aws

使用者指南

Amazon DataZone

Amazon DataZone: 使用者指南

Table of Contents

什麼是 Amazon DataZone？

Amazon DataZone 是一種資料管理服務，可讓您更快、更輕鬆地分類、探索、共用和管理跨 AWS 現場部署和第三方來源存放的資料。透過 Amazon DataZone，監督組織資料資產的管理員可以使用精細的控制來管理和控管資料的存取。這些控制項有助於確保具有正確層級的權限和前後關聯的存取。Amazon 可 DataZone 讓工程師、資料科學家、產品經理、分析師和商業使用者輕鬆地在整個組織中共用和存取資料，以便他們能夠探索、使用和協同合作以獲得資料驅動的洞見。

Amazon DataZone 透過整合資料管理服務 (包括 Amazon Redshift、Amazon Amazon Athena、亞馬遜、 AWS Glue、 AWS Lake Formation、現場部署來源、第三方來源等) QuickSight，協助您直接將資料交付給最終使用者，並簡化您的架構。

主題

我可以用 Amazon 做什麼 DataZone？

使用 Amazon DataZone，您可以執行以下操作：

- 控管跨組織界限的資料存取。使用 Amazon DataZone，您可以根據組織的安全規定，協助確保正確的使用者存取正確的資料，以達到正確目的，而無需依賴個別登入資料。您也可以提供資料資產使用的透明度，並使用受控管的工作流程來核准資料訂閱。您也可以透過使用情況稽核功能監視跨專案的資料資產。
- 透過共用資料和工具 Connect 結資料工作者，以推動業務洞察力。使用 Amazon DataZone，您可以跨團隊無縫協作，並提供資料和分析工具的自助存取，以提高業務團隊的效率。您可以使用商業術語來搜尋、共用和存取儲存在 AWS內部部署或與第三方供應商提供者共用的目錄資料。此外，您還可以使用 Amazon DataZone 商業詞彙表，進一步了解您想要使用的資料。
- 利用機器學習自動化資料探索和編目。使用 Amazon DataZone，您可以減少手動將資料屬性輸入商業資料型錄所花費的時間。資料型錄中更豐富的資料也可改善搜尋體驗。

Amazon 如何 DataZone 支援並與其他 AWS 服務整合？

Amazon DataZone 支援三種與其他 AWS 服務的整合類型：

- 生產者資料來源-您可以從儲存在 AWS Glue 資料 DataZone 型錄和 Amazon Redshift 表格和檢視中的資料，將資料資產發佈到 Amazon 目錄。您也可以手動將物件從 Amazon Simple Storage Service (S3) 發佈到 Amazon DataZone 目錄。
- 消費者工具-您可以使用 Amazon Athena 或 Amazon Redshift 查詢編輯器來存取和分析您的資料資產。
- 存取控制和履行-亞馬遜 DataZone 支援授予對 AWS Lake Formation 管理 AWS Glue 表和 Amazon Redshift 表格和檢視的存取權。對於所有其他資料資產，Amazon 會向 Amazon DataZone 發佈與您動作相關的標準事件 (例如，授予訂閱請求的核准) EventBridge。您可以使用這些標準事件與其他 AWS 服務或第三方解決方案整合，以進行自訂整合。

我怎樣才能訪問 Amazon DataZone？

您可以通過以下任何一種方式訪問 Amazon DataZone ：

- Amazon DataZone 遊戲

  您可以使用 Amazon DataZone 管理主控台存取和設定 Amazon 網 DataZone 域、藍圖和使用者。如需詳細資訊，請參閱 https://console.aws.amazon.com/datazone。Amazon DataZone 管理控制台也用於創建 Amazon DataZone 數據門戶。
- Amazon DataZone 數據門戶

  Amazon DataZone 資料入口網站是以瀏覽器為基礎的 Web 應用程式，您可以在其中以自助方式編目、探索、管理、共用和分析資料。資料入口網站可透過 AWS IAM 身分中心 (AWS SSO 的繼任者) 或您的 IAM 登入資料，使用身分供應商的登入資料來驗證您的身分。您可以通過訪問 Amazon DataZone 控制台 https://console.aws.amazon.com/datazone 獲取數據門戶網站 URL。
- Amazon DataZone HTTPS API

  您可以使用 Amazon DataZone HTTPS API 以 DataZone 程式設計方式存取 Amazon，這可讓您直接向服務發出 HTTPS 請求。如需詳細資訊，請參閱 Amazon DataZone API 參考資料。

Amazon DataZone 術語和概念

開始使用 Amazon 時 DataZone，請務必了解其關鍵概念、術語和元件。

主題

Amazon DataZone 組件

Amazon DataZone 包括以下四個主要組成部分：

- 業務資料目錄-您可以使用此元件，在整個組織中針對具有業務情境的資料進行分類，從而使組織中的每個人都能快速搜尋和瞭解資料。
- 發布和訂閱工作-您可以使用這些自動化工作以自助服務方式保護生產者和消費者之間的數據，並確保組織中的每個人都可以訪問正確的數據以達到正確的目的。
- 項目和環境
  - 在 Amazon DataZone 專案中，是以商業使用案例為基礎的人員群組、資產 (資料) 以及用於簡化分析存取的工具。 AWS 專案提供專案成員可以協同合作、交換資料和共用資產的區域。默認情況下，項目是進行設置的，以便只有明確添加到項目中的人才能訪問其中的數據和分析工具。專案管理根據專案政策產生的資產的擁有權，以供資料使用者存取。
  - 在 Amazon DataZone 專案中，環境是零或多個已設定資源的集合 (例如，Amazon S3 儲存貯體、資 AWS Glue 料庫或 Amazon Athena 工作群組)，可在其上操作一組指定的 IAM 主體 (例如，具有參與者權限的使用者)。
- 資料入口網站 (AWS 管理主控台外)-這是一個以瀏覽器為基礎的 Web 應用程式，不同的使用者可以在其中以自助服務的方式前往目錄、探索、控管、共用和分析資料。資料入口網站會透過 IAM 登入資料或身分供應商提供的現有登入資料來驗證使用者。 AWS IAM Identity Center

什麼是 Amazon DataZone 域名？

您可以使用 Amazon DataZone 網域來組織資產、使用者及其專案。透過將其他 AWS 帳戶與 Amazon DataZone 網域建立關聯，您可以將資料來源整合在一起。然後，您可以將資產從這些資料來源發佈到您的網域目錄，並使用中繼資料表單和詞彙表，以改善中繼資料的完整性和品質。您也可以搜尋和瀏覽這些資產，以查看網域中發佈的資料。此外，您還可以加入專案以與其他使用者共同作業、訂閱資產，以及使用專案環境存取分析工具，包括 Amazon Athena 和 Amazon Redshift。Amazon DataZone 網域可讓您彈性反映組織結構的資料和分析需求，無論是為企業建立單一 Amazon 網 DataZone 域，還是為不同業務單位建立多個 Amazon DataZone 網域。

什麼是 Amazon DataZone 項目和環境？

Amazon DataZone 透過建立團隊、工具和資料的使用案例分組，讓團隊和分析使用者能夠在專案上進行協作。

- 在 Amazon 中 DataZone，專案可讓一組使用者在涉及發佈、探索、訂閱和使用 Amazon DataZone 目錄中的資料的各種商業使用案例上進行協作。專案成員使用 Amazon DataZone 目錄中的資產，並使用一或多個分析工作流程產生新資產。專案支援資料入口網站內的下列活動：
  - 專案擁有者可以新增具有擁有者和參與者權限的成員
  - 專案成員可以是 SSO 使用者、SSO 群組和 IAM 使用者
  - 專案成員可以要求訂閱資料目錄中的資產

    訂閱批准提供給項目
- 在 Amazon DataZone 專案中，環境是零或多個已設定資源 (例如 Amazon S3、資 AWS Glue 料庫或 Amazon Athena 工作群組) 的集合，其中包含一組可在這些資源上操作的 IAM 主體。環境是透過使用環境設定檔建立的，這些設定檔是預先設定的資源集和藍圖，提供可重複使用的範本來建立環境。環境設定檔定義設定，例如部署環境的 AWS 帳戶 或區域。

什麼是 Amazon DataZone 藍圖？

建立環境的藍圖定義了環境所屬專案的 AWS 工具和服務 (例如 Amazon Redshift) 成員在處理 Amazon DataZone 目錄中的資產時， AWS Glue 可以使用哪些工具和服務。

在目前版本的 Amazon 中 DataZone，支援下列預設藍圖：

藍圖名稱	描述	建立的資源
資料湖藍圖	讓 Amazon DataZone 專案成員能夠在環境中啟動資料湖生產者和消費者服務。 身為消費者，它可讓 Amazon DataZone 專案成員直接在 Amazon Athena 和其他支援 Lake 格式化的查詢引擎中，存取湖泊格式化管理資產的「唯讀」副本。 作為生產者，它使 Amazon DataZone 項目成員能夠使用 Amazon Athena 創建新的 LakeFormation受管表，並將其發佈到亞馬遜 DataZone目錄。	為使用者提供使用 Amazon Athena 建立和查詢 Lake Formation 資料表的功能。Amazon Athena 工作群組、具有「唯讀」Lake Formation 許可的 AWS Glue 資料庫、「唯讀」IAM 許可，以及存取由專案管理的 Amazon S3。AWS Glue 具有「創建」和「授予」Lake Formation 權限，「讀取」和「寫入」IAM 許可，具有標記的 AWS Glue ETL（提取，轉換和加載）的數據庫。
資料倉儲藍圖	身為消費者，此藍圖可讓 Amazon DataZone 專案成員連線到自己的 Amazon Redshift 叢集，以查詢遠端資料存放區，以及建立和存放新的資料集。 身為生產者，此藍圖可讓 Amazon DataZone 專案成員連接到自己的 Amazon Redshift 叢集，以查詢遠端資料存放區、建立新資料集，並將其發佈到 Amazon DataZone 目錄。	存取 Amazon Redshift 查詢編輯器、從 Amazon DataZone 目錄「讀取」存取訂閱的資料來源，以及在已設定的 Amazon Redshift 叢集中建立本機資產的功能。存取 Amazon Redshift 查詢編輯器、從 Amazon DataZone 目錄「讀取」存取訂閱的資料來源，以及從已設定的 Amazon Redshift 叢集建立和發佈資產的功能。
Amazon Sageemaker 藍圖	此藍圖可協助資料生產者和消費者順暢切換 SageMaker 至 Amazon，在機器學習 (ML) 專案上進行協作，同時強制對資	您可以建立可以在 Amazon 中搜尋、訂閱和發佈資料和 ML 資產的 Amazon SageMaker 網域 DataZone。也可以根據配置

藍圖名稱	描述	建立的資源
	料和 ML 資產執行存取控管。透過 Amazon DataZone 和 Amazon 之間的全新內建整合 SageMaker，資料消費者和生產者可以簡化基礎設施設定之間的 ML 管理、針對商業計劃進行協作，以及輕鬆控管資料和機器學習資產。	訂閱並發佈到 AWS Glue 資料庫和湖泊形成。

什麼是 Amazon DataZone 庫存和發佈工作流程？

建立專案庫存資產

為了使用 Amazon 對數據 DataZone 進行分類，您必須首先將數據（資產）作為 Amazon 項目的庫存 DataZone。建立專案的庫存，只有該專案的成員才能找到資產。除非明確發佈，否則並非所有網域使用者都可以在搜尋/瀏覽中使用專案庫存資產。在目前版本的 Amazon 中 DataZone，您可以使用下列方式將資產新增至專案庫存：

- 透過資料入口網站或使用 Amazon DataZone API 建立和執行資料來源。在目前版本的 Amazon 中 DataZone，您可以為 AWS Glue 和 Amazon Redshift 建立和執行資料來源。透過建立和執行 AWS Glue 或 Amazon Redshift 資料來源，您可以在選定的專案庫存中建立資產，並將其技術中繼資料從來源資料庫表格或資料倉儲作為庫存匯入 Amazon DataZone。
- 您可以使用 API 從可用的系統資產類型 (AWS Glue、Amazon Redshift、Amazon S3 物件) 或從自訂資產類型建立資產。
  - 使用 Amazon DataZone API 在專案庫存中建立自訂資產類型。自訂資產類型可以包括機器學習模型、儀表板、內部部署資料表等。
  - 使用 Amazon DataZone API 從這些自訂資產類型建立資產。
- 使用 Amazon 資 DataZone 料入口網站為 S3 物件手動建立資產。

規劃專案庫存資產-建立專案清查後，資料擁有者可以透過新增或更新業務名稱 (資產和結構描述)、說明 (資產和結構描述)、讀我、詞彙術語 (資產和架構) 和中繼資料表單，來規劃其庫存資產與所需的業務中繼資料。您可以透過資料入口網站或使用 Amazon DataZone API 執行此操作。對資產進行的每次編輯都會建立新的庫存版本。

將專案庫存資產發佈到 Amazon DataZone 目錄

使用 Amazon 對資料 DataZone 進行分類的下一步是讓網域使用者可以探索專案的庫存資產。您可以將庫存資產發佈到 Amazon DataZone 目錄來執行此操作。只有最新版本的庫存資產可以發佈至目錄，而且探索目錄中只有最新發佈的版本處於作用中狀態。如果庫存資產在發佈到 Amazon DataZone 目錄後進行更新，您必須再次明確發佈該資產，以便將最新版本放在探索目錄中。在目前版本的 Amazon 中 DataZone，您可以透過下列方式將專案庫存資產發佈到 Amazon DataZone 目錄：

- 透過資料入口網站或使用 Amazon DataZone API，將專案庫存資產手動發佈到 Amazon DataZone 目錄。
- 在建立或編輯資料來源時，啟用選用的將 AWS Glue 資產發佈到目錄，或將 Amazon Redshift 資產發佈到目錄設定，以便在排程或自動化資料來源執行期間使用。啟用此設定後，資料來源執行會將資產新增至專案的庫存，然後將庫存資產發佈到 Amazon DataZone 目錄。請注意，如果您直接發佈，這些資產可能沒有任何業務中繼資料，而且可直接找到所有網域使用者。您可以透過資料入口網站或使用 Amazon DataZone API 在資料來源上使用此設定。

什麼是 Amazon DataZone 訂閱和履行工作流程？

將您的資產發佈到 Amazon DataZone 目錄後，您的網域使用者可以探索這些資產、請求並取得這些資產的存取權，並繼續使用 Amazon DataZone 來管理、共用和分析這些資產。

使用者代表專案訂閱該資產，以要求存取資產。建立訂閱請求後，資產的擁有者會收到通知，並可以檢閱訂閱請求，並決定他們是要核准還是拒絕。如果訂閱請求獲得資料擁有者的核准，則訂閱專案會被授與該資產的存取權。

一旦訂閱請求獲得核准，Amazon 就會 DataZone 開始訂閱履行工作流程，透過在 AWS Lake Formation 或 Amazon Redshift 中建立必要的授權，自動將資產新增到專案內的所有適用環境。這可讓訂閱專案成員在其環境中使用其中一個查詢工具 (Amazon Athena 或 Amazon Redshift 查詢編輯器) 查詢資產。

Amazon 只 DataZone 能針對受管資產 (包括 AWS Glue 資料表和 Amazon Redshift 表格和檢視) 觸發此自動履行邏輯。對於所有其他資產類型 (非受管資產)，Amazon DataZone 無法自動觸發履行，而是在 Amazon Eventbridge 中發佈事件，其中包含事件承載中的所有必要詳細資訊，以便您可以在 Amazon 以外建立必要的授權。 DataZoneAmazon DataZone 還提供了 `updateSubscriptionStatus` API，該 API 使您可以在 Amazon 以外完成訂閱後更新訂閱的狀態，以 DataZone 便 Amazon DataZone 可以通知項目成員他們可以開始使用該資產。

Amazon 的用戶角色 DataZone

以下是主要的 Amazon DataZone 用戶角色：

- 擁有將 Amazon 設定 DataZone 為其組織分析平台的網域管理員。

  在 Amazon 的環境中 DataZone，網域管理員會 DataZone 在 AWS 帳戶中安裝 Amazon、建立 Amazon DataZone 網域，以及設定 AWS 帳戶關聯和身分供應商與 Amazon DataZone 網域的關聯。網域管理員也會使用其他 AWS 服務主控台 (例如 AWS 組織和 Service Catalog) 來設定 Amazon DataZone。
- 身為 Amazon 主要使用者 DataZone (資產發佈者和訂閱者) 進行分析和機器學習任務的資料使用者。

  資料使用者包括產生和使用資料資產的資料分析工作者、資料科學家和系統使用者。在 Amazon 環境中 DataZone，資料使用者建立和加入專案和環境、使用預先設定的分析或機器學習工具訂閱和使用資料資產，以及將輸出資料資產發佈回 Amazon DataZone 網域目錄以與其他人共用。
- 建立自訂基礎設施範本，並將 Amazon DataZone 與內部目錄或生產系統整合的系統開發人員。

  在 Amazon 的環境中 DataZone，系統開發人員將環境藍圖 (基礎設施範本) 或基礎設施即程式碼 CI/CD 管道建置為環境提供者、資料管道以跨環境推廣資料資產、目錄同步和訂閱授予履行配接器以與內部目錄整合，或在需要時在 Amazon DataZone API 與內部使用者界面或生產系統之間進行整合。
- 擁有組織安全、隱私權和其他合規政策的定義和風險，並確保 Amazon DataZone 在其組織中的使用符合這些定義的資料控管主管。

Amazon DataZone 术语

網域

Amazon DataZone 網域是將資產、使用者及其專案連接在一起的組織實體。使用 Amazon DataZone 網域，您可以靈活地反映組織結構的資料和分析需求，無論是為您的企業建立單一 Amazon DataZone 網域，還是為不同業務單位或團隊建立多個 Datazone 網域，您都可以靈活地反映組織結構的資料和分析需求。

關聯帳戶

將 AWS 帳戶與 Amazon DataZone 網域建立關聯，可讓您將這些 AWS 帳戶的資料發佈到 Amazon DataZone 目錄中，並建立 Amazon DataZone 專案，以便在多個 AWS 帳戶中處理資料。帳戶關聯請求只能在擁有 Amazon DataZone 網域的 AWS 帳戶中啟動。帳戶關聯要求只能由受邀 AWS 帳

戶的管理使用者接受。一旦 AWS 帳戶與某個 Amazon DataZone 網域建立關聯，您就可以在此帳戶中將 AWS Glue 目錄和 Amazon Redshift 等資料來源註冊到此網域。關聯還可以使 AWS 帳戶創建 Amazon DataZone 項目和環境。

一個 AWS 帳戶 可以與一個或多個 Amazon DataZone 網域相關聯。

資料來源

在 Amazon 中 DataZone，您可以使用資料來源將資產 (資料) 的技術中繼資料從來源資料庫或資料倉儲匯入 Amazon DataZone。在目前版本的 Amazon 中 DataZone，您可以為 AWS Glue 和 Amazon Redshift 建立和執行資料來源。透過建立資料來源，您可以在 Amazon DataZone 和來源 (AWS Glue Data Catalog 或 Amazon Redshift 倉儲) 之間建立連線，以便讀取技術中繼資料，包括表名稱、欄名稱和資料類型。透過建立資料來源，您還可以啟動初始資料來源執行，在 Amazon 中建立新資產或更新現有資產 DataZone。建立資料來源時或成功建立資料來源後，您也可以選擇為資料來源執行指定排程。

資料來源執行

在 Amazon 中 DataZone，資料來源執行是 Amazon DataZone 執行的一項任務，以便在專案庫存中建立資產，也可以選擇將專案庫存資產發佈到 Amazon DataZone 目錄。可以自動執行資料來源 (在最初建立資料來源時啟動)，也可以排程或手動執行。資料選取準則可讓您微調現有和 future 的資料集，以擷取到專案庫存或 Amazon DataZone 目錄中，以及這些庫存或目錄資產的中繼資料更新頻率。

訂閱目標

在 Amazon 中 DataZone，訂閱目標可讓您存取在專案中訂閱的資料。訂閱目標指定 Amazon 可用於與來源資料建立連線並建立必要授權的位置 (例如資料庫或結構描述) 和必要許 DataZone 可 (例如 IAM 角色)，以便 Amazon DataZone 專案成員可以開始查詢他們已訂閱的資料。

訂閱請求

在 Amazon 中 DataZone，訂閱請求是 Amazon DataZone 專案必須遵循的程序，才能授予特定資產的存取權。您可以核准、拒絕、撤銷或授與訂閱要求。

資產

在 Amazon 中 DataZone，資產是顯示單一實體資料物件 (例如，資料表、儀表板、檔案) 或虛擬資料物件 (例如，檢視) 的實體。

資產類型設定

資產類型定義了資產在 Amazon DataZone 目錄中的表示方式。資產類型可定義特定資產類型的資料架構。建立資產時，會根據其資產類型 (依預設為最新版本) 定義的資產架構來驗證資產。發生資

產更新時，Amazon 會 DataZone 建立新的資產版本，並讓 Amazon DataZone 使用者能夠在所有資產版本上操作。

商業詞彙

在 Amazon 中 DataZone，商業詞彙表是可能與資產相關聯的商業術語集合。商業詞彙表有助於確保整個組織在各種資料分析工作中使用相同的術語和定義。

您可以將商業詞彙表中的術語新增至資產和欄，以便在搜尋期間對這些屬性進行分類或加強識別。您可以在與資產關聯的中繼資料表單中，選取字彙作為欄位的值類型。選取特定字詞做為資產中繼資料表單欄位的值時，使用者可以搜尋商業詞彙字詞並尋找相關資產。

元數據表單類型

中繼資料表單類型是一種範本，用於定義資產建立為庫存或在 Amazon DataZone 網域中發佈時收集和儲存的中繼資料。中繼資料表單類型可以與資料資產產生關聯。中繼資料表單類型可協助網域管理員定義該網域所需的中繼資料表單，例如合規性資訊、法規資訊或分類。它可讓網域管理員自訂其資產的其他中繼資料。Amazon DataZone 具有系統元數據表單類 asset-common-details-form型，例如類 column-business-metadata-form型 glue-table-form-type glue-view-form-type，類型 redshift-table-form-type redshift-view-form-type，，，object-collection-form-type，s3-subscription-terms-form-type，和 suggestion-form-type。

元數據表單

在 Amazon 中 DataZone，中繼資料表單定義資產建立為庫存或在 Amazon DataZone 網域中發佈時收集和儲存的中繼資料。中繼資料表單定義是由網域管理員在目錄網域中建立的。中繼資料表單定義由一或多個欄位定義組成，支援布林值、日期、十進位、整數、字串和商業詞彙表欄位值資料類型。

網域管理員會將中繼資料表單新增至其網域，將中繼資料表單套用至其網域中的資產。然後，資產發佈者會在中繼資料表單中提供任何選擇性和必要欄位值。

專案

在 Amazon 中 DataZone，專案可讓一組使用者在各種商業使用案例上進行協作，這些使用案例涉及在專案清單中建立資產，進而讓所有專案成員都能探索這些資產，然後發佈、探索、訂閱和使用 Amazon 目錄中的資產。 DataZone 專案成員使用 Amazon DataZone 目錄中的資產，並使用一或多個分析工作流程產生新資產。專案成員可以是擁有者或貢獻者。項目所有者可以添加或刪除其他用戶作為擁有者或貢獻者，他們可以修改或刪除項目。對貢獻者的其他限制可以使用政策來定義。當使用者建立專案時，他們會成為該專案的第一個擁有者。

環境

環境是已設定資源的集合 (例如，Amazon S3 儲存貯體、資 AWS Glue 料庫或 Amazon Athena 工作群組)，其中包含一組可在這些資源上操作的指定 IAM 主體 (具有指派的參與者許可)。每個環境也可能有授權存取資源並透過訂閱和履行存取資料的使用者主體。環境旨在將可操作的鏈接存儲到 AWS 服務和外部 IDE 和控制台中。專案成員可以透過在環境中設定的深層連結存取 Amazon Athena 主控台等服務。專案中的 SSO 使用者和 IAM 使用者可進一步設定為使用/存取特定環境。

環境設定檔

在 Amazon 中 DataZone，環境設定檔是可用來建立環境的範本。環境設定檔是使用藍圖建立的。

透過環境設定檔，網域管理員可以使用預先設定的參數來包裝藍圖，然後資料工作者可以透過選取現有的環境設定檔並指定新環境的名稱，快速建立任意數量的新環境。這可讓資料工作者有效管理其專案和環境，同時確保資料工作者滿足其網域管理員強制執行的資料控管原則。

藍圖

建立環境的藍圖定義了環境所屬專案的 AWS 工具和服務 (例如 Amazon Redshift) 成員在處理 Amazon DataZone 目錄中的資產時， AWS Glue 可以使用哪些工具和服務。

在目前版本的 Amazon DataZone 中，支援下列預設藍圖：

- 資料湖藍圖
- 資料倉儲藍圖
- Amazon Sageemaker 藍圖

使用者概況

用戶配置文件代表 Amazon DataZone 用戶。Amazon 同時 DataZone 支援 IAM 角色和 SSO 身分識別，以便與 Amazon DataZone 管理主控台和資料入口網站進行互動，以達到不同用途。網域管理員使用 IAM 角色在 Amazon DataZone 管理主控台中執行與管理網域相關的初始工作，包括建立新的 Amazon DataZone 網域、設定中繼資料表單類型以及實作政策。資料工作者透過身分識別中心使用其 SSO 公司身分登入 Amazon DataZone 資料入口網站，並存取擁有會員資格的專案。

集團概況

群組設定檔代表 Amazon DataZone 使用者群組。您可以手動建立群組，或對應至企業客戶的 Active Directory 群組。在 Amazon DataZone，團體有兩個目的。首先，群組可以對應到組織圖中的使用者團隊，因此在有新員工加入或離開團隊時減少 Amazon DataZone 專案擁有者的管理工作。其次，企業管理員使用 Active Directory 群組來管理和更新使用者狀態，讓 Amazon DataZone 網域管理員可以使用這些群組成員資格來實作 Amazon DataZone 網域政策。

網域管理員

在 Amazon 中 DataZone，建立 Amazon DataZone 網域的 IAM 主體是該網域的預設網域管理員。Amazon 中的網域管理員 DataZone 執行網域的關鍵功能，包括建立網域、指派其他網域管理員、新增資料來源和訂閱目標、建立專案和環境，以及指派專案擁有者。

出版商

在 Amazon 中 DataZone，出版商將資產發佈到 Amazon DataZone 目錄中，並可編輯其發佈資產的中繼資料。如果授予此授權，發布者可以核准或拒絕對他們在 Amazon DataZone 目錄中發佈的資產的訂閱請求。

Subscriber

在 Amazon DataZone，訂戶是一個 Amazon DataZone 項目，希望查找，訪問和使用 Amazon DataZone 目錄中的資產。

AWS 帳戶 owner

在 Amazon 中 DataZone， AWS 帳戶 擁有者在其 AWS 帳戶 中建立角色、政策和許可，以 AWS 帳戶 便將這些角色、政策和許可與 Amazon DataZone 網域建立關聯。

Amazon 有什麼新功能 DataZone？

本節說明 Amazon DataZone 按發行日期顯示的新功能和改進項目。

主題

2024

Amazon DataZone 推出與 Amazon 集成 SageMaker

二零二四年六月五日發行

Amazon DataZone 推出與 Amazon 的整合，協 SageMaker助資料生產者和消費者順暢切換 SageMaker 至 Amazon，以便在機器學習 (ML) 專案上進行協作，同時強制對資料和 ML 資產執行存取控管。透過 Amazon DataZone 和 Amazon 之間的全新內建整合 SageMaker，資料消費者和生產者可以簡化基礎設施設定之間的 ML 管理、針對商業計劃進行協作，並輕鬆控管資料和機器學習資產。如需詳細資訊，請參閱 使用 Amazon 內 DataZone置藍圖 及 使用關聯帳戶以發佈和使用資料。

Amazon DataZone 推出與 AWS Lake Formation 混合訪問模式集成

二零二四年三月四日發行

Amazon DataZone 已經推出了與 AWS Lake Formation 混合訪問模式的集成。這項整合可讓您透過 Amazon 輕鬆發佈和共用 AWS Glue 表格 DataZone，而無需先在 AWS Lake Formation 中註冊。若要開始使用，管理員在 Amazon DataZone 主控台的`DefaultDataLake`藍圖下啟用資料位置登錄設定。然後，當資料取用者訂閱透過 IAM 許可管理的 AWS Glue 表格時，Amazon 會 DataZone 先以混合模式註冊此資料表的 Amazon S3 位置，然後透過 AWS Lake Formation 管理資料表上的許可，授予資料取用者的存取權。這可確保資料表上的 IAM 許可繼續以新授予的 AWS Lake Formation 權限存在，而不會中斷任何現有的工作流程。如需更多資訊，請參閱Amazon DataZone 與 AWS Lake Formation 混合模式集成 。

Amazon DataZone 推出與 AWS Glue 數據質量集成

二零二四年三月四日發行

Amazon DataZone 推出與 AWS Glue 資料品質的整合，並提供 API 來整合第三方資料品質解決方案的資料品質指標。新的整合可讓您將 AWS Glue 資料品質分數自動發佈到 Amazon DataZone 商業資料目錄中。Amazon DataZone API 可用來擷取第三方來源的品質指標。發佈之後，資料消費者可以輕鬆搜尋資料資產、檢視精細的品質指標，以及識別失敗的檢查和規則，進而賦予業務決策的能力。如需更多資訊，請參閱Amazon 的數據質量 DataZone。

針對 Amazon 中說明的 AI 建議正式發行版本 DataZone

二零二四年三月二十一日發行

Amazon DataZone 宣布新的生成 AI 型功能正式推出，透過豐富商業資料目錄來改善資料探索、資料理解和資料使用量。只要按一下，資料生產者就可以產生全面的業務資料說明和內容、反白顯示有影響力的資料欄，並包含有關分析使用案例的建議。此次推出新增了對 API 的支援，資料生產者可使用這些 API 以程式設計方式產生資產描述 如需詳細資訊，請參閱 使用機器學習和生成人工智慧。

Amazon DataZone 推出亞 Amazon Redshift 集成的增強功能

二零二四年三月二十一日發行

Amazon DataZone 已經對其 Amazon Redshift 集成進行了一些增強功能，從而簡化了發布和訂閱 Amazon Redshift 表和視圖的過程。這些更新簡化了資料生產者和消費者的體驗，讓他們能夠使用 Amazon DataZone 管理員提供的預先設定登入資料和連線參數快速建立資料倉儲環境。此外，這些增強功能可讓管理員進一步控制誰可以在其 AWS 帳戶和 Amazon Redshift 叢集中使用資源，以及用於何種目的。

- 藍圖組態：啟用`DefaultDataWarehouseBlueprint`藍圖後，您可以透過將管理專案指派給已啟用的`DefaultDataWarehouseBlueprint`藍圖，來控制哪些專案可以使用帳戶中的藍圖來建立環境設定檔。您也可以`DefaultDataWarehouseBlueprint`透過提供叢集、資料庫和機 AWS 密等參數來建立參數集。您也可以從 Amazon DataZone 主控台內建立 AWS 密碼。
- 環境設定檔：建立環境設定檔時，您可以選擇提供自己的 Amazon Redshift 參數，或使用藍圖組態中的其中一個參數集。如果您選擇使用在藍圖組態中建立的參數集，則 AWS 密碼只需要`AmazonDataZoneDomain`標`AmazonDataZoneProject`籤 (只有在您選擇在環境設定檔中提供自己的參數集時，才需要標籤)。在環境設定檔中，您可以指定授權專案的清單。只有獲得授權的專案可以使用此環境設定檔來建立資料倉儲環境。您也可以指定允許發佈哪些資料授權專案。目前您可以選擇下列其中一個選項：1) 從任何結構描述發佈、2) 從預設環境結構描述發佈、3) 不允許發佈。
- 環境：資料生產者或取用者現在可以選取環境設定檔來建立環境，而不需要提供自己的 Amazon Redshift 參數，包括機 AWS 密、叢集、工作群組和資料庫。這些參數會從環境設定檔移植到環境中。除了建立環境之外，Amazon DataZone 現在也會為環境建立預設結構描述。專案的成員具有此

結構描述的讀取和寫入存取權，並且可以透過執行作為環境建立一部分而建立的預設資料來源，輕鬆將在此結構描述中建立的任何表格發佈到目錄。用於建立環境的 Amazon Redshift 參數也可用於建立新的資料來源 (而不是資料生產者在建立資料來源時提供自己的參數)。

AWS Amazon 雲形成 Support DataZone

二零二四年一月十八日發行

Amazon 的用戶現在 DataZone 可以利 AWS CloudFormation 用有效地建模和管理一套 Amazon DataZone 資源。這種方法可促進資源的一致性佈建，同時也可透過基礎結構即程式碼實務來實現生命週期 使用自訂範本，您可以精確定義所需的資源及其相互依存性。如需詳細資訊，請參閱 Amazon DataZone 資源類型參考資料。

直接將 IAM 主體新增為 Amazon DataZone 專案的成員

二零二四年五月一日發行

您現在可以將 IAM 主體新增為專案成員，即使這些 IAM 主體尚未登入 Amazon DataZone (先前的要求)。網域管理員或 IT 管理員新增`iam:GetUser`並`iam:GetRole`加入網域的網域執行角色後，專案擁有者只需提供 IAM 角色或 IAM 使用者的 Amazon 資源名稱 (ARN)，即可將 IAM 主體新增為成員。IAM 主體仍必須具有存取 Amazon 所需的 IAM 許可， DataZone 而且可以在 IAM 主控台中設定這些許可。如需詳細資訊，請參閱 將成員新增至專案。

從資料入口網站 Support 自訂資產類型

二零二四年五月一日發行

對自訂資產的支援可讓 Amazon DataZone 透過 Data Portal 為非結構化資料 (包括儀表板、查詢和模型) 分類資產，讓您可以更輕鬆地直接在資料入口網站中新增自訂資產，以及先前可用的 API 支援。在 Amazon 中建立、更新和發佈自訂資產的功能 DataZone，可讓您共用、尋找、訂閱任何類型的資產，以及建立提供這些資產管理的業務工作流程。如需詳細資訊，請參閱 建立自訂資產類型。

2023

刪除網域

二零二三年二月二十二日發行

這項功能可讓您更輕鬆地刪除網域。現在，即使域不是空的，您也可以繼續刪除域名（如包含項目，環境，資產，數據源等）。如需詳細資訊，請參閱 刪除網域。

混合模式

二零二三年二月二十二日發行

Amazon 增加 DataZone 了對 AWS Lake Formation 型混合模式的支持。有了這項支援，如果您將 AWS Glue 資料表發佈到 Amazon，其 AWS S3 位置在 Lake Formation 以混合模式註冊，Amazon 會 DataZone 將此表視為受管資產，並且可以管理此表格的訂閱授 DataZone 與。在此功能發布之前，Amazon DataZone 會將此表視為非託管資產，即 Amazon DataZone 無法授予此表的訂閱。如需詳細資訊，請參閱 為 Amazon 配置 Lake Formation 許可 DataZone。

HIPAA 合格服務

二零二三年十二月十四日發行

Amazon 現 DataZone 在符合 1996 年美國 Health 保險可攜性和責任法案 (HIPAA) 標準。若要檢視符合 HIPAA 規範的 AWS 服務清單，請參閱 https://aws.amazon.com/compliance/ hipaa-eligible-services-reference/。

有關 Amazon 描述的 AI 建議 DataZone（預覽版）

二零二三年十一月八日發行

AWS 宣布預覽 Amazon 中新的生成 AI 功能，藉由豐富商業資料目錄 DataZone來改善資料探索、資料理解和資料使用量。只要按一下，資料生產者就可以產生全面的業務資料說明和內容、反白顯示有影響力的資料欄，並包含有關分析使用案例的建議。透過針對 Amazon 中描述的 AI 建議 DataZone，資料消費者可以識別分析所需的資料表和欄，進而增強資料可探索性並減少與資料生產者的 back-and-forth 通訊。預覽版適用於下列 AWS 區 DataZone 域佈建的 Amazon 網域：美國東部 (維吉尼亞北部)、美國西部 (奧勒岡)。如需詳細資訊，請參閱 使用機器學習和生成人工智慧。

DefaultDataLake 藍圖增強

二零二三年十一月二十日發行

Amazon 在 DefaultDataLake 藍圖中新增 DataZone 了一項增強功能，可讓您更好地控制誰可以從您的 AWS 帳戶發佈哪些資料。此功能啟動時引入了兩項關鍵變更。

- 在主控台中啟用 DefaultDataLake 藍圖後，您可以透過將管理專案指派給已啟用的 DefaultDataLake 藍圖，來控制哪些專案可以使用帳戶中的藍圖來建立環境設定檔。

- 第二個變更是在入口網站中。如果您使用 DefaultDataLake 藍圖建立環境設定檔，您也可以選取允許使用環境設定檔來建立環境的授權專案。依預設，允許所有專案使用資料湖環境紀要，但是您可以將環境紀要限制為特定專案，也可以控制可以使用使用縱斷面建立的環境發佈哪些資料。

如需更多詳細資訊，請參閱 建立環境設定檔。

設定

若要設定 Amazon DataZone，您必須擁有一個 AWS 帳戶，並為 Amazon 設定所需的 IAM 政策和許可 DataZone。

設定 Amazon DataZone 許可後，建議您完成「入門」部分中的步驟，以引導您建立 Amazon DataZone 網域、取得資料入口網站 URL，以及適用於資料生產者和資料消費者的基本 Amazon DataZone 工作流程。

主題

註冊一個 AWS 帳戶

如果您沒有 AWS 帳號，請完成以下步驟來建立帳號。

如果您有一個 AWS 組織，請創建一個帳戶：

1. 登入 AWS 管理主控台，然後開啟 Organizations 主控台，網址為 https://console.aws.amazon.com/organizations/。
2. 在功能窗格中，選擇 [AWS 帳戶]。
3. 選擇 [新增 AWS 帳戶]。
4. 選擇「建立 AWS 帳戶」並提供要求的詳細資料。選擇 [建立 AWS 帳戶]。

註冊一個帳 AWS 戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

當您註冊 AWS 帳號時，會建立AWS 帳號根使用者。root 使用者可以存取帳號中的所有 AWS 服務和資源。作為安全最佳實務，將管理存取權指派給管理使用者，並且僅使用根使用者來執行 需要根使用者存取權的任務。

設定使用 Amazon DataZone 管理主控台所需的 IAM 許可

任何想要使用 Amazon DataZone 管理主控台的使用者、群組或角色都必須具有必要的許可。

主題

- 將必要和選用政策附加到 Amazon DataZone 主控台存取的使用者、群組或角色
- 建立 IAM 許可的自訂政策，以簡化 Amazon DataZone 服務主控台的角色建立
- 為許可建立自訂政策，以管理與 Amazon DataZone 網域關聯的帳戶
- (選擇性) 建立 AWS 身分識別中心權限的自訂原則，以便為您的網域啟用單一登入 (SSO)
- (選擇性) 為 AWS 身分識別中心許可建立自訂政策，以新增和移除對 Amazon DataZone 網域的 SSO 使用者和 SSO 群組存取權。
- (選擇性) 將 IAM 主體新增為金鑰使用者，以使用金鑰管理服務 (KMS) 的客戶管理金 AWS 鑰建立 Amazon DataZone 網域

將必要和選用政策附加到 Amazon DataZone 主控台存取的使用者、群組或角色

完成下列程序，將必要和選用的自訂原則附加至使用者、群組或角色。如需詳細資訊，請參閱 AWS Amazon 的受管政策 DataZone。

1. 登入 AWS 管理主控台，然後開啟 IAM 主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在導覽窗格中，選擇政策。
3. 選擇下列原則以附加至您的使用者、群組或角色。

    - 在策略清單中，選取旁邊的核取方塊AmazonDataZoneFullAccess。您可用篩選功能表和搜尋方塊來篩選政策清單。如需詳細資訊，請參閱 AWS 受管理的策略：AmazonDataZoneFullAccess。
    - (選擇性) 建立 IAM 許可的自訂政策，以簡化 Amazon DataZone 服務主控台的角色建立。
    - (選擇性) 建立 AWS 身分識別中心權限的自訂原則，以便為您的網域啟用單一登入 (SSO)。

- (選擇性) 為 AWS 身分識別中心許可建立自訂政策，以新增和移除對 Amazon DataZone 網域的 SSO 使用者和 SSO 群組存取權。

4. 選擇 Actions (動作)，然後選擇 Attach (連接)。
5. 選擇要附加原則的使用者、群組或角色。您可用篩選功能表和搜尋方塊來篩選主體實體清單。選擇使用者、群組或角色後，請選擇 [附加原則]。

建立 IAM 許可的自訂政策，以簡化 Amazon DataZone 服務主控台的角色建立

完成下列程序以建立自訂內嵌政策，以取得必要的許可，讓 Amazon DataZone 代表您在 AWS 管理主控台中建立必要的角色。

1. 登入 AWS 管理主控台，然後開啟 IAM 主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在導覽窗格中，選擇群組或使用者。
3. 在清單中，選擇要內嵌政策的使用者或群組名稱。
4. 選擇 Permissions (許可) 索引標籤，並在必要時，展開 Permissions policies (許可政策) 部分。
5. 選擇新增權限和建立內嵌原則連結。
6. 在「建立策略」畫面的「策略編輯器」區段中，選擇「JSON」。

   使用下列 JSON 陳述式建立政策文件，然後選擇 [下一步]。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:CreateRole"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/service-role/AmazonDataZone*",
                "arn:aws:iam::*:role/service-role/AmazonDataZone*"
            ]
        },
        {
            "Effect": "Allow",
```

```
            "Action": "iam:AttachRolePolicy",
            "Resource": "arn:aws:iam::*:role/service-role/AmazonDataZone*",
            "Condition": {
                "ArnLike": {
                    "iam:PolicyARN": [
                        "arn:aws:iam::aws:policy/AmazonDataZone*",
                        "arn:aws:iam::*:policy/service-role/AmazonDataZone*"
                    ]
                }
            }
        }
    ]
}
```

7. 在「檢閱策略」畫面上，輸入策略的名稱。當您滿意時，選擇 Create policy (建立政策)。確認畫面頂端的紅色方塊未出現任何錯誤。如出現任何錯誤，請加以修正。

為許可建立自訂政策，以管理與 Amazon DataZone 網域關聯的帳戶

完成下列程序以建立自訂內嵌原則，以在關聯 AWS 帳戶中擁有必要的權限，以列出、接受和拒絕網域的資源共用，然後啟用、設定和停用關聯帳戶中的環境藍圖。若要在藍圖組態期間啟用選用的 Amazon DataZone 服務主控台簡化角色建立，您還必須建立 IAM 許可的自訂政策，以簡化 Amazon DataZone 服務主控台的角色建立 。

1. 登入 AWS 管理主控台，然後開啟 IAM 主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在導覽窗格中，選擇群組或使用者。
3. 在清單中，選擇要內嵌政策的使用者或群組名稱。
4. 選擇 Permissions (許可) 索引標籤，並在必要時，展開 Permissions policies (許可政策) 部分。
5. 選擇新增權限和建立內嵌原則連結。
6. 在「建立策略」畫面的「策略編輯器」區段中，選擇「JSON」。使用下列 JSON 陳述式建立政策文件，然後選擇 [下一步]。

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

```
            "Action": [
                "datazone:ListEnvironmentBlueprintConfigurations",
                "datazone:PutEnvironmentBlueprintConfiguration",
                "datazone:GetDomain",
                "datazone:ListDomains",
                "datazone:GetEnvironmentBlueprintConfiguration",
                "datazone:ListEnvironmentBlueprints",
                "datazone:GetEnvironmentBlueprint",
                "datazone:ListAccountEnvironments",
                "datazone:DeleteEnvironmentBlueprintConfiguration"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::*:role/AmazonDataZone",
                "arn:aws:iam::*:role/service-role/AmazonDataZone*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:passedToService": "datazone.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:AttachRolePolicy",
            "Resource": "arn:aws:iam::*:role/service-role/AmazonDataZone*",
            "Condition": {
                "ArnLike": {
                    "iam:PolicyARN": [
                        "arn:aws:iam::aws:policy/AmazonDataZone*",
                        "arn:aws:iam::*:policy/service-role/AmazonDataZone*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:CreateRole"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/service-role/AmazonDataZone*",
                "arn:aws:iam::*:role/service-role/AmazonDataZone*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ram:AcceptResourceShareInvitation",
                "ram:RejectResourceShareInvitation",
                "ram:GetResourceShareInvitations"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:CreateBucket",
            "Resource": "arn:aws:s3:::amazon-datazone*"
        }
    ]
}
```

7. 在「檢閱策略」畫面上，輸入策略的名稱。當您滿意時，選擇 Create policy (建立政策)。確認畫面頂端的紅色方塊未出現任何錯誤。如出現任何錯誤，請加以修正。

(選擇性) 建立 AWS 身分識別中心權限的自訂原則，以便為您的網域啟用單一登入 (SSO)

完成下列程序以建立自訂內嵌政策，以取得使用 Amazon 中的 AWS IAM 身分中心啟用單一登入 (SSO) 的必要許可 DataZone。

1. 登入 AWS 管理主控台，然後開啟 IAM 主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在導覽窗格中，選擇群組或使用者。
3. 在清單中，選擇要內嵌政策的使用者或群組名稱。
4. 選擇 Permissions (許可) 索引標籤，並在必要時，展開 Permissions policies (許可政策) 部分。
5. 選擇 [新增權限] 和 [建立內嵌原則]
6. 在「建立策略」畫面的「策略編輯器」區段中，選擇「JSON」。

   使用下列 JSON 陳述式建立政策文件，然後選擇 [下一步]。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DeleteManagedApplicationInstance",
                "sso:CreateManagedApplicationInstance",
                "sso:PutApplicationAssignmentConfiguration"
            ],
            "Resource": "*"
        }
    ]
}
```

7. 在「檢閱策略」畫面上，輸入策略的名稱。當您滿意時，選擇 Create policy (建立政策)。確認畫面頂端的紅色方塊未出現任何錯誤。如出現任何錯誤，請加以修正。

(選擇性) 為 AWS 身分識別中心許可建立自訂政策，以新增和移除對 Amazon DataZone 網域的 SSO 使用者和 SSO 群組存取權。

完成下列程序以建立自訂內嵌政策，以取得新增和移除 Amazon DataZone 網域的 SSO 使用者和 SSO 群組存取權限的必要許可。

1. 登入 AWS 管理主控台，然後開啟 IAM 主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在導覽窗格中，選擇群組或使用者。
3. 在清單中，選擇要內嵌政策的使用者或群組名稱。
4. 選擇 Permissions (許可) 索引標籤，並在必要時，展開 Permissions policies (許可政策) 部分。
5. 選擇 [新增權限] 和 [建立內嵌原則]
6. 在「建立策略」畫面的「策略編輯器」區段中，選擇「JSON」。

   使用下列 JSON 陳述式建立政策文件，然後選擇 [下一步]。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:GetManagedApplicationInstance",
        "sso:ListProfiles",
        "sso:GetProfiles",
        "sso:AssociateProfile",
        "sso:DisassociateProfile",
        "sso:GetProfile"
      ],
      "Resource": "*"
    }
  ]
}
```

7. 在「檢閱策略」畫面上，輸入策略的名稱。當您滿意時，選擇 Create policy (建立政策)。確認畫面頂端的紅色方塊未出現任何錯誤。如出現任何錯誤，請加以修正。

(選擇性) 將 IAM 主體新增為金鑰使用者，以使用金鑰管理服務 (KMS) 的客戶管理金 AWS 鑰建立 Amazon DataZone 網域

在您可以選擇性地從金鑰管理服務 (KMS) 使用客戶管理金 AWS 鑰 (CMK) 建立 Amazon DataZone 網域之前，請完成以下程序，讓 IAM 主體成為 KMS 金鑰的使用者。

1. 登入 AWS 管理主控台，然後開啟 KMS 主控台，網址為 https://console.aws.amazon.com/kms/。
2. 若要檢視您所建立及管理帳戶中的金鑰，請在導覽窗格中選擇Customer managed keys (客戶受管金鑰)。
3. 在 KMS 金鑰清單中，選擇您要檢查之 KMS 金鑰的別名或金鑰 ID。
4. 若要新增或移除金鑰使用者，以及允許或禁止外部 AWS 帳戶使用 KMS 金鑰，請使用頁面 [金鑰使用者] 區段中的控制項。金鑰使用者可以在密碼編譯操作中使用 KMS 金鑰，例如加密、解密、重新加密和產生資料金鑰。

設定使用 Amazon DataZone 資料入口網站所需的 IAM 許可

任何想要使用 Amazon DataZone 資料入口網站或目錄的使用者、群組或角色都必須具有必要的許可。

主題

- 將必要的政策附加到使用者、群組或角色，以存取 Amazon DataZone 資料入口網站
- 將必要的政策附加到 Amazon DataZone 目錄存取的使用者、群組或角色
- 如果您的網域使用金鑰管理服務 (KMS) 的客戶管理金鑰加密，則將選用政策附加至 Amazon DataZone 資料入口網站或目錄存取的使用者、群組或角色 AWS

將必要的政策附加到使用者、群組或角色，以存取 Amazon DataZone 資料入口網站

您可以使用登入 DataZone 資料或單一登入 (SSO) AWS 登入資料存取 Amazon 資料入口網站。依照以下章節中的指示設定使用您的 AWS 認證存取資料入口網站所需的權限。如需將 Amazon DataZone 與 SSO 搭配使用的詳細資訊，請參閱為 Amazon 設置 AWS IAM 身份中心 DataZone。

> **Note**
>
> 只有您網域 AWS 帳戶中的 IAM 主體可以存取網域的資料入口網站。來自其他 AWS 帳戶的 IAM 主體無法存取網域的資料入口網站。

完成下列程序，將必要的原則附加至使用者、群組或角色。如需詳細資訊，請參閱 AWS Amazon 的受管政策 DataZone。

1. 登入 AWS 管理主控台，然後開啟 IAM 主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在導覽窗格中，選擇 [使用者]、[使用者群組] 或 [角色]。
3. 在清單中，選擇要內嵌政策的使用者、群組或角色名稱。
4. 選擇 Permissions (許可) 索引標籤，並在必要時，展開 Permissions policies (許可政策) 部分。
5. 選擇新增權限和建立內嵌原則連結。
6. 在「建立策略」畫面的「策略編輯器」區段中，選擇「JSON」。使用下列 JSON 陳述式建立政策文件，然後選擇 [下一步]。

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

7. 在「檢閱策略」畫面上，輸入策略的名稱。當您滿意時，選擇 Create policy (建立政策)。確認畫面頂端的紅色方塊未出現任何錯誤。如出現任何錯誤，請加以修正。

將必要的政策附加到 Amazon DataZone 目錄存取的使用者、群組或角色

> **Note**
>
> 只有您網域 AWS 帳戶中的 IAM 主體可以存取網域的目錄。來自其他 AWS 帳戶的 IAM 主體無法存取網域的目錄。

您可以使用下列程序透過 API 和開發套件授與 IAM 身分存取您 Amazon DataZone 網域目錄的存取權。如果您希望這些 IAM 身分也能存取 Amazon 資 DataZone 料入口網站，請另外遵循上述程序將必要的政策附加到使用者、群組或角色，以存取 Amazon DataZone 資料入口網站。如需詳細資訊，請參閱 AWS Amazon 的受管政策 DataZone。

1. 登入 AWS 管理主控台，然後開啟 IAM 主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在導覽窗格中，選擇政策。
3. 在策略清單中，選取AmazonDataZoneFullUserAccess策略旁邊的圓鈕。您可用篩選功能表和搜尋方塊來篩選政策清單。如需更多資訊，請參閱AWS 受管理的策略：AmazonDataZoneFullUserAccess
4. 選擇 Actions (動作)，然後選擇 Attach (連接)。
5. 選取每個主參與者旁邊的核取方塊，選擇要附加原則的使用者、群組或角色。您可用篩選功能表和搜尋方塊來篩選主體實體清單。選擇使用者、群組或角色後，請選擇 [附加原則]。

如果您的網域使用金鑰管理服務 (KMS) 的客戶管理金鑰加密，則將選用政策附加至 Amazon DataZone 資料入口網站或目錄存取的使用者、群組或角色 AWS

如果您使用自己的 KMS 金鑰建立 Amazon DataZone 網域以進行資料加密，則還必須建立具有下列許可的內嵌政策，並將其附加到 IAM 主體，以便他們可以存取 Amazon DataZone 資料入口網站或目錄。

1. 登入 AWS 管理主控台，然後開啟 IAM 主控台，網址為 https://console.aws.amazon.com/iam/。
2. 在導覽窗格中，選擇 [使用者]、[使用者群組] 或 [角色]。
3. 在清單中，選擇要內嵌政策的使用者、群組或角色名稱。
4. 選擇 Permissions (許可) 索引標籤，並在必要時，展開 Permissions policies (許可政策) 部分。
5. 選擇新增權限和建立內嵌原則連結。
6. 在「建立策略」畫面的「策略編輯器」區段中，選擇「JSON」。使用下列 JSON 陳述式建立政策文件，然後選擇 [下一步]。

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

```
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

7. 在「檢閱策略」畫面上，輸入策略的名稱。當您滿意時，選擇 Create policy (建立政策)。確認畫面頂端的紅色方塊未出現任何錯誤。如出現任何錯誤，請加以修正。

為 Amazon 設置 AWS IAM 身份中心 DataZone

> **Note**
>
> AWS 身分識別中心必須在與您的 Amazon DataZone 網 AWS 域相同的區域中啟用。目前，AWS 身分識別中心只能在單一 AWS 區域中啟用。

您可以使用單一登入 (SSO) 登入 DataZone 資料或 AWS 登入資料存取 Amazon 資料入口網站。請依照本節中的指示設定適用於 Amazon 的 AWS IAM 身分中心 DataZone。如需將 Amazon DataZone 與您的 AWS 登入資料搭配使用的詳細資訊，請參閱設定使用 Amazon DataZone 管理主控台所需的 IAM 許可。

如果您已在要建立 Amazon DataZone 網域的相同 AWS 區域中啟用並設定 AWS IAM 身分中心 (AWS 單一登入的後續任務)，則可以略過本節中的程序。

完成下列程序以啟用 AWS IAM 身分中心 (AWS 單一登入的後續任務)。

1. 若要啟用 AWS IAM 身分中心，您必須使用 Organ AWS izations AWS 管理帳戶的登入資料登入管理主控台。使用 Organ AWS izations 成員帳戶的登入資料登入時，無法啟用 IAM 身分中心。如需詳細資訊，請參閱《組織使用指南》中的〈建立和管理組 Organ AWS izations〉。
2. 開啟 AWS IAM 身分中心 (AWS 單一登入的後續任務) 主控台，然後使用頂端導覽列中的 AWS 區域選擇器來選擇要在其中建立 Amazon DataZone 網域的區域。
3. 選擇 啟用 。

4. 選擇您的身分識別來源。

   根據預設，您會取得 IAM 身分中心存放區，以便快速輕鬆地管理使用者。或者，您可以改為連線外部身分識別提供者。在此程序中，我們會使用預設的 IAM 身分中心存放區。

   如需詳細資訊，請參閱選擇您的身分識別來源。
5. 在 [IAM 身分中心] 瀏覽窗格中，選擇 [群組]，然後選擇 [建立群組]。輸入群組名稱，然後選擇 [建立]。
6. 在 [IAM 身分中心] 瀏覽窗格中，選擇 [使用者]。
7. 在「新增使用者」畫面上，輸入必要資訊，然後選擇「傳送電子郵件給使用者，並附有密碼設定指示」。用戶應收到有關下一個設置步驟的電子郵件。
8. 選擇「下一步：群組」，選擇您要的群組，然後選擇「新增使用者」。使用者應該會收到邀請他們使用 SSO 的電子郵件。在此電子郵件中，他們需要選擇接受邀請並設置密碼。

建立 Amazon DataZone 網域後，您可以啟用 Amazon 的 AWS 身分中心， DataZone 並提供對 SSO 使用者和 SSO 群組的存取權。如需更多詳細資訊，請參閱 啟用 Amazon 的 IAM 身分中心 DataZone。

開始使用

本節中的資訊可協助您開始使用 Amazon DataZone。如果您不熟悉 Amazon 的新手 DataZone，請先熟悉中提供的概念和術語Amazon DataZone 術語和概念。

本入門章節會引導您完成下列 Amazon DataZone 快速入門工作流程：

主題

- Amazon DataZone 快速入門與 AWS Glue 數據
- Amazon DataZone 快速入門與 Amazon Redshift 數據
- Amazon DataZone 快速入門與示例腳本

> **Important**
>
> 在您開始執行這些快速入門工作流程中的步驟之前，您必須完成本指南〈設定〉一節中所述的程序。如果您使用的是全新 AWS 帳戶，則必須設定使用 Amazon DataZone 管理主控台所需的許可。如果您使用的 AWS 帳戶具有現有的 AWS Glue 資料目錄物件，則還必須設定 Amazon 的 Lake Formation 許可 DataZone。

Amazon DataZone 快速入門與 AWS Glue 數據

主題

- 步驟 1-建立 Amazon DataZone 網域和資料入口網站
- 步驟 2-建立發佈專案
- 第 3 步-創建環境
- 第 4 步-生成用於發布的數據
- 第 5 步-從 AWS Glue 收集元數據
- 步驟 6-組織和發佈資料資產
- 第 7 步-創建用於數據分析的項目
- 第 8 步-創建用於數據分析的環境
- 步驟 9-搜尋資料目錄並訂閱資料

- 步驟 10-核准訂閱要求
- 第 11 步-在 Amazon Athena 建立查詢和分析數據

步驟 1-建立 Amazon DataZone 網域和資料入口網站

本節說明為此工作流程建立 Amazon DataZone 網域和資料入口網站的步驟。

請完成以下程序來建立 Amazon DataZone 網域。如需 Amazon DataZone 網域的詳細資訊，請參閱Amazon DataZone 術語和概念。

1. 在 https://console.aws.amazon.com/datazone 瀏覽至 Amazon DataZone 主控台，登入，然後選擇「建立網域」。

   > **Note**
   >
   > 如果您想要在此工作流程中使用現有的 Amazon DataZone 網域，請選擇 [檢視網域]，然後選擇要使用的網域，然後繼續建立發佈專案的步驟 2。

2. 在 [建立網域] 頁面上，提供下列欄位的值：

   - 名稱-指定網域的名稱。對於此工作流程的目的，您可以調用此域營銷。
   - 說明-指定選擇性的網域描述。
   - 數據加密-默認情況下，您的數據使用為您 AWS 擁有和管理的密鑰進行加密。對於此使用案例，您可以保留預設的資料加密設定。

     如需使用客戶受管金鑰的詳細資訊，請參閱適用於 Amazon 的靜態資料加密 DataZone。如果您使用自己的 KMS 金鑰進行資料加密，則必須在預設值中包含下列陳述式AmazonDataZoneDomainExecutionRole。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
```

```
      "Resource": "*"
    }
  ]
}
```

- 服務存取-預設情況下保持選取 [使用預設角色] 選項不變。

> **Note**
>
> 如果您在此工作流程中使用現有的 Amazon DataZone 網域，可以選擇「使用現有的服務角色」選項，然後從下拉式功能表中選擇現有角色。

- 在 [快速設定] 下方，選擇 [設定此帳戶以供資料使用和發佈]。此選項可啟用資料湖和資料倉儲的內建 Amazon DataZone 藍圖，並為此帳戶設定所需的許可、資源、預設專案以及預設資料湖和資料倉儲環境設定檔。如需 Amazon DataZone 藍圖的詳細資訊，請參閱Amazon DataZone 術語和概念。
- 保持權限詳細信息下的其餘字段不變。

> **Note**
>
> 如果您有現有的 Amazon DataZone 網域，可以選擇使用現有的服務角色選項，然後從 Glue 管理存取角色、Redshift 管理存取角色和佈建角色的下拉式功能表中選擇現有角色。

- 保持「標籤」下的欄位不變。
- 選擇建立網域。

3. 成功建立網域後，請選擇此網域，然後在網域的摘要頁面上記下此網域的資料入口網站 URL。您可以使用此 URL 存取 Amazon 資 DataZone 料入口網站，以完成此工作流程的其餘步驟。您也可以選擇開放資料入口網站來導覽至資料入口網站。

> **Note**
>
> 在目前版本的 Amazon 中 DataZone，一旦建立網域，就無法修改為資料入口網站產生的 URL。

網域建立可能需要幾分鐘的時間才能完成。請等候網域的狀態為 [可用]，然後再繼續進行下一個步驟。

步驟 2-建立發佈專案

本節描述為此工作流程建立發佈專案所需的步驟。

1. 一旦你完成上面的步驟 1 並創建一個域名，你會看到歡迎來到 Amazon DataZone！ 窗口。在此視窗中，選擇 [建立專案]。
2. 指定專案名稱，例如，對於此工作流程，您可以為其命名 SalesDataPublishingProject，然後將其餘欄位保持不變，然後選擇 [建立]。

第 3 步-創建環境

本節說明為此工作流程建立環境所需的步驟。

1. 完成上面的步驟 2 並創建項目後，您將看到「您的項目已準備就緒可以使用」窗口。在此視窗中，選擇 [建立環境]。
2. 在 [建立環境] 頁面上，指定下列項目，然後選擇 [建立環境]。
3. 指定下列項目的值：
   - 名稱-指定環境的名稱。對於本逐步解說，您可以呼叫它`Default data lake environment`。
   - 描述-指定環境的描述。
   - 環境設定檔-選擇DataLakeProfile環境設定檔。這可讓您在此工作流程 DataZone 中使用 Amazon 來處理 Amazon S3、 AWS Glue 目錄和亞馬 Amazon Athena 中的資料。
   - 對於此逐步解說，請保持其餘欄位不變。
4. 選擇 Create environment (建立環境)。

第 4 步-生成用於發布的數據

本節描述產生資料以在此工作流程中發佈所需的步驟。

1. 完成上述步驟 3 之後，請在`SalesDataPublishingProject`專案的右側面板的「分析工具」下選擇 Amazon Athena。這會開啟 Athena 查詢編輯器，使用專案的認證進行驗證。請確定已在 Amazon 環境下拉式清單中選取您的發佈 DataZone 環境，並在查詢編輯器中選取`<environment_name>%_pub_db`資料庫。

2. 在本逐步解說中，您使用「將資料表建立為選取項目」 (CTAS) 查詢指令碼建立要發佈到 Amazon DataZone 的新資料表。在您的查詢編輯器中，執行此 CTAS 指令碼以建立您可以發佈的`mkt_sls_table`資料表，並可供搜尋和訂閱使用。

```
CREATE TABLE mkt_sls_table AS
SELECT 146776932 AS ord_num, 23 AS sales_qty_sld, 23.4 AS wholesale_cost, 45.0 as
 lst_pr, 43.0 as sell_pr, 2.0 as disnt, 12 as ship_mode,13 as warehouse_id, 23 as
 item_id, 34 as ctlg_page, 232 as ship_cust_id, 4556 as bill_cust_id
UNION ALL SELECT 46776931, 24, 24.4, 46, 44, 1, 14, 15, 24, 35, 222, 4551
UNION ALL SELECT 46777394, 42, 43.4, 60, 50, 10, 30, 20, 27, 43, 241, 4565
UNION ALL SELECT 46777831, 33, 40.4, 51, 46, 15, 16, 26, 33, 40, 234, 4563
UNION ALL SELECT 46779160, 29, 26.4, 50, 61, 8, 31, 15, 36, 40, 242, 4562
UNION ALL SELECT 46778595, 43, 28.4, 49, 47, 7, 28, 22, 27, 43, 224, 4555
UNION ALL SELECT 46779482, 34, 33.4, 64, 44, 10, 17, 27, 43, 52, 222, 4556
UNION ALL SELECT 46779650, 39, 37.4, 51, 62, 13, 31, 25, 31, 52, 224, 4551
UNION ALL SELECT 46780524, 33, 40.4, 60, 53, 18, 32, 31, 31, 39, 232, 4563
UNION ALL SELECT 46780634, 39, 35.4, 46, 44, 16, 33, 19, 31, 52, 242, 4557
UNION ALL SELECT 46781887, 24, 30.4, 54, 62, 13, 18, 29, 24, 52, 223, 4561
```

請確定已在左側的 [資料表和檢視表] 區段中成功建立 mkt_sls_ table 資料表。現在您擁有可以發佈到 Amazon DataZone 目錄中的資料資產。

第 5 步-從 AWS Glue 收集元數據

本節說明從 AWS Glue 針對此工作流程收集中繼資料的步驟。

1. 完成上述步驟 4 後，在 Amazon DataZone 資料入口網站中選擇`SalesDataPublishingProject`專案，然後選擇 [資料] 索引標籤，然後選擇左側面板中的 [資料來源]。
2. 選擇作為環境建立程序一部分而建立的來源。
3. 選擇 [動作] 下拉式功能表旁的 [執行]，然後選擇 [重新整理] 按鈕 資料來源執行完成後，資產就會新增至 Amazon DataZone 庫存。

步驟 6-組織和發佈資料資產

本節說明在此工作流程中策劃和發佈資料資產的步驟。

1. 完成上述步驟 5 後，在 Amazon DataZone 資料入口網站中，選擇您在上一步中建立的SalesDataPublishingProject專案，選擇 [資料] 索引標籤，在左側面板中選擇 [庫存資料]，然後找到mkt_sls_table表格。
2. 開啟mkt_sls_table資產的詳細資料頁面，查看自動產生的商家名稱。選擇「自動產生的中繼資料」圖示，以檢視資產和欄的自動產生名稱。您可以個別接受或拒絕每個名稱，或選擇全部接受以套用產生的名稱。或者，您也可以將可用的中繼資料表單新增至資產，並選取詞彙詞彙來分類資料。
3. 選擇「發佈資產」以發佈mkt_sls_table資產。

第 7 步-創建用於數據分析的項目

本節說明建立專案以進行資料分析的步驟。這是此工作流程之資料取用者步驟的開始。

1. 完成上述步驟 6 後，在 Amazon DataZone 資料入口網站中，從「專案」下拉式功能表中選擇「建立專案」。
2. 在 [建立專案] 頁面上，指定專案名稱，例如，對於此工作流程，您可以為其命名 MarketingDataAnalysisProject，然後將其餘欄位保持不變，然後選擇 [建立]。

第 8 步-創建用於數據分析的環境

本節說明建立資料分析環境的步驟。

1. 完成上述步驟 7 後，在 Amazon DataZone 資料入口網站中選擇MarketingDataAnalysisProject專案，然後選擇「環境」索引標籤，然後選擇「建立環境」。
2. 在 [建立環境] 頁面上，指定下列項目，然後選擇 [建立環境]。
   - 名稱-指定環境的名稱。對於本逐步解說，您可以呼叫它Default data lake environment。
   - 描述-指定環境的描述。
   - 環境設定檔-選擇內建的DataLakeProfile環境設定檔。
   - 對於此逐步解說，請保持其餘欄位不變。

步驟 9-搜尋資料目錄並訂閱資料

本節說明搜尋資料目錄和訂閱資料的步驟。

1. 完成上述步驟 8 後，在 Amazon 資 DataZone 料入口網站中選擇 Amazon DataZone 圖示，然後在 Amazon DataZone 搜尋欄位中，在資料入口網站的搜尋列中使用關鍵字 (例如「目錄」或「銷售」) 搜尋資料資產。

   如有必要，請套用篩選或排序，找到「產品銷售資料」資產後，您可以選擇它來開啟資產的詳細資訊頁面。
2. 在「目錄銷售資料」資產的詳細資料頁面上，選擇「訂閱」。
3. 在 [訂閱] 對話方塊中，從下拉式清單中選擇您的MarketingDataAnalysisProject消費者專案，然後指定訂閱要求的原因，然後選擇 [訂閱]。

步驟 10-核准訂閱要求

本節說明核准訂閱要求的步驟。

1. 完成上述步驟 9 後，請在 Amazon 資 DataZone 料入口網站中選擇您發佈資產時所使用的SalesDataPublishingProject專案。
2. 依序選擇 [資料] 索引標籤、[已發佈的資料]，然後選擇 [內送要求
3. 現在，您可以看到需要核准的新請求的列。選擇「檢視請求」。提供核准的理由，然後選擇「核准」。

第 11 步-在 Amazon Athena 建立查詢和分析數據

現在，您已成功將資產發佈到 Amazon DataZone 目錄並訂閱，您可以對其進行分析。

1. 在 Amazon DataZone 資料入口網站中，選擇您的MarketingDataAnalysisProject消費者專案，然後從右側面板的分析工具下，選擇與 Amazon Athena 的查詢資料連結。這會開啟 Amazon Athena 查詢編輯器，使用您專案的登入資料進行身份驗證。從查詢編輯器的 Amazon 環 DataZone 境下拉式清單中選擇MarketingDataAnalysisProject消費者環境，然後<environment_name>%sub_db從資料庫下拉式清單中選擇您的專案。
2. 您現在可以在訂閱的資料表上執行查詢。您可以從 [表格和檢視表] 中選擇表格，然後選擇 [預覽]，在編輯器畫面上顯示 select 陳述式。執行查詢以查看結果。

Amazon DataZone 快速入門與 Amazon Redshift 數據

主題

步驟 1-建立 Amazon DataZone 網域和資料入口網站

請完成以下程序來建立 Amazon DataZone 網域。如需 Amazon DataZone 網域的詳細資訊，請參閱Amazon DataZone 術語和概念。

1. 在 https://console.aws.amazon.com/datazone 瀏覽至 Amazon DataZone 主控台，登入，然後選擇「建立網域」。

   > **Note**
   >
   > 如果您想要在此工作流程中使用現有的 Amazon DataZone 網域，請選擇 [檢視網域]，然後選擇要使用的網域，然後繼續建立發佈專案的步驟 2。

2. 在 [建立網域] 頁面上，提供下列欄位的值：

   - 名稱-指定網域的名稱。基於此工作流程的目的，您可以呼叫此網域`Marketing`。
   - 說明-指定選擇性的網域描述。
   - 數據加密-默認情況下，您的數據使用為您 AWS 擁有和管理的密鑰進行加密。在本逐步解說中，您可以保留預設的資料加密設定。

如需使用客戶受管金鑰的詳細資訊，請參閱適用於 Amazon 的靜態資料加密 DataZone。
如果您使用自己的 KMS 金鑰進行資料加密，則必須在預設值中包含下列陳述
式AmazonDataZoneDomainExecutionRole。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*"
    }
  ]
}
```

- 服務存取-選擇 [使用自訂服務角色] 選項，然後AmazonDataZoneDomainExecutionRole從下拉式功能表中選擇。
- 在 [快速設定] 下方，選擇 [設定此帳戶以供資料使用和發佈]。此選項可啟用資料湖和資料倉儲的內建 Amazon DataZone 藍圖，並設定必要的許可和資源，以完成此工作流程中的其餘步驟。如需 Amazon DataZone 藍圖的詳細資訊，請參閱Amazon DataZone 術語和概念。
- 保持 [權限詳細資料] 和 [標籤] 下的其餘欄位不變，然後選擇 [建立網域

3. 成功建立網域後，請選擇此網域，然後在網域的摘要頁面上記下此網域的資料入口網站 URL。您可以使用此 URL 存取 Amazon 資 DataZone 料入口網站，以完成此工作流程的其餘步驟。

> **Note**
>
> 在目前版本的 Amazon 中 DataZone，一旦建立網域，就無法修改為資料入口網站產生的 URL。

網域建立可能需要幾分鐘的時間才能完成。請等候網域的狀態為 [可用]，然後再繼續進行下一個步驟。

步驟 2-建立發佈專案

下節說明在此工作流程中建立發佈專案的步驟。

1. 完成步驟 1 後，使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用單一登入 (SSO) 或 AWS IAM 登入資料登入。
2. 選擇 [建立專案]，指定專案名稱，例如，對於此工作流程，您可以為其命名 SalesDataPublishingProject，然後將其餘欄位保持不變，然後選擇 [建立]。

第 3 步-創建環境

下節說明在此工作流程中建立環境的步驟。

1. 完成步驟 2 後，在 Amazon DataZone 資料入口網站中選擇您在上一步中建立的`SalesDataPublishingProject`專案，然後選擇 [環境] 索引標籤，然後選擇 [建立環境]。
2. 在 [建立環境] 頁面上，指定下列項目，然後選擇 [建立環境]。
   - 名稱-指定環境的名稱。對於本逐步解說，您可以呼叫它`Default data warehouse environment`。
   - 描述-指定環境的描述。
   - 環境設定檔-選擇DataWarehouseProfile環境設定檔。
   - 為儲存資料的 Amazon Redshift 叢集提供您的 Amazon Redshift 叢集的名稱、資料庫名稱和秘密 ARN。

> **Note**
>
> 請確定您在 Sec AWS rets Manager 中的密碼包含下列標籤 (機碼/值)：
>
> - 對於 Amazon Redshift 集群-數據集群：<cluster_name:database name>
>
> 對於 Amazon Redshift 無伺服器工作群組-資料機. 工作群組：<workgroup_name:database_name>
> - AmazonDataZoneProject: <projectID>
> - AmazonDataZoneDomain: <domainID>
>
> 如需詳細資訊，請參閱在 AWS Secrets Manager 中儲存資料庫認證。
> 您在 AWS Secrets Manager 中提供的資料庫使用者必須具有超級使用者權限。

第 4 步-生成用於發布的數據

下節說明產生資料以在此工作流程中發佈的步驟。

1. 完成步驟 3 後，在 Amazon DataZone 資料入口網站中選擇SalesDataPublishingProject專案，然後在右側面板的「分析工具」下選擇 Amazon Redshift。這會開啟 Amazon Redshift 查詢編輯器，並使用專案的登入資料進行身份驗證。
2. 在本逐步解說中，您使用「將資料表建立為選取項目」 (CTAS) 查詢指令碼建立要發佈到 Amazon DataZone 的新資料表。在您的查詢編輯器中，執行此 CTAS 指令碼以建立您可以發佈的mkt_sls_table資料表，並可供搜尋和訂閱使用。

```
CREATE TABLE mkt_sls_table AS
SELECT 146776932 AS ord_num, 23 AS sales_qty_sld, 23.4 AS wholesale_cost, 45.0 as
 lst_pr, 43.0 as sell_pr, 2.0 as disnt, 12 as ship_mode,13 as warehouse_id, 23 as
 item_id, 34 as ctlg_page, 232 as ship_cust_id, 4556 as bill_cust_id
UNION ALL SELECT 46776931, 24, 24.4, 46, 44, 1, 14, 15, 24, 35, 222, 4551
UNION ALL SELECT 46777394, 42, 43.4, 60, 50, 10, 30, 20, 27, 43, 241, 4565
UNION ALL SELECT 46777831, 33, 40.4, 51, 46, 15, 16, 26, 33, 40, 234, 4563
UNION ALL SELECT 46779160, 29, 26.4, 50, 61, 8, 31, 15, 36, 40, 242, 4562
UNION ALL SELECT 46778595, 43, 28.4, 49, 47, 7, 28, 22, 27, 43, 224, 4555
UNION ALL SELECT 46779482, 34, 33.4, 64, 44, 10, 17, 27, 43, 52, 222, 4556
UNION ALL SELECT 46779650, 39, 37.4, 51, 62, 13, 31, 25, 31, 52, 224, 4551
UNION ALL SELECT 46780524, 33, 40.4, 60, 53, 18, 32, 31, 31, 39, 232, 4563
UNION ALL SELECT 46780634, 39, 35.4, 46, 44, 16, 33, 19, 31, 52, 242, 4557
UNION ALL SELECT 46781887, 24, 30.4, 54, 62, 13, 18, 29, 24, 52, 223, 4561
```

請確定已成功建立 mkt_sls_table 資料表。現在您擁有可以發佈到 Amazon DataZone 目錄中的資料資產。

第 5 步-從 Amazon Redshift 收集元數據

下一節說明從 Amazon Redshift 收集中繼資料的步驟。

1. 完成步驟 4 後，在 Amazon DataZone 資料入口網站中選擇SalesDataPublishingProject專案，然後選擇 [資料] 索引標籤，然後選擇 [資料來源]。
2. 選擇作為環境建立程序一部分而建立的來源。

3. 選擇 [動作] 下拉式功能表旁的 [執行]，然後選擇 [重新整理] 按鈕 資料來源執行完成後，資產就會新增至 Amazon DataZone 庫存。

步驟 6-組織和發佈資料資產

下節描述在此工作流程中策劃和發佈資料資產的步驟。

1. 完成步驟 5 後，在 Amazon DataZone 資料入口網站中選擇SalesDataPublishingProject專案，然後選擇「資料」索引標籤，選擇「庫存資料」，然後找到mkt_sls_table表格。
2. 開啟mkt_sls_table資產的詳細資料頁面，查看自動產生的商家名稱。選擇「自動產生的中繼資料」圖示，以檢視資產和欄的自動產生名稱。您可以個別接受或拒絕每個名稱，或選擇全部接受以套用產生的名稱。或者，您也可以將可用的中繼資料表單新增至資產，並選取詞彙詞彙來分類資料。
3. 選擇「發佈」以發佈mkt_sls_table資產。

第 7 步-創建用於數據分析的項目

下一節說明在此工作流程中建立 te 專案以進行資料分析的步驟。

1. 完成步驟 6 後，請在 Amazon DataZone 資料入口網站中選擇建立專案。
2. 在 [建立專案] 頁面中，指定專案名稱，例如，對於此工作流程，您可以為其命名 MarketingDataAnalysisProject，然後將其餘欄位保持不變，然後選擇 [建立]。

第 8 步-創建用於數據分析的環境

下節說明在此工作流程中建立資料分析環境的步驟。

1. 完成步驟 7 後，在 Amazon DataZone 資料入口網站中，選擇您在上一步中建立的MarketingDataAnalysisProject專案，然後選擇 [環境] 索引標籤，然後選擇 [新增環境]。
2. 在 [建立環境] 頁面上，指定下列項目，然後選擇 [建立環境]。
   - 名稱-指定環境的名稱。對於本逐步解說，您可以呼叫它Default data warehouse environment。
   - 描述-指定環境的描述。
   - 環境設定檔-選擇DataWarehouseProfile環境設定檔。

- 為儲存資料的 Amazon Redshift 叢集提供您的 Amazon Redshift 叢集的名稱、資料庫名稱和秘密 ARN。

> **Note**
>
> 請確定您在 Sec AWS rets Manager 中的密碼包含下列標籤 (機碼/值)：
>
> - 對於 Amazon Redshift 集群-數據集群：<cluster_name:database name>
>
> 對於 Amazon Redshift 無伺服器工作群組-資料機. 工作群組：<workgroup_name:database_name>
>
> - AmazonDataZoneProject: <projectID>
> - AmazonDataZoneDomain: <domainID>
>
> 如需詳細資訊，請參閱在 AWS Secrets Manager 中儲存資料庫認證。
> 您在 AWS Secrets Manager 中提供的資料庫使用者必須具有超級使用者權限。

- 對於此逐步解說，請保持其餘欄位不變。

步驟 9-搜尋資料目錄並訂閱資料

下節介紹搜尋資料目錄和訂閱資料的步驟。

1. 完成步驟 8 後，在 Amazon 資 DataZone 料入口網站中，使用資料入口網站的搜尋列中的關鍵字 (例如「目錄」或「銷售」) 搜尋資料資產。

   如有必要，請套用篩選或排序，找到「產品銷售資料」資產後，您可以選擇它來開啟資產的詳細資訊頁面。
2. 在「產品銷售資料」資產的詳細資料頁面上，選擇「訂閱」。
3. 在對話方塊中，從下拉式清單中選擇您的消費者專案，提供存取要求的原因，然後選擇 [訂閱]。

步驟 10-核准訂閱要求

下節說明在此工作流程中核准訂閱要求的步驟。

1. 完成步驟 9 後，請在 Amazon 資 DataZone 料入口網站中選擇您發佈資產時所使用的SalesDataPublishingProject專案。
2. 依序選擇 [資料] 索引標籤、[已發佈的資料] 和 [內送要求]。

3. 選擇檢視請求連結，然後選擇「核准」。

第 11 步-在 Amazon Redshift 建立查詢和分析數據

現在，您已成功將資產發佈到 Amazon DataZone 目錄並訂閱，您可以對其進行分析。

1. 在 Amazon 資 DataZone 料入口網站的右側面板上，按一下 Amazon Redshift 連結。這會開啟 Amazon Redshift 查詢編輯器，使用專案的登入資料進行身份驗證。
2. 您現在可以在訂閱的資料表上執行查詢 (select 陳述式)。您可以單擊表格（three-vertical-dots 選項），然後選擇預覽以在編輯器屏幕上顯示 select 語句。執行查詢以查看結果。

Amazon DataZone 快速入門與示例腳本

下節說明範例指令碼，這些指令碼會叫用各種 Amazon DataZone API 來完成下列任務：

主題

- 建立 Amazon DataZone 網域和資料入口網站
- 建立發佈專案
- 建立環境設定檔
- 建立環境
- 從 AWS Glue 收集中繼資料
- 組織和發佈資料資產
- 搜尋資料目錄並訂閱資料
- 其他有用的範例腳本

建立 Amazon DataZone 網域和資料入口網站

您可以使用下列範例指令碼建立 Amazon DataZone 網域。如需 Amazon DataZone 網域的詳細資訊，請參閱Amazon DataZone 術語和概念。

```
import sys
import boto3

// Initialize datazone client
region = 'us-east-1'
```

```
dzclient = boto3.client(service_name='datazone', region_name='us-east-1')

// Create DataZone domain
def create_domain(name):
    return dzclient.create_domain(
        name = name,
        description = "this is a description",
        domainExecutionRole = "arn:aws:iam::<account>:role/
AmazonDataZoneDomainExecutionRole",
    )
```

建立發佈專案

您可以使用下列範例指令碼在 Amazon 中建立發佈專案 DataZone。

```
// Create Project
def create_project(domainId):
    return dzclient.create_project(
        domainIdentifier = domainId,
        name = "sample-project"
    )
```

建立環境設定檔

您可以使用下列範例指令碼在 Amazon 中建立環境設定檔 DataZone。

呼叫 `CreateEnvironmentProfile` API 時會使用此範例承載：

```
Sample Payload
{
    "Content":{
        "project_name": "Admin_project",
        "domain_name": "Drug-Research-and-Development",
        "blueprint_account_region": [
            {
                "blueprint_name": "DefaultDataLake",
                "account_id": ["066535990535",
                "413878397724",
                "676266385322",
```

```
                "747721550195",
                "755347404384"
                ],
                "region": ["us-west-2", "us-east-1"]
            },
            {
                "blueprint_name": "DefaultDataWarehouse",
                "account_id": ["066535990535",
                "413878397724",
                "676266385322",
                "747721550195",
                "755347404384"
                ],
                "region":["us-west-2", "us-east-1"]
            }
        ]
    }
}
```

此範例指令碼會叫用 `CreateEnvironmentProfile` API：

```
def create_environment_profile(domain_id, project_id, env_blueprints)
        try:
            response = dz.list_environment_blueprints(
                domainIdentifier=domain_id,
                managed=True
            )
            env_blueprints = response.get("items")
            env_blueprints_map = {}
            for i in env_blueprints:
                env_blueprints_map[i["name"]] = i['id']

            print("Environment Blueprint map", env_blueprints_map)
            for i in blueprint_account_region:
                print(i)
                for j in i["account_id"]:
                    for k in i["region"]:
                        print("The env blueprint name is", i['blueprint_name'])
                        dz.create_environment_profile(
                            description='This is a test environment profile created via
 lambda function',
```

```
                            domainIdentifier=domain_id,
                            awsAccountId=j,
                            awsAccountRegion=k,

 environmentBlueprintIdentifier=env_blueprints_map.get(i["blueprint_name"]),
                            name=i["blueprint_name"] + j + k + "_profile",
                            projectIdentifier=project_id
                        )
        except Exception as e:
            print("Failed to created Environment Profile")
            raise e
```

這是調用 CreateEnvironmentProfile API 後的示例輸出有效負載：

```
{
    "Content":{
        "project_name": "Admin_project",
        "domain_name": "Drug-Research-and-Development",
        "blueprint_account_region": [
            {
                "blueprint_name": "DefaultDataWarehouse",
                "account_id": ["111111111111"],
                "region":["us-west-2"],
                "user_parameters":[
                    {
                        "name": "dataAccessSecretsArn",
                        "value": ""
                    }
                ]
            }
        ]
    }
}
```

建立環境

您可以使用下列範例指令碼在 Amazon 中建立環境 DataZone。

```
def create_environment(domain_id, project_id,blueprint_account_region ):
```

```
         try:
            #refer to get_domain_id and get_project_id for fetching ids using names.
            sts_client = boto3.client("sts")
            # Get the current account ID
            account_id = sts_client.get_caller_identity()["Account"]
            print("Fetching environment profile ids")
            env_profile_map = get_env_profile_map(domain_id, project_id)

            for i in blueprint_account_region:
                for j in i["account_id"]:
                    for k in i["region"]:
                        print(" env blueprint name", i['blueprint_name'])
                        profile_name = i["blueprint_name"] + j + k + "_profile"
                        env_name = i["blueprint_name"] + j + k + "_env"
                        description = f'This is environment is created for
{profile_name}, Account {account_id} and region {i["region"]}'
                        try:
                            dz.create_environment(
                                description=description,
                                domainIdentifier=domain_id,

environmentProfileIdentifier=env_profile_map.get(profile_name),
                                name=env_name,
                                projectIdentifier=project_id
                            )
                            print(f"Environment created - {env_name}")
                        except:
                            dz.create_environment(
                                description=description,
                                domainIdentifier=domain_id,

environmentProfileIdentifier=env_profile_map.get(profile_name),
                                name=env_name,
                                projectIdentifier=project_id,
                                userParameters= i["user_parameters"]
                            )
                            print(f"Environment created - {env_name}")
       except Exception as e:
            print("Failed to created Environment")
            raise e
```

從 AWS Glue 收集中繼資料

您可以使用此範例指令碼從 AWS Glue 收集中繼資料。此指令碼會依標準排程執行。您可以從範例指令碼擷取參數，並使其成為全域參數。使用標準函數擷取專案、環境和網域 ID。 AWS Glue 資料來源會在標準時間建立並執行，該時間可在指令碼的 cron 區段中進行更新。

```
def crcreate_data_source(domain_id, project_id,data_source_name)
        print("Creating Data Source")
        data_source_creation = dz.create_data_source(
            # Define data source : Customize the data source to which you'd like to
 connect
            # define the name of the Data source to create, example: name
 ='TestGlueDataSource'
            name=data_source_name,
            # give a description for the datasource (optional), example:
 description='This is a dorra test for creation on DZ datasources'
            description=data_source_description,
            # insert the domain identifier corresponding to the domain to which the
 datasource will belong, example: domainIdentifier= 'dzd_6f3gst5jjmrrmv'
            domainIdentifier=domain_id,
            # give environment identifier , example: environmentIdentifier=
 '3weyt6hhn8qcvb'
            environmentIdentifier=environment_id,
            # give corresponding project identifier, example: projectIdentifier=
 '6tl4csoyrg16ef',
            projectIdentifier=project_id,
            enableSetting="ENABLED",
            # publishOnImport used to select whether assets are added to the inventory
 and/or discovery catalog .
            # publishOnImport = True : Assets will be added to project's inventory as
 well as published to the discovery catalog
            # publishOnImport = False : Assets will only be added to project's
 inventory.
            # You can later curate the metadata of the assets and choose subscription
 terms to publish them from the inventory to the discovery catalog.
            publishOnImport=False,
            # Automated business name generation : Use AI to automatically generate
 metadata for assets as they are published or updated by this data source run.
            # Automatically generated metadata can be be approved, rejected, or edited
 by data publishers.
            # Automatically generated metadata is badged with a small icon next to the
 corresponding metadata field.
```

```
            recommendation={"enableBusinessNameGeneration": True},
            type="GLUE",
            configuration={
                "glueRunConfiguration": {
                    "dataAccessRole": "arn:aws:iam::"
                    + account_id
                    + ":role/service-role/AmazonDataZoneGlueAccess-"
                    + current_region
                    + "-"
                    + domain_id
                    + "",
                    "relationalFilterConfigurations": [
                        {
                            #
                            "databaseName": glue_database_name,
                            "filterExpressions": [
                                {"expression": "*", "type": "INCLUDE"},
                            ],
                            #    "schemaName": "TestSchemaName",
                        },
                    ],
                },
            },
            # Add metadata forms to the data source (OPTIONAL).
            # Metadata forms will be automatically applied to any assets that are
created by the data source.
            # assetFormsInput=[
            #     {
            #         "content": "string",
            #         "formName": "string",
            #         "typeIdentifier": "string",
            #         "typeRevision": "string",
            #     },
            # ],
            schedule={
                "schedule": "cron(5 20 * * ? *)",
                "timezone": "UTC",
            },
        )
        # This is a suggested syntax to return values
        #        return_values["data_source_creation"] = data_source_creation["items"]
        print("Data Source Created")
```

```
//This is the sample response payload after the CreateDataSource API is invoked:

{
    "Content":{
        "project_name": "Admin",
        "domain_name": "Drug-Research-and-Development",
        "env_name": "GlueEnvironment",
        "glue_database_name": "test",
        "data_source_name" : "test",
        "data_source_description" : "This is a test data source"
    }
}
```

組織和發佈資料資產

您可以使用下列範例指令碼來組織和發佈 Amazon DataZone 中的資料資產。

您可以使用下列指令碼建立自訂表單類型：

```
def create_form_type(domainId, projectId):
    return dzclient.create_form_type(
        domainIdentifier = domainId,
        name = "customForm",
        model = {
            "smithy": "structure customForm { simple: String }"
        },
        owningProjectIdentifier = projectId,
        status = "ENABLED"
    )
```

您可以使用下列範例指令碼建立自訂資產類型：

```
def create_custom_asset_type(domainId, projectId):
    return dzclient.create_asset_type(
        domainIdentifier = domainId,
        name = "userCustomAssetType",
        formsInput = {
            "Model": {
```

```
                "typeIdentifier": "customForm",
                "typeRevision": "1",
                "required": False
            }
        },
        owningProjectIdentifier = projectId,
    )
```

您可以使用下列範例指令碼建立自訂資產：

```
def create_custom_asset(domainId, projectId):
    return dzclient.create_asset(
        domainIdentifier = domainId,
        name = 'custom asset',
        description = "custom asset",
        owningProjectIdentifier = projectId,
        typeIdentifier = "userCustomAssetType",
        formsInput = [
            {
                "formName": "UserCustomForm",
                "typeIdentifier": "customForm",
                "content": "{\"simple\":\"sample-catalogId\"}"
            }
        ]
    )
```

您可以使用下列範例指令碼建立辭彙：

```
def create_glossary(domainId, projectId):
    return dzclient.create_glossary(
        domainIdentifier = domainId,
        name = "test7",
        description = "this is a test glossary",
        owningProjectIdentifier = projectId
    )
```

您可以使用下列範例指令碼來建立辭彙術語：

```
def create_glossary_term(domainId, glossaryId):
    return dzclient.create_glossary_term(
        domainIdentifier = domainId,
        name = "soccer",
        shortDescription = "this is a test glossary",
        glossaryIdentifier = glossaryId,
    )
```

您可以使用下列範例指令碼，使用系統定義的資產類型建立資產：

```
def create_asset(domainId, projectId):
    return dzclient.create_asset(
        domainIdentifier = domainId,
        name = 'sample asset name',
        description = "this is a glue table asset",
        owningProjectIdentifier = projectId,
        typeIdentifier = "amazon.datazone.GlueTableAssetType",
        formsInput = [
            {
                "formName": "GlueTableForm",
                "content": "{\"catalogId\":\"sample-catalogId\",\"columns\":
[{\"columnDescription\":\"sample-columnDescription\",\"columnName\":\"sample-
columnName\",\"dataType\":\"sample-dataType\",\"lakeFormationTags\":{\"sample-
key1\":\"sample-value1\",\"sample-key2\":\"sample-value2\"}}],\"compressionType\":
\"sample-compressionType\",\"lakeFormationDetails\":{\"lakeFormationManagedTable
\":false,\"lakeFormationTags\":{\"sample-key1\":\"sample-value1\",\"sample-key2\":
\"sample-value2\"}},\"primaryKeys\":[\"sample-Key1\",\"sample-Key2\"],\"region\":
\"us-east-1\",\"sortKeys\":[\"sample-sortKey1\"],\"sourceClassification\":\"sample-
sourceClassification\",\"sourceLocation\":\"sample-sourceLocation\",\"tableArn\":
\"sample-tableArn\",\"tableDescription\":\"sample-tableDescription\",\"tableName\":
\"sample-tableName\"}"
            }
        ]
    )
```

您可以使用下列範例指令碼建立資產修訂版本並附加辭彙字詞：

```
def create_asset_revision(domainId, assetId):
    return dzclient.create_asset_revision(
        domainIdentifier = domainId,
        identifier = assetId,
        name = 'glue table asset 7',
        description = "glue table asset description update",
        formsInput = [
            {
                "formName": "GlueTableForm",
                "content": "{\"catalogId\":\"sample-catalogId\",\"columns\":
[{\"columnDescription\":\"sample-columnDescription\",\"columnName\":\"sample-
columnName\",\"dataType\":\"sample-dataType\",\"lakeFormationTags\":{\"sample-
key1\":\"sample-value1\",\"sample-key2\":\"sample-value2\"}}],\"compressionType\":
\"sample-compressionType\",\"lakeFormationDetails\":{\"lakeFormationManagedTable
\":false,\"lakeFormationTags\":{\"sample-key1\":\"sample-value1\",\"sample-key2\":
\"sample-value2\"}},\"primaryKeys\":[\"sample-Key1\",\"sample-Key2\"],\"region\":
\"us-east-1\",\"sortKeys\":[\"sample-sortKey1\"],\"sourceClassification\":\"sample-
sourceClassification\",\"sourceLocation\":\"sample-sourceLocation\",\"tableArn\":
\"sample-tableArn\",\"tableDescription\":\"sample-tableDescription\",\"tableName\":
\"sample-tableName\"}"
            }
        ],
        glossaryTerms = ["<glossaryTermId:>"]
    )
```

您可以使用下列範例指令碼來發佈資產：

```
def publish_asset(domainId, assetId):
    return dzclient.create_listing_change_set(
        domainIdentifier = domainId,
        entityIdentifier = assetId,
        entityType = "ASSET",
        action = "PUBLISH",
    )
```

搜尋資料目錄並訂閱資料

您可以使用下列範例指令碼來搜尋資料目錄並訂閱資料：

```
def search_asset(domainId, projectId, text):
    return dzclient.search(
        domainIdentifier = domainId,
        owningProjectIdentifier = projectId,
        searchScope = "ASSET",
        searchText = text,
    )
```

您可以使用下列範例指令碼取得資產的清單 ID：

```
def search_listings(domainId, assetName, assetId):
    listings = dzclient.search_listings(
        domainIdentifier=domainId,
        searchText=assetName,
        additionalAttributes=["FORMS"]
    )

    assetListing = None
    for listing in listings['items']:
        if listing['assetListing']['entityId'] == assetId:
            assetListing = listing

    return listing['assetListing']['listingId']
```

您可以使用下列範例指令碼，使用清單 ID 建立訂閱要求：

```
create_subscription_response = def create_subscription_request(domainId, projectId,
 listingId):
    return dzclient.create_subscription_request(
        subscribedPrincipals=[{
            "project": {
                "identifier": projectId
            }
        }],
        subscribedListings=[{
            "identifier": listingId
        }],
        requestReason="Give request reason here."
    )
```

使用上create_subscription_response述方法，取得 subscription_request_id，然後使用下列範例指令碼接受/核准訂閱：

```
subscription_request_id = create_subscription_response["id"]

def accept_subscription_request(domainId, subscriptionRequestId):
    return dzclient.accept_subscription_request(
        domainIdentifier=domainId,
        identifier=subscriptionRequestId
    )
```

其他有用的範例腳本

在 Amazon 中處理資料時，您可以使用下列範例指令碼來完成各種任務 DataZone。

使用下列範例指令碼列出現有的 Amazon DataZone 網域：

```
def list_domains():
    datazone = boto3.client('datazone')
    response = datazone.list_domains(status='AVAILABLE')
    [print("%12s | %16s | %12s | %52s" % (item['id'], item['name'],
 item['managedAccountId'], item['portalUrl'])) for item in response['items']]
    return
```

使用下列範例指令碼列出現有的 Amazon DataZone 專案：

```
def list_projects(domain_id):
    datazone = boto3.client('datazone')
    response = datazone.list_projects(domainIdentifier=domain_id)
    [print("%12s | %16s " % (item['id'], item['name'])) for item in response['items']]
    return
```

使用下列範例指令碼列出現有的 Amazon DataZone 中繼資料表單：

```
def list_metadata_forms(domain_id):
    datazone = boto3.client('datazone')
    response = datazone.search_types(domainIdentifier=domain_id,
        managed=False,
        searchScope='FORM_TYPE')
    [print("%16s | %16s | %3s | %8s" % (item['formTypeItem']['name'],
 item['formTypeItem']['owningProjectId'],item['formTypeItem']['revision'],
 item['formTypeItem']['status'])) for item in response['items']]
    return
```

管理 Amazon DataZone 域和用戶訪問

主題

建立網域

> **Note**
>
> 如果您透過 AWS 身分中心使 DataZone 用 Amazon 來提供 SSO 使用者和群組的存取權，則您的 Amazon DataZone 網域目前必須與 AWS 身分中心執行個體位於相同的 AWS 區域。

Amazon DataZone，域是一個組織實體，用於將您的資產，用戶和他們的項目連接在一起。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。

若要建立 Amazon DataZone 網域，您必須在具有管理許可的帳戶中擔任 IAM 角色。 設定使用 Amazon DataZone 管理主控台所需的 IAM 許可以取得建立網域所需的最低權限。

Amazon 需要其他 IAM 角色， DataZone 才能代表具有預設組態的網域使用者執行動作。您可以事先建立這些 IAM 角色，也可以讓 Amazon 為您 DataZone 建立這些角色。如果您希 DataZone 望 Amazon 在網域建立過程中為您建立這些 IAM 角色，則對於網域建立，您必須擔任具有角色建立許可的 IAM 角色。請參閱建立 IAM 許可的自訂政策，以簡化 Amazon DataZone 服務主控台的角色建立 。根據您的網域建立選擇，Amazon DataZone 將為您建立最多四個新的 IAM 角色：AmazonDataZoneDomainExecutionRoleAmazonDataZoneGlueManageAccessRoleAmazonDataZoneRe和AmazonDataZoneProvisioningRole。

請完成以下程序來建立 Amazon DataZone 網域。

1. 瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，然後使用頂端導覽列中的區域選擇器來選擇適當的 AWS 區域。
2. 選擇 [建立網域] 並提供下列欄位的值：

   - 名稱-指定網域的易記名稱。一旦建立網域，就無法變更此名稱。
   - 說明-(選擇性) 指定網域描述。
   - 資料加密-您的 Amazon DataZone 網域、中繼資料和報告資料會由金 AWS 鑰管理服務 (KMS) 使用 Amazon 專屬的金鑰加密 DataZone。使用此欄位可指定是要使用 AWS 擁有的金鑰還是選擇不同的 AWS KMS 金鑰。

     如需使用客戶受管金鑰的詳細資訊，請參閱適用於 Amazon 的靜態資料加密 DataZone。如果您使用自己的 KMS 金鑰進行資料加密，則必須在預設值中包含下列陳述式AmazonDataZoneDomainExecutionRole。

     ```
     {
       "Version": "2012-10-17",
       "Statement": [
         {
           "Sid": "Statement1",
           "Effect": "Allow",
           "Action": [
             "kms:Decrypt",
             "kms:DescribeKey",
             "kms:GenerateDataKey"
           ],
           "Resource": [
             "*"
           ]
         }
       ]
     }
     ```

   - 服務存取-選擇要讓 Amazon DomainExecutionRole為您 DataZone 建立和使用新角色，或選擇現有的 IAM 角色。
   - 快速設定-(選用) 核取此方塊，讓 Amazon DataZone 設定您的帳戶以進行資料使用和發佈，以更快速地開始使用。Amazon DataZone 將建立三個 IAM 角色來佈建、導入和管理 AWS Glue 和 Amazon Redshift 資源的存取權、建立新的 Amazon S3 儲存貯體、建立管理 Amazon DataZone 專案，以及為資料湖和資料倉儲預設藍圖建立環境設定檔。

- 標籤- (選用) 指定網域的 AWS 標籤 (金鑰與值配對)。
- 成功建立網域後，應重新整理瀏覽器以顯示新 Amazon DataZone 網域的詳細資訊頁面。

編輯網域

在 Amazon 中 DataZone，網域是將資產、使用者及其專案連接在一起的組織實體。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。

建立 Amazon DataZone 網域後，您可以稍後將網域編輯為：變更說明、啟用 IAM 身分中心，以及新增、編輯或移除標籤金鑰及其值。若要編輯 Amazon DataZone 網域，您必須在具有管理許可的帳戶中擔任 IAM 角色。 設定使用 Amazon DataZone 管理主控台所需的 IAM 許可取得編輯網域所需的最低權限。

若要編輯網域，請完成以下步驟：

1. 登入 AWS 管理主控台，然後開啟 Amazon 主 DataZone 控台，網址為 https://console.aws.amazon.com/datazone。
2. 選擇查看域名，然後從列表中選擇域名。該名稱是一個超鏈接。
3. 在網域的詳細資料頁面上，選擇 [編輯]。
4. • 編輯「描述」。
   • 設定 IAM 身分中心設定。進一步瞭解這些設定，請參閱為 Amazon 設置 AWS IAM 身份中心 DataZone。
   • 加入、編輯或移除標籤鍵及其值。
5. 編輯完成後，請選擇 [更新網域]。

刪除網域

在 Amazon 中 DataZone，網域是將資產、使用者及其專案連接在一起的組織實體。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。

刪除域名的行為是最終的。刪除不可撤銷地移除每個 Amazon DataZone 實體，包括資料來源、專案、環境、資產、詞彙表和中繼資料表單。刪除不會刪除 Amazon DataZone 可能協助您建立的非 Amazon DataZone AWS 資源，例如 IAM 角色、S3 儲存貯體、 AWS Glue 資料庫，以及透過 LakeFormation 或 Redshift 訂閱授與。如果您不再需要這些資源，請在相應的 AWS 服務中刪除這些資源。

為了防止某人惡意刪除網域，刪除網域需要 Amazon 的管理 IAM 許可 DataZone，您可以使用 IAM 進行設定。為了防止某人意外刪除網域，刪除網域需要輸入確認字 (在 Amazon DataZone 主控台中)。

若要刪除網域，請完成以下步驟：

1. 登入 AWS 管理主控台，然後開啟 Amazon 主 DataZone 控台，網址為 https://console.aws.amazon.com/datazone。
2. 選擇查看域名，然後從列表中選擇域名。該名稱是一個超鏈接。
3. 選擇刪除並檢閱資訊性警告。
4. 輸入要求的文字，以確認您瞭解這些警告。選擇刪除。

Important

刪除網域是不可撤銷的動作，您或您無法復原。 AWS

Note

當您或您的網域使用者在專案中建立環境時，Amazon DataZone 會在您的網域或關聯帳戶中建立 AWS 資源，為您和您的網域使用者提供功能。以下是 Amazon DataZone 可能為您網域中的專案建立的 AWS 資源清單，以及預設名稱。刪除網域並不會刪除 AWS 帳戶中的任何 AWS 資源。

- <environmentId>身分與存取權管理角色：資料加密。
- <environmentName>Glue 資料庫：(1) <environmentName>_pub_db-*、(2) _ 子資料庫 *。如果已有此名稱的現有資料庫，Amazon DataZone 將新增環境 ID。
- Athena 工作群組：<environmentName>-*。如果已有此名稱的現有工作群組，Amazon DataZone 將新增環境 ID。
- CloudWatch 記錄群組：資料區 _ <environmentId>

啟用 Amazon 的 IAM 身分中心 DataZone

> **Note**
>
> 若要完成此程序，您必須在與 Amazon DataZone 網域相同的 AWS 區域中啟用 AWS IAM 身分中心。

您可以使用 AWS IAM 身分中心為 SSO 使用者和群組提供對 Amazon 資 DataZone 料入口網站的存取權限。完成後為 Amazon 設置 AWS IAM 身份中心 DataZone，您可以讓 SSO 使用者和群組存取 Amazon DataZone 網域資料入口網站。

若要啟用 AWS IAM 身分中心以搭配 Amazon DataZone 網域使用，您必須在具有管理許可的帳戶中擔任 IAM 角色。 設定使用 Amazon DataZone 管理主控台所需的 IAM 許可並取建立 IAM 許可的自訂政策，以簡化 Amazon DataZone 服務主控台的角色建立 得啟用 IAM 身分中心以搭配 Amazon 使用所需的最低許可 DataZone。

請完成下列程序以啟用適用於 Amazon 的 AWS IAM 身分中心 DataZone。

1. 登入 AWS 管理主控台，然後開啟 DataZone 主控台，網址為 https://console.aws.amazon.com/datazone。
2. 選取 [檢視網域]，然後從清單中選擇網域名稱。該名稱是一個超鏈接。
3. 在網域的詳細資料頁面上，選擇 [編輯]。
   - 選取「在 IAM 身分中心啟用使用者」核取方塊。
   - 在兩種使用者指派模式之間進行選擇。一旦您的網域更新為您的選擇，之後便無法變更。
     - 透過隱含使用者指派，任何新增到 IAM 身分中心目錄的使用者都可以存取您的 Amazon DataZone 網域。
     - 透過明確使用者指派，您將從 IAM 身分中心目錄新增特定使用者或群組，讓他們存取您的 Amazon DataZone 網域。稍後您將在 Amazon DataZone 主控台中新增和移除這些使用者和群組。
4. 一旦您對您的選擇感到滿意，請選擇「更新域名」。

停用 Amazon 的 IAM 身分中心 DataZone

停用 Amazon DataZone 網域的 AWS IAM 身分中心會移除所有 SSO 使用者的存取權。

> **Note**
>
> 停用 IAM 身分中心不會停止 SSO 使用者的帳單。若要停止針對 SSO 使用者計費，您必須在網域中停用他們。帳單會持續到停用使用者月底為止。若要停用使用者，請參閱在 Amazon DataZone 控制台中管理用戶。

您可以使用 AWS IAM 身分中心為 SSO 使用者和群組提供對 Amazon 資 DataZone 料入口網站的存取權限。如果您已啟用適用於 Amazon 的 AWS IAM 身分中心 DataZone，稍後可以停用所有使用者的存取權限。

若要停用 AWS IAM 身分中心以搭配 Amazon DataZone 網域使用，您必須在具有管理許可的帳戶中擔任 IAM 角色。 設定使用 Amazon DataZone 管理主控台所需的 IAM 許可並取建立 IAM 許可的自訂政策，以簡化 Amazon DataZone 服務主控台的角色建立 得停用 IAM 身分中心不與 Amazon 搭配使用所需的最低許可 DataZone。

請完成下列程序，以停用適用於 Amazon 的 AWS IAM 身分中心 DataZone。

1. 登入 AWS 管理主控台，然後開啟 DataZone 主控台，網址為 https://console.aws.amazon.com/datazone。
2. 選取 [檢視網域]，然後從清單中選擇網域名稱。該名稱是一個超鏈接。
3. <regionName><accountId><domainName>複製您的域的 Amazon 資源名稱（ARN），該名稱以 arn: aw:aw:one:: 域/開頭。
4. 開啟身分識別中心主控台，網址為 https://console.aws.amazon.com/singlesignon/。
5. 選擇 Applications (應用程式)。
6. 選擇您要停用 AWS IAM 身分中心的網域，因此會移除所有 SSO 使用者對網域資料入口網站的存取權。您可以使用「篩選」功能表和搜尋方塊來篩選應用程式清單。
7. 從「動作」功能表中選擇「停用」。
8. SSO 使用者將無法存取 Amazon DataZone 網域。
9. 若要重新啟用 Amazon DataZone 網域的 AWS IAM 身分中心，請選擇要重新啟用 AWS IAM 身分中心的網域，然後從 [動作] 功能表中選擇 [啟用]。

在 Amazon DataZone 控制台中管理用戶

您的使用者可以使用其 AWS 登入 DataZone 資料或單一登入 (SSO) 登入資料存取 Amazon 資料入口網站。若要在 Amazon DataZone 主控台中管理 Amazon DataZone 網域的使用者，您必須在具有

管理許可的帳戶中擔任 IAM 角色。 設定使用 Amazon DataZone 管理主控台所需的 IAM 許可取得在 Amazon DataZone 主控台管理使用者所需的最低許可。

主題

管理 IAM 角色和使用者

IAM 角色和使用者是使用 AWS Identity and Access Management (IAM) 建立的，並透過政策附加至 Amazon DataZone 網域的許可來存取您的 Amazon 網域。如需詳細資訊，請參閱 設定使用 Amazon DataZone 資料入口網站所需的 IAM 許可。您可以檢視已啟用 Amazon DataZone 網域訂閱的 IAM 角色和使用者清單、停用其存取權，以及啟用其存取權 (如果先前停用)。

1. 登入 AWS 管理主控台，然後開啟 DataZone 主控台，網址為 https://console.aws.amazon.com/datazone。
2. 選取 [檢視網域]，然後從清單中選擇網域名稱。該名稱是一個超鏈接。
3. 在網域的詳細資料頁面上，選擇 [使用者管理]。
4. 對於使用者類型，請選取 IAM 使用者以檢視目前已啟用和停用的 IAM 使用者和角色清單。
    - 「名稱」欄會顯示 IAM 使用者或角色的 arn。
    - 「狀態」欄會顯示網域中 IAM 使用者或角色的目前狀態。
        - 已啟用表示 IAM 使用者或角色已呼叫 API、發出命令 (透過命令列界面)，或存取您網域的 Amazon DataZone 入口網站，而您需要支付使用者訂閱的費用。
        - 停用表示 IAM 使用者或角色已封鎖對您 Amazon DataZone 網域的存取權。
5. 若要停用目前啟用的 IAM 使用者或角色，請勾選使用者旁邊的核取方塊，然後從 [動作] 功能表中選取 [停用]。用戶將失去對 Amazon DataZone 域的訪問權限。使用者的帳單將於當月月底結束。
6. 若要啟用目前停用的 IAM 使用者或角色，請勾選使用者旁邊的核取方塊，然後從「動作」功能表中選取「啟用」。如果 IAM 使用者或角色具有適當的許可，使用者將可存取 Amazon DataZone 網域。使用者的帳單將會重新開始。

管理 SSO 使用者

您可以在 AWS IAM 身分中心建立 SSO 使用者，或與您的身分提供者同步。如需詳細資訊，請參閱為 Amazon 設置 AWS IAM 身份中心 DataZone和啟用 Amazon 的 IAM 身分中心 DataZone用和設定適用於 Amazon 的 AWS IAM 身分中心 DataZone。您可以檢視指派給網域的 SSO 使用者清單、新增 SSO 使用者，以及移除 SSO 使用者。

1. 登入 AWS 管理主控台，然後開啟 DataZone 主控台，網址為 https://console.aws.amazon.com/datazone。
2. 選取 [檢視網域]，然後從清單中選擇網域名稱。該名稱是一個超鏈接。
3. 在網域的詳細資訊頁面上，向下捲動並選擇 [使用者管理]。
4. 對於使用者類型，請選取 SSO 使用者以檢視目前的 SSO 使用者清單。

   - 「名稱」欄會顯示 SSO 使用者的名稱。
   - 狀態欄會顯示網域中 SSO 使用者的目前狀態。
     - 「已指派」表示 SSO 使用者已明確指派給網域。其結果是，用戶可以訪問 Amazon DataZone。只有當網域的身分識別提供者模式設定為明確指派時，才會使用此狀態。
     - 已啟用表示 SSO 使用者已存取網域的 Amazon DataZone 入口網站，而您需要支付使用者訂閱的費用。激活自動發生。
     - 停用表示 SSO 使用者的存取遭到網域的資料入口網站封鎖。使用者的帳單會在停用其存取權的月底結束。
     - 已移除表示 SSO 使用者先前已指派給網域，但在存取之前已移除。
5. 選擇新增和新增使用者來新增 SSO 使用者。如果網域設定為隱含使用者指派，則無法使用此選項，這表示身分集區中的所有使用者都可以存取 Amazon DataZone 網域。

   - 在 [新增使用者] 頁面上，搜尋要新增之使用者的別名。搜尋方塊下方會出現一個可能相符項目的清單。
   - 選擇您要新增的使用者。他們的別名將顯示為搜索框下方的芯片。
   - 如果您滿意要新增的使用者清單，請選擇 [新增使用者]。
   - 使用者會被指派到狀態為「已指派」的 Amazon DataZone 網域。
   - 當使用者第一次存取網域的資料入口網站時，狀態會自動變更為 [已啟動]，而您將開始為使用者的訂閱付費。
6. 選取使用者，然後從動作功能表中選擇停用，以移除指派的 SSO 使用者。因此，使用者將無法存取 Amazon DataZone 網域。使用者的狀態會顯示為「已移除」。如果網域設定為隱含使用者指派，則無法使用此選項。

7. 選取使用者並從「動作」功能表中選擇「停用」，以停用已啟動的 SSO 使用者。因此，使用者對 Amazon DataZone 網域的存取權將會遺失並遭到封鎖。使用者的訂閱會繼續計費，直到月底為止。使用者的狀態會顯示為「已停用」。
8. 選取使用者，然後從「動作」功能表中選擇「啟動」，以啟動已停用的 SSO 使用者。因此，使用者將重新獲得對 Amazon DataZone 網域的存取權。帳單將立即開始。使用者會顯示為 [已啟動]。

管理 SSO 群組

SSO 群組會在 AWS IAM 身分中心建立或與您的身分提供者同步。如需詳細資訊，請參閱為 Amazon 設置 AWS IAM 身份中心 DataZone和啟用 Amazon 的 IAM 身分中心 DataZone用和設定適用於 Amazon 的 AWS IAM 身分中心 DataZone。您可以檢視指派給網域的 SSO 群組清單、新增 SSO 群組，以及移除 SSO 群組。

1. 登入 AWS 管理主控台，然後開啟 DataZone 主控台，網址為 https://console.aws.amazon.com/datazone。
2. 選取 [檢視網域]，然後從清單中選擇網域名稱。該名稱是一個超鏈接。
3. 在網域的詳細資訊頁面上，向下捲動並選擇 [使用者管理]。
4. 針對使用者類型，選取 SSO 群組以檢視目前的 SSO 群組清單。

   - [名稱] 資料行會顯示 SSO 群組的名稱。
   - 狀態欄會顯示網域中 SSO 群組的目前狀態。
     - 已指派表示 SSO 群組已明確指派給網域。因此，群組中的所有使用者都可以存取網域的資料入口網站 (除非使用者已停用)。
     - 未指派表示 SSO 群組已從網域中移除。群組中的使用者無法透過其在此群組中的成員資格存取網域的資料入口網站。
5. 選擇新增和新增群組來新增 SSO 群組。如果網域設定為隱含使用者指派，則無法使用此選項，這表示身分集區中的所有使用者都可以存取 Amazon DataZone 網域，而不論群組成員資格為何。

   - 在「新增群組」頁面上，搜尋要新增之群組的別名。搜尋方塊下方會出現一個可能相符項目的清單。
   - 選擇您要新增的群組。他們的別名將顯示為搜索框下方的芯片。
   - 如果您滿意要新增的群組清單，請選擇 [新增群組]。
   - 這些群組會指派給狀態為「已指派」的 Amazon DataZone 網域。
   - 當群組成員存取網域的資料入口網站時，狀態會自動變更為 [已啟動]，而您將開始為使用者的訂閱付費。

6. 選取群組，然後從 「動作」功能表中選擇「取消指派」，以移除指派的 SSO 群組。因此，該群組將失去對 Amazon DataZone 網域的存取權。群組的狀態會顯示為「未指派」。 DataZone 透過此群組中的成員資格取得 Amazon 存取權的使用者將失去存取權。如果網域設定為隱含使用者指派，則無法使用此選項。若要停止透過取消指派群組來移除存取權限的使用者計費，您必須接下來手動選取並停用其使用者設定檔。

在 Amazon DataZone 資料入口網站中管理使用者許可

在目前版本的 Amazon 中 DataZone，預設授權機制可讓 Amazon DataZone 網域的所有已驗證使用者 (IAM 和 SSO) 建立專案、在專案中建立實體以及執行搜尋。專案成員仍必須遵守針對其指定專案擁有者或專案貢獻者角色授予他們的權限。

使用 Amazon 內 DataZone置藍圖

建立環境的藍圖定義了環境所屬專案的工具和服務成員在處理 Amazon DataZone 目錄中的資產時，可以使用哪些工具和服務。在 Amazon 的當前版本中 DataZone，有以下內置藍圖：

- 資料湖藍圖
- 資料倉儲藍圖
- Amazon SageMaker 藍圖

主題

在擁有 Amazon DataZone 網域的 AWS 帳戶中啟用內建藍圖

建立環境的藍圖定義了環境所屬專案的工具和服務成員在處理 Amazon DataZone 目錄中的資產時，可以使用哪些工具和服務。

在目前版本的 Amazon 中 DataZone，有數個內建藍圖：資料湖藍圖、資料倉儲藍圖和 Amazon SageMaker 藍圖。

- 資料湖藍圖包含啟動和設定一組服務 (AWS Glue、 AWS Lake Formation、Amazon Athena) 的定義，以便在 Amazon DataZone 目錄中發佈和使用資料湖資產。
- 資料倉儲藍圖包含啟動和設定一組服務 (Amazon Redshift) 的定義，以便在 Amazon 目錄中發佈和使用 Amazon Redshift 資產。 DataZone
- Amazon SageMaker 藍圖包含用於啟動和配置一組服務（Amazon SageMaker 工作室）的定義，以在 Amazon DataZone 目錄中發布和使用 Amazon SageMaker 資產。

如需詳細資訊，請參閱 Amazon DataZone 術語和概念。

建立 Amazon DataZone 網域時，您可以選擇自動啟用預設資料湖和預設資料倉儲內建藍圖的快速設定，做為網域建立程序的一部分。快速設定也會使用這些內建藍圖，為您建立預設環境設定檔和預設環境。

如果您在建立 Amazon DataZone 網域時未選擇「快速設定」，可以使用以下程序在包含此 Amazon 網 DataZone 域的 AWS 帳戶中啟用可用的內建藍圖。您必須先啟用這些內建藍圖，才能在此網域中使用它們建立環境設定檔和環境。

若要透過 Amazon DataZone 管理主控台在 Amazon DataZone 網域中啟用內建藍圖，您必須在具有管理許可的帳戶中擔任 IAM 角色。 設定使用 Amazon DataZone 管理主控台所需的 IAM 許可以取得最低權限。

在 Amazon 網 DataZone域中啟用內建藍圖

1. 在 https://console.aws.amazon.com/datazone 上導航到 Amazon DataZone 控制台，然後使用您的帳戶憑據登錄。
2. 選擇 [檢視網域]，然後選擇您要啟用一或多個內建藍圖的網域。
3. 在網域詳細資料頁面上，導覽至藍圖索引標籤。
4. 從藍圖清單中，選擇DefaultDataLake或 DefaultDataWarehouse，或 Amazon SageMaker 藍圖。
5. 在所選藍圖的詳細資料頁面上，選擇在此帳戶中啟用。
6. 在 [權限和資源] 頁面上，指定下列項目：

   - 如果您要啟用DefaultDataLake藍圖，請針對 Glue 管理存取角色指定新的或現有的服務角色，以授予 Amazon DataZone 授權，以擷取和管理 AWS Glue 和 AWS Lake Formation 中表格的存取權。
   - 如果您正在啟用DefaultDataWarehouse藍圖，請針對 Redshift 管理存取角色指定新的或現有的服務角色，以授予 Amazon DataZone 授權，以擷取和管理 Amazon Redshift 中資料倉、資料表和檢視的存取權。
   - 如果您要啟用 Amazon SageMaker 藍圖，對於SageMaker 管理存取角色，請指定新的或現有的服務角色，以授 DataZone予 Amazon 許可，將 Amazon SageMaker 資料發佈到目錄。它還授予 Amazon DataZone 許可，以授予對目錄中 Amazon SageMaker 已發佈資產的存取權或撤銷存取權。

   > **Important**
   >
   > 當您啟用 Amazon SageMaker 藍圖時，Amazon DataZone 會檢查目前帳戶和區域中是否 DataZone 存在以下 Amazon 的 IAM 角色。如果這些角色不存在，Amazon DataZone 會自動建立這些角色。
   >
   > - AmazonDataZoneGlueAccess-<region>-<domainId>
   > - AmazonDataZoneRedshiftAccess-<region>-<domainId>

- 對於佈建角色，請指定授與 Amazon DataZone 授權的新服務角色或現有服務角色，以便在環境帳戶和區域 AWS CloudFormation 中使用建立和設定環境資源。
- 如果您要啟用 Amazon SageMaker 藍圖，請針對 SageMaker-Glue 資料來源的 Amazon S3 儲存貯體，指定 AWS 帳戶中所有 SageMaker 環境要使用的 Amazon S3 儲存貯體。您指定的值區前置字元必須是下列其中一項：
  - 亞馬遜數據氮 *
  - 數據發射器 *
  - 箭頭-數據酮 *
  - DataZone-射手機 *
  - 下垂器-* DataZone
  - DataZone-SageMaker*
  - SageMaker-DataZone*

7. 選擇啟用藍圖。

啟用選擇的藍圖後，您可以控制哪些專案可以使用帳戶中的藍圖來建立環境設定檔。您可以透過將管理專案指派給藍圖的組態來執行此操作。

指定管理已啟用藍圖上的專案

1. 在 https://console.aws.amazon.com/datazone 上導航到 Amazon DataZone 控制台，然後使用您的帳戶憑據登錄。
2. 選擇 [檢視網域]，然後選擇要為所選藍圖新增管理專案的網域。
3. 選擇藍圖索引標籤，然後選擇您要使用的藍圖。
4. 依預設，網域內的所有專案都可以使用帳戶中的或或 Amazon SageMaker 藍圖來建立環境設定檔。 DefaultDataLake DefaultDataWareshouse但是，您可以透過將管理專案指派給藍圖來限制此問題。若要新增管理專案，請選擇 [選取管理專案]，然後從下拉式功能表中選擇要新增為管理專案的專案，然後選擇 [選取管理專案]。

在 AWS 帳戶中啟用 DefaultDataWarehouse 藍圖後，您可以將參數集新增至藍圖組態。參數集是一組金鑰和值，Amazon 必須建立與 Amazon DataZone Redshift 叢集的連線，並用來建立資料倉儲環境。這些參數包括 Amazon Redshift 叢集的名稱、資料庫，以及保留叢集登入資料的 AWS 密碼。

將參數集新增至 DefaultDataWarehouse 藍圖

1. 在 https://console.aws.amazon.com/datazone 上導航到 Amazon DataZone 控制台，然後使用您的帳戶憑據登錄。
2. 選擇 [檢視網域]，然後選擇要新增參數集的網域。
3. 選擇藍圖索引標籤，然後選擇藍 DefaultDataWareshouse 圖以開啟藍圖詳細資料頁面。
4. 在藍圖詳細資料頁面的 [參數集] 索引標籤下，選擇 [建立參數集]。
   - 提供參數組的「名稱」。
   - (可選) 提供參數集的描述。
   - 選擇區域
   - 選取 Amazon Redshift 叢集或 Amazon Redshift 無伺服器。
   - 選取保留所選 Amazon Redshift 叢集或 Amazon Redshift 無伺服器工作群組的登入資料的 AWS 秘密 ARN。 AWS 密碼必須使用標籤加上`AmazonDataZoneDomain : [Domain_ID]`標籤，才有資格在參數組中使用。
     - 如果您沒有現有的 AWS 密碼，也可以選擇建立新密碼來建立新 AWS 密碼。這將打開一個對話框，您可以在其中提供密碼的名稱，用戶名和密碼。一旦您選擇建 DataZone立新 AWS 密碼，Amazon 就會在 Sec AWS rets Manager 服務中建立一個新密碼，並確保密碼會以您嘗試建立參數集的網域加上標記。
   - 如果您在上述步驟中選擇了 Amazon Redshift 叢集，現在可以從下拉式清單中選擇叢集。如果您在上述步驟中選擇了 Amazon Redshift 工作組，現在從下拉菜單中選擇一個工作組。
   - 輸入所選亞馬遜紅移叢集或亞馬遜 Redshift 無伺服器工作群組內的資料庫名稱。
   - 選擇「建立參數組」。

在 AWS 帳戶中啟用 Amazon SageMaker 藍圖後，您可以將參數集新增至藍圖組態。參數集是 Amazon 建立與 Amazon DataZone 的連接所需的一組密鑰和值， SageMaker 並用於創建 Sageemaker 環境。

將參數集添加到 Amazon SageMaker 藍圖

1. 在 https://console.aws.amazon.com/datazone 上導航到 Amazon DataZone 控制台，然後使用您的帳戶憑據登錄。
2. 選擇 [檢視網域]，然後選擇包含要在其中新增參數集之已啟用藍圖的網域。
3. 選擇藍圖索引標籤，然後選擇 Amazon 藍 SageMaker 圖以開啟藍圖的詳細資料頁面。
4. 在藍圖詳細資料頁面的 [參數集] 索引標籤下，選擇 [建立參數集]，然後指定下列項目：

- 提供參數組的「名稱」。
- (可選) 提供參數集的「描述」。
- 指定 Amazon SageMaker 網域身份驗證類型。您可以選擇 IAM 或 IAM 身分中心 (SSO)。
- 指定 AWS 區域。
- 指定用於資料加密的 AWS KMS 金鑰。您可以選擇現有的金鑰或建立新金鑰。
- 在「環境參數」下，指定下列項目：
  - VPC ID-您用於 Amazon SageMaker 環境 VPC 的 ID。您可以指定現有的 VPC 或建立新的 VPC。
  - 子網路-VPC 內特定資源的 IP 位址範圍的一或多個 ID。
  - 網路存取-選擇僅限 VPC 或僅公用網際網路。
  - 安全群組-設定 VPC 和子網路時要使用的安全性群組。
- 在 [資料來源參數] 下，選擇下列其中一項：
  - AWS 僅 Glue
  - AWS Glue + Amazon Redshift 無服務器。如果您選擇此選項，請指定下列項目：
    - 指定保留所選 Amazon Redshift 叢集登入資料的 AWS 秘密 ARN。 AWS 密碼必須使用標籤加上`AmazonDataZoneDomain : [Domain_ID]`標籤，才有資格在參數組中使用。

      如果您沒有現有的 AWS 密碼，也可以選擇建立新密碼來建立新 AWS 密碼。這將打開一個對話框，您可以在其中提供密碼的名稱，用戶名和密碼。一旦您選擇建 DataZone 立新 AWS 密碼，Amazon 就會在 Sec AWS rets Manager 服務中建立一個新密碼，並確保密碼會以您嘗試建立參數集的網域加上標記。
    - 指定建立環境時要使用的 Amazon Redshift 工作群組。
    - 指定建立環境時要使用的資料庫名稱 (在您選擇的工作群組內)。
  - AWS 僅 Glue + Amazon Redshift 集群
    - 指定保留所選 Amazon Redshift 叢集登入資料的 AWS 秘密 ARN。 AWS 密碼必須使用標籤加上`AmazonDataZoneDomain : [Domain_ID]`標籤，才有資格在參數組中使用。

      如果您沒有現有的 AWS 密碼，也可以選擇建立新密碼來建立新 AWS 密碼。這將打開一個對話框，您可以在其中提供密碼的名稱，用戶名和密碼。一旦您選擇建 DataZone 立新 AWS 密碼，Amazon 就會在 Sec AWS rets Manager 服務中建立一個新密碼，並確保密碼會以您嘗試建立參數集的網域加上標記。
    - 指定建立環境時要使用的 Amazon Redshift 叢集。
    - 指定建立環境時要使用的資料庫名稱 (在您選擇的叢集內)。

5. 選擇「建立參數組」。

在擁有 Amazon DataZone 域的 AWS 帳戶中添加 Amazon SageMaker 作為受信任的服務

如果您已啟用 Amazon SageMaker 藍圖，則還必須新增 SageMaker 為 Amazon 中受信任的服務之一 DataZone。若要這麼做，請完成下列程序：

1. 在 https://console.aws.amazon.com/datazone 上導航到 Amazon DataZone 控制台，然後使用您的帳戶憑據登錄。
2. 選擇 [檢視網域]，然後選擇包含已啟用 SageMaker 藍圖的網域。
3. 選擇受信任的服務，然後選擇 Amazon SageMaker，然後選擇啟用。

使用關聯帳戶以發佈和使用資料

將您的 AWS 帳戶與 Amazon DataZone 網域建立關聯，可讓網域使用者從這些 AWS 帳戶發佈和使用資料。設定帳戶關聯有三個步驟。

- 首先，通過請求關聯與所需 AWS 帳戶共享域。如果帳戶與域的 AWS AWS 帳戶不同，Amazon DataZone 使用 AWS Resource Access Manager（RAM）。帳戶關聯只能由 Amazon DataZone 網域啟動。
- 其次，讓帳戶擁有者接受關聯要求。
- 第三，讓帳戶擁有者啟用所需的環境藍圖。透過啟用藍圖，帳戶擁有者可為網域中的使用者提供必要的 IAM 角色和資源組態，以便在其帳戶中建立和存取資源，例如 AWS Glue 資料庫和 Amazon Redshift 叢集。

主題

請求與其他 AWS 帳戶建立關聯

> **Note**
>
> 藉由傳送關聯要求至另一個 AWS 帳號，即表示您與 AWS Resource Access Manager (RAM) 的另一個 AWS 帳號共用您的網域。請務必檢查您輸入的帳戶 ID 的正確性。

若要請求 Amazon DataZone 主控台中的其他 AWS 帳戶關聯 Amazon DataZone 網域，您必須在具有管理許可的帳戶中擔任 IAM 角色。 設定使用 Amazon DataZone 管理主控台所需的 IAM 許可取得要求帳戶關聯所需的最低權限。

請完成下列程序以要求與其他 AWS 帳戶建立關聯。

1. 登入 AWS 管理主控台並開啟 Amazon DataZone 管理主控台，網址為 https://console.aws.amazon.com/datazone。
2. 選擇查看域名，然後從列表中選擇域名。該名稱是一個超鏈接。
3. 向下捲動至「關聯帳戶」標籤，然後選擇「要求關聯」。
4. 輸入您要請求關聯的帳戶 ID。如果您滿意帳號 ID 清單，請選擇要求關聯。
5. Amazon 代表您的帳戶在 AWS Resource Access Manager 中 DataZone 建立資源共用，並以輸入的帳戶 ID 做為主體。
6. 您必須通知其他 AWS 帳戶的擁有者才能接受您的請求。邀請會在七 (7) 天後過期。

提供客戶管理 KMS 金鑰的帳戶存取權

Amazon DataZone 網域及其中繼資料會 (依預設) 使用您在網域建立期間擁有並提供的金鑰管理服務 (KMS) 中的客戶管理金 AWS 鑰 (選擇性) 加密 (依 AWS預設)。如果您的網域使用客戶管理的金鑰加密，請按照下列程序授予相關帳戶使用 KMS 金鑰的權限。

1. 登入 AWS 管理主控台，然後開啟 KMS 主控台，網址為 https://console.aws.amazon.com/kms/。
2. 若要檢視您所建立及管理帳戶中的金鑰，請在導覽窗格中選擇Customer managed keys (客戶受管金鑰)。
3. 若要檢視您所建立及管理帳戶中的金鑰，請在導覽窗格中選擇Customer managed keys (客戶受管金鑰)。
4. 在 KMS 金鑰清單中，選擇您要檢查之 KMS 金鑰的別名或金鑰 ID。
5. 若要允許或禁止外部 AWS 帳戶使用 KMS 金鑰，請使用頁面 [其他 AWS 帳戶] 區段中的控制項。這些帳戶中的 IAM 主體 (本身擁有適當的 KMS 權限) 可以在加密作業中使用 KMS 金鑰，例如加密、解密、重新加密和產生資料金鑰。

接受來自 Amazon DataZone 網域的帳戶關聯請求並啟用環境藍圖

若要接受 Amazon DataZone 管理主控台與 Amazon DataZone 網域的關聯，您必須在具有管理許可的帳戶中擔任 IAM 角色。 設定使用 Amazon DataZone 管理主控台所需的 IAM 許可以取得最低權限。

請完成以下步驟以接受與 Amazon DataZone 網域的關聯。

1. 登入 AWS 管理主控台並開啟 Amazon DataZone 管理主控台，網址為 https://console.aws.amazon.com/datazone。
2. 選擇 [檢視請求]，然後從清單中選取邀請網域。邀請的狀態應該被請求。選擇 [檢閱請求]。

3. 選擇是否要啟用預設的資料湖和/或資料倉儲環境藍圖，方法是選取兩者，或選取其中一個方塊。您可以稍後再執行此操作。

   - 資料湖環境藍圖可讓網域使用者建立和管理 AWS Glue、Amazon S3 和 Amazon Athena 資源，以便從資料湖發佈和使用。
   - 資料倉儲環境藍圖可讓網域使用者建立和管理 Amazon Redshift 資源，以便從資料倉儲發佈和使用。

4. 如果您選擇選取一個或兩個預設環境藍圖，請設定下列權限和資源。

   - 管理存取 IAM 角色為 Amazon 提供許可， DataZone讓網域使用者能夠擷取和管理表格的存取權，例如 AWS Glue 和 Amazon Redshift。您可以選擇讓 Amazon DataZone 建立並使用新的 IAM 角色，也可以從現有 IAM 角色清單中進行選擇。
   - 佈建 IAM 角色為 Amazon DataZone 提供許可，讓網域使用者能夠建立和設定環境資源，例如 AWS Glue 資料庫。您可以選擇讓 Amazon DataZone 建立並使用新的 IAM 角色，也可以從現有 IAM 角色清單中進行選擇。
   - 適用於資料湖的 Amazon S3 儲存貯體是 Amazon 在網域使用者存放資料湖資料時 DataZone 將使用的儲存貯體或路徑。您可以使用 Amazon 選取的預設儲存貯體， DataZone 或輸入路徑字串來選擇自己的現有 Amazon S3 路徑。如果您選擇自己的 Amazon S3 路徑，則需要更新 IAM 政策，以便向 Amazon DataZone 提供使用該路徑的許可。

5. 當您滿意您的組態時，請選擇接受並配置關聯。

拒絕來自 Amazon DataZone 網域的帳戶關聯請求

若要從 Amazon DataZone 網域拒絕 Amazon DataZone 管理主控台中的關聯請求，您必須在具有管理許可的帳戶中擔任 IAM 角色。 設定使用 Amazon DataZone 管理主控台所需的 IAM 許可以取得最低權限。

完成以下步驟以拒絕來自 Amazon DataZone 網域的關聯請求。

1. 登入 AWS 管理主控台並開啟 Amazon DataZone 管理主控台，網址為 https://console.aws.amazon.com/datazone。
2. 選擇 [檢視請求]，然後從清單中選取邀請網域。邀請的狀態應該被請求。選擇「拒絕關聯」。選擇拒絕關聯以確認您的選擇。

在關聯 AWS 帳戶中啟用環境藍圖

若要在 Amazon DataZone 管理主控台中啟用環境藍圖，您必須在具有管理許可的帳戶中擔任 IAM 角色。 設定使用 Amazon DataZone 管理主控台所需的 IAM 許可以取得最低權限。

完成以下步驟以啟用關聯網域中的藍圖。

1. 登入 AWS 管理主控台並開啟 Amazon DataZone 管理主控台，網址為 https://console.aws.amazon.com/datazone。
2. 開啟左側導覽面板，然後選擇 [關聯網域]。
3. 選擇您要為其啟用環境藍圖的網域。
4. 從藍圖清單中，選擇DefaultDataLake或 DefaultDataWarehouse，或 Amazon SageMaker 藍圖。
5. 在所選藍圖的詳細資料頁面上，選擇在此帳戶中啟用。
6. 在 [權限和資源] 頁面上，指定下列項目：

   - 如果您要啟用DefaultDataLake藍圖，請針對 Glue 管理存取角色指定新的或現有的服務角色，以授予 Amazon DataZone 授權，以擷取和管理 AWS Glue 和 AWS Lake Formation 中表格的存取權。
   - 如果您要啟用DefaultDataWarehouse藍圖，請針對 Redshift 管理存取角色指定新的或現有的服務角色，以授予 Amazon DataZone 授權，以擷取和管理 Amazon Redshift 中資料倉、資料表和檢視的存取權。
   - 如果您要啟用 Amazon SageMaker 藍圖，對於SageMaker 管理存取角色，請指定新的或現有的服務角色，以授 DataZone 予 Amazon 許可，將 Amazon SageMaker 資料發佈到目錄。它還授予 Amazon DataZone 許可，以授予目錄中 Amazon SageMaker 已發佈資產的存取權或撤銷存取權。

     > **Important**
     >
     > 當您啟用 Amazon SageMaker 藍圖時，Amazon DataZone 會檢查目前帳戶和區域中是否 DataZone 存在以下 Amazon 的 IAM 角色。如果這些角色不存在，Amazon DataZone 會自動建立這些角色。
     >
     > - AmazonDataZoneGlueAccess-<region>-<domainId>
     > - AmazonDataZoneRedshiftAccess-<region>-<domainId>

   - 對於佈建角色，請指定授與 Amazon DataZone 授權的新服務角色或現有服務角色，以便在環境帳戶和區域 AWS CloudFormation 中使用建立和設定環境資源。

- 如果您要啟用 Amazon SageMaker 藍圖，請針對 SageMaker-Glue 資料來源的 Amazon S3 儲存貯體，指定 AWS 帳戶中所有 SageMaker 環境要使用的 Amazon S3 儲存貯體。您指定的值區前置字元必須是下列其中一項：
  - 亞馬遜數據氮 *
  - 數據發射器 *
  - 箭頭-數據酮 *
  - DataZone-射手機 *
  - 下垂器-* DataZone
  - DataZone-SageMaker*
  - SageMaker-DataZone*
7. 選擇啟用藍圖。

啟用選擇的藍圖後，您可以控制哪些專案可以使用帳戶中的藍圖來建立環境設定檔。您可以透過將管理專案指派給藍圖的組態來執行此操作。

指定管理已啟用 DefaultDataLake 或 DefaultDataWarehouse 藍圖上的專案

1. 在 https://console.aws.amazon.com/datazone 上導航到 Amazon DataZone 控制台，然後使用您的帳戶憑據登錄。
2. 開啟左側導覽面板並選擇 [關聯的網域]，然後選擇要新增管理專案的網域。
3. 選擇藍圖索引標籤，然後選擇 DefaultDataLake 或 DefaultDataWareshouse 建立藍圖。
4. 根據預設，網域內的所有專案都可以使用帳戶中的 DefaultDataLake 或 DefaultDataWareshouse 藍圖來建立環境設定檔。但是，您可以透過將管理專案指派給藍圖來限制此問題。若要新增管理專案，請選擇 [選取管理專案]，然後從下拉式功能表中選擇要新增為管理專案的專案，然後選擇 [選取管理專案]。

在 AWS 帳戶中啟用 DefaultDataWarehouse 藍圖後，您可以將參數集新增至藍圖組態。參數集是一組金鑰和值，Amazon 必須建立與 Amazon DataZone Redshift 叢集的連線，並用來建立資料倉儲環境。這些參數包括 Amazon Redshift 叢集的名稱、資料庫，以及保留叢集登入資料的 AWS 密碼。

將參數集新增至 DefaultDataWarehouse藍圖

1. 在 https://console.aws.amazon.com/datazone 上導航到 Amazon DataZone 控制台，然後使用您的帳戶憑據登錄。
2. 開啟左側導覽面板並選擇 [關聯的網域]，然後選擇要新增參數集的網域。

3. 選擇藍圖索引標籤，然後選擇藍 DefaultDataWareshouse 圖以開啟藍圖詳細資料頁面。
4. 在藍圖詳細資料頁面的 [參數集] 索引標籤下，選擇 [建立參數集]。

   - 提供參數組的「名稱」。
   - (可選) 提供參數集的描述。
   - 選擇區域
   - 選取 Amazon Redshift 叢集或 Amazon Redshift 無伺服器。
   - 選取保留所選 Amazon Redshift 叢集或 Amazon Redshift 無伺服器工作群組的登入資料的 AWS 秘密 ARN。 AWS 密碼必須使用標籤加上`AmazonDataZoneDomain : [Domain_ID]`標籤，才有資格在參數組中使用。
     - 如果您沒有現有的 AWS 密碼，也可以選擇建立新密碼來建立新 AWS 密碼。這將打開一個對話框，您可以在其中提供密碼的名稱，用戶名和密碼。一旦您選擇建 DataZone 立新 AWS 密碼，Amazon 就會在 Sec AWS rets Manager 服務中建立一個新密碼，並確保密碼會以您嘗試建立參數集的網域加上標記。
   - 選取 Amazon Redshift 叢集或 Amazon Redshift 無伺服器工作群組。
   - 輸入所選亞馬遜紅移叢集或亞馬遜 Redshift 無伺服器工作群組內的資料庫名稱。
   - 選擇「建立參數組」。

在 AWS 帳戶中啟用 Amazon SageMaker 藍圖後，您可以將參數集新增至藍圖組態。參數集是 Amazon 建立與 Amazon DataZone 的連接所需的一組密鑰和值， SageMaker 並用於創建 Sageemaker 環境。

將參數集添加到 Amazon SageMaker 藍圖

1. 在 https://console.aws.amazon.com/datazone 上導航到 Amazon DataZone 控制台，然後使用您的帳戶憑據登錄。
2. 選擇 [檢視網域]，然後選擇包含要在其中新增參數集之已啟用藍圖的網域。
3. 選擇藍圖索引標籤，然後選擇 Amazon 藍 SageMaker圖以開啟藍圖的詳細資料頁面。
4. 在藍圖詳細資料頁面的 [參數集] 索引標籤下，選擇 [建立參數集]，然後指定下列項目：

   - 提供參數組的「名稱」。
   - (可選) 提供參數集的「描述」。
   - 指定 Amazon SageMaker 網域身份驗證類型。您可以選擇 IAM 或 IAM 身分中心 (SSO)。
   - 指定一個 AWS 區域。

- 指定用於資料加密的 AWS KMS 金鑰。您可以選擇現有的金鑰或建立新金鑰。
- 在「環境參數」下，指定下列項目：
  - VPC ID-您用於 Amazon SageMaker 環境 VPC 的 ID。您可以指定現有的 VPC 或建立新的 VPC。
  - 子網路-VPC 內特定資源的 IP 位址範圍的一或多個 ID。
  - 網路存取-選擇僅限 VPC 或僅公用網際網路。
  - 安全群組-設定 VPC 和子網路時要使用的安全性群組。
- 在 [資料來源參數] 下，選擇下列其中一項：
  - AWS 只有 Glue
  - AWS Glue + Amazon Redshift 無服務器。如果您選擇此選項，請指定下列項目：
    - 指定保留所選 Amazon Redshift 叢集登入資料的 AWS 秘密 ARN。 AWS 密碼必須使用標籤加上`AmazonDataZoneDomain : [Domain_ID]`標籤，才有資格在參數組中使用。

      如果您沒有現有的 AWS 密碼，也可以選擇建立新密碼來建立新 AWS 密碼。這將打開一個對話框，您可以在其中提供密碼的名稱，用戶名和密碼。一旦您選擇建 DataZone 立新 AWS 密碼，Amazon 就會在 Sec AWS rets Manager 服務中建立一個新密碼，並確保密碼會以您嘗試建立參數集的網域加上標記。
    - 指定建立環境時要使用的 Amazon Redshift 工作群組。
    - 指定建立環境時要使用的資料庫名稱 (在您選擇的工作群組內)。
  - AWS 僅 Glue + Amazon Redshift 集群
    - 指定保留所選 Amazon Redshift 叢集登入資料的 AWS 秘密 ARN。 AWS 密碼必須使用標籤加上`AmazonDataZoneDomain : [Domain_ID]`標籤，才有資格在參數組中使用。

      如果您沒有現有的 AWS 密碼，也可以選擇建立新密碼來建立新 AWS 密碼。這將打開一個對話框，您可以在其中提供密碼的名稱，用戶名和密碼。一旦您選擇建 DataZone 立新 AWS 密碼，Amazon 就會在 Sec AWS rets Manager 服務中建立一個新密碼，並確保密碼會以您嘗試建立參數集的網域加上標記。
    - 指定建立環境時要使用的 Amazon Redshift 叢集。
    - 指定建立環境時要使用的資料庫名稱 (在您選擇的叢集內)。

5. 選擇「建立參數組」。

在關聯 AWS 帳戶中將 Amazon 添加 SageMaker 為受信任的服務

如果您已啟用 Amazon SageMaker 藍圖，則還必須新增 SageMaker 為 Amazon 中受信任的服務之一 DataZone。若要這麼做，請完成下列程序：

1. 在 https://console.aws.amazon.com/datazone 上導航到 Amazon DataZone 控制台，然後使用您的帳戶憑據登錄。
2. 選擇 [檢視網域]，然後選擇包含已啟用 SageMaker 藍圖的網域。
3. 選擇受信任的服務，然後選擇 Amazon SageMaker，然後選擇啟用。

移除關聯的帳戶

若要在 Amazon DataZone 管理主控台中移除關聯 AWS 帳戶，您必須在具有管理許可的帳戶中擔任 IAM 角色。 設定使用 Amazon DataZone 管理主控台所需的 IAM 許可以取得最低權限。

請完成下列程序，從您的網域移除相關聯的帳戶。

1. 登入 AWS 管理主控台並開啟 Amazon DataZone 管理主控台，網址為 https://console.aws.amazon.com/datazone。
2. 選擇查看域名，然後從列表中選擇域名。該名稱是一個超鏈接。
3. 向下捲動至 [關聯帳戶] 索引標籤。選擇您要移除的 AWS 帳戶 ID。
4. 選擇取消關聯。在欄位中輸入 [取消關聯] 並選擇 [取消關聯]，以確認您的選擇。
5. 該帳戶現在已從您的網域移除，網域的使用者無法使用此帳戶來發佈和使用資料。

使用 Amazon 數 DataZone 據目錄

您可以使用 Amazon DataZone 商業資料型錄，在組織中分類具有業務內容的資料，從而使組織中的每個人都能快速搜尋和瞭解資料。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。

主題

建立、編輯或刪除商業詞彙

在 Amazon 中 DataZone，商業詞彙表是可能與資產 (資料) 相關聯的商業術語 (文字) 的集合。它為企業使用者提供適當的詞彙和商業術語清單及其定義，以確保整個組織在分析資料時使用相同的定義。商業詞彙表是在目錄領域中建立的，可套用至資產和欄，以協助瞭解該資產或欄的主要特性。可以套用一個或多個辭彙術語。商業詞彙表可以是術語的平面清單，其中商業詞彙表中的任何術語都可以與其他術語的子清單相關聯。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。若要在 Amazon DataZone 網域中建立、編輯或刪除詞彙表，您必須是擁有專案的成員，並且擁有該網域的正確許可。

若要建立辭彙，請完成以下步驟：

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。
2. 導覽至「搜尋」旁邊頂端導覽列中的「目錄」功能表。
3. 在 Amazon DataZone 資料入口網站中，選擇詞彙表，然後選擇「建立詞彙表」。
4. 指定辭彙的名稱、說明、擁有者，然後選擇 [建立辭彙]。
5. 選擇 [啟用] 切換開關以啟用新的辭彙表。
6. 在辭彙的詳細資料頁面上，您可以選擇「建立讀我檔案」來新增一些關於此辭彙的其他資訊。

若要停用或啟用商業辭彙，請完成以下步驟：

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。
2. 導覽至「搜尋」旁邊頂端導覽列中的「目錄」功能表。
3. 在 Amazon DataZone 資料入口網站中，選擇詞彙表，然後找出您要停用/啟用的商業詞彙表。
4. 在辭彙詳細資料頁面上，找出「啟用/停用」開關，然後使用它來啟用或停用您選取的辭彙。

> **Note**
>
> 停用辭彙也會停用其中包含的所有術語。

若要編輯商業辭彙，請完成以下步驟：

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。
2. 導覽至「搜尋」旁邊頂端導覽列中的「目錄」功能表。
3. 在 Amazon 資 DataZone 料入口網站中，選擇詞彙表，然後找出您要編輯的商業詞彙表。
4. 在辭彙詳細資料頁面上，展開 [動作]，然後選擇 [編輯] 以編輯辭彙表。
5. 更新名稱、說明，然後選擇 [儲存]。

若要刪除商業辭彙，請完成以下步驟：

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。
2. 導覽至「搜尋」旁邊頂端導覽列中的「目錄」功能表。
3. 在 Amazon 資 DataZone 料入口網站中，選擇詞彙表，然後找出您要刪除的商業詞彙表。
4. 在辭彙詳細資料頁面上，展開 [動作]，然後選擇 [刪除] 以刪除辭彙表。

> **Note**
>
> 您必須先刪除辭彙表中的所有現有詞彙，才能刪除辭彙。

5. 選擇刪除以確認刪除辭彙。

建立、編輯或刪除辭彙中的字詞

在 Amazon 中 DataZone，商業詞彙表是可能與資產 (資料) 相關聯的商業術語集合。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。若要在 Amazon DataZone 網域中建立、編輯或刪除詞彙表中的詞彙，您必須是擁有專案的成員，並且擁有該網域的正確許可。

在 Amazon 中 DataZone，商業詞彙表術語可以有詳細描述。若要設定特定字詞的前後關聯，您可以指定字詞之間的關係。當您定義術語的關係時，它會自動新增至相關術語的定義中。Amazon 提供的術語詞彙關係 DataZone 包括以下內容：

- 為類型-表示目前詞彙是已識別術語的類型。指出已識別的術語是目前術語的父項。
- 具有類型-表示目前術語是指定特定術語的一般術語。此關係可以表示一般術語的下階術語。

若要建立新詞彙，請完成下列步驟：

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。
2. 導覽至「搜尋」旁邊頂端導覽列中的「目錄」功能表。
3. 在 Amazon 資 DataZone 料入口網站中，選擇詞彙表，然後選擇要在其中建立新詞彙的詞彙表。
4. 指定字詞的名稱、說明、擁有者，然後選擇 [建立字詞]。
5. 選擇「已啟用」切換以啟用新字詞。
6. 若要新增讀我檔案，請瀏覽至術語詳細資料頁面，然後您可以選擇「建立讀我檔案」來新增關於此辭彙的其他資訊。
7. 若要新增關係，請導覽至術語詳細資料頁面，選擇「詞彙關係」區段，然後選擇「新增詞彙術語」。在對話方塊中，選擇您要關聯的關係和術語，然後選擇「關閉」，將字詞新增至適當的關係類型。此關係也會新增至您所建立的所有相關術語中。

若要編輯辭彙中的字詞，請完成下列步驟：

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。
2. 導覽至「搜尋」旁邊頂端導覽列中的「目錄」功能表。
3. 在 Amazon DataZone 資料入口網站中，選擇詞彙表，找出包含您要編輯的詞彙表，然後選擇該詞彙。
4. 在術語詳細資料頁面上，展開 [動作]，然後選擇 [編輯] 以編輯字詞。
5. 更新名稱、說明，然後選擇 [儲存]。

若要刪除辭彙中的字詞，請完成下列步驟：

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。
2. 導覽至「搜尋」旁邊頂端導覽列中的「目錄」功能表。
3. 在 Amazon DataZone 資料入口網站中，選擇詞彙表，找出包含您要刪除的術語的詞彙表，然後選擇該詞彙。
4. 在辭彙詳細資料頁面上，展開 [動作]，然後選擇 [刪除] 以刪除字詞。
5. 選擇刪除以確認刪除字詞。

建立、編輯或刪除中繼資料表單

在 Amazon 中 DataZone，中繼資料表單是簡單的表單，可將額外的業務內容擴充至目錄中的資產中繼資料。它可作為資料擁有者的可擴充機制，以豐富資產的資訊，以協助資料使用者在搜尋和尋找資料時提供協助。中繼資料表單也可提供一種機制，以強制對發佈至 Amazon DataZone 目錄的所有資產執行一致性。

中繼資料表單定義由一或多個欄位定義組成，支援布林值、日期、十進位、整數、字串和商業詞彙表欄位值資料類型。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。若要在 Amazon DataZone 網域中建立、編輯或刪除中繼資料表單，您必須是擁有專案的成員，且擁有正確的登入資料。

若要建立中繼資料表單，請完成以下步驟：

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。
2. 導覽至「搜尋」旁邊頂端導覽列中的「目錄」功能表。
3. 在 Amazon DataZone 資料入口網站中，選擇中繼資料表單，然後選擇建立表單。
4. 指定中繼資料表單名稱、說明、擁有者，然後選擇 [建立表單]。

若要編輯中繼資料表單，請完成以下步驟：

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。
2. 導覽至「搜尋」旁邊頂端導覽列中的「目錄」功能表。
3. 在 Amazon DataZone 資料入口網站中，選擇中繼資料表單，然後找出您要編輯的中繼資料表單。
4. 在中繼資料表單的詳細資料頁面上，展開 [動作]，然後選擇 [編輯]。
5. 更新名稱、說明、擁有者欄位，然後選擇 [更新表單]。

若要刪除中繼資料表單，請完成以下步驟：

> **Note**
>
> 刪除中繼資料表單之前，您必須先從套用該表單的所有資產類型或資產中移除該表單。

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。
2. 導覽至「搜尋」旁邊頂端導覽列中的「目錄」功能表。
3. 在 Amazon 資 DataZone 料入口網站中，選擇中繼資料表單，然後找出要刪除的中繼資料表單。
4. 如果您要刪除的中繼資料表單已啟用，請選擇「啟用」切換來停用中繼資料表單。
5. 在中繼資料表單的詳細資料頁面上，展開 [動作]，然後選擇 [刪除]。

6. 選擇刪除以確認刪除。

建立、編輯或刪除中繼資料表單中的欄位

在 Amazon 中 DataZone，中繼資料表單是簡單的表單，可將額外的業務內容擴充至目錄中的資產中繼資料。它可作為資料擁有者的可擴充機制，以豐富資產的資訊，以協助資料使用者在搜尋和尋找資料時提供協助。中繼資料表單也可提供一種機制，以強制對發佈至 Amazon DataZone 目錄的所有資產執行一致性。

中繼資料表單定義由一或多個欄位定義組成，支援布林值、日期、十進位、整數、字串和商業詞彙表欄位值資料類型。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。若要在 Amazon DataZone 網域中建立、編輯或刪除中繼資料表單中的欄位，您必須是擁有正確登入資料的擁有專案的成員。

若要在中繼資料表單中建立欄位，請完成以下步驟：

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。
2. 導覽至「搜尋」旁邊頂端導覽列中的「目錄」功能表。
3. 在 Amazon DataZone 資料入口網站中，選擇中繼資料表單，然後選擇要在其中建立欄位的中繼資料表單。
4. 在表單的詳細資料頁面上，選擇 [建立欄位]。
5. 指定欄位名稱、說明、類型，以及此欄位是否為必要欄位，然後選擇 [建立欄位]。

若要編輯中繼資料表單中的欄位，請完成以下步驟：

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。
2. 導覽至「搜尋」旁邊頂端導覽列中的「目錄」功能表。
3. 在 Amazon 資 DataZone 料入口網站中，選擇中繼資料表單，然後選擇要編輯欄位的中繼資料表單。
4. 在表單的詳細資料頁面上，選擇您要編輯的欄位，然後展開 [動作]，然後選擇 [編輯]。
5. 更新欄位名稱、說明、類型，以及這是否為必填欄位，然後選擇 [更新欄位]。

若要刪除中繼資料表單中的欄位，請完成以下步驟：

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。
2. 導覽至「搜尋」旁邊頂端導覽列中的「目錄」功能表。
3. 在 Amazon 資 DataZone 料入口網站中，選擇中繼資料表單，然後選擇要刪除欄位的中繼資料表單。
4. 在表單的詳細資訊頁面上，選擇您要刪除的欄位，然後展開 [動作]，然後選擇 [刪除]。
5. 選擇刪除以確認刪除。

在 Amazon 中使用項目和環境 DataZone

在 Amazon 中 DataZone，專案可讓一組使用者在涉及發佈、探索、訂閱和使用 Amazon DataZone 目錄中的資料資產的各種商業使用案例上進行協作。每個 Amazon DataZone 專案都套用了一組存取控制，因此只有獲得授權的個人、群組和角色才能存取專案和此專案訂閱的資料資產，而且只能使用由專案許可取代的工具。專案充當身分識別主體，可接收對基礎資源的存取權授與，讓 Amazon DataZone 能夠在組織的基礎設施中運作，而無需依賴個別使用者的登入資料。如需更多資訊，請參閱Amazon DataZone 術語和概念

主題

建立環境設定檔

在 Amazon 中 DataZone，環境設定檔是可用來建立環境的範本。環境設定檔的目的是透過將 AWS 帳戶和區域等放置資訊嵌入設定檔中，以簡化環境的建立。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。若要在 Amazon DataZone 網域中建立環境設定檔，您必須屬於 Amazon DataZone 專案。所有環境設定檔均由專案所擁有，並且可供任何專案中的所有授權使用者使用，以建立新環境。

建立環境設定檔

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中

存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。

2. 在資料入口網站中，選擇瀏覽專案，然後選取要在其中建立環境設定檔的專案。
3. 導覽至專案中的「環境」頁籤，然後選擇「建立環境設定檔」。
4. 設定下列欄位：

- 名稱 — 環境設定檔的名稱。
- 說明 — (選用) 環境設定檔的說明。
- 擁有者專案-依預設，會在此欄位中選取要建立設定檔的專案。
- 藍圖 — 為其建立此設定檔的藍圖。您可以選擇其中一個預設的 Amazon DataZone 藍圖 (資料湖或資料倉儲)。

  如果您已指定資料倉儲藍圖，請執行下列動作：

  - 提供參數組。若要選取現有參數集，請選擇「選擇參數集」選項。如果您要輸入自己的參數，請選擇 [輸入我自己的參數]。
  - 如果您選擇選取現有參數，請執行下列操作：
    - 從下拉式清單中選取一個 AWS 帳戶。
    - 從下拉式清單中選取參數集。
  - 如果您選擇輸入自己的參數，請執行以下操作：
    - 從下拉式清單中選取「 AWS 帳戶」和「區域」來提供 AWS 參數。
    - 提供 Redshift 數據倉庫參數：
      - 選擇 Amazon Redshift 群集或 Amazon Redshift 無服務器
      - 輸入保留所選亞馬遜紅移叢集或亞馬遜 Redshift 無伺服器工作群組的登入資料的 AWS 秘密 ARN。 AWS 密碼必須使用您要建立環境設定檔的網域 ID 和專案 ID 加上標籤。
        - `AmazonDataZoneDomain: [Domain_ID]`
        - `AmazonDataZoneProject: [Project_ID]`
      - 輸入亞馬遜紅移集群或亞馬 Amazon Redshift 無服務器工作組的名稱。
      - 輸入所選亞馬遜紅移叢集或亞馬遜無伺服器工作群組內的資料庫名稱。
  - 在「授權專案」區段中，指定可以使用環境設定檔來建立環境的專案。根據預設，網域內的所有專案都可以使用帳戶中的環境設定檔來建立環境。若要保留此預設設定，請選擇 [所有專案]。但是，您可以透過將授權專案指派給環境來限制此項目。若要這樣做，請選擇 [僅授權專案]，然後指定可以使用此專案設定檔建立環境的專案。
  - 在「發佈」區段中，選擇下列其中一個選項：

- 從任何結構描述發佈：如果您選擇此選項，則使用此環境設定檔建立的環境可用於從上述 Redshift 參數中選取的資料庫中選取的任何結構描述發行。使用此環境設定檔建立的環境使用者也可以提供自己的 Amazon Redshift 參數，以便從環境設定檔中選取的 AWS 帳戶和區域內的任何結構描述發佈。
- 僅從預設環境結構描述發佈：如果選擇此選項，使用此選項建立的環境只能用於從 Amazon DataZone 為該環境建立的預設結構描述發佈。使用此環境設定檔建立的環境使用者無法提供自己的 Amazon Redshift 參數。
- 不允許發佈：如果您選擇此選項，使用此環境設定檔建立的環境只能用於訂閱和使用資料。環境根本無法用於發佈任何資料。

如果您已指定資料湖藍圖，請執行下列動作：

- 在AWS 帳戶參數區段中，指定 AWS 將在其中建立潛在環境的 AWS 帳戶編號和帳戶區域。
- 在 [授權專案] 區段中，指定可使用環境設定檔搭配內建 Data Lake 環境設定檔來建立環境的專案。依預設，網域內的所有專案都可以使用帳戶中的資料湖藍圖來建立環境設定檔。若要保留此預設設定，請選擇 [所有專案]。但是，您可以透過將專案指派給藍圖來限制此問題。若要這樣做，請選擇 [僅授權專案]，然後指定可以使用此專案設定檔建立環境的專案。
- 在 [資料庫] 區段中，選擇 [任何資料庫] 以啟用從建立環境之 AWS 帳戶和區域內的任何資料庫發佈，或選擇 [僅預設資料庫]，以僅啟用透過環境建立的預設發行資料庫進行發行。

5. 選擇建立環境設定檔。

編輯環境設定檔

在 Amazon 中 DataZone，環境設定檔是可用來建立環境的範本。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。若要編輯 Amazon DataZone 網域中的現有環境設定檔，您必須屬於 Amazon DataZone 專案。

編輯環境設定檔

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 在資料入口網站中，選擇瀏覽專案，然後選取您要編輯環境設定檔的專案。
3. 導覽至專案中的「環境」頁籤，然後選擇「環境設定檔」，然後選擇要編輯的環境設定檔。

   如果您正在編輯資料倉儲環境設定檔，則只能編輯現有環境設定檔的名稱和描述。

如果您正在編輯 Data Lake 環境設定檔，則可以編輯設定檔的名稱和描述，也可以編輯授權使用此設定檔建立環境的專案，並且可以編輯資料庫。若要編輯這些設定，請執行下列動作：

- 在 [授權專案] 區段中，指定可使用環境設定檔搭配內建 Data Lake 環境設定檔來建立環境的專案。依預設，網域內的所有專案都可以使用帳戶中的資料湖藍圖來建立環境設定檔。若要保留此預設設定，請選擇 [所有專案]。但是，您可以透過將專案指派給藍圖來限制此問題。若要這樣做，請選擇 [僅授權專案]，然後指定可以使用此專案設定檔建立環境的專案。
- 在 [資料庫] 區段中，選擇 [任何資料庫] 以啟用從建立環境之 AWS 帳戶和區域內的任何資料庫發佈，或選擇 [僅預設資料庫]，以僅啟用透過環境建立的預設發行資料庫進行發行。

完成編輯後，請選擇「編輯環境設定檔」。

刪除環境設定檔

在 Amazon 中 DataZone，環境設定檔是可用來建立環境的範本。環境設定檔的目的是透過將 AWS 帳戶和區域等放置資訊嵌入設定檔中，以簡化環境的建立。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。若要刪除 Amazon DataZone 網域中的環境設定檔，您必須屬於 Amazon DataZone 專案。

> **Note**
>
> 刪除環境設定檔時，您無法使用此設定檔建立任何其他環境。

刪除環境設定檔

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 在資料入口網站中，選擇 [瀏覽專案]，然後選取要刪除環境設定檔的專案。
3. 導覽至專案中的「環境」頁籤，然後選擇「環境設定檔」，然後選擇要刪除的環境設定檔。
4. 選取您要刪除的環境設定檔，然後選擇「動作」、「刪除」，然後確認刪除。

建立新的環境

在 Amazon DataZone 專案中，環境是已設定資源的集合 (例如，Amazon S3 儲存貯體、 AWS Glue 資料庫或 Amazon Athena 工作群組)，其中包含一組指定的 IAM 主體 (環境使用者角色)，具有可在這些資源上操作的指派擁有者或參與者許可。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。

任何具有 DataZone 存取資料入口網站所需許可的 Amazon 使用者都可以在專案中建立 Amazon DataZone 環境。

若要建立新環境，請完成以下步驟。

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 選擇「瀏覽所有專案」，然後選取要在其中建立新環境的專案。
3. 選擇 [建立環境]，指定下列欄位的值，然後選擇 [建立環境]：

   - 名稱 — 環境名稱
   - 描述 — 環境的描述
   - 環境設定檔 — 選擇現有的環境設定檔或建立新的設定檔。環境設定檔是可用來建立環境的範本。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。

     選取環境設定檔後，在「參數」區段下，指定屬於此環境設定檔一部分的欄位值。

編輯環境

在 Amazon DataZone 專案中，環境是已設定資源的集合 (例如，Amazon S3 儲存貯體、 AWS Glue 資料庫或 Amazon Athena 工作群組)，其中包含一組可在這些資源上操作的 IAM 主體 (具有指派的參與者許可)。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。

任何具有 DataZone 存取資料入口網站所需許可的 Amazon 使用者都可以在專案中編輯 Amazon DataZone 環境。

若要編輯現有環境，請完成以下步驟。

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/

datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。

2. 從頂端導覽窗格中選擇「瀏覽專案」，然後選取包含您要編輯之環境的專案。
3. 尋找並選擇要開啟其詳細資訊頁面的環境。然後展開動作並選擇編輯環境。
4. 編輯環境的名稱和描述，然後選擇「儲存變更」。

刪除環境

在 Amazon DataZone 專案中，環境是已設定資源的集合 (例如，Amazon S3 儲存貯體、 AWS Glue 資料庫或 Amazon Athena 工作群組)，其中包含一組可在這些資源上操作的 IAM 主體 (具有指派的參與者許可)。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。

任何具有 DataZone 存取資料入口網站所需許可的 Amazon 使用者都可以刪除專案內的 Amazon DataZone 環境。

若要刪除現有環境，請完成以下步驟。

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從頂端導覽窗格中選擇「瀏覽專案」，然後選取包含要刪除之環境的專案。
3. 找出並選擇要開啟其詳細資訊頁面的環境，然後展開「動作」 並選擇「刪除環境」。
4. 在 [刪除環境] 快顯視窗`Delete`中，輸入欄位來確認刪除，然後選擇 [刪除環境]。

   只有在刪除與此環境相依性的所有實體之後，您才能成功刪除環境。若要刪除環境，您必須先刪除其所有關聯的資料來源和訂閱目標。

建立新專案

在 Amazon 中 DataZone，專案可讓一組使用者在涉及發佈、探索、訂閱和使用 Amazon DataZone 目錄中的資料資產的各種商業使用案例上進行協作。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。

任何具有 DataZone 存取資料入口網站所需許可的 Amazon 使用者都可以建立 Amazon DataZone 專案。

若要建立新專案，請完成下列步驟。

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 在 Amazon 資 DataZone 料入口網站中，選擇建立專案。
3. 指定下列欄位的值，然後選擇 [建立專案]：
   - 「名稱」— 項目名稱。
   - 「描述」— 計划的描述。

編輯專案

在 Amazon 中 DataZone，專案可讓一組使用者在涉及發佈、探索、訂閱和使用 Amazon DataZone 目錄中的資料資產的各種商業使用案例上進行協作。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。若要編輯 Amazon DataZone 專案，您必須是該專案的擁有者，或是包含此專案之網域的網域管理員。

若要編輯現有專案，請完成以下步驟。

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 選擇 [瀏覽專案]。
3. 選擇您要編輯的專案。如果您在專案清單中看不到它，可以在 [尋找專案] 欄位中指定專案名稱來搜尋它。
4. 展開「動作」 並選擇 「編輯專案」
5. 對專案名稱和說明執行更新，然後選擇 [儲存]。

刪除專案

在 Amazon 中 DataZone，專案可讓一組使用者在涉及發佈、探索、訂閱和/或使用 Amazon DataZone 目錄中的資料資產的各種商業使用案例上進行協作。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。

刪除項目的行為是最終的。刪除不可撤銷地刪除專案的內容，包括資料來源、環境、資產、詞彙表和中繼資料表單。Amazon DataZone 撤銷 Amazon 通過 Lake Formation 和亞 DataZone 馬 Amazon Redshift 放置在受管資產上的贈款。刪除專案並不會刪除 Amazon DataZone 可能幫助您建立的非 Amazon DataZone AWS 資源。如果您不再需要這些 AWS 資源，請在各自的 AWS 服務和帳戶中刪除這些資源。

若要刪除 Amazon DataZone 專案，您必須是該專案的擁有者。

若要刪除現有專案，請完成以下步驟。

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。IAM 主體可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon 主 DataZone 控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從頂部導航窗格中選擇瀏覽項目。
3. 選擇您要刪除的專案。如果您在專案清單中沒有看到它，可以在「尋找專案」欄位中指定專案名稱來搜尋它。
4. 展開「動作」 並選擇「刪除專案」

   檢閱有關刪除專案潛在影響的資訊警告。
5. 如果您接受警告，請輸入確認文字，然後選擇「刪除」。

> **Important**
>
> 刪除專案是不可撤銷的動作，您或由您無法復原。 AWS

> **Note**
>
> 當您或您的網域使用者在專案中建立環境時，Amazon DataZone 會在您的網域或關聯帳戶中建立 AWS 資源，為您和您的網域使用者提供功能。以下是 Amazon DataZone 可能為項目創建的 AWS 資源列表以及默認名稱。刪除專案並不會刪除 AWS 帳戶中的任何 AWS 資源。
>
> - <environmentId>身分與存取權管理角色：
> - <environmentName>Glue 資料庫：(1) <environmentName>_pub_db-*、(2) _ 子資料庫 *。如果已有此名稱的現有資料庫，Amazon DataZone 將新增環境 ID。
> - Athena 工作群組：<environmentName>-*。如果已有此名稱的現有工作群組，Amazon DataZone 將新增環境 ID。

- CloudWatch 記錄群組：資料區 _ <environmentId>

離開專案

在 Amazon 中 DataZone，專案可讓一組使用者在涉及發佈、探索、訂閱和使用 Amazon DataZone 目錄中的資料資產的各種商業使用案例上進行協作。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。

若要離開現有專案，請完成以下步驟。

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 選擇從頂部導航窗格中選擇項目，然後選擇項目。
3. 選擇您要離開的專案。如果您在專案清單中看不到它，可以在 [尋找專案] 欄位中指定專案名稱來搜尋它。
4. 展開「動作」 並選擇「離開專案」

將成員新增至專案

在 Amazon 中 DataZone，專案可讓一組使用者在涉及發佈、探索、訂閱和使用 Amazon DataZone 目錄中的資料資產的各種商業使用案例上進行協作。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。

您必須是專案擁有者或參與者，才能將成員新增至專案。您可以將 SSO 群組、SSO 使用者或 IAM 主體 (角色或使用者) 新增為專案成員。

若要將成員新增至現有的專案，請完成以下步驟。

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 選擇從頂部導航窗格中選擇項目，然後選擇項目。

3. 選擇您要新增記憶體的專案。如果您在專案清單中看不到它，可以在 [尋找專案] 欄位中指定專案名稱來搜尋它。
4. 在專案的詳細資訊頁面上，選取 [成員] 索引標籤，然後選擇 [所有成員] 節點。
5. 在「專案成員」標籤中，選擇「新增成員」。
6. 在 [新增成員至專案] 快顯視窗中，指定您要新增的使用者，並指定其在專案中的角色 (擁有者或參與者)，然後選擇 [新增成員]。

> **Note**
>
> 如果該主體在網域中已有 Amazon DataZone 使用者設定檔，您可以將 IAM 主體新增為專案成員。當 IAM 主體透過入口網站、API 或 CLI 成功與網域互動時，Amazon DataZone 會自動為 IAM 主體建立使用者設定檔。您無法為 IAM 主體建立使用者設定檔。若要在 IAM 主體在網域中沒有現有 Amazon DataZone 使用者設定檔的情況下將 IAM 主體新增為專案成員，請要求管理員在 IAM 主控台中將下列兩個 IAM 許可新增至您AmazonDataZoneDomainExecutionRole的網域：`iam:GetUser`和`iam:GetRole`。另外，若要在網域中執行動作，IAM 主體必須具有此類動作的對應 IAM 許可。

從專案中移除成員

在 Amazon 中 DataZone，專案可讓一組使用者在涉及發佈、探索、訂閱和使用 Amazon DataZone 目錄中的資料資產的各種商業使用案例上進行協作。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。您必須是專案擁有者，才能從專案中移除成員。

若要從現有專案中移除成員，請完成以下步驟。

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。
2. 選擇從頂部導航窗格中選擇項目，然後選擇項目。
3. 選擇您要移除記憶體的專案。如果您在專案清單中看不到它，可以在 [尋找專案] 欄位中指定專案名稱來搜尋它。
4. 在專案的詳細資訊頁面上，選取 [成員] 索引標籤，然後選擇 [所有成員] 節點。
5. 在專案 [成員] 索引標籤中，選擇您要從專案中移除的成員，然後選擇 [移除]。

6. 在「移除成員」快顯視窗中，選擇「移除成員」以確認移除。

在 Amazon 中建立庫存和發佈資料 DataZone

本節描述您要執行的任務和程序，以便在 Amazon 中建立資料庫存以 DataZone 及在 Amazon 中發佈資料 DataZone。

為了使用 Amazon 對數據 DataZone 進行分類，您必須首先將數據（資產）作為 Amazon 項目的庫存 DataZone。建立特定專案的庫存，只有該專案的成員才能找到資產。除非明確發佈，否則並非所有網域使用者都可以在搜尋/瀏覽中使用專案庫存資產。建立專案詳細目錄後，資料擁有者可以新增或更新商業名稱 (資產和結構描述)、說明 (資產和結構描述)、Read me、詞彙術語 (資產和結構描述) 和中繼資料表單，使用所需的業務中繼資料來規劃其庫存資產。

使用 Amazon 對資料 DataZone 進行分類的下一步是讓網域使用者可以探索專案的庫存資產。您可以將庫存資產發佈到 Amazon DataZone 目錄來執行此操作。只有最新版本的庫存資產可以發佈至目錄，而且探索目錄中只有最新發佈的版本處於作用中狀態。如果庫存資產在發佈到 Amazon DataZone 目錄後進行更新，您必須再次明確發佈該資產，以便將最新版本放在探索目錄中。

主題

為 Amazon 配置 Lake Formation 許可 DataZone

使用內建資料湖藍圖 (DefaultDataLake) 建立環境時，Amazon 會新增 AWS Glue 資料庫 DataZone 做為此環境建立程序的一部分。如果您想要從此 AWS Glue 資料庫發佈資產，則不需要其他權限。

但是，如果您想要從 Amazon DataZone 環境外的 AWS Glue 資料庫發佈資產並訂閱資產，則必須明確向 Amazon DataZone 提供存取此外部 AWS Glue 資料庫中資料表的權限。若要執行此操作，您必須在 AWS 湖泊陣型中完成以下設定，並將必要的 Lake Formation 權限附加到AmazonDataZoneGlueAccess-<region>-<domainId>。

- 使用湖泊 Lake Formation 成權限模式或混合存取模式，為 Lake Formation 中 AWS 的資料湖設定 Amazon S3 位置。如需詳細資訊，請register-data-lake參閱：https://docs.aws.amazon.com/lake-formation/latest/dg/
- 從 Amazon DataZone 處理`IAMAllowedPrincipals`許可的 Amazon Lake Formation 表中刪除許可。如需詳細資訊，請參閱 upgrade-glue-lake-formation-background.html。https://docs.aws.amazon.com/lake-formation/latest/dg/
- 將以下 AWS Lake Formation 權限附加到AmazonDataZoneGlueAccess-<region>-<domainId>：
  - `Describe`和表所在的數據庫上的`Describe grantable`權限
  - `Describe`、`Select`、`Describe Grantable`、上述資料庫中您要代表您管理存取`Select Grantable`權 DataZone 的所有表格的權限。

> **Note**
>
> Amazon DataZone 支持 L AWS ake Formation 混合模式。Lake Formation 混合模式可讓您透過 Lake Formation 開始管理 AWS Glue 資料庫和資料表的許可，同時繼續維護這些資料表和資料庫上的任何現有 IAM 許可。如需更多資訊，請參閱Amazon DataZone 與 AWS Lake Formation 混合模式集成

如需詳細資訊，請參閱 Amazon 的 AWS Lake Formation 許可的故障 DataZone。

Amazon DataZone 與 AWS Lake Formation 混合模式集成

Amazon DataZone 與 AWS Lake Formation 混合模式集成。這項整合可讓您輕鬆地透過 Amazon 發佈和共用 AWS Glue 表格， DataZone而無需先在 AWS Lake Formation 中註冊。混合模式可讓您透過 AWS Lake Formation 開始管理 AWS Glue 資料表的許可，同時繼續維護這些資料表上的任何現有 IAM 許可。

若要開始使用，您可以在 Amazon DataZone 管理主控台的DefaultDataLake藍圖下啟用資料位置登錄設定。

啟用與 AWS Lake Formation 混合模式集成

1. 導航到 Amazon DataZone 控制台 https://console.aws.amazon.com/datazone 並使用您的帳戶憑據登錄。
2. 選擇查看域，然後選擇要啟用與 AWS 湖泊形成混合模式集成的域。
3. 在網域詳細資料頁面上，導覽至藍圖索引標籤。
4. 從藍圖清單中選擇藍DefaultDataLake圖。
5. 確保 DefaultDataLake 藍圖已啟用。如果未啟用，請按照中的步驟在在擁有 Amazon DataZone 網域的 AWS 帳戶中啟用內建藍圖您的 AWS 帳戶中啟用它。
6. 在 DefaultDataLake 詳細資訊頁面上，開啟啟動設定索引標籤，然後選擇頁面右上角的編輯按鈕。
7. 在 [資料位置註冊] 下，核取方塊以啟用資料位置註冊。
8. 對於資料位置管理角色，您可以建立新的 IAM 角色或選取現有的 IAM 角色。Amazon DataZone 使用此角色，使 AWS 用湖泊 Lake Formation 混合存取模式管理對資料湖所選 Amazon S3 儲存貯體的讀取/寫入存取。如需詳細資訊，請參閱 AmazonDataZone<region>S3 管理--<domainId>。
9. 或者，如果您不希望 Amazon 以混合模式自動註冊某些 Amazon DataZone S3 位置，您可以選擇排除某些 Amazon S3 位置。為此，請完成以下步驟：
   - 選擇切換按鈕以排除指定的 Amazon S3 位置。
   - 提供您要排除的 Amazon S3 儲存貯體的 URI。
   - 若要新增其他儲存貯體，請選擇新增 S3 位置。

     > **Note**
     >
     > Amazon DataZone 僅允許排除根 S3 位置。根 S3 位置路徑內的任何 S3 位置都會自動從註冊中排除。

   - 選擇儲存變更。

在 AWS 帳戶中啟用資料位置註冊設定後，當資料使用者訂閱透過 IAM 許可管理的 AWS Glue 表時，Amazon DataZone 會先以混合模式註冊此表格的 Amazon S3 位置，然後透過 AWS Lake Formation 管理表格上的許可，以授予資料消費者的存取權。這可確保資料表上的 IAM 許可繼續以新授予的 AWS Lake Formation 權限存在，而不會中斷任何現有的工作流程。

在 Amazon 中啟用 AWS Lake Formation 混合模式整合時，如何處理加密的 Amazon S3 位置 DataZone

如果您使用以客戶受管或受 AWS 管 KMS 金鑰加密的 Amazon S3 位置，則 AmazonDataZoneS3Manage 角色必須具有使用 KMS 金鑰加密和解密資料的權限，否則 KMS 金鑰政策必須授與該角色金鑰的權限。

如果您的 Amazon S3 位置使用 AWS 受管金鑰加密，請將下列內嵌政策新增至AmazonDataZoneDataLocationManagement角色：

```
 {
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:DescribeKey"
    ],
    "Resource": "<AWS managed key ARN>"
  }
]
```

如果您的 Amazon S3 位置使用客戶受管金鑰加密，請執行下列動作：

1. 在 https://console.aws.amazon.com/kms 開啟 AWS KMS 主控台，然後以 AWS Identity and Access Management (IAM) 管理使用者身分登入，或以可修改用於加密位置之 KMS 金鑰金鑰金鑰政策的使用者身分登入。
2. 在瀏覽窗格中，選擇 [客戶受管金鑰]，然後選擇所需 KMS 金鑰的名稱。
3. 在 KMS 金鑰詳細資料頁面上，選擇金鑰原則索引標籤，然後執行下列其中一項動作，以 KMS 金鑰使用者身分新增您的自訂角色或 Lake Formation 服務連結角色：
   - 如果顯示預設檢視 (包含金鑰管理員、金鑰刪除、金鑰使用者和其他 AWS 帳戶區段) — 在 [金鑰使用者] 區段下，新增AmazonDataZoneDataLocationManagement角色。

- 如果金鑰原則 (JSON) 顯示 — 編輯原則，將 AmazonDataZoneDataLocationManagementrole 新增至物件「允許使用金鑰」，如下列範例所示

```
...
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/service-role/
AmazonDataZoneDataLocationManage-<region>-<domain-id>",
                    "arn:aws:iam::111122223333:user/keyuser"
                ]
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        ...
```

> **Note**
>
> 如果 KMS 金鑰或 Amazon S3 位置與資料目錄不在同一個 AWS 帳戶中，請遵循跨 AWS 帳戶註冊加密的 Amazon S3 位置中的指示。

建立自訂資產類型

在 Amazon 中 DataZone，資產代表特定類型的資料資源，例如資料庫表格、儀表板或機器學習模型。為了在描述目錄資產時提供一致性和標準化，Amazon DataZone 網域必須具有一組資產類型，以定義資產在目錄中的表現方式。資產類型可定義特定資產類型的資料架構。資產類型有一組必要和選用的可命名中繼資料表單類型 (例如，GovForm 或 GovernanceFormType)。Amazon 中的資產類型

DataZone 是版本控制的。建立資產時，會根據資產類型 (通常是最新版本) 定義的結構描述來驗證資產，如果指定了無效的結構，則資產建立會失敗。

系統資產類型-Amazon DataZone 佈建服務擁有的系統資產類型 (包括 GlueTableAssetType GlueViewAssetType RedshiftTableAssetType RedshiftViewAssetType、、和 S3ObjectCollectionAssetType) 和系統表單類型 (包括 DataSourceReferenceFormType AssetCommonDetailsFormType、和 SubscriptionTermsFormType)。無法編輯系統資產類型。

自訂資產類型-若要建立自訂資產類型，請先建立要在表單類型中使用的必要中繼資料表單類型和詞彙表。然後，您可以透過指定名稱、說明和相關聯的中繼資料表單來建立自訂資產類型，這些表單可為必要或選用。

對於具有結構化資料的資產類型，若要在資料入口網站中代表欄結構描述，您可以使用將技術中繼資料新增`RelationalTableFormType`至欄，包括欄名稱、說明和資料類型)，`ColumnBusinessMetadataForm`以及新增欄的業務說明，包括商業名稱、詞彙表術語和自訂索引鍵值配對。

若要透過資料入口網站建立自訂資產類型，請完成以下步驟：

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從上方導覽窗格中選擇 [選取專案]，然後選取要在其中建立自訂資產類型的專案。
3. 導覽至專案的「資料」頁籤。
4. 從左側導覽窗格中選擇「資產類型」，然後選擇「建立資產類型」。
5. 指定下列項目，然後選擇 [建立]。
   - 名稱-自訂資產類型的名稱
   - 說明-自訂資產類型的說明。
   - 選擇 [新增中繼資料表單]，將中繼資料表單新增至這個自訂資產
6. 建立自訂資產類型後，您可以使用它來建立資產。

若要透過 API 建立自訂資產類型，請完成以下步驟：

1. 透過叫用 `CreateFormType` API 動作建立中繼資料表單類型。

   以下是一個 Amazon SageMaker 示例：

```
m_model = "

structure SageMakerModelFormType {
   @required
   @amazon.datazone#searchable
   modelName: String

   @required
   modelArn: String

   @required
   creationTime: String
}
"

CreateFormType(
    domainIdentifier="my-dz-domain",
    owningProjectIdentifier="d4bywm0cja1dbb",
    name="SageMakerModelFormType",
    model=m_model
    status="ENABLED"
    )
```

2. 接下來，您可以叫用 CreateAssetType API 動作來建立資產類型。您只能使用可用的系統表單類型 (SubscriptionTermsFormType在以下範例中) 或您的自訂表單類型，透過 Amazon DataZone API 建立資產類型。對於系統表單類型，類型名稱必須以開頭amazon.datazone。

```
CreateAssetType(
    domainIdentifier="my-dz-domain",
    owningProjectIdentifier="d4bywm0cja1dbb",
    name="SageMakerModelAssetType",
    formsInput={
        "ModelMetadata": {
            "typeIdentifier": "SageMakerModelMetadataFormType",
            "typeRevision": 7,
            "required": True,
        },
        "SubscriptionTerms": {
            "typeIdentifier": "amazon.datazone.SubscriptionTermsFormType",
```

```
            "typeRevision": 1,
            "required": False,
        },
    },
)
```

以下是為結構化資料建立資產類型的範例：

```
CreateAssetType(
    domainIdentifier="my-dz-domain",
    owningProjectIdentifier="d4bywm0cja1dbb",
    name="OnPremMySQLAssetType",
    formsInput={
        "OnpremMySQLForm": {
            "typeIdentifier": "OnpremMySQLFormType",
            "typeRevision": 5,
            "required": True,
        },
        "RelationalTableForm": {
            "typeIdentifier": "RelationalTableFormType",
            "typeRevision": 1,
            "required": True,
        },
        "ColumnBusinessMetadataForm": {
            "typeIdentifier": "ColumnBusinessMetadataForm",
            "typeRevision": 1,
            "required": False,
        },
        "SubscriptionTerms": {
            "typeIdentifier": "SubscriptionTermsFormType",
            "typeRevision": 1,
            "required": False,
        },
    },
)
```

3. 現在，您可以使用在上述步驟中建立的自訂資產類型來建立資產。

```
CreateAsset(
   domainIdentifier="my-dz-domain",
   owningProjectIdentifier="d4bywm0cja1dbb",
   owningProjectIdentifier="my-project",
   name="MyModelAsset",
   glossaryTerms="xxx",
   formsInput=[{
        "formName": "SageMakerModelForm",
        "typeIdentifier": "SageMakerModelForm",
        "typeRevision": "5",
        "content": "{\n \"ModelName\" : \"sample-ModelName\",\n \"ModelArn\" :
 \"999999911111\"\n}"
        }
        ]
)
```

在此範例中，您要建立結構化資料資產：

```
CreateAsset(
   domainIdentifier="my-dz-domain",
   owningProjectIdentifier="d4bywm0cja1dbb",
   name="MyModelAsset",
   glossaryTerms="xxx",
   formsInput=[{
        "formName": "RelationalTableForm",
        "typeIdentifier": "amazon.datazone.RelationalTableForm",
        "typeRevision": "1",
        "content": ".."
        },
        {
        "formName": "mySQLTableForm",
        "typeIdentifier": "mySQLTableForm",
        "typeRevision": "6",
        "content": ".."
        },
        {
        "formName": "mySQLTableForm",
        "typeIdentifier": "mySQLTableForm",
        "typeRevision": "1",
```

```
        "content": ".."
        },
        .....
        ]
)
```

建立並執行 Amazon DataZone 資料來源 AWS Glue Data Catalog

在 Amazon 中 DataZone，您可以建立 AWS Glue Data Catalog 資料來源，以便從中匯入資料庫表的技術中繼資料 AWS Glue。若要新增的資料來源 AWS Glue Data Catalog，中必須已存在來源資料庫 AWS Glue。

建立和執行資 AWS Glue 料來源時，您可以將來源資料 AWS Glue 庫中的資產新增至 Amazon DataZone 專案的庫存。您可以按照設定的排程或隨需執行 AWS Glue 資料來源，以建立或更新資產的技術中繼資料。在資料來源執行期間，您可以選擇性地選擇將資產發佈到 Amazon DataZone 目錄，讓所有網域使用者都能探索這些資產。您也可以在編輯專案庫存資產後，發佈其業務中繼資料。網域使用者可以搜尋和探索您已發佈的資產，並要求訂閱這些資產。

若要新增資 AWS Glue 料來源

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從頂端導覽窗格中選擇 [選取專案]，然後選取要新增資料來源的專案。
3. 導覽至專案的「資料」頁籤。
4. 從左側導覽窗格中選擇 [資料來源]，然後選擇 [建立資料來源]。
5. 設定下列欄位：
   - 名稱 — 資料來源名稱。
   - 「描述」— 數據源描述。
6. 在 [資料來源類型] 下，選擇AWS Glue。
7. 在 「選取環境」下，指定要在其中發佈 AWS Glue 表格的環境。
8. 在「資料選取」下，提供資料 AWS Glue 庫並輸入表格選取準則。例如，如果您選擇「包含」並輸入`*corporate`，則資料庫將包含所有以該字結尾的來源表格`corporate`。

您可以從下拉式清單中選擇 AWS Glue 資料庫，也可以輸入資料庫名稱。下拉式清單包括兩個資料庫：發行資料庫和環境的訂閱資料庫。如果您想要將資產帶入不是由環境建立的資料庫，則必須輸入資料庫的名稱，而不是從下拉式清單中選取它。

您可以為單一資料庫中的資料表新增多個納入和排除規則。您也可以使用 [新增其他資料庫] 按鈕來新增多個資料庫。

9. 在 [資料品質] 下，您可以選擇 [啟用此資料來源的資料品質]。如果您這麼做，Amazon 會將您現有的 AWS Glue 資料品質輸出 DataZone匯入您的 Amazon DataZone 目錄。根據預設，Amazon 會從 AWS Glue DataZone 匯入最新的 100 份現有品質報告，且沒有到期日。

   Amazon 中的資料品質指標可 DataZone 協助您瞭解資料來源的完整性和準確性。Amazon 會從 AWS Glue 提 DataZone 取這些資料品質指標，以便在某個時間點 (例如，在商業資料目錄搜尋期間) 提供內容。資料使用者可以查看其訂閱資產的資料品質指標隨時間變化的情形。資料生產者可依排程擷取 AWS Glue 資料品質分數。Amazon DataZone 商業資料型錄也可以透過資料品質 API 顯示第三方系統的資料品質指標。如需更多資訊，請參閱Amazon 的數據質量 DataZone
10. 選擇下一步。
11. 對於「發佈」設定，請選擇是否可立即在業務資料目錄中探索資產。如果您只將它們新增至詳細目錄，您可以稍後選擇訂閱條款，並將其發佈到業務資料目錄。如需詳細資訊，請參閱 the section called “管理現有資料來源”。
12. 對於自動產生商家名稱，請選擇是否要在從來源匯入資產時自動產生中繼資料。
13. (選擇性) 對於中繼資料表單，請新增表單以定義資產匯入 Amazon 時收集和儲存的中繼資料 DataZone。如需詳細資訊，請參閱 the section called “建立、編輯或刪除中繼資料表單”。
14. 對於「執行」偏好設定，請選擇執行資料來源的時間。

    - 按排程執行 — 指定執行資料來源的日期和時間。
    - 按需執行 — 您可以手動啟動資料來源執行。
15. 選擇下一步。
16. 檢閱資料來源組態，然後選擇 [建立]。

為 Amazon 紅移創建和運行亞馬遜 DataZone 數據源

在亞馬遜中 DataZone，您可以建立 Amazon Redshift 資料來源，以便從 Amazon Redshift 資料倉儲匯入資料庫表格和檢視的技術中繼資料。若要為 Amazon Redshift 新增亞馬遜 DataZone 資料來源，來源資料倉儲必須已存在於 Amazon Redshift 中。

當您建立和執行 Amazon Redshift 資料來源時，您可以將來源 Amazon Redshift 資料倉儲中的資產新增到您的 Amazon DataZone 專案的庫存。您可以按照設定的排程或隨需執行 Amazon Redshift 資料來源，以建立或更新資產的技術中繼資料。在資料來源執行期間，您可以選擇選擇將專案庫存資產發佈到 Amazon DataZone 目錄，讓所有網域使用者都能探索這些資產。您也可以在編輯庫存資產的業務中繼資料後發佈資產。網域使用者可以搜尋和探索您已發佈的資產，並要求訂閱這些資產。

若要新增亞 Amazon Redshift 資料來源

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從頂端導覽窗格中選擇 [選取專案]，然後選取要新增資料來源的專案。
3. 導覽至專案的「資料」頁籤。
4. 從左側導覽窗格中選擇 [資料來源]，然後選擇 [建立資料來源]。
5. 設定下列欄位：
   - 名稱 — 資料來源名稱。
   - 「描述」— 數據源描述。
6. 在 [資料來源類型] 下，選擇 [Amazon Redshift]。
7. 在 「選取環境」下，指定要在其中發佈 Amazon Redshift 表格的環境。
8. 視您選取的環境而定，Amazon DataZone 會直接從環境自動套用 Amazon Redshift 登入資料和其他參數，或提供您選擇自己的登入資料的選項。
   - 如果您選擇的環境只允許從環境的預設 Amazon Redshift 架構進行發佈，亞馬遜 DataZone 將自動套用 Amazon Redshift 登入資料和其他參數，包括 Amazon Redshift 叢集或工作群組名稱、 AWS 密碼、資料庫名稱和結構描述名稱。您無法編輯這些自動填入的參數。
   - 如果您選取的環境不允許發佈任何資料，您將無法繼續建立資料來源。
   - 如果您選取允許從任何結構描述發佈資料的環境，您將看到使用該環境中的登入資料和其他 Amazon Redshift 參數的選項，或是輸入您自己的登入資料/參數。
9. 如果您選擇使用自己的認證來建立資料來源，請提供下列詳細資訊：
   - 在「提供亞馬遜 Redshift 登入資料」下，選擇要使用佈建的 Amazon Redshift 叢集還是使用 Amazon Redshift 無伺服器工作區做為您的資料來源。
   - 根據您在上述步驟中的選擇，從下拉式功能表中選擇 Amazon Redshift 叢集或工作區，然後在 AWS Secrets Manager 中選擇要用於身份驗證的密碼。您可以選擇現有密碼或建立新密碼。

- 為了讓現有密碼出現在下拉式清單中，請確定您在 AWS Secret Manager 中的密碼包含下列標籤 (機碼/值)：
  - AmazonDataZoneProject: <projectID>
  - AmazonDataZoneDomain: <domainID>

  如果您選擇建立新密碼，則會自動使用上述標籤來標記密碼，而且不需要額外的步驟。如需詳細資訊，請參閱 < 儲存資料庫認證 > AWS Secrets Manager。

  提供用於建立資料來源的 AWS 密碼中的 Amazon Redshift 使用者必須SELECT擁有要發佈之資料表的許可。如果您希 DataZone 望 Amazon 也代表您管理訂閱（訪問），則 AWS 密碼中的數據庫用戶還必須具有以下許可：
  - `CREATE DATASHARE`
  - `ALTER DATASHARE`
  - `DROP DATASHARE`

10. 在「資料選取」下，提供 Amazon Redshift 資料庫、結構描述，然後輸入您的表格或檢視選取準則。例如，如果您選擇「包含」並輸入`*corporate`，資產將包含所有以該字結尾的來源表格`corporate`。

    您可以為單一資料庫中的資料表新增多個包含規則。您也可以使用 [新增其他資料庫] 按鈕來新增多個資料庫。
11. 選擇下一步。
12. 對於「發佈」設定，請選擇是否可立即在資料目錄中探索資產。如果您只將它們新增至詳細目錄，您可以稍後選擇訂閱條款，並將其發佈到業務資料目錄。如需詳細資訊，請參閱 the section called “管理現有資料來源”。
13. 對於自動產生商家名稱，請選擇是否要在資產發佈和從來源更新時自動產生中繼資料。
14. (選擇性) 對於中繼資料表單，請新增表單以定義資產匯入 Amazon 時收集和儲存的中繼資料 DataZone。如需詳細資訊，請參閱 the section called “建立、編輯或刪除中繼資料表單”。
15. 對於「執行」偏好設定，請選擇執行資料來源的時間。
    - 按排程執行 — 指定執行資料來源的日期和時間。
    - 按需執行 — 您可以手動啟動資料來源執行。
16. 選擇下一步。
17. 檢閱資料來源組態，然後選擇 [建立]。

管理現有 Amazon DataZone 資料來源

建立 Amazon DataZone 資料來源後，您可以隨時修改它以變更來源詳細資訊或資料選取準則。當您不再需要資料來源時，可以將其刪除。

若要完成這些步驟，您必須附加受AmazonDataZoneFullAccess AWS 管理的原則。如需詳細資訊，請參閱 the section called “AWS 受管理政策”。

主題

編輯資料來源

您可以編輯 Amazon DataZone 資料來源以修改其資料選取設定，包括新增、移除或變更表格選取條件。您也可以新增和移除資料庫。您無法變更資料來源類型或發佈資料來源的環境。

編輯資料來源

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從頂端導覽窗格中選擇 [選取專案]，然後選取資料來源所屬的專案。
3. 導覽至專案的「資料」頁籤。
4. 從左側導覽窗格中選擇 [資料來源]，然後選擇您要修改的資料來源。
5. 導覽至「資料來源定義」標籤，然後選擇「編輯」。
6. 對資料來源定義進行變更。您可以更新資料來源詳細資訊，並變更資料選取準則。
7. 修改完成後，請選擇 Save (儲存)。

刪除資料來源

當您不再需要 Amazon 資 DataZone 料來源時，可以永久移除它。刪除資料來源後，所有源自該資料來源的資產仍可在目錄中使用，且使用者仍然可以訂閱這些資產。但是，資產將停止從來源接收更新。建議您先將相依資產移至其他資料來源，然後再刪除它。

> **Note**
>
> 您必須先移除資料來源上的所有出貨，然後才能刪除它。如需詳細資訊，請參閱 探索、訂閱和使用 Amazon 中的資料 DataZone。

刪除資料來源

1. 在專案的 [資料] 索引標籤上，從左側導覽窗格中選擇 [資料來源]。
2. 選擇您要刪除的資料來源。
3. 選擇 [動作]、[刪除資料來源] 並確認刪除。

從專案庫存將資產發佈到 Amazon DataZone 目錄

您可以將 Amazon DataZone 資產及其中繼資料從專案清單發佈到 Amazon 目 DataZone 錄中。您只能將資產的最新版本發佈至目錄。

將資產發佈至目錄時，請考量下列事項：

- 若要將資產發佈至目錄，您必須是該專案的擁有者或參與者。
- 對於 Amazon Redshift 資產，請確保與發佈者和訂閱者叢集相關聯的 Amazon Redshift 叢集符合 Amazon Redshift 資料共用的所有要求，以便 Amazon DataZone 管理 Redshift 表格和檢視的存取。請參閱 Amazon Redshift 的資料共用概念。
- Amazon DataZone 僅支持從和亞馬 Amazon Redshift 發布的資產 AWS Glue Data Catalog 的訪問管理。對於所有其他資產 (例如 Amazon S3 物件)，Amazon DataZone 不會管理已核准訂閱者的存取權。如果您訂閱這些未受管理的資產，系統會通知您下列訊息：

  ```
  Subscription approval does not provide access to data. Subscription
  grants on this asset are not managed by Amazon DataZone. For more
  information or help, reach out to your administrator.
  ```

發佈資產

如果您在建立資料來源時未選擇讓資產立即可在資料目錄中找到，請執行下列步驟以稍後發佈資產。

若要發佈資產

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從頂端導覽窗格中選擇「選取專案」，然後選取資產所屬的專案。
3. 導覽至專案的「資料」頁籤。
4. 從左側導覽窗格中選擇「庫存資料」，然後選取您要發佈的資產。

   > **Note**
   >
   > 依預設，所有資產都需要訂閱核准，這表示資料擁有者必須核准資產的所有訂閱請求。如果您要在發佈資產之前變更此設定，請開啟資產詳細資料，然後選擇 「訂閱核准」旁邊的「編輯」。您可以稍後修改並重新發佈資產來變更此設定。

5. 選擇「發佈資產」。資產會直接發佈至目錄。

   如果您對資產進行變更 (例如修改其核准需求)，您可以選擇「重新發佈」，將更新發佈至目錄。

管理庫存和策劃資產

為了使用 Amazon 對數據 DataZone 進行分類，您必須首先將數據（資產）作為 Amazon 項目的庫存 DataZone。建立特定專案的庫存，只有該專案的成員才能找到資產。

在專案詳細目錄中建立資產後，即可策劃其中繼資料。例如，您可以編輯資產的名稱、說明或讀取我資訊。每次對資產進行編輯都會建立資產的新版本。您可以使用資產詳細資料頁面上的「歷史記錄」標籤來檢視所有資產版本。

您可以編輯「讀我」區段，並新增資產的豐富說明。「讀我」區段支援 markdown，因此您可以根據需要設定說明的格式，並向消費者描述有關資產的重要資訊。

您可以填寫可用的表格，在資產層級新增詞彙術語。

若要組織結構描述，您可以檢閱資料欄、新增商家名稱、說明，以及在欄層級新增詞彙術語。

如果在建立資料來源時啟用了自動化中繼資料產生功能，則資產和欄的企業名稱可供個別檢閱和接受或拒絕，或者一次全部檢閱和接受或拒絕。

您也可以編輯訂閱條款，以指定是否需要核准資產。

Amazon 中的中繼資料表單可 DataZone 讓您新增自訂屬性 (例如銷售區域、銷售年度和銷售季度) 來擴充資料資產的中繼資料模型。附加至資產類型的中繼資料表單會套用至從該資產類型建立的所有資產。您也可以在資料來源執行過程中或建立資料來源之後，將其他中繼資料表單新增至個別資產。若要建立新表單，請參閱the section called “建立、編輯或刪除中繼資料表單”。

若要更新資產的中繼資料，您必須是資產所屬專案的擁有者或參與者。

更新資產的中繼資料的步驟

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從上方導覽窗格中選擇「選取專案」，然後選取包含您要更新其中繼資料之資產的專案。
3. 導覽至專案的「資料」頁籤。
4. 從左側導覽窗格中選擇「庫存資料」，然後選擇要更新其中繼資料的資產名稱。
5. 在資產詳細資料頁面的「中繼資料表單」下，選擇「編輯」，然後視需要編輯現有表單。您也可以將其他中繼資料表單附加至資產。如需詳細資訊，請參閱 the section called “附加其他中繼資料表單至資產”。
6. 完成更新後，請選擇 [儲存表格]。

   當您儲存表單時，Amazon DataZone 會產生資產的新庫存版本。若要將更新版本發佈至目錄，請選擇「重新發佈資產」。

附加其他中繼資料表單至資產

依預設，附加至網域的中繼資料表單會附加至發佈至該網域的所有資產。資料發佈者可以將其他中繼資料表單關聯至個別資產，以提供其他內容。

將其他中繼資料表單附加至資產

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從頂端導覽窗格中選擇「選取專案」，然後選取包含要新增其中繼資料的資產的專案。

3. 導覽至專案的「資料」頁籤。
4. 從左側導覽窗格中選擇「庫存資料」，然後選擇要新增其中繼資料的資產名稱。
5. 在資產詳細資料頁面的「中繼資料表單」下，選擇「新增表單」。
6. 選取要新增至資產的表單，然後選擇「新增表單」。
7. 輸入每個中繼資料欄位的值，然後選擇「儲存表格」。

   當您儲存表單時，Amazon DataZone 會產生資產的新庫存版本。若要將更新版本發佈至目錄，請選擇「重新發佈資產」。

組織後將資產發佈至目錄

一旦對資產管理感到滿意，資料擁有者就可以將資產版本發佈到 Amazon DataZone 目錄，因此所有網域使用者都可以探索資產版本。資產會顯示庫存版本和已發佈的版本。在探索目錄中，只會顯示最新發佈的版本。如果中繼資料在發佈後更新，則新的詳細目錄版本將可用於發佈至目錄。

手動建立資產

在 Amazon 中 DataZone，資產是顯示單一實體資料物件 (例如資料表、儀表板、檔案) 或虛擬資料物件 (例如檢視) 的實體。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。手動發佈資產是一次性作業。您不會為資產指定執行排程，因此資產的來源變更時不會自動更新。

若要透過專案手動建立資產，您必須是該專案的擁有者或參與者。

手動建立資產

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從頂端導覽窗格中選擇「選取專案」，然後選取要建立資產的專案。
3. 導覽至專案的「資料」頁籤。
4. 從左側導覽窗格中選擇 [資料來源]，然後選擇 [建立資料資產]。
5. 如需資產詳細資訊，請設定下列設定：

   - 資產類型 — 資產類型。
   - 名稱 — 資產的名稱。

- 描述 — 資產的描述。

6. 對於 S3 位置，請輸入來源 S3 儲存貯體的 Amazon 資源名稱 (ARN)。

   選擇性地輸入 S3 存取點。如需詳細資訊，請參閱使用 Amazon S3 存取點來管理資料存取。

7. 對於「發佈」設定，請選擇是否可立即在目錄中尋找資產。如果您只將它們新增至詳細目錄，則可以稍後選擇訂閱條款以將其發佈至目錄。

8. 選擇建立。

   建立資產後，資產將直接發佈為目錄中的作用中資產，或儲存在詳細目錄中，直到您決定發佈資產為止。

從 Amazon DataZone 目錄中取消發布資產

從目錄中取消發佈 Amazon DataZone 資產時，該資產不會再出現在全域搜尋結果中。新使用者將無法在目錄中尋找或訂閱資產清單，但所有現有的訂閱保持不變。

若要取消發佈資產，您必須是資產所屬專案的擁有者或參與者：

若要取消發佈資產

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從頂端導覽窗格中選擇「選取專案」，然後選取資產所屬的專案。
3. 導覽至專案的「資料」頁籤。
4. 從左側導覽窗格中選擇 [已發佈的資料]。
5. 從已發佈資產清單中找出資產，然後選擇「取消發佈」。

   資產即會從目錄中移除。您可以選擇「發佈」，隨時重新發佈資產。

刪除 Amazon DataZone 資產

當您不再需要 Amazon 中的資產時 DataZone，可以將其永久刪除。刪除資產與從目錄中取消發佈資產不同。您可以刪除目錄中的資產及其相關清單，這樣就不會顯示在任何搜尋結果中。若要刪除資產清單，您必須先撤銷其所有訂閱項目。

若要刪除資產，您必須是資產所屬專案的擁有者或參與者：

> **Note**
>
> 若要刪除資產清單，您必須先撤銷該資產的所有現有訂閱項目。您無法刪除擁有現有訂閱者的資產清單。

若要刪除和資產

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從上方導覽窗格中選擇 [選取專案]，然後選取包含您要刪除之資產的專案。
3. 導覽至專案的「資料」頁籤。
4. 從左側導覽窗格中選擇「已發佈的資料」，然後找出並選擇您要刪除的資產。這會開啟資產詳細資訊頁面。
5. 選擇「操作」，「刪除」並確認刪除。

   刪除資產後，就無法再檢視資產，使用者也無法訂閱該資產。

手動啟動在 Amazon 中運行的數據源 DataZone

當您執行資料來源時，Amazon 會從來源 DataZone 提取所有新的或修改過的中繼資料，並更新庫存中的相關資產。將資料來源新增至 Amazon 時 DataZone，您可以指定來源的執行偏好設定，該偏好設定定義來源是按排程執行還是按需執行。如果您的來源依需求執行，您必須手動啟動資料來源執行。

即使您的來源按排程執行，您仍然可以隨時手動執行。將商業中繼資料新增至資產後，您可以選取資產並將其發佈到 Amazon DataZone 目錄，以便所有網域使用者都能探索這些資產。其他網域使用者只能搜尋已發佈的資產。

手動執行資料來源的步驟

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。

2. 從頂端導覽窗格中選擇 [選取專案]，然後選取資料來源所屬的專案。
3. 導覽至專案的「資料」頁籤。
4. 從左側導覽窗格中選擇 [資料來源]，然後找出並選擇您要執行的資料來源。這會開啟資料來源詳細資訊頁面。
5. 選擇「視需求執行」。

   `Running`當 Amazon 使用來源的最新資料 DataZone 更新資產中繼資料時，資料來源狀態會變更為。您可以在 [資料來源執行] 索引標籤上監視執行狀態。

Amazon 中的資產修訂 DataZone

當您編輯資產的業務或技術中繼資料時，Amazon 會 DataZone 增加資產的修訂。這些編輯包括修改資產名稱、說明、辭彙字詞、欄名稱、中繼資料表單和中繼資料表單欄位值。這些變更可能是由於手動編輯、資料來源工作執行或 API 作業所導致。Amazon DataZone 會在您對資產進行編輯時自動產生新的資產修訂。

更新資產並產生新修訂後，您必須將新修訂發佈至目錄，以便更新該資產並可供訂閱者使用。如需詳細資訊，請參閱 the section called “從專案庫存將資產發佈至目錄”。您只能將資產的最新版本發佈至目錄。

若要檢視資產的過去修訂

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從頂端導覽窗格中選擇 [選取專案]，然後選取包含資產的專案。
3. 導覽至專案的「資料」標籤，然後找出並選擇資產。這會開啟資產詳細資訊頁面。
4. 導覽至「歷程」索引標籤，此標籤會顯示資產過去修訂的清單。

Amazon 的數據質量 DataZone

Amazon 中的資料品質指標可 DataZone 協助您了解不同的品質指標，例如資料來源的完整性、及時性和準確性。Amazon 與 AWS Glue 資料品質 DataZone整合，並提供 API 以整合來自第三方資料品質解決方案的資料品質指標。資料使用者可以查看其訂閱資產的資料品質指標隨時間變化的情形。若要編寫並執行資料品質規則，您可以使用您選擇的資料品質工具，例如 AWS Glue 資料品質。透過 Amazon

中的資料品質指標 DataZone，資料消費者可以視覺化資產和資料欄的資料品質分數，協助建立對決策所用資料的信任度。

先決條件和 IAM 角色變更

如果您使用 Amazon 的 AWS 受管 DataZone政策，則不需要額外的組態步驟，而且這些受管政策會自動更新以支援資料品質。如果您使用自己的政策來授予 Amazon DataZone 與支援的服務互通所需權限的角色，則必須更新附加到這些角色的政策，以支援讀取中的 AWS Glue 資料品質資訊，AWS 受管理的策略：AmazonDataZoneGlueManageAccessRolePolicy並支援AWS 受管理的策略：AmazonDataZoneDomainExecutionRolePolicy和中的時間序列 API。AWS 受管理的策略：AmazonDataZoneFullUserAccess

啟用 AWS Glue 資產的資料品質

Amazon 會從 AWS Glue DataZone 擷取資料品質指標，以便在某個時間點 (例如，在搜尋業務資料目錄期間) 提供內容。資料使用者可以查看其訂閱資產的資料品質指標隨時間變化的情形。資料生產者可依排程擷取 AWS Glue 資料品質分數。Amazon DataZone 商業資料型錄也可以透過資料品質 API 顯示第三方系統的資料品質指標。如需詳細資訊，請參閱資料目錄的 G AWS lue 資料品質和 AWS Glue 資料品質入門。

您可以透過下列方式為 Amazon 資 DataZone 產啟用資料品質指標：

- 使用資料入口網站或 Amazon DataZone API，在建立新的或編輯現有 AWS Glue 資料來源時，透過 Amazon DataZone 資料入口網站為 AWS Glue 資料來源啟用資料品質。

  如需透過入口網站為資料來源啟用資料品質的詳細資訊，請參閱建立並執行 Amazon DataZone 資料來源 AWS Glue Data Catalog和管理現有 Amazon DataZone 資料來源。

  > **Note**
  >
  > 您可以使用資料入口網站，僅為 AWS Glue 庫存資產啟用資料品質。在此版本的亞馬遜中，不支援透過資料入口網站為 Amazon Redshift 或自訂類型資產 DataZone 啟用資料品質。

  您也可以使用 API 來啟用新資料來源或現有資料來源的資料品質。您可以通過調用CreateDataSource或UpdateDataSource並將`autoImportDataQualityResult`參數設置為「真」來執行此操作。

  啟用資料品質後，您可以依需求或按排程執行資料來源。每次執行每項資產最多可產生 100 個指標。使用資料來源獲得資料品質時，無需手動建立表單或新增指標。資產發佈時，對資料品質表單所

做的更新 (每個歷史記錄規則最多 30 個資料點) 會反映在消費者的清單中。隨後，資產的每個新增量度都會自動新增至清單。消費者無需重新發佈資產即可獲得最新分數。

啟用自訂資產類型的資料品質

您可以使用 Amazon DataZone API 為任何自訂類型資產啟用資料品質。如需詳細資訊，請參閱下列內容：

- PostTimeSeriesDataPoints
- ListTimeSeriesDataPoints
- GetTimeSeriesDataPoint
- DeleteTimeSeriesDataPoints

以下步驟提供使用 API 或 CLI 為 Amazon 中資產匯入第三方指標的範例 DataZone：

1. 調用 `PostTimeSeriesDataPoints` API，如下所示：

```
aws datazone post-time-series-data-points  \
--cli-input-json file://createTimeSeriesPayload.json \
```

具有以下有效載荷：

```
{
"domainIdentifier": "dzd_bqqlk3nz21zp2f",
"entityIdentifier": "4nwl5ew0dsu27b",
"entityType": "ASSET",
"forms": [
{
"content": "{\n \"evaluationsCount\" : 11,\n \"evaluations\" : [ {\n \"description
\" : \"IsComplete \\\"Id\\\"\",\n \"details\" : {\n \"STATISTIC_NAME\" :
 \"Completeness\",\n \"COLUMN_NAME\" : \"Id\"\n },\n \"status\" : \"PASS\"\n },
 {\n \"description\" : \"Uniqueness \\\"Id\\\" > 0.95\",\n \"details\" : {\n
 \"STATISTIC_NAME\" : \"Uniqueness\",\n \"COLUMN_NAME\" : \"Id\"\n },\n \"status
\" : \"PASS\"\n }, {\n \"description\" : \"ColumnLength \\\"Id\\\" = 18\",\n
 \"details\" : {\n \"STATISTIC_NAME\" : \"MinimumLength,MaximumLength\",\n
 \"COLUMN_NAME\" : \"Id,Id\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
```

```
\" : \"IsComplete \\\"IsDeleted\\\"\",\n \"details\" : {\n \"STATISTIC_NAME\" :
 \"Completeness\",\n \"COLUMN_NAME\" : \"IsDeleted\"\n },\n \"status\" : \"PASS
\"\n }, {\n \"description\" : \"Completeness \\\"Type\\\" >= 0.59\",\n \"details
\" : {\n \"STATISTIC_NAME\" : \"Completeness\",\n \"COLUMN_NAME\" : \"Type\"\n },
\n \"status\" : \"PASS\"\n }, {\n \"description\" : \"ColumnValues \\\"Type\
\\" in [\\\"Customer - Direct\\\",\\\"Customer - Channel\\\"] with threshold
 >= 0.8\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"\",\n \"COLUMN_NAME\" :
 \"\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description\" : \"ColumnLength \\
\"Type\\\" <= 18\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"MaximumLength\",\n
 \"COLUMN_NAME\" : \"Type\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
\" : \"ColumnLength \\\"ParentId\\\" <= 18\",\n \"details\" : {\n \"STATISTIC_NAME
\" : \"MaximumLength\",\n \"COLUMN_NAME\" : \"ParentId\"\n },\n \"status\" :
 \"PASS\"\n }, {\n \"description\" : \"Completeness \\\"AnnualRevenue\\\" >=
 0.28\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"Completeness\",\n \"COLUMN_NAME
\" : \"AnnualRevenue\"\n },\n \"status\" : \"PASS\"\n }, {\n \"description
\" : \"StandardDeviation \\\"AnnualRevenue\\\" between 1658483123.39 and
 1833060294.28\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"StandardDeviation
\",\n \"COLUMN_NAME\" : \"AnnualRevenue\"\n },\n \"status\" : \"PASS\"\n }, {\n
 \"description\" : \"ColumnValues \\\"AnnualRevenue\\\" between 29999999 and
 5600000001\",\n \"details\" : {\n \"STATISTIC_NAME\" : \"Minimum,Maximum\",\n
 \"COLUMN_NAME\" : \"AnnualRevenue,AnnualRevenue\"\n },\n \"status\" : \"PASS
\"\n } ],\n \"passingPercentage\" : 1.0\n}",
"formName": "GREAT_EXPECTATION_NEW",
"typeIdentifier": "amazon.datazone.DataQualityResultFormType",
"timestamp": 1608969556
}
]
}
```

2. 調用 DeleteTimeSeriesDataPoints API，如下所示：

```
aws datazone delete-time-series-data-points\
--domain-identifier dzd_bqqlk3nz21zp2f \
--entity-identifier dzd_bqqlk3nz21zp2f \
--entity-type ASSET \
--form-name rulesET1 \
```

使用機器學習和生成人工智慧

> **Note**
>
> 由 Amazon 基岩提供支援： AWS 實作自動濫用偵測。由於 Amazon 中針對描述功能的 AI 建議 DataZone 是建立在 Amazon 基岩上，因此使用者會繼承 Amazon 基岩中實作的控制項，以強制執行人工智慧的安全性、安全性和負責任的使用。

在目前版本的 Amazon 中 DataZone，您可以使用 AI 建議提供描述功能來自動化資料探索和編目。Amazon 中對生成 AI 和機器學習的 Support 可 DataZone 建立資產和欄的說明。您可以使用這些說明為資料新增業務內容，並為資料集提供分析建議，這有助於提升資料探索結果。

Amazon 中針對資料資產描述的 AI 建議採用 Amazon 基岩的大型語言模型，可 DataZone 協助您確保資料易於理解且易於探索。AI 建議也會針對資料集提供最相關的分析應用程式。透過減少手動文件工作並針對適當的資料使用提供建議，自動產生的描述可協助您提升資料的可信度，並將有價值的資料忽略到最少，從而加速做出明智的決策。

> **Important**
>
> 在目前的 Amazon DataZone 版本中，僅支援下列區域的 AI 描述建議功能：
>
> - 美國東部 (維吉尼亞北部)
> - 美國西部 (奧勒岡)
> - 歐洲 (法蘭克福)
> - 亞太區域 (東京)

下列程序說明如何針對 Amazon 中的說明產生 AI 建議 DataZone：

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，請瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的 AWS 帳戶 位置登入，然後選擇開啟資料入口網站。
2. 在頂端導覽窗格中，選擇 [選取專案]，然後選擇包含您要針對其產生描述之 AI 建議之資產的專案。
3. 導覽至專案的「資料」頁籤。

4. 在左側導覽窗格中，選擇 [詳細目錄資料]，然後選擇要為其產生資產描述之 AI 建議的資產名稱。
5. 在資產的詳細資料頁面的 [商務中繼資料] 索引標籤中，選擇 [產生說明]。
6. 產生描述後，您可以編輯、接受或拒絕它們。綠色圖示會顯示在資料資產的每個自動產生的中繼資料描述旁邊。在 [商務中繼資料] 索引標籤中，您可以選擇自動產生的 [摘要] 旁邊的綠色圖示，然後選擇 [編輯]、[接受] 或 [拒絕]，以解決產生的描述。您也可以選擇「全部接受」或「拒絕所有」選項，這些選項會在頁面頂端選取「商務中繼資料」標籤，因此對所有自動產生的描述執行選取的動作。

   或者，您可以選擇 [結構描述] 索引標籤，然後一次選擇一個資料欄說明的綠色圖示，然後選擇 [接受] 或 [拒絕]，以個別處理自動產生的描述。在「結構描述」頁籤中，您也可以選擇「全部接受」或「全部拒絕」，從而對所有自動產生的描述執行選取的動作。
7. 若要將資產發佈至含有產生說明的目錄，請選擇「發佈資產」，然後在「發佈資產」快顯視窗中再次選擇「發佈資產」，以確認此動作。

> **Note**
>
> 如果您不接受或拒絕資產產生的說明，然後發佈此資產，則此未審核自動產生的中繼資料不會包含在已發佈的資料資產中。

探索、訂閱和使用 Amazon 中的資料 DataZone

在 Amazon 中 DataZone，一旦將資產發佈到網域，訂閱者就可以探索並請求訂閱此資產。訂閱程序從訂閱者搜尋和瀏覽目錄以尋找他們想要的資產開始。在 Amazon 入 DataZone口網站中，他們選擇透過提交訂閱請求來訂閱資產，其中包括理由和請求原因。訂閱核准者 (如發佈合約中所定義)，然後檢閱存取要求。他們可以核准或拒絕請求。

授與訂閱之後，出貨程序便會開始以便於訂閱者存取資產。資產存取控制和履行有兩種主要模式：適用於 Amazon DataZone 管理的資產，以及非 Amazon DataZone 管理的資產。

- 受管資產 — Amazon DataZone 可以管理受管資產的履行和許可，例如資 AWS Glue 料表和 Amazon Redshift 表格和檢視。
- 非受管資產 — Amazon 將與您的動作相關的標準事件 (例如，授予訂閱請求的核准) DataZone 發佈給 Amazon EventBridge。您可以使用這些標準事件與其他 AWS 服務或第三方解決方案整合，以進行自訂整合。

主題

探索資料

下列任務說明在 Amazon 中探索資料的各種方法 DataZone。

主題

搜尋和檢視目錄中的資產

Amazon DataZone 提供了一種簡化的方式來搜索數據。任何具有存取資料入口網站權限的 Amazon DataZone 使用者都可以搜尋 Amazon DataZone 目錄中的資產，並檢視資產名稱和指派給他們的中繼資料。您可以檢查資產的詳細資訊頁面，仔細查看資產。

> **Note**
>
> 若要檢視資產包含的實際資料，您必須先訂閱該資產，並核准訂閱要求並授予存取權。如需詳細資訊，請參閱 訂閱資料。

搜尋目錄中的資產

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 您可以在資料入口網站首頁的搜尋列中輸入要尋找的資產名稱。
3. 若要瀏覽命名空間，請從頁面右上角選擇目錄以開啟目錄。目錄提供多面化的搜尋體驗，讓您透過搜尋資料擁有者和詞彙字詞等條件來尋找資產。
4. 在其中一個搜尋方塊中輸入您的搜尋字詞。執行搜尋後，您可以套用各種篩選器來縮小搜尋結果範圍。結果包括資產類型、來源帳戶 AWS 區域 以及資產所屬的帳戶。
5. 若要檢視特定資產的詳細資訊，請選擇要開啟其詳細資訊頁面的資產。詳細資訊頁面包含下列資訊：

   - 資產名稱、資料來源 (AWS Glue Amazon Redshift 或 Amazon S3)、類型 (資料表、檢視或 S3 物件)、欄數和大小。
   - 資產的描述。
   - 資產目前發佈的修訂版本、擁有者、訂閱、名稱和更新記錄是否需要核准。
   - 「概觀」標籤，其中包含詞彙詞彙和中繼資料表單。
   - 「結構描述」標籤，顯示資產的結構描述，包括業務和技術欄名稱、資料類型，以及欄的商業說明。結構描述索引標籤僅適用於資料表和檢視 (不適用於 Amazon S3 物件)。
   - 「訂閱」索引標籤，其中包含網域的訂閱者清單。
   - 「歷史記錄」標籤，其中包含資產過去修訂的清單。

訂閱資料

下列任務提供訂閱 Amazon DataZone 資產的詳細資訊。

主題

要求訂閱資產

Amazon DataZone 允許您查找，訪問和使用 Amazon DataZone 目錄中的資產。當您在目錄中找到想要存取的資產時，您需要訂閱該資產，以建立訂閱請求。然後，核准者可以核准或請求您的請求。

您必須是專案的成員，才能要求訂閱該專案中的資產。

若要訂閱資產

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 使用搜尋列搜尋並選擇您要訂閱的資產，然後選擇 [訂閱]。
3. 在「訂閱」快顯視窗中，提供下列資訊：
   - 您要訂閱資產的專案。
   - 訂閱請求的簡短理由。
4. 選擇 Subscribe (訂閱)。

   當發佈者核准您的請求時，您會在資料入口網站中收到通知。

若要檢視訂閱要求的狀態，請找出並選擇您訂閱資產的專案。導覽至專案的 [資料] 索引標籤，然後從左側導覽窗格中選擇 [要求的資料]。此頁面會列出專案要求存取的資產。您可以依要求狀態篩選清單。

核准或拒絕訂閱要求

Amazon DataZone 允許您查找，訪問和使用 Amazon DataZone 目錄中的資產。當您在目錄中找到想要存取的資產時，您必須訂閱該資產，以建立訂閱請求。然後，核准者可以核准或拒絕您的請求。

您必須是擁有專案 (發佈資產的專案) 的成員，才能核准或拒絕訂閱要求。

核准或拒絕訂閱要求

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 在資料入口網站中，選擇 [瀏覽專案清單]，然後選取包含含有訂閱要求之資產的專案。
3. 導覽至 [資料] 索引標籤，然後從左側導覽窗格中選擇 [內送要求]。
4. 找出要求，然後選擇 [檢視請求]。您可以依 「擱置中」 進行篩選，以僅查看仍處於開啟狀態的要求。
5. 檢閱訂閱要求和存取原因，並決定要核准還是拒絕。
6. (選擇性) 輸入回應，說明您接受或拒絕請求的理由。
7. 選擇「核准」或「拒絕」。

身為專案擁有者，您可以隨時撤銷訂閱。如需詳細資訊，請參閱 the section called “撤銷現有的訂閱”。

若要檢視所有訂閱要求，請參閱使用 Amazon DataZone 事件和通知。

撤銷現有的訂閱

Amazon DataZone 允許您查找，訪問和使用 Amazon DataZone 目錄中的資產。當您在目錄中找到想要存取的資產時，您需要訂閱該資產，以建立訂閱請求。然後，核准者可以核准或請求您的請求。您可能需要在核准訂閱之後撤銷訂閱，可能是因為核准錯誤，或是訂閱者不再需要存取資產。

您必須是擁有專案 (發佈資產的專案) 的成員，才能撤銷訂閱。

撤銷訂閱

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從上方導覽窗格中選擇 [選取專案]，然後選取包含您要撤銷之訂閱的專案。
3. 導覽至 [資料] 索引標籤，然後從左側導覽窗格中選擇 [內送要求]。
4. 找出您要撤銷的訂閱，然後選擇 [檢視訂閱]。

5. (選擇性) 啟用核取方塊，允許訂閱者將資產保留在專案的訂閱目標中。訂閱目標是一組資源的參考，其中訂閱的資料可在環境中使用。

   如果您想要稍後從訂閱目標撤銷對資產的存取權，則必須在中撤銷對資產的存取權 AWS Lake Formation。
6. 選擇 [撤銷訂閱]。

撤銷訂閱後，您無法重新核准訂閱。訂閱者必須再次訂閱資產，您才能核准資產。

取消訂閱請求

Amazon DataZone 允許您查找，訪問和使用 Amazon DataZone 目錄中的資產。當您在目錄中找到想要存取的資產時，您需要訂閱該資產，以建立訂閱請求。然後，核准者可以核准或請求您的請求。您可能需要取消待處理的訂閱請求，可能是因為您錯誤地提交了該資產，或者您不再需要對資產的讀取存取權限。

若要取消訂閱要求，您必須是專案擁有者或參與者。

若要取消訂閱要求

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從上方導覽窗格中選擇 [選取專案]，然後選取包含訂閱要求的專案。
3. 導覽至專案的 [資料] 索引標籤，然後從左側導覽窗格中選擇 [要求的資料]。此頁面會列出專案要求存取的資產。
4. 依「要求」進行篩選，以僅查看仍處於擱置中的要求。找出要求，然後選擇 [檢視請求]。
5. 檢閱訂閱要求，然後選擇 [取消要求]。

如果您要重新訂閱資產 (或訂閱其他資產)，請參閱the section called “要求訂閱資產”。

取消訂閱資產

Amazon DataZone 允許您查找，訪問和使用 Amazon DataZone 目錄中的資產。當您在目錄中找到想要存取的資產時，您需要訂閱該資產，以建立訂閱請求。然後，核准者可以核准或請求您的請求。您可能需要取消訂閱資產，可能是因為您錯誤地訂閱並獲得核准，或是因為您不再需要資產的讀取權限。

您必須是專案的成員，才能取消訂閱其中一個資產。

若要取消訂閱資產

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。
2. 從上方導覽窗格中選擇 [選取專案]，然後選取包含您要取消訂閱之資產的專案。
3. 導覽至專案的 [資料] 索引標籤，然後從左側導覽窗格中選擇 [要求的資料]。此頁面會列出專案要求存取的資產。
4. 依「已核准」進行篩選，以僅查看已核准的請求。找出要求，然後選擇 [檢視訂閱]。
5. 檢閱訂閱並選擇 [取消訂閱]。

如果您要重新訂閱資產 (或訂閱其他資產)，請參閱the section called “要求訂閱資產”。

使用現有的 IAM 角色履行 Amazon DataZone 訂閱

在目前版本中，Amazon DataZone 支援您使用現有的 IAM 角色存取資料。為了實現這一目標，您可以在用於履行訂閱的 Amazon DataZone 環境中創建訂閱目標。若要在其中一個相關聯 AWS 帳戶中建立環境的訂閱目標，您可以使用下列步驟：

步驟 1：確保您的 Amazon DataZone 網域使用的是第 2 版或更高版本的 RAM 政策

1. 瀏覽至 AWS RAM 主控台中的 [由我共用：資源共用] 頁面。
2. 由於 AWS RAM 資源共用存在於特定 AWS 區 AWS 域，因此請從主控台右上角的下拉式清單中選擇適當的「區域」。
3. 選取與 Amazon DataZone 網域對應的資源共用，然後選擇 [修改]。您可以使用 DataZone 網域的名稱或 ID 來識別 Amazon 網域的 RAM 共用，因為 RAM 共用是以下名稱建立的`DataZone-<domain-name>-<domain-id>`。
4. 選擇 [下一步] 繼續進行下一個步驟，您可以在其中檢查 RAM 原則的版本並加以修改。
5. 請確定 RAM 原則的版本為第 2 版或更新版本。如果沒有，請使用下拉菜單選擇版本 2 或更高版本。
6. 選擇「跳至步驟 4：檢閱和更新」。
7. 選擇 [更新資源共用]。

步驟 2：從關聯帳戶建立訂閱目標

- 在目前版本中，Amazon 僅 DataZone 支援使用 API 建立訂閱目標。以下是您可用來建立訂閱目標的一些承載範例，以履行 AWS Glue 資料表和 Amazon Redshift 表格或檢視的訂閱。如需詳細資訊，請參閱CreateSubscriptionTarget。

  AWS Glue 的訂閱目標範例

```
{
        "domainIdentifier": "<DOMAIN_ID>",
        "environmentIdentifier": "<ENVIRONMENT_ID>",
        "name": "<SUBSCRIPTION_TARGET_NAME>",
        "type": "GlueSubscriptionTargetType",
        "authorizedPrincipals" : ["IAM_ROLE_ARN"],
        "subscriptionTargetConfig" : [{"content": "{\"databaseName\":
 \"<DATABASE_NAME>\"}", "formName": "GlueSubscriptionTargetConfigForm"}],
        "manageAccessRole": "<GLUE_DATA_ACCESS_ROLE_IN_ASSOCIATED_ACCOUNT_ARN>",
        "applicableAssetTypes" : ["GlueTableAssetType"],
        "provider": "Amazon DataZone"
}
```

  Amazon Redshift 訂閱目標示例：

```
{
        "domainIdentifier": "<DOMAIN_ID>",
        "environmentIdentifier": "<ENVIRONMENT_ID>",
        "name": "<SUBSCRIPTION_TARGET_NAME>",
        "type": "RedshiftSubscriptionTargetType",
        "authorizedPrincipals" : ["REDSHIFT_DATABASE_ROLE_NAME"],
        "subscriptionTargetConfig" : [{"content": "{\"databaseName\":
 \"<DATABASE_NAME>\", \"secretManagerArn\": \"<SECRET_MANAGER_ARN>
\",\"clusterIdentifier\": \"<CLUSTER_IDENTIFIER>\"}", "formName":
 "RedshiftSubscriptionTargetConfigForm"}],
        "manageAccessRole":
 "<REDSHIFT_DATA_ACCESS_ROLE_IN_ASSOCIATED_ACCOUNT_ARN>",
        "applicableAssetTypes" : ["RedshiftViewAssetType",
 "RedshiftTableAssetType"],
        "provider": "Amazon DataZone"
}
```

> **Important**
>
> - 您在上面的 API 調用中使用的環境標識符應存在於您進行 API 調用的相同關聯帳戶中。否則，API 呼叫將無法成功。
> - 您在「授權主體」中使用的 IAM 角色 ARN 是將訂閱的資產新增到訂閱目標後，Amazon DataZone 將授予存取權的角色。這些授權的主參與者必須屬於與建立訂閱目標所在環境相同的帳戶。
> - 供應商欄位的值必須是「Amazon DataZone」，Amazon DataZone 才能完成訂閱履行。
> - 中提供的資料庫名稱 subscriptionTargetConfig 應該已經存在於建立目標的帳戶中。Amazon 不 DataZone 會創建這個數據庫。同時確定管理存取角色具有此資料庫的 CREATE TABLE 權限。
> - 此外，請確定已提供作為授權主體的角色 (AWS Glue 的 IAM 角色和 Amazon Redshift 的資料庫角色) 已存在於環境帳戶中。對於 Amazon Redshift 訂閱目標，連線到叢集時所假定的角色需要其他更新。此角色必須有附加至角色的 RedshiftDbRoles 標籤。標籤的值可以是逗號分隔的清單。值應該是建立訂閱目標時作為授權主體提供的資料庫角色。

步驟 3：訂閱新表格並履行新目標的訂閱

- 創建訂閱目標後，您可以訂閱一個新表，Amazon DataZone 將履行到上述目標。如需詳細資訊，請參閱 訂閱資料。

授予資料存取權

下列任務提供授與已核准訂閱存取權給 Amazon 中資產的詳細資訊 DataZone。

在 Amazon 中 DataZone，資產讀取存取權的訂閱請求以及已核准或授與的訂閱由訂閱核准人管理。資產的訂閱核准者取決於將此資產發佈到 Amazon DataZone 目錄的發佈協議。

主題

- 授予受管理 AWS Glue Data Catalog 資產的存取權
- 授予對受管 Amazon Redshift 資產的存取權

- 授與未受管理資產的已核准訂閱的存取權

授予受管理 AWS Glue Data Catalog 資產的存取權

> **Note**
>
> 不支援使用 AWS Lake Formation LF-TBAC 方法的 AWS Glue Data Catalog 資產存取管理。不 Support 援中 AWS Glue Data Catalog 跨區域共用資產的支援。

一旦對受管 AWS Glue Data Catalog 資產的訂閱請求獲得核准，Amazon 就 DataZone會自動將這些資產新增到專案中的所有現有資料湖環境。 DataZone 然後，Amazon 會代表您透過授予和管理對已核准 AWS Glue Data Catalog 表格的存取權 AWS Lake Formation。對於訂閱者專案，授與的資產會顯示在您帳戶的 AWS Glue Data Catalog 身分資源中。然後，您可以使用 Amazon Athena 查詢表。

> **Note**
>
> 如果在已訂閱的資產自動新增至現有資料湖環境之後，新增 AWS Glue Data Catalog 資料湖環境至專案，您必須手動將這些已訂閱的 AWS Glue Data Catalog 資產新增至此新的資料湖環境。您可以在 Amazon DataZone 資料入口網站的專案概觀頁面的 [資料] 索引標籤中選擇 [新增授權] 選項來執行此操作。

DataZone 若要讓 Amazon 能夠授與 AWS Glue 資料目錄表格的存取權，必須符合下列條件。

- 由於 Amazon 透過管理 Lake Formation 許可 DataZone授予存取權限，因此 AWS Glue 表必須由湖格式化管理。
- 用於發佈 AWS Glue 資料目錄表格之資料湖環境的「管理」存取角色必須具有下列 Lake Formation 權限：
  - `DESCRIBE`以及包含已發行`DESCRIBE GRANTABLE`資料表之 AWS Glue 資料庫的權限。
  - `DESCRIBE`,, `SELECT``DESCRIBE GRANTABLE`, 在發布的表本身的 Lake Formation 的`SELECT GRANTABLE`權限。

如需詳細資訊，請參閱AWS Lake Formation 開發人員指南中的授與和撤銷目錄資源的權限。

授予對受管 Amazon Redshift 資產的存取權

Amazon Redshift 表格或檢視的訂閱獲得核准後，Amazon DataZone 可以自動將訂閱的資產新增到專案內的所有資料倉儲環境，以便專案成員可以使用環境中的 Amazon Redshift 查詢編輯器連結查詢資料。在引擎蓋下 DataZone，Amazon 在源和訂閱目標之間創建必要的授權和數據庫。

授與存取權的程序視來源資料庫 (發行者) 和目標資料庫 (訂戶) 所在的位置而有所不同。

- 相同的叢集、相同的資料庫-如果資料必須在同一個資料庫中共用，Amazon 會直接在來源資料表上 DataZone 授予許可。
- 相同的叢集、不同的資料庫-如果必須在同一叢集中的兩個資料庫之間共用資料庫，Amazon DataZone 會在目標資料庫中建立檢視，並在建立的檢視上授予許可。
- 相同帳戶不同的叢集-Amazon DataZone 會在來源叢集和目標叢集之間建立資料清單，並在共用資料表頂端建立檢視。權限已授與檢視。
- 跨帳戶-與上述相同，但需要額外的步驟來授權生產者叢集端的跨帳戶資料護理，以及在消費者叢集端建立資料共用關聯的另一個步驟。

> **Note**
>
> 如果訂閱的 Amazon Redshift 資產自動新增至現有資料倉儲環境後，新增資料倉儲環境至專案，您必須手動將這些訂閱的 Amazon Redshift 資產新增到這個新的資料倉儲環境。您可以在 Amazon DataZone 資料入口網站的專案概觀頁面的 [資料] 索引標籤中選擇 [新增授權] 選項來執行此操作。

請確定您的發佈和訂閱 Amazon Redshift 叢集符合 Amazon Redshift 資料存放器的所有要求。如需詳細資訊，請參閱 Amazon Redshift 開發人員指南。

> **Note**
>
> Amazon DataZone 支持自動向亞馬遜紅移集群和亞 Amazon Redshift 無服務器資產授予訂閱。
> 不支援使用 Amazon Redshift 進行跨區域資料共用。

> **Note**
>
> 在目前的版本中，只有當來源和目標 Amazon Redshift 叢集或工作群組位於屬於同一組織的 AWS 帳戶中時，亞馬遜才 DataZone 能管理對 Amazon Redshift 表格和檢視的存取。 AWS

授與未受管理資產的已核准訂閱的存取權

Amazon DataZone 讓使用者能夠在商業資料目錄中發佈任何類型的資產。對於其中一些資產，Amazon DataZone 可以自動管理存取授權。這些資產稱為受管資產，包括湖泊格式化管理的 AWS Glue 資料目錄資料表和 Amazon Redshift 表格和檢視。Amazon 無法自動授予訂閱 DataZone 的所有其他資產稱為非託管。

Amazon 為您 DataZone 提供管理非受管資產存取授權的途徑。資料擁有者核准商業資料目錄中資產的訂閱後，Amazon 會在您的帳戶中 DataZone 發佈事件，以及承載中的所有必要資訊，讓您能夠在來源和目標之間建立存取授權。 EventBridge 當您收到此事件時，您可以觸發自訂處理常式，該處理常式可以使用事件中的資訊來建立必要的授權或權限。授予存取權後，您可以在 Amazon 中報告並更新訂閱的狀態，以 DataZone 便它可以通知訂閱資產的使用者他們可以開始使用資產。如需詳細資訊，請參閱使用 Amazon DataZone 事件和通知。

消費數據

下列任務提供您在 Amazon 中訂閱的使用資料的詳細資訊 DataZone。

主題

- 查詢 Amazon Athena 或亞馬 Amazon Redshift 中的數據

查詢 Amazon Athena 或亞馬 Amazon Redshift 中的數據

在 Amazon DataZone，一旦訂閱者可以存取目錄中的資產，就可以使用亞馬遜 Athena 或亞馬 Amazon Redshift 查詢編輯器 v2 使用該資產 (查詢和分析)。您必須是專案擁有者或參與者才能完成此任務。視專案中啟用的藍圖而定，Amazon 會在資料入口網站的專案頁面右側窗格中 DataZone 提供 Amazon Athena 和/或 Amazon Redshift 查詢編輯器 v2 的連結。

1. 導覽至 Amazon 資 DataZone 料入口網站 URL，然後使用單一登入 (SSO) 或您的登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以瀏覽至 https://console.aws.amazon.com/datazone 的 Amazon DataZone 主控台，並使用建立網域的位 AWS 帳戶 置登入，然後選擇開啟資料入口網站。

2. 在 Amazon DataZone 資料入口網站中，選擇瀏覽專案清單，然後尋找並選擇您要分析資料的專案。
3. 如果此專案已啟用資料湖藍圖，則專案首頁右側面板中會顯示 Amazon Athena 的連結。

   如果此專案已啟用資料倉儲藍圖，則專案首頁右側面板中會顯示查詢編輯器的連結。

   > **Note**
   >
   > 藍圖是在用來建立專案的環境設定檔中定義的。

主題

- 使用 Amazon Athena 查詢資
- 使用 Amazon Redshift 查詢數據

使用 Amazon Athena 查詢資

選擇 Amazon Athena 連結，使用專案的登入資料進行身份驗證，在瀏覽器的新索引標籤中開啟 Amazon Athena 查詢編輯器。您正在使用的 Amazon DataZone 專案會在查詢編輯器中自動選取為目前的工作群組。

在 Amazon Athena 查詢編輯器中，撰寫並執行查詢。一些常見工作包括：

- 查詢和分析您訂閱的資產
- 建立新表格
- 從外部 S3 儲存貯體的查詢結果 (CTAS) 建立資料表

查詢和分析您訂閱的資產

如果 Amazon 未自動授予專案訂閱資產的存取權 DataZone，您必須獲得存取基礎資料的授權。如需如何授與這些資產存取權的詳細資訊，請參閱授與未受管理資產的已核准訂閱的存取權。

如果 Amazon 自動授予專案訂閱資產的存取權 DataZone，您可以在資料表上執行 SQL 查詢，並在 Amazon Athena 中查看結果。如需在 Amazon Athena 使用 SQL 的詳細資訊，請參閱 Ath ena 的 SQL 參考資料。

選擇專案首頁右側面板中的 Amazon Athena 連結後，導覽至 Amazon Athena 查詢編輯器時，Amazon Athena 查詢編輯器右上角會顯示專案下拉式清單，而且會自動選取您的專案內容。

您可以在數據庫下拉列表中看到以下數據庫：

- 發行資料庫 (*{environmentname}*_pub_db)。此資料庫的目的是為您提供一個環境，讓您可以在專案環境中產生新資料，然後將此資料發佈到 Amazon 目 DataZone 錄中。專案擁有者和貢獻者具有此資料庫的讀取和寫入權限。專案檢視者只有此資料庫的讀取權限。
- 訂閱資料庫 (*{environmentname}*_sub_db)。此資料庫的目的是與您共用您在 Amazon 目 DataZone 錄中以專案成員身分訂閱的資料，並讓您能夠查詢該資料。

建立新表格

如果您已連線到外部 S3 儲存貯體，則可以使用 Amazon Athena 從外部 Amazon S3 儲存貯體查詢和分析資產。在這種情況下，Amazon DataZone 沒有權限直接授予對外部 Amazon S3 儲存貯體中基礎資料的存取權，而且在專案外部建立的外部 Amazon S3 資料不會在 Lake Formation 中自動管理，也無法由 Amazon 管理 DataZone。另一種方法是使用 Amazon Athena 中的CREATE TABLE聲明，將資料從外部 Amazon S3 儲存貯體複製到專案 Amazon S3 儲存貯體內的新表格。當您在 Amazon Athena 執行CREATE TABLE查詢時，請在 AWS Glue Data Catalog.

若要在 Amazon S3 中指定資料的路徑，請使用 LOCATION 屬性，如下列範例所示：

```
CREATE EXTERNAL TABLE 'test_table'(
...
)
ROW FORMAT ...
STORED AS INPUTFORMAT ...
OUTPUTFORMAT ...
LOCATION 's3://bucketname/folder/'
```

如需詳細資訊，請參閱 Amazon S3 中的表格位置。

從外部 S3 儲存貯體的查詢結果 (CTAS) 建立資料表

當您訂閱資產時，對基礎資料的存取是唯讀的。您可以使用 Amazon Athena 創建表的副本。在 Amazon Athena 中，A CREATE TABLE AS SELECT (CTAS)查詢會根據另一個查詢的SELECT陳述式結果，在 Amazon Athena 中建立新資料表。如需有關 CTA 語法的資訊，請參閱建立資料表 AS。

以下範例會透過複製資料表的所有資料欄來建立資料表：

```
CREATE TABLE new_table AS
SELECT *
FROM old_table;
```

在相同範例的以下變化中，您的 SELECT 陳述式也包含 WHERE 子句。在這種情況下，查詢只會從資料表中選取滿足 WHERE 子句的那些資料列：

```
CREATE TABLE new_table AS
SELECT *
FROM old_table WHERE condition;
```

以下範例會建立對來自另一個資料表的一組資料欄執行的新查詢：

```
CREATE TABLE new_table AS
SELECT column_1, column_2, ... column_n
FROM old_table;
```

相同範例的這個變化會來自多個資料表的特定資料欄建立新的資料表：

```
CREATE TABLE new_table AS
SELECT column_1, column_2, ... column_n
FROM old_table_1, old_table_2, ... old_table_n;
```

這些新建立的表格現在已成為專案資料 AWS Glue 庫的一部分，其他人可以將資料作為資產發佈到 Amazon DataZone 目錄，讓其他人可以探索並與其他 Amazon DataZone 專案共用。

使用 Amazon Redshift 查詢數據

在 Amazon 資 DataZone 料入口網站中，開啟使用資料倉儲藍圖的環境。在環境頁面的右側面板中選擇 Amazon Redshift 連結。這會開啟包含必要詳細資訊的確認對話方塊，協助您在 Amazon Redshift 查詢編輯器 2.0 中建立與環境的 Amazon Redshift 叢集或 Amazon Redshift 無伺服器工作群組的連線。找出建立連線的必要詳細資料後，請選擇「開啟 Amazon Redshift」按鈕。這會使用 Amazon 環境的臨時登入資料，在瀏覽器的新索引標籤中開啟 Amazon DataZone Redshift 查詢編輯器 v2.0。

在查詢編輯器中，根據您的環境是使用 Amazon Redshift 無伺服器工作群組還是 Amazon Redshift 叢集，請依照下列步驟執行。

適用於亞 Amazon Redshift 無伺服器工作群組

1. 在查詢編輯器中，識別您的 Amazon DataZone 環境的 Amazon Redshift 無伺服器工作群組，在其上按一下滑鼠右鍵，然後選擇「建立連線」。
2. 選擇 [同盟使用者] 進行驗證。
3. 提供 Amazon DataZone 環境的數據庫的名稱。
4. 選擇建立連線。

對於亞 Amazon Redshift 集群：

1. 在查詢編輯器中，識別您的 Amazon DataZone 環境的 Amazon Redshift 叢集，在其上按一下滑鼠右鍵，然後選擇 [建立連線]。
2. 選取使用 IAM 身分進行身份驗證的臨時登入資料。
3. 如果上述身份驗證方法不可用，請通過選擇左下角的齒輪按鈕打開帳戶設置，然後選擇使用 IAM 憑據進行身份驗證並保存。這是一個 one-time-only設置。
4. 提供 Amazon DataZone 環境資料庫的名稱以建立連線。
5. 選擇建立連線。

現在，您可以開始查詢針對 Amazon 環境設定的 Amazon Redshift 叢集或 Amazon Redshift 無伺服器工作群組內的資料表和檢視。 DataZone

您訂閱的任何 Amazon Redshift 表格或檢視都會連結至針對該環境設定的亞馬 Amazon Redshift 叢集或亞馬遜 Redshift 無伺服器工作群組。您可以訂閱表格和檢視，也可以發行在環境叢集或資料庫中建立的任何新表格和檢視表。

例如，讓我們以環境連結到名為的 Amazon Redshift 叢集`redshift-cluster-1`和該叢集`dev`中呼叫的資料庫的案例。使用 Amazon DataZone 資料入口網站，您可以查詢新增至環境的資料表和檢視。在資料入口網站右側窗格的`Analytics tools`區段下，您可以選擇此環境的 Amazon Redshift 連結，這會開啟查詢編輯器。然後，您可以在`redshift-cluster-1`叢集上按一下滑鼠右鍵，並使用 IAM 身分使用臨時登入資料建立連線。建立連接後，您可以在 dev 數據庫下看到您的環境可以訪問的所有表和視圖。

使用 Amazon DataZone 事件和通知

Amazon 會 DataZone 隨時通知您資料入口網站中的重要活動，例如訂閱請求、更新、註解和系統事件。 DataZone Amazon 會在資料入口網站的專用收件匣中或透過 Amazon EventBridge 預設匯流排傳送訊息，為您提供此資訊。

主題

透過 Amazon DataZone 資料入口網站中的專用收件匣處理事件

Amazon 在資料入口網站中 DataZone 提供專用的收件匣，您可以在其中查看訊息並對其採取行動。最近的訊息也會顯示在首頁、專案頁面和目錄頁面上。例如，如果使用者要求存取資料資產，則發佈專案的擁有者和該資產的參與者會在資料入口網站中看到要求，而且一旦採取動作，與此請求相關的訂閱專案的專案成員會在資料入口網站中看到通知。有兩種類型的消息：

- 任務-這些消息通知收件人某處需要採取行動。他們有一個可選的狀態字段，您可以使用它來跟踪。
- 事件-這些訊息僅供參考，且沒有指派狀態。事件提供最近更新的稽核追蹤。

在 Amazon 中 DataZone，會針對下列事件類型產生訊息：

事件類別	事件名稱	事件描述	事件類型
訂閱	訂閱請求已建立	建立訂閱要求時會產生事件	任務
訂閱	訂閱請求已接受	接受訂閱要求時會產生事件	事件
訂閱	訂閱請求被拒絕	拒絕訂閱要求時會產生事件	事件
訂閱	訂閱請求已刪除	刪除訂閱要求時會產生事件	事件

事件類別	事件名稱	事件描述	事件類型
專案	專案建立成功	項目創建成功時生成事件	事件
專案成員	專案成員新增成功	當一個新成員被添加到項目中生成事件	事件
專案成員	專案成員移除成功	將成員移除至專案時會產生事件	事件
專案成員	專案成員角色變更成功	事件生成一個成員在項目中的角色被改變	事件
環境	環境部署已開始	啟動環境部署時會產生事件	事件
環境	環境部署完成	環境部署成功完成時會產生事件	事件
環境	環境部署失敗	環境部署失敗時會產生事件	事件
環境	啟動環境部署自訂工作流	啟動具有自訂工作流程的環境時會產生事件	事件
資料資產	已新增至庫存的資產	當新的資料資產新增至庫存 (即以草稿狀態新增至目錄) 時，會產生事件	事件
資料資產	已發佈資產	發佈新資料資產 (即可供訂閱) 時產生事件	事件
資料資產	資產架構已變更	自上次擷取工作以來，資產結構描述已變更時，會產生事件	事件

事件類別	事件名稱	事件描述	事件類型
訂閱	已建立訂閱	當有人請求訂閱資料資產時會產生事件	任務
訂閱	已核准訂閱	當公開專案擁有者或貢獻者核准訂閱時，就會產生事件	事件
訂閱	訂閱被拒絕	當公開專案擁有者或貢獻者拒絕訂閱時，就會產生事件	事件
訂閱	訂閱已刪除	訂閱者取消訂閱時會產生事件	事件
訂閱	要求訂閱授予	有人要求存取資產時會產生事件	事件
訂閱	訂閱授權已完成	公開專案擁有者或貢獻者授予訂閱資產存取權時，就會產生事件	事件
訂閱	訂閱授權失敗	訂閱授與失敗時會產生事件	事件
訂閱	要求撤銷訂閱授權	由公開專案擁有者或貢獻者啟動撤銷的訂閱授權時，會產生事件	事件
訂閱	訂閱授權撤銷完成	完成訂閱授權撤銷時會產生事件	事件
訂閱	訂閱授權撤銷失敗	訂閱授與撤銷失敗時會產生事件	事件

事件類別	事件名稱	事件描述	事件類型
自動產生企業名稱	企業名稱產生成功	當自動化企業名稱產生的作業成功完成時產生的 Eventis	事件
自動產生企業名稱	商業名稱產生失敗	當自動化企業名稱產生的工作失敗時，會產生事件	事件
資料來源執行	資料來源已建立	建立新資料來源時會產生事件	事件
資料來源執行	資料來源已更新	更新現有資料來源時會產生事件	事件
資料來源執行	觸發資料來源執行	啟動資料來源執行時會產生事件	事件
資料來源執行	資料來源執行成功	資料來源執行成功時會產生事件	事件
資料來源執行	資料來源執行失敗	資料來源執行失敗時會產生事件	事件

若要檢視資料入口網站收件匣中的工作，請完成以下步驟：

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon 網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口 DataZone 網站 URL。
2. 在資料入口網站中，若要檢視包含最近一組工作的快顯視窗，請選取搜尋列旁邊的鈴鐺圖示。
3. 選取檢視全部以檢視所有工作。您可以選取「事件」(Events) 標籤來變更檢視和查看所有事件。
4. 您可以依事件主旨、使用中或非使用中狀態或日期範圍來篩選搜尋。
5. 選擇任何個別工作，以導覽至您可以回應工作的位置。

若要檢視資料入口網站收件匣中的事件，請完成以下步驟：

1. 使用 DataZone 資料入口網站 URL 導覽至 Amazon 資料入口網站，然後使用 SSO 或登入資料 AWS 登入。如果您是 Amazon DataZone 管理員，則可以在建立 Amazon DataZone 根網域的 AWS 帳戶中存取 Amazon DataZone 主控台 https://console.aws.amazon.com/datazone，以取得資料入口網站 URL。
2. 在資料入口網站中，若要檢視最近一組事件的快顯視窗，請選取搜尋列旁邊的鈴鐺圖示。
3. 選取檢視全部以檢視所有事件。您可以選取 [工作] 索引標籤來變更檢視和查看所有工作。
4. 依事件主旨或日期範圍篩選搜尋。
5. 選擇任何個別事件以瀏覽至您可以檢視該事件詳細資訊的位置。

通過 Amazon EventBridge 默認總線與事件工作

除了將訊息傳送到資料入口網站中的專用收件匣外， DataZone 還會將這些訊息傳送到託管 Amazon DataZone 根網域的同一 AWS 帳戶中的 Amazon EventBridge 預設事件匯流排。這可啟用事件驅動的自動化功能，例如訂閱履行或與其他工具的自訂整合。您可以建立符合傳入 Amazon EventBridge 事件的規則，並將其傳送到 Amazon EventBridge 目標進行處理。單一規則可將事件傳送至多個目標，然後再 parallel 執行。

以下是一個示例事件：


```
{
  "version": "0",
  "id": "bd3d6239-2877-f464-0572-b1d76760e085",
  "detail-type": "Subscription Request Created",
  "source": "aws.datazone",
  "account": "111111111111",
  "time": "2023-11-13T17:57:00Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "version": "655",
    "metadata": {
      "domain": "dzd_bc8e1ez8r2a6xz",
      "user": "44f864b8-50a1-70cc-736f-c1f763934ab7",
      "id": "5jbc0lie0sr99j",
      "version": "1",
      "typeName": "SubscriptionRequestEntityType",
      "owningProjectId": "6oy92hwk937pgn",
      "awsAccountId": "111111111111",
```

```
      "clientToken": "e781b7b5-78c5-4608-961e-3792a6c3ff0d"
    },
    "data": {
      "autoApproved": true,
      "requesterId": "44f864b8-50a1-70cc-736f-c1f763934ab7",
      "status": "PENDING",
      "subscribedListings": [
        {
          "id": "ayzstznnx4dxyf",
          "ownerProjectId": "5a3se66qm88947",
          "version": "12"
        }
      ],
      "subscribedPrincipals": [
        {
          "id": "6oy92hwk937pgn",
          "type": "PROJECT"
        }
      ]
    }
  }
}
```

Amazon DataZone 支援的詳細資料類型完整清單包括：

- 訂閱請求已建立
- 訂閱請求已接受
- 訂閱請求被拒絕
- 訂閱請求已刪除
- 要求訂閱授予
- 訂閱授權已完成
- 訂閱授權失敗
- 已要求撤銷訂閱授權
- 訂閱授權撤銷完成
- 訂閱授權撤銷失敗
- 已新增至存貨的資產
- 資產已新增至目錄

- 已變更資產架構
- 資料來源狀態變更
- 資料來源已建立
- 資料來源已更新
- 已觸發資料來源執行
- 資料來源執行成功
- 資料來源執行失敗
- 網域建立成功
- 網域建立失敗
- 網域刪除成功
- 網域刪除失敗
- 環境部署已開始
- 環境部署完成
- 環境部署失敗
- 已開始刪除環境
- 環境刪除已完成
- 環境刪除失敗
- 專案建立成功
- 專案成員新增成功
- 專案成員移除成功
- 專案成員角色變更成功
- 啟動環境部署客戶工作流
- 商業名稱產生成功
- 商業名稱產生失敗

有關更多信息，請參閱 Amazon EventBridge。

Amazon 的安全 DataZone

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同承擔的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。若要了解適用於 Amazon 的合規計劃 DataZone，請參閱AWS 合規計劃的合規計劃 AWS 服務範的服務。
- 雲端安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 Amazon 時應用共同的責任模型 DataZone。下列主題說明如何設定 Amazon DataZone 以符合安全和合規目標。您也會學到如何使用其他可 AWS 協助您監控和保護 Amazon DataZone 資源的服務。

主題

Amazon 的數據保護 DataZone

AWS 共同責任模型適用於 Amazon 中的資料保護 DataZone。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用控制台，API DataZone 或 AWS SDK 與 Amazon 或其他 AWS 服務 AWS CLI人合作時。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。

資料加密

授予許可時，您可以決定誰取得哪些 Amazon DataZone 資源的許可。您還需針對這些資源啟用允許執行的動作，因此，您只應授予執行任務所需的許可。對降低錯誤或惡意意圖所引起的安全風險和影響而言，實作最低權限存取是相當重要的一環。

靜態加密

Amazon 預設 DataZone 會使用為您擁有和管理的金AWS 鑰管理服務 (AWS KMS) 金鑰來加密您的所 AWS 有資料。您也可以使用透過 AWS KMS 管理的金鑰來加密儲存在 Amazon DataZone 目錄中的資料。

在 Amazon 中建立網域時 DataZone，您可以選取資料加密下自訂加密設定 (進階) 旁邊的核取方塊，並提供 KMS 金鑰，以提供加密設定。

傳輸中加密

Amazon DataZone 使用傳輸層安全性 (TLS) 和用戶端加密來進行傳輸中的加密。與 Amazon 的通訊 DataZone 一律透過 HTTPS 完成，因此您的資料在傳輸過程中始終會加密。

網際網路流量隱私權

為了保護帳戶之間的連接，Amazon DataZone 使用服務角色和 IAM 角色安全地連接到客戶帳戶並代表客戶執行操作。

主題

- 適用於 Amazon 的靜態資料加密 DataZone
- 使用 Amazon 的接口 VPC 端點 DataZone

適用於 Amazon 的靜態資料加密 DataZone

依預設加密靜態資料，有助於降低保護敏感資料所涉及的營運開銷和複雜性。同時，其可讓您建置符合嚴格加密合規性和法規要求的安全應用程式。

Amazon DataZone 使用預設 AWS擁有的金鑰自動加密靜態資料。您無法檢視、管理或稽核 AWS 擁有金鑰的使用。如需詳細資訊，請參閱AWS 擁有的金鑰。

雖然您無法停用此層加密或選取替代加密類型，但您可以在建立 Amazon DataZone 網域時選擇客戶管理的金鑰，在現有 AWS 擁有的加密金鑰上新增第二層加密。Amazon DataZone 支援使用對稱的客戶受管金鑰，您可以建立、擁有和管理這些金鑰，透過現有 AWS 擁有的加密新增第二層加密。由於您可以完全控制此加密層，因此您可以在其中執行以下任務：

- 建立和維護關鍵政策
- 建立和維護 IAM 政策和撥款
- 啟用和停用金鑰原則
- 旋轉密鑰加密材料
- 新增標籤
- 建立金鑰別名
- 要刪除的排程關鍵字

如需詳細資訊，請參閱客戶管理的金鑰。

> **Note**
>
> Amazon 使用 DataZone 自有的金鑰 AWS 自動啟用靜態加密，以免費保護客戶資料。

AWS 使用客戶受管金鑰需支付 KMS 費用。如需有關定價的詳細資訊，請參閱AWS 金鑰管理服務定價。

Amazon 如何在 AWS KMS 中 DataZone 使用贈款

Amazon DataZone 需要三次授權才能使用您的客戶受管金鑰。當您建立使用客戶受管金鑰加密的 Amazon DataZone 網域時，Amazon DataZone 會將CreateGrant請求傳送到 AWS KMS 代表您建立授權和子授權。 AWS KMS 中的贈款用於授予 Amazon DataZone 存取您帳戶中的 KMS 金鑰。Amazon DataZone 建立下列授權，將客戶受管金鑰用於下列內部作業：

一次授權用於加密靜態數據，以進行以下操作：

- 傳送DescribeKey請求至 AWS KMS，以確認在建立 Amazon DataZone 網域集合時輸入的對稱客戶受管 KMS 金鑰識別碼是否有效。
- 傳送GenerateDataKeyrequests至 AWS KMS 以產生由客戶管理金鑰加密的資料金鑰。
- 傳送解密請求至 AWS KMS 以解密加密的資料金鑰，以便使用這些要求來加密您的資料。
- RetireGrant以在刪除網域時淘汰授權。

搜尋和探索資料的兩項補助金：

- 授予 2:
  - DescribeKey
  - GenerateDataKey
  - 加密, 解密, ReEncrypt
  - CreateGrant為內部使用的 AWS 服務建立子授權 DataZone。
  - RetireGrant
- 授予 3:
  - GenerateDataKey
  - 解密
  - RetireGrant

您可以隨時撤銷授予的存取權，或移除服務對客戶受管金鑰的存取權。如果這樣做，Amazon 將 DataZone 無法存取客戶受管金鑰加密的任何資料，這會影響依賴該資料的操作。例

如，如果您嘗試獲取 Amazon DataZone 無法訪問的數據資產詳細信息，則操作將返回錯`AccessDeniedException`誤。

建立客戶受管金鑰

您可以使用管 AWS 理主控台或 AWS KMS API 建立對稱的客戶受管金鑰。

若要建立對稱的客戶管理金鑰，請遵循金鑰管理服務開發人員指南中關於建立對稱客戶管理 AWS 金鑰的步驟。

金鑰原則-關鍵原則可控制對客戶管理金鑰的存取。每個客戶受管金鑰都必須只有一個金鑰政策，其中包含決定誰可以使用金鑰及其使用方式的陳述式。在建立客戶受管金鑰時，可以指定金鑰政策。如需詳細資訊，請參閱金鑰管理服務開發人員指南中的 AWS 管理客戶受管理金鑰的存取權限。

若要將客戶受管金鑰與 Amazon 資 DataZone 源搭配使用，必須在金鑰政策中允許下列 API 操作：

- kms：CreateGrant— 將授權新增至客戶管理的金鑰。授予對指定 KMS 金鑰的控制存取權，以便授予 Amazon 所 DataZone 需操作的存取權。如需有關使用授權的詳細資訊，請參閱 AWS 金鑰管理服務開發人員指南。
- kms：DescribeKey— 提供客戶託管的密鑰詳細信息，以允許 Amazon DataZone 驗證密鑰。
- kms: GenerateDataKey — 傳回在 KMS 外部使用的唯一對稱資料 AWS 金鑰。
- KMS：解密 — 解密由 KMS 金鑰加密的加密文字。

以下是您可以為 Amazon 新增的政策聲明範例 DataZone：

```
"Statement" : [
    {
      "Sid" : "Allow access to principals authorized to manage Amazon DataZone",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::<account_id>:root"
      },
      "Action" : [
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource" : "arn:aws:kms:region:<account_id>:key/key_ID",
    }
```

```
  ]
```

> **Note**
>
> KMS 上的拒絕政策不適用於透過 Amazon 資 DataZone 料入口網站存取的資源。

如需有關在原則中指定權限的詳細資訊，請參閱 AWS 金鑰管理服務開發人員指南。

如需疑難排解金鑰存取的詳細資訊，請參閱 AWS 金鑰管理服務開發人員指南。

為 Amazon 指定客戶受管金鑰 DataZone

Amazon DataZone 加密環境

加密內容是一組選用的金鑰值對，包含資料的其他相關內容資訊。

AWS KMS 會使用加密內容做為其他驗證資料，以支援驗證的加密。當您在加密資料的要求中包含加密內容時， AWS KMS 會將加密內容繫結至加密的資料。若要解密資料，您必須在請求中包含相同的加密內容。

Amazon DataZone 使用以下加密上下文：

```
"encryptionContextSubset": {
    "aws:datazone:domainId": "{root-domain-uuid}"
}
```

使用加密內容進行監控-當您使用對稱的客戶受管金鑰來加密 Amazon 時 DataZone，您也可以在稽核記錄和日誌中使用加密內容來識別客戶受管金鑰的使用方式。加密內容也會出現在 AWS CloudTrail 或 Amazon 日誌產生的 CloudWatch 日誌中。

使用加密內容來控制對客戶管理金鑰的存取-您可以使用金鑰政策和 IAM 政策中的加密內容作為條件，以控制對對稱客戶受管金鑰的存取。您也可以在授予中使用加密內容條件。

Amazon 在授權中 DataZone 使用加密內容約束來控制對您帳戶或區域中客戶受管金鑰的存取。授予條件會要求授予允許的操作使用指定的加密內容。

以下是授予特定加密內容之客戶受管金鑰存取權的金鑰政策陳述式範例。此政策陳述式中的條件會要求具有指定加密內容的加密內容條件。

```
{
    "Sid": "Enable DescribeKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": "kms:DescribeKey",
     "Resource": "*"
},{
    "Sid": "Enable Decrypt, GenerateDataKey",
     "Effect": "Allow",
     "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
     ],
     "Resource": "*",
     "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:datazone:domainId": "{root-domain-uuid}"
        }
    }
}
```

監控 Amazon 的加密金鑰 DataZone

當您將 AWS KMS 客戶受管金鑰與 Amazon DataZone 資源搭配使用時，您可以用AWS CloudTrail來追蹤 Amazon DataZone 傳送至 AWS KMS 的請求。下列範例是針對`CreateGrant`、`GenerateDataKey`、`Decrypt`和監控 Amazon DataZone 呼叫`DescribeKey`的 KMS 操作以存取由客戶受管金鑰加密的資料的 AWS CloudTrail 事件。當您使用 AWS KMS 客戶受管金鑰加密 Amazon DataZone 網域時，Amazon DataZone 會代表您傳送存取 AWS 帳戶中的 KMS 金鑰的`CreateGrant`請求。Amazon DataZone 建立的授權僅限於與 AWS KMS 客戶受管金鑰相關聯的資源。此外，Amazon DataZone 會在您刪除網域時使用該`RetireGrant`操作移除授權。下面的範例事件會記錄 `CreateGrant` 操作：

```
{
```

```
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-04-22T17:02:00Z"
            }
        },
        "invokedBy": "datazone.amazonaws.com"
    },
    "eventTime": "2021-04-22T17:07:02Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "172.12.34.56",
    "userAgent": "ExampleDesktop/1.0 (V1; OS)",
    "requestParameters": {
        "constraints": {
            "encryptionContextSubset": {
                "aws:datazone:domainId": "SAMPLE-root-domain-uuid"
            }
        },
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "operations": [
            "Decrypt",
            "GenerateDataKey",
            "RetireGrant",
            "DescribeKey"
        ],
        "granteePrincipal": "datazone.us-west-2.amazonaws.com"
```

```
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

建立涉及加密 AWS Glue 目錄的資料湖環境

在進階使用案例中，當您使用已加密的 AWS Glue 目錄時，必須授與 Amazon DataZone 服務的存取權，才能使用客戶管理的 KMS 金鑰。您可以透過更新自訂 KMS 政策並在金鑰中新增標籤來執行此操作。若要授與 Amazon DataZone 服務的存取權以處理加密 AWS Glue 目錄中的資料，請完成以下操作：

- 將下列原則新增至您的自訂 KMS 金鑰。如需詳細資訊，請參閱變更金鑰政策。

```
{
  "Sid": "Allow datazone environment roles to use the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "*"
  },
  "Action": [
    "kms:Decrypt",
```

```
      "kms:Describe*",
      "kms:Get*"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "aws:PrincipalArn": "arn:aws:iam::*:role/*datazone_usr*"
      }
    }
}
```

- 將下列標記新增至您的自訂 KMS 金鑰。如需詳細資訊，請參閱使用標記控制 KMS 金鑰的存取權。

```
key: AmazonDataZoneEnvironment
value: all
```

使用 Amazon 的接口 VPC 端點 DataZone

如果您使用 Amazon Virtual Private Cloud（Amazon VPC）託管資 AWS 源，則可以在 Amazon VPC 和 Amazon 之間建立連接。 DataZone您可以在 Amazon 上使用此連接， DataZone 而無需跨越公共互聯網。

Amazon VPC 可讓您在自訂虛擬網路中啟動 AWS 資源。您可利用 VPC 來控制您的網路設定，例如 IP 地址範圍、子網路、路由表和網路閘道。如需有關 Amazon VPC 的詳細資訊，請參閱《Amazon VPC 使用者指南》。

若要將 Amazon VPC 連接到 Amazon DataZone，您必須先定義一個接口 VPC 端點，以便將 VPC 連接到其他服務。 AWS 端點可提供可靠、可擴展的連線能力，且不需要網際網路閘道、網路地址轉譯 (NAT) 執行個體或 VPN 連接。有關如何建立 VPC 端點的詳細資訊和詳細步驟，請參閱 Amazon VPC 使用者指南中的介面 VPC 端點 (AWS PrivateLink)。

> **Important**
>
> 在 VPC 中，端點策略是以資源為基礎的策略，您可以將其連接到 VPC 端點，以控制哪些 AWS 主體可以使用該端點存取服務。 AWS

在目前版本的 Amazon 中 DataZone，不支援使用端點政策來建立和使用 Amazon VPC 和 Amazon DataZone 之間的連線。Amazon DataZone 存取管理依賴於服務層級定義的 RAM 組態和 IAM 主體政策。

Amazon 授權 DataZone

Amazon DataZone 的界面由內部的管理主控台 AWS 和離開主控台的 Web 應用程式 (資料入口網站) 組成。

DataZone 管理 AWS 員可以將 Amazon 管理主控台用於 top-level-resource API，包括建立和管理網域、這些網域的 AWS 帳戶關聯，以及要將存取管理委派給 Amazon 的資料來源 DataZone。您可以使用 Amazon DataZone 管理主控台管理所需的所有 IAM 角色和組態，以將存取管理控制委派給 Amazon DataZone 服務為其明確設定的 AWS 帳戶。Amazon 資 DataZone 料入口網站是適用於 SSO 使用者的第一方 AWS 身分識別中心應用程式。如果啟用，則獲授權的 IAM 主體也可以使用主控台聯合到資料入口網站，而不是使用 SSO 身分。

Amazon DataZone 的資料入口網站主要由經過 AWS IAM 身分識別中心驗證的使用者使用，用於管理資料存取，以及執行資料發佈、探索、訂閱和分析任務。

Amazon DataZone 控制台中的授權

Amazon 主 DataZone 控台授權模型使用 IAM 授權。主控台主要由系統管理員用於安裝。Amazon DataZone 使用網域管理員帳戶和成員 AWS AWS 帳戶的概念，並使用所有這些帳戶中的主控台來建立信任關係，同時遵守 AWS 組織界限。

在 Amazon DataZone 門戶網站授權

Amazon 資 DataZone 料入口網站授權模型是具有靜態角色原型 (設定檔) 的階層 ACL，其中包括管理員和檢視者。例如，使用者可以擁有管理員或使用者的設定檔。在域級別，他們可能會指定數據所有者的域用戶。在專案層級，使用者可以是擁有者或參與者。這些設定檔可以設定為兩種類型之一：使用者和群組。然後，這些設定檔會與網域和專案相關聯，而這些權限的狀態會儲存在關聯表格中。

在此授權模式中，Amazon DataZone 允許使用者管理使用者和群組許可。使用者可管理專案成員資格、要求專案成員資格，以及核准成員資格。使用者發佈資料、定義資料訂閱核准人、訂閱資料，以及核准訂閱。

當使用者的資料入口網站用戶端要求 Amazon 根據使用者在特定專案環境中的有效設定檔 DataZone 產生的 IAM 工作階段登入資料時，會在特定專案中執行資料分析。此工作階段的範圍包括使用者的權

限，也是特定專案的資源。使用者接著進入 Athena 或 Redshift 來查詢相關資料，所有基礎 IAM 工作都會完全抽取出去。

Amazon DataZone 設定檔和角色

驗證使用者之後，已驗證的內容會對應至使用者設定檔 ID。此使用者設定檔可以有多個不同的關聯 (專案擁有者、網域管理員等)，用來授權使用者。每個關聯 (例如，專案擁有者、網域管理員等) 都具有以前後關聯為基礎之特定活動的權限。例如，具有網域管理員關聯的使用者可以建立其他網域、可以將其他網域管理員指派給網域，以及在其網域內建立專案範本。專案擁有者可以為其專案新增或移除專案成員、建立具有網域的發佈合約，以及將資產發佈至網域。

使用 IAM 控制對 Amazon DataZone 資源的存取

您需要 AWS Identity and Access Management (IAM) 完成下列安全性相關工作：

- 在您的 AWS 帳戶.
- 為您下的每個使用者指派唯一的安全認證 AWS 帳戶。
- 控制每個使用者使用 AWS 資源執行工作的權限。
- 允許其他使用者共 AWS 帳戶 用您的 AWS 資源。
- 為您的角色建立角色， AWS 帳戶 並定義可以擔任他們的使用者或服務。
- 使用企業的現有身分識別授與使用 AWS 資源執行工作的權限

如需 IAM 的詳細資訊，請參閱下列各項：

- AWS Identity and Access Management (IAM)
- 入門
- IAM 使用者指南

以下各節說明設定 Amazon 及其元件所需的政策 DataZone 和許可，例如網域 (包括網域)、關聯帳戶、專案和資料來源。如需詳細資訊，請參閱 Amazon DataZone 術語和概念。

目錄

- 暫時登入資料
- 主體許可

AWS Amazon 的受管政策 DataZone

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

目錄

AWS 受管理的策略：AmazonDataZoneFullAccess

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

此政策提供 DataZone 透過 Amazon 的完整存取權 AWS Management Console。

許可詳細資訊

此政策包含以下許可：

- datazone— 授予校長完全訪問 Amazon DataZone 通過 AWS Management Console.
- kms— 允許主參與者列出別名並描述金鑰。
- s3— 允許主體選擇現有的或建立新的 S3 儲存貯體來存放 Amazon DataZone 資料。
- ram— 允許校長跨 AWS 帳戶共享 Amazon DataZone 域。
- iam— 可讓主參與者列出並傳遞角色，以及取得原則。
- sso— 允許主參與者取得已啟用 AWS IAM Identity Center 的區域。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonDataZoneStatement",
      "Effect": "Allow",
      "Action": [
        "datazone:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "ReadOnlyStatement",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:ListAliases",
        "iam:ListRoles",
        "sso:DescribeRegisteredRegions",
        "s3:ListAllMyBuckets",
        "redshift:DescribeClusters",
        "redshift-serverless:ListWorkgroups",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
```

```
        "secretsmanager:ListSecrets"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "BucketReadOnlyStatement",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Sid": "CreateBucketStatement",
      "Effect": "Allow",
      "Action": "s3:CreateBucket",
      "Resource": "arn:aws:s3:::amazon-datazone*"
    },
    {
      "Sid": "RamCreateResourceStatement",
      "Effect": "Allow",
      "Action": [
        "ram:CreateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "StringEqualsIfExists": {
          "ram:RequestedResourceType": "datazone:Domain"
        }
      }
    },
    {
      "Sid": "RamResourceStatement",
      "Effect": "Allow",
      "Action": [
        "ram:DeleteResourceShare",
        "ram:AssociateResourceShare",
        "ram:DisassociateResourceShare",
        "ram:RejectResourceShareInvitation"
      ],
      "Resource": "*",
```

```
      "Condition": {
        "StringLike": {
          "ram:ResourceShareName": [
            "DataZone*"
          ]
        }
      }
    },
    {
      "Sid": "RamResourceReadOnlyStatement",
      "Effect": "Allow",
      "Action": [
        "ram:GetResourceShares",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShareAssociations"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMPassRoleStatement",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": [
        "arn:aws:iam::*:role/AmazonDataZone*",
        "arn:aws:iam::*:role/service-role/AmazonDataZone*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:passedToService": "datazone.amazonaws.com"
        }
      }
    },
    {
      "Sid": "IAMGetPolicyStatement",
      "Effect": "Allow",
      "Action": "iam:GetPolicy",
      "Resource": [
        "arn:aws:iam::*:policy/service-role/AmazonDataZoneRedshiftAccessPolicy*"
      ]
    },
    {
      "Sid": "DataZoneTagOnCreate",
      "Effect": "Allow",
      "Action": [
```

```
        "secretsmanager:TagResource"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AmazonDataZoneDomain"
          ]
        },
        "StringLike": {
          "aws:RequestTag/AmazonDataZoneDomain": "dzd_*",
          "aws:ResourceTag/AmazonDataZoneDomain": "dzd_*"
        },
        "Null": {
          "aws:TagKeys": "false"
        }
      }
    },
    {
      "Sid": "CreateSecretStatement",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:CreateSecret"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/AmazonDataZoneDomain": "dzd_*"
        }
      }
    }
  ]
}
```

政策考量和限制

AmazonDataZoneFullAccess政策不涵蓋某些功能。

- 如果您使用自己的 AWS KMS 金鑰建立 Amazon DataZone 網域，則必須擁有權限才kms:CreateGrant能成功建立網域kms:GenerateDataKey，kms:Decrypt以及允許該金鑰叫用其他 Amazon DataZone API，例如listDataSources和createDataSource。而且您還必須具有權限 kms:CreateGrantkms:Decrypt，kms:GenerateDataKey，和kms:DescribeKey該密鑰的資源策略。

如果您使用預設服務擁有的 KMS 金鑰，則不需要這樣做。

如需詳細資訊，請參閱 AWS Key Management Service。

- 如果要在 Amazon DataZone 主控台中使用建立和更新角色功能，則必須具有管理員權限或擁有必要的 IAM 許可，才能建立 IAM 角色和建立/更新政策。必要的權限包括`iam:CreateRole`、`iam:CreatePolicy`、`iam:CreatePolicyVersion`、`iam:DeletePolicyVers`和`iam:AttachRolePolicy`權限。
- 如果您在 Amazon 中建立新網域並啟 DataZone 用 AWS IAM Identity Center 使用者登入，或者在 Amazon 中為現有網域啟用該網域 DataZone，則必須具有下列項目的許可：`sso:CreateManagedApplicationInstance`、`sso:DeleteManagedApplicationInstance`、和`sso:PutApplicationAssignmentConfiguration`。
- 為了在 Amazon 接受 AWS 帳戶關聯請求 DataZone，您必須`ram:AcceptResourceShareInvitation`獲得許可。

AWS 受管理的策略： AmazonDataZoneFullUserAccess

此政策授予對 Amazon 的完整存取權限 DataZone，但不允許管理網域、使用者或關聯帳戶。

許可詳細資訊

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonDataZoneUserOperations",
      "Effect": "Allow",
      "Action": [
        "datazone:GetDomain",
        "datazone:CreateFormType",
        "datazone:GetFormType",
        "datazone:GetIamPortalLoginUrl",
        "datazone:SearchUserProfiles",
        "datazone:SearchGroupProfiles",
        "datazone:GetUserProfile",
        "datazone:GetGroupProfile",
        "datazone:ListGroupsForUser",
        "datazone:DeleteFormType",
        "datazone:CreateAssetType",
```

```
        "datazone:GetAssetType",
        "datazone:DeleteAssetType",
        "datazone:CreateGlossary",
        "datazone:GetGlossary",
        "datazone:DeleteGlossary",
        "datazone:UpdateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:GetGlossaryTerm",
        "datazone:DeleteGlossaryTerm",
        "datazone:UpdateGlossaryTerm",
        "datazone:CreateAsset",
        "datazone:GetAsset",
        "datazone:DeleteAsset",
        "datazone:CreateAssetRevision",
        "datazone:ListAssetRevisions",
        "datazone:AcceptPredictions",
        "datazone:RejectPredictions",
        "datazone:Search",
        "datazone:SearchTypes",
        "datazone:CreateListingChangeSet",
        "datazone:DeleteListing",
        "datazone:SearchListings",
        "datazone:GetListing",
        "datazone:CreateDataSource",
        "datazone:GetDataSource",
        "datazone:DeleteDataSource",
        "datazone:UpdateDataSource",
        "datazone:ListDataSources",
        "datazone:StartDataSourceRun",
        "datazone:GetDataSourceRun",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:GetEnvironmentBlueprint",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:ListEnvironmentBlueprints",
        "datazone:CreateProject",
        "datazone:UpdateProject",
        "datazone:GetProject",
        "datazone:DeleteProject",
        "datazone:ListProjects",
        "datazone:CreateProjectMembership",
```

```
        "datazone:DeleteProjectMembership",
        "datazone:ListProjectMemberships",
        "datazone:CreateEnvironmentProfile",
        "datazone:GetEnvironmentProfile",
        "datazone:UpdateEnvironmentProfile",
        "datazone:DeleteEnvironmentProfile",
        "datazone:ListEnvironmentProfiles",
        "datazone:CreateEnvironment",
        "datazone:GetEnvironment",
        "datazone:DeleteEnvironment",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:ListEnvironments",
        "datazone:ListAccountEnvironments",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetSubscriptionTarget",
        "datazone:DeleteSubscriptionTarget",
        "datazone:ListSubscriptionTargets",
        "datazone:CreateSubscriptionRequest",
        "datazone:AcceptSubscriptionRequest",
        "datazone:UpdateSubscriptionRequest",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectSubscriptionRequest",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:ListSubscriptionRequests",
        "datazone:DeleteSubscriptionRequest",
        "datazone:GetSubscription",
        "datazone:CancelSubscription",
        "datazone:GetSubscriptionEligibility",
        "datazone:ListSubscriptions",
        "datazone:RevokeSubscription",
        "datazone:CreateSubscriptionGrant",
        "datazone:DeleteSubscriptionGrant",
        "datazone:GetSubscriptionGrant",
        "datazone:ListSubscriptionGrants",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:ListNotifications",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource": "*"
```

```
    },
    {
      "Sid": "RAMResourceShareOperations",
      "Effect": "Allow",
      "Action": "ram:GetResourceShareAssociations",
      "Resource": "*"
    }
  ]
}
```

AWS 受管理的策略： AmazonDataZoneCustomEnvironmentDeploymentPolicy

您可以使用此原則來更新使用自訂藍圖建立之環境的組態。此政策也可用於建立 Amazon DataZone 訂閱目標和資料來源。

許可詳細資訊

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDataZoneCustomEnvironment",
   "Effect": "Allow",
   "Action": [
    "datazone:ListAssociatedAccounts",
    "datazone:GetAccountAssociation",
    "datazone:GetEnvironment",
    "datazone:GetEnvironmentProfile",
    "datazone:GetEnvironmentBlueprint",
    "datazone:GetProject",
    "datazone:UpdateEnvironmentConfiguration",
    "datazone:UpdateEnvironmentDeploymentStatus",
    "datazone:CreateSubscriptionTarget",
    "datazone:CreateDataSource"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS 受管理的策略：AmazonDataZoneEnvironmentRolePermissionsBoundary

> **Note**
>
> 此原則是權限界限。許可界限設定以身分為基礎的政策可授與 IAM 實體的最大許可。您不應該自行使用和附加 Amazon DataZone 許可邊界政策。Amazon DataZone 許可界限政策只能附加至 Amazon DataZone 受管角色。如需有關許可界限的詳細資訊，請參閱《IAM 使用者指南》中的 IAM 實體的許可界限。

當您透過 Amazon DataZone 資料入口網站建立環境時，Amazon 會將此許可界限 DataZone 套用至在建立環境期間產生的 IAM 角色。許可界限會限制 Amazon DataZone 建立的角色和您新增的任何角色的範圍。

Amazon DataZone 使用受`AmazonDataZoneEnvironmentRolePermissionsBoundary`管政策來限制所附加的佈建 IAM 主體。主體可能採用 Amazon DataZone 可代表互動式企業使用者或分析服務 (AWS Glue例如) 承擔的使用者角色形式，然後執行處理資料的動作，例如從 Amazon S3 讀取和寫入或執 AWS Glue 編目程式行。

該`AmazonDataZoneEnvironmentRolePermissionsBoundary`政策授予 Amazon 對 Amazon S3 AWS Glue，亞馬遜 Amazon DataZone Redshift 和亞馬 Amazon Athena 等服務的讀寫訪問權限。AWS Lake Formation此原則也會為使用這些服務 (例如網路介面和 AWS KMS 金鑰) 所需的某些基礎結構資源提供讀取和寫入權限。

Amazon DataZone 將`AmazonDataZoneEnvironmentRolePermissionsBoundary` AWS 受管政策作為所有 Amazon DataZone 環境角色 (擁有者和參與者) 的許可界限套用。此權限界限將這些角色限制為僅允許存取環境所需的必要資源和動作。

界限包括下列 JSON 陳述式：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateGlueConnection",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags"
      ],
```

```
      "Resource": [
        "arn:aws:ec2:*:*:network-interface/*"
      ],
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "aws-glue-service-resource"
          ]
        }
      }
    },
    {
      "Sid": "GlueOperations",
      "Effect": "Allow",
      "Action": [
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
```

```
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
```

```
    {
      "Sid": "PassRole",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/datazone*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "glue.amazonaws.com"
        }
      }
    },
    {
      "Sid": "SameAccountKmsOperations",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "KmsOperationsWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ListKeys",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:Verify",
        "kms:Sign"
      ],
      "Resource": "*",
      "Condition": {
```

```
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
    {
      "Sid": "AnalyticsOperations",
      "Effect": "Allow",
      "Action": [
        "datazone:*",
        "sqlworkbench:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QueryOperations",
      "Effect": "Allow",
      "Action": [
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
```

```
        "athena:ListQueryExecutions",
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:Describe*",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
```

```
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:SearchTables",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateDatabase",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListGroups",
        "iam:ListRolePolicies",
        "iam:ListRoles",
        "iam:ListUsers",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:DescribeMetricFilters",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
```

```
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "secretsmanager:ListSecrets",
        "tag:GetResources"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QueryOperationsWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "athena:GetQueryResultsStream"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
        }
      }
    },
    {
      "Sid": "SecretsManagerOperationsWithTagKeys",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:CreateSecret",
        "secretsmanager:TagResource"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/AmazonDataZoneDomain": "*",
          "aws:ResourceTag/AmazonDataZoneProject": "*"
        },
```

```
        "Null": {
          "aws:TagKeys": "false"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AmazonDataZoneDomain",
            "AmazonDataZoneProject"
          ]
        }
      }
    },
    {
      "Sid": "DataZoneS3Buckets",
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject"
      ],
      "Resource": [
        "arn:aws:s3:::*/datazone/*"
      ]
    },
    {
      "Sid": "DataZoneS3BucketLocation",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ListDataZoneS3Bucket",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "*"
```

```
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "*/datazone/*",
            "datazone/*"
          ]
        }
      }
    },
    {
      "Sid": "NotDeniedOperations",
      "Effect": "Deny",
      "NotAction": [
        "datazone:*",
        "sqlworkbench:*",
        "athena:BatchGetNamedQuery",
        "athena:BatchGetPreparedStatement",
        "athena:BatchGetQueryExecution",
        "athena:CreateNamedQuery",
        "athena:CreateNotebook",
        "athena:CreatePreparedStatement",
        "athena:CreatePresignedNotebookUrl",
        "athena:DeleteNamedQuery",
        "athena:DeleteNotebook",
        "athena:DeletePreparedStatement",
        "athena:ExportNotebook",
        "athena:GetDatabase",
        "athena:GetDataCatalog",
        "athena:GetNamedQuery",
        "athena:GetPreparedStatement",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryResultsStream",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetTableMetadata",
        "athena:GetWorkGroup",
        "athena:ImportNotebook",
        "athena:ListDatabases",
        "athena:ListDataCatalogs",
        "athena:ListEngineVersions",
        "athena:ListNamedQueries",
        "athena:ListPreparedStatements",
        "athena:ListQueryExecutions",
```

```
        "athena:ListTableMetadata",
        "athena:ListTagsForResource",
        "athena:ListWorkGroups",
        "athena:StartCalculationExecution",
        "athena:StartQueryExecution",
        "athena:StartSession",
        "athena:StopCalculationExecution",
        "athena:StopQueryExecution",
        "athena:TerminateSession",
        "athena:UpdateNamedQuery",
        "athena:UpdateNotebook",
        "athena:UpdateNotebookMetadata",
        "athena:UpdatePreparedStatement",
        "ec2:CreateNetworkInterface",
        "ec2:CreateTags",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteTags",
        "ec2:Describe*",
        "glue:*DataQuality*",
        "glue:BatchCreatePartition",
        "glue:BatchDeleteConnection",
        "glue:BatchDeletePartition",
        "glue:BatchDeleteTable",
        "glue:BatchDeleteTableVersion",
        "glue:BatchGetJobs",
        "glue:BatchGetPartition",
        "glue:BatchGetWorkflows",
        "glue:BatchStopJobRun",
        "glue:BatchUpdatePartition",
        "glue:CreateBlueprint",
        "glue:CreateConnection",
        "glue:CreateCrawler",
        "glue:CreateDatabase",
        "glue:CreateJob",
        "glue:CreatePartition",
        "glue:CreatePartitionIndex",
        "glue:CreateTable",
        "glue:CreateWorkflow",
        "glue:DeleteBlueprint",
        "glue:DeleteColumnStatisticsForPartition",
        "glue:DeleteColumnStatisticsForTable",
        "glue:DeleteConnection",
        "glue:DeleteCrawler",
        "glue:DeleteJob",
```

```
        "glue:DeletePartition",
        "glue:DeletePartitionIndex",
        "glue:DeleteTable",
        "glue:DeleteTableVersion",
        "glue:DeleteWorkflow",
        "glue:GetColumnStatisticsForPartition",
        "glue:GetColumnStatisticsForTable",
        "glue:GetConnection",
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:ListSchemas",
        "glue:ListJobs",
        "glue:NotifyEvent",
        "glue:PutWorkflowRunProperties",
        "glue:ResetJobBookmark",
        "glue:ResumeWorkflowRun",
        "glue:SearchTables",
        "glue:StartBlueprintRun",
        "glue:StartCrawler",
        "glue:StartCrawlerSchedule",
        "glue:StartJobRun",
        "glue:StartWorkflowRun",
        "glue:StopCrawler",
        "glue:StopCrawlerSchedule",
        "glue:StopWorkflowRun",
        "glue:UpdateBlueprint",
        "glue:UpdateColumnStatisticsForPartition",
        "glue:UpdateColumnStatisticsForTable",
        "glue:UpdateConnection",
        "glue:UpdateCrawler",
        "glue:UpdateCrawlerSchedule",
        "glue:UpdateDatabase",
        "glue:UpdateJob",
        "glue:UpdatePartition",
        "glue:UpdateTable",
        "glue:UpdateWorkflow",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:List*",
        "iam:PassRole",
```

```
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey",
        "kms:ListKeys",
        "kms:Verify",
        "kms:Sign",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:DescribeMetricFilters",
        "logs:DescribeQueries",
        "logs:DescribeQueryDefinitions",
        "logs:StartQuery",
        "logs:StopQuery",
        "logs:GetLogEvents",
        "logs:GetLogGroupFields",
        "logs:GetQueryResults",
        "logs:GetLogRecord",
        "logs:PutLogEvents",
        "logs:CreateLogStream",
        "logs:FilterLogEvents",
        "lakeformation:GetDataAccess",
        "lakeformation:GetDataLakeSettings",
        "lakeformation:GetResourceLFTags",
        "lakeformation:ListPermissions",
        "redshift-data:ListTables",
        "redshift-data:DescribeTable",
        "redshift-data:ListSchemas",
        "redshift-data:ListDatabases",
        "redshift-data:ExecuteStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:DescribeStatement",
        "redshift:CreateClusterUser",
        "redshift:DescribeClusters",
        "redshift:DescribeDataShares",
        "redshift:GetClusterCredentials",
        "redshift:GetClusterCredentialsWithIAM",
        "redshift:JoinGroup",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetNamespace",
        "redshift-serverless:GetWorkgroup",
        "redshift-serverless:GetCredentials",
        "s3:AbortMultipartUpload",
```

```
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:PutObject",
        "s3:PutObjectRetention",
        "s3:ReplicateObject",
        "s3:RestoreObject",
        "secretsmanager:CreateSecret",
        "secretsmanager:ListSecrets",
        "secretsmanager:TagResource",
        "tag:GetResources"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

AWS 受管理的策略：AmazonDataZoneRedshiftGlueProvisioningPolicy

該AmazonDataZoneRedshiftGlueProvisioningPolicy政策授予 Amazon DataZone 與 AWS Glue 和亞 Amazon Redshift 互操作所需的許可。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonDataZonePermissionsToCreateEnvironmentRole",
   "Effect": "Allow",
   "Action": [
    "iam:CreateRole",
    "iam:DetachRolePolicy",
    "iam:DeleteRolePolicy",
    "iam:AttachRolePolicy",
    "iam:PutRolePolicy"
   ],
```

```
    "Resource": "arn:aws:iam::*:role/datazone*",
    "Condition": {
     "StringEquals": {
      "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonDataZoneEnvironmentRolePermissionsBoundary",
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "IamPassRolePermissions",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/datazone*"
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "glue.amazonaws.com",
       "lakeformation.amazonaws.com"
      ],
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZonePermissionsToManageCreatedEnvironmentRole",
    "Effect": "Allow",
    "Action": [
     "iam:DeleteRole",
     "iam:GetRole"
    ],
    "Resource": "arn:aws:iam::*:role/datazone*",
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
```

```
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneCFStackCreationForEnvironments",
    "Effect": "Allow",
    "Action": [
     "cloudformation:CreateStack",
     "cloudformation:TagResource"
    ],
    "Resource": [
     "arn:aws:cloudformation:*:*:stack/DataZone*"
    ],
    "Condition": {
     "ForAnyValue:StringLike": {
      "aws:TagKeys": "AmazonDataZoneEnvironment"
     },
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "AmazonDataZoneCFStackManagementForEnvironments",
    "Effect": "Allow",
    "Action": [
     "cloudformation:DeleteStack",
     "cloudformation:DescribeStacks",
     "cloudformation:DescribeStackEvents"
    ],
    "Resource": [
     "arn:aws:cloudformation:*:*:stack/DataZone*"
    ]
   },
   {
    "Sid": "AmazonDataZoneEnvironmentParameterValidation",
    "Effect": "Allow",
    "Action": [
     "lakeformation:GetDataLakeSettings",
     "lakeformation:PutDataLakeSettings",
     "lakeformation:RevokePermissions",
     "lakeformation:ListPermissions",
     "glue:CreateDatabase",
```

```
    "glue:GetDatabase",
    "athena:GetWorkGroup",
    "logs:DescribeLogGroups",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift:DescribeClusters",
    "secretsmanager:ListSecrets"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AmazonDataZoneEnvironmentLakeFormationPermissions",
   "Effect": "Allow",
   "Action": [
    "lakeformation:RegisterResource",
    "lakeformation:DeregisterResource",
    "lakeformation:GrantPermissions",
    "lakeformation:ListResources"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentGlueDeletePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:DeleteDatabase"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
```

```
    "Sid": "AmazonDataZoneEnvironmentAthenaDeletePermissions",
    "Effect": "Allow",
    "Action": [
     "athena:DeleteWorkGroup"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentAthenaResourceCreation",
    "Effect": "Allow",
    "Action": [
     "athena:CreateWorkGroup",
     "athena:TagResource",
     "iam:TagRole",
     "iam:TagPolicy",
     "logs:TagLogGroup"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringLike": {
      "aws:TagKeys": "AmazonDataZoneEnvironment"
     },
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     },
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentLogGroupCreation",
    "Effect": "Allow",
    "Action": [
     "logs:CreateLogGroup",
```

```
    "logs:DeleteLogGroup"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:datazone-*",
   "Condition": {
    "ForAnyValue:StringLike": {
     "aws:TagKeys": "AmazonDataZoneEnvironment"
    },
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    },
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentLogGroupManagement",
   "Action": [
    "logs:PutRetentionPolicy"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:datazone-*",
   "Effect": "Allow",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentIAMPolicyManagement",
   "Effect": "Allow",
   "Action": [
    "iam:DeletePolicy",
    "iam:CreatePolicy",
    "iam:GetPolicy",
    "iam:ListPolicyVersions"
   ],
   "Resource": [
    "arn:aws:iam::*:policy/datazone*"
   ],
```

```
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentS3ValidationPermissions",
    "Effect": "Allow",
    "Action": [
     "s3:ListAllMyBuckets",
     "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::*"
   },
   {
    "Sid": "AmazonDataZoneEnvironmentKMSDecryptPermissions",
    "Effect": "Allow",
    "Action": [
     "kms:GenerateDataKey",
     "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "PermissionsToTagAmazonDataZoneEnvironmentGlueResources",
    "Effect": "Allow",
    "Action": [
     "glue:TagResource"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringLike": {
      "aws:TagKeys": "AmazonDataZoneEnvironment"
     },
     "Null": {
      "aws:RequestTag/AmazonDataZoneEnvironment": "false"
```

```
    }
   }
  },
  {
   "Sid": "PermissionsToGetAmazonDataZoneEnvironmentBlueprintTemplates",
   "Effect": "Allow",
   "Action": "s3:GetObject",
   "Resource": "*",
   "Condition": {
    "StringNotEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    },
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "RedshiftDataPermissions",
   "Effect": "Allow",
   "Action": [
    "redshift-data:ListSchemas",
    "redshift-data:ExecuteStatement"
   ],
   "Resource": [
    "arn:aws:redshift-serverless:*:*:workgroup/*",
    "arn:aws:redshift:*:*:cluster:*"
   ]
  },
  {
   "Sid": "DescribeStatementPermissions",
   "Effect": "Allow",
   "Action": [
    "redshift-data:DescribeStatement"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GetSecretValuePermissions",
   "Effect": "Allow",
   "Action": [
    "secretsmanager:GetSecretValue"
```

```
    ],
    "Resource": "*",
    "Condition": {
     "StringLike": {
      "secretsmanager:ResourceTag/AmazonDataZoneDomain": "dzd*"
     }
    }
   }
  ]
}
```

AWS 受管理的策略：AmazonDataZoneGlueManageAccessRolePolicy

此政策授予 Amazon DataZone 許可將 AWS Glue 資料發佈到目錄。它還授予 Amazon DataZone 許可，以授予目錄中 AWS Glue 已發佈資產的存取權或撤銷存取權限。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "GlueDataQualityPermissions",
   "Effect": "Allow",
   "Action": [
    "glue:ListDataQualityResults",
    "glue:GetDataQualityResult"
   ],
   "Resource": "arn:aws:glue:*:*:dataQualityRuleset/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "GlueTableDatabasePermissions",
   "Effect": "Allow",
   "Action": [
    "glue:CreateTable",
    "glue:DeleteTable",
```

```
    "glue:GetDatabases",
    "glue:GetTables"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*",
    "arn:aws:glue:*:*:table/*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "LakeformationResourceSharingPermissions",
   "Effect": "Allow",
   "Action": [
    "lakeformation:BatchGrantPermissions",
    "lakeformation:BatchRevokePermissions",
    "lakeformation:CreateLakeFormationOptIn",
    "lakeformation:DeleteLakeFormationOptIn",
    "lakeformation:GrantPermissions",
    "lakeformation:GetResourceLFTags",
    "lakeformation:ListLakeFormationOptIns",
    "lakeformation:ListPermissions",
    "lakeformation:RegisterResource",
    "lakeformation:RevokePermissions",
    "glue:GetDatabase",
    "glue:GetTable",
    "organizations:DescribeOrganization",
    "ram:GetResourceShareInvitations",
    "ram:ListResources"
   ],
   "Resource": "*"
  },
  {
   "Sid": "CrossAccountRAMResourceSharingPermissions",
   "Effect": "Allow",
   "Action": [
    "glue:DeleteResourcePolicy",
    "glue:PutResourcePolicy"
   ],
   "Resource": [
```

```
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/*",
    "arn:aws:glue:*:*:table/*"
   ],
   "Condition": {
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "ram.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountLakeFormationResourceSharingPermissions",
   "Effect": "Allow",
   "Action": [
    "ram:CreateResourceShare"
   ],
   "Resource": "*",
   "Condition": {
    "StringEqualsIfExists": {
     "ram:RequestedResourceType": [
      "glue:Table",
      "glue:Database",
      "glue:Catalog"
     ]
    },
    "ForAnyValue:StringEquals": {
     "aws:CalledVia": [
      "lakeformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "CrossAccountRAMResourceShareInvitationPermission",
   "Effect": "Allow",
   "Action": [
    "ram:AcceptResourceShareInvitation"
   ],
   "Resource": "arn:aws:ram:*:*:resource-share-invitation/*"
  },
  {
   "Sid": "CrossAccountRAMResourceSharingViaLakeFormationPermissions",
```

```
    "Effect": "Allow",
    "Action": [
     "ram:AssociateResourceShare",
     "ram:DeleteResourceShare",
     "ram:DisassociateResourceShare",
     "ram:GetResourceShares",
     "ram:ListResourceSharePermissions",
     "ram:UpdateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
     "StringLike": {
      "ram:ResourceShareName": [
       "LakeFormation*"
      ]
     },
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
       "lakeformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "CrossAccountRAMResourceSharingViaLakeFormationHybrid",
    "Effect": "Allow",
    "Action": "ram:AssociateResourceSharePermission",
    "Resource": "*",
    "Condition": {
     "StringLike": {
      "ram:PermissionArn": "arn:aws:ram::aws:permission/AWSRAMLFEnabled*"
     },
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
       "lakeformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "KMSDecryptPermission",
    "Effect": "Allow",
    "Action": [
     "kms:Decrypt"
```

```
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/datazone:projectId": "proj-all"
     }
    }
   },
   {
    "Sid": "GetRoleForDataZone",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/AmazonDataZone*",
     "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ]
   },
   {
    "Sid": "PassRoleForDataLocationRegistration",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/AmazonDataZone*",
     "arn:aws:iam::*:role/service-role/AmazonDataZone*"
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "lakeformation.amazonaws.com"
      ]
     }
    }
   }
  ]
}
```

AWS 受管理的策略：AmazonDataZoneRedshiftManageAccessRolePolicy

此政策授予 Amazon DataZone 許可，將 Amazon Redshift 數據發佈到目錄。它還授予 Amazon DataZone 許可，以授予目錄中亞馬遜 Redshift 或 Amazon Redshift 無伺服器已發佈資產的存取權限或撤銷存取權。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "redshiftDataScopeDownPermissions",
   "Effect": "Allow",
   "Action": [
    "redshift-data:BatchExecuteStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:ListTables",
    "redshift-data:ListSchemas",
    "redshift-data:ListDatabases"
   ],
   "Resource": [
    "arn:aws:redshift-serverless:*:*:workgroup/*",
    "arn:aws:redshift:*:*:cluster:*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "listSecretsPermission",
   "Effect": "Allow",
   "Action": "secretsmanager:ListSecrets",
   "Resource": "*"
  },
  {
   "Sid": "getWorkgroupPermission",
   "Effect": "Allow",
   "Action": "redshift-serverless:GetWorkgroup",
   "Resource": [
    "arn:aws:redshift-serverless:*:*:workgroup/*"
```

```
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "getNamespacePermission",
    "Effect": "Allow",
    "Action": "redshift-serverless:GetNamespace",
    "Resource": [
     "arn:aws:redshift-serverless:*:*:namespace/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "redshiftDataPermissions",
    "Effect": "Allow",
    "Action": [
     "redshift-data:DescribeStatement",
     "redshift-data:GetStatementResult",
     "redshift:DescribeClusters"
    ],
    "Resource": "*"
   },
   {
    "Sid": "dataSharesPermissions",
    "Effect": "Allow",
    "Action": [
     "redshift:AuthorizeDataShare",
     "redshift:DescribeDataShares"
    ],
    "Resource": [
     "arn:aws:redshift:*:*:datashare:*/datazone*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
```

```
   }
  },
  {
   "Sid": "associateDataShareConsumerPermission",
   "Effect": "Allow",
   "Action": "redshift:AssociateDataShareConsumer",
   "Resource": "arn:aws:redshift:*:*:datashare:*/datazone*"
  }
 ]
}
```

AWS 受管政策：AmazonDataZoneCrossAccountAdmin

您可以將政 AmazonDataZoneCrossAccountAdmin 策附加到 IAM 身分。

此政策可讓使用者使用 Amazon DataZone 關聯帳戶。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ram:UpdateResourceShare",
                "ram:DeleteResourceShare",
                "ram:AssociateResourceShare",
                "ram:DisassociateResourceShare",
                "ram:GetResourceShares"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ram:ResourceShareName": [
                        "DataZone*"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "datazone:PutEnvironmentBlueprintConfiguration",
```

```
                "datazone:GetEnvironmentBlueprintConfiguration",
                "datazone:DeleteEnvironmentBlueprintConfiguration",
                "datazone:ListEnvironmentBlueprintConfigurations",
                "datazone:ListDomains",
                "datazone:GetDomain",
                "datazone:GetEnvironmentBlueprint",
                "datazone:ListEnvironmentBlueprints",
                "datazone:ListEnvironments",
                "datazone:GetEnvironment",
                "ram:AcceptResourceShareInvitation",
                "ram:RejectResourceShareInvitation",
                "ram:Get*",
                "ram:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 受管理的策略：AmazonDataZoneDomainExecutionRolePolicy

這是 Amazon DataZone DomainExecutionRole 服務角色的預設政策。Amazon 使用此角色 DataZone 來編目、探索、管理、共用和分析 Amazon DataZone 網域中的資料。

您可以將 AmazonDataZoneDomainExecutionRolePolicy 政策附加到您的AmazonDataZoneDomainExecutionRole.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DomainExecutionRoleStatement",
      "Effect": "Allow",
      "Action": [
        "datazone:AcceptPredictions",
        "datazone:AcceptSubscriptionRequest",
        "datazone:CancelSubscription",
        "datazone:CreateAsset",
        "datazone:CreateAssetRevision",
        "datazone:CreateAssetType",
        "datazone:CreateDataSource",
```

```
        "datazone:CreateEnvironment",
        "datazone:CreateEnvironmentBlueprint",
        "datazone:CreateEnvironmentProfile",
        "datazone:CreateFormType",
        "datazone:CreateGlossary",
        "datazone:CreateGlossaryTerm",
        "datazone:CreateListingChangeSet",
        "datazone:CreateProject",
        "datazone:CreateProjectMembership",
        "datazone:CreateSubscriptionGrant",
        "datazone:CreateSubscriptionRequest",
        "datazone:DeleteAsset",
        "datazone:DeleteAssetType",
        "datazone:DeleteDataSource",
        "datazone:DeleteEnvironment",
        "datazone:DeleteEnvironmentBlueprint",
        "datazone:DeleteEnvironmentProfile",
        "datazone:DeleteFormType",
        "datazone:DeleteGlossary",
        "datazone:DeleteGlossaryTerm",
        "datazone:DeleteListing",
        "datazone:DeleteProject",
        "datazone:DeleteProjectMembership",
        "datazone:DeleteSubscriptionGrant",
        "datazone:DeleteSubscriptionRequest",
        "datazone:DeleteSubscriptionTarget",
        "datazone:GetAsset",
        "datazone:GetAssetType",
        "datazone:GetDataSource",
        "datazone:GetDataSourceRun",
        "datazone:GetDomain",
        "datazone:GetEnvironment",
        "datazone:GetEnvironmentActionLink",
        "datazone:GetEnvironmentBlueprint",
        "datazone:GetEnvironmentCredentials",
        "datazone:GetEnvironmentProfile",
        "datazone:GetFormType",
        "datazone:GetGlossary",
        "datazone:GetGlossaryTerm",
        "datazone:GetGroupProfile",
        "datazone:GetListing",
        "datazone:GetProject",
        "datazone:GetSubscription",
        "datazone:GetSubscriptionEligibility",
```

```
        "datazone:GetSubscriptionGrant",
        "datazone:GetSubscriptionRequestDetails",
        "datazone:GetSubscriptionTarget",
        "datazone:GetUserProfile",
        "datazone:ListAccountEnvironments",
        "datazone:ListAssetRevisions",
        "datazone:ListDataSourceRunActivities",
        "datazone:ListDataSourceRuns",
        "datazone:ListDataSources",
        "datazone:ListEnvironmentBlueprintConfigurations",
        "datazone:ListEnvironmentBlueprintConfigurationSummaries",
        "datazone:ListEnvironmentBlueprints",
        "datazone:ListEnvironmentProfiles",
        "datazone:ListEnvironments",
        "datazone:ListGroupsForUser",
        "datazone:ListNotifications",
        "datazone:ListProjectMemberships",
        "datazone:ListProjects",
        "datazone:ListSubscriptionGrants",
        "datazone:ListSubscriptionRequests",
        "datazone:ListSubscriptionTargets",
        "datazone:ListSubscriptions",
        "datazone:ListWarehouseMetadata",
        "datazone:RejectPredictions",
        "datazone:RejectSubscriptionRequest",
        "datazone:RevokeSubscription",
        "datazone:Search",
        "datazone:SearchGroupProfiles",
        "datazone:SearchListings",
        "datazone:SearchTypes",
        "datazone:SearchUserProfiles",
        "datazone:StartDataSourceRun",
        "datazone:UpdateDataSource",
        "datazone:UpdateEnvironment",
        "datazone:UpdateEnvironmentBlueprint",
        "datazone:UpdateEnvironmentDeploymentStatus",
        "datazone:UpdateEnvironmentProfile",
        "datazone:UpdateGlossary",
        "datazone:UpdateGlossaryTerm",
        "datazone:UpdateProject",
        "datazone:UpdateSubscriptionGrantStatus",
        "datazone:UpdateSubscriptionRequest",
        "datazone:StartMetadataGenerationRun",
        "datazone:GetMetadataGenerationRun",
```

```
        "datazone:CancelMetadataGenerationRun",
        "datazone:ListMetadataGenerationRuns"
      ],
      "Resource": "*"
    },
    {
      "Sid": "RAMResourceShareStatement",
      "Effect": "Allow",
      "Action": "ram:GetResourceShareAssociations",
      "Resource": "*"
    }
  ]
}
```

AWS 受管理的策略：AmazonDataZoneSageMakerProvisioning

該 AmazonDataZoneSageMakerProvisioning 政策授予 Amazon 與 Amazon SageMaker 互操作所需 DataZone 的許可。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CreateSageMakerStudio",
   "Effect": "Allow",
   "Action": [
    "sagemaker:CreateDomain"
   ],
   "Resource": [
    "*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    },
    "ForAnyValue:StringEquals": {
     "aws:TagKeys": [
      "AmazonDataZoneEnvironment"
     ]
    },
```

```
    "Null": {
     "aws:TagKeys": "false",
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false",
     "aws:RequestTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "DeleteSageMakerStudio",
   "Effect": "Allow",
   "Action": [
    "sagemaker:DeleteDomain"
   ],
   "Resource": [
    "*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    },
    "ForAnyValue:StringLike": {
     "aws:TagKeys": [
      "AmazonDataZoneEnvironment"
     ]
    },
    "Null": {
     "aws:TagKeys": "false",
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentSageMakerDescribePermissions",
   "Effect": "Allow",
   "Action": [
    "sagemaker:DescribeDomain"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
```

```
      ]
     }
    }
   },
   {
    "Sid": "IamPassRolePermissions",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "glue.amazonaws.com",
       "lakeformation.amazonaws.com",
       "sagemaker.amazonaws.com"
      ],
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "AmazonDataZonePermissionsToCreateEnvironmentRole",
    "Effect": "Allow",
    "Action": [
     "iam:CreateRole",
     "iam:DetachRolePolicy",
     "iam:DeleteRolePolicy",
     "iam:AttachRolePolicy",
     "iam:PutRolePolicy"
    ],
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ],
```

```
     "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary"
    }
   }
  },
  {
   "Sid": "AmazonDataZonePermissionsToManageEnvironmentRole",
   "Effect": "Allow",
   "Action": [
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:DeleteRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/sm-provisioning/datazone_usr*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZonePermissionsToCreateSageMakerServiceRole",
   "Effect": "Allow",
   "Action": [
    "iam:CreateServiceLinkedRole"
   ],
   "Resource": [
    "arn:aws:iam::*:role/aws-service-role/sagemaker.amazonaws.com/
AWSServiceRoleForAmazonSageMakerNotebooks"
   ],
   "Condition": {
    "StringEquals": {
     "aws:CalledViaFirst": [
      "cloudformation.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AmazonDataZoneEnvironmentParameterValidation",
```

```
    "Effect": "Allow",
    "Action": [
     "ec2:DescribeVpcs",
     "ec2:DescribeSubnets",
     "sagemaker:ListDomains"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AmazonDataZoneEnvironmentKMSKeyValidation",
    "Effect": "Allow",
    "Action": [
     "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "AmazonDataZoneEnvironmentGluePermissions",
    "Effect": "Allow",
    "Action": [
     "glue:CreateConnection",
     "glue:DeleteConnection"
    ],
    "Resource": [
     "arn:aws:glue:*:*:connection/dz-sm-athena-glue-connection-*",
     "arn:aws:glue:*:*:connection/dz-sm-redshift-cluster-connection-*",
     "arn:aws:glue:*:*:connection/dz-sm-redshift-serverless-connection-*",
     "arn:aws:glue:*:*:catalog"
    ],
    "Condition": {
     "StringEquals": {
      "aws:CalledViaFirst": [
       "cloudformation.amazonaws.com"
      ]
     }
    }
   }
  ]
}
```

AWS 受管理的策略：AmazonDataZoneSageMakerAccess

此政策授予 Amazon DataZone 許可，將 Amazon SageMaker 資產發佈到目錄。它還授予 Amazon DataZone 許可，以授予對目錄中 Amazon SageMaker 已發佈資產的存取權或撤銷存取權。

此政策包含執行以下動作的許可：

- 雲軌道 — 檢索有關跟 CloudTrail 踪的信息。
- 雲觀察-檢索當前的 CloudWatch 警報。
- logs — 擷取防護記 CloudWatch 錄的指標篩選器。
- SNS — 擷取 SNS 主題的訂閱清單。
- Config — 擷取有關組態記錄器、資源和組 AWS 態規則的資訊。也允許服務連結角色建立和刪除 AWS Config 規則，以及針對規則執行評估。
- iam — 獲取並生成帳戶的憑據報告。
- 組織 — 擷取組織的帳戶和組織單位 (OU) 資訊。
- 安全中心 — 擷取有關如何設定 Security Hub 服務、標準和控制項的資訊。
- 標籤 — 擷取有關資源標籤的資訊。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "AmazonSageMakerReadPermission",
   "Effect": "Allow",
   "Action": [
    "sagemaker:DescribeFeatureGroup",
    "sagemaker:ListModelPackages",
    "sagemaker:DescribeModelPackage",
    "sagemaker:DescribeModelPackageGroup",
    "sagemaker:DescribeAlgorithm",
    "sagemaker:ListTags",
    "sagemaker:DescribeDomain",
    "sagemaker:GetModelPackageGroupPolicy",
    "sagemaker:Search"
   ],
   "Resource": "*"
```

```
  },
  {
   "Sid": "AmazonSageMakerTaggingPermission",
   "Effect": "Allow",
   "Action": [
    "sagemaker:AddTags",
    "sagemaker:DeleteTags"
   ],
   "Resource": "*",
   "Condition": {
    "ForAnyValue:StringLike": {
     "aws:TagKeys": [
      "sagemaker:shared-with:*"
     ]
    }
   }
  },
  {
   "Sid": "AmazonSageMakerModelPackageGroupPolicyPermission",
   "Effect": "Allow",
   "Action": [
    "sagemaker:PutModelPackageGroupPolicy",
    "sagemaker:DeleteModelPackageGroupPolicy"
   ],
   "Resource": [
    "arn:*:sagemaker:*:*:model-package-group/*"
   ]
  },
  {
   "Sid": "AmazonSageMakerRAMPermission",
   "Effect": "Allow",
   "Action": [
    "ram:GetResourceShares",
    "ram:GetResourceShareInvitations",
    "ram:GetResourceShareAssociations"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AmazonSageMakerRAMResourcePolicyPermission",
   "Effect": "Allow",
   "Action": [
    "sagemaker:PutResourcePolicy",
    "sagemaker:GetResourcePolicy",
```

```
    "sagemaker:DeleteResourcePolicy"
   ],
   "Resource": [
    "arn:*:sagemaker:*:*:feature-group/*"
   ]
  },
  {
   "Sid": "AmazonSageMakerRAMTagResourceSharePermission",
   "Effect": "Allow",
   "Action": [
    "ram:TagResource"
   ],
   "Resource": "arn:*:ram:*:*:resource-share/*",
   "Condition": {
    "Null": {
     "aws:RequestTag/AwsDataZoneDomainId": "false"
    }
   }
  },
  {
   "Sid": "AmazonSageMakerRAMDeleteResourceSharePermission",
   "Effect": "Allow",
   "Action": [
    "ram:DeleteResourceShare"
   ],
   "Resource": "arn:*:ram:*:*:resource-share/*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AwsDataZoneDomainId": "false"
    }
   }
  },
  {
   "Sid": "AmazonSageMakerRAMCreateResourceSharePermission",
   "Effect": "Allow",
   "Action": [
    "ram:CreateResourceShare"
   ],
   "Resource": "*",
   "Condition": {
    "StringLikeIfExists": {
     "ram:RequestedResourceType": [
      "sagemaker:*"
     ]
```

```
    },
    "Null": {
     "aws:RequestTag/AwsDataZoneDomainId": "false"
    }
   }
  },
  {
   "Sid": "AmazonSageMakerS3BucketPolicyPermission",
   "Effect": "Allow",
   "Action": [
    "s3:DeleteBucketPolicy",
    "s3:PutBucketPolicy",
    "s3:GetBucketPolicy"
   ],
   "Resource": [
    "arn:aws:s3:::sagemaker-datazone*",
    "arn:aws:s3:::SageMaker-DataZone*",
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::amazon-datazone*"
   ]
  },
  {
   "Sid": "AmazonSageMakerS3Permission",
   "Effect": "Allow",
   "Action": [
    "s3:GetObject",
    "s3:ListBucket"
   ],
   "Resource": [
    "arn:aws:s3:::sagemaker-datazone*",
    "arn:aws:s3:::SageMaker-DataZone*",
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::DataZone-SageMaker*",
    "arn:aws:s3:::amazon-datazone*"
   ]
  },
  {
   "Sid": "AmazonSageMakerECRPermission",
   "Effect": "Allow",
   "Action": [
    "ecr:GetRepositoryPolicy",
    "ecr:SetRepositoryPolicy",
    "ecr:DeleteRepositoryPolicy"
```

```
    ],
    "Resource": "*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "AmazonSageMakerKMSReadPermission",
    "Effect": "Allow",
    "Action": [
     "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
       "AmazonDataZoneEnvironment"
      ]
     }
    }
   },
   {
    "Sid": "AmazonSageMakerKMSGrantPermission",
    "Effect": "Allow",
    "Action": [
     "kms:CreateGrant"
    ],
    "Resource": "*",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
       "AmazonDataZoneEnvironment"
      ]
     },
     "ForAllValues:StringEquals": {
      "kms:GrantOperations": [
       "Decrypt"
      ]
     }
    }
   }
  ]
```

```
}
```

AWS 受管理的策略：AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary

> **Note**
>
> 此原則是權限界限。許可界限設定以身分為基礎的政策可授與 IAM 實體的最大許可。您不應該自行使用和附加 Amazon DataZone 許可邊界政策。Amazon DataZone 許可界限政策只能附加至 Amazon DataZone 受管角色。如需有關許可界限的詳細資訊，請參閱《IAM 使用者指南》中的 IAM 實體的許可界限。

當您透過 Amazon DataZone 資料入口網站建立 Amazon SageMaker 環境時，Amazon 會將此許可界限 DataZone 套用至在建立環境期間產生的 IAM 角色。許可界限會限制 Amazon DataZone 建立的角色和您新增的任何角色的範圍。

Amazon DataZone 使用受`AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`管政策來限制所附加的佈建 IAM 主體。主體可能採用 Amazon DataZone 可代表互動式企業使用者或分析服務 (AWS SageMaker例如) 承擔的使用者角色形式，然後執行處理資料的動作，例如從 Amazon S3 或 Amazon Redshift 讀取和寫入，或執行 AWS Glue 爬行程式。

該`AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`政策授予 Amazon 對 Amazon SageMaker， AWS Glue，Amazon DataZone S3， AWS Lake Formation，亞馬遜 Redshift 和亞馬 Amazon Athena 等服務的讀寫訪問權限。該政策還為使用這些服務 (例如網路界面、Amazon ECR 存放庫和 AWS KMS 金鑰) 所需的某些基礎設施資源提供讀取和寫入許可。它還可以訪問 Amazon SageMaker 應用程序，如 Amazon SageMaker 帆布。

Amazon DataZone 將`AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary`受管政策作為所有 Amazon DataZone 環境角色 (擁有者和參與者) 的許可界限套用。此權限界限將這些角色限制為僅允許存取環境所需的必要資源和動作。

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

```
    "Effect": "Allow",
    "Action": [
     "sagemaker:*",
     "sagemaker-geospatial:*"
    ],
    "NotResource": [
     "arn:aws:sagemaker:*:*:domain/*",
     "arn:aws:sagemaker:*:*:user-profile/*",
     "arn:aws:sagemaker:*:*:app/*",
     "arn:aws:sagemaker:*:*:space/*",
     "arn:aws:sagemaker:*:*:flow-definition/*"
    ]
   },
   {
    "Sid": "AllowSageMakerProfileManagement",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateUserProfile",
     "sagemaker:DescribeUserProfile",
     "sagemaker:UpdateUserProfile",
     "sagemaker:CreatePresignedDomainUrl"
    ],
    "Resource": "arn:aws:sagemaker:*:*:*/*"
   },
   {
    "Sid": "AllowLakeFormation",
    "Effect": "Allow",
    "Action": [
     "lakeformation:GetDataAccess"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AllowAddTagsForAppAndSpace",
    "Effect": "Allow",
    "Action": [
     "sagemaker:AddTags"
    ],
    "Resource": [
     "arn:aws:sagemaker:*:*:app/*",
     "arn:aws:sagemaker:*:*:space/*"
    ],
    "Condition": {
     "StringEquals": {
```

```
      "sagemaker:TaggingAction": [
       "CreateApp",
       "CreateSpace"
      ]
     }
    }
   },
   {
    "Sid": "AllowStudioActions",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreatePresignedDomainUrl",
     "sagemaker:DescribeApp",
     "sagemaker:DescribeDomain",
     "sagemaker:DescribeSpace",
     "sagemaker:DescribeUserProfile",
     "sagemaker:ListApps",
     "sagemaker:ListDomains",
     "sagemaker:ListSpaces",
     "sagemaker:ListUserProfiles"
    ],
    "Resource": "*"
   },
   {
    "Sid": "AllowAppActionsForUserProfile",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateApp",
     "sagemaker:DeleteApp"
    ],
    "Resource": "arn:aws:sagemaker:*:*:app/*/*/*/*",
    "Condition": {
     "Null": {
      "sagemaker:OwnerUserProfileArn": "true"
     }
    }
   },
   {
    "Sid": "AllowAppActionsForSharedSpaces",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateApp",
     "sagemaker:DeleteApp"
    ],
```

```
    "Resource": "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
    "Condition": {
     "StringEquals": {
      "sagemaker:SpaceSharingType": [
       "Shared"
      ]
     }
    }
   },
   {
    "Sid": "AllowMutatingActionsOnSharedSpacesWithoutOwner",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateSpace",
     "sagemaker:DeleteSpace",
     "sagemaker:UpdateSpace"
    ],
    "Resource": "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
    "Condition": {
     "Null": {
      "sagemaker:OwnerUserProfileArn": "true"
     }
    }
   },
   {
    "Sid": "RestrictMutatingActionsOnSpacesToOwnerUserProfile",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateSpace",
     "sagemaker:DeleteSpace",
     "sagemaker:UpdateSpace"
    ],
    "Resource": "arn:aws:sagemaker:*:*:space/${sagemaker:DomainId}/*",
    "Condition": {
     "ArnLike": {
      "sagemaker:OwnerUserProfileArn": "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
     },
     "StringEquals": {
      "sagemaker:SpaceSharingType": [
       "Private",
       "Shared"
      ]
     }
```

```
    }
   },
   {
    "Sid": "RestrictMutatingActionsOnPrivateSpaceAppsToOwnerUserProfile",
    "Effect": "Allow",
    "Action": [
     "sagemaker:CreateApp",
     "sagemaker:DeleteApp"
    ],
    "Resource": "arn:aws:sagemaker:*:*:app/${sagemaker:DomainId}/*/*/*",
    "Condition": {
     "ArnLike": {
      "sagemaker:OwnerUserProfileArn": "arn:aws:sagemaker:*:*:user-profile/
${sagemaker:DomainId}/${sagemaker:UserProfileName}"
     },
     "StringEquals": {
      "sagemaker:SpaceSharingType": [
       "Private"
      ]
     }
    }
   },
   {
    "Sid": "AllowFlowDefinitionActions",
    "Effect": "Allow",
    "Action": "sagemaker:*",
    "Resource": [
     "arn:aws:sagemaker:*:*:flow-definition/*"
    ],
    "Condition": {
     "StringEqualsIfExists": {
      "sagemaker:WorkteamType": [
       "private-crowd",
       "vendor-crowd"
      ]
     }
    }
   },
   {
    "Sid": "AllowAWSServiceActions",
    "Effect": "Allow",
    "Action": [
     "sqlworkbench:*",
     "datazone:*",
```

```
    "application-autoscaling:DeleteScalingPolicy",
    "application-autoscaling:DeleteScheduledAction",
    "application-autoscaling:DeregisterScalableTarget",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingActivities",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:DescribeScheduledActions",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling:PutScheduledAction",
    "application-autoscaling:RegisterScalableTarget",
    "aws-marketplace:ViewSubscriptions",
    "cloudformation:GetTemplateSummary",
    "cloudwatch:DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:PutMetricData",
    "codecommit:BatchGetRepositories",
    "codecommit:CreateRepository",
    "codecommit:GetRepository",
    "codecommit:List*",
    "ec2:CreateNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2:DeleteNetworkInterface",
    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeVpcs",
    "ecr:BatchCheckLayerAvailability",
    "ecr:BatchGetImage",
    "ecr:Describe*",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:StartImageScan",
    "elastic-inference:Connect",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
```

```
    "fsx:DescribeFileSystems",
    "groundtruthlabeling:*",
    "iam:GetRole",
    "iam:ListRoles",
    "kms:DescribeKey",
    "kms:ListAliases",
    "lambda:ListFunctions",
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DeleteLogDelivery",
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:UpdateLogDelivery",
    "redshift-data:BatchExecuteStatement",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-serverless:GetCredentials",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
    "secretsmanager:ListSecrets",
    "servicecatalog:Describe*",
    "servicecatalog:List*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProducts",
    "servicecatalog:SearchProvisionedProducts",
    "sns:ListTopics",
    "tag:GetResources"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowRAMInvitation",
```

```
    "Effect": "Allow",
    "Action": "ram:AcceptResourceShareInvitation",
    "Resource": "*",
    "Condition": {
     "StringLike": {
      "ram:ResourceShareName": "dzd_*"
     }
    }
   },
   {
    "Sid": "AllowECRActions",
    "Effect": "Allow",
    "Action": [
     "ecr:SetRepositoryPolicy",
     "ecr:CompleteLayerUpload",
     "ecr:CreateRepository",
     "ecr:BatchDeleteImage",
     "ecr:UploadLayerPart",
     "ecr:DeleteRepositoryPolicy",
     "ecr:InitiateLayerUpload",
     "ecr:DeleteRepository",
     "ecr:PutImage",
     "ecr:TagResource",
     "ecr:UntagResource"
    ],
    "Resource": [
     "arn:aws:ecr:*:*:repository/sagemaker*",
     "arn:aws:ecr:*:*:repository/datazone*"
    ]
   },
   {
    "Sid": "AllowCodeCommitActions",
    "Effect": "Allow",
    "Action": [
     "codecommit:GitPull",
     "codecommit:GitPush"
    ],
    "Resource": [
     "arn:aws:codecommit:*:*:*sagemaker*",
     "arn:aws:codecommit:*:*:*SageMaker*",
     "arn:aws:codecommit:*:*:*Sagemaker*"
    ]
   },
   {
```

```
    "Sid": "AllowCodeBuildActions",
    "Action": [
     "codebuild:BatchGetBuilds",
     "codebuild:StartBuild"
    ],
    "Resource": [
     "arn:aws:codebuild:*:*:project/sagemaker*",
     "arn:aws:codebuild:*:*:build/*"
    ],
    "Effect": "Allow"
   },
   {
    "Sid": "AllowStepFunctionsActions",
    "Action": [
     "states:DescribeExecution",
     "states:GetExecutionHistory",
     "states:StartExecution",
     "states:StopExecution",
     "states:UpdateStateMachine"
    ],
    "Resource": [
     "arn:aws:states:*:*:statemachine:*sagemaker*",
     "arn:aws:states:*:*:execution:*sagemaker*:*"
    ],
    "Effect": "Allow"
   },
   {
    "Sid": "AllowSecretManagerActions",
    "Effect": "Allow",
    "Action": [
     "secretsmanager:DescribeSecret",
     "secretsmanager:GetSecretValue",
     "secretsmanager:CreateSecret",
     "secretsmanager:PutResourcePolicy"
    ],
    "Resource": [
     "arn:aws:secretsmanager:*:*:secret:AmazonSageMaker-*"
    ]
   },
   {
    "Sid": "AllowServiceCatalogProvisionProduct",
    "Effect": "Allow",
    "Action": [
     "servicecatalog:ProvisionProduct"
```

```
    ],
    "Resource": "*"
   },
   {
    "Sid": "AllowServiceCatalogTerminateUpdateProvisionProduct",
    "Effect": "Allow",
    "Action": [
     "servicecatalog:TerminateProvisionedProduct",
     "servicecatalog:UpdateProvisionedProduct"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "servicecatalog:userLevel": "self"
     }
    }
   },
   {
    "Sid": "AllowS3ObjectActions",
    "Effect": "Allow",
    "Action": [
     "s3:AbortMultipartUpload",
     "s3:DeleteObject",
     "s3:DeleteObjectVersion",
     "s3:GetObject",
     "s3:PutObject",
     "s3:PutObjectRetention",
     "s3:ReplicateObject",
     "s3:RestoreObject",
     "s3:GetBucketAcl",
     "s3:PutObjectAcl"
    ],
    "Resource": [
     "arn:aws:s3:::SageMaker-DataZone*",
     "arn:aws:s3:::DataZone-SageMaker*",
     "arn:aws:s3:::Sagemaker-DataZone*",
     "arn:aws:s3:::DataZone-Sagemaker*",
     "arn:aws:s3:::sagemaker-datazone*",
     "arn:aws:s3:::datazone-sagemaker*",
     "arn:aws:s3:::amazon-datazone*"
    ]
   },
   {
    "Sid": "AllowS3GetObjectWithSageMakerExistingObjectTag",
```

```
    "Effect": "Allow",
    "Action": [
     "s3:GetObject"
    ],
    "Resource": [
     "arn:aws:s3:::*"
    ],
    "Condition": {
     "StringEqualsIgnoreCase": {
      "s3:ExistingObjectTag/SageMaker": "true"
     }
    }
   },
   {
    "Sid": "AllowS3GetObjectWithServiceCatalogProvisioningExistingObjectTag",
    "Effect": "Allow",
    "Action": [
     "s3:GetObject"
    ],
    "Resource": [
     "arn:aws:s3:::*"
    ],
    "Condition": {
     "StringEquals": {
      "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
     }
    }
   },
   {
    "Sid": "AllowS3BucketActions",
    "Effect": "Allow",
    "Action": [
     "s3:GetBucketLocation",
     "s3:ListBucket",
     "s3:ListAllMyBuckets",
     "s3:GetBucketCors",
     "s3:PutBucketCors"
    ],
    "Resource": [
     "arn:aws:s3:::SageMaker-DataZone*",
     "arn:aws:s3:::DataZone-SageMaker*",
     "arn:aws:s3:::Sagemaker-DataZone*",
     "arn:aws:s3:::DataZone-Sagemaker*",
     "arn:aws:s3:::sagemaker-datazone*",
```

```
    "arn:aws:s3:::datazone-sagemaker*",
    "arn:aws:s3:::amazon-datazone*"
   ]
  },
  {
   "Sid": "ReadSageMakerJumpstartArtifacts",
   "Effect": "Allow",
   "Action": "s3:GetObject",
   "Resource": [
    "arn:aws:s3:::jumpstart-cache-prod-us-west-2/*",
    "arn:aws:s3:::jumpstart-cache-prod-us-east-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-us-east-2/*",
    "arn:aws:s3:::jumpstart-cache-prod-eu-west-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-eu-central-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-south-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-2/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-northeast-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-1/*",
    "arn:aws:s3:::jumpstart-cache-prod-ap-southeast-2/*"
   ]
  },
  {
   "Sid": "AllowLambdaInvokeFunction",
   "Effect": "Allow",
   "Action": [
    "lambda:InvokeFunction"
   ],
   "Resource": [
    "arn:aws:lambda:*:*:function:*SageMaker*",
    "arn:aws:lambda:*:*:function:*sagemaker*",
    "arn:aws:lambda:*:*:function:*Sagemaker*",
    "arn:aws:lambda:*:*:function:*LabelingFunction*"
   ]
  },
  {
   "Sid": "AllowCreateServiceLinkedRoleForSageMakerApplicationAutoscaling",
   "Action": "iam:CreateServiceLinkedRole",
   "Effect": "Allow",
   "Resource": "arn:aws:iam::*:role/aws-service-role/sagemaker.application-
autoscaling.amazonaws.com/AWSServiceRoleForApplicationAutoScaling_SageMakerEndpoint",
   "Condition": {
    "StringLike": {
     "iam:AWSServiceName": "sagemaker.application-autoscaling.amazonaws.com"
    }
```

```
    }
   },
   {
    "Sid": "AllowSNSActions",
    "Effect": "Allow",
    "Action": [
     "sns:Subscribe",
     "sns:CreateTopic",
     "sns:Publish"
    ],
    "Resource": [
     "arn:aws:sns:*:*:*SageMaker*",
     "arn:aws:sns:*:*:*Sagemaker*",
     "arn:aws:sns:*:*:*sagemaker*"
    ]
   },
   {
    "Sid": "AllowPassRoleForSageMakerRoles",
    "Effect": "Allow",
    "Action": [
     "iam:PassRole"
    ],
    "Resource": [
     "arn:aws:iam::*:role/sm-provisioning/datazone_usr_sagemaker_execution_role_*"
    ],
    "Condition": {
     "StringEquals": {
      "iam:PassedToService": [
       "glue.amazonaws.com",
       "bedrock.amazonaws.com",
       "states.amazonaws.com",
       "lakeformation.amazonaws.com",
       "events.amazonaws.com",
       "sagemaker.amazonaws.com",
       "forecast.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "CrossAccountKmsOperations",
    "Effect": "Allow",
    "Action": [
     "kms:DescribeKey",
```

```
    "kms:Decrypt",
    "kms:ListKeys"
   ],
   "Resource": "*",
   "Condition": {
    "StringNotEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "KmsOperationsWithResourceTag",
   "Effect": "Allow",
   "Action": [
    "kms:DescribeKey",
    "kms:Decrypt",
    "kms:ListKeys",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:RetireGrant"
   ],
   "Resource": "*",
   "Condition": {
    "Null": {
     "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
    }
   }
  },
  {
   "Sid": "AllowAthenaActions",
   "Effect": "Allow",
   "Action": [
    "athena:BatchGetNamedQuery",
    "athena:BatchGetPreparedStatement",
    "athena:BatchGetQueryExecution",
    "athena:CreateNamedQuery",
    "athena:CreateNotebook",
    "athena:CreatePreparedStatement",
    "athena:CreatePresignedNotebookUrl",
    "athena:DeleteNamedQuery",
    "athena:DeleteNotebook",
    "athena:DeletePreparedStatement",
    "athena:ExportNotebook",
    "athena:GetDatabase",
```

```
    "athena:GetDataCatalog",
    "athena:GetNamedQuery",
    "athena:GetPreparedStatement",
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryResultsStream",
    "athena:GetQueryRuntimeStatistics",
    "athena:GetTableMetadata",
    "athena:GetWorkGroup",
    "athena:ImportNotebook",
    "athena:ListDatabases",
    "athena:ListDataCatalogs",
    "athena:ListEngineVersions",
    "athena:ListNamedQueries",
    "athena:ListPreparedStatements",
    "athena:ListQueryExecutions",
    "athena:ListTableMetadata",
    "athena:ListTagsForResource",
    "athena:ListWorkGroups",
    "athena:StartCalculationExecution",
    "athena:StartQueryExecution",
    "athena:StartSession",
    "athena:StopCalculationExecution",
    "athena:StopQueryExecution",
    "athena:TerminateSession",
    "athena:UpdateNamedQuery",
    "athena:UpdateNotebook",
    "athena:UpdateNotebookMetadata",
    "athena:UpdatePreparedStatement"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "AllowGlueCreateDatabase",
   "Effect": "Allow",
   "Action": [
    "glue:CreateDatabase"
   ],
   "Resource": [
    "arn:aws:glue:*:*:catalog",
    "arn:aws:glue:*:*:database/default"
   ]
```

```
  },
  {
   "Sid": "AllowRedshiftGetClusterCredentials",
   "Effect": "Allow",
   "Action": [
    "redshift:GetClusterCredentials"
   ],
   "Resource": [
    "arn:aws:redshift:*:*:dbuser:*/sagemaker_access*",
    "arn:aws:redshift:*:*:dbname:*"
   ]
  },
  {
   "Sid": "AllowListTags",
   "Effect": "Allow",
   "Action": [
    "sagemaker:ListTags"
   ],
   "Resource": [
    "arn:aws:sagemaker:*:*:user-profile/*",
    "arn:aws:sagemaker:*:*:domain/*"
   ]
  },
  {
   "Sid": "AllowCloudformationListStackResources",
   "Effect": "Allow",
   "Action": [
    "cloudformation:ListStackResources"
   ],
   "Resource": "arn:aws:cloudformation:*:*:stack/SC-*"
  },
  {
   "Sid": "AllowGlueActions",
   "Effect": "Allow",
   "Action": [
    "glue:GetColumnStatisticsForPartition",
    "glue:GetColumnStatisticsForTable",
    "glue:ListJobs",
    "glue:CreateSession",
    "glue:RunStatement",
    "glue:BatchCreatePartition",
    "glue:CreatePartitionIndex",
    "glue:CreateTable",
    "glue:BatchGetWorkflows",
```

```
    "glue:BatchUpdatePartition",
    "glue:BatchDeletePartition",
    "glue:GetPartition",
    "glue:GetPartitions",
    "glue:UpdateTable",
    "glue:DeleteTableVersion",
    "glue:DeleteTable",
    "glue:DeleteColumnStatisticsForPartition",
    "glue:DeleteColumnStatisticsForTable",
    "glue:DeletePartitionIndex",
    "glue:UpdateColumnStatisticsForPartition",
    "glue:UpdateColumnStatisticsForTable",
    "glue:BatchDeleteTableVersion",
    "glue:BatchDeleteTable",
    "glue:CreatePartition",
    "glue:DeletePartition",
    "glue:UpdatePartition",
    "glue:CreateBlueprint",
    "glue:CreateJob",
    "glue:CreateConnection",
    "glue:CreateCrawler",
    "glue:CreateDataQualityRuleset",
    "glue:CreateWorkflow",
    "glue:GetDatabases",
    "glue:GetTables",
    "glue:GetTable",
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:ListSchemas",
    "glue:BatchGetJobs",
    "glue:GetConnection",
    "glue:GetDatabase"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "AllowGlueActionsWithEnvironmentTag",
   "Effect": "Allow",
   "Action": [
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:StartBlueprintRun",
```

```
     "glue:PutWorkflowRunProperties",
     "glue:StopCrawler",
     "glue:DeleteJob",
     "glue:DeleteWorkflow",
     "glue:UpdateCrawler",
     "glue:DeleteBlueprint",
     "glue:UpdateWorkflow",
     "glue:StartCrawler",
     "glue:ResetJobBookmark",
     "glue:UpdateJob",
     "glue:StartWorkflowRun",
     "glue:StopCrawlerSchedule",
     "glue:ResumeWorkflowRun",
     "glue:ListSchemas",
     "glue:DeleteCrawler",
     "glue:UpdateBlueprint",
     "glue:BatchStopJobRun",
     "glue:StopWorkflowRun",
     "glue:BatchGetJobs",
     "glue:BatchGetWorkflows",
     "glue:UpdateCrawlerSchedule",
     "glue:DeleteConnection",
     "glue:UpdateConnection",
     "glue:GetConnection",
     "glue:GetDatabase",
     "glue:GetTable",
     "glue:GetPartition",
     "glue:GetPartitions",
     "glue:BatchDeleteConnection",
     "glue:StartCrawlerSchedule",
     "glue:StartJobRun",
     "glue:CreateWorkflow",
     "glue:*DataQuality*"
    ],
    "Resource": "*",
    "Condition": {
     "Null": {
      "aws:ResourceTag/AmazonDataZoneEnvironment": "false"
     }
    }
   },
   {
    "Sid": "AllowGlueDefaultAccess",
    "Effect": "Allow",
```

```
    "Action": [
     "glue:BatchGet*",
     "glue:Get*",
     "glue:SearchTables",
     "glue:List*",
     "glue:RunStatement"
    ],
    "Resource": [
     "arn:aws:glue:*:*:catalog",
     "arn:aws:glue:*:*:database/default",
     "arn:aws:glue:*:*:connection/dz-sm-*",
     "arn:aws:glue:*:*:session/*"
    ]
   },
   {
    "Sid": "AllowRedshiftClusterActions",
    "Effect": "Allow",
    "Action": [
     "redshift:GetClusterCredentialsWithIAM",
     "redshift:DescribeClusters"
    ],
    "Resource": [
     "arn:aws:redshift:*:*:cluster:*",
     "arn:aws:redshift:*:*:dbname:*"
    ]
   },
   {
    "Sid": "AllowCreateClusterUser",
    "Effect": "Allow",
    "Action": [
     "redshift:CreateClusterUser"
    ],
    "Resource": [
     "arn:aws:redshift:*:*:dbuser:*"
    ]
   },
   {
    "Sid": "AllowCreateSecretActions",
    "Effect": "Allow",
    "Action": [
     "secretsmanager:CreateSecret",
     "secretsmanager:TagResource"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:AmazonDataZone-*",
```

```
    "Condition": {
     "StringLike": {
      "aws:ResourceTag/AmazonDataZoneDomain": "dzd_*",
      "aws:RequestTag/AmazonDataZoneDomain": "dzd_*"
     },
     "Null": {
      "aws:TagKeys": "false",
      "aws:ResourceTag/AmazonDataZoneProject": "false",
      "aws:ResourceTag/AmazonDataZoneDomain": "false",
      "aws:RequestTag/AmazonDataZoneDomain": "false",
      "aws:RequestTag/AmazonDataZoneProject": "false"
     },
     "ForAllValues:StringEquals": {
      "aws:TagKeys": [
       "AmazonDataZoneDomain",
       "AmazonDataZoneProject"
      ]
     }
    }
   },
   {
    "Sid": "ForecastOperations",
    "Effect": "Allow",
    "Action": [
     "forecast:CreateExplainabilityExport",
     "forecast:CreateExplainability",
     "forecast:CreateForecastEndpoint",
     "forecast:CreateAutoPredictor",
     "forecast:CreateDatasetImportJob",
     "forecast:CreateDatasetGroup",
     "forecast:CreateDataset",
     "forecast:CreateForecast",
     "forecast:CreateForecastExportJob",
     "forecast:CreatePredictorBacktestExportJob",
     "forecast:CreatePredictor",
     "forecast:DescribeExplainabilityExport",
     "forecast:DescribeExplainability",
     "forecast:DescribeAutoPredictor",
     "forecast:DescribeForecastEndpoint",
     "forecast:DescribeDatasetImportJob",
     "forecast:DescribeDataset",
     "forecast:DescribeForecast",
     "forecast:DescribeForecastExportJob",
     "forecast:DescribePredictorBacktestExportJob",
```

```
    "forecast:GetAccuracyMetrics",
    "forecast:InvokeForecastEndpoint",
    "forecast:GetRecentForecastContext",
    "forecast:DescribePredictor",
    "forecast:TagResource",
    "forecast:DeleteResourceTree"
   ],
   "Resource": [
    "arn:aws:forecast:*:*:*Canvas*"
   ]
  },
  {
   "Sid": "RDSOperation",
   "Effect": "Allow",
   "Action": "rds:DescribeDBInstances",
   "Resource": "*"
  },
  {
   "Sid": "AllowEventBridgeRule",
   "Effect": "Allow",
   "Action": [
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/*",
   "Condition": {
    "StringEquals": {
     "aws:RequestTag/sagemaker:is-canvas-data-prep-job": "true"
    }
   }
  },
  {
   "Sid": "EventBridgeOperations",
   "Effect": "Allow",
   "Action": [
    "events:DescribeRule",
    "events:PutTargets"
   ],
   "Resource": "arn:aws:events:*:*:rule/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceTag/sagemaker:is-canvas-data-prep-job": "true"
    }
   }
  },
```

```
{
 "Sid": "EventBridgeTagBasedOperations",
 "Effect": "Allow",
 "Action": [
  "events:TagResource"
 ],
 "Resource": "arn:aws:events:*:*:rule/*",
 "Condition": {
  "StringEquals": {
   "aws:RequestTag/sagemaker:is-canvas-data-prep-job": "true",
   "aws:ResourceTag/sagemaker:is-canvas-data-prep-job": "true"
  }
 }
},
{
 "Sid": "EventBridgeListTagOperation",
 "Effect": "Allow",
 "Action": "events:ListTagsForResource",
 "Resource": "*"
},
{
 "Sid": "AllowEMR",
 "Effect": "Allow",
 "Action": [
  "elasticmapreduce:DescribeCluster",
  "elasticmapreduce:ListInstanceGroups",
  "elasticmapreduce:ListClusters"
 ],
 "Resource": "*"
},
{
 "Sid": "AllowSSOAction",
 "Effect": "Allow",
 "Action": [
  "sso:CreateApplicationAssignment",
  "sso:AssociateProfile"
 ],
 "Resource": "*"
},
{
 "Sid": "DenyNotAction",
 "Effect": "Deny",
 "NotAction": [
  "sagemaker:*",
```

```
    "sagemaker-geospatial:*",
    "sqlworkbench:*",
    "datazone:*",
    "forecast:*",
    "application-autoscaling:DeleteScalingPolicy",
    "application-autoscaling:DeleteScheduledAction",
    "application-autoscaling:DeregisterScalableTarget",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingActivities",
    "application-autoscaling:DescribeScalingPolicies",
    "application-autoscaling:DescribeScheduledActions",
    "application-autoscaling:PutScalingPolicy",
    "application-autoscaling:PutScheduledAction",
    "application-autoscaling:RegisterScalableTarget",
    "athena:BatchGetNamedQuery",
    "athena:BatchGetPreparedStatement",
    "athena:BatchGetQueryExecution",
    "athena:CreateNamedQuery",
    "athena:CreateNotebook",
    "athena:CreatePreparedStatement",
    "athena:CreatePresignedNotebookUrl",
    "athena:DeleteNamedQuery",
    "athena:DeleteNotebook",
    "athena:DeletePreparedStatement",
    "athena:ExportNotebook",
    "athena:GetDatabase",
    "athena:GetDataCatalog",
    "athena:GetNamedQuery",
    "athena:GetPreparedStatement",
    "athena:GetQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryResultsStream",
    "athena:GetQueryRuntimeStatistics",
    "athena:GetTableMetadata",
    "athena:GetWorkGroup",
    "athena:ImportNotebook",
    "athena:ListDatabases",
    "athena:ListDataCatalogs",
    "athena:ListEngineVersions",
    "athena:ListNamedQueries",
    "athena:ListPreparedStatements",
    "athena:ListQueryExecutions",
    "athena:ListTableMetadata",
    "athena:ListTagsForResource",
```

```
    "athena:ListWorkGroups",
    "athena:StartCalculationExecution",
    "athena:StartQueryExecution",
    "athena:StartSession",
    "athena:StopCalculationExecution",
    "athena:StopQueryExecution",
    "athena:TerminateSession",
    "athena:UpdateNamedQuery",
    "athena:UpdateNotebook",
    "athena:UpdateNotebookMetadata",
    "athena:UpdatePreparedStatement",
    "aws-marketplace:ViewSubscriptions",
    "cloudformation:GetTemplateSummary",
    "cloudformation:ListStackResources",
    "cloudwatch:DeleteAlarms",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch:ListMetrics",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:PutMetricData",
    "codebuild:BatchGetBuilds",
    "codebuild:StartBuild",
    "codecommit:BatchGetRepositories",
    "codecommit:CreateRepository",
    "codecommit:GetRepository",
    "codecommit:List*",
    "codecommit:GitPull",
    "codecommit:GitPush",
    "ec2:CreateNetworkInterface",
    "ec2:CreateNetworkInterfacePermission",
    "ec2:DeleteNetworkInterface",
    "ec2:DeleteNetworkInterfacePermission",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeVpcs",
    "ecr:BatchCheckLayerAvailability",
    "ecr:BatchGetImage",
    "ecr:CreateRepository",
```

```
    "ecr:Describe*",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:SetRepositoryPolicy",
    "ecr:CompleteLayerUpload",
    "ecr:BatchDeleteImage",
    "ecr:UploadLayerPart",
    "ecr:DeleteRepositoryPolicy",
    "ecr:InitiateLayerUpload",
    "ecr:DeleteRepository",
    "ecr:PutImage",
    "ecr:StartImageScan",
    "ecr:TagResource",
    "ecr:UntagResource",
    "elastic-inference:Connect",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeMountTargets",
    "elasticmapreduce:DescribeCluster",
    "elasticmapreduce:ListInstanceGroups",
    "elasticmapreduce:ListClusters",
    "events:PutRule",
    "events:DescribeRule",
    "events:PutTargets",
    "events:TagResource",
    "events:ListTagsForResource",
    "fsx:DescribeFileSystems",
    "glue:SearchTables",
    "glue:NotifyEvent",
    "glue:StartBlueprintRun",
    "glue:PutWorkflowRunProperties",
    "glue:StopCrawler",
    "glue:DeleteJob",
    "glue:DeleteWorkflow",
    "glue:UpdateCrawler",
    "glue:DeleteBlueprint",
    "glue:UpdateWorkflow",
    "glue:StartCrawler",
    "glue:ResetJobBookmark",
    "glue:UpdateJob",
    "glue:StartWorkflowRun",
    "glue:StopCrawlerSchedule",
    "glue:ResumeWorkflowRun",
    "glue:DeleteCrawler",
    "glue:UpdateBlueprint",
```

```
    "glue:BatchStopJobRun",
    "glue:StopWorkflowRun",
    "glue:BatchGet*",
    "glue:UpdateCrawlerSchedule",
    "glue:DeleteConnection",
    "glue:UpdateConnection",
    "glue:Get*",
    "glue:BatchDeleteConnection",
    "glue:StartCrawlerSchedule",
    "glue:StartJobRun",
    "glue:CreateWorkflow",
    "glue:*DataQuality*",
    "glue:List*",
    "glue:CreateSession",
    "glue:RunStatement",
    "glue:BatchCreatePartition",
    "glue:CreateDatabase",
    "glue:CreatePartitionIndex",
    "glue:CreateTable",
    "glue:BatchUpdatePartition",
    "glue:BatchDeletePartition",
    "glue:UpdateTable",
    "glue:DeleteTableVersion",
    "glue:DeleteTable",
    "glue:DeleteColumnStatisticsForPartition",
    "glue:DeleteColumnStatisticsForTable",
    "glue:DeletePartitionIndex",
    "glue:UpdateColumnStatisticsForPartition",
    "glue:UpdateColumnStatisticsForTable",
    "glue:BatchDeleteTableVersion",
    "glue:BatchDeleteTable",
    "glue:CreatePartition",
    "glue:DeletePartition",
    "glue:UpdatePartition",
    "glue:CreateBlueprint",
    "glue:CreateJob",
    "glue:CreateConnection",
    "glue:CreateCrawler",
    "groundtruthlabeling:*",
    "iam:CreateServiceLinkedRole",
    "iam:GetRole",
    "iam:ListRoles",
    "iam:PassRole",
    "kms:DescribeKey",
```

```
    "kms:ListAliases",
    "kms:Decrypt",
    "kms:ListKeys",
    "kms:Encrypt",
    "kms:GenerateDataKey",
    "kms:RetireGrant",
    "lakeformation:GetDataAccess",
    "lambda:ListFunctions",
    "lambda:InvokeFunction",
    "logs:CreateLogDelivery",
    "logs:CreateLogGroup",
    "logs:CreateLogStream",
    "logs:DeleteLogDelivery",
    "logs:Describe*",
    "logs:GetLogDelivery",
    "logs:GetLogEvents",
    "logs:ListLogDeliveries",
    "logs:PutLogEvents",
    "logs:UpdateLogDelivery",
    "ram:AcceptResourceShareInvitation",
    "rds:DescribeDBInstances",
    "redshift:CreateClusterUser",
    "redshift:GetClusterCredentials",
    "redshift:GetClusterCredentialsWithIAM",
    "redshift:DescribeClusters",
    "redshift-data:BatchExecuteStatement",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:DescribeTable",
    "redshift-data:ExecuteStatement",
    "redshift-data:GetStatementResult",
    "redshift-data:ListSchemas",
    "redshift-data:ListTables",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
    "redshift-serverless:GetNamespace",
    "redshift-serverless:GetWorkgroup",
    "redshift-serverless:GetCredentials",
    "s3:GetBucketAcl",
    "s3:PutObjectAcl",
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject",
    "s3:AbortMultipartUpload",
```

```
    "s3:CreateBucket",
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketCors",
    "s3:PutBucketCors",
    "s3:DeleteObjectVersion",
    "s3:PutObjectRetention",
    "s3:ReplicateObject",
    "s3:RestoreObject",
    "secretsmanager:ListSecrets",
    "secretsmanager:DescribeSecret",
    "secretsmanager:GetSecretValue",
    "secretsmanager:CreateSecret",
    "secretsmanager:PutResourcePolicy",
    "secretsmanager:TagResource",
    "servicecatalog:Describe*",
    "servicecatalog:List*",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProducts",
    "servicecatalog:SearchProvisionedProducts",
    "servicecatalog:ProvisionProduct",
    "servicecatalog:TerminateProvisionedProduct",
    "servicecatalog:UpdateProvisionedProduct",
    "sns:ListTopics",
    "sns:Subscribe",
    "sns:CreateTopic",
    "sns:Publish",
    "states:DescribeExecution",
    "states:GetExecutionHistory",
    "states:StartExecution",
    "states:StopExecution",
    "states:UpdateStateMachine",
    "tag:GetResources",
    "sso:CreateApplicationAssignment",
    "sso:AssociateProfile"
   ],
   "Resource": "*"
  }
 ]
}
```

Amazon DataZone 更新受 AWS 管政策

檢視有關 Amazon AWS 受管政策更新的詳細資訊， DataZone 因為此服務開始追蹤這些變更。如需有關此頁面變更的自動警示，請訂閱 Amazon DataZone 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary -新的權限邊界	新的權限邊界稱為AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary。當您透過 Amazon DataZone 資料入口網站建立 Amazon SageMaker 環境時，Amazon 會將此許可界限 DataZone 套用至在建立環境期間產生的 IAM 角色。許可界限會限制 Amazon DataZone 建立的角色和您新增的任何角色的範圍。	2024年4月30日
AmazonDataZoneSageMakerAccess -新政策	名為的新政策授AmazonDataZoneSageMakerAccess予 Amazon DataZone 許可，將 Amazon SageMaker 資產發佈到目錄。它還授予 Amazon DataZone 許可，以授予對目錄中 Amazon SageMaker 已發佈資產的存取權或撤銷存取權。	2024年4月30日
AmazonDataZoneFullAccess -政策更新	AmazonDataZoneFullAccess政策的更新，可新增對`DescribeSecurityGroups` 動作的存取權，以改善帳戶管理員在主控台中設定藍圖的可用性，以及協助擷取有關指定受管理策略之資	2024年4月30日

變更	描述	日期
	訊的GetPolicy 動作的可用性。	
AmazonDataZoneSageMakerProvisioning -新政策	稱為新政策AmazonDataZoneSageMakerProvisioning授予 Amazon 與 Amazon SageMaker 互操作所需 DataZone 的許可。	2024年4月30日
AmazonDataZoneS3 管理 <region>--<domainId>-新角色	稱為 AmazonDataZoneS3Manage-的新角色- <region><domainId>當 Amazon DataZone 調用 AWS Lake Formation 註冊 Amazon Simple Storage Service (Amazon S3) 位置時使用。AWS 在訪問該位置的數據時，Lake Formation 承擔了這個角色。	2024年4月1日
AmazonDataZoneGlueManageAccessRolePolicy -政策更新	已更新，AmazonDataZoneGlueManageAccessRolePolicy以啟用對允許 Amazon DataZone 啟用資料發佈和存取授權的許可支援。	2024年4月1日
AmazonDataZoneDomainExecutionRolePolicy 和 AmazonDataZoneFullUserAccess -政策更新	已更新AmazonDataZoneDomainExecutionRolePolicy和AmazonDataZoneFullUserAccess以啟用 CancelMetadataGenerationRun API 的支援。	2024年3月29 日

變更	描述	日期
AmazonDataZoneFullAccess - 政策更新	已更新，`AmazonDataZoneFullAccess` 讓使用者能夠在 Amazon DataZone 管理主控台中選擇其密碼、叢集、vpc 和子網路，而不是在文字方塊中輸入。	2024年3月13日
AmazonDataZoneDomainExecutionRolePolicy -政策更新	已更新，藉由識別在哪個帳戶和區域中啟用了哪些藍圖，以啟用建立環境設定檔所需 `ListEnvironmentBlueprintConfigurationSummaries` API 的支援。AmazonDataZoneDomainExecutionRolePolicy	2024年2月01 日
AmazonDataZoneGlueManageAccessRolePolicy -政策更新	更新了AmazonDataZoneGlueManageAccessRolePolicy以啟用對 AWS Lake Formation 型混合模式的支援。	2023 年 12 月 14 日
AmazonDataZoneFullUserAccess 和 AmazonDataZoneDomainExecutionRolePolicy -政策更新	更新了AmazonDataZoneFullUserAccess和AmazonDataZoneDomainExecutionRolePolicy政策，以支援 Amazon DataZone 中採用人工智慧技術的生成式資料描述功能。	2023 年 11 月 28 日

變更	描述	日期
AmazonDataZoneEnvironmentRolePermissionsBoundary -政策更新	Amazon DataZone 對AmazonDataZoneEnvironmentRolePermissionsBoundary受管政策進行了更新，該政策包含根據條件範圍縮小的額外athena:GetQueryResultsStream 許可。ResourceTag	2023 年 11 月 17 日
AmazonDataZoneRedshiftManageAccessRolePolicy -政策更新	Amazon AmazonDataZoneRedshiftManageAccessRolePolicy通過刪除對redshift:AssociateDataShareConsumer 動作的組織 ID 檢查來 DataZone 更新了。這可讓您跨 AWS 組織共用資源。	2023 年 11 月 16 日
AmazonDataZoneFullUserAccess -政策更新	Amazon DataZone 更新了授予對 Amazon 完全訪問權限的AmazonDataZoneFullUserAccess政策 DataZone，但不允許管理域，用戶或關聯帳戶。	2023年10月02 日
AmazonDataZonePortalFullAccessPolicy -政策已棄用	Amazon DataZone 棄用了 AmazonDataZonePortalFullAccessPolicy.	2023 年 9 月 29 日
AmazonDataZonePreviewConsoleFullAccess -政策已棄用	Amazon DataZone 棄用了 AmazonDataZonePreviewConsoleFullAccess.	2023 年 9 月 29 日

變更	描述	日期
AmazonDataZoneDomainExecutionRolePolicy -新政策	Amazon DataZone 增加了一個名為的新政策AmazonDataZoneDomainExecutionRolePolicy。 這是 Amazon DataZone `AmazonDataZoneDomainExecutionRole` 服務角色的預設政策。Amazon 使用此角色 DataZone 來編目、探索、管理、共用和分析 Amazon DataZone 網域中的資料。 您可以將`AmazonDataZoneDomainExecutionRolePolicy` 政策附加到您的`AmazonDataZoneDomainExecutionRole` .	2023 年 9 月 25 日
AmazonDataZoneCrossAccountAdmin -新政策	Amazon DataZone 添加了一個名為AmazonDataZoneCrossAccountAdmin的新政策，使用戶能夠使用 Amazon DataZone 及其關聯帳戶。	2023 年 9 月 19 日
AmazonDataZoneFullUserAccess -新政策	Amazon DataZone 添加了一項名AmazonDataZoneFullUserAccess為授予對 Amazon 的完全訪問權限的新政策 DataZone，但不允許管理域，用戶或關聯帳戶。	2023 年 9 月 12 日

變更	描述	日期
AmazonDataZoneRedshiftManageAccessRolePolicy - 新政策	Amazon DataZone 添加了一項名為授予許AmazonDataZoneRedshiftManageAccessRolePolicy可的新政策，以允許 Amazon 啟 DataZone 用對數據的發布和訪問授予。	2023 年 9 月 12 日
AmazonDataZoneGlueManageAccessRolePolicy -新政策	Amazon DataZone 添加了一個名為的新政策，AmazonDataZoneGlueManageAccessRolePolicy該政策授 DataZone 予 Amazon 許可以將 AWS Glue 數據發佈到目錄。它還授予 Amazon DataZone 許可，以授予目錄中 AWS Glue 已發佈資產的存取權或撤銷存取權限。	2023 年 9 月 12 日
AmazonDataZoneRedshiftGlueProvisioningPolicy -新政策	Amazon 新 DataZone 增了一項名為的新政策，AmazonDataZoneRedshiftGlueProvisioningPolicy該政策授予 Amazon DataZone 與支援的資料來源互操作所需的許可。	2023 年 9 月 12 日
AmazonDataZoneEnvironmentRolePermissionsBoundary -新政策	Amazon 新 DataZone 增了一項名為的新政策，AmazonDataZoneEnvironmentRolePermissionsBoundary該政策會限制其所附加的已佈建 IAM 主體。	2023 年 9 月 12 日

變更	描述	日期
AmazonDataZoneFullAccess - 新政策	Amazon DataZone 添加了一個名為的新政策 AmazonDataZoneFullAccess，可 DataZone 通過 AWS 管理控制台對 Amazon 的完全訪問。	2023 年 9 月 12 日
受管政策更新	包含其他`iam:GetPolicy` 權限的AmazonDataZonePreviewConsoleFullAccess受管理策略的更新。	2023 年 6 月 13 日
Amazon DataZone 開始跟踪變化	Amazon DataZone 開始追蹤其 AWS 受管政策的變更。	2023 年 3 月 20 日

Amazon 的 IAM 角色 DataZone

主題

- AmazonDataZoneProvisioningRole-<domainAccountId>
- AmazonDataZoneDomainExecutionRole
- AmazonDataZoneGlueAccess-<region>-<domainId>
- AmazonDataZoneRedshiftAccess-<region>-<domainId>
- AmazonDataZone<region>S3 管理--<domainId>
- AmazonDataZoneSageMakerManageAccessRole-<region>-<domainId>
- AmazonDataZoneSageMakerProvisioningRole-<domainAccountId>

AmazonDataZoneProvisioningRole-<domainAccountId>

具`AmazonDataZoneProvisioningRole-<domainAccountId>`有`AmazonDataZoneRedshiftGlueProvisioningPolicy`附件。此角色授予亞馬遜 DataZone 與 AWS Glue 和 Amazon 紅移互操作所需的許可。

預設值`AmazonDataZoneProvisioningRole-<domainAccountId>`已附加下列信任原則：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

AmazonDataZoneDomainExecutionRole

AmazonDataZoneDomainExecutionRole已AmazonDataZoneDomainExecutionRolePolicy附加受 AWS 管理策略。Amazon 代表您為您 DataZone 創建這個角色。對於資料入口網站中的某些動作，Amazon 會在建立角色的帳戶中 DataZone 擔任此角色，並檢查此角色是否已獲授權執行動作。

該AmazonDataZoneDomainExecutionRole角色在託管您的 Amazon DataZone 域中是必需的。 AWS 帳戶 當您建立 Amazon DataZone 網域時，系統會自動為您建立此角色。

預設AmazonDataZoneDomainExecutionRole角色具有下列信任原則。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "datazone.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:TagSession"
            ],
```

```
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{{source_account_id}}"
                },
                "ForAllValues:StringLike": {
                    "aws:TagKeys": [
                        "datazone*"
                    ]
                }
            }
        }
    ]
}
```

AmazonDataZoneGlueAccess-<region>-<domainId>

`AmazonDataZoneGlueAccess-<region>-<domainId>`角色已`AmazonDataZoneGlueManageAccessRolePolicy`附加。此角色授與 Amazon DataZone 許可，將 AWS Glue 資料發佈到目錄。它還授予 Amazon DataZone 許可，以授予目錄中 AWS Glue 已發佈資產的存取權或撤銷存取權限。

預設`AmazonDataZoneGlueAccess-<region>-<domainId>`角色已附加下列信任原則：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "{{domain_account}}"
            },
            "ArnEquals": {
                "aws:SourceArn": "arn:aws:datazone:{{region}}:
{{domain_account}}:domain/{{root_domain_id}}"
            }
        }
```

```
    }
  ]
}
```

AmazonDataZoneRedshiftAccess-<region>-<domainId>

AmazonDataZoneRedshiftAccess-<region>-<domainId>角色已AmazonDataZoneRedshiftManageAccessRolePolicy附加。此角色授予 Amazon DataZone 許可，將 Amazon Redshift 數據發佈到目錄。它還授予 Amazon DataZone 許可，以授予目錄中亞馬遜 Redshift 或 Amazon Redshift 無伺服器已發佈資產的存取權限或撤銷存取權。

預設AmazonDataZoneRedshiftAccess-<region>-<domainId>角色已附加下列內嵌權限原則：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

預設值AmazonDataZoneRedshiftManageAccessRole<timestamp>已附加下列信任原則：

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

```
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "{{domain_account}}"
            },
            "ArnEquals": {
                "aws:SourceArn": "arn:aws:datazone:{{region}}:
{{domain_account}}:domain/{{root_domain_id}}"
            }
        }
    }
  ]
}
```

AmazonDataZone<region>S3 管理--<domainId>

<region><domainId>當 Amazon DataZone 呼叫 AWS Lake Formation 註冊 Amazon 簡單存儲服務（亞馬遜 S3）位置時使用 AmazonDataZone S3 管理-。 AWS 在訪問該位置的數據時，Lake Formation 承擔了這個角色。如需詳細資訊，請參閱用於註冊位置的角色需求。

此角色已附加下列內嵌權限原則。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
```

```
            }
        },
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3ListBucket",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3ListAllMyBuckets",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "arn:aws:s3:::*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        },
        {
            "Sid": "LakeFormationExplicitDenyPermissionsForS3",
            "Effect": "Deny",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::[[BucketNames]]/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
```

```
        },
        {
            "Sid": "LakeFormationExplicitDenyPermissionsForS3ListBucket",
            "Effect": "Deny",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::[[BucketNames]]"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "{{accountId}}"
                }
            }
        }
    ]
}
```

AmazonDataZoneS3 管理 <region>-附加<domainId>了以下信任策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TrustLakeFormationForDataLocationRegistration",
            "Effect": "Allow",
            "Principal": {
                "Service": "lakeformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{{source_account_id}}"
                }
            }
        }
    ]
}
```

AmazonDataZoneSageMakerManageAccessRole-<region>-<domainId>

AmazonDataZoneSageMakerManageAccessRole角色具有AmazonDataZoneSageMakerAccessAmazonDataZoneRedshiftManageAccessRolePolicy、和AmazonDataZoneGlueManageAccessRolePolicy附加的。此角色授予 Amazon DataZone 許可，以發佈和管理資料湖、資料倉儲和 Amazon Sageemaker 資產的訂閱。

此AmazonDataZoneSageMakerManageAccessRole角色已附加下列內嵌原則：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "RedshiftSecretStatement",
         "Effect":"Allow",
         "Action":"secretsmanager:GetSecretValue",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "secretsmanager:ResourceTag/AmazonDataZoneDomain":"{{domainId}}"
            }
         }
      }
   ]
}
```

此AmazonDataZoneSageMakerManageAccessRole角色已附加下列信任原則：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DatazoneTrustPolicyStatement",
      "Effect": "Allow",
      "Principal": {
        "Service":  ["datazone.amazonaws.com",
                    "sagemaker.amazonaws.com"]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```

```
            "StringEquals": {
                "aws:SourceAccount": "{{domain_account}}"
            },
            "ArnEquals": {
                "aws:SourceArn": "arn:aws:datazone:{{region}}:
{{domain_account}}:domain/{{root_domain_id}}"
            }
        }
    }
]
}
```

AmazonDataZoneSageMakerProvisioningRole-<domainAccountId>

AmazonDataZoneSageMakerProvisioningRole角色具有AmazonDataZoneSageMakerProvisioning和AmazonDataZoneRedshiftGlueProvisioningPoli加的。此角色授予與 AWS Glue、Amazon Amazon Redshift Sageemaker 互操作所需的 Amazon DataZone 許可。

此AmazonDataZoneSageMakerProvisioningRole角色已附加下列內嵌原則：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SageMakerStudioTagOnCreate",
            "Effect": "Allow",
            "Action": [
                "sagemaker:AddTags"
            ],
            "Resource": "arn:aws:sagemaker:*:{{AccountId}}:*/*",
            "Condition": {
                "Null": {
                    "sagemaker:TaggingAction": "false"
                }
            }
        }
    ]
}
```

此AmazonDataZoneSageMakerProvisioningRole角色已附加下列信任原則：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DataZoneTrustPolicyStatement",
      "Effect": "Allow",
      "Principal": {
        "Service": "datazone.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "{{domain_account}}"
        }
      }
    }
  ]
}
```

以身分為基礎的角色

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

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。

當您在入口網站中建立 Amazon DataZone 專案時，會為此專案建立三個 IAM 角色，每個專案成員角色類型各一個：擁有者和參與者。附加至每個角色的權限範圍為專案角色，而附加的權限原則則取決於部署專案時使用的功能。

為了 DataZone 讓 Amazon 能夠管理許可並與訂閱者專案共用資產，訂閱者專案使用者角色會自動新增為發佈資產 AWS Lake Formation 的資料湖管理員。 AWS 帳戶

您可以在 AWS IAM 管理主控台中檢視最多 up-to-date 版本的角色，或檢閱下表中的不同角色許可。

專案擁有者權限

環境類型	IAM 許可
預設資料湖	這是基本、資料湖生產者和資料湖消費者功能的組合。
主要	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:List*", "s3:Get*", "s3:Describe*", "s3:DeleteObjectVersion", "s3:RestoreObject", "s3:ReplicateObject", "s3:PutObject", "s3:AbortMultipartUpload", "s3:PutObjectRetention", "s3:DeleteObject"], "Resource": ["s3BucketArn", "s3BucketArn/*"] }, { "Action": ["s3:List*"], "Resource": "*", "Effect": "Allow" }, { "Action": ["kms:List*",

環境類型	IAM 許可	
	"kms:Get*", "kms:Desc ribe*", "kms:Decrypt", "kms:Encrypt", "kms:ReEn crypt*", "kms:Verify", "kms:Sign", "kms:Gene rateDataKey"], "Resource": "keyArn", "Effect": "Allow" }, { "Action": ["kms:ListKeys", "kms:ListAliases"], "Resource": "*", "Effect": "Allow" }, { "Action": ["ec2:Desc ribeSecurityGroups", "ec2:Desc ribeSecurityGroupR ules", "ec2:Desc ribeTags"], "Resource": "*", "Effect": "Allow" }, { "Action": ["logs:Des cribe*", "logs:Sta rtQuery",	

環境類型	IAM 許可	
	"logs:StopQuery", "logs:Get*", "logs:List*", "logs:PutLogEvents", "logs:CreateLogStream", "logs:FilterLogEvents"], "Resource": "arn:aws:logs:region:account-id:log-group:log-group-name:*", "Effect": "Allow" }, { "Effect": "Allow", "Action": ["s3:Get*", "s3:List*", "kms:List*", "kms:Get*", "kms:Describe*", "kms:Decrypt"], "Resource": "*", "Condition": { "StringNotEquals": { "aws:ResourceAccount": "project-account-id" } } }] }	

環境類型	IAM 許可	

環境類型	IAM 許可	
資料湖生產者	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["glue:BatchGet*", "glue:Get*", "glue:SearchTables", "glue:List*", "glue:BatchCreateP artition", "glue:CreatePartit ionIndex", "glue:CreateTable", "glue:BatchUpdateP artition", "glue:BatchDeleteP artition", "glue:UpdateTable", "glue:DeleteTableV ersion", "glue:DeleteTable", "glue:DeleteColumn	

環境類型	IAM 許可	

```
StatisticsForParti
tion",

 "glue:DeleteColumn
StatisticsForTable",

 "glue:DeletePartit
ionIndex",

 "glue:UpdateColumn
StatisticsForParti
tion",

 "glue:UpdateColumn
StatisticsForTable",

 "glue:BatchDeleteT
ableVersion",

 "glue:BatchDeleteT
able",

 "glue:CreatePartit
ion",

 "glue:DeletePartit
ion",

 "glue:UpdatePartit
ion"
            ],
            "Resource":
 [

 "arn:aws:glue:regi
on:account:database/
dbName",

 "arn:aws:glue:regi
on:account:catalog",

 "arn:aws:glue:regi
```

環境類型	IAM 許可	

```
on:account:table/d
bName/*"
            ]
        },
        {
            "Sid":
 "VisualEditor0",
            "Effect":
 "Allow",
            "Action": [

 "glue:SearchTables",

 "glue:NotifyEvent",

 "glue:StartBluepri
ntRun",

 "glue:PutWorkflowR
unProperties",

 "glue:StopCrawler",

 "glue:DeleteJob",

 "glue:DeleteWorkfl
ow",

 "glue:UpdateCrawler",

 "glue:DeleteBluepr
int",

 "glue:UpdateWorkfl
ow",

 "glue:StartCrawler",

 "glue:ResetJobBook
mark",

 "glue:UpdateJob",
```

環境類型	IAM 許可	
	"glue:StartWorkflowRun", "glue:StopCrawlerSchedule", "glue:ResumeWorkflowRun", "glue:List*", "glue:DeleteCrawler", "glue:UpdateBlueprint", "glue:BatchStopJobRun", "glue:StopWorkflowRun", "glue:BatchGet*", "glue:UpdateCrawlerSchedule", "glue:DeleteConnection", "glue:UpdateConnection", "glue:Get*", "glue:BatchDeleteConnection", "glue:StartCrawlerSchedule",	

環境類型	IAM 許可	

```
 "glue:StartJobRun",

 "glue:CreateWorkfl
ow",

 "glue:PublishDataQ
uality",

 "glue:*DataQuality*"
            ],
            "Resource":
 "*",
            "Conditio
n": {

 "ForAnyValue:Strin
gEquals": {

 "aws:ResourceTag/n
oah-analytics:proj
ectId": "projectId"
                }
            }
        },
        {
            "Sid":
 "CreateGlueResourc
es",
            "Effect":
 "Allow",
            "Action": [

 "glue:CreateBluepr
int",

 "glue:CreateJob",

 "glue:CreateConnec
tion",

 "glue:CreateCrawler",
```

環境類型	IAM 許可	

```
 "glue:CreateDataQu
alityRuleset"
            ],
            "Resource":
 "*"
        },
        {
            "Sid":
 "VisualEditor0",
            "Effect":
 "Allow",
            "Action": [

 "iam:ListRoles",

 "iam:ListUsers",

 "iam:ListGroups",

 "iam:ListRolePolic
ies",

 "iam:GetRole",

 "iam:GetRolePolicy"
            ],
            "Resource":
 "*"
        }
    ]
}
```

環境類型	IAM 許可	

資料湖消費者	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "athena:TerminateSession",
	  "athena:CreatePreparedStatement",
	  "athena:StopCalculationExecution",
	  "athena:StartQueryExecution",
	  "athena:UpdatePreparedStatement",
	  "athena:BatchGet*",
	  "athena:UpdateNotebook",
	  "athena:DeleteNotebook",
	  "athena:DeletePreparedStatement",
	  "athena:UpdateNotebookMetadata",
	  "athena:DeleteNamedQuery",
	  "athena:Get*",
	  "athena:UpdateNamedQuery",
	  "athena:CreateNamedQuery",	

環境類型	IAM 許可	

```
        "athena:E
xportNotebook",
        "athena:S
topQueryExecution",
        "athena:S
tartCalculationExe
cution",
        "athena:S
tartSession",
        "athena:C
reatePresignedNote
bookUrl",
        "athena:C
reateNotebook",
        "athena:I
mportNotebook"
      ],
      "Resource": [
        "arn:aws:
athena:region:acco
unt-id:workgroup/w
orkGroupName",
        "arn:aws:
athena:region:acco
unt-id:datacatalog/
AwsDataCatalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:L
istWorkGroups",
        "athena:L
istDataCatalogs",
        "athena:List*"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
```

環境類型	IAM 許可	
	"glue:Bat chGet*", "glue:Get*", "glue:Sea rchTables", "glue:List*"], "Resource": ["arn:aws: glue:region:account- id:database/dbName", "arn:aws: glue:region:account- id:catalog", "arn:aws: glue:region:account- id:table/dbName/*"] }] }	

環境類型	IAM 許可	

資料倉儲生產者	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift:GetClusterCredentials",
	        "redshift:JoinGroup",
	        "redshift:CreateClusterUser",
	        "redshift:DescribeClusters"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    },
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift-data:DescribeStatement",
	        "redshift-data:ExecuteStatement"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    }
	  ]
	}	

環境類型	IAM 許可	

環境類型	IAM 許可	

資料倉儲消費者	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow",
	"Action": [
	"redshift:GetClusterCredentials",
	"redshift:JoinGroup",
	"redshift:CreateClusterUser",
	"redshift:DescribeClusters"
	],
	"Resource": [
	"arn:aws:redshift:region:account:dbuser:cluster-identifier/dbUser",
	"arn:aws:redshift:region:account:dbgroup:cluster-identifier/project_owner@projectName",
	"arn:aws:redshift:region:account:dbname:cluster-identifier/*"
	],
	"Condition": {
	"ForAnyValue:StringEquals": {
	"aws:PrincipalTag/RedshiftDbUser": "dbUser"
	}	

環境類型	IAM 許可	

	`}`
	`},`
	`{`
	`"Sid": "VisualEd itor2",`
	`"Effect": "Allow",`
	`"Action": [`
	`"redshift- data:DescribeStat ement",`
	`"redshift- data:ExecuteStatement"`
	`],`
	`"Resource": "arn:aws:redshift: region:account-id: cluster:cluster-id entifier"`
	`}`
	`]`
	`}`	

環境類型	IAM 許可	

Amazon Redshift 查詢編輯器第 2 版	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Action": "redshift:DescribeClusters",
	      "Effect": "Allow",
	      "Resource": "arn:aws:redshift:region:account-id:cluster:*",
	      "Sid": "RedshiftPermissions"
	    },
	    {
	      "Action": "tag:GetResources",
	      "Condition": {
	        "StringEquals": { "aws:CalledViaLast": "sqlworkbench.amazonaws.com" }
	      },
	      "Effect": "Allow",
	      "Resource": "*",
	      "Sid": "ResourceGroupsTaggingPermissions"
	    },
	    {
	      "Action": [
	        "sqlworkbench:DriverExecute",
	        "sqlworkbench:GenerateSession",	

環境類型	IAM 許可	

```
        "sqlworkb
ench:ListConnectio
ns",
        "sqlworkb
ench:ListDatabases",
        "sqlworkb
ench:ListFiles",
        "sqlworkb
ench:ListNotebooks",
        "sqlworkb
ench:ListQueryExec
utionHistory",
        "sqlworkb
ench:ListRedshiftC
lusters",
        "sqlworkb
ench:ListSampleDat
abases",
        "sqlworkb
ench:ListTabs",
        "sqlworkb
ench:ListTaggedRes
ources"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart1"
    },
    {
      "Action":
 "sqlworkbench:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:
sqlworkbench:regio
n:account-id:query/
*",
        "arn:aws:
sqlworkbench:regio
```

環境類型	IAM 許可	
	n:account-id:noteb ook/*", "arn:aws: sqlworkbench:regio n:account-id:conne ction/*", "arn:aws: sqlworkbench:regio n:account-id:chart/ *", "arn:aws: sqlworkbench:regio n:account-id:/*"], "Sid": "AmazonRe dshiftQueryEditorV 2PermissionsPart2" }] }	

專案貢獻者權限

環境類型	IAM 許可	
預設資料湖	這是基本、資料湖生產者和資料湖消費者功能的組合。	
主要	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:List*",	

環境類型	IAM 許可	
	"s3:Get*", "s3:Describe*", "s3:DeleteObjectVersion", "s3:RestoreObject", "s3:ReplicateObject", "s3:PutObject", "s3:AbortMultipartUpload", "s3:PutObjectRetention", "s3:DeleteObject"], "Resource": ["s3BucketArn", "s3BucketArn/*"] }, { "Action": ["s3:List*"], "Resource": "*", "Effect": "Allow" }, { "Action": ["kms:List*", "kms:Get*", "kms:Describe*", "kms:Decrypt", "kms:Encrypt", "kms:ReEncrypt*", "kms:Verify", "kms:Sign", "kms:GenerateDataKey"], "Resource": "keyArn", "Effect": "Allow"	

環境類型	IAM 許可	
	}, { "Action": ["kms:ListKeys", "kms:ListAliases"], "Resource": "*", "Effect": "Allow" }, { "Action": ["ec2:DescribeSecurityGroups", "ec2:DescribeSecurityGroupRules", "ec2:DescribeTags"], "Resource": "*", "Effect": "Allow" }, { "Action": ["logs:Describe*", "logs:StartQuery", "logs:StopQuery", "logs:Get*", "logs:List*", "logs:PutLogEvents", "logs:CreateLogStream", "logs:FilterLogEvents"], "Resource": "arn:aws:logs:region:account-id:log-	

環境類型	IAM 許可	

```
group:log-group-na
me:*",
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
        "kms:List*",
        "kms:Get*",
        "kms:Desc
ribe*",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringNo
tEquals": {
          "aws:Reso
urceAccount":
 "project-account-id"
        }
      }
    }
  ]
}
```

環境類型	IAM 許可	
資料湖生產者	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["glue:BatchGet*", "glue:Get*", "glue:SearchTables", "glue:List*", "glue:BatchCreatePartition", "glue:CreatePartitionIndex", "glue:CreateTable", "glue:BatchUpdatePartition", "glue:BatchDeletePartition", "glue:UpdateTable", "glue:DeleteTableVersion", "glue:DeleteTable", "glue:DeleteColumnStatisticsForPartition", "glue:DeleteColumnStatisticsForTable", "glue:DeletePartitionIndex", "glue:UpdateColumnStatisticsForPartition",	

環境類型	IAM 許可	

```
        "glue:Upd
ateColumnStatistic
sForTable",
        "glue:Bat
chDeleteTableVersi
on",
        "glue:Bat
chDeleteTable",
        "glue:Cre
atePartition",
        "glue:Del
etePartition",
        "glue:Upd
atePartition"
      ],
      "Resource": [
        "arn:aws:
glue:region:accoun
t:database/dbName",
        "arn:aws:
glue:region:accoun
t:catalog",
        "arn:aws:
glue:region:accoun
t:table/dbName/*"
      ]
    },
    {
      "Sid": "VisualEd
itor0",
      "Effect": "Allow",
      "Action": [
        "glue:Sea
rchTables",
        "glue:Not
ifyEvent",
        "glue:Sta
rtBlueprintRun",
        "glue:Put
WorkflowRunPropert
ies",
```

環境類型	IAM 許可	

```
        "glue:Sto
pCrawler",
        "glue:Del
eteJob",
        "glue:Del
eteWorkflow",
        "glue:Upd
ateCrawler",
        "glue:Del
eteBlueprint",
        "glue:Upd
ateWorkflow",
        "glue:Sta
rtCrawler",
        "glue:Res
etJobBookmark",
        "glue:Upd
ateJob",
        "glue:Sta
rtWorkflowRun",
        "glue:Sto
pCrawlerSchedule",
        "glue:Res
umeWorkflowRun",
        "glue:List*",
        "glue:Del
eteCrawler",
        "glue:Upd
ateBlueprint",
        "glue:Bat
chStopJobRun",
        "glue:Sto
pWorkflowRun",
        "glue:Bat
chGet*",
        "glue:Upd
ateCrawlerSchedule",
        "glue:Del
eteConnection",
        "glue:Upd
ateConnection",
        "glue:Get*",
```

環境類型	IAM 許可	

```
        "glue:Bat
chDeleteConnection",
        "glue:Sta
rtCrawlerSchedule",
        "glue:Sta
rtJobRun",
        "glue:Cre
ateWorkflow",
        "glue:Pub
lishDataQuality",
        "glue:*Da
taQuality*"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyVa
lue:StringEquals": {
          "aws:Reso
urceTag/noah-analy
tics:projectId":
 "projectId"
        }
      }
    },
    {
      "Sid": "CreateGl
ueResources",
      "Effect": "Allow",
      "Action": [
        "glue:Cre
ateBlueprint",
        "glue:Cre
ateJob",
        "glue:Cre
ateConnection",
        "glue:Cre
ateCrawler",
        "glue:Cre
ateDataQualityRule
set"
      ],
      "Resource": "*"
```

環境類型	IAM 許可	

```
    },
    {
      "Sid": "VisualEd
itor0",
      "Effect": "Allow",
      "Action": [
        "iam:List
Roles",
        "iam:List
Users",
        "iam:List
Groups",
        "iam:List
RolePolicies",
        "iam:GetRole",
        "iam:GetR
olePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

環境類型	IAM 許可	
資料湖消費者	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["athena:TerminateSession", "athena:CreatePreparedStatement", "athena:StopCalculationExecution", "athena:StartQueryExecution", "athena:UpdatePreparedStatement", "athena:BatchGet*", "athena:UpdateNotebook", "athena:DeleteNotebook", "athena:DeletePreparedStatement", "athena:UpdateNotebookMetadata", "athena:DeleteNamedQuery", "athena:Get*", "athena:UpdateNamedQuery", "athena:CreateNamedQuery",	

環境類型	IAM 許可	

```
        "athena:E
xportNotebook",
        "athena:S
topQueryExecution",
        "athena:S
tartCalculationExe
cution",
        "athena:S
tartSession",
        "athena:C
reatePresignedNote
bookUrl",
        "athena:C
reateNotebook",
        "athena:I
mportNotebook"
      ],
      "Resource": [
        "arn:aws:
athena:region:acco
unt-id:workgroup/w
orkGroupName",
        "arn:aws:
athena:region:acco
unt-id:datacatalog/
AwsDataCatalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:L
istWorkGroups",
        "athena:L
istDataCatalogs",
        "athena:List*"
      ],
      "Resource": ["*"]
    },
    {
      "Effect": "Allow",
      "Action": [
```

環境類型	IAM 許可	
	"glue:Bat chGet*", "glue:Get*", "glue:Sea rchTables", "glue:List*"], "Resource": ["arn:aws: glue:region:account- id:database/dbName", "arn:aws: glue:region:account- id:catalog", "arn:aws: glue:region:account- id:table/dbName/*"] }] }	

環境類型	IAM 許可	

資料倉儲生產者	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift:GetClusterCredentials",
	        "redshift:JoinGroup",
	        "redshift:CreateClusterUser",
	        "redshift:DescribeClusters"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    },
	    {
	      "Effect": "Allow",
	      "Action": [
	        "redshift-data:DescribeStatement",
	        "redshift-data:ExecuteStatement"
	      ],
	      "Resource": "arn:aws:redshift:region:account:cluster:producerRedshiftCluster"
	    }
	  ]
	}	

環境類型	IAM 許可	

環境類型	IAM 許可	

資料倉儲消費者	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow",
	"Action": [
	"redshift:GetClusterCredentials",
	"redshift:JoinGroup",
	"redshift:CreateClusterUser",
	"redshift:DescribeClusters"
	],
	"Resource": [
	"arn:aws:redshift:region:account:dbuser:cluster-identifier/dbUser",
	"arn:aws:redshift:region:account:dbgroup:cluster-identifier/project_owner@projectName",
	"arn:aws:redshift:region:account:dbname:cluster-identifier/*"
	],
	"Condition": {
	"ForAnyValue:StringEquals": {
	"aws:PrincipalTag/RedshiftDbUser": "dbUser"
	}	

環境類型	IAM 許可	
	`} }, { "Sid": "VisualEd itor2", "Effect": "Allow", "Action": [ "redshift- data:DescribeStat ement", "redshift- data:ExecuteStatement" ], "Resource": "arn:aws:redshift: region:account-id: cluster:cluster-id entifier" } ] }`	

環境類型	IAM 許可	

Amazon Redshift 查詢編輯器第 2 版	{
	  "Version": "2012-10-17",
	  "Statement": [
	    {
	      "Action": "redshift:DescribeClusters",
	      "Effect": "Allow",
	      "Resource": "arn:aws:redshift:region:account-id:cluster:*",
	      "Sid": "RedshiftPermissions"
	    },
	    {
	      "Action": "tag:GetResources",
	      "Condition": {
	        "StringEquals": { "aws:CalledViaLast": "sqlworkbench.amazonaws.com" }
	      },
	      "Effect": "Allow",
	      "Resource": "*",
	      "Sid": "ResourceGroupsTaggingPermissions"
	    },
	    {
	      "Action": [
	        "sqlworkbench:DriverExecute",
	        "sqlworkbench:GenerateSession",	

環境類型	IAM 許可	

```
        "sqlworkb
ench:ListConnectio
ns",
        "sqlworkb
ench:ListDatabases",
        "sqlworkb
ench:ListFiles",
        "sqlworkb
ench:ListNotebooks",
        "sqlworkb
ench:ListQueryExec
utionHistory",
        "sqlworkb
ench:ListRedshiftC
lusters",
        "sqlworkb
ench:ListSampleDat
abases",
        "sqlworkb
ench:ListTabs",
        "sqlworkb
ench:ListTaggedRes
ources"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart1"
    },
    {
      "Action":
 "sqlworkbench:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:
sqlworkbench:regio
n:account-id:query/
*",
        "arn:aws:
sqlworkbench:regio
```

環境類型	IAM 許可	

```
n:account-id:noteb
ook/*",
        "arn:aws:
sqlworkbench:regio
n:account-id:conne
ction/*",
        "arn:aws:
sqlworkbench:regio
n:account-id:chart/
*",
        "arn:aws:
sqlworkbench:regio
n:account-id:/*"
      ],
      "Sid": "AmazonRe
dshiftQueryEditorV
2PermissionsPart2"
    }
  ]
}
```

暫時登入資料

當您使用臨時登入資料登入時，某些 AWS 服務無法運作。如需其他資訊，包括哪些 AWS 服務可搭配臨時登入資料使用，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而非使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

主體許可

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。政策能將許可授予主體。當您使用某些服務時，您可能會執行一個動作，然後在不同的服務中觸發另一個動作。在此情況下，您必須具有執行這兩個動作的許可。若要查看動作是否需要原則中的其他相依動作，請參閱服務授權參考中的 AWS 文件基本資訊的動作、資源和條件索引鍵。

Amazon 的合規驗證 DataZone

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。

- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求，例如 PCI DSS，滿足特定合規性架構所規定的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

Amazon 的安全最佳實踐 DataZone

DataZone Amazon 在開發和實作自己的安全政策時，提供許多安全功能供您考慮。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。

實作最低權限存取

授予許可時，您可以決定誰取得哪些 Amazon DataZone 資源的許可。您還需針對這些資源啟用允許執行的動作，因此，您只應授與執行任務所需的許可。對降低錯誤或惡意意圖所引起的安全風險和影響而言，實作最低權限存取是相當重要的一環。

使用 IAM 角色

生產者和用戶端應用程式必須具有有效的登入 DataZone資料才能存取 Amazon 您不應將 AWS 登入資料直接存放在用戶端應用程式或 Amazon S3 儲存貯體中。這些是不會自動輪換的長期憑證，如果遭到盜用，可能會對業務造成嚴重的影響。

相反地，您應該使用 IAM 角色來管理生產者和用戶端應用程式的臨時登入資料，以存取 Amazon DataZone 資源。使用角色時，您不必使用長期登入資料 (例如使用者名稱和密碼或存取金鑰) 來存取其他資源。

如需詳細資訊，請參閱《IAM 使用者指南》中的以下主題：

- IAM 角色
- 常見的角色方案：使用者、應用程式和服務

在相依資源實作伺服器端加密

靜態資料和傳輸中的資料可以在 Amazon 中加密 DataZone。

用 CloudTrail 於監控 API 呼叫

Amazon DataZone 集成了一種服務 AWS CloudTrail，該服務可提供 Amazon 中的用戶，角色或 AWS 服務採取的操作記錄 DataZone。

使用收集的資訊 CloudTrail，您可以判斷向 Amazon 發出的請求 DataZone、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。

Amazon 的韌性 DataZone

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎結構。

除了 AWS 全球基礎設施之外，Amazon 還 DataZone 提供多種功能來協助支援您的資料彈性和備份需求。

主題

- 資料來源彈性
- 資產彈性
- 資產類型和中繼資料表單彈性
- 詞彙彈性
- 全球搜尋彈性
- 訂閱彈性
- 環境韌性
- 環境藍圖恢復力
- 專案韌性
- 記憶體彈性
- 使用者設定檔管理彈
- 網域復原

資料來源彈性

在 Amazon DataZone 可用性事件期間，任DataSource務會定期重試最多 24 小時。如果工作因配置錯誤而失敗，則會發出DataSourceRunFailed事件。如果 Amazon DataZone 網域使用 KMS 金鑰設定，且在任務執行期間 AmazonDataZoneDomainExecutionRole 失去對此金鑰的存取權，則執行將以INACCESSIBLE狀態結束。還原 KMS 存取權後，應手動更新工作以觸發轉換回可用狀態。

資產彈性

在 Amazon 中 DataZone，資產是版本控制的。如果資產的某個版本需要復原，您可以使用上一個穩定版本的內容建立新版本。可以發佈資產版本。除非透過發佈新版本，否則無法編輯資產的已發佈版本。可以訂閱已發布的資產（又名列表）。若要防止對資產進行新訂閱，可以取消發佈該資產。取消發佈資產不會對現有訂閱產生影響。刪除資產會刪除資產的所有未發佈版本。資產的已發佈版本必須個別刪除。只有在沒有訂閱的情況下，才能刪除資產的已發佈版本。

資產類型和中繼資料表單彈性

在 Amazon 中 DataZone，資產類型和中繼資料表單類型是版本控制的。如果資產正在使用某個資產，則無法刪除該資產類型。如果資產類型或資產正在使用中繼資料表單類型，則無法刪除該表單類型。如果您不想將特 metadata-form-type 定內容用於組織，您可以停用它們，這不會影響其已附加的項目。

詞彙彈性

在 Amazon 中 DataZone，詞彙表和詞彙表詞彙如果正在使用中，則無法刪除它們。如果您不想將特定辭彙或詞彙用於組織，您可以停用這些詞彙表或詞彙，而不會影響已附加的詞彙表或詞彙。

全球搜尋彈性

在 Amazon 中 DataZone，可以通過全球搜索發現已發布的資產（又名列表）。您可以透過取消發佈資產來回復資產的發佈。取消發佈資產不會影響現有的訂閱。透過重新發佈該版本，可將已發佈的資產回復為特定版本的資產。這不會影響現有的訂閱。

訂閱彈性

在 Amazon 中 DataZone，訂閱授權出貨將在失敗之前嘗試兩次淘汰。如果失敗，則必須手動刪除才能重試。如果 Amazon DataZone 無法撤銷訂閱的許可，刪除訂閱可能會失敗。應該解決基礎錯誤，或者可以在 DeleteSubscriptionGrant API 操作中使用該retainPermissions標誌來強制從 Amazon 刪除授權， DataZone 而無需撤銷許可。

如果 Amazon DataZone 網域使用 KMS 金鑰設定，且在SubscriptionGrant工作流程期間AmazonDataZoneDomainExecutionRole失去對此金鑰的存取權，則會標記授權INACCESSIBLE。還原 KMS 存取權後，必須刪除並重新建立INACCESSIBLE授權。

環境韌性

如果 Amazon DataZone 網域使用 KMS 金鑰設定，且在環境工作流程期間AmazonDataZoneDomainExecutionRole失去對此金鑰的存取權，則會標記環境INACCESSIBLE。還原 KMS 存取權後，必須刪除並重新建立INACCESSIBLE環境。在失敗之前，環境建立將嘗試兩次淘汰。如果失敗，則必須手動刪除才能重試。如果環境工作流程失敗，環境將進入失敗狀態。此時，它只能被刪除和重新創建。

環境藍圖恢復力

在 Amazon 中 DataZone，如果有任何基礎環境設定檔，則無法刪除環境藍圖。

專案韌性

在 Amazon 中 DataZone，如果有任何包含的環境，則無法刪除項目。

記憶體彈性

如需記憶體恢復能力的資訊，請參閱 security-disaster-recovery-resiliency https://docs.aws.amazon.com/ram/latest/userguide/

使用者設定檔管理彈

如需使用者設定檔恢復性資訊，請參閱AWS 身分識別

網域復原

在 Amazon 中 DataZone，如果網域包含專案或資料來源，則無法刪除該網域。

Amazon 基礎設施安全 DataZone

作為一項受管服務，Amazon DataZone 受到 AWS 全球網路安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫 DataZone 透過網路存取 Amazon。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。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，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

Amazon 的跨服務混淆副預防 DataZone

混淆代理人問題屬於安全性議題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在中 AWS，跨服務模擬可能會導致混淆的副問題。在某個服務 (呼叫服務) 呼叫另一個服務 (被呼叫服務) 時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了防止這種情況發生， AWS 提供的工具可協助您透過已授予您帳戶中資源存取權的服務主體來保護所有服務的資料。

我們建議在資源政策中使用 aws: SourceAccount 全域條件上下文鍵，以限制 Amazon 向資源 DataZone 提供其他服務的許可。使用 aws：SourceAccount 如果您想允許該帳戶中的任何資源與跨服務使用相關聯。

Amazon 的組態和漏洞分析 DataZone

AWS 處理基本安全性工作，例如客體作業系統 (OS) 和資料庫修補、防火牆組態和嚴重損壞修復。這些程序已由適當的第三方進行檢閱並認證。如需詳細資訊，請參閱 AWS 共用的責任模型。

要新增至允許清單的網域

若要讓 Amazon DataZone 資料入口網站存取 Amazon DataZone 服務，您必須將下列網域新增至資料入口網站嘗試存取服務的網路上的允許清單。

- `*.api.aws`
- `*.on.aws`

監控 Amazon DataZone

監控是維護 Amazon DataZone 和其他 AWS 解決方案的可靠性、可用性和效能的重要組成部分。AWS 提供以下監控工具來觀看 Amazon DataZone、在發生錯誤時報告，並在適當時採取自動動作：

- Amazon 會即時 CloudWatch監控您的 AWS 資源和執行 AWS 的應用程式。您可以收集和追蹤指標、建立自訂儀板表，以及設定警示，在特定指標達到您指定的閾值時通知您或採取動作。例如，您可以 CloudWatch 追蹤 Amazon EC2 執行個體的 CPU 使用率或其他指標，並在需要時自動啟動新執行個體。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。
- Amazon CloudWatch 日誌可讓您從 Amazon EC2 執行個體和其他來源監控 CloudTrail、存放和存取日誌檔。 CloudWatch 記錄檔可以監控記錄檔中的資訊，並在符合特定臨界值時通知您。您也可以將日誌資料存檔在高耐用性的儲存空間。如需詳細資訊，請參閱 Amazon CloudWatch 日誌使用者指南。
- Amazon EventBridge 可用於自動化 AWS 服務並自動回應系統事件，例如應用程式可用性問題或資源變更。來自 AWS 服務的事件會以近乎即時 EventBridge 的方式傳送到。您可編寫簡單的規則，來指示您在意的事件，以及當事件符合規則時所要自動執行的動作。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南。
- AWS CloudTrail擷取您帳戶或代表您 AWS 帳戶發出的 API 呼叫和相關事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 位址，以及呼叫發生的時間。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

DataZone 用 Amazon 監控 Amazon CloudWatch

您可以 DataZone 使用 CloudWatch收集原始資料並將其處理為可讀且接近即時的指標來監控 Amazon。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。

Amazon 資 DataZone 料入口網站使用具有 JWT 身份驗證和授權的 Amazon DataZone 資料平面 API。Amazon DataZone 假定 Amazon DataZone 預設服務角色，並將透過 Amazon DataZone 資料入口網站發出的所有 Amazon DataZone API 呼叫記錄在名為 DataZoneDataPortalAPI 的日誌群組中 CallLogs。

在 Amazon 監控 Amazon DataZone 事件 EventBridge

您可以在中監控 Amazon DataZone 事件 EventBridge，從您自己的應用程式、 software-as-a-service (SaaS) 應用程式和 AWS 服務提供即時資料串流。 EventBridge將資料路由到目標，例如 AWS Lambda Amazon 簡單通知服務。這些事件與 Amazon Events 中出現的 CloudWatch 事件相同，可提供描述 AWS 資源變更的近乎即時的系統事件串流。

如需更多詳細資訊，請參閱 通過 Amazon EventBridge 默認總線與事件工作。

使用記錄 Amazon DataZone API 呼叫 AWS CloudTrail

Amazon 集 DataZone 成了一種服務 AWS CloudTrail，該服務可提供 Amazon 中用戶，角色或 AWS 服務採取的操作記錄 DataZone。 CloudTrail 捕獲 Amazon 的所有 API 調用 DataZone 作為事件。擷取的呼叫包括來自 Amazon DataZone 主控台的呼叫，以及對 Amazon DataZone API 操作的程式碼呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail事件到 Amazon S3 儲存貯體，包括 Amazon 的事件 DataZone。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷向 Amazon 發出的請求 DataZone、提出請求的 IP 地址、提出請求的人員、提出請求的時間以及其他詳細資訊。

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

Amazon DataZone 信息 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。在 Amazon DataZone 管理主控台中發生活動時，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。您可以在您的. 中檢視、搜尋和下載最近的活動 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

對於您的事件的持續記錄 AWS 帳戶，包括 Amazon 的事件 DataZone，請創建一個跟踪。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

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

所有 Amazon DataZone 動作都由記錄 CloudTrail。

Amazon 故障 DataZone

如果您在使用 Amazon 時遇到存取遭拒的問題或類似的困難， DataZone請參閱本節中的主題。

Amazon 的 AWS Lake Formation 許可的故障 DataZone

本節包含您可能遇到的問題的疑難排解說明為 Amazon 配置 Lake Formation 許可 DataZone。

資料入口網站中的錯誤訊息	解析度
無法承擔資料存取角色。	當 Amazon DataZone 無法假定您用來DefaultDataLakeBlueprint在帳戶中啟用AmazonDataZoneGlueDataAccessRole的內容時，會顯示此錯誤。若要修正此問題，請前往資料資產所在帳戶中的 AWS IAM 主控台，並確定與 Amazon DataZone 服務主體AmazonDataZoneGlueDataAccessRole具有正確的信任關係。如需更多資訊，請參閱AmazonDataZoneGlueAccess-<region>-<domainId>
資料存取角色沒有讀取您嘗試訂閱之資產中繼資料的必要權限。	當 Amazon DataZone 成功擔任該AmazonDataZoneGlueDataAccessRole角色時，會顯示此錯誤，但該角色沒有必要的許可。若要修正此問題，請前往資料資產所在帳戶中的 AWS IAM 主控台，並確定該角色已AmazonDataZoneGlueManageAccessRolePolicy附加該資產。如需詳細資訊，請參閱 AmazonDataZoneGlueAccess-<region>-<domainId>。
資產是資源連結。Amazon DataZone 不支持訂閱資源鏈接。	當您嘗試發佈到 Amazon DataZone 的資產是指向 AWS Glue 表格的資源連結時，會顯示此錯誤。
資產不由 AWS Lake Formation 管理。	此錯誤表示不會對您要發佈的資產強制執行 AWS Lake Formation 權限。在以下情況下可能會發生這種情況。

資料入口網站中的錯誤訊息	解析度
	• 該資產的 Amazon S3 位置未在 AWS Lake Formation 註冊。若要修正此問題，請在表格所在的帳戶中登入 AWS Lake Formation 主控台，然後以 AWS Lake Formation 模式或混合模式註冊 Amazon S3 位置。如需詳細資訊，請參閱 Registering an Amazon S3 location (註冊 Amazon S3 位置)。有幾種情況需要進一步的修改。其中包括加密的 AmazonS3 儲存貯體或跨帳戶 S3 儲存貯體和 AWS Glue 目錄設定。在這種情況下，可能需要修改 KMS 和/或 S3 設定。如需詳細資訊，請參閱註冊加密的 Amazon S3 位置。 • Amazon S3 位置在 AWS Lake Formation 模式下註冊，但 IAM AllowedPrincipal 會新增至資料表的許可中。若要修正此問題，您可以AllowedPrincipal從資料表的許可中移除 IAM，或以混合模式註冊 S3 位置。如需詳細資訊，請參閱關於升級至 Lake Formation 權限模型。如果您的 S3 位置已加密或 S3 位置與 AWS Glue 表格不同，請依照註冊加密的 Amazon S3 位置中的指示操作。

資料入口網站中的錯誤訊息	解析度
資料存取角色沒有必要的 Lake Formation 權限來授與此資產的存取權。	此錯誤表示AmazonDataZoneGlueDataAccessRole您用來在帳戶DefaultDataLakeBlueprint中啟用的項目沒有 Amazon DataZone 管理已發佈資產許可的必要許可。您可以新增AmazonDataZoneGlueDataAccessRole為 AWS Lake Formation 管理員，或授與您要發佈之資產的下列權限來解決此問題。AmazonDataZoneGlueDataAccessRole • 描述和描述資產所在的資料庫上可授予的權限 • 描述，選擇，描述可授予，選擇可授予的權限，對數據庫中的所有資產，您想要 Amazon DataZone 代表您管理的 acecss 的所有資產。

Amazon 的配額 DataZone

您的 AWS 帳戶有每項 AWS 服務的預設配額 (先前稱為限制)。除非另有說明，否則每個配額都是特定地區的。

Amazon DataZone 具有以下配額和限制。

資源	描述	Value
資料資產類型	可在 DataZone 網域中建立的資料資產類型數目上限	1000
資料資產	可在 Amazon DataZone 網域中建立的資料資產數量上限	100 萬
詞彙表	您可以在網域中建立的企業詞彙表數目上限	1000
商業詞彙	您可以在網域中建立的商業詞彙術語總數上限	10000
網域中的環境	Amazon DataZone 網域中環境的最大數量	500

Amazon DataZone 用戶指南的文檔歷史記錄

下表說明適用於 Amazon 的文件發行版本 DataZone。

變更	描述	日期
AmazonDataZoneSageMakerProvisioning -新政策	稱為新政策AmazonDataZoneSageMakerProvisioning授予 Amazon 與 Amazon SageMaker 互操作所需 DataZone 的許可。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2024 年 4 月 30 日
AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary -新的權限邊界	新的權限邊界稱為AmazonDataZoneSageMakerEnvironmentRolePermissionsBoundary。當您透過 Amazon DataZone 資料入口網站建立 Amazon SageMaker 環境時，Amazon 會將此許可界限 DataZone 套用至在建立環境期間產生的 IAM 角色。許可界限會限制 Amazon DataZone 建立的角色和您新增的任何角色的範圍。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2024 年 4 月 30 日
AmazonDataZoneSageMakerAccess -新政策	稱為新政策授AmazonDataZoneSageMakerAccess予 Amazon DataZone 授予用戶訪問 Amazon SageMaker 環境中各種資源所需的許可。如需詳細資訊，請參閱 Amazon	2024 年 4 月 30 日

	DataZone 更新 AWS 受管政策。	
AmazonDataZoneFullAccess - 政策更新	AmazonDataZoneFull Access政策的更新，可新增對`DescribeSecurityGroups` 動作的存取權，以改善帳戶管理員在主控台中設定藍圖的可用性，以及協助擷取有關指定受管理策略之資訊的`GetPolicy` 動作的可用性。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2024 年 4 月 30 日
AmazonDataZoneS3 管理---新角色 <region><domainId>	稱為 AmazonDataZoneS3Manage-的新角色- <region><domainId>當 Amazon DataZone 調用 AWS Lake Formation 註冊 Amazon Simple Storage Service (Amazon S3) 位置時使用。AWS 在訪問該位置的數據時，Lake Formation 承擔了這個角色。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2024年4月1日
AmazonDataZoneGlue ManageAccessRolePolicy -政策更新	已更新，AmazonDataZoneGlueManageAccessRolePolicy以啟用對允許 Amazon DataZone 啟用資料發佈和存取授權的許可支援。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2024年4月1日

AmazonDataZoneDomainExecutionRolePolicy 和 AmazonDataZoneFullUserAccess -政策更新	已更新AmazonDataZoneDomainExecutionRolePolicy和AmazonDataZoneFullUserAccess以啟用 `CancelMetadataGenerationRun` API 的支援。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2024年3月29 日
AmazonDataZoneFullAccess -政策更新	已更新，`AmazonDataZoneFullAccess` 讓使用者能夠在 Amazon DataZone 管理主控台中選擇其密碼、叢集、vpc 和子網路，而不是在文字方塊中輸入。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2024年3月13日
AmazonDataZoneDomainExecutionRolePolicy -政策更新	已更新，藉由識別在哪個帳戶和區域中啟用了哪些藍圖，以啟用建立環境設定檔所需 ListEnvironmentBlueprintConfigurationSummaries API 的支援。AmazonDataZoneDomainExecutionRolePolicy如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2024年2月1日
AmazonDataZoneGlueManageAccessRolePolicy -政策更新	更新了AmazonDataZoneGlueManageAccessRolePolicy以啟用對 AWS Lake Formation 型混合模式的支援。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2023 年 12 月 14 日

AmazonDataZoneFullUserAccess 和 AmazonDataZoneDomainExecutionRolePolicy -政策更新	Amazon DataZone 更新了AmazonDataZoneFullUserAccess和AmazonDataZoneDomainExecutionRolePolicy政策，以支持 Amazon DataZone 中的生成 AI 驅動的數據描述功能。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2023 年 11 月 28 日
AmazonDataZoneEnvironmentRolePermissionsBoundary -政策更新	Amazon DataZone 對AmazonDataZoneEnvironmentRolePermissionsBoundary受管政策進行了更新，該政策包含根據條件範圍縮小的額外`athena:GetQueryResultsStream` 許可。`ResourceTag` 如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2023 年 11 月 17 日
AmazonDataZoneRedshiftManageAccessRolePolicy -政策更新	Amazon 通過刪除對該操作的組織 ID 檢查來 DataZone 更新了AmazonDataZoneRedshiftManageAccessRolePolicy政`redshift:AssociateDataShareConsumer` 策。這可讓您跨 AWS 組織共用資源。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2023 年 11 月 16 日

AmazonDataZoneFull UserAccess -政策更新	Amazon DataZone 更新了授予 Amazon 完整存取權限的AmazonDataZoneFull UserAccess政策 DataZone，但不允許管理網域、使用者或關聯帳戶。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2023 年 10 月 2 日
AmazonDataZonePrev iewConsoleFullAccess -政策已棄用	Amazon DataZone 棄用了AmazonDataZonePrev iewConsoleFullAccess。有關更多信息，請參閱 Amazon 更 DataZone 新 AWS 受管政策。	2023 年 9 月 29 日
AmazonDataZonePort alFullAccessPolicy -政策已棄用	Amazon DataZone 棄用了AmazonDataZonePort alFullAccessPolicy。有關更多信息，請參閱 Amazon 更 DataZone 新 AWS 受管政策。	2023 年 9 月 29 日

AmazonDataZoneDomainExecutionRolePolicy -新政策	Amazon DataZone 增加了一個名為的新政策AmazonDataZoneDomainExecutionRolePolicy。這是 Amazon DataZone `AmazonDataZoneDomainExecutionRole` 服務角色的預設政策。Amazon 使用此角色 DataZone 來編目、探索、管理、共用和分析 Amazon DataZone 網域中的資料。您可以將`AmazonDataZoneDomainExecutionRolePolicy` 政策附加到您的`AmazonDataZoneDomainExecutionRole` 。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2023 年 9 月 25 日
AmazonDataZoneCrossAccountAdmin -新政策	Amazon DataZone 添加了一個名為AmazonDataZoneCrossAccountAdmin的新政策，使用戶能夠使用 Amazon DataZone 及其關聯帳戶。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2023 年 9 月 19 日

AmazonDataZoneRedshiftManageAccessRolePolicy - 新政策	Amazon DataZone 添加了一項名為授予許AmazonDataZoneRedshiftManageAccessRolePolicy可的新政策，以允許 Amazon 啟 DataZone 用對數據的發布和訪問授予。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2023 年 9 月 12 日
AmazonDataZoneRedshiftGlueProvisioningPolicy -新政策	Amazon 新 DataZone 增了一項名為的新政策，AmazonDataZoneRedshiftGlueProvisioningPolicy該政策授予 Amazon DataZone 與支援的資料來源互操作所需的許可。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2023 年 9 月 12 日
AmazonDataZoneGlueManageAccessRolePolicy -新政策	Amazon DataZone 添加了一個名為AmazonDataZoneGlueManageAccessRolePolicy授予 Amazon DataZone 許可的新政策，以將 AWS Glue 數據發佈到目錄。它還授予 Amazon DataZone 許可，以授予目錄中 AWS Glue 已發佈資產的存取權或撤銷存取權限。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2023 年 9 月 12 日

AmazonDataZoneFullUserAccess -新政策	Amazon DataZone 添加了一個名為的新政策 AmazonDataZoneFullUserAccess，DataZone 通過數據門戶授予對 Amazon 的完全訪問權限。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2023 年 9 月 12 日
AmazonDataZoneFullAccess -新政策	Amazon DataZone 添加了一個名為的新政策 AmazonDataZoneFullAccess，可 DataZone 通過 AWS 管理控制台對 Amazon 的完全訪問。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2023 年 9 月 12 日
AmazonDataZoneEnvironmentRolePermissionsBoundary -新政策	Amazon 新 DataZone 增了一項名為的新政策，AmazonDataZoneEnvironmentRolePermissionsBoundary該政策會限制其所附加的已佈建 IAM 主體。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2023 年 9 月 12 日
受管理政策更新	AmazonDataZonePreviewConsoleFullAccess 受管理策略的更新。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2023 年 6 月 13 日

受管理政策更新	AmazonDataZoneProjectDeploymentPermissionsBoundary 受管理策略的更新。如需詳細資訊，請參閱 Amazon DataZone 更新 AWS 受管政策。	2023 年 4 月 3 日
???	Amazon DataZone （預覽版） 用戶指南的初始版本。	2023 年 3 月 29 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。