使用者指南

AWS Artifact

AWS Artifact: 使用者指南

Table of Contents

什麼是 AWS Artifact？

AWS Artifact提供按需下載AWS安全性和合規性文件，例如AWS ISO 認證、支付卡產業 (PCI) 報告和服務組織控制 (SOC) 報告。您可以提交安全與合規文件 (也稱為 稽核成品) 給您的稽核機構或監管機構，展示您使用的 AWS 基礎設施和服務的安全和合規性。您也可以使用這些文件作為準則，以評估您自己的雲端架構，並評估公司內部控制的有效性。

此外，還AWS Artifact提供隨需下載安全性和合規性文件，例如 ISO 認證，以及銷售其產品的獨立軟體廠商 (ISV) 的服務組織控制 (SOC) 報告AWS Marketplace。如需詳細資訊，請參閱績效AWS Marketplace詳情 Insights。

AWS客戶有責任開發或獲取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。

您也可以使用 AWS Artifact 來檢閱、接受和追蹤 AWS 協議的狀態，例如商業夥伴增補合約 (BAA)。BAA 的公司通常需要受美國健康保險流通與責任法案 (HIPAA) 的規範，以確保適當地保護受保護的醫療資訊 (PHI)。透過 AWS Artifact，您可以接受AWS 協議和指定可合法處理受限資訊的 AWS 帳戶。您可以代表多個帳戶接受協議。若要接受多個帳戶的協議，請使用 AWS Organizations 建立一個組織。

如需詳細資訊，請參閱AWS Artifact。

定價

AWS免費為您提供AWS Artifact文件和協議。

開始使用 AWS Artifact

AWS Artifact 提供 AWS 安全性與符合性報告的中央資源。其中可用的成品 AWS Artifact 包括服務組織控制 (SOC) 報告、支付卡產業 (PCI) 報告，以及來自驗證 AWS 安全控制項實作與作業有效性的認證機構的認證。此外，還 AWS Artifact 提供隨需訪問安全性和合規文件，例如 ISO 認證，以及銷售其產品的獨立軟件供應商（ISV）的服務組織控制（SOC）報告。 AWS Marketplace如需詳細資訊，請參閱AWS Marketplace 廠商洞察。

AWS Artifact 可讓您接受及管理法律合約，例如「商業夥伴增補合約」(BAA)。如果您使用 AWS Organizations，則可以代表組織內的所有帳戶接受合約。接受後，所有現有和後續的成員帳戶會自動涵蓋於協議中。

任務

- 步驟 1：註冊 AWS
- 步驟 2：下載報告
- 步驟 3：管理合約
- 步驟 4：管理通知

步驟 1：註冊 AWS

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 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。

   當您註冊時 AWS 帳戶，會建立AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

步驟 2：下載報告

您可以使用 Adobe 閱讀器下載報告。不支援其他 PDF 閱讀器。如需詳細資訊，請參閱 下載報告。

下載報告

1. 開啟主 AWS Artifact 控台，網址為 https://console.aws.amazon.com/artifact/。
2. 在 AWS Artifact 首頁上，選擇 [檢視報表]。
3. 在 [報告] 頁面上，使用 [AWS 報告] 索引標籤存取 AWS 報告，並瀏覽至 [協力廠商報告] 索引標籤，以存取銷售其產品之獨立軟體廠商 (ISV) 的報告。 AWS Marketplace
4. (選擇性) 在搜尋欄位中輸入關鍵字以尋找報表。
5. 選取報告，然後選擇 [下載報告]。
6. (選擇性) 在 [協力廠商報告] 索引標籤上，您可以按一下 [報告] 標題來存取 ISV 報告的詳細資料頁面，進一步瞭解報告。
7. 系統可能會要求您接受適用於您下載之特定報告的條款與條件。我們建議您仔細閱讀。完成後，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]。
8. 通過 PDF 查看器打開下載的文件。檢閱接受的條款與條件，然後向下捲動以尋找稽核報告。報告可能會將其他資訊作為附件嵌入 PDF 文件中，因此請務必檢查 PDF 檔案中的附件以取得支援文件。請在此處查看有關如何查看附件的說明。

第三方報告僅適用於已登入 AWS Marketplace 供應商洞察的 AWS 客戶。要了解更多信息，請參閱AWS Marketplace 供應商洞察。

步驟 3：管理合約

在您簽訂協議之前，您必須下載並同意保 AWS Artifact 密協議 (NDA) 的條款。每份合約都是機密的，不能與公司以外的其他人共用。

若要接受與的協議 AWS

1. 開啟主 AWS Artifact 控台，網址為 https://console.aws.amazon.com/artifact/。
2. 在 AWS Artifact 瀏覽窗格中，選擇 [合約]。
3. 選擇「帳戶合約」以管理帳戶的合約，或選擇「組織合約」以代表您的組織管理合約。
4. 展開合約的區段。
5. 選擇下載並查看。
6. 閱讀條款和條件。完成後，選擇「接受並下載」。
7. 複查協議，然後選取核取方塊以表示您同意。
8. 選擇「接受」以接受協議。

如需詳細資訊，請參閱 管理協定。

步驟 4：管理通知

您可以訂閱通知，以取得新報告與合約的可用性，或是現有報告與合約的更新。AWS Artifact 使用 AWS 使用者通知服務傳送通知。通知會傳送至使用者在通知組態設定期間提供的電子郵件地址。

建立模型組態

1. 在 AWS 使用者通知服務中開啟通知中樞頁面
2. 選取您要存放 AWS 使用者通知資源的區域。根據預設，您的「使用者通知」資料將儲存在美國東部 (維吉尼亞北部)，並在您選取的其他區域複寫。如需詳細資訊，請參閱通知中樞文件。
3. 點擊創建配置。
4. 若要接收合約通知，請按一下 AWS 協議更新核取方塊。
5. 若要接收報告通知，請按一下 AWS 報告更新核取方塊。若只要接收特定類別和系列的報告通知，請按一下「報告子集」核取方塊，然後按一下您感興趣的類別和系列的核取方塊。
6. 輸入組態的名稱。
7. 輸入要傳送通知的電子郵件清單 (逗號分隔)。
8. (選擇性) 若要將標籤指派給通知組態，請展開「標記」區段來輸入金鑰值配對。注意：標籤是您可以指派給 AWS 資源的標籤，每個標籤都包含可定義的金鑰和選用值。標籤可協助您管理、搜尋和篩選資源。
9. 請按 Submit (提交)。
10. 驗證電子郵件將發送到提供的電子郵件地址，並且電子郵件收件人將需要單擊發送給他們的驗證電子郵件中的「驗證電子郵件」鏈接。請注意，只有驗證的電子郵件地址才會開始接收通知。

如需更多詳細資訊，請參閱 管理通知。

下載報告 AWS Artifact

您可以從 AWS Artifact 主控台下載報告。當您從 AWS Artifact 下載報告時，會特別為您產生報告，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。要共享報告，請使用 Amazon 等安全共享服務 WorkDocs。某些報告會要求您先接受條款與條件，然後才能下載。

目錄

下載報告

若要下載報告，您必須具備必要的權限。如需詳細資訊，請參閱AWS Artifact 中的 Identity and Access Management。

當您註冊 AWS Artifact 時，您的帳戶會自動授予許可，以下載某些報告。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. 請在以下位置開啟AWS Artifact主控台。 https://console.aws.amazon.com/artifact/
2. 在AWS Artifact首頁上，選擇 [檢視報表]。
3. 在 [報告] 頁面上，使用 [AWS報告] 索引標籤存取AWS報告，並瀏覽至 [協力廠商報告] 索引標籤，以存取銷售其產品之獨立軟體廠商 (ISV) 的報告。AWS Marketplace
4. (選擇性) 在搜尋欄位中輸入關鍵字以尋找報表。
5. 選取報告，然後選擇 [下載報告]。
6. (選擇性) 在 [協力廠商報告] 索引標籤上，您可以按一下 [報告] 標題來存取 ISV 報告的詳細資料頁面，進一步瞭解報告。
7. 系統可能會要求您接受適用於您正在下載之特定報告的條款與條件。我們建議您仔細閱讀它們。完成後，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]。

8. 通過 PDF 查看器打開下載的文件。檢閱接受的條款與條件，然後向下捲動以尋找稽核報告。報告可能會將其他資訊作為附件嵌入 PDF 文件中，因此請務必檢查 PDF 檔案中的附件以取得支援文件。請在此處查看有關如何查看附件的說明。

檢視 PDF 文件中的附件

建議您使用下列目前支援檢視 PDF 附件的應用程式：

Adobe 雜技查看器

1. 從這裡下載最新版本的 Adobe
2. 在 Adobe 檢視器中開啟檔案。
3. 若要開啟「附件」面板，請按一下 PDF 文件左側的迴紋針圖示，或選擇「檢視 > 顯示/隱藏 > 導覽窗格 > 附件」。
4. 在「附件」面板中，按兩下附件以檢視文件。

火狐瀏覽器

1. 從這裡下載火狐瀏覽器
2. 使用「檔案」選單中的「開啟檔案」選項，在 Firefox 瀏覽器中開啟 PDF 檔案。
3. 若要開啟附件，請按一下畫面左上方的切換側邊欄圖示。

保護您的文件

AWS Artifact文件是機密的，應始終保持安全。 AWS Artifact對其文件使用AWS共同的責任模型。這意味著在文檔在AWS雲中時負責保護文檔的安全，但AWS是您有責任在下載文檔後保護文檔的安全。AWS Artifact您可能需要先接受條款及細則，才能下載文件。每個文件下載都有一個唯一的、可追蹤的浮水印。

您只能與公司內部標記為機密的文件、您的監管機構以及您的稽核人員共用。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用服務 (例如 Amazon WorkDocs) 與他人共用文件。不要通過電子郵件發送文檔或將其上傳到不安全的網站。

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常見問題集中的疑難排解。

管理協定 AWS Artifact

AWS Artifact 協議可讓您使用 AWS Management Console 來為您的帳戶或組織檢閱、接受和管理協議。例如，商業夥伴增補合約 (BAA) 的公司通常需要受美國健康保險流通與責任法案 (HIPAA) 的規範，以確保適當地保護受保護的醫療資訊 (PHI)。您可以使用 AWS Artifact 接受協議 (例如 BAA AWS)，並指定一個可合法處理 PHI 的 AWS 帳戶。如果您使用 AWS Organizations，您可以代表組織中的所有帳戶接受協議 (例如 AWS 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，以及檢閱所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合約，您可以使用AWS Artifact來終止合約。如果您終止協議，但後來意識到您需要它，則可以再次激活它。

目錄

管理單一帳戶的合約 AWS Artifact

您可以只針對您的帳戶接受協議，即使您的帳戶在 AWS Organizations 中為組織的成員帳戶。如需有關 AWS Organizations 的詳細資訊，請參閱《使用者指南》AWS Organizations。

接受與的協議 AWS

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，則可以授予具有角色的 IAM 使用者和聯合身分使用者存取和管理一或多個合約的權限。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具有以下許可：

```
artifact:DownloadAgreement
artifact:AcceptAgreement
```

如需詳細資訊，請參閱身分識別和存取管理。

接受協議與 AWS

1. 請在以下位置開啟AWS Artifact主控台。 https://console.aws.amazon.com/artifact/
2. 在 AWS Artifact 導覽窗格上，選擇 Agreements (協議)。
3. 選擇 Account agreements (帳戶協議) 標籤。
4. 展開合約的區段。
5. 選擇下載並查看。
6. 閱讀條款和條件。完成後，選擇「接受並下載」。
7. 複查協議，然後選取核取方塊以表示您同意。
8. 選擇「接受」以接受您帳戶的合約。

終止協議 AWS

如果使用 AWS Artifact 主控台接受協議，您可以使用主控台來終止該協議。否則，請參閱離線協議。

所需的許可

若要終止協議，IAM 和聯合身分使用者必須具有以下許可：

```
artifact:TerminateAgreement
```

如需詳細資訊，請參閱身分識別和存取管理。

若要終止 AWS 的線上協議

1. 請在以下位置開啟AWS Artifact主控台。 https://console.aws.amazon.com/artifact/
2. 在 AWS Artifact 導覽窗格上，選擇 Agreements (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，表示您同意終止協定。
6. 選擇 Terminate (終止)。出現確認提示時，請選擇終止。

管理多個帳戶的合約 AWS Artifact

如果您是組織管理帳戶的擁有者，您可以代表AWS Organizations組織中的所有帳戶接受合約。您必須以正確的AWS Artifact權限登入管理帳戶，才能接受或終止組織合約。具有

organizations:DescribeOrganization 許可的成員帳戶使用者可以檢視所代表接受的組織協議。

如果您的帳戶不屬於組織，您可以按照AWS Organizations使用者指南中的建立和管理組織中的指示來建立或加入組織。

AWS Organizations 有兩個可用的功能集：合併帳單功能和所有功能。若要為您的組織使用 AWS Artifact，您所屬的組織必須啟用才能使用所有功能。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。

如果成員帳戶被從組織中移除，該成員帳戶即不再涵蓋於組織協議中。管理帳戶管理員應在從組織移除成員帳戶之前，與成員帳戶溝通此事，以便在必要時成員帳戶可以簽訂新的協議。您可以在「組織協定」中檢視使用中AWS Artifact組織協定的清單。

如需詳細資訊，請參閱AWS Organizations使用者指南中的管理組織中的 AWS 帳戶。

接受貴組織的合約

您可以在 AWS Organizations 中代表組織中的所有成員帳戶接受協議。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

若要接受合約，管理帳戶的擁有者必須具備下列權限：

```
artifact:DownloadAgreement
artifact:AcceptAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

如需詳細資訊，請參閱身分識別和存取管理。

為組織接受協議

1. 請在以下位置開啟AWS Artifact主控台。 https://console.aws.amazon.com/artifact/
2. 在 AWS Artifact 儀表板上，選擇 Agreements (協議)。

3. 選擇 Organization agreements (組織帳戶) 標籤。
4. 展開合約的區段。
5. 選擇下載並查看。
6. 閱讀條款和條件。完成後，選擇「接受並下載」。
7. 複查協議，然後選取核取方塊以表示您同意。
8. 選擇 Accept (接受)，為組織中所有現有和未來的帳戶接受協議。

終止組織協議

如果您使用 AWS Artifact 主控台代表組織中所有成員帳戶接受協議，您可以使用主控台來終止該協議。否則，請參閱離線協議。

所需的許可

若要終止合約，管理帳戶的擁有者必須具備下列權限：

```
artifact:DownloadAgreement
artifact:TerminateAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

如需詳細資訊，請參閱身分識別和存取管理。

若要終止 AWS 的線上組織協議

1. 請在以下位置開啟AWS Artifact主控台。 https://console.aws.amazon.com/artifact/
2. 在 AWS Artifact 儀表板上，選擇 Agreements (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，表示您同意終止協定。
6. 選擇 Terminate (終止)。出現確認提示時，請選擇終止。

管理中的現有離線協定 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。

如果您的帳戶是AWS Organizations組織中的管理帳戶，您可以使AWS Artifact用將離線合約的條款套用至組織中的所有帳戶。若要將離線接受的協議套用到您的組織和組織中的所有帳戶，您必須擁有以下許可：

```
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

如果您的帳戶是組織中的成員帳戶，您必須擁有以下許可才能查看離線組織協議：

```
organizations:DescribeOrganization
```

如需詳細資訊，請參閱 身分識別和存取管理。

管理通知 AWS Artifact

AWS Artifact 通知可讓您設定電子郵件通知。在通知設定頁面上，您可以訂閱通知並管理其他通知設定，如下所述。AWS Artifact 使用 AWS 使用者通知服務傳送通知。若要使用 AWS Artifact 通知，您必須擁有 AWS Artifact 和 AWS 使用者通知服務的必要許可。如需詳細資訊，請參閱身分識別和存取管理。

目錄

設定通知

在開始接收通知之前，您需要指定要儲存「使用者通知」資料的區域。請依照下列步驟設定通知中樞。

若要設定通知中樞

1. 在 AWS 使用者通知服務中開啟通知中樞頁面。
2. 選取您要存放 AWS 使用者通知資源的區域。根據預設，您的「使用者通知」資料將儲存在美國東部 (維吉尼亞北部)，並且會在您選取的其他區域複寫。如需詳細資訊，請參閱通知中樞文件。
3. 請按 Submit (提交)。

訂閱 通知

1. 開啟 AWS Artifact 通知設定頁面。
2. 按一下訂閱成品通知切換以訂閱 AWS Artifact 上的通知。

取消訂閱通知

1. 開啟 AWS Artifact 通知設定頁面。
2. 按一下訂閱成品通知切換，即可取消訂閱 AWS Artitfact 上的通知。

建立模型組態

1. 開啟 AWS Artifact 通知設定頁面。
2. 按一下建立組態。
3. 若要接收合約通知，請保持選取 AWS 協議更新旁邊的核取方塊。
4. 若要接收報告通知，請保持選取 AWS 報告更新旁邊的核取方塊。
5. 若要接收所有報告的通知，請保持選取 [所有報告] 旁的核取方塊。
6. 若只要針對特定類別和系列的報告接收通知，請按一下報告子集的核取方塊。然後，單擊您感興趣的類別和系列的複選框。
7. 輸入組態的名稱。
8. 輸入要傳送通知的電子郵件清單 (以逗號分隔)。
9. (選擇性) 若要將標籤指派給通知組態，請展開「標記」區段來輸入金鑰值配對。注意：標籤是您可以指派給 AWS 資源的標籤，每個標籤都包含可定義的金鑰和選用值。標籤可協助您管理、搜尋和篩選資源。
10. 按一下建立組態。
11. 驗證電子郵件將發送到提供的電子郵件地址，並且電子郵件收件人將需要單擊發送給他們的驗證電子郵件中的「驗證電子郵件」鏈接。請注意，只有驗證的電子郵件地址才會開始接收通知。

編輯組態

1. 開啟 AWS Artifact 通知設定頁面。
2. 按一下您要編輯的組態列。
3. 按一下頁面右上角的「編輯」按鈕。
4. 您可以編輯任何欄位。一旦您滿意您的變更，請按儲存變更。
5. 如果您添加了新的電子郵件地址，則會向每個電子郵件地址發送驗證電子郵件。按一下驗證電子郵件中的驗證電子郵件連結。

刪除組態

1. 開啟 AWS Artifact 通知設定頁面。
2. 按一下您要刪除的組態列。
3. 按一下 Delete (刪除)。
4. 閱讀警告訊息後，按一下「刪除」。

指派標籤給組態

標籤是您指派給 AWS 資源的標籤。每個標籤皆包含由您定義的一個金鑰與一個選用值。標籤可協助您管理、搜尋和篩選資源。您可以在建立或編輯組態時選擇性地設定標籤。要閱讀更多信息，請參閱標記資源

疑難排解

如果您在使用 AWS Artifact 通知時收到錯誤訊息，請參閱AWS Artifact常見問答集中的疑難排解。

AWS Artifact 中的 Identity and Access Management

當您註冊 AWS 時，您會提供與 AWS 帳戶相關聯的電子郵件地址和密碼。這些是您的根憑證，它們提供對所有AWS資源的完整存取權，包括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。

您應該為自己和可能需要存取中文件或合約的任何人建立一個稱為 IAM 使用者的特殊使用者身分，而不是使用根登入憑證或與他人共用您的登入資料登入您的AWS帳戶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。您也可以將許可授與 IAM 群組，然後將 IAM 使用者新增至群組，以授予多個 IAM 使用者相同的許可。

如果您已經在外部管理使用者身分AWS，則可以使用 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識別提供者和聯合。

目錄

設定使用者存取 AWS Artifact

完成下列步驟，AWS Artifact根據使用者所需的存取層級授與權限。

任務

步驟 1：建立 IAM 政策

身為 IAM 管理員，您可以建立政策來授與AWS Artifact動作和資源的許可。

建立 IAM 政策

使用下列程序建立 IAM 政策，以便將許可授與 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。您可以建立自己的策略，也可以從中使用其中一個策略範例 IAM 政策。
6. 選擇檢閱政策。政策驗證程式會回報任何語法錯誤。
7. 在 [檢閱原則] 頁面上，輸入可協助您記住原則用途的唯一名稱。您也可以提供描述。
8. 選擇建立政策。

步驟 2：建立 IAM 群組並附加政策

身為 IAM 管理員，您可以建立群組，並將您建立的政策附加到群組。您可以隨時將 IAM 使用者新增至群組。

建立 IAM 群組並附加您的政策

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. 在群組名稱中，輸入群組的名稱，然後選擇下一步。
3. 在搜尋欄位中，輸入您建立之策略的名稱。選取原則的核取方塊，然後選擇 [下一步]。
4. 檢閱群組名稱和政策。準備就緒時，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。這會授與使用者授與群組的權限。

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. 在使用者名稱中，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 Next: Permissions (下一步：許可)。
5. 選擇 [新增使用者至群組]，然後選取您建立的群組。
6. 選擇下一步：標籤。您可以選擇性地向使用者新增標籤。
7. 選擇 下一步：檢閱。準備就緒後，請選擇 [建立使用者]。

移轉至精細的權限

AWS Artifact 現在可讓客戶使用精細的許可。透過這些精細的權限，客戶可以精細控制提供功能的存取權，例如接受條款和下載報告。

若要透過精細的權限存取報表，客戶應該利用AWSArtifactReportsReadOnlyAccess 受管政策或依照下列建議更新其權限。然後，客戶應該使用主控台中提供的新 AWS 報告頁面連結來選擇加入。

如果更新至新權限發生問題，使用者可以選擇透過使用主控台中可用的舊報告頁面連結來存取具有舊權限的報告。

移轉至新權限

移轉非資源特定權限

使用者需要將包含舊版權限的現有原則取代為包含精細權限的原則

舊版政策：

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

具有精細權限的新政策：

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

移轉資源特定權限

使用者必須將包含舊版權限的現有原則取代為包含精細權限的原則。報表資源萬用字元權限已被條件索引鍵取代。

舊版政策：

```
{
  "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/*"
      ]
    }
  ]
}
```

具有精細權限和條件金鑰的新原則。

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

範例 IAM 政策

您可以建立許可政策，將許可授與 IAM 使用者。您可以授與使用者存取 AWS Artifact 報表，以及代表單一帳戶或組織接受和下載合約的能力。

下列範例政策顯示您可以根據他們需要的存取層級指派給 IAM 使用者的許可。

- 使用精細權限管理 AWS 報表的範例原則
- 管理第三方報告的原則範例
- 管理合約的原則範例
- 要整合的原則範例 AWS Organizations
- 管理管理帳戶合約的範例原則
- 管理組織協議的原則範例
- 管理通知的原則範例

Example 透過精細權限管理 AWS 報表的範例原則

> **Tip**
>
> 您應該考慮使用受AWSArtifactReportsReadOnlyAccess 管政策，而不是定義自己的策略。

下列原則授與透過精細權限下載所有 AWS 報表的權限。

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

下列原則授予透過精細權限僅下載 AWS SOC、PCI 和 ISO 報告的權限。

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

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

Example 管理第三方報告的原則範例

> **Tip**
>
> 您應該考慮使用受AWSArtifactReportsReadOnlyAccess 管政策，而不是定義自己的策略。

第三方報告由 IAM 資源`report`表示。

下列原則會授與所有協力廠商報告功能的權限。

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

```
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

下列原則授與下載協力廠商報告的權限。

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

下列原則授與列出第三方報告的權限。

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

下列原則授與檢視所有版本之協力廠商報告詳細資料的權限。

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

下列原則授與檢視特定版本之協力廠商報告詳細資料的權限。

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

Example 管理合約的原則範例

下列原則授與下載所有合約的權限。IAM 使用者也必須擁有此權限才能接受協議。

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

下列原則授與接受合約的權限。

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

下列原則授與終止合約的權限。

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

```
      ]
    }
  ]
}
```

下列原則授與管理單一帳戶合約的權限。

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

Example 要整合的原則範例 AWS Organizations

下列政策授予建立 AWS Artifact 用於整合的 IAM 角色的權限 AWS Organizations。您組織的管理帳戶必須具有這些權限，才能開始使用組織合約。

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

下列原則授與授與使 AWS Artifact 用權限的權限 AWS Organizations。您組織的管理帳戶必須具有這些權限，才能開始使用組織合約。

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

Example 管理管理帳戶合約的範例原則

下列策略授與管理帳戶管理合約的權限。

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

Example 管理組織協議的原則範例

下列原則授與管理組織合約的權限。其他具有必要權限的使用者必須設定組織合約。

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

下列原則授與檢視組織合約的權限。

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

Example 管理通知的原則範例

下列原則授與使用 AWS Artifact 通知的完整權限。

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

下列原則授與列出所有組態的權限。

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

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

下列原則授與建立組態的權限。

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

下列原則授與編輯組態的權限。

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

下列原則授與刪除組態的權限。

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

```
      ]
    }
  ]
}
```

下列原則授與檢視組態詳細資料的權限。

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

下列原則授與註冊或取消註冊通知中樞的權限。

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

```
}
```

AWSAWS Artifact 的受管政策

AWS 管理的政策是由 AWS 建立和管理的獨立政策。AWS 管理的政策的設計在於為許多常見使用案例提供許可，如此您就可以開始將許可指派給使用者、群組和角色。

請謹記，AWS 管理的政策可能不會授予您特定使用案例的最低權限許可，因為它們可供所有 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。

您無法更改 AWS 管理的政策中定義的許可。如果 AWS 更新 AWS 管理的政策中定義的許可，更新會影響政策連接的所有主體身分 (使用者、群組和角色)。在推出新的 AWS 服務 或有新的 API 操作可供現有服務使用時，AWS 很可能會更新 AWS 管理的政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS受管理的策略： AWSArtifactReportsReadOnlyAccess

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

此原則會授與##權限，以便列出、檢視和下載報表。

許可詳細資訊

此政策包含以下許可。

- `artifact`-可讓主參與者從AWS Artifact中列出、檢視及下載報告。

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

```
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS受管策略的 Artifact 更新

檢視有關 Artifact 為此服務開始追蹤這些變更後，AWS受管理原則的更新詳細資訊。如需有關此頁面變更的自動警示，請訂閱「Artifact 文件歷史記錄」頁面上的 RSS 摘要。

變更	描述	日期
Artifact 開始追蹤變	Artifact 開始追蹤其AWS受管理原則的變更並引入 AWSArtifactReportsReadOnlyAccess。	2023-12-15

針對 AWS Artifact 使用服務連結角色

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

服務連結角色可讓您輕鬆設定 AWS Artifact，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，否則只有 AWS Artifact 可以擔任其角色。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。這樣可以保護您的 AWS Artifact 資源，因為您無法意外移除存取資源的許可。

如需關於支援服務連結角色的其他服務資訊，請參閱《可搭配 IAM 運作的 AWS 服務》，尋找 Service-linked roles (服務連結角色) 欄中顯示為 Yes (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。

AWS Artifact 的服務連結角色許可

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

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

- `artifact.amazonaws.com`

名為的角色許可政策 AWSArtifactServiceRolePolicy 允許 AWS Artifact 對`organizations`資源完成以下動作。

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

為 AWS Artifact 建立服務連結角色

您不需要手動建立一個服務連結角色。當您造訪組織管理帳戶中的組織協議索引標籤，並選取中的「開始使用」連結時AWS Management Console，AWS Artifact 會為您建立服務連結角色。

若您刪除此服務連結角色然後需要再次建立，便可在帳戶中使用相同程序重新建立角色。當您造訪組織管理帳戶中的「組織協議」索引標籤並選取「開始使用」連結時，AWS Artifact 會再次為您建立服務連結角色。

編輯 AWS Artifact 的服務連結角色

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 使用者指南中的編輯服務連結角色。

刪除 AWS Artifact 的服務連結角色

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

> **Note**
>
> 如果您嘗試刪除資源時，AWS Artifact 服務正在使用該角色，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。

若要刪除使用的 AWS Artifact 資源 AWSServiceRoleForArtifact

1. 瀏覽 AWS Artifact 主控台中的「組織協議」表格
2. 終止任何有效的組織協議

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台或 AWS API 刪除 AWSServiceRoleForArtifact 服務連結角色。AWS CLI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 服務連結角色的支援區域

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

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

區域名稱	區域身分	AWS Artifact 中的 Support
亞太區域 (大阪)	ap-northeast-3	否
亞太區域 (首爾)	ap-northeast-2	否
亞太區域 (新加坡)	ap-southeast-1	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
歐洲 (巴黎)	eu-west-3	否
歐洲 (斯德哥爾摩)	eu-north-1	否
中東 (巴林)	me-south-1	否
中東 (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	否

使用 IAM 條件金鑰

您可以使用 IAM 條件金鑰，根據特定的報告類別和系列，提供對 AWS Artifact 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報告讀取存取權限的範例原則

AWS Artifact報告由 IAM 資源表示。`report`

下列政策授予讀取該`Certifications and Attestations`類別下所有AWS Artifact報告的權限。

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

下列原則可讓您授與讀取SOC系列下所有AWS Artifact報告的權限。

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

下列原則可讓您授與讀取所有AWS Artifact報告的權限，但Certifications and Attestations類別下的報告除外。

```
{
  "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 AWS CloudTrail 記錄 AWS Artifact API 呼叫

AWS Artifact與 (提供中的使用者AWS CloudTrail、角色或服務所採取的動作記錄) 的AWS服務整合 AWS Artifact。 CloudTrail 擷取AWS Artifact做為事件的 API 呼叫。擷取的呼叫包括從 AWS Artifact 主控台進行的呼叫，以及針對 AWS Artifact API 操作的程式碼呼叫。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AWS Artifact. 如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷提出的要求AWS Artifact、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail用者指南。

AWS Artifact中的資訊 CloudTrail

CloudTrail 在您創建帳戶AWS 帳戶時啟用。當活動發生在中時AWS Artifact，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。

如需您 AWS 帳戶 帳戶中正在進行事件的記錄 (包含 AWS Artifact 的事件)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他AWS服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

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

AWS Artifact支援將下列動作記錄為記 CloudTrail 錄檔中的事件：

- ListReports
- GetAccountSettings
- GetReportMetadata
- GetReport
- GetTermForReport
- PutAccountSettings

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

- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務提出。

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

了解 AWS Artifact 日誌檔案項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

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


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

AWS Artifact 的文件歷程記錄

下表說明 AWS Artifact 各版本。

變更	描述	日期
精細的報表存取和 AWSArtifactReportReadOnlyAccess 受管原則	啟用對 Artifact 報表、啟用報表條件金鑰和啟動的AWSArtifactReportsReadOnlyAccess 受管理原則的精細存取。	2023 年 12 月 15 日
AWS Artifact 服務連結角色	針對 AWS 成品和 AWS Organizations 整合新增服務連結角色文 Artifact 和更新的範例政策。	2023 年 9 月 26 日
通知	發佈用於管理通知的文件，並對 API 參考指南、CloudTrail 記錄文件和 AWS Artifact Identity and Access Management 頁面進行相關更新。	2023 年 8 月 1 日
第三方報告-一般提供	添加了 API 參考文檔，CloudTrail 日誌文檔，並使第三方報告正式可用。	2023 年 1 月 27 日
第三方報告 (預覽版)	針對銷售其產品的獨立軟體廠商 (ISV) 推出合規性報告。AWS Marketplace此外，將範例原則新增至第三方報告的 [身分識別與存取管理] 頁面。	2022 年 11 月 30 日
安全性	新增「身分識別與存取管理」頁面的區段，以防止混淆副手。	2021 年 12 月 20 日

報告	移除保密合約，並引入了報表下載的條款與條件。	2020 年 12 月 17 日
主頁和搜索	在報告和合約頁面上新增服務首頁和搜尋列。	2020 年 5 月 15 日
GovCloud 啟動	AWS Artifact在 GovCloud 地區推出。	2019 年 11 月 7 日
AWS Organizations協議	已新增對管理組織合約的支援。	2018 年 6 月 20 日
協議	已新增管理合AWS Artifact約的支援。	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。