aws

管理指南

AWS AppFabric

AWS AppFabric: 管理指南

Table of Contents

什麼是 AWS AppFabric？

AWS AppFabric 快速連接整個組織的軟體即服務 (SaaS) 應用程式，讓 IT 和安全團隊可以使用標準結構描述輕鬆管理和保護應用程式，員工可以使用生成式 AI 更快完成日常工作。

主題

產品

探索以下兩個方面 AWS AppFabric： AppFabric 針對安全性、專為簡化管理和安全性而設計，以及 AppFabric 透過生成式 AI 功能強化生產力 (預覽)。如需詳細資訊，請參閱下列主題：

- 什麼是 AWS AppFabric 安全性？
- 什麼是 AWS AppFabric 生產力？

優勢

您可以使用 AppFabric 來執行下列動作：

- 在幾分鐘內 Connect 您的應用程式，並降低營運成本。
- 提高 SaaS 應用程式資料的可見度，以提升您的安全狀態。
- 利用生成式 AI 自動促進跨應用程式的工作。

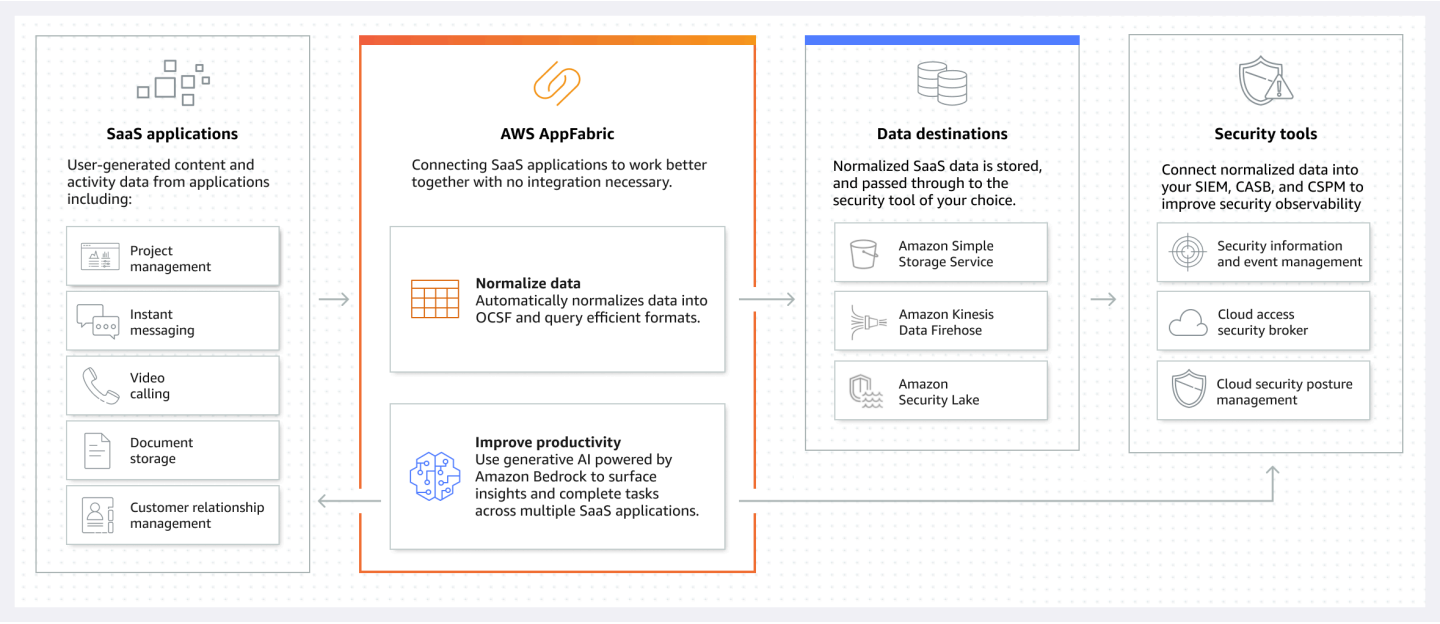
使用案例

您可以使 AppFabric 用：

- 快速 Connect 您的 SaaS 應用程式
  - AppFabric 對於安全性，將頂尖的 SaaS 生產力和安全性應用程式原生連接起來，提供完全受控的 SaaS 互通性解決方案。
- 提升您的安全態勢
  - 應用程式資料會自動標準化，讓管理員能夠設定通用原則、標準化安全警示，並輕鬆管理多個應用程式的使用者存取。
- 重新想像生產力
  - 有了通用的生成 AI 助理， AppFabric 提高生產力，員工能夠快速獲得答案、自動化任務管理，並在其 SaaS 生產力應用程式中產生深入分析。

如何 AppFabric 工作

AppFabric 快速連接多個 SaaS 應用程式，無需編碼即可提高生產力和安全性。下圖顯示的好處 AppFabric。



> **Note**
>
> AppFabric 提高生產力目前以預覽版的形式推出，並於美國東部 (維吉尼亞北部) 提供 AWS 區域。如需相關資AWS AppFabric 訊 AWS 區域，請參閱 AWS 一般參考.

定價

如需 AppFabric 定價詳細資訊和範例，請參閱AWS AppFabric 定價。

可用性

若要檢視目前支援的 AWS 區域和端點 AppFabric，請參閱AWS 一般參考中的AWS AppFabric 端點和配額。

什麼是 AWS AppFabric 安全性？

AWS AppFabric 為了達到安全性，可快速連接整個組織的軟體即服務 (SaaS) 應用程式，因此 IT 和安全團隊可以使用標準結構描述輕鬆管理和保護應用程式。

主題

優勢

您可以使用以確 AppFabric 保安全性來執行以下操作：

- 在幾分鐘內 Connect 您的應用程式，並降低營運成本。
- 提高 SaaS 應用程式資料的可見度，以提升您的安全狀態。

使用案例

您可以使 AppFabric 用以下安全性：

- 快速 Connect 您的 SaaS 應用程式
  - AppFabric 對於安全性，將頂尖的 SaaS 生產力和安全性應用程式原生連接起來，提供完全受控的 SaaS 互通性解決方案。
- 提升您的安全態勢
  - 應用程式資料會自動標準化，讓系統管理員能夠設定通用原則、標準化安全警示，並輕鬆管理多個應用程式的使用者存取。

AppFabric 為了安全而存取

AppFabric 安全性目前已在美國東部 (維吉尼亞北部)、歐洲 (愛爾蘭) 和亞太區域 (東京) 提供 AWS 區域。如需有關的詳細AWS AppFabric 資訊 AWS 區域，請參閱 AWS 一般參考.

在每個區域中，您可以通 AppFabric 過以下任何一種方式訪問以確保安全：

AWS Management Console

這 AWS Management Console 是一個基於瀏覽器的介面，您可以使用它來建立和管理 AWS 資源。主 AppFabric 控台可讓您存取 AppFabric 資源。您可以使用主 AppFabric控台來建立和管理所有 AppFabric 資源。

AppFabric API

若要 AppFabric 以程式設計方式存取，請使用 AppFabric API，並直接向服務發出 HTTPS 要求。如需詳細資訊，請參閱 AWS AppFabric API 參考資料。

AWS Command Line Interface (AWS CLI)

使用時 AWS CLI，您可以在系統的指令列中發出指令以 AppFabric與其他互動 AWS 服務。如果您想要建置執行工作的指令碼，命令列工具也很有用。若要取得有關安裝和使用的資訊 AWS CLI，請參閱第 2 版的使用AWS Command Line Interface 者指南。若要取得有關的 AWS CLI 指令的資訊 AppFabric，請參閱〈AWS CLI 參考〉—AppFabric 節。

相關服務

AppFabric 為了安全 AWS 服務 起見，您可以使用以下內容：

Amazon 數據 Firehose

Amazon Data Firehose 是一種擷取、轉換和載入 (ETL) 服務，可靠地擷取、轉換串流資料並將其交付到資料湖、資料存放區和分析服務。使用時 AppFabric，您可以選擇將 JSON 格式的開放網路安全結構描述架構 (OCSF) 標準化或原始稽核記錄輸出至 Firehose 串流作為目的地。如需詳細資訊，請參閱在 Firehose 中建立輸出位置。

Amazon Security Lake

Amazon Security Lake 會自動將來自 AWS 環境、SaaS 供應商、內部部署和雲端來源的安全資料集中到存放在您帳戶中的專用資料湖。您可以將 AppFabric 稽核日誌資料與安全湖整合，方法是選取 Amazon 資料 Firehose 做為目的地，然後設定 Firehose 在安全湖中以正確的格式和路徑交付資料。如需詳細資訊，請參閱 Amazon Security Lake 使用者指南中的從自訂來源收集資料。

Amazon Simple Storage Service

Amazon Simple Storage Service (Amazon S3) 是一種物件儲存服務，提供業界領先的可擴展性、資料可用性、安全性和效能。使用時 AppFabric，您可以選擇將 OCSF 標準化 (JSON 或Apache Parquet) 或原始 (JSON) 稽核日誌輸出到新的或現有的 Amazon S3 儲存貯體做為目的地。如需詳細資訊，請參閱在 Amazon S3 中建立輸出位置。

Amazon QuickSight

Amazon 透過超大規模統一商業智慧 (BI) 為資料驅動的組織提 QuickSight 供支援。透過現代化的互動式儀表板 QuickSight、分頁報告、嵌入式分析和自然語言查詢，所有使用者都可以從相同的事實來源滿足各種分析需求。您可以選擇將日誌存放為來源的 Amazon S3 儲存貯體來分析中 QuickSight的 AppFabric 稽核 AppFabric 日誌資料。如需詳細資訊，請參閱 Amazon 使用 QuickSight 者指南中的使用 Amazon S3 檔案建立資料集。您也可以將 Amazon S3 中的 AppFabric 資料匯入亞馬 Amazon Athena，然後選取 Amazon Athena 做為中的資料來源 QuickSight。如需詳細資訊，請參閱 Amazon 使用 QuickSight 者指南中的使用 Amazon Athena 資料建立資料集。

AWS Key Management Service

使用 AWS Key Management Service (AWS KMS)，您可以在應用程式和. 中建立、管理和控制加密金鑰。 AWS 服務當您在中建立應用程式套件組合時 AppFabric，您會設定加密金鑰，以安全地保護您授權的應用程式資料。此金鑰會加密您在 AppFabric 服務中的資料。 AppFabric 可以使用由您 AWS 擁有的金鑰 創建和管理 AppFabric 的代表，或者您在其中創建和管理的客戶管理密鑰 AWS KMS。如需詳細資訊，請參閱建立 AWS KMS 金鑰。

開放式網路安全架構

開放網絡安全架構框架（OCSF）是網絡安全行業領先合作夥伴 AWS 和領先合作夥伴的協作開源工作。OCSF 提供常見安全性事件的標準結構描述、定義版本控制準則以促進結構描述演進，並包含安全性記錄檔產生者和取用者的自我控管程序。OCSF 的公開原始程式碼託管於 GitHub.

以 OCF 為基礎的結構描述 AppFabric

基 AWS AppFabric 於安全性 OCSF 1.0.0-rc.3 的結構描述專為滿足您對軟體即服務 (SaaS) 產品組合的標準化、一致、低精力可觀察性的需求而量身打造。 AppFabric與 OCSF 開放原始碼社群合作，引入了新的 OCSF 事件類別、事件類別、活動和物件，以便 OCSF 適用於 SaaS 應用程式事件。AppFabric 自動標準化從 SaaS 應用程式接收到的稽核事件，並將此資料傳遞至您的 Amazon 簡單儲存服務 (Amazon S3) 或 Amazon 資料 Firehose 服務。 AWS 帳戶對於 Amazon S3 目的地，您可以選擇兩個標準化選項 (OCSF 或原始) 和兩種資料格式選項 (JSON 或Parquet)。傳送至 Firehose 時，您也可以選擇兩個標準化選項 (OCSF 或 Raw)，但資料格式僅限於 JSON。

OCSF 活動類別和類別

AppFabric 使用下列兩個 OCSF 事件類別：

- Identity and Access Management — AppFabric 為了安全起見，請在此類別中使用下列事件類別：
  - 帳戶變更
  - 身分驗證
  - 使用者存取管理
  - 群組管理
- 應用程序活動- AppFabric 為了安全起見，使用此類別中的以下事件類：
  - 網路資源活動
  - Web 資源存取活動

先決條件和建議

如果您是新 AWS 客戶，請先完成此頁面上列出的設定先決條件，然後再開始使 AWS AppFabric 用以確保安全性。對於這些設定程序，可以使用 AWS Identity and Access Management (IAM) 服務。如需 IAM 的完整資訊，請參閱《IAM 使用者指南》。

主題

- 註冊一個 AWS 帳戶
- 建立具有管理權限的使用者
- (必填) 完整的申請先決條件
- (選擇性) 建立輸出位置
- (選擇性) 建立 AWS KMS 金鑰

註冊一個 AWS 帳戶

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。

   當您註冊一個時 AWS 帳戶，將創建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。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理權限的使用者

註冊後，請保護您的 AWS 帳戶 AWS 帳戶根使用者 AWS IAM Identity Center、啟用和建立系統管理使用者，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

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

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。
2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

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

建立具有管理權限的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南中的啟用 AWS IAM Identity Center。
2. 在 IAM 身分中心中，將管理存取權授予使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。

以具有管理權限的使用者身分登入

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

  如需使用 IAM 身分中心使用者登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「建立權限集」。
2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

   如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「新增群組」。

(必填) 完整的申請先決條件

若要使 AppFabric 用安全性來接收應用程式的使用者資訊和稽核記錄，許多應用程式都需要您具有特定的角色和計劃類型。請確定您已針對您要授權安全性的每個應用程式複查先決條件，且您擁有適當的計劃與角色。 AppFabric 如需應用程式特定先決條件的相關資訊，請參閱支援的應用程式，或選擇下列其中一個應用程式特定主題。

- 1Password
- Asana
- Azure Monitor
- Atlassian Confluence

- Atlassian Jira suite
- Box
- Cisco Duo
- Dropbox
- Genesys Cloud
- GitHub
- Google Analytics
- Google Workspace
- HubSpot
- IBM Security® Verify
- Microsoft365
- Miro
- Okta
- OneLogin by One Identity
- PagerDuty
- Ping Identity
- Salesforce
- ServiceNow
- Singularity Cloud
- Slack
- Smartsheet
- Terraform Cloud
- Webex by Cisco
- Zendesk
- Zoom

(選擇性) 建立輸出位置

AppFabric 對於安全性，支持 Amazon Simple Storage Service (Amazon S3) 和 Amazon 數據 Firehose 作為審計日誌導入目的地。

Amazon S3

您可以在建立擷取目的地時，使用主 AppFabric 控台建立新的 Amazon S3 儲存貯體。您也可以使用 Amazon S3 服務建立儲存貯體。如果您選擇使用 Amazon S3 服務建立儲存貯體，則必須在建立 AppFabric 擷取目的地之前建立儲存貯體，然後在建立擷取目標時選取儲存貯體。您可以選擇在您的儲存貯體中使用現有的 Amazon S3 儲存貯體 AWS 帳戶，只要它符合現有儲存貯體的下列要求：

- AppFabric 為了安全起見，您的 Amazon S3 儲存貯體必須與您的 Amazon S3 資源位於 AWS 區域相同的位置。
- 您可以使用下列其中一種方式加密儲存貯體：
  - 使用 Amazon S3 受管金鑰 (SSE-S3) 的伺服器端加密
  - 使用預 AWS 受管金鑰 設值 AWS Key Management Service (AWS KMS) 金鑰 (SSE-KMS) 進行伺服器端加密。`aws/s3`

Amazon 數據 Firehose

您可以選擇使用 Amazon 資料 Firehose 做為安全資料的擷取目 AppFabric 的地。若要使用 Firehose，您可以在建立擷取 AWS 帳戶 之前或在中建立擷取目的地時，先在中建立 Firehose 傳送串流。AppFabric您可以使用 AWS Management Console、 AWS CLI或 AWS API 或 SDK 建立 Firehose 交付串流。如需串流設定指示，請參閱下列主題：

- AWS Management Console 說明 — 在 Amazon 數據 Firehose 開發人員指南中創建 Amazon 數據 Firehose 交付流
- AWS CLI 指示 — create-delivery-stream在AWS CLI 指令參考中
- AWS API 和 SDK 說明 — CreateDeliveryStream在 Amazon 數據 Firehose API 參考

使用 Amazon 資料 Firehose 做為安全輸出目的地的要求如下： AppFabric

- 您必須建立與您的安全性資源 AWS 區域 相同 AppFabric 的串流。
- 您必須選取「直接放入」作為來源。
- 將AmazonKinesisFirehoseFullAccess AWS 受管理的原則附加至您的使用者，或將下列權限附加至您的使用者：

```
{
    "Sid": "TagFirehoseDeliveryStream",
    "Effect": "Allow",
    "Action": ["firehose:TagDeliveryStream"],
```

```
    "Condition": {
        "ForAllValues:StringEquals": {"aws:TagKeys": "AWSAppFabricManaged"}
    },
    "Resource": "arn:aws:firehose:*:*:deliverystream/*"
}
```

Firehose 支援與各種協力廠商安全性工具的整合，例如Splunk和Logz.io. 如需如何正確設定 Amazon Kinesis 以便將資料輸出到這些工具的詳細資訊，請參閱 Amazon 資料 Firehose 開發人員指南中的目的地設定。

(選擇性) 建立 AWS KMS 金鑰

在建立 For Security 應用程式 AppFabric 套件組合的過程中，您將選取或設定加密金鑰，以安全地保護您的資料不受所有授權應用程式的攻擊。此金鑰將用於加密您在 AppFabric 服務中的資料。

AppFabric 為了安全默認加密數據。 AppFabric 為了安全起見，可以使用由 AppFabric 您 AWS 擁有的金鑰 創建和管理的代表或您在 AWS Key Management Service （AWS KMS）中創建和管理的客戶管理密鑰。 AWS 擁有的金鑰 是 AWS 服務 擁有和管理以在多個中使用的 AWS KMS 密鑰的集合 AWS 帳戶。客戶管理的 AWS KMS 金鑰是您 AWS 帳戶 建立、擁有及管理的金鑰。如需有關 AWS 擁有的金鑰 和客戶管理金鑰的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的客戶 AWS 金鑰和金鑰。

為了安全起見，如果您想使用客戶託管密鑰來加密數據（例如授權令牌），則可以使用 AWS KMS. AppFabric 如需有關授與客戶管理金鑰存取權的權限原則的詳細資訊 AWS KMS，請參閱本指南的「金鑰政策」一節。

AWS AppFabric 為了安全起見，開始使用

AWS AppFabric 為了安全起見，您必須先創建一個應用程序包，然後授權並將應用程序連接到您的應用程序包。將應用程式授權連線至應用程式後，您可以使用 AppFabric 安全性功能，例如稽核記錄擷取和使用者存取。

本節說明如何 AppFabric 在中開始使用 AWS Management Console。

主題

- 必要條件
- 步驟 1：建立應用程式套件
- 步驟 2：授權應用程式

- 步驟 3：設定稽核記錄擷取
- 步驟 4：使用使用者存取工具
- 步驟 5：Connect 以 AppFabric 取得安全性工具和其他目的地中的安全性資料

必要條件

在開始之前，您必須先建立 AWS 帳戶 和管理使用者。如需詳細資訊，請參閱 註冊一個 AWS 帳戶 及 建立具有管理權限的使用者。

步驟 1：建立應用程式套件

應用程式套件會儲存您所有 AppFabric 的安全性應用程式授權和擷取。若要建立應用程式套件組合，請設定加密金鑰以安全地保護您授權的應用程式資料。

1. 請在以下位置開啟 AppFabric 主控台。 https://console.aws.amazon.com/appfabric/
2. 在頁面右上角的「選取地區」選取器中，選取一個 AWS 區域。 AppFabric 僅在美國東部 (維吉尼亞北部)、歐洲 (愛爾蘭) 和亞太區域 (東京) 區域提供。
3. 選擇 Getting started (入門)。
4. 在 [開始使用] 頁面上，對於步驟 1。創建應用程序包，選擇創建應用程序包。
5. 在「加密」區段中，設定加密金鑰，以安全地保護資料不受所有授權應用程式的攻擊。此密鑰用於AppFabric為安全服務中加密您的數據。

   AppFabric 為了安全默認加密數據。 AppFabric 可以使用由您 AWS 擁有的金鑰 創建和管理 AppFabric 的代表或您在 AWS Key Management Service （ AWS KMS ）中創建和管理的客戶管理密鑰。
6. 針對AWS KMS 金鑰，選擇使用金鑰 AWS 擁有的金鑰或客戶管理金鑰。

   如果您選擇使用客戶受管金鑰，請輸入 Amazon 資源名稱 (ARN) 或要使用之現有金鑰的金鑰 ID，或選擇建立 AWS KMS 金鑰。

   選擇 AWS 擁有的金鑰 或客戶管理的金鑰時，請考量下列事項：

   - AWS 擁有的金鑰是 AWS 服務 擁有和管理以在多個中使用的 AWS Key Management Service （ AWS KMS ）密鑰的集合 AWS 帳戶。雖然不 AWS 擁有的金鑰 在你的 AWS 帳戶，但 AWS 服務 可以使用一個 AWS 擁有的金鑰 來保護您帳戶中的資源。 AWS 擁有的金鑰 請勿計入您帳戶的 AWS KMS 配額。您不需要建立或維護金鑰或其金鑰政策。的輪換 AWS 擁有的金鑰 因服務而異。如需有關的循環的 AWS 擁有的金鑰 資訊 AppFabric，請參閱靜態加密。

- 客戶受管金鑰是您 AWS 帳戶 建立、擁有和管理的 KMS 金鑰。您可以完全控制這些 AWS KMS 按鍵。您可以建立和維護其金鑰政策、 AWS Identity and Access Management (IAM) 政策和授權。您可以啟用和停用它們、旋轉其加密材料、新增標籤、建立參考 AWS KMS 索引鍵的別名，以及排定要刪除的 AWS KMS 金鑰。客戶管理的金鑰會顯示在的 [客戶管理的金鑰] 頁面上 AWS KMS。 AWS Management Console

  若要明確識別客戶管理的金鑰，請使用`DescribeKey`作業。對於客戶受管金鑰，`DescribeKey` 回應的 `KeyManager` 欄位值是 `CUSTOMER`。您可以在密碼編譯作業中使用客戶管理金鑰，並在 AWS CloudTrail 記錄中稽核使用情況。有了許多與 AWS 服務 之整合的金鑰 AWS KMS，您可以指定客戶管理的金鑰，以保護為您儲存和管理的資料。客戶受管金鑰會產生每月費用和超出 AWS 免費方案的使用費用。客戶管理金鑰會計入您帳戶的 AWS KMS 配額。

如需有關 AWS 擁有的金鑰 和客戶管理金鑰的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的客戶 AWS 金鑰和金鑰。

> **Note**
>
> 建立應用程式套件組合時， AppFabric 為了安全起見，也會在您 AWS 帳戶 呼叫的服務連結角色 (SLR) 中建立特殊的 IAM 角色。 AppFabric它允許服務將指標發送到 Amazon CloudWatch。新增稽核日誌目的地後，SLR 允許安全服務存取您的 AWS 資源 (Amazon S3 儲存貯體、Amazon 資料 Firehose 交付串流)。 AppFabric 如需詳細資訊，請參閱 使用 AppFabric 的服務連結角色。

7. （可選）對於標籤，您可以選擇將標籤添加到應用程序包中。標籤是索引鍵值配對，可將中繼資料指派給您建立的資源。若要取得更多資訊，請參閱〈AWS 標籤編輯器使用指南〉中的〈標記 AWS 資源〉
8. 若要建立應用程式套件，請選擇 [建立應用程式套件

步驟 2：授權應用程式

成功創建應用程序包後，您現在可以授權安全 AppFabric 性以連接每個應用程序並與其進行交互。授權應用程式會加密並儲存在您的應用程式套件中。要為每個應用程序包設置多個應用程序授權，請根據需要為每個應用程序重複應用程序授權步驟。

在開始授權應用程式的步驟之前，請先檢閱並確認中每個應用程式的必要條件，例如所需的計劃類型支援的應用程式。

1. 在 [開始使用] 頁面上，對於步驟 2。授權應用程序，選擇創建應用授權。
2. 在 [應用程式授權] 區段中，從 [應用程式] 下拉式清單中選取 AppFabric 您要授與安全性連線權限的應用程式。顯示的應用程式是目前受到安全性支援的應 AppFabric 用程式。
3. 當您選取應用程式時，會顯示必要的資訊欄位。這些欄位包括承租人識別碼和承租人名稱，也可能包括用戶端識別碼、用戶端密碼或個人存取權杖。這些欄位的輸入值會因應用程式而異。如需如何尋找這些值的應用程式特定指示，請參閱支援的應用程式。
4. （可選）對於「標籤」，您可以選擇在應用程序授權中添加標籤。標籤是索引鍵值配對，可將中繼資料指派給您建立的資源。若要取得更多資訊，請參閱〈AWS 標籤編輯器使用指南〉中的〈標記 AWS 資源〉
5. 選擇建立應用程式授權。
6. 如果出現快顯視窗 (視所連線的應用程式而定)，請選取 [允許授權 AppFabric 安全性以與您的應用程式連線]。

   如果您的應用程序授權成功，您將在入門頁面上看到已連接應用程序授權的成功消息。
7. 您可以隨時在功能窗格中列出的 [應用程式授權] 頁面上，在 [每個應用程式的狀態] 下，查看應用程式授權的狀態。「已連線」狀態表示您的應用程式授權已獲得授權，以確保連線到應用程式的安全性並且已完成。 AppFabric
8. 下表顯示可能的應用程式授權狀態，包括您可以採取的疑難排解步驟來修正相關錯誤。

狀態名稱	狀態描述	疑難排解步驟
待定	「待處理」狀態表示已建立應用程式的應用程式授權，但 AppFabric 為了安全起見，尚未連線至應用程式。	當您看到此狀態時，請從 [應用程式授權] 頁面的 [動作] 下拉式清單中選取 [Connect 線] 以啟動連線。如果此錯誤仍然存在，請檢查瀏覽器的彈出窗口阻止程序是否已禁用。如果有任何錯誤訊息 (例如快顯視窗中的 400 錯誤要求)，請檢查是否正確輸入了所有資訊，例如租用戶識別碼、用戶端識別碼和用戶端密碼。也可能未正確建立應用程式的應用程式授權。有關詳情，請參閱支援的應用程式。

狀態名稱	狀態描述	疑難排解步驟
連線驗證失敗	連接驗證失敗的狀態意味著 AppFabric 為了安全起見，無法驗證應用程序授權與應用程序的連接。	檢查所有信息（例如租用戶 ID，客戶端 ID 和客戶端密鑰）是否正確輸入以進行應用程序授權。
權杖自動循環失敗	令牌自動旋轉失敗的狀態意味著 OAuth 刷新令牌在應用授權成功連接後失敗。	如果此錯誤仍然存在，請檢查應用程式的驗證應用程式。有關詳情，請參閱支援的應用程式。

9. 若要授權其他應用程式，請視需要重複步驟 1 到 8。

步驟 3：設定稽核記錄擷取

在您的應用程式套件中建立至少一個應用程式授權之後，您現在可以設定稽核記錄擷取。稽核記錄擷取會使用授權應用程式的稽核記錄，並將其標準化為開放網路安全結構描述架構 (OCSF)。然後，它將它們傳送到內部的一個或多個目的地 AWS。您也可以選擇將原始 JSON 檔案傳送至目的地。

1. 在 [開始使用] 頁面上，針對步驟 3。設定稽核記錄擷取區段，選取擷取快速設定。

> **Note**
>
> 若要加快設定速度，請使用僅可從 [開始使用] 頁面存取的 [Ingestions 快速設定] 頁面，為具有相同擷取目的地的多個應用程式授權建立擷取。例如，相同的 Amazon S3 存儲桶或 Amazon 數據 Firehose 數據流。
>
> 您也可以從 [擷取] 頁面 (可從導覽窗格存取) 建立擷取。在「擷取」頁面上，您可以一次為不同目的地設定一個擷取。在 [擷取] 頁面上，您也可以建立擷取的標籤。下列說明適用於擷取快速設定頁面。

2. 針對 [選取應用程式授權]，選取您要建立稽核記錄擷取的應用程式授權。出現在 [應用程式授權] 下拉式清單中的租用戶名稱是您先前為安全性建立應用程式授權的應用程式的 AppFabric 租用戶名稱。
3. 在 [新增目的地] 中，選取所選應用程式之稽核記錄擷取的目的地。目的地選項包括 Amazon S3-現有存儲桶，Amazon S3-新存儲桶或 Amazon 數據 Firehose。如果您選取多個租用戶名稱，則您選擇的目的地會套用至每次擷取應用程式授權。
4. 當您選擇目的地時，系統會顯示其他必填欄位。

a. 如果您選擇 Amazon S3 — 新儲存貯體做為目的地，則必須輸入要建立的 S3 儲存貯體的名稱。如需有關如何建立 Amazon S3 儲存貯體的詳細指示，請參閱建立輸出目的地。

b. 如果您選擇 Amazon S3 — 現有儲存貯體做為目的地，請選取您要使用的 Amazon S3 儲存貯體名稱。

c. 如果您選擇 Amazon 資料 Firehose 做為目的地，請從 Firehose 交付串流名稱下拉式清單中選取交付串流的名稱。如需有關如何建立 Amazon Data Firehose 交付串流的詳細指示，請參閱建立輸出目的地，並記下安全所需 AppFabric 的許可政策。

5. 對於結構描述和格式，您可以選擇將稽核日誌存放在原始資料-JSON、JSON、OCSF 中 (Parquet 適用於 Amazon S3 儲存貯體) 或原始 JSON 或 OCSF-JSON (適用於 Firehose)。

   原始資料格式提供從資料字串轉換為 JSON 的稽核記錄資料。OCSF 資料格式會將稽核記錄資料標準化 AppFabric 為安全性開放網路安全結構描述架構 (OCSF) 結構描述。如需如何 AppFabric 使用 OCSF 的詳細資訊，請參閱開放式網路安全架構。您一次只能選取一個結構描述和格式化資料類型以進行擷取。如果您要新增其他結構描述和格式化資料類型，可以重複擷取建立程序來設定其他擷取目的地。

6. (選擇性) 如果您要將標籤新增至擷取，請從導覽窗格移至 [擷取] 頁面。若要移至擷取詳細資料頁面，請選取承租人名稱。對於「標籤」，您可以選擇在擷取中新增標籤。標籤是索引鍵值配對，可將中繼資料指派給您建立的資源。若要取得更多資訊，請參閱〈AWS 標籤編輯器使用指南〉中的〈標記 AWS 資源〉

7. 選擇 [設定擷取]。

   成功設定擷取後，您會看到 [開始使用] 頁面上建立的擷取成功訊息。

8. 您也可以隨時在導覽窗格的 [擷取] 頁面上檢查擷取狀態和擷取目的地的狀態。在此頁面上，您可以看到在建立應用程式授權、目的地和擷取狀態時建立的租用戶名稱。擷取的 [已啟用] 狀態表示您的擷取已啟用。如果您在此頁面上選擇應用程式授權的租用戶名稱，則會看到該應用程式授權的詳細資料頁面，包括目的地詳細資料和狀態。擷取目的地的狀態為「作用中」，表示目的地設定正確且處於作用中狀態。如果應用程式授權具有 [已連線] 狀態，且擷取目的地狀態為 [使用中]，則應處理並傳送稽核記錄。如果應用程式授權狀態或擷取目的地狀態為任何失敗狀態，即使擷取狀態已啟用，也不會處理或傳送稽核記錄。若要修正應用程式授權失敗，請參閱步驟 2。授權應用程式。

9. 下表顯示可能的擷取和擷取目的地狀態，以及您可以採取的疑難排解步驟來修正任何錯誤狀態。

狀態或狀態名稱	描述	疑難排解步驟
已停用	擷取的 [已停用] 狀態表示您的擷取已停用。	您可以從 [擷取] 頁面的 [動作] 下拉式清單中選取 [啟用] 來啟用擷取。
失敗	擷取目的地的失敗狀態表示擷取目的地不接受稽核記錄。例如，由於儲存位置已滿，可能會發生此狀態。	若要修正這些問題，請前往 Amazon S3 或 Firehose 主控台。

步驟 4：使用使用者存取工具

使用基 AppFabric 於安全性的使用者存取工具，安全性和 IT 管理團隊可以使用員工的公司電子郵件地址執行簡單搜尋，快速查看有權存取特定應用程式的使用者。這種方法有助於減少使用者取消佈建等工作所花費的時間，這些工作可能需要手動檢查或稽核使用者跨 SaaS 應用程式的存取。如果找到使用者， AppFabric 為了安全起見，會在應用程式中提供使用者的名稱及其應用程式內使用者狀態 (例如，Active) (如果應用程式提供)。 AppFabric in 安全性會搜索應用程序包中的所有授權應用程序，以返回用戶可以訪問的應用程序列表。

1. 在 [開始使用] 頁面上，針對步驟 4。使用使用者存取工具，選擇 [查詢使用者]。
2. 在 [電子郵件地址] 欄位中，輸入使用者的電子郵件地址，然後選擇 [搜尋]。
3. 在 [搜尋結果] 區段中，您會看到使用者有權存取的所有授權應用程式的清單。若要在應用程式中顯示使用者的名稱及其狀態 (如果有的話)，請選取搜尋結果。
4. 在搜索結果列中找到用戶的消息表示用戶可以訪問列出的應用程序。下表顯示可能的搜尋結果、錯誤，以及解決錯誤時可採取的動作。

搜尋結果	描述
找不到該用戶	找不到使用的電子郵件地址的使用者。
找不到授權令牌。Connect 應用程序的應用程序授權。	檢查所有資訊 (例如租用戶 ID、用戶端識別碼和用戶端密碼) 是否已正確輸入應用程式授權。

搜尋結果	描述
授權令牌被撤銷。Connect 應用程序的應用程序授權。	檢查所有資訊 (例如租用戶 ID、用戶端識別碼和用戶端密碼) 是否已正確輸入應用程式授權。
我們無法輪換授權令牌。Connect 應用程序的應用程序授權。	成功連接應用程序授權後，OAuth 刷新令牌失敗。如果此錯誤仍然存在，請檢查應用程式的驗證應用程式。有關詳情，請參閱支援的應用程式。
找不到所需的權限。Connect 應用程序的應用程序授權。	檢查所有資訊 (例如租用戶 ID、用戶端識別碼和用戶端密碼) 是否已正確輸入應用程式授權。
應用程式授權無效。	檢查所有資訊 (例如租用戶 ID、用戶端識別碼和用戶端密碼) 是否已正確輸入應用程式授權。
由於權限不足，我們無法調用應用程序 API。	檢查所有資訊 (例如租用戶 ID、用戶端識別碼和用戶端密碼) 是否已正確輸入應用程式授權。
超出應用程式要求限制。	這是從應用程式收到的錯誤訊息。您可以稍後嘗試搜尋電子郵件地址。
應用程式發生內部伺服器錯誤	這是從應用程式收到的錯誤訊息。您可以稍後嘗試搜尋電子郵件地址。
應用程式遇到錯誤的閘道錯誤	這是從應用程式收到的錯誤訊息。您可以稍後嘗試搜尋電子郵件地址。
應用程序沒有準備好處理請求	這是從應用程式收到的錯誤訊息。您可以稍後嘗試搜尋電子郵件地址。
應用程式遇到錯誤的要求錯誤。	這是我們從應用程式收到的錯誤訊息。您可以稍後再次嘗試搜尋電子郵件。

搜尋結果	描述
應用程式遇到服務無法使用的錯誤。	這是我們從應用程式收到的錯誤訊息。您可以稍後再次嘗試搜尋電子郵件。

步驟 5：Connect 以 AppFabric 取得安全性工具和其他目的地中的安全性資料

來自的標準化 (或原始) 應用程式資料與任何支援 Amazon S3 資料擷取並與 Firehose 整合的工具相容，包括、、、、和等安全工具 Barracuda XDR Dynatrace Logz.io Netskope NetWitness Rapid7Splunk，或 AppFabric 是您專屬的安全解決方案。若要從中取得標準化 (或原始) 應用程式資料 AppFabric，請依照前面的步驟 1 到 3 執行。如需如何設定特定安全性工具和服務的詳細資訊，請參閱相容的安全性工具和服務。

支援的應用程式

AWS AppFabric 為了安全支持與以下應用程序集成。選擇應用程式的名稱，以取得有關如何設定安全性以連線到應 AppFabric 用程式的詳細資訊。

主題

- 1Password
- Asana
- Azure Monitor
- Atlassian Confluence
- Atlassian Jira suite
- Box
- Cisco Duo
- Dropbox
- Genesys Cloud
- GitHub
- Google Analytics
- Google Workspace
- HubSpot
- IBM Security® Verify
- Microsoft365

- Miro
- Okta
- OneLogin by One Identity
- PagerDuty
- Ping Identity
- Salesforce
- ServiceNow
- Singularity Cloud
- Slack
- Smartsheet
- Terraform Cloud
- Webex by Cisco
- Zendesk
- Zoom

1Password

1Password是一個密碼管理器，可幫助您為所有在線帳戶創建，存儲和使用高強度密碼。它還通過加密保護您的數據，提醒您有關漏洞的信息，並允許您共享密碼。

您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料1Password、將資料標準化為開放網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支持 1Password
- 連接 AppFabric 到您的1Password帳戶

AppFabric 支持 1Password

AppFabric 支持從中接收用戶信息和審計日誌1Password。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸1Password到支援的目的地，您必須符合下列需求：

- 您必須擁有有效的付費1Password商務或企業訂閱方案。如需詳細資訊，請參閱1Password網站上的1Password企業。
- 您必須在帳戶中具有管理員角色或小組擁有1Password者。如需詳細資訊，請參閱1Password支援網站中的群組。

速率限制考量

1Password AuditLog 事件 API 將請求限制為每分鐘 600 個，每小時最多 30,000 個。超過這些限制會傳回錯誤。如需詳細資訊，請參閱1Password事件 1Password API 參考資料中的 API 速率限制。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的1Password帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabric1Password。若要尋找授權所需1Password的資訊 AppFabric，請使用下列步驟。

建立個人1Password存取權杖

1Password支持公共客戶端的個人訪問令牌。完成以下步驟以產生個人存取權杖。

1. 登入 1Password 帳戶。
2. 在導覽窗格中選擇 [整合]。
3. 如果存在現有整合，請選擇「目錄」。否則，請繼續至下一個步驟。
4. 在事件報告整合下選擇其他。
5. 在新增整合頁面上，輸入您的安全性資訊和事件管理 (SIEM) 系統名稱 (例如， AppFabric安全)
6. 選擇新增整合，然後在「設定權杖」頁面中完成下列步驟。
    a. 提供要在 AppFabric 安全環境中使用的權杖名稱。
    b. 建議您在「過期後」下拉式清單中選擇「永不」。如果選取任何其他值，則會在到期時間過後1Password撤銷 Token。
    c. 在 [要報告的事件] 區段中，選擇 [登入嘗試]、[項目使用事件] 和 [稽核事件]。
7. 選擇「發行權杖」以建立權杖。

8. 選擇 [儲存於] 1Password 並完成下列步驟。

    a. 標題將根據您的系統和權杖名稱自動填入。
    b. 在選擇保管庫下選擇私人。
    c. 選擇儲存。

如需詳細資訊，請參閱1Password網站上的1Password事件報告開始使用。

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的租用戶 ID AppFabric 將是您的1Password登入地址。完成下列步驟以尋找您的租用戶 ID。

1. 登入 1Password 帳戶。
2. 在導覽窗格中選擇 Settings (設定)。
3. 頁面上會列出您的1Password登入資訊。例如，例如帳戶 .1 密碼 .com。

租戶名稱

輸入可識別此唯一1Password組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

服務帳戶令牌

您必須擁有來自服務帳戶的1Password服務帳戶令牌才能進入 AppFabric 1Password應用授權。如果您沒有服務帳戶令牌，請使用以下說明：

AppFabric 將請求服務帳戶令牌。中的服務帳戶令牌 AppFabric是您創建的個人訪問令牌。在 1Password 入口網站中完成以下步驟，以尋找個人存取權杖。

1. 選擇 Dashboard (儀表板)。
2. 選擇 [人員]。
3. 選擇帳戶擁有者名稱。
4. 選擇 Private (私有)。
5. 選擇檢視資料保險箱
6. 選擇權杖名稱。

用戶端授權

使用租 AppFabric 用戶 ID，租戶名稱和服務帳戶令牌創建應用程序授權。然後選擇 Connect 激活授權。

Asana

Asana是一個工作管理平台，可幫助個人，團隊和組織協調工作，從日常任務到跨職能戰略計劃。它提供了一個清晰的生活系統，每個人都可以在其中進行交流，協作和協調工作。有了團隊將重要的業務工具整合到一個位置Asana，因此無論發生在何處，工作都能向前邁進。

您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Asana、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 Asana
- 連接 AppFabric 到您的Asana帳戶

AppFabric 支援 Asana

AppFabric 支持從中接收用戶信息和審計日誌Asana。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Asana到支援的目的地，您必須符合下列需求：

- 您必須擁有一個企業帳戶Asana。如需有關建立或升級至Asana企業帳戶的詳細資訊，請參閱Asana網站上的Asana企業。
- 您的帳戶中必須有具有超級管理員角色的使用Asana者。如需有關角色的詳細資訊，請參閱Asana網站Asana上的管理員和超級管理員角色。

速率限制考量

Asana對 Asana API 施加速率限制。如需 Asana API 速率限制的詳細資訊，請參閱Asana開發人員指南網站上的速率限制。如果 AppFabric 與您現有Asana應用程式的組合超出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Asana帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricAsana。若要尋找授權所需Asana的資訊 AppFabric，請使用下列步驟。

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的承租人識別碼稱 AppFabric 為中的網域識別碼Asana。若要尋找網域 ID，請使用Asana主畫面上的下列指示：

1. 選擇您的帳戶設定檔圖片並選取 [管理控制台]
2. 然後選取 [設定]。
3. 捲動至 [網域設定]。
4. 將此區段中的網域識別碼輸入 AppFabric 承租人識別碼組態。

租戶名稱

輸入可識別此唯一Asana組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

服務帳戶令牌

您必須擁有來自服務帳戶的Asana服務帳戶令牌才能進入 AppFabric Asana應用授權。如果您沒有服務帳戶令牌，請使用以下說明：

1. 若要建立服務帳戶，請依照指Asana南網站上服務帳戶中的指示進行。
2. 首次檢視 [新增服務帳戶] 頁面時，從 [新增服務帳戶] 頁面底部複製並儲存權杖。
3. 如果在保存令牌之前關閉了「添加服務帳戶」頁面，則必須編輯服務帳戶，生成新令牌並保存它。

Azure Monitor

Azure Monitor是一個全方位的監控解決方案，用於收集、分析和回應來自雲端和內部部署環境的監控資料。您可以使用Azure Monitor來最大化應用程式和服務的可用性和效能。它可協助您瞭解應用程式的執行方式，並允許您以手動方式和程式設計方式回應系統事件。

Azure Monitor跨多個 Azure 和非 Azure 訂用帳戶和租用戶，從系統的每個層和元件收集和彙總資料。它將其存儲在一個共同的數據平台中，以便通過一組可以關聯，分析，可視化和/或響應數據的通用工具消費。您也可以整合其他 Microsoft 和非 Microsoft 工具。Azure Monitor活動記錄是一種平台記錄，可提供訂閱層級事件的深入分析資訊。活動記錄包含資訊，例如何時修改資源或啟動虛擬機器。

您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Azure Monitor、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

AppFabric 支援 Azure Monitor

AppFabric 能夠從以下Azure Monitor服務接收用戶信息和審計日誌：

- Azure Monitor
- API Management
- Microsoft Sentinel
- Security Center

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Azure Monitor到支援的目的地，您必須符合下列需求：

- 您需要擁有一個具有免費試用或 pay-as-you-go 訂閱的Microsoft Azure帳戶。
- 至少需要一個訂閱才能擷取該訂閱內的事件。

速率限制考量

Azure Monitor對發出要求的安全性主體 (使用者或應用程式) 以及訂閱識別碼或租用戶識別碼強加速限制。如需 Azure Monitor API 速率限制的詳細資訊，請參閱了解Azure Monitor開發人員網站上的要求 Azure Resource Manager節流方式。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Azure Monitor帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricAzure Monitor。若要尋找授權所需 Azure Monitor的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與Azure Monitor使用 OAuth2 集成。請完成下列步驟，以在中建立 OAuth2 應用程式：Azure Monitor

1. 導覽至入Microsoft Azure口網站並登入。
2. 導覽至 Microsoft EntraID。
3. 選擇 [應用程式註冊]。
4. 選擇新註冊。
5. 輸入用戶端的名稱，例如 Azure Monitor OAuth 用戶端。這將是註冊應用程序的名稱。
6. 確認 [支援的帳戶類型] 設定為 [單一承租人]。
7. 對於重定向 URI，選擇 Web 作為平台並添加重定向 URI。重新導向 URI 使用下列格式：

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   在該地址中，*<region>*是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

   成功驗證用戶後，身份驗證響應將發送到提供的 URI。現在提供此功能是選擇性的，稍後可以變更，但大多數驗證案例都需要值。

8. 選擇註冊。
9. 在註冊的應用程序中，選擇證書和密碼，然後選擇新客戶端密鑰。
10. 新增密碼的說明。
11. 選取密碼到期時間。您可以從下拉菜單中選擇任何預設持續時間或設置自定義持續時間。
12. 選擇新增。用戶端密碼值只能在建立之後立即檢視。在離開頁面之前，請務必將秘密保存在安全的地方。

所需的許可

您必須將下列權限新增至 OAuth 應用程式。若要新增權限，請依照Microsoft Entra開發人員指南中「新增存取 Web API 的權限」一節中的指示進行。

- Microsoft Graph使用者存取 API > 使用者 .Read. 全部 (選取委派類型)
- Microsoft Graph使用者存取 API > 離線存取 (選取委派類型)
- Azure服務管理稽核記錄 API > 使用者模擬 (選取委派類型)

添加權限後，要授予管理員同意權限，請按照Microsoft Entra開發人員指南中的管理員同意按鈕部分中的說明進行操作。

應用程式授權

AppFabric 支援從您的Azure Monitor帳戶接收使用者資訊和稽核記錄。若要從中接收稽核記錄和使用者資料Azure Monitor，您必須建立兩個應用程式授權，一個Azure Monitor在應用程式授權下拉式清單中命名，另一個在應用程式授權下拉式清單中命名為Azure Monitor稽核記錄。您可以對兩個應用程式授權使用相同的租用戶 ID、用戶端 ID 和用戶端密碼。要從中接收審計日誌，Azure Monitor您需要Azure Monitor和Azure Monitor審計日誌應用程序授權。要單獨使用用戶訪問工具，只需要Azure Monitor應用程序授權。

租用戶 ID

AppFabric 將要求您的租用戶 ID。請完成下列步驟，以在 Azure 監視器中尋找您的用戶端識別碼：

1. 導覽至入Microsoft Azure口網站。
2. 導航到 Azure 活動目錄。
3. 在「應用程式註冊」區段中，選擇先前建立的應用程式。
4. 在概觀區段中，從目錄 (承租人) 識別碼欄位複製承租人識別碼。

租戶名稱

輸入識別此唯一Azure Monitor訂閱的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

> **Note**
>
> 承租人名稱最多應為 2,048 個字元，由數字、小寫/大寫字母以及下列特殊字元組成：句號 (.)、底線 (_)、破折號 (-) 和空白字元。

用戶端 ID

AppFabric 將要求一個客戶端 ID。請完成下列程序，在中尋找您的用戶端 IDAzure Monitor：

1. 導覽至入Microsoft Azure口網站。
2. 導航到 Azure 活動目錄。
3. 在「應用程式註冊」區段中，選擇先前建立的應用程式。
4. 在「概觀」區段中，從「應用程式 (用戶端) ID」欄位複製用戶端 ID。

Client secret (用戶端密碼)

AppFabric 將要求客戶端密碼。註冊 OAuth 應用程序的客戶端密鑰是您在 OAuth 應用程序創建部分的步驟 11 中生成的。如果您錯誤了在 OAuth 應用程序創建過程中生成的客戶端密鑰，請重複 OAuth 應用程序創建部分中的步驟 8-11 以重新生成新密碼。

應用授權

在中創建應用程序授權後 AppFabric，您將收到一個彈出窗口，Microsoft Azure用於批准授權。從視窗登入您的帳戶，然後選擇 [允許] 來核准 AppFabric 授權。

Atlassian Confluence

在單一位置建立、共同作業和整理您的所有工作。 Confluence是一個團隊工作空間，其中知識和協作相遇。動態頁面可讓您的團隊在任何專案或構想上建立、擷取和協作。Spaces 可協助您的團隊組織、組織和共用工作，因此每個團隊成員都可以掌握機構知識，並存取他們發揮最佳工作所需的資訊。您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Confluence、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

AppFabric 支持 Atlassian Confluence

AppFabric 支援從中接收稽核記錄Atlassian Confluence。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Atlassian Confluence到支援的目的地，您必須符合下列需求：

- 若要存取稽核記錄，您必須擁有標準帳戶、進階或企業帳戶。如需有關建立或升級至適用Confluence方案類型的詳細資訊，請參閱Atlassian網站上的Confluence定價。
- 若要存取稽核記錄，您必須擁有帳戶的系統管理員權限。如需有關角色的詳細資訊，請參閱在 Sup Atlassian port 網站上授予使用者管理員權限。

速率限制考量

Confluence對 Atlassian Confluence API 施加速率限制。如果 AppFabric 與您現有 Atlassian Confluence API 應用程式的組合超Atlassian Confluence出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Atlassian Confluence帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricAtlassian Confluence。若要尋找授權所需Atlassian Confluence的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與Atlassian Confluence使用 OAuth 集成。若要在中建立 OAuth 應用程式Atlassian Confluence，請使用下列步驟。

1. 導航到Atlassian開發人員控制台。

2. 選擇右上角的個人資料圖標，然後選擇開發人員控制台。
3. 在 [我的應用程式] 旁，選擇 [建立]，[OAuth 2.0 整合]。
4. 在左側導航窗格中選擇權限，然後選擇 Confluence API 旁邊的添加。
5. 在 [傳統範圍] 下，選取 [讀取使用者 (`read:confluence-user`)]。
6. 在 [精細範圍] 下，選取 [檢視稽核記錄 (`read:audit-log:confluence`)]。
7. 在左側導覽窗格中選擇「授權」，然後選擇 OAuth 2.0 (3LO) 旁邊的「新增」。
8. 在回撥 URL 文字方塊中使用下列格式的重新導向 URL，然後選擇 [儲存變更]。

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

在此 URL 中，<region>是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為`us-east-1`。對於該區域，重新導向 URL 是`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。

所需範圍

您必須將下列其中一個範圍新增至 Atlassian Confluence OAuth 應用程式。如需有關範圍的詳細資訊，請參閱Atlassian開發人員網站上的 OAuth 2.0 (3LO) 範圍和偽造應用程式。在可用的情況下使用經典範圍。

- 經典範圍：
  - `read:confluence-user`
- 粒度範圍：
  - `read:audit-log:confluence`

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的承租人 ID AppFabric 是您的Atlassian Confluence執行個體子網域。您可以在 https://和之間的瀏覽器地址欄中找到Atlassian Confluence實例子域。 atlassian。淨。

租戶名稱

輸入可識別此唯一Atlassian Confluence組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求客戶端 ID。若要在中尋找您的用戶端 IDAtlassian Confluence，請使用下列步驟：

1. 導航到Atlassian開發人員控制台。
2. 選擇右上角的個人資料圖標，然後選擇開發人員控制台，我的應用。
3. 選取您用來連線 AppFabric的 OAuth 應用程式。
4. 在中的 「設定」頁面中輸入用戶端 ID 欄位中的用戶端 ID AppFabric。

Client secret (用戶端密碼)

AppFabric 將要求客戶端密碼。若要在中尋找您的用戶端密碼Atlassian Confluence，請使用下列步驟：

1. 導航到Atlassian開發人員控制台。
2. 選擇右上角的個人資料圖標，然後選擇開發人員控制台，我的應用。
3. 選取您用來連線 AppFabric的 OAuth 應用程式。
4. 在中的 [用戶端密碼] 欄位中輸入 [設定] 頁面的密碼 AppFabric。

核准授權

在中創建應用程序授權後 AppFabric，您將收到一個彈出窗口，Atlassian Confluence用於批准授權。若要核准 AppFabric 授權，請選擇 [允許]。

Atlassian Jira suite

Atlassian釋放每個團隊的潛力。其靈活的 IT 服務管理和工作管理軟件可幫助團隊組織，討論和完成共享工作。 DevOps財星 500 大企業中的大多數以及全球各種規模的 24 萬多家公司-包括 NASA，KivaDeutsche Bank, 和 Salesforce-依靠Atlassian解決方案來幫助他們的團隊更好地共同合作並準時交付高質量的結果。進一步了解Atlassian產品，包括、、、和Jira Software，Confluence，，Jira Service Management，，Trello，，Bitbucket，，，，Jira Align，，，，Atlassian

您可以使 AWS AppFabric 用安全性從 Jira suite (除此之外Jira Align) 接收稽核日誌和使用者資料、將資料標準化為開放網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 對於支持 Jira suite
- 連接 AppFabric 到您的Jira帳戶

AppFabric 對於支持 Jira suite

AppFabric 支援從中接收使用者資訊和稽核記錄Jira suite，但不包括Jira Align。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Jira suite到支援的目的地，您必須符合下列需求：

- 您必須擁有Jira標準計劃或更高版本。如需Jira計劃功能的詳細資訊，請參閱Jira軟體、Jira服務管理、Jira工作管理和Jira產品探索定價頁面。
- 您的帳戶中必須有具有組織管理員角色的使用Jira者。如需有關角色的詳細資訊，請參閱在 Sup Atlassian port 網站上授予使用者管理員權限。

速率限制考量

該Jira套件對 Jira API 施加速率限制。如需 Jira suite API 速率限制的詳細資訊，請參閱Atlassian開發人員指南網站上的速率限制。如果 AppFabric 與您現有 Jira API 應用程式的組合超出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Jira帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricJira。若要尋找授權所需Jira的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與Jira suite使用的 OAuth 集成。若要在中建立 OAuth 應用程式Jira，請使用下列步驟：

1. 導航到Atlassian開發人員控制台。
2. 在 [我的應用程式] 旁，選擇 [建立]，[OAuth 2.0 整合]。
3. 為您的應用程式命名，然後選擇 [建立]。

4. 導覽至「授權」區段，然後選擇「OAuth 2.0」旁邊的「新增」。
5. 在「回呼 URL」欄位中使用下列格式的 URL，然後選擇「儲存變更」。

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

在此 URL 中，<region>是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

6. 導航到「設置」部分，複製您的客戶端 ID 和客戶端密鑰，然後將其保存以用於 AppFabric 應用程序授權。

所需範圍

您必須將以下範圍添加到 Jira OAuth 應用程序的權限頁面：

- 在經典範圍下：
  - JiraAPI > `read:jira-user`
- 在「粒度範圍」下：
  - JiraAPI > `read:audit-log:jira`
  - JiraAPI > `read:user:jira`

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的承租人 ID AppFabric 是您的Jira執行個體子網域。您可以在https://和之間的瀏覽器地址欄中找到Jira實例子域。 atlassian。淨。

租戶名稱

輸入可識別此唯一Jira伺服器的名稱。 AppFabric使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求您的客戶 ID。要在 Jira 中找到您的客戶 ID，請使用以下步驟：

1. 導航到Atlassian開發人員控制台。

2. 選取您用來連線 AppFabric的 OAuth 應用程式。
3. 在中的 「設定」頁面中輸入用戶端 ID 欄位中的用戶端 ID AppFabric。

Client secret (用戶端密碼)

AppFabric 將要求您的客戶密碼。中的用戶端密碼 AppFabric 是中的秘密Jira。若要在中尋找您的密碼Jira，請使用下列步驟：

1. 導航到Atlassian開發人員控制台。
2. 選取您用來連線 AppFabric的 OAuth 應用程式。
3. 在中的 [用戶端密碼] 欄位中輸入 [設定] 頁面的密碼 AppFabric。

核准授權

在中創建應用授權後， AppFabric 您將收到一個彈出窗口，Jira用於批准授權。若要核准 AppFabric授權，請選擇 [允許]。

Box

Box是領先業界的 Content Cloud，這是一個單一平台，可讓組織管理整個內容生命週期、隨時隨地安全工作，以及跨 best-of-breed 應用程式整合。

您可以使用從中 AWS AppFabric 接收稽核日誌和使用者資料Box、將資料標準化為開放網路安全架構架構 (OCSF) 格式，以及將資料輸出到 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 對於支持 Box
- 連接 AppFabric 到您的Box帳戶

AppFabric 對於支持 Box

AppFabric 支持從中接收用戶信息和審計日誌Box。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Box到支援的目的地，您必須符合下列需求：

- 若要存取稽核記錄，您必須擁有商務、商務版、企業版或企業版方案的有效付費訂閱。

- 您必須擁有具有管理員權限的使用者。
- 您必須在Box帳戶上啟用雙因素驗證，才能從配置選項卡查看和複製應用程序的客戶端密碼。

速率限制考量

Box對 Box API 施加速率限制。如需 Box API 速率限制的詳細資訊，請參閱Box開發人員指南網站上的速率限制。如果 AppFabric 與您現有Box應用程式的組合超出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

在稽核事件中，您可能會看到最多 30 分鐘的延遲，才能傳送到目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。但是，這可能是在帳戶級別自定義的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Box帳戶

在 AppFabric 服務中創建應用程序包後，您需要授權 AppFabricBox。若要尋找授權所需Box的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與Box使用的 OAuth 集成。如需詳細資訊，請參閱在中建立 OAuth 應用程式Box，請參閱在網站上建立 OAuth 應用程式Box。

1. 登錄Box並轉到開發人員控制台。
2. 選擇建立新的應用程式。
3. 從應用程式類型清單中選擇「自訂應用程式」。將出現一個強制回應，提示您進行下一個步驟的選擇。
4. 輸入應用程式名稱和說明。
5. 從「目的」下拉式清單選擇「整合」。
    a. 選擇安全性與合規性來自類別下拉列表。
    b. 輸AWS AppFabric Secure入您要與哪個外部系統整合？ 文字方塊。
6. 如果您要使用用戶端 ID 和用戶端密碼來驗證應用程式身分識別，請選擇 [伺服器驗證 (用戶端認證授與)]。
7. 選擇 Create App (建立應用程式)。
8. 選擇 Configuration (組態) 索引標籤。

9. 在頁面的 [應用程式存取層級] 區段中，選擇 [應用程式 + 企業存取權]。
10. 在頁面的「應用程式範圍」段落中，選擇管理使用者和管理企業特性。
11. 選擇 Save Changes (儲存變更)。

    Box管理員必須先在Box管理控制台中授權應用程式，才能使用應用程式。請完成以下步驟以申請授權。

    a. 在開發人員控制台中為您的應用程序選擇授權選項卡。
    b. 選擇 [檢閱並提交]，將電子郵件傳送給您的Box企業管理員以供核准。如需詳細資訊，請參閱Box指南中的授權。

    > **Note**
    >
    > 如果在提交後進行任何更改，則必須重新提交您的應用程序。

所需範圍

需要下列應用程式範圍。如需有關範圍的詳細資訊，請參閱 Box 文件網站上的範圍。

- 管理企業屬性 (`manage_enterprise_properties`)
- 管理使用者 (`manage_managed_users`)

應用程式授權

租用戶 ID

AppFabric 將要求租用戶 ID。中的承租人識別碼 AppFabric 是Box企業識別碼。您可以在管理主控台的 [帳戶與帳單] > [帳戶資訊] > [企業 ID] 下找到企業 ID。Box如需詳細資訊，請參閱 Box 文件網站上的企業 ID。

租戶名稱

輸入可識別此唯一Box組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID 和用戶端密碼

1. 登錄Box並轉到開發人員控制台。

2. 在導航菜單中選擇我的應用程序。
3. 選擇您用來連線 AppFabric的 OAuth 應用程式。
4. 選擇 Configuration (組態) 索引標籤。
5. 捲動至頁面的「Oauth 2.0 認證」區段。
6. 在中的「用戶端識別碼」欄位中輸入 OAuth 用戶端識別碼中 AppFabric的用戶端識別碼。
7. 選擇擷取用戶端密碼。
8. 在 AppFabric中的「用戶端密碼」欄位中輸入來自 OAuth 用戶端密碼的用戶端密碼。

Cisco Duo

Cisco Duo通過領先的訪問管理套件防止漏洞，該套件提供強大的多層防禦和創新功能，允許合法用戶進入並阻止不良行為者。對於任何擔心被破壞並需要快速解決方案的組織，可以快Cisco Duo速實現強大的安全性，同時還可以提高用戶生產力。您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Cisco Duo、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支持 Cisco Duo
- Connect AppFabric 到您的Cisco Duo帳戶

AppFabric 支持 Cisco Duo

AppFabric 支持從中接收用戶信息和審計日誌Cisco Duo。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Cisco Duo到支援的目的地，您必須符合下列需求：

- 若要存取稽核記錄，您必須擁有有效訂閱 Duo Essentials、雙核優勢或雙核頂級版。此外，使用「優勢」或「頂級」試用版的新客戶也可以存取。如需有關Cisco Duo版本的詳細資訊，請參閱版本與定價。
- 您必須是具有擁有者角色的管理員，才能建立或修改 Admin API。
- 您需要添加授予讀取日誌資源」權限才能訪問管理員 API 中的審核日誌。

速率限制考量

Cisco Duo對 Cisco Duo API 施加速率限制。如需 Cisco Duo API 速率限制的詳細資訊，請參閱驗證記錄下的速率限制。如果 AppFabric 與您現有 Cisco Duo API 應用程式的組合超Cisco Duo出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。如果您需要提高速率限制，請聯絡 Cisco Duo。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

Connect AppFabric 到您的Cisco Duo帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricCisco Duo。若要尋找授權所需Cisco Duo的資訊 AppFabric，請使用下列步驟。

建立Cisco Duo管理員 API 應用程式

AppFabric 與Cisco Duo使用 API 服務令牌集成。若要在中建立應用程式Cisco Duo，請使用下列步驟。

- 若要建立Cisco Duo管理 API 應用程式，請遵循Cisco Duo管理 API 第一個步驟中的指示。

所需的許可

您必須將下列範圍新增至Cisco Duo應用程式：

- 授予讀取記錄檔
- 授予讀取資源

應用程式授權

租用戶 ID

AppFabric 將要求租用戶 ID。您可以在Cisco Duo主機名稱中找到承租人識別碼。若要在中尋找主機名稱Cisco Duo，請依照下列步驟執行。

1. 導覽至「Cisco Duo管理員登入」頁面並登入。
2. 導航到應用程序，然後選擇保護應用程序。

3. 在應用程式清單中找到 Admin API 的項目，然後選擇最右邊的「保護」來設定應用程式並取得 API 主機名稱。
4. API 主機名稱的格式為`api-<tenant-id>.duosecurity.com`，其中`<tenant-id>`是租用戶識別碼。

租戶名稱

輸入可識別此唯一Cisco Duo組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

服務令牌

AppFabric 將請求一個服務令牌。服務 Token 是以冒號分隔的整合金鑰和密鑰，格式如下。

```
integrationkey:secretkey
```

若要在中尋找您的整合金鑰和私密金鑰Cisco Duo，請使用下列步驟。

1. 導覽至「Cisco Duo管理員登入」頁面並登入。
2. 導航到應用程序，然後選擇保護應用程序。
3. 「單擊保護應用程序，然後在應用程序列表中找到 Admin API 的條目。按一下最右邊的「保護」以設定應用程式。向下滾動到範圍部分並添加**`Grant read log`**和**`Grant read resource`**。

Dropbox

Dropbox協助您的組織更快地完成更好的工作，無論他們在哪裡工作，或者他們碰巧正在使用什麼樣的工具。它使用戶能夠通過提供一種簡單，安全的方式來共享內容，加速創新和效率。 Dropbox是一個讓生活保持井然有序並保持工作移動的地方。在 180 個國家/地區擁有超過 7 億註冊用戶，其使命Dropbox是設計一種更開明的工作方式。

您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Dropbox、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 Dropbox
- 連接 AppFabric 到您的Dropbox帳戶

AppFabric 支援 Dropbox

AppFabric 支持從中接收用戶信息和審計日誌Dropbox。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Dropbox到支援的目的地，您必須符合下列需求：

- 您必須擁有Dropbox企業帳戶。如需有關建立或升級至Dropbox企業帳戶的詳細資訊，請參閱Dropbox網站上的Dropbox企業帳戶。
- 您的帳戶中必須有具有團隊管理員角色的使用Dropbox者。如需有關角色的詳細資訊，請參閱Dropbox說明中心網站上的如何變更Dropbox團隊的管理員權限。

速率限制考量

Dropbox對 Dropbox API 施加速率限制。如需 Dropbox API 速率限制的詳細資訊，請參閱Dropbox效能指南網站上的速率限制。如果 AppFabric 與您現有 Dropbox API 應用程式的組合超出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Dropbox帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricDropbox。若要尋找授權所需Dropbox的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與Dropbox使用 OAuth 集成。若要在中建立 OAuth 應用程式Dropbox，請使用下列步驟：

1. 在應用程式主控台中選擇建立Dropbox應用程式 https://www.dropbox.com/developers/apps。
2. 在新的應用程式設定頁面上，選擇 API 的範圍存取權限。
3. 接下來，選取 [完整] Dropbox 做為存取類型。
4. 為您的 OAuth 應用程式命名，然後選擇 [建立應用程式] 以完成初始 OAuth 應用程式設定。
5. 在應用程式資訊頁面上，在 OAuth2 重新導向 URI 欄位中新增具有下列格式的重新導向 URL。

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

在此 URL 中，*<region>*是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

6. 選擇新增。
7. 複製並儲存應用程式金鑰和應用程式密鑰，以便在應用 AppFabric 程式授權中使用。
8. 您可以將「設定」索引標籤上的所有其他欄位保留其預設值。

所需範圍

您必須使用Dropbox應用程序信息屏幕上的「權限」選項卡將以下範圍添加到您的應用中：

- account_info.read
- team_data.member
- events.read
- members.read
- team_info.read

完成後，請選擇「提交」。

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。輸入可唯一識別您Dropbox帳戶的任何值，例如團隊名稱。

租戶名稱

輸入識別此唯一Dropbox帳戶的名稱。 AppFabric使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求一個客戶端 ID。中的用戶端 ID AppFabric 是您的Dropbox應用程式金鑰。若要尋找您的 Dropbox 應用程式金鑰，請依照下列步驟進行：

1. 瀏覽至Dropbox應用程式主控台，網址為 https://www.dropbox.com/developers/apps。

2. 尋找您用來連線的應用程式 AppFabric。
3. 在應用程式資訊頁面的「狀態」區段中找到應用程式金鑰。
4. 在中的「用戶端 ID」欄位中輸入Dropbox應用程式的應用程式金鑰 AppFabric。

Client secret (用戶端密碼)

AppFabric 將要求客戶端密碼。中的用戶端密碼 AppFabric 是您的Dropbox應用程式秘密。若要尋找您的Dropbox應用程式密碼，請使用下列步驟：

1. 瀏覽至Dropbox應用程式主控台，網址為 https://www.dropbox.com/developers/apps。
2. 尋找您用來連線的應用程式 AppFabric。
3. 在應用程式資訊頁面的「狀態」區段中找到應用程式密碼。
4. 在中的「用戶端密碼」欄位中輸入Dropbox應用程式的應用程式密碼 AppFabric。

核准授權

在中創建應用程序授權後 AppFabric，您將收到一個彈出窗口，Dropbox用於批准授權。若要核准 AppFabric 授權，請選擇 [允許]。

Genesys Cloud

Genesys Cloud在簡單的 all-in-one 介面中，跨數位和語音通道建立流暢的對話。這使公司能夠為員工和客戶提供卓越的體驗，並獲得快速部署、降低複雜性和簡單管理所帶來的好處。您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Genesys Cloud、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 Genesys Cloud
- 連接 AppFabric 到您的Genesys Cloud帳戶

AppFabric 支援 Genesys Cloud

AppFabric 支持從中接收用戶信息和審計日誌Genesys Cloud。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Genesys Cloud到支援的目的地，您必須符合下列需求：

- 您必須擁有一個Genesys Cloud帳戶。
- 您的帳戶中必須有具有管理員角色的使用Genesys Cloud者。

速率限制考量

Genesys Cloud對 Genesys Cloud API 施加速率限制。如需 Genesys Cloud API 速率限制的詳細資訊，請參閱Genesys Cloud Developer網站上的速率限制。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Genesys Cloud帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricGenesys Cloud。若要尋找授權所需Genesys Cloud的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與Genesys Cloud使用 OAuth 集成。若要在中建立 OAuth 應用程式Genesys Cloud，請使用下列步驟：

1. 依照Genesys Cloud資源中心網站上建立 OAuth 用戶端中的指示進行。

   對於授權類型，請選擇「代碼授權」。
2. 使用具有下列格式的重新導向 URL 作為授權重新導向 URI。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   在此 URL 中，<region>是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。
3. 選取 [範圍] 方塊以顯示應用程式可用的範圍清單。選取範圍audits:readonly和users:readonly。如需範圍的相關資訊，請參閱Genesys Cloud開發人員中心中的 OAuth 範圍。
4. 選擇 [儲存]。 Genesys Cloud創建一個客戶端 ID 和一個客戶端密鑰（令牌）。

所需範圍

您必須將以下範圍添加到 Genesys Cloud OAuth 應用程序：

- audits:readonly
- users:readonly

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的承租人 ID AppFabric 是您的Genesys Cloud執行個體名稱。您可以在瀏覽器的網址列中找到租用戶 ID。例如，usw2.pure.cloud是下列 URL 中的承租人識別碼https://login.usw2.pure.cloud。

租戶名稱

輸入可識別此唯一Genesys Cloud組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求一個客戶端 ID。若要在中尋找您的用戶端 IDGenesys Cloud，請使用下列步驟：

1. 選擇管理員。
2. 在 [整合] 下，選擇 [OAuth]。
3. 選擇 OAuth 用戶端以取得用戶端識別碼。

Client secret (用戶端密碼)

AppFabric 將要求客戶端密碼。若要在中尋找您的用戶端密碼Genesys Cloud，請使用下列步驟：

1. 選擇管理員。
2. 在 [整合] 下，選擇 [OAuth]。
3. 選擇 OAuth 客戶端以獲取客戶端密鑰。

GitHub

GitHub是使用 Git 進行軟件開發和版本控制的平台和基於雲的服務，允許開發人員存儲和管理其代碼。它為每個項目提供 Git 的分佈式版本控制以及訪問控制，錯誤跟踪，軟件功能請求，任務管理，持續集成和維基。您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料GitHub、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 GitHub
- 連接 AppFabric 到您的GitHub帳戶

AppFabric 支援 GitHub

AppFabric 支持從中接收用戶信息和審計日誌GitHub。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸GitHub到支援的目的地，您必須符合下列需求：

- 要訪問審計日誌，您需要有一個企業帳戶。
- 若要存取企業稽核記錄，您必須具有企業帳戶的系統管理員角色。
- 若要從組織取得稽核記錄，您必須是組織擁有者。

速率限制考量

GitHub對 GitHub API 施加速率限制。如需 GitHub API 速率限制的詳細資訊，請參閱GitHub網站上的API 要求限制和配置。如果 AppFabric 與您現有 GitHub API 應用程式的組合超出GitHub’s限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的GitHub帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricGitHub。若要尋找授權所需GitHub的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與GitHub使用的 OAuth 集成。請使用下列步驟在中建立 OAuth 應用程式GitHub。如需詳細資訊，請參閱在GitHub網站上建立 GitHubs 應用程式。

1. 選擇位於頁面右上角的個人資料照片，然後選擇「設置」。
2. 選擇開發人員設置在左側導航窗格中。
3. 在左側導覽窗格中選擇 OAuth 應用程式。
4. 選擇新的 OAuth 應用程式。

> **Note**
>
> 如果您之前尚未創建 OAuth 應用程序，則此按鈕將被標記為「註冊新應用程序」。

5. 在應用程式名稱文字方塊中輸入應用程式的名稱。
6. 在首頁 URL 文字方塊中輸入完整的應用程式實例 URL。
7. (選擇性) 在應用程式說明文字方塊中輸入應用程式的說明。使用者將會看到此說明。
8. 在授權回呼 URL 文字方塊中輸入具有下列格式的 URL。

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

在此 URL 中，<region>是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

9. 如果您的 OAuth 應用程序將使用設備流來識別和授權用戶，請選擇啟用設備流。有關設備流程的詳細信息，請參閱在網站上授權 OAuth 應用程序。GitHub
10. 選擇註冊應用程式。

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。承租人識別碼應以下列其中一種格式提供：

企業稽核記錄：

如果您想瞭解您企業帳戶所擁有之所有組織的彙總動作，請使用企業的稽核記錄。

若要使用企業稽核記錄檔，承租人識別碼是您帳戶的企業識別碼。您可以在瀏覽器的網址列中找到您的企業 ID。例如，*exampleenterprise*是下列 URL 中的企業 ID `https://github.com/settings/enterprises/`*`examplenterprise`*。

當您指定企業稽核記錄檔的承租人識別碼時，必須使用前置碼`enterprise:`。因此，請將前面的範例指定為`enterprise:examplenterprise`。

組織稽核記錄：

如果您想知道組織成員所執行的動作，請使用組織的稽核記錄做為組織管理員。它包括詳細資訊，例如執行動作的人員、動作是什麼，以及執行的時間。

若要使用組織稽核記錄檔，承租人識別碼是您的組織識別碼。您可以在瀏覽器的網址列中找到您的組織 ID。例如，*exampleorganization*是下列 URL 中的組織 ID `https://github.com/settings/organizations/`*`exampleorganization`*。

當您指定組織稽核記錄檔的承租人識別碼時，必須在其前置詞加上`organization:`。因此，請將前面的範例指定為`organization:exampleorganization`。

租戶名稱

輸入可識別此唯一GitHub企業或組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求一個客戶端 ID。使用以下步驟在GitHub中找到您的用戶端 ID

1. 選擇位於頁面右上角的個人資料照片，然後選擇「設置」。
2. 選擇開發人員設置在左側導航窗格中。
3. 在左側導覽窗格中選擇 OAuth 應用程式。
4. 選擇特定的 OAuth 應用程序，然後查找客戶端 ID 值。

Client secret (用戶端密碼)

AppFabric 將要求一個客戶端密碼。使用下列步驟在中尋找您的用戶端密碼GitHub。

1. 選擇位於頁面右上角的個人資料照片，然後選擇「設置」。
2. 選擇開發人員設置在左側導航窗格中。

3. 在左側導覽窗格中選擇 OAuth 應用程式。
4. 選擇特定的 OAuth 應用程式，然後尋找用戶端密碼值。如果您找不到現有的用戶端密碼，則可能需要產生一個新的用戶端密碼。

核准授權

在中創建應用程序授權後 AppFabric，您將收到一個彈出窗口，GitHub用於批准授權。若要核准 AppFabric 授權，請選擇 [允許]。

如果啟用了 OAuth 應用程序訪問限制，請確保您的組織已授予 OAuth 應用程序的訪問權限。

Google Analytics

Google Analytics是一個網絡分析服務，提供統計和基本的分析工具，用於搜索引擎優化（SEO）和營銷目的。 Google Analytics用於跟踪網站性能並收集訪問者見解。它可以幫助組織確定用戶流量的主要來源，衡量其營銷活動和廣告系列的成功率，跟踪目標完成情況（例如購買，將產品添加到購物車），發現用戶參與度的模式和趨勢，以及獲取其他訪客信息，例如人口統計信息。中小型零售網站通常用於獲Google Analytics取和分析各種客戶行為分析，這些分析可用於改善營銷活動，吸引網站流量並更好地留住訪客。

您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Azure Monitor、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 Google Analytics
- 連接 AppFabric 到您的Google Analytics帳戶

AppFabric 支援 Google Analytics

AppFabric 支援從中接收稽核記錄Google Analytics。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Google Analytics到支援的目的地，您必須符合下列需求：

- 您必須是Google Analytics帳戶的管理員。
- AppFabric 為了交付日誌，您需要在Google Cloud項目上啟用 Google AnalyticsAdmin API。設定 Google Analytics OAuth 應用程式時，請務必使用新專案。

速率限制考量

Google Analytics對 Google Analytics API 施加速率限制。如需 Google Analytics API 速率限制的詳細資訊，請參閱 Google 分析網站上的限制和配額。如果 AppFabric 和您現有的 Google Analytics（分析）API 應用程序的組合超出限制，則顯示在中的審核日誌 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Google Analytics帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricGoogle Analytics。請使用下列步驟尋找授權Google Analytics所需的資訊 AppFabric。

建立 OAuth 應用程式

AppFabric 與Google Analytics使用的 OAuth 集成。請完成下列步驟，以在中建立 OAuth 應用程式 Google Analytics：

1. 要配置您的 OAuth 同意屏幕，請按照 Google 網站上 Google 開發人員指南中的配置 OAuth 同意屏幕中的說明進行操作。
2. 為使用者類型選擇外部
3. 要配置 OAuth 憑據 AppFabric，請按照 Google 開發人員指南中「創建訪問憑據」頁面中「OAuth 客戶端 ID 憑據」部分中的說明進行操作。
4. 使用下列格式的重新導向 URL。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   在該地址中，*<region>*是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

所需範圍

您必須將以下範圍添加到 Google Analytics OAuth 應用程序：

```
https://www.googleapis.com/auth/analytics.edit
```

應用程式授權

租用戶 ID

AppFabric 將要求租用戶 ID。中的承租人識別碼 AppFabric 是您的Google Analytics帳戶識別碼。

1. 轉到Google Analytics主頁。
2. 在導覽窗格中選擇 [管理員]。
3. 您可以在帳戶 > 帳戶設置 > 帳戶詳細信息 > 帳戶 ID 下找到您的帳戶 ID。

租戶名稱

輸入可識別此唯一Google Analytics組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求一個客戶端 ID。使用下列步驟在中尋找您的用戶端 IDGoogle Analytics：

1. 移至「證明資料」頁面。
2. 在 OAuth 2.0 客戶端 ID 部分中，選擇您創建的客戶端 ID。
3. 從屬端 ID 會列在頁面的「其他資訊」區段中。

Client secret (用戶端密碼)

AppFabric 將要求客戶端密碼。使用下列步驟在中尋找您的用戶端密碼Google Analytics：

1. 移至「證明資料」頁面。
2. 在 OAuth 2.0 用戶端識別碼區段中，選擇用戶端名稱。
3. 用戶端密碼會列在頁面的 [用戶端密碼] 區段中。

應用授權

在中創建應用程序授權後， AppFabric 您將收到一個彈出窗口，Google Analytics用於批准授權。若要核准 AppFabric 授權，請選擇 [允許]。

Google Workspace

Google Workspace是 Google 開發和銷售的雲計算，生產力和協作工具，軟件和產品的集合。

您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Google Workspace、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 Google Workspace
- 連接 AppFabric 到您的Google Workspace帳戶

AppFabric 支援 Google Workspace

AppFabric 支持從中接收用戶信息和審計日誌Google Workspace。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Google Workspace到支援的目的地，您必須符合下列需求：

- 您必須訂閱Google Workspace企業標準方案。如需有關建立或升級至Google Workspace企業標準方案的詳細資訊，請參閱方Google Workspace案網站。
- 您必須在中具有「管理員」角色的使用者Google Workspace。
- 為了 AppFabric 提供日誌，您需要啟用谷歌管理 SDK API 在您的谷歌雲項目。如需詳細資訊，請參閱Google Workspace開發人員指南中的啟用 Google 工作區 API。

速率限制考量

Google Workspace對 Google Workspace API 施加速率限制。如需 Google Workspace API 速率限制的詳細資訊，請參閱Google Workspace網站上的Google Workspace管理指南中的限制和配額。如果 AppFabric 與您現有 Google Workspace API 應用程式的組合超出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

對於大多數稽核事件，您可能會看到最多 30 分鐘的延遲，對於將特定稽核事件傳送至目的地，最多可能會延遲 4 小時。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。如需詳細資訊，請參閱 Google WorkSpace 管理說明網站中的資料保留和延遲時間。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Google Workspace帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricGoogle Workspace。若要尋找授權所需Google Workspace的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與Google Workspace使用 OAuth 集成。若要在中建立 OAuth 應用程式Google Workspace，請使用下列步驟：

1. 要配置您的 OAuth 同意屏幕，請按照網站上Google Workspace開發人員指南中的配置 OAuth 同意屏幕中的說明進行操作。Google Workspace

   為 [使用者] 類型選擇 [內部]。
2. 要配置 OAuth 憑據 AppFabric，請按照Google Workspace 開發人員指南中「創建訪問憑據」頁面的 OAuth 客戶端 ID 憑據部分中的說明進行操作。
3. 使用下列格式的重新導向 URL。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   在此 URL 中，*<region>*是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

所需範圍

您必須將以下範圍添加到 Google Workspace OAuth 應用程序：

- `https://www.googleapis.com/auth/admin.reports.audit.readonly`
- `https://www.googleapis.com/auth/admin.directory.user`

如果您沒有看到這些範圍，請將管理員 SDK API 新增至您的Google雲端 API 程式庫。

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的承租人識別碼 AppFabric 是您的Google Workspace專案識別碼。若要尋找您的專案 ID，請參閱 Google API 主控台說明網站上的尋找專案 ID。

租戶名稱

輸入識別此唯一性的名稱Google Workspace。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求您的客戶 ID。若要尋找您的用戶端 ID，請使用下列步驟：

1. 使用「Google Workspace開發人員指南」中「管理憑證」頁面的「檢視認證」區段中的資訊，尋找您的用戶端 ID。
2. 在 AppFabric中的「用戶端識別碼」欄位中輸入 OAuth 用戶端的用戶端識別碼。

Client secret (用戶端密碼)

AppFabric 將要求您的客戶密碼。若要尋找您的用戶端密碼，請使用下列步驟：

1. 使用「Google Workspace開發人員指南」中「管理認證」頁面的「檢視認證」區段中的資訊，尋找您的用戶端密碼。
2. 如果您需要重設用戶端密碼，請使用「Google Workspace開發人員指南」中「管理憑證」頁面中「重設用戶端密碼」區段中的指示。
3. 在中的 [用戶端密碼] 欄位中輸入您的用戶端密碼 AppFabric。

核准授權

在中創建應用程序授權後， AppFabric 您將收到一個彈出窗口，Google Workspace用於批准授權。若要核准 AppFabric 授權，請選擇 [允許]。

HubSpot

HubSpot是一個客戶平台，其中包含連接營銷，銷售，內容管理和客戶服務所需的所有軟件，集成和資源。 HubSpot互聯平台可讓您專注於最重要的事情：您的客戶，從而更快地發展業務。您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料HubSpot、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 HubSpot
- 連接 AppFabric 到您的HubSpot帳戶

AppFabric 支援 HubSpot

AppFabric 支持從中接收用戶信息和審計日誌HubSpot。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸HubSpot到支援的目的地，您必須符合下列需求：

- 您必須在中擁有具有 Enterprise 訂閱的帳戶，HubSpot才能存取稽核記錄。如需有關HubSpot訂閱的詳細資訊，請參HubSpot閱在HubSpot知識庫中管理您的訂閱。
- 您必須擁有與該帳戶相關聯的開發人員帳戶和應用程式。
- 您應該是在HubSpot帳戶中安裝應用程序的超級管理員，或者具有應用程序 Marketplace 訪問權限以及用戶權限，以接受應用程序請求的範圍。

速率限制考量

HubSpot對 HubSpot API 施加速率限制。有關 HubSpot API 速率限制的更多信息，包括使用 OAuth 的應用程序的限制，請參閱HubSpot網站上的速率限制。如果 AppFabric 與您現有 HubSpot API 應用程式的組合超HubSpot出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的HubSpot帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricHubSpot。若要尋找授權所需HubSpot的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與HubSpot使用 OAuth 集成。若要在中建立 OAuth 應用程式HubSpot，請使用下列步驟：

1. 請依照網站上指南中「建立公開應用程式」區段中的HubSpot指示進HubSpot行。
2. 從「驗證」選項卡中，添加中列出的三個範圍所需的範圍。
3. 在重定向 URL 中使用具有以下格式的重定向 URL。

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

在此 URL 中，<region>是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

4. 選擇建立應用程式。

所需的範圍

您必須將以下範圍添加到 HubSpot OAuth 應用程序：

- settings.users.read
- crm.objects.owners.read
- account-info.security.read

應用程式授權

租用戶 ID

輸入識別此唯一HubSpot組織的 ID。例如，輸入您的HubSpot帳戶 ID。

租戶名稱

輸入可識別此唯一HubSpot組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求一個客戶端 ID。若要在中尋找您的用戶端 IDHubSpot，請使用下列步驟：

1. 導航到HubSpot登錄頁面並使用您的開發人員帳戶憑據登錄。
2. 從「應用程式」選單中選擇您的應用程式。
3. 從身份驗證選項卡中，查找客戶端 ID 值。

Client secret (用戶端密碼)

AppFabric 將要求客戶端密碼。若要在中尋找您的用戶端密碼HubSpot，請使用下列步驟：

1. 導航到HubSpot登錄頁面並使用您的開發人員帳戶憑據登錄。

2. 從「應用程式」選單中選擇您的應用程式。
3. 從「驗證」選項卡中，查找客戶端密鑰值。

核准授權

在中創建應用程序授權後 AppFabric，您將收到一個彈出窗口，HubSpot用於批准授權。使用您的企業帳戶憑據（而不是您的開發人員帳戶）登錄到您的帳戶以批准 AppFabric 授權。選擇允許。

IBM Security® Verify

該IBM Security® Verify系列提供自動化、雲端式和內部部署功能，用於管理身分治理、管理員工和消費者身分識別與存取權限，以及控制特權帳戶。無論您是需要部署雲端還是內部部署解決方案，都能IBM Security® Verify協助您建立信任並防範員工和消費者的內部威脅。

您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料IBM Security® Verify、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 對於支持 IBM Security® Verify
- 連接 AppFabric 到您的IBM Security® Verify帳戶

AppFabric 對於支持 IBM Security® Verify

AppFabric 支持從中接收用戶信息和審計日誌IBM Security® Verify。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸IBM Security® Verify到支援的目的地，您必須符合下列需求：

- 若要存取稽核記錄，您必須擁有 IBM Security® VerifySaaS 帳戶。
- 若要存取稽核記錄，您必須在 IBM Security® Verify SaaS 帳戶中具有系統管理員角色。

速率限制考量

IBM Security® Verify對 IBM Security® Verify API 施加速率限制。如需 IBM Security® Verify API 速率限制的詳細資訊，請參閱 IBM 條款。如果 AppFabric 與您現有 IBM Security® Verify API 應用程式的組合超出IBM Security® Verify限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

在稽核事件中，您可能會看到最多 30 分鐘的延遲，才能傳送到目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。但是，這可能是在帳戶級別自定義的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的IBM Security® Verify帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricIBM Security® Verify。若要尋找授權所需IBM Security® Verify的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與IBM Security® Verify使用的 OAuth 集成。若要在中建立 OAuth 應用程式IBM Security® Verify，請參閱 IBM 說明文件網站上的建立 API 用戶端。

1. 對於首次登錄，請使用發送到您註冊的電子郵件地址的登錄 URL 和憑據。
2. 存取管理主控台，位於`https://<hostname>.verify.ibm.com/ui/admin/`。如需詳細資訊，請參閱存取IBM Security® Verify。
3. 在管理主控台的安全性 < API 存取 < API 用戶端下，選擇新增。
4. 選取下列選項。這些是讀取稽核記錄和使用者詳細資料所必需的。
   - 閱讀報告
   - 讀取使用者和群組
5. 保留 [用戶端驗證] 方法中的 [預設] 選項。

   請勿編輯「自訂範圍」欄位。
6. 選擇下一步。
7. 請勿編輯 IP 篩選器欄位。
8. 選擇下一步。
9. 請勿編輯 [其他屬性] 欄位。
10. 選擇下一步。
11. 指定「名稱」和「描述」。描述是選用。
12. 選擇「建立 API 用戶端」。

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。您可以在IBM Security® Verify標準 URL 中找到承租人識別碼。例如，在 `https://hostname.verify.ibm.com/` URL 中，承租人 ID 是可以在之前找到的`####.verify.ibm.com` (`ice.ibmcloud.com`如果您使用之前的主機名稱，則可以在之前找到)。如果您使用的是虛名 URL，請聯絡您的IBM Security® Verify支援團隊以取得標準 URL。

租戶名稱

輸入可識別此唯一IBM Security® Verify承租人的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求一個客戶端 ID。若要在中尋找您的用戶端 IDIBM Security® Verify，請使用下列步驟：

1. 對於首次登錄，請使用發送到您註冊的電子郵件地址的登錄 URL 和憑據。
2. 存取管理主控台，位於`https://<hostname>.verify.ibm.com/ui/admin/`。如需詳細資訊，請參閱存取IBM Security® Verify。
3. 在管理主控台的安全性 < API 存取 < API 用戶端下，選擇特定 OAuth 應用程式旁邊的省略號 ()。
4. 選擇連線詳細資料。
5. 在 API 憑證下找到客戶端 ID。

Client secret (用戶端密碼)

AppFabric 將要求客戶端密碼。若要在中尋找您的用戶端密碼IBM Security® Verify，請使用下列步驟：

1. 對於首次登錄，請使用發送到您註冊的電子郵件地址的登錄 URL 和憑據。
2. 存取管理主控台，位於`https://<hostname>.verify.ibm.com/ui/admin/`。如需詳細資訊，請參閱存取IBM Security® Verify。
3. 在管理主控台的安全性 < API 存取 < API 用戶端下，選擇特定 OAuth 應用程式旁邊的省略號 ()。
4. 選擇連線詳細資料。
5. 在 API 憑證下找到用戶端密碼。

Microsoft365

Microsoft365 是由擁有的生產力軟體、協同作業和雲端服務的產品系列Microsoft。

您可以使 AWS AppFabric 用安全性從 Microsoft 365 接收稽核日誌和使用者資料、將資料標準化為開放網路安全架構架構 (OCSF) 格式，然後將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 對於 Microsoft 365 的支持
- 連接 AppFabric 到您的 Microsoft 365 帳戶

AppFabric 對於 Microsoft 365 的支持

AppFabric 支持從 Microsoft 365 接收用戶信息和審計日誌。

必要條件

若要用 AppFabric 來將稽核記錄從 Microsoft 365 傳輸到支援的目的地，您必須符合下列需求：

- 您必須訂閱 Microsoft 365 企業版方案。如需建立或升級至 Microsoft 365 企業版方案的詳細資訊，請參閱Microsoft網站上的 Microsoft365 企業方案。
- 您的 Microsoft 365 帳戶中必須擁有具有管理員權限的用戶。
- 您必須開啟組織的稽核記錄。如需詳細資訊，請參閱開啟或關閉Microsoft網站上的稽核功能。

速率限制考量

Microsoft365 對 Microsoft 365 API 施加了速率限制。如需 Microsoft 365 API 速率限制的詳細資訊，請參閱網站上 MicrosoftGraph 文件中的圖形服務特定節流限制Microsoft圖形。Microsoft如果 AppFabric 與您現有的 Microsoft 365 API 應用程式的組合超出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的 Microsoft 365 帳戶

在 AppFabric 服務中創建應用程序包後，您必須使用 Microsoft 365 進 AppFabric行授權。若要尋找授權 Microsoft 365 所需的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 使用 OAuth 與 Microsoft 365 集成。若要在 Microsoft 365 中建立 OAuth 應用程式，請使用下列步驟：

1. 依照網站上 Azure 作用中目錄開發人員指南中 [註冊應用程式] 區段中的指示進Microsoft行。

   僅在「支援的帳戶類型」設定中選擇此組織目錄中的帳號。
2. 依照 Azure 作用中目錄開發人員指南中 [新增重新導向 URI] 區段中的指示進行。

   選擇網頁平台。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   在此 URL 中，*<region>*是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

   您可以略過 Web 平台的其他輸入欄位。
3. 依照 Azure 作用中目錄開發人員指南的 [新增用戶端密碼] 區段中的指示進行。

所需的許可

您必須將下列權限新增至 OAuth 應用程式。若要新增權限，請依照 Azure 作用中目錄開發人員指南的 [新增權限以存取您的 Web API] 區段中的指示執行。

- `Microsoft Graph API>` `User.Read` (自動新增)
- `Office 365 Management APIs>` `ActivityFeed.Read` (選取委派類型)
- `Office 365 Management APIs>` `ActivityFeed.ReadDlp` (選取委派類型)
- `Office 365 Management APIs>` `ServiceHealth.Read` (選取委派類型)

新增權限之後，若要授與系統管理員同意權限，請依照 Azure Active Directory 開發人員指南的 [系統管理員同意] 按鈕區段中的指示執行。

應用程式授權

AppFabric 支持從您的 Microsoft 365 帳戶接收用戶信息和審計日誌。若要從 Microsoft 365 接收稽核記錄和使用者資料，您必須建立兩個應用程式授權，一個在應用程式授權下拉式清單中名為 Microsoft365，另一個在應用程式授權下拉式清單中名為 Microsoft365 稽核記錄。您可以針對兩個應用程式授權使用相同的租用戶 ID、用戶端 ID 和用戶端密碼。若要從 Microsoft 365 接收稽核記錄，您需要 Microsoft365 和 Microsoft 365 稽核記錄應用程式授權。要單獨使用用戶訪問工具，只需要 Microsoft365 應用程序授權。

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的租用戶識別碼 AppFabric 是您的 Azure 作用中目錄租用戶識別碼。若要尋找您的 Azure 作用中目錄租用戶識別碼，請參閱如何在Microsoft網站上的 Azure 產品文件中尋找您的 Azure 作用中目錄租用戶識別碼。

租戶名稱

輸入識別此唯一 Microsoft 365 帳戶的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求您的客戶 ID。中的用戶端識別碼 AppFabric 是 Microsoft 365 應用程式 (用戶端) 識別碼。若要尋找您的 Microsoft 365 應用程式 (用戶端) ID，請使用下列步驟：

1. 開啟您搭 AppFabric配使用之 OAuth 應用程式的概觀頁面。
2. 應用程式 (用戶端) ID 會出現在 [基本資訊] 下
3. 在 AppFabric中的「用戶端識別碼」欄位中輸入 OAuth 用戶端的應用程式（用戶端）ID。

Client secret (用戶端密碼)

AppFabric 將要求您的客戶密碼。 Microsoft365 只有在您最初為 OAuth 應用程式建立用戶端密碼時，才會提供此值。如果您沒有用戶端密碼，請使用下列步驟來產生新的用戶端密碼：

1. 若要建立用戶端密碼，請依照 Azure Active Directory 開發人員指南的 [新增用戶端密碼] 區段中的指示執行。
2. 在中的「用戶端密碼」欄位中輸入「值」欄位的內容 AppFabric。

核准授權

在中創建應用程序授權後 AppFabric，您將收到一個來自 Microsoft 365 的彈出窗口，用於批准授權。若要核准 AppFabric 授權，請選擇 [允許]。

Miro

Miro是一個用於創新的線上工作空間，可讓任何規模的分散式團隊建立下一件大事。該平台的無限畫布使團隊能夠領導引人入勝的研討會和會議，設計產品，集思廣益的想法等。 Miro總部位於舊金山和阿姆斯特丹，為全球 50 多萬用戶提供服務，包括 99% 的財富 100 大企業。 Miro成立於 2011 年，目前在全球 12 個樞紐擁有 1,500 多名員工。要了解更多信息，請訪問Miro。

Miro包括專為創新而設計的完整協作功能套件，包括圖表製作、線框圖、即時資料視覺化、工作坊簡化，以及針對敏捷實務、研討會和互動式簡報的內建支援。 Miro最近宣布的 Miro AI 通過 AI 驅動Miro的映射和圖表製作，聚類和摘要以及內容生成來擴展了功能。 Miro使組織能夠減少獨立工具的數量，從而減少信息碎片和成本。

您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Miro、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 Miro
- 連接 AppFabric 到您的Miro帳戶

AppFabric 支援 Miro

AppFabric 支持從中接收用戶信息和審計日誌Miro。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Miro到支援的目的地，您必須符合下列需求：

- 您必須擁有Miro企業方案。如需 Miro 方案類型的詳細資訊，請參閱Miro網站上的Miro定價頁面。
- 您的帳戶中必須有具有「公司管理員」角色的使用Miro者。如需有關角色的詳細資訊，請參閱 Miro 說明中心網站上 Miro 角色的公司層級部分。
- 您的Miro帳戶中必須有企業開發人員團隊。如需建立開發人員團隊的相關資訊，請參閱 Miro 說明中心網站上的企業開發人員團隊。

速率限制考量

Miro對 Miro API 施加速率限制。如需 Miro API 速率限制的詳細資訊，請參閱Miro網站Miro開發人員指南中的速率限制。如果 AppFabric 與您現有 Miro API 應用程式的組合超出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Miro帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricMiro。若要尋找授權所需Miro的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與Miro使用 OAuth 集成。若要在中建立 OAuth 應用程式Miro，請使用下列步驟：

1. 若要建立 OAuth 應用程式，請依照 Miro 說明中心網站上企業開發團隊文章中「建立和安裝應用程式」一節中的指示進行。
2. 在應用程式建立對話方塊中，選取企業組織上的開發人員團隊之後，選取 [過期使用者授權權杖] 核取方塊。

   > **Note**
   >
   > 您必須在建立應用程式之前執行此動作，因為建立應用程式之後就無法變更此選項。

3. 在應用程式頁面上，在 OAuth 2.0 的重新導向 URI 區段中輸入具有下列格式的 URL。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   在此 URL 中，<region>是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。
4. 複製並保存您的客戶端 ID 和客戶密碼，以在 AppFabric 應用授權中使用。

所需範圍

您必須在 Miro OAuth 應用程序頁面的Permissions部分中添加以下範圍：

- auditlogs:read
- organizations:read

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的承租人 ID AppFabric 是您的Miro團隊 ID。有關如何找到您的 Miro 團隊 ID 的資訊，請參閱我是新Miro管理員的常見問題部分。從哪裡開始？ 在Miro說明中心網站上。

租戶名稱

輸入可識別此唯一Miro組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求您的客戶 ID。若要尋找您的用戶端 ID，請使用下列步驟：

1. 瀏覽至您的設定Miro檔設定。
2. 選取 [您的應用程式] 分頁。
3. 選取您用來連線的應用程式 AppFabric。
4. 在中的「用戶端 ID」欄位中，將「應用程式憑證」區段中的用戶端 ID 輸入 AppFabric。

Client secret (用戶端密碼)

AppFabric 將要求您的客戶密碼。若要尋找您的用戶端密碼，請使用下列步驟：

1. 瀏覽至您的設定Miro檔設定。
2. 選取 [您的應用程式] 分頁。
3. 選取您用來連線的應用程式 AppFabric。
4. 將「應用程式認證」區段中的用戶端密碼輸入到的「用戶端密碼」欄位中 AppFabric。

核准授權

在中創建應用程序授權後 AppFabric，您將收到一個彈出窗口，Miro用於批准授權。若要核准 AppFabric 授權，請選擇 [允許]。

Okta

Okta是世界上的身份識別公司。身為領先的獨立身分合作夥伴，Okta讓每個人都能隨時隨地在任何裝置或應用程式上安全使用任何技術。最值得信賴的品牌信任可Okta以實現安全訪問，身份驗證和自動化。憑藉員Okta工身份識別和客戶身份雲的核心靈活性和中立性，業務領導者和開發人員可以專注於創新並加速數字轉型，這要歸功於可自定義的解決方案和 7,000 多個預先構建的集成。 Okta正在建立一個身份屬於你的世界。前往 okta .com 瞭解更多資訊。

您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Okta、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 Okta
- 連接 AppFabric 到您的Okta帳戶

AppFabric 支援 Okta

AppFabric 支持從中接收用戶信息和審計日誌Okta。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Okta到支援的目的地，您必須符合下列需求：

- 您可以使 AppFabric 用任何Okta計劃類型。
- 您的帳戶中必須有具有超級管理員角色的使用Okta者。
- 核准應用程式授權的使用者在您的Okta帳戶中也 AppFabric 必須具有超級管理員角色。

速率限制考量

Okta對 Okta API 施加速率限制。如需 Okta API 速率限制的詳細資訊，請參閱Okta網站上Okta開發人員指南中的速率限制。如果 AppFabric 與您現有 Okta API 應用程式的組合超Okta出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Okta帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricOkta。若要尋找授權所需Okta的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與Okta使用 OAuth 集成。若要建立要連線的 OAuth 應用程式 AppFabric，請遵循說明中心網站上建立 OIDC 應用程式整合中的Okta指示。以下是設定的考量 AppFabric：

1. 針對應用程式類型，選擇 Web 應用程式。
2. 對於授權類型，選擇授權碼和重新整理權杖。
3. 使用具有下列格式的重新導向 URL 作為登入重新導向 URI 和登出重新導向 URI。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   在此 URL 中，<region>是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。
4. 您可以略過信任的來源組態。
5. 在受控制的存取設定中，將存取權授予Okta組織中每個人的權限。

   > **Note**
   >
   > 如果您在初始 OAuth 應用程式建立期間略過此步驟，您可以使用應用程式設定頁面上的 [指派] 索引標籤，將組織中的每個人指派為群組。

6. 您可以將所有其他選項保留為預設值。

所需範圍

您必須將以下範圍添加到 Okta OAuth 應用程序：

- okta.logs.read
- okta.users.read

應用程式授權

租用戶 ID

AppFabric 將要求租用戶 ID。中的承租人識別碼 AppFabric 是您的Okta網域。如需尋找網Okta域的詳細資訊，請參閱網站上的Okta開發人員指南中的「尋找您的Okta網Okta域」。

租戶名稱

輸入可識別此唯一Okta組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求一個客戶端 ID。若要在中尋找您的用戶端 IDOkta，請使用下列步驟：

1. 導航到Okta開發人員控制台。
2. 選擇「應用程式」標籤。
3. 選擇您的應用程序，然後選擇常規選項卡。
4. 捲動至「用戶端認證」區段。
5. 將 OAuth 用戶端的用戶端識別碼輸入中的「用戶端識別碼」欄位 AppFabric。

Client secret (用戶端密碼)

AppFabric 將要求客戶端密碼。若要在中尋找您的用戶端密碼Okta，請使用下列步驟：

1. 導航到Okta開發人員控制台。
2. 選擇「應用程式」標籤。
3. 選擇您的應用程序，然後選擇常規選項卡。
4. 捲動至「用戶端認證」區段。
5. 將 OAuth 應用程式中的用戶端密碼輸入到中的「用戶端密碼」欄位中 AppFabric。

核准授權

在中創建應用程序授權後 AppFabric，您將收到一個彈出窗口，Okta用於批准授權。若要核准 AppFabric 授權，請選擇 [允許]。核准Okta授權的使用者必須在Okta中擁有超級管理員權限。

OneLogin by One Identity

OneLogin by One Identity是一種現代化的雲端存取管理解決方案，可無縫管理員工、客戶和合作夥伴的所有數位身分識別。 OneLogin提供安全的單一登入 (SSO)、多重要素驗證 (MFA)、調適性驗證、桌面層級 MFA、目錄整合至 AD、LDAP、G Suite 和其他外部目錄、身分識別生命週期管理等。您可以使用OneLogin安全性來接收稽核日誌和使用者資料、將資料標準化為開放網路安全架構架構 (OCSF) 格式，並將資料標準化 AWS AppFabric 為開放網路安全架構架構 (OCSF) 格式，並將資料輸出到 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。OneLogin

主題

- AppFabric 支援 OneLogin by One Identity
- 連接 AppFabric 到您的OneLogin by One Identity帳戶

AppFabric 支援 OneLogin by One Identity

AppFabric 支持從中接收用戶信息和審計日誌OneLogin by One Identity。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸OneLogin by One Identity到支援的目的地，您必須符合下列需求：

- 您必須擁有OneLogin高級或專業帳戶。
- 您必須擁有具有管理員/委派管理員權限的使用者。

速率限制考量

OneLogin by One Identity對 OneLogin API 施加速率限制。如需 OneLogin API 速率限制的詳細資訊，請參閱 OneLoginAPI 參考資料中的取得速率限制。如果 AppFabric 與您現有 OneLogin API 應用程式的組合超OneLogin出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。但是，OneLogin速率限制可以增加。如需協助，請聯絡您的OneLogin by One Identity客戶經理或聯絡One Identity。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的OneLogin by One Identity帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricOneLogin by One Identity。若要尋找授權所需OneLogin的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與OneLogin by One Identity使用 OAuth 集成。若要在中建立 OAuth 應用程式OneLogin，請使用下列步驟：

1. 瀏覽至OneLogin登入頁面並登入。
2. 從「開發人員」功能表中選擇「API 認證」。
3. 選擇 [新增認證]，輸入新認證的名稱，然後選擇 [讀取全部]。
4. 選擇 [儲存]。 OneLogin會建立用戶端 ID 和用戶端密碼。

所需的範圍

您必須將以下範圍添加到 OneLogin by One Identity OAuth 應用程序：

- 閱讀全部。有關範圍和用戶端認證的詳細資訊，請參閱 API 參考中的使用 OneLogin API 認證。

應用程式授權

租用戶 ID

AppFabric 將要求租用戶 ID。中的承租人 ID AppFabric 是您的執行個體子網域。您可以在瀏覽器的網址列中找到租用戶 ID。例如，`subdomain`是下列 URL 中的承租人識別碼`https://subdomain.onelogin.com`。

租戶名稱

輸入可識別此唯一OneLogin by One Identity組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求一個客戶端 ID。若要在中尋找您的用戶端 IDOneLogin by One Identity，請使用下列步驟：

1. 瀏覽至OneLogin登入頁面並登入。
2. 從「開發人員」功能表中選擇「API 認證」。
3. 選擇 API 憑證以獲取客戶端 ID。

Client secret (用戶端密碼)

AppFabric 將要求一個客戶端密碼。若要在中尋找您的用戶端密碼OneLogin by One Identity，請使用下列步驟：

1. 瀏覽至OneLogin登入頁面並登入。
2. 從「開發人員」功能表中選擇「API 認證」。
3. 選擇 API 憑證以取得用戶端密碼。

客戶端應用授權

在中 AppFabric，使用租用戶 ID 和名稱以及用戶端 ID 和名稱來建立應用程式授權。選擇「連線」以啟用授權。

PagerDuty

PagerDuty是一個數位營運管理平台，可協助團隊將任何訊號轉化為行動，協助團隊減輕對客戶造成影響的問題，讓您能夠更快速地解決問題並更有效率地 與CloudWatch、GuardDutyCloudTrail、和整合Personal Health Dashboard。您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料PagerDuty、將資料標準化為開放網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支持 PagerDuty
- 連接 AppFabric 到您的PagerDuty帳戶

AppFabric 支持 PagerDuty

AppFabric 支持從中接收用戶信息和審計日誌PagerDuty。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸PagerDuty到支援的目的地，您必須符合下列需求：

- 若要存取稽核記錄，您必須擁有PagerDuty商業或數位營運計劃。
- 您應該是帳戶的全域管理員或帳PagerDuty戶擁有者。

速率限制考量

PagerDuty對 PagerDuty API 施加速率限制。如需 PagerDuty API 速率限制的詳細資訊，請參閱PagerDuty開發人員平台上的 REST API 速率限制。如果 AppFabric 與您現有 PagerDuty API 應用程式的組合超PagerDuty出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的PagerDuty帳戶

該PagerDuty平台支持 API 訪問密鑰。若要產生 API 存取金鑰，請使用下列步驟。

建立 API 存取金鑰

AppFabric 與PagerDuty使用公共用戶端的 API 存取金鑰整合。若要在中建立 API 存取金鑰 PagerDuty，請使用下列步驟：

1. 瀏覽至PagerDuty登入頁面並登入。
2. 選擇 [整合]、[API 存取金鑰]。
3. 選擇「建立新的 API 金鑰」。
4. 輸入說明，然後選取 [唯讀 API 金鑰]。
5. 選擇 Create Key (建立金鑰)。
6. 複製並儲存 API 金鑰。你稍後會需要這個 AppFabric。如果在保存 API 密鑰之前關閉頁面，則必須生成新的 API 密鑰並保存它。此金鑰應專用於 AppFabric 避免與其他整合共用 PagerDuty API 速率限制。

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。您PagerDuty帳戶的承租人識別碼是您帳戶的基本 URL。您可以通過登錄PagerDuty並從 Web 瀏覽器的地址欄複製來找到此信息。承租人識別碼應遵循下列其中一種格式：

- 對於美國帳戶，*subdomain*.pagerduty.com
- 對於歐盟帳戶，*subdomain*.eu.pagerduty.com

租戶名稱

輸入可識別此唯一PagerDuty組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

服務帳戶令牌

AppFabric 將請求您的服務帳戶令牌。中的服務帳戶令牌 AppFabric 是您在其中創建的 API 訪問密鑰建立 API 存取金鑰。

Ping Identity

在Ping Identity，我們堅信為所有用戶提供安全無縫的數字體驗，而不會妥協。這就是為什麼超過一半的財富 100 大企業選擇Ping Identity保護用戶的數字互動，同時使體驗無摩擦。2023 年 8 月 23 日，共同為客戶Ping Identity和ForgeRock合作夥伴提供更多選擇、更深入的專業知識以及更完整的身分識別解決方案。您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Ping Identity、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 Ping Identity
- 連接 AppFabric 到您的Ping Identity帳戶

AppFabric 支援 Ping Identity

AppFabric 支持從中接收用戶信息和審計日誌Ping Identity。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Ping Identity到支援的目的地，您必須符合下列需求：

- 您必須擁有基本帳戶、Plus 或進階Ping Identity帳戶。如需有關建立或升級至適用Ping Identity方案類型的詳細資訊，請參閱Ping Identity網站上所有功能的Ping Identity定價。
- 您的Ping Identity帳戶中必須具有「身分資料唯讀」角色。您可以透過為應用程式授予角色，將角色新增至您的帳戶。如需角色的詳細資訊，請參閱 Sup Ping Identity port 網站上的角色。

速率限制考量

Ping Identity不發布費率限制。您必須建立支援案例或聯絡您的Ping Identity客戶成功團隊。如果 AppFabric 與您現有 Ping Identity API 應用程式的組合超Ping Identity出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Ping Identity帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricPing Identity。若要尋找授權所需Ping Identity的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與Ping Identity使用 OAuth 集成。若要在中建立 OAuth 應用程式Ping Identity，請使用下列步驟：

1. 請依照網站上「開發人員使用」指南中「建立應用程式連線」一節中的指示進Ping Identity行。PingOne
2. 建立應用程式之後，請自訂授權類型。
    a. 登入應用程式後，請選擇「組態」索引標籤，然後按一下鉛筆圖示，在現有的組態中進行變更。
    b. 在「授權類型」下，選取「授權碼」。將 PKCE 強制保持為選擇性。
    c. 選取重新整理權杖，然後選擇重新整理持續時間

3. 在重定向 URL /回調URL 中使用具有以下格式的重定向 URL。

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

在此 URL 中，<region>是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的承租人 ID AppFabric 是您的Ping Identity執行個體名稱。您可以在瀏覽器的網址列中找到租用戶 ID。例如 *API_PATH*/v1/environments/*environmentID*。其中*API_PATH*代表PingOne伺服器的地區網域，例如api.pingone.com，並*environmentID*代表您在應用程式環境屬性中指定的環境 ID。如需有關環境屬性的詳細資訊，請參閱Ping Identity網站上的環境屬性。

租戶名稱

輸入可識別此唯一Ping Identity組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求一個客戶端 ID。若要在中尋找您的用戶端 IDPing Identity，請使用下列步驟：

1. 登入PingOne管理控制台，然後選擇 [應用程式]。
2. 從清單中選擇應用程式。
3. 選擇 [概觀] 索引標籤，然後尋找 [用戶端 ID] 值。

Client secret (用戶端密碼)

AppFabric 將要求客戶端密碼。若要在中尋找您的用戶端密碼Ping Identity，請使用下列步驟：

1. 登入PingOne管理控制台，然後選擇 [應用程式]。
2. 從清單中選擇應用程式。
3. 選擇 [概觀] 索引標籤，然後尋找 [用戶端密碼] 值。

核准授權

在中創建應用程序授權後 AppFabric，您將收到一個彈出窗口，Ping Identity用於批准授權。若要核准 AppFabric 授權，請選擇 [允許]。

Salesforce

Salesforce使基於雲的軟件旨在幫助企業找到更多潛在客戶，完成更多交易，並通過出色的服務為客戶帶來驚喜。 Salesforce'sCustomer 360 提供完整的產品套件，將銷售、服務、行銷、商務和 IT 團隊與單一共用的客戶資訊檢視結合在一起，協助組織與客戶和員工建立關係。您可以使用從中 AWS AppFabric 接收稽核日誌和使用者資料Salesforce、將資料標準化為開放網路安全架構架構 (OCSF) 格式，以及將資料輸出到 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 Salesforce
- 連接 AppFabric 到您的Salesforce帳戶

AppFabric 支援 Salesforce

AppFabric 支持從中接收用戶信息和審計日誌Salesforce。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Salesforce到支援的目的地，您必須符合下列需求：

- 您必須擁有的「效能」、「企業版」或「無限制」版本Salesforce。請聯絡Salesforce以升級至其中一個版本。
- 如果您想要從中 AppFabric 傳輸具有完整記錄事件集的每小時事件記錄檔Salesforce，您必須訂閱事件監控，做為的 Shield 功能的一部分Salesforce。否則， AppFabric將從Salesforce's標準每日日誌文件傳輸有限的事件（即登錄， InsecureExternalAssets註銷，API 總使用量，CORS 違規和 HostnameRedirects ELF 事件）。您可以前往「設定 > 事件管理員」來檢查您的Salesforce帳戶是否已訂閱 Shield 功能。如果您看到列出 19 個以上的事件，表示您的帳戶已訂閱事件監控。如果您沒有事件監控，則可以通過聯繫購買此附加組件的訂閱Salesforce。
- 您需要在設置中選擇加入事件日誌文Salesforce件的生成。
- 您應該使用系統管理員設定檔來建立 OAuth 應用程式，並使用相同的認證登入。 AppFabric

> **Note**
>
> API 總使用量、CORS 違規記錄、主機名稱重新導向、不安全的外部資產、登入和登出事件在支援的版本中無需額外付費。Salesforce請聯絡Salesforce以購買剩餘的活動類型。如需Salesforce事件類型的詳細資訊，請參閱Salesforce網站上EventLogFile 支援的事件類型。AppFabric 每個記錄檔執行個體每個事件類型最多可支援 100,000 個事件 (每日或每小時，視事件監控附加元件訂閱而定)。超過臨界值的記錄檔可能會導致整個記錄檔遭到擷取排除。

速率限制考量

Salesforce對 Salesforce API 施加速率限制。如需 Salesforce API 速率限制的詳細資訊，請參閱Salesforce網站上的 API 要求限制和配置。如果 AppFabric 與您現有 Salesforce API 應用程式的組合超出Salesforce's限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會在每日記錄檔上看到最多 6 小時的延遲，或者每小時記錄檔最多可能會延遲 29 小時，以便將稽核事件傳送至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Salesforce帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricSalesforce。若要尋找授權所需Salesforce的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與Salesforce使用的 OAuth 集成。若要在中建立 OAuth 應用程式Salesforce，請使用下列步驟：

1. 登錄到您的Salesforce帳戶。
2. 依照說明Salesforce文件中所述移至「設定」頁面。
3. 在快速查找中搜索應用程序管理器。
4. 選擇新連線的應用程式。
5. 在表格欄位中輸入必要資訊。
6. 選擇啟用 OAuth 設定。

7. 請務必關閉以下選項：

   - 支援的授權流程需要驗證金鑰才能進行程式碼交換 (PKCE) 延伸
   - Web 伺服器流程需要密碼
   - 重新整理權杖流需要密碼

8. 在回呼 URL 文字方塊中輸入下列格式的 URL，然後選擇 [儲存變更]。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   在此 URL 中，<region>是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

9. 視需要填入範圍 (如下所需範圍節所述)。所有其他欄位都可以保留其預設值。
10. 選擇儲存。
11. 完成以下步驟以驗證新 OAuth 應用程式的重新整理權杖原則：

    a. 在 [設定] 頁面上，在 [快速尋找] 文字方塊中輸入連線的應用程式，然後選擇 [管理連線的應用程式
    b. 選擇新創建的應用程序旁邊的編輯。
    c. 請確定已選取 [重新整理權杖在撤銷之前是有效的] 選項。
    d. 儲存您的變更。

12. 完成下列步驟，以確認是否正在產生稽核記錄：

    a. 在 [設定] 頁面上，在 [快速尋找] 文字方塊中輸入事件記錄檔案，然後選擇 [事件記錄檔瀏覽器]。
    b. 確認事件記錄檔列在事件記錄檔瀏覽器中。

13. 導航到創建的應用程序，然後從下拉菜單中選擇查看。
14. 選擇管理消費者詳細資訊。

    您將被重定向到一個新標籤，您將需要在其中驗證您的身份。在該索引標籤上，記下「取用者金鑰」和「取用者密碼」值。您稍後需要這些資訊才能登入。

所需範圍

您必須將以下範圍添加到 Salesforce OAuth 應用程序：

- 透過 API 管理使用者資料 (API)。
- 隨時執行請求（ refresh_token和offline_access ）。

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的承租人識別碼 AppFabric 是「我的網域」的Salesforce子網域。您可以在瀏覽器的網址列中找到「我的網域」子網域。https:// .my.salesforce.com

若要尋找您的「Salesforce我的網域」，請使用Salesforce主畫面上的下列指示。

1. 依照說明Salesforce文件中所述移至「設定」頁面。
2. 在快速尋找中搜尋「公司設定」，然後在結果中選擇「我的網域」。

租戶名稱

輸入可識別此唯一Salesforce組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求一個客戶端 ID。若要在中尋找您的用戶端 IDSalesforce，請使用下列步驟：

1. 導覽至「設定」頁面。
2. 選擇設定，然後選擇 [應用程式管理員]。
3. 選擇創建的應用程序，然後選擇查看從下拉菜單中。
4. 選擇管理消費者詳細資訊。您將被重定向到一個新標籤。
5. 驗證您的身分，然後尋找消費者金鑰值。
6. 在中的用戶端 ID 欄位中輸入消費者金鑰 AppFabric。

Client secret (用戶端密碼)

AppFabric 將要求您的客戶密碼。中的用戶端密碼 AppFabric 是中的消費者密碼Salesforce。若要在中尋找您的密碼Salesforce，請使用下列步驟：

1. 導覽至「設定」頁面。

2. 選擇設定，然後選擇 [應用程式管理員]。
3. 選擇創建的應用程序，然後選擇查看從下拉菜單中。
4. 選擇管理消費者詳細資訊。您將被重定向到一個新標籤。
5. 驗證您的身分，然後尋找消費者密碼值。
6. 在中的用戶端密碼欄位中輸入消費者密碼 AppFabric。

核准授權

在中創建應用程序授權後 AppFabric，您將收到一個彈出窗口，Salesforce用於批准授權。在核准頁面上，請務必使用Salesforce系統管理員角色，或在授權時具有 [檢視事件記錄檔] 和 [啟用 API] 使用者權限的使用者。Salesforce選擇允許以核准 AppFabric授權。

ServiceNow

ServiceNow是雲端式服務的領先供應商，可自動化企業 IT 作業。 ServiceNow的 ITOM 為企業提供全面的能見度和控制其整個 IT 環境，包括虛擬化和雲端基礎架構。它簡化了服務對應、交付和保證，將 IT 服務和基礎架構資料整合到單一記錄系統中。它還可以自動化並簡化關鍵流程，包括事件、事件、問題、組態和變更管理。您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料ServiceNow、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 ServiceNow
- 資料延遲考量
- 連接 AppFabric 到您的ServiceNow帳戶

AppFabric 支援 ServiceNow

AppFabric 支持從中接收用戶信息和審計日誌ServiceNow。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸ServiceNow到支援的目的地，您必須符合下列需求：

- 您可以搭 AppFabric 配任何ServiceNow計劃類型使用。
- 您的帳戶中必須有具有管理員角色的使用ServiceNow者。

- 您必須擁有ServiceNow執行個體。

速率限制考量

ServiceNow對 ServiceNow API 施加速率限制。如需 ServiceNow API 速率限制的詳細資訊，請參閱ServiceNow網站上的傳入 REST API 速率限制。如果 AppFabric 與您現有 ServiceNow API 應用程式的組合超出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的ServiceNow帳戶

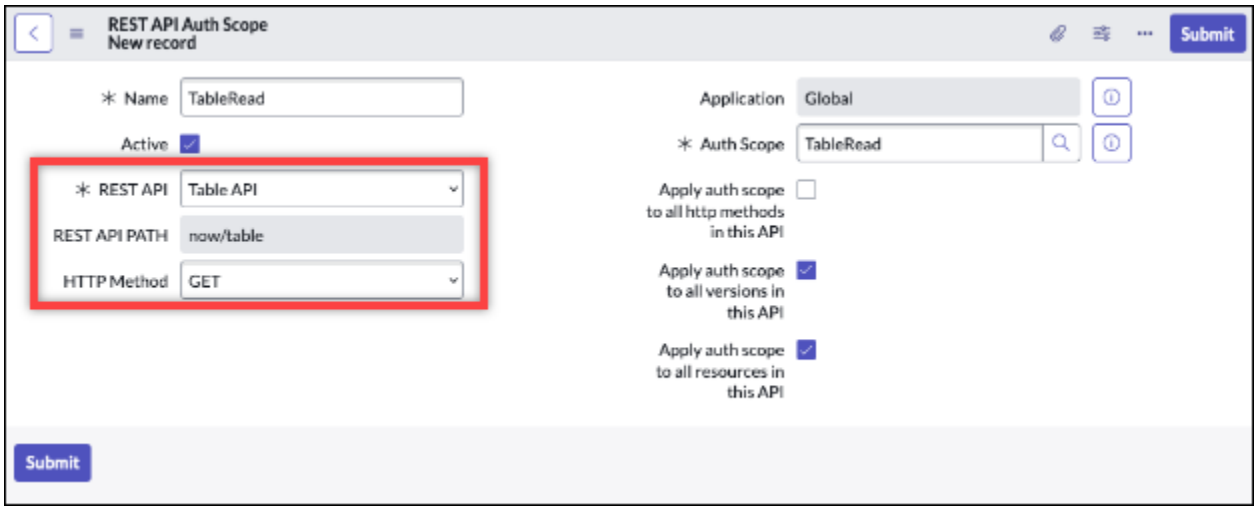
在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricServiceNow。請使用下列步驟尋找授權ServiceNow所需的資訊 AppFabric。

建立 OAuth 應用程式

Now Platform支持 OAuth 2.0-授權授予類型，供公共客戶端生成訪問令牌。

1. 註冊您的 OAuth 應用程式。這需要以下三個步驟。有關完成這些步驟的更多信息，請參閱在ServiceNow網站ServiceNow上註冊您的應用程序。

   a. 註冊應用程序，並確保身份驗證範圍可以訪問表 API，現在/表的 REST API 路徑，以及 GET 的 HTTP 方法，如下面的示例所示。



b. 產生授權碼。

c. 使用授權碼生成承載令牌。

2. 使用下列格式的重新導向 URL。

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

在此 URL 中，<region>是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

應用程式授權

租用戶 ID

AppFabric 將要求租用戶 ID。中的承租人 ID AppFabric 是您的執行個體名稱。您可以在瀏覽器的網址列中找到租用戶 ID。例如，*example*是下列 URL 中的承租人識別碼https://*example*.service-now.com。

租戶名稱

輸入可識別此唯一ServiceNow組織的名稱。 AppFabric 使用租用戶的名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求一個客戶端 ID。使用下列步驟在中尋找您的用戶端 ID ServiceNow。

1. 導覽至 ServiceNow 主控台。
2. 選擇 [系統 OAuth]，然後選擇 [應用程式登錄] 索引標籤。
3. 選擇您的應用程式。
4. 將 OAuth 用戶端的用戶端識別碼輸入中的「用戶端識別碼」欄位 AppFabric。

Client secret (用戶端密碼)

AppFabric 將要求客戶端密碼。使用下列步驟在中尋找您的用戶端密碼ServiceNow。

1. 導覽至 ServiceNow 主控台。

2. 選擇 [系統 OAuth]，然後選擇 [應用程式登錄] 索引標籤。
3. 選擇您的應用程式。
4. 將 OAuth 應用程式中的用戶端密碼輸入到中的「用戶端密碼」欄位中 AppFabric。

核准授權

在中創建應用程序授權後 AppFabric，您將收到一個彈出窗口，ServiceNow用於批准授權。選擇允許以核准 AppFabric 授權。

Singularity Cloud

該Singularity Cloud平台可在所有階段保護您的企業免受所有類別的威脅。其專利人工智慧將安全性從已知的特徵碼和模式延伸到最複雜的攻擊，例如零時差和勒索軟體。

您可以使用從中 AWS AppFabric 接收稽核日誌和使用者資料Singularity Cloud、將資料標準化為開放網路安全架構架構 (OCSF) 格式，以及將資料輸出到 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

> **Note**
>
> Singularity Cloud只有在您登入Singularity Cloud帳戶後，才能存取文件。因此，我們無法直接連結至本Singularity Cloud文件中的文件。

主題

- AppFabric 支援 Singularity Cloud
- 連接 AppFabric 到您的Singularity Cloud帳戶

AppFabric 支援 Singularity Cloud

AppFabric 支持從中接收用戶信息和審計日誌Singularity Cloud。

必要條件

若 AppFabric 要用於將稽核記錄從轉移Singularity Cloud到支援的目的地，您的Singularity Cloud帳戶中必須具有系統管理員角色。如需 Singularity Cloud API 速率限制的詳細資訊，請登入您的奇點雲端帳戶、瀏覽文件區段，然後搜尋角色。

速率限制考量

Singularity Cloud對 Singularity Cloud API 施加速率限制。如需 Singularity Cloud API 速率限制的詳細資訊，請登入您的奇點雲端帳戶、瀏覽文件區段，然後搜尋 API 速率限制。

資料延遲考量

您可能會看到將稽核事件傳送至目的地的延遲最多 30 分鐘。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Singularity Cloud帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricSingularity Cloud。若要尋找授權所需 Singularity Cloud的資訊 AppFabric，請使用下列步驟。

為以下項目建立 API 權杖 Singularity Cloud

請完成下列程序，以建立與服務使用者相關聯的 API 權杖。API 令牌不會鏈接到特定的控制台用戶或電子郵件地址。

> **Note**
>
> 建立新使用者或複製服務使用者，以在服務使用者 API 權杖到期之前或之後取得新的 API 權杖。

1. 登入 Singularity Cloud 帳戶。
2. 在 [設定] 工具列中選擇 [使用者]，然後選擇 [服務使用者]。
3. 選擇 [動作]，然後選取 [建立新服務使用者]。
4. 在 [建立新服務使用者] 頁面中，輸入服務使用者的名稱、說明和到期日。
5. 選擇下一步。
6. 在「選取存取範圍」 區段中，選取範圍。
   - 選取 [帳戶] 做為存取層級。
   - 選取您要取得稽核記錄的帳戶。
7. 選擇 Create User (建立使用者)。

即會產生 API 權杖。隨即開啟一個視窗，並顯示 Token 字串，其中包含一則訊息，指出這是您上次可以檢視權杖的時間。

8. （可選）選擇複製 API 令牌並將其存儲在安全的位置。
9. 選擇關閉。

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的租用戶 ID AppFabric 將是您登入服務之Sentinel One網站位址的子網域。例如，如果您使用該`example-company-1.sentinelone.net`地址登入您的Singularity Cloud帳戶，則您的租用戶 ID 為`example-company-1`。

租戶名稱

輸入可識別此唯一Singularity Cloud組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

服務帳戶令牌

使用您使用本指南一為以下項目建立 API 權杖 Singularity Cloud節中的步驟產生的權杖。如果您找不到權杖或找不到權杖，您可以再次執行相同的步驟來產生新的權杖。

> **Note**
>
> 如果在擷取稽核記錄時在奇點雲端主控台中產生新 AppFabric 的 API 權杖，擷取將會停止。如果發生這種情況，您將需要使用新的 API 令牌更新應用程序授權，以繼續審核日誌導入。

Slack

Slack是一個使命，使人們的工作生活更簡單，更愉快，更有效率。它是客戶公司的生產力平台，透過讓每個人都能進行無程式碼自動化、順暢地進行搜尋和知識共用，並在團隊共同推進工作時保持聯繫和參與，從而提高績效。作為其中的Slack一部分Salesforce，深入整合到Salesforce客戶 360 中，提高銷售、服務和行銷團隊的生產力。要了解更多信息並免費開始使Slack用，請訪問 slack.com。

您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Slack、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

AppFabric 支援 Slack

AppFabric 支持從中接收用戶信息和審計日誌Slack。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Slack到支援的目的地，您必須符合下列需求：

- 您必須擁有使用的企業網格方案Slack。如需詳細資訊，請參閱Slack網站上的Slack企業方格簡介。
- 您的帳戶中必須具有「組織擁有者」角色的使用Slack者。如需有關角色的詳細資訊，請參閱Slack網站上Slack說明Slack中心中的角色類型。

速率限制考量

Slack對 Slack API 施加速率限制。如需 Slack API 速率限制的詳細資訊，請參閱Slack網站上的 SlackAPI 使用指南中的速率限制。如果 AppFabric 與您現有 Slack API 應用程式的組合超出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Slack帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricSlack。若要尋找授權所需Slack的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與Slack使用 OAuth 集成。有兩種方法可以創建 OAuth 應用程序：使用應用程序清單或從頭開始。若要在中建立 OAuth 應用程式Slack，請使用下列步驟。

Using an app manifest

1. 導航到瀏覽器中的Slack應用程序管理 UI。

2. 選擇建立新的應用程式。
3. 從應用程式資訊清單中選擇。
4. 選擇您要授權的工作區 AppFabric。
5. 在 [輸入應用程式資訊清單下方] 方塊中，選擇 [JSON]，並以下列方式取代現有的 JSON。以 <region>適當的取代 AWS 區域 (例如，*us-east-1*)。

```
{
    "display_information": {
        "name": "AppFabric"
    },
    "oauth_config": {
        "redirect_urls": [
            "https://<region>.console.aws.amazon.com/appfabric/oauth2"
        ],
        "scopes": {
            "user": [
                "auditlogs:read",
                "users:read.email",
                "users:read"
            ]
        }
    },
    "settings": {
        "org_deploy_enabled": false,
        "socket_mode_enabled": false,
        "token_rotation_enabled": true
    }
}
```

6. 從「基本資訊」頁面複製並儲存用戶端 ID 和用戶端密碼。
7. 對於範`auditLogs:read`圍，您必須啟用應用程序的公共分發。如需詳細資訊，請參閱在 Slack 網站上啟用公開發佈。

From scratch

1. 在「建立應用程式」畫面上選擇「從頭開始」。
2. 為您的應用程式命名並選擇工作區。
3. 從「基本資訊」頁面複製並儲存用戶端 ID 和用戶端密碼。
4. 在 OAuth 和權限頁面上，選擇通過令牌輪換選項加入高級令牌安全性。

5. 在 OAuth 與權限頁面的「重新導向 URL」區段中新增具有下列格式的 URL。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   在此 URL 中，*<region>*是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。
6. 對於範auditLogs:read圍，您必須啟用應用程序的公共分發。如需詳細資訊，請參閱在 Slack 網站上啟用公開發佈。

所需範圍

> **Note**
>
> 僅當您選擇從頭開始創建 OAuth 應用程序時，此部分才適用。如果您選擇使用應用程式資訊清單建立應用程式授權，請略過本節。

您必須在 OAuth 應用程序的 OAuth 和權限頁面上添加以下用戶Slack令牌範圍：

- auditlogs:read
- users:read.email
- users:read

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的承租人識別碼 AppFabric 是您的Slack工作區識別碼。若要取得租用戶 ID，請依照Slack網站上說明中心的「Slack尋找您的 Slack URL」中的指示操作。您的Slack工作區 URL 具有類似於examplecorp.slack.com或的格式examplecorp.enterprise.slack.com。您需要的租用戶識別碼examplecorp不含.slack.com或.enterprise.slack.com。

租戶名稱

輸入可識別您的Slack工作區 ID 的名稱。 AppFabric使用租戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取

用戶端 ID

AppFabric 將從您的 Slack OAuth 應用程序請求客戶端 ID。若要尋找用戶端 ID，請使用下列步驟：

1. 導航到瀏覽器中的Slack應用程序管理 UI。
2. 選擇您搭 AppFabric配使用的 OAuth 應用程式。
3. 在中的「用戶端 ID」欄位中，將「基本資訊」頁面中的用戶端 ID 輸入 AppFabric。

Client secret (用戶端密碼)

AppFabric 將從您的 Slack OAuth 應用程序請求客戶端密鑰。若要尋找用戶端密碼，請使用下列步驟：

1. 導航到瀏覽器中的Slack應用程序管理 UI。
2. 選擇與 AppFabric您搭配使用的 OAuth 應用程式。
3. 在中的「用戶端密碼」欄位中，將「基本資訊」頁面中的用戶端密碼輸入 AppFabric。

核准授權

在中創建應用程序授權後 AppFabric，您將收到一個彈出窗口，Slack用於批准授權。若要核准 AppFabric 授權，請選擇 [允許]。

Smartsheet

Smartsheet是一個工作管理平台，可幫助您調整整個企業的工作，人員和技術。 Smartsheet提供一組強大的企業級功能，讓每個人都能夠管理專案、自動化工作流程，並快速建置大規模解決方案，為創新創造環境，同時維持安全性和合規性。

您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Smartsheet、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 Smartsheet
- 連接 AppFabric 到您的Smartsheet帳戶

AppFabric 支援 Smartsheet

AppFabric 支持從中接收用戶信息和審計日誌Smartsheet。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Smartsheet到支援的目的地，您必須符合下列需求：

- 您必須擁有Smartsheet商業帳戶、企業或進階帳戶。如需建立或升級Smartsheet帳戶的詳細資訊，請參閱Smartsheet網站上的「Smartsheet定價」或「Smartsheet進階」。
- 您必須完成Smartsheet開發人員註冊程序。

速率限制考量

Smartsheet對 Smartsheet API 施加速率限制。如需 Smartsheet API 速率限制的詳細資訊，請參閱 Smartsheet 網站上的 Smartsheet API 參考資料中的速率限制。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Smartsheet帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricSmartsheet。若要尋找授權所需Smartsheet的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與Smartsheet使用 OAuth 集成。若要在中建立 OAuth 應用程式Smartsheet，請使用下列步驟：

1. 瀏覽至Smartsheet帳戶中的開發人員工具。
2. 從開發人員工具屏幕中選擇創建新的應用程序。
3. 完成「建立新應用程式」畫面上的所有輸入欄位。
4. 針對應用程式 URL 和應用程式連絡人/支援使用任何唯一值。
5. 使用具有下列格式的重新導向 URL 作為應用程式重新導向 URL。

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

在此 URL 中，*<region>*是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

6. 選擇儲存。
7. 複製並儲存應用程式用戶端 ID 和應用程式密碼。

所需範圍

Smartsheet不要求您明確地將範圍添加到 OAuth 配置中。 AppFabric 將在授權請求中向您的Smartsheet帳戶請求以下範圍：

- READ_EVENTS
- READ_USERS

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的承租人識別碼 AppFabric 是您的Smartsheet帳戶識別碼。

租戶名稱

AppFabric 將要求您的租用戶 ID。輸入可唯一識別您Smartsheet帳戶的任何值。

用戶端 ID

AppFabric 將要求您的客戶 ID。中的用戶端 ID AppFabric 是您的Smartsheet應用程式用戶端 ID。要在中找到您的應用程序客戶端 IDSmartsheet，請使用以下步驟：

1. 瀏覽至Smartsheet帳戶中的開發人員工具。
2. 選取您用來連線的 OAuth 應用程式 AppFabric。
3. 將「應用程式設定檔」畫面中的應用程式用戶端 ID 輸入到的「用戶端 ID」欄位 AppFabric。

Client secret (用戶端密碼)

AppFabric 將要求您的客戶密碼。中的用戶端密碼 AppFabric 是您的Smartsheet應用程式秘密。若要在中尋找您的應用程式密碼Smartsheet，請使用下列步驟：

1. 瀏覽至Smartsheet帳戶中的開發人員工具。
2. 選取您用來連線的 OAuth 應用程式 AppFabric。

3. 從「應用程式設定檔」畫面輸入應用程式密碼到中 AppFabric的「用戶端密碼」欄

核准授權

在中創建應用程序授權後 AppFabric，您將收到一個彈出窗口，Smartsheet用於批准授權。若要核准 AppFabric 授權，請選擇 [允許]。

Terraform Cloud

HashiCorp Terraform Cloud是全球使用最廣泛的多雲端佈建產品。該Terraform生態系統擁有 3,000 多家提供商，14,000 個模塊和 2.5 億次下載。 Terraform Cloud是採用最快速的方式Terraform，提供從業人員、團隊和全球企業在基礎架構上建立和協作所需的一切，以及管理安全性、合規性和營運限制的風險。您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Terraform Cloud、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 Terraform Cloud
- 連接 AppFabric 到您的Terraform Cloud帳戶

AppFabric 支援 Terraform Cloud

AppFabric 支持從中接收用戶信息和審計日誌Terraform Cloud。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Terraform Cloud到支援的目的地，您必須符合下列需求：

- 若要存取稽核記錄，您必須擁有 Terraform Cloud Plus Edition 方案，並且是組織的擁有者。有關Terraform Cloud計劃的更多信息，請參閱HashiCorp Terraform網站上的Terraform定價。
- TBD 稽核記錄可供從Terraform Cloud帳戶建立的組織使用。

速率限制考量

Terraform Cloud對 Terraform Cloud API 施加速率限制。如需 Terraform Cloud API 速率限制的詳細資訊，請參閱Terraform Cloud網站上Terraform Cloud開發人員管理一般設定中的 API 速率限制。如果 AppFabric 與您現有 Terraform Cloud API 應用程式的組合超Terraform Cloud出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Terraform Cloud帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricTerraform Cloud。若要尋找授權所需Terraform Cloud的資訊 AppFabric，請使用下列步驟。

建立組織 API 權杖

AppFabric 與Terraform Cloud使用組織 API 令牌集成。如需有關Terraform Cloud組織 API 權杖的詳細資訊，請參閱組織 API 權杖。欲建立組織，請遵循建立組 Organizations 中的指示。若要在中建立組織 API 權杖Terraform Cloud，請使用下列步驟。

1. 導覽至Terraform Cloud登入頁面並登入。
2. 選擇左側面板上的「組織」，「設置」，然後選擇「API 令牌」。
3. 在「組織權杖」下，選擇「建立組織權杖」，然後選擇「產生權杖」。
4. (選擇性) 輸入權杖的到期日或時間，或建立永不過期的權杖。
5. 複製並儲存權杖。你稍後會需要這個 AppFabric。如果在保存令牌之前關閉頁面，則必須撤銷舊令牌並創建一個新令牌。

應用程式授權

租用戶 ID

AppFabric 將要求租用戶 ID。您帳戶的承租人識別碼是您Terraform Cloud帳戶目前的組織 URL。您可以透過登入您的Terraform Cloud組織並複製目前的組織 URL 來找到此資訊。承租人識別碼應遵循下列其中一種格式：

```
https://app.terraform.io/app/organization_URL
```

租戶名稱

輸入可識別此唯一Terraform Cloud組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

服務帳戶令牌

AppFabric 將請求您的服務帳戶令牌。中的服務帳戶令牌 AppFabric 是您在其中創建的組織 API 令牌建立組織 API 權杖。

Webex by Cisco

Cisco是為互聯網提供動力的全球技術領導者。 Cisco透過重新構想您的應用程式、保護資料安全、轉型您的基礎架構，以及讓您的團隊能夠實現全球性和包容性的 future，激發新的可能性。

關於 Webex by Cisco

Webex是雲端協作解決方案的領先供應商，其中包括視訊會議、通話、訊息傳遞、活動、客戶體驗解決方案，例如客服中心和專門打造的協作裝置。 Webex專注於提供包容性協作體驗，推動了利用 AI 和 Machine Learning 的創新，以消除地理、語言、個性和熟悉技術的障礙。其解決方案在設計上以安全性和隱私為基礎。 Webex與全球領先的商業和生產力應用程式搭配使用 — 透過單一應用程式和介面提供。如需進一步了解，請參閱webex.com。

您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Webex、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 Webex
- 連接 AppFabric 到您的Webex帳戶

AppFabric 支援 Webex

AppFabric 支持從中接收用戶信息和審計日誌Webex。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Webex到支援的目的地，您必須符合下列需求：

- 您必須擁有「協作彈性計劃」、「會議計劃」、「通話方案」或更高版本。如需有關建立或升級至適用Webex方案類型的詳細資訊，請參閱Webex網站上所有功能的Webex定價。
- 您的帳戶必須擁有 Pro Pack 授權，才能存取其中一個 Cisco AuditLog API 提供的安全稽核事件。
- 您必須擁有具有「組織管理員」>「完全管理員」角色的使用者。

- 您的「完整管理員」的「管理員角色」組態必須啟用「規範遵循官」選項。

速率限制考量

Webex對 Webex API 施加速率限制。如需 Webex API 速率限制的詳細資訊，請參閱Webex網站Webex開發人員指南中的速率限制。如果 AppFabric 與您現有 Webex API 應用程式的組合超出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Webex帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricWebex。若要尋找授權所需Webex的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與Webex使用 OAuth 集成。若要在中建立 OAuth 應用程式Webex，請使用下列步驟：

1. 依照Webex開發人員指南「整合與授權」頁面中「註冊您的整合」區段中的指示進行。
2. 使用下列格式的重新導向 URL。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   在此 URL 中，*<region>*是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

所需的範圍

您必須將以下範圍添加到 Webex OAuth 應用程序：

- `spark-compliance:events_read`
- `audit:events_read`

- `spark-admin:people_read`

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的承租人識別碼 AppFabric 是您的Webex組織識別碼。如需如何尋找Webex組織 ID 的詳細資訊，請參閱Webex說明中心網站上的 CiscoWebexControl Hub 中查詢您的組織 ID。

租戶名稱

輸入可識別此唯一Webex執行處理的名稱。 AppFabric使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求您的Webex客戶 ID。若要尋找您的用Webex戶端 ID，請使用下列步驟：

1. 登入您的Webex帳戶，請到 https://developer.webex.com。
2. 在右上角選擇您的虛擬人偶。
3. 選擇我的 Webex 應用程式。
4. 選擇您用於的 OAuth2 應用程式。 AppFabric
5. 在中的「用戶端 ID」欄位中輸入此頁面上的用戶端 ID AppFabric。

Client secret (用戶端密碼)

AppFabric 將要求您的Webex客戶密碼。 Webex當您最初建立 OAuth 應用程式時，只會顯示一次用戶端密碼。若要在未儲存初始用戶端密碼時產生新的用戶端密碼，請使用下列步驟：

1. 登入您的Webex帳戶，請到 https://developer.webex.com。
2. 在右上角選擇您的虛擬人偶。
3. 選擇我的 Webex 應用程式。
4. 選擇您用於的 OAuth2 應用程式。 AppFabric
5. 在此頁面上，產生新的用戶端密碼。
6. 在中的 [用戶端密碼] 欄位中輸入新的用戶端密碼 AppFabric。

核准授權

在中創建應用程序授權後， AppFabric 您將收到一個彈出窗口，Webex用於批准授權。若要核准AppFabric授權，請選擇 [接受]。

Zendesk

Zendesk2007 年開始了客戶體驗革命，使全球任何企業都能在線上使用客戶服務。如今，它Zendesk是為所有人提供優質服務的冠軍，並為數十億次對話提供支持，通過電話，聊天，電子郵件，消息傳遞，社交渠道，社區，評論網站和幫助中心將 100,000 多個品牌與數億客戶聯繫起來。 Zendesk產品是用愛而建立的。該公司成立於丹麥哥本哈根，在加利福尼亞州建立和發展，如今在世界各地僱用了 6,000 多名員工。

您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Zendesk、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- AppFabric 支援 Zendesk
- 連接 AppFabric 到您的Zendesk帳戶

AppFabric 支援 Zendesk

AppFabric 支持從中接收用戶信息和審計日誌Zendesk。

必要條件

若要用 AppFabric 來將稽核記錄從傳輸Zendesk到支援的目的地，您必須符合下列需求：

- 您必須擁有企業Zendesk套件或企業 Plus 帳戶或 Sup Zendesk port 企業帳戶。如需建立或升級至 Zendesk 企業帳戶的詳細資訊，請參閱在Zendesk網站Zendesk上檢查您的方案類型。
- 您的帳戶中必須有具有管理員角色的使用Zendesk者。如需有關角色的詳細資訊，請參閱了解Zendesk網站上的 Sup Zendesk port 使用者角色。

速率限制考量

Zendesk對 Zendesk API 施加速率限制。如需 Zendesk API 速率限制的詳細資訊，請參閱Zendesk網站Zendesk開發人員指南中的速率限制。如果 AppFabric 與您現有 Zendesk API 應用程式的組合超出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到最多 30 分鐘的延遲，讓稽核事件傳遞至您的目的地。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。不過，這可能是在帳戶層級自訂的。如需協助，請聯絡AWS Support。

連接 AppFabric 到您的Zendesk帳戶

在 AppFabric 服務中創建應用程序包後，您必須授權 AppFabricZendesk。若要尋找授權所需Zendesk的資訊 AppFabric，請使用下列步驟。

建立 OAuth 應用程式

AppFabric 與Zendesk使用 OAuth 集成。在中Zendesk，您必須使用下列設定建立 OAuth 應用程式：

1. 請依照Zendesk支援網站上的 OAuth 驗證搭配您的應用程式文章的「向 Zendesk 註冊應用程式」一節中的指示 Support 行。
2. 使用下列格式的重新導向 URL。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   在此 URL 中，*<region>*是您 AWS 區域 在其中配置 AppFabric 應用程序包的代碼。例如，美國東部 (維吉尼亞北部) 區域的代碼為us-east-1。對於該區域，重新導向 URL 是https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的承租人 ID AppFabric 是您的Zendesk子網域。如需尋找Zendesk子網域的詳細資訊，請參閱 Sup Zendesk port 網站上哪裡可以找到我的Zendesk子網域。

租戶名稱

輸入可識別此唯一Zendesk組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求一個客戶端 ID。中的用戶端 ID AppFabric 是您的 Zendesk API 唯一識別碼。若要尋找您的 Zendesk 唯一識別碼，請使用下列步驟：

1. 導覽至您Zendesk帳戶中的系統管理中心。
2. 選擇應用程式和整合。
3. 選擇 API、ZendeskAPI。
4. 選擇 OAuth 用戶端索引標籤。
5. 選擇您為其建立的 OAuth 應用程式 AppFabric。
6. 在 AppFabric中的「用戶端識別碼」欄位中輸入 OAuth 用戶端的唯一識別碼。

Client secret (用戶端密碼)

AppFabric 將要求客戶端密碼。中的用戶端密碼 AppFabric 是您的Zendesk秘密權杖。 Zendesk首次創建 Zendesk OAuth 應用程序時，僅顯示一次秘密令牌。若要在未儲存初始密碼權杖時產生新的密碼權杖，請使用下列步驟：

1. 導覽至您Zendesk帳戶中的系統管理中心。
2. 選擇應用程式和整合。
3. 選擇 API、ZendeskAPI。
4. 選擇 OAuth 用戶端索引標籤。
5. 選擇您為其建立的 OAuth 應用程式 AppFabric。
6. 選擇「密碼權杖」欄位旁邊的「重新產生」按鈕。
7. 在中的 [用戶端密碼] 欄位中輸入新的密碼權杖 AppFabric。

核准授權

在中創建應用程序授權後 AppFabric，您將收到一個彈出窗口，Zendesk用於批准授權。若要核准 AppFabric 授權，請選擇 [允許]。

Zoom

Zoom是一個 all-in-one 智能協作平台，使企業和個人的連接更加輕鬆，更加沉浸，更具動態性。Zoom技術將人們置於中心，實現有意義的聯繫，促進現代協作，並通過諸如團隊聊天，電話，會議，全渠道雲端聯絡中心，智能錄音，白板等解決方案推動人類創新。

您可以使 AWS AppFabric 用安全性來接收稽核日誌和使用者資料Zoom、將資料標準化為開放式網路安全架構架構 (OCSF) 格式，以及將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

AppFabric 支援 Zoom

AppFabric 支持從中接收用戶信息和審計日誌Zoom。

必要條件

若 AppFabric 要用於將稽核記錄從傳輸Zoom到支援的目的地，您必須符合下列需求：

- 您必須擁有Zoom專業版、商務版、教育版或企業版方案。
- 您的Zoom管理員角色必須具有建立 server-to-server OAuth 應用程式的權限。如需啟用 server-to-server OAuth 應用程式的相關資訊，請參閱網站上Zoom開發人員指南中「伺服器對伺服器 OAuth」頁面的「啟用權限」一節。Zoom
- 您的Zoom管理員角色必須具有檢視管理員活動記錄和登入/登出稽核活動的權限。如需啟用權限以檢視稽核活動的詳細資訊，請參閱 Sup Zoom port 網站上的使用角色管理和使用管理員活動記錄。

速率限制考量

Zoom對 Zoom API 施加速率限制。如需 Zoom API 速率限制的詳細資訊，請參閱Zoom開發人員指南中的速率限制。如果 AppFabric 與您現有Zoom應用程式的組合超出限制，則顯示在中的稽核記錄 AppFabric 可能會延遲。

資料延遲考量

您可能會看到將稽核事件傳送至目的地的大約 24 小時延遲。這是由於應用程式提供的稽核事件延遲，以及為減少資料遺失而採取的預防措施所致。

連接 AppFabric 到您的Zoom帳戶

在 AppFabric 服務中創建應用程序包後，您必須 AppFabric 使用授權Zoom。若要尋找授權所需Zoom的資訊 AppFabric，請使用下列步驟。

建立 server-to-server OAuth 應用程式

AppFabric 使用 server-to-server OAuth 與應用程序憑據進行集成Zoom。若要在中建立 server-to-server OAuth 應用程式Zoom，請遵循開發人員指南中建立伺服器對伺服器 OAuth 應用程式中的指示。Zoom AppFabric 不支持Zoom網絡掛鉤，您可以跳過添加 webhook 訂閱的部分。

所需的範圍

您必須將以下範圍添加到 Zoom server-to-server OAuth 應用程序：

- `user:read:admin`
- `report:read:admin`

應用程式授權

租用戶 ID

AppFabric 將要求您的租用戶 ID。中的承租人識別碼 AppFabric 是Zoom帳戶識別碼。若要尋找您的Zoom帳戶 ID，請執行下列步驟：

1. 導航到Zoom市場。
2. 選擇管理。
3. 選擇您使用的 server-to-server OAuth 應用程式 AppFabric。
4. 將「應用程式認證」頁面中的帳戶 ID 輸入至中的「租用戶 ID」欄位 AppFabric。

租戶名稱

輸入可識別此唯一Zoom組織的名稱。 AppFabric 使用租用戶名稱來標記應用程式授權，以及從應用程式授權建立的任何擷取。

用戶端 ID

AppFabric 將要求您的客戶 ID。若要尋找您的用Zoom戶端 ID，請使用下列步驟：

1. 導航到Zoom市場。
2. 選擇管理。
3. 選擇您使用的 server-to-server OAuth 應用程式 AppFabric。
4. 從「應用程式憑證」頁面輸入用戶端 ID 到的「用戶端 ID」欄位中 AppFabric。

Client secret (用戶端密碼)

AppFabric 將要求您的客戶密碼。若要尋找您的用Zoom戶端密碼，請使用下列步驟：

1. 導航到Zoom市場。

2. 選擇管理。
3. 選擇您使用的 server-to-server OAuth 應用程式 AppFabric。
4. 從「應用程式認證」頁面輸入用戶端密碼到中的「用戶端密碼」欄位中 AppFabric。

稽核記錄傳送

Zoom通過每 24 小時訪問 API 使審核日誌可用。使用檢視稽核記錄時 AppFabric，您所看到的資料 Zoom適用於前一天的活動。

兼容的安全工具和服務

AWS AppFabric 為了安全支持與以下安全工具和服務集成。選擇服務的名稱，以取得有關如何設定連線到服務 AppFabric 的安全性的詳細資訊。

主題

- Barracuda XDR
- Dynatrace
- Logz.io
- Netskope
- NetWitness
- Amazon QuickSight
- Rapid7
- Amazon Security Lake
- Singularity Cloud
- Splunk

Barracuda XDR

Barracuda Networks是值得信賴的合作夥伴，也是雲端優先安全解決方案的領先供應商，透過創新的解決方案來保護電子郵件、網路、資料和應用程式，這些解決方案可隨著企業 Barracuda XDR是一個開放式擴展檢測和響應解決方案，結合了先進的技術與安全分析師團隊在我們的安全操作中心（SOC）。該Barracuda XDR平台每天分析來自 40 多個整合式資料來源的數十億個原始事件，並搭配對應至 MITRE ATT&CK® 架構的廣泛威脅偵測規則，可以更快地偵測威脅並縮短回應時間。

AWS AppFabric 稽核記錄擷取考量

下列各節說明要搭配使用的輸出結構描述、輸出格式和輸出目的地Barracuda XDR。 AppFabric

結構描述和格式

Barracuda XDR支援下列 AppFabric 輸出結構描述和格式：

- OCSF-JSON： AppFabric 使用開放網路安全架構架構 (OCSF) 將資料標準化，並以 JSON 格式輸出資料。

輸出位置

Barracuda XDR支援從 Amazon 安全湖接收稽核日誌。要將數據從發送 AppFabric 到Barracuda XDR，請按照以下說明進行操作：

1. 將資料傳送至 Amazon 安全湖：設定 AppFabric 以透過 Amazon 資料 Firehose 將資料傳送至 Amazon 安全湖。如需詳細資訊，請參閱 Amazon Security Lake。
2. 將資料傳送至Barracuda XDR：將資料設Barracuda XDR定為接收來自 Amazon 安全湖的稽核日誌。如需詳細資訊，請參閱設定和使用 Amazon 安全湖。

Dynatrace

此系統Dynatrace® Platform結合了廣泛且深入的觀察能力以及持續的執行階段應用程式安全性與進階 AIOps，提供解答並從資料進行智慧 這使創新者能夠實現雲端作業現代化和自動化、更快速、更安全地交付軟體，並確保完美的數位體驗。

AWS AppFabric 稽核記錄擷取考量

下列各節說明要搭配使用的輸出結構描述、輸出格式和輸出目的地Dynatrace Platform。 AppFabric

結構描述和格式

Dynatrace Platform支援下列 AppFabric 輸出結構描述和格式：

- OCSF-JSON： AppFabric 使用開放網路安全架構架構 (OCSF) 將資料標準化，並以 JSON 格式輸出資料。

輸出位置

Dynatrace Platform支援從下列 AppFabric 輸出位置接收稽核記錄。

- Amazon Simple Storage Service (Amazon S3)
  - 若要設定Dynatrace Platform以從包含稽核日誌的 Amazon S3 儲存貯體接收資料，請按照 Dynatrace 的 S3 日誌轉發器專案中的指示進行操作。GitHub

Logz.io

Logz.io透過Logz.io開放式 360 平台協助雲端原生企業監控環境並保護其環境的安全性，從高成本、低價值的負擔轉變為具有成本效益的高價值、具成本效益的推動者，以取得更好的業務成果。

Logz.ioCloud SIEM 透過快速查詢、多維度偵測和深度可自訂的安全性內容，直接解決當今主要的安全性挑戰，從資料超載到無所不在的網路技能落差，無論資料量如何，都能協助監控和調查全面的雲端環境。

此Logz.io解決方案專為提供進階威脅分析與調查而打造，而且複雜性和成本更低。客戶得到專門的安全分析師、威脅內容即服務和 AI 支援功能的後盾，這些功能旨在協助減少雜訊的資料，並專注於讓您的團隊能夠快速排定真實世界威脅優先順序的資訊。

AWS AppFabric 稽核記錄擷取考量

下列各節說明要搭配使用的輸出結構描述、輸出格式和輸出目的地Logz.io。 AppFabric

結構描述和格式

Logz.io支援下列 AppFabric 輸出結構描述和格式：

- 原始-JSON
  - AppFabric 以 JSON 格式輸出來源應用程式所使用的原始結構描述中的資料。
- 十字-JSON
  - AppFabric 使用開放網路安全架構架構 (OCSF) 將資料標準化，並以 JSON 格式輸出資料。

輸出位置

Logz.io支持以下 AppFabric 輸出位置：

- Amazon 數據 Firehose
  - 若要設定 Firehose 交付串流以便將資料傳送至其中Logz.io，請遵循 Amazon Data Firehose 開發人員指南中「Logz.io為您的目的地選擇目的地」中的說明進行操作。
- Amazon Simple Storage Service (Amazon S3)

- 若Logz.io要設定為從包含稽核日誌的 Amazon S3 儲存貯體接收資料，請遵循Logz.io網站上設定 Amazon S3 儲存貯體中的指示。

Netskope

Netskope身為全球網路安全領導者，正在重新定義雲端、資料和網路安全性，以協助組織採用零信任原則來保護資料。該Netskope平台快速且易於使用，可為人員、設備和數據隨時隨地提供優化的訪問和零信任安全性。 Netskope協助客戶降低風險、加速效能，並在任何雲端、Web 和私有應用程式活動中獲得無與倫比的能見度。成千上萬的客戶，包括超過 25 家財星 100 大企業、信任Netskope及其強大的 NewEdge 網路，可因應不斷變化的威脅、新的風險、技術轉變、組織和網路變更，以及新的法規要求。了解如何Netskope幫助客戶為 SASE 旅程做好準備，請訪問 netskope.com。

AWS AppFabric 稽核記錄擷取考量

下列各節說明要搭配使用的輸出結構描述、輸出格式和輸出目的地Netskope。 AppFabric

結構描述和格式

Netskope支援下列 AppFabric 輸出結構描述和格式：

- 原始-JSON
  - AppFabric 以 JSON 格式輸出來源應用程式所使用的原始結構描述中的資料。
- 十字-JSON
  - AppFabric 使用開放網路安全架構架構 (OCSF) 將資料標準化，並以 JSON 格式輸出資料。

輸出位置

Netskope支持以下 AppFabric 輸出位置：

- Amazon Simple Storage Service (Amazon S3)
  - 若Netskope要設定為從包含稽核日誌的 Amazon S3 儲存貯體接收資料，請按照Netskope網站上 Amazon Web Services S3 的資料保護中的指示進行操作。

NetWitness

NetWitness是擴展檢測和響應（XDR）軟件的領先開發商。他們高度注重安全性的全球客戶基礎仰賴 NetWitness XDR 來抵禦複雜且積極的對手。NetWitnessXDR 擁有業界最完整、整合且最成熟的平台，可偵測、調查和回應數位攻擊，是現代高效 SOC 的統一基礎。

NetWitnessXDR 採用高度模組化的架構，無論發生在雲端、內部部署、行動和遠端工作者，或是介於兩者之間的任何地方，都能偵測威脅。P NetWitness latform XDR 提供完整的能見度，結合應用的威脅情報和使用者行為分析，以偵測威脅、排定活動優先順序、調查及自動回應。所有這些都能讓安全分析師獲得更好、更快的效率，讓安全性作業領先於影響業務的威脅。

AWS AppFabric 稽核記錄擷取考量

下列各節說明要搭配使用的輸出結構描述、輸出格式和輸出目的地NetWitness。 AppFabric

結構描述和格式

NetWitness 支援下列 AppFabric 輸出結構描述和格式：

- 原始-JSON
  - AppFabric 以 JSON 格式輸出來源應用程式所使用的原始結構描述中的資料。
- 十字-JSON
  - AppFabric 使用開放網路安全架構架構 (OCSF) 將資料標準化，並以 JSON 格式輸出資料。

輸出位置

NetWitness支持以下 AppFabric 輸出位置：

- Amazon Simple Storage Service (Amazon S3)
  - 若NetWitness要設定為從包含稽核日誌的 Amazon S3 儲存貯體接收資料，請遵循NetWitness網站NetWitness平台整合頁面上 S3 通用連接器事件來源日誌組態指南中的指示進行操作。

Amazon QuickSight

Amazon 透過超大規模統一商業智慧 (BI) 為資料驅動的組織提 QuickSight 供支援。透過現代化的互動式儀表板 QuickSight、分頁報告、嵌入式分析和自然語言查詢，所有使用者都可以從相同的事實來源滿足各種分析需求。您可以選擇 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體 QuickSight，在儲存貯體中分析 AWS AppFabric 稽核日誌資料，將您 AppFabric 的安全日誌作為來源存放。

AppFabric 稽核記錄擷取考量

以下各節說明與 Amazon 搭配使用的輸出結構描述、輸出格式和輸出目的地 QuickSight。 AppFabric

結構描述和格式

QuickSight 支援下列 AppFabric 輸出結構描述和格式：

- 原始-JSON
  - AppFabric 以 JSON 格式輸出來源應用程式所使用的原始結構描述中的資料。
- 十字-JSON
  - AppFabric 使用開放網路安全架構架構 (OCSF) 將資料標準化，並以 JSON 格式輸出資料。

輸出位置

QuickSight 支持以下 AppFabric 輸出位置：

- Amazon S3
  - 您可以使用 Amazon S3 檔案建立資料集，將 QuickSight 資料直接從 Amazon S3 導入。若要確認您的目標檔案集未超過 QuickSight 資料來源配額，請參閱 Amazon QuickSight 使用者指南中的資料來源配額。
  - 如果您的檔案集超出 Amazon S3 資料來源的 QuickSight 配額，您可以使用 Amazon Athena 和 AWS Glue 表格在 Amazon S3 中擷取資料。在 QuickSight 資料集中使用 Athena 會產生額外費用。如需有關 Athena 定價的詳細資訊，請參閱 Athena 定價頁面。

    若要使用 Athena：

    1. 依照 A thena 使用者指南中的使用連線 AWS Glue 至 Amazon S3 中的資料來源中的指示進行。
    2. 請依照 Amazon 使用者指南中的使用 Athena 資料建立資料集中的 QuickSight 指示進行。

Rapid7

Rapid7, Inc. 的使命是通過使網絡安全更簡單，更易於訪問來創建一個更安全的數字世界。 Rapid7透過 best-in-class 技術、尖端研究和廣泛的策略專業知識，讓安全專業人員能夠管理現代化的攻擊破綻。 Rapid7全方位的安全解決方案可協助 10,000 多名全球客戶統一雲端風險管理和威脅偵測，以快速且精確的方式減少攻擊面並消除威脅。

AWS AppFabric 稽核記錄擷取考量

下列各節說明要搭配使用的輸出結構描述、輸出格式和輸出目的地Rapid7。 AppFabric

結構描述和格式

Rapid7支援下列 AppFabric 輸出結構描述和格式：

- 原始-JSON

  - AppFabric 以 JSON 格式輸出來源應用程式所使用的原始結構描述中的資料。
- 十字-JSON
  - AppFabric 使用開放網路安全架構架構 (OCSF) 將資料標準化，並以 JSON 格式輸出資料。

輸出位置

Rapid7支持以下 AppFabric 輸出位置：

- Amazon Simple Storage Service (Amazon S3)
  - 若要設定 Rapid7 以接收來自包含稽核日誌的 Amazon S3 儲存貯體的資料，請遵循部落格網站上如何使用 InsighTidR 來監控 Amazon S3 活動部落格文章中的指示進行操作。Rapid7

Amazon Security Lake

Amazon Security Lake 會自動將 AWS 環境、軟體即服務 (SaaS) 供應商、內部部署和雲端來源的安全資料集中到儲存在您的專用資料湖中。 AWS 帳戶使用 Security Lake，您可以更全面地了解整個組織中的安全性資料。安全湖採用了開放式網路安全架構架構 (OCSF)，這是一個開放原始碼安全事件結構描述。透過 OCSF 支援，此服務可將來自以及各種企業安全性資料來源的安全性資料標準化 AWS 並結合。

AppFabric 稽核記錄擷取考量

您可以將自訂來源新增至安全湖，將 SaaS 稽核日誌放入您 AWS 帳戶 的 Amazon 安全湖。下列各節說明要搭配 Security Lake 使用的輸出結構描述、輸出格式和輸出目的地。 AppFabric

結構描述和格式

安全湖支援下列 AppFabric 輸出結構描述和格式：

- 十字-JSON
  - AppFabric 使用開放網路安全架構架構 (OCSF) 將資料標準化，並以 JSON 格式輸出資料。

輸出位置

安全湖使用 Amazon 資料 Firehose 交付串流 AppFabric 作為 AppFabric 擷取輸出位置來支援做為自訂來源。若要設定資料 AWS Glue 表和 Firehose 傳遞串流，以及在安全性湖泊中設定自訂來源，請使用下列程序。

創建一個 AWS Glue 表

1. 瀏覽至亞馬遜簡單儲存服務 (Amazon S3)，並使用您選擇的名稱建立儲存貯體。
2. 導覽至主 AWS Glue 控台。
3. 對於「資料目錄」，移至「表格」區段，然後選擇「新增表格」。
4. 為此表格輸入您選擇的名稱。
5. 選取您在步驟 1 中建立的 Amazon S3 儲存貯體。
6. 對於資料格式，請選取 [JSON]，然後選擇 [下一步]。
7. 在 [選擇或定義結構定義] 頁面上，選擇 [編輯結構定義為 JSON]。
8. 輸入下列結構定義，並完成 AWS Glue 表格建立程序。

```
[
    {
        "Name": "activity_id",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "activity_name",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "actor",
        "Type":
 "struct<session:struct<created_time:bigint,uid:string,issuer:string>,user:struct<uid:strin
        "Comment": ""
    },
    {
        "Name": "user",
        "Type":
 "struct<uid:string,email_addr:string,credential_uid:string,name:string,type:string>",
        "Comment": ""
    },
    {
        "Name": "group",
        "Type":
 "struct<uid:string,desc:string,name:string,type:string,privileges:array<string>>",
        "Comment": ""
    },
```

```
    {
        "Name": "privileges",
        "Type": "array<string>",
        "Comment": ""
    },
    {
        "Name": "web_resources",
        "Type":
 "array<struct<type:string,uid:string,name:string,data:struct<current_value:string,previous
    },
    {
        "Name": "http_request",
        "Type": "struct<http_method:string,user_agent:string,url:string>",
        "Comment": ""
    },
    {
        "Name": "auth_protocol",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "auth_protocol_id",
        "Type": "int",
        "Comment": ""
    },
    {
        "Name": "category_name",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "category_uid",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "class_name",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "class_uid",
        "Type": "string",
        "Comment": ""
```

```
    },
    {
        "Name": "is_mfa",
        "Type": "boolean",
        "Comment": ""
    },
    {
        "Name": "raw_data",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "severity",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "severity_id",
        "Type": "int",
        "Comment": ""
    },
    {
        "Name": "status",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "status_detail",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "status_id",
        "Type": "int",
        "Comment": ""
    },
    {
        "Name": "time",
        "Type": "bigint",
        "Comment": ""
    },
    {
        "Name": "type_name",
        "Type": "string",
```

```
        "Comment": ""
    },
    {
        "Name": "type_uid",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "description",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "metadata",
        "Type":
 "struct<product:struct<uid:string,vendor_name:string,name:string>,processed_time:string,ve
    },
    {
        "Name": "device",
        "Type":
 "struct<uid:string,hostname:string,ip:string,name:string,region:string,type:string,os:stru
    },
    {
        "Name": "unmapped",
        "Type": "map<string,string>"
    }
]
```

在安全湖中建立自訂來源

1. 導覽至 Amazon 安全湖主控台。
2. 在導覽窗格中選取 [自訂來源]。
3. 選擇「建立自訂來源」。
4. 輸入自訂來源的名稱，然後選取適用的 OCSF 事件類別。

> **Note**
>
> AppFabric 使用帳戶變更、驗證、使用者存取管理、群組管理、Web 資源活動和 Web 資源存取活動事件類別。

5. 對於 AWS 帳戶 ID 和外部 ID，請輸入您的 AWS 帳戶 ID。然後，選擇 Create (建立)。
6. 儲存自訂來源的 Amazon S3 位置。您將使用它來設置 Amazon 數據 Firehose 交付流。

在 Firehose 中建立交付串流

1. 導覽至 Amazon 資料 Firehose 主控台。
2. 選擇 [建立交付串流]。
3. 對於「來源」，選取「直接放入」
4. 對於目的地，選擇 S3。
5. 在「轉換和轉換記錄」部分中，選擇「啟用記錄格式轉換」，然後選擇Apache Parquet作為輸出格式。
6. 對於AWS Glue 表格，請選擇您在上一個程序中建立的 AWS Glue 表格，然後選擇最新版本。
7. 對於目的地設定，請選擇您使用安全湖自訂來源建立的 Amazon S3 儲存貯體。
8. 對於動態磁碟分割，請選擇啟用。
9. 針對 JSON 的內嵌剖析，請選擇 [啟用]。
   - 對於「金鑰名稱」，輸入`eventDayValue`。
   - 對於 JQ 表示式，請輸入`(.time/1000)|strftime("%Y%m%d")`。
10. 針對 S3 儲存貯體前置詞，輸入下列值。

```
ext/AppFabric/region=<region>/accountId=<account_id>/eventDay=!
{partitionKeyFromQuery:eventDayValue}/
```

    <region><account_id>用您的 *AWS ##* 和 AWS 帳戶 ID 替換。

11. 對於 S3 儲存貯體錯誤輸出前置詞，請輸入下列值。

```
ext/AppFabric/error/
```

12. 對於「重試」持續時間，選取 300。
13. 對於緩衝區大小，請選取 128 MiB。
14. 對於緩衝區間隔，選取 60s。
15. 完成 Firehose 交付串流的建立程序。

建立 AppFabric 擷取

若要將資料傳送至 Amazon Security Lake，您必須在 AppFabric主控台中建立一個擷取，該擷取使用您先前建立的 Firehose 交付串流做為輸出位置。如需有關設定 AppFabric 擷取以使用 Firehose 做為輸出位置的詳細資訊，請參閱建立輸出位置。

Singularity Cloud

該Singularity Cloud平台可在所有階段保護您的企業免受所有類別的威脅。其獲得專利的 AI（人工智能）將安全性從已知的特徵碼和模式擴展到最複雜的攻擊，例如零時差和勒索軟件。

AWS AppFabric 稽核記錄擷取考量

下列各節說明要搭配使用的輸出結構描述、輸出格式和輸出目的地Singularity Cloud。 AppFabric

結構描述和格式

Singularity Cloud支援下列 AppFabric 輸出結構描述和格式：

OCSF-JSON： AppFabric 使用開放網路安全架構架構 (OCSF) 將資料標準化，並以 JSON 格式輸出資料。

輸出位置

Singularity Cloud支援從以下 AppFabric 輸出位置接收稽核記錄。

- Amazon Simple Storage Service (Amazon S3)
  - 若Singularity Cloud要設定為從包含稽核日誌的 Amazon S3 儲存貯體接收資料，請遵循Singularity Cloud’s文件中的指示。

Splunk

Splunk有助於使組織更具彈性。領先的組織使用統一Splunk的安全性和可觀察性平台來確保其數位系統的安全性和可靠性。Organizations 信任能Splunk夠防止安全性、基礎架構和應用程式問題成為重大事件、吸收數位中斷的衝擊，並加速數位轉型。

AWS AppFabric 稽核記錄擷取考量

下列各節說明要搭配使用的輸出結構描述、輸出格式和輸出目的地Splunk。 AppFabric

結構描述和格式

Splunk 支援下列 AppFabric 輸出結構描述和格式：

- 原始-JSON
  - AppFabric 以 JSON 格式輸出來源應用程式所使用的原始結構描述中的資料。
- 十字-JSON
  - AppFabric 使用開放網路安全架構架構 (OCSF) 將資料標準化，並以 JSON 格式輸出資料。
- OCSF-Parquet
  - AppFabric 使用開放網路安全架構架構 (OCSF) 將資料標準化，並以格式輸出資料。Apache Parquet

輸出位置

Splunk支持以下 AppFabric 輸出位置：

- Amazon 數據 Firehose
  - 若Splunk要設定為從包含稽核日誌的 Firehose 串流接收稽核日誌，請按照網站上 Amazon Data Firehose Splunk 附加元件中的指示進行操作。Splunk
- Amazon Simple Storage Service (Amazon S3)
  - 若Splunk要設定為從包含稽核日誌的 Amazon S3 儲存貯體接收資料，請遵循為Splunk網站 AWS 上的Splunk附加元件設定以 SQL 為基礎的 S3 輸入中的指示進行操作。

刪除 AWS AppFabric 安全性資源

如果您不想繼續使用基 AWS AppFabric 於安全性考量，請務必刪除您在安裝期間建立的輸出位置中的資料，以及安全性資源 AppFabric 的資料，以避免產生額外費用。若要清理 AppFabric 資源，您必須依照為每個軟體即服務 (SaaS) 應用程式建立資源的相反順序刪除資源：[擷取目的地] > [擷取] > [應用程式授權] > [應用程式套件]

刪除最終應用程式授權後，您可以刪除應用程式套件。

主題

- 刪除擷取目的地
- 刪除擷取
- 刪除應用程式授權
- 刪除應用程式套件

刪除擷取目的地

如果您在建立擷取時選取輸出位置， AppFabric 為了安全起見，會代表您建立擷取目的地。若要刪除擷取目的地，請遵循下列步驟：

1. 開啟主 AppFabric 控台，網址為 https://console.aws.amazon.com/appfabric/。
2. 在 [開始使用] 頁面中，展開左側的選單。
3. 選擇嵌入。
4. 選擇應用程式授權。
5. 選取您要刪除的目的地旁邊的選項按鈕，然後選擇「刪除」。
6. 在「刪除目的地」對話方塊中選擇「刪除」以確認。
7. 對所有目的地重複上述步驟。

刪除擷取

若要刪除擷取，請遵循下列步驟：

1. 在 [開始使用] 頁面中，展開左側的選單。
2. 選擇嵌入。
3. 選取應用程式授權旁邊的選項按鈕。
4. 選擇動作下拉式選單。
5. 選擇刪除。
6. 在 [刪除擷取] 對話方塊中選擇 [刪除] 以確認。

刪除應用程式授權

若要刪除應用程式授權，請遵循下列步驟：

1. 在 [開始使用] 頁面中，展開左側的選單。
2. 選擇 [應用程式授權]。
3. 選取您要刪除的應用程式授權旁邊的選項按鈕。
4. 選擇動作下拉式選單。
5. 選擇刪除。
6. 在 [刪除擷取] 對話方塊中選擇 [刪除] 以確認。

刪除應用程式套件

若要刪除您的應用程式套件，請執行下列步驟：

1. 在 [開始使用] 頁面中，展開左側的選單。
2. 選擇應用程序包。
3. 選擇 Delete (刪除) 按鈕。
4. 輸入`delete`以確認，然後選擇 [刪除]。

什麼是 AWS AppFabric 生產力？

提高 AWS AppFabric 生產力功能為預覽狀態，可能會有所變更。

> **Note**
>
> 由 Amazon 基岩提供支援： AWS 實作自動濫用偵測。由 AWS AppFabric 於生產力是建立在 Amazon 基岩之上，因此使用者會繼承 Amazon Bedrock 中實作的控制項，以強制執行人工智慧的安全性、安全性和負責任的使用。

AWS AppFabric 提高生產力 (預覽) 可從多個應用程式產生洞察與動作，藉此重新構想第三方應用程式中的使用者生產力。應用程式開發人員認識到，從其他應用程式存取使用者資料對於建立更具生產力的應用程式體驗很重要，但他們不想建立和管理與每個應用程式的整合。 AppFabric 為了提高生產力，應用程式開發人員可以存取生成 AI 技術的 API，以產生跨應用程式資料見解和動作，以便透過全新或現有的生成式 AI 助理，提供更豐富的使用者體驗。 AppFabric in 生產力整合來自多個應用程式的資料，讓開發人員無需建立或維護 point-to-point 整合。應用程式開發人員可以將生產力直接嵌入 AppFabric 其應用程式的 UI 中，為使用者維持一致的體驗，同時從其他應用程式呈現相關內容。

AppFabric 提高生產力可連接來自常用應用程式的資料 Asana Atlassian Jira SuiteGoogle Workspace，例如Microsoft 365Miro、、Slack、Smartsheet、、、等等。 AppFabric 為了提高生產力，應用程式開發人員可以更輕鬆地打造更個人化的應用程式體驗，進而提升使用者採用率、滿意 同時，終端使用者可以從各個應用程式中存取所需的見解，而不會中斷工作流程。

主題

- 優勢

- 使用案例
- 存取 AppFabric 生產力
- 適用於應用程式開發人員 AppFabric 的生產力 (預覽) 入門
- 開始使用者 AppFabric 的生產力 (預覽版)
- AppFabric 生產力 API
- 資料處理

優勢

AppFabric 為了提高生產力，應用程式開發人員可以存取可產生跨應用程式資料見解和動作的 API，以便透過全新或現有的生成式 AI 助理，提供更豐富的使用者體驗。

- 跨應用程式使用者資料的單一來源：生產力整 AppFabric 合來自多個應用程式的資料，讓開發人員無須建立或維護 point-to-point 整合。SaaS 應用程式資料會自動將不同的資料類型標準化為任何應用程式都可以理解的格式，進而在其他應用程式中使用，讓應用程式開發人員納入更多資料，進而實際提高使用者的生產力。
- 完全控制使用者體驗：開發人員可以將生產力直接嵌入其應用程式的 UI 中，保留 AppFabric 對使用者體驗的完全控制，同時為使用者提供個人化的見解和建議動作，並從各個應用程式中取得情境。這樣可以在使 AppFabric 用者偏好的 SaaS 應用程式中提供生產力，並可在他們偏好完成工作的應用程式中存取。最終用戶花費更少的時間在應用程序之間切換，並且可以保持工作流程。
- 加速上市時間：在單一 API 呼叫中，應用程式開發人員可以透過產生的使用者資料獲得使用者層級的見解，而無需微調模型、撰寫自訂提示或跨多個應用程式建立整合。 AppFabric 抽象化這種複雜性，讓應用程式開發人員能夠更快地建置、嵌入或豐富生成式 AI 功能。這使應用程序開發人員可以將重點放在最重要的任務上的資源。
- 建立使用者信任的成 Artifact 參考：作為輸出的一部分， AppFabric 為了提高生產力，會顯示相關的成品或來源檔案，用於產生深入解析，以建立最終使用者對 LLM 輸出的信任。
- 簡化的使用者權限：用於產生見解的使用者成品是根據使用者有權存取的內容而定。 AppFabric 為了提高生產力，使用 ISV 的許可和訪問控制作為事實的源泉。

使用案例

應用程式開發人員可利 AppFabric 用生產力來重新構想應用程式內部的生產力 AppFabric 為了提高生產力，提供了兩個專注於以下使用案例的 API，以幫助其最終使用者提高生產力：

- 優先您的一天

- 可操作的洞察 API 通過顯示來自各個應用程序（包括電子郵件，日曆，消息，任務等）的及時見解，幫助用戶最好地管理他們的一天。此外，使用者可以執行跨應用程式動作，例如從偏好的應用程式建立電子郵件、排程會議和建立行動項目。例如，在一夜之間進行客戶升級的員工不僅會看到隔夜對話的摘要，還可以看到建議的動作來排定與客戶帳戶經理的會議。動作會預先填入必要欄位(例如工作名稱和擁有者，或電子郵件傳送者/收件者)，並可在執行動作之前編輯預先填入的內容。
- 準備即將到來的會議
  - 會議準備 API 通過總結會議目的並顯示相關的跨應用程序成品（例如電子郵件，消息等）來幫助用戶最好地為會議做準備。使用者現在可以快速準備會議，不必浪費時間在應用程式之間切換來尋找內容。

存取 AppFabric 生產力

AppFabric 提高生產力目前以預覽版的形式推出，並於美國東部 (維吉尼亞北部) 提供 AWS 區域。如需相關資AWS AppFabric 訊 AWS 區域，請參閱 AWS 一般參考.

在每個區域中，您可以通 AppFabric 過以下任何一種方式訪問生產力：

- 作為應用程式開發者
  - 適用於應用程式開發人員 AppFabric 的生產力 (預覽) 入門
- 作為一般使用者
  - 開始使用者 AppFabric 的生產力 (預覽版)

適用於應用程式開發人員 AppFabric 的生產力 (預覽) 入門

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

本節可協助應用程式開發人員將生產力 (預覽) 整合 AWS AppFabric 至其應用程式中。 AWS AppFabric 提高生產力，開發人員能夠透過電子郵件、行事曆事件、工作、訊息等產生 AI 技術的見解和動作，從而為其使用者建立更豐富的應用程式體驗。如需支援的應用程式清單，請參閱AWS AppFabric 支援的應用程式。

AppFabric 為了提高生產力，應用程序開發人員可以在安全受控的環境中進行構建和實驗。當您第一次開始使用以 AppFabric 提高生產力時，您可以建立 AppClient 並註冊單一測試使用者。此方法旨在幫助您了解和測試應用程序和. 之間的身份驗證和通信流程 AppFabric。在您與單一使用者進行測試之後，

您可以將應用程式提交至 AppFabric 以進行驗證，然後再將存取權擴展至其他使用者 (請參閱步驟 5. 請求 AppFabric 驗證您的申請)。 AppFabric 將驗證應用程式資訊，然後再進行廣泛採用，以協助保護應用程式開發人員、使用者及其資料，為以負責任的方式擴大使用者採用鋪平道路。

主題

必要條件

在開始之前，您需要創建一個 AWS 帳戶. 如需詳細資訊，請參閱 註冊一個 AWS 帳戶。您還需要建立至少一個可存取下列 "appfabric:CreateAppClient" IAM 政策的使用者，以便使用者向其註冊您的應用程式 AppFabric。如需授與生產力功能之權限的 AppFabric 詳細資訊，請參閱AppFabric 以取得生產力 IAM 政策範例。雖然擁有系統管理使用者是有益的，但對於初始設定來說並不是強制性的。如需詳細資訊，請參閱 建立具有管理權限的使用者。

AppFabric 生產力僅在美國東部 (維吉尼亞北部) 預覽期間。在開始執行以下步驟之前，請確定您位於此區域。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

步驟 1. 創造一個提高 AppFabric 生產力 AppClient

您必須先建立一個 AppFabric AppClient. AppFabric 基本上 AppClient 是您通往提高生產力 AppFabric 的閘道，可作為安全的 OAuth 應用程式用戶端，在應用程式與 AppFabric. 當您創建一個 ID 時 AppClient，系統會為您提供一個 AppClient ID，這是一個唯一的標識符，這對於確保 AppFabric 知道它正在使用您的應用程序和 AWS 帳戶.

AppFabric 為了提高生產力，應用程序開發人員可以在安全受控的環境中進行構建和實驗。當您第一次開始使用以 AppFabric 提高生產力時，您可以建立 AppClient並註冊單一測試使用者。此方法旨在幫助您了解和測試應用程序和. 之間的身份驗證和通信流程 AppFabric。在您與單一使用者進行測試之後，您可以將應用程式提交至 AppFabric 以進行驗證，然後再將存取權擴展至其他使用者 (請參閱步驟 5. 請求 AppFabric 驗證您的申請)。 AppFabric 將驗證應用程式資訊，然後再進行廣泛採用，以協助保護應用程式開發人員、使用者及其資料，為以負責任的方式擴大使用者採用鋪平道路。

若要建立 AppClient，請使用 AWS AppFabric `CreateAppClient` API 作業。如果您需要更新之 AppClient 後，您可以使用 `UpdateAppClient` API 操作僅更改重定向圖表。如果您需要變更與您相關聯的任何其他參數， AppClient 例如 AppName 或說明，您必須刪除 AppClient 並建立新的參數。如需詳細資訊，請參閱 CreateAppClient。

您可以使用多種編程語言，包括 Python，Node.js，Java，C# ，圍棋和銹病毒，使用 `CreateAppClient` API 註冊您的應用程序。 AWS 如需詳細資訊，請參閱 IAM 使用者指南中的要求簽名範例。您需要使用帳戶簽名版本 4 憑據才能執行此 API 操作。如需簽名版本 4 的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

請求欄位

- `appName`-將在使用 AppFabric 者入口網站的同意頁面上顯示給使用者的應用程式名稱。同意頁面會詢問使用者是否有權在應用程式內顯示 AppFabric 見解。如需有關同意頁面的詳細資訊，請參閱步驟 2. 同意應用程式顯示見解。
- `description`-應用程序的說明。
- `redirectUrls`-授權後將使用者重新導向至的 URI。您最多可以新增 5 個重新導向。例如 `https://localhost:8080`。
- `starterUserEmails`-一個用戶電子郵件地址，允許訪問以接收見解，直到應用程序通過驗證。只允許使用一個電子郵件地址。例如：`anyuser@example.com`
- `customerManagedKeyIdentifier`(選擇性)-用於加密資料的客戶管理金鑰 (由 KMS 產生) 的 ARN。如果未指定，則將使用 AWS AppFabric 託管密鑰。如需有關 AWS 擁有的金鑰 和客戶管理金鑰的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的客戶 AWS 金鑰和金鑰。

響應字段

- `appClientArn`-包含 AppClient ID 的 Amazon 資源名稱 (ARN)。例如， AppClient 識別碼為`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`。
- `verificationStatus`- AppClient 驗證狀態。
  - `pending_verification`-的驗證 AppClient仍在進行中 AppFabric。在驗證之 AppClient 前，只有一個使用者 (在中指定`starterUserEmails`) 可以使用 AppClient. 使用者將在中介紹的 AppFabric 使用者入口網站中看到通知步驟 3。新增 AppFabric 使用者入口網站 URL 至您的應用程式，表示應用程式未經過驗證。
  - `verified`-驗證程序已由順利完成 AppFabric ，現 AppClient 已完成驗證。
  - `rejected`-的驗證程序已 AppClient 遭拒絕 AppFabric。 AppClient 在重新啟動並成功完成驗證程序之前，其他使用者無法使用。

```
curl --request POST \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients/ \
  --data '{
    "appName": "Test App",
    "description": "This is a test app",
    "redirectUrls": ["https://localhost:8080"],
    "starterUserEmails": ["anyuser@example.com"],
    "customerManagedKeyIdentifier": "arn:aws:kms:<region>:<account>:key/<key>"
}'
```

如果動作成功，則服務傳回 HTTP 200 回應。

```
{
    "appClientConfigSummary": {
        "appClientArn": "arn:aws:appfabric:<region>:<account>:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "verificationStatus": "pending_verification"
    }
}
```

步驟 2. 驗證並授權您的應用程式

透過建立 OAuth 2.0 授權流程，讓您的應用程式能夠安全地整合 AppFabric 見解。首先，您需要創建一個驗證您的應用程序身份的授權碼。如需詳細資訊，請參閱 授權。然後，您將交換此授權代碼為訪問令牌，該訪問令牌授予應用程序在應用程序中獲取和顯示 AppFabric見解的權限。如需詳細資訊，請參閱 權杖。

如需授與應用程式授權權限的詳細資訊，請參閱允許存取授權應用程式。

1. 若要建立授權碼，請使用 AWS AppFabric `oauth2/authorize` API 作業。

   請求欄位

   - `app_client_id`(必要)-在步驟 1 中 AWS 帳戶 建立之 AppClient ID。創建一個 AppClient. 例如 `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`。
   - `redirect_uri`(必要)-在您在步驟 1 中使用的授權後，將使用者重新導向至的 URI。創建一個 AppClient. 例如 `https://localhost:8080`。
   - `state`（必要）-用於維護請求和回調之間狀態的唯一值。例如 `a8904edc-890c-1005-1996-29a757272a44`。

   ```
   GET https://productivity.appfabric.<region>.amazonaws.com/oauth2/authorize?
   app_client_id=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111\
   redirect_uri=https://localhost:8080&state=a8904edc-890c-1005-1996-29a757272a44
   ```

2. 驗證後，您將被重定向到指定的 URI，並使用作為查詢參數返回的授權碼。例如，在哪裡`code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc`。

   ```
   https://localhost:8080/?code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-
   sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-
   oampc&state=a8904edc-890c-1005-1996-29a757272a44
   ```

3. 使用 AppFabric `oauth2/token` API 操作將此授權碼交換為訪問令牌。

   此令牌用於 API 請求，並且最初在驗證`starterUserEmails`之 AppClient 前有效。驗證 AppClient 之後，此權杖可用於任何使用者。您需要使用帳戶簽名版本 4 憑據才能執行此 API 操作。如需簽名版本 4 的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

請求欄位

- code（必填）-您在最後一個步驟驗證後收到的授權碼。例如 mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc。
- app_client_id(必要)-在步驟 1 中 AWS 帳戶 建立之 AppClient ID。創建一個 AppClient. 例如 a1b2c3d4-5678-90ab-cdef-EXAMPLE11111。
- grant_type(必要)-值必須是authorization_code。
- redirect_uri(必要)-在您在步驟 1 中使用的授權後，將使用者重新導向至的 URI。創建一個 AppClient. 這必須與用於創建授權代碼的重定向 URI 相同。例如 https://localhost:8080。

響應字段

- expires_in-令牌到期前多久。預設到期時間為 12 小時。
- refresh_token-從初始 /token 要求接收到的重新整理權杖。
- token-從初始 /token 要求接收到的權杖。
- token_type-該值將是Bearer。
- appfabric_user_id- AppFabric 使用者識別碼。這只會針對使用authorization_code授權類型的要求傳回。

```
curl --location \
"https://appfabric.<region>.amazonaws.com/oauth2/token" \
--header "Content-Type: application/json" \
--header "X-Amz-Content-Sha256: <sha256_payload>" \
--header "X-Amz-Security-Token: <security_token>" \
--header "X-Amz-Date: 20230922T172215Z" \
--header "Authorization: AWS4-HMAC-SHA256 ..." \
--data "{
    \"code\": \"mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-
gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc",
    \"app_client_id\": \"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111\",
    \"grant_type\": \"authorization_code\",
    \"redirect_uri\": \"https://localhost:8080\"
}"
```

如果動作成功，則服務傳回 HTTP 200 回應。

```
{
    "expires_in": 43200,
    "refresh_token": "apkaeibaerjr2example",
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "<userId>"
}
```

步驟 3。新增 AppFabric 使用者入口網站 URL 至您的應用程式

使用者需要授權 AppFabric 才能從用來產生深入解析的應用程式存取資料。 AppFabric 透過建立專用的使用者入口網站 (快顯畫面)，讓最終使用者授權其應用程式，消除應用程式開發人員擁有此程序的複雜性。當使用者準備好啟 AppFabric 用生產力時，他們會被帶到使用者入口網站，讓他們能夠連接和管理用來產生深入解析和跨應用程式動作的應用程式。登入後，使用者可以將應用程式連線到以 AppFabric 提高生產力，然後返回您的應用程式以探索深入解析和動作。若要整合您的應 AppFabric 用程式以提高生產力，您需要在應用程式中新增特定的 AppFabric URL。此步驟對於讓使用者能夠直接從您的應用程式存取 AppFabric 使用者入口網站至關重要。

1. 導航到應用程序的設置，然後找到添加重定向 URL 的部分。
2. 找到適當的區域後，將下列 AppFabric URL 新增為應用程式的重新導向 URL：

```
https://userportal.appfabric.<region>.amazonaws.com/eup_login
```

新增 URL 之後，您的應用程式將設定為將使用者導向至使用 AppFabric者入口網站。在這裡，用戶可以登錄並連接和管理用於生成生產力洞察 AppFabric 的應用程序。

步驟 4. 用 AppFabric 於顯示跨應用程式深入解析和動作

使用者連接其應用程式之後，您可以透過協助減少應用程式和內容切換，提高使用者的生產力。 AppFabric 只會根據使用者有權存取的內容，為使用者產生深入分析資訊。 AppFabric 將使用者資料儲存在 AWS 帳戶 所擁有的 AppFabric。如需有關如何 AppFabric 使用資料的資訊，請參閱資料處理。

您可以使用下列 AI 技術的 API，在應用程式中產生並顯示使用者層級的見解和動作：

- `ListActionableInsights`— 有關更多信息，請參閱下面的可操作見解部分。

- ListMeetingInsights— 如需詳細資訊，請參閱本指南稍後的「會議準備」一節。

可行的見解 (**ListActionableInsights**)

該 ListActionableInsights API 可幫助用戶根據其應用程序中的活動（包括電子郵件，日曆，消息，任務等）最好地管理他們的一天，提供可操作的見解。傳回的見解也會顯示用來產生深入解析之成品的內嵌連結，協助使用者快速檢視用來產生深入解析的資料。此外，API 可能會根據見解傳回建議的動作，並允許使用者從您的應用程式內執行跨應用程式動作。具體而言，API 與平台（例如 Asana，Google Workspace，）集成Microsoft 365，並使用戶能Smartsheet夠發送電子郵件，創建日曆事件和創建任務。大型語言模型 (LLM) 可能會在建議的動作 (例如電子郵件內文或任務名稱) 中預先填入詳細資料，使用者可以在執行前自訂這些動作，從而簡化決策並提高生產力。與終端使用者授權應用程式的體驗類似， AppFabric 使用相同的專用入口網站供使用者檢視、編輯和執行跨應用程式動作。若要執行動作， AppFabric 需要 ISV 將使用者重新導向至使用 AppFabric 者入口網站，讓使用者可以在其中查看動作詳細資訊並執行它們。由產生的每個動作都 AppFabric 有唯一的 URL。此 URL 可用於 ListActionableInsights API 回應的回應中。

以下是支援的跨應用程式動作及其應用程式的摘要：

- 傳送電子郵件 (Google Workspace,Microsoft 365)
- 建立行事曆事件 (Google Workspace,Microsoft 365)
- 建立工作 (Asana,Smartsheet)

請求欄位

- nextToken（可選）-用於獲取下一組見解的分頁令牌。
- includeActionExecutionStatus-接受動作執行狀態清單的篩選器。動作會根據傳入的狀態值進行篩選。可能的值：NOT_EXECUTED | EXECUTED

請求標頭

- 授權標頭需要與Bearer Token 值一起傳遞。

響應字段

- insightId-生成的見解的唯一 ID。
- insightContent-這會傳回見解的摘要，以及用來產生深入解析之成品的內嵌連結。注意：這將是一個包含嵌入鏈接（<a>標籤）的 HTML 內容。

- insightTitle-生成的見解的標題。
- createdAt-產生洞察力的時候
- actions-針對生成的見解建議的操作列表。動作對象：
  - actionId-所產生動作的唯一 ID。
  - actionIconUrl-建議執行動作的應用程序的圖標 URL。
  - actionTitle-產生動作的標題。
  - actionUrl-最終使用者在使用者入口網站中檢視和執行動作 AppFabric的唯一 URL。注意：若要執行動作，ISV 應用程式會使用此 URL 將使用 AppFabric 者重新導向至使用者入口網站 (快顯畫面)。
  - actionExecutionStatus-指示動作狀態的列舉。可能的值為：EXECUTED| NOT_EXECUTED
- nextToken（可選）-用於獲取下一組見解的分頁令牌。這是一個可選字段，如果返回 null 意味著沒有更多的見解加載。

如需詳細資訊，請參閱 ActionableInsights。

```
curl -v --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/actionableInsights" \
  --header "Authorization: Bearer <token>"
```

如果動作成功，則服務傳回 HTTP 200 回應。

```
200 OK

{
    "insights": [
        {
            "insightId": "7tff3412-33b4-479a-8812-30EXAMPLE1111",
            "insightContent": "You received an email from James
            regarding providing feedback
            for upcoming performance reviews.",
            "insightTitle": "New feedback request",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "actions": [
                {
                    "actionId": "5b4f3412-33b4-479a-8812-3EXAMPLE2222",
                    "actionIconUrl": "https://d3gdwnnn63ow7w.cloudfront.net/
eup/123.svg",
```

```
                    "actionTitle": "Send feedback request email",
                    "actionUrl": "https://userportal.appfabric.us-east-1.amazonaws.com/
action/action_id_1"
                    "actionExecutionStatus": "NOT_EXECUTED"
                }
            ]
        },
        {
            "insightId": "2dff3412-33b4-479a-8812-30bEXAMPLE3333",
            "insightContent":"Steve sent you an email asking for details on project.
 Consider replying to the email.",
            "insightTitle": "New team launch discussion",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "actions": [
                {
                    "actionId": "74251e31-5962-49d2-9ca3-1EXAMPLE1111",
                    "actionIconUrl": "https://d3gdwnnn63ow7w.cloudfront.net/
eup/123.svg",
                    "actionTitle": "Reply to team launch email",
                    "actionUrl": "https://userportal.appfabric.us-east-1.amazonaws.com/
action/action_id_2"
                    "actionExecutionStatus": "NOT_EXECUTED"
                }
            ]
        }
    ],
    "nextToken": null
}
```

會議準備 (**ListMeetingInsights**)

該 ListMeetingInsights API 通過總結會議目的並顯示相關的跨應用程序成品（例如電子郵件，消息等）來幫助用戶最好地為即將舉行的會議做準備。使用者現在可以快速準備會議，不必浪費時間在應用程式之間切換來尋找內容。

請求欄位

- nextToken（可選）-用於獲取下一組見解的分頁令牌。

請求標頭

- 授權標頭需要與Bearer Token值一起傳遞。

響應字段

- insightId-生成的見解的唯一 ID。
- insightContent-以字符串格式突出顯示詳細信息的見解描述。與在一樣，為什麼這種見解很重要。
- insightTitle-生成的見解的標題。
- createdAt-產生洞察力的時候
- calendarEvent-使用者應關注的重要行事曆事件或會議。日曆事件對象：
  - startTime-活動的開始時間。
  - endTime-活動的結束時間。
  - eventUrl-ISV 應用程式上行事曆事件的 URL。
- resources-包含與生成見解相關的其他資源的列表。資源物件：
  - appName-資源所屬的應用程式名稱。
  - resourceTitle-資源標題。
  - resourceType-資源的類型。可能的值為：EMAIL| EVENT | MESSAGE | TASK
  - resourceUrl-應用程序中的資源 URL。
  - appIconUrl-資源所屬應用程序的圖像 URL。
- nextToken（可選）-用於獲取下一組見解的分頁令牌。這是一個可選字段，如果返回 null 意味著沒有更多的見解加載。

如需詳細資訊，請參閱 MeetingInsights。

```
curl --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/meetingContexts" \
  --header "Authorization: Bearer <token>"
```

如果動作成功，則服務傳回 HTTP 201 回應。

```
200 OK

{
    "insights": [
        {
            "insightId": "74251e31-5962-49d2-9ca3-15EXAMPLE4444"
```

```
            "insightContent": "Project demo meeting coming up soon. Prepare
accordingly",
            "insightTitle": "Demo meeting next week",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "calendarEvent": {
                    "startTime": {
                        "timeInUTC": 2023-10-08T10:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "endTime": {
                        "timeInUTC": 2023-10-08T11:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "eventUrl": "http://someapp.com/events/1234",
            }
            "resources": [
                {
                    "appName": "SOME_EMAIL_APP",
                    "resourceTitle": "Email for project demo",
                    "resourceType": "EMAIL",
                    "resourceUrl": "http://someapp.com/emails/1234",
                    "appIconUrl":"https://d3gdwnnn63ow7w.cloudfront.net/eup/123.svg"
                }
            ]
        },
        {
            "insightId": "98751e31-5962-49d2-9ca3-15EXAMPLE5555"
            "insightContent": "Important code complete task is now due. Consider
updating the status.",
            "insightTitle": "Code complete task is due",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "calendarEvent":{
                    "startTime": {
                        "timeInUTC": 2023-10-08T10:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "endTime": {
                        "timeInUTC": 2023-10-08T11:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "eventUrl": "http://someapp.com/events/1234",
            },
            "resources": [
                {
```

```
                    "appName": "SOME_TASK_APPLICATION",
                    "resourceTitle": "Code Complete task is due",
                    "resourceType": "TASK",
                    "resourceUrl": "http://someapp.com/task/1234",
                    "appIconUrl": "https://d3gdwnnn63ow7w.cloudfront.net/eup/123.svg"
                }
            ]
        }
    ],
    "nextToken": null
}
```

針對您的見解或行動提供意見反應

使用 AppFabric PutFeedback API 操作為所產生的見解和動作提供意見反應。您可以在應用程式中內嵌此功能，以便提交給定 InsightId 或的意見反應評分 (1 到 5，其中評分越高越好) ActionId。

請求欄位

- id-正在提交意見反應之物件的識別碼。這可以是 InsightId 或 ActionId.
- feedbackFor-正在提交意見反應的資源類型。可能的值：ACTIONABLE_INSIGHT | MEETING_INSIGHT | ACTION
- feedbackRating-信用評級從1到5。評分越高越好。

響應字段

- 沒有響應字段。

如需詳細資訊，請參閱 PutFeedback。

```
curl --request POST \
  --url "https://productivity.appfabric.<region>.amazonaws.com"\
"/feedback" \
  --header "Authorization: Bearer <token>" \
  --header "Content-Type: application/json" \
  --data '{
    "id": "1234-5678-9012",
    "feedbackFor": "ACTIONABLE_INSIGHT"
    "feedbackRating": 3
}'
```

如果動作成功，則服務會傳回具有空 HTTP 內文的 HTTP 201 回應。

步驟 5. 請求 AppFabric 驗證您的申請

為此，您已更新應用程式 UI，以嵌入 AppFabric 跨應用程式深入解析和動作，並為單一使用者獲得深入解析。當您對測試感到滿意並希望將 AppFabric豐富的體驗擴展到其他用戶之後，您可以將申請提交到以進 AppFabric 行審查和驗證。 AppFabric 將驗證應用程式資訊，然後再進行廣泛採用，以協助保護應用程式開發人員、使用者及其資料，為以負責任的方式擴大使用者採用鋪平道路。

啟動驗證程序

傳送電子郵件至 appfabric-appverification@amazon.com 並要求驗證您的應用程式，以開始驗證程序。

在您的電子郵件中包含以下詳細信息：

- 您的 AWS 帳戶 身份證
- 您要尋求驗證的應用程式名稱
- 您的 AppClient 身份證
- 您的聯絡資訊

此外，請提供以下資訊 (如果有的話)，以協助我們評估優先順序和影響：

- 您計劃授予存取權限的估計使用者人數
- 您的目標推出日期

> **Note**
>
> 如果您有 AWS 帳戶 經理或 AWS 合作夥伴開發經理，請將他們複製到您的電子郵件中。包括這些聯繫人可以幫助加快驗證過程。

驗證標準

開始驗證程序之前，您必須符合下列條件：

- 您必須使用有效 AWS 帳戶 的生 AppFabric 產力

此外，您至少符合下列其中一項條件：

- 您的組織是至少 AWS Partner Network 具有「AWS 選取」層級的 AWS 合作夥伴。如需詳細資訊，請參閱AWS 合作夥伴服務層級。
- 您的組織應該在過去三年內至少花費 10,000 美元在 AppFabric 服務上。
- 您的應用程式應列在 AWS Marketplace. 如需詳細資訊，請參閱 AWS Marketplace。

等待驗證狀態更新

審核您的申請後，我們會透過電子郵件回覆，您的狀態 AppClient 會從變更`pending_verification`為`verified`。如果您的申請被拒絕，您將需要重新啟動驗證程序。

管理提升 AppFabric 生產力 AppClients

提高 AWS AppFabric 生產力功能為預覽狀態，可能會有所變更。

您可以管理您 AppFabric 的生產力， AppClients 以確保身份驗證和授權過程的順利運行和維護。

獲取的詳細信息 AppClient

使用 AppFabric `GetAppClient` API 操作可查看有關您的詳細信息 AppClient，包括檢查 AppClient 狀態。如需詳細資訊，請參閱 GetAppClient。

若要取得的詳細資訊 AppClient，您至少必須擁有 `"appfabric:GetAppClient"` IAM 政策許可。如需詳細資訊，請參閱 允許存取以取得詳細資料 AppClients。

請求欄位

- `appClientId`-身 AppClient 份證

響應字段

- `appName`-將在使用 AppFabric 者入口網站的同意頁面上顯示給使用者的應用程式名稱。
- `customerManagedKeyIdentifier`(選擇性)-用於加密資料的客戶受管金鑰 (由 KMS 產生) 的 ARN。如果未指定，則將使用 AWS AppFabric 託管密鑰。
- `description`-應用程序的說明。

- `redirectUrls`-授權後將使用者重新導向至的 URI。您最多可以新增 5 個重新導向。例如 `https://localhost:8080`。
- `starterUserEmails`-一個用戶電子郵件地址，允許訪問以接收見解，直到應用程序通過驗證。只允許使用一個電子郵件地址。例如 `anyuser@example.com`。
- `verificationStatus`- AppClient 驗證狀態。
  - `pending_verification`-的驗證 AppClient仍在進行中 AppFabric。在驗證之 AppClient 前，只有一個使用者 (在中指定`starterUserEmails`) 可以使用 AppClient.
  - `verified`-驗證程序已由順利完成 AppFabric ，現 AppClient 已完成驗證。
  - `rejected`-的驗證程序已 AppClient 遭拒絕 AppFabric。 AppClient 在重新啟動並成功完成驗證程序之前，其他使用者無法使用。

```
curl --request GET \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

如果動作成功，則服務傳回 HTTP 200 回應。

```
200 OK

{
    "appClient": {
        "appName": "Test App",
        "arn": "arn:aws:appfabric:<region>:111122223333:appclient/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "customerManagedKeyArn": "arn:aws:kms:<region>:111122223333:key/<key>",
        "description": "This is a test app",
        "redirectUrls": [
            "https://localhost:8080"
        ],
        "starterUserEmails": [
            "anyuser@example.com"
        ],
        "verificationDetails": {
            "verificationStatus": "pending_verification"
```

```
        }
    }
}
```

清單 AppClients

使用 AppFabric `ListAppClients` API 作業檢視您的 AppClients. AppFabric 每個只允許一 AppClient 個 AWS 帳戶。這可能會在 future 發生變化。如需詳細資訊，請參閱 ListAppClients。

若要列出 AppClients，您至少必須擁有 `"appfabric:ListAppClients"` IAM 政策許可。如需詳細資訊，請參閱 允許存取清單 AppClients。

請求欄位

- 沒有必填欄位。

響應字段

- `appClientARN`-包含 AppClient ID 的 Amazon 資源名稱 (ARN)。例如， AppClient 識別碼為`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`。
- `verificationStatus`- AppClient 驗證狀態。
  - `pending_verification`-的驗證 AppClient仍在進行中 AppFabric。在驗證之 AppClient 前，只有一個使用者 (在中指定`starterUserEmails`) 可以使用 AppClient.
  - `verified`-驗證程序已由順利完成 AppFabric ，現 AppClient 已完成驗證。
  - `rejected`-的驗證程序已 AppClient 遭拒絕 AppFabric。 AppClient 在重新啟動並成功完成驗證程序之前，其他使用者無法使用。

```
curl --request GET \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients
```

如果動作成功，則服務傳回 HTTP 200 回應。

```
200 OK
```

```
{
    "appClientList": [
        {
            "appClientArn": "arn:aws:appfabric:<region>:111122223333:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "verificationStatus": "pending_verification"
        }
    ]
}
```

更新一個 AppClient

使用 AppFabric UpdateAppClient API 作業更新對應至您的. AppClient 如果您需要變更任何其他參數，例如 AppName starterUserEmails、或其他參數，您必須刪除 AppClient 並建立新參數。如需詳細資訊，請參閱 UpdateAppClient。

若要更新 AppClient，您至少必須擁有 "appfabric:UpdateAppClient" IAM 政策許可。如需詳細資訊，請參閱 允許存取更新 AppClients。

請求欄位

- appClientId(必要)-您要更新重新導覽的 AppClient ID。
- redirectUrls(必要)-重新導向的更新清單。您最多可以新增 5 個重新導向。

響應字段

- appName-將在使用 AppFabric 者入口網站的同意頁面上顯示給使用者的應用程式名稱。
- customerManagedKeyIdentifier(選擇性)-用於加密資料的客戶受管金鑰 (由 KMS 產生) 的 ARN。如果未指定，則將使用 AWS AppFabric 託管密鑰。
- description-應用程序的說明。
- redirectUrls-授權後將使用者重新導向至的 URI。例如 https://localhost:8080。
- starterUserEmails-一個用戶電子郵件地址，允許訪問以接收見解，直到應用程序通過驗證。只允許使用一個電子郵件地址。例如 anyuser@example.com。
- verificationStatus- AppClient 驗證狀態。
  - pending_verification-的驗證 AppClient仍在進行中 AppFabric。在驗證之 AppClient 前，只有一個使用者 (在中指定starterUserEmails) 可以使用 AppClient.
  - verified-驗證程序已由順利完成 AppFabric ，現 AppClient 已完成驗證。

- `rejected`-的驗證程序已 AppClient 遭拒絕 AppFabric。 AppClient 在重新啟動並成功完成驗證程序之前，其他使用者無法使用。

```
curl --request PATCH \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111 \
  --data '{
    "redirectUrls": ["https://localhost:8081"]
}'
```

如果動作成功，則服務傳回 HTTP 200 回應。

```
200 OK

{
    "appClient": {
        "appName": "Test App",
        "arn": "arn:aws:appfabric:<region>:111122223333:appclient/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "customerManagedKeyArn": "arn:aws:kms:<region>:111122223333:key/<key>",
        "description": "This is a test app",
        "redirectUrls": [
            "https://localhost:8081"
        ],
        "starterUserEmails": [
            "anyuser@example.com"
        ],
        "verificationDetails": {
            "verificationStatus": "pending_verification"
        }
    }
}
```

刪除一個 AppClient

使用 AppFabric `DeleteAppClient` API 操作刪除 AppClients 您不再需要的任何內容。如需詳細資訊，請參閱 DeleteAppClient。

若要刪除 AppClient，您至少必須擁有 `"appfabric:DeleteAppClient"` IAM 政策許可。如需詳細資訊，請參閱 允許存取刪除 AppClients。

請求欄位

- `appClientId`-身 AppClient 份證

響應字段

- 沒有響應字段。

```
curl --request DELETE \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111
```

如果動作成功，則服務會送回具有空 HTTP 主體的 HTTP 204 回應。

為最終用戶刷新令牌

您為最終用戶 AppClient 獲取的令牌可以在到期時刷新。這可以使用帶有 grant `refresh_token` _ 權杖 type 的 API 來完成。當 grant_type 為時，將`refresh_token`要使用的作為權杖 API 回應的一部分傳回。`authorization_code`預設到期日為 12 小時。若要呼叫重新整理 API，您必須擁有 `"appfabric:Token"` IAM 政策權限。如需詳細資訊，請參閱 權杖 及 允許存取更新 AppClients。

請求欄位

- `refresh_token`（必要）-從初始`/token`請求接收到的刷新令牌。
- `app_client_id`(必要)-為的建立的 AppClient 資源 ID AWS 帳戶。
- `grant_type`（必填）-這必須是`refresh_token`。

響應字段

- `expires_in`-令牌到期前多久。預設到期時間為 12 小時。
- `refresh_token`-從初始 /token 要求接收到的重新整理權杖。
- `token`-從初始 /token 要求接收到的權杖。
- `token_type`-該值將是`Bearer`。
- `appfabric_user_id`- AppFabric 使用者識別碼。這只會針對使用`authorization_code`授權類型的要求傳回。

```
curl --location \
"https://appfabric.<region>.amazonaws.com/oauth2/token" \
--header "Content-Type: application/json" \
--header "X-Amz-Content-Sha256: <sha256_payload>" \
--header "X-Amz-Security-Token: <security_token>" \
--header "X-Amz-Date: 20230922T172215Z" \
--header "Authorization: AWS4-HMAC-SHA256 ..." \
--data "{
    \"refresh_token\": \"<refresh_token>",
    \"app_client_id\": \"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111\",
    \"grant_type\": \"refresh_token\"
}"
```

如果動作成功，則服務傳回 HTTP 200 回應。

```
200 OK

{
    "expires_in": 43200,
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "${UserID}"
}
```

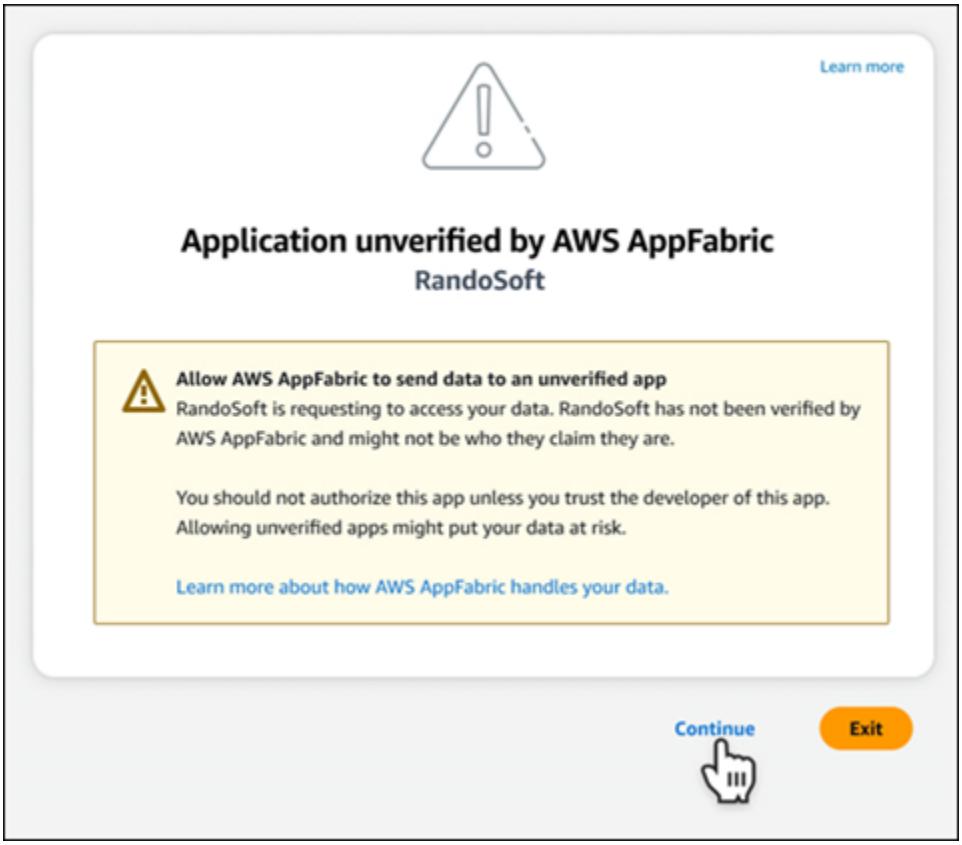
故障診斷

提高 AWS AppFabric 生產力功能為預覽狀態，可能會有所變更。

本節描述了 AppFabric 生產力的常見錯誤和疑難排解。

未驗證的應用

如果應用程式開發人員使 AppFabric 用生產力來豐富其應用程式體驗，則在向使用者啟動其功能之前，會先經過驗證程序。所有應用程序都以未經驗證的方式啟動，並且僅在驗證過程完成後才更改為已驗證。這意味著`starterUserEmails`您在創建時使用的 AppClient 將看到此消息。



`CreateAppClient` 錯誤

ServiceQuotaExceededException

如果您在建立時收到下列例外狀況 AppClient，表示您已超過每個 AppClients 可建立的例外數目 AWS 帳戶。限制為 1。狀態碼：

```
ServiceQuotaExceededException / SERVICE_QUOTA_EXCEEDED
You have exceeded the number of AppClients that can be created per AWS Account. The
 limit is 1.
HTTP Status Code: 402
```

`GetAppClient` 錯誤

ResourceNotFoundException

如果您在取得的詳細資訊時收到下列例外狀況 AppClient，請確定您輸入了正確的 AppClient 識別碼。此錯誤表示未找 AppClient 到指定的。

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

`DeleteAppClient` 錯誤

ConflictException

如果您在刪除時收到下列例外狀況 AppClient，表示正在進行另一個刪除請求。請等待完成，然後再試一次。HTTP 狀態碼：409

```
ConflictException
Another delete request is in progress. Wait until it completes then try again.
HTTP Status Code: 409
```

ResourceNotFoundException

如果您在刪除時收到下列例外狀況 AppClient，請確定您輸入了正確的 AppClient 識別碼。此錯誤表示未找 AppClient 到指定的。

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

`UpdateAppClient` 錯誤

ResourceNotFoundException

如果您在更新時收到下列例外狀況 AppClient，請確定您輸入了正確的 AppClient 識別碼。此錯誤表示未找 AppClient 到指定的。

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
```

```
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

`Authorize` 錯誤

ValidationException

如果任何 API 參數不符合 API 規範中定義的限制，您可能會收到下列例外狀況。

```
ValidationException
HTTP Status Code: 400
```

原因 1：未指定 AppClient ID 時

請求參數中缺少。`app_client_id`請建立 (AppClient如果尚未建立)，或使用您現有的檔案，`app_client_id`然後再試一次。若要尋找 AppClient 識別碼，請使用 ListAppClientAPI 作業。

原因 2： AppFabric 無法存取客戶管理金鑰時

```
Message: AppFabric couldn't access the customer managed key configured for AppClient.
```

AppFabric 目前無法存取客戶管理的金鑰，這可能是由於其權限的最近變更。驗證指定的密鑰是否存在，並確保 AppFabric 被授予適當的訪問權限。

原因 3：指定的重定向 URL 無效

```
Message: Redirect url invalid
```

請確定要求中的重新導向 URL 正確無誤。它必須符合建立或更新時指定的其中一個重新導向 URL AppClient。若要檢視允許的重新導向 URL 清單，請使用 GetAppClientAPI 作業。

`Token` 錯誤

TokenException

您可能會因為幾個原因而收到下列例外狀況。

```
TokenException
HTTP Status Code: 400
```

原因 1：指定無效的電子郵件時

```
Message: Invalid Email used
```

請確定您使用的電子郵件地址與建立時所列`starterUserEmails`屬性的電子郵件地址相符 AppClient。如果電子郵件不相符，請變更為相符的電子郵件地址，然後再試一次。若要檢視使用的電子郵件，請使用 GetAppClientAPI 作業。

原因 2：當未指定令牌時，對於 grant_type 作為刷新令牌。

```
Message: refresh_token must be non-null for Refresh Token Grant-type
```

請求中指定的刷新令牌為空或空。指定在 Token API 呼叫回應中`refresh_token`接收的作用中。

ThrottlingException

如果呼叫 API 的速率超過允許的配額，您可能會收到下列例外狀況。

```
ThrottlingException
HTTP Status Code: 429
```

`ListActionableInsights`、`ListMeetingInsights`、和`PutFeedback`錯誤

ValidationException

如果任何 API 參數不符合 API 規格上定義的約束，您可能會收到下列例外狀況。

```
ValidationException
HTTP Status Code: 400
```

ThrottlingException

如果呼叫 API 的速率超過允許的配額，您可能會收到下列例外狀況。

```
ThrottlingException
HTTP Status Code: 429
```

開始使用者 AppFabric 的生產力 (預覽版)

提高 AWS AppFabric 生產力功能為預覽狀態，可能會有所變更。

本節適用於 SaaS 應用程式的使用者，他們希望提高生產力 (預覽)，以改善其工作管理和工作流程效率。 AWS AppFabric 請依照下列步驟連線應用程式，並授權 AppFabric 顯示跨應用程式的深入解析，並協助您從偏好的應用程式完成動作 (例如傳送電子郵件或排程會議)。您可以連接諸如 Asana、、、Atlassian Jira Suite、Google Workspace、、Microsoft 365MiroSlackSmartsheet、等等的應用程式。授權 AppFabric 存取內容後，可直接在偏好的應用程式中 AppFabric提供跨應用程式深入解析和動作，協助您更有效率地工作，並保持在目前的工作流程中。

AppFabric 使用由 Amazon 基岩提供支援的生成人工智慧來提高生產力。 AppFabric 只有在收到您的明確許可後，才會產生見解和行動。您授權每個單獨的應用程序完全控制使用哪些內容。 AppFabric 不會使用您的資料來訓練或改善用於產生見解的基礎大型語言模型。如需詳細資訊，請參閱 Amazon 基岩常見問題集。

主題

必要條件

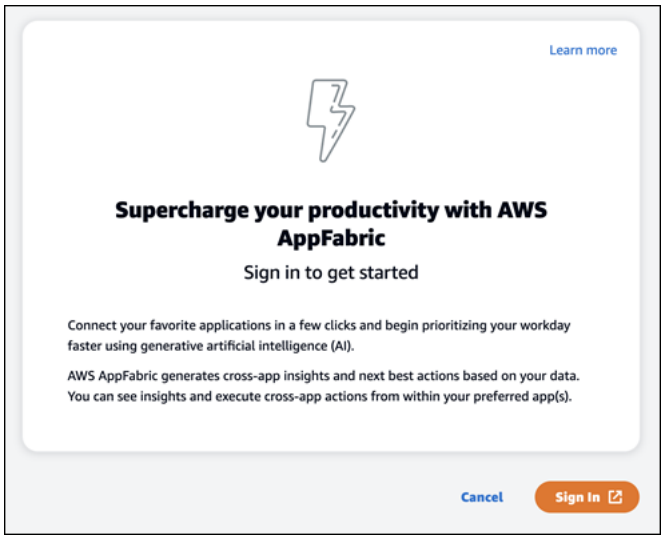
在開始之前，請確保您具備以下內容：

- 登入的認證 AppFabric：若要開始使 AppFabric 用以提高生產力，您將需要下列其中一個提供者的聯合登入認證 (使用者名稱和密碼)：AsanaGoogle Workspace、Microsoft 365、或Slack。登入以 AppFabric 協助我們將您識別為您提高生產力的每個應用程式中 AppFabric 的使用者。登入後，您可以連接應用程式以開始產生見解。
- 連接應用程式的認證：跨應用程式深入解析和動作只會根據您授權的應用程式產生。您將需要登錄憑據（用戶名和密碼）為您要授權的每個應用程序。支援的應用程式包括AsanaAtlassian Jira SuiteGoogle WorkspaceMicrosoft 365、Miro、Slack、、和Smartsheet。

步驟 1. 登入至 AppFabric

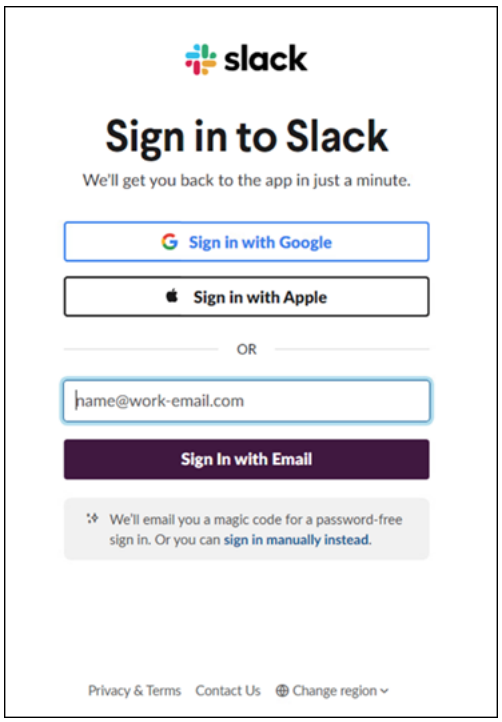
Connect 應用程式，直接將您的內容和見解帶入您偏好的應用程式中。 AppFabric

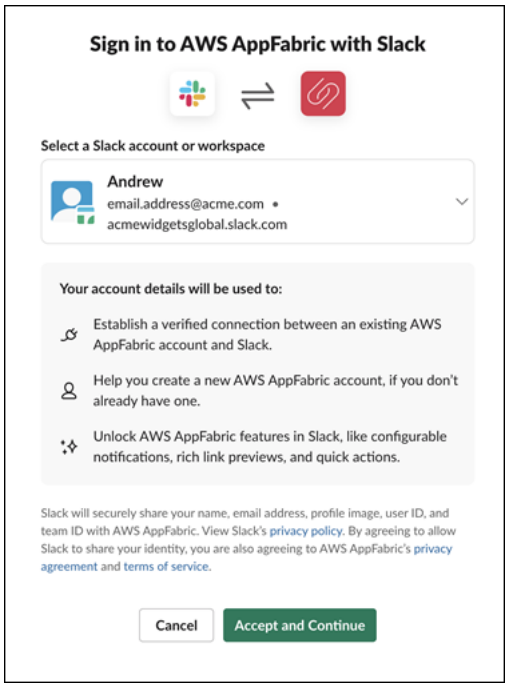
1. 每個應用程式都會以不同方式運用生產力， AppFabric 為您帶來更豐富的應用程式體驗 因此，每個應用程序都有不同的進入點，以訪問以下 AppFabric 提高生產力首頁。首頁會設定要啟用之程序的相關內容， AppFabric 並首先提示您登入。您要在其 AppFabric 中啟用的每個應用程序都將到達此屏幕。



2. 使用下列其中一個供應商提供的認證登入：AsanaGoogle WorkspaceMicrosoft 365、、或Slack。為了獲得最佳體驗，我們建議您在其中啟 AppFabric 用的每個應用程式使用相同的提供者登入。舉例來說，如果您在 App1 中選擇 Google Workspace 憑證，我們建議您Google Workspace在 App2 中選擇，以及每隔一次您需要重新登入。如果您使用不同的供應商登入，則需要重新啟動連線應用程式的程序。

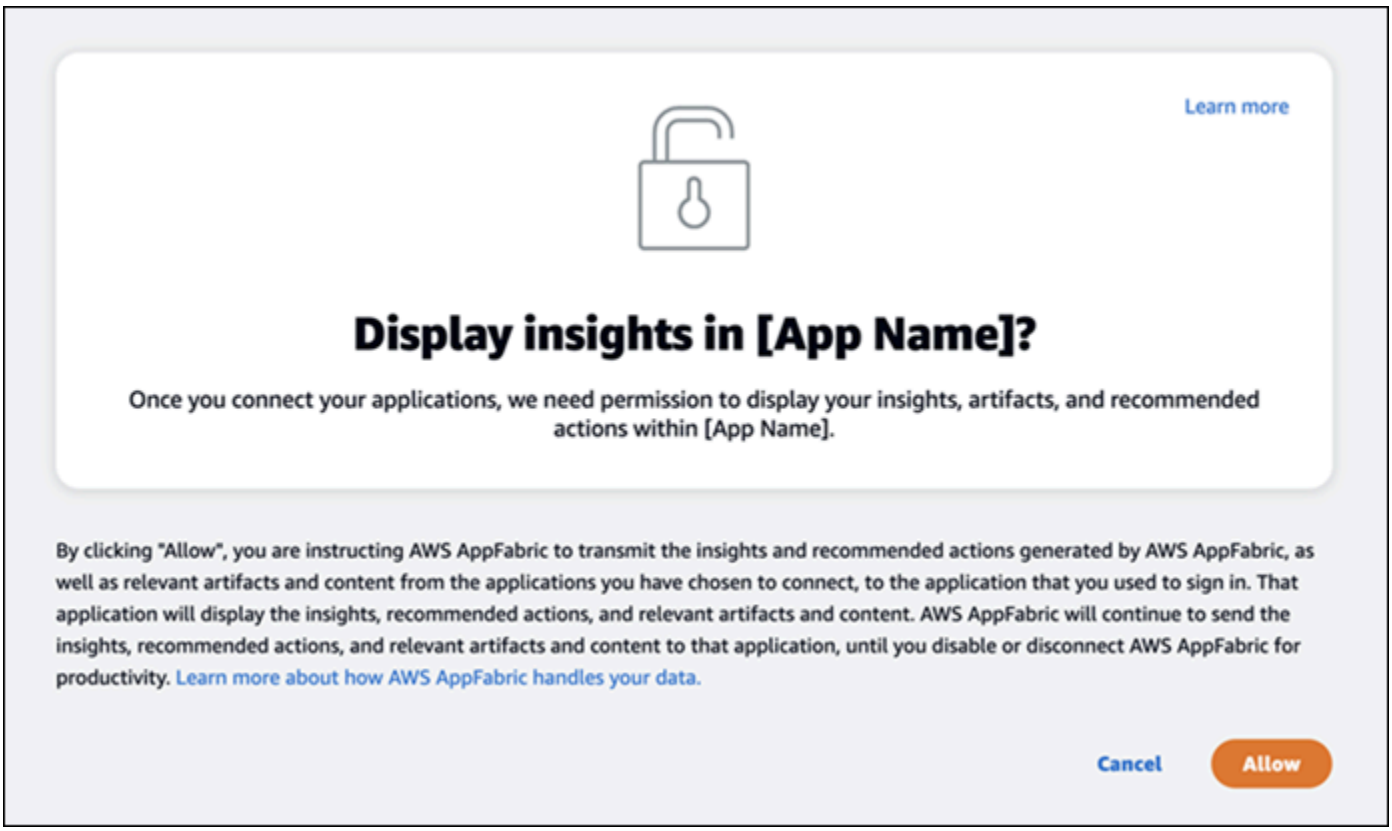
3. 如果出現提示，請輸入您的登錄憑據並接 AppFabric 受此提供程序的登錄。





步驟 2. 同意應用程式顯示見解

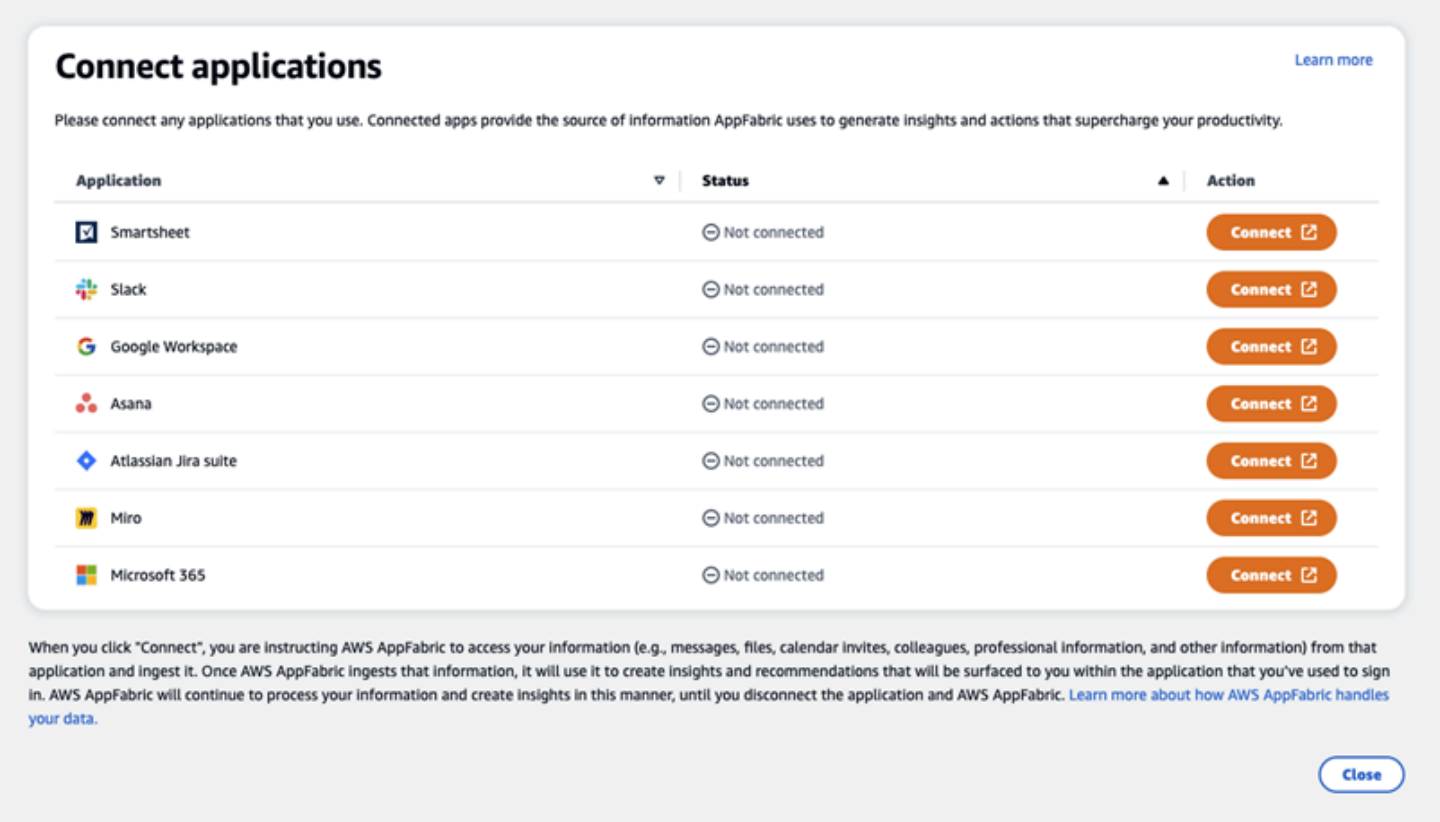
登入後， AppFabric 會顯示同意頁面，詢問您是否允許在啟 AppFabric 用生產力的應用程式內顯示跨應用 AppFabric 程式深入解析和動作。例如，您是否允許 AppFabric 將電Google Workspace子郵件和日曆事件顯示在中Asana。您只需要 AppFabric 在中啟用的每個應用程式完成此同意步驟一次。



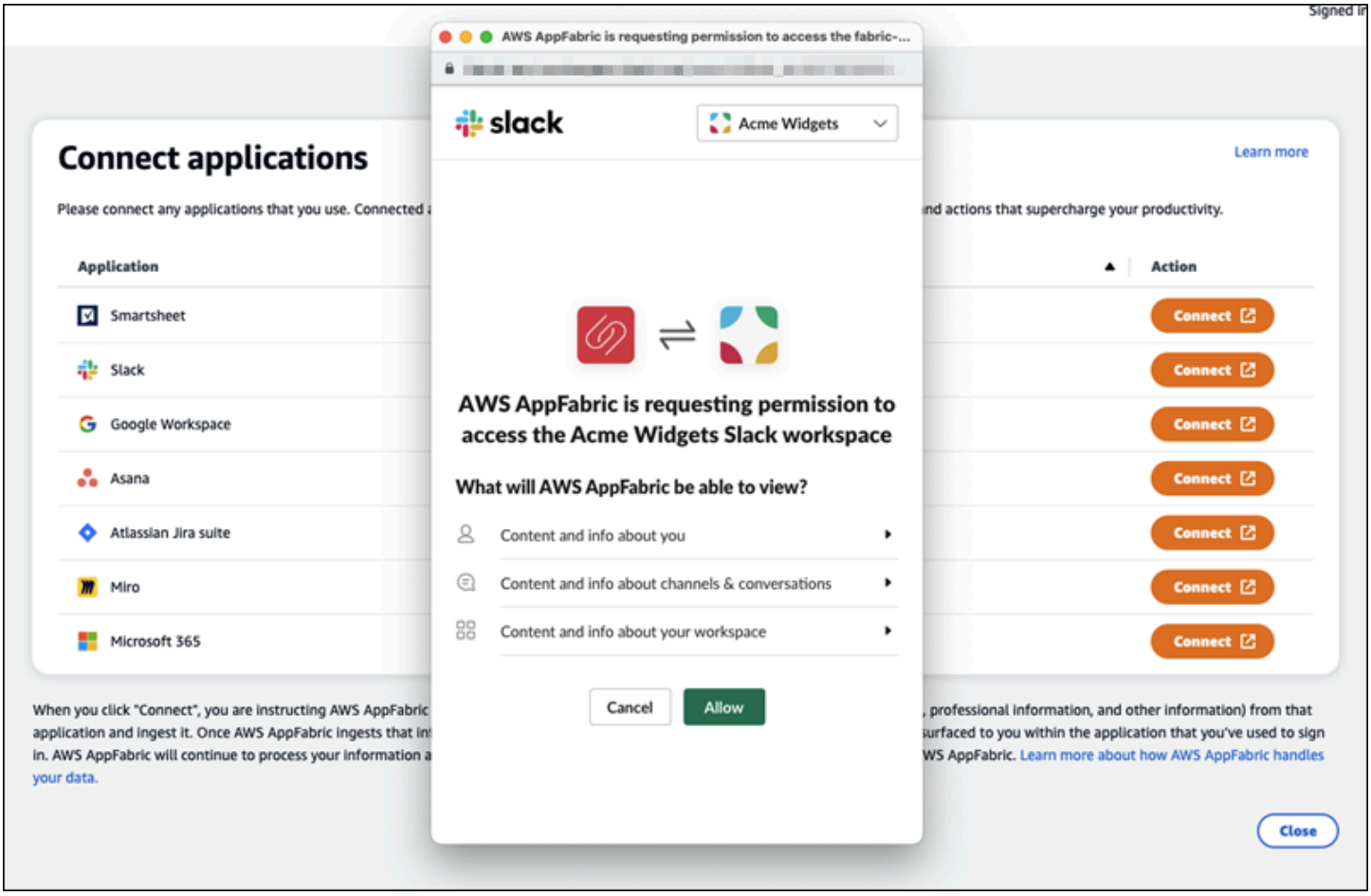
步驟 3。Connect 您的應用程式以產生見解和動作

完成同意頁面後，您將進入「Connect 應用程式」頁面，您可以在此連接、中斷連線或重新連接個別應用程式，這些應用程式最終用於產生跨應用程式見解和動作。在大多數情況下，在您登入並提供同意後，您將繼續使用此頁面來管理連線的應用程式。

若要 Connect 應用程式，請選擇您使用的任何應用程式旁的「連線」按鈕。



您將需要提供應用程式的登入認證，並允許存取資料的 AppFabric權限，以產生深入解析和完成動作。

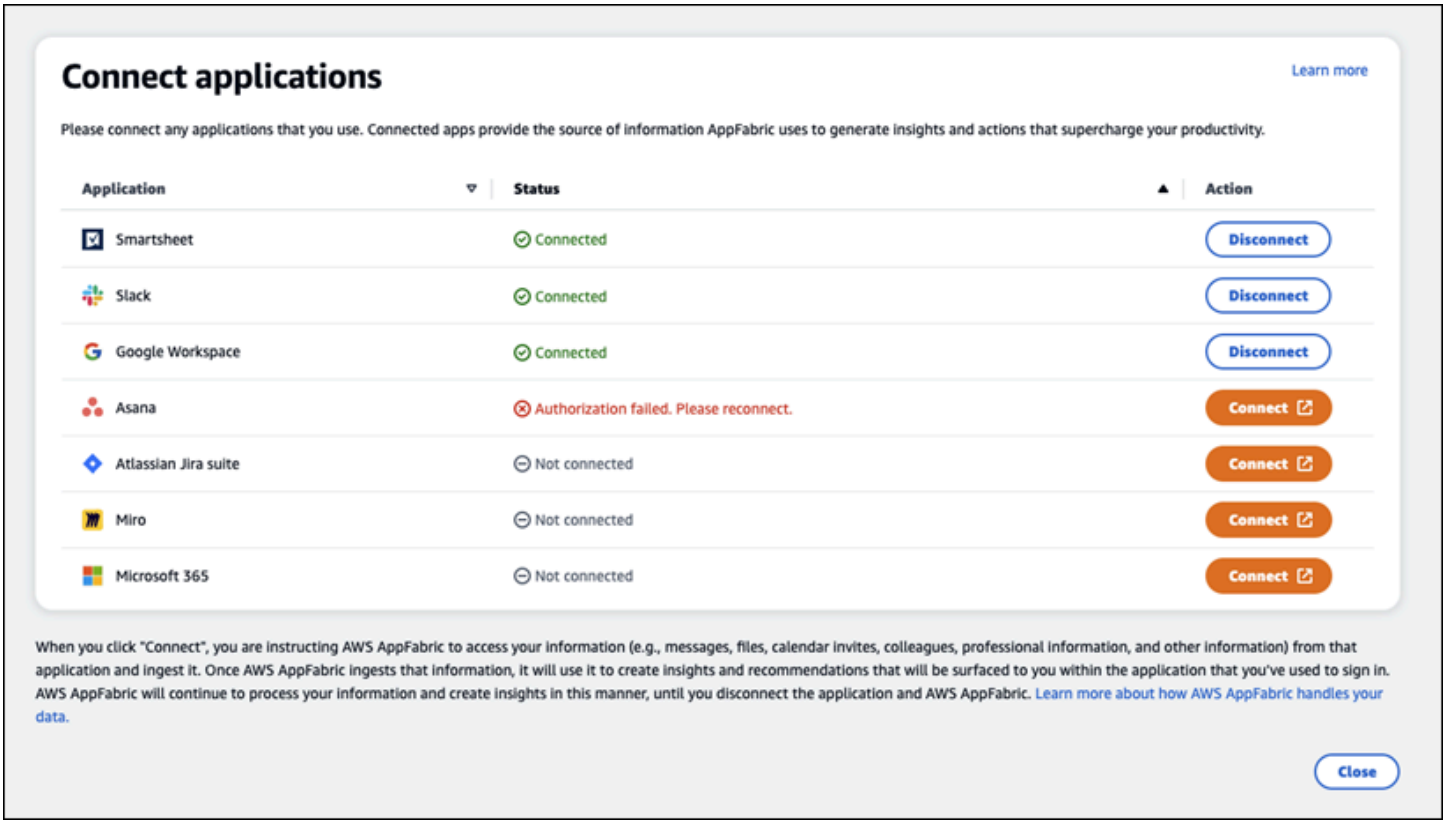


成功連線應用程式後，該應用程式的 [狀態] 會從 [未連線] 變更為 [已連線]。提醒：您需要針對要用於產生見解和動作的每個應用程式完成此授權步驟。

連接應用程式之後，它不會永遠連線。您需要定期重新連線應用程式。我們這樣做是為了確保我們仍然獲得您的許可以產生見解。

可能的應用程式狀態如下：

- 已連接- AppFabric 已獲得授權，並正在使用此應用程序中的數據生成見解。
- 未連接- AppFabric 不使用此應用程序中的數據生成見解。您可以連接以開始生成見解。
- 授權失敗。請重新連線。-特定應用程式可能發生授權失敗。如果看到此錯誤，請嘗試使用「連線」按鈕重新連線應用程式。



設定已完成，您可以返回您的申請。至少需要幾個小時才能開始查看應用程式中的見解。

視需要，您可以瀏覽回此頁面以管理連線的應用程式。如果您選擇中斷應用程式的連線， AppFabric 將停止使用該應用程式的資料或收集新資料來產生新的見解。如果您選擇在該時間內不重新連接應用程序，則來自已斷開連接應用程序的數據將在 7 天內自動刪除。

步驟 4. 開始在應用程式中查看見解並執行跨應用程式動作

將應用程式與連接之後 AppFabric，您將可以存取寶貴的見解，並能夠直接從偏好的應用程式執行跨應用程式動作。注意：並非每個應用程式都能保證這項功能，完全取決 AppFabric 於應用程式開發人員選擇啟用哪些生產力功能。

跨應用程式洞察

AppFabric 為了生產力提供了兩種類型的見解：

- 可操作的見解： AppFabric 分析來自連線應用程式的電子郵件、行事曆事件、工作和訊息中的資訊，並產生重要的見解，這些洞察對您來說可能很重要。此外，可 AppFabric 能會產生建議的動作 (例如傳送電子郵件、排程會議和建立工作)，您可以在停留在偏好的應用程式時編輯和執行這些動作。例如，您可能會收到一個洞察力，說明有一個客戶升級要處理，以及建議的下一個行動來安排與客戶的會議。

- 會議準備見解：此功能可協助您為即將到來的會議做好準備。 AppFabric 將分析您即將舉行的會議，並產生有關會議目的的的簡要摘要。此外，它還會顯示連線應用程式中的相關成品 (例如電子郵件、訊息和工作)，這些成品可協助您有效率地為會議做好準備，而無需在應用程式之間切換以尋找內容。

跨應用程式動作

對於某些見解，也 AppFabric 可能會產生建議的動作，例如傳送電子郵件、排程會議或建立工作。產生動作時， AppFabric 可能會根據連線應用程式的內容和內容預先填入特定欄位。例如， AppFabric 可能會根據洞察產生建議的電子郵件回覆或工作名稱。當您按一下建議的動作時，系統會將您帶到 AppFabric 擁有的使用者介面，您可以在其中編輯預先填入的內容，然後再執行動作。 AppFabric 如果沒有用戶審查並首先輸入，因為生成 AI 不會執行操作，並且基礎的大語言模型（LLM）可能會不時產生幻覺。

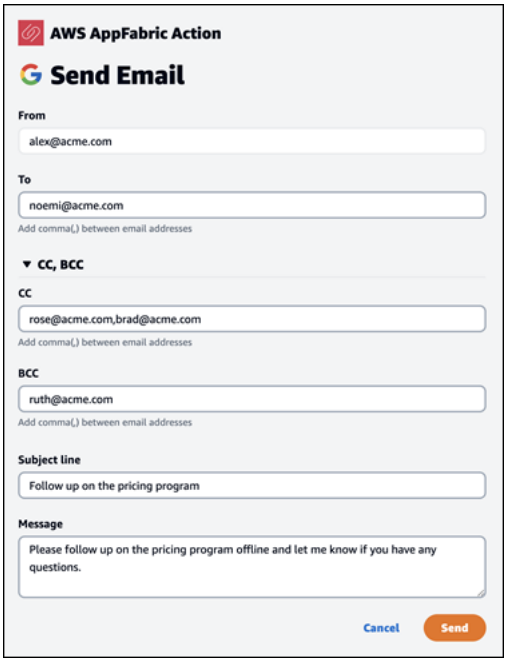
> **Note**
>
> 您有責任驗證和確認 AppFabric LLM 輸出。 AppFabric 不保證其 LLM 輸出的準確性或質量。如需詳細資訊，請參閱AWS 負責任的 AI 政策。

建立電子郵件 (Google Workspace,Microsoft 365)

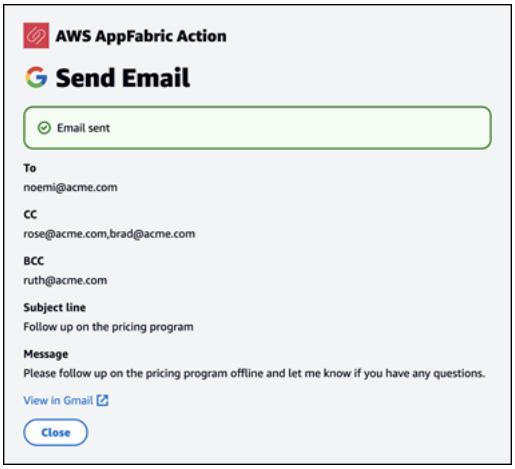
AppFabric 允許您從首選應用程序中編輯和發送電子郵件。我們支援基本的電子郵件欄位，包括 [寄件者]、[收件者]、[抄送/密件副本]、[電子郵件主旨行] 和 [AppFabric 可能會在這些欄位中產生內容，以協助您縮短完成工作的時間。編輯完電子郵件後，請選擇「傳送」來傳送電子郵件。

傳送電子郵件需要下列欄位：

- 至少有一個收件人電子郵件（收件人，抄送和密件抄送）是必需的，並且必須是有效的電子郵件地址。
- 「主旨行」和「訊息」欄位。



傳送電子郵件後，您會看到確認電子郵件已傳送。此外，您將看到一個鏈接，用於在指定的應用程序中查看電子郵件。您可以使用此鏈接快速導航到應用程序並驗證電子郵件已發送。



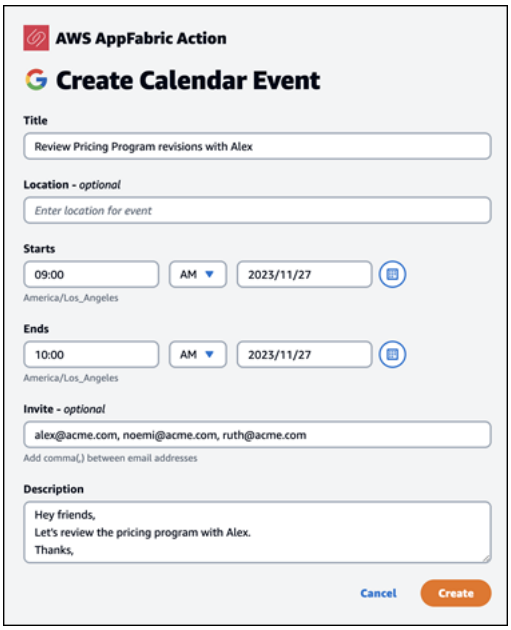
建立行事曆事件 (Google Workspace,Microsoft 365)

AppFabric 可讓您從偏好的應用程式中編輯和建立行事曆事件。我們支援基本的行事曆活動欄位，包括活動標題、位置、開始/結束時間和日期、受邀者清單和活動詳細資料。 AppFabric 可能會在這些欄位中產生內容，以協助您縮短完成工作的時間。編輯完日曆事件後，請選擇「建立」來建立活動。

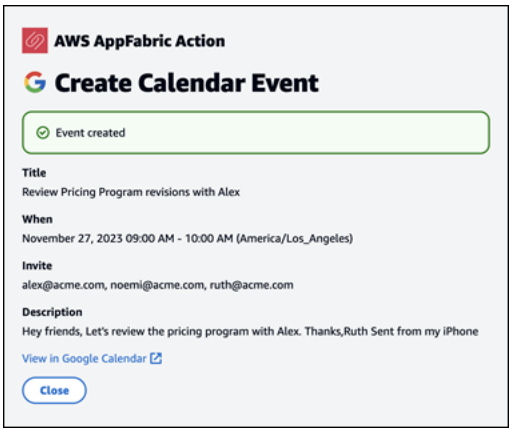
建立行事曆事件需要下列欄位：

- 「標題」、「開始」、「結束」和「描述」

- 開始時間和日期不得早於結束時間和日期。
- 邀請欄位是可選的，但需要有效的電子郵件地址 (如果提供)



傳送行事曆活動後，您會看到已建立活動的確認訊息。此外，您將看到一個鏈接，用於在指定的應用程序中查看事件。您可以使用此連結快速導覽至應用程式，並確認事件是否已建立。

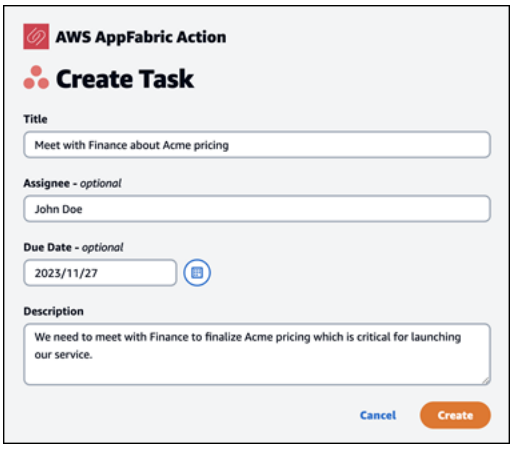


建立工作 (Asana)

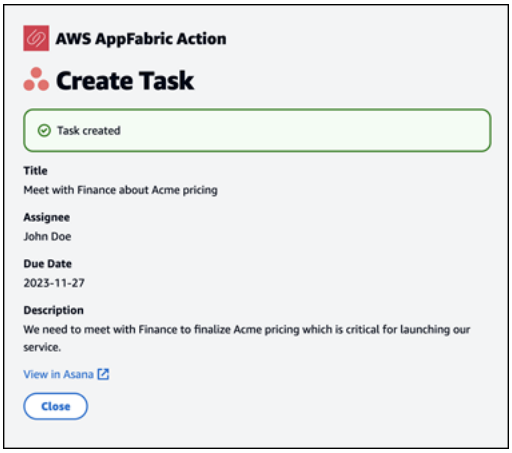
AppFabric 可讓您從偏好的應用程式Asana中編輯和建立工作。我們支援基本任務欄位，例如「任務名稱」、「任務擁有者」、「到期日」和「任務描述」。 AppFabric 可能會在這些欄位中產生內容，以協助您縮短建立工作的時間。編輯完工作後，選擇 [建立] 以建立工作。按照 LLM 的建議，在適用的Asana工作區或項目或任務中創建任務。

建立Asana任務需要下列欄位：

- 標題和描述欄位。
- 如果修改，受指派人必須是有效的電子郵件地址



建立工作後，您會看到已在中建立工作的確認訊息Asana。此外，您還會看到一個用於在中查看任務的鏈接Asana。您可以使用此連結快速導覽至應用程式，以確認工作是否已建立，或將其移至適當的Asana工作區或專案或工作。



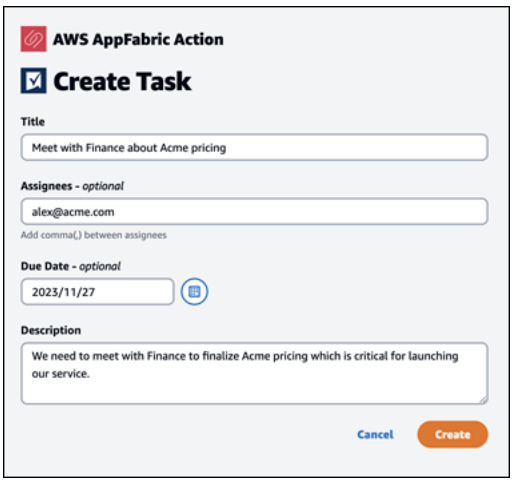
建立工作 (Smartsheet)

AppFabric 可讓您從偏好的應用程式Smartsheet中編輯和建立工作。我們支援基本任務欄位，例如「任務名稱」、「任務擁有者」、「到期日」和「任務描述」。 AppFabric 可能會在這些欄位中產生內容，以協助您縮短建立工作的時間。編輯完工作後，選擇 [建立] 以建立工作。對於Smartsheet任務， AppFabric 將創建一個新的私人工作Smartsheet表並填充任何創建的任務。這樣做是為了幫助集中 AppFabric 生成的操作在一個結構化的方式在一個地方。

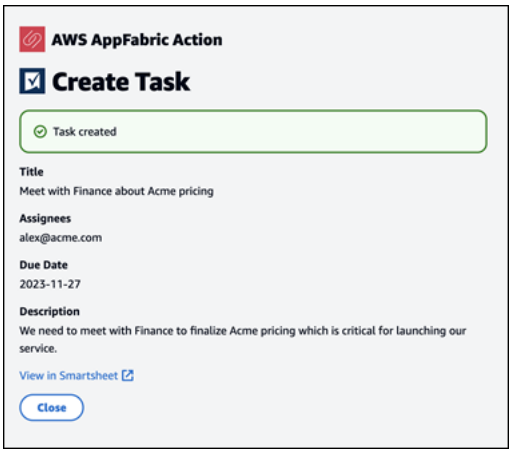
建立Smartsheet任務需要下列欄位：

- 標題和描述欄位。

- 受指派人必須是有效的電子郵件地址 (若提供)



建立工作後，您會看到已在中建立工作的確認訊息Smartsheet。此外，您還會看到一個用於在中查看任務的鏈接Smartsheet。您可以使用此鏈接快速導航到應用程序以查看創建的工作Smartsheet表中的任務。所有 future 的Smartsheet任務都將填入此工作表中。如果工作表被刪除， AppFabric 將創建一個新的。



IT 與安全性管理員注意：管理存取以 AppFabric 提升生產力 (預覽) 功能

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

所有已與 AppFabric 生產力 (預覽) 功能整合的 SaaS 應用程式使用者都可以公開存取生產力使用者入口網站。 AppFabric 如果您是 IT 管理員，想要管理組織內這些生成 AI 功能的存取權限，請考慮下列選項：

- 限制身分提供者 (IdP) 登入：您可以透過身分識別提供者封鎖登入存取，以控制使用者對生成 AI 功能的存取。
- 針對特定應用程式停用 OAuth：透過停用 OAuth 來實作下游限制。此動作可防止使用者將需要 OAuth 驗證的應用程式連線至公司的工作區。

故障診斷

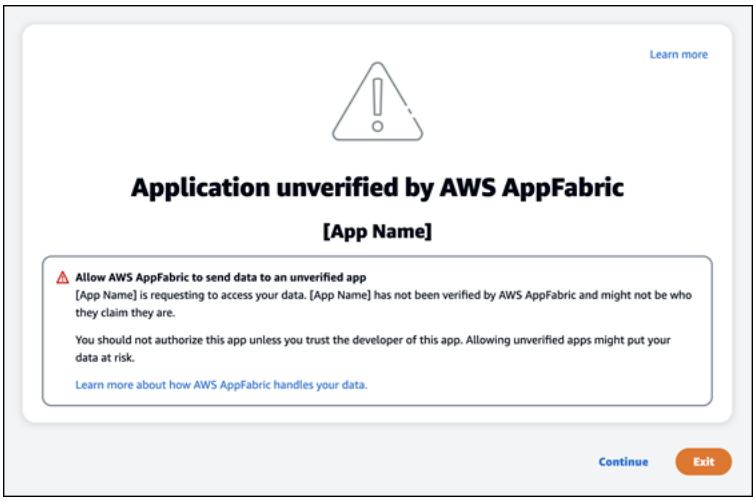
AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

本節描述了 AppFabric 生產力的常見錯誤和疑難排解。

未驗證的應用

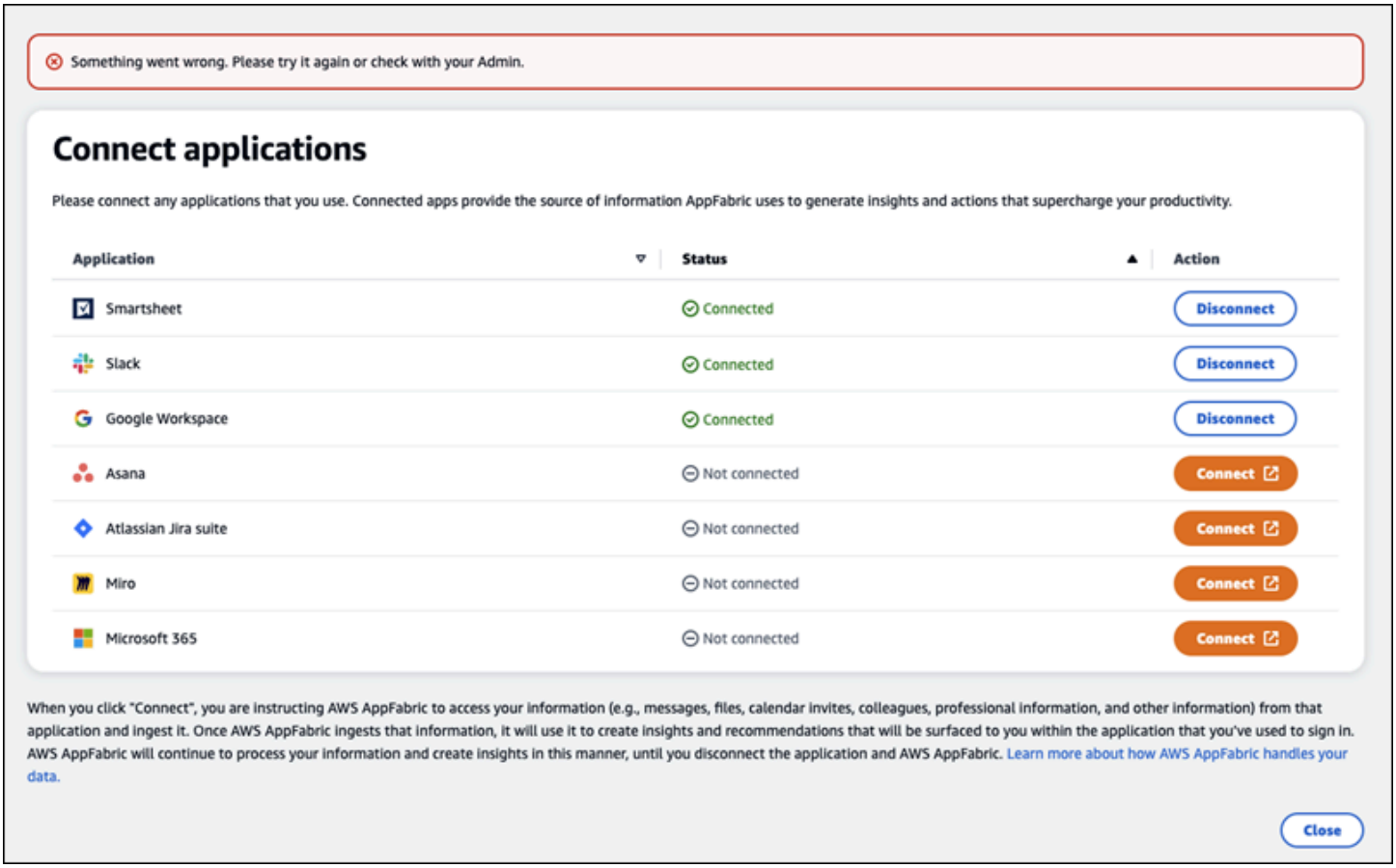
用 AppFabric 於提高生產力來豐富應用程式體驗的應用程式，在向使用者啟動其功能之前，會先經過驗證程序。如果您在嘗試登入時遇到「未驗證」橫幅 AppFabric，這表示應用程式尚未經 AppFabric過驗證程序，這會確認應用程式開發人員的身分和應用程式註冊資訊的正確性。所有應用程序都以未經驗證的方式啟動，並且僅在驗證過程完成後才更改為已驗證。

使用未經驗證的應用程序時要小心。如果您不確定應用程序開發人員，則可以等到應用程序達到已驗證狀態，然後再繼續操作。



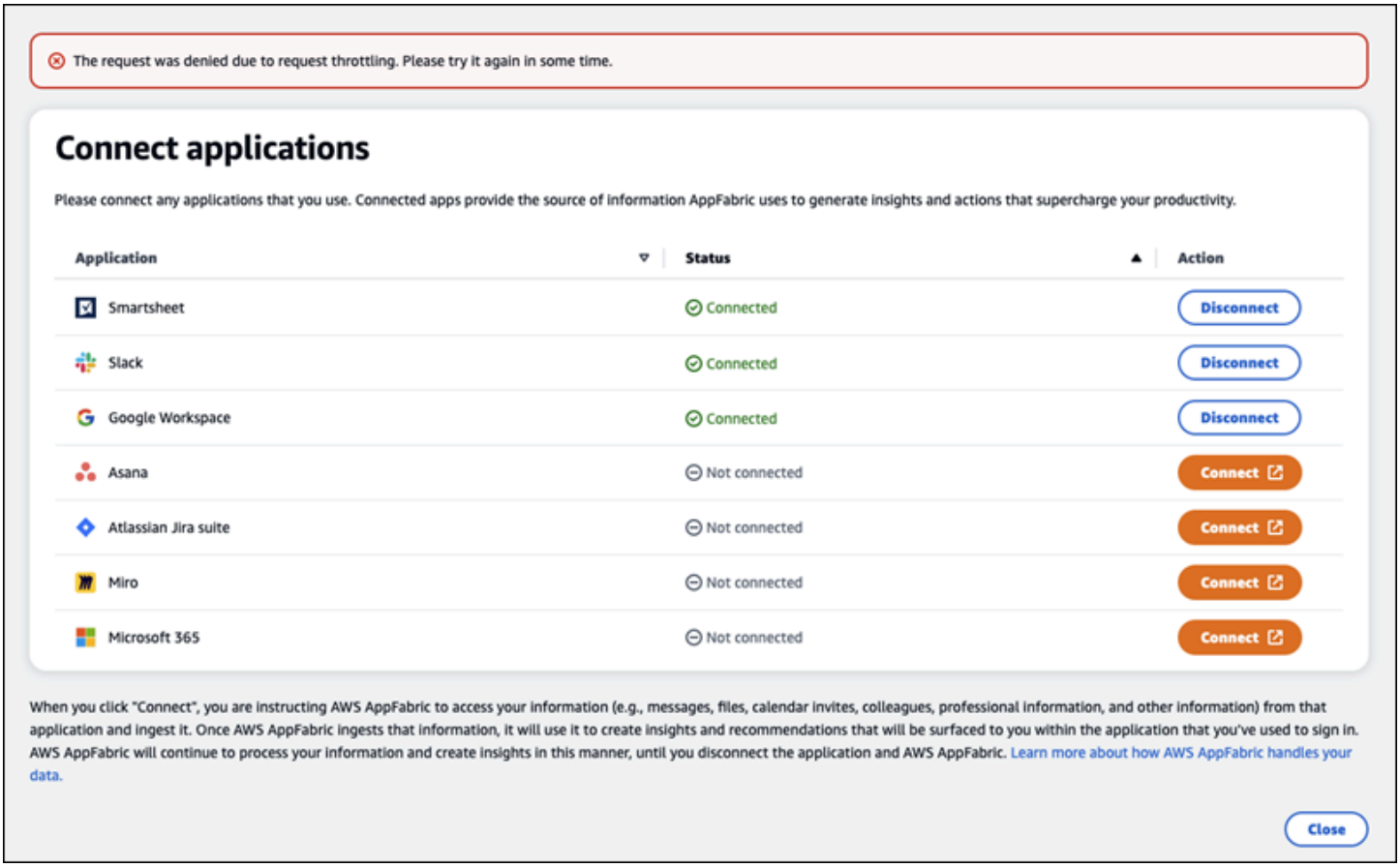
出了什麼問題。請再試一次或洽詢您的管理員 (**`InternalServerException`**)

當 AppFabric 使用者入口網站因未知的錯誤、例外狀況或失敗而無法列出應用程式或中斷應用程式連線時，您可能會收到此訊息。請稍後再試。



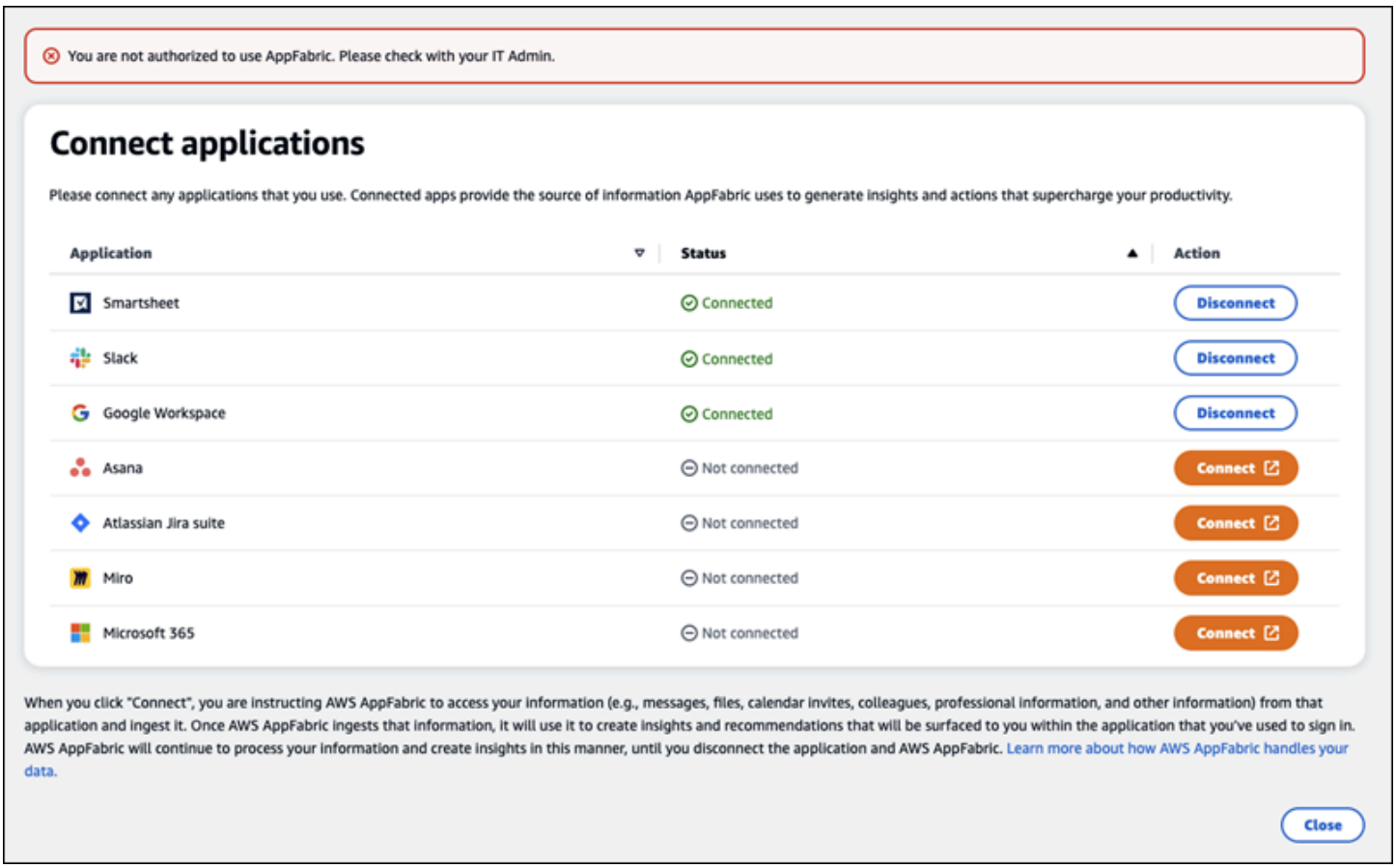
由於請求調節，因此請求遭到拒絕。請稍後再試一次 (**`ThrottlingException`**)

當 AppFabric 使用者入口網站因節流問題而無法列出應用程式或中斷應用程式連線時，您可能會收到此訊息。請稍後再試。



您沒有使用的授權 AppFabric。請 AppFabric 重新登入 (**`AccessDeniedException`**)

當 AppFabric 使用者入口網站因存取遭拒例外狀況而無法列出應用程式或中斷應用程式連線時，您可能會收到此訊息。 AppFabric 再次登入。



AppFabric 生產力 API

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

本節提供了 AWS AppFabric生產力功能的 API 操作、資料類型和常見錯誤。

> **Note**
>
> 對於所有其他 AppFabric API，請參閱 AWS AppFabric API 參考。

主題

- 動作
- 資料類型
- 常見錯誤

動作

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

AppFabric 生產力功能支援下列動作。

如需所有其他 AppFabric API 動作，請參閱 AWS AppFabric API 動作。

主題

- 授權
- CreateAppClient
- DeleteAppClient
- GetAppClient
- ListActionableInsights
- ListAppClients
- ListMeetingInsights
- PutFeedback
- 權杖
- UpdateAppClient

授權

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

授權. AppClient

主題

- 請求內文

請求內文

請求接受採用 JSON 格式的下列資料。

參數	描述
應用程式用戶端識別碼	AppClient 要授權的識別碼。
redirect_uri	要在授權後將最終使用者重新導向至的 URI。
state	用於維護請求和回調之間狀態的唯一值。

CreateAppClient

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

創建一個 AppClient.

主題

- 請求內文
- 回應元素

請求內文

請求接受採用 JSON 格式的下列資料。

參數	描述
應用名稱	應用程式的名稱。 類型：字串 長度限制：長度下限為 1。長度上限為 255。 必要：是
clientToken	指定您提供的唯一且區分大小寫的識別碼，以確保要求的冪等性。這可讓您安全地重試要求，而不會意外地再次執行相同的作業。將相同的值傳遞給稍後的作業呼叫時，您也必須為所有其他參數傳遞相同的值。我們建議您使用 UUID 類型的值。

參數	描述
	如果您不提供此值，則為您 AWS 生成一個隨機值。 如果您使用相同的參數重試作業ClientToken ，但使用不同的參數，則重試會失敗並顯示錯IdempotentParameterMismatch 誤。 類型：String 模式：[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12} 必要：否
customerManagedKey标识符	由所 客戶受管金鑰 AWS Key Management Service產生的 ARN。該密鑰用於加密數據。 如果未指定任何索引鍵， AWS 受管金鑰 則會使用 a。要指派給資源的一或多個標籤的索引鍵值配對的對映。 如需有關 AWS 擁有的金鑰 和客戶管理金鑰的詳細資訊，請參閱AWS Key Management Service 開發人員指南中的客戶 AWS 金鑰和金鑰。 類型：字串 長度限制：長度下限為 1。最大長度為 1011。 模式：arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12} 必要：否
description	應用程式的說明。 類型：字串 必要：是

參數	描述
圖標網址	圖示或標誌的 URL AppClient。 類型：字串 必要：否
重定向	要在授權後將最終使用者重新導向至的 URI。您最多可以新增 5 個重新導向。例如 `https://localhost:8080` 。 類型：字串陣列 陣列成員：項目數下限為 1。項目數上限為 5。 長度限制：長度下限為 1。長度上限為 2048。 模式：`(http|https):\/\/[-a-zA-Z0-9_:.\/]+` 必要：是
starterUserEmails	入門電子郵件地址，適用於在驗證之前被允許存取以接收見解的 AppClient 使用者。 類型：字串陣列 陣列成員：固定項目數為 1。 長度限制：長度下限為 0。最大長度為 320。 模式：`[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` 必要：是
tags	要指派給資源的一或多個標籤的索引鍵值配對的對映。 類型：標籤物件的陣列 陣列成員：項目數下限為 0。項目數上限為 50。 必要：否

回應元素

如果動作成功，則服務傳回 HTTP 201 回應。

服務會傳回下列 JSON 格式的資料。

參數	描述
appClientSummary	包含的摘要 AppClient。 類型：AppClientSummary 物件

DeleteAppClient

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

刪除應用程式用戶端。

主題

- 請求內文
- 回應元素

請求內文

請求接受採用 JSON 格式的下列資料。

參數	描述
appClientIdentifier	AppClient 要用於請求的 Amazon 資源名稱 (ARN) 或通用唯一識別碼 (UUID)。 長度限制：長度下限為 1。最大長度為 1011。 模式：`arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必要：是

回應元素

如果動作成功，則服務會送回具有空 HTTP 主體的 HTTP 204 回應。

GetAppClient

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

傳回有關的資訊 AppClient。

主題

- 請求內文
- 回應元素

請求內文

請求接受採用 JSON 格式的下列資料。

參數	描述
appClientIdentifier	AppClient 要用於請求的 Amazon 資源名稱 (ARN) 或通用唯一識別碼 (UUID)。 長度限制：長度下限為 1。最大長度為 1011。 模式：`arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必要：是

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

參數	描述
应用客户端	包含關於 AppClient. 類型：AppClient 物件

ListActionableInsights

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

列出最重要的可操作電子郵件訊息、工作和其他更新。

主題

- 請求內文
- 回應元素

請求內文

請求接受採用 JSON 格式的下列資料。

參數	描述
nextToken	如nextToken 果傳回，則會有更多可用的結果。的值nextToken 是每個頁面的唯一分頁標記。使用返回的令牌再次進行呼叫以檢索下一頁。保持所有其他參數不變。每個分頁令牌在 24 小時後過期。使用過期的分頁權杖會傳回 HTTP 400 InvalidToken 錯誤。

回應元素

如果動作成功，則服務傳回 HTTP 201 回應。

服務會傳回下列 JSON 格式的資料。

參數	描述
ActionableInsightsList	列出可操作的見解，包括標題、說明、動作和建立的時間戳記。如需詳細資訊，請參閱 ActionableInsights。
nextToken	如nextToken 果傳回，則會有更多可用的結果。的值nextToken 是每個頁面的唯一分頁標記。使用返回的令牌再次進行呼叫以檢索下一頁。保持所有其他參數不變。每個分頁令牌在 24 小時後過期。使用過期的分頁權杖會傳回 HTTP 400 InvalidToken 錯誤。 類型：字串

ListAppClients

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

返回所有的列表 AppClients。

主題

- 請求內文
- 回應元素

請求內文

請求接受採用 JSON 格式的下列資料。

參數	描述
maxResults	每次呼叫傳回的結果數目上限。您可以使用nextToken 來獲得更多的結果頁面。 這只是一個上限。每次呼叫傳回的實際結果數量可能小於指定的最大值。 有效範圍：最小值為 1。最大值為 100。

參數	描述
nextToken	如nextToken 果傳回，則會有更多可用的結果。的值nextToken 是每個頁面的唯一分頁標記。使用返回的令牌再次進行呼叫以檢索下一頁。保持所有其他參數不變。每個分頁令牌在 24 小時後過期。使用過期的分頁權杖會傳回 HTTP 400 InvalidToken 錯誤。

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

參數	描述
appClientList	包含 AppClient 結果清單。 類型：AppClientSummary 物件陣列
nextToken	如nextToken 果傳回，則會有更多可用的結果。的值nextToken 是每個頁面的唯一分頁標記。使用返回的令牌再次進行呼叫以檢索下一頁。保持所有其他參數不變。每個分頁令牌在 24 小時後過期。使用過期的分頁權杖會傳回 HTTP 400 InvalidToken 錯誤。 類型：字串

ListMeetingInsights

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

列出最重要的可操作日曆事件。

主題

- 請求內文

- 回應元素

請求內文

請求接受採用 JSON 格式的下列資料。

參數	描述
nextToken	如nextToken 果傳回，則會有更多可用的結果。的值nextToken 是每個頁面的唯一分頁標記。使用返回的令牌再次進行呼叫以檢索下一頁。保持所有其他參數不變。每個分頁令牌在 24 小時後過期。使用過期的分頁權杖會傳回 HTTP 400 InvalidToken 錯誤。

回應元素

如果動作成功，則服務傳回 HTTP 201 回應。

服務會傳回下列 JSON 格式的資料。

參數	描述
MeetingInsightList	列出可行的會議深入解析。如需詳細資訊，請參閱 MeetingInsights。
nextToken	如nextToken 果傳回，則會有更多可用的結果。的值nextToken 是每個頁面的唯一分頁標記。使用返回的令牌再次進行呼叫以檢索下一頁。保持所有其他參數不變。每個分頁令牌在 24 小時後過期。使用過期的分頁權杖會傳回 HTTP 400 InvalidToken 錯誤。 類型：字串

PutFeedback

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

允許使用者針對特定的見解或動作提交意見反應。

主題

- 請求內文
- 回應元素

請求內文

請求接受採用 JSON 格式的下列資料。

參數	描述
id	要提交意見反應的物件識別碼。這可以是 InsightId 或 ActionId.
反饋對於	正在提交意見反應的洞察力類型。 可能的值：ACTIONABLE_INSIGHT | MEETING_INSIGHT | ACTION
意見回饋評分	信用指數從15到 評分越高越好。

回應元素

如果動作成功，則服務會傳回具有空 HTTP 內文的 HTTP 201 回應。

權杖

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

包含允許 AppClients 將授權碼交換為存取權杖的資訊。

主題

- 請求內文
- 回應元素

請求內文

請求接受採用 JSON 格式的下列資料。

參數	描述
code	從授權端點收到的授權碼。 類型：字串 長度限制：長度下限為 1。長度上限為 2048。 必要：否
補助類型	權杖的授權類型。必須為 `authorization_code` 或 `refresh_token` 。 類型：字串 必要：是
應用程式用戶端識別碼	AppClient 的 ID。 類型：String 模式：`[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必要：是
redirect_uri	傳遞至授權端點的重新導向 URI。 類型：字串 必要：否
刷新令牌	從初始令牌請求收到的刷新令牌。 類型：字串 長度限制：長度下限為 1。長度上限為 4096。

參數	描述
	必要：否

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

參數	描述
應用程序用戶 ID	權杖的使用者識別碼。這只會針對使用authorization_code 授權類型的要求傳回。 類型：字串
到期 _	直到權杖到期的秒數。 類型：Long
刷新令牌	用於後續請求的刷新令牌。 類型：字串 長度限制：長度下限為 1。長度上限為 2048。
token	訪問令牌。 類型：字串 長度限制：長度下限為 1。長度上限為 2048。
令牌類型	權杖類型。 類型：字串

UpdateAppClient

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

更新 AppClient.

主題

請求內文

請求接受採用 JSON 格式的下列資料。

參數	描述
appClientIdentifier	AppClient 要用於請求的 Amazon 資源名稱 (ARN) 或通用唯一識別碼 (UUID)。 長度限制：長度下限為 1。最大長度為 1011。 模式：`arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必要：是
重定向	要在授權後將最終使用者重新導向至的 URI。您最多可以新增 5 個重新導向。例如 `https://localhost:8080` 。 類型：字串陣列 陣列成員：項目數下限為 1。項目數上限為 5。 長度限制：長度下限為 1。長度上限為 2048。 模式：`(http|https):\/\/[-a-zA-Z0-9_:.\/]+`

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

參數	描述
应用客户端	包含關於 AppClient. 類型：AppClient 物件

資料類型

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

該 AppFabric API 包含多種數據類型，各種操作使用。本節詳細介紹 AppFabric 生產力功能的資料類型。

有關所有其他 AppFabric API 數據類型，請參閱 AWS AppFabric API 數據類型。

> **Important**
> 不能保證資料類型結構中每個元素的順序。應用程式不該認定採取某一特定順序。

主題

- ActionableInsights
- AppClient
- AppClientSummary
- MeetingInsights
- VerificationDetails

ActionableInsights

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

根據其應用程序組合中的電子郵件，日曆邀請，消息和任務，包含用戶的重要和合適操作的摘要。使用者可以從各個應用程式中看到主動洞察，協助他們達到最佳的一天需求。這些見解提供了理由，說明使用者為何應關心見解摘要，以及產生深入解析之個別應用程式和成品的參考資料 (例如嵌入式連結)。

參數	描述
洞察时间	產生的見解的唯一 ID。
洞察內容	這會傳回見解摘要，以及用來產生深入解析之成品的內嵌連結。 這將是一個包含嵌入鏈接（ <a>標籤）的 HTML 內容。
洞察標題	所產生見解的標題。
createdAt	產生洞察力的時間。
動作	針對產生的見解建議的動作清單。 動作物件包含下列參數： • actionId— 所產生動作的唯一 ID。 • actionIconUrl — 建議在其中執行動作的應用程序的圖標 URL。 • actionTitle — 產生動作的標題。 • actionUrl — 終端使用者在使用者入口網站中檢視和執行動作 AppFabric的唯一 URL。 若要執行動作，ISV 應用程式會使用此 URL 將使用 AppFabric 者重新導向至使用者入口網站 (快顯畫面)。 • actionExecutionStatus — 指示動作狀態的列舉。 可能的值為：EXECUTED | NOT_EXECUTED

AppClient

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

包含關於 AppClient.

參數	描述
應用名稱	應用程式名稱。 類型：字串 必要：是
arn	Amazon 資源名稱 (ARN) 的 AppClient. 類型：字串 長度限制：長度下限為 1。最大長度為 1011。 模式：`arn:.+` 必要：是
description	應用程式的說明。 類型：字串 必要：是
圖標網址	圖示或標誌的 URL AppClient。 類型：字串 必要：否
重定向	允許的重新導向 URL AppClient。 類型：字串陣列 陣列成員：項目數下限為 1。項目數上限為 5。 長度限制：長度下限為 1。長度上限為 2048。 模式：`(http|https):\/\/[-a-zA-Z0-9_:.\/]+` 必要：是

參數	描述
starterUserEmails	入門電子郵件地址，適用於在驗證之前被允許存取以接收見解的 AppClient 使用者。 類型：字串陣列 陣列成員：固定項目數為 1。 長度限制：長度下限為 0。最大長度為 320。 模式：`[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` 必要：是
驗證詳情	包含 AppClient驗證的狀態和原因。 類型：VerificationDetails 物件 必要：是
customerManagedKey阿恩	Amazon 資源名稱 (ARN) 由 客戶受管金鑰 AWS Key Management Service 產生的. AppClient 類型：字串 長度限制：長度下限為 1。最大長度為 1011。 模式：`arn:.+` 必要：否
appClientId	AppClient 的 ID。旨在用於應用程序客戶端的 o 身份驗證流程中。 類型：String 模式：`[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必要：否

AppClientSummary

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

包含關於 AppClient.

參數	描述
arn	Amazon 資源名稱 (ARN) 的 AppClient. 類型：字串 長度限制：長度下限為 1。最大長度為 1011。 模式：`arn:.+` 必要：是
驗證狀態	AppClient 驗證狀態。 類型：字串 有效值:`pending_verification | verified | rejected` 必要：是
appClientId	AppClient 的 ID。旨在用於應用程序客戶端的 o 身份驗證流程中。 類型：String 模式：`[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必要：否

MeetingInsights

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

包含前 3 個會議的摘要，以及會議目的，相關的跨應用程序成品以及任務，電子郵件，消息和日曆事件中的活動。

參數	描述
洞察时间	產生的見解的唯一 ID。
洞察內容	洞察力的描述以字符串格式突出顯示詳細信息。與在一樣，為什麼這種見解很重要。
洞察標題	所產生見解的標題。
createdAt	產生洞察力的時間。
卡倫達爾文	使用者應關注的重要行事曆事件或會議。 日曆事件對象： • `startTime` — 事件的開始時間。 • `endTime`— 活動的結束時間。 • `eventUrl`— ISV 應用程式上行事曆事件的 URL。
resources	包含與生成見解相關的其他資源的列表。 資源物件： • `appName`— 資源所屬的應用程式名稱。 • `resourceTitle` — 資源標題。 • `resourceType` — 資源的類型。 可能的值為：`EMAIL | EVENT | MESSAGE | TASK` • `resourceUrl` — 應用程式中的資源 URL。 • `appIconUrl` — 資源所屬應用程式的影像 URL。

參數	描述
nextToken	用於獲取下一組見解的分頁令牌。這是一個可選字段，如果返回 null 意味著沒有更多的見解加載。

VerificationDetails

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

包含 AppClient 驗證的狀態和原因。

參數	描述
驗證狀態	AppClient 驗證狀態。 類型：字串 有效值:`pending_verification | verified | rejected` 必要：是
狀態原因	AppClient 驗證狀態的原因。 類型：字串 長度限制：長度下限為 1。長度上限為 1024。 必要：否

常見錯誤

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

本節列出 AWS AppFabric 生產力功能的 API 動作常見的錯誤。

對於所有其他 AppFabric 常見的 API 錯誤，請參閱 AWS AppFabric API 參考資料中的故障診斷和 AWS AppFabric API 常見錯誤。

例外名稱	描述
TokenException	令牌請求無效。 HTTP 狀態碼：400

資料處理

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

AppFabric 採取步驟將使用者內容個別存放在由 AppFabric管理或分開管理的 Amazon S3 儲存貯體中；這有助於確保我們產生使用者特定的見解。我們使用合理的保護措施來保護您的內容，其中可能包括靜態和傳輸中的加密。我們已將系統設定為在擷取後 30 天內自動刪除客戶內容。 AppFabric 不會使用使用者不再具有存取權的資料人工因素產生深入解析。例如，當使用者中斷資料來源 (應用程式) 的連線時，會 AppFabric 停止從該應用程式收集資料，並且不會使用已中斷連線應用程式的任何延遲成品來產生深入解析。 AppFabric的系統配置為在 30 天內刪除此類數據。

AppFabric 不會使用使用者內容來訓練或改善用來產生見解的基礎大型語言模型。如需有關生成 AI 功能 AppFabric的詳細資訊，請參閱 Amazon 基岩常見問答集。

靜態加密

AWS AppFabric 支持靜態加密，這是一種服務器端加密功能，在保存到磁盤時，對與用戶相關的所有數據進行 AppFabric 透明加密，並在您訪問數據時對其進行解密。

傳輸中加密

AppFabric 使用 TLS 1.2 保護傳輸中的所有內容，並使用 AWS 簽名版本 4 簽署 AWS 服務的 API 要求。

術語與概念

本主題說明中協助您開始使用的主 AWS AppFabric 要術語和概念。

應用程序包

AppFabric 應用程式套件會儲存您的所有 AppFabric 應用程式授權和擷取 (請參閱下列擷取定義)。您可以為每 AWS 帳戶 個建立一個應用程式套件包 AWS 區域。

AppClient （ 也是應用客戶端和應用程序客戶端 ）

資料收件者應用程式的 OAuth AppClient 。每個數據接收者應用程序都需要註冊一個 AppClient 才能訪問 AppFabric 數據。開發人員用戶需要一個 AWS 帳戶才能註冊 AppClient。每個 AWS 帳戶只能註冊一個 AppClient。 AppFabric 將根據. AppClient AppClient 將包含有關將通過此訪問 AppFabric 數據的數據接收者應用程序的信息 AppClient。

應用授權

應用程式授權會授 AppFabric 予與應用程式連線和互動的權限。它允許從您的應用程式擷取稽核記錄，使用 OAuth (開放授權-存取委派授與應用程式存取權的開放標準) 或個人存取權杖 (PAT) 認證。您可以為每個應用程式套件設定多個應用程式授權 (最多 50 個)。這可讓您從應 AppFabric 用程式的多個租用戶擷取稽核記錄，方法是視需要為應用程式的每個租用戶重複應用程式授權建立步驟。共用的認證會使用 AWS Key Management Service (AWS KMS) 中的 AWS 擁有的金鑰 或客戶管理的金鑰加密，並儲存在中 AppFabric。

攝入

AppFabric 擷取會使用應用程式授權，透過應用程式的公用 API 從應用程式提取稽核記錄。然後，它會將稽核記錄傳送至一或多個 (最多五個) 目的地。

用戶端 ID

當您創建應用程序授權以與使用 OAuth 流程的應用程序連接時， AppFabric 可能會要求您提供客戶端 ID 和客戶端密鑰。客戶端 ID 和客戶端密鑰可以在應用程序的身份驗證應用程序中找到。有關在給定身份驗證應用程序中何處找到客戶端 ID 的說明，請參閱支持的應用程序。共用的用戶端 ID 和用戶端密碼會使用 AWS 擁有的金鑰 或客戶管理的金 AWS KMS 鑰加密並儲存在中 AppFabric。

Client secret (用戶端密碼)

當您創建應用程序授權以與使用 OAuth 流程的應用程序連接時， AppFabric 可能會要求您提供客戶端 ID 和客戶端密鑰。客戶端 ID 和客戶端密鑰可以在應用程序的身份驗證應用程序中找到。有關在給定身

份驗證應用程序中何處找到客戶端密鑰的說明，請參閱支持的應用程序。共用的用戶端 ID 和用戶端密碼會使用 AWS 擁有的金鑰 或客戶管理的金 AWS KMS 鑰加密並儲存在中 AppFabric。

擷取目的地

擷取目的地定義應儲存從擷取擷取的稽核記錄的位置。每個擷取都可以將稽核日誌交付到一或多個目的地 (最多五個)，這些目的地是 Amazon Simple Storage Service (Amazon S3) 儲存貯體或您的 Amazon 資料 Firehose。 AWS 帳戶對於每個目的地，您可以定義日誌是以原始形式還是將日誌標準化為開放網絡安全架構框架（OCSF）結構描述。選取 OCSF 結構描述時，您可以定義記錄檔的格式 (JSON 或 ApacheParquet)。只有在選取 Amazon S3 做為目的地時，才能使用此ApacheParquet格式。

數據接收者應用

將呼叫 AppFabric 以從中獲取生成見解的應用程序 AppFabric。

OAuth

OAuth 是一種開放式通訊協定，可透過簡單且標準的方法從 Web、行動裝置和桌面應用程式進行安全授權。 AppFabric 使用 OAuth 來創建一些應用程序授權。

開放網路安全架構架構架構 (OCSF)

開放網絡安全架構框架（OCSF）是一個開源項目，提供用於開發模式的可擴展框架以及與供應商無關的核心安全模式。廠商和其他資料生產者可以採用和擴充其特定網域的結構描述。我們的目標是提供在任何環境、應用程式或解決方案中採用的開放標準，同時補充現有的安全性標準和程序。 AppFabric 擴展此模式以創建以軟件即服務（SaaS）為中心的事件結構，支持的所有 SaaS 應用程序審核日誌 AppFabric 將被標準化為。如需詳細資訊，請參閱 開放式網路安全架構。

個人存取權杖 (PAT)

個人存取權杖 (PAT) 是一串字元，可用來存取電腦系統，而非常用來存取一般密碼。當您建立應用程式授權以連接使用 PAT 流程的應用程式時， AppFabric 可能會要求您提供 PAT。PAT 可以在應用程序的身份驗證應用程序中找到。如需在特定驗證應用程式中何處尋找 PAT 的指示，請參閱支援的應用程式。共享的服務帳戶令牌使用 AWS 擁有的金鑰 或客戶管理的密 AWS KMS 鑰進行加密並存儲在中 AppFabric。

服務帳戶令牌

當您建立應用 AppFabric 程式授權以與應用程式連線時，部分應用程式需要建立服務帳戶以進行應用程式驗證。 AppFabric 可能會要求提供服務帳戶令牌作為應用授權過程的一部分。有關在給定身份

驗證應用程序中在何處找到服務帳戶令牌的說明，請參閱支持的應用程序。共享的服務帳戶令牌使用 AWS 擁有的金鑰 或客戶管理的密 AWS KMS 鑰進行加密並存儲在中 AppFabric。

租用戶 ID

建立應用程式授權時， AppFabric 可能會要求您提供應用程式的租用戶 ID 和租用戶名稱。承租人識別碼是應用程式承租人的唯一識別碼。每個應用程式對於租用戶可能有不同的條款，例如用於的工作區識別碼Slack或的網域識別碼Asana。如需在特定應用程式中何處尋找租用戶 ID 的指示，請參閱支援的應用程式。

租戶名稱

建立應用程式授權時， AppFabric 可能會要求您提供應用程式的租用戶 ID 和租用戶名稱。租用戶名稱是您提供給租用戶識別碼的唯一名稱，以便在應用程式服務包中使用。此值用於標記應用程式授權和任何相關擷取。

中的安全性 AWS AppFabric

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 — AWS 負責保護 AWS 服務 中執行的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。若要深入瞭解適用於的規範遵循計劃 AWS AppFabric，請參閱合規計劃的AWS 服務範圍範圍)。
- 雲端中的安全性 — 您的責任取決於您使用的資料。 AWS 服務 您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用時套用共同責任模型 AppFabric。下列主題說明如何設定 AppFabric 以符合安全性與合規性目標。您還將學習如何使用其 AWS 服務 他幫助您監控和保護 AppFabric 資源的其他方法。

主題

- 資料保護 AWS AppFabric
- 的身分識別與存取管理 AWS AppFabric
- 符合性驗證 AWS AppFabric
- 安全性最佳做法 AWS AppFabric
- 韌性在 AWS AppFabric
- 基礎架構安全性 AWS AppFabric
- 中的配置和漏洞分析 AWS AppFabric

資料保護 AWS AppFabric

AWS 共用責任模型適用於中的資料保護 AWS AppFabric。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用主控台、API AppFabric 或 AWS SDK 時 AWS 服務 使用或其他使用時。 AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

> **Note**
>
> 如需適用於安全性之資料保護的 AppFabric 詳細資訊，請參閱資料處理。

靜態加密

AWS AppFabric 支持靜態加密，這是一種服務器端加密功能，其中當應用程序包保存到磁盤時，將與應用程序包相關的所有數據 AppFabric透明地加密，並在訪問數據時對其進行解密。默認情況下，使用 AWS 擁有的金鑰 從 AWS Key Management Service （ AWS KMS ） AppFabric 加密您的數據。您也可以選擇使用您自己的客戶管理金鑰來加密資料 AWS KMS。

刪除應用程式套件時，其所有中繼資料都會永久刪除。

傳輸中加密

設定應用程式套件組合時，您可以選擇 AWS 擁有的金鑰 或客戶管理的金鑰。收集和標準化用於稽核日誌擷取的資料時，請將資料暫時 AppFabric 存放在中繼 Amazon Simple Storage Service (Amazon S3) 儲存貯體中，並使用此金鑰對其進行加密。此中繼值區會在 30 天後使用儲存貯體生命週期政策刪除。

AppFabric 使用 TLS 1.2 保護傳輸中的所有資料，並使用 AWS 簽名 V4 簽署 API 要求。 AWS 服務

金鑰管理

AppFabric 支援使用 AWS 擁有的金鑰 或客戶管理的金鑰加密資料。我們建議您使用客戶管理的金鑰，因為這可讓您完全掌控加密資料。當您選擇客戶管理的金鑰時，會將資源策略 AppFabric 附加至客戶管理的金鑰，以授予其存取客戶管理金鑰的權限。

客戶受管金鑰

若要建立客戶受管金鑰，請遵循AWS KMS 開發人員指南中關於建立對稱加密 KMS 金鑰的步驟。

金鑰政策

關鍵原則可控制對客戶管理金鑰的存取。每個客戶受管金鑰都必須只有一個金鑰政策，其中包含決定誰可以使用金鑰及其使用方式的陳述式。在建立客戶受管金鑰時，可以指定金鑰政策。如需有關建立金鑰原則的詳細資訊，請參閱AWS KMS 開發人員指南中的建立金鑰政策。

若要在中使用客戶受管金鑰 AppFabric，建立 AppFabric資源的 AWS Identity and Access Management (IAM) 使用者或角色必須具有使用客戶受管金鑰的權限。我們建議您建立僅與金鑰搭配使用的金鑰， AppFabric 並將使用 AppFabric 者新增為金鑰的使用者。這種方法限制了對數據的訪問範圍。您的使用者需要的權限如下：

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:Decrypt`

主 AWS KMS 控台會引導您使用適當的金鑰原則建立金鑰。如需關鍵原則的詳細資訊，請參閱AWS KMS 開發人員指南 AWS KMS中的主要政策。

以下是允許的金鑰原則範例：

- 鑰匙的 AWS 帳戶根使用者 完全控制。
- 允許使用者搭配 AppFabric 使用您的客戶管理金鑰 AppFabric。
- 中應用程式套件組合設定的關鍵原則`us-east-1`。

```
{
```

```
    "Id": "key-consolepolicy-3",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": ["kms:*"],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/key_ID"
        },
        {
            "Sid": "Allow read-only access to key metadata to the account",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": [
                "kms:Describe*",
                "kms:Get*",
                "kms:List*",
                "kms:RevokeGrant"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow access to principals authorized to use AWS AppFabric",
            "Effect": "Allow",
            "Principal": {"AWS": "IAM-role/user-creating-appfabric-resources"},
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:ListAliases"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "appfabric.us-east-1.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        }
    ]
}
```

如何 AppFabric 使用補助金 AWS KMS

AppFabric 需要授權才能使用您的客戶管理金鑰。如需詳細資訊，請參閱AWS KMS 開發人員指南 AWS KMS中的授權。

建立應用程式套件組合時，CreateGrant請將要求傳送至，以代表您建 AppFabric 立授權 AWS KMS。中的贈款 AWS KMS 用於授予對客戶帳戶中 AWS KMS 密鑰的 AppFabric 訪問權限。AppFabric 要求授權使用您的客戶管理密鑰進行以下內部操作：

- 傳送GenerateDataKey要求 AWS KMS 以產生由客戶管理金鑰加密的資料金鑰。
- 傳送Decrypt AWS KMS 要求以解密加密的資料金鑰，以便使用這些金鑰來加密您的資料，以及解密傳輸中的應用程式存取權杖。
- 傳送Encrypt要求以 AWS KMS 加密傳輸中的應用程式存取權杖。

以下是授予的一個例子。

```
{
  "KeyId": "arn:aws:kms:us-east-1:111122223333:key/ff000af-00eb-00ce-0e00-
ea000fb0fba0SAMPLE",
  "GrantId": "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
  "Name": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "CreationDate": "2022-10-11T20:35:39+00:00",
  "GranteePrincipal": "appfabric.us-east-1.amazonaws.com",
  "RetiringPrincipal": "appfabric.us-east-1.amazonaws.com",
  "IssuingAccount": "arn:aws:iam::111122223333:root",
  "Operations": [
    "Decrypt",
    "Encrypt",
    "GenerateDataKey"
  ],
  "Constraints": {
    "EncryptionContextSubset": {
      "appBundleArn": "arn:aws:fabric:us-east-1:111122223333:appbundle/
ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE"
    }
  }
},
```

當您刪除應用程式套件時，會 AppFabric 淘汰已核發客戶管理金鑰的授權。

監控您的加密金鑰 AppFabric

當您搭配使用 AWS KMS 客戶受管金鑰時 AppFabric，您可以使用 AWS CloudTrail 記錄來追蹤 AppFabric 傳送至的要求 AWS KMS。

以下是 AppFabric 用`CreateGrant`於客戶管理金鑰時記錄的 CloudTrail 事件範例。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser",
        "arn": "arn:aws:sts::111122223333:assumed-role/AssumedRole/SampleUser",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AssumedRole",
                "accountId": "111122223333",
                "userName": "SampleUser"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-04-28T14:01:33Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-04-28T14:05:48Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "appfabric.amazonaws.com",
    "userAgent": "appfabric.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "appfabric.us-east-1.amazonaws.com",
        "constraints": {
            "encryptionContextSubset": {
                "appBundleArn": "arn:aws:appfabric:us-east-1:111122223333:appbundle/
ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE"
            }
```

```
        },
        "keyId": "arn:aws:kms:us-east-1:111122223333:key/EXAMPLEID",
        "retiringPrincipal": "appfabric.us-east-1.amazonaws.com",
        "operations": [
            "Encrypt",
            "Decrypt",
            "GenerateDataKey"
        ]
    },
    "responseElements": {
        "grantId": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
        "keyId": "arn:aws:kms:us-east-1:111122223333:key/KEY_ID"
    },
    "additionalEventData": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:111122223333:key/key_ID"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_256_GCM_SHA384",
        "clientProvidedHostHeader": "kms.us-east-1.amazonaws.com"
    }
}
```

的身分識別與存取管理 AWS AppFabric

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

主題

物件

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，具體取決於您在進行的工作 AppFabric。

服務使用者 — 如果您使用 AppFabric 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 AppFabric 功能來完成工作時，您可能需要其他權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果無法存取中的特徵 AppFabric，請參閱疑難排解 AWS AppFabric 身分和存取。

服務管理員 — 如果您負責公司的 AppFabric 資源，您可能擁有完整的存取權 AppFabric。決定您的服務使用者應該存取哪些 AppFabric 功能和資源是您的工作。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步瞭解貴公司如何搭配使用 IAM AppFabric，請參閱如何與 IAM AWS AppFabric 搭配使用。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要瞭解如何撰寫政策來管理存取權限的詳細資訊 AppFabric。若要檢視可在 IAM 中使用的 AppFabric 基於身分的政策範例，請參閱。AWS AppFabric 的身分型政策範例

使用身分驗證

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

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

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

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

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

AWS 帳戶 根使用者

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

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用

程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

IAM 使用者和群組

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

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

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱 IAM 使用者指南中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

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

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 – 若要向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取權角色和資源型政策間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源類型政策的差異。

- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需更多資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

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

使用政策管理存取權

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

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

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

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

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

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

存取控制清單 (ACL)

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

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

其他政策類型

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

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政

策中的明確拒絕都會覆寫該允許。如需許可範圍的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 實體許可範圍。

- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需組織和 SCP 的更多相關資訊，請參閱 AWS Organizations 使用者指南中的 SCP 運作方式。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需更多資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

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

如何與 IAM AWS AppFabric 搭配使用

在您使用 IAM 管理存取權限之前 AppFabric，請先了解哪些 IAM 功能可搭配使用 AppFabric。

您可以搭配使用的 IAM 功能 AWS AppFabric

IAM 功能	AppFabric 支持
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	否
ACL	否
ABAC (政策中的標籤)	是

IAM 功能	AppFabric 支持
臨時憑證	否
主體許可	是
服務角色	否
服務連結角色	是

若要深入瞭解如何以 AppFabric 及其他如何使 AWS 服務 用大多數 IAM 功能，請參閱 IAM 使用者指南中的與 IAM 搭配使用的AWS 服務。

以身分識別為基礎的原則 AppFabric

支援身分型政策	是

身分型政策是可以連接到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

以身分識別為基礎的原則範例 AppFabric

若要檢視以 AppFabric 身分為基礎的原則範例，請參閱。AWS AppFabric 的身分型政策範例

以資源為基礎的政策 AppFabric

支援以資源基礎的政策	否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源

的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策有何差異。

的政策動作 AppFabric

支援政策動作	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 AppFabric 動作清單，請參閱服務授權參考 AWS AppFabric中所定義的動作。

中的策略動作在動作之前 AppFabric 使用下列前置詞：

```
appfabric
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "appfabric:action1",
      "appfabric:action2"
         ]
```

您可以使用萬用字元 (*) 指定多個動作。例如，如需指定開頭是 List 文字的所有動作，請包含以下動作：

```
"Action": "appfabric:List*"
```

若要檢視以 AppFabric 身分為基礎的原則範例，請參閱。AWS AppFabric 的身分型政策範例

的政策資源 AppFabric

支援政策資源	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

若要查看 AppFabric 資源類型及其 ARN 的清單，請參閱服務授權參考 AWS AppFabric中所定義的資源類型。若要瞭解可以使用哪些動作指定每個資源的 ARN，請參閱定義的動作。 AWS AppFabric

若要檢視以 AppFabric 身分為基礎的原則範例，請參閱。AWS AppFabric 的身分型政策範例

的政策條件索引鍵 AppFabric

支援服務特定政策條件金鑰	否

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要查看 AppFabric 條件索引鍵清單，請參閱服務授權參考 AWS AppFabric中的條件金鑰。若要瞭解您可以使用條件索引鍵的動作和資源，請參閱定義的動作 AWS AppFabric。

若要檢視以 AppFabric 身分為基礎的原則範例，請參閱。AWS AppFabric 的身分型政策範例

ACL 在 AppFabric

支援 ACL	否

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

阿巴克與 AppFabric

支援 ABAC (政策中的標籤)	是

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC?。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

使用臨時登入資料 AppFabric

支援臨時憑證	否

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

的跨服務主體權限 AppFabric

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

AppFabric 的服務角色

支援服務角色	否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。

> **Warning**
>
> 變更服務角色的權限可能會中斷 AppFabric 功能。只有在 AppFabric 提供指引時才編輯服務角色。

服務連結角色 AppFabric

支援服務連結角色	是

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需有關建立或管理 AppFabric 服務連結角色的詳細資訊，請參閱使用 AppFabric 的服務連結角色。

AWS AppFabric 的身分型政策範例

依預設，使用者和角色沒有建立或修改 AppFabric資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

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

如需有關由定義的動作和資源類型的詳細資訊 AppFabric，包括每個資源類型的 ARN 格式，請參閱服務授權參考 AWS AppFabric中的動作、資源和條件索引鍵。

內容

- 允許存取生產力功能的唯讀存取權
- 完全存取生產力功能
- 允許存取以建立 AppClients
- 允許存取以取得詳細資料 AppClients
- 允許存取清單 AppClients
- 允許存取更新 AppClients
- 允許存取刪除 AppClients
- 允許存取授權應用程式
- 其他 IAM 政策範例
  - 允許使用者檢視他們自己的許可

政策最佳實務

以身分識別為基礎的政策會決定某人是否可以建立、存取或刪除您帳戶中的 AppFabric 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

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

使用 AppFabric 主控台

將受AWSAppFabricReadOnlyAccess AWS 管政策附加到您的 IAM 身分，以便授與 AppFabric 服務的唯讀權限，包括中的 AppFabric主控台 AWS Management Console。或者，您可以將AWSAppFabricFullAccess AWS 受管政策附加到 IAM 身分，以授予他們對 AppFabric 服務的完整管理權限。如需詳細資訊，請參閱 AWS 受管理的政策 AWS AppFabric。

AppFabric 如需安全性 IAM 政策範例

下列原則範例適用 AppFabric 於安全性功能。

允許存取應用程式套件

以下策略示例授予對 AppFabric服務中應用程序包的訪問權限。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

限制對應用程序包的訪問

以下策略示例限制對 AppFabric服務中應用程序包的訪問。

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

```
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

限制刪除或停止擷取

下列原則範例會限制服務中擷取的刪除或停止。 AppFabric

```
{
    "Statement": [
        {
            "Action": ["appfabric:*"],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StopIngestion",
                "appfabric:DeleteIngestion",
                "appfabric:DeleteIngestionDestination"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

AppFabric 以取得生產力 IAM 政策範例

AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

下列原則範例適用 AppFabric 於生產力功能。

允許存取生產力功能的唯讀存取權

下列原則範例授與生產力功能 AppFabric 的唯讀存取權。

> **Important**
>
> 在 IAM 主控台的 JSON 政策編輯器中新增此政策時，您可能會看到無效的動作錯誤。這是因 AppFabric 為生產力功能目前處於預覽狀態。您應該忽略錯誤並繼續建立原則。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppClient",
                "appfabric:ListActionableInsights",
                "appfabric:ListAppClients",
                "appfabric:ListMeetingInsights"
            ],
            "Resource": "*"
        }
    ],
    "Version": "2012-10-17"
}
```

完全存取生產力功能

下列原則範例授與 AppFabric 對於生產力功能的完整存取權。

> **Important**
>
> 在 IAM 主控台的 JSON 政策編輯器中新增此政策時，您可能會看到無效的動作錯誤。這是因 AppFabric 為生產力功能目前處於預覽狀態。您應該忽略錯誤並繼續建立原則。

```
{
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "appfabric:CreateAppClient",
                "appfabric:DeleteAppClient",
                "appfabric:GetAppClient",
                "appfabric:ListActionableInsights",
                "appfabric:ListAppClients",
                "appfabric:ListMeetingInsights",
                "appfabric:PutFeedback",
                "appfabric:Token"
                "appfabric:UpdateAppClient"
            ],
            "Resource": "*"
        }
    ],
    "Version": "2012-10-17"
}
```

允許存取以建立 AppClients

下列原則範例授與建立的存取權 AppClients。如需詳細資訊，請參閱建立 AppFabric 提高生產力 AppClient。

> **Important**
>
> 在 IAM 主控台的 JSON 政策編輯器中新增此政策時，您可能會看到無效的動作錯誤。這是因 AppFabric 為生產力功能目前處於預覽狀態。您應該忽略錯誤並繼續建立原則。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

允許存取以取得詳細資料 AppClients

下列政策範例授與取得詳細資料的存取權 AppClients。如需詳細資訊，請參閱取得 AppClient.

> **Important**
>
> 在 IAM 主控台的 JSON 政策編輯器中新增此政策時，您可能會看到無效的動作錯誤。這是因 AppFabric 為生產力功能目前處於預覽狀態。您應該忽略錯誤並繼續建立原則。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppClient",
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

允許存取清單 AppClients

下列原則範例會授與清單的存取權 AppClients。如需詳細資訊，請參閱取得 AppClient.

> **Important**
>
> 在 IAM 主控台的 JSON 政策編輯器中新增此政策時，您可能會看到無效的動作錯誤。這是因 AppFabric 為生產力功能目前處於預覽狀態。您應該忽略錯誤並繼續建立原則。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:ListAppClients"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
```

```
        }
    ],
    "Version": "2012-10-17"
}
```

允許存取更新 AppClients

下列原則範例會授與更新的存取權 AppClients。如需詳細資訊，請參閱更新 AppClient.

> **Important**
>
> 在 IAM 主控台的 JSON 政策編輯器中新增此政策時，您可能會看到無效的動作錯誤。這是因 AppFabric 為生產力功能目前處於預覽狀態。您應該忽略錯誤並繼續建立原則。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:UpdateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

允許存取刪除 AppClients

下列原則範例授與刪除的存取權 AppClients。如需詳細資訊，請參閱更新 AppClient.

> **Important**
>
> 在 IAM 主控台的 JSON 政策編輯器中新增此政策時，您可能會看到無效的動作錯誤。這是因 AppFabric 為生產力功能目前處於預覽狀態。您應該忽略錯誤並繼續建立原則。

```
{
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "appfabric:DeleteAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

允許存取授權應用程式

下列原則範例會授與使用 Token API 授權應用程式的存取權。如需詳細資訊，請參閱驗證和授權您的應用程式。

> **Important**
>
> 在 IAM 主控台的 JSON 政策編輯器中新增此政策時，您可能會看到無效的動作錯誤。這是因 AppFabric 為生產力功能目前處於預覽狀態。您應該忽略錯誤並繼續建立原則。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:Token"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

其他 IAM 政策範例

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
```

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

使用 AppFabric 的服務連結角色

AWS AppFabric 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到 AppFabric的唯一 IAM 角色類型。服務連結角色由預先定義， AppFabric 並包含服務代表您呼叫其他人所需 AWS 服務 的所有權限。

服務連結角色可讓您 AppFabric 更輕鬆地設定，因為您不需要手動新增必要的權限。 AppFabric 定義其服務連結角色的權限，除非另有定義，否則只 AppFabric 能擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這樣可以保護您的 AppFabric 資源，因為您無法不小心移除存取資源的權限。

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》，尋找服務連結角色欄中顯示為是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

AppFabric 的服務連結角色許可

AppFabric 使用名為的服務連結角色 `AWSServiceRoleForAppFabric` — AppFabric 允許將資料放入擷取目標資源中，例如 Amazon S3 儲存貯體或 Amazon Data Firehose 交付串流。它還允許將 AppFabric CloudWatch 指標數據放在`AWS/AppFabric`命名空間中。

`AWSServiceRoleForAppFabric` 服務連結角色信任下列服務以擔任角色：

- `appfabric.amazonaws.com`

名為的角色權限原則`AWSAppFabricServiceRolePolicy` AppFabric 允許對指定的資源完成下列動作：

- 動作：`cloudwatch:PutMetricData`在`AWS/AppFabric`命名空間中。此動作授與將指標資料放入 Amazon CloudWatch `AWS/AppFabric` 命名空間的權限。 AppFabric 如需有關中可用 AppFabric 測量結果的詳細資訊 CloudWatch，請參閱AWS AppFabric 使用 Amazon 監控 CloudWatch。
- 動作：`s3:PutObject`在 Amazon S3 存儲桶中。此動作授與將擷取的 AppFabric 資料放入您指定的 Amazon S3 儲存貯體的權限。
- 動作：`firehose:PutRecordBatch`在 Amazon 資料 Firehose 交付串流中。此動作授予將擷取的 AppFabric 資料放入您指定的 Amazon 資料 Firehose 交付串流的權限。

如需詳細資訊，請參閱的AWS 受管理原則 AppFabric。

您必須設定許可，以允許您的使用者、群組或角色建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

建立服務連結角色 AppFabric

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、或 AWS API 中建立 AppFabric 應用程式套件時 AWS CLI， AppFabric 會為您建立服務連結角色。

編輯下列項目的服務連結角色 AppFabric

AppFabric 不允許您編輯AWSServiceRoleForAppFabric服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除的服務連結角色 AppFabric

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。不過，您必須先刪除所有 AppFabric 應用程式套件，才能刪除服務連結角色。

清除服務連結角色

在您使用 IAM 刪除服務連結角色之前，您必須先刪除該角色所使用的任何資源。您在中建立的應用程式套件 AppFabric 會由角色使用。如需詳細資訊，請參閱 刪除 AWS AppFabric 安全性資源。

> **Note**
>
> 當您嘗試刪除資源時，如果 AppFabric 服務正在使用此角色，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。

手動刪除 服務連結角色

使用 IAM 主控台或 AWS API 刪除AWSServiceRoleForAppFabric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。

支援 AppFabric 服務連結角色的區域

AppFabric 支援在所有可用服務的 AWS 區域 地方使用服務連結角色。如需詳細資AppFabric 訊，請參閱 AWS 一般參考.

AWS 受管理的政策 AWS AppFabric

若要新增使用者、群組和角色的權限，使用 AWS 受管理的原則比自己撰寫原則更容易。建立 IAM 客戶受管政策需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可以使用我們的 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中使用。如需 AWS 受管政策的詳細資訊，請參閱 IAM 使用者指南中的AWS 受管政策。

AWS 服務 維護和更新 AWS 受管理的策略。您無法變更 AWS 受管理原則中的權限。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管理的政策移除權限，因此政策更新不會破壞您現有的權限。

此外，還 AWS 支援跨多個服務之工作職能的受管理原則。例如，ReadOnlyAccess AWS 受管理的策略提供對所有資源 AWS 服務 和資源的唯讀存取權。當服務啟動新功能時，會為新作業和資源新 AWS 增唯讀權限。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中有關任務職能的AWS 受管政策。

AWS 受管理策略：AWSAppFabricReadOnlyAccess

您可將 AWSAppFabricReadOnlyAccess 政策連接到 IAM 身分。此原則會授與 AppFabric 服務的唯讀權限。

> **Note**
>
> 此原AWSAppFabricReadOnlyAccess則不會 AppFabric 針對生產力功能授與唯讀存取權。

許可詳細資訊

此政策包含以下許可：

- appfabric— 授予獲取應用程序包，列出應用程序包，獲取應用程序授權，列出應用程序授權，獲取攝入，列出獲取目的地，列出獲取目的地以及列出資源標籤的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppAuthorization",
                "appfabric:GetAppBundle",
                "appfabric:GetIngestion",
                "appfabric:GetIngestionDestination",
                "appfabric:ListAppAuthorizations",
                "appfabric:ListAppBundles",
                "appfabric:ListIngestionDestinations",
```

```
                "appfabric:ListIngestions",
                "appfabric:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 受管理策略：AWSAppFabricFullAccess

您可將 AWSAppFabricFullAccess 政策連接到 IAM 身分。此原則會授與 AppFabric 服務的管理權限。

> **Important**
>
> 此AWSAppFabricFullAccess原則不會授與 AppFabric 對於生產力功能的存取權，因為它們目前處於預覽狀態。若要取得有關針對生產力功能進行存取權的更多 AppFabric 資訊，請參閱〈〉AppFabric 以取得生產力 IAM 政策範例。

許可詳細資訊

此政策包含以下許可：

- appfabric— 授予完整的管理權限 AppFabric。
- kms— 授予列出別名的權限。
- s3— 授予列出所有 Amazon S3 儲存貯體並取得儲存貯體位置的權限。
- firehose— 授予列出 Amazon 資料 Firehose 交付串流和描述交付串流的權限。
- iam— 授與建立AWSServiceRoleForAppFabric服務連結角色的權限。 AppFabric如需詳細資訊，請參閱 使用 AppFabric 的服務連結角色。

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

```
        {
            "Sid": "KMSListAccess",
            "Effect": "Allow",
            "Action": ["kms:ListAliases"],
            "Resource": "*"
        },
        {
            "Sid": "S3ReadAccess",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "FirehoseReadAccess",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:ListDeliveryStreams"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUseOfServiceLinkedRole",
            "Effect": "Allow",
            "Action": ["iam:CreateServiceLinkedRole"],
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "appfabric.amazonaws.com"}
            },
            "Resource": "arn:aws:iam::*:role/aws-service-role/appfabric.amazonaws.com/
AWSServiceRoleForAppFabric"
        }
    ]
}
```

AWS 受管理策略：AWSAppFabricServiceRolePolicy

您無法將 AWSAppFabricServiceRolePolicy 政策附加至 IAM 實體。此原則附加至服務連結角色，可 AppFabric 代表您執行動作。如需詳細資訊，請參閱 使用 AppFabric 的服務連結角色。

許可詳細資訊

此政策包含以下許可：

- `cloudwatch`— 授予將指標資料放入 Amazon CloudWatch `AWS/AppFabric` 命名空間的權限。AppFabric 如需有關中可用 AppFabric 測量結果的詳細資訊 CloudWatch，請參閱AWS AppFabric 使用 Amazon 監控 CloudWatch。
- `s3`— 授予將擷取資料放入您指定之 Amazon S3 儲存貯體的權限。 AppFabric
- `firehose`— 授予將擷取的 AppFabric 資料放入您指定的 Amazon 資料 Firehose 交付串流的權限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CloudWatchEmitMetric",
            "Effect": "Allow",
            "Action": ["cloudwatch:PutMetricData"],
            "Resource": "*",
            "Condition": {
                "StringEquals": {"cloudwatch:namespace": "AWS/AppFabric"}
            }
        },
        {
            "Sid": "S3PutObject",
            "Effect": "Allow",
            "Action": ["s3:PutObject"],
            "Resource": "arn:aws:s3:::*/AWSAppFabric/*",
            "Condition": {
                "StringEquals": {"s3:ResourceAccount": "${aws:PrincipalAccount}"}
            }
        },
        {
            "Sid": "FirehosePutRecord",
            "Effect": "Allow",
            "Action": ["firehose:PutRecordBatch"],
            "Resource": "arn:aws:firehose:*:*:deliverystream/*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/AWSAppFabricManaged":
 "true"}
            }
        }
    ]
}
```

AppFabric AWS 受管理策略的更新

檢視 AppFabric 自此服務開始追蹤這些變更以來的 AWS 受管理策略更新詳細資料。如需有關此頁面變更的自動警示，請訂閱「AppFabric 文件歷史記錄」頁面上的 RSS 摘要。

變更	描述	日期
AWSAppFabricReadOnlyAccess – 新政策	AppFabric 添加了一個新的策略，以授予 AppFabric服務只讀權限。	2023 年 6 月 27 日
AWSAppFabricFullAccess – 新政策	AppFabric 添加了一個新的策略，以授予 AppFabric 服務的管理權限。	2023 年 6 月 27 日
AWSAppFabricServiceRolePolicy – 新政策	AppFabric 新增`AWSServiceRoleForAppFabric` 服務連結角色的新原則。	2023 年 6 月 27 日
AppFabric 開始追蹤變更	AppFabric 開始追蹤其 AWS 受管理策略的變更。	2023 年 6 月 27 日

疑難排解 AWS AppFabric 身分和存取

使用下列資訊可協助您診斷和修正使用和 IAM 時可能會遇到的 AppFabric 常見問題。

主題

- 我沒有執行操作的授權 AppFabric
- 我未獲得執行 iam:PassRole 的授權
- 我想允許我以外的人訪 AWS 帳戶 問我的 AppFabric 資源

我沒有執行操作的授權 AppFabric

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在`mateojackson` IAM 使用者嘗試使用主控台檢視一個虛構 *`my-example-widget`* 資源的詳細資訊，但卻無虛構 `appfabric:`*`GetWidget`* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 appfabric:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 appfabric:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我未獲得執行 iam:PassRole 的授權

如果您收到未獲授權執行iam:PassRole動作的錯誤訊息，則必須更新您的原則以允許您將角色傳遞給 AppFabric。

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

當名為的 IAM 使用者marymajor嘗試使用主控台執行中的動作時，會發生下列範例錯誤 AppFabric。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪 AWS 帳戶 問我的 AppFabric 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要瞭解是否 AppFabric 支援這些功能，請參閱如何與 IAM AWS AppFabric 搭配使用。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 IAM 使用者指南中您擁有的另一個 AWS 帳戶 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。

- 若要了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源型政策的差異。

符合性驗證 AWS AppFabric

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

安全性最佳做法 AWS AppFabric

AWS AppFabric 在您開發和實作自己的安全性原則時，提供數項安全性功能供您考量。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

監控沒有管理員存取權的應用

透過唯讀 AWS Identity and Access Management (IAM) 權限，任何人都可以 AppFabric 與 Amazon QuickSight 及其他安全資訊和事件管理 (SIEM) 工具 (例如Splunk. 為了監控應用程式安全性，資料會傳送至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon 資料 Firehose 交付串流。

監控事 AppFabric 件

您可以 AppFabric 使用 Amazon CloudWatch 指標進行監控。 CloudWatch AppFabric 每分鐘收集資料，並將其處理為指標。您可以設定警示，以便在測量結果符合指定臨界值時設定通知。如需詳細資訊，請參閱 AWS AppFabric 使用 Amazon 監控 CloudWatch。

韌性在 AWS AppFabric

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎結構。

基礎架構安全性 AWS AppFabric

作為受管服務， AWS AppFabric 受 Amazon Web Services：安 AWS 全流程概觀白皮書中所述的全球網路安全程序保護。

您可以使用 AWS 已發佈的 API 呼叫透 AppFabric 過網路進行存取。用戶端必須支援 TLS 1.0 或更新版本。建議使用 TLS 1.2 或更新版本。用戶端也必須支援具備完美轉送私密 (PFS) 的密碼套件，例如臨時 Diffie-Hellman (DHE) 或橢圓曲線臨時 Diffie-Hellman (ECDHE)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，若要產生用於簽署要求的臨時安全登入資料，您可以使用 AWS Security Token Service(AWS STS)。

中的配置和漏洞分析 AWS AppFabric

配置和 IT 控制是與您（我們的客戶） AWS 之間的共同責任。如需詳細資訊，請參閱 AWS 共用的責任模型。

監控 AWS AppFabric

監控是維持其他 AWS 解決方案的可靠性、可用性和效能的 AWS AppFabric 重要組成部分。 AWS 提供下列監控工具來監視 AppFabric、在發生錯誤時回報，並在適當時自動採取行動：

- Amazon 會即時 CloudWatch監控您的 AWS 資源和執行 AWS 的應用程式。您可以收集和追蹤指標、建立自訂儀板表，以及設定警示，在特定指標達到您指定的閾值時通知您或採取動作。例如，您可以 CloudWatch 追蹤 Amazon EC2 執行個體的 CPU 使用率或其他指標，並在需要時自動啟動新執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。
- Amazon CloudWatch 日誌可讓您從 Amazon EC2 執行個體和其他來源監控 AWS CloudTrail、存放和存取日誌檔。 CloudWatch 記錄檔可以監控記錄檔中的資訊，並在符合特定臨界值時通知您。您也可以將日誌資料存檔在高耐用性的儲存空間。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南。
- AWS CloudTrail擷取由您或代表您發出的 API 呼叫和相關事件， AWS 帳戶 並將日誌檔傳遞到您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

AWS AppFabric 使用 Amazon 監控 CloudWatch

您可以 AWS AppFabric 使用監視器 CloudWatch，它收集原始數據並將其處理為可讀的近實時指標。這些統計資料會保留 15 個月，以便您存取歷史資訊，並更清楚 Web 應用程式或服務的執行效能。您也可以設定留意特定閾值的警示，當滿足這些閾值時傳送通知或採取動作。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

AppFabric 服務會在`AWS/AppFabric`命名空間中報告下列度量。

指標	描述
AppFabric 應用授權狀態	應用程序授權的狀態（用`1`於已連接；`0`對於任何其他）。
AppFabric 資料傳遞延遲	從 SaaS 應用程式收集稽核日誌並將其交付 AppFabric 到設定的目的地 (Amazon S3 或 Amazon Data Firehose) 所花費的時間 (以秒為單位)。

指標	描述
擷取目的地狀態	擷取目的地的狀態 (1適用於作用中；適用0於任何其他目的地)。
整體資料延遲	SaaS 應用程式上發生事件與對應稽核日誌交付至已設定目的地 (Amazon S3 或 Amazon Data Firehose) 之間的時差 (以秒為單位)。AppFabric
擷取資料量	交付到 Amazon 簡單存儲服務（Amazon S3）或亞馬遜數據 Firehose 的數據大小。

量度支援下列維 AppFabric 度。

維度	描述
擷取目的地 ARN	擷取目的地的 Amazon 資源名稱 (ARN)。

使用記錄 AWS AppFabric API 呼叫 AWS CloudTrail

AWS AppFabric 與提供使用者 AWS CloudTrail、角色或 AWS 服務 中所採取之動作記錄的服務整合 AppFabric。 CloudTrail 擷取 AppFabric 作為事件的所有 API 呼叫。擷取的呼叫包括來自 AppFabric 主控台的呼叫和 AppFabric API 作業的程式碼呼叫。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 AppFabric. 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 AppFabric、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。

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

AppFabric 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 AppFabric，該活動會與事件歷史記錄中的其他 CloudTrail AWS 服務 事件一起記錄在事件中。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱AWS CloudTrail 使用指南中的檢視具有 CloudTrail 事件歷程記錄的事件。

對於您的事件的持續記錄 AWS 帳戶，包括事件 AppFabric，請創建一個跟踪。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。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他， AWS 服務 以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南中的以下主題：

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

所有 AppFabric 動作均由「API 參考」記錄 CloudTrail 並記錄在「AWS AppFabric API 參考」中。例如，呼叫`CreateAppBundle`、`UpdateAppBundle`和`GetAppBundle`動作會在 CloudTrail 記錄檔中產生項目。

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

- 要求是使用根使用者登入資料還是 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。
- 該請求是否由另一項 AWS 服務服務提出。

若要取得更多資訊，請參閱《AWS CloudTrail 使用指南》中的CloudTrail userIdentity元素。

瞭解 AppFabric 記錄檔項目

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`CreateAppBundle`動作的 CloudTrail 記錄項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser",
```

```
        "arn": "arn:aws:sts::111122223333:assumed-role/AssumedRole/SampleUser",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAXUFER33B4FVC2GCYR",
                "arn": "arn:aws:iam::111122223333:role/AssumedRole",
                "accountId": "111122223333",
                "userName": "SampleUser"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-31T21:11:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-31T21:22:16Z",
    "eventSource": "appfabric.amazonaws.com",
    "eventName": "CreateAppBundle",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "3.90.81.91",
    "userAgent": "Coral/Apache-HttpClient5",
    "requestParameters": {
        "clientToken": "64d9069f-e565-49a4-9374-6dc8631142e2"
    },
    "responseElements": {
        "appBundle": {
            "arn": "arn:aws:appfabric:us-
east-1:111122223333:appbundle/6aa92da0-5eeb-4ff4-aabf-4db7fd022ad1",
            "idpClientConfiguration": {
                "samlAudience": "urn:amazon:cognito:sp:us-east-1_GEdGiavzr",
                "samlRedirect": "https://6aa92da0-5eeb-4ff4-aabf-4db7fd022ad1.auth.us-
east-1.amazoncognito.com/saml2/idpresponse",
                "oidcRedirect": "https://6aa92da0-5eeb-4ff4-aabf-4db7fd022ad1.auth.us-
east-1.amazoncognito.com/oauth2/idpresponse"
            }
        }
    },
    "requestID": "17e15a5d-8c66-46c7-ad5b-f521004fa9c2",
    "eventID": "ba1dd847-86f6-4386-85be-0398e844a358",
    "readOnly": false,
    "eventType": "AwsApiCall",
```

```
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "frontend.fabric.us-east-1.amazonaws.com"
    }
}
```

的配額 AWS AppFabric

您的每個配額都 AWS 帳戶 有預設配額 (先前稱為限制) AWS 服務。除非另有說明，否則每個配額都是區域特定規定。您可以請求提高某些配額，而其他配額無法提高。

若要檢視的配額 AppFabric，請開啟「Service Quotas」主控台。在功能窗格中，選擇AWS 服務並選取AppFabric。

若要請求提高配額，請參閱《Service Quotas 使用者指南》中的請求提高配額。如果 Service Quotas 中尚未提供配額，請使用增加服務配額表單。

與您的配額相關的配額 AWS 帳戶 如下表所示。 AppFabric

名稱	預設	可調整	描述
應用程式包	每個受支援的區域：1	否	您可以在目前 AWS 區域的帳戶中建立的應用程式套件數目上限。
應用程式授權	每個受支援的區域：50	否	您可以在目前 AWS 區域的帳戶中建立的應用程式授權數目上限。
攝取	每個受支援的區域：50	否	您可以在目前區域的帳戶中建立的擷取數目 AWS 上限。
擷取目的地	每個受支援的區域：5	否	目前區域中帳戶中每個擷取可建立的擷取目的地數目 AWS 上限。
AppClient	每個受支援的區域：1	否	您可以在當前 AWS 區域的 AppClients 帳戶中創建的最大數量。

名稱	預設	可調整	描述
			AWS AppFabric 針對生產力的功能已處於預覽狀態，可能會有所變更。

《 AppFabric 管理指南》的文件歷史記錄

下表說明的文件版本 AWS AppFabric。

變更	描述	日期
新支援的應用程	新增SentinelOne為支援的應用程式。如需詳細資訊，請參閱中的支援應用程式 AWS AppFabric。	2024年4月25日
新支援的應用程	新增1Password為支援的應用程式。如需詳細資訊，請參閱中的支援應用程式 AWS AppFabric。	2024年4月23 日
新支援的安全性工具	新增Dynatrace為相容的安全性工具。如需詳細資訊，請參閱相容安全性工具	2024年3月26日
新量度	新增「 AppFabric 應用程式授權狀態」度量。如需詳細資訊，請參閱AWS AppFabric 使用 Amazon CloudWatch 日誌進行監控。	2024年3月8日
新支援的應用程	新增IBM Security® Verify為支援的應用程式。如需詳細資訊，請參閱中的支援應用程式 AWS AppFabric。	2024年3月6日
新支援的應用程	新增Box為支援的應用程式。如需詳細資訊，請參閱中的支援應用程式 AWS AppFabric。	2024年2月28日
新支援的應用程式和指標	新增Cisco DuoSalesforce、和Terraform Cloud作為支援的應用程式。如需有關這	2024年2月1日

	些應用程式的詳細資訊，請參閱 AWS AppFabric。新增「資 AppFabric 料傳遞延遲」和「整體資料延遲」量度。如需詳細資訊，請參閱AWS AppFabric使用 Amazon CloudWatch 日誌進行監控。	
新增Atlassian Confluence、、Genesys Cloud、Hub SpotOneLogin by One IdentityPagerDuty、和Ping Identity作為支援的應用程式，並Barracuda XDR作為相容的安全性工具	如需有關新支援應用程式的詳細資訊，請參閱中的支援應用程式 AWS AppFabric和相容安全性工具。	2023 年 12 月 15 日
新增Atlassian Confluence、、Genesys Cloud、Hub SpotOneLogin by One IdentityPagerDuty、和Ping Identity作為支援的應用程式，並Barracuda XDR作為相容的安全性工具	如需有關新支援應用程式的詳細資訊，請參閱中的支援應用程式 AWS AppFabric和相容安全性工具。	2023 年 12 月 15 日
增加了生 AWS AppFabric 產力預覽文檔	如需提高生產力的 AppFabric 詳細資訊，請參閱何謂 AWS AppFabric 生產力？	2023 年 11 月 27 日
已新增GitHub並ServiceNow作為支援的應用	如需新支援應用程式的詳細資訊，請參閱支援的應用程式。	2023 年 10 月 31 日
開始追蹤 AWS 受管理的政策 AWS AppFabric	如需有關的 AWS 受管理原則的詳細資訊 AppFabric，請參閱的AWS 受管理原則 AWS AppFabric。	2023 年 6 月 27 日
初始版本	《 AWS AppFabric 管理指南》的初始版本。	2023 年 6 月 27 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。