管理指南

AWS AppFabric

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS AppFabric: 管理指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 is AWS AppFabric？ 1
產品 1
優勢 1
使用案例 1
AppFabric 的運作方式 2
定價 3
可用性 3
什麼是 is AWS AppFabric 安全？ 4
優勢 1
使用案例 1
存取 AppFabric 以確保安全 5
相關服務 5
OCSF 結構描述 6
AppFabric 中的 OCSF 型結構描述 6
先決條件和建議 7
註冊 AWS 帳戶 7
建立具有管理存取權的使用者 8
（必要） 完成應用程式先決條件 9
（選用） 建立輸出位置 10
（選用） 建立 AWS KMS 金鑰 11
開始使用 12
先決條件 12
步驟 1：建立應用程式套件 12
步驟 2：授權應用程式 14
步驟 3：設定稽核日誌擷取 15
步驟 4：使用使用者存取工具 17
步驟 5：連接 AppFabric 以取得安全工具和其他目的地中的安全資料 19
支援的應用程式 19
1Password 20
Asana 23
Azure Monitor 25
Atlassian Confluence 28
Atlassian Jira suite 31
Box 34

Cisco Duo 37
Dropbox 39
Genesys Cloud 42
GitHub 45
Google Analytics 48
Google Workspace 51
HubSpot 53
IBM Security® Verify 56
JumpCloud 為 AppFabric 設定 59
Microsoft 365 61
Miro 64
Okta 67
OneLogin 70
PagerDuty 73
Ping Identity 74
Salesforce 77
ServiceNow 81
Singularity Cloud 84
Slack 86
Smartsheet 90
Terraform Cloud 93
Webex by Cisco 95
Zendesk 98
Zoom 100
相容的安全工具 103
Barracuda XDR 104
Dynatrace 105
Logz.io 105
Netskope 106
NetWitness 107
QuickSight 108
Rapid7 109
Security Lake 110
Singularity Cloud 131
Splunk 132
刪除資源 133

刪除擷取目的地 133
刪除擷取 133
刪除應用程式授權 134
刪除應用程式套件 134
生產力的 is AWS AppFabric 是什麼？ 135
優勢 1
使用案例 1
存取 AppFabric 以提高生產力 5
應用程式開發人員入門 137
先決條件 12
步驟 1. 建立 AppFabric 以提高生產力 AppClient 138
步驟 2. 驗證和授權您的應用程式 140
步驟 3。將 AppFabric 使用者入口網站 URL 新增至您的應用程式 143
步驟 4. 使用 AppFabric 呈現跨應用程式洞見和動作 143
步驟 5. 請求 AppFabric 驗證您的應用程式 149
管理 AppClients 151
疑難排解 157
最終使用者入門 161
先決條件 12
步驟 1. 登入 AppFabric 162
步驟 2. 同意應用程式顯示洞見 164
步驟 3。連接您的應用程式以產生洞見和動作 165
步驟 4. 開始在您的應用程式中查看洞見並執行跨應用程式動作 168
管理存取 173
疑難排解 174
生產力 APIs的 AppFabric 177
動作 178
資料類型 192
常見錯誤 199
AppFabric 中的資料處理 199
靜態加密 199
傳輸中加密 200
術語與概念 201
安全 204
資料保護 204
靜態加密 205

傳輸中加密 205
金鑰管理 206
金鑰政策 206
AppFabric 如何在 中使用授予 AWS KMS 208
監控 AppFabric 的加密金鑰 209
身分與存取管理 211
目標對象 211
使用身分驗證 212
使用政策管理存取權 214
How AWS AppFabric 可與 IAM 搭配使用 216
身分型政策範例 222
使用服務連結角色 231
AWS 受管政策 233
故障診斷 238
法規遵循驗證 240
安全最佳實務 240
在沒有管理員存取權的情況下監控應用程式 241
監控 AppFabric 事件 241
恢復能力 241
基礎架構安全 241
組態與漏洞分析 241
監控 242
使用 CloudWatch 進行監控 242
CloudTrail 日誌 243
CloudTrail 中的 AppFabric 資訊 243
了解 AppFabric 日誌檔案項目 244
配額 247
文件歷史紀錄 249
..... cclii

什麼是 is AWS AppFabric？

AWS AppFabric 會快速將軟體即服務 (SaaS) 應用程式連接到整個組織，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，而員工可以使用生成式 AI 更快地完成日常任務。

主題

- 產品
- 優勢
- 使用案例
- AppFabric 的運作方式
- 定價
- 可用性

產品

探索 AWS AppFabric 的兩個面向：AppFabric 安全，旨在簡化管理和安全性，以及 AppFabric 生產力（預覽），透過生成式 AI 功能增強。如需詳細資訊，請參閱下列主題：

- 什麼是 is AWS AppFabric 安全？
- 生產力的 is AWS AppFabric 是什麼？

優勢

您可以使用 AppFabric 執行下列動作：

- 在幾分鐘內連接您的應用程式，並降低營運成本。
- 提高 SaaS 應用程式資料的可見性，以提升您的安全狀態。
- 使用生成式 AI 自動促進應用程式之間的任務。

使用案例

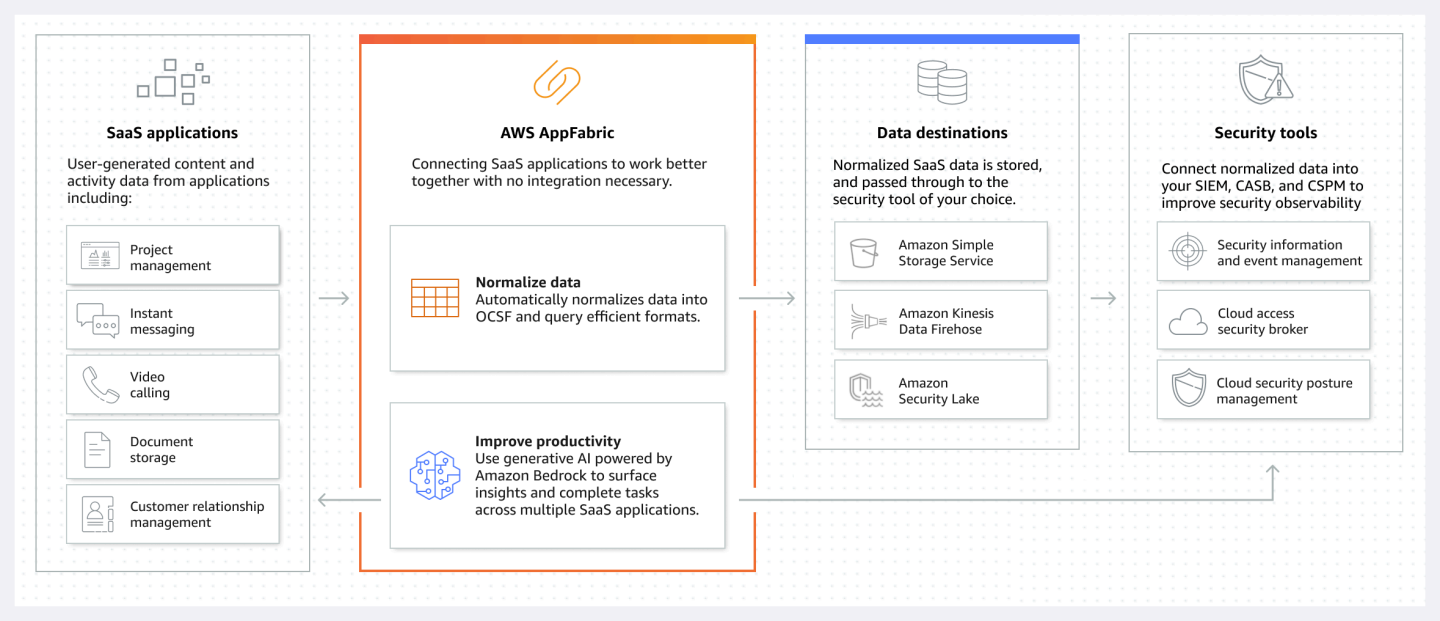
您可以使用 AppFabric 來：

- 快速連接您的 SaaS 應用程式

- AppFabric for security 以原生方式將最佳的 SaaS 生產力和安全應用程式相互連接，提供全受管的 SaaS 互通性解決方案。
- 提升您的安全狀態
  - 應用程式資料會自動標準化，讓管理員能夠設定常用政策、標準化安全提醒，以及輕鬆管理多個應用程式的使用者存取權。
- 重新構想生產力
  - AppFabric for productivity 是常見的生成式 AI 助理，可讓員工快速取得答案、自動化任務管理，並跨 SaaS 生產力應用程式產生洞見。

AppFabric 的運作方式

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



> **Note**
>
> AppFabric 的生產力目前以預覽形式啟動，並在美國東部（維吉尼亞北部）提供 AWS 區域。如需詳細資訊 AWS 區域，請參閱 中的 AWS AppFabric 端點和配額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 AppFabric AWS 區域和端點，請參閱 AWS 一般參考中的 AWS AppFabric 端點和配額。

什麼是 is AWS AppFabric 安全？

AWS AppFabric for security 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
- 使用案例
- 存取 AppFabric 以確保安全
- 相關服務
- 開啟網路安全結構描述架構 for AWS AppFabric
- use AWS AppFabric 的先決條件和建議
- 開始使用 AWS AppFabric 以確保安全
- AppFabric 中支援的應用程式以確保安全
- AppFabric 中的相容安全工具和服務，以確保安全
- 安全資源的 Delete AWS AppFabric

優勢

您可以使用 AppFabric 的安全性來執行下列動作：

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

使用案例

您可以使用 AppFabric 實現安全性，以：

- 快速連接您的 SaaS 應用程式
  - 用於安全性的 AppFabric 可原生將最佳的 SaaS 生產力和安全應用程式彼此連接，提供全受管的 SaaS 互通性解決方案。
- 提升您的安全狀態

- 應用程式資料會自動標準化，讓管理員能夠設定常見政策、標準化安全提醒，以及輕鬆管理多個應用程式的使用者存取權。

存取 AppFabric 以確保安全

AppFabric 的安全性已在美國東部（維吉尼亞北部）、歐洲（愛爾蘭）和亞太區域（東京）AWS 區域提供。如需詳細資訊 AWS 區域，請參閱《》中的 AWS AppFabric 端點和配額AWS 一般參考。

在每個區域中，您可以透過下列任何方式存取 AppFabric 以確保安全：

AWS Management Console

AWS Management Console 是以瀏覽器為基礎的界面，可用來建立和管理 AWS 資源。AppFabric 主控台可讓您存取 AppFabric 資源。您可以使用 AppFabric 主控台來建立和管理所有 AppFabric 資源。

AppFabric API

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

AWS Command Line Interface (AWS CLI)

使用 AWS CLI，您可以在系統的命令列發出命令，以與 AppFabric 和其他 互動 AWS 服務。如果您想要建置執行任務的指令碼，命令列工具也很有用。如需安裝和使用 的資訊 AWS CLI，請參閱 第 AWS Command Line Interface 2 版使用者指南。如需 AppFabric AWS CLI 命令的相關資訊，請參閱 參考的 AppFabric AWS CLI 區段。

相關服務

為安全起見，您可以 AWS 服務 搭配 AppFabric 使用下列項目：

Amazon Data Firehose

Amazon Data Firehose 是一種擷取、轉換和載入 (ETL) 服務，可可靠地擷取、轉換串流資料，並將資料交付至資料湖、資料存放區和分析服務。使用 AppFabric 時，您可以選擇以 JSON 格式將 Open Cybersecurity Schema Framework (OCSF) 標準化或原始稽核日誌輸出至 Firehose 串流做為目的地。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 提供者、內部部署和雲端來源的安全資料集中到您帳戶中存放的專用資料湖。您可以透過選取 Amazon Data Firehose 作為目的地，並設定 Firehose 在 Security Lake 中以正確的格式和路徑交付資料，將 AppFabric 稽核日誌資料與 Security Lake 整合。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 AppFabric 時，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

QuickSight 以超大規模的統一商業智慧 (BI) 為資料驅動型組織提供支援。透過 QuickSight，所有使用者都可以透過現代互動式儀表板、分頁報告、內嵌分析和自然語言查詢，滿足來自相同事實來源的不同分析需求。您可以選擇儲存 AppFabric 日誌做為來源的 Amazon S3 儲存貯體，以分析 QuickSight 中的 AppFabric 稽核日誌資料。如需詳細資訊，請參閱 QuickSight 使用者指南中的使用 Amazon S3 檔案建立資料集。您也可以將 Amazon S3 中的 AppFabric 資料匯入 Amazon Athena，然後選取 Amazon Athena 作為 QuickSight 中的資料來源。如需詳細資訊，請參閱 QuickSight 使用者指南中的使用 Amazon Athena 資料建立資料集。

AWS Key Management Service

使用 AWS Key Management Service (AWS KMS)，您可以跨應用程式和 建立、管理和控制密碼編譯金鑰 AWS 服務。當您在 AppFabric 中建立應用程式套件時，您可以設定加密金鑰以安全地保護授權的應用程式資料。此金鑰會加密 AppFabric 服務中的資料。AppFabric 可以代表您使用由 AppFabric AWS 擁有的金鑰 建立和管理的 ，或您建立和管理的客戶受管金鑰 AWS KMS。如需詳細資訊，請參閱建立 AWS KMS 金鑰。

開啟網路安全結構描述架構 for AWS AppFabric

Open Cybersecurity 結構描述架構 (OCSF) 是由網路安全產業中的 AWS 和 領導合作夥伴所共同努力的開放原始碼工作。OCSF 為常見安全事件提供標準結構描述、定義版本控制條件以促進結構描述演變，並包含安全日誌生產者和消費者的自我監督程序。OCSF 的公有原始碼託管在 GitHub 上。

AppFabric 中的 OCSF 型結構描述

安全 OCSF 1.1 型結構描述的 The AWS AppFabric 專為滿足您對軟體即服務 (SaaS) 產品組合的標準化、一致、低工作量可觀測性的需求而量身打造。AppFabric 會決定每個欄位和事件的正確映

射。AppFabric 與 OCSF 開放原始碼社群合作推出新的 OCSF 事件類別、事件類別、活動和物件，讓 OCSF 適用於 SaaS 應用程式事件。AppFabric 會自動標準化從 SaaS 應用程式收到的稽核事件，並將此資料交付至您 中的 Amazon Simple Storage Service (Amazon S3) 或 Amazon Data 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） 和兩個資料格式選項 (JSON 或 Parquet)。交付至 Firehose 時，您也可以選擇兩個標準化選項 (OCSF 或原始），但資料格式僅限於 JSON。

use AWS AppFabric 的先決條件和建議

如果您是新 AWS 客戶，請先完成此頁面列出的設定先決條件，再開始使用 AWS AppFabric 以確保安全。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 AWS 帳戶
- 建立具有管理存取權的使用者
- （必要） 完成應用程式先決條件
- （選用） 建立輸出位置
- （選用） 建立 AWS KMS 金鑰

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個。

註冊 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   註冊程序的一部分包括接聽電話或文字訊息，並在電話鍵盤上輸入驗證碼。

   當您註冊 時 AWS 帳戶，AWS 帳戶根使用者會建立 。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理存取權的使用者

註冊 後 AWS 帳戶，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center和建立管理使用者，以免將根使用者用於日常任務。

保護您的 AWS 帳戶根使用者

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

   如需說明，請參閱《IAM 使用者指南》中的為您的 AWS 帳戶 根使用者 （主控台） 啟用虛擬 MFA 裝置。

建立具有管理存取權的使用者

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 Identity Center 中，將管理存取權授予使用者。

   如需使用 IAM Identity Center 目錄 做為身分來源的教學課程，請參閱AWS IAM Identity Center《 使用者指南》中的使用預設值設定使用者存取 IAM Identity Center 目錄。

以具有管理存取權的使用者身分登入

- 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 Identity Center 使用者登入的說明，請參閱AWS 登入 《 使用者指南》中的登入 AWS 存取入口網站。

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的新增群組。

（必要）完成應用程式先決條件

若要使用 AppFabric 的安全性從應用程式接收使用者資訊和稽核日誌，許多應用程式會要求您有特定的角色和計劃類型。請確定您已檢閱您想要使用 AppFabric 授權的每個應用程式的先決條件，以確保安全，而且您擁有適當的計劃和角色。如需應用程式特定先決條件的詳細資訊，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 為 AppFabric 設定
- Asana 為 AppFabric 設定
- Azure Monitor 為 AppFabric 設定
- Atlassian Confluence 為 AppFabric 設定
- Atlassian Jira suite 為 AppFabric 設定
- Box 設定 AppFabric
- Cisco Duo 為 AppFabric 設定
- Dropbox 為 AppFabric 設定
- Genesys Cloud 為 AppFabric 設定
- GitHub 為 AppFabric 設定
- Google Analytics 為 AppFabric 設定
- Google Workspace 為 AppFabric 設定
- HubSpot 為 AppFabric 設定
- IBM Security® Verify 為 AppFabric 設定
- JumpCloud 為 AppFabric 設定
- 設定 AppFabric 的 Microsoft 365
- Miro 為 AppFabric 設定
- Okta 為 AppFabric 設定
- OneLogin by One Identity 為 AppFabric 設定
- PagerDuty 為 AppFabric 設定

- Ping Identity 為 AppFabric 設定
- Salesforce 為 AppFabric 設定
- ServiceNow 為 AppFabric 設定
- Singularity Cloud 為 AppFabric 設定
- Slack 為 AppFabric 設定
- Smartsheet 為 AppFabric 設定
- Terraform Cloud 為 AppFabric 設定
- Webex by Cisco 為 AppFabric 設定
- Zendesk 為 AppFabric 設定
- Zoom 為 AppFabric 設定

（選用）建立輸出位置

AppFabric for security 支援 Amazon Simple Storage Service (Amazon S3) 和 Amazon Data Firehose 作為稽核日誌擷取目的地。

Amazon S3

您可以在建立擷取目的地時使用 AppFabric 主控台建立新的 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，您必須在建立 AppFabric 擷取目的地之前建立儲存貯體，然後在建立擷取目的地時選取儲存貯體。您可以選擇在 中使用現有的 Amazon S3 儲存貯體 AWS 帳戶，只要其符合下列現有儲存貯體的要求：

- 基於安全考量AppFabric 需要您的 Amazon S3 儲存貯體與 Amazon S3 資源位於相同的 AWS 區域中。
- 您可以使用下列其中一項來加密儲存貯體：
  - 使用 Amazon S3 受管金鑰 (SSE-S3) 的伺服器端加密
  - 使用 default AWS Key Management Service (AWS KMS) 搭配 () 金鑰 (SSE-KMS) 的伺服器端加密 AWS 受管金鑰 `aws/s3`。

Amazon Data Firehose

您可以選擇使用 Amazon Data Firehose 做為 AppFabric 的安全資料的擷取目的地。若要使用 Firehose，您可以在建立擷取 AWS 帳戶 之前或在 AppFabric 中建立擷取目的地時，在 中建立

Firehose 交付串流。您可以使用 AWS Management Console、 AWS CLI或 AWS APIs 或 SDKs 建立 Firehose 交付串流。如需串流組態指示，請參閱下列主題：

- AWS Management Console 指示 – 《Amazon Data Firehose 開發人員指南》中的建立 Amazon Data Firehose 交付串流
- AWS CLI 指示 – 在 AWS CLI 命令參考create-delivery-stream中
- AWS APIs和 SDKs說明 – 請參閱《Amazon Data Firehose API 參考CreateDeliveryStream》中的

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

- 您必須在與安全資源 AppFabric AWS 區域 相同的 中建立串流。
- 您必須選取直接 PUT 做為來源。
- 將 AmazonKinesisFirehoseFullAccess AWS 受管政策連接至您的使用者，或將下列許可連接至您的使用者：

```
{
    "Sid": "TagFirehoseDeliveryStream",
    "Effect": "Allow",
    "Action": ["firehose:TagDeliveryStream"],
    "Condition": {
        "ForAllValues:StringEquals": {"aws:TagKeys": "AWSAppFabricManaged"}
    },
    "Resource": "arn:aws:firehose:*:*:deliverystream/*"
}
```

Firehose 支援與各種第三方安全工具整合，例如 Splunk和 Logz.io。如需有關如何正確設定 Amazon Kinesis 以便將資料輸出到這些工具的資訊，請參閱《Amazon Data Firehose 開發人員指南》中的目的地設定。

（選用）建立 AWS KMS 金鑰

在為安全應用程式套件建立 AppFabric 的過程中，您將選取或設定加密金鑰，以安全地保護資料不受所有授權應用程式影響。此金鑰將用於加密 AppFabric 服務中的資料。

安全 AppFabric 預設會加密資料。安全 AppFabric 可以使用 AppFabric 代表您建立和管理的 AWS 擁有的金鑰 ，或您在 AWS Key Management Service () 中建立和管理的客戶受管金鑰AWS KMS。AWS 擁有的金鑰 是 AWS 服務 擁有和管理的 AWS KMS 金鑰集合，可用於多個 AWS 帳戶。客戶受

管金鑰是您 AWS 帳戶 建立、擁有和管理的 AWS KMS 金鑰。如需 AWS 擁有的金鑰 和客戶受管金鑰的詳細資訊，請參閱《 AWS Key Management Service 開發人員指南》中的客戶金鑰和 AWS 金鑰。

如果您想要在 AppFabric 內使用客戶受管金鑰來加密資料，例如授權字符，為了安全起見，您可以使用 建立一個金鑰AWS KMS。如需授予存取客戶受管金鑰之許可政策的詳細資訊 AWS KMS，請參閱本指南的金鑰政策一節。

開始使用 AWS AppFabric 以確保安全

若要開始使用 AWS AppFabric 以確保安全，您必須先建立應用程式套件，然後授權應用程式套件並將其連線至您的應用程式套件。將應用程式授權連接到應用程式後，您可以使用 AppFabric 進行安全功能，例如稽核日誌擷取和使用者存取。

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

主題

- 先決條件
- 步驟 1：建立應用程式套件
- 步驟 2：授權應用程式
- 步驟 3：設定稽核日誌擷取
- 步驟 4：使用使用者存取工具
- 步驟 5：連接 AppFabric 以取得安全工具和其他目的地中的安全資料

先決條件

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 AWS 帳戶及建立具有管理存取權的使用者。

步驟 1：建立應用程式套件

應用程式套件會存放所有 AppFabric 以進行安全應用程式授權和擷取。若要建立應用程式套件，請設定加密金鑰以安全地保護您的授權應用程式資料。

1. 在 https：//https://console.aws.amazon.com/appfabric/ 開啟 AppFabric 主控台。
2. 在頁面右上角的選取區域選擇器中，選取 AWS 區域。AppFabric 僅適用於美國東部（維吉尼亞北部）、歐洲（愛爾蘭）和亞太區域（東京）區域。
3. 選擇 Getting started (入門)。

4. 在入門頁面上，針對步驟 1。建立應用程式套件，選擇建立應用程式套件。
5. 在加密區段中，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影響。此金鑰用於加密 AppFabric 中的安全服務資料。

   安全 AppFabric 預設會加密資料。AppFabric 可以代表您使用由 AppFabric AWS 擁有的金鑰 建立和管理的 ，也可以使用您在 () 中 AWS Key Management Service 建立和管理的客戶受管金鑰 AWS KMS。
6. 針對AWS KMS 金鑰，選擇使用或 AWS 擁有的金鑰客戶受管金鑰。

   如果您選擇使用客戶受管金鑰，請輸入您要使用的現有金鑰的 Amazon Resource Name (ARN) 或金鑰 ID，或選擇建立 AWS KMS 金鑰。

   選擇 AWS 擁有的金鑰 或客戶受管金鑰時，請考慮下列事項：

   - AWS 擁有的金鑰 是 AWS 服務 擁有和管理用於多個 的 AWS Key Management Service (AWS KMS) 金鑰集合 AWS 帳戶。雖然 AWS 擁有的金鑰 不在您的 中 AWS 帳戶，但 AWS 服務 可以使用 AWS 擁有的金鑰 來保護您帳戶中的資源。 AWS 擁有的金鑰 不計入 AWS KMS 您帳戶的配額。您不需要建立或維護金鑰或其金鑰政策。的輪換會因服務 AWS 擁有的金鑰 而異。如需 AWS 擁有的金鑰 針對 AWS AppFabric 輪換 的相關資訊，請參閱靜態加密。
   - 客戶受管金鑰是您建立、擁有和管理 AWS 帳戶 之 中的 KMS 金鑰。您可以完全控制這些 AWS KMS 金鑰。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、輪換其密碼編譯材料、新增標籤、建立參考 AWS KMS 金鑰的別名，以及排定要刪除的 AWS KMS 金鑰。客戶受管金鑰會出現在 AWS Management Console 的客戶受管金鑰頁面上 AWS KMS。

     若要明確識別客戶受管金鑰，請使用 `DescribeKey`操作。對於客戶受管金鑰，`DescribeKey` 回應的 `KeyManager` 欄位值是 `CUSTOMER`。您可以在密碼編譯操作中使用客戶受管金鑰，並在 AWS CloudTrail 日誌中稽核用量。透過與 整合 AWS 服務 的許多 AWS KMS，您可以指定客戶受管金鑰來保護為您存放和管理的資料。客戶受管金鑰會產生月費，以及超過 AWS 免費方案的使用費。客戶受管金鑰會計入您帳戶的 AWS KMS 配額。

   如需 AWS 擁有的金鑰 和客戶受管金鑰的詳細資訊，請參閱《 AWS Key Management Service 開發人員指南》中的客戶金鑰和 AWS 金鑰。

   > **Note**
   >
   > 建立應用程式套件時，AppFabric for Security 也會在 AWS 帳戶 稱為 AppFabric 服務連結角色 (SLR) 的 中建立特殊 IAM 角色。它允許服務將指標傳送至 Amazon CloudWatch。

新增稽核日誌目的地之後，SLR 允許 AppFabric 存取您的 AWS 資源 (Amazon S3 儲存貯體、Amazon Data Firehose 交付串流）。如需詳細資訊，請參閱使用 AppFabric 的服務連結角色。

7. （選用）對於標籤，您可以選擇將標籤新增至應用程式套件。標籤是金鑰值對，可將中繼資料指派給您建立的資源。如需詳細資訊，請參閱AWS 《標籤編輯器使用者指南》中的標記您的 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

成功建立應用程式套件後，您現在可以授權 AppFabric 進行安全連線，並與每個應用程式互動。授權的應用程式會加密並存放在您的應用程式套件中。若要為每個應用程式套件設定多個應用程式授權，請視需要為每個應用程式重複應用程式授權步驟。

在開始授權應用程式的步驟之前，請在 中檢閱和驗證每個應用程式的先決條件，例如所需的計劃類型AppFabric 中支援的應用程式以確保安全。

1. 在入門頁面上，針對步驟 2。授權應用程式，選擇建立應用程式授權。
2. 在應用程式授權區段中，從應用程式下拉式清單中選取您要授予 AppFabric 安全連線許可的應用程式。顯示的應用程式是 AppFabric 目前支援的應用程式，以確保安全。
3. 當您選取應用程式時，會顯示必要的資訊欄位。這些欄位包含租戶 ID 和租戶名稱，也可能包含用戶端 ID、用戶端秘密或個人存取字符。這些欄位的輸入值因應用程式而異。如需如何尋找這些值的詳細應用程式特定指示，請參閱 AppFabric 中支援的應用程式以確保安全。
4. （選用）對於標籤，您可以選擇將標籤新增至應用程式授權。標籤是金鑰值對，可將中繼資料指派給您建立的資源。如需詳細資訊，請參閱AWS 《標籤編輯器使用者指南》中的標記您的 AWS 資源。
5. 選擇建立應用程式授權。
6. 如果出現快顯視窗（取決於正在連線的應用程式），請選取允許 授權 AppFabric 以與您的應用程式連線。

   如果您的應用程式授權成功，您會在入門頁面上看到連線的應用程式授權成功訊息。
7. 您可以在導覽窗格中列出的應用程式授權頁面上，於每個應用程式的狀態下，隨時檢查應用程式授權的狀態。連線狀態表示您的應用程式授權已授予 AppFabric 以安全連線至應用程式，且已完成。
8. 下表顯示可能的應用程式授權狀態，包括您可以採取來修正相關錯誤的疑難排解步驟。

狀態名稱	狀態描述	疑難排解步驟
待定	狀態為待定表示應用程式的應用程式授權已建立，但 AppFabric 的安全性尚未連線到應用程式。	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連線，以啟動連線。如果此錯誤仍然存在，請檢查瀏覽器的快顯封鎖程式是否已停用。如果快顯視窗中有任何錯誤訊息，例如 400 個錯誤請求，請檢查所有資訊，例如租用戶 ID、用戶端 ID 和用戶端秘密，是否已正確輸入。也可能會無法正確建立應用程式的應用程式授權。如需詳細資訊，請參閱支援的應用程式。
連線驗證失敗	連線驗證狀態失敗表示 AppFabric 安全功能無法驗證應用程式授權與應用程式的連線。	檢查是否已針對應用程式授權正確輸入所有資訊，例如租戶 ID、用戶端 ID 和用戶端秘密。
字符自動輪換失敗	權杖自動輪換失敗的狀態表示應用程式授權成功連線後，OAuth 重新整理權杖已失敗。	如果此錯誤仍然存在，請檢查應用程式的身分驗證應用程式。如需詳細資訊，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：設定稽核日誌擷取

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日誌擷取。稽核日誌擷取會使用授權應用程式的稽核日誌，並將其標準化為開放式網路安全結構描述架構 (OCSF)。然後將它們交付到其中的一或多個目的地 AWS。您也可以選擇將原始 JSON 檔案交付至目的地。

1. 在入門頁面上，針對步驟 3。設定稽核日誌擷取區段，選取擷取快速設定。

> **Note**
>
> 為了加快設定速度，請使用擷取快速設定頁面，只能從入門頁面存取，以相同的擷取目的地一次為多個應用程式授權建立擷取。例如，相同的 Amazon S3 儲存貯體或 Amazon Data Firehose 資料串流。
>
> 您也可以從擷取頁面建立擷取，可從導覽窗格存取。在擷取頁面上，您可以一次設定一個擷取到不同的目的地。在擷取頁面上，您也可以為擷取建立標籤。下列指示適用於擷取快速設定頁面。

2. 針對選取應用程式授權，選取您要為其建立稽核日誌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使用 AppFabric 建立應用程式授權的應用程式租用戶名稱，以確保安全。
3. 對於新增目的地，為您選取的應用程式選取稽核日誌擷取的目的地。目的地選項包括 Amazon S3 - 現有儲存貯體、Amazon S3 - 新儲存貯體或 Amazon Data Firehose。如果您選取多個租用戶名稱，您選擇的目的地會套用至應用程式授權的每個擷取。
4. 當您選擇目的地時，會顯示其他必要欄位。
   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 儲存貯體名稱。如需如何建立 Amazon S3 儲存貯體的詳細資訊，請參閱建立輸出目的地。
   b. 如果您選擇 Amazon S3 — 現有的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 Data 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。如需如何建立 Amazon Data Firehose 交付串流的更多說明，請參閱建立輸出目的地，並記下 AppFabric 所需的許可政策以確保安全。
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 - JSON、OCSF - JSON、OCSF - Parquet Amazon S3 儲存貯體，或原始 - JSON 或 OCSF-JSON for Firehose。

   原始資料格式提供從資料字串轉換為 JSON 的稽核日誌資料。OCSF 資料格式會將稽核日誌資料標準化為 AppFabric，以實現安全性開放式網路安全結構描述架構 (OCSF) 結構描述。如需 AppFabric 如何使用 OCSF 的詳細資訊，請參閱 開啟網路安全結構描述架構 for AWS AppFabric。您一次只能為擷取選擇一個結構描述和格式資料類型。如果您想要新增額外的結構描述和格式資料類型，您可以透過重複擷取建立程序來設定額外的擷取目的地。
6. （選用）如果您想要將標籤新增至擷取，請從導覽窗格前往擷取頁面。若要前往擷取詳細資訊頁面，請選取租戶名稱。對於標籤，您可以選擇將標籤新增至擷取。標籤是金鑰值對，可將中繼資

料指派給您建立的資源。如需詳細資訊，請參閱AWS 《標籤編輯器使用者指南》中的標記您的 AWS 資源。

7. 選擇設定擷取。

   當您成功設定擷取時，您會在入門頁面上看到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。啟用您擷取的狀態表示您的擷取已啟用。如果您在此頁面選擇應用程式授權的租戶名稱，您可以看到該應用程式授權的詳細資訊頁面，包括目的地詳細資訊和狀態。擷取目的地的狀態為作用中，表示目的地設定正確且作用中。如果應用程式授權的狀態為已連線，且擷取目的地狀態為作用中，則應該處理並交付稽核日誌。如果應用程式授權狀態或擷取目的地狀態是任何失敗狀態，即使啟用擷取狀態，也不會處理或交付稽核日誌。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，其中包含您可以採取的故障診斷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，以啟用擷取。
失敗	擷取目的地的失敗狀態表示擷取目的地不接受稽核日誌。例如，此狀態可能會因完整的儲存位置而發生。	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 AppFabric 進行安全使用者存取工具，安全與 IT 管理員團隊可以使用員工的公司電子郵件地址執行簡單的搜尋，快速查看誰可以存取特定應用程式。此方法有助於減少使用者取消佈建等任務所花費的時間，這些任務可能需要手動檢查或稽核使用者跨 SaaS 應用程式的存取權。如果找到使用者，AppFabric for security 會提供應用程式中的使用者名稱及其應用程式內使用者狀態（例如，Active)，如果應用程式提供的話。AppFabric 用於安全搜尋應用程式套件中的所有授權應用程式，以傳回使用者可存取的應用程式清單。

1. 在入門頁面上，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，您會看到使用者可存取的所有授權應用程式清單。若要在應用程式中顯示使用者名稱及其狀態（如果可用），請選取搜尋結果。
4. 在搜尋結果欄中找到的使用者訊息表示使用者可以存取列出的應用程式。下表顯示可能的搜尋結果、錯誤，以及您可以採取以解決錯誤的動作。

搜尋結果	描述
找不到使用者	找不到使用電子郵件地址的使用者。
找不到授權字符。連接應用程式的應用程式授權。	檢查是否已針對應用程式授權正確輸入所有資訊，例如租戶 ID、用戶端 ID 和用戶端秘密。
授權字符已撤銷。連接應用程式的應用程式授權。	檢查是否已針對應用程式授權正確輸入所有資訊，例如租戶 ID、用戶端 ID 和用戶端秘密。
我們無法輪換授權字符。連接應用程式的應用程式授權。	OAuth 重新整理字符在應用程式授權成功連線後失敗。如果此錯誤仍然存在，請檢查應用程式的身分驗證應用程式。如需詳細資訊，請參閱支援的應用程式。
找不到所需的許可。連接應用程式的應用程式授權。	檢查是否已針對應用程式授權正確輸入所有資訊，例如租戶 ID、用戶端 ID 和用戶端秘密。
應用程式授權無效。	檢查是否已針對應用程式授權正確輸入所有資訊，例如租戶 ID、用戶端 ID 和用戶端秘密。
由於許可不足，我們無法呼叫應用程式 API。	檢查是否已針對應用程式授權正確輸入所有資訊，例如租戶 ID、用戶端 ID 和用戶端秘密。
已超過應用程式請求限制。	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。
應用程式遇到內部伺服器錯誤	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。

搜尋結果	描述
應用程式尚未準備好處理請求	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請求錯誤。	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。
應用程式遇到服務無法使用錯誤。	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：連接 AppFabric 以取得安全工具和其他目的地中的安全資料

AppFabric 的標準化（或原始）應用程式資料與任何支援從 Amazon S3 擷取資料並與 Firehose 整合的工具相容，包括 Barracuda XDR、Dynatrace、、Rapid7、、 Logz.io Netskope NetWitness和 等安全工具Splunk，或您的專屬安全解決方案。若要從 AppFabric 取得標準化（或原始）應用程式資料，請遵循先前的步驟 1 到 3。如需如何設定特定安全工具和服務的詳細資訊，請參閱相容的安全工具和服務。

AppFabric 中支援的應用程式以確保安全

AWS AppFabric for Security 支援與下列應用程式整合。選擇應用程式的名稱，以取得如何設定 AppFabric 以安全連線至應用程式的詳細資訊。

主題

- 1Password 為 AppFabric 設定
- Asana 為 AppFabric 設定
- Azure Monitor 為 AppFabric 設定
- Atlassian Confluence 為 AppFabric 設定
- Atlassian Jira suite 為 AppFabric 設定
- Box 設定 AppFabric
- Cisco Duo 為 AppFabric 設定
- Dropbox 為 AppFabric 設定
- Genesys Cloud 為 AppFabric 設定
- GitHub 為 AppFabric 設定

- Google Analytics 為 AppFabric 設定
- Google Workspace 為 AppFabric 設定
- HubSpot 為 AppFabric 設定
- IBM Security® Verify 為 AppFabric 設定
- JumpCloud 為 AppFabric 設定
- 設定 AppFabric 的 Microsoft 365
- Miro 為 AppFabric 設定
- Okta 為 AppFabric 設定
- OneLogin by One Identity 為 AppFabric 設定
- PagerDuty 為 AppFabric 設定
- Ping Identity 為 AppFabric 設定
- Salesforce 為 AppFabric 設定
- ServiceNow 為 AppFabric 設定
- Singularity Cloud 為 AppFabric 設定
- Slack 為 AppFabric 設定
- Smartsheet 為 AppFabric 設定
- Terraform Cloud 為 AppFabric 設定
- Webex by Cisco 為 AppFabric 設定
- Zendesk 為 AppFabric 設定
- Zoom 為 AppFabric 設定

1Password 為 AppFabric 設定

1Password 是一種密碼管理器，可協助您為所有線上帳戶建立、存放和使用高強度密碼。它還透過加密保護您的資料、提醒您違規，並允許您共用密碼。

您可以使用 AWS AppFabric 進行安全性稽核1Password，以將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 1Password
- 將 AppFabric 連接到1Password您的帳戶

的 AppFabric 支援 1Password

AppFabric 支援從 接收使用者資訊和稽核日誌1Password。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸1Password到支援的目的地，您必須符合下列要求：

- 您必須擁有有效的付費1Password商業或企業訂閱計劃。如需詳細資訊，請參閱 1Password 網站上的 1Password Enterprise。
- 您必須在1Password帳戶中擁有管理員角色或團隊擁有者。如需詳細資訊，請參閱 1Password支援網站上的群組。

速率限制考量

1Password AuditLog Events API 會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 參考中的 API 速率限制。

資料延遲考量

您可能會看到稽核事件延遲最多 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級自訂。如需協助，請聯絡 支援。

將 AppFabric 連接到1Password您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabric1Password。若要尋找1Password使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立個人1Password存取權杖

1Password 支援公有用戶端的個人存取字符。請完成下列步驟，以產生個人存取字符。

1. 登入 1Password 帳戶。
2. 在導覽窗格中選擇整合。
3. 如果現有的整合存在，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，輸入您的安全資訊和事件管理 (SIEM) 系統名稱 （例如 AppFabric Secure)
6. 選擇新增整合，然後完成設定字符頁面中的下列步驟。

   a. 提供要在 AppFabric 安全環境中使用的字符名稱。
   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 會在過期時間過後1Password撤銷權杖。
   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. 選擇儲存並完成1Password下列步驟。
   a. 標題會根據您的系統和字符名稱自動填入。
   b. 在選取保存庫下選擇私有。
   c. 選擇 Save (儲存)。

如需詳細資訊，請參閱 1Password 網站上的1Password事件報告入門。

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。AppFabric 中的租戶 ID 將是您的1Password登入地址。請完成下列步驟以尋找您的租戶 ID。

1. 登入 1Password 帳戶。
2. 在導覽窗格中選擇 Settings (設定)。
3. 您的1Password登入會列在 頁面上。例如，https：//example-account.1password.com。

租戶名稱

輸入可識別此唯一1Password組織的名稱。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。

服務帳戶字符

您必須擁有服務帳戶的服務1Password帳戶字符，才能進入 AppFabric 1Password 應用程式授權。如果您沒有服務帳戶字符，請使用下列指示：

AppFabric 將請求服務帳戶字符。AppFabric 中的服務帳戶字符是您建立的個人存取字符。請完成1Password 入口網站中的下列步驟，以尋找個人存取字符。

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. 選擇檢視保存庫。
6. 選擇權杖名稱。

用戶端授權

使用租戶 ID、租戶名稱和服務帳戶字符在 AppFabric 中建立應用程式授權。然後選擇連線以啟用授權。

Asana 為 AppFabric 設定

Asana 是一種工作管理平台，可協助個人、團隊和組織協調工作，從日常任務到跨職能策略計劃。它提供了一個清晰的活體系統，讓每個人都可以進行通訊、協作和協調工作。使用 Asana，團隊會將關鍵商業工具整合到一個位置，因此無論工作在何處發生，工作都會向前邁進。

您可以針對安全性使用 AWS AppFabric 來稽核 的日誌和使用者資料Asana、將資料標準化為開放網路安全結構描述架構 (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。

主題

- 的 AppFabric 支援 Asana
- 將 AppFabric 連接到Asana您的帳戶

的 AppFabric 支援 Asana

AppFabric 支援從 接收使用者資訊和稽核日誌Asana。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Asana到支援的目的地，您必須符合下列要求：

- 您必須擁有具有 的企業帳戶Asana。如需建立或升級至Asana企業帳戶的詳細資訊，請參閱 Asana 網站上的Asana企業。
- Asana 您的帳戶中必須有具有超級管理員角色的使用者。如需角色的詳細資訊，請參閱 Asana 網站上的 中的管理員和超級管理員角色Asana。

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 和現有Asana應用程式的組合超過限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件延遲最多 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連接到Asana您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricAsana。若要尋找Asana使用 AppFabric 授權所需的資訊，請使用下列步驟。

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。AppFabric 中的租用戶 ID 稱為 中的網域 IDAsana。若要尋找網域 ID，請使用Asana主畫面中的下列指示：

1. 選擇您的帳戶設定檔圖片，然後選取管理員主控台。
2. 然後選取設定。
3. 捲動至網域設定。
4. 將本節中的網域 ID 輸入 AppFabric 租用戶 ID 組態。

租戶名稱

輸入可識別此唯一Asana組織的名稱。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。

服務帳戶字符

您必須擁有服務帳戶的服務Asana帳戶字符，才能進入 AppFabric Asana 應用程式授權。如果您沒有服務帳戶字符，請使用下列指示：

1. 若要建立服務帳戶，請遵循 Asana 指南網站上的服務帳戶中的指示。
2. 當您第一次檢視新增服務帳戶頁面時，請從新增服務帳戶頁面底部複製並儲存權杖。

3. 如果您在儲存權杖之前關閉新增服務帳戶頁面，則必須編輯您的服務帳戶、產生新的權杖並儲存它。

Azure Monitor 為 AppFabric 設定

Azure Monitor 是一種全面的監控解決方案，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。它可協助您了解應用程式的效能，並可讓您以手動和程式設計方式回應系統事件。

Azure Monitor 會跨多個 Azure 和非 Azure 訂閱和租用戶，從系統的每個 layer 和元件收集和彙總資料。它會將其存放在常見的資料平台中，以供一組可以關聯、分析、視覺化和/或回應資料的常用工具使用。您也可以整合其他 Microsoft 和非 Microsoft 工具。Azure Monitor 活動日誌是一種平台日誌，可讓您深入了解訂閱層級事件。活動日誌包含修改資源或啟動虛擬機器等資訊。

為了安全起見，您可以使用 AWS AppFabric 從 稽核日誌和使用者資料Azure Monitor、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Azure Monitor
- 將 AppFabric 連線至Azure Monitor您的帳戶

的 AppFabric 支援 Azure Monitor

AppFabric 能夠從下列Azure Monitor服務接收使用者資訊和稽核日誌：

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

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Azure Monitor到支援的目的地，您必須符合下列要求：

- 您需要擁有具有免費試用或pay-as-you-go訂閱Microsoft Azure的帳戶。
- 至少需要一個訂閱才能擷取該訂閱中的事件。

速率限制考量

Azure Monitor 會對提出請求的安全委託人（使用者或應用程式）和訂閱 ID 或租戶 ID 強加速率限制。如需 Azure Monitor API 速率限制的詳細資訊，請參閱 Azure Monitor開發人員網站上的了解 如何 Azure Resource Manager調節請求。

資料延遲考量

您可能會看到稽核事件最多延遲 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Azure Monitor您的帳戶

在 AppFabric 服務中建立應用程式套件之後，您必須使用 授權 AppFabricAzure Monitor。若要尋找 Azure Monitor使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

AppFabric Azure Monitor使用 OAuth2 與 整合。完成下列步驟以在 中建立 OAuth2 應用程式Azure Monitor：

1. 導覽至Microsoft Azure入口網站並登入。
2. 導覽至 Microsoft Entra ID。
3. 選擇應用程式註冊。
4. 在新註冊時選擇 。
5. 輸入用戶端的名稱，例如 OAuth Azure Monitor 用戶端。這將是已註冊應用程式的名稱。
6. 確認支援的 帳戶類型設定為單一租用戶。
7. 針對重新導向 URI，選取 Web 做為平台，並新增重新導向 URI。針對重新導向 URI 使用下列格式：

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

   在該地址中， *<region>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。

   成功驗證使用者之後，身分驗證回應將傳送至提供的 URI。現在提供此功能是選用的，稍後可以變更，但大多數身分驗證案例都需要值。

8. 選擇註冊。
9. 在已註冊的應用程式中，選擇憑證和秘密，然後選擇新用戶端秘密。
10. 新增秘密的描述。
11. 選取秘密過期持續時間。您可以從下拉式清單中選取任何預設的持續時間，或設定自訂持續時間。
12. 選擇新增。用戶端秘密值只能在建立後立即檢視。離開頁面之前，請務必將秘密存放在安全的地方。

所需的許可

您必須將下列許可新增至 OAuth 應用程式。若要新增許可，請遵循《 Microsoft Entra開發人員指南》的新增許可一節中的指示來存取您的 Web API。

- Microsoft Graph 使用者存取 API > User.Read.All （選取委派類型）
- Microsoft Graph 使用者存取 API > offline_access （選取委派類型）
- Azure 服務管理稽核日誌 API > user_impersonation （選取委派類型）

新增許可後，若要授予管理員許可的同意，請遵循《 Microsoft Entra開發人員指南》的管理員同意按鈕一節中的指示。

應用程式授權

AppFabric 支援從Azure Monitor您的帳戶接收使用者資訊和稽核日誌。若要從 接收稽核日誌和使用者資料Azure Monitor，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Azure Monitor中命名，另一個在應用程式授權下拉式清單中命名為Azure Monitor稽核日誌。您可以對這兩個應用程式授權使用相同的租用戶 ID、用戶端 ID 和用戶端秘密。若要從 接收稽核日誌Azure Monitor，您需要 Azure Monitor和 Azure Monitor Audit Logs 應用程式授權。若要單獨使用使用者存取工具，只需要Azure Monitor應用程式授權。

租用戶 ID

AppFabric 將請求您的租戶 ID。請完成下列步驟，以在 Azure Monitor 中尋找您的用戶端 ID：

1. 導覽至 Microsoft Azure 入口網站。
2. 導覽至 Azure Active Directory。
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 （租戶） ID 欄位複製租戶 ID。

租戶名稱

輸入可識別此唯一Azure Monitor訂閱的名稱。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。

> **Note**
>
> 租戶名稱最多應為 2，048 個字元，由數字、小寫/大寫字母和下列特殊字元組成：句點 (.)、底線 (_)、破折號 (-) 和空格。

用戶端 ID

AppFabric 將請求用戶端 ID。完成下列程序，在 中尋找您的用戶端 IDAzure Monitor：

1. 導覽至 Microsoft Azure 入口網站。
2. 導覽至 Azure Active Directory。
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 將請求用戶端秘密。已註冊 OAuth 應用程式的用戶端秘密是您在 OAuth 應用程式建立區段的步驟 11 中產生的秘密。如果您誤置在建立 OAuth 應用程式期間產生的用戶端秘密，請重複 OAuth 應用程式建立區段中的步驟 8-11，以重新產生新的秘密。

應用程式授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗Microsoft Azure以核准授權。從視窗登入您的帳戶，然後選擇允許來核准 AppFabric 授權。

Atlassian Confluence 為 AppFabric 設定

在一個地方建立、協作和組織您的所有工作。 Confluence 是知識和協作相遇的團隊工作空間。動態頁面可讓您的團隊建立、擷取和協作任何專案或想法。Spaces 可協助您的團隊建構、組織和共用工作，因此每個團隊成員都能了解機構知識，並存取他們執行最佳工作所需的資訊。

為了安全起見，您可以使用 AWS AppFabric 從 接收稽核日誌和使用者資料Confluence、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Atlassian Confluence
- 將 AppFabric 連線至Atlassian Confluence您的帳戶

的 AppFabric 支援 Atlassian Confluence

AppFabric 支援從 接收稽核日誌Atlassian Confluence。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Atlassian Confluence到支援的目的地，您必須符合下列要求：

- 若要存取稽核日誌，您需要有標準、高級或企業帳戶。如需建立或升級至適用Confluence計劃類型的詳細資訊，請參閱 Atlassian 網站上的 Confluence 定價。
- 若要存取稽核日誌，您需要擁有帳戶的管理員許可。如需角色的詳細資訊，請參閱Atlassian支援網站上的授予使用者管理員許可。

速率限制考量

Confluence 會對 Atlassian Confluence API 強加速率限制。如果 AppFabric 和現有 Atlassian Confluence API 應用程式的組合超過 的限制，AppFabric 中出現Atlassian Confluence的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件最多延遲 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Atlassian Confluence您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricAtlassian Confluence。若要尋找Atlassian Confluence使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

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

1. 導覽至Atlassian開發人員主控台。

2. 在右上角選擇您的設定檔圖示，然後選擇開發人員主控台。
3. 在我的應用程式旁邊，選擇建立、OAuth 2.0 整合。
4. 在左側導覽窗格中選擇許可，然後選擇 Confluence API 旁的新增。
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) 旁的新增。
8. 在回呼 URL 文字方塊中使用具有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>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。

必要範圍

您必須將下列其中一個範圍新增至 Atlassian Confluence OAuth 應用程式。如需範圍的詳細資訊，請參閱 Atlassian開發人員網站上的 OAuth 2.0 (3LO) 和 Forge 應用程式的範圍。使用可用的傳統範圍。

- Classic 範圍：
  - `read:confluence-user`
- 精細範圍：
  - `read:audit-log:confluence`

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。AppFabric 中的租戶 ID 是您的Atlassian Confluence執行個體子網域。您可以在 https：// 和 ..net 之間的瀏覽器地址列中找到Atlassian Confluence執行個體子網域。atlassian

租戶名稱

輸入可識別此唯一Atlassian Confluence組織的名稱。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 將請求用戶端 ID。若要在 中尋找您的用戶端 IDAtlassian Confluence，請使用下列步驟：

1. 導覽至Atlassian開發人員主控台。
2. 在右上角選擇您的設定檔圖示，然後選擇開發人員主控台、我的應用程式。
3. 選取您用來連接 AppFabric 的 OAuth 應用程式。
4. 從設定頁面將用戶端 ID 輸入 AppFabric 中的用戶端 ID 欄位。

Client secret (用戶端密碼)

AppFabric 將請求用戶端秘密。若要在 中尋找您的用戶端秘密Atlassian Confluence，請使用下列步驟：

1. 導覽至Atlassian開發人員主控台。
2. 在右上角選擇您的設定檔圖示，然後選擇開發人員主控台、我的應用程式。
3. 選取您用來連接 AppFabric 的 OAuth 應用程式。
4. 從設定頁面將秘密輸入 AppFabric 中的用戶端秘密欄位。

核准授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗Atlassian Confluence以核准授權。若要核准 AppFabric 授權，請選擇允許。

Atlassian Jira suite 為 AppFabric 設定

Atlassian 釋放每個團隊的潛力。他們的敏捷性和 DevOps、IT 服務管理和工作管理軟體可協助團隊組織、討論和完成共用工作。全球大多數的 Fortune 500 和超過 240，000 家各種規模的公司，包括 NASA、Deutsche Bank、 Kiva和 Salesforce ，都依賴Atlassian解決方案來協助團隊更好地合作，並及時交付高品質的結果。進一步了解 Atlassian產品，包括 Jira Software、Confluence、Bitbucket、、Jira Service Management Trello和 Jira Align Atlassian。

為了安全起見，您可以使用 AWS AppFabric 從 Jira suite(除外Jira Align) 稽核日誌和使用者資料、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Jira suite
- 將 AppFabric 連線至Jira您的帳戶

的 AppFabric 支援 Jira suite

AppFabric 支援從 接收使用者資訊和稽核日誌Jira suite，但 除外Jira Align。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Jira suite到支援的目的地，您必須滿足下列要求：

- 您必須擁有 Jira Standard Plan 或更高版本。如需有關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。
- Jira 您的帳戶中必須有具有 Organization 管理員角色的使用者。如需角色的詳細資訊，請參閱Atlassian支援網站上的授予使用者管理員許可。

速率限制考量

Jira 套件會對 Jira API 強加速率限制。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 和現有 Jira API 應用程式的組合超過限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件最多延遲 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Jira您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricJira。若要尋找Jira使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

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

1. 導覽至Atlassian開發人員主控台。
2. 在我的應用程式旁邊，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 旁的新增。
5. 在回呼 URL 欄位中，使用具有下列格式的 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 設定 AppFabric 應用程式套件的 程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。
6. 導覽至設定區段，複製您的用戶端 ID 和用戶端秘密，並將其儲存為用於 AppFabric 應用程式授權。

必要範圍

您必須將下列範圍新增至 Jira OAuth 應用程式的許可頁面：

- 在傳統範圍下：
  - Jira API > `read:jira-user`
- 在精細範圍下：
  - Jira API > `read:audit-log:jira`
  - Jira API > `read:user:jira`

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。AppFabric 中的租戶 ID 是您的Jira執行個體子網域。您可以在瀏覽器的網址列中找到Jira執行個體子網域，介於 https：// 和 .net 之間atlassian。

租戶名稱

輸入可識別此唯一Jira伺服器的名稱。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 會請求您的用戶端 ID。若要在 Jira 中尋找您的用戶端 ID，請使用下列步驟：

1. 導覽至 Atlassian 開發人員主控台。

2. 選取您用來連接 AppFabric 的 OAuth 應用程式。
3. 從設定頁面將用戶端 ID 輸入 AppFabric 中的用戶端 ID 欄位。

Client secret (用戶端密碼)

AppFabric 將請求您的用戶端秘密。AppFabric 中的用戶端秘密是 中的秘密Jira。若要在 中尋找您的秘密Jira，請使用下列步驟：

1. 導覽至Atlassian開發人員主控台。
2. 選取您用來連接 AppFabric 的 OAuth 應用程式。
3. 從設定頁面將秘密輸入 AppFabric 中的用戶端秘密欄位。

核准授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗Jira，以核准授權。若要核准 AppFabric 授權，請選擇允許。

Box 設定 AppFabric

Box 是領先的內容雲端，這是一個單一平台，可讓組織管理整個內容生命週期、安全地從任何地方工作，並跨同best-of-breed應用程式整合。

您可以使用 AWS AppFabric 從 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結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Box
- 將 AppFabric 連接到Box您的帳戶

的 AppFabric 支援 Box

AppFabric 支援從 接收使用者資訊和稽核日誌Box。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Box到支援的目的地，您必須符合下列要求：

- 若要存取稽核日誌，您需要主動訂閱 Business、Business Plus、Enterprise 或 Enterprise Plus 計劃。
- 您必須擁有具有管理員權限的使用者。
- Box 您的帳戶必須啟用 2 因素身分驗證，才能從組態索引標籤檢視和複製應用程式的用戶端秘密。

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 和現有Box應用程式的組合超過限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會在稽核事件中看到最多 30 分鐘的延遲，以交付至目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級上自訂。如需協助，請聯絡支援。

將 AppFabric 連接到Box您的帳戶

在 AppFabric 服務中建立應用程式套件後，您需要使用 授權 AppFabricBox。若要尋找Box使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

AppFabric Box使用 OAuth 與 整合。使用下列步驟在 中建立 OAuth 應用程式Box，如需詳細資訊，請參閱在 Box 網站上建立 OAuth 應用程式。

1. 登入 Box並前往 開發人員主控台。
2. 選擇建立新應用程式。
3. 從應用程式類型清單中選擇自訂應用程式。模態會出現，提示選取下一個步驟。
4. 輸入應用程式名稱和描述。
5. 從用途下拉式清單中選擇整合。
   a. 從類別下拉式清單中選擇安全與合規。
   b. 在您要整合AWS AppFabric Secure的外部系統中輸入 ？文字方塊。
6. 如果您想要使用用戶端 ID 和用戶端秘密驗證應用程式身分，請選擇伺服器身分驗證（用戶端憑證授予）。
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。
10. 在頁面的應用程式範圍區段中，選擇管理使用者和管理企業屬性。
11. 選擇 Save Changes (儲存變更)。

    Box 管理員必須先在Box管理員主控台中授權應用程式，才能使用應用程式。完成下列步驟以請求授權。

    a. 在開發人員主控台中為您的應用程式選擇授權索引標籤。
    b. 選擇檢閱和提交，將電子郵件傳送給您的Box企業管理員進行核准。如需詳細資訊，請參閱Box指南中的授權。

    > **Note**
    > 如果在提交之後進行任何變更，您必須重新提交您的應用程式。

必要範圍

需要下列應用程式範圍。如需範圍的詳細資訊，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 將請求租戶 ID。AppFabric 中的租戶 ID 是Box企業 ID。Box 企業 ID 可在 admin 主控台的帳戶與帳單 > 帳戶資訊 > 企業 ID 下找到。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. 登入 Box並前往 開發人員主控台。

2. 在導覽功能表中選擇我的應用程式。
3. 選擇您用來連接 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 登入資料區段。
6. 在 AppFabric 的用戶端 ID 欄位中輸入 OAuth 用戶端 ID。
7. 選擇擷取用戶端秘密。
8. 將 OAuth 用戶端秘密中的用戶端秘密輸入 AppFabric 中的用戶端秘密欄位。

Cisco Duo 為 AppFabric 設定

Cisco Duo 使用領先的存取管理套件來防止違規，該套件提供強大的多層防禦和創新功能，允許合法使用者進入 並防止惡意行為者進入。對於任何擔心遭到違規且需要快速解決方案的組織， 可Cisco Duo快速提高安全性，同時提高使用者生產力。

為了安全起見，您可以使用 AWS AppFabric 從 接收稽核日誌和使用者資料Cisco Duo、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Cisco Duo
- 將 AppFabric 連接至Cisco Duo您的帳戶

的 AppFabric 支援 Cisco Duo

AppFabric 支援從 接收使用者資訊和稽核日誌Cisco Duo。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Cisco Duo到支援的目的地，您必須符合下列要求：

- 若要存取稽核日誌，您需要有 Duo Essentials、Duo Advantage 或 Duo Premier 版本的作用中訂閱。或者，具有 Advantage 或 Premier 試用的新客戶也可以存取。如需Cisco Duo版本的詳細資訊，請參閱版本和定價。
- 您必須是具有擁有者角色的管理員，才能建立或修改 Admin API。
- 您需要新增授予讀取日誌資源的許可，才能存取管理員 API 中的稽核日誌。

速率限制考量

Cisco Duo 會對 Cisco Duo API 強加速率限制。如需 Cisco Duo API 速率限制的詳細資訊，請參閱身分驗證日誌下的速率限制。如果 AppFabric 和現有 Cisco Duo API 應用程式的組合超過 的限制，AppFabric 中出現Cisco Duo的稽核日誌可能會延遲。如果您需要提高速率限制，請聯絡 Cisco Duo。

資料延遲考量

您可能會看到稽核事件延遲最多 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連接至Cisco Duo您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricCisco Duo。若要尋找Cisco Duo使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 Cisco Duo Admin API 應用程式

AppFabric Cisco Duo使用 API 服務字符與 整合。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 Admin API 應用程式，請遵循 Cisco Duo Admin API 中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您的Cisco Duo應用程式：

- 授予讀取日誌
- 授予讀取資源

應用程式授權

租用戶 ID

AppFabric 將請求租戶 ID。您可以在Cisco Duo主機名稱中找到租戶 ID。若要在 中尋找主機名稱Cisco Duo，請遵循下列步驟。

1. 導覽至Cisco Duo管理員登入頁面並登入。

2. 導覽至應用程式，然後選擇保護應用程式。
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，以設定您的應用程式並取得您的 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 ID。

租戶名稱

輸入可識別此唯一Cisco Duo組織的名稱。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。

服務字符

AppFabric 將請求服務字符。服務字符是以冒號分隔的整合金鑰和私密金鑰，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. 導覽至應用程式，然後選擇保護應用程式。
3. 「按一下保護應用程式，並在應用程式清單中尋找 Admin API 的項目。按一下最右邊的保護以設定應用程式。向下捲動至範圍區段，然後新增 **`Grant read log`**和 **`Grant read resource`**。

Dropbox 為 AppFabric 設定

Dropbox 有助於您的組織更快速地完成更好的工作，方法是將人員集合在一起，無論他們正在處理什麼工作、在哪裡工作，或他們使用哪種工具。它可讓使用者透過提供簡單、安全的方式來共用內容，來加速創新和效率。 Dropbox 是讓生活井然有序並持續工作的地方。擁有超過 7 億註冊使用者，遍及 180 個國家/地區，Dropbox致力於設計更啟發的工作方式。

為了安全起見，您可以使用 AWS AppFabric 從 稽核日誌和使用者資料Dropbox、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Dropbox

- 將 AppFabric 連線至Dropbox您的帳戶

的 AppFabric 支援 Dropbox

AppFabric 支援從 接收使用者資訊和稽核日誌Dropbox。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Dropbox到支援的目的地，您必須滿足下列要求：

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

速率限制考量

Dropbox 會對 Dropbox API 強加速率限制。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 和現有 Dropbox API 應用程式的組合超過限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件最多延遲 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Dropbox您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricDropbox。若要尋找Dropbox使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

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

1. 在 https：// 的應用程式主控台中選擇建立Dropbox應用程式。 https://www.dropbox.com/developers/apps
2. 在新的應用程式組態頁面上，選擇 API 的範圍存取。

3. 接著，針對存取類型選取完整Dropbox。
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URIs重新導向 URL。

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

   在此 URL 中， *<region>*是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。
6. 選擇新增。
7. 複製並儲存您的應用程式金鑰和應用程式秘密，以用於 AppFabric 應用程式授權。
8. 您可以在設定索引標籤上保留所有其他欄位及其預設值。

必要範圍

您必須使用Dropbox應用程式資訊畫面上的許可索引標籤，將下列範圍新增至應用程式：

- `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 將請求您的租戶 ID。輸入任何可唯一識別您Dropbox帳戶的值，例如團隊名稱。

租戶名稱

輸入可識別此唯一Dropbox帳戶的名稱。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 將請求用戶端 ID。AppFabric 中的用戶端 ID 是您的Dropbox應用程式金鑰。若要尋找您的 Dropbox 應用程式金鑰，請使用下列步驟：

1. 導覽至Dropbox位於 https：//https://www.dropbox.com/developers/apps 的應用程式主控台。
2. 尋找您用來連接 AppFabric 的應用程式。
3. 在應用程式資訊頁面的狀態區段中尋找應用程式金鑰。
4. 在 AppFabric 的用戶端 ID 欄位中輸入Dropbox您應用程式的應用程式金鑰。

Client secret (用戶端密碼)

AppFabric 將請求用戶端秘密。AppFabric 中的用戶端秘密是您的Dropbox應用程式秘密。若要尋找您的Dropbox應用程式秘密，請使用下列步驟：

1. 導覽至Dropbox位於 https：//https://www.dropbox.com/developers/apps 的應用程式主控台。
2. 尋找您用來連接 AppFabric 的應用程式。
3. 在應用程式資訊頁面的狀態區段中尋找應用程式秘密。
4. 在 AppFabric 的 Client Secret 欄位中輸入Dropbox您應用程式的應用程式秘密。

核准授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗Dropbox，以核准授權。若要核准 AppFabric 授權，請選擇允許。

Genesys Cloud 為 AppFabric 設定

Genesys Cloud 在簡單的all-in-one界面中跨數位和語音管道建立流暢對話。這可讓公司為員工和客戶提供卓越的體驗，並享有快速部署、降低複雜性和簡單管理的優勢。

您可以使用安全性 AWS AppFabric 從 接收稽核日誌和使用者資料Genesys Cloud、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Genesys Cloud
- 將 AppFabric 連線至Genesys Cloud您的帳戶

的 AppFabric 支援 Genesys Cloud

AppFabric 支援從 接收使用者資訊和稽核日誌Genesys Cloud。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Genesys Cloud到支援的目的地，您必須符合下列要求：

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

速率限制考量

Genesys Cloud 會對 Genesys Cloud API 強加速率限制。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

您可能會看到稽核事件延遲最多 30 分鐘交付至目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Genesys Cloud您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricGenesys Cloud。若要尋找 Genesys Cloud使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

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

1. 請遵循 Genesys Cloud 資源中心網站上的建立 OAuth 用戶端中的指示。

   針對授予類型，選擇程式碼授權。
2. 使用具有下列格式的重新導向 URL 做為授權重新導向 URIs。

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

   在此 URL 中，*<region>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。

3. 選取範圍方塊以顯示您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會建立用戶端 ID 和用戶端秘密 （ 金鑰 ）。

必要範圍

您必須將下列範圍新增至 Genesys Cloud OAuth 應用程式：

- `audits:readonly`
- `users:readonly`

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。AppFabric 中的租戶 ID 是您的Genesys Cloud執行個體名稱。您可以在瀏覽器的地址列中找到您的租戶 ID。例如， `usw2.pure.cloud` 是下列 URL 中的租戶 IDhttps://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 會請求用戶端 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 ID。

Client secret (用戶端密碼)

AppFabric 將請求用戶端秘密。若要在 中尋找您的用戶端秘密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 用戶端以取得用戶端秘密。

GitHub 為 AppFabric 設定

GitHub 是使用 Git 進行軟體開發和版本控制的平台和雲端服務，可讓開發人員存放和管理其程式碼。它為每個專案提供 Git plus 存取控制、錯誤追蹤、軟體功能請求、任務管理、持續整合和 wiki 的分散式版本控制。

為了安全起見，您可以使用 AWS AppFabric 從 接收稽核日誌和使用者資料GitHub、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 GitHub
- 將 AppFabric 連線至GitHub您的帳戶

的 AppFabric 支援 GitHub

AppFabric 支援從 接收使用者資訊和稽核日誌GitHub。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸GitHub到支援的目的地，您必須滿足下列要求：

- 若要存取稽核日誌，您需要擁有 企業帳戶。
- 若要存取企業稽核日誌，您需要擁有企業帳戶的管理員角色。
- 若要從組織取得稽核日誌，您必須是組織擁有者。

速率限制考量

GitHub 會對 GitHub API 強加速率限制。如需 GitHub API 速率限制的詳細資訊，請參閱 GitHub 網站上的 API 請求限制和配置。如果 AppFabric 和現有 GitHub API 應用程式的組合超過GitHub’s限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件最多延遲 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至GitHub您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricGitHub。若要尋找GitHub使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

AppFabric GitHub使用 OAuth 與 整合。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 GitHub 網站上的建立 GitHubs 應用程式。

1. 選擇位於頁面右上角的設定檔相片，然後選擇設定。
2. 在左側導覽窗格中選擇開發人員設定。
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**
   >
   > 如果您先前尚未建立 OAuth 應用程式，此按鈕會標記為註冊新應用程式。

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執行個體 URL。
7. （選用）在應用程式描述文字方塊中輸入應用程式的描述。使用者將看到此描述。
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>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。
9. 如果您的 OAuth 應用程式將使用裝置流程來識別和授權使用者，請選擇啟用裝置流程。如需裝置流程的詳細資訊，請參閱 GitHub 網站上的授權 OAuth 應用程式。
10. 選擇註冊應用程式。

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。租用戶 ID 應以下列其中一種格式提供：

企業稽核日誌：

如果您想要了解企業帳戶擁有的所有組織的彙總動作，請使用企業的稽核日誌。

若要使用企業稽核日誌，租戶 ID 是您帳戶的企業 ID。您可以在瀏覽器的地址列中找到您的企業 ID。例如，*exampleenterprise*是下列 URL 中的企業 IDhttps://github.com/settings/enterprises/*examplenterprise*。

當您為企業稽核日誌指定租用戶 ID 時，必須以 為字首enterprise:。因此，請將先前的範例指定為enterprise:examplenterprise。

組織稽核日誌：

如果您想要了解組織成員執行的動作，請使用組織的稽核日誌做為組織管理員。它包含詳細資訊，例如執行動作的人員、動作的內容，以及執行動作的時間。

若要使用組織稽核日誌，租戶 ID 是您的組織 ID。您可以在瀏覽器的地址列中找到您的組織 ID。例如，*exampleorganization* 是下列 URL 中的組織 IDhttps://github.com/settings/organizations/*exampleorganization*。

當您為組織稽核日誌指定租戶 ID 時，必須以 為字首organization:。因此，請將先前的範例指定為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 將請求用戶端 ID。使用下列步驟在 中尋找您的用戶端 IDGitHub，

1. 選擇位於頁面右上角的設定檔相片，然後選擇設定。
2. 在左側導覽窗格中選擇開發人員設定。
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 ID 值。

Client secret (用戶端密碼)

AppFabric 將請求用戶端秘密。使用下列步驟在 中尋找您的用戶端秘密GitHub。

1. 選擇位於頁面右上角的設定檔相片，然後選擇設定。
2. 在左側導覽窗格中選擇開發人員設定。
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，然後尋找用戶端秘密值。如果您找不到現有的用戶端秘密，則可能需要產生新的秘密。

核准授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗GitHub，以核准授權。若要核准 AppFabric 授權，請選擇允許。

如果啟用 OAuth 應用程式存取限制，請確定您的組織已授予 OAuth 應用程式的存取權。

Google Analytics 為 AppFabric 設定

Google Analytics 是一種 Web 分析服務，可提供統計資料和基本分析工具，用於搜尋引擎最佳化 (SEO) 和行銷目的。 Google Analytics 用於追蹤網站效能並收集訪客洞見。它可協助組織判斷使用者流量的主要來源、衡量行銷活動和行銷活動的成功、追蹤目標完成（例如購買、將產品新增至購物車）、探索使用者參與度的模式和趨勢，以及取得人口統計等其他訪客資訊。中小型零售網站通常使用 Google Analytics 來取得和分析各種客戶行為分析，這些分析可用於改善行銷活動、推動網站流量，以及更好地保留訪客。

為了安全起見，您可以使用 AWS AppFabric 從 稽核日誌和使用者資料Azure Monitor、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Google Analytics
- 將 AppFabric 連線至Google Analytics您的帳戶

的 AppFabric 支援 Google Analytics

AppFabric 支援從 接收稽核日誌Google Analytics。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Google Analytics到支援的目的地，您必須符合下列要求：

- 您必須是 Google Analytics帳戶的管理員。
- 若要讓 AppFabric 交付日誌，您需要在Google Cloud專案上啟用 Google Analytics Admin API。設定 Google AnalyticsOAuth 應用程式時，請務必使用新的專案。

速率限制考量

Google Analytics 會對 Google Analytics API 強加速率限制。如需 Google Analytics API 速率限制的詳細資訊，請參閱 Google Analytics 網站上的限制和配額。如果 AppFabric 和現有 Google Analytics API 應用程式的組合超過限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件最多延遲 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Google Analytics您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricGoogle Analytics。使用下列步驟來尋找Google Analytics使用 AppFabric 授權所需的資訊。

建立 OAuth 應用程式

AppFabric Google Analytics使用 OAuth 與 整合。完成下列步驟以在 中建立 OAuth 應用程式Google Analytics：

1. 若要設定 OAuth 同意畫面，請遵循 Google 網站上的 Google 開發人員指南中設定 OAuth 同意畫面的指示。
2. 為使用者類型選擇外部
3. 若要設定 AppFabric 的 OAuth 登入資料，請遵循 Google 開發人員指南中建立存取登入資料頁面的 OAuth 用戶端 ID 登入資料一節中的指示。
4. 使用具有下列格式的重新導向 URL。

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

   在該地址中， *<region>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。

必要範圍

您必須將下列範圍新增至 Google Analytics OAuth 應用程式：

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

應用程式授權

租用戶 ID

AppFabric 將請求租戶 ID。AppFabric 中的租戶 ID 是Google Analytics您的帳戶 ID。

1. 前往 Google Analytics 首頁。
2. 在導覽窗格中選擇管理員。
3. 您可以在帳戶 > 帳戶設定 > 帳戶詳細資訊 > 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 將請求用戶端 ID。使用下列步驟在 中尋找您的用戶端 IDGoogle Analytics：

1. 前往登入資料頁面。
2. 在 OAuth 2.0 用戶端 IDs區段中，選擇您建立的用戶端 ID。
3. 用戶端 ID 會列在頁面的其他資訊區段中。

Client secret (用戶端密碼)

AppFabric 將請求用戶端秘密。使用下列步驟在 中尋找您的用戶端秘密Google Analytics：

1. 前往登入資料頁面。
2. 在 OAuth 2.0 用戶端 IDs區段中，選擇用戶端名稱。
3. 用戶端秘密會列在頁面的用戶端秘密區段中。

應用程式授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗Google Analytics以核准授權。選擇允許來核准 AppFabric 授權。

Google Workspace 為 AppFabric 設定

Google Workspace 是由 Google 開發和行銷的雲端運算、生產力和協作工具、軟體和產品的集合。

為了安全起見，您可以使用 AWS AppFabric 從 稽核日誌和使用者資料Google Workspace、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Google Workspace
- 將 AppFabric 連線至Google Workspace您的帳戶

的 AppFabric 支援 Google Workspace

AppFabric 支援從 接收使用者資訊和稽核日誌Google Workspace。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Google Workspace到支援的目的地，您必須符合下列要求：

- 您必須訂閱 Google Workspace Enterprise Standard 計劃。如需建立或升級至 Google Workspace Enterprise Standard 計劃的詳細資訊，請參閱 Google Workspace Plans 網站。
- 您的 中必須有具有管理員角色的使用者Google Workspace。
- 若要讓 AppFabric 交付日誌，您需要在 Google Cloud 專案上啟用 Google Admin SDK API。如需詳細資訊，請參閱《 Google Workspace開發人員指南》中的啟用 Google Workspace APIs。

速率限制考量

Google Workspace 會對 Google Workspace API 強加速率限制。如需 Google Workspace API 速率限制的詳細資訊，請參閱 Google Workspace 網站上的 管理指南中的限制和配額。 Google Workspace 如果 AppFabric 和現有 Google Workspace API 應用程式的組合超過限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

大多數稽核事件最多可能會延遲 30 分鐘，而某些稽核事件最多可能會延遲 4 小時交付到您的目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。如需詳細資訊，請參閱 Google WorkSpace Admin 說明網站中的資料保留和延遲時間。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Google Workspace您的帳戶

在 AppFabric 服務中建立應用程式套件之後，您必須使用 授權 AppFabricGoogle Workspace。若要尋找Google Workspace使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

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

1. 若要設定 OAuth 同意畫面，請遵循 Google Workspace網站上的Google Workspace開發人員指南中設定 OAuth 同意畫面的指示。

   針對使用者類型選擇內部。
2. 若要設定 AppFabric 的 OAuth 登入資料，請遵循《 Google Workspace 開發人員指南》中建立存取登入資料頁面的 OAuth 用戶端 ID 登入資料一節中的指示。
3. 使用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>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。

必要範圍

您必須將下列範圍新增至 Google Workspace OAuth 應用程式：

- `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 Admin 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 將請求您的租戶 ID。AppFabric 中的租戶 ID 是您的Google Workspace專案 ID。若要尋找專案 ID，請參閱 Google API 主控台說明網站上的尋找專案 ID。

租戶名稱

輸入可識別此唯一 的名稱Google Workspace。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 將請求您的用戶端 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》中管理登入資料頁面的檢視登入資料一節中的資訊，尋找您的用戶端 ID。
2. 在 AppFabric 的用戶端 ID 欄位中輸入 OAuth 用戶端的用戶端 ID。

Client secret (用戶端密碼)

AppFabric 將請求您的用戶端秘密。若要尋找您的用戶端秘密，請使用下列步驟：

1. 使用《 Google Workspace開發人員指南》中管理登入資料頁面的檢視登入資料一節中的資訊，尋找您的用戶端秘密。
2. 如果您需要重設用戶端秘密，請使用 Google Workspace開發人員指南中管理登入資料頁面的重設用戶端秘密一節中的指示。
3. 在 AppFabric 的用戶端秘密欄位中輸入用戶端秘密。

核准授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗Google Workspace，以核准授權。若要核准 AppFabric 授權，請選擇允許。

HubSpot 為 AppFabric 設定

HubSpot 是一種客戶平台，具有連線行銷、銷售、內容管理和客戶服務所需的所有軟體、整合和資源。 HubSpot的連線平台可讓您透過專注於最重要的事項來更快速地擴展業務：您的客戶。

為了安全起見，您可以使用 AWS AppFabric 從 接收稽核日誌和使用者資料HubSpot、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 HubSpot
- 將 AppFabric 連線至HubSpot您的帳戶

的 AppFabric 支援 HubSpot

AppFabric 支援從 接收使用者資訊和稽核日誌HubSpot。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸HubSpot到支援的目的地，您必須符合下列要求：

- 您必須擁有 中具有企業訂閱的帳戶HubSpot，才能存取稽核日誌。如需HubSpot訂閱的詳細資訊，請參閱HubSpot知識庫上的管理您的HubSpot訂閱。
- 您必須擁有與帳戶相關聯的開發人員帳戶和應用程式。
- 您應該是超級管理員，才能在HubSpot帳戶中安裝應用程式，或擁有 App Marketplace 存取許可，以及接受應用程式請求範圍的使用者許可。

速率限制考量

HubSpot 會對 HubSpot API 強加速率限制。如需 HubSpot API 速率限制的詳細資訊，包括使用 OAuth 的應用程式限制，請參閱HubSpot網站上的速率限制。如果 AppFabric 和現有 HubSpot API 應用程式的組合超過 的限制，AppFabric 中出現HubSpot的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件最多延遲 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至HubSpot您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricHubSpot。若要尋找HubSpot使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

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

1. 請遵循 HubSpot 網站上的HubSpot指南中建立公有應用程式一節中的指示。
2. 從驗證索引標籤中，新增 中列出的三個範圍必要範圍。
3. 在重新導向 URL 中使用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>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。
4. 選擇建立應用程式。

必要範圍

您必須將下列範圍新增至 HubSpot OAuth 應用程式：

- `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HubSpot您的帳戶 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 將請求用戶端 ID。若要在 中尋找您的用戶端 IDHubSpot，請使用下列步驟：

1. 導覽至HubSpot登入頁面，並使用開發人員帳戶登入資料登入。

2. 從應用程式功能表中，選擇您的應用程式。
3. 從驗證索引標籤中，尋找用戶端 ID 值。

Client secret (用戶端密碼)

AppFabric 將請求用戶端秘密。若要在 中尋找您的用戶端秘密HubSpot，請使用下列步驟：

1. 導覽至HubSpot登入頁面，並使用開發人員帳戶登入資料登入。
2. 從應用程式功能表中，選擇您的應用程式。
3. 從驗證索引標籤中，尋找用戶端秘密值。

核准授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗HubSpot，以核准授權。使用您的企業帳戶登入資料（而非您的開發人員帳戶）登入您的帳戶，以核准 AppFabric 授權。選擇允許。

IBM Security® Verify 為 AppFabric 設定

IBM Security® Verify 系列提供自動化的雲端和內部部署功能，用於管理身分控管、管理人力資源和消費者身分和存取，以及控制特權帳戶。無論您需要部署雲端或內部部署解決方案， IBM Security® Verify都可協助您建立信任並防範對人力資源和消費者的內部威脅。

為了安全起見，您可以使用 AWS AppFabric 從 接收稽核日誌和使用者資料IBM Security® Verify、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 IBM Security® Verify
- 將 AppFabric 連線至IBM Security® Verify您的帳戶

的 AppFabric 支援 IBM Security® Verify

AppFabric 支援從 接收使用者資訊和稽核日誌IBM Security® Verify。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸IBM Security® Verify到支援的目的地，您必須符合下列要求：

- 若要存取稽核日誌，您需要擁有 IBM Security® Verify SaaS 帳戶。
- 若要存取稽核日誌，您需要在 IBM Security® Verify SaaS 帳戶中擁有管理員角色。

速率限制考量

IBM Security® Verify 會對 IBM Security® Verify API 強加速率限制。如需 IBM Security® Verify API 速率限制的詳細資訊，請參閱 IBM 條款。如果 AppFabric 和現有 IBM Security® Verify API 應用程式的組合超過IBM Security® Verify限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會在稽核事件中看到最多 30 分鐘的延遲，以傳送到您的目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級上自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至IBM Security® Verify您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricIBM Security® Verify。若要尋找IBM Security® Verify使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

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

1. 對於第一次登入，請使用傳送到您註冊電子郵件地址的登入 URL 和登入資料。
2. 在 存取管理主控台`https://<hostname>.verify.ibm.com/ui/admin/`。如需詳細資訊，請參閱存取 IBM Security® Verify。
3. 在管理主控台中，在安全性 < API 存取 < API 用戶端下，選擇新增。
4. 選取下列選項。這些是讀取稽核日誌和使用者詳細資訊的必要項目。
   - 讀取報告
   - 讀取使用者和群組
5. 在用戶端身分驗證方法中保留預設選項。

   請勿編輯自訂範圍欄位。
6. 選擇下一步。
7. 請勿編輯 IP 篩選條件欄位。

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 將請求您的租戶 ID。您可以在IBM Security® Verify標準 URL 中找到租戶 ID。例如，在 `https://hostname.verify.ibm.com/` URL 中，租戶 ID 是可在之前 `.verify.ibm.com`（或者`ice.ibmcloud.com`如果您使用的是先前的`####`，則為之前）找到的主機名稱。如果您使用的是虛設 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租用戶的名稱。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 將請求用戶端 ID。若要在 中尋找您的用戶端 IDIBM Security® Verify，請使用下列步驟：

1. 對於第一次登入，請使用傳送到您註冊電子郵件地址的登入 URL 和登入資料。
2. 在 存取管理主控台`https://<hostname>.verify.ibm.com/ui/admin/`。如需詳細資訊，請參閱存取 IBM Security® Verify。
3. 在管理主控台中，於安全性 < API Access < API Client 下，選擇特定 OAuth 應用程式旁的省略符號 (⋮)。
4. 選擇連線詳細資訊。
5. 在 API 登入資料下尋找用戶端 ID。

Client secret (用戶端密碼)

AppFabric 將請求用戶端秘密。若要在 中尋找您的用戶端秘密IBM Security® Verify，請使用下列步驟：

1. 對於第一次登入，請使用傳送到您註冊電子郵件地址的登入 URL 和登入資料。
2. 在 存取管理主控台`https://<hostname>.verify.ibm.com/ui/admin/`。如需詳細資訊，請參閱存取 IBM Security® Verify。
3. 在管理主控台中，於安全性 < API 存取 < API 用戶端下，選擇特定 OAuth 應用程式旁的省略符號 (⋮)。
4. 選擇連線詳細資訊。
5. 在 API 登入資料下尋找用戶端秘密。

JumpCloud 為 AppFabric 設定

JumpCloud Inc. 是美國企業軟體公司，提供雲端目錄平台進行身分管理。它集中並簡化身分管理，允許使用者使用一組登入資料安全地存取其系統、應用程式、網路和檔案伺服器，無論平台、通訊協定、提供者或位置為何。

您可以使用 AWS AppFabric 從 JumpCloud 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結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 JumpCloud
- 將 AppFabric 連線至JumpCloud您的帳戶

的 AppFabric 支援 JumpCloud

AppFabric 支援從 接收使用者資訊和稽核日誌JumpCloud。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸JumpCloud到支援的目的地，您必須滿足下列要求：

- 您必須擁有作用中的付費JumpCloud訂閱計劃。如需詳細資訊，請參閱 JumpCloud Select a package that's right for you網站上的 。
- 您必須具有「使用帳單的管理員」角色。

速率限制考量

JumpCloud 不會發佈速率限制。您必須建立支援案例或聯絡您的JumpCloud客戶團隊。如果 AppFabric 和現有 JumpCloud API 應用程式的組合超過JumpCloud's限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件延遲最多 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至JumpCloud您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricJumpCloud。若要尋找 JumpCloud使用 AppFabric 授權所需的資訊，請遵循下一節中的步驟。

從JumpCloud帳戶建立組織字符

AppFabric 使用 API 金鑰與 整合 JumpCloud 若要在 JumpCloud 中建立 API 金鑰，請遵循下列步驟：

1. 以管理員身分登入您的帳戶JumpCloud。
2. 在管理員入口網站中，選擇您的帳戶首字母，位於右上角 n，然後從功能表中選擇我的 API 金鑰。
3. 選擇產生新的 API 金鑰，或選取現有的金鑰。

> **Note**
>
> JumpCloud 僅允許一個作用中 API 金鑰。產生新的 API 金鑰將撤銷對目前 API 金鑰的存取權。這會讓使用先前 API 金鑰的所有呼叫無法存取。您必須更新使用先前 API 金鑰與新金鑰值的任何現有整合。

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。這裡的「組織 ID」將是租戶 ID。若要尋找「組織 ID」，請遵循下列步驟。

1. 登入 JumpCloud 帳戶。

2. 在導覽窗格中，選擇設定，然後選擇組織設定檔，然後選擇一般。
3. 選擇「眼睛」圖示以移除遮蔽的檢視。
4. 選擇「兩頁」圖示來複製 ID。

租戶名稱

輸入可識別此唯一JumpCloud組織的名稱。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。

服務帳戶字符

AppFabric 將請求您的服務帳戶字符。在 AppFabric 中，這是您在此主題從JumpCloud帳戶建立組織字符稍早在 中建立的組織 API 字符。

設定 AppFabric 的 Microsoft 365

Microsoft 365 是 擁有的一系列生產力軟體、協作和雲端服務Microsoft。

為了安全起見，您可以使用 AWS AppFabric 從 Microsoft 365 稽核日誌和使用者資料、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 365 的 AppFabric Microsoft 支援
- 將 AppFabric 連線至您的 Microsoft 365 帳戶

365 的 AppFabric Microsoft 支援

AppFabric 支援從 365 Microsoft 接收使用者資訊和稽核日誌。

先決條件

若要使用 AppFabric 將稽核日誌從 Microsoft 365 傳輸到支援的目的地，您必須滿足下列要求：

- 您必須訂閱 Microsoft 365 Enterprise 計劃。如需建立或升級至 Microsoft 365 Enterprise 計劃的詳細資訊，請參閱 Microsoft 網站上的 Microsoft 365 Enterprise Plans。
- 您必須擁有 365 Microsoft 帳戶中具有管理員許可的使用者。
- 您必須開啟組織的稽核記錄。如需詳細資訊，請參閱 Microsoft 網站上的開啟或關閉稽核。

速率限制考量

Microsoft 365 會對 365 API Microsoft 強加速率限制。如需 Microsoft 365 API 速率限制的詳細資訊，請參閱 Microsoft Microsoft 網站上的圖形文件中的圖形服務特定限流限制。 Microsoft如果 AppFabric 和現有 Microsoft 365 API 應用程式的組合超過限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件延遲最多 30 分鐘交付至目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至您的 Microsoft 365 帳戶

在 AppFabric 服務中建立應用程式套件之後，您必須使用 365 Microsoft 授權 AppFabric。若要尋找使用 AppFabric 授權 Microsoft 365 所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

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

1. 請遵循 Microsoft 網站上的 Azure Active Directory 開發人員指南中註冊應用程式一節中的指示。

   僅在支援的 帳戶類型組態中選擇此組織目錄中的帳戶。
2. 遵循 Azure Active Directory 開發人員指南中新增重新導向 URI 一節中的指示。

   選擇 Web 平台。

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

   在此 URL 中， *<region>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `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. 請遵循 Azure Active Directory 開發人員指南中新增用戶端秘密一節中的指示。

所需的許可

您必須將下列許可新增至 OAuth 應用程式。若要新增許可，請遵循 Azure Active Directory 開發人員指南的新增許可一節中的指示來存取您的 Web API。

- `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）

新增許可後，若要授予管理員許可的同意，請遵循 Azure Active Directory 開發人員指南的管理員同意按鈕一節中的指示。

應用程式授權

AppFabric 支援從您的 365 Microsoft 帳戶接收使用者資訊和稽核日誌。若要從 Microsoft 365 接收稽核日誌和使用者資料，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 Microsoft 365，另一個在應用程式授權下拉式清單中名為 Microsoft 365 稽核日誌。您可以對這兩個應用程式授權使用相同的租用戶 ID、用戶端 ID 和用戶端秘密。若要從 Microsoft 365 接收稽核日誌，您需要 Microsoft365 和 Microsoft 365 稽核日誌應用程式授權。若要單獨使用使用者存取工具，只需要 Microsoft 365 應用程式授權。

租用戶 ID

AppFabric 將請求您的租戶 ID。AppFabric 中的租用戶 ID 是您的 Azure Active Directory 租用戶 ID。若要尋找您的 Azure Active Directory 租用戶 ID，請參閱 Microsoft 網站上的 Azure 產品文件中的如何尋找您的 Azure Active Directory 租用戶 ID。

租戶名稱

輸入可識別此唯一 365 Microsoft 帳戶的名稱。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 將請求您的用戶端 ID。AppFabric 中的用戶端 ID 是 Microsoft 365 應用程式（用戶端）ID。若要尋找 Microsoft 365 應用程式（用戶端）ID，請使用下列步驟：

1. 開啟您搭配 AppFabric 使用的 OAuth 應用程式概觀頁面。
2. 應用程式（用戶端）ID 會顯示在 Essentials 下。
3. 在 AppFabric 的用戶端 ID 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 Microsoft 將請求您的用戶端秘密。365 僅在您最初為 OAuth 應用程式建立用戶端秘密時提供此值。若要在您沒有用戶端秘密時產生新的用戶端秘密，請使用下列步驟：

1. 若要建立用戶端秘密，請遵循 Azure Active Directory 開發人員指南中新增用戶端秘密一節中的指示。
2. 在 AppFabric 的用戶端秘密欄位中輸入值欄位的內容。

核准授權

在 AppFabric 中建立應用程式授權後，您將收到來自 365 Microsoft 的快顯視窗來核准授權。若要核准 AppFabric 授權，請選擇允許。

Miro 為 AppFabric 設定

Miro 是創新的線上工作區，可讓任何規模的分散式團隊建置下一個大物件。平台的無限畫布可讓團隊領導參與研討會和會議、設計產品、腦力激盪想法等。 Miro總部位於舊金山和阿姆斯特丹，為全球超過 50M使用者提供服務，包括 99% 的 Fortune 100。 Miro 成立於 2011 年，目前在全球 12 個中樞擁有超過 1，500 名員工。若要進一步了解，請造訪 Miro。

Miro 包含專為創新所設計的完整協作功能套件，包括圖表、 wireframing、 即時資料視覺化、 研討會協助、 和內建的靈活實務支援， 研討會、 和互動式簡報。 Miro最近宣布Miro了 AI，擴展 Miro的功能， 使用 AI 驅動的映射和圖表， 叢集和摘要、 和內容產生。 Miro可讓組織減少獨立工具的數量， 減少資訊分段和成本。

為了安全起見，您可以使用 AWS AppFabric 從 稽核日誌和使用者資料Miro、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Miro
- 將 AppFabric 連線至Miro您的帳戶

的 AppFabric 支援 Miro

AppFabric 支援從 接收使用者資訊和稽核日誌Miro。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Miro到支援的目的地，您必須符合下列要求：

- 您必須擁有 Miro Enterprise Plan。如需 Miro 計劃類型的詳細資訊，請參閱 Miro 網站上的Miro定價頁面。
- Miro 您的帳戶中必須有具有公司管理員角色的使用者。如需角色的詳細資訊，請參閱 Miro 說明中心網站上的 Miro 中角色的公司層級區段。
- Miro 您的帳戶中必須有企業開發人員團隊。如需有關建立開發人員團隊的資訊，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 會對 Miro API 強加速率限制。如需 Miro API 速率限制的詳細資訊，請參閱 Miro 網站上的Miro開發人員指南中的速率限制。如果 AppFabric 和現有 Miro API 應用程式的組合超過限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件延遲最多 30 分鐘交付至目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Miro您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricMiro。若要尋找Miro使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

AppFabric Miro使用 OAuth 與 整合。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，請遵循 Miro 說明中心網站上的企業開發人員團隊文章中建立和安裝應用程式一節中的指示。
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字符核取方塊。

> **Note**
>
> 您必須在建立應用程式之前執行此操作，因為您在建立應用程式之後無法變更此選項。

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>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。

4. 複製並儲存您的用戶端 ID 和用戶端秘密，以用於 AppFabric 應用程式授權。

必要範圍

您必須在 OAuth 應用程式頁面的 Miro `Permissions`區段中新增下列範圍：

- `auditlogs:read`
- `organizations:read`

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。AppFabric 中的租戶 ID 是您的團隊 Miro ID。如需有關如何尋找 Miro 團隊 ID 的資訊，請參閱我是新管理員的常見問答集一節。 Miro 說明Miro中心網站上的開始位置？。

租戶名稱

輸入可識別此唯一Miro組織的名稱。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 將請求您的用戶端 ID。若要尋找您的用戶端 ID，請使用下列步驟：

1. 導覽至您的Miro設定檔設定。
2. 選取您的應用程式索引標籤。
3. 選取您用來與 AppFabric 連線的應用程式。
4. 從 App Credentials 區段將用戶端 ID 輸入 AppFabric 中的用戶端 ID 欄位。

Client secret (用戶端密碼)

AppFabric 將請求您的用戶端秘密。若要尋找您的用戶端秘密，請使用下列步驟：

1. 導覽至您的Miro設定檔設定。
2. 選取您的應用程式索引標籤。
3. 選取您用來與 AppFabric 連線的應用程式。
4. 從 App Credentials 區段將用戶端秘密輸入 AppFabric 中的用戶端秘密欄位。

核准授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗Miro，以核准授權。若要核准 AppFabric 授權，請選擇允許。

Okta 為 AppFabric 設定

Okta 是世界的 Identity Company。身為領導性獨立身分合作夥伴， Okta 可讓每個人安全地在任何地點在任何裝置或應用程式上使用任何技術。最信任的品牌信任 Okta 來啟用安全存取、身分驗證和自動化。憑藉Okta人力資源身分和客戶身分雲端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位轉型，這要歸功於可自訂的解決方案和超過 7，000 個預先建置的整合。 Okta 正在建立一個 Identity 屬於您的世界。如需進一步了解，請參閱 .comokta。

為了安全起見，您可以使用 AWS AppFabric 從 稽核日誌和使用者資料Okta、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Okta
- 將 AppFabric 連線至Okta您的帳戶

的 AppFabric 支援 Okta

AppFabric 支援從 接收使用者資訊和稽核日誌Okta。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Okta到支援的目的地，您必須符合下列要求：

- 您可以搭配任何Okta計劃類型使用 AppFabric。
- Okta 您的帳戶中必須有具有超級管理員角色的使用者。
- 在 AppFabric 中核准應用程式授權的使用者也必須在Okta您的帳戶中具有超級管理員角色。

速率限制考量

Okta 會對 Okta API 強加速率限制。如需 Okta API 速率限制的詳細資訊，請參閱 Okta 網站上的Okta開發人員指南中的速率限制。如果 AppFabric 和現有 Okta API 應用程式的組合超過 的限制，AppFabric 中出現Okta的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件延遲最多 30 分鐘交付至目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Okta您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricOkta。若要尋找Okta使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

AppFabric Okta使用 OAuth 與 整合。若要建立 OAuth 應用程式以與 AppFabric 連線，請遵循Okta說明中心網站上的建立 OIDC 應用程式整合中的指示。以下是 AppFabric 的組態考量：

1. 針對應用程式類型，選擇 Web 應用程式。
2. 針對授予類型，選擇授權碼並重新整理權杖。
3. 使用具有下列格式的重新導向 URL 做為登入重新導向 URI 和登出重新導向 URI。

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

   在此 URL 中，*<region>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。
4. 您可以略過信任的原始伺服器組態。
5. 在受控存取組態中將存取權授予Okta組織中的每個人。

> **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組態頁面上的指派索引標籤，將組織中的每個人指派為群組。

6. 您可以保留所有其他選項及其預設值。

必要範圍

您必須將下列範圍新增至 Okta OAuth 應用程式：

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

應用程式授權

租用戶 ID

AppFabric 將請求租戶 ID。AppFabric 中的租戶 ID 是您的Okta網域。如需尋找Okta網域的詳細資訊，請參閱 Okta 網站上的Okta開發人員指南中的尋找您的Okta網域。

租戶名稱

輸入可識別此唯一Okta組織的名稱。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 會請求用戶端 ID。若要在 中尋找您的用戶端 IDOkta，請使用下列步驟：

1. 導覽至Okta開發人員主控台。
2. 選擇應用程式索引標籤。
3. 選擇您的應用程式，然後選擇一般索引標籤。
4. 捲動至用戶端登入資料區段。
5. 將 OAuth 用戶端的用戶端 ID 輸入 AppFabric 中的用戶端 ID 欄位。

Client secret (用戶端密碼)

AppFabric 將請求用戶端秘密。若要在 中尋找您的用戶端秘密Okta，請使用下列步驟：

1. 導覽至Okta開發人員主控台。
2. 選擇應用程式索引標籤。
3. 選擇您的應用程式，然後選擇一般索引標籤。
4. 捲動至用戶端登入資料區段。
5. 將 OAuth 應用程式的用戶端秘密輸入 AppFabric 中的用戶端秘密欄位。

核准授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗Okta，以核准授權。若要核准 AppFabric 授權，請選擇允許。核准Okta授權的使用者必須在 中具有超級管理員許可Okta。

OneLogin by One Identity 為 AppFabric 設定

OneLogin by One Identity 是一種現代化的雲端存取管理解決方案，可無縫管理人力資源、客戶和合作夥伴的所有數位身分。 OneLogin提供安全的單一登入 (SSO)、多重要素驗證 (MFA)、適應性驗證、桌面層級 MFA、與 AD、LDAP、G Suite 和其他外部目錄的目錄整合、身分生命週期管理等。透過 OneLogin，您可以保護您的組織免受最常見的攻擊，進而提高安全性、無摩擦的使用者體驗，以及符合法規要求。

您可以針對安全性使用 AWS AppFabric 從 接收稽核日誌和使用者資料OneLogin、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 OneLogin by One Identity
- 將 AppFabric 連接到OneLogin by One Identity您的帳戶

的 AppFabric 支援 OneLogin by One Identity

AppFabric 支援從 接收使用者資訊和稽核日誌OneLogin by One Identity。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸OneLogin by One Identity到支援的目的地，您必須符合下列要求：

- 您必須擁有OneLogin進階或專業帳戶。
- 您必須擁有具有 Admin/Delegated Admin 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 OneLogin API 參考中的取得速率限制。如果 AppFabric 和現有 OneLogin API 應用程式的組合超過 的限制，AppFabric 中出現OneLogin的稽核日誌可能會延遲。不過，可以提高OneLogin速率限制。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

您可能會看到稽核事件延遲最多 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連接到OneLogin by One Identity您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricOneLogin by One Identity。若要尋找OneLogin使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

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

1. 導覽至OneLogin登入頁面並登入。
2. 從開發人員功能表中，選擇 API 登入資料。
3. 選擇新登入資料，輸入新登入資料的名稱，然後選擇全部讀取。
4. 選擇儲存。 OneLogin會建立用戶端 ID 和用戶端秘密。

必要範圍

您必須將下列範圍新增至 OneLogin by One Identity OAuth 應用程式：

- 全部讀取。如需範圍和用戶端登入資料的詳細資訊，請參閱 API 參考中的使用 API 登入資料。OneLogin

應用程式授權

租用戶 ID

AppFabric 將請求租戶 ID。AppFabric 中的租用戶 ID 是您的執行個體子網域。您可以在瀏覽器的地址列中找到您的租戶 ID。例如， `subdomain`是下列 URL 中的租戶 ID`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 將請求用戶端 ID。若要在 中尋找您的用戶端 IDOneLogin by One Identity，請使用下列步驟：

1. 導覽至OneLogin登入頁面並登入。
2. 從開發人員功能表中，選擇 API 登入資料。
3. 選擇 API 登入資料以取得用戶端 ID。

Client secret (用戶端密碼)

AppFabric 將請求用戶端秘密。若要在 中尋找用戶端秘密OneLogin by One Identity，請使用下列步驟：

1. 導覽至OneLogin登入頁面並登入。
2. 從開發人員功能表中，選擇 API 登入資料。
3. 選擇 API 登入資料以取得用戶端秘密。

用戶端應用程式授權

在 AppFabric 中，使用您的租戶 ID 和名稱，以及您的用戶端 ID 和名稱來建立應用程式授權。選擇連線以啟用授權。

PagerDuty 為 AppFabric 設定

PagerDuty 是一種數位操作管理平台，可將任何訊號轉換為動作，協助團隊減輕影響客戶的問題，讓您可以更快地解決問題，並更有效率地操作。與 CloudWatch、CloudTrail、 GuardDuty和 整合Personal Health Dashboard。

您可以針對安全性使用 AWS AppFabric 從 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結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 PagerDuty
- 將 AppFabric 連接到PagerDuty您的帳戶

的 AppFabric 支援 PagerDuty

AppFabric 支援從 接收使用者資訊和稽核日誌PagerDuty。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸PagerDuty到支援的目的地，您必須符合下列要求：

- 若要存取稽核日誌，您必須擁有PagerDuty商業或數位操作計劃。
- 您應該是 PagerDuty 帳戶的 Global Admin 或帳戶擁有者。

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 和現有 PagerDuty API 應用程式的組合超過 的限制，AppFabric 中出現PagerDuty的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件延遲最多 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級自訂。如需協助，請聯絡 支援。

將 AppFabric 連接到PagerDuty您的帳戶

PagerDuty 平台支援 API 存取金鑰。若要產生 API 存取金鑰，請使用下列步驟。

建立 API 存取金鑰

AppFabric PagerDuty使用適用於公有用戶端的 API 存取金鑰與 整合。若要在 中建立 API 存取金鑰 PagerDuty，請使用下列步驟：

1. 導覽至PagerDuty登入頁面並登入。
2. 選擇整合、API 存取金鑰。
3. 選擇建立新 API 金鑰。
4. 輸入描述，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。稍後在 AppFabric 中需要此項目。如果您在儲存 API 金鑰之前關閉頁面，則必須產生新的 API 金鑰並進行儲存。此金鑰應專用於 AppFabric，以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 將請求您的租戶 ID。PagerDuty 您帳戶的租戶 ID 是您帳戶的基本 URL。您可以登入 Web 瀏覽器的地址列PagerDuty並從中複製，以找到此項目。租戶 ID 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。

服務帳戶字符

AppFabric 將請求您的服務帳戶字符。AppFabric 中的服務帳戶權杖是您在 中建立的 API 存取金鑰建立 API 存取金鑰。

Ping Identity 為 AppFabric 設定

在 Ping Identity，我們相信為所有使用者提供安全且無縫的數位體驗，而不會受到影響。這就是為什麼超過一半的 Fortune 100 選擇Ping Identity保護其使用者的數位互動，同時讓體驗順暢無阻。2023 年 8

月 23 日， Ping Identity 和 ForgeRock 共同為客戶提供更多選擇、更深入的專業知識和更完整的身分解決方案。

為了安全起見，您可以使用 AWS AppFabric 從 接收稽核日誌和使用者資料Ping Identity、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Ping Identity
- 將 AppFabric 連線至Ping Identity您的帳戶

的 AppFabric 支援 Ping Identity

AppFabric 支援從 接收使用者資訊和稽核日誌Ping Identity。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Ping Identity到支援的目的地，您必須滿足下列要求：

- 您必須擁有 Essential、Plus 或 Premium Ping Identity帳戶。如需建立或升級至適用Ping Identity計劃類型的詳細資訊，請參閱 Ping Identity 網站上的Ping Identity所有功能的定價。
- Ping Identity 您的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 Ping Identity 支援網站上的角色。

速率限制考量

Ping Identity 不會發佈速率限制。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 和現有 Ping Identity API 應用程式的組合超過 的限制，AppFabric 中出現Ping Identity的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件最多延遲 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Ping Identity您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricPing Identity。若要尋找Ping Identity使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

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

1. 請遵循 Ping Identity 網站上的PingOne開發人員指南中的建立應用程式連線一節中的指示。
2. 建立應用程式後，請自訂授予類型。
   a. 登入應用程式時，請選擇組態索引標籤，然後按一下鉛筆圖示以變更現有組態。
   b. 在授予類型下，選取授權碼。將 PKCE 強制執行保留為選用。
   c. 選取重新整理權杖，然後選擇您的重新整理持續時間。
3. 在重新導向 URL/回呼 URL 中使用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>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。AppFabric 中的租戶 ID 是您的Ping Identity執行個體名稱。您可以在瀏覽器的地址列中找到您的租戶 ID。例如 *API_PATH*`/v1/environments/`*environmentID*。其中 *API_PATH*代表PingOne伺服器的區域網域，例如 `api.pingone.com`，而 *environmentID*代表應用程式環境屬性中指出的環境 ID。如需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 將請求用戶端 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管理員主控台，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 將請求用戶端秘密。若要在 中尋找您的用戶端秘密Ping Identity，請使用下列步驟：

1. 登入PingOne管理員主控台，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，然後尋找用戶端秘密值。

核准授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗Ping Identity來核准授權。若要核准 AppFabric 授權，請選擇允許。

Salesforce 為 AppFabric 設定

Salesforce 讓雲端型軟體旨在協助企業尋找更多潛在客戶、完成更多交易，並讓客戶驚嘆不已的服務。Salesforce'sCustomer 360 提供完整的產品套件，將銷售、服務、行銷、商業和 IT 團隊與單一、共用的客戶資訊檢視相結合，協助組織與客戶和員工建立關係。

您可以使用 AWS AppFabric 從 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結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Salesforce
- 將 AppFabric 連線至Salesforce您的帳戶

的 AppFabric 支援 Salesforce

AppFabric 支援從 接收使用者資訊和稽核日誌Salesforce。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Salesforce到支援的目的地，您必須符合下列要求：

- 您必須擁有 的效能、企業或無限制版本Salesforce。請聯絡 Salesforce 以升級至其中一個版本。
- 如果您要讓 AppFabric 從 傳輸具有完整日誌事件集的每小時事件日誌檔案Salesforce，則必須訂閱事件監控，做為 Shield 功能的一部分Salesforce。否則，AppFabric 將從Salesforce's標準每日日誌檔案傳輸有限事件（即 Login、Logout、InsecureExternalAssets、API Total Usage、CORS Violation 和 HostnameRedirects ELF Events)。您可以前往設定 > 事件管理員，檢查Salesforce您的帳戶是否已訂閱 Shield 功能。如果您看到列出 19 個或更多事件，您的帳戶會訂閱事件監控。如果您沒有事件監控，您可以聯絡 購買此附加元件的訂閱Salesforce。
- 您需要在Salesforce設定中選擇加入事件日誌檔案產生。
- 您應該使用系統管理員設定檔來建立 OAuth 應用程式，並使用 AppFabric 的相同登入資料登入。

> **Note**
>
> API 總用量、CORS 違規記錄、主機名稱重新導向、不安全的外部資產、登入和登出事件可在支援的 版本中免費使用Salesforce。請聯絡 Salesforce 購買剩餘的事件類型。如需Salesforce事件類型的詳細資訊，請參閱 Salesforce 網站上的 EventLogFile 支援的事件類型。AppFabric 每個日誌檔案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，取決於事件監控附加元件訂閱）。超過閾值的日誌檔案可能會導致整個日誌檔案被排除在擷取之外。

速率限制考量

Salesforce 會對 Salesforce API 強加速率限制。如需 Salesforce API 速率限制的詳細資訊，請參閱 Salesforce 網站上的 API 請求限制和配置。如果 AppFabric 和現有 Salesforce API 應用程式的組合超過Salesforce's限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會在每日日誌檔案上看到最多 6 小時的延遲，或在每小時日誌檔案上看到最多 29 小時的延遲，以便將稽核事件交付到您的目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Salesforce您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricSalesforce。若要尋找Salesforce使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

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

1. 登入Salesforce您的帳戶。
2. 前往 Salesforce 文件中所述的設定頁面。
3. 在快速尋找中搜尋 App Manager。
4. 選擇新的連線應用程式。
5. 在表單欄位中輸入必要資訊。
6. 選擇啟用 OAuth 設定。
7. 請務必關閉下列選項：
   - 支援的授權流程需要程式碼交換 (PKCE) 延伸的證明金鑰
   - 需要 Web 伺服器流程的秘密
   - 重新整理權杖流程需要秘密
   - 啟用重新整理權杖輪換
8. 在回呼 URL 文字方塊中輸入具有下列格式的 URL，然後選擇儲存變更。

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

   在此 URL 中，*<region>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。
9. 視需要填入範圍（下必要範圍節說明）。所有其他欄位都可以保留其預設值。
10. 選擇儲存。
11. 完成下列步驟，以驗證新 OAuth 應用程式的重新整理權杖政策：
    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. 選擇新建立的應用程式旁的編輯。
    c. 在選取撤銷選項之前，請確定重新整理字符有效。
    d. 儲存您的變更。
12. 請完成下列步驟，以確認正在產生稽核日誌：
    a. 在設定頁面上，在快速尋找文字方塊中輸入事件日誌檔案，然後選擇事件日誌檔案瀏覽器。

b. 確認事件日誌已列在事件日誌檔案瀏覽器中。

13. 導覽至建立的應用程式，然後從下拉式清單中選擇檢視。
14. 選擇管理消費者詳細資訊。

    系統會將您重新導向至需要驗證身分的新標籤。在該索引標籤上，記下消費者金鑰和消費者秘密值。稍後您需要這些項目才能登入。

必要範圍

您必須將下列範圍新增至 Salesforce OAuth 應用程式：

- 透過 APIs(`API`)。
- 隨時執行請求 (`refresh_token` 和 `offline_access`)。

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。AppFabric 中的租用戶 ID 是您 Salesforce My Domain 的子網域。您可以在瀏覽器的地址列中找到 My Domain 子網域，介於 `https://`和 之間`.my.salesforce.com`。

若要尋找您的 Salesforce My Domain，請使用Salesforce主畫面中的下列指示。

1. 前往 Salesforce 文件中所述的設定頁面。
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 會請求用戶端 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 App Manager。
3. 選擇建立的應用程式，然後選擇從下拉式功能表檢視。

4. 選擇管理消費者詳細資訊。系統會將您重新導向至新的索引標籤。
5. 驗證您的身分，然後尋找消費者金鑰值。
6. 在 AppFabric 的用戶端 ID 欄位中輸入消費者金鑰。

Client secret (用戶端密碼)

AppFabric 將請求您的用戶端秘密。AppFabric 中的用戶端秘密是 中的消費者秘密Salesforce。若要在中尋找您的秘密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 App Manager。
3. 選擇建立的應用程式，然後選擇從下拉式功能表檢視。
4. 選擇管理消費者詳細資訊。系統會將您重新導向至新的索引標籤。
5. 驗證您的身分，然後尋找消費者秘密值。
6. 在 AppFabric 的用戶端秘密欄位中輸入消費者秘密。

核准授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗Salesforce，以核准授權。在核准頁面上，請務必在授權時使用Salesforce系統管理員角色或具有檢視事件日誌檔案和已啟用 API 的使用者許可Salesforce的使用者。選擇允許以核准 AppFabric 授權。

ServiceNow 為 AppFabric 設定

ServiceNow 是雲端型服務的領導供應商，可自動化企業 IT 操作。ServiceNow 的 ITOM 可讓企業完整掌握和控制整個 IT 環境，包括虛擬化和雲端基礎設施。它簡化了服務映射、交付和保證，將 IT 服務和基礎設施資料合併為單一記錄系統。它也會自動化和簡化關鍵程序，包括事件、事件、問題、組態和變更管理。

為了安全起見，您可以使用 AWS AppFabric 從 接收稽核日誌和使用者資料ServiceNow、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 ServiceNow
- 資料延遲考量

- 將 AppFabric 連線至ServiceNow您的帳戶

的 AppFabric 支援 ServiceNow

AppFabric 支援從 接收使用者資訊和稽核日誌ServiceNow。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸ServiceNow到支援的目的地，您必須符合下列要求：

- 您可以搭配任何ServiceNow計劃類型使用 AppFabric。
- ServiceNow 您的帳戶中必須有具有管理員角色的使用者。
- 您必須擁有ServiceNow執行個體。

速率限制考量

ServiceNow 會對 ServiceNow API 強加速率限制。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 和現有 ServiceNow API 應用程式的組合超過限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件最多延遲 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至ServiceNow您的帳戶

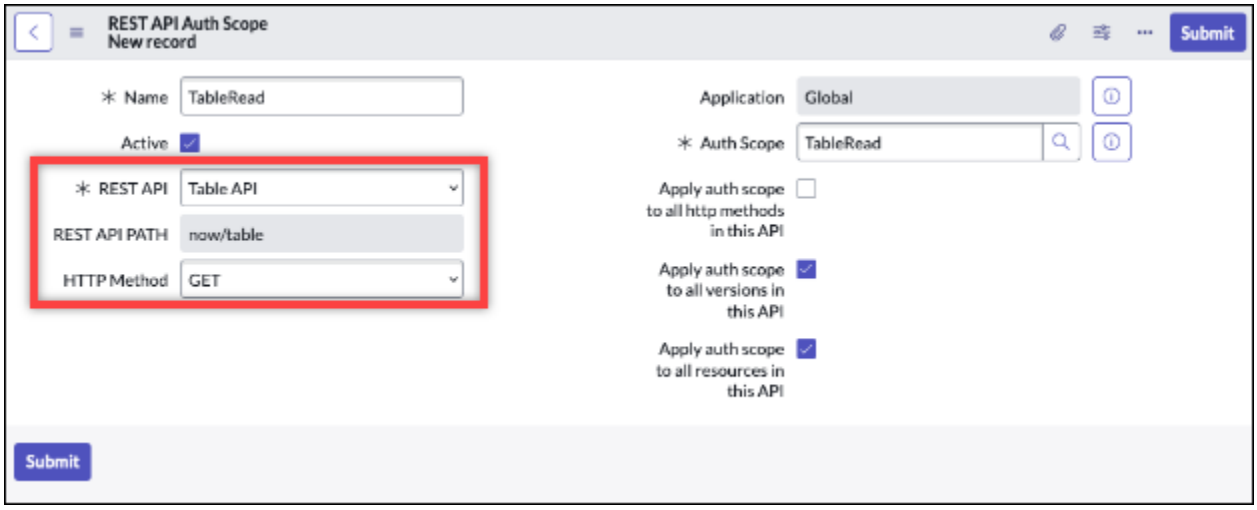
在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricServiceNow。使用下列步驟來尋找ServiceNow使用 AppFabric 授權所需的資訊。

建立 OAuth 應用程式

Now Platform 支援公有用戶端產生存取權杖的 OAuth 2.0 - 授權授予類型。

1. 註冊您的 OAuth 應用程式。這需要以下三個步驟。如需完成這些步驟的詳細資訊，請參閱 ServiceNow 網站上的向 註冊您的應用程式ServiceNow。

    a. 註冊應用程式，並確保驗證範圍可存取資料表 API，其 REST API PATH 現在/資料表，以及 HTTP 方法 GET，如下列範例所示。



b. 產生授權碼。

c. 使用授權碼產生承載字符。

2. 使用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>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2`。

應用程式授權

租用戶 ID

AppFabric 將請求租戶 ID。AppFabric 中的租戶 ID 是您的執行個體名稱。您可以在瀏覽器的地址列中找到您的租戶 ID。例如， *example* 是下列 URL 中的租戶 IDhttps://*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 將請求用戶端 ID。使用下列步驟在 中尋找您的用戶端 IDServiceNow。

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 ID 輸入 AppFabric 中的用戶端 ID 欄位。

Client secret (用戶端密碼)

AppFabric 將請求用戶端秘密。使用下列步驟在 中尋找您的用戶端秘密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 應用程式的用戶端秘密輸入 AppFabric 中的用戶端秘密欄位。

核准授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗ServiceNow，以核准授權。選擇允許以核准 AppFabric 授權。

Singularity Cloud 為 AppFabric 設定

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。其獲得專利的人工智慧將安全性從已知的簽章和模式延伸至最複雜的攻擊，例如零時差攻擊和勒索軟體。

您可以使用 AWS AppFabric 從 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結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

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

主題

- 的 AppFabric 支援 Singularity Cloud
- 將 AppFabric 連接到Singularity Cloud您的帳戶

的 AppFabric 支援 Singularity Cloud

AppFabric 支援從 接收使用者資訊和稽核日誌Singularity Cloud。

先決條件

若要使用 AppFabric 將稽核日誌從 Singularity Cloud 轉移到支援的目的地，您必須在Singularity Cloud 帳戶中具有管理員角色。如需 Singularity Cloud API 速率限制的詳細資訊，請登入您的 Singularity Cloud 帳戶、瀏覽文件區段，並搜尋角色。

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 Singularity Cloud 帳戶、瀏覽文件區段，並搜尋 API 速率限制。

資料延遲考量

您可能會看到稽核事件延遲最多 30 分鐘交付至目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級自訂。如需協助，請聯絡 支援。

將 AppFabric 連接到Singularity Cloud您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricSingularity Cloud。若要尋找 Singularity Cloud使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 的 API 權杖 Singularity Cloud

完成下列程序，以建立與服務使用者相關聯的 API 權杖。API 權杖不會連結至特定主控台使用者或電子郵件地址。

> **Note**
>
> 在服務使用者 API 權杖過期之前或之後，建立新的使用者或複製服務使用者以取得新的 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，然後選擇建立新服務使用者。
4. 在建立新服務使用者頁面中，輸入服務使用者的名稱、描述和過期日期。
5. 選擇 Next (下一步)。

6. 在選取存取範圍區段中，選取範圍。
   - 選取存取層級的帳戶。
   - 選取您要取得稽核日誌的帳戶。
7. 選擇 Create User (建立使用者)。

   會產生 API 權杖。此時會開啟一個視窗，並顯示字符字串，其中包含訊息指出這是您最後一次可以檢視字符。
8. （選用）選擇複製 API 權杖並將其存放在安全的位置。
9. 選擇關閉。

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。AppFabric 中的租戶 ID 將是您登入服務Sentinel One之網站地址的子網域。例如，如果您在 `example-company-1.sentinelone.net`地址登入Singularity Cloud您的帳戶，您的租戶 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。

服務帳戶字符

使用您在本指南 建立 的 API 權杖 Singularity Cloud區段中使用步驟產生的字符。如果您放錯位置或找不到權杖，您可以再次依照相同的步驟產生新的權杖。

> **Note**
>
> 如果在 AppFabric 擷取稽核日誌時，在 Singularity Cloud 主控台中產生新的 API 字符，則擷取將會停止。如果發生這種情況，您將需要使用新的 API 權杖更新應用程式授權，以繼續擷取稽核日誌。

Slack 為 AppFabric 設定

Slack 的任務是讓人們的工作生活更簡單、更愉快且更有生產力。這是客戶公司的生產力平台，透過無程式碼自動化增強每個人的能力、讓搜尋和知識共用順暢，以及讓團隊在推動工作時保持聯繫和參與，

從而提高效能。作為 的一部分Salesforce， Slack 深度整合到Salesforce客戶 360 中，在銷售、服務和行銷團隊之間產生超增壓生產力。若要進一步了解並Slack免費開始使用 ，請造訪 slack.com。

為了安全起見，您可以使用 AWS AppFabric 從 稽核日誌和使用者資料Slack、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Slack
- 將 AppFabric 連線至Slack您的帳戶

的 AppFabric 支援 Slack

AppFabric 支援從 接收使用者資訊和稽核日誌Slack。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Slack到支援的目的地，您必須符合下列要求：

- 您必須擁有具有 的企業網格計劃Slack。如需詳細資訊，請參閱 Slack 網站上的Slack企業網格簡介。
- 您的帳戶中必須有具有組織擁有者角色的使用者Slack。如需角色的詳細資訊，請參閱 Slack 網站上的Slack說明中心 中的 角色類型Slack。

速率限制考量

Slack 會對 Slack API 強加速率限制。如需 Slack API 速率限制的詳細資訊，請參閱 Slack 網站上的 Slack API 使用者指南中的速率限制。如果 AppFabric 和現有 Slack API 應用程式的組合超過限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件延遲最多 30 分鐘交付至目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Slack您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricSlack。若要尋找Slack使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

AppFabric Slack使用 OAuth 與 整合。有兩種方法可以建立 OAuth 應用程式：使用應用程式資訊清單或從頭開始。若要在 中建立 OAuth 應用程式Slack，請使用下列步驟。

Using an app manifest

1. 在瀏覽器中導覽至 Slack App Management UI。
2. 選擇建立新應用程式。
3. 從應用程式資訊清單選擇 。
4. 選擇您要授權 AppFabric 的工作區。
5. 在下方的輸入應用程式資訊清單方塊中，選擇 JSON，並將現有的 JSON 取代為下列項目。以適當的 AWS 區域（例如，）取代 *<region>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. 從基本資料頁面複製並儲存用戶端 ID 和用戶端秘密。
7. 對於 `auditLogs:read`範圍，您必須啟用應用程式的公有分佈。如需詳細資訊，請參閱 Slack 網站上的啟用公有分佈。

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. 從基本資料頁面複製並儲存用戶端 ID 和用戶端秘密。
4. 在 OAuth & Permissions 頁面上，選擇透過權杖輪換來加入進階權杖安全性選項。
5. 在 OAuth & Permissions 頁面的重新導向 URL 區段中新增具有下列格式的 URLs。

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

   在此 URL 中， *<region>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。
6. 對於 `auditLogs:read`範圍，您必須啟用應用程式的公有分佈。如需詳細資訊，請參閱 Slack 網站上的啟用公有分佈。

必要範圍

> **Note**
>
> 只有在您選擇從頭開始建立 OAuth 應用程式時，本節才適用。如果您選擇使用應用程式資訊清單來建立應用程式授權，請略過本節。

您必須在 OAuth 應用程式的 OAuth & Permissions Slack 頁面上新增下列使用者字符範圍： OAuth

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

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。AppFabric 中的租戶 ID 是您的Slack工作區 ID。若要取得您的租戶 ID，請遵循 Slack 網站上的Slack說明中心尋找 Slack URL 中的指示。您的Slack工作區 URL 格式類

似於 `examplecorp.slack.com`或 `examplecorp.enterprise.slack.com`。您需要的租戶 ID `examplecorp`沒有 `.slack.com`或 `.enterprise.slack.com`。

租戶名稱

輸入可識別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 Slack 將從您的 OAuth 應用程式請求用戶端 ID。若要尋找用戶端 ID，請使用下列步驟：

1. 在瀏覽器中導覽至 Slack App Management UI。
2. 選擇您搭配 AppFabric 使用的 OAuth 應用程式。
3. 從基本資料頁面將用戶端 ID 輸入 AppFabric 中的用戶端 ID 欄位。

Client secret (用戶端密碼)

AppFabric Slack 將從您的 OAuth 應用程式請求用戶端秘密。若要尋找用戶端秘密，請使用下列步驟：

1. 導覽至瀏覽器中的 Slack App Management UI。
2. 選擇您搭配 AppFabric 使用的 OAuth 應用程式。
3. 從基本資料頁面將用戶端秘密輸入 AppFabric 中的用戶端秘密欄位。

核准授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗Slack，以核准授權。若要核准 AppFabric 授權，請選擇允許。

Smartsheet 為 AppFabric 設定

Smartsheet 是一種工作管理平台，可協助您在整個企業中調整工作、人員和技術。 Smartsheet提供一組強大的企業級功能，讓每個人能夠大規模管理專案、自動化工作流程和快速建置解決方案，同時建立創新環境，同時維護安全性和合規性。

為了安全起見，您可以使用 AWS AppFabric 從 稽核日誌和使用者資料Smartsheet、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Smartsheet
- 將 AppFabric 連線至Smartsheet您的帳戶

的 AppFabric 支援 Smartsheet

AppFabric 支援從 接收使用者資訊和稽核日誌Smartsheet。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Smartsheet到支援的目的地，您必須符合下列要求：

- 您必須擁有Smartsheet商業、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 會對 Smartsheet API 強加速率限制。如需 Smartsheet API 速率限制的詳細資訊，請參閱 Smartsheet 網站上的 Smartsheet API 參考中的速率限制。

資料延遲考量

您可能會看到稽核事件最多延遲 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Smartsheet您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricSmartsheet。若要尋找 Smartsheet使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

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

1. 導覽至您Smartsheet帳戶中的開發人員工具。
2. 從開發人員工具畫面中選擇建立新應用程式。

3. 完成建立新應用程式畫面上的所有輸入欄位。
4. 使用應用程式 URL 和應用程式聯絡人/支援的任何唯一值。
5. 使用具有下列格式的重新導向 URL 做為應用程式重新導向 URL。

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

   在此 URL 中， *<region>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `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 和應用程式秘密。

必要範圍

Smartsheet 不需要您將範圍明確新增至 OAuth 組態。AppFabric 會在授權請求中向Smartsheet您的帳戶請求下列範圍：

- `READ_EVENTS`
- `READ_USERS`

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。AppFabric 中的租戶 ID 是Smartsheet您的帳戶 ID。

租戶名稱

AppFabric 將請求您的租戶 ID。輸入任何可唯一識別您Smartsheet帳戶的值。

用戶端 ID

AppFabric 會請求您的用戶端 ID。AppFabric 中的用戶端 ID 是您的Smartsheet應用程式用戶端 ID。若要在 中尋找您的應用程式用戶端 IDSmartsheet，請使用下列步驟：

1. 導覽至您Smartsheet帳戶中的開發人員工具。
2. 選取您用來與 AppFabric 連線的 OAuth 應用程式。
3. 從 App Profile 畫面將應用程式用戶端 ID 輸入 AppFabric 中的用戶端 ID 欄位。

Client secret (用戶端密碼)

AppFabric 將請求您的用戶端秘密。AppFabric 中的用戶端秘密是您的Smartsheet應用程式秘密。若要在 中尋找您的應用程式秘密Smartsheet，請使用下列步驟：

1. 導覽至您Smartsheet帳戶中的開發人員工具。
2. 選取您用來與 AppFabric 連線的 OAuth 應用程式。
3. 從 App Profile 畫面將應用程式秘密輸入 AppFabric 中的 Client Secret 欄位。

核准授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗Smartsheet，以核准授權。若要核准 AppFabric 授權，請選擇允許。

Terraform Cloud 為 AppFabric 設定

HashiCorp Terraform Cloud 是全球最廣泛使用的多雲端佈建產品。Terraform 生態系統有超過 3，000 個供應商、14，000 個模組和 2.5 億次下載。 Terraform Cloud是採用 的最快方式Terraform，提供從業人員、團隊和全球企業在基礎設施上建立和協作所需的一切，並管理安全、合規和營運限制的風險。

為了安全起見，您可以使用 AWS AppFabric 從 接收稽核日誌和使用者資料Terraform Cloud、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Terraform Cloud
- 將 AppFabric 連線至Terraform Cloud您的帳戶

的 AppFabric 支援 Terraform Cloud

AppFabric 支援從 接收使用者資訊和稽核日誌Terraform Cloud。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Terraform Cloud到支援的目的地，您必須符合下列要求：

- 若要存取稽核日誌，您必須擁有 Terraform Cloud Plus Edition 計畫，且為組織的擁有者。如需Terraform Cloud計劃的詳細資訊，請參閱 HashiCorp Terraform 網站上的Terraform定價。

- TBD 稽核日誌適用於可以從Terraform Cloud帳戶建立的組織。

速率限制考量

Terraform Cloud 會對 Terraform Cloud API 強加速率限制。如需 Terraform Cloud API 速率限制的詳細資訊，請參閱 Terraform Cloud 網站上的Terraform Cloud開發人員管理一般設定中的 API 速率限制。如果 AppFabric 和現有 Terraform Cloud API 應用程式的組合超過 的限制，AppFabric 中出現Terraform Cloud的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件最多延遲 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Terraform Cloud您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricTerraform Cloud。若要尋找Terraform Cloud使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立組織 API 字符

AppFabric Terraform Cloud使用組織 API 字符與 整合。如需Terraform Cloud組織 API 權杖的詳細資訊，請參閱組織 API 權杖。若要建立組織，請遵循建立組織中的指示。若要在 中建立組織 API 字符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、設定，然後選擇 API 字符。
3. 在組織字符下，選擇建立組織字符，然後選擇產生字符。
4. （選用）輸入字符的過期日期或時間，或建立永不過期的字符。
5. 複製並儲存字符。稍後您會在 AppFabric 中需要此功能。如果您在儲存字符之前關閉頁面，則必須撤銷舊字符並建立新的字符。

應用程式授權

租用戶 ID

AppFabric 將請求租戶 ID。Terraform Cloud 您帳戶的租戶 ID 是您帳戶的目前組織 URL。您可以登入您的Terraform Cloud組織並複製目前的組織 URL 來找到。租用戶 ID 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。

服務帳戶字符

AppFabric 將請求您的服務帳戶字符。AppFabric 中的服務帳戶字符是您在 中建立的組織 API 字符建立組織 API 字符。

Webex by Cisco 為 AppFabric 設定

Cisco 是推動網際網路技術的全球領導者。 透過重新構想應用程式、保護您的資料、轉換基礎設施，以及為您的團隊提供全球和包容性的未來，來Cisco激發新的可能性。

關於 Webex by Cisco

Webex 是雲端型協作解決方案的領導供應商，包括視訊會議、通話、簡訊、事件、客戶經驗解決方案，例如聯絡中心和專門打造Webex的協作裝置。 專注於提供包容性協作體驗，可推動創新，利用 AI 和Machine Learning來消除地理、語言、人格和熟悉技術的障礙。其解決方案的設計以安全性和隱私權為基礎。 與全球領先的商業和生產力應用程式Webex搭配使用，透過單一應用程式和界面提供。如需進一步了解，請參閱webex.com。

為了安全起見，您可以使用 AWS AppFabric 從 稽核日誌和使用者資料Webex、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Webex
- 將 AppFabric 連線至Webex您的帳戶

的 AppFabric 支援 Webex

AppFabric 支援從 接收使用者資訊和稽核日誌Webex。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Webex到支援的目的地，您必須符合下列要求：

- 您必須擁有 Collaboration Flex 計畫、Meet Plan、Call Plan 或更高版本。如需建立或升級至適用Webex計劃類型的詳細資訊，請參閱 Webex 網站上的Webex所有功能的定價。
- 您的帳戶必須擁有 Pro Pack 授權，才能存取其中一個 Cisco AuditLog APIs提供的安全稽核事件。
- 您必須擁有具有組織管理員 > 完整管理員角色的使用者。
- 完整管理員的管理員角色組態必須啟用合規主管選項。

速率限制考量

Webex 會對 Webex API 強加速率限制。如需 Webex API 速率限制的詳細資訊，請參閱 Webex 網站上的Webex開發人員指南中的速率限制。如果 AppFabric 和現有 Webex API 應用程式的組合超過限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件延遲最多 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Webex您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricWebex。若要尋找Webex使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

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

1. 請遵循《 Webex開發人員指南》的整合與授權頁面中註冊整合一節中的指示。
2. 使用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>* 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。

必要範圍

您必須將下列範圍新增至 Webex OAuth 應用程式：

- `spark-compliance:events_read`
- `audit:events_read`
- `spark-admin:people_read`

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。AppFabric 中的租戶 ID 是您的Webex組織 ID。如需有關如何尋找Webex組織 ID 的資訊，請參閱 Webex說明中心網站上的在 CiscoWebex Control Hub 中查詢您的組織 ID。

租戶名稱

輸入可識別此唯一Webex執行個體的名稱。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 會請求您的Webex用戶端 ID。若要尋找您的Webex用戶端 ID，請使用下列步驟：

1. 在 https：//https://developer.webex.com 登入Webex您的帳戶。
2. 選擇右上角的虛擬人偶。
3. 選擇我的 Webex 應用程式。
4. 選擇您用於 AppFabric 的 OAuth2 應用程式。
5. 在 AppFabric 的用戶端 ID 欄位中輸入此頁面的用戶端 ID。

Client secret (用戶端密碼)

AppFabric 將請求您的Webex用戶端秘密。當您最初建立 OAuth 應用程式時， Webex只會顯示您的用戶端秘密一次。若要在未儲存初始用戶端秘密時產生新的用戶端秘密，請使用下列步驟：

1. 在 https：//https://developer.webex.com 登入Webex您的帳戶。
2. 選擇右上角的虛擬人偶。
3. 選擇我的 Webex 應用程式。
4. 選擇您用於 AppFabric 的 OAuth2 應用程式。

5. 在此頁面上，產生新的用戶端秘密。
6. 在 AppFabric 的用戶端秘密欄位中輸入新的用戶端秘密。

核准授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗Webex，以核准授權。若要核准 AppFabric 授權，請選擇接受。

Zendesk 為 AppFabric 設定

Zendesk 2007 年開始客戶體驗革命，讓全球任何企業都能將客戶服務上線。今天， Zendesk 是每個人在任何地方都擁有卓越服務的擁護者，並支援數十億個對話，透過電話、聊天、電子郵件、簡訊、社交管道、社群、評論網站和協助中心連接超過 100，000 個品牌和數億個客戶。 Zendesk產品是為愛所打造。該公司在丹麥哥本哈根被設想，在加利佛尼亞州建立和成長，目前在全球僱用超過 6，000 名員工。

為了安全起見，您可以使用 AWS AppFabric 從 稽核日誌和使用者資料Zendesk、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Zendesk
- 將 AppFabric 連線至Zendesk您的帳戶

的 AppFabric 支援 Zendesk

AppFabric 支援從 接收使用者資訊和稽核日誌Zendesk。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Zendesk到支援的目的地，您必須滿足下列要求：

- 您必須擁有 Zendesk Suite Enterprise 或 Enterprise Plus 帳戶或 Zendesk Support Enterprise 帳戶。如需建立或升級至Zendesk 企業帳戶的詳細資訊，請參閱 Zendesk 網站上的檢查您的計劃類型Zendesk。
- Zendesk 您的帳戶中必須有具有管理員角色的使用者。如需角色的詳細資訊，請參閱 Zendesk 網站上的了解Zendesk支援使用者角色。

速率限制考量

Zendesk 會對 Zendesk API 強加速率限制。如需 Zendesk API 速率限制的詳細資訊，請參閱 Zendesk 網站上的Zendesk開發人員指南中的速率限制。如果 AppFabric 和現有 Zendesk API 應用程式的組合超過限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件延遲最多 30 分鐘交付到目的地。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。不過，這可以在帳戶層級進行自訂。如需協助，請聯絡 支援。

將 AppFabric 連線至Zendesk您的帳戶

在 AppFabric 服務中建立應用程式套件之後，您必須使用 授權 AppFabricZendesk。若要尋找Zendesk使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立 OAuth 應用程式

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

1. 請遵循 Zendesk Support 網站上的使用 OAuth 身分驗證與應用程式文章中向 Zendesk 註冊應用程式一節中的指示。 OAuth
2. 使用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>` 是您設定 AppFabric 應用程式套件 AWS 區域 之 的程式碼。例如，美國東部（維吉尼亞北部）區域的程式碼為 。 `us-east-1`對於該區域，重新導向 URL 為 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。AppFabric 中的租用戶 ID 是您的Zendesk子網域。如需尋找Zendesk子網域的詳細資訊，請參閱 Zendesk 支援網站上的我可以在哪裡找到我的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 會請求用戶端 ID。AppFabric 中的用戶端 ID 是您的 Zendesk API 唯一識別符。若要尋找您的 Zendesk 唯一識別符，請使用下列步驟：

1. 導覽至您Zendesk帳戶中的管理員中心。
2. 選擇應用程式和整合。
3. 選擇 APIs、ZendeskAPIs。
4. 選擇 OAuth 用戶端索引標籤。
5. 選擇您為 AppFabric 建立的 OAuth 應用程式。
6. 在 AppFabric 的用戶端 ID 欄位中輸入 OAuth 用戶端的唯一識別符。

Client secret (用戶端密碼)

AppFabric 將請求用戶端秘密。AppFabric 中的用戶端秘密是您的Zendesk秘密權杖。當您第一次建立 OAuth 應用程式時， Zendesk 只會Zendesk顯示您的秘密權杖一次。若要在未儲存初始秘密權杖時產生新的秘密權杖，請使用下列步驟：

1. 導覽至您Zendesk帳戶中的管理員中心。
2. 選擇應用程式和整合。
3. 選擇 APIs、ZendeskAPIs。
4. 選擇 OAuth 用戶端索引標籤。
5. 選擇您為 AppFabric 建立的 OAuth 應用程式。
6. 選擇機密字符欄位旁的重新產生按鈕。
7. 在 AppFabric 的用戶端秘密欄位中輸入新的秘密字符。

核准授權

在 AppFabric 中建立應用程式授權後，您會收到來自 的快顯視窗Zendesk以核准授權。若要核准 AppFabric 授權，請選擇允許。

Zoom 為 AppFabric 設定

Zoom 是一種all-in-one的智慧型協作平台，可讓企業和個人更輕鬆、更身歷其境且更動態地連線。Zoom技術將人員放在中心、實現有意義的連線、促進現代協作，並透過團隊聊天、電話、會議、全通道雲端聯絡中心、智慧型錄音、白板等解決方案，在一個產品中推動人類創新。

為了安全起見，您可以使用 AWS AppFabric 從 稽核日誌和使用者資料Zoom、將資料標準化為開放網路安全結構描述架構 (OCSF) 格式，並將資料輸出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 串流。

主題

- 的 AppFabric 支援 Zoom
- 將 AppFabric 連線至Zoom您的帳戶

的 AppFabric 支援 Zoom

AppFabric 支援從 接收使用者資訊和稽核日誌Zoom。

先決條件

若要使用 AppFabric 將稽核日誌從 傳輸Zoom到支援的目的地，您必須滿足下列要求：

- 您必須擁有Zoom專業、商業、教育或企業計劃。
- 您的Zoom管理員角色必須具有建立server-to-server OAuth 應用程式的許可。如需有關啟用server-to-server OAuth 應用程式的資訊，請參閱 Zoom 網站上的Zoom開發人員指南中的Server-to-Server OAuth 頁面的啟用許可區段。
- 您的Zoom管理員角色必須具有檢視管理員活動日誌和登入/登出稽核活動的許可。如需啟用檢視稽核活動許可的詳細資訊，請參閱Zoom支援網站上的使用角色管理和使用管理員活動日誌。

速率限制考量

Zoom 會對 Zoom API 強加速率限制。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 和現有Zoom應用程式的組合超過限制，AppFabric 中出現的稽核日誌可能會延遲。

資料延遲考量

您可能會看到稽核事件交付到目的地的延遲時間約為 24 小時。這是因為應用程式提供的稽核事件延遲，以及為了減少資料遺失而採取的預防措施。

將 AppFabric 連線至Zoom您的帳戶

在 AppFabric 服務中建立應用程式套件後，您必須使用 授權 AppFabricZoom。若要尋找Zoom使用 AppFabric 授權所需的資訊，請使用下列步驟。

建立server-to-server OAuth 應用程式

AppFabric 使用server-to-server OAuth 搭配應用程式登入資料來與 整合Zoom。若要在 中建立server-to-server OAuth 應用程式Zoom，請遵循《 Zoom 開發人員指南》中建立Server-to-Server OAuth 應用程式的指示。AppFabric 不支援 Zoom Webhook，您可以略過新增 Webhook 訂閱的 區段。

必要範圍

Zoom 提供兩種類型的範圍：精細範圍 （適用於新建立的應用程式） 和傳統範圍 （適用於先前建立的應用程式）。

您必須將下列精細範圍新增至Zoomserver-to-server OAuth 應用程式：

- `report:read:user_activities:admin`
- `report:read:operation_logs:admin`
- `user:read:email:admin`
- `user:read:user:admin`

如果您使用先前建立的應用程式，則需要新增下列傳統範圍：

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

應用程式授權

租用戶 ID

AppFabric 將請求您的租戶 ID。AppFabric 中的租戶 ID 是Zoom帳戶 ID。若要尋找Zoom您的帳戶 ID，請使用下列步驟：

1. 導覽至 Zoom 市集。
2. 選擇管理。
3. 選擇您用於 AppFabric server-to-server OAuth 應用程式。
4. 從 App Credentials 頁面將帳戶 ID 輸入 AppFabric 中的租戶 ID 欄位。

租戶名稱

輸入可識別此唯一Zoom組織的名稱。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 會請求您的用戶端 ID。若要尋找您的Zoom用戶端 ID，請使用下列步驟：

1. 導覽至 Zoom 市集。
2. 選擇管理。
3. 選擇您用於 AppFabric server-to-server OAuth 應用程式。
4. 從 App Credentials 頁面將用戶端 ID 輸入 AppFabric 中的用戶端 ID 欄位。

Client secret (用戶端密碼)

AppFabric 將請求您的用戶端秘密。若要尋找您的Zoom用戶端秘密，請使用下列步驟：

1. 導覽至 Zoom 市集。
2. 選擇管理。
3. 選擇您用於 AppFabric server-to-server OAuth 應用程式。
4. 從 App Credentials 頁面將用戶端秘密輸入 AppFabric 中的用戶端秘密欄位。

稽核日誌交付

Zoom 每 24 小時透過存取 API 來提供稽核日誌。使用 AppFabric 檢視稽核日誌時，您看到的 資料Zoom適用於前一天的活動。

AppFabric 中的相容安全工具和服務，以確保安全

AWS AppFabric for Security 支援與下列安全工具和服務的整合。選擇 服務的名稱，以取得如何設定 AppFabric 以安全連線至服務的詳細資訊。

主題

- Barracuda XDR
- Dynatrace

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

Barracuda XDR

Barracuda Networks 是受信任的合作夥伴和雲端優先安全解決方案的領導供應商，使用創新解決方案來保護電子郵件、網路、資料和應用程式，以因應企業旅程的成長和適應。 Barracuda XDR 是一種開放式延伸偵測和回應解決方案，結合了複雜的技術與安全營運中心 (SOC) 的安全分析師團隊。該Barracuda XDR平台每天分析來自 40 多個整合資料來源的數十億個原始事件，以及映射到 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 稽核日誌擷取考量事項

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

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 使用開放網路安全結構描述架構 (OCSF) 標準化資料，並以 JSON 格式輸出資料。

輸出位置

Barracuda XDR 支援從 Amazon Security Lake 接收稽核日誌。若要將資料從 AppFabric 傳送至 Barracuda XDR，請遵循下列指示：

1. 將資料傳送至 Amazon Security Lake：設定 AppFabric 透過 Amazon Data Firehose 將資料傳送至 Amazon Security Lake。如需詳細資訊，請參閱Amazon Security Lake。
2. 將資料傳送至 Barracuda XDR：設定 從 Amazon Security Lake Barracuda XDR接收稽核日誌。如需詳細資訊，請參閱設定和使用 Amazon Security Lake。

Dynatrace

Dynatrace® Platform 結合了廣泛且深入的可觀測性和持續的執行期應用程式安全性，以及進階 AIOps，以提供來自資料的答案和智慧型自動化。這可讓創新者現代化和自動化雲端操作、更快速安全地交付軟體，並確保完美的數位體驗。

AWS AppFabric 稽核日誌擷取考量事項

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

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 使用開放網路安全結構描述架構 (OCSF) 標準化資料，並以 JSON 格式輸出資料。

輸出位置

Dynatrace Platform 支援從下列 AppFabric 輸出位置接收稽核日誌。

- Amazon Simple Storage Service (Amazon S3)
  - 若要設定 從包含稽核日誌的 Amazon S3 儲存貯體Dynatrace Platform接收資料，請遵循 上 Dynatrace 的 S3 Log Forwarder 專案中的指示GitHub。

Logz.io

Logz.io 協助雲端原生企業透過 Logz.io Open 360 平台監控和保護其環境 – 將可觀測性和安全性從高成本、低價值的負擔轉換為高價值、經濟實惠的推動因素，以獲得更好的業務成果。

Logz.io 雲端 SIEM 會透過快速查詢、多維度偵測和深度可自訂的安全內容，直接解決從資料過載到全局網路技能差距等目前主要的安全挑戰，以協助監控和調查您雲端環境的完整範圍，無論資料量為何，都不會降低效能。

Logz.io 解決方案專為提供進階威脅分析和調查而打造，並降低複雜性和成本。客戶由專門的安全分析師、威脅內容即服務和 AI 支援的 功能提供支援，這些功能旨在協助減少雜訊資料，並專注於可讓團隊快速排定實際威脅優先順序的資訊。

AWS AppFabric 稽核日誌擷取考量事項

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

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 會以 JSON 格式在來源應用程式所使用的原始結構描述中輸出資料。
- OCSF - JSON
  - AppFabric 使用開放網路安全結構描述架構 (OCSF) 標準化資料，並以 JSON 格式輸出資料。

輸出位置

Logz.io 支援下列 AppFabric 輸出位置：

- Amazon Data Firehose
  - 若要設定 Firehose 交付串流以便將資料傳送至 Logz.io，請遵循《Amazon Data Firehose 開發人員指南》中的Logz.io為您的目的地選擇中的指示。
- Amazon Simple Storage Service (Amazon S3)
  - 若要Logz.io設定 從包含稽核日誌的 Amazon S3 儲存貯體接收資料，請遵循 Logz.io 網站上的設定 Amazon S3 儲存貯體中的指示。

Netskope

Netskope是全球網路安全領導者，正在重新定義雲端、資料和網路安全，以協助組織套用零信任原則來保護資料。Netskope 平台快速且易於使用，可為人員、裝置和資料提供最佳化的存取和零信任安全性。 Netskope協助客戶降低風險、加速效能，並取得任何雲端、Web 和私有應用程式活動的無可匹敵可見性。數千名客戶，包括超過 25 個 Fortune 100、信任Netskope及其強大的 NewEdge 網路，以因應不斷演進的威脅、新的風險、技術轉移、組織和網路變更，以及新的法規要求。了解 如何Netskope協助客戶準備好接受 SASE 旅程中的任何內容，請造訪 netskope.com。

AWS AppFabric 稽核日誌擷取考量

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

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 會以 JSON 格式輸出來源應用程式使用的原始結構描述中的資料。
- OCSF - JSON
  - AppFabric 使用開放網路安全結構描述架構 (OCSF) 標準化資料，並以 JSON 格式輸出資料。

輸出位置

Netskope 支援下列 AppFabric 輸出位置：

- Amazon Simple Storage Service (Amazon S3)
  - 若要Netskope將 設定為從包含稽核日誌的 Amazon S3 儲存貯體接收資料，請遵循 Netskope 網站上的 Amazon Web Services S3 資料保護中的指示。

NetWitness

NetWitness 是延伸偵測和回應 (XDR) 軟體的領導開發人員。他們高度重視安全的客戶的全球基礎倚賴 NetWitness「XDR」來防禦複雜且積極的對手。藉由業界最完整、整合且成熟的平台來偵測、調查和回應數位攻擊，NetWitnessXDR 是現代有效 SOC 的統一基礎。

由於其高度模組化的架構，NetWitnessXDR 可在雲端、內部部署、行動和遠端工作者或介於兩者之間的任何位置偵測威脅。結合套用的威脅情報和使用者行為分析，NetWitnessPlatform XDR 可提供完整的可見性，以偵測威脅、排定活動優先順序、調查和自動化回應。所有這些都為安全分析師提供了更好、更快的效率，以保持安全操作領先於業務影響的威脅。

AWS AppFabric 稽核日誌擷取考量事項

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

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 會以 JSON 格式在來源應用程式所使用的原始結構描述中輸出資料。
- OCSF - JSON

- AppFabric 使用開放網路安全結構描述架構 (OCSF) 標準化資料，並以 JSON 格式輸出資料。

輸出位置

NetWitness 支援下列 AppFabric 輸出位置：

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

Amazon QuickSight

Amazon QuickSight 以超大規模的統一商業智慧 (BI) 為資料驅動型組織提供支援。透過 QuickSight，所有使用者都可以透過現代互動式儀表板、分頁報告、內嵌分析和自然語言查詢，滿足來自相同事實來源的不同分析需求。您可以分析 QuickSight 中的 AWS AppFabric 稽核日誌資料，方法是選擇 Amazon Simple Storage Service (Amazon S3) 儲存貯體，其中將安全日誌的 AppFabric 儲存為您的來源。

AppFabric 稽核日誌擷取考量事項

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

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 會以 JSON 格式在來源應用程式所使用的原始結構描述中輸出資料。
- OCSF - JSON
  - AppFabric 使用開放網路安全結構描述架構 (OCSF) 標準化資料，並以 JSON 格式輸出資料。

輸出位置

QuickSight 支援下列 AppFabric 輸出位置：

- Amazon S3
  - 您可以使用 Amazon S3 檔案建立資料集，將資料從 Amazon S3 直接擷取到 QuickSight。若要確認您的目標檔案集不超過 QuickSight 資料來源配額，請參閱 QuickSight 使用者指南中的資料來源配額。

- 如果您的檔案集超過 Amazon S3 資料來源的 QuickSight 配額，您可以使用 Amazon Athena 和資料表在 Amazon S3 中擷取資料。 Amazon Athena AWS Glue 在 QuickSight 資料集中使用 Athena 會產生額外費用。如需 Athena 定價的詳細資訊，請參閱 Athena 定價頁面。

  若要使用 Athena：

  1. 遵循《Athena 使用者指南》中的使用 AWS Glue 連線至 Amazon S3 中的資料來源中的指示。
  2. 請遵循 QuickSight 使用者指南中的使用 Athena 資料建立資料集中的指示。

Rapid7

Rapid7， Inc. 致力於建立更安全的數位世界，讓網路安全更簡單且更易於存取。 Rapid7 讓安全專業人員能夠透過best-in-class技術、尖端研究和廣泛的策略專業知識來管理現代攻擊面。 Rapid7的全方位安全解決方案可協助超過 10，000 名全球客戶整合雲端風險管理和威脅偵測，以減少攻擊面，並快速且精準地消除威脅。

AWS AppFabric 稽核日誌擷取考量事項

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

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 會以 JSON 格式在來源應用程式所使用的原始結構描述中輸出資料。
- OCSF - JSON
  - AppFabric 會使用開放網路安全結構描述架構 (OCSF) 標準化資料，並以 JSON 格式輸出資料。

輸出位置

Rapid7 支援下列 AppFabric 輸出位置：

- Amazon Simple Storage Service (Amazon S3)
  - 若要設定 Rapid7 從包含稽核日誌的 Amazon S3 儲存貯體接收資料，請遵循Rapid7部落格網站上的如何使用 InsightIDR 監控 Amazon S3 活動部落格文章中的指示。

Amazon Security Lake

Amazon Security Lake 會自動將來自 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存放在您 中的專用資料湖 AWS 帳戶。使用 Security Lake，您可以更完整地了解整個組織的安全資料。Security Lake 已採用開放網路安全結構描述架構 (OCSF)，這是一種開放原始碼安全事件結構描述。透過 OCSF 支援，此服務會標準化和合併來自 AWS 和各種企業安全資料來源的安全性資料。

AppFabric 稽核日誌擷取考量

您可以將自訂來源新增至 Security Lake， AWS 帳戶 以將 SaaS 稽核日誌傳送到 中的 Amazon Security Lake。下列各節說明要與 Security Lake 搭配使用的 AppFabric 輸出結構描述、輸出格式和輸出目的地。

結構描述和格式

Security Lake 支援下列 AppFabric 輸出結構描述和格式：

- OCSF - JSON
  - AppFabric 使用開放網路安全結構描述架構 (OCSF) 標準化資料，並以 JSON 格式輸出資料。

輸出位置

Security Lake 支援 AppFabric 做為自訂來源，使用 Amazon Data Firehose 交付串流做為 AppFabric 擷取輸出位置。若要設定 AWS Glue 資料表和 Firehose 交付串流，以及在 Security Lake 中設定自訂來源，請使用下列程序。

建立 AWS Glue 資料表

1. 導覽至 Amazon Simple Storage Service (Amazon S3)，並使用您選擇的名稱建立儲存貯體。
2. 導覽至 AWS Glue 主控台。
3. 對於資料型錄，請前往資料表區段，然後選擇新增資料表。
4. 輸入您為此資料表選擇的名稱。
5. 選取您在步驟 1 中建立的 Amazon S3 儲存貯體。
6. 針對資料格式，選取 JSON，然後選擇下一步。
7. 在選擇或定義結構描述頁面上，選擇將結構描述編輯為 JSON。
8. 輸入下列結構描述，並完成 AWS Glue 資料表建立程序。

```
[
    {
        "Name": "message",
        "Type": "string"
    },
    {
        "Name": "process",
        "Type":
 "struct<name:string,pid:int,user:struct<name:string,type:string,domain:string,uid:string,t
    },
    {
        "Name": "status",
        "Type": "string"
    },
    {
        "Name": "time",
        "Type": "bigint"
    },
    {
        "Name": "device",
        "Type":
 "struct<name:string,owner:struct<name:string,type:string,uid:string,type_id:int,risk_level
    },
    {
        "Name": "metadata",
        "Type":
 "struct<version:string,product:struct<name:string,version:string,uid:string,data_classific
    },
    {
        "Name": "severity",
        "Type": "string"
    },
    {
        "Name": "duration",
        "Type": "int"
    },
    {
        "Name": "type_name",
        "Type": "string"
    },
    {
        "Name": "activity_id",
        "Type": "int"
```

```
    },
    {
        "Name": "type_uid",
        "Type": "int"
    },
    {
        "Name": "observables",
        "Type": "array<struct<name:string,type:string,type_id:int,value:string>>"
    },
    {
        "Name": "category_name",
        "Type": "string"
    },
    {
        "Name": "class_uid",
        "Type": "int"
    },
    {
        "Name": "category_uid",
        "Type": "int"
    },
    {
        "Name": "class_name",
        "Type": "string"
    },
    {
        "Name": "timezone_offset",
        "Type": "int"
    },
    {
        "Name": "end_time",
        "Type": "bigint"
    },
    {
        "Name": "activity_name",
        "Type": "string"
    },
    {
        "Name": "cloud",
        "Type":
"struct<account:struct<name:string,type:string,uid:string,type_id:int>,project_uid:string,
    },
    {
        "Name": "query_info",
```

```
        "Type": "struct<name:string,uid:string,query_string:string>"
    },
    {
        "Name": "query_result",
        "Type": "string"
    },
    {
        "Name": "query_result_id",
        "Type": "int"
    },
    {
        "Name": "severity_id",
        "Type": "int"
    },
    {
        "Name": "status_code",
        "Type": "string"
    },
    {
        "Name": "status_detail",
        "Type": "string"
    },
    {
        "Name": "status_id",
        "Type": "int"
    },
    {
        "Name": "network_interfaces",
        "Type":
 "array<struct<name:string,type:string,hostname:string,mac:string,type_id:int,ip:string>>"
    },
    {
        "Name": "file",
        "Type":
 "struct<attributes:int,name:string,type:string,path:string,type_id:int,accessor:struct<nam
    },
    {
        "Name": "actor",
        "Type":
 "struct<process:struct<pid:int,file:struct<name:string,size:bigint,type:string,version:str
    },
    {
        "Name": "dst_endpoint",
```

```
        "Type":
"struct<owner:struct<name:string,type:string,uid:string,type_id:int,full_name:string,risk_
    },
    {
        "Name": "src_endpoint",
        "Type":
"struct<name:string,owner:struct<name:string,type:string,domain:string,uid:string,org:stru
    },
    {
        "Name": "user",
        "Type":
"struct<name:string,type:string,groups:array<struct<name:string,uid:string>>,type_id:int>"
    },
    {
        "Name": "resource",
        "Type":
"struct<version:string,uid:string,agent_list:array<struct<name:string,type:string,uid:stri
    },
    {
        "Name": "privileges",
        "Type": "array<string>"
    },
    {
        "Name": "action",
        "Type": "string"
    },
    {
        "Name": "action_id",
        "Type": "int"
    },
    {
        "Name": "protocol_ver",
        "Type": "string"
    },
    {
        "Name": "proxy",
        "Type":
"struct<name:string,port:int,type:string,ip:string,hostname:string,uid:string,type_id:int,
    },
    {
        "Name": "client_hassh",
        "Type":
"struct<algorithm:string,fingerprint:struct<value:string,algorithm:string,algorithm_id:int
    },
```

```
    {
        "Name": "authorizations",
        "Type": "array<string>"
    },
    {
        "Name": "proxy_tls",
        "Type":
"struct<version:string,certificate:struct<version:string,uid:string,subject:string,issuer:
    },
    {
        "Name": "load_balancer",
        "Type":
"struct<name:string,classification:string,dst_endpoint:struct<owner:struct<type:string,dom
    },
    {
        "Name": "disposition_id",
        "Type": "int"
    },
    {
        "Name": "disposition",
        "Type": "string"
    },
    {
        "Name": "proxy_traffic",
        "Type": "struct<bytes:bigint,packets:int>"
    },
    {
        "Name": "auth_type_id",
        "Type": "int"
    },
    {
        "Name": "proxy_http_response",
        "Type": "struct<code:int,message:string,status:string,length:int>"
    },
    {
        "Name": "server_hassh",
        "Type":
"struct<algorithm:string,fingerprint:struct<value:string,algorithm:string,algorithm_id:int
    },
    {
        "Name": "auth_type",
        "Type": "string"
    },
    {
```

```
        "Name": "firewall_rule",
        "Type": "struct<version:string,uid:string>"
    },
    {
        "Name": "proxy_connection_info",
        "Type":
"struct<direction:string,direction_id:int,protocol_num:int,protocol_ver:string>"
    },
    {
        "Name": "connection_info",
        "Type": "struct<direction:string,direction_id:int>"
    },
    {
        "Name": "api",
        "Type":
"struct<request:struct<data:string,uid:string>,response:struct<error:string,code:int,messa
    },
    {
        "Name": "attacks",
        "Type":
"array<struct<version:string,tactics:array<struct<name:string,uid:string>>,technique:struc
    },
    {
        "Name": "raw_data",
        "Type": "string"
    },
    {
        "Name": "email_uid",
        "Type": "string"
    },
    {
        "Name": "malware",
        "Type":
"array<struct<name:string,path:string,uid:string,classification_ids:array<int>,cves:array<
    },
    {
        "Name": "start_time_dt",
        "Type": "string"
    },
    {
        "Name": "direction",
        "Type": "string"
    },
    {
```

```
        "Name": "smtp_hello",
        "Type": "string"
    },
    {
        "Name": "unmapped",
        "Type": "string"
    },
    {
        "Name": "direction_id",
        "Type": "int"
    },
    {
        "Name": "email_auth",
        "Type":
"struct<spf:string,dkim:string,dkim_domain:string,dkim_signature:string,dmarc:string,dmarc
    },
    {
        "Name": "email",
        "Type":
"struct<uid:string,from:string,to:array<string>,data_classification:struct<category:string
    },
    {
        "Name": "impact_id",
        "Type": "int"
    },
    {
        "Name": "resources",
        "Type":
"array<struct<owner:struct<name:string,type:string,uid:string,type_id:int,full_name:string
    },
    {
        "Name": "finding_info",
        "Type":
"struct<title:string,uid:string,attacks:array<struct<version:string,tactics:array<struct<n
    },
    {
        "Name": "evidences",
        "Type":
"array<struct<process:struct<name:string,pid:int,file:struct<name:string,type:string,versi
    },
    {
        "Name": "impact",
        "Type": "string"
    },
```

```
    {
        "Name": "count",
        "Type": "int"
    },
    {
        "Name": "confidence_id",
        "Type": "int"
    },
    {
        "Name": "enrichments",
        "Type":
 "array<struct<data:string,name:string,type:string,value:string,provider:string>>"
    },
    {
        "Name": "rcode",
        "Type": "string"
    },
    {
        "Name": "app_name",
        "Type": "string"
    },
    {
        "Name": "rcode_id",
        "Type": "int"
    },
    {
        "Name": "query",
        "Type":
 "struct<type:string,hostname:string,class:string,opcode_id:int,packet_uid:int>"
    },
    {
        "Name": "proxy_endpoint",
        "Type":
 "struct<name:string,owner:struct<name:string,type:string,domain:string,uid:string,groups:a
    },
    {
        "Name": "response_time",
        "Type": "bigint"
    },
    {
        "Name": "delay",
        "Type": "int"
    },
    {
```

```
        "Name": "start_time",
        "Type": "bigint"
    },
    {
        "Name": "proxy_http_request",
        "Type":
 "struct<version:string,url:struct<port:int,scheme:string,path:string,hostname:string,query
    },
    {
        "Name": "version",
        "Type": "string"
    },
    {
        "Name": "stratum",
        "Type": "string"
    },
    {
        "Name": "stratum_id",
        "Type": "int"
    },
    {
        "Name": "dispersion",
        "Type": "int"
    },
    {
        "Name": "traffic",
        "Type":
 "struct<bytes_out:int,chunks:bigint,bytes:int,packets:int,packets_in:bigint>"
    },
    {
        "Name": "precision",
        "Type": "int"
    },
    {
        "Name": "size",
        "Type": "int"
    },
    {
        "Name": "actual_permissions",
        "Type": "int"
    },
    {
        "Name": "base_address",
        "Type": "string"
```

```
    },
    {
        "Name": "requested_permissions",
        "Type": "int"
    },
    {
        "Name": "end_time_dt",
        "Type": "string"
    },
    {
        "Name": "compliance",
        "Type":
"struct<control:string,status:string,standards:array<string>,status_id:int>"
    },
    {
        "Name": "remediation",
        "Type": "struct<desc:string>"
    },
    {
        "Name": "kb_article_list",
        "Type":
"array<struct<os:struct<name:string,type:string,type_id:int,cpe_name:string,edition:string
    },
    {
        "Name": "peripheral_device",
        "Type":
"struct<name:string,class:string,uid:string,model:string,serial_number:string,vendor_name:
    },
    {
        "Name": "time_dt",
        "Type": "string"
    },
    {
        "Name": "group",
        "Type": "struct<name:string,type:string,uid:string>"
    },
    {
        "Name": "users",
        "Type":
"array<struct<name:string,type:string,uid:string,type_id:int,risk_level:string,risk_level_
    },
    {
        "Name": "confidence_score",
        "Type": "int"
```

```
    },
    {
        "Name": "state",
        "Type": "string"
    },
    {
        "Name": "state_id",
        "Type": "int"
    },
    {
        "Name": "evidence",
        "Type": "string"
    },
    {
        "Name": "confidence",
        "Type": "string"
    },
    {
        "Name": "risk_level",
        "Type": "string"
    },
    {
        "Name": "risk_score",
        "Type": "int"
    },
    {
        "Name": "impact_score",
        "Type": "int"
    },
    {
        "Name": "risk_level_id",
        "Type": "int"
    },
    {
        "Name": "finding",
        "Type":
 "struct<title:string,uid:string,modified_time:bigint,modified_time_dt:string,first_seen_ti
    },
    {
        "Name": "user_result",
        "Type":
 "struct<name:string,type:string,uid:string,type_id:int,account:struct<name:string,uid:stri
    },
    {
```

```
        "Name": "codes",
        "Type": "array<int>"
    },
    {
        "Name": "command",
        "Type": "string"
    },
    {
        "Name": "type",
        "Type": "string"
    },
    {
        "Name": "kernel",
        "Type": "struct<name:string,type:string,type_id:int>"
    },
    {
        "Name": "http_response",
        "Type":
"struct<code:int,status:string,http_headers:array<struct<name:string,value:string>>>"
    },
    {
        "Name": "http_request",
        "Type":
"struct<url:struct<scheme:string,path:string,hostname:string,query_string:string,category_
    },
    {
        "Name": "tls",
        "Type":
"struct<version:string,certificate:struct<subject:string,issuer:string,fingerprints:array<
    },
    {
        "Name": "web_resources",
        "Type":
"array<struct<name:string,type:string,data_classification:struct<category:string,category_
    },
    {
        "Name": "http_cookies",
        "Type":
"array<struct<name:string,value:string,is_http_only:boolean,is_secure:boolean,samesite:str
    },
    {
        "Name": "type_id",
        "Type": "int"
    },
```

```
    {
        "Name": "databucket",
        "Type":
"struct<name:string,type:string,file:struct<attributes:int,name:string,owner:struct<name:s
    },
    {
        "Name": "table",
        "Type": "struct<uid:string,created_time_dt:string>"
    },
    {
        "Name": "session",
        "Type":
"struct<count:int,uid:string,uuid:string,issuer:string,created_time:bigint,is_remote:boole
    },
    {
        "Name": "certificate",
        "Type":
"struct<version:string,uid:string,subject:string,issuer:string,fingerprints:array<struct<v
    },
    {
        "Name": "is_mfa",
        "Type": "boolean"
    },
    {
        "Name": "logon_type_id",
        "Type": "int"
    },
    {
        "Name": "auth_protocol_id",
        "Type": "int"
    },
    {
        "Name": "logon_type",
        "Type": "string"
    },
    {
        "Name": "is_remote",
        "Type": "boolean"
    },
    {
        "Name": "is_cleartext",
        "Type": "boolean"
    },
    {
```

```
        "Name": "auth_protocol",
        "Type": "string"
    },
    {
        "Name": "is_renewal",
        "Type": "boolean"
    },
    {
        "Name": "lease_dur",
        "Type": "int"
    },
    {
        "Name": "relay",
        "Type":
 "struct<name:string,type:string,ip:string,mac:string,namespace:string,type_id:int>"
    },
    {
        "Name": "transaction_uid",
        "Type": "string"
    },
    {
        "Name": "file_result",
        "Type":
 "struct<name:string,size:int,type:string,path:string,desc:string,product:struct<name:strin
    },
    {
        "Name": "file_diff",
        "Type": "string"
    },
    {
        "Name": "create_mask",
        "Type": "string"
    },
    {
        "Name": "web_resources_result",
        "Type":
 "array<struct<type:string,data_classification:struct<category:string,category_id:int,confi
    },
    {
        "Name": "app",
        "Type":
 "struct<name:string,version:string,uid:string,data_classification:struct<category:string,c
    },
    {
```

```
        "Name": "src_url",
        "Type": "string"
    },
    {
        "Name": "priority_id",
        "Type": "int"
    },
    {
        "Name": "verdict",
        "Type": "string"
    },
    {
        "Name": "desc",
        "Type": "string"
    },
    {
        "Name": "verdict_id",
        "Type": "int"
    },
    {
        "Name": "priority",
        "Type": "string"
    },
    {
        "Name": "finding_info_list",
        "Type":
 "array<struct<title:string,uid:string,attacks:array<struct<version:string,tactics:array<st
    },
    {
        "Name": "expiration_time_dt",
        "Type": "string"
    },
    {
        "Name": "expiration_time",
        "Type": "bigint"
    },
    {
        "Name": "comment",
        "Type": "string"
    },
    {
        "Name": "entity",
        "Type": "struct<data:string,name:string,version:string,uid:string>"
    },
```

```
    {
        "Name": "entity_result",
        "Type":
"struct<data:string,name:string,type:string,version:string,uid:string>"
    },
    {
        "Name": "module",
        "Type":
"struct<type:string,file:struct<name:string,type:string,path:string,desc:string,type_id:in
    },
    {
        "Name": "exit_code",
        "Type": "int"
    },
    {
        "Name": "injection_type",
        "Type": "string"
    },
    {
        "Name": "injection_type_id",
        "Type": "int"
    },
    {
        "Name": "request",
        "Type": "struct<uid:string>"
    },
    {
        "Name": "response",
        "Type": "struct<error:string,code:int,message:string,error_message:string>"
    },
    {
        "Name": "driver",
        "Type":
"struct<file:struct<name:string,type:string,version:string,path:string,type_id:int,parent_
    },
    {
        "Name": "prev_security_states",
        "Type": "array<string>"
    },
    {
        "Name": "security_states",
        "Type": "array<string>"
    },
    {
```

```
        "Name": "folder",
        "Type":
"struct<name:string,type:string,path:string,desc:string,type_id:int,mime_type:string,paren
    },
    {
        "Name": "url",
        "Type":
"struct<port:int,scheme:string,path:string,hostname:string,query_string:string,resource_ty
    },
    {
        "Name": "tunnel_type_id",
        "Type": "int"
    },
    {
        "Name": "tunnel_type",
        "Type": "string"
    },
    {
        "Name": "protocol_name",
        "Type": "string"
    },
    {
        "Name": "job",
        "Type":
"struct<name:string,file:struct<name:string,type:string,path:string,signature:struct<certi
    },
    {
        "Name": "num_trusted_items",
        "Type": "int"
    },
    {
        "Name": "command_uid",
        "Type": "string"
    },
    {
        "Name": "num_registry_items",
        "Type": "int"
    },
    {
        "Name": "num_network_items",
        "Type": "int"
    },
    {
        "Name": "schedule_uid",
```

```
            "Type": "string"
        },
        {
            "Name": "num_resolutions",
            "Type": "int"
        },
        {
            "Name": "scan",
            "Type": "struct<name:string,type:string,type_id:int>"
        },
        {
            "Name": "num_detections",
            "Type": "int"
        },
        {
            "Name": "num_processes",
            "Type": "int"
        },
        {
            "Name": "num_files",
            "Type": "int"
        },
        {
            "Name": "total",
            "Type": "int"
        },
        {
            "Name": "num_folders",
            "Type": "int"
        },
        {
            "Name": "dce_rpc",
            "Type":
    "struct<command:string,flags:array<string>,command_response:string,opnum:int,rpc_interface
        },
        {
            "Name": "share",
            "Type": "string"
        },
        {
            "Name": "client_dialects",
            "Type": "array<string>"
        },
        {
```

```
        "Name": "open_type",
        "Type": "string"
    },
    {
        "Name": "tree_uid",
        "Type": "string"
    },
    {
        "Name": "share_type_id",
        "Type": "int"
    },
    {
        "Name": "share_type",
        "Type": "string"
    },
    {
        "Name": "dialect",
        "Type": "string"
    },
    {
        "Name": "cis_benchmark_result",
        "Type": "struct<name:string>"
    },
    {
        "Name": "vulnerabilities",
        "Type":
 "array<struct<references:array<string>,severity:string,affected_packages:array<struct<name
    },
    {
        "Name": "service",
        "Type": "struct<name:string,uid:string>"
    },
    {
        "Name": "data_security",
        "Type":
 "struct<category:string,pattern_match:string,category_id:int,confidentiality:string,confid
    },
    {
        "Name": "database",
        "Type":
 "struct<name:string,type:string,uid:string,type_id:int,data_classification:struct<category
    }
]
```

在 Security Lake 中建立自訂來源

1. 導覽至 Amazon Security Lake 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、身分驗證、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. 針對 AWS 帳戶 ID 和外部 ID，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。您將使用它來設定 Amazon Data Firehose 交付串流。

在 Firehose 中建立交付串流

1. 導覽至 Amazon Data Firehose 主控台。
2. 選擇建立交付串流。
3. 針對來源，選取直接 PUT。
4. 針對目的地，選擇 S3。
5. 在轉換和轉換記錄區段中，選擇啟用記錄格式轉換，然後選擇 Apache Parquet做為輸出格式。
6. 針對AWS Glue 資料表，選擇您在先前程序中建立的 AWS Glue 資料表，然後選擇最新版本。
7. 針對目的地設定，選擇您使用 Security Lake 自訂來源建立的 Amazon S3 儲存貯體。
8. 針對動態分割，選擇已啟用。
9. 針對 JSON 的內嵌剖析，選擇已啟用。
   - 針對 Keyname，輸入 `eventDayValue`。
   - 對於 JQ Expression，輸入 `(.time/1000)|strftime("%Y%m%d")`。
10. 針對 S3 儲存貯體字首，輸入下列值。

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

將 *<custom source name>*、*<region>* 和 *<account_id>* 取代為您的 Security Lake 自訂來源名稱 AWS 區域 和 AWS 帳戶 ID。

11. 針對 S3 儲存貯體錯誤輸出字首，輸入下列值。

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

12. 針對重試持續時間，選取 300。
13. 針對緩衝區大小，選取 128 MiB。
14. 針對緩衝間隔，選取 60 秒。
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 主控台中建立擷取，該擷取會使用您先前建立做為輸出位置的 Firehose 交付串流。如需設定 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

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 （人工智慧）將安全性從已知的簽章和模式擴展到最複雜的攻擊，例如零時差攻擊和勒索軟體。

AWS AppFabric 稽核日誌擷取考量事項

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

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 使用開放網路安全結構描述架構 (OCSF) 標準化資料，並以 JSON 格式輸出資料。

輸出位置

Singularity Cloud 支援從下列 AppFabric 輸出位置接收稽核日誌。

- Amazon Simple Storage Service (Amazon S3)

- 若要Singularity Cloud設定 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 有助於讓組織更具彈性。領導組織使用 Splunk的統一安全性和可觀測性平台，以確保其數位系統的安全和可靠性。組織信任 Splunk以防止安全、基礎設施和應用程式問題成為重大事件、吸收數位中斷造成的衝擊並加速數位轉型。

AWS AppFabric 稽核日誌擷取考量事項

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

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 會以 JSON 格式在來源應用程式所使用的原始結構描述中輸出資料。
- OCSF - JSON
  - AppFabric 會使用開放網路安全結構描述架構 (OCSF) 標準化資料，並以 JSON 格式輸出資料。
- OCSF - Parquet
  - AppFabric 使用開放網路安全結構描述架構 (OCSF) 標準化資料，並以 Apache Parquet 格式輸出資料。

輸出位置

Splunk 支援下列 AppFabric 輸出位置：

- Amazon Data Firehose
  - 若要Splunk設定 從包含稽核日誌的 Firehose 串流接收稽核日誌，請遵循 Splunk 網站上的 Splunk Amazon Data Firehose 附加元件中的指示。
- Amazon Simple Storage Service (Amazon S3)
  - 若要Splunk設定 從包含稽核日誌的 Amazon S3 儲存貯體接收資料，請遵循 Splunk 網站上的設定Splunk附加元件的 SQS 型 S3 輸入 AWS中的指示。

安全資源的 Delete AWS AppFabric

如果您不想為了安全而繼續使用 AWS AppFabric，請務必刪除您在設定期間建立的輸出位置中的資料，以及針對安全資源的 AppFabric，以避免產生額外費用。若要清除 AppFabric 資源，您必須以您為每個軟體即服務 (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之後，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，安全 AppFabric 會代表您建立擷取目的地。若要刪除擷取目的地，請使用下列步驟：

1. 在 https：//https://console.aws.amazon.com/appfabric/ 開啟 AppFabric 主控台。
2. 從入門頁面，展開左側的選單。
3. 選擇擷取。
4. 選擇應用程式授權。
5. 選取您要刪除之目的地旁的選項按鈕，然後選擇刪除。
6. 在刪除目的地對話方塊上，選擇刪除以確認。
7. 針對所有目的地重複上述步驟。

刪除擷取

若要刪除擷取，請使用下列步驟：

1. 從入門頁面，展開左側的選單。
2. 選擇擷取。
3. 選取應用程式授權旁的選項按鈕。

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，請使用下列步驟：

1. 從入門頁面，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，請使用下列步驟：

1. 從入門頁面，展開左側的選單。
2. 選擇應用程式套件。
3. 選擇 Delete (刪除) 按鈕。
4. 輸入 `delete` 進行確認，然後選擇刪除。

生產力的 is AWS AppFabric 是什麼？

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

> **Note**
>
> 採用 Amazon Bedrock： AWS 實作自動濫用偵測。Because AWS AppFabric 的生產力建立在 Amazon Bedrock 上，使用者會繼承在 Amazon Bedrock 中實作的控制項，以強制執行 AI 的安全性和負責任的使用。

AWS AppFabric for productivity （預覽） 透過從多個應用程式產生具有內容的洞察和動作，協助重新構想第三方應用程式中的最終使用者生產力。應用程式開發人員了解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非常重要，但他們不想與每個應用程式建置和管理整合。透過 AppFabric 提高生產力，應用程式開發人員可以存取產生跨應用程式資料洞見和動作的生成式 AI 支援 APIs，以便透過新的或現有的生成式 AI 助理提供更豐富的最終使用者體驗。AppFabric for productivity 整合了來自多個應用程式的資料，無需開發人員建置或維護point-to-point整合。應用程式開發人員可以直接將 AppFabric 的生產力嵌入其應用程式的 UI，為其最終使用者維持一致的體驗，同時從其他應用程式浮現相關內容。

生產力的 AppFabric 會從常用應用程式連線資料，例如 Asana、Atlassian Jira Suite、Google Workspace、Microsoft 365、Miro、Slack、 Smartsheet等。AppFabric for productivity 可讓應用程式開發人員更輕鬆地建置更個人化的應用程式體驗，以改善使用者採用率、滿意度和忠誠度。同時，最終使用者會從其應用程式間存取所需的洞見，而不會中斷其工作流程。

主題

- 優勢
- 使用案例
- 存取 AppFabric 以提高生產力
- 開始使用 AppFabric 為應用程式開發人員提高生產力 （預覽）
- 開始使用 AppFabric 提高最終使用者的生產力 （預覽）
- 生產力 APIs的 AppFabric （預覽）
- AppFabric 中的資料處理

優勢

透過 AppFabric 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洞見和動作APIs，以便透過新的或現有的生成式 AI 助理提供更豐富的最終使用者體驗。

- 跨應用程式使用者資料的單一來源：用於生產力的 AppFabric 整合了來自多個應用程式的資料，不再需要開發人員建置或維護point-to-point整合。處理 SaaS 應用程式資料以供其他應用程式使用，方法是將不同的資料類型自動標準化為任何應用程式可理解的格式，讓應用程式開發人員能夠納入更多資料，實際改善最終使用者的生產力。
- 完全控制使用者體驗：開發人員將 AppFabric 直接嵌入其應用程式的 UI 以提高生產力，保留使用者體驗的完全控制，同時為具有跨應用程式內容的最終使用者提供個人化的洞見和建議的動作。這可讓 AppFabric 在最終使用者的偏好 SaaS 應用程式中取得生產力，並在他們偏好完成任務的應用程式中存取。最終使用者花較少的時間在應用程式之間切換，並且可以在工作過程中保持。
- 加速上市時間：在單一 API 呼叫中，應用程式開發人員可以接收使用者資料的使用者層級洞見，而不必微調模型、撰寫自訂提示或跨多個應用程式建置整合。AppFabric 可消除此複雜性，讓應用程式開發人員更快速地建置、嵌入或豐富生成式 AI 功能。這可讓應用程式開發人員專注於最重要的任務上的資源。
- 建置使用者信任的成品參考：作為輸出的一部分，用於生產力的 AppFabric 將呈現相關的成品或來源檔案，用於產生洞見，以在 LLM 輸出中建置最終使用者信任。
- 簡化的使用者許可：用於產生洞見的使用者成品取決於使用者可存取的內容。AppFabric for productivity 使用 ISV 的許可和存取控制作為事實來源。

使用案例

應用程式開發人員可以使用 AppFabric 提高生產力，以重新構想其應用程式內的生產力。AppFabric for productivity 提供兩個著重於下列使用案例APIs，以協助最終使用者提高生產力：

- 排定一天的優先順序
  - 可採取行動的洞見 API 可讓使用者從應用程式中及時獲得洞見，包括電子郵件、行事曆、訊息、任務等，協助他們妥善管理一天。此外，使用者可以執行跨應用程式動作，例如從他們偏好的應用程式建立電子郵件、排程會議和建立動作項目。例如，在夜間進行客戶呈報的員工不僅會看到夜間對話的摘要，還會看到與客戶客戶經理安排會議的建議動作。動作會預先填入必要欄位（例如任務名稱和擁有者，或電子郵件寄件者/收件人），能夠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 可摘要會議目的並顯示電子郵件、訊息等相關的跨應用程式成品，協助使用者為會議做好準備。使用者現在可以快速準備會議，而且不會浪費應用程式之間切換的時間來尋找內容。

存取 AppFabric 以提高生產力

生產力的 AppFabric 目前以預覽形式啟動，並在美國東部（維吉尼亞北部）提供 AWS 區域。如需詳細資訊 AWS 區域，請參閱《》中的 AWS AppFabric 端點和配額AWS 一般參考。

在每個區域中，您可以透過下列任何方式存取 AppFabric 以提高生產力：

- 身為應用程式開發人員
  - 開始使用 AppFabric 為應用程式開發人員提高生產力（預覽）
- 身為最終使用者
  - 開始使用 AppFabric 提高最終使用者的生產力（預覽）

開始使用 AppFabric 為應用程式開發人員提高生產力（預覽）

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

本節協助應用程式開發人員將 AWS AppFabric 的生產力（預覽）整合到應用程式中。 AWS AppFabric 的生產力可讓開發人員在多個應用程式中從電子郵件、行事曆事件、任務、訊息等產生 AI 支援的洞見和動作，為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 for productivity 可讓應用程式開發人員在安全且受控的環境中進行建置和實驗。當您第一次開始使用 AppFabric 提高生產力時，您可以建立 AppClient 並註冊單一測試使用者。此方法旨在協助您了解和測試應用程式與 AppFabric 之間的身分驗證和通訊流程。使用單一使用者進行測試後，您可以將應用程式提交至 AppFabric 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 驗證您的應用程式)。AppFabric 將在啟用廣泛採用之前驗證應用程式資訊，以協助保護應用程式開發人員、最終使用者及其資料，以負責任的方式擴展使用者採用。

主題

- 先決條件
- 步驟 1. 建立 AppFabric 以提高生產力 AppClient
- 步驟 2. 驗證和授權您的應用程式

- 步驟 3。將 AppFabric 使用者入口網站 URL 新增至您的應用程式
- 步驟 4. 使用 AppFabric 呈現跨應用程式洞見和動作
- 步驟 5. 請求 AppFabric 驗證您的應用程式
- 管理 AppFabric 以提高生產力 AppClients
- 故障診斷 AppFabric 中的 AppClients 以提高生產力 AppFabric

先決條件

開始使用之前，您需要建立 AWS 帳戶。如需詳細資訊，請參閱註冊 AWS 帳戶。您也需要建立至少一個可存取下列 "appfabric:CreateAppClient" IAM 政策的使用者，以允許使用者向 AppFabric 註冊您的應用程式。如需授予 AppFabric 生產力功能許可的詳細資訊，請參閱 適用於生產力的 AppFabric IAM 政策範例。雖然擁有管理使用者是有益的，但初始設定並非強制性的。如需詳細資訊，請參閱建立具有管理存取權的使用者。

提高生產力的 AppFabric 僅適用於預覽期間的美國東部（維吉尼亞北部）。開始以下步驟之前，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. 建立 AppFabric 以提高生產力 AppClient

您需要建立 AppFabric AppClient，才能開始在應用程式中浮現 AppFabric 以取得生產力洞察。AppClient 基本上是 AppFabric 生產力的閘道，可做為安全的 OAuth 應用程式用戶端，在您的應用程式和 AppFabric 之間進行安全通訊。當您建立 AppClient 時，您會獲得一個 AppClient ID，這是確保 AppFabric 知道它正在與您的應用程式和您的 搭配使用的關鍵唯一識別符 AWS 帳戶。

AppFabric for productivity 可讓應用程式開發人員在安全且受控的環境中進行建置和實驗。當您第一次開始使用 AppFabric 提高生產力時，您可以建立 AppClient 並註冊單一測試使用者。此方法旨在協助

您了解和測試應用程式與 AppFabric 之間的身分驗證和通訊流程。使用單一使用者進行測試後，您可以將應用程式提交至 AppFabric 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 驗證您的應用程式)。AppFabric 將在啟用廣泛採用之前驗證應用程式資訊，以協助保護應用程式開發人員、最終使用者及其資料，以負責任的方式擴展使用者採用。

若要建立 AppClient，請使用 AWS AppFabric `CreateAppClient` API 操作。如果您需要在 之後更新 AppClient，您可以使用 `UpdateAppClient` API 操作來僅變更 redirectUrls。如果您需要變更與 AppClient 相關聯的任何其他參數，例如 appName 或描述，您必須刪除 AppClient 並建立新的參數。如需詳細資訊，請參閱CreateAppClient。

您可以使用多種程式設計語言，包括 Python、Node.js、Java、C#、Go 和 Rust，使用 `CreateAppClient` API 向 AWS 服務註冊應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的請求簽章範例。您需要使用帳戶簽章第 4 版登入資料來執行此 API 操作。如需簽章第 4 版的詳細資訊，請參閱《IAM 使用者指南》中的簽署 AWS API 請求。

請求欄位

- `appName` - AppFabric 使用者入口網站的同意頁面上將向使用者顯示的應用程式名稱。同意頁面會要求最終使用者在應用程式中顯示 AppFabric 洞見的許可。如需同意頁面的詳細資訊，請參閱 步驟 2. 同意應用程式顯示洞見。
- `description` - 應用程式的說明。
- `redirectUrls` - 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 redirectUrls。例如 `https://localhost:8080`。
- `starterUserEmails` - 允許存取的使用者電子郵件地址，以接收洞見，直到驗證應用程式為止。只允許一個電子郵件地址。例如 `anyuser@example.com`
- `customerManagedKeyIdentifier`（選用）- 用於加密資料之客戶受管金鑰（由 KMS 產生）的 ARN。如果未指定，則會使用 AWS AppFabric 受管金鑰。如需 AWS 擁有的金鑰 和客戶受管金鑰的詳細資訊，請參閱《 AWS Key Management Service 開發人員指南》中的客戶金鑰和 AWS 金鑰。

回應欄位

- `appClientArn` - 包含 AppClient ID 的 Amazon Resource Name (ARN)。例如，AppClient ID 為 `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`。
- `verificationStatus` - AppClient 驗證狀態。
  - `pending_verification` - AppClient 的驗證仍在使用 AppFabric 進行。在 AppClient 驗證之前，只有一個使用者（在 中指定`starterUserEmails`) 可以使用 AppClient。使用者會在

AppFabric 使用者入口網站中看到通知，在 中介紹步驟 3。將 AppFabric 使用者入口網站 URL 新增至您的應用程式，指出應用程式未驗證。

- `verified` - AppFabric 已成功完成驗證程序，現在已完全驗證 AppClient。
- `rejected` - AppFabric 已拒絕 AppClient 的驗證程序。 AppFabric 在驗證程序重新啟動並成功完成之前，其他使用者無法使用 AppClient。

```
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. 驗證和授權您的應用程式

建立 OAuth 2.0 授權流程，讓您的應用程式安全地整合 AppFabric 洞見。首先，您需要建立授權碼，以驗證您的應用程式身分。如需詳細資訊，請參閱授權。然後，您將交換此授權碼做為存取字符，授予您的應用程式在應用程式中擷取和顯示 AppFabric 洞見的許可。如需詳細資訊，請參閱權杖。

如需授予授權應用程式許可的詳細資訊，請參閱 允許存取以授權應用程式。

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

請求欄位

- app_client_id（必要）- 在步驟 1 中 AWS 帳戶 建立之 的 AppClient ID。 建立 AppClient。例如 a1b2c3d4-5678-90ab-cdef-EXAMPLE11111。
- redirect_uri（必要）- 您在步驟 1 中使用的授權後，將最終使用者重新導向至 的 URI。建立 AppClient。例如 https://localhost:8080。
- state（必要）- 用來維持請求與回呼之間狀態的唯一值。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. 身分驗證之後，系統會將您重新導向至指定的 URI，並將授權碼傳回為查詢參數。例如，其中 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 操作交換此授權碼以取得存取權杖。

   此字符用於 API 請求，最初對 有效，starterUserEmails直到 AppClient 驗證為止。驗證 AppClient 之後，此字符可用於任何使用者。您需要使用帳戶簽章第 4 版登入資料來執行此 API 操作。如需簽章第 4 版的詳細資訊，請參閱《IAM 使用者指南》中的簽署 AWS API 請求。

   請求欄位

   - code（必要）- 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 的 AppClient ID。 建立 AppClient。例如 a1b2c3d4-5678-90ab-cdef-EXAMPLE11111。
   - grant_type（必要）- 值必須為 authorization_code。

- `redirect_uri`（必要）- 您在步驟 1 中使用的授權後，將使用者重新導向至 的 URI。建立 AppClient。這必須是用來建立授權碼的相同重新導向 URI。例如 `https://localhost:8080`。

回應欄位

- `expires_in` - 字符過期前多久。預設過期時間為 12 小時。
- `refresh_token` - 從初始 / 權杖請求收到的重新整理權杖。
- `token` - 從初始 / 權杖請求收到的權杖。
- `token_type` - 值為 `Bearer`。
- `appfabric_user_id` - AppFabric 使用者 ID。這只會針對使用 `authorization_code`授予類型的請求傳回。

```
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。將 AppFabric 使用者入口網站 URL 新增至您的應用程式

最終使用者需要授權 AppFabric 從用於產生洞見的應用程式存取資料。AppFabric 透過為最終使用者建立專用使用者入口網站（快顯畫面）以授權其應用程式，消除應用程式開發人員擁有此程序的複雜性。當使用者準備好啟用 AppFabric 以提高生產力時，他們將被帶到使用者入口網站，這讓他們能夠連接和管理用於產生洞見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至 AppFabric 以提高生產力，然後返回您的應用程式以探索洞見和動作。若要將應用程式與 AppFabric 整合以提高生產力，您需要將特定的 AppFabric URL 新增至應用程式。此步驟對於讓使用者直接從您的應用程式存取 AppFabric 使用者入口網站至關重要。

1. 導覽至應用程式的設定，並找到新增重新導向 URLs 區段。
2. 找到適當的區域後，請將下列 AppFabric URL 做為重新導向 URL 新增至您的應用程式：

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

新增 URL 後，您的應用程式將設定為將使用者導向 AppFabric 使用者入口網站。在這裡，使用者可以登入和管理其用於產生 AppFabric 的應用程式，以取得生產力洞察。

步驟 4. 使用 AppFabric 呈現跨應用程式洞見和動作

使用者連線其應用程式後，您可以利用使用者的洞見，藉由協助減少應用程式和內容切換來提高生產力。AppFabric 只會根據使用者有權存取的內容，為使用者產生洞見。AppFabric 會將使用者資料存放在 AppFabric AWS 帳戶 擁有的 中。如需有關 AppFabric 如何使用您的資料的資訊，請參閱 AppFabric 中的資料處理。

您可以使用下列 AI 支援的 APIs在應用程式中產生和顯示使用者層級的洞見和動作：

- `ListActionableInsights` — 如需詳細資訊，請參閱以下可採取行動的洞見一節。
- `ListMeetingInsights` — 如需詳細資訊，請參閱本指南稍後的會議準備一節。

可行的洞見 (**`ListActionableInsights`**)

`ListActionableInsights` API 可協助使用者根據其應用程式的活動，包括電子郵件、行事曆、訊息、任務等，以最佳方式管理其日出的可行洞見。傳回的洞見也會顯示用於產生洞見的成品的內嵌連結，協助使用者快速檢視用於產生洞見的資料。此外，API 可能會根據洞見傳回建議的動作，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 會與 Asana、Microsoft 365、Google Workspace和 等平台整合Smartsheet，讓使用者能夠傳送電子郵件、建立行事曆事件和建

立任務。大型語言模型 (LLMs) 可能會在建議的動作（例如電子郵件內文或任務名稱）中預先填入詳細資訊，使用者可以在執行之前自訂這些動作，進而簡化決策並提高生產力。與最終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，讓使用者檢視、編輯和執行跨應用程式動作。對於執行動作，AppFabric 需要 ISVs 將使用者重新導向至 AppFabric 使用者入口網站，讓他們可以查看動作詳細資訊並執行它們。AppFabric 產生的每個動作都有唯一的 URL。此 URL 可用於 `ListActionableInsights` API 回應的回應。

以下是支援的跨應用程式動作和其中應用程式摘要：

- 傳送電子郵件 (Google Workspace、Microsoft 365)
- 建立行事曆事件 (Google Workspace、Microsoft 365)
- 建立任務 (Asana、Smartsheet)

請求欄位

- `nextToken`（選用）- 擷取下一組洞見的分頁字符。
- `includeActionExecutionStatus` - 接受動作執行狀態清單的篩選條件。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` 值一起傳入。

回應欄位

- `insightId` - 產生洞見的唯一 ID。
- `insightContent` - 這會傳回用於產生洞見之成品的洞見和內嵌連結摘要。注意：這是包含內嵌連結 (<a> 標籤）的 HTML 內容。
- `insightTitle` - 產生的洞見標題。
- `createdAt` - 產生洞見的時間。
- `actions` - 為產生的洞見建議的動作清單。動作物件：
  - `actionId` - 所產生動作的唯一 ID。
  - `actionIconUrl` - 建議在其中執行動作之應用程式的圖示 URL。
  - `actionTitle` - 所產生動作的標題。

- `actionUrl` - 最終使用者在 AppFabric 使用者入口網站中檢視和執行動作的唯一 URL。注意：若要執行動作，ISV 應用程式會使用此 URL 將使用者重新導向至 AppFabric 使用者入口網站（彈出畫面）。
- `actionExecutionStatus` - 指出動作狀態的列舉。可能的值為： `EXECUTED` | `NOT_EXECUTED`
- `nextToken`（選用）- 擷取下一組洞見的分頁字符。這是一個選用欄位，如果傳回 null，表示沒有更多需要載入的洞見。

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`)

`ListMeetingInsights` API 可摘要會議目的和出現相關的跨應用程式成品，例如電子郵件、訊息等，協助使用者為即將到來的會議做好準備。使用者現在可以快速準備會議，而且不會浪費應用程式之間切換的時間來尋找內容。

請求欄位

- `nextToken`（選用）- 擷取下一組洞見的分頁字符。

請求標頭

- 授權標頭需要與 `Bearer Token`值一起傳入。

回應欄位

- `insightId` - 產生洞見的唯一 ID。
- `insightContent` - 洞見的描述，以字串格式反白顯示詳細資訊。如同 ，為什麼此洞見很重要。
- `insightTitle` - 產生的洞見標題。
- `createdAt` - 產生洞見的時間。

- `calendarEvent` - 使用者應關注的重要行事曆事件或會議。行事曆事件物件：
  - `startTime` - 事件的開始時間。
  - `endTime` - 事件的結束時間。
  - `eventUrl` - ISV 應用程式上行事曆事件的 URL。
- `resources` - 包含與 相關其他資源的清單會產生洞見。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` - 資源所屬之應用程式的影像 URL。
- `nextToken`（選用）- 擷取下一組洞見的分頁字符。這是一個選用欄位，如果傳回 null，表示沒有更多需要載入的洞見。

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
```

```
}
```

為您的洞見或動作提供意見回饋

使用 AppFabric `PutFeedback` API 操作，為產生的洞見和動作提供意見回饋。您可以在應用程式中內嵌此功能，以提供提交特定 InsightId 或 ActionId 意見回饋評分 (1 到 5，評分越高） 的方法。

請求欄位

- `id` - 要提交意見回饋之物件的識別符。這可以是 InsightId 或 ActionId。
- `feedbackFor` - 提交意見回饋的資源類型。可能的值：`ACTIONABLE_INSIGHT` | `MEETING_INSIGHT` | `ACTION`
- `feedbackRating` - 從 1到 的意見回饋評分5。評分越高越好。

回應欄位

- 沒有回應欄位。

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 驗證您的應用程式

此時，您已更新應用程式 UI 以嵌入 AppFabric 跨應用程式洞見和動作，並收到單一使用者的洞見。當您對測試感到滿意，並希望將您的 AppFabric 豐富體驗擴展到其他使用者後，您可以將應用程式提交到 AppFabric 進行審核和驗證。AppFabric 將在啟用廣泛採用之前驗證應用程式資訊，以協助保護應用程式開發人員、最終使用者及其資料，以負責任的方式擴展使用者採用。

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下列詳細資訊：

- 您的 AWS 帳戶 ID
- 您要驗證的應用程式名稱
- 您的 AppClient ID
- 您的聯絡資訊

此外，如果可用，請提供下列資訊，以協助我們評估優先順序和影響：

- 您計劃授予存取權的使用者估計數量
- 您的目標啟動日期

> **Note**
> 如果您有 AWS 帳戶 經理或 AWS 合作夥伴開發經理，請在您的電子郵件中複製他們。包含這些聯絡人有助於加速驗證程序。

驗證條件

啟動驗證程序之前，您必須符合下列條件：

- 您必須使用有效的 AWS 帳戶 ，以使用 AppFabric 提高生產力

此外，您至少符合下列其中一項條件：

- 您的組織是 上的 AWS 合作夥伴，至少 AWS Partner Network 具有「AWS 選取」層。如需詳細資訊，請參閱 AWS 合作夥伴服務方案。
- 您的組織應該在過去三年內在 AppFabric 服務上花費至少 10，000 美元。
- 您的應用程式應列在 上 AWS Marketplace。如需詳細資訊，請參閱 AWS Marketplace。

等待驗證狀態更新

檢閱您的應用程式後，我們會透過電子郵件回應，而 AppClient 的狀態將從 變更為 `pending_verification` `verified`。如果您的應用程式遭到拒絕，您將需要重新啟動驗證程序。

管理 AppFabric 以提高生產力 AppClients

> 生產力的 The AWS AppFabric 功能為預覽版，可能會有所變更。

您可以管理 AppFabric 以提高生產力 AppClients，以確保身分驗證和授權程序的順暢操作和維護。

取得 AppClient 的詳細資訊

使用 AppFabric `GetAppClient` API 操作來檢視 AppClient 的詳細資訊，包括檢查 AppClient 狀態。如需詳細資訊，請參閱GetAppClient。

若要取得 AppClient 的詳細資訊，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 AppClients 的詳細資訊。

請求欄位

- `appClientId` - AppClient ID。

回應欄位

- `appName` - AppFabric 使用者入口網站的同意頁面上將向使用者顯示的應用程式名稱。
- `customerManagedKeyIdentifier`（選用）- 用於加密資料之客戶受管金鑰（由 KMS 產生）的 ARN。如果未指定，則會使用 AWS AppFabric 受管金鑰。
- `description` - 應用程式的描述。
- `redirectUrls` - 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 redirectUrls。例如 `https://localhost:8080`。
- `starterUserEmails` - 允許存取的使用者電子郵件地址，以接收洞見，直到驗證應用程式為止。僅允許一個電子郵件地址。例如 `anyuser@example.com`。
- `verificationStatus` - AppClient 驗證狀態。
  - `pending_verification` - AppClient 的驗證仍在 AppFabric 進行。驗證 AppClient 之前，只有一個使用者（在 中指定`starterUserEmails`) 可以使用 AppClient。
  - `verified` - AppFabric 已成功完成驗證程序，現在已完整驗證 AppClient。

- `rejected` - AppFabric 已拒絕 AppClient 的驗證程序。 AppFabric 在驗證程序重新啟動並成功完成之前，其他使用者無法使用 AppClient。

```
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"
        }
    }
}
```

列出 AppClients

使用 AppFabric `ListAppClients` API 操作來檢視 AppClients 的清單。AppFabric 每個 僅允許一個 AppClient AWS 帳戶。這可能會在未來變更。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，請參閱允許存取列出 AppClients。

請求欄位

- 沒有必要欄位。

回應欄位

- appClientARN - 包含 AppClient ID 的 Amazon Resource Name (ARN)。例如，AppClient ID 為 a1b2c3d4-5678-90ab-cdef-EXAMPLE11111。
- verificationStatus - AppClient 驗證狀態。
  - pending_verification - AppClient 的驗證仍在 AppFabric 進行。驗證 AppClient 之前，只有一個使用者（在 中指定starterUserEmails) 可以使用 AppClient。
  - verified - AppFabric 已成功完成驗證程序，現在已完整驗證 AppClient。
  - rejected - AppFabric 已拒絕 AppClient 的驗證程序。 AppFabric 在驗證程序重新啟動並成功完成之前，其他使用者無法使用 AppClient。

```
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 AppClient

使用 AppFabric `UpdateAppClient` API 操作來更新映射至 AppClient 的 redirectUrls。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 並建立新的參數。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，請參閱允許存取以更新 AppClients。

請求欄位

- `appClientId`（必要）- 您要更新 redirectUrls 的 AppClient ID。
- `redirectUrls`（必要）- redirectUrls 的更新清單。您最多可以新增 5 個 redirectUrls。

回應欄位

- `appName` - AppFabric 使用者入口網站的同意頁面上將向使用者顯示的應用程式名稱。
- `customerManagedKeyIdentifier`（選用）- 用於加密資料之客戶受管金鑰（由 KMS 產生）的 ARN。如果未指定，則會使用 AWS AppFabric 受管金鑰。
- `description` - 應用程式的描述。
- `redirectUrls` - 授權後將最終使用者重新導向至 的 URI。例如 `https://localhost:8080`。
- `starterUserEmails` - 允許存取的使用者電子郵件地址，以接收洞見，直到驗證應用程式為止。僅允許一個電子郵件地址。例如 `anyuser@example.com`。
- `verificationStatus` - AppClient 驗證狀態。
  - `pending_verification` - AppClient 的驗證仍在 AppFabric 進行。驗證 AppClient 之前，只有一個使用者（在 中指定`starterUserEmails`) 可以使用 AppClient。
  - `verified` - AppFabric 已成功完成驗證程序，現在已完整驗證 AppClient。
  - `rejected` - AppFabric 已拒絕 AppClient 的驗證程序。 AppFabric 在驗證程序重新啟動並成功完成之前，其他使用者無法使用 AppClient。

```
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 AppClient

使用 AppFabric `DeleteAppClient` API 操作刪除您不再需要的任何 AppClients。如需詳細資訊，請參閱DeleteAppClient。

若要刪除 AppClient，您至少必須擁有 IAM `"appfabric:DeleteAppClient"` 政策許可。如需詳細資訊，請參閱允許存取以刪除 AppClients。

請求欄位

- `appClientId` - AppClient ID。

回應欄位

- 沒有回應欄位。

```
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。

重新整理最終使用者的字符

AppClient 為最終使用者取得的權杖可以在到期時重新整理。您可以使用 權杖 API 搭配 grant_type 來完成此操作`refresh_token`。當 grant_type 為 時，將傳回`refresh_token`要使用的 做為字符 API 回應的一部分`authorization_code`。預設過期時間為 12 小時。若要呼叫重新整理 API，您必須擁有 IAM `"appfabric:Token"` 政策許可。如需詳細資訊，請參閱權杖及允許存取以更新 AppClients。

請求欄位

- `refresh_token`（必要）- 從初始`/token`請求收到的重新整理字符。
- `app_client_id`（必要）- 為 建立的 AppClient 資源 ID AWS 帳戶。
- `grant_type`（必要）- 這必須是 `refresh_token`。

回應欄位

- `expires_in` - 字符過期前多久。預設過期時間為 12 小時。
- `refresh_token` - 從初始 / 權杖請求收到的重新整理權杖。
- `token` - 從初始 / 權杖請求收到的權杖。
- `token_type` - 值為 `Bearer`。
- `appfabric_user_id` - AppFabric 使用者 ID。這只會針對使用 `authorization_code`授予類型的請求傳回。

```
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}"
}
```

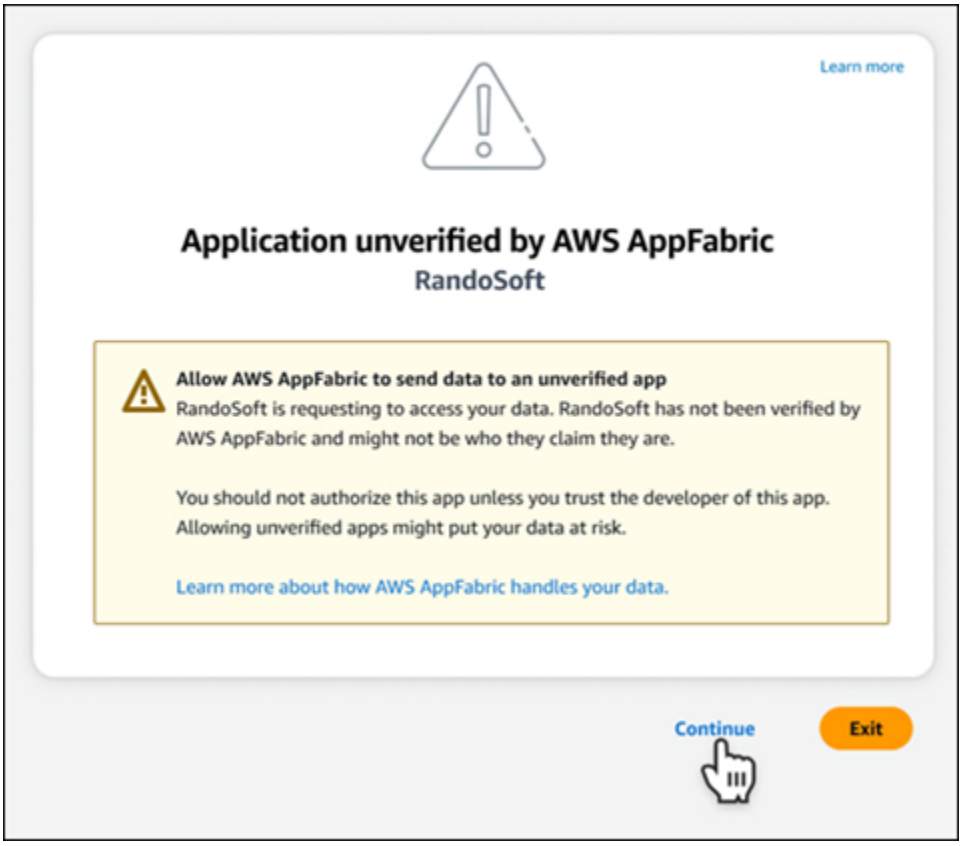
故障診斷 AppFabric 中的 AppClients 以提高生產力 AppFabric

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

本節說明 AppFabric 的常見錯誤和疑難排解，以提高生產力。

未驗證的應用程式

使用 AppFabric 提高生產力的應用程式開發人員，在向最終使用者啟動其功能之前，將會經歷驗證程序。所有應用程式都開始為未驗證，只有在驗證程序完成時才會變更為已驗證。這表示`starterUserEmails`您在建立 AppClient 時使用的 會看到此訊息。



`CreateAppClient` 錯誤

ServiceQuotaExceededException

如果您在建立 AppClient 時收到下列例外狀況，表示您已超過每個 可建立的 AppClients 數量 AWS 帳戶。限制為 1。HTTP 狀態碼：402

```
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 AppClient 的詳細資訊時收到下列例外狀況，請確定您已輸入正確的 AppClient 識別符。此錯誤表示找不到指定的 AppClient。

```
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 AppClient 時收到下列例外狀況，表示另一個刪除請求正在進行中。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 AppClient 時收到下列例外狀況，請確定您已輸入正確的 AppClient 識別符。此錯誤表示找不到指定的 AppClient。

```
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 AppClient 時收到下列例外狀況，請確定您已輸入正確的 AppClient 識別符。此錯誤表示找不到指定的 AppClient。

```
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 規格中定義的限制條件，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`app_client_id`缺少 。如果尚未建立 AppClient，請建立 AppClient，或使用您現有的 AppClient`app_client_id`，然後再試一次。若要尋找 AppClient ID，請使用 ListAppClient API 操作。

原因 2：當 AppFabric 無法存取客戶受管金鑰時

```
Message: AppFabric couldn't access the customer managed key configured for AppClient.
```

AppFabric 目前無法存取客戶受管金鑰，可能是因為其許可最近有所變更。驗證指定的金鑰是否存在，並確保 AppFabric 獲得適當的存取許可。

原因 3：指定的重新導向 URL 無效

```
Message: Redirect url invalid
```

確保請求中的重新導向 URL 正確。它必須符合您在建立或更新 AppClient 時指定的其中一個重新導向 URLs。若要檢視允許的重新導向 URLs 清單，請使用 GetAppClient API 操作。

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
```

確保您使用的電子郵件地址與建立 AppClient 時為 `starterUserEmails` 屬性列出的電子郵件地址相符。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 GetAppClient API 操作。

原因 2：未指定字符時，Grant_type 為 refresh_token。

```
Message: refresh_token must be non-null for Refresh Token Grant-type
```

請求中指定的重新整理字符為 null 或空白。指定在權杖 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 規格上定義的限制條件，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 AppFabric 提高最終使用者的生產力（預覽）

> 生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

本節適用於希望 enable AWS AppFabric 提高生產力（預覽）以改善其任務管理和工作流程效率的 SaaS 應用程式最終使用者。請依照下列步驟來連接您的應用程式，並授權 AppFabric 呈現跨應用程式洞見，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安排會議）。您可以連接應用程式，例如 Asana、Atlassian Jira Suite、Google Workspace、Microsoft 365、Miro、Slack、

Smartsheet等。在您授權 AppFabric 存取您的內容後，AppFabric 會在您偏好的應用程式中直接提供跨應用程式洞見和動作，協助您更有效率地工作，並保持在目前的工作流程中。

生產力的 AppFabric 使用由 Amazon Bedrock 提供的生成式 AI。AppFabric 只會在收到明確許可後產生洞見和動作。您授權每個個別應用程式保持完全控制使用的內容。AppFabric 不會使用您的資料來訓練或改善用於產生洞見的基礎大型語言模型。如需詳細資訊，請參閱 Amazon Bedrock FAQs。

主題

- 先決條件
- 步驟 1. 登入 AppFabric
- 步驟 2. 同意應用程式顯示洞見
- 步驟 3。連接您的應用程式以產生洞見和動作
- 步驟 4. 開始在您的應用程式中查看洞見並執行跨應用程式動作
- 管理對 AppFabric 的存取，以提高 IT 和安全管理員的生產力（預覽）功能
- 針對 AppFabric 中的最終使用者錯誤進行故障診斷，以提高生產力

先決條件

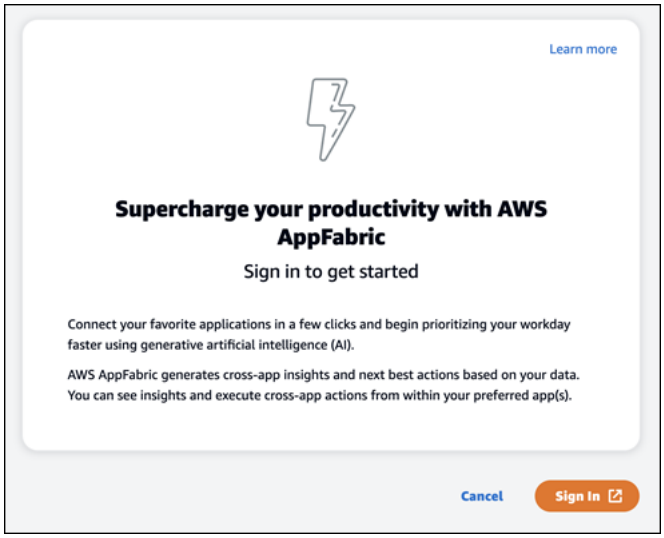
開始之前，請確定您有下列項目：

- 登入 AppFabric 的登入資料：若要開始使用 AppFabric 提高生產力，您需要下列其中一個供應商的聯合登入憑證（使用者名稱和密碼）：Asana、Microsoft 365、 Google Workspace或 Slack。登入 AppFabric 可協助我們將您識別為啟用 AppFabric 以提高生產力的每個應用程式的使用者。登入後，您可以連接應用程式以開始產生洞見。
- 連線應用程式的登入資料：跨應用程式洞見和動作只會根據您授權的應用程式產生。對於您要授權的每個應用程式，您將需要登入憑證（使用者名稱和密碼）。支援的應用程式包括 Asana、Atlassian Jira Suite、Google Workspace、Microsoft 365、Miro、 Slack和 Smartsheet。

步驟 1. 登入 AppFabric

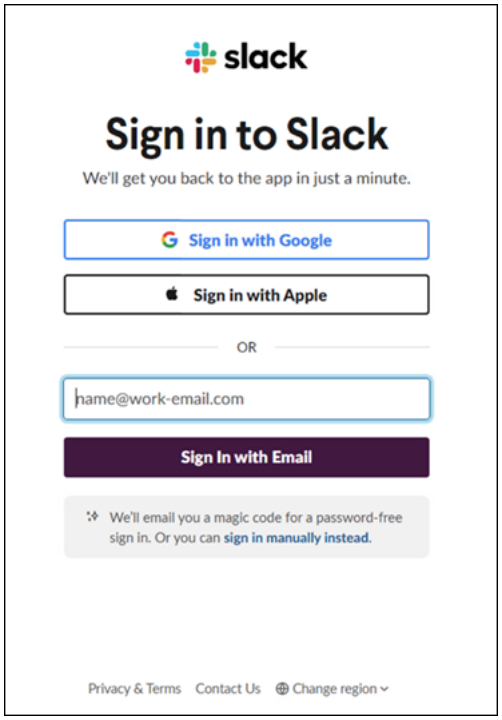
將應用程式連線至 AppFabric，以直接在偏好的應用程式中取得您的內容和洞見。

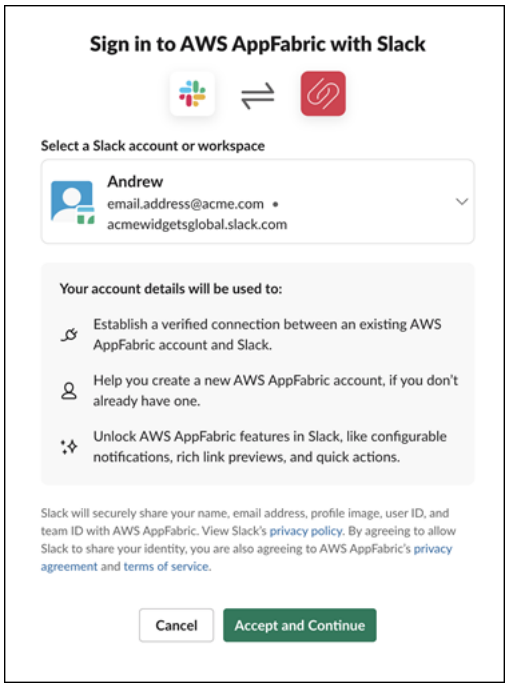
1. 每個應用程式都會以不同方式使用 AppFabric 來提高生產力，讓您擁有更豐富的應用程式體驗。因此，每個應用程式都會有不同的進入點，以連線到下方的 AppFabric 提高生產力首頁。首頁會設定程序的相關內容，以啟用 AppFabric，並提示您登入。您要在 中啟用 AppFabric 的每個應用程式都會到達此畫面。



2. 使用其中一個供應商的登入資料登入：Asana、Microsoft 365、 Google Workspace或 Slack。為了獲得最佳體驗，我們建議您為啟用 AppFabric 的每個應用程式使用相同的供應商登入。例如，如果您在 App1 中選擇 Google Workspace 登入資料，我們建議您Google Workspace在 App2 中選擇，以及每隔您需要重新登入一次。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，請輸入您的登入憑證，並接受從此供應商登入 AppFabric。

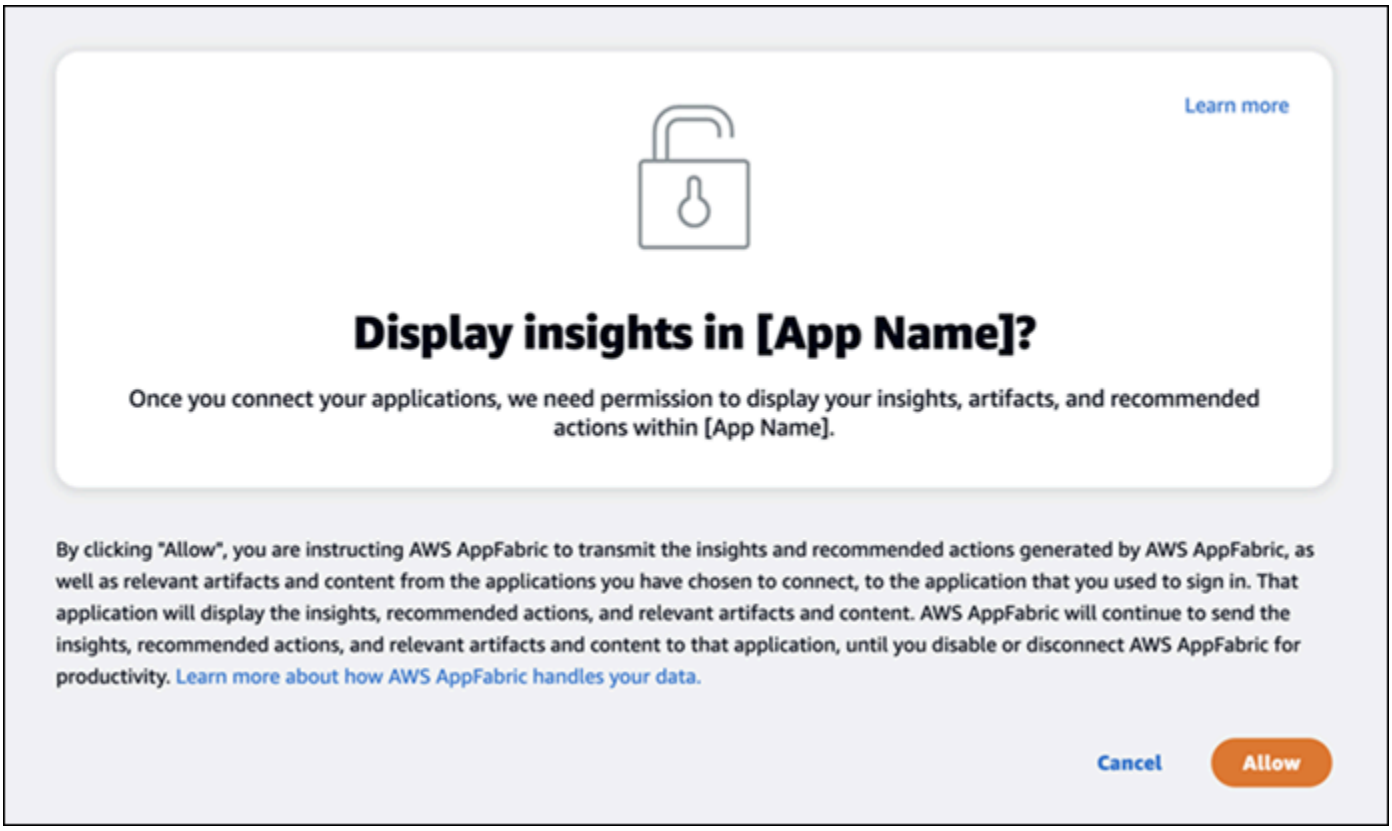




步驟 2. 同意應用程式顯示洞見

登入後，AppFabric 將顯示同意頁面，詢問您是否允許 AppFabric 在您啟用 AppFabric 以提高生產力的應用程式內顯示跨應用程式洞見和動作。例如，您是否允許 AppFabric 接收您的Google Workspace

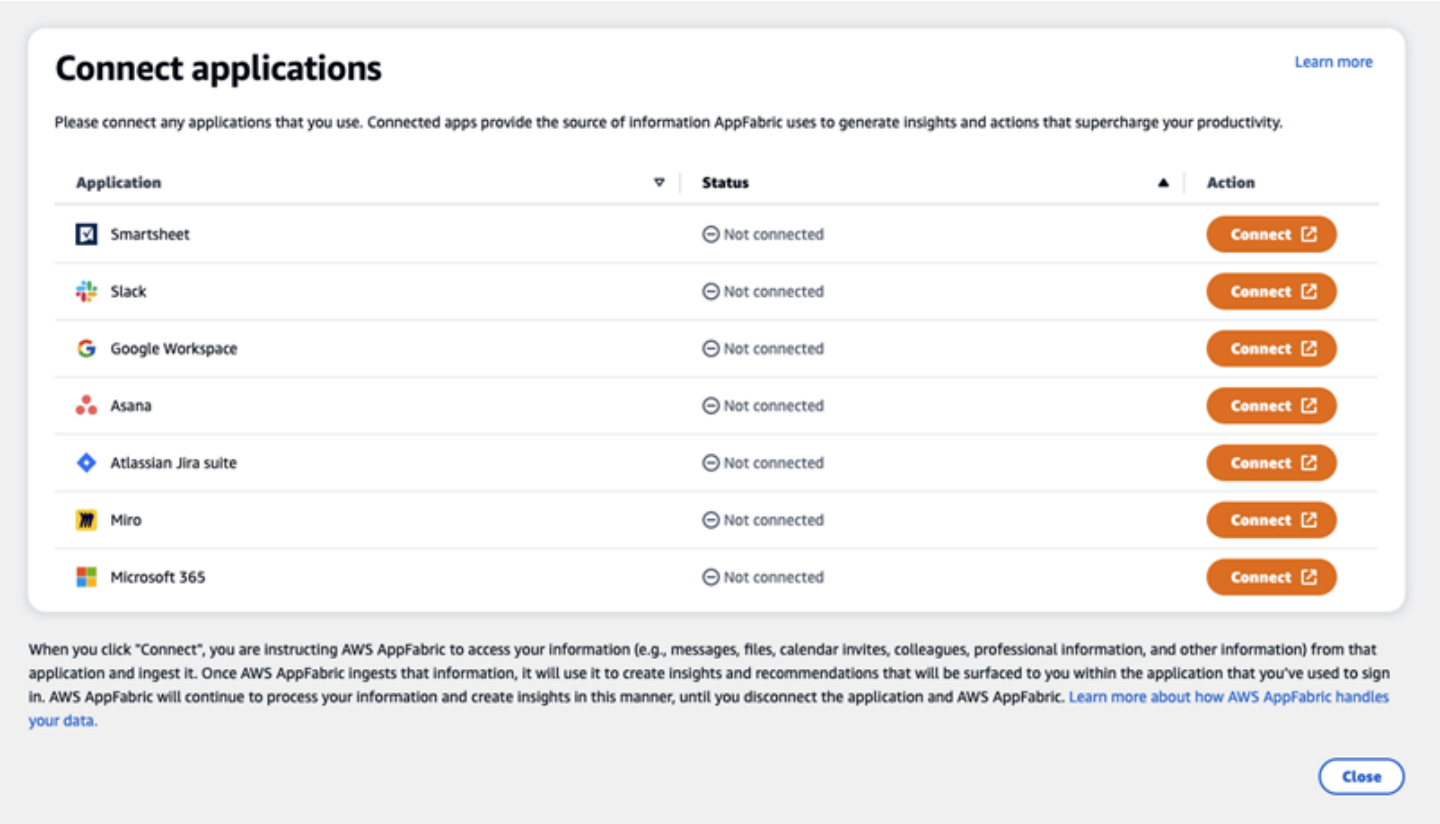
電子郵件和行事曆事件，並將其顯示在 中Asana。您只需要在每個啟用 AppFabric 的應用程式完成此同意步驟一次。



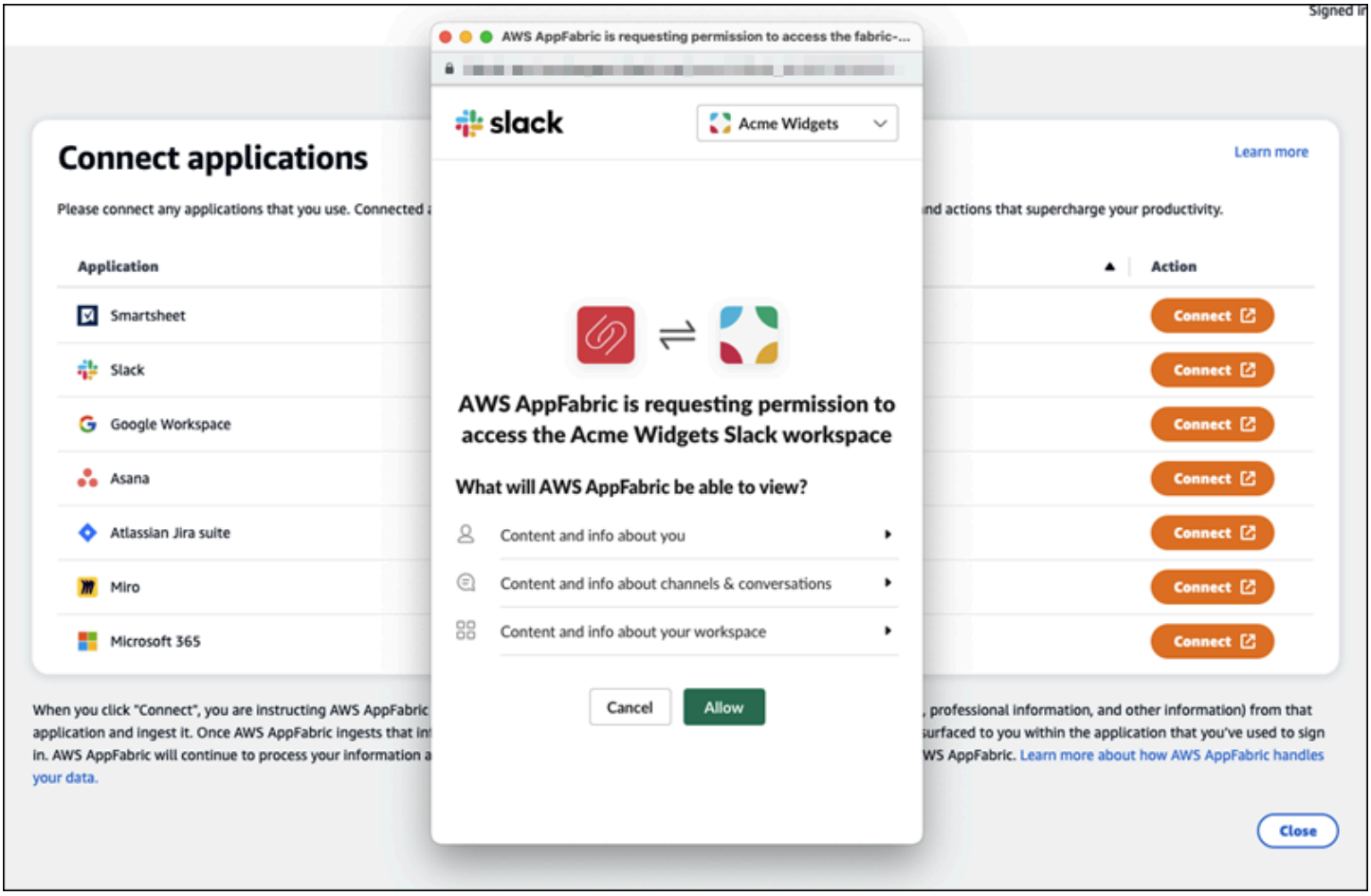
步驟 3。連接您的應用程式以產生洞見和動作

完成同意頁面後，系統會將您導向 Connect 應用程式頁面，您可以在其中連接、中斷連接或重新連接最終用於產生跨應用程式洞見和動作的個別應用程式。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。

若要連接應用程式，請選擇您使用的任何應用程式旁的連線按鈕。



您需要提供應用程式的登入憑證，並允許 AppFabric 存取您的資料以產生洞見和完成動作。

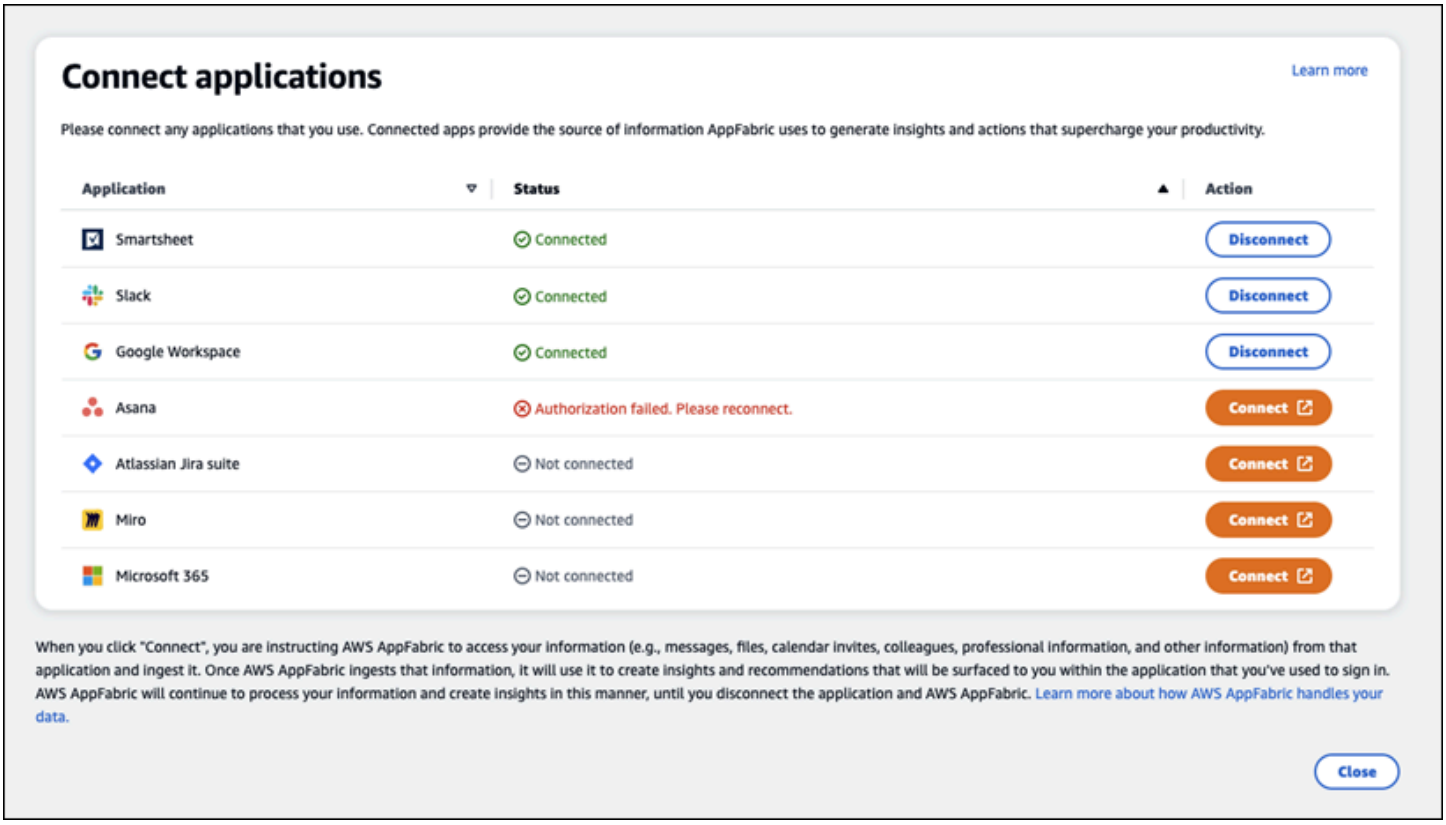


成功連接應用程式後，該應用程式的狀態將從「未連線」變更為「已連線」。提醒：您需要為要用於產生洞見和動作的每個應用程式完成此授權步驟。

連接應用程式後，應用程式永遠不會連線。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擁有產生洞見的許可。

可能的應用程式狀態為：

- 已連線 - AppFabric 已獲授權，且正在使用來自此應用程式的資料產生洞見。
- 未連線 - AppFabric 不會使用此應用程式中的資料產生洞見。您可以連線 以開始產生洞見。
- 授權失敗。請重新連線。- 特定應用程式可能發生授權失敗。如果您看到此錯誤，請嘗試使用 Connect 按鈕重新連接應用程式。



設定已完成，您可以返回您的應用程式。可能需要至少幾個小時才能開始在您的應用程式中看到洞見。

您可以視需要導覽回此頁面，以管理連線的應用程式。如果您選擇中斷連接應用程式，AppFabric 將停止使用該應用程式的資料，或收集新資料以產生新的洞見。如果您選擇在該時間不重新連線應用程式，則會在 7 天內自動刪除中斷連線應用程式的資料。

步驟 4. 開始在您的應用程式中查看洞見並執行跨應用程式動作

將應用程式連線至 AppFabric 後，您將能夠存取寶貴的洞見，並直接從您偏好的應用程式執行跨應用程式動作。注意：每個應用程式不保證此功能，並且完全取決於應用程式開發人員選擇啟用哪些 AppFabric 的生產力功能。

跨應用程式洞見

AppFabric for productivity 提供兩種類型的洞見：

- 可行的洞見：AppFabric 會分析您連線應用程式中電子郵件、行事曆事件、任務和訊息中的資訊，並產生重要洞見，供您排定優先順序。此外，AppFabric 可能會產生建議的動作（例如傳送電子郵件、排程會議和建立任務），您可以在保留在偏好的應用程式中時編輯和執行這些動作。例如，您可能會收到洞見，指出需要處理客戶呈報，並建議下一個動作來排定與客戶的會議。

- 會議準備洞見：此功能可協助您為即將舉行的會議做好準備。AppFabric 將分析您即將舉行的會議，並產生有關會議目的的簡潔摘要。此外，它會顯示連線應用程式的相關成品（例如電子郵件、訊息和任務），這有助於您有效地準備會議，而無需在應用程式之間切換以尋找內容。

跨應用程式動作

對於某些洞見，AppFabric 也可能會產生建議的動作，例如傳送電子郵件、安排會議或建立任務。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 可能會根據洞見產生建議的電子郵件回應或任務名稱。當您按一下建議的動作時，系統會將您導向 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 不會在沒有使用者檢閱和輸入的情況下執行動作，因為生成式 AI 和基礎大型語言模型 (LLM) 可能會不時出現幻覺。

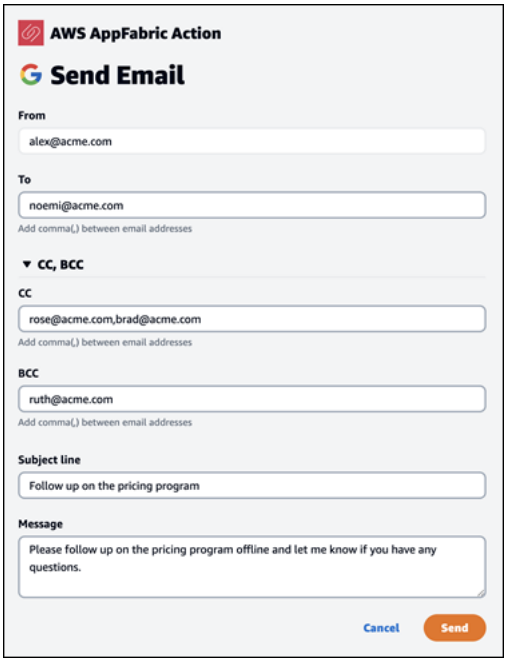
> **Note**
>
> 您有責任驗證和確認 AppFabric LLM 輸出。AppFabric 不保證其 LLM 輸出的準確性或品質。如需詳細資訊，請參閱AWS 負責任的 AI 政策。

建立電子郵件 (Google Workspace、Microsoft 365)

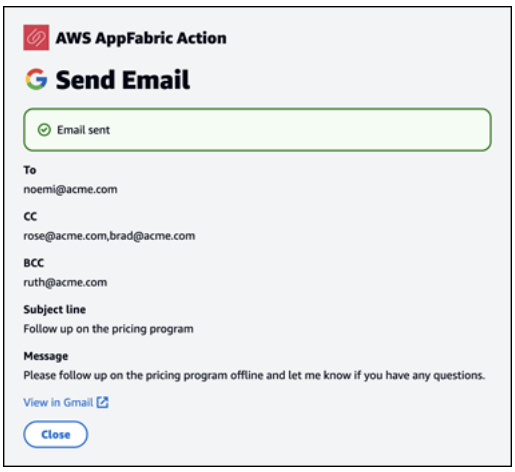
AppFabric 可讓您從偏好的應用程式內編輯和傳送電子郵件。我們支援基本電子郵件欄位，包括寄件者、收件人、副本/副本、電子郵件主旨行和電子郵件內文訊息。AppFabric 可能會在這些欄位中產生內容，以協助您縮短完成任務的時間。編輯完電子郵件後，請選擇傳送以傳送電子郵件。

傳送電子郵件時需要下列欄位：

- 至少需要其中一個收件人電子郵件（收件人、副本和密件副本），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，您會看到電子郵件已傳送的確認。此外，您會在指定的應用程式中看到檢視電子郵件的連結。您可以使用此連結快速導覽至應用程式，並確認電子郵件已傳送。



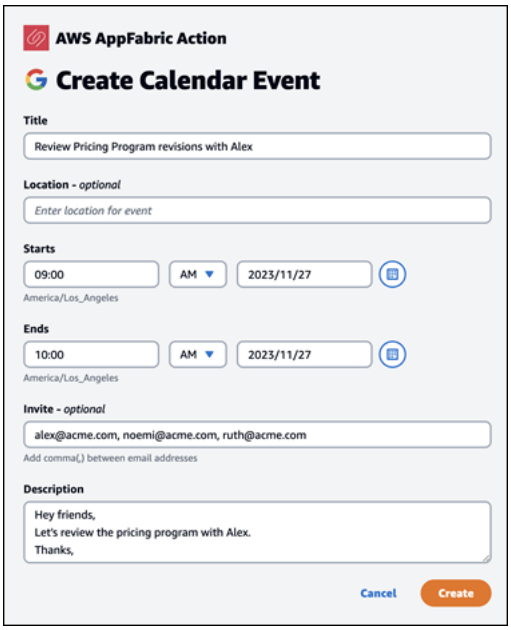
建立行事曆事件 (Google Workspace、Microsoft 365)

AppFabric 可讓您從偏好的應用程式內編輯和建立行事曆事件。我們支援基本行事曆事件欄位，包括事件標題、位置、開始/結束時間和日期、受邀者清單和事件詳細資訊。AppFabric 可能會在這些欄位中產生內容，以協助您縮短完成任務的時間。編輯行事曆事件完成後，請選擇建立以建立事件。

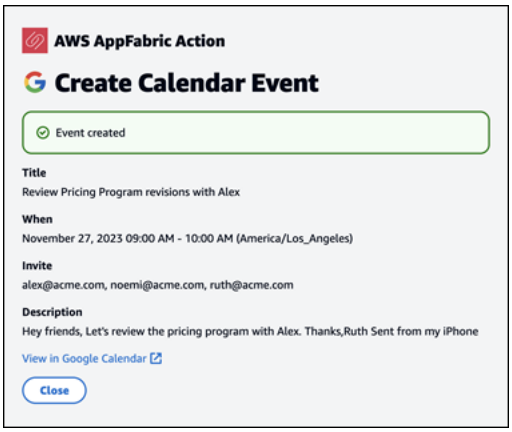
建立行事曆事件需要下列欄位：

- 標題、開始、結束和描述欄位。

- 開始時間和日期不得早於結束時間和日期。
- 邀請欄位是選用的，但如果提供，則需要有效的電子郵件地址。



傳送行事曆事件後，您會看到事件已建立的確認。此外，您會在指定的應用程式中看到檢視事件的連結。您可以使用此連結快速導覽至應用程式，並確認事件已建立。

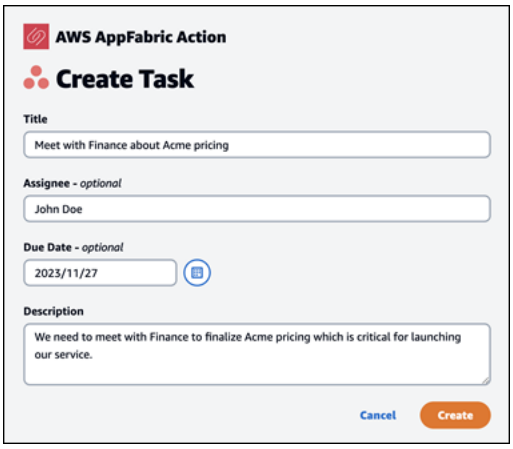


建立任務 (Asana)

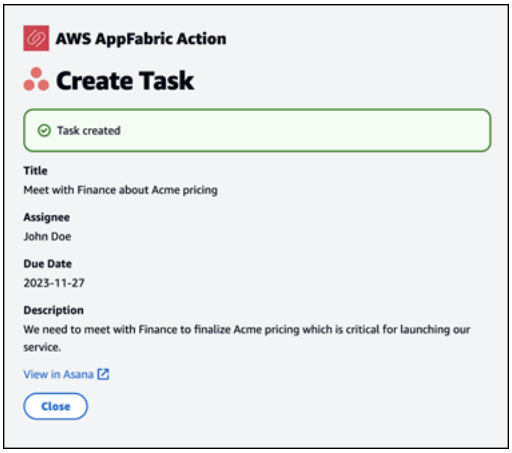
AppFabric 可讓您Asana在偏好的應用程式中，在 中編輯和建立任務。我們支援基本任務欄位，例如任務名稱、任務擁有者、到期日和任務描述。AppFabric 可能會在這些欄位中產生內容，以協助您縮短建立任務的時間。編輯任務完成後，請選擇建立以建立任務。任務是在適用的Asana工作區、專案或任務中建立，如 LLM 所建議。

建立Asana任務需要下列欄位：

- 標題和描述欄位。
- 如果修改，被指派者必須是有效的電子郵件地址。



建立任務後，您會看到任務已在 中建立的確認Asana。此外，您會看到在 中檢視任務的連結Asana。您可以使用此連結快速導覽至應用程式，以確認任務已建立，或將其移至適當的Asana工作區、專案或任務。



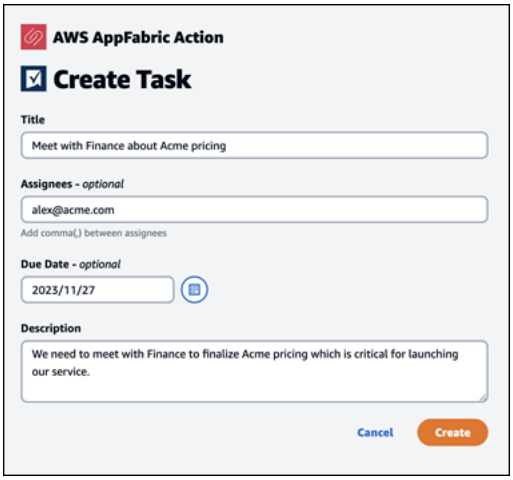
建立任務 (Smartsheet)

AppFabric 可讓您在偏好的應用程式中Smartsheet，在 中編輯和建立任務。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，以協助您縮短建立任務的時間。編輯任務完成後，請選擇建立以建立任務。對於Smartsheet任務，AppFabric 將建立新的私有Smartsheet工作表，並填入任何建立的任務。這是為了協助以結構化方式將 AppFabric 產生的動作集中在單一位置。

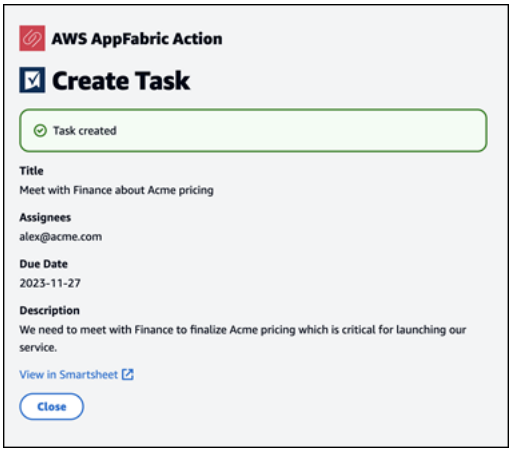
建立Smartsheet任務需要下列欄位：

- 標題和描述欄位。

- 如果提供，被指派者必須是有效的電子郵件地址。



建立任務後，您會看到任務已在 中建立的確認Smartsheet。此外，您會看到在 中檢視任務的連結Smartsheet。您可以使用此連結快速導覽至應用程式，以在建立的Smartsheet工作表中檢視任務。所有未來的Smartsheet任務都會填入此工作表中。如果工作表已刪除，AppFabric 將建立新的工作表。



管理對 AppFabric 的存取，以提高 IT 和安全管理員的生產力（預覽）功能

生產力的 The AWS AppFabric 功能為預覽版，可能會有所變更。

AppFabric for productivity 使用者入口網站可供已與 AppFabric 整合的 SaaS 應用程式所有使用者公開存取，以取得生產力（預覽）功能。如果您是想要管理組織內這些生成式 AI 功能的存取權的 IT 管理員，請考慮以下選項：

- 限制身分提供者 (IdP) 登入：您可以透過身分提供者封鎖登入存取，以控制使用者對生成式 AI 功能的存取。
- 停用特定應用程式的 OAuth：停用 OAuth 來實作下游限制。此動作可防止使用者將需要 OAuth 身分驗證的應用程式連線至公司的工作區。

針對 AppFabric 中的最終使用者錯誤進行故障診斷，以提高生產力

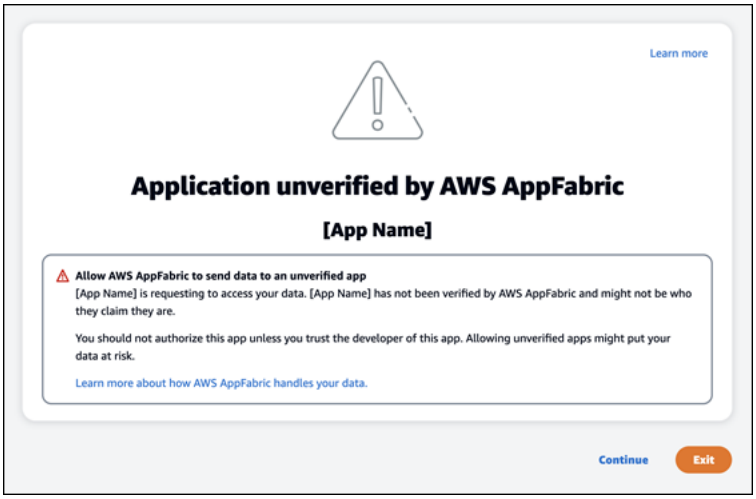
生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

本節說明 AppFabric 生產力的常見錯誤和疑難排解。

未驗證的應用程式

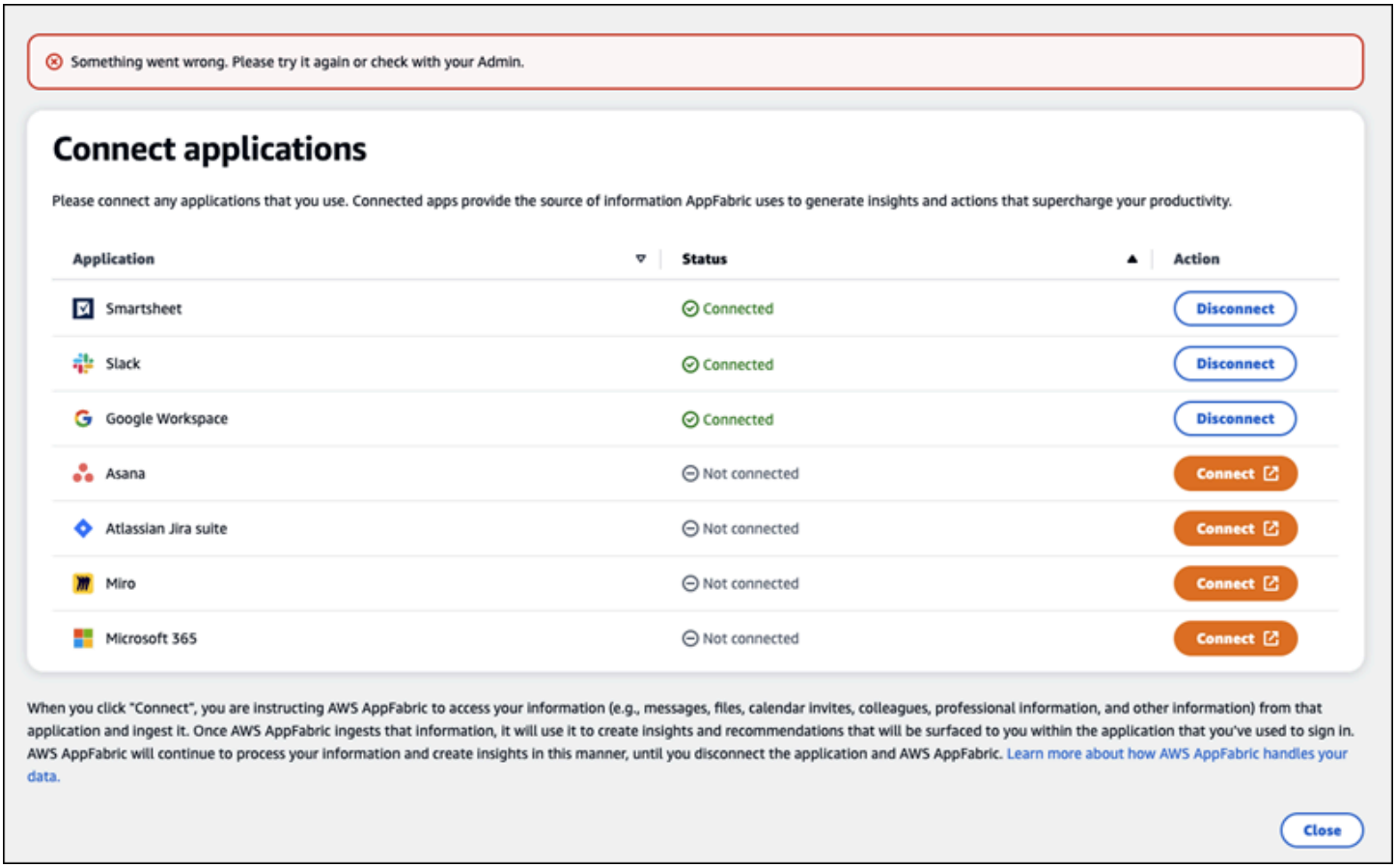
使用 AppFabric 提高生產力的應用程式在向最終使用者啟動其功能之前，將會經過驗證程序。如果您在嘗試登入 AppFabric 時遇到「未驗證」橫幅，這表示應用程式尚未經過 AppFabric 驗證程序，以確認應用程式開發人員的身分和應用程式註冊資訊的準確性。所有應用程式都開始為未驗證，只有在驗證程序完成時才會變更為已驗證。

使用未經驗證的應用程式時請小心。如果您不確定應用程式開發人員，您可以等到應用程式達到已驗證狀態後再繼續。



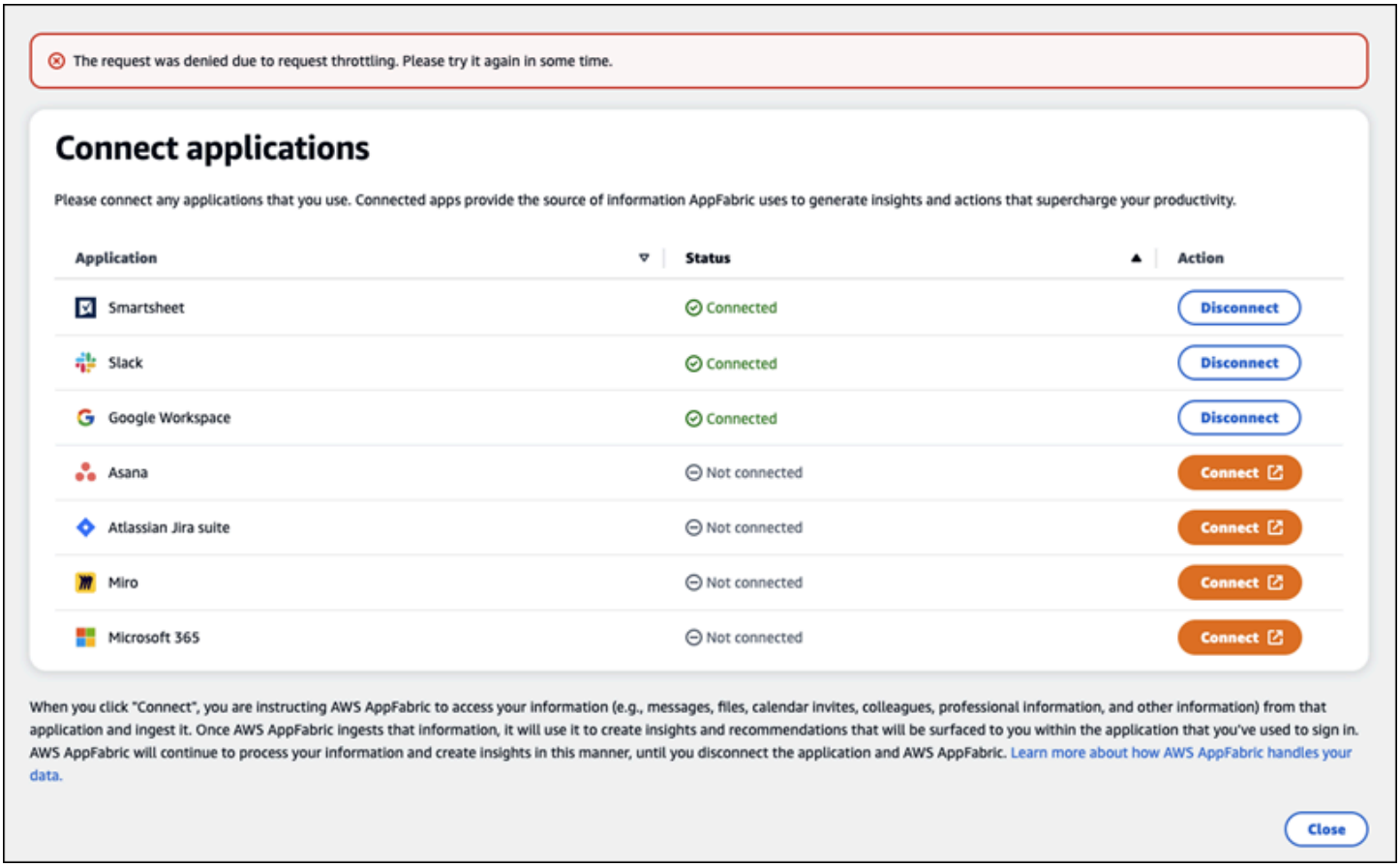
發生錯誤。請再試一次，或向您的管理員確認 (`InternalServerException`)

當 AppFabric 使用者入口網站因為未知錯誤、例外狀況或失敗而無法列出應用程式或中斷連線應用程式時，您可能會收到此訊息。請稍後再試。



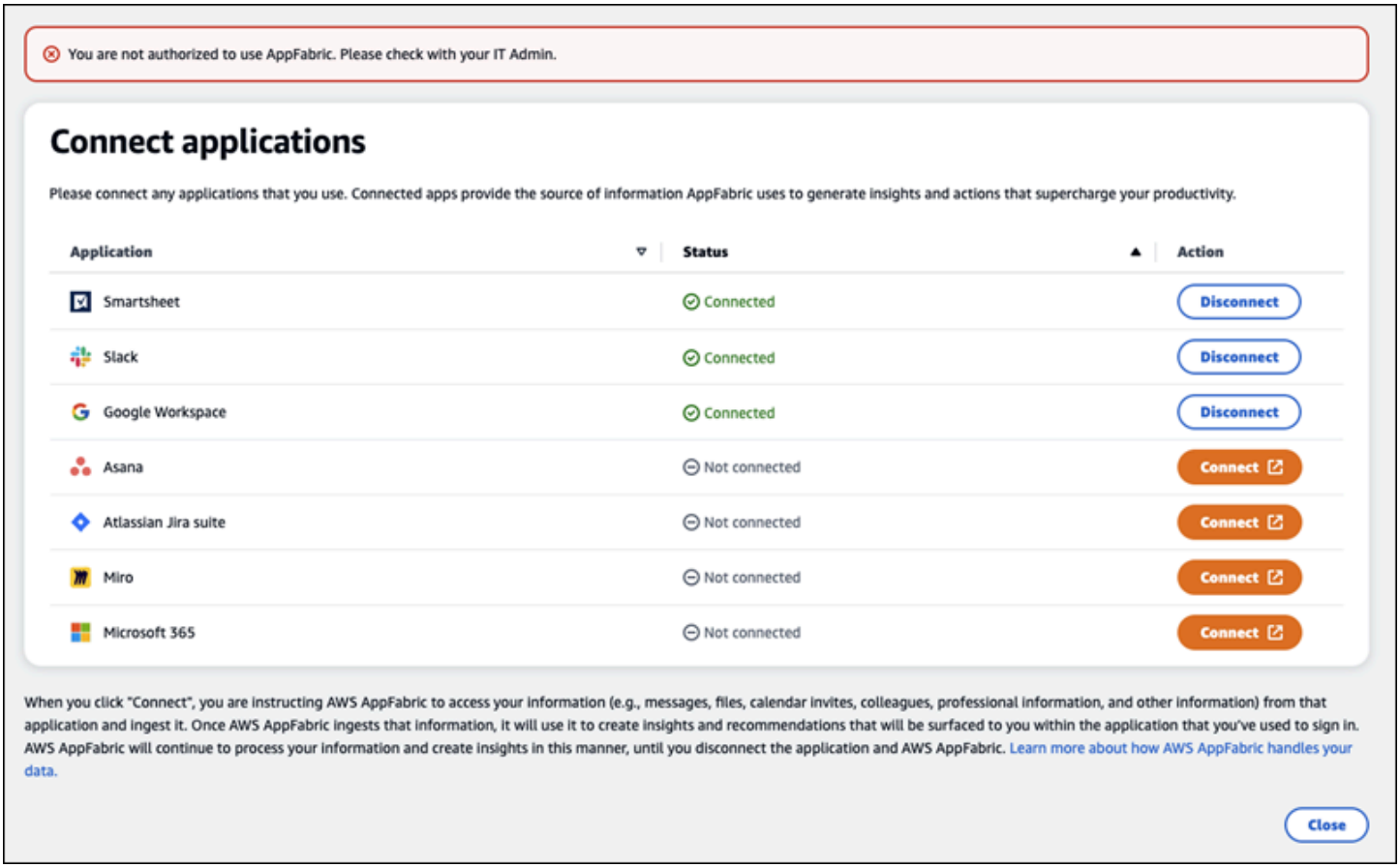
由於請求調節，因此請求遭到拒絕。請稍後再試 (`ThrottlingException`)

當 AppFabric 使用者入口網站因為限流問題而無法列出應用程式或中斷連接應用程式時，您可能會收到此訊息。請稍後再試。



您無權使用 AppFabric。請再次登入 AppFabric (**`AccessDeniedException`**)

當 AppFabric 使用者入口網站因為存取遭拒的例外狀況而無法列出應用程式或中斷連接應用程式時，您可能會收到此訊息。再次登入 AppFabric。



生產力 APIs的 AppFabric （預覽）

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

本節提供 API 操作、資料類型和 the AWS AppFabric 生產力功能的常見錯誤。

> **Note**
>
> 如需所有其他 AppFabric APIs請參閱 AWS AppFabric API 參考。

主題

- 提高生產力的 AppFabric API 動作（預覽）
- 提高生產力的 AppFabric API 資料類型（預覽）
- AppFabric 的常見 API 錯誤以提高生產力（預覽）

提高生產力的 AppFabric API 動作（預覽）

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

AppFabric 支援下列動作以實現生產力功能。

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

生產力的 The AWS AppFabric 功能處於預覽狀態，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
app_client_id	要授權的 AppClient ID。
redirect_uri	授權後將最終使用者重新導向至 的 URI。
state	用來維持請求與回呼之間狀態的唯一值。

CreateAppClient

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

建立 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
appName	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、區分大小寫的識別符，以確保請求的冪等性。這可讓您安全地重試請求，而不會意外再次執行相同的操作。將相同的值傳遞給 操作的後續呼叫，也需要您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
	如果您未提供此值，則 會為您 AWS 產生隨機值。 如果您使用相同的 重試操作`ClientToken` ，但使用不同的參數，則重試會失敗並顯示`IdempotentParameterMismatch` 錯誤。 類型：字串 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
customerManagedKeyIdentifier	由 客戶受管金鑰 產生的 ARN AWS Key Management Service。金鑰用於加密資料。 如果未指定金鑰，則會 AWS 受管金鑰 使用 。要指派給資源之標籤或標籤的鍵值對映射。 如需 AWS 擁有的金鑰 和客戶受管金鑰的詳細資訊，請參閱《 AWS Key Management Service 開發人員指南》中的客戶金鑰和 AWS 金鑰。 類型：字串 長度限制：長度下限為 1。長度上限為 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
iconUrl	AppClient 圖示或標誌的 URL。 類型：字串 必要：否
redirectUrls	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 redirectUrls。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	允許存取以接收洞見的使用者的入門電子郵件地址，直到 AppClient 驗證為止。 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。長度上限為 320。 模式：`[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` 必要：是
tags	要指派給資源之標籤或標籤的鍵值對映射。 類型：標籤物件陣列 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 AppClient 的摘要。 類型：AppClientSummary 物件

DeleteAppClient

生產力的 The AWS AppFabric 功能處於預覽狀態，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	要用於請求之 AppClient 的 Amazon Resource Name (ARN) 或 Universal Unique Identifier (UUID)。 長度限制：長度下限為 1。長度上限為 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

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

傳回 AppClient 的相關資訊。

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
appClientIdentifier	要用於請求之 AppClient 的 Amazon Resource Name (ARN) 或 Universal Unique Identifier (UUID)。 長度限制：長度下限為 1。長度上限為 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
appClient	包含 AppClient 的相關資訊。 類型：AppClient 物件

ListActionableInsights

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

列出最重要的可行電子郵件訊息、任務和其他更新。

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	如果`nextToken` 傳回 ，則會有更多結果可用。的值`nextToken` 是每個頁面的唯一分頁字符。使用傳回的字符再次進行呼叫，以擷取下一頁。讓所有其他引數保持不變。每個分頁字符會在 24 小時後過期。使用過期的分頁字符將傳回 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	列出可行的洞見，包括標題、描述、動作和建立的時間戳記。如需詳細資訊，請參閱ActionableInsights。
nextToken	如果`nextToken` 傳回 ，則會有更多結果可用。的值`nextToken` 是每個頁面的唯一分頁字符。使用傳回的字符再次進行呼叫，以擷取下一頁。讓所有其他引數保持不變。每個分頁字符會在 24 小時後過期。使用過期的分頁字符將傳回 HTTP 400 InvalidToken 錯誤。 類型：字串

ListAppClients

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

傳回所有 AppClients 的清單。

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` 取得進一步的結果頁面。 這只是上限。每次呼叫傳回的實際結果數量可能少於指定的最大值。 有效範圍：最小值為 1。最大值為 100。

參數	描述
nextToken	如果`nextToken` 傳回，則會有更多結果可用。的值`nextToken` 是每個頁面的唯一分頁字符。使用傳回的字符再次進行呼叫，以擷取下一頁。讓所有其他引數保持不變。每個分頁字符會在 24 小時後過期。使用過期的分頁字符將傳回 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	如果`nextToken` 傳回，則會有更多結果可用。的值`nextToken` 是每個頁面的唯一分頁字符。使用傳回的字符再次進行呼叫，以擷取下一頁。讓所有其他引數保持不變。每個分頁字符會在 24 小時後過期。使用過期的分頁字符將傳回 HTTP 400 InvalidToken 錯誤。 類型：字串

ListMeetingInsights

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

列出最重要的可行行事曆事件。

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	如果`nextToken` 傳回，則會有更多結果可用。的值`nextToken` 是每個頁面的唯一分頁字符。使用傳回的字符再次進行呼叫，以擷取下一頁。讓所有其他引數保持不變。每個分頁字符會在 24 小時後過期。使用過期的分頁字符將傳回 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	列出可行的會議洞見。如需詳細資訊，請參閱MeetingInsights。
nextToken	如果`nextToken` 傳回，則會有更多結果可用。的值`nextToken` 是每個頁面的唯一分頁字符。使用傳回的字符再次進行呼叫，以擷取下一頁。讓所有其他引數保持不變。每個分頁字符會在 24 小時後過期。使用過期的分頁字符將傳回 HTTP 400 InvalidToken 錯誤。 類型：字串

PutFeedback

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

允許使用者提交特定洞見或動作的意見回饋。

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	正在提交意見回饋的物件 ID。這可以是 InsightId 或 ActionId。
feedbackFor	正在提交意見回饋的洞見類型。 可能的值： `ACTIONABLE_INSIGHT` | `MEETING_INSIGHT` | `ACTION`
feedbackRating	從 1到 的意見回饋評分5。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

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

包含的資訊可讓 AppClients 交換存取字符的授權碼。

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
grant_type	字符的授予類型。必須為 `authorization_code` 或 `refresh_token` 。 類型：字串 必要：是
app_client_id	AppClient 的 ID。 類型：字串 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
refresh_token	從初始權杖請求收到的重新整理權杖。 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
appfabric_user_id	字符的使用者 ID。這只會針對使用 `authorization_code` 授予類型的請求傳回。 類型：字串
expires_in	直到字符過期的秒數。 類型：Long
refresh_token	用於後續請求的重新整理字符。 類型：字串 長度限制：長度下限為 1。長度上限為 2048。
token	存取權杖。 類型：字串 長度限制：長度下限為 1。長度上限為 2048。
token_type	字符類型。 類型：字串

UpdateAppClient

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

更新 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	要用於請求之 AppClient 的 Amazon Resource Name (ARN) 或 Universal Unique Identifier (UUID)。 長度限制：長度下限為 1。長度上限為 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
redirectUrls	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 redirectUrls。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
appClient	包含 AppClient 的相關資訊。 類型：AppClient 物件

提高生產力的 AppFabric API 資料類型（預覽）

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

AppFabric API 包含各種動作使用的多種資料類型。本節詳細說明用於生產力功能的 AppFabric 資料類型。

如需所有其他 AppFabric API 資料類型，請參閱 AWS AppFabric API 資料類型。

> **Important**
> 不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

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

包含根據使用者應用程式產品組合中的電子郵件、行事曆邀請、訊息和任務，為使用者提供重要和適當動作的摘要。使用者可以跨應用程式查看主動洞見，以協助他們以最佳方式安排一天的方向。這些洞見提供理由，說明使用者為何應該關心洞見摘要以及產生洞見的個別應用程式和成品的參考，例如內嵌連結。

參數	描述
insightId	所產生洞見的唯一 ID。
insightContent	這會將洞見和內嵌連結的摘要傳回用於產生洞見的成品。 這是包含內嵌連結 (<a> 標籤） 的 HTML 內容。
insightTitle	產生的洞見標題。
createdAt	產生洞見的時間。
動作	為產生的洞見建議的動作清單。 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之應用程式的圖示 URL。 • `actionTitle` — 所產生動作的標題。 • `actionUrl` — 最終使用者在 AppFabric 使用者入口網站中檢視和執行動作的唯一 URL。 為了執行動作，ISV 應用程式會使用此 URL 將使用者重新導向至 AppFabric 使用者入口網站（彈出畫面）。 • `actionExecutionStatus` — 指出動作狀態的列舉。 可能的值為： `EXECUTED` | `NOT_EXECUTED`

AppClient

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

包含 AppClient 的相關資訊。

參數	描述
appName	應用程式名稱。 類型：字串 必要：是
arn	AppClient 的 Amazon Resource Name (ARN)。 類型：字串 長度限制：長度下限為 1。長度上限為 1011。 模式：`arn:.+` 必要：是
description	應用程式的說明。 類型：字串 必要：是
iconUrl	AppClient 圖示或標誌的 URL。 類型：字串 必要：否
redirectUrls	AppClient 允許的重新導向 URLs。 類型：字串陣列 陣列成員：項目數下限為 1。項目數上限為 5。

參數	描述
	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	允許存取以接收洞見的使用者的入門電子郵件地址，直到 AppClient 驗證為止。 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。長度上限為 320。 模式：`[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` 必要：是
verificationDetails	包含 AppClient 驗證的狀態和原因。 類型：VerificationDetails 物件 必要：是
customerManagedKeyArn	AWS Key Management Service 為 AppClient 產生的 客戶受管金鑰 Amazon Resource Name (ARN)。 類型：字串 長度限制：長度下限為 1。長度上限為 1011。 模式：`arn:.+` 必要：否

參數	描述
appClientId	AppClient 的 ID。表示用於應用程式用戶端的 o-auth 流程。 類型：字串 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

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

包含 AppClient 的相關資訊。

參數	描述
arn	AppClient 的 Amazon Resource Name (ARN)。 類型：字串 長度限制：長度下限為 1。長度上限為 1011。 模式：`arn:.+` 必要：是
verificationStatus	AppClient 驗證狀態。 類型：字串 有效值:`pending_verification | verified | rejected` 必要：是
appClientId	AppClient 的 ID。表示用於應用程式用戶端的 o-auth 流程。

參數	描述
	類型：字串 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

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

包含前 3 個會議的摘要，以及會議目的、相關的跨應用程式成品，以及任務、電子郵件、訊息和行事曆事件的活動。

參數	描述
insightId	所產生洞見的唯一 ID。
insightContent	洞見的描述會以字串格式反白顯示詳細資訊。如同 ，為什麼此洞見很重要。
insightTitle	產生的洞見標題。
createdAt	產生洞見的時間。
calendarEvent	使用者應關注的重要行事曆事件或會議。 行事曆事件物件： • `startTime` — 事件的開始時間。 • `endTime` — 事件的結束時間。 • `eventUrl` — ISV 應用程式上行事曆事件的 URL。
resources	包含與 相關其他資源的清單會產生洞見。 資源物件：

參數	描述
	• 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 — 資源所屬之應用程式的影像 URL。
nextToken	擷取下一組洞見的分頁字符。這是一個選用欄位，如果傳回 null，表示沒有更多需要載入的洞見。

VerificationDetails

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

包含 AppClient 驗證的狀態和原因。

參數	描述
verificationStatus	AppClient 驗證狀態。 類型：字串 有效值:pending_verification | verified | rejected 必要：是
statusReason	AppClient 驗證狀態原因。 類型：字串 長度限制：長度下限為 1。長度上限為 1024。 必要：否

AppFabric 的常見 API 錯誤以提高生產力（預覽）

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

本節列出適用於 the AWS AppFabric 生產力功能的 API 動作常見的錯誤。

如需所有其他 AppFabric 常見 API 錯誤，請參閱《AppFabric API 參考》中的 故障診斷 AppFabric 中的 AppClients 以提高生產力 AppFabric 和 AppFabric API 常見錯誤。 AWS AppFabric AWS AppFabric

例外狀況名稱	描述
TokenException	字符請求無效。 HTTP 狀態碼：400

AppFabric 中的資料處理

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

AppFabric 會採取步驟，將使用者內容個別存放在由 AppFabric 管理的 Amazon S3 儲存貯體中，並個別存放；這有助於確保我們產生使用者特定的洞見。我們使用合理的保護措施來保護您的內容，其中可能包括靜態加密和傳輸中加密。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 不會使用使用者無法再存取的資料成品產生洞見。例如，當使用者中斷連線資料來源（應用程式）時，AppFabric 會停止從該應用程式收集資料，而且不會使用中斷連線應用程式的任何停留成品來產生洞見。AppFabric 的系統設定為在 30 天內刪除此類資料。

AppFabric 不會使用使用者內容來訓練或改善用於產生洞見的基礎大型語言模型。如需 AppFabric 生成式 AI 功能的詳細資訊，請參閱 Amazon Bedrock FAQs。

靜態加密

AWS AppFabric 支援靜態加密，這是一種伺服器端加密功能，其中 AppFabric 會在保留至磁碟時透明地加密與使用者相關的所有資料，並在您存取資料時解密這些資料。

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 Signature 第 4 版簽署 AWS 服務的 API 請求。

AppFabric 中的術語和概念

本主題說明 in AWS AppFabric 的關鍵術語和概念，以協助您開始使用。

應用程式套件

AppFabric 應用程式套件會存放所有 AppFabric 應用程式授權和擷取（請參閱下列擷取定義）。您可以 AWS 帳戶 為每個 建立一個應用程式套件 AWS 區域。

AppClient（也是應用程式用戶端和應用程式用戶端）

資料收件人應用程式的 OAuth AppClient。每個資料接收者應用程式都需要註冊 AppClient 才能存取 AppFabric 資料。開發人員使用者需要 AWS 帳戶才能註冊 AppClient。每個 AWS 帳戶只能註冊一個 AppClient。AppFabric 會根據 AppClient 提供存取權杖。AppClient 將包含將透過此 AppClient 存取 AppFabric 資料之資料收件人應用程式的相關資訊。

應用程式授權

應用程式授權會授予 AppFabric 與您的應用程式連線和互動的許可。它允許從您的應用程式擷取稽核日誌，使用 OAuth（開放授權 - 開放標準，用於授予應用程式存取權的存取委派）或個人存取字符 (PAT) 登入資料。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 AppFabric 透過重複應用程式的每個租用戶所需的應用程式授權建立步驟，從多個應用程式租用戶擷取稽核日誌。共用的登入資料會使用 AWS 擁有的金鑰 或來自 AWS Key Management Service (AWS KMS) 的客戶受管金鑰加密，並存放在 AppFabric 中。

擷取

AppFabric 擷取會使用應用程式授權，透過應用程式的公有 APIs 從應用程式提取稽核日誌。然後，它會將稽核日誌交付至一或多個（最多五個）目的地。

用戶端 ID

當您建立應用程式授權以與使用 OAuth 流程的應用程式連線時，AppFabric 可能會要求您提供用戶端 ID 和用戶端秘密。您可以在應用程式的身分驗證應用程式中找到用戶端 ID 和用戶端秘密。如需在指定身分驗證應用程式中尋找用戶端 ID 位置的說明，請參閱支援的應用程式。共用的用戶端 ID 和用戶端秘密會使用 AWS 擁有的金鑰 或客戶受管 AWS KMS 金鑰加密，並存放在 AppFabric 中。

Client secret (用戶端密碼)

當您建立應用程式授權以與使用 OAuth 流程的應用程式連線時，AppFabric 可能會要求您提供用戶端 ID 和用戶端秘密。您可以在應用程式的身分驗證應用程式中找到用戶端 ID 和用戶端秘密。如需有關在

指定身分驗證應用程式中尋找用戶端秘密位置的說明，請參閱支援的應用程式。共用的用戶端 ID 和用戶端秘密會使用 AWS 擁有的金鑰 或客戶受管 AWS KMS 金鑰加密，並存放在 AppFabric 中。

擷取目的地

擷取目的地定義應存放從擷取提取的稽核日誌的位置。每個擷取都可以將稽核日誌交付至一或多個目的地（最多五個），即 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose AWS 帳戶。對於每個目的地，您可以定義日誌是原始形式還是標準化為開放式網路安全結構描述架構 (OCSF) 結構描述。選取 OCSF 結構描述時，您可以定義日誌的格式 (JSON 或 Apache Parquet)。只有在選取 Amazon S3 做為目的地時，才能使用 Apache Parquet 格式。

資料收件人應用程式

將呼叫 AppFabric 以從 AppFabric 取得產生洞見的應用程式。

OAuth

OAuth 是一種開放式通訊協定，可在 Web、行動和桌面應用程式的簡單標準方法中允許安全授權。AppFabric 使用 OAuth 來建立一些應用程式授權。

Open Cybersecurity Schema Framework (OCSF)

Open Cybersecurity 結構描述架構 (OCSF) 是一個開放原始碼專案，提供可擴展的架構來開發結構描述，以及與廠商無關的核心安全結構描述。廠商和其他資料生產者可以採用並擴展其特定網域的結構描述。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標準和程序。AppFabric 已擴展此結構描述，以建立以服務 (SaaS) 為中心的軟體事件結構，AppFabric 支援的所有 SaaS 應用程式稽核日誌都會標準化。如需詳細資訊，請參閱開啟網路安全結構描述架構 for AWS AppFabric。

個人存取字符 (PAT)

個人存取字符 (PAT) 是一組字元，可用來存取電腦系統，而不是一般密碼。當您建立與使用 PAT 流程的應用程式連線的應用程式授權時，AppFabric 可能會要求您提供 PAT。您可以在應用程式的身分驗證應用程式中找到 PAT。如需在特定身分驗證應用程式中何處尋找 PAT 的說明，請參閱支援的應用程式。共用的服務帳戶字符會使用 AWS 擁有的金鑰 或客戶受管 AWS KMS 金鑰加密，並存放在 AppFabric 中。

服務帳戶字符

當您建立 AppFabric 應用程式授權以與應用程式連線時，某些應用程式需要建立服務帳戶以進行應用程式身分驗證。AppFabric 可能會在應用程式授權程序中要求服務帳戶字符。如需在指定身分驗證應用

程式中尋找服務帳戶字符的說明，請參閱支援的應用程式。共用的服務帳戶字符會使用 AWS 擁有的金鑰 或客戶受管 AWS KMS 金鑰加密，並存放在 AppFabric 中。

租用戶 ID

當您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。租戶 ID 是您應用程式租戶的唯一識別符。每個應用程式對於租用戶可能會有不同的術語，例如 的工作區 ID Slack或 的網域 IDAsana。如需在特定應用程式中尋找租用戶 ID 位置的說明，請參閱支援的應用程式。

租戶名稱

當您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 ID 的唯一名稱，可用於應用程式套件。此值用於標記應用程式授權和任何相關的擷取。

安全 in AWS AppFabric

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。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 負責保護在 AWS 服務 中執行的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。在AWS 合規計畫中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用於 AWS AppFabric 的合規計劃，請參閱AWS 合規計劃的 服務範圍。
- 雲端的安全性 – 您的責任取決於您使用 AWS 服務 的 。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 AppFabric 時套用共同責任模型。下列主題說明如何設定 AppFabric 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務 來協助您監控和保護 AppFabric 資源。

主題

- in AWS AppFabric 資料保護
- for AWS AppFabric 的身分和存取管理
- for AWS AppFabric 的合規驗證
- AWS AppFabric 的安全最佳實務
- in AWS AppFabric 的彈性
- 基礎設施安全 in AWS AppFabric
- in AWS AppFabric 中的組態和漏洞分析

in AWS AppFabric 資料保護

AWS 共同責任模型適用於 in AWS AppFabric 的資料保護。如此模型所述， AWS 負責保護執行所有 的全域基礎設施 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，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 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。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 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 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，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) 140-3。

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 AppFabric 或使用主控台、API AWS CLI或 AWS SDKs的其他 AWS 服務 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

> **Note**
>
> 如需適用於 AppFabric 之資料保護的詳細資訊，請參閱 AppFabric 中的資料處理。

靜態加密

AWS AppFabric 支援靜態加密，這是一種伺服器端加密功能，在此功能中AppFabric 會在應用程式套件保留至磁碟時透明地加密與應用程式套件相關的所有資料，並在您存取資料時解密這些資料。根據預設，AppFabric 會使用 AWS 擁有的金鑰 from AWS Key Management Service () 加密您的資料AWS KMS。您也可以選擇使用自己的客戶受管金鑰來加密資料 AWS KMS。

當您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

設定應用程式套件時，您可以選擇 AWS 擁有的金鑰 或客戶受管金鑰。收集和標準化稽核日誌擷取的資料時，AppFabric 會將資料暫時存放在中繼 Amazon Simple Storage Service (Amazon S3) 儲存貯體中，並使用此金鑰對其進行加密。此中繼儲存貯體會在 30 天後使用儲存貯體生命週期政策刪除。

AppFabric 會使用 TLS 1.2 保護傳輸中的所有資料，並使用 AWS Signature V4 簽署 的 AWS 服務 API 請求。

金鑰管理

AppFabric 支援使用 AWS 擁有的金鑰 或客戶受管金鑰加密資料。我們建議您使用客戶受管金鑰，因為它可讓您完全控制加密的資料。當您選擇客戶受管金鑰時，AppFabric 會將資源政策連接至客戶受管金鑰，以授予其存取客戶受管金鑰的權限。

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》中的建立對稱加密 KMS 金鑰的步驟。

金鑰政策

金鑰政策控制對客戶受管金鑰的存取。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。如需建立金鑰政策的相關資訊，請參閱《 AWS KMS 開發人員指南》中的建立金鑰政策。

若要搭配 AppFabric 使用客戶受管金鑰，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許可。我們建議您建立僅與 AppFabric 搭配使用的金鑰，並將 AppFabric 使用者新增為金鑰的使用者。此方法會限制對您資料的存取範圍。您的使用者所需的許可如下：

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:Decrypt`

AWS KMS 主控台會引導您建立具有適當金鑰政策的金鑰。如需金鑰政策的詳細資訊，請參閱《 AWS KMS 開發人員指南》中的 中的金鑰政策 AWS KMS。

以下是允許 的範例金鑰政策：

- 金鑰的完整 AWS 帳戶根使用者 控制權。
- 允許使用者使用 AppFabric 搭配 AppFabric 使用您的客戶受管金鑰。
- 在 中設定應用程式套件的金鑰政策`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"
                }
            }
        }
    ]
```

```
}
```

AppFabric 如何在 中使用授予 AWS KMS

AppFabric 需要授予才能使用您的客戶受管金鑰。如需詳細資訊，請參閱《 AWS KMS 開發人員指南》中的在 中授予 AWS KMS。

當您建立應用程式套件時，AppFabric 會透過傳送CreateGrant請求至 來代表您建立授予 AWS KMS。中的授權 AWS KMS 用於授予 AppFabric 存取客戶帳戶中的 AWS KMS 金鑰。AppFabric 要求授予 將客戶受管金鑰用於下列內部操作：

- 將GenerateDataKey請求傳送至 AWS KMS ，以產生由客戶受管金鑰加密的資料金鑰。
- 將Decrypt請求傳送至 AWS KMS 以解密加密的資料金鑰，以便它們可用於加密您的資料，並在傳輸中解密應用程式存取字符。
- 傳送Encrypt請求至 AWS KMS ，以加密傳輸中的應用程式存取字符。

以下是授予的範例。

```
{
  "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，AppFabric 會淘汰客戶受管金鑰的發行授予。

監控 AppFabric 的加密金鑰

當您搭配 AppFabric 使用 AWS KMS 客戶受管金鑰時，您可以使用 AWS CloudTrail 日誌來追蹤 AppFabric 傳送的請求 AWS KMS。

以下是 AppFabric `CreateGrant`用於客戶受管金鑰時所記錄的 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"
    }
}
```

for AWS AppFabric 的身分和存取管理

AWS Identity and Access Management (IAM) 是 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （登入） 和授權 （具有許可），以使用 AppFabric 資源。IAM 是您可以免費使用 AWS 服務 的 。

主題

- 目標對象
- 使用身分驗證
- 使用政策管理存取權
- How AWS AppFabric 可與 IAM 搭配使用
- AWS AppFabric 的身分型政策範例
- 使用 AppFabric 的服務連結角色
- AWS for AWS AppFabric 的 受管政策
- 故障診斷 AWS AppFabric 身分和存取

目標對象

您使用 AWS Identity and Access Management (IAM) 的方式會有所不同，取決於您在 AppFabric 中執行的工作。

服務使用者 – 如果您使用 AppFabric 服務來執行任務，管理員會為您提供所需的登入資料和許可。當您使用更多 AppFabric 功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 AppFabric 中的功能，請參閱 故障診斷 AWS AppFabric 身分和存取。

服務管理員 – 如果您在公司負責 AppFabric 資源，您可能擁有 AppFabric 的完整存取權。您的任務是判斷服務使用者應存取的 AppFabric 功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何搭配 AppFabric 使用 IAM，請參閱 How AWS AppFabric 可與 IAM 搭配使用。

IAM 管理員 – 如果您是 IAM 管理員，建議您了解撰寫政策以管理 AppFabric 存取的詳細資訊。若要檢視您可以在 IAM 中使用的 AppFabric 身分型政策範例，請參閱 AWS AppFabric 的身分型政策範例。

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者身分、IAM 使用者身分或擔任 IAM 角色來驗證 （登入 AWS)。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分身分登入 。 AWS IAM Identity Center (IAM Identity Center) 使用者、您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。當您使用聯合 AWS 身分存取 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。如需登入的詳細資訊 AWS，請參閱AWS 登入 《 使用者指南》中的如何登入您的 AWS 帳戶 。

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的 憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的適用於 API 請求的AWS Signature 第 4 版。

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 建議您使用多重驗證 (MFA) 來提高帳戶的安全性。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 IAM 中的AWS 多重要素驗證。

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，該身分可完整存取帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 Theroot 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

最佳實務是， 要求人類使用者，包括需要管理員存取權的使用者，使用臨時 AWS 服務 憑證與身分提供者聯合來存取 。

聯合身分是您企業使用者目錄、Web 身分提供者、 AWS Directory Service、Identity Center 目錄或任何使用透過身分來源提供的登入資料 AWS 服務 存取的使用者。當聯合身分存取時 AWS 帳戶，它們會擔任 角色，而角色會提供臨時登入資料。

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，也可以連接並同步到您自己的身分來源中的一組使用者 AWS 帳戶 和群組，以便

在所有 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，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 中的身分 AWS 帳戶 ，具有單一人員或應用程式的特定許可。建議您盡可能依賴臨時憑證，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，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要暫時在 中擔任 IAM 角色 AWS Management Console，您可以從使用者切換至 IAM 角色（主控台）。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並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 (聯合) 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 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，在某些 中 AWS 服務，您可以將政策直接連接到資源（而不是使用角色做為代理）。如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。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。
  - 轉送存取工作階段 (FAS) – 當您使用 IAM 使用者或角色在其中執行動作時 AWS，您會被視為委託人。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 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。
  - 服務連結角色 – 服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。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 執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。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臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策是 中的物件，當與身分或資源建立關聯時， AWS 會定義其許可。當委託人（使用者、根使用者或角色工作階段）發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。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。具有該政策的使用者可以從 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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。如需了解如何在受管政策及內嵌政策之間選擇，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。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

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

存取控制清單 (ACL)

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。

Amazon S3 AWS WAF和 Amazon VPC 是支援 ACLs的服務範例。如需進一步了解 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政策類型。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。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。

- 服務控制政策 SCPs) – SCPs是 JSON 政策，可指定 中組織或組織單位 (OU) 的最大許可 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶 之多個 的服務。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 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs的詳細資訊，包括支援 RCPs AWS 服務 的 清單，請參閱AWS Organizations 《 使用者指南》中的資源控制政策 (RCPs)。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。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。如需詳細資訊，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。若要了解如何 AWS 決定是否在涉及多個政策類型時允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

How AWS AppFabric 可與 IAM 搭配使用

在您使用 IAM 管理 AppFabric 的存取權之前，請先了解哪些 IAM 功能可與 AppFabric 搭配使用。

您可以搭配 AWS AppFabric 使用的 IAM 功能

IAM 功能	AppFabric 支援
身分型政策	是
資源型政策	否
政策動作	是

IAM 功能	AppFabric 支援
政策資源	是
政策條件索引鍵	否
ACL	否
ABAC (政策中的標籤)	是
臨時憑證	否
主體許可	是
服務角色	否
服務連結角色	是

若要全面了解 AppFabric 和其他 如何與大多數 IAM 功能 AWS 服務 搭配使用，請參閱《IAM 使用者指南》中的與 IAM AWS 搭配使用的 服務。

AppFabric 的身分型政策

支援身分型政策：是

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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

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。

AppFabric 的身分型政策範例

若要檢視 AppFabric 身分型政策的範例，請參閱 AWS AppFabric 的身分型政策範例。

AppFabric 中的資源型政策

支援資源型政策：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。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，做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。當委託人和資源位於不同位置時 AWS 帳戶，信任帳戶中的 IAM 管理員也必須授予委託人實體（使用者或角色）存取資源的許可。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 中的快帳戶資源存取。

AppFabric 的政策動作

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內容。也就是說，哪個主體在什麼条件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API 操作相同的名稱。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中的 AWS AppFabric 定義的動作。

AppFabric 中的政策動作在動作之前使用以下字首：

```
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 AppFabric 身分型政策的範例，請參閱 AWS AppFabric 的身分型政策範例。

AppFabric 的政策資源

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 ARNs 的清單，請參閱服務授權參考中的 AWS AppFabric 定義的資源類型。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 AWS AppFabric 定義的動作。

若要檢視 AppFabric 身分型政策的範例，請參閱 AWS AppFabric 的身分型政策範例。

AppFabric 的政策條件索引鍵

支援服務特定的政策條件索引鍵：否

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。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， 會使用邏輯OR操作 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的條件金鑰。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要查看 AppFabric 條件索引鍵的清單，請參閱服務授權參考中的適用於 AWS AppFabric 的條件索引鍵。若要了解您可以使用條件索引鍵的動作和資源，請參閱 AWS AppFabric 定義的動作。

若要檢視 AppFabric 身分型政策的範例，請參閱 AWS AppFabric 的身分型政策範例。

AppFabric ACLs

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。

ABAC 搭配 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。您可以將標籤連接到 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。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，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》中的使用 ABAC 授權定義許可。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)。

搭配 AppFabric 使用臨時登入資料

支援臨時登入資料：否

當您使用臨時登入資料登入時，有些 AWS 服務 無法運作。如需詳細資訊，包括哪些 AWS 服務 使用臨時登入資料，請參閱《AWS 服務 IAM 使用者指南》中的使用 IAM 的 。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入 ，則會使用臨時登入資料。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取 時，該程序會自動建立臨時登入資料。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》中的從使用者切換至 IAM 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。

AppFabric 的跨服務主體許可

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，您會被視為委託人。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 使用呼叫 的委託人許可 AWS 服務，結合 AWS 服務 請求向下游服務提出請求。只有當服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會提出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱轉發存取工作階段。

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。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。

> **Warning**
>
> 變更服務角色的許可可能會中斷 AppFabric 功能。只有在 AppFabric 提供指引時，才能編輯服務角色。

AppFabric 的服務連結角色

支援服務連結角色：是

服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。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

根據預設，使用者和角色沒有建立或修改 AppFabric 資源的許可。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行任務。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。

如需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 (主控台)。

如需 AppFabric 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 格式，請參閱服務授權參考中的適用於 AWS AppFabric 的動作、資源和條件索引鍵。

內容

- 政策最佳實務
- 使用 AppFabric 主控台
- 適用於安全 IAM 政策範例的 AppFabric
  - 允許存取應用程式套件
  - 限制對應用程式套件的存取
  - 限制刪除或停止擷取
- 適用於生產力的 AppFabric IAM 政策範例
  - 允許存取唯讀存取生產力功能
  - 允許完整存取生產力功能
  - 允許建立 AppClients 的存取權
  - 允許存取以取得 AppClients 的詳細資訊
  - 允許存取列出 AppClients
  - 允許存取以更新 AppClients
  - 允許存取以刪除 AppClients
  - 允許存取以授權應用程式

- 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

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 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 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。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。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 AWS CloudFormation。如需詳細資訊，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，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html中的透過 MFA 的安全 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 `AWSAppFabricReadOnlyAccess` AWS 受管政策連接至您的 IAM 身分，將唯讀許可授予 AppFabric 服務，包括 中的 AppFabric 主控台 AWS Management Console。或者，您可以將 `AWSAppFabricFullAccess` AWS 受管政策連接至您的 IAM 身分，將完整的管理許可授予 AppFabric 服務。如需詳細資訊，請參閱AWS for AWS AppFabric 的 受管政策。

適用於安全 IAM 政策範例的 AppFabric

下列政策範例適用於 AppFabric 的安全功能。

允許存取應用程式套件

下列政策範例會授予 AppFabric 服務中應用程式套件的存取權。

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

限制對應用程式套件的存取

下列政策範例限制對 AppFabric 服務中應用程式套件的存取。

```
{
    "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

下列政策範例會限制刪除或停止 AppFabric 服務中的擷取。

```
{
    "Statement": [
        {
            "Action": ["appfabric:*"],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StopIngestion",
                "appfabric:DeleteIngestion",
                "appfabric:DeleteIngestionDestination"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

適用於生產力的 AppFabric IAM 政策範例

生產力的 The AWS AppFabric 功能處於預覽狀態，可能會有所變更。

下列政策範例適用於 AppFabric 的生產力功能。

允許存取唯讀存取生產力功能

下列政策範例授予對 AppFabric 的唯讀存取權，以實現生產力功能。

> **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。這是因為適用於生產力功能的 AppFabric 目前處於預覽狀態。您應該忽略錯誤並繼續建立政策。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppClient",
                "appfabric:ListActionableInsights",
                "appfabric:ListAppClients",
                "appfabric:ListMeetingInsights"
            ],
            "Resource": "*"
        }
    ],
    "Version": "2012-10-17"
}
```

允許完整存取生產力功能

下列政策範例會授予 AppFabric 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。這是因為適用於生產力功能的 AppFabric 目前處於預覽狀態。您應該忽略錯誤並繼續建立政策。

```
{
    "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"
}
```

允許建立 AppClients 的存取權

下列政策範例會授予建立 AppClients 的存取權。如需詳細資訊，請參閱建立 AppFabric 以提高生產力 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。這是因為適用於生產力功能的 AppFabric 目前處於預覽狀態。您應該忽略錯誤並繼續建立政策。

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

允許存取以取得 AppClients 的詳細資訊

下列政策範例會授予存取權，以取得 AppClients 的詳細資訊。如需詳細資訊，請參閱取得 AppClient 的詳細資訊。

> **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。這是因為適用於生產力功能的 AppFabric 目前處於預覽狀態。您應該忽略錯誤並繼續建立政策。

```
{
```

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

允許存取列出 AppClients

下列政策範例授予列出 AppClients 的存取權。如需詳細資訊，請參閱取得 AppClient 的詳細資訊。

> **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。這是因為適用於生產力功能的 AppFabric 目前處於預覽狀態。您應該忽略錯誤並繼續建立政策。

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

允許存取以更新 AppClients

下列政策範例授予更新 AppClients 的存取權。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。這是因為適用於生產力功能的 AppFabric 目前處於預覽狀態。您應該忽略錯誤並繼續建立政策。

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

允許存取以刪除 AppClients

下列政策範例授予刪除 AppClients 的存取權。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。這是因為適用於生產力功能的 AppFabric 目前處於預覽狀態。您應該忽略錯誤並繼續建立政策。

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

```
}
```

允許存取以授權應用程式

下列政策範例授予使用權杖 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。這是因為適用於生產力功能的 AppFabric 目前處於預覽狀態。您應該忽略錯誤並繼續建立政策。

```
{
    "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。此政策包含在 主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
```

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

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至 AppFabric 的唯一 IAM 角色類型。服務連結角色由 AppFabric 預先定義，並包含該服務 AWS 服務 代表您呼叫其他 所需的所有許可。

服務連結角色可讓您更輕鬆地設定 AppFabric，因為您不必手動新增必要的許可。AppFabric 定義其服務連結角色的許可，除非另有定義，否則只有 AppFabric 可以擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 IAM 實體。

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

如需有關支援服務連結角色的其他 服務的資訊，請參閱服務連結角色欄中與 AWS IAM 搭配使用的 服務，並尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

AppFabric 的服務連結角色許可

AppFabric 使用名為 的服務連結角色 `AWSServiceRoleForAppFabric` – 允許 AppFabric 將資料放入擷取目的地資源，例如 Amazon S3 儲存貯體或 Amazon Data Firehose 交付串流。它還允許 AppFabric 將 CloudWatch 指標資料放在`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 的角色許可政策`AWSAppFabricServiceRolePolicy`允許 AppFabric 對指定的資源完成下列動作：

- 動作：在 `AWS/AppFabric` 命名空間`cloudwatch:PutMetricData`中。此動作授予 AppFabric 將指標資料放入 Amazon CloudWatch `AWS/AppFabric`命名空間的許可。如需 CloudWatch 中可用 AppFabric 指標的詳細資訊，請參閱 搭配 Amazon CloudWatch 的 Monitoring AWS AppFabric 。
- 動作：在 Amazon S3 儲存貯體`s3:PutObject`中。此動作授予 AppFabric 將擷取資料放入您指定之 Amazon S3 儲存貯體的許可。
- 動作：在 Amazon Data Firehose 交付串流`firehose:PutRecordBatch`中。此動作授予 AppFabric 將擷取資料放入您指定之 Amazon Data Firehose 交付串流的許可。

如需詳細資訊，請參閱 AWS AppFabric 的 受管政策。

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。

為 AppFabric 建立服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、 AWS CLI或 AWS API 中建立 AppFabric 應用程式套件時，AppFabric 會為您建立服務連結角色。

編輯 AppFabric 的服務連結角色

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」的編輯服務連結角色。

刪除 AppFabric 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。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。角色會使用您在 AppFabric 中建立的應用程式套件。如需詳細資訊，請參閱安全資源的 Delete AWS AppFabric 。

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

手動刪除 服務連結角色

使用 IAM 主控台 AWS CLI、 或 AWS API 來刪除`AWSServiceRoleForAppFabric`服務連結角色。如需詳細資訊，請參閱「IAM 使用者指南」中的刪除服務連結角色。

AppFabric 服務連結角色支援的區域

AppFabric 支援在所有提供服務 AWS 區域 的 中使用服務連結角色。如需詳細資訊，請參閱《》中的 AppFabric 端點和配額AWS 一般參考。

AWS for AWS AppFabric 的 受管政策

若要新增許可給使用者、群組和角色，使用 AWS 受管政策比自行撰寫政策更容易。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 受管政策。您無法變更 AWS 受管政策中的許可。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 受管政策中移除許可，因此政策更新不會破壞您現有的許可。

此外， AWS 支援跨多個 服務之任務函數的受管政策。例如，ReadOnlyAccess AWS 受管政策提供所有 AWS 服務 和 資源的唯讀存取權。當服務啟動新功能時， 會為新操作和資源 AWS 新增唯讀許可。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 受管政策： AWSAppFabricReadOnlyAccess

您可將 `AWSAppFabricReadOnlyAccess` 政策連接到 IAM 身分。此政策會將唯讀許可授予 AppFabric 服務。

> **Note**
>
> 該`AWSAppFabricReadOnlyAccess`政策不會授予對 AppFabric 的唯讀存取權，以實現生產力功能。

許可詳細資訊

此政策包含以下許可：

- `appfabric` – 准許取得應用程式套件、列出應用程式套件、取得應用程式授權、列出應用程式授權、取得擷取、列出擷取、取得擷取目的地、列出擷取目的地，以及列出資源標籤。

```
{
    "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 受管政策： AWSAppFabricFullAccess

您可將 `AWSAppFabricFullAccess` 政策連接到 IAM 身分。此政策會將管理許可授予 AppFabric 服務。

> **Important**
>
> 此`AWSAppFabricFullAccess`政策不會授予 AppFabric 的生產力功能存取權，因為它們目前處於預覽狀態。如需針對生產力功能執行 AppFabric 存取權的詳細資訊，請參閱 適用於生產力的 AppFabric IAM 政策範例。

許可詳細資訊

此政策包含以下許可：

- `appfabric` – 授予 AppFabric 完整的管理許可。
- `kms` – 准許列出別名。
- `s3` – 准許列出所有 Amazon S3 儲存貯體，並取得儲存貯體位置。
- `firehose` – 准許列出 Amazon Data Firehose 交付串流，並描述交付串流。
- `iam` – 准許為 AppFabric 建立`AWSServiceRoleForAppFabric`服務連結角色。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 受管政策： AWSAppFabricServiceRolePolicy

您無法將 `AWSAppFabricServiceRolePolicy` 政策附加至 IAM 實體。此政策會連接到服務連結角色，允許 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` – 准許 AppFabric 將指標資料放入 Amazon CloudWatch `AWS/AppFabric`命名空間。如需 CloudWatch 中可用 AppFabric 指標的詳細資訊，請參閱 搭配 Amazon CloudWatch 的 Monitoring AWS AppFabric 。

- `s3` – 准許 AppFabric 將擷取的資料放入您指定的 Amazon S3 儲存貯體。
- `firehose` – 准許 AppFabric 將擷取的資料放入您指定的 Amazon Data Firehose 交付串流。

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

AWS 受管政策的 AppFabric 更新

檢視自此服務開始追蹤這些變更以來，AppFabric AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱 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 新增了新的政策，將唯讀許可授予 AppFabric 服務。	2023 年 6 月 27 日
AWSAppFabricFullAccess – 新政策	AppFabric 新增了新的政策，將管理許可授予 AppFabric 服務。	2023 年 6 月 27 日
AWSAppFabricServiceRolePolicy – 新政策	AppFabric 新增`AWSServiceRoleForAppFabric` 了服務連結角色的新政策。	2023 年 6 月 27 日
AppFabric 已開始追蹤變更	AppFabric 開始追蹤其 AWS 受管政策的變更。	2023 年 6 月 27 日

故障診斷 AWS AppFabric 身分和存取

使用以下資訊來協助您診斷和修正使用 AppFabric 和 IAM 時可能遇到的常見問題。

主題

- 我無權在 AppFabric 中執行動作
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 以外的人員 AWS 帳戶 存取我的 AppFabric 資源

我無權在 AppFabric 中執行動作

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

如果您收到錯誤，告知您無權執行 `iam:PassRole`動作，您的政策必須更新，以允許您將角色傳遞至 AppFabric。

有些 AWS 服務 可讓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 `marymajor` 使用者嘗試使用主控台在 AppFabric 中執行動作時，會發生下列範例錯誤。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。

我想要允許 以外的人員 AWS 帳戶 存取我的 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：

- 若要了解 AppFabric 是否支援這些功能，請參閱 How AWS AppFabric 可與 IAM 搭配使用。
- 若要了解如何提供您擁有 AWS 帳戶 的資源存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 中為 IAM 使用者提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。

- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

for AWS AppFabric 的合規驗證

若要了解 是否 AWS 服務 在特定合規計劃的範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 AWS Compliance Programs。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載報告 in AWS Artifact

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源來協助合規：

- 安全合規與治理 - 這些解決方案實作指南內容討論了架構考量，並提供部署安全與合規功能的步驟。
- HIPAA 合格服務參考 – 列出 HIPAA 合格服務。並非所有 AWS 服務 都符合 HIPAA 資格。
- AWS 合規資源 – 此工作手冊和指南集合可能適用於您的產業和位置。
- AWS 客戶合規指南 – 透過合規的角度了解共同責任模型。本指南摘要說明跨多個架構 （包括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)) 保護 AWS 服務 和映射指南至安全控制的最佳實務。
- 《 AWS Config 開發人員指南》中的使用規則評估資源 – AWS Config 服務會評估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 可讓您全面檢視其中的安全狀態 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 控制參考」。
- Amazon GuardDuty – 這會監控您的環境是否有可疑和惡意活動，以 AWS 服務 偵測對您 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可滿足特定合規架構所規定的入侵偵測需求，以協助您因應 PCI DSS 等各種不同的合規需求。
- AWS Audit Manager – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和業界標準的方式。

AWS AppFabric 的安全最佳實務

AWS AppFabric 提供數種安全功能，供您在開發和實作自己的安全政策時考慮。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。

在沒有管理員存取權的情況下監控應用程式

透過唯讀 AWS Identity and Access Management (IAM) 許可，任何人都可以將 AppFabric 與 Amazon QuickSight 和其他安全資訊和事件管理 (SIEM) 工具整合，例如 Splunk。為了監控應用程式安全性，資料會交付至 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 Amazon Data Firehose 交付串流。

監控 AppFabric 事件

您可以使用 Amazon CloudWatch 指標監控 AppFabric。CloudWatch 每分鐘從 AppFabric 收集資料，並將其處理為指標。您可以設定警示，在指標符合指定的閾值時觸發通知。如需詳細資訊，請參閱搭配 Amazon CloudWatch 的 Monitoring AWS AppFabric 。

in AWS AppFabric 的彈性

AWS 全球基礎設施是以 AWS 區域 和 可用區域為基礎建置。 AWS 區域 提供多個實體隔離和隔離的可用區域，這些可用區域與低延遲、高輸送量和高備援聯網連接。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 全球基礎設施。

基礎設施安全 in AWS AppFabric

作為受管服務， AWS AppFabric 受到 Amazon Web Services：安全程序概觀白皮書中所述的 AWS 全球網路安全程序的保護。

您可以使用 AWS 已發佈的 API 呼叫，透過網路存取 AppFabric。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，若要產生臨時安全登入資料來簽署請求，您可以使用 AWS Security Token Service(AWS STS) 。

in AWS AppFabric 中的組態和漏洞分析

組態和 IT 控制是客戶 AWS 與您之間的共同責任。如需詳細資訊，請參閱 AWS 共同的責任模型。

Monitoring AWS AppFabric

監控是維護 AWS AppFabric 和其他 AWS 解決方案可靠性、可用性和效能的重要部分。 AWS 提供下列監控工具來監看 AppFabric、報告錯誤，並在適當時自動採取動作：

- Amazon CloudWatch AWS 會即時監控您的 AWS 資源和您在 上執行的應用程式。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，您可以讓 CloudWatch 追蹤 CPU 使用量或其他 Amazon EC2 執行個體指標，並在需要時自動啟動新的執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。
- Amazon CloudWatch Logs 可讓您從 Amazon EC2 執行個體和其他來源監控 AWS CloudTrail、存放和存取您的日誌檔案。CloudWatch Logs 可監控日誌檔案中的資訊，並在達到特定閾值時通知您。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 Logs 使用者指南。
- AWS CloudTrail 會擷取由 或 代您發出的 API 呼叫和相關事件， AWS 帳戶 並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。您可以識別呼叫哪些使用者和帳戶 AWS、進行呼叫的來源 IP 地址，以及呼叫的時間。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》https://docs.aws.amazon.com/awscloudtrail/latest/userguide/。

搭配 Amazon CloudWatch 的 Monitoring AWS AppFabric

您可以使用 CloudWatch 監控 AWS AppFabric，這會收集原始資料並將其處理為可讀的近乎即時的指標。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指標。

指標	描述
AppFabric 應用程式授權狀態	應用程式授權的狀態 (1 表示已連線； 0 表示任何其他）。
AppFabric 資料交付延遲	AppFabric 從 SaaS 應用程式收集稽核日誌並將其交付至設定目的地 (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 表示作用中； 0表示任何其他）。
整體資料延遲	事件發生在 SaaS 應用程式上，以及對應稽核日誌交付至 AppFabric 所設定目的地 (Amazon S3 或 Amazon Data Firehose) 之間的時間差異（以秒為單位）。
擷取資料的磁碟區	傳送至 Amazon Simple Storage Service (Amazon S3) 或 Amazon Data Firehose 的資料大小。

AppFabric 指標支援以下維度。

維度	描述
擷取目的地 Arn	擷取目的地的 Amazon Resource Name (ARN)。

Logging AWS AppFabric API 呼叫使用 AWS CloudTrail

AWS AppFabric 已與 整合 AWS CloudTrail，此服務提供使用者、角色或 AppFabric AWS 服務 中所採取動作的記錄。CloudTrail 會將 AppFabric 的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 AppFabric 主控台的呼叫，以及對 AppFabric API 操作的程式碼呼叫。如果您建立線索，則可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 AppFabric 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。使用 CloudTrail 收集的資訊，您可以判斷對 AppFabric 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

如需有關 CloudTrail 的相關資訊，請參閱 AWS CloudTrail 使用者指南。

CloudTrail 中的 AppFabric 資訊

建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當活動在 AppFabric 中發生時，該活動會記錄於 CloudTrail 事件，以及事件歷史記錄中的其他 AWS 服務 事件。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 使用者指南中的 使用 CloudTrail 事件歷史記錄檢視事件。

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

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

CloudTrail 會記錄所有 AppFabric 動作，並記錄在 AWS AppFabric API 參考中。例如，對 `CreateAppBundle`、`UpdateAppBundle` 以及 `GetAppBundle` 動作發出的呼叫會在 CloudTrail 日誌檔案中產生項目。

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：

- 請求是使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務服務提出。

如需詳細資訊，請參閱AWS CloudTrail 《 使用者指南》中的 CloudTrail userIdentity元素。

了解 AppFabric 日誌檔案項目

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

以下範例顯示的是展示 `CreateAppBundle` 動作的 CloudTrail 日誌項目。

```
{
    "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"
    }
}
```

AppFabric 的配額

您的 AWS 帳戶 具有每個 的預設配額，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 AppFabric 的配額，請開啟 Service Quotas 主控台。在導覽窗格中，選擇 AWS 服務，然後選取 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。

下表 AWS 帳戶 顯示與 中 AppFabric 相關的配額。

名稱	預設	可調整	描述
應用程式套件	每個受支援的區域：1	否	您可以在目前 AWS 區域中的 帳戶中建立的應用程式套件數量上限。
應用程式授權	每個受支援的區域：50	否	您可以在目前 AWS 區域中的 帳戶中建立的應用程式授權數目上限。
擷取	每個受支援的區域：50	否	您可以在目前 AWS 區域中的 帳戶中建立的擷取數目上限。
擷取目的地	每個受支援的區域：5	否	您可以在目前 AWS 區域中的帳戶中為每個擷取建立的擷取目的地數量上限。
AppClient	每個受支援的區域：1	否	您可以在目前 AWS 區域中的 帳戶中建立的 AppClients 數量上限。

名稱	預設	可調整	描述
			生產力的 The AWS AppFabric 功能為預覽版，可能會有所變更。

AppFabric 管理指南的文件歷史記錄

下表說明 for AWS AppFabric 的文件版本。

變更	描述	日期
新的支援應用程式	新增 JumpCloud 為支援的應用程式。如需詳細資訊，請參閱 AWS AppFabric 中支援的應用程式。	2024 年 6 月 5 日
新的支援應用程式和安全工具	新增 Azure Monitor和 Google Analytics 做為支援的應用程式。如需詳細資訊，請參閱 AWS AppFabric 中支援的應用程式。新增 Singularity Cloud 做為支援的安全工具。如需詳細資訊，請參閱相容的安全工具。	2024 年 4 月 30 日
新的支援應用程式	新增 SentinelOne 為支援的應用程式。如需詳細資訊，請參閱 AWS AppFabric 中支援的應用程式。	2024 年 4 月 25 日
新的支援應用程式	新增 1Password 為支援的應用程式。如需詳細資訊，請參閱 AWS AppFabric 中支援的應用程式。	2024 年 4 月 23 日
新的支援安全工具	新增 Dynatrace 做為相容的安全工具。如需詳細資訊，請參閱相容的安全工具。	2024 年 3 月 26 日
新指標	新增 AppFabric 應用程式授權狀態指標。如需詳細資訊，請參閱使用 Amazon CloudWatc	2024 年 3 月 8 日

	h Logs 的 Monitoring AWS AppFabric。	
新的支援應用程式	新增 IBM Security® Verify 為支援的應用程式。如需詳細資訊，請參閱 AWS AppFabric 中支援的應用程式。	2024 年 3 月 6 日
新的支援應用程式	新增 Box 為支援的應用程式。如需詳細資訊，請參閱 in AWS AppFabric 中支援的應用程式。	2024 年 2 月 28 日
新的支援應用程式和指標	新增 Cisco Duo、 Salesforce 和 Terraform Cloud做為支援的應用程式。如需詳細資訊，請參閱 in AWS AppFabric 中支援的應用程式。新增 AppFabric 資料交付延遲和整體資料延遲指標。如需詳細資訊，請參閱使用 Amazon CloudWatch Logs 的 Monitoring AWS AppFabric。	2024 年 2 月 1 日
新增 Atlassian Confluence、Genesys Cloud、HubSpot、PagerDuty、 OneLogin by One Identity和 Ping Identity做為支援的應用程式，並 Barracuda XDR做為相容的安全工具	如需新支援應用程式的詳細資訊，請參閱 in AWS AppFabric 中支援的應用程式和相容的安全工具。	2023 年 12 月 15 日

新增 Atlassian Confluence、Genesys Cloud、Hub Spot、PagerDuty、 OneLogin by One Identity和 Ping Identity做為支援的應用程式，並 Barracuda XDR做為相容的安全工具	如需新支援應用程式的詳細資訊，請參閱 in AWS AppFabric 中支援的應用程式和相容的安全工具。	2023 年 12 月 15 日
新增生產力預覽文件的 The AWS AppFabric	如需 AppFabric 提高生產力的詳細資訊，請參閱什麼是 AWS AppFabric 提高生產力？	2023 年 11 月 27 日
新增 GitHub和 ServiceNow做為支援的應用程式	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 for AWS AppFabric 的 AWS 受管政策	如需 AppFabric AWS 受管政策的詳細資訊，請參閱 AWS for AWS AppFabric 的受管政策。	2023 年 6 月 27 日
初始版本	初始版本的 AWS AppFabric 管理指南。	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。