傳	下載	防止下載	Share (分享)	撤銷股份	檢視	查看股票	檢視註解	檢視活動	檢視版本	刪除版本	復原版本	檢視所有私人評論**
擁有																
資料夾共同擁有	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
文件夾貢獻者	✓			✓	✓				✓	✓	✓	✓	✓			
資料夾檢視					✓				✓	✓						

	標註	Delete	重新命名	上傳	下載	防止下載	Share (分享)	撤銷股份	檢視	查看股票	檢視註解	檢視活動	檢視版本	刪除版本	復原版本	檢視所有私人評論**
匿名查看器									✓	✓						

* 在此情況下，檔案擁有者是已將檔案的原始版本上傳至已分享資料夾的人員。此角色的許可只會套用至所擁有的檔案，而非已分享資料夾中的所有檔案。

** 檔案擁有者/共同擁有者可以查看所有私人意見。作者群只能查看本身為其意見回覆的私人意見。

不在共享文件夾中的文件的權限

下列權限適用於不在共用資料夾中的檔案的使用者角色：

- 註解— 將反饋添加到文件中。
- 刪除— 刪除檔案。
- 重命名— 重命名文件。
- 上传— 上傳檔案的新版本。
- 下載— 下載一個文件. 這是預設許可。您可以使用檔案屬性來允許或拒絕下載共用檔案的功能。
- 防止下載— 防止下載檔案。

> **Note**
>
> 當 MP4 檔案的擁有者或共同擁有者不允許下載該檔案時，貢獻者和檢視者將無法在 Amazon 上播放該檔案WorkDocs網頁用戶端。

- 分享— 與其他使用者共用檔案。
- 撤銷股份— 撤銷文件的共享。
- 檢視— 檢視檔案。
- 查看股票— 檢視檔案共用的其他使用者。
- 檢視註解— 查看其他用戶的反饋。
- 檢視活動— 查看文件的活動歷史記錄。
- 檢視版本— 檢視檔案的先前版本。
- 刪除版本— 刪除檔案的一個或多個版本。
- 復原版本— 恢復文件的一個或多個已刪除版本。

	標註	Delete	重新命名	上傳	下載	防止下載	Share (分享)	撤銷股份	檢視	查看股票	檢視註解	檢視活動	檢視版本	刪除版本	復原版本
擁有者	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
共同擁有者	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Contributor (作者群)	✓			✓	✓				✓	✓	✓	✓	✓		
Viewer (檢視者)					✓				✓	✓					

	標註	Delete	重新命名	上傳	下載	防止下載	Share (分享)	撤銷股份	檢視	查看股票	檢視註解	檢視活動	檢視版本	刪除版本	復原版本
匿名查看器									✓	✓					

啟用協作編輯

您可以使用管理員控制台中的「線上編輯設定」 區段來啟用協同編輯選項。

目錄

啟用漢康 ThinkFree

您可以 ThinkFree 為您的 Amazon WorkDocs 網站啟用 Hancom，以便用戶可以從 Amazon WorkDocs 網絡應用程序創建和協作編輯 Microsoft Office 文件。如需詳細資訊，請參閱使用 Hancom ThinkFree 進行編輯。

Hancom ThinkFree 無需支付額外費用即可為 Amazon 用 WorkDocs 戶提供。不需其他授權或軟體安裝。

若要啟用漢柯姆 ThinkFree

從管理控制面板啟用 Hancom ThinkFree 編輯。

1. 在 My account (我的帳戶) 中選擇 Open admin control panel (開啟管理控制面板)。
2. 對於 Hancom Online Editing，選擇 Change (變更)。
3. 選擇 Enable Hancom Online Editing Feature (啟用 Hancom Online Editing 功能)，檢視用量條款，然後選擇 Save (儲存)。

若要停用漢柯姆 ThinkFree

從管理控制面板禁用 Hancom ThinkFree 編輯。

1. 在 My account (我的帳戶) 中選擇 Open admin control panel (開啟管理控制面板)。
2. 對於 Hancom Online Editing，選擇 Change (變更)。
3. 取消選取 Enable Hancom Online Editing Feature (啟用 Hancom Online Editing 功能) 核取方塊，然後選擇 Save (儲存)。

啟用 Open with Office Online

為您的 Amazon WorkDocs 網站啟用「使用 Office 在線打開」，以便用戶可以從 Amazon WorkDocs 網絡應用程序協作編輯 Microsoft Office 文件。

對於 Amazon WorkDocs 用戶也擁有 Microsoft Office 365 工作或學校帳戶，並具有可在辦公室在線編輯許可證的亞馬遜用戶，可以免費使用「在線辦公室」打開。如需詳細資訊，請參閱 Open with Office Online。

啟用 Open with Office Online

從 Admin control panel (管理控制面板) 啟用 Open with Office Online。

1. 在 My account (我的帳戶) 中選擇 Open admin control panel (開啟管理控制面板)。
2. 對於 Office Online，選擇 Change (變更)。
3. 選取 Enable Office Online (啟用 Office Online)，然後選擇 Save (儲存)。

停用 Open with Office Online

從 Admin control panel (管理控制面板) 停用 Open with Office Online。

1. 在 My account (我的帳戶) 中選擇 Open admin control panel (開啟管理控制面板)。
2. 對於 Office Online，選擇 Change (變更)。
3. 取消選取 Enable Office Online (啟用 Office Online) 核取方塊，然後選擇 Save (儲存)。

將文件遷移到亞馬遜 WorkDocs

Amazon WorkDocs 管理員可以使用 Amazon WorkDocs 遷移服務，將多個檔案和資料夾大規模遷移到其 Amazon WorkDocs 網站。Amazon Simple S WorkDocs torage Service 使用 Amazon Simple Storage Service (Amazon S3) 使用 Amazon S3。這可讓您將部門檔案共用和家用磁碟機或使用者檔案共用遷移到 Amazon WorkDocs。

在此過程中，Amazon 會為您 WorkDocs 提供AWS Identity and Access Management (IAM) 政策。使用此政策建立新的 IAM 角色，以授予 Amazon WorkDocs 遷移服務的存取權，以執行以下操作：

- 閱讀並列出您指定的 Amazon S3 儲存貯體。
- 讀取和寫入您指定的亞馬遜 WorkDocs 網站。

完成下列任務，將檔案和資料夾遷移到 Amazon WorkDocs。開始之前，請確認您具備下列許可：

- 您的亞馬遜 WorkDocs 網站的管理員許可
- 建立 IAM 角色的 IAM 角色的 IAM 角色

如果您的 Amazon WorkDocs 網站設定在與 WorkSpaces 叢集相同的目錄中，則必須遵循以下要求：

- 請勿將管理員用於您的亞馬遜 WorkDocs 帳戶用戶名。管理員是 Amazon 中的保留使用者角色 WorkDocs。
- 您的 Amazon WorkDocs 管理員使用者類型必須是升級版 WS 使用者。如需詳細資訊，請參閱使用者角色概觀及編輯使用者。

> **Note**
>
> 移轉到 Amazon 時，會保留目錄結構、檔案名稱和檔案內容 WorkDocs。檔案所有權和許可不予保留。

任務

- 步驟 1：準備要移轉的內容
- 步驟 2：將檔案上傳到 Amazon S3
- 步驟 3：排程遷移

步驟 1：準備要移轉的內容

準備您要移轉的內容

1. 在您的 Amazon WorkDocs 網站上，在「我的文件」下，建立要將檔案和資料夾遷移到其中的資料夾。
2. 請確認以下內容：
   - 來源資料夾包含的檔案和子資料夾不超過 100,000 個。如果您超過該限制，移轉會失敗。
   - 個別檔案不得超過 5 TB。
   - 每個檔案名稱包含 255 個字元或更少。Amazon WorkDocs 雲端硬碟只會顯示完整目錄路徑不超過 260 個字元的檔案。

> **Warning**
>
> 嘗試遷移名稱包含以下字元的檔案或資料夾，可能會導致錯誤並造成遷移程序停止。如果發生這種情況，請選擇 Download report (下載報告) 以下載日誌，其中會列出錯誤、無法遷移的檔案以及成功遷移的檔案。

- 尾隨空格 — 例如：檔案名稱結尾的額外空格。
- 開始或結束時的週期 — 例如：`.file`、`file.ppt`、`.`、`..`、或`file.`
- 開頭或結尾處的波浪符號 — 例如：`file.doc~`、`~file.doc`、或`~$file.doc`
- 檔案名稱結尾為`.tmp` — 例如：`file.tmp`
- 檔案名稱與這些區分大小寫的詞彙完全相符 —`Microsoft User Data`、`Outlook`、`filesThumbs.db`、`.`、或`Thumbnails`
- 包含任何這些字元的檔案名稱 —`*`/ (星號)、\ (正斜線)、: (反斜線)、< (冒號)、(小於)、> (大於)、? (問號)、| (垂直列/直線)、" (雙引號)，或`\202E`（字符代碼 202E）。

步驟 2：將檔案上傳到 Amazon S3

將檔案上傳到 Amazon S3

1. 在AWS帳戶中建立您要向其上傳檔案和資料夾的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。Amazon S3 儲存貯體必須在 Amazon S3 儲存貯體必須在 Amazon WorkDocs S3 儲存貯體相同的AWS帳戶和AWS區域。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用 Amazon Simple Stor age Service 使用 Amazon Simple Storage Service，
2. 將檔案上傳至上一步驟中建立的 Amazon S3 儲存貯體。建議您使AWS DataSync用您的 Amazon S3 儲存貯體的檔案和資料夾。 DataSync 提供其他追蹤、報告和同步功能。如AWS DataSync需詳細資訊，請參閱《使用指南》 DataSync中的《使用方式》和《使用身分型政策 (IAM 政策)》。AWS DataSync

步驟 3：排程遷移

完成步驟 1 和步驟 2 後，請使用 Amazon WorkDocs 遷移服務排程遷移。遷移服務最多可能需要一週的時間來處理遷移要求，並傳送電子郵件告知您可以開始遷移。如果您在收到電子郵件之前開始遷移，管理主控台會顯示一則訊息，告訴您要等待。

當您排程遷移時，您的 Amazon WorkDocs 使用者帳戶儲存空間設定會自動變更為無限制。

> **Note**
>
> 遷移超出 Amazon WorkDocs 儲存限制的檔案可能會產生額外費用。如需詳細資訊，請參閱 Amazon WorkDocs 定價。

Amazon WorkDocs 遷移服務提供AWS Identity and Access Management (IAM) 政策供您用於移轉。透過此政策，您可以建立新的 IAM 角色，以授與 Amazon WorkDocs 遷移服務存取您指定之 Amazon S3 儲存貯體和 Amazon WorkDocs 網站的存取權。您也可以訂閱 Amazon SNS 電子郵件通知，以便在排程遷移請求時以及開始和結束時接收更新。

排程遷移

1. 從 Amazon 主 WorkDocs 控台選擇應用程式，移轉。
    - 如果這是您第一次存取 Amazon WorkDocs 遷移服務，系統會提示您訂閱 Amazon SNS 電子郵件通知。訂閱、在您收到的電子郵件中進行確認，然後選擇 Continue (繼續)。

2. 選擇 Create Migration (建立遷移)。
3. 針對 Source Type (來源類型)，選擇 Amazon S3。
4. 選擇 Next (下一步)。
5. 對於資料來源與驗證，在範例政策下，複製提供的 IAM 政策。
6. 使用您在上一步複製的 IAM 政策建立新的 IAM 政策和角色，如下所示：
   a. 前往網址 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
   b. 選擇 Policies (政策)、Create policy (建立政策)。
   c. 選擇 JSON 並貼上您先前複製到剪貼簿的 IAM 政策。
   d. 選擇 Review policy (檢閱政策)。輸入政策名稱及描述。
   e. 選擇 Create policy (建立政策)。
   f. 選擇 Roles (角色)、Create role (建立角色)。
   g. 選取 Another AWS account (其他 AWS 帳戶)。對於 Account ID (帳戶 ID)，輸入下列其中一個值：
      - 針對美國東部 (N. Virginia 北部) 區域，輸入`899282061130`
      - 針對美國西部 (奧勒岡) 區域，輸入`814301586344`
      - 針對亞太區域 (Singapore) Region，輸入`900469912330`
      - 針對亞太區域 (Sydney) Region，輸入`031131923584`
      - 針對亞太區域 (東京) 輸入`178752524102`
      - 對於 Europe (Ireland) Region，輸入`191921258524`
   h. 選取您建立的新政策，然後選取 Next: Review (下一步：檢閱)。如果您未看到新的問題清單，請選擇重新整理圖示。
   i. 輸入角色名稱和描述。選擇 Create Role (建立角色)。
   j. 在 Roles (角色) 頁面的 Role name (角色名稱) 下方，選擇您剛建立的角色名稱。
   k. 在 Summary (摘要) 頁面上，將 Maximum CLI/API session duration (最大 CLI/API 工作階段持續時間) 變更為 12 小時。
   l. 將 Role ARN (角色 ARN) 複製到剪貼簿以便用於下一個步驟。
7. 返回亞馬遜 WorkDocs 遷移服務。對於資料來源和驗證，在角色 ARN 下，貼上您在上一個步驟中複製的 IAM 角色中的角色 ARN。
8. 對於儲存貯體，選擇您要向其移轉檔案的 Amazon S3 儲存貯體。
9. 選擇 Next (下一步)。

10. 對於 「選取目標 WorkDocs 資料夾」，請在 Amazon 中選取要將檔案移轉 WorkDocs 至的目標資料夾。
11. 選擇 Next (下一步)。
12. 在 Review (檢閱) 下方的 Title (標題) 中，輸入遷移的名稱。
13. 選取遷移的日期和時間。
14. 選擇 Send (傳送)。

步驟 4：追蹤遷移

您可以從 Amazon 遷移服務登陸頁面追蹤 WorkDocs 遷移。要從 Amazon WorkDocs 網站訪問登陸頁面，請選擇應用程序，遷移。選擇您的遷移以檢視其詳細資訊並追蹤其進度。如果需要取消遷移也可以選擇 Cancel Migration (取消遷移)，或選擇 Update (更新) 以更新遷移的時間軸。遷移完成後，您可以選擇 Download report (下載報告) 下載記錄已成功遷移檔案、失敗或錯誤的日誌。

以下遷移狀態提供您的遷移的狀態：

Scheduled (已排程)

遷移已排定但尚未開始。您可以在排定開始時間最多五分鐘之前取消遷移或更新遷移開始時間。

Migrating (遷移中)

遷移正在進行中。

Success (成功)

遷移已完成。

Partial Success (部分成功)

遷移部分完成。如需詳細資訊，請參閱遷移摘要並下載提供的報告。

失敗

遷移失敗。如需詳細資訊，請參閱遷移摘要並下載提供的報告。

已取消

遷移已取消。

步驟 5：清除資源

移轉完成後，請刪除您從 IAM 主控台建立的移轉政策和角色。

刪除 IAM 政策和角色

1. 前往網址 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
2. 選擇 Policies (政策)。
3. 搜尋並選取您建立的政策。
4. 對於 Policy actions (政策動作)，請選擇 Delete (刪除)。
5. 選擇 Delete (刪除)。
6. 選擇 Roles (角色)。
7. 搜尋並選取您建立的角色。
8. 選擇 Delete role (刪除角色)、Delete (刪除)。

當排程遷移開始時，您的 Amazon WorkDocs 使用者帳戶儲存空間設定會自動變更為無限制。遷移後，您可以透過從管理員控制面板編輯使用者帳戶來變更 Storage (儲存空間) 設定。如需詳細資訊，請參閱編輯使用者。

Amazon 故障診斷 WorkDocs問題

以下資訊有助於排解 Amazon Amazon 的問題進行疑難排解 WorkDocs。

問題

無法設置我的亞馬遜 WorkDocs 網站在一個特定的AWSRegion (區域)

如果你正在建立一個新的亞馬遜 WorkDocs 網站上，在設定期間選取 AWS 區域。如需詳細資訊，請參閱開始使用 Amazon WorkDocs之下與您特定使用案例有關的教學課程。

想要設置我的亞馬遜 WorkDocs 現有 Amazon VPC 中的網站

當設置你的新亞馬遜 WorkDocs 網站，使用現有 Virtual Private Cloud (VPC) 建立目錄。亞馬遜 WorkDocs 使用此目錄來驗證使用者。

使用者必須重設其密碼

使用者可在登入畫面中選擇 Forgot password? (忘記密碼？)。

使用者意外分享敏感文件

若要撤銷該文件的存取，請選擇該文件旁邊的 Share by invite (邀請分享)，然後移除不應再存取該文件的使用者。如果文件是使用連結分享的，請選擇 Share a link (分享連結)，然後停用該連結。

使用者離開組織且未傳輸文件所有權

在管理員控制面板中，將文件擁有權轉移給其他使用者。如需詳細資訊，請參閱 轉移文件所有權。

需要部署亞馬遜 WorkDocs 開車或 Amazon Amazon (Amazon) WorkDocs 同伴多使用者

使用群組政策部署至企業中的多位使用者。如需詳細資訊，請參閱 Amazon 的身份和訪問管理 WorkDocs。有關部署亞馬遜的特定信息 WorkDocs 開車給多位使用者，請參閱將 Amazon WorkDocs 驅動器部署到多台計算機。

線上編輯無法使用

驗證你有亞馬遜 WorkDocs 配套已安裝。安裝亞馬遜 WorkDocs 同伴，請參閱亞馬遜的應用程序和集成 WorkDocs。

Amazon WorkDocs usiness

如果您是 Amazon Business 的管理員，則可以使用https://workdocs.aws/使用您的亞馬遜企業商城憑證。

若要邀請新使用者使用 Amazon Business

1. 使用您的 Amazon Business 憑證登入 https://workdocs.aws/。
2. 在 Amazon WorkDocs Business 首頁上，開啟左側的導覽窗格。
3. 選擇 Admin Settings (管理員設定)。
4. 選擇 Add people (新增人員)。
5. 在 Recipients (收件者) 中，輸入要邀請之使用者的電子郵件地址或使用者名稱。
6. (選擇性) 自訂邀請訊息。
7. 選擇 Done (完成)。

在 Amazon WorkDocs Business 上搜尋使用者

1. 使用您的 Amazon Business 憑證登入 https://workdocs.aws/。
2. 在 Amazon WorkDocs Business 首頁上，開啟左側的導覽窗格。
3. 選擇 Admin Settings (管理員設定)。
4. 在 Search users (搜尋使用者) 中，輸入使用者的名字，然後按下 **Enter**。

若要在 Amazon WorkDocs usiness 上選擇使用者角色

1. 使用您的 Amazon Business 憑證登入 https://workdocs.aws/。
2. 在 Amazon WorkDocs Business 首頁上，開啟左側的導覽窗格。
3. 選擇 Admin Settings (管理員設定)。
4. 在 People (人員) 下的該使用者旁邊，選取要指派給使用者的 Role (角色)。

刪除亞馬遜企業採購商城的 Amazon WorkDocs 上的用户

1. 使用您的 Amazon Business 憑證登入 https://workdocs.aws/。
2. 在 Amazon WorkDocs Business 首頁上，開啟左側的導覽窗格。
3. 選擇 Admin Settings (管理員設定)。

4. 在 People (人員) 下方，選擇該使用者旁的省略符號 (...)。
5. 選擇 Delete (刪除)。
6. 如果出現提示，請輸入要傳輸使用者檔案的新使用者，然後選擇 Delete (刪除)。

要新增至允許清單的 IP 位址和網域

如果您在存取 Amazon 的裝置上實作 IP 篩選 WorkDocs，將下列 IP 位址和網域新增至您的允許清單。這樣做可以使亞馬遜 WorkDocs 和 Amazon WorkDocs 驅動器連接到 WorkDocs Service (服務)

- zocal.ap-northeast-1.amazonaws.com
- zocal.ap-southeast-2.amazonaws.com
- zocal.eu-west-1.amazonaws.com
- zocal.eu-central-1.amazonaws.com
- zocal.us-east-1.amazonaws.com
- 佐卡洛。us-gov-west-amazonaws.com
- zocal.us-west-2.amazonaws.com
- awsapp.com
- amazonaws.com
- 雲前網
- 亚马逊
- 亞馬遜工作
- 控制台亚马逊
- gonaws.com us-east-1.amazonaws.com
- Firehose.us-east-1.amazonaws.com

如果您要使用 IP 位址範圍，請參閱AWSIP 地址範圍在AWS一般參考。

文件歷史紀錄

下表說明從 2018 年 2 月開始對 Amazon WorkDocs 管理指南進行的重要變更。如需有關此文件更新的通知，您可以訂閱 RSS 摘要。

變更	描述	日期
新增檔案擁有者權限	管理員現在可以提供「刪除版本」和「復原版本」權限。權限是 DeleteDocumentVersionAPI 發行版本的一部分。	2022 年 7 月 29 日
Amazon WorkDocs Backup	已從 Amazon WorkDocs 管理指南中移除 Amazon WorkDocs Backup 文件，因為該元件不再受支援。	2021 年 6 月 24 日
Amazon WorkDocs 業務管理 Amazon	Amazon 商業 WorkDocs 用 Amazon 支持管理員的用戶管理。有關更多信息，請參閱 Amazon WorkDocs 管理指南中的 Amazon 業務 WorkDocs 管理 Amazon 業務。	2020 年 3 月 26 日
將文件遷移到 Amazon WorkDocs	Amazon WorkDocs 管理員可以使用 Amazon WorkDocs 遷移服務，將多個檔案和資料夾大規模遷移到其 Amazon WorkDocs 網站。如需詳細資訊，請參閱 Amazon WorkDocs 管理指南 WorkDocs中的將檔案遷移到 Amazon。	2019 年 8 月 8 日
IP 允許清單設定	IP 允許清單設定可用於依 IP 位址範圍篩選對 Amazon WorkDocs 網站的存取。如需	2018 年 10 月 22 日

	詳細資訊，請參閱《Amazon WorkDocs 管理指南》中的 IP 允許清單設定。	
汉科姆 ThinkFree	漢康 ThinkFree 是可用的。用戶可以從 Amazon WorkDocs 網絡應用程序創建和協作編輯 Microsoft Office 文件。如需詳細資訊，請參閱 Amazon WorkDocs 管理指南 ThinkFree 中的啟用 Hancom。	2018 年 6 月 21 日
在線辦公室打開	Open with Office Online 已可使用。用戶可以從 Amazon WorkDocs 網絡應用程序協作編輯 Microsoft Office 文件。如需詳細資訊，請參閱 Amazon WorkDocs 管理指南中的啟用線上 Office 開啟。	2018 年 6 月 6 日
疑難排解	已新增故障診斷主題。如需詳細資訊，請參閱 Amazon WorkDocs 管理指南中的疑難排解 Amazon WorkDocs 問題。	2018 年 5 月 23 日
變更復原資料匣保留期	復原筒保留期間可以修改。如需詳細資訊，請參閱 Amazon WorkDocs 管理指南中的復原資料匣保留設定。	2018 年 2 月 27 日

AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 AWS 詞彙表。