使用者指南

AWS Artifact

AWS Artifact: 使用者指南

Table of Contents

什麼是 AWS Artifact？

AWS Artifact 提供隨需下載 AWS 的安全和合規文件。例如， 報告符合國際標準化組織 (ISO) 標準和支付卡產業 (PCI) 安全標準，以及系統和組織控制 (SOC) 報告。 AWS Artifact 也提供從驗證 AWS 安全控制實作和操作有效性的認證機構下載。

使用 AWS Artifact，您也可以為銷售其產品的獨立軟體供應商 (ISVs下載安全與合規文件 AWS Marketplace。如需詳細資訊，請參閱 AWS Marketplace Vendor Insights。

此外，您可以使用 AWS Artifact 來檢閱、接受和追蹤您 AWS 帳戶 組織中多個 與 AWS AWS 帳戶 的協議狀態。如需 中協議的詳細資訊 AWS Artifact，請參閱在 中管理協議 AWS Artifact。

若要示範您使用的 AWS 基礎設施和服務的安全性和合規性，您可以將 AWS Artifact 文件做為稽核成品提交給稽核人員或監管機構。您也可以使用這些稽核成品做為準則，以評估您自己的雲端架構，以及評估公司內部控制的有效性。如需稽核成品的詳細資訊，請參閱AWS Artifact FAQs。

> **Note**
>
> AWS 客戶負責開發或取得可證明其公司安全性和合規性的文件。如需詳細資訊，請參閱共同責任模型。

定價

AWS 免費提供您 AWS Artifact 文件和協議。

入門 AWS Artifact

若要開始使用 AWS Artifact，請在 AWS Artifact 主控台中試用其主要功能。在 主控台中，您可以下載 AWS 安全和合規報告、下載和接受法律協議，以及訂閱 AWS Artifact 文件的通知。

先決條件

若要使用 的功能 AWS Artifact，您必須擁有 AWS 帳戶。如需設定說明，請參閱 設定使用者指南中的設定新 AWS 帳戶 。 AWS

功能

如需使用 功能的指示 AWS Artifact，請參閱下列主題：

- 下載報告
- 管理協議
- 設定通知

在 中下載報告 AWS Artifact

您可以從 AWS Artifact 主控台下載報告。當您從 下載報告時 AWS Artifact，報告會特別為您產生，而且每個報告都有唯一的浮水印。因此，您應該只與您信任的人共用報告。請勿將報告做為電子郵件附件傳送，而且不在線上共用它們。若要共用報告，請使用安全共用服務，例如 Amazon WorkDocs。有些報告會要求您接受條款與條件，才能下載。

目錄

下載報告

若要下載報告，您必須擁有必要的許可。如需詳細資訊，請參閱中的身分和存取管理 AWS Artifact。

當您註冊 時 AWS Artifact，系統會自動授予您的帳戶下載一些報告的許可。如果您在存取時遇到問題 AWS Artifact，請遵循AWS Artifact 服務授權參考頁面上的指引。

下載報告

1. 在 https：//https://console.aws.amazon.com/artifact/ 開啟 AWS Artifact 主控台。
2. 在 AWS Artifact 首頁上，選擇檢視報告。

   在報告頁面上的報告AWS 索引標籤上，您可以存取 AWS 報告 （ 例如 SOC 1/2/3、PCI、C5 等 ）。在第三方報告索引標籤上，您可以從銷售其產品的獨立軟體供應商 (ISVs存取報告 AWS Marketplace。
3. （選用） 若要尋找報告，請在搜尋欄位中輸入關鍵字。您也可以根據個別資料欄執行目標式搜尋，包括報告標題、類別、系列和描述。例如，若要尋找雲端運算合規控制目錄 (C5) 報告，您可以使用「標題」、「包含」運算子 (:) 和術語「C5」 () 來搜尋標題欄**`Title : C5`**。
4. （選用） 如需報告的詳細資訊，請選擇報告標題以開啟其詳細資訊頁面。
5. 選取報告，然後選擇下載報告。
6. 系統可能會提示您接受要下載之特定報告的條款與條件 (接受下載報告的條款與條件)。建議您仔細閱讀條款與條件。當您完成閱讀時，請選取我已閱讀並同意條款，然後選擇接受條款並下載報告。

7. 透過 PDF 檢視器開啟下載的檔案。檢閱接受的條款與條件，並向下捲動以尋找稽核報告。報告可能將其他資訊內嵌為 PDF 文件中的附件，因此請務必檢查 PDF 檔案中的附件，以取得支援文件。如需如何檢視附件的說明，請參閱 檢視 PDF 文件中的附件。

檢視 PDF 文件中的附件

我們建議下列目前支援檢視 PDF 附件的應用程式：

Adobe Acrobat Reader

從 Adobe 網站 https：//https://get.adobe.com/reader/ 下載最新版本的 Adobe Acrobat Reader。

如需有關如何在 Acrobat Reader 中檢視 PDF 附件的說明，請參閱 Adobe Support 網站上的 PDFs中的連結和附件。

Firefox 瀏覽器

1. 從 Mozilla 網站 https：//https://www.mozilla.org/en-US/firefox/new/ 下載最新的 Firefox Web 瀏覽器。
2. 在 Firefox 的內建 PDF 檢視器中開啟 PDF 檔案。如需說明，請參閱在 Firefox 中檢視 PDF 檔案，或在 Mozilla Support 網站上選擇其他檢視器。
3. 若要在 Firefox 的內建 PDF 檢視器中檢視 PDF 附件，請選擇切換側邊欄、顯示附件。

保護您的文件

AWS Artifact 文件是機密的，應該隨時保持安全。 會為其文件 AWS Artifact 使用 AWS 共同的責任模型。這表示 AWS 負責在文件位於 AWS 雲端時確保文件安全，但您需負責在下載後確保文件安全。在下載文件之前， AWS Artifact 可能會要求您接受條款與條件。每個文件下載都有一個唯一的、可追蹤的浮水印。

您只能與公司內部、監管機構和稽核人員共用標記為機密的文件。您不被允許與您的客戶或是在您的網站上分享這些文件。我們強烈建議您使用安全的文件共享服務，例如 Amazon WorkDocs，與他人共享文件。請勿透過電子郵件傳送文件或將其上傳至不安全的網站。

故障診斷

如果您無法下載文件或收到錯誤訊息，請參閱 AWS Artifact 常見問答集中的疑難排解。

在 中管理協議 AWS Artifact

您可以使用 AWS Artifact 來檢閱和管理您 AWS 帳戶 或組織的協議。例如，受健康保險流通與責任法案 (HIPAA) 約束的公司通常需要與 簽訂商業夥伴增補合約 (BAA) AWS ，以確保受保護醫療資訊 (PHI) 受到適當的保護。在 AWS Artifact 主控台中，您可以檢閱並接受這類協議，也可以指定可合法處理 PHI AWS 帳戶 的 。

如果您使用 AWS Organizations，您可以代表 AWS 帳戶 組織中的所有人接受協議 AWS，例如與 簽訂的 BAA。協議自動涵蓋所有現有和後續成員帳戶，並可合法處理 PHI。

您也可以使用 AWS Artifact 來確認您的 AWS 帳戶 或組織已接受協議，並檢閱已接受協議的條款，以了解您的義務。如果您的帳戶或組織不再需要使用已接受的協議，您可以使用 AWS Artifact 來終止協議。如果您終止協議，但後來發現您需要它，則可以再次啟用協議。

目錄

在 AWS 帳戶 中接受 的協議 AWS Artifact

您可以使用 AWS Artifact 主控台來檢閱和接受 AWS 的 協議 AWS 帳戶。

> **Important**
>
> 接受協議之前，我們建議您諮詢法律、隱私權和合規團隊。

所需的許可

如果您是 帳戶的管理員，則可以授予 IAM 使用者和聯合身分使用者存取和管理一或多個協議的許可。在預設情況下，只有具有管理權限的使用者可以接受協議。若要接受協議，IAM 和聯合身分使用者必須擁有必要的許可。

如需詳細資訊，請參閱中的身分和存取管理 AWS Artifact。

接受與 的協議 AWS

1. 在 https：//https://console.aws.amazon.com/artifact/ 開啟 AWS Artifact 主控台。
2. 在 AWS Artifact 導覽窗格中，選擇協議。
3. 選擇 Account agreements (帳戶協議) 標籤。
4. 在 https：//https://console.aws.amazon.com/artifact/ 開啟 AWS Artifact 主控台。
5. 在導覽窗格中，選擇協議。
6. 在協議頁面上，執行下列其中一項操作：
   - 若要僅接受您帳戶的協議，請選擇帳戶協議索引標籤。
   - 若要代表您的組織接受協議，請選擇組織協議索引標籤。
7. 選取協議，然後選擇下載協議。

   隨即顯示接受 NDA 下載報告對話方塊。
8. 您必須先接受保密協議 AWS Artifact (AWS Artifact NDA) 的條款，才能下載您選擇的協議。

   a. 在接受 NDA 下載報告對話方塊中，檢閱 AWS Artifact NDA。

   b. （選用）若要列印 AWS Artifact NDA 的副本（或將其儲存為 PDF)，請選擇列印 NDA。

   c. 選取我已閱讀並同意 NDA 的所有條款。

   d. 若要接受 AWS Artifact NDA 和下載您所選協議的 PDF，請選擇接受 NDA 並下載。
9. 在 PDF 檢視器中，檢閱您下載的協議 PDF。
10. 在 AWS Artifact 主控台中，選取協議後，選擇接受協議。
11. 在接受協議對話方塊中，執行下列動作：

    a. 檢閱協議。

    b. 選取我同意所有這些條款與條件。

    c. 選擇接受協議。
12. 選擇接受以接受您帳戶的協議。

在 AWS 帳戶 中終止 的協議 AWS Artifact

如果您使用 AWS Artifact 主控台來接受單一 的協議 AWS 帳戶，則可以使用主控台來終止該協議。否則，請參閱 中的離線協議 AWS Artifact。

所需的許可

若要終止協議，IAM 和聯合身分使用者必須擁有必要的許可。

如需詳細資訊，請參閱中的身分和存取管理 AWS Artifact。

終止您與 的線上協議 AWS

1. 在 https：//https://console.aws.amazon.com/artifact/ 開啟 AWS Artifact 主控台。
2. 在 AWS Artifact 導覽窗格中，選擇協議。
3. 選擇 Account agreements (帳戶協議) 標籤。
4. 選取協議，然後選擇終止協議。
5. 選取所有核取方塊，表示您同意終止協議。
6. 選擇終止。出現確認提示時，請選擇終止。

在 中接受您組織的協議 AWS Artifact

如果您是 AWS Organizations 組織的管理帳戶的擁有者，則可以 AWS 代表您 AWS 帳戶 組織中的所有人接受與 的協議。

> **Important**
> 接受協議之前，我們建議您諮詢法律、隱私權和合規團隊。

AWS Organizations 有兩個可用的功能集：合併帳單功能和所有功能。若要 AWS Artifact 針對您的組織使用 ，您必須針對所有功能啟用您所屬的組織。如果您的組織僅針對合併帳單設定，請參閱AWS Organizations 《 使用者指南》中的啟用組織中的所有功能。

若要接受或終止組織協議，您必須以正確的 AWS Artifact 許可登入管理帳戶。具有`organizations:DescribeOrganization`許可的成員帳戶使用者可以檢視代其接受的組織協議。

如需詳細資訊，請參閱AWS Organizations 《 使用者指南》中的使用 管理組織中的帳戶 AWS Organizations。

所需的許可

若要接受協議，管理帳戶的擁有者必須擁有必要的許可。

如需詳細資訊，請參閱中的身分和存取管理 AWS Artifact。

為組織接受協議

1. 在 https：//https://console.aws.amazon.com/artifact/ 開啟 AWS Artifact 主控台。
2. 在 AWS Artifact 儀表板上，選擇協議。
3. 選擇 Organization agreements (組織帳戶) 標籤。
4. 在 https：//https://console.aws.amazon.com/artifact/ 開啟 AWS Artifact 主控台。
5. 在導覽窗格中，選擇協議。
6. 在協議頁面上，執行下列其中一項操作：
   - 若要僅接受您帳戶的協議，請選擇帳戶協議索引標籤。
   - 若要代表您的組織接受協議，請選擇組織協議索引標籤。
7. 選取協議，然後選擇下載協議。

   顯示接受 NDA 下載報告對話方塊。
8. 您必須先接受保密協議 AWS Artifact (AWS Artifact NDA) 的條款，才能下載您選擇的協議。

   a. 在接受 NDA 下載報告對話方塊中，檢閱 AWS Artifact NDA。
   b. （選用）若要列印 AWS Artifact NDA 的副本（或將其儲存為 PDF)，請選擇列印 NDA。
   c. 選取 我已經閱讀並同意 NDA 的所有條款。
   d. 若要接受 AWS Artifact NDA 和下載您所選協議的 PDF，請選擇接受 NDA 並下載。
9. 在 PDF 檢視器中，檢閱您下載的協議 PDF。
10. 在 AWS Artifact 主控台中，選取協議後，選擇接受協議。
11. 在接受協議對話方塊中，執行下列動作：

    a. 檢閱協議。
    b. 選取我同意所有這些條款與條件。
    c. 選擇接受協議。
12. 選擇接受以接受組織中所有現有和未來帳戶的協議。

在 中終止您組織的協議 AWS Artifact

如果您使用 AWS Artifact 主控台代表組織中的所有成員帳戶接受協議 AWS Organizations，則可以使用主控台終止該協議。否則，請參閱 中的離線協議 AWS Artifact。

如果成員帳戶已從組織中移除，則該成員帳戶會受到組織協議的較長涵蓋。從組織移除成員帳戶之前，管理帳戶管理員應該與成員帳戶進行通訊，以便在必要時簽訂新的協議。您可以在 協議頁面的組織協議下，在 AWS Artifact 主控台中檢視作用中組織協議的清單。

如需 的詳細資訊 AWS Organizations，請參閱AWS Organizations 《 使用者指南》中的使用 管理組織中的帳戶 AWS Organizations。

所需的許可

若要終止協議，管理帳戶的擁有者必須擁有必要的許可。

如需詳細資訊，請參閱中的身分和存取管理 AWS Artifact。

若要終止 AWS 的線上組織協議

1. 在 https：//https://console.aws.amazon.com/artifact/ 開啟 AWS Artifact 主控台。
2. 在 AWS Artifact 儀表板上，選擇協議。
3. 選擇 Organization agreements (組織帳戶) 標籤。
4. 選取協議，然後選擇終止協議。
5. 選取所有核取方塊，表示您同意終止協議。
6. 選擇終止。出現確認提示時，請選擇終止。

中的離線協議 AWS Artifact

如果您有現有的離線協議， AWS Artifact 會顯示您離線接受的協議。例如，主控台會顯示離線商業夥伴增補合約 (BAA) 為 Active (作用中) 狀態。作用中狀態表示協議已接受。若要終止離線協議，請參閱協議中所含的終止準則和指示。

如需詳細資訊，請參閱中的身分和存取管理 AWS Artifact。

在 中設定電子郵件通知 AWS Artifact

> **Note**
>
> 此頁面的內容僅適用於 commercial AWS Regions，目前不適用於 AWS GovCloud (US) Regions。

您可以使用 AWS Artifact 主控台來設定電子郵件通知，以取得 中協議和報告的更新 AWS Artifact。使用這些 AWS Artifact 電子郵件通知 AWS 使用者通知。若要接收 AWS Artifact 電子郵件通知，您必須先在 使用者通知 主控台中選取 AWS 使用者通知 通知中樞。然後，在 AWS Artifact 主控台中，您可以建立通知設定的組態，在其中指定通知收件人及其接收的通知。

若要設定 AWS Artifact 電子郵件通知，您必須擁有 AWS Artifact 和 的必要許可 AWS 使用者通知。如需詳細資訊，請參閱中的身分和存取管理 AWS Artifact。

目錄

先決條件：在 中選取通知中樞 使用者通知

您必須先開啟 使用者通知 主控台，並在 AWS 區域 您要存放 使用者通知 資料的 中選取通知中樞，才能接收 AWS Artifact 電子郵件通知。需要選取通知中樞 AWS 使用者通知，以 AWS Artifact 使用 傳送通知。

選取通知中樞

1. 開啟 AWS 使用者通知 主控台的通知中樞頁面。
2. 在您要存放 AWS 使用者通知 資源 AWS 區域 的 中選取通知中樞。根據預設， 使用者通知 您的資料會存放在美國東部（維吉尼亞北部）區域。 會複 使用者通知 寫您所選其他區域的通知資料。如需詳細資訊，請參閱AWS 使用者通知 《 使用者指南》中的通知中樞文件。
3. 選擇儲存並繼續。

建立 AWS Artifact 通知設定的組態

> **Note**
>
> 此頁面的內容僅適用於 commercial AWS Regions，目前不適用於 AWS GovCloud (US) Regions。

選取 使用者通知 通知中樞後，您可以在 AWS Artifact 主控台中建立通知設定的組態。在您建立的組態中，您可以指定要接收 AWS Artifact 通知的收件人電子郵件地址。您也可以指定這些收件人應該收到哪些更新的通知，例如 AWS Artifact 協議的更新，以及所有（或一部分）AWS Artifact 報告的更新。

建立組態

1. 開啟 AWS Artifact 主控台的通知設定頁面。
2. 選擇建立組態。
3. 在建立組態頁面上，執行下列動作：
   - 若要接收協議的通知，請根據協議，保持已選取 AWS 協議的更新。
   - 若要接收報告的通知，請在報告下，保持選取 AWS 報告更新。
     a. 若要接收所有報告的通知，請選擇所有報告。
     b. 若要僅針對特定類別和系列下的報告接收通知，請選擇報告子集。然後，選取您感興趣的類別和系列。
   - 在組態名稱下，輸入組態的名稱。
   - 在電子郵件下，針對收件人，輸入您希望接收 AWS Artifact 通知電子郵件的電子郵件地址逗號分隔清單。
   - （選用）若要將標籤新增至通知組態，請展開標籤，選擇新增標籤，然後輸入標籤做為鍵/值對。如需標記 使用者通知 資源的詳細資訊，請參閱AWS 使用者通知 《使用者指南》中的標記 AWS 使用者通知 資源。
   - 選擇建立組態。

     使用者通知 會將驗證電子郵件傳送至您提供的每個收件人電子郵件地址。若要驗證電子郵件地址，在驗證電子郵件中，收件人必須選擇驗證電子郵件。只有已驗證的電子郵件地址才會收到 AWS Artifact 通知。

編輯 AWS Artifact 通知設定的組態

> **Note**
>
> 此頁面的內容僅適用於 commercial AWS Regions，目前不適用於 AWS GovCloud (US) Regions。

建立通知設定的組態後，您可以隨時編輯組態以變更通知設定。 AWS Artifact 例如，若要新增或移除收件人，請變更他們收到的通知類型，以及新增或移除標籤。

編輯組態

1. 開啟 AWS Artifact 主控台的通知設定頁面。
2. 選取您要編輯的組態。
3. 選擇編輯。
4. 編輯任何組態選擇和欄位。完成後，請選擇儲存變更。

   如果您已將新的電子郵件地址新增為通知收件人，則 會 AWS 使用者通知 傳送驗證電子郵件地址。若要驗證電子郵件地址，在驗證電子郵件中，收件人必須選擇驗證電子郵件。只有已驗證的電子郵件地址才會收到 AWS Artifact 通知。

刪除 AWS Artifact 通知設定的組態

> **Note**
>
> 此頁面的內容僅適用於 commercial AWS Regions，目前不適用於 AWS GovCloud (US) Regions。

如果您不再需要為 AWS Artifact 通知設定建立的組態，則可以在 AWS Artifact 主控台中刪除組態。

刪除組態

1. 開啟 AWS Artifact 主控台的通知設定頁面。
2. 選取您要刪除的組態。
3. 選擇 刪除 。

4. 在刪除組態對話方塊中，選擇刪除。

中的身分和存取管理 AWS Artifact

當您註冊 時 AWS，您會提供與 AWS 您的帳戶相關聯的電子郵件地址和密碼。這些是您的根登入資料，它們可讓您完整存取所有 AWS 資源，包括 的資源 AWS Artifact。但是，我們極力建議您不要使用根帳戶進行日常存取。我們也建議您不會與他人分享帳戶登入資料，提供他們您帳戶的完整存取權。

您不應該使用根登入資料登入 AWS 您的帳戶或與他人共用登入資料，而是為自己和任何可能需要存取文件或協議的人建立稱為 IAM 使用者的特殊使用者身分 AWS Artifact。透過這種方法，您可以提供個別登入資訊給每位使用者，而您可以只授予使用特定文件所需的必要許可給每位使用者。您也可以將許可授予 IAM 群組，並將 IAM 使用者新增至群組，以授予多個 IAM 使用者相同的許可。

如果您已在外部管理使用者身分 AWS，您可以使用 IAM 身分提供者，而不是建立 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的身分提供者和聯合。

目錄

授予使用者對 的存取權 AWS Artifact

完成下列步驟， AWS Artifact 根據使用者所需的存取層級，將許可授予 。

任務

- 步驟 1：建立 IAM 政策
- 步驟 2：建立 IAM 群組並連接政策
- 步驟 3：建立 IAM 使用者並將其新增至群組

步驟 1：建立 IAM 政策

身為 IAM 管理員，您可以建立將許可授予 AWS Artifact 動作和資源的政策。

建立 IAM 政策

使用下列程序來建立 IAM 政策，您可以使用該政策將許可授予您的 IAM 使用者和群組。

1. 開啟位於 https://console.aws.amazon.com/iam/ 的 IAM 主控台。
2. 在導覽窗格中，選擇政策。
3. 選擇 Create policy (建立政策)。
4. 請選擇 JSON 標籤。
5. 輸入政策文件。您可以建立自己的政策，也可以從 使用其中一個政策商業 AWS 區域中 AWS Artifact 的 IAM 政策範例。
6. 選擇檢閱政策。政策驗證程式會回報任何語法錯誤。
7. 在檢閱政策頁面上，輸入可協助您記住政策目的的唯一名稱。您也可以提供描述。
8. 選擇 建立政策。

步驟 2：建立 IAM 群組並連接政策

身為 IAM 管理員，您可以建立 群組，並將您建立的政策連接至群組。您可以隨時將 IAM 使用者新增至群組。

建立 IAM 群組並連接您的政策

1. 在導覽窗格中選擇 Groups (群組)，然後選擇 Create New Group (建立新群組)。
2. 對於群組名稱，輸入群組的名稱，然後選擇下一步。
3. 在搜尋欄位中，輸入您建立的政策名稱。選取政策的核取方塊，然後選擇下一步。
4. 檢閱群組名稱和政策。當您準備好時，請選擇建立群組。

步驟 3：建立 IAM 使用者並將其新增至群組

身為 IAM 管理員，您可以隨時將使用者新增至群組。這會授予使用者授予 群組的許可。

建立 IAM 使用者並將使用者新增至群組

1. 在導覽窗格中，選擇 Users (使用者)，然後選擇 Add user (新增使用者)。

2. 針對使用者名稱，輸入一或多個使用者的名稱。
3. 選取 AWS Management Console access (AWS Management Console 管理主控台存取) 旁的核取方塊。設定自動產生的或自訂密碼。您可以選擇性地選取使用者必須在下次登入時建立新密碼，以便在使用者第一次登入時要求重設密碼。
4. 選擇下一步：許可。
5. 選擇新增使用者至群組，然後選擇您建立的群組。
6. 選擇下一步：標籤。您可以選擇性地將標籤新增至使用者。
7. 選擇下一步：檢閱。當您準備好時，請選擇建立使用者。

將報告遷移至 的精細許可 AWS Artifact

您現在可以使用 的精細許可 AWS Artifact。透過這些精細的許可，您可以精細控制提供對功能的存取，例如接受條款和下載報告。

若要透過精細許可存取報告，您可以利用 AWSArtifactReportsReadOnlyAccess 受管政策，或依照下列建議更新您的許可。

> **Note**
>
> IAM 動作`artifact:Get`將於 2025 年 7 月 1 日在 AWS GovCloud (US) 分割區中棄用。相同的動作已於 2025 年 3 月 3 日在 AWS 分割區中棄用。

將報告遷移至新許可

遷移非資源特定許可

將包含舊版許可的現有政策取代為包含精細許可的政策。

舊版政策：

AWS

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

```
        "Effect": "Allow",
        "Action": [
            "artifact:Get"
        ],
        "Resource": [
            "arn:aws:artifact:::report-package/*"
        ]
    }]
}
```

AWS GovCloud (US)

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "artifact:Get"
        ],
        "Resource": [
            "arn:aws-us-gov:artifact:::report-package/*"
        ]
    }]
}
```

具有精細許可的新政策：

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "artifact:ListReports",
            "artifact:GetReportMetadata",
            "artifact:GetReport",
            "artifact:GetTermForReport"
        ],
        "Resource": "*"
```

```
    }]
}
```

遷移資源特定的許可

將包含舊版許可的現有政策取代為包含精細許可的政策。報告資源萬用字元許可已取代為條件索引鍵。

舊版政策：

AWS

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "artifact:Get"
        ],
        "Resource": [
            "arn:aws:artifact:::report-package/Certifications and Attestations/SOC/
*",
            "arn:aws:artifact:::report-package/Certifications and Attestations/PCI/
*",
            "arn:aws:artifact:::report-package/Certifications and Attestations/ISO/
*"
        ]
    }]
}
```

AWS GovCloud (US)

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "artifact:Get"
        ],
        "Resource": [
```

```
            "arn:aws-us-gov:artifact:::report-package/Certifications and
 Attestations/SOC/*",
            "arn:aws-us-gov:artifact:::report-package/Certifications and
 Attestations/PCI/*",
            "arn:aws-us-gov:artifact:::report-package/Certifications and
 Attestations/ISO/*"
        ]
    }]
}
```

具有精細許可和條件索引鍵的新政策：

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "artifact:ListReports"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "artifact:GetReportMetadata",
                "artifact:GetReport",
                "artifact:GetTermForReport"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "artifact:ReportSeries": [
                        "SOC",
                        "PCI",
                        "ISO"
                    ],
                    "artifact:ReportCategory": [
                        "Certifications and Attestations"
                    ]
                }
            }
```

```
        }
    ]
}
```

遷移至 AWS Artifact 協議的精細許可

AWS Artifact 現在可讓客戶針對協議使用精細的許可。透過這些精細的許可，客戶可以精細控制提供對檢視和接受不公開協議等功能的存取，以及接受和終止協議。

若要透過精細許可存取協議，您可以使用 AWSArtifactAgreementsReadOnlyAccess 或 AWSArtifactAgreementsFullAccess 受管政策，或依照下列建議更新您的許可。

> **Note**
>
> IAM 動作`artifact:DownloadAgreement`將於 2025 年 7 月 1 日在 AWS GovCloud (US) 分割區中棄用。相同的動作已於 2025 年 3 月 3 日在 AWS 分割區中棄用。

遷移至新許可

舊版 IAM 動作「DownloadAgreement」已由「GetAgreement」動作取代，以下載未接受的協議，並已由「GetCustomerAgreement」動作取代，以下載接受的協議。此外，已推出更精細的動作來控制檢視和接受保密協議 (NDAs) 的存取。若要利用這些精細動作並維持檢視和執行協議的能力，使用者必須將包含舊版許可的現有政策取代為包含精細許可的政策。

在帳戶層級遷移下載協議的許可

舊版政策：

AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:DownloadAgreement"
      ],
```

```
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

AWS GovCloud (US)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "arn:aws-us-gov:artifact::*:customer-agreement/*",
        "arn:aws-us-gov:artifact:::agreement/*"
      ]
    }
  ]
}
```

具有精細許可的新政策：

AWS

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

```
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:GetAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptNdaForAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

AWS GovCloud (US)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementsActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:GetAgreement",
```

```
        "artifact:GetNdaForAgreement",
        "artifact:AcceptNdaForAgreement"
      ],
      "Resource": [
        "arn:aws-us-gov:artifact::*:customer-agreement/*",
        "arn:aws-us-gov:artifact:::agreement/*"
      ]
    }
  ]
}
```

遷移非資源特定許可，以在帳戶層級下載、接受和終止協議

舊版政策：

AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

AWS GovCloud (US)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws-us-gov:artifact::*:customer-agreement/*",
        "arn:aws-us-gov:artifact:::agreement/*"
      ]
    }
  ]
}
```

具有精細許可的新政策：

AWS

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
        "Sid": "ListAgreementActions",
        "Effect": "Allow",
        "Action": [
            "artifact:ListAgreements",
            "artifact:ListCustomerAgreements"
        ],
        "Resource": "*"
      },
      {
        "Sid": "AWSAgreementActions",
        "Effect": "Allow",
        "Action": [
          "artifact:GetAgreement",
          "artifact:AcceptNdaForAgreement",
```

```
          "artifact:GetNdaForAgreement",
          "artifact:AcceptAgreement"
        ],
        "Resource": "arn:aws:artifact:::agreement/*"
      },
      {
        "Sid": "CustomerAgreementActions",
        "Effect": "Allow",
        "Action": [
            "artifact:GetCustomerAgreement",
            "artifact:TerminateAgreement"
        ],
        "Resource": "arn:aws:artifact::*:customer-agreement/*"
      }
    ]
}
```

AWS GovCloud (US)

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
        "Sid": "ListAgreementActions",
        "Effect": "Allow",
        "Action": [
            "artifact:ListAgreements",
            "artifact:ListCustomerAgreements"
        ],
        "Resource": "*"
      },
      {
        "Sid": "AWSAgreementActions",
        "Effect": "Allow",
        "Action": [
          "artifact:GetAgreement",
          "artifact:AcceptNdaForAgreement",
          "artifact:GetNdaForAgreement",
          "artifact:AcceptAgreement"
        ],
        "Resource": "arn:aws-us-gov:artifact:::agreement/*"
```

```
      },
      {
        "Sid": "CustomerAgreementActions",
        "Effect": "Allow",
        "Action": [
            "artifact:GetCustomerAgreement",
            "artifact:TerminateAgreement"
        ],
        "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
      }
    ]
}
```

遷移非資源特定許可，以在組織層級下載、接受和終止協議

舊版政策：

AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam:::role/*"
    },
    {
```

```
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam:::role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS GovCloud (US)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws-us-gov:artifact::*:customer-agreement/*",
        "arn:aws-us-gov:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws-us-gov:iam:::role/*"
    },
    {
```

```
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws-us-gov:iam:::role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

具有精細許可的新政策：

AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
```

```
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
```

```
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS GovCloud (US)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
```

```
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

遷移資源特定許可，以在帳戶層級下載、接受和終止協議

舊版政策：

AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "arn:aws:artifact:::agreement/AWS Business Associate Addendum"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*"
      ]
    }
  ]
}
```

AWS GovCloud (US)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement"
      ],
```

```
      "Resource": [
        "arn:aws-us-gov:artifact:::agreement/AWS Business Associate Addendum"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws-us-gov:artifact::*:customer-agreement/*"
      ]
    }
  ]
}
```

具有精細許可的新政策：

AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
```

```
      ],
      "Resource": "arn:aws:artifact:::agreement/agreement-9c1kBcYznTkcpRIm"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

AWS GovCloud (US)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/agreement-Og8HCNyYwYNp8AR1"
    },
    {
```

```
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    }
  ]
}
```

遷移資源特定許可，以在組織層級下載、接受和終止協議

舊版政策：

AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/AWS Organizations Business Associate Addendum"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam:::role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
```

```
      "Resource": "arn:aws:iam:::role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS GovCloud (US)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws-us-gov:artifact::*:customer-agreement/*",
        "arn:aws-us-gov:artifact:::agreement/AWS Organizations Business Associate
 Addendum"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws-us-gov:iam:::role/*"
    },
    {
      "Effect": "Allow",
```

```
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws-us-gov:iam:::role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

具有精細許可的新政策：

AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
```

```
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/agreement-y03aUwMAEorHtqjv"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
```

```
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS GovCloud (US)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/agreement-B47fK0ArVebC9XE1"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    },
```

```
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

協議的舊版至精細資源映射

協議 ARN 已更新，以取得精細許可。任何先前對舊版協議資源的參考，都應該以新的 ARN 取代。以下是傳統資源與精細資源之間的協議 ARN 映射。

AWS

協議名稱	舊版許可的成品 ARN	精細許可的成品 ARN
AWS 商業夥伴增補合約	arn：aws：artifact：：agreement/AWS 商業夥伴增補合約	arn：aws：artifact：：agreement/agreement-9c1kBcYznTkcpRIm
AWS 紐西蘭可公告資料外洩增補合約	arn：aws：artifact：：：agreement/AWS New Zealand Notifiable Data Breach 增補合約	arn：aws：artifact：：：agreement/agreement-3YRq9rGUIu72r7Gt
AWS 澳洲公告資料外洩增補合約	arn：aws：artifact：：：agreement/AWS 澳洲可公告資料外洩增補合約	arn：aws：artifact：：：agreement/agreement-sbLSDe8bitmAXNr9
AWS SEC 規則 17a-4 增補合約	arn：aws：artifact：：：agreement/AWS SEC 規則 17a-4 增補合約	arn：aws：artifact：：agreement/agreement-bexgr7sjvXAW4Gxu
AWS SEC 規則 18a-6 增補合約	arn：aws：artifact：：：agreement/AWS SEC 規則 18a-6 增補合約	arn：aws：artifact：：agreement/agreement-HZTdNwJuqOKLReXC
AWS Organizations 商業夥伴增補合約	arn：aws：artifact：：agreement/AWS Organizations 商業夥伴增補合約	arn：aws：artifact：：：agreement/agreement-y03aUwMAEorHtqjv
AWS Organizations 澳洲公告資料外洩增補合約	arn：aws：artifact：：：agreement/AWS Organizations 澳洲可公告資料外洩增補合約	arn：aws：artifact：：：agreement/agreement-YpDMFXTePE7kEg4b

協議名稱	舊版許可的成品 ARN	精細許可的成品 ARN
AWS Organizations New Zealand Notifiable Data Breach 增補合約	arn：aws：artifact：：：agreement/AWS Organizations New Zealand Notifiable Data Breach 增補合約	arn：aws：artifact：：agreement/agreement-uojEjr3vOnvrhV52

AWS GovCloud (US)

協議名稱	舊版許可的成品 ARN	精細許可的成品 ARN
AWS 商業夥伴增補合約	arn：aws-us-gov：artifact：：agreement/AWS 商業夥伴增補合約	arn：aws-us-gov：artifact：：agreement/agreement-Og8HCNyYwYNp8AR1
AWS 澳洲公告資料外洩增補合約	arn：aws-us-gov：artifact：：：agreement/AWS 澳洲可公告資料外洩增補合約	arn：aws-us-gov：artifact：：agreement/agreement-G1rBS2MGYjLiCCXy
AWS Organizations 商業夥伴增補合約	arn：aws-us-gov：artifact：：：agreement/AWS Organizations 商業夥伴增補合約	arn：aws-us-gov：artifact：：：agreement/agreement-B47fK0ArVebC9XE1
AWS Organizations 澳洲公告資料外洩增補合約	arn：aws-us-gov：artifact：：：agreement/AWS Organizations 澳洲可公告資料外洩增補合約	arn：aws-us-gov：artifact：：agreement/agreement-OsnlbilP8RB73Nw5

商業 AWS 區域中 AWS Artifact 的 IAM 政策範例

您可以建立許可政策，將許可授予 IAM 使用者。您可以授予使用者對 AWS Artifact 報告的存取權，以及代表單一帳戶或組織接受和下載協議的能力。

下列範例政策顯示您可以根據 IAM 使用者所需的存取層級，將其指派給 IAM 使用者的許可。

這些政策適用於 commercial AWS Regions。如需適用於 的政策 AWS GovCloud (US) Regions，請參閱 AWS Artifact 中 的範例 IAM 政策 AWS GovCloud (US) Regions

- 使用精細許可管理 AWS 報告的範例政策
- 管理第三方報告的範例政策
- 管理協議的政策範例
- 要與 整合的政策範例 AWS Organizations
- 管理管理帳戶協議的政策範例
- 管理組織協議的政策範例
- 管理通知的政策範例

Example 透過精細許可管理 AWS 報告的範例政策

> **Tip**
>
> 您應該考慮使用 AWSArtifactReportsReadOnlyAccess 受管政策，而不是定義您自己的政策。

下列政策授予許可，以透過精細的許可下載所有 AWS 報告。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

下列政策授予許可，透過精細的許可僅下載 AWS SOC、PCI 和 ISO 報告。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": [
            "SOC",
            "PCI",
            "ISO"
          ],
          "artifact:ReportCategory": [
            "Certifications and Attestations"
          ]
        }
      }
    }
  ]
}
```

Example 管理第三方報告的範例政策

> **Tip**
>
> 您應該考慮使用 AWSArtifactReportsReadOnlyAccess 受管政策，而不是定義您自己的政策。

第三方報告由 IAM 資源 表示`report`。

下列政策授予所有第三方報告功能的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

下列政策授予下載第三方報告的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

下列政策授予列出第三方報告的許可。

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

```
        "artifact:ListReport"
      ],
      "Resource": "*"
    }
  ]
}
```

下列政策授予檢視第三方報告所有版本詳細資訊的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:*"
      ]
    }
  ]
}
```

下列政策授予許可，以檢視特定版本的第三方報告詳細資訊。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:1"
      ]
    }
  ]
}
```

> **Tip**
>
> 您應該考慮使用 AWSArtifactAgreementsReadOnlyAccess 或 AWSArtifactAgreementsFullAccess 受管政策，而不是定義您自己的政策。

Example 管理協議的政策範例

下列政策授予下載所有協議的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
```

```
}
```

下列政策授予許可，以接受所有協議。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    }
  ]
}
```

下列政策授予終止所有協議的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
```

```
      "Resource": "*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

下列政策授予檢視和執行帳戶層級協議的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
```

```
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

Example 要與 整合的政策範例 AWS Organizations

下列政策會授予許可，以建立 AWS Artifact 用來與 整合的 IAM 角色 AWS Organizations。您組織的管理帳戶必須擁有這些許可，才能開始使用組織協議。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

下列政策授予許可，以授予使用 AWS Artifact 的許可 AWS Organizations。您組織的管理帳戶必須擁有這些許可，才能開始使用組織協議。

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

```
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
   }
 ]
}
```

Example 管理管理帳戶協議的政策範例

下列政策會授予許可，以管理 管理帳戶的協議。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
```

```
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 管理組織協議的政策範例

下列政策授予管理組織協議的許可。具有必要許可的另一個使用者必須設定組織協議。

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

```
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

下列政策授予檢視組織協議的許可。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 管理通知的政策範例

下列政策授予使用 AWS Artifact 通知的完整許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DisassociateChannel",
        "notifications:GetEventRule",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts:DeleteEmailContact",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:SendActivationCode"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

下列政策授予列出所有組態的許可。

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

```
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

下列政策會授予建立組態的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts:SendActivationCode",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:ListEventRules",
        "notifications:ListNotificationHubs",
        "notifications:TagResource",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

下列政策授予編輯組態的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:DisassociateChannel",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

下列政策授予刪除組態的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeleteNotificationConfiguration",
        "notifications:ListEventRules"
      ],
      "Resource": [
        "*"
```

```
      ]
    }
  ]
}
```

下列政策授予檢視組態詳細資訊的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

下列政策授予註冊或取消註冊通知中樞的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeregisterNotificationHub",
        "notifications:RegisterNotificationHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
```

```
}
```

AWS Artifact 中 的 IAM 政策範例 AWS GovCloud (US) Regions

這些政策僅適用於 AWS GovCloud (US) Regions。如需適用於 commercial AWS Regions 的政策，請參閱AWS Artifact 商業 AWS 區域中適用於 的範例 IAM 政策

您可以建立許可政策，將許可授予 IAM 使用者。您可以授予使用者報告存取權， AWS Artifact 以及代表單一帳戶或組織接受和下載協議的能力。

下列範例政策顯示您可以根據 IAM 使用者所需的存取層級，將其指派給 IAM 使用者的許可。

- 管理 AWS 報告的範例政策
- 管理協議的政策範例
- 要與 整合的政策範例 AWS Organizations
- 管理管理帳戶協議的範例政策
- 管理組織協議的政策範例

Example 管理報告的範例政策

下列政策授予下載所有報告的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

下列政策僅授予下載 SOC、PCI 和 ISO 報告的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": [
            "SOC",
            "PCI",
            "ISO"
          ],
          "artifact:ReportCategory": [
            "Certifications and Attestations"
          ]
        }
      }
    }
  ]
}
```

Example 管理協議的政策範例

下列政策授予下載所有協議的許可。IAM 使用者也必須擁有此許可才能接受協議。

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

```
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    }
  ]
}
```

下列政策授予許可，以接受所有協議。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements"
      ],
      "Resource": [
        "*"
      ]
```

```
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    }
  ]
}
```

下列政策授予終止所有協議的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    }
  ]
}
```

下列政策授予檢視和執行帳戶層級協議的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    }
  ]
}
```

Example 要與 整合的政策範例 AWS Organizations

下列政策會授予許可，以建立 AWS Artifact 用來與 整合的 IAM 角色 AWS Organizations。您組織的管理帳戶必須擁有這些許可，才能開始使用組織協議。

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

```
  "Statement": [
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

下列政策授予許可，以授予使用 AWS Artifact 的許可 AWS Organizations。您組織的管理帳戶必須擁有這些許可，才能開始使用組織協議。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

Example 管理管理帳戶協議的政策範例

下列政策授予許可，以管理 管理帳戶的協議。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
```

```
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 管理組織協議的政策範例

下列政策授予管理組織協議的許可。具有必要許可的另一個使用者必須設定組織協議。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
```

```
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

下列政策授予檢視組織協議的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
```

```
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

使用 的 AWS 受管政策 AWS Artifact

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新 AWS 受管政策中定義的許可，則更新會影響政策連接的所有委託人身分 （使用者、群組和角色）。 AWS 服務 當新的 啟動或新的 API 操作可用於現有服務時， AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管政策：AWSArtifactReportsReadOnlyAccess

您可將 `AWSArtifactReportsReadOnlyAccess` 政策連接到 IAM 身分。

此政策授予##許可，允許列出、檢視和下載報告。

許可詳細資訊

此政策包含以下許可。

- `artifact` – 允許主體從中列出、檢視和下載報告 AWS Artifact。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS 受管政策：AWSArtifactAgreementsReadOnlyAccess

您可將 `AWSArtifactAgreementsReadOnlyAccess` 政策連接到 IAM 身分。

此政策授予##存取權，以列出 AWS Artifact 服務協議並下載接受的協議。它也包含列出和描述組織詳細資訊的許可。此外，政策提供檢查所需服務連結角色是否存在的能力。

許可詳細資訊

此政策包含以下許可。

- `artifact` – 允許主體列出所有協議，並從中檢視已接受的協議 AWS Artifact。
- `IAM` – 允許主體使用 GetRole 檢查服務連結角色是否存在。

- organization – 允許主體描述組織並列出組織的服務存取權。

AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementsActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetCustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "AWSOrganizationActions",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetRole",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
```

```
  ]
}
```

AWS GovCloud (US)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementsActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetCustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "AWSOrganizationActions",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetRole",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
```

```
      "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact"
    }
  ]
}
```

AWS 受管政策：AWSArtifactAgreementsFullAccess

您可將 AWSArtifactAgreementsFullAccess 政策連接到 IAM 身分。

此政策授予列出、下載、接受和終止 AWS Artifact 協議###許可。它還包含列出和啟用 Organization 服務中 AWS 服務存取的許可，以及描述組織詳細資訊的許可。此外，該政策提供檢查所需服務連結角色是否存在的能力，如果不存在，則建立一個。

許可詳細資訊

此政策包含以下許可。

- artifact – 允許主體列出、下載、接受和終止協議 AWS Artifact。
- IAM – 允許主體建立服務連結角色，以及使用 GetRole 檢查服務連結角色是否存在。
- organization – 允許主體描述組織，並列出/啟用組織的服務存取權。

AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
```

```
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
```

```
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS GovCloud (US)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
```

```
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws-us-gov:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws-us-gov:iam::*:role/aws-service-role/
artifact.amazonaws.com/AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS ArtifactAWS 受管政策的更新

檢視自此服務開始追蹤這些變更 AWS Artifact 以來 AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱 AWS Artifact 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
更新的 AWS 報告受管政策	更新 AWSArtifactReportsReadOnlyAccess 受管政策以移除 artifact：get 許可。	2025-03-21
引進 AWS 協議受管政策	推出 AWSArtifactAgreementsReadOnlyAccess 和 AWSArtifactAgreementsFullAccess 受管政策。	2024-11-21
AWS Artifact 開始追蹤變更	AWS Artifact 開始追蹤其 AWS 受管政策的變更，並推出 AWSArtifactReportsReadOnlyAccess。	2023-12-15

使用 AWS Artifact的服務連結角色

AWS Artifact use AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 的唯一 IAM 角色類型 AWS Artifact。服務連結角色由 預先定義， AWS Artifact 並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓設定 AWS Artifact 更容易，因為您不必手動新增必要的許可。 AWS Artifact 會定義其服務連結角色的許可，除非另有定義，否則只能 AWS Artifact 擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除角色的相關資源，才能刪除服務連結角色。這可保護您的 AWS Artifact 資源，因為您不會不小心移除存取資源的許可。

如需支援服務連結角色的其他 服務的資訊，請參閱AWS 使用 IAM 的服務，並在服務連結角色欄中尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

的服務連結角色許可 AWS Artifact

AWS Artifact 使用名為 AWSServiceRoleForArtifact 的服務連結角色 – 允許 透過 AWS Artifact 收集組織的相關資訊 AWS Organizations。

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

- `artifact.amazonaws.com`

名為 AWSArtifactServiceRolePolicy 的角色許可政策允許 在 `organizations` 資源上 AWS Artifact 完成下列動作。

- `DescribeOrganization`
- `DescribeAccount`
- `ListAccounts`
- `ListAWSServiceAccessForOrganization`

為 建立服務連結角色 AWS Artifact

您不需要手動建立一個服務連結角色。當您前往組織管理帳戶中的組織協議索引標籤，並選擇 中的入門連結時 AWS Management Console， 會為您 AWS Artifact 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。當您前往組織管理帳戶中的組織協議索引標籤並選擇開始使用連結時， 會再次為您 AWS Artifact 建立服務連結角色。

編輯 的服務連結角色 AWS Artifact

AWS Artifact 不允許您編輯 AWSServiceRoleForArtifact 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱「IAM 使用者指南」的編輯服務連結角色。

刪除 的服務連結角色 AWS Artifact

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

> **Note**
>
> 如果 AWS Artifact 服務在您嘗試刪除資源時使用角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

刪除 AWSServiceRoleForArtifact 使用 AWS Artifact 的資源

1. 前往 AWS Artifact 主控台中的「組織協議」資料表
2. 終止任何作用中的組織協議

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 AWSServiceRoleForArtifact 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。

AWS Artifact 服務連結角色支援的區域

AWS Artifact 不支援在提供服務的每個區域中使用服務連結角色。您可以在下列區域中使用 AWSServiceRoleForArtifact 角色。

區域名稱	區域身分	中的支援 AWS Artifact
美國東部 (維吉尼亞北部)	us-east-1	是
美國東部 (俄亥俄)	us-east-2	否
美國西部 (加利佛尼亞北部)	us-west-1	否
美國西部 (奧勒岡)	us-west-2	是
Africa (Cape Town)	af-south-1	否
亞太區域 (香港)	ap-east-1	否
亞太區域 (雅加達)	ap-southeast-3	否
亞太區域 (孟買)	ap-south-1	否
亞太區域 (大阪)	ap-northeast-3	否

區域名稱	區域身分	中的支援 AWS Artifact
亞太區域 (首爾)	ap-northeast-2	否
亞太區域 (新加坡)	ap-southeast-1	否
亞太區域 (雪梨)	ap-southeast-2	否
亞太區域 (東京)	ap-northeast-1	否
加拿大 (中部)	ca-central-1	否
歐洲 (法蘭克福)	eu-central-1	否
歐洲 (愛爾蘭)	eu-west-1	否
歐洲 (倫敦)	eu-west-2	否
歐洲 (米蘭)	eu-south-1	否
Europe (Paris)	eu-west-3	否
Europe (Stockholm)	eu-north-1	否
Middle East (Bahrain)	me-south-1	否
中東 (阿拉伯聯合大公國)	me-central-1	否
南美洲 (聖保羅)	sa-east-1	否
AWS GovCloud （美國東部）	us-gov-east-1	否
AWS GovCloud （美國西部）	us-gov-west-1	是

針對 AWS Artifact 報告使用 IAM 條件索引鍵

您可以使用 IAM 條件金鑰， AWS Artifact根據特定報告類別和系列，提供對 報告的精細存取。

下列範例政策顯示您可以根據特定報告類別和系列指派給 IAM 使用者的許可。

Example 管理 AWS 報告讀取存取權的政策範例

AWS Artifact 報告由 IAM 資源 表示`report`。

下列政策授予許可，以讀取 `Certifications and Attestations`類別下的所有 AWS Artifact 報告。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

下列政策可讓您授予讀取 SOC 系列下所有 AWS Artifact 報告的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "artifact:ListReports"
```

```
            ],
            "Resource": "*"
        },{
            "Effect": "Allow",
            "Action": [
                "artifact:GetReport",
                "artifact:GetReportMetadata",
                "artifact:GetTermForReport"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "artifact:ReportSeries": "SOC",
                    "artifact:ReportCategory": "Certifications and Attestations"
                }
            }
        }
    ]
}
```

下列政策可讓您授予許可，以讀取 Certifications and Attestations類別和SOC系列下的所有 AWS Artifact 報告。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
```

```
      "Condition": {
        "StringEquals": {
          "artifact:ReportSeries": "SOC",
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

使用 記錄 AWS Artifact API 呼叫 AWS CloudTrail

AWS Artifact 已與 服務整合 AWS CloudTrail，此服務提供由使用者、角色或 AWS 服務在其中採取的動作記錄 AWS Artifact。CloudTrail 會擷取 AWS Artifact 的 API 呼叫當作事件。擷取的呼叫包括從 AWS Artifact 主控台的呼叫，以及對 AWS Artifact API 操作的程式碼呼叫。如果您建立線索，您可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 的事件 AWS Artifact。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。使用 CloudTrail 收集的資訊，您可以判斷提出的請求 AWS Artifact、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

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

AWS Artifact CloudTrail 中的資訊

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

若要持續記錄 中的事件 AWS 帳戶，包括 的事件 AWS Artifact，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

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

AWS Artifact 支援將下列動作記錄為 CloudTrail 日誌檔案中的事件：

- ListReports
- GetAccountSettings
- GetReportMetadata
- GetReport
- GetTermForReport

- PutAccountSettings
- AcceptAgreement
- AcceptNdaForAgreement
- GetAgreement
- GetCustomerAgreement
- GetNdaForAgreement
- ListAgreements
- ListCustomerAgreements
- TerminateAgreement

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：

- 請求是使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

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

了解 AWS Artifact 日誌檔案項目

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

下列範例顯示示範 GetReportMetadata 動作的 CloudTrail 日誌項目。

```
{
  "Records": [
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:03:36Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "errorCode": "AccessDenied",
      "errorMessage": "User: arn:aws:iam::999999999999:user/myUserName is not
 authorized to perform: artifact:GetReportMetadata on resource: arn:aws:artifact:us-
east-1::report/report-f1DIWBmGa2Lhsadg",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "7aebcd0f-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "e92a3e85-8ecd-4d23-8074-843aabfe89bf",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:04:42Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "requestParameters": {
        "reportId": "report-f1DIWBmGa2Lhsadg"
      },
      "responseElements": null,
      "requestID": "a2198ecc-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "20b84ce5-730f-482e-b2b2-e8fcc87ceb22",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
```

```
    }
  ]
}
```

的文件歷史記錄 AWS Artifact

下表提供 AWS Artifact 使用者指南的 AWS Artifact 版本和相關變更的歷史記錄。

變更	描述	日期
AWS Artifact 中 的精細許可 AWS GovCloud (US) Regions	更新和擴展了在 AWS Artifact 中使用 的政策 AWS GovCloud (US) Regions，同時移除有關限制的備註，因為 AWS Artifact 功能現在更廣泛適用於所有區域。	2025 年 3 月 31 日
更新的 AWSArtifactReportReadOnlyAccess 受管政策	已更新 AWSArtifactReportsReadOnlyAccess 受管政策，以移除 artifact：get 許可。	2025 年 3 月 21 日
AWS Artifact 中的 政策範例 AWS GovCloud (US) Regions	已新增在 AWS Artifact 中使用的範例政策 AWS GovCloud (US) Regions，並記下哪些頁面不適用於 AWS Artifact 在中使用 AWS GovCloud (US) Regions。	2024 年 12 月 6 日
協議執行、AWSArtifactAgreementsFullAccess 和 AWSArtifactAgreementsReadOnlyAccess 受管政策的精細許可	啟用 AWS Artifact 協議執行的精細存取，並啟動 AWSArtifactAgreementsFullAccess 和 AWSArtifactAgreementsReadOnlyAccess AWS 受管政策。	2024 年 11 月 21 日
精細報告存取和 AWSArtifactReportReadOnlyAccess 受管政策	啟用對 AWS Artifact 報告的精細存取、啟用的報告條件金鑰，以及啟動的 AWSArtifactReportsReadOnlyAccess 受管政策。	2023 年 12 月 15 日

AWS Artifact 服務連結角色	新增服務連結角色文件，並更新 AWS Artifact 和 AWS Organizations 整合的範例政策。	2023 年 9 月 26 日
通知	已發佈管理通知的文件，並對 AWS Artifact API 參考、CloudTrail 記錄文件和 Identity and Access Management 頁面進行相關更新。	2023 年 8 月 1 日
第三方報告 - 一般可用	新增 API 參考文件和 CloudTrail 記錄文件，並使第三方報告全面可用。	2023 年 1 月 27 日
第三方報告 （預覽）	啟動銷售其產品的獨立軟體廠商 (ISVs的合規報告 AWS Marketplace。將範例政策新增至第三方報告的身分和存取管理頁面。	2022 年 11 月 30 日
安全性	已將 區段新增至身分和存取管理頁面，以預防混淆代理人。	2021 年 12 月 20 日
報告	已移除不公開協議，並引入報告下載的條款和條件。	2020 年 12 月 17 日
首頁和搜尋	在報告和協議頁面上新增了服務首頁和搜尋列。	2020 年 5 月 15 日
AWS GovCloud (US) 啟動	在 AWS Artifact 中啟動 AWS GovCloud (US) Regions。	2019 年 11 月 7 日
AWS Organizations 協議	新增管理組織協議的支援。	2018 年 6 月 20 日
協議	新增管理 AWS Artifact 協議的支援。	2017 年 6 月 17 日

初始版本	此版本推出 AWS Artifact。	2016 年 11 月 30 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。