AWS 白皮书

SageMaker 工作室管理最佳做法

SageMaker 工作室管理最佳做法: AWS 白皮书

Table of Contents

SageMaker 工作室管理最佳做法

出版日期：二零二三年四月二十五日（ ）文件修訂

摘要

Amazon SageMaker Studio 提供單一網頁式視覺化介面，您可以在其中執行所有機器學習 (ML) 開發步驟，進而提高資料科學團隊的生產力。 SageMaker Studio 可讓您完整存取、控制和檢視建置、訓練和評估模型所需的每個步驟。

在本白皮書中，我們討論主題的最佳做法，包括作業模式、網域管理、身分識別管理、權限管理、網路管理、記錄、監控和自訂。此處討論的最佳做法適用於企業 SageMaker Studio 部署，包括多租用戶部署。本文件適用於 ML 平台管理員、ML 工程師和 ML 架構設計人員。

你是否 Well-Architected？

AWSWell-Architected 的架構可協助您瞭解在雲端中建置系統時所做決策的優缺點。Framework 的六大支柱可讓您學習如何設計和操作可靠、安全、高效、符合成本效益且可持續發展的系統的架構最佳實務。使用中免費提供的 AWS Well-Architected ToolAWS Management Console，您可以針對每個支柱回答一組問題，根據這些最佳實務來檢閱工作負載。

在 M achine Learning 鏡頭中，我們專注於如何在中設計、部署和架構您的機器學習工作負載AWS 雲端。此鏡頭增加了 Well-Architected 的框架中描述的最佳實踐。

簡介

當您將 SageMaker Studio 管理為 ML 平台時，您需要做出明智決策的最佳實務指引，以協助您隨著工作負載的成長擴充機器學習平台。若要佈建、操作和擴展 ML 平台，請考慮下列事項：

- 選擇正確的作業模式並組織機器學習環境，以符合您的業務目標。
- 選擇如何設定使用者身分識別的 SageMaker Studio 網域驗證，並考量網域層級限制。
- 決定如何將使用者的身分識別和授權聯合至 ML 平台，以進行精細的存取控制和稽核。
- 考慮為 ML 角色的各種角色設置權限和護欄。
- 根據機器學習工作負載的敏感度、使用者數量、執行個體類型、應用程式和啟動的工作，規劃您的虛擬私有雲 (VPC) 網路拓撲。
- 使用加密功能，分類並保護靜態和傳輸中的資料。

- 考慮如何記錄和監視各種應用程式設計介面 (API) 和使用者活動，以確保合規性。
- 使用您自己的映像檔和生命週期組態指令碼，自訂 SageMaker Studio 筆記本體驗。

經營模式

作業模型是將人員、程序和技術結合在一起的架構，協助組織以可擴充、一致且有效率的方式提供商業價值。ML 作業模型為整個組織的團隊提供標準的產品開發流程。有三種模式用於實現操作模型，具體取決於大小，複雜性和業務驅動因素：

- 集中式資料科學團隊 — 在此模型中，所有資料科學活動都集中在單一團隊或組織中。這類似於卓越中心 (COE) 模型，所有業務單位都會前往此團隊進行資料科學專案。
- 去中心化的數據科學團隊 — 在這個模型中，數據科學活動分佈在不同的業務職能或部門，或基於不同的產品線。
- 聯合資料科學團隊 — 在此模型中，共用服務功能，例如程式碼儲存庫、持續整合和持續交付 (CI/CD) 管道等，由集中式團隊管理，每個業務單位或產品層級功能均由分散的團隊管理。這類似於中樞和支點模型，其中每個業務單位都有自己的資料科學團隊；但是，這些業務單位團隊會與集中式團隊協調其活動。

在決定為生產使用案例啟動您的第一個 studio 網域之前，請考慮您的作業模型和組織環境的AWS最佳實務。如需詳細資訊，請參閱使用多個帳戶組織AWS環境。

下一節提供針對每個作業模式組織帳戶結構的指引。

建議的帳戶結構

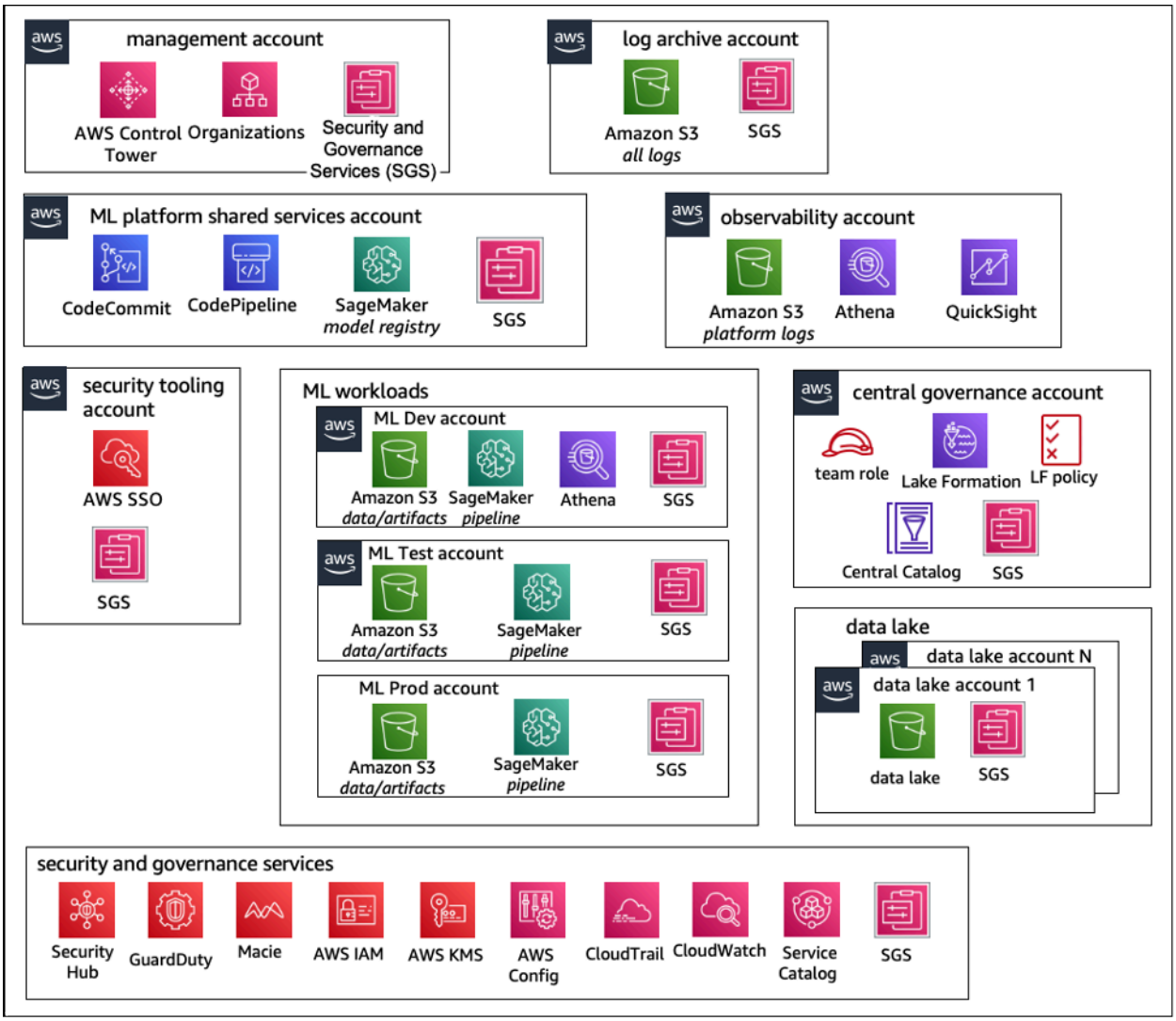
在本節中，我們簡要介紹一個操作模型帳戶結構，您可以根據組織的營運需求開始並進行修改。無論您選擇哪種操作模式，我們都建議您實施以下常見的最佳實踐：

- 用AWS Control Tower於設定、管理和管理您的帳戶。
- 透過委派的管理員 Securitiy Tokine 帳戶，透過您的身分識別提供者 (IdP) 和 AWSIAM 身分中心集中您的身分識別，並啟用對工作負載的安全存取。
- 透過跨開發、測試和生產工作負載的帳戶層級隔離來執行 ML 工作負載。
- 將 ML 工作負載記錄檔串流至記錄封存帳戶，然後在觀察性帳戶中篩選並套用記錄分析。
- 執行集中式控管帳戶以供佈建、控制和稽核資料存取。
- 根據您的組織和工作負載要求，將安全和治理服務 (SGS) 嵌入適當的預防性和偵探護欄到每個帳戶中，以確保安全性和合規性。

集中式模型帳戶結構

在此模型中，ML 平台小組負責提供：

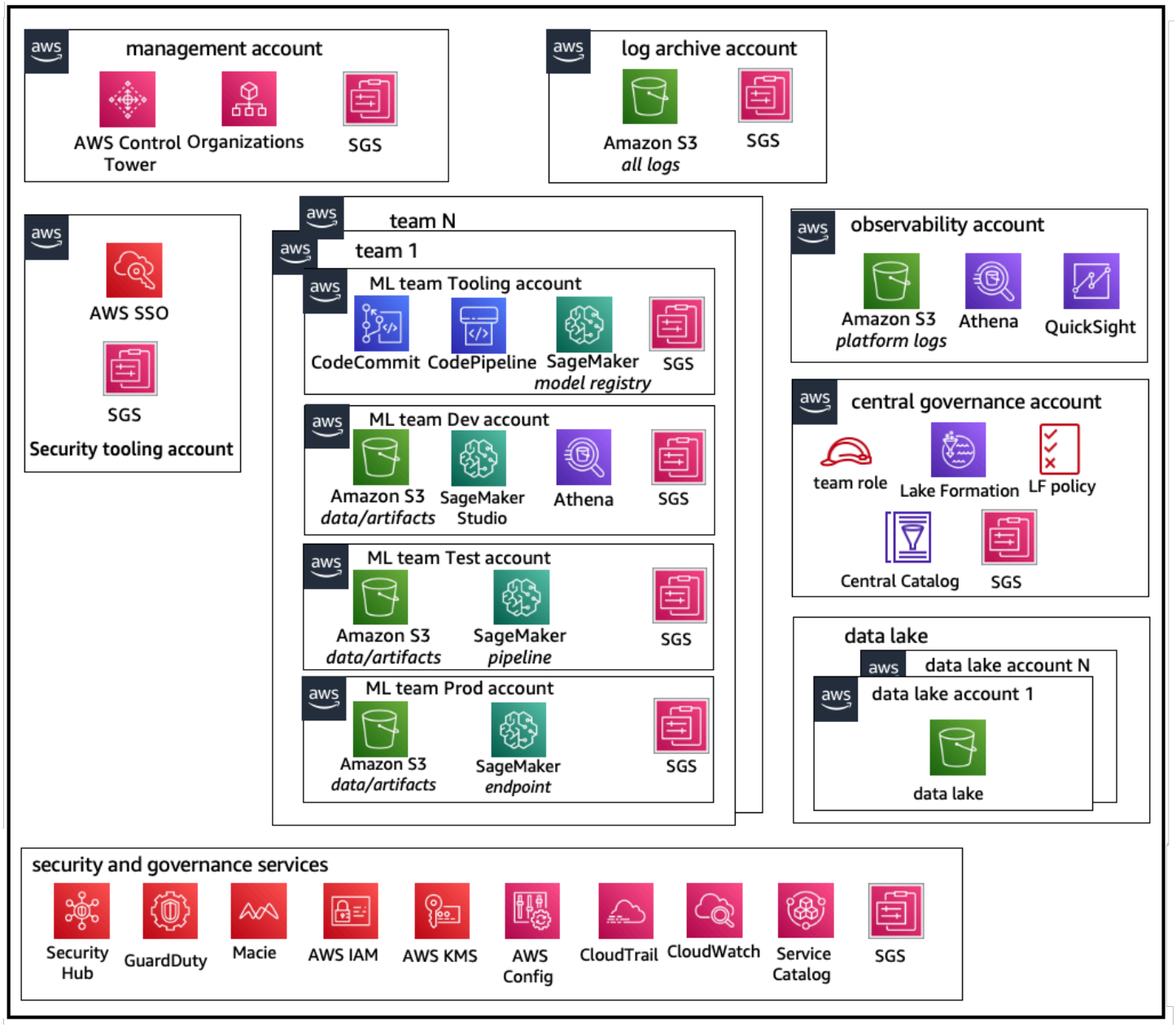
- 一個共用服務工具帳戶，可滿足資料科學團隊間的 Machine Learning 作業 (MLOP) 需求。
- 在資料科學團隊之間共用的 ML 工作負載開發、測試和生產帳戶。
- 控管原則可確保每個資料科學團隊工作負載獨立執行。
- 常見的最佳做法。



集中營運模式帳戶結構

分散式模型帳戶結構

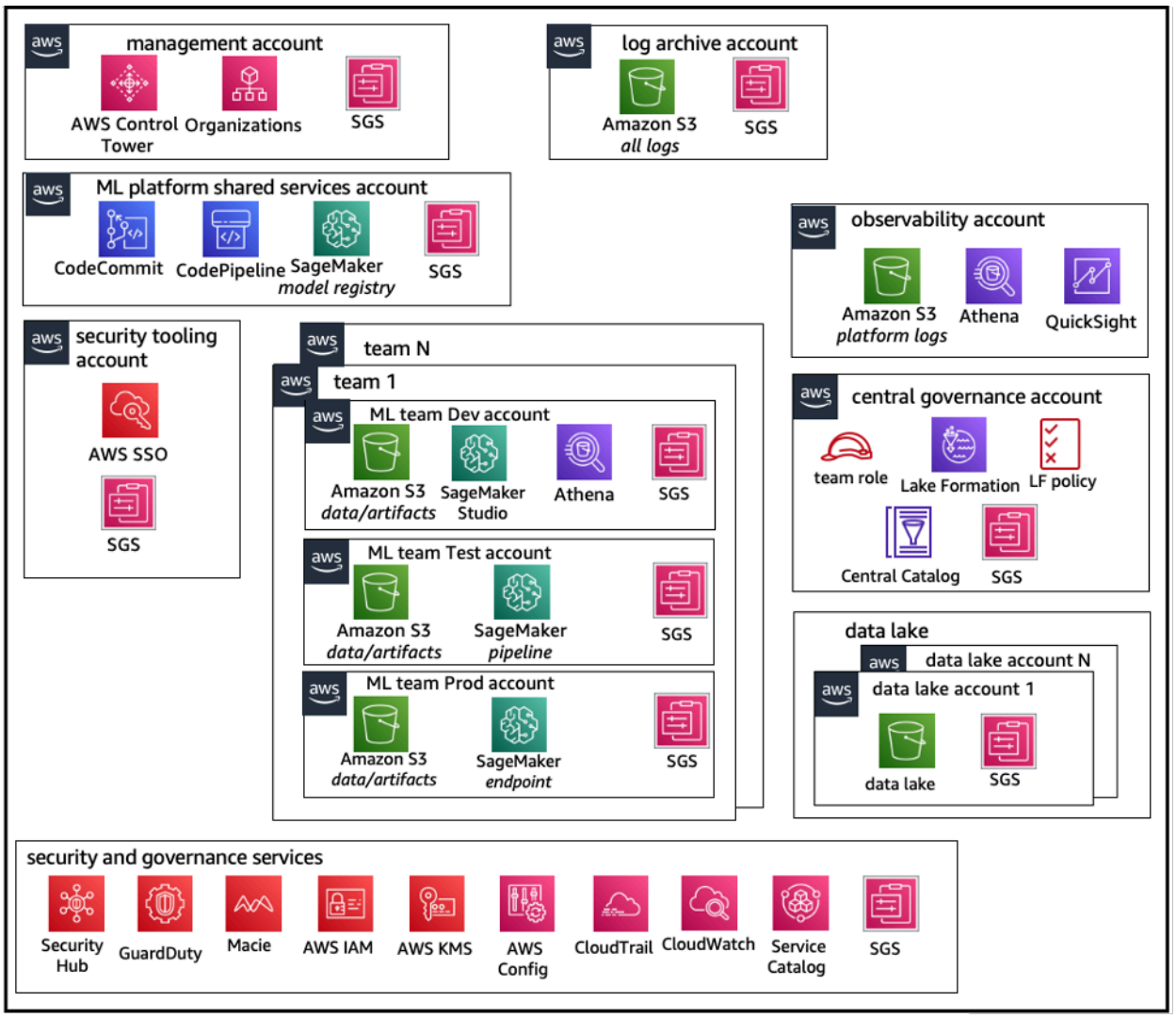
在此模型中，每個 ML 團隊會獨立運作，以供佈建、管理和管理 ML 帳戶和資源。不過，我們建議機器學習團隊使用集中的可觀察性和資料控管模型方法來簡化資料控管和稽核管理。



去中心化的操作模式賬戶

聯合模型帳戶結構

此模型類似於集中式模型；不過，主要差異在於，每個資料科學/ML 團隊都有自己的開發/測試/生產工作負載帳戶，以實現穩固的實體隔離機器學習資源，並讓每個團隊能夠獨立擴充，而不會影響其他團隊。



聯合作業模型帳戶結構

ML 平台多租戶

多租戶是一種軟體架構，單一軟體執行個體可以為多個不同的使用者群組提供服務。承租人是一組使用者，他們擁有軟體執行個體的特定權限共用一般存取權。例如，如果您要建立數個 ML 產品，則具有類似存取需求的每個產品團隊都可以視為租用戶或團隊。

雖然可以在 SageMaker Studio 執行個體 (例如SageMaker網域) 中實作多個團隊，但是當您將多個團隊納入單 SageMaker 一 Studio 網域時，可以權衡這些優勢，例如爆炸半徑、成本歸因和帳戶層級限制。請參閱以下章節，進一步瞭解這些權衡和最佳做法。

如果您需要絕對的資源隔離，請考慮為不同帳戶中的每個租用戶實 SageMaker 作 Studio 網域。視您的隔離需求而定，您可以在單一帳戶和區域內將多個企業營運單位 (LOB) 實作為多個網域。使用共用空間，在相同團隊 /LOB 的成員之間進行近乎即時的協同作業。對於多個網域，您仍然可以使用身分存取管理 (IAM) 政策和許可來確保資源隔離。

SageMaker 從網域建立的資源會自動標記為網域 Amazon 資源名稱 (ARN) 和使用者設定檔或空間 ARN，以便輕鬆隔離資源。如需原則範例，請參閱網域資源隔離說明文件。您可以在此處查看何時使用多帳戶或多網域策略的詳細參考資料，以及說明文件中的功能比較，您也可以檢視範例指令碼來回填儲存庫上現有網域的標記。GitHub

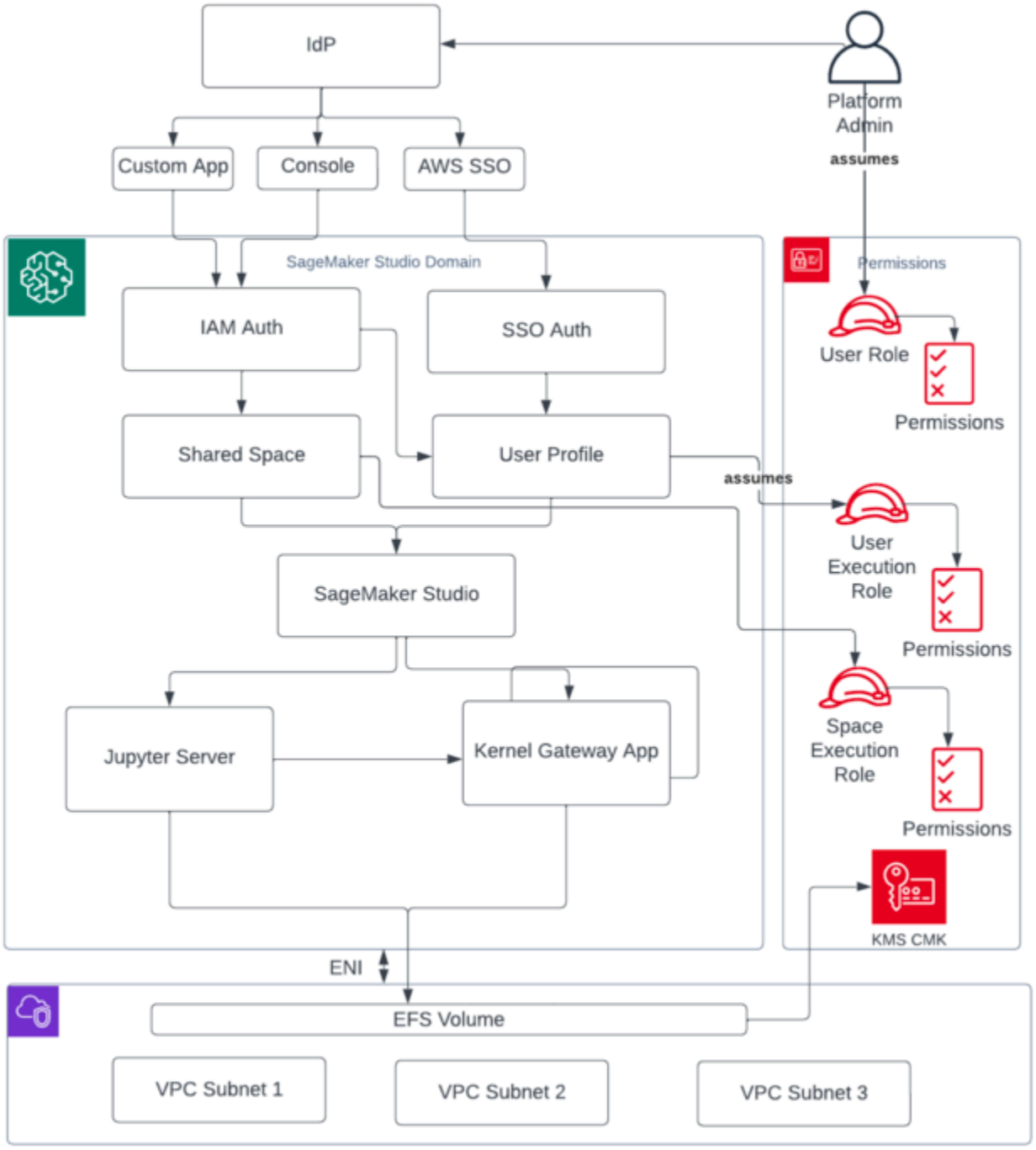
最後，您可以使用將 SageMaker Studio 資源的自助服務部署到多個帳戶中AWS Service Catalog。如需詳細資訊，請參閱在多個AWS 帳戶和中管理AWS Service Catalog產品AWS 區域。

網域管理

亞馬遜 SageMaker 域名包括：

- 關聯的 Amazon Elastic File System (Amazon EFS) 磁碟區
- 授權使用者清單
- 各種安全性、應用程式、政策和 Amazon Virtual Private Cloud (Amazon VPC) 組態

下圖提供構成 SageMakerStudio 網域之各種元件的高階檢視：

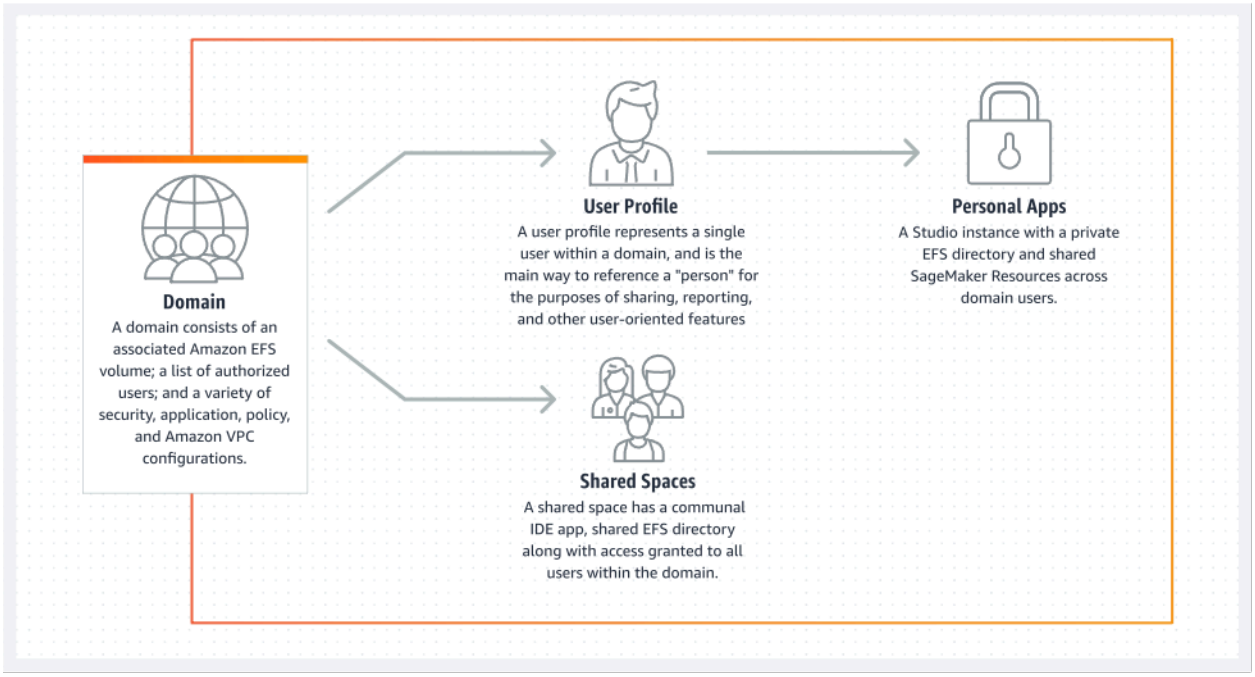


構成 SageMaker Studio 域的各種組件的高級視圖

多個網域和共用空間

Amazon SageMaker 現在支持為每個帳戶在一個單AWS 區域一的創建多個 SageMaker 域。每個網域都可以有自己的網域設定，例如驗證模式和網路設定，例如 VPC 和子網路。使用者設定檔無法跨網域共用。如果人類使用者是由網域分隔的多個團隊的一員，請為每個網域中的使用者建立使用者設定檔。請參閱多重網域概觀以瞭解現有網域的回填標籤。

在 IAM 身份驗證模式下設定的每個網域都可以利用共用空間，在使用者之間進行近乎即時的協作。透過共用空間，使用者可以存取共用的 Amazon EFS 目錄和使用者介面的共用JupyterServer應用程式，並且可以近乎即時地共同編輯。自動標記共用空間所建立的資源，可讓管理員追蹤專案層級的成本。共用 JupyterServer UI 也會篩選實驗和模型登錄項目等資源，以便只顯示與共用 ML 努力相關的項目。下圖提供每個網域內私人應用程式和共用空間的概觀。



單一網域內的私人應用程式和共用空間概觀

在您的網域中設定共用空間

共用空間通常是為特定的 ML 工作或專案建立，其中單一網域的成員需要近乎即時地存取相同的基礎檔案儲存空間和 IDE。使用者可以近乎即時地存取、讀取、編輯和共用筆記本，讓他們能以最快速的方式開始與同儕進行迭代作業。

若要建立共用空間，您必須先指定空間預設執行角色，以管理任何使用空間的使用者的權限。撰寫本文時，網域內的所有使用者都可以存取其網域中的所有共用空間。如需將共用空間新增至現有網域的最新文件，請參閱建立共用空間。

為 IAM 聯盟設定您的網域

在為您的 SageMaker Studio 網域設定 AWS Identity and Access Management (IAM) 聯合之前，您需要在 IdP 中設定 IAM 聯合使用者角色 (例如平台管理員)，如身分管理一節所述。

如需使用 IAM 選項設定 SageMaker Studio 的詳細說明，請參閱使用 IAM 身分識別中心板載到 Amazon SageMaker 網域。

設定您的網域以進行單一登入 (SSO) 聯盟

若要使用單一登入 (SSO) 聯盟，您必須AWS IAM Identity Center在您需要執行 SageMaker Studio 的相同區域中啟用AWS Organizations管理帳戶。網域設定步驟與 IAM 聯合步驟類似，不同之處在於您在「驗證」區段中選取 AWS IAM Identity Center(IdC)。

如需詳細指示，請參閱使用 IAM 身分識別中心板載到 Amazon SageMaker 網域。

SageMaker 工作室用戶配置

使用者設定檔代表網域中的單一使用者，也是為了共用、報告和其他使用者導向功能而引用「人員」的主要方式。當使用者登上 toSageMaker 工作室時，會建立此實體。如果管理員透過電子郵件邀請某人或從 IdC 匯入他們，則會自動建立使用者設定檔。使用者設定檔是個別使用者設定的主要持有者，並參考使用者的私有 Amazon Elastic File System (Amazon EFS) 主目錄。我們建議您為 SageMaker Studio 應用程式的每個實體使用者建立使用者設定檔。每個使用者在 Amazon EFS 上都有自己的專用目錄，而且使用者設定檔無法在同一帳戶的網域之間共用。

共用 SageMaker Studio 網域的每個使用者設定檔都會取得專用的運算資源 (例如 SageMaker Amazon 彈性運算雲端 (Amazon EC2) 執行個體) 以執行筆記本。分配給使用者 1 的運算執行個體與分配給使用者二的運算執行個體完全隔離。同樣地，配置給某個帳戶中使用者的計算資源，與配置給另一個AWS帳戶中使用者的運算資源完全不同。每個使用者最多可以在獨立的 Docker 容器中執行四個應用程式 (應用程式)，或在相同執行個體類型上執行映像檔。

木偶服務器應用程序

當您透過存取預先簽署的 URL 或使用 AWS IAM IDC 登入來為使用者啟動 Amazon SageMaker Studio 筆記本時，Jupyter 伺服器應用程式會在服務管理的 VPC 執行個體中 SageMaker 啟動。每個用戶都可以在私人應用程序中獲得自己的專用 Jupyter Server 應用程序。根據預設， SageMaker Studio 筆記本的 Jupyter Server 應用程式會在專用執行個`ml.t3.medium`體上執行 (保留為系統執行個體類型)。此執行個體的運算不會向客戶收費。

Jupyter 內核網關應用程序

核心閘道應用程式可透過 API 或 SageMaker Studio 介面建立，並在選擇的執行個體類型上執行。這個應用程式可以使用預先配置了流行的資料科學的內建 SageMaker Studio 映像之一，以及深度學習套件 (例如 TensorFlowApache MXNet 和. PyTorch

用戶可以在同一個 SageMaker Studio 映像/內核網關應用程序中啟動和運行多個 Jupyter 筆記本內核，終端會話和交互式控制台。使用者也可以在相同的實體執行個體上執行最多四個 Kernel Gateway 應用程式或映像檔，每個應用程式或映像都會隔離。

若要建立其他應用程式，您必須使用不同的執行個體類型。一個使用者設定檔只能執行一個執行個體，任何執行個體類型。例如，使用者可以在同一個執行個體上同時執行使用 SageMaker Studio 內建資料科學映像檔的簡單筆記本，以及使用內建 TensorFlow 映像檔的另一個筆記本。使用者需依執行個體執行的時間向使用者收費。若要在使用者未主動執行 SageMaker Studio 時避免成本，使用者必須關閉執行個體。如需詳細資訊，請參閱關閉並更新 Studio 應用程式。

每次從 SageMaker Studio 界面關閉並重新打開內核網關應用程序時，該應用程序都會在新實例上啟動。這表示套件的安裝不會透過重新啟動相同應用程式而持續存在。同樣地，如果使用者變更筆記本上的執行個體類型，其已安裝的套件和工作階段變數也會遺失。不過，您可以使用自己的映像檔和生命週期指令碼等功能，將使用者自己的套件帶到 SageMaker Studio，並透過執行個體切換和新執行個體啟動來保留它們。

Amazon Elastic File System 卷

建立網域時，會建立單一 Amazon Elastic File System (Amazon EFS) 磁碟區，供網域內的所有使用者使用。每個使用者設定檔都會收到 Amazon EFS 磁碟區內的私人主目錄，用於存放使用者的筆記本、儲存 GitHub 庫和資料檔案。網域內的每個空間都會收到 Amazon EFS 磁碟區內的私人目錄，可由多個使用者設定檔存取。用戶通過文件系統權限隔離對文件夾的訪問。 SageMaker Studio 會為每個使

用者設定檔或空間建立全域唯一使用者 ID，並將其套用為 EFS 上使用者主目錄的可攜式作業系統介面 (POSIX) 使用者/群組 ID，以防止其他使用者/空間存取其資料。

備份與復原

現有的 EFS 磁碟區無法附加至新 SageMaker 網域。在生產設定中，請確定已備份 Amazon EFS 磁碟區 (到另一個 EFS 磁碟區或亞馬遜簡單儲存服務 (Amazon S3))。如果意外刪除 EFS 磁碟區，系統管理員必須拆除並重新建立 SageMaker Studio 網域。程序如下：

透過、、和 `DescribeSpace` API 呼叫備份使用者設定檔、空間和關聯的 EFS 使用者 ID (UID) 清單。`ListUserProfiles` `DescribeUserProfile` `List Spaces`

1. 建立新的 SageMaker 工作室網域。
2. 建立使用者設定檔和空間。
3. 對於每個使用者設定檔，請從 EFS/Amazon S3 上的備份複製檔案。
4. 或者，刪除舊 SageMaker Studio 域上的所有應用程序和用戶配置文件。

如需詳細指示，請參閱附錄一節 SageMaker Studio 網域備份與復原。

> **Note**
>
> 這也可以通過`LifecycleConfigurations`在每次用戶啟動其應用程序時將數據備份到 S3 和從 S3 備份數據來實現。

Amazon EBS 磁碟區

Amazon 彈性區塊存放區 (Amazon EBS) 儲存磁碟區也會附加至每個 SageMaker Studio 筆記型電腦執行個體。它用作容器的根磁碟區或執行個體上執行的映像檔。雖然 Amazon EFS 儲存是持久性的，但連接到容器的 Amazon EBS 磁碟區是暫時的。如果客戶刪除應用程式，儲存在 Amazon EBS 磁碟區的本機資料將不會保留。

保護對預先簽署 URL 的存取

當 SageMaker Studio 使用者開啟筆記本連結時， SageMakerStudio 會驗證聯合身分識別使用者的 IAM 政策以授權存取權，並為使用者產生和解析預先簽署的 URL。由於 SageMaker 主控台在網際網路

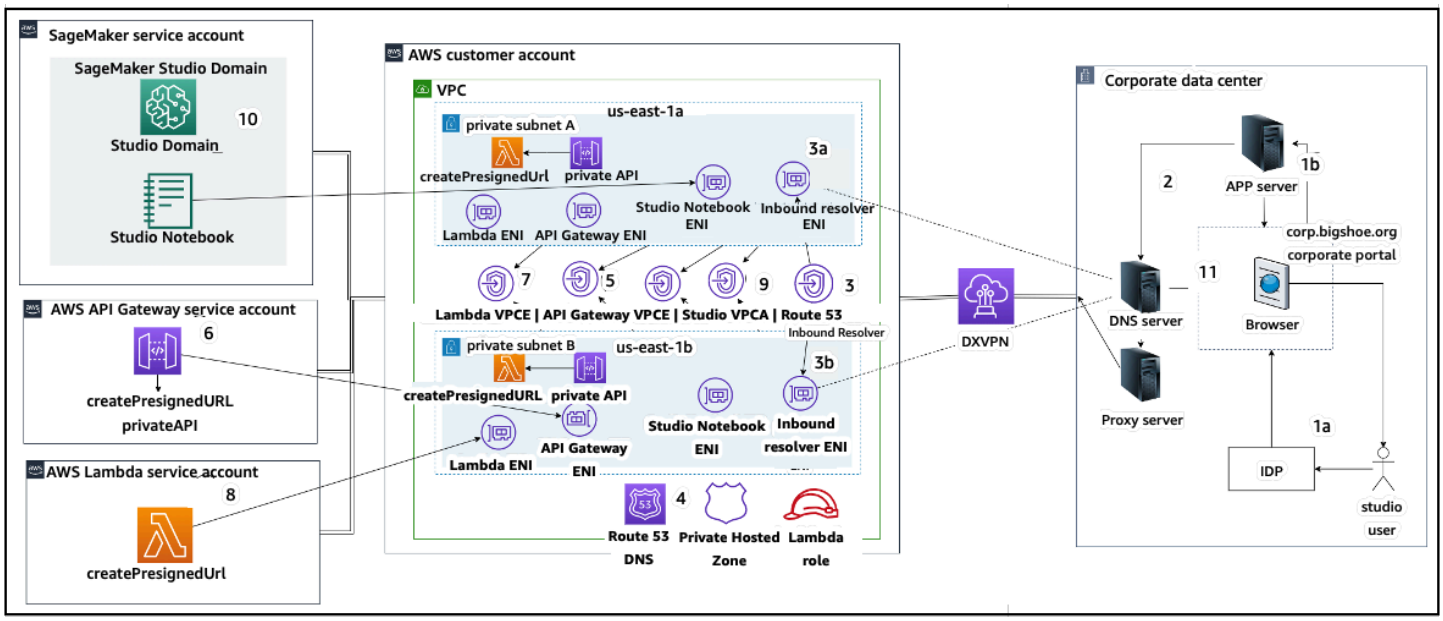
網域上執行，因此在瀏覽器工作階段中會顯示此產生的預先簽署 URL。這提出了一種不受歡迎的威脅媒介，用於資料竊取，並在未強制執行適當的存取控制時取得客戶資料的存取權。

Studio 支援幾種方法來強制執行存取控制，以防止預先簽署的 URL 資料竊取：

- 使用 IAM 政策條件進行用戶端 IP 驗證 `aws:sourceIp`
- 使用 IAM 條件進行用戶端 VPC 驗證 `aws:sourceVpc`
- 使用 IAM 政策條件進行用戶端 VPC 端點驗證 `aws:sourceVpce`

當您從 SageMaker主控台存取 SageMaker Studio 筆記本時，唯一可用的選項是搭配 IAM 政策條件使用用戶端 IP 驗證`aws:sourceIp`。但是，您可以使用瀏覽器流量路由產品（例如 Zscaler）來確保您的員工互聯網訪問的規模和合規性。這些流量路由產品會產生自己的來源 IP，其 IP 範圍不受企業客戶控制。這使得這些企業客戶無法使用該`aws:sourceIp`條件。

若要使用 IAM 政策條件使用用戶端 VPC 端點驗證`aws:sourceVpce`，建立預先簽署的 URL 必須源自部署 SageMaker Studio 的相同客戶 VPC，而且需要透過客戶 VPC 上的 SageMaker Studio VPC 端點解析預先簽署的 URL。企業網路使用者在存取期間對預先簽署的 URL 解析可以使用 DNS 轉送規則 (在 Zscaler 和企業 DNS 中) 完成，然後使用 Amazon Route 53 輸入解析程式進入客戶 VPC 端點，如下列架構所示：



透過企業網路使用虛擬私人雲端端點存取 Studio 預先簽署的 URL

如需設定先前架構的 step-by-step 指引，請參閱安全 Amazon SageMaker Studio 預先簽署的 URL 第 1 部分：基礎基礎設施。

SageMaker 網域配額和限制

- SageMaker Studio 網域 SSO 聯盟僅在該區域支援，跨佈建AWS身分識別中心的AWS組織成員帳戶。
- 使用AWS身分識別中心設定的網域目前不支援共用空間。
- 建立網域後，無法變更 VPC 和子網路組態。但是，您可以使用不同的 VPC 和子網路組態建立新網域。
- 建立網域後，無法在 IAM 和 SSO 模式之間切換網域存取。您可以使用不同的驗證模式建立新網域。
- 針對每位使用者啟動的每個執行個體類型，最多只能有四個核心閘道應用程式。
- 每個使用者只能啟動每個執行個體類型的一個執行個體。
- 網域內使用的資源有限制，例如依執行個體類型啟動的執行個體數量，以及可建立的使用者設定檔數目。如需完整的服務限制清單，請參閱服務配額頁面。
- 客戶可以提交具有商業理由的企業支援案例，以提高預設資源限制，例如網域數量或使用者設定檔，受到帳戶層級護衛的影響。
- 每個帳戶的並發應用程序數量的硬性限制為 2,500 個應用程序。網域和使用者設定檔限制取決於這個硬性限制。例如，一個帳戶可以有一個包含 1,000 個使用者設定檔的單一網域，或 20 個網域，每個使用者設定檔 50 個。

身分管理

本節討論公司目錄中的員工使用者如何聯合 AWS 帳戶 和存取 SageMaker Studio。首先，我們將簡要說明如何對應使用者、群組和角色，以及使用者同盟的運作方式。

使用者、群組和角色

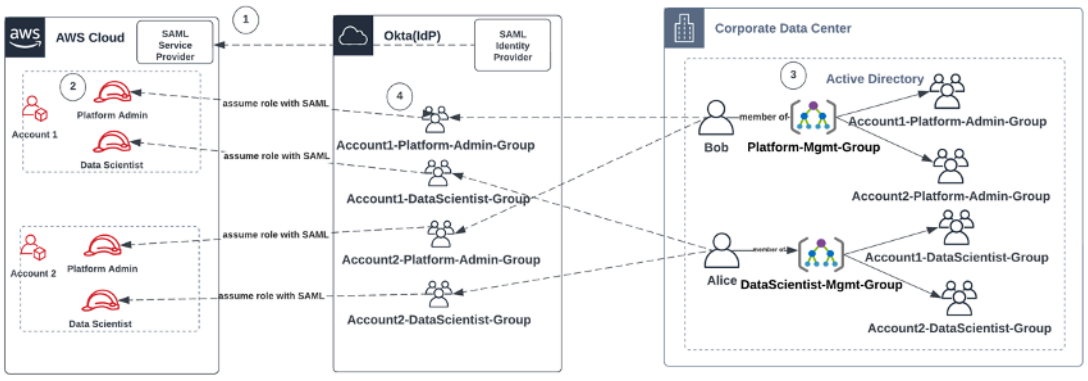
在中 AWS，可以使用使用者、群組和角色來管理資源權限。客戶可以透過 IAM 或透過外部 IdP (例如 Okta) 啟用的公司目錄 (例如 Active Directory (AD) 管理其使用者和群組，以驗證雲端和內部部署中執行的各種應用程式的使用者。

如「 AWS 安全性支柱身分識別管理」一節所討論的，在中央 IdP 中管理使用者身分識別是最佳實務，因為這有助於輕鬆地與後端人力資源流程整合，並有助於管理員工使用者的存取。

IdPs 例如 Okta 允許使用者對一或多個進行驗證，AWS 帳戶 並使用具有安全性判斷提示標記語言 (SAML) 的 SSO 來存取特定角色。IdP 管理員能夠將角色下載到 IdP 中，並 AWS 帳戶 將這些角色指派給使用者。登入時 AWS，會看到一個 AWS 畫面，其中顯示一個或多個指派給他們的清單 AWS 角色 AWS 帳戶。他們可以選取要承擔登入的角色，該角色會定義其在該已驗證工作階段期間的權限。

您要提供存取權的每個特定帳戶和角色組合，IdP 中必須存在群組。您可以將這些群組視為AWS 角色特定群組。屬於這些角色特定群組成員的任何使用者都會獲得單一權利：存取某個特定角色中的一個特定角色 AWS 帳戶。但是，此單一權利程序不會透過將每位使用者指派給特定 AWS 角色群組來擴展以管理使用者存取。為了簡化管理，我們建議您也為組織中需要不同 AWS 權利組的所有不同使用者集建立數個群組。

若要說明中央 IdP 設定，請考慮具有 AD 設定的企業，其中使用者和群組會同步至 IdP 目錄。在中 AWS，這些 AD 群組會對應至 IAM 角色。工作流程的主要步驟如下：



上線 AD 使用者、AD 群組和 IAM 角色的工作流程

1. 在中 AWS，為您 AWS 帳戶 的每個 IdP 設定 SAML 整合。
2. 在中 AWS，在每個角色中設定角色 AWS 帳戶 並同步至 IdP。
3. 在公司 AD 系統中：
   a. 為每個帳戶角色建立 AD 群組，並同步至 IdP (例如 `Account1-Platform-Admin-Group` (又稱 AWS 角色群組))。
   b. 在每個角色層級 (例如，`Platform-Mgmt-Group`) 建立管理群組，並將 AWS 角色群組指派為成員。
   c. 將使用者指派給該管理群組，以允許存取 AWS 帳戶 角色。
4. 在 IdP 中，將 AWS 角色群組 (例如`Account1-Platform-Admin-Group`) 對應至 AWS 帳戶 角色 (例如，帳戶 1 中的平台管理員)。
5. 當資料科學家 Alice 登入 Idp 時，他們會看到 AWS 聯合應用程式使用者介面，其中有兩個選項可供選擇：「帳戶 1 資料科學家」和「帳戶 2 資料科學家」。
6. 愛麗絲選擇「帳戶 1 數據科學家」選項，並將其連接到 AWS 帳戶 1（ SageMaker 控制台）中的授權應用程序。

如需設定 SAML 帳戶聯合的詳細指示，請參閱 Okta 的如何為 AWS 聯合帳戶設定 SAML 2.0。

使用者同盟

SageMaker 工作室的身份驗證可以使用 IAM 或 IAM IDC 來完成。如果使用者透過 IAM 進行管理，則可以選擇 IAM 模式。如果企業使用外部 IdP，則可以透過 IAM 或 IAM IdC 進行聯合。請注意，無法針對現有 SageMaker Studio 網域更新驗證模式，因此在建立生產 SageMaker Studio 網域之前做出決定是非常重要的。

如果 SageMaker Studio 是以 IAM 模式設定，則 SageMaker Studio 使用者會透過預先簽署的 URL 存取應用程式，當使用者透過瀏覽器存取 Studio 應用程式時，該 URL 會自動將使用者登入 SageMaker Studio 應用程式。

IAM 使用者

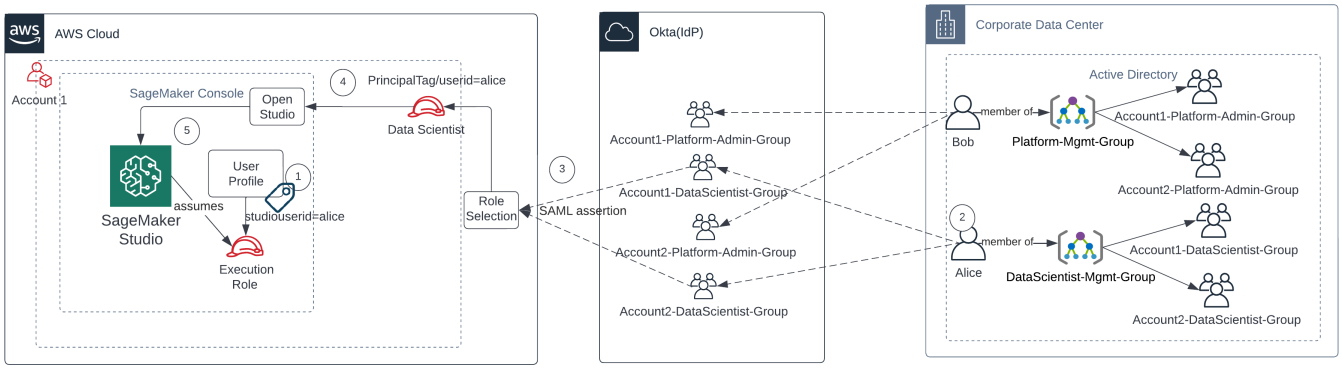
對於 IAM 使用者，管理員會為每個使用者建立 SageMaker Studio 使用者設定檔，並將使用者設定檔與 IAM 角色建立關聯，該角色允許使用者需要在 Studio 中執行必要的動作。若要限制 AWS 使用者僅

存取其 SageMaker Studio 使用者設定檔，管理員應標記 SageMaker Studio 使用者設定檔，並將 IAM 政策附加至使用者，讓他們只有在標籤值與 AWS 使用者名稱相同時才能存取。政策聲明如下所示：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonSageMakerPresignedUrlPolicy",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreatePresignedDomainUrl"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "sagemaker:ResourceTag/studiouserid": "${aws:username}"
                }
            }
        }
    ]
}
```

AWS IAM 或帳戶同盟

同 AWS 帳戶 盟方法可讓客戶從其 SAML IdP (例如 Okta) 聯合到 SageMaker 主控台。若要限制使用者僅存取其使用者設定檔，系統管理員應標記 SageMaker Studio 使用者設定檔、在 IdP `PrincipalTags` 上新增，並將其設定為傳遞標籤。下圖說明聯合使用者 (資料科學家愛麗絲) 如何獲得授權存取自己的 SageMaker Studio 使用者設定檔。



以 IAM 聯合模 SageMaker 式存取工作室

1. 愛麗絲 SageMaker 工作室用戶配置文件被標記為其用戶 ID，並與執行角色相關聯。
2. 愛麗絲認證 IdP（奧克塔）。
3. IdP 會驗證愛麗絲，並以兩個角色（帳戶 1 和 2 的資料科學家）張貼 SAML 斷言。愛麗絲為帳戶 1 選擇資料科學家角色。
4. Alice 以資料科學家的假定角色登入帳號 1 SageMaker 主控台。愛麗絲從工作室應用程序實例列表中打開他們的 Studio 應用程序實例。
5. 假設角色工作階段中的 Alice 主要標籤會根據選取的 SageMaker Studio 應用程式執行個體使用者設定檔標記驗證。如果配置文件標記有效，則會啟動 SageMaker Studio 應用程序實例，假定執行角色。

如果您想要在使用者加入過程中自動建立 Ex SageMaker ecution 角色和原則，以下是完成此操作的一種方法：

1. 設置一個 AD 組，例如`SageMaker-Account1-Group`在每個帳戶和 Studio 域級別。
2. 當您需要將使用者加入 Studio 時，將 SageMaker-Account1-群組新增至使用者的群組成員資格。SageMaker

設定偵聽成員資格事件的自動化程序，並根據其 AD 群組成`SageMaker-Account1-Group`員資格，使用 AWS API 建立角色、原則、標記和 SageMaker Studio 使用者設定檔。將角色附加至使用者設定檔。如需原則範例，請參閱防止 SageMaker Studio 用戶訪問其他用戶配置文件。

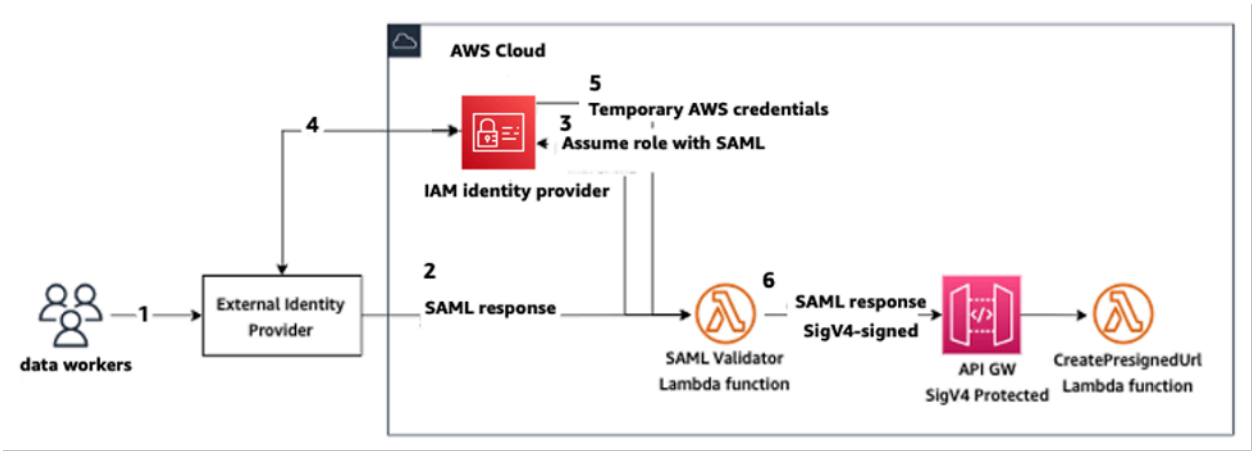
使用 SAML 驗證 AWS Lambda

在 IAM 模式中，使用者也可以使用 SAML 判斷提示在 SageMaker Studio 中進行驗證。在此架構中，客戶擁有現有的 IdP，他們可以在其中建立 SAML 應用程式供使用者存取 Studio (而不是 AWS 身分聯合應用程式)。客戶的 IdP 即會新增至 IAM。 AWS Lambda 函數可協助使用 IAM 和 STS 驗證 SAML 宣告，然後直接叫用 API 閘道或 Lambda 函數，以建立預先簽署的網域 URL。

此解決方案的優點是 Lambda 函數可以自訂邏輯以存取 SageMaker Studio。例如：

- 如果沒有使用者設定檔，則自動建立使用者設定檔。
- 透過剖析 SAML 屬性，將角色或原則文件附加至 SageMaker Studio 執行角色或原則文件。
- 透過新增生命週期組態 (LCC) 並新增標籤來自訂使用者設定檔。

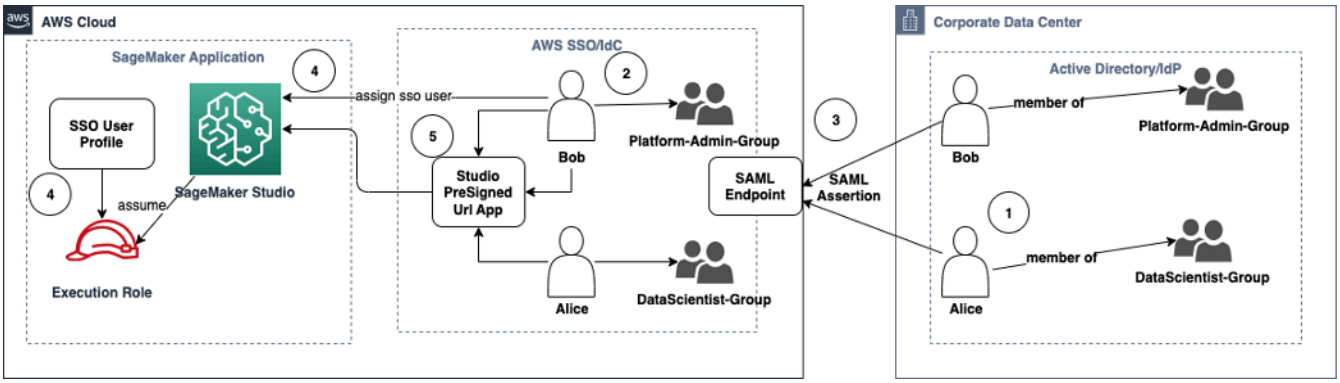
總之，此解決方案將公開 SageMaker Studio 作為 SAML2.0 應用程序，其中包含用於身份驗證和授權的自定義邏輯。如需實作詳細資訊，請參閱附錄一節使用 SAML 宣告的 SageMaker Studio 存取。



使用自訂 SAML 應用程 SageMaker 式存取工作室

AWS IAM IDC 聯合

IdC 聯合方法可讓客戶直接從其 SAML IdP (例如 Okta) 聯合到 SageMaker Studio 應用程式。下圖說明聯合身分使用者如何獲得授權存取自己的 SageMaker Studio 執行個體。



以 IAM IDC 模 SageMaker 式存取工作室

1. 在公司 AD 中，使用者是 AD 群組的成員，例如「平台管理員」群組和「資料科學家」群組。
2. 身分識別提供者 (IdP) 的 AD 使用者和 AD 群組會同步至 AWS IAM 身分中心，並分別以單一登入使用者和群組的形式提供給指派。
3. IdP 會將 SAML 宣告張貼至 AWS IdC SAML 端點。
4. 在 SageMaker 工作室中，IdC 用戶被分配給 SageMaker Studio 應用程序。此分配可以使用 IdC 組來完成，並且 SageMaker Studio 將在每個 IdC 用戶級別應用。建立此指派時， SageMaker Studio 會建立 IdC 使用者設定檔，並附加網域執行角色。

5. 使用者使用從 IdC 作為雲端應用程式託管的安全預先簽署 URL 存取 SageMaker Studio 應用程式。SageMaker Studio 假定附加到其 IdC 用戶配置文件的執行角色。

網域驗證指引

以下是選擇網域驗證模式時的一些注意事項：

1. 如果您希望使用者不要直接存取 AWS Management Console 和檢視 SageMaker Studio UI，請搭配 AWS IAM IDC 使用單一登入模式。
2. 如果您希望使用者不能直接在 IAM 模式下存取 AWS Management Console 和檢視 SageMaker Studio UI，可以使用後端中的 Lambda 函數為使用者設定檔產生預先簽署的 URL，並將其重新導向至 SageMaker Studio UI。
3. 在 IdC 模式下，每個使用者都會對應至單一使用者設定檔。
4. 所有使用者設定檔都會在 IdC 模式下自動指派預設執行角色。如果您希望為使用者指派不同的執行角色，則需要使用 UpdateUserProfileAPI 更新使用者設定檔。
5. 如果您想要在 IAM 模式下 (使用產生的預先簽署 URL) 限制 SageMaker Studio UI 存取至 VPC 端點，而不要遍歷網際網路，您可以使用自訂 DNS 解析程式。請參閱 Amazon SageMaker Studio 預先簽署的安全網址第 1 部分：基礎設施部落格文章。

許可管理

本節討論設定用於佈建和操作 SageMaker Studio 網域的常用 IAM 角色、政策和護欄的最佳實務。

(IAM) 角色和政策

最佳作法是，您可能會想要先識別相關人員和應用程式 (稱為 ML 生命週期中涉及的主參與者)，以及您需要授與他們的AWS權限。與受管理服務一樣，您也需要考慮服務主體，這些服AWS務主體 SageMaker 是可以代表使用者進行 API 呼叫的服務。下圖說明您可能要建立的不同 IAM 角色，對應於組織中的不同角色。

SageMaker IAM 角色

這些角色將詳細描述，以及一些他們將需要的特定 IAMPerications 範例。

- ML Admin 使用者角色 — 這是為資料科學家佈建環境的主體，方法是建立 Studio 網域和使用者設定檔 (`sagemaker:CreateDomain`,`sagemaker:CreateUserProfile`)、為使用者建立 AWS Key Management Service (AWS KMS) 金鑰、為資料科學家建立 S3 儲存貯體，以及建立 Amazon ECR 儲存庫來容納容器。他們還可以為使用者設定預設組態和生命週期指令碼、建立自訂映像並將其附加到 SageMaker Studio 網域，以及提供 Service Catalog 產品，例如自訂專案、Amazon EMR 範本。

  例如，由於此主參與者不會執行訓練工作，因此不需要啟動 SageMaker 訓練或處理工作的權限。如果他們使用基礎結構作為代碼模板（例如 CloudFormation 或 Terraform）來佈建域和用戶，則佈建服務將假定此角色代表管理員創建資源。此角色可能具有 SageMaker 使用的唯讀存取權AWS Management Console。

  此使用者角色還需要特定的 EC2 許可才能在私有 VPC 內啟動網域、用於加密 EFS 磁碟區的 KMS 許可，以及為 Studio (`iam:CreateServiceLinkedRole`) 建立服務連結角色的許可。我們將在文件稍後說明這些細微的權限。
- 資料科學家使用者角色 — 此主體是登入 SageMaker Studio、探索資料、建立處理和訓練工作和管線等的使用者。使用者需要的主要權限是啟動 SageMaker Studio 的權限，其餘的原則可以由 SageMaker 執行服務角色來管理。

- SageMaker 執行服務角色 — 由於 SageMaker 是受管理的服務，因此它會代表使用者啟動工作。就允許的權限而言，此角色通常是最廣泛的角色，因為許多客戶選擇使用單一執行角色來執行訓練工作、處理工作或模型託管工作。雖然這是一種簡單的入門方式，但是因為客戶在旅程中成熟，但他們通常會將筆記本執行角色分成不同的角色，以執行不同的 API 動作，尤其是在部署的環境中執行這些工作時。

  您可以在建立時將角色與 SageMaker Studio 網域產生關聯。但是，由於客戶可能需要靈活地將不同角色與網域中的不同使用者設定檔相關聯 (例如，根據他們的工作職能)，因此您也可以將個別的 IAM 角色與每個使用者設定檔建立關聯。建議您將單一實體使用者對應至單一使用者設定檔。如果您在建立時未將角色附加至使用者設定檔，預設行為也會將 SageMakerStudio 網域執行角色與使用者設定檔建立關聯。

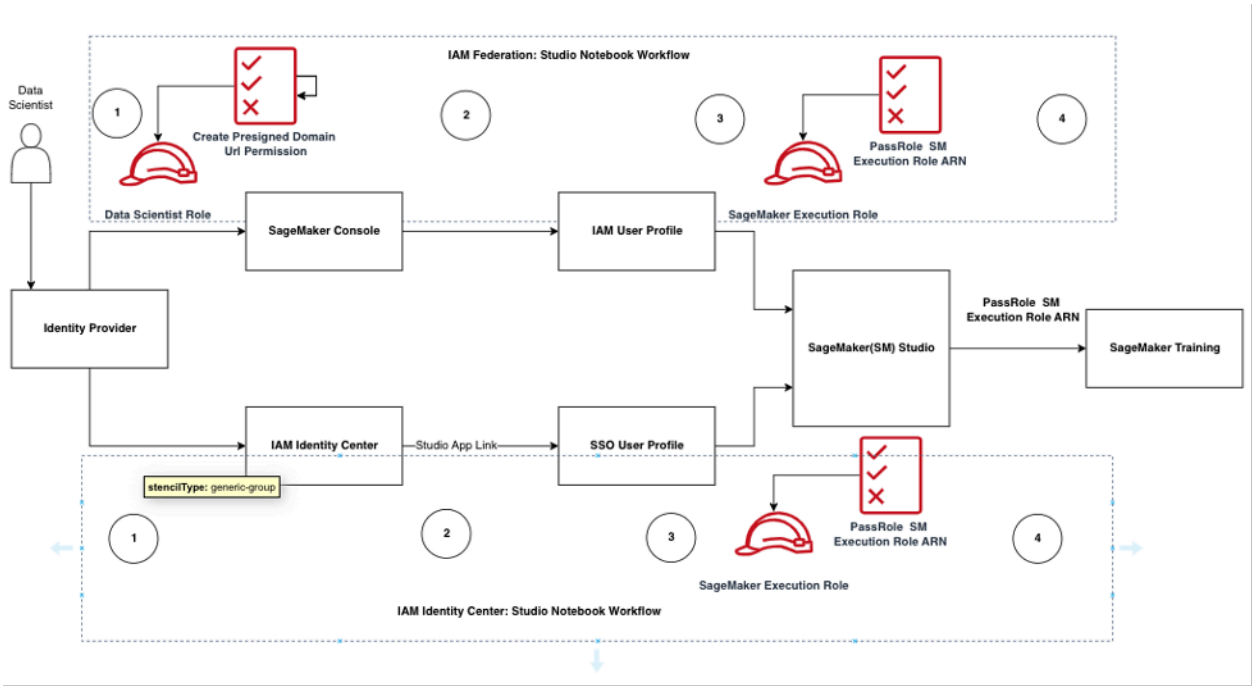
  如果有多位資料科學家和機器學習工程師在專案上共同合作，而且需要共用權限模型來存取資源，建議您建立小組層級的 SageMaker 服務執行角色，以便在團隊成員之間共用 IAM 許可。在需要在每個使用者層級鎖定權限的執行個體中，您可以建立個別的使用者層級 SageMaker 服務執行角色；不過，您必須注意您的服務限制。

SageMaker Studio 筆記本授權工作流

本節將討論 SageMaker Studio 筆記本授權如何處理資料科學家需要執行的各種活動，以便直接從 SageMaker Studio 筆記本建立和訓練模型。 SageMaker 網域支援兩種授權模式：

- IAM 聯合
- IAM Identity Center

接下來，本 paper 將引導您完成每種模式的資料科學家授權工作流程。



Studio 使用者的驗證和授權工作流程

IAM 同盟： SageMaker Studio 筆記本工作流程

1. 資料科學家會對其公司身分識別提供者進行驗證，並在主控台中擔任資料科學家使用者角色（使用者聯合角色）。 SageMaker此聯合角色具有 SageMaker 執行角色的 `iam:PassRole` API 權限，可將角色 Amazon 資源名稱 (ARN) 傳遞至 SageMaker Studio。
2. 資料科學家從與 SageMaker 執行角色相關聯的 Studio IAM 使用者設定檔中選取開放式工作室連結
3. 假設使用者設定檔的 SageMaker 執行角色權限，即會啟動 SageMaker Studio IDE 服務。此角色具有 SageMaker 執行角色的 `iam:PassRole` API 權限，可將角色 ARN 傳遞至 SageMaker 訓練服務。
4. 當資料科學家在遠端運算節點中啟動訓練工作時， SageMaker 執行角色 ARN 會傳遞至 SageMaker 訓練服務。這會使用此 ARN 建立新的角色工作階段，並執行訓練工作。如果您需要進一步縮減訓練工作的權限範圍，則可以建立訓練特定角色，並在呼叫訓練 API 時傳遞該角色 ARN。

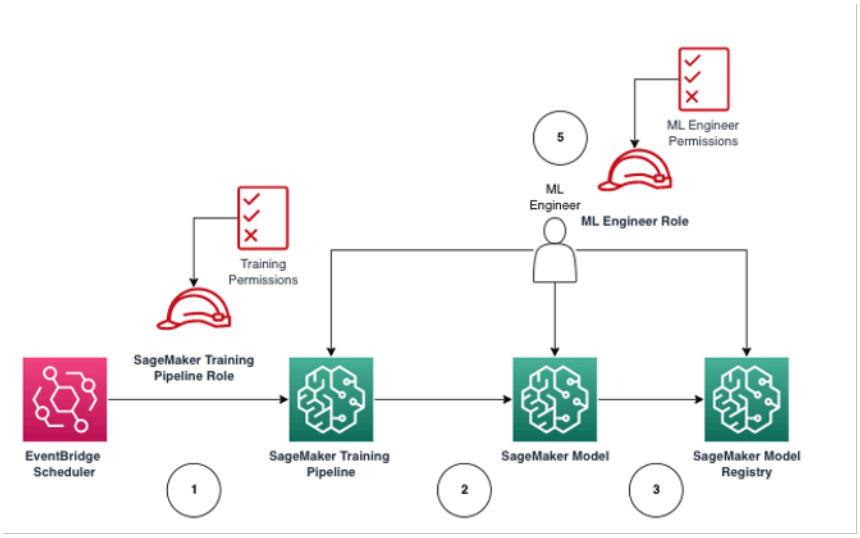
IAM 身分中心： SageMakerStudio 筆記本工作流程

1. 資料科學家會驗證其企業身分供應商，然後按一下 AWS IAM 身分中心。資料科學家會向使用者介紹身分中心入口網站。

2. 資料科學家按一下從與 SageMaker 執行角色相關聯的 IdC 使用者設定檔建立的 SageMaker Studio App 連結。
3. 假設使用者設定檔的 SageMaker 執行角色權限，即會啟動 SageMaker Studio IDE 服務。此角色具有 SageMaker 執行角色的 `iam:PassRole` API 權限，可將角色 ARN 傳遞至 SageMaker 訓練服務。
4. 當資料科學家在遠端運算節點中啟動訓練工作時， SageMaker 執行角色 ARN 會傳遞至 SageMaker 訓練服務。執行角色 ARN 會使用此 ARN 建立新的角色工作階段，並執行訓練工作。如果您需要進一步縮小訓練工作權限的範圍，您可以建立訓練特定角色，並在呼叫訓練 API 時傳遞該角色 ARN。

部署環境： SageMaker 訓練工作流程

在部署的環境中，例如系統測試和生產環境中，工作會透過自動化排程器和事件觸發程序執行，而 SageMaker Studio Notebook 限制對這些環境的人類存取。本節討論 IAM 角色如何與已部署環境中的 SageMaker 訓練管道搭配運作。



SageMaker 受管理生產環境中的訓練工作流程

1. Amazon EventBridge 排程器會觸發 SageMaker 訓練管道工作。
2. SageMaker 訓練管線工作擔任 SageMaker 訓練管道角色來訓練模型。
3. 訓練過的 SageMaker 模型會註冊到 SageMaker 模型登錄中。
4. ML 工程師擔任 ML 工程師使用者角色來管理訓練管線和 SageMaker 模型。

資料權限

SageMaker Studio 使用者存取任何資料來源的能力受其 SageMaker IAM 執行角色相關聯的許可控制。附加的政策可以授權他們從特定 Amazon S3 儲存貯體或首碼讀取、寫入或刪除，以及連接到 Amazon RDS 資料庫。

存取 AWS Lake Formation 資料

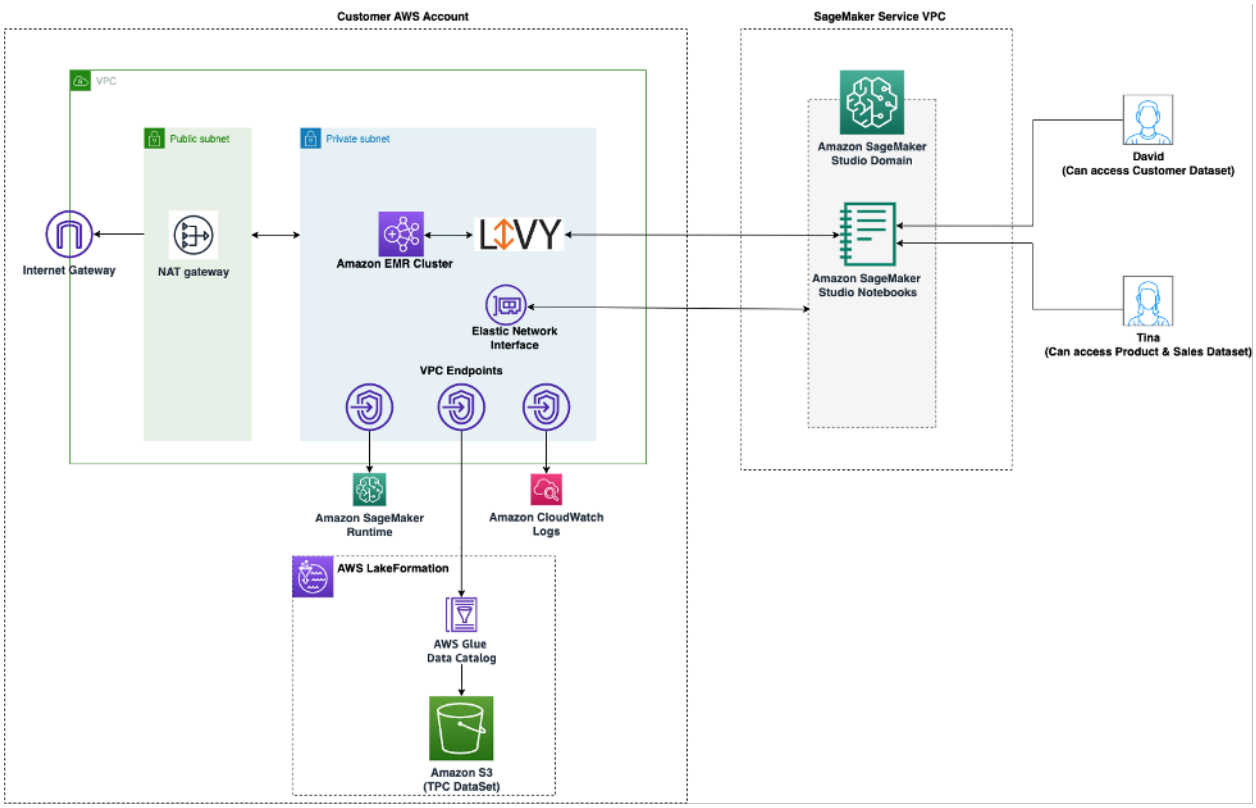
許多企業已開始使用受管理的資料湖，為其使用者提供精細的資料存取。AWS Lake Formation作為此類受控資料的範例，管理員可以遮罩部分使用者的敏感資料欄，同時仍可啟用相同基礎資料表的查詢。

若要利用 SageMaker Studio 的 Lake Formation，管理員可以將 SageMaker IAM 執行角色註冊為`DataLakePrincipals`. 有關更多信息，請參閱 Lake Formation 許可參考。一旦獲得授權，有三種主要方法可用於從 SageMaker Studio 訪問和寫入受管理的數據：

1. 使用者可以從 SageMaker Studio 筆記本使用查詢引擎 (例如 Amazon Athena) 或建立在 boto3 之上的程式庫，將資料直接提取到筆記本。熊貓適用的 AWS 開發套件 (以前稱為大熊貓) 是一個受歡迎的程式庫。以下是一個代碼示例，以顯示如何無縫這可以是：

```
transaction_id = wr.lakeformation.start_transaction(read_only=True)
df = wr.lakeformation.read_sql_query(
    sql=f"SELECT * FROM {table};",
    database=database,
    transaction_id=transaction_id
)
```

2. 使用 SageMaker Studio 原生連線至 Amazon EMR，大規模讀取和寫入資料。透過使用 Apache Livy 和 Amazon EMR 執行階段角色， SageMaker Studio 建立了原生連線功能，可讓您將 SageMaker 執行 IAM 角色 (或其他授權角色) 傳遞給 Amazon EMR 叢集以進行資料存取和處理。如需 up-to-date指示，請參閱從 Studio Connect 到亞馬遜 EMR 叢集。



從 SageMaker 工作室訪問由 Lake Formation 管理的數據的體系結構

3. 使用 SageMaker Studio 原生連線至AWS Glue互動式工作階段，大規模讀取和寫入資料。SageMaker Studio 筆記本具有內置內核，允許用戶以交互方式運行命令。AWS Glue如此可擴充使用 Python、Spark 或 Ray 後端，從受控管的資料來源大規模無縫讀取和寫入資料。內核允許用戶傳遞其 SageMaker 執行或其他授權的 IAM 角色。如需詳細資訊，請參閱使用AWS Glue互動工作階段準備資料。

普通護欄

本節討論使用 IAM 政策、資源政策、VPC 端點政策和服務控制政策 (SCP) 在 ML 資源上套用控管的最常用防護。

限制筆記本對特定實例的訪問

此服務控制原則可用來限制資料科學家可存取的執行個體類型，同時建立 Studio 筆記本。請注意，任何用戶都需要允許「系統」實例來創建託 SageMaker 管 Studio 的默認 Jupyter 服務器應用程序。

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

```
    "Statement": [
        {
            "Sid": "LimitInstanceTypesforNotebooks",
            "Effect": "Deny",
            "Action": [
                "sagemaker:CreateApp"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotLike": {
                    "sagemaker:InstanceTypes": [
                        "ml.c5.large",
                        "ml.m5.large",
                        "ml.t3.medium",
                        "system"
                    ]
                }
            }
        }
    ]
}
```

限制不符合規範的 SageMaker Studio 網域

對於 SageMaker Studio 網域，下列服務控制政策可用於強制流量以存取客戶資源，使其不會透過公用網際網路，而是透過客戶的 VPC：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {   "Sid": "LockDownStudioDomain",
            "Effect": "Deny",
            "Action": [
                "sagemaker:CreateDomain"
            ],
            "Resource": "*",
            "Condition": {
                        "StringNotEquals": {"sagemaker:AppNetworkAccessType":
"VpcOnly"
                },
                "Null": {
                        "sagemaker:VpcSubnets": "true",
                        "sagemaker:VpcSecurityGroupIds": "true"
```

```
                }
            }
        }
    ]
}
```

限制啟動未授權 SageMaker 影像

下列原則可防止使用者在其網域中啟動未經授權的 SageMaker 影像：f

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sagemaker:CreateApp"
             ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringNotLike": {
                    "sagemaker:ImageArns":
                        [
                        "arn:aws:sagemaker:*:*:image/{ImageName}"
                        ]
                }
            }
        }
    ]
}
```

僅透過 SageMaker VPC 端點啟動筆記型電腦

除了 SageMaker 控制平面的 VPC 端點之外，還 SageMaker 支援 VPC 端點，讓使用者連線至 SageMakerStudio 筆記型電腦或SageMaker筆記型電腦執行個體。如果您已經為 SageMaker 工作室/筆記本執行個體設定 VPC 端點，則下列 IAM 條件金鑰只會在透過 SageMaker Studio VPC 端點或 API 端點建立時，才允許連線至 SageMaker Studio 筆記本。 SageMaker

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

```
        {
            "Sid": "EnableSageMakerStudioAccessviaVPCEndpoint",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreatePresignedDomainUrl",
                "sagemaker:DescribeUserProfile"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:sourceVpce": [
                        "vpce-111bbccc",
                        "vpce-111bbddd"
                    ]
                }
            }
        }
    ]
}
```

將 SageMaker Studio 筆記型電腦存取限制在有限的 IP 範圍內

公司通常會將 SageMaker Studio 存取限制在特定允許的企業 IP 範圍內。下列具有SourceIP條件金鑰的 IAM 政策可能會限制此問題。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnableSageMakerStudioAccess",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreatePresignedDomainUrl",
                "sagemaker:DescribeUserProfile"
            ],
            "Resource": "*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": [
                        "192.0.2.0/24",
                        "203.0.113.0/24"
                    ]
                }
```

```
            }
        }
    ]
}
```

防止 SageMaker Studio 用戶訪問其他用戶配置文件

身為管理員，當您建立使用者設定檔時，請確定使用標籤金鑰的 SageMaker Studio 使用者名稱來標記設定檔`studiouserid`。主參與者 (附加至使用者的使用者或角色) 也應具有含索引鍵的標籤`studiouserid` (此標籤可以命名為任何項目，且不限於`studiouserid`) 。

接下來，將以下策略附加到用戶啟動 SageMaker Studio 時將承擔的角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonSageMakerPresignedUrlPolicy",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreatePresignedDomainUrl"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "sagemaker:ResourceTag/studiouserid": "${aws:PrincipalTag/
studiouserid}"
                }
            }
        }
    ]
}
```

強制標記

資料科學家需要使用 SageMaker Studio 筆記本來探索資料，以及建置和訓練模型。將標籤套用至筆記型電腦有助於監控使用情況和控制成本，並確保擁有權和可稽核性。

若是 SageMaker Studio 應用程式，請確定已標記使用者設定檔。標籤會從使用者設定檔自動傳播至應用程式。要使用標籤（通過 CLI 和 SDK 支持）強制創建用戶配置文件，請考慮將此策略添加到管理員角色：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceUserProfileTags",
            "Effect": "Allow",
            "Action": "sagemaker:CreateUserProfile",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "studiouserid"
                    ]
                }
            }
        }
    ]
}
```

對於其他資源 (例如訓練工作和處理工作)，您可以使用下列原則將標籤設為強制性：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceTagsForJobs",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateTrainingJob",
                "sagemaker:CreateProcessingJob",
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "studiouserid"
                    ]
                }
            }
        }
    ]
}
```

SageMaker 工作室中的根訪問

在 SageMaker Studio 中，筆記本在 Docker 容器中運行，默認情況下，它不具有對主機實例的根訪問權限。同樣地，除了預設的執行身分使用者外，容器內的所有其他使用者識別碼範圍都會重新對應為主機執行個體本身上的非授權使用者 ID。因此，權限提升的威脅僅限於筆記型電腦容器本身。

建立自訂映像檔時，您可能想要為使用者提供更嚴格控制項的非 root 權限；例如，避免以 root 身份執行不需要的程序，或是安裝公開可用的套件。在這種情況下，您可以創建映像以 Dockerfile 中的非 root 用戶身份運行。無論您是以根用戶還是非根用戶身份創建用戶，都需要確保用戶的 UID/GID 與自定義應用程序中的 UID/GID 相同，該AppImageConfig應用程序將創建使用自定義映像運行應用程序的 SageMaker 配置。例如，如果您的 Dockerfile 是為非 root 用戶構建的，例如以下內容：

```
ARG NB_UID="1000"
ARG NB_GID="100"
...
USER $NB_UID
```

該AppImageConfig文件需要在其中提及相同的 UID 和 GID：KernelGatewayConfig

```
{
    "KernelGatewayImageConfig": {
        "FileSystemConfig": {
            "DefaultUid": 1000,
            "DefaultGid": 100
        }
    }
}
```

對於工作室映像，可接受的 UID/GID 值為 0/0 和 1000/100。有關構建自定義映像和相關AppImageConfig設置的示例，請參閱此 Github 存儲庫。

為了避免使用者竄改此問題，請勿將CreateAppImageConfigUpdateAppImageConfig、或DeleteAppImageConfig權限授與 SageMaker Studio 筆記本使用者。

網路管理

若要設定 SageMaker Studio 網域，您需要指定 VPC 網路、子網路和安全性群組。指定 VPC 和子網路時，請確保您根據使用量和預期成長 (在以下各節中討論) 來配置 IP。

VPC 網路規劃

與 SageMaker Studio 網域相關聯的客戶 VPC 子網路必須使用適當的無類別網域間路由 (CIDR) 範圍建立，具體取決於下列因素：

- 使用者數目。
- 每位使用者的應用程式數量。
- 每個使用者的唯一執行個體類型數目。
- 每位使用者的平均訓練執行個體數。
- 預期增長百分比。

SageMaker 和參與的AWS服務會針對下列使用案例，將彈性網路介面 (ENI) 插入客戶 VPC 子網路：

- Amazon EFS 會為網域注入 ENI 的 EFS 掛載目標 (每個子網路/可用區 SageMaker 域附加一個 IP)。SageMaker
- SageMaker Studio 會為使用者設定檔或共用空間使用的每個唯一執行個體注入 ENI。例如：
  - 如果用戶配置文件運行默認的 Jupyter 服務器應用程序（一個「系統」實例），一個數據科學應用程序和一個基本 Python 應用程序（都在`ml.t3.medium`實例上運行），Studio 會注入兩個 IP 地址。
  - 如果使用者設定檔執行預設的 Jupyter 伺服器應用程式 (一個「系統」執行個體)、Tensorflow GPU 應用程式 (在`ml.g4dn.xlarge`執行個體上) 和資料牧馬人應用程式 (在執行個`ml.m5.4xlarge`體上)，Studio 會注入三個 IP 位址。
- 針對跨網域 VPC 子網路/可用區域的每個VPC 端點插入 ENI (四個 IP 用於 SageMaker VPC 端點；約六個 IP 用於參與服務的 VPC 端點，例如 S3、ECR 和.) CloudWatch
- 如果使用相同的 VPC 組態啟動 SageMaker 訓練和處理工作，則每個工作需要每個執行個體兩個 IP 位址。

> **Note**
>
> SageMaker Studio 的 VPC 設定 (例如子網路和僅限 VPC 的流量) 不會自動傳遞至從 Studio 建立的訓練/處理工作。 SageMaker 呼叫建立 * Job API 時，使用者必須視需要設定 VPC 設定和網路隔離。如需詳細資訊，請參閱以免網際網路模式執行訓練和推論容器。

案例：資料科學家在兩種不同的執行個體類型上執行

在此案例中，假設 SageMaker 網域是在僅限 VPC 流量模式下設定。已設定 VPC 端點，例如 SageMaker API、 SageMaker 執行階段、Amazon S3 和 Amazon ECR。

資料科學家正在 Studio 筆記本上執行實驗，在兩種不同的執行個體類型 (例如`ml.t3.medium`和`ml.m5.large`) 上執行，並在每個執行個體類型中啟動兩個應用程式。

假設資料科學家也在執行個體上同時`ml.m5.4xlarge`執行具有相同 VPC 組態的訓練工作。

對於這種情況下， SageMaker Studio 服務將插入 ENI，如下所示：

表 1 — 針對實驗案例插入客戶 VPC 的 ENI

實體	目標	ENI 注射	備註	Level
EFS 掛載目標	VPC 子網路	三	三個AZ/子網路	網域
VPC 端點	VPC 子網路	30	三個可用區塊/子網路，每個子網路各有 10 個 VPCE	網域
木偶伺服器	VPC 子網路	一	每個執行個體一個 IP	使用者
KernelGateway 应用	VPC 子網路	Two	每個執行個體類型一個 IP	使用者
培訓	VPC 子網路	Two	每個訓練執行個體兩個 IP	使用者

實體	目標	ENI 注射	備註	Level
			如果使用 EFA，則每個訓練執行個體五個 IP	

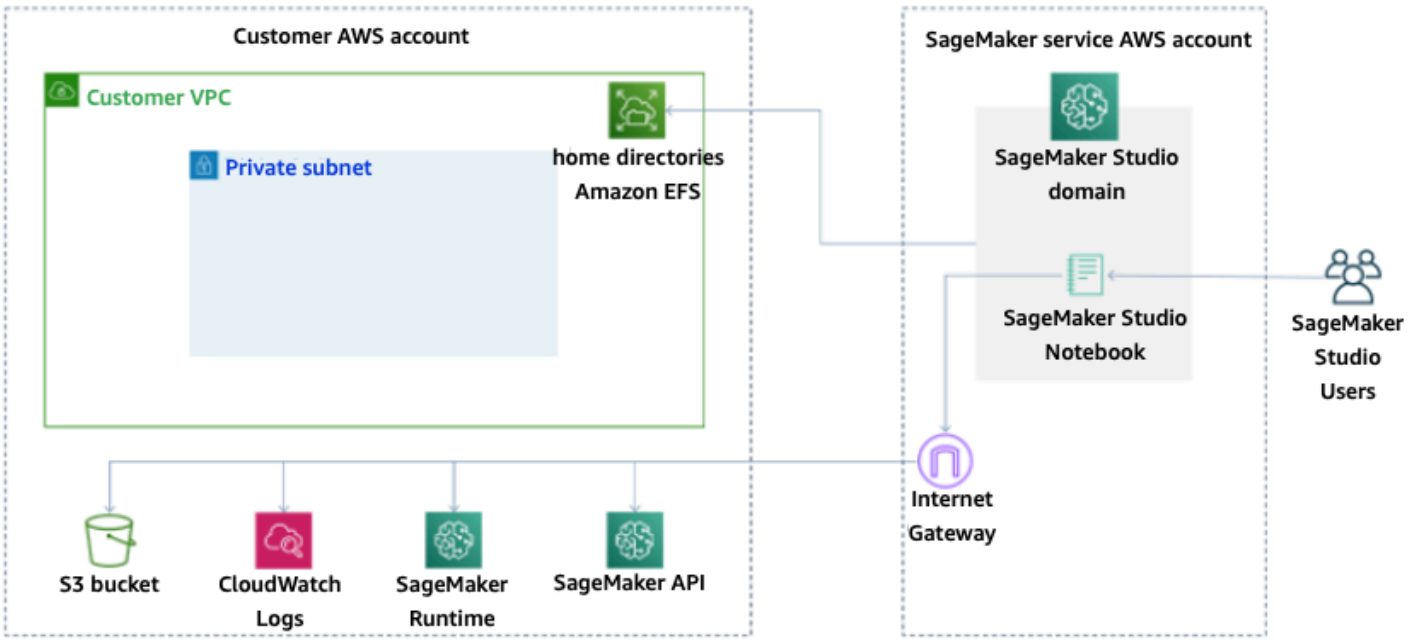
在此案例中，客戶 VPC 中總共消耗了 38 個 IP，其中 33 個 IP 在網域層級與使用者共用，並在使用者層級使用 5 個 IP。如果您在此網域中有 100 位使用者具有類似使用者設定檔並行執行這些活動，則您將在使用者層級使用 5 x 100 = 500 個 IP，在網域層級 IP 消耗 (每個子網路 11 個 IP)，總共 511 個 IP。在此案例中，您需要使用 /22 建立 VPC 子網路 CIDR，以配置 1024 個 IP 位址，並有成長空間。

VPC 網路選項

SageMaker Studio 網域支援使用下列其中一個選項來設定 VPC 網路：

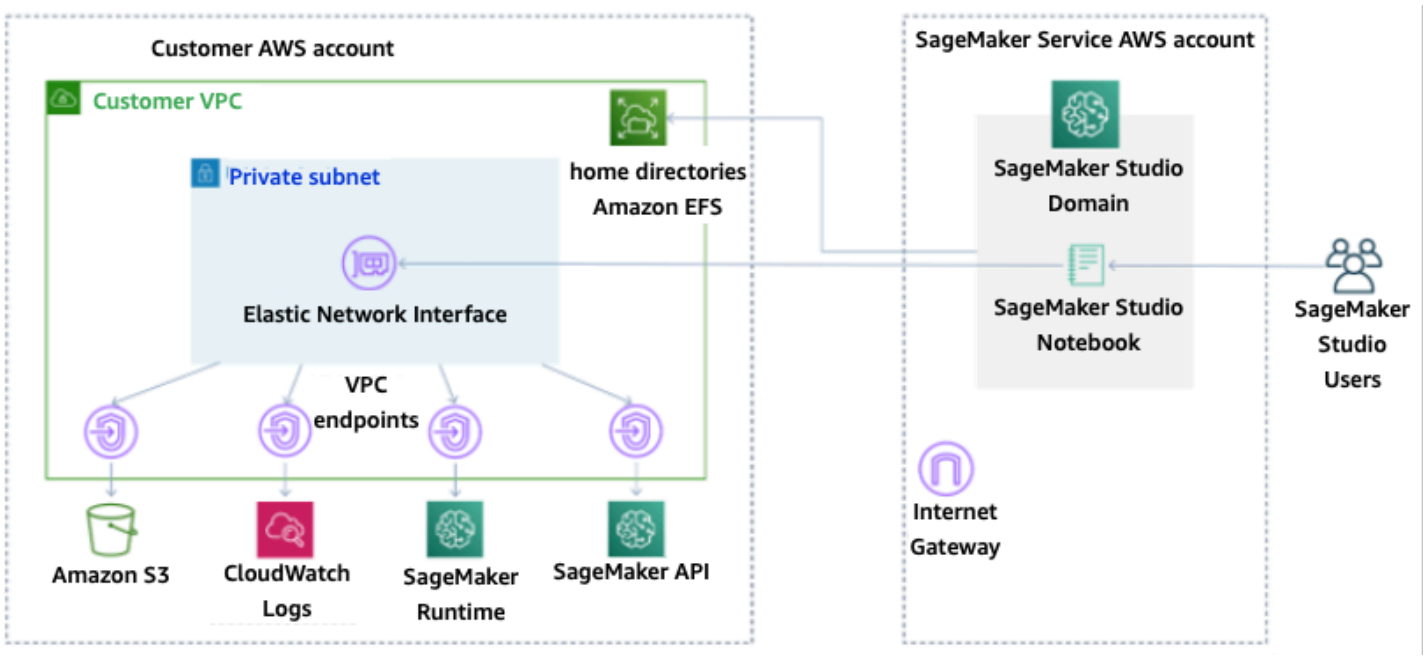
- 僅限公共互聯網
- 僅 VPC

僅公用網際網路選項允許 SageMaker API 服務透過 VPC 中佈建的網際網路閘道使用公用網際網路，由 SageMaker服務帳戶管理，如下圖所示：



預設模式：透過 SageMaker 服務帳戶存取網際網路

僅限 VPC 選項會停用來自 SageMaker 服務帳戶管理之 VPC 的網際網路路由，並允許客戶設定要透過 VPC 端點路由傳送的流量，如下圖所示：



僅限 VPC 模式：無法通過 SageMaker 服務帳戶訪問互聯網

對於在僅限 VPC 模式下設定的網域，請為每個使用者設定檔設定安全群組，以確保基礎執行個體完全隔離。AWS帳戶中的每個網域都可以有自己的 VPC 組態和網際網路模式。如需有關設定虛擬私人雲端網路組態的詳細資訊，請參閱將 VPC 中的 SageMaker Studio 筆記型電腦連線到外部資源。

限制

- 建立 SageMaker Studio 網域之後，您就無法將新的子網路與網域建立關聯。
- 虛擬私人雲端網路類型 (僅限公用網際網路或僅限 VPC) 無法變更。

資料保護

在架構機器學習工作負載之前，應先制定影響安全性的基本實務。例如，資料分類提供了一種根據敏感度等級對資料進行分類的方法，而加密功能則會使資料難以理解到未經授權的存取來保護資料。這些方法非常重要，因為它們支持諸如防止處理不當或遵守監管義務之類的目標。

SageMaker Studio 提供多種功能，用於保護靜態和傳輸中的資料。不過，如「AWS共同責任」模型中所述，客戶必須負責維持控制AWS全球基礎架構上託管的內容。在本節中，我們將說明客戶如何使用這些功能來保護其資料。

保護靜態資料

若要保護您的 SageMaker Studio 筆記本以及模型建置資料和模型成品，請 SageMaker 加密筆記本，以及訓練和批次轉換工作的輸出。 SageMaker 依預設，使用 Amazon S3 的AWS受管金鑰加密這些資訊。這個適用於 Amazon S3 的AWS受管金鑰無法共用於跨帳戶存取。對於跨帳戶存取，請在建立SageMaker資源時指定您的客戶管理金鑰，以便跨帳戶存取共用金鑰。

使用 SageMaker Studio，數據可以存儲在以下位置：

- S3 儲存貯體 — 啟用可共用的筆記本時， SageMaker Studio 會在 S3 儲存貯體中共用筆記本快照和中繼資料。
- EFS 磁碟區 — SageMaker Studio 會將 EFS 磁碟區附加至您的網域，以儲存筆記本和資料檔案。即使在刪除網域之後，此 EFS 磁碟區仍然存在。
- EBS 磁碟區 — EBS 會連接至執行筆記型電腦的執行個體。此磁碟區會在執行個體持續時間內持續存在。

靜態加密 AWS KMS

- 您可以傳遞AWS KMS金鑰來加密連接至筆記型電腦的 EBS 磁碟區、訓練、調整、批次轉換工作和端點。
- 如果您未指定 KMS 金鑰，請使用系統管理的 KMS 金鑰 SageMaker 加密作業系統 (OS) 磁碟區和 ML 資料磁碟區。
- 出於合規原因需要使用 KMS 金鑰加密的敏感資料應存放在 ML 儲存磁碟區或 Amazon S3 中，兩者都可以使用您指定的 KMS 金鑰加密。

保護傳輸中的資料

SageMaker Studio 可確保 ML 模型構件和其他系統成品在傳輸和靜態時加密。對 SageMaker API 和主控台發出的請求，都在安全 (SSL) 連線中進行。有些內部網路傳輸中資料 (服務平台內部) 未加密。其中包括：

- 服務控制平面與訓練任務執行個體 (不是客戶資料) 之間的命令和控制通訊。
- 分散式處理中的節點與訓練工作 (網內) 之間的通訊。

不過，您可以選擇加密訓練叢集中節點之間的通訊。啟用包含所有容器的流量加密可能會增加訓練時間，特別是使用分散式深入學習演算法時。

根據預設，Amazon SageMaker 會在 Amazon VPC 中執行訓練任務，以協助確保資料安全。您可以藉由設定「私有」VPC 來新增其他層級的安全性，以保護您的訓練容器和資料。此外，您可以將 SageMaker Studio 網域設定為僅在 VPC 模式下執行，並設定 VPC 端點以透過私人網路路由流量，而不會透過網際網路傳輸流量。

資料保護護欄

加密靜態 SageMaker 託管卷

在託管線上推論的 SageMaker 端點期間，請使用下列原則強制執行加密：

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
         "Sid": "Encryption",
         "Effect": "Allow",
         "Action": [
             "sagemaker:CreateEndpointConfig"
         ],
         "Resource": "*",
         "Condition": {
             "Null": {
                 "sagemaker:VolumeKmsKey": "false"
             }
         }
     }
   ]
```

```
 }
```

加密模型監控期間使用的 S3 儲存貯

模型監控會擷取傳送到 SageMaker 端點的資料，並將其存放在 S3 儲存貯體中。設定資料擷取組 Config 時，您需要加密 S3 儲存貯體。目前沒有補償控制。

除了擷取端點輸出之外，Model Monitoring 服務還會根據預先指定的基準檢查漂移。您需要加密用於監視漂移的輸出和中繼儲存磁碟區。

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
         "Sid": "Encryption",
         "Effect": "Allow",
         "Action": [
             "sagemaker:CreateMonitoringSchedule",
             "sagemaker:UpdateMonitoringSchedule"
         ],
         "Resource": "*",
         "Condition": {
             "Null": {
                 "sagemaker:VolumeKmsKey": "false",
                 "sagemaker:OutputKmsKey": "false"
             }
         }
     }
   ]
 }
```

加密 SageMaker 工作室網域儲存磁碟區

對連接至 Studio 網域的儲存磁碟區強制加密。此原則需要使用者提供 CMK 來加密連接至 Studio 網域的儲存磁碟區。

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

```
            "Action": [
                "sagemaker:CreateDomain"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "sagemaker:VolumeKmsKey": "false"
                }
            }
        }
    ]
}
```

加密存放在 S3 中用來共用筆記本的資料

這是將儲存在儲存貯體中的任何資料 (用於在 SageMaker Studio 網域中的使用者之間共用筆記本) 加密的原則：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EncryptDomainSharingS3Bucket",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateDomain",
                "sagemaker:UpdateDomain"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "sagemaker:DomainSharingOutputKmsKey": "false"
                }
            }
        }
    ]
}
```

限制

- 建立網域之後，您就無法使用自訂AWS KMS金鑰更新連結的 EFS 磁碟區儲存。

- 建立 KMS 金鑰後，您就無法使用 KMS 金鑰更新訓練/處理工作或端點設定。

記錄和監控

為了協助您偵錯編譯任務、處理任務、訓練任務、端點、轉換任務、筆記本執行個體和筆記型電腦執行個體生命週期組態，還會將演算法容器、模型容器或筆記本執行個體生命週期組態傳送至 stdout 或 stderr 的任何內容傳送至 stdout 或 stderr。 CloudWatch 您可以使用 Amazon 監控 SageMaker Studio CloudWatch，該 Amazon 會收集原始資料並將其處理為可讀且接近即時的指標。這些統計數據保留 15 個月，因此您可以訪問歷史信息，並更好地了解 Web 應用程序或服務的性能。

使用記錄 CloudWatch

由於資料科學程序本質上是實驗性和反覆運算，因此記錄活動非常重要，例如筆記本使用情況、訓練/處理工作執行時間、訓練指標和端點服務指標 (例如叫用延遲)。根據預設，會將指標 SageMaker發佈至 CloudWatch 記錄，而且這些記錄檔可使用客戶管理的金鑰使用AWS KMS.

您也可以使用 VPC 端點在不使用公用網際網路的 CloudWatch 情況下將記錄檔傳送到。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。

SageMaker 為 Studio 建立單一記錄群組，位於下/aws/sagemaker/studio。每個用戶配置文件和應用程序在此日誌組下都有自己的日誌流，生命週期配置腳本也有自己的日誌流。例如，名為「studio-user」的用戶配置文件，其中包含 Jupyter Server 應用程序和附加的生命週期腳本，以及數據科學內核網關應用程序具有以下日誌流：

```
/aws/sagemaker/studio/<domain-id>/studio-user/JupyterServer/default
```

```
/aws/sagemaker/studio/<domain-id>/studio-user/JupyterServer/default/
LifecycleConfigOnStart
```

```
/aws/sagemaker/studio/<domain-id>/studio-user/KernelGateway/datascience-app
```

SageMaker 為了代表您傳送 CloudWatch 記錄檔，訓練/處理/轉換工作 API 的呼叫者將需要下列權限：

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

```
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:DeleteLogDelivery",
                "logs:Describe*",
                "logs:GetLogEvents",
                "logs:GetLogDelivery",
                "logs:ListLogDeliveries",
                "logs:PutLogEvents",
                "logs:PutResourcePolicy",
                "logs:UpdateLogDelivery"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

若要使用自訂AWS KMS金鑰加密這些記錄檔，您必須先修改金鑰原則，以允許 CloudWatch 服務加密和解密金鑰。建立記錄加密AWS KMS金鑰後，請修改金鑰原則以包含下列項目：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "logs.region.amazonaws.com"
            },
            "Action": [
                "kms:Encrypt*",
                "kms:Decrypt*",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:Describe*"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "kms:EncryptionContext:aws:logs:arn": "arn:aws:logs:region:account-
id:*"
                }
            }
        }
```

```
    ]
}
```

請注意，您始終可以為要加密的 CloudWatch 日誌使用`ArnEquals`並提供特定的 Amazon 資源名稱 (ARN)。在這裡，我們顯示了為了簡單起見，您可以使用此密鑰來加密帳戶中的所有日誌。此外，訓練、處理和模型端點會發佈有關執行個體 CPU 和記憶體使用率、託管叫用延遲等的指標。您可以進一步設定 Amazon SNS，以在超過特定閾值時通知管理員事件。訓練和處理 API 的使用者必須具備下列權限：

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Action": [
                 "cloudwatch:DeleteAlarms",
                 "cloudwatch:DescribeAlarms",
                 "cloudwatch:GetMetricData",
                 "cloudwatch:GetMetricStatistics",
                 "cloudwatch:ListMetrics",
                 "cloudwatch:PutMetricAlarm",
                 "cloudwatch:PutMetricData",
                 "sns:ListTopics"
             ],
             "Resource": "*",
             "Effect": "Allow",
             "Condition": {
                 "StringLike": {
                     "cloudwatch:namespace": "aws/sagemaker/*"
                 }
             }

         },
         {
             "Action": [
                 "sns:Subscribe",
                 "sns:CreateTopic"
             ],
             "Resource": [
                 "arn:aws:sns:*:*:*SageMaker*",
                 "arn:aws:sns:*:*:*Sagemaker*",
                 "arn:aws:sns:*:*:*sagemaker*"
             ],
             "Effect": "Allow"
```

```
        }
    ]
}
```

使用稽核 AWS CloudTrail

若要改善合規狀態，請使用AWS CloudTrail. 根據預設，所有 SageMaker API 都會使用 AWS CloudTrail. 您不需要任何其他 IAM 許可即可啟用 CloudTrail。

除了`InvokeEndpoint`和之外的所有 SageMaker 動作均由記錄`InvokeEndpointAsync`，CloudTrail 並記錄在作業中。例如，呼叫`CreateTrainingJob``CreateEndpoint`、和`CreateNotebookInstance`動作會在 CloudTrail 記錄檔中產生項目。

每個 CloudTrail 事件項目都包含產生請求者的相關資訊。身分資訊可協助您判斷下列事項：

- 該請求是否使用根或 AWS IAM 使用者憑證提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務提出。如需範例事件，請參閱記錄 SageMaker API 呼叫及 CloudTrail說明文件。

根據預設，會將使用者設定檔的 Studio 執行角色名稱 CloudTrail 記錄為每個事件的識別碼。如果每個用戶都有自己的執行角色，這將起作用。如果多個使用者共用相同的執行角色，您可以使用`sourceIdentity`組態將 Studio 使用者設定檔名稱傳播至 CloudTrail。請參閱監控來自 Amazon SageMaker 工作室的使用者資源存取以啟用`sourceIdentity`此功能。在共用空間中，所有動作都將空間 ARN 視為來源，您無法透過`sourceIdentity`稽核。

成本歸因

SageMaker Studio 內建的功能可協助管理員追蹤其個別網域、共用空間和使用者的支出。

自動標記

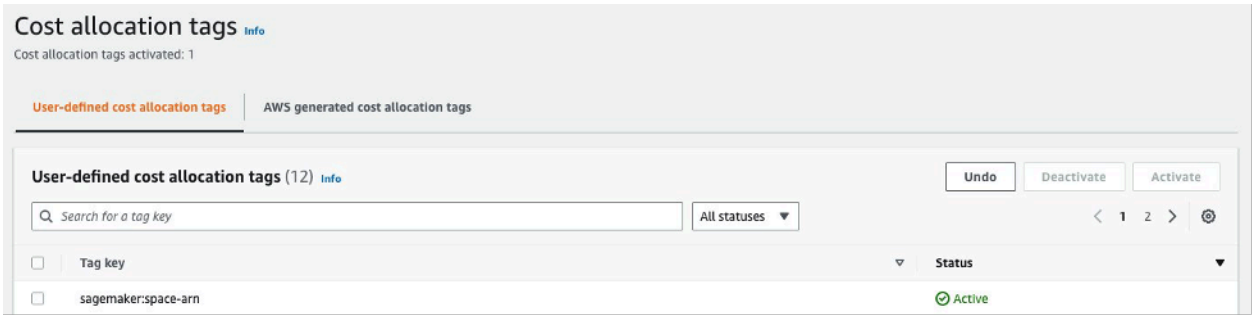
SageMaker Studio 現在會自動標記新 SageMaker 資源，例如培訓任務，處理任務和內核應用程序各自`sagemaker:domain-arn`。在更精細的層級上， SageMaker 也會使用`sagemaker:user-profile-arn`或標記資源，`sagemaker:space-arn`以指定資源的主參與者建立者。

SageMaker 網域 EFS 磁碟區會以名稱為`ManagedByAmazonSageMakerResource`網域 ARN 值的金鑰加上標籤。他們沒有精細的標籤來了解每個用戶級別的空間使用情況。管理員可以將 EFS 磁碟區連接到 EC2 執行個體，以進行自訂監控。

成本監控

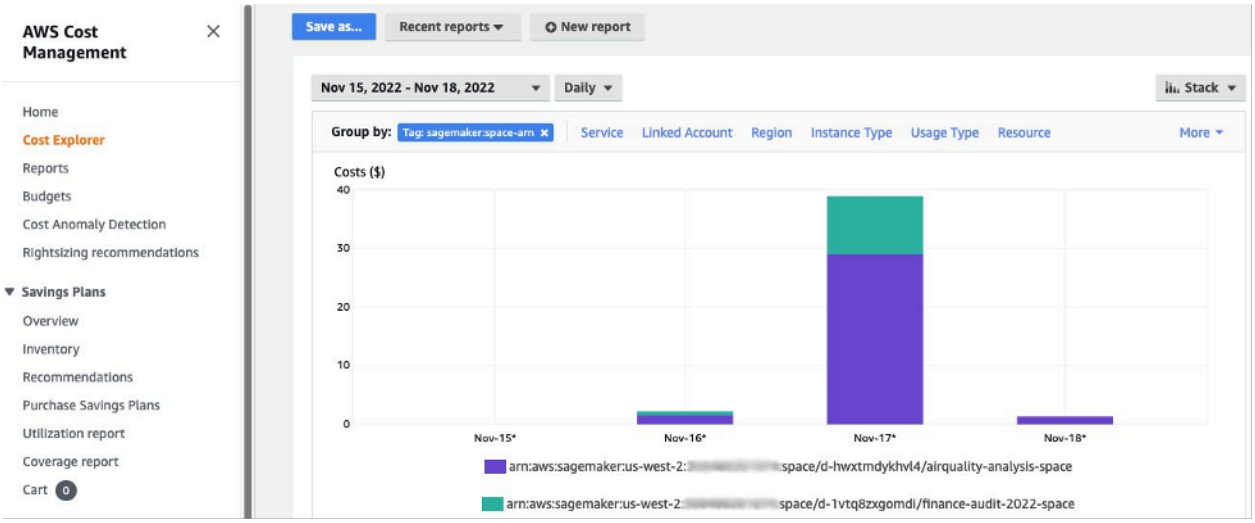
自動化標籤可讓管理員透過 out-of-the-box 解決方案 (例如和)，以及根據AWS成本AWS Cost Explorer和使用量報告 (CURs) 資料建立的自訂解決方案 AWS Budgets，來追蹤、報告及監控您的機器學習支出。

若要使用附加的標籤進行成本分析，必須先在AWS Billing主控台的「成本配置標籤」區段中啟動這些標籤。標籤最多可能需要 24 小時才會顯示在成本分配標籤面板中，因此您必須先建立 SageMaker 資源，才能啟用這些標籤。



在 Cost Explorer 上啟用空間 ARN 作為成本配置標記

啟用成本分配標籤後，AWS將開始追蹤已標記的資源，而在 24-48 小時後，標籤會在成本總管中顯示為可選擇的篩選器。



範例網域依共用空間分組的成本

成本控制

當第一個 SageMaker Studio 使用者上線時， SageMaker 會為網域建立 EFS 磁碟區。此 EFS 磁碟區會產生儲存成本，因為筆記本和資料檔案儲存在使用者的主目錄中。當使用者啟動 Studio 筆記本時，會針對執行筆記本的運算執行個體啟動它們。如需詳細的成本明細，請參閱 Amazon SageMaker 定價。

管理員可以使用「一般防護」一節中所述的 IAM 政策，指定使用者可以啟動的執行個體清單來控制運算成本。此外，我們建議客戶使用 SageMaker Studio 自動關機擴充功能，藉由自動關閉閒置的應用程式來節省成本。此伺服器延伸功能會定期輪詢每個使用者設定檔執行的應用程式，並根據系統管理員設定的逾時關閉閒置應用程式。

若要為網域中的所有使用者設定此擴充功能，您可以使用生命週期組態，如「自訂」一節中所述。此外，您也可以使用擴充套件檢查程式，確保網域的所有使用者都已安裝擴充功能。

客製化

生命週期組態

生命週期組態是由 SageMaker Studio 生命週期事件 (例如啟動新的 SageMaker Studio 筆記本) 所啟動的殼層指令碼。您可以使用這些 shell 指令碼為您的 SageMaker Studio 環境自動化自訂，例如安裝自訂套件、自動關閉非作用中筆記本應用程式的 Jupyter 擴充功能，以及設定 Git 組態。如需如何建立生命週期組態的詳細指示，請參閱此部落格：使用生命週期組態自訂 Amazon SageMaker Studio。

SageMaker Studio 筆記本的自訂映像檔

工作室筆記本隨附一組預先建置的映像檔，其中包含 Amazon SageMaker Python 開發套件和最新版本的 IPython 執行階段或核心。使用此功能，您可以將自己的自訂映像帶到 Amazon SageMaker 筆記本電腦。然後，這些映像可供通過網域驗證的所有使用者使用。

開發人員和資料科學家可能需要數種不同使用案例的自訂映像檔：

- 存取特定或最新版本的熱門 ML 架構 TensorFlow，例如 MXNet 或其他。 PyTorch
- 將本機開發的自訂程式碼或演算法帶到 SageMaker Studio 筆記本，以進行快速迭代和模型訓練。
- 透過 API 存取資料湖或內部部署資料存放區。管理員必須在映像中包含對應的驅動程式。
- 訪問後端運行時（也稱為內核），而不是 IPython（例如 R，Julia 或其他）。您也可以使用概述的方法來安裝自訂核心。

如需如何建立自訂映像檔的詳細指示，請參閱建立自訂 SageMaker 映像檔。

JupyterLab 副檔名

有了 SageMaker Studio JuypterLab 3 筆記型電腦，您就可以充分利用不斷成長的開放原始碼 JupyterLab擴充功能社群。本節重點介紹了一些自然適合 SageMaker 開發人員工作流程的內容，但我們鼓勵您瀏覽可用的擴展程序，甚至創建自己的擴展程序。

JupyterLab 3 現在使打包和安裝擴展的過程變得更加容易。您可以通過 bash 腳本安裝上述擴展。例如，在 SageMaker Studio 中，從 Studio 啟動器打開系統終端並運行以下命令。此外，您可以使用生命週期組態自動安裝這些擴充功能，以便在 Studio 重新啟動之間保留這些擴充功能。您可以針對網域中的所有使用者或個別使用者層級進行設定。

例如，若要安裝 Amazon S3 檔案瀏覽器的擴充功能，請在系統終端機中執行下列命令，並確保重新整理瀏覽器：

```
conda init
conda activate studio
pip install jupyterlab_s3_browser
jupyter serverextension enable --py jupyterlab_s3_browser
conda deactivate
restart-jupyter-server
```

如需有關擴充功能管理的詳細資訊，包括如何撰寫適用於筆記本第 1 版和第 3 版 JupyterLab 筆記本的生命週期組態以提供回溯相容性，請參閱安裝 JupyterLab 和 Jupyter Server 延伸功能。

Git 儲存庫

SageMaker Studio 預先安裝了 Jupyter Git 擴展程序，供用戶輸入 Git 存儲庫的定制 URL，將其克隆到 EFS 目錄，推送更改和查看提交歷史記錄。系統管理員可以在網域層級設定建議的 git 存放庫，使其顯示為使用者的下拉式選項。如需 up-to-date 指示，請參閱將建議的 Git 存放庫附加至 Studio。

如果存儲庫是私有的，擴展程序將要求用戶使用標準 git 安裝將其憑據輸入到終端中。或者，使用者也可以將 ssh 認證儲存在其個別的 EFS 目錄上，以便於管理。

康達環境

SageMaker 工作室筆記本使用 Amazon EFS 做為持久性儲存層。數據科學家可以利用持久性存儲來創建自定義 conda 環境，並使用這些環境來創建內核。這些內核由 EFS 支持，並且在內核，應用程序或 Studio 重新啟動之間是持久的。Studio 會自動拿起所有有效的環境作為 KernelGateway內核。

對於數據科學家來說，創建 conda 環境的過程很簡單，但內核需要大約一分鐘的時間才能填充到內核選擇器上。若要建立環境，請在系統終端機中執行下列指令：

```
mkdir -p ~/.conda/envs
conda create --yes -p ~/.conda/envs/custom
conda activate ~/.conda/envs/custom
conda install -y ipykernel
conda config --add envs_dirs ~/.conda/envs
```

如需詳細指示，請參閱在 Amazon Studio 筆記本中管理 Python 套件的四種方法中的 SageMaker 工作室 EFS 磁碟區部分。

結論

在本白皮書中，我們檢閱了多個領域的最佳實務，例如操作模式、網域管理、身分識別管理、權限管理、網路管理、記錄、監控和自訂，讓平台管理員能夠設定和管理 SageMaker Studio Platform。

附錄

多租戶比較

表 2 — 多租戶比較

多重網域	多賬戶	單一網域中以屬性為基礎的存取控制 (ABAC)
資源隔離是使用標籤來實現的。 SageMaker Studio 會自動使用域 ARN 和用戶配置文件/空間 ARN 標記所有資源。	每個租用戶都在自己的帳戶中，因此存在絕對的資源隔離。	資源隔離是使用標籤來實現的。用戶必須管理 ABAC 創建資源的標記。
清單 API 無法受標籤限制。資源的 UI 過濾是在共享空間上完成的，但是，通過 AWS CLI 或 Boto3 SDK 進行的列表 API 調用將列出整個區域的資源。	清單 API 隔離也是可能的，因為租用戶位於其專用帳戶中。	清單 API 無法受標籤限制。列出透過 AWS CLI 或 Boto3 SDK 進行的 API 呼叫，否則會列出整個區域內的資源。
SageMaker 使用網域 ARN 做為成本分配標記，即可輕鬆監控每個租用戶的 Studio 運算和儲存成本。	SageMaker 使用專用帳戶可輕鬆監控每個租用戶的 Studio 運算和儲存成本。	SageMaker 每個租用戶的 Studio 運算成本必須使用自訂標籤來計算。 SageMaker 由於所有租用戶共用相同的 EFS 磁碟區，因此無法監控每個網域的 Studio 儲存成本。
服務配額是在帳戶層級設定，因此單一租用戶仍可使用所有資源。	您可以在每個租用戶的帳戶層級設定服務配額。	服務配額是在帳戶層級設定，因此單一租用戶仍可使用所有資源。
可透過基礎結構即程式碼 (IaC) 或 Service Catalog 來擴充至多個租用戶。	擴展到多個租戶涉及 Organizations 和自動售貨多個帳戶。	Scaling 需要為每個新承租人提供承租人特定角色，而且使用者設定檔必須以承租人名稱手動標記。

多重網域	多賬戶	單一網域中以屬性為基礎的存取控制 (ABAC)
租用戶內的使用者之間可透過共用空間進行協同合作。	租用戶內的使用者之間的協同作業可透過共用空間進行。	所有租戶都可以使用相同的共享空間進行協作。

SageMaker 工作室網域備份與復原

如果 EFS 意外刪除，或者由於網路或驗證的變更而需要重新建立網域，請遵循下列指示。

選項 1：使用 EC2 從現有的 EFS 備份

SageMaker 工作室域備份

1. 列出 SageMaker 工作室（CLI，SDK）中的用戶配置文件和空間。
2. 將使用者設定檔/空間對應至 EFS 上的 UID。
   a. 對於使用者/空間清單中的每個使用者，請描述使用者設定檔/空間 (CLI、SDK)。
   b. 將使用者設定檔/空間對應至。`HomeEfsFileSystemUid`
   c. `UserSettings['ExecutionRole']`如果使用者具有不同的執行角色，則將使用者設定檔
   d. 識別預設的 Space 執行角色。
3. 建立新網域並指定預設的 Space 執行角色。
4. 建立使用者設定檔和空間。
   - 對於使用者清單中的每個使用者，請使用執行角色對應來建立使用者設定檔 (CLI、SDK)。
5. 為新的 EFS 和 UID 建立對應。
   a. 對於使用者清單中的每個使用者，請描述使用者設定檔 (CLI、SDK)。
   b. 將使用者設定檔對應至`HomeEfsFileSystemUid`。
6. (選擇性) 刪除所有應用程式、使用者設定檔、空間，然後刪除網域。

EFS 備份

若要備份 EFS，請使用下列指示：

1. 啟動 EC2 執行個體，然後將舊 SageMaker Studio 網域的入站/輸出安全群組連接到新的 EC2 執行個體 (允許在連接埠 2049 上透過 TCP 進行 NFS 流量。請參閱將 VPC 中的 SageMaker Studio 筆記本 Connect 到外部資源。
2. 將 SageMaker 工作室 EFS 磁碟區掛接到新的 EC2 執行個體。請參閱掛載 EFS 檔案系統。
3. 將文件複製到 EBS 本地存儲：`>sudo cp -rp /efs /studio-backup:`
   a. 將新網域安全群組連接至 EC2 執行個體。
   b. 將新的 EFS 磁碟區掛接到 EC2 執行個體。
   c. 將檔案複製到新的 EFS 磁碟區。
   d. 對於用戶集合中的每個用戶：
      i. 創建目錄：`mkdir new_uid`。
      ii. 將文件從舊 UID 目錄複製到新的 UID 目錄。
      iii. 更改所有文件的所有權：`chown <new_UID>`對於所有文件。

選項 2：使用 S3 和生命週期組態從現有 EFS 備份

1. 請參閱使用 Amazon Linux 2 將您的工作遷移到 Amazon SageMaker 筆記本執行個體。
2. 建立 S3 儲存貯體以進行備份 (例如`>studio-backup`.
3. 列出具有執行角色的所有使用者設定檔
4. 在目前 SageMaker Studio 網域中，在網域層級設定預設的 LCC 指令碼。
   - 在 LCC 中，將所有內容複製`/home/sagemaker-user`到 S3 中的使用者設定檔前綴 (例如`s3://studio-backup/studio-user1`)。
5. 重新啟動所有預設 Jupyter 伺服器應用程式 (要執行的 LCC)。
6. 刪除所有應用程式、使用者設定檔和網域。
7. 建立新的 SageMaker 工作室網域。
8. 從使用者設定檔和執行角色清單建立新的使用者設定檔。
9. 在網域層級設定 LCC：
   - 在 LCC 中，將 S3 中使用者設定檔前綴中的所有內容複製到 `/home/sagemaker-user`
10. 使用 LCC 設定 (CLI、SDK)，為所有使用者建立預設 Jupyter 伺服器應用程式。

SageMaker 使用 SAML 判斷提示存取工作室

解決方案設置：

1. 在外部 IdP 中建立 SAML 應用程式。
2. 在 IAM 中將外部 IdP 設定為身分識別提供者。
3. 建立可由 IdP 存取的 `SAMLValidator` Lambda 函數 (透過函數 URL 或 API Gateway)。
4. 建立 `GeneratePresignedUrl` Lambda 函數和 API Gateway 以存取函數。
5. 建立使用者可假設呼叫 API Gateway 的 IAM 角色。此角色應以下列格式在 SAML 宣告中作為屬性傳遞：
   - 屬性名稱 https://aws.amazon.com/SAML/Attributes/Role
   - 屬性值：`<IdentityProviderARN><RoleARN>`
6. 將 SAML 宣告用戶服務 (ACS) 端點更新為`SAMLValidator`呼叫 URL。

SAML 驗證程式範例程式碼：

```
import requests
import os
import boto3
from urllib.parse import urlparse, parse_qs
import base64
import requests
from aws_requests_auth.aws_auth import AWSRequestsAuth
import json


# Config for calling AssumeRoleWithSAML
idp_arn = "arn:aws:iam::0123456789:saml-provider/MyIdentityProvider"
api_gw_role_arn = 'arn:aws:iam:: 0123456789:role/APIGWAccessRole'
studio_api_url = "abcdef.execute-api.us-east-1.amazonaws.com"
studio_api_gw_path = "https://" + studio_api_url + "/Prod "

# Every customer will need to get SAML Response from the POST call
def get_saml_response(event):
    saml_response_uri = base64.b64decode(event['body']).decode('ascii')
    request_body = parse_qs(saml_response_uri)
    print(f"b64 saml response: {request_body['SAMLResponse'][0]}")
    return request_body['SAMLResponse'][0]


def lambda_handler(event, context):
    sts = boto3.client('sts')
```

```
    # get temporary credentials
    response = sts.assume_role_with_saml(
                    RoleArn=api_gw_role_arn,
                    PrincipalArn=durga_idp_arn,
                    SAMLAssertion=get_saml_response(event)
                )
    auth = AWSRequestsAuth(aws_access_key=response['Credentials']['AccessKeyId'],
                      aws_secret_access_key=response['Credentials']['SecretAccessKey'],
                      aws_host=studio_api_url,
                      aws_region='us-west-2',
                      aws_service='execute-api',
                      aws_token=response['Credentials']['SessionToken'])

    presigned_response = requests.post(
        studio_api_gw_path,
        data=saml_response_data,
        auth=auth)

    return presigned_response
```

深入閱讀

- 在上設定安全且受到良好管理的機器學習環境 AWS (AWS部落格)
- 為團隊和群組設定具有完整資源隔離功能的 Amazon SageMaker Studio (AWS部落格)
- 使用 AWS SSO 和 Okta 通用目錄（AWS博 SageMaker 客）入職亞馬遜工作室
- 如何設定AWS帳戶聯盟的 SAML 2.0 (確認文件)
- 建置安全的企業 Machine Learning 平台 AWS (AWS技術指南)
- 使用生命週期組態自訂 Amazon SageMaker 工作室 (AWS部落格)
- 將您自己的自訂容器映像帶到 Amazon SageMaker Studio 筆記型電腦 (AWS部落格)
- 建立自訂 SageMaker 專案範本 — 最佳做法 (AWS部落格)
- 使用 Amazon SageMaker 管道進行多帳戶模型部署 (部AWS落格)
- 第 1 部分： NatWest 集團如何構建可擴展，安全和可持續的 MLOP 平台（AWS博客）
- 安全的 Amazon SageMaker Studio 預先簽署網址第 1 部分：基礎基礎設施 (部落格) AWS

貢獻者

本文件的貢獻者包括：

- 拉姆維塔爾，ML 解決方案架構師，Amazon Web Services
- 肖恩·摩根，ML 解決方案架構師，Amazon Web Services
- 杜爾加蘇里, ML 解決方案架構師, Amazon Web Services

特別感謝以下誰貢獻了想法，修改和觀點：

- 亞歷山德羅·塞雷, AI/ML 解決方案架構師, Amazon Web Services
- 薩米特， SageMaker 產品負責人，Amazon Web Services
- Amazon Web Services 軟體開發高級工程師張瀚
- 工作人員, 軟件開發工程師, Amazon Web Services, Amazon Web Services

文件修訂

若要收到有關此白皮書更新的通知，請訂閱 RSS 摘要。

變更	描述	日期
白皮書已更新	斷開的鏈接固定和許多編輯變化。	2023 年 4 月 25 日
初始出版	白皮書已發佈。	2022 年 10 月 19 日

注意

客戶有責任自行對本文件中的資訊進行獨立評估。本文件：(a) 僅供參考，(b) 代表目前的AWS產品供應項目和做法，如有變更，恕不另行通知，且 (c) 不會向其關聯公司、供應商或授權人建立任何承諾或保證。AWS AWS產品或服務係依「原狀」提供，不含任何明示或暗示之擔保、陳述或條件。客戶的責任和責任由AWS協議控制，本文件不屬於與客戶之間AWS的任何協議的一部分，也不會修改。AWS

AWS 詞彙表

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

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。