管理員指南

Amazon Nimble Studio

Amazon Nimble Studio: 管理員指南

Table of Contents

什麼是亞馬遜靈活工作室？

Nimble Studio 為一套應用程序和服務提供基礎架構和集中管理，藝術家可以使用這些應用程序和服務在雲中製作視覺效果，動畫和遊戲內容。

有了靈活工作室，您將獲得用戶和群組管理的基本工具。您還可以添加和管理應用程序，包括AWSThinkbox靈活的 Studio 文件傳輸。

Nimble Studio 具有統一的界面，可將所有工作室資源集中在一個位置。您可以讓使用者上線、指派應用程式，以及附加其工作功能特定的權限。靈活工作室不需要任何AWS經驗，您可以在大約五分鐘內完成設置。

目錄

功能和優點

以下是您使用靈活工作室獲得的一些功能和優勢：

- 免費使用 Nimble Studio；只需為應用程式使用的工作室資源付費。
- 集中管理您的工作室，檢查其狀態，並獲得其操作的高階見解。
- 新增和管理敏捷的 Studio 應用程式、使用者和群組，以及附加權限。
- 使用 AWS Identity and Access Management (IAM) 政策和角色，安全地管理對工作室資源的存取。
- 使用 AWS IAM Identity Center (IAM 身分中心) 管理工作室使用者和外部身分提供者的登入安全性。
- 使用工作室資源的標籤整理並輕鬆找到工作室資源。

相關應用

Nimble Studio 為數字內容創作者提供應用程序，以運營基於雲的工作室，用於製作視覺效果（VFX），動畫和交互式內容。

您可以使用 Amazon 彈性運算雲端 (Amazon EC2) 執行個體將這些應用程式安裝到本機電腦或雲端。您也可以使用 Amazon 簡易儲存服務 (Amazon S3) 安全地傳輸和存放數位媒體資產。這意味著您可以使用 Nimble Studio 來降低實體基礎設施、設備和技術人員的成本。

敏捷工作室目前提供以下應用程序：

- AWSThinkbox: Thinkbox 軟體包括渲染農場經理Thinkbox截止日期, 和 3D 外掛程式, Thinkbox 包括. 您可以使用Thinkbox軟體協助您增加工作室在內部部署、Amazon EC2 雲端或兩者的組合中的創意輸出。如需詳細資訊，請參閱AWS Thinkbox產品。
- Nimble Studio File Transfer：File Transfer加速將數位媒體資產傳入和傳出 Amazon S3 的媒體資產。 File Transfer提供圖形化使用者介面，您可以使用該介面快速移動數千個大型媒體檔案。如需詳細資訊，請參閱「什麼是 Nimble Studio File Transfer」頁面。

靈活工作室的定價

設置 Nimble Studio 並使用它來管理您的工作室基礎設施，用戶，安全性和服務免費。

但是，如果您在 Studio 中設定服務和應用程式，則可能需要支付儲存空間和其他 Studio 資源的費用。如需有關 Nimble Studio 應用程式定價的詳細資訊，請參閱個別應用程式的定價頁面。

如需管理AWS成本的相關資訊，請參閱AWS Cost Explorer Service和AWS Budgets。

開始使用靈活工作室

靈活的 Studio 設置和部署大約需要五分鐘。

熟悉靈活工作室的概念和術語後，請參閱亞馬遜敏捷工作室入門。在其中，您會發現部署您的工作室的step-by-step說明。

亞馬遜靈活工作室的概念和術語

若要協助您開始使用 Amazon Nimble Studio 並瞭解其運作方式，您可以參考本指南中的關鍵概念和術語。

主要功能

Amazon Nimble Studio

Amazon Nimble Studio 可讓創意工作室完全在雲端中製作視覺效果、動畫和互動式內容，從故事板草圖到最終交付項目。AWS 服務

亞馬遜靈活工作室控制台

靈活的 Studio 主控台是專門為我們 IT 管理員客戶提供的一部分。AWS Management Console這個主控台是管理員建立雲端工作室並管理許多設定的地方。例如，Studio 管理員頁面可讓您新增或移除資源、新增應用程式，以及授與使用者和群組的權限。

亞馬遜靈活工作室門戶

靈活的工作室門戶提供了一個用戶界面，用於與靈活的 Studio 應用程序和服務進行day-to-day交互。使用者直接使用其使用者名稱和密碼登入入口網站，而不必與 AWS Management Console.

Nimble Studio File Transfer

File Transfer加速數位媒體資產進出 Amazon 簡單儲存服務 (Amazon S3) 的媒體資產傳輸速度。 File Transfer提供圖形化使用者介面，您可以使用該介面快速移動數千個大型媒體檔案。如需詳細資訊，請參閱「什麼是 Nimble Studio File Transfer」頁面。

AWS Thinkbox

Thinkbox軟件包括渲染農場經理Thinkbox截止日期, 和 3D 插件, Thinkbox 特寫. 您可以使用Thinkbox軟體協助您增加工作室在內部部署、Amazon EC2 雲端或兩者的組合中的創意輸出。如需詳細資訊，請參閱AWS Thinkbox產品。

關鍵概念和術語

AWS受管理政策

受AWS管理的策略是由建立和管理的獨立策略AWS。獨立政策表示政策有自己的 Amazon Resource Name (ARN)，其中包含政策名稱。例如，arn: aw:iam:: AWS: 政策 /IAM 是受管政策。ReadOnlyAccess AWS如需 ARN 的詳細資訊，請參閱 IAM ARN。

AWS受管理的原則是用來授與一般工作功能的權限。工作職能政策會在引入新服務和 API 作業AWS時進行維護和更新。例如，AdministratorAccess工作功能可為中的每個服務和資源提供完整存取權和權限委派AWS。然而，部分存取AWS受管政策 (例如 AmazonMobileAnalyticsWriteOnlyAccess和 AmazonEC2) ReadOnlyAccess 可以提供特定層級的存取權，而AWS 服務不允許完全存取。如需有關存取原則的詳細資訊，請參閱了解原則摘要中的存取層級摘要。

AWS Management Console

這AWS Management Console是一個 Web 應用程式，可讓您存取廣泛的服務主控台集合以進行管理 AWS 服務。

每個服務還包括自己的控制台。這些主控台提供廣泛的雲端運算工具。甚至還有一項可協助您管理帳單和成本的服務。

AWS IAM Identity Center(IAM 身分識別中心)

IAM 身分識別中心是一項AWS服務，可讓您輕鬆集中管理多個AWS 帳戶商業應用程式的存取。透過 IAM 身分中心，您可以從單一位置為使用者提供所有指派帳戶和應用程式的單一登入存取權。您也可以集中AWS Organizations管理中所有帳戶的多帳戶存取和使用者權限。如需詳細資訊，請造訪AWS IAM Identity Center常見問題集

AWS PrivateLink

AWSPrivateLink在 VPC 和內部部署網路之間提供私人連線，而不會將流量暴露到公用網際網路。AWS 服務 AWS PrivateLink可讓您輕鬆連接不同帳戶和 VPC 之間的服務。 AWS PrivateLink可用於向您收取的月費AWS 帳戶。

數位內容創作 (DCC)

數位內容創作 (DCC) 是指用來製作創意內容的應用程式類別，包括BlenderNuke、Maya、和Houdini。

區域

靈活的工作室提供 11 AWS 區域 從中選擇部署你的工作室。區域是基本工作室基礎架構存在的地方，例如您的資料和應用程式。

該地區應該位於最接近您的工作室用戶。這樣可以減少延遲並提高數據傳輸速度。

工作室

工作室是其他靈活的工作室相關資源的頂級容器。您的雲端工作室會管理 Nimble Studio 入口網站，以及與您的虛擬私人雲端、使用者目錄和儲存加密金鑰AWS 帳戶等基本資源的連線。

工作室應用

Studio 元件是客戶 Nimble Studio 中的組態，可告訴服務如何存取檔案系統、授權伺服器和渲染伺服器陣列等資源。AWS 帳戶

敏捷工作室包含了許多工作室組件的子類型，包括共享文件系統，計算服務器陣列，活動目錄和許可證組件。這些子類型描述了您希望工作室使用的資源。

工作室資源

Studio 資源是一個術語，封裝了工作室在日常運營中所需的東西。在描述資源如何融入雲工作室的基礎架構時，它們可能也被稱為工作室組件。

Tags (標籤)

標籤是您指派給 AWS 資源的標籤。每個標籤都包含一個鍵和一個您定義的可選值。

標籤可讓您以不同方式來分類 AWS 資源。例如，您可以為帳戶的 Amazon 彈性運算雲端 (Amazon EC2) 執行個體定義一組標籤，以協助您追蹤每個執行個體的擁有者和堆疊層級。標籤還可讓您整合組織的共用檔案系統，並使用 Nimble Studio 轉譯伺服器陣列，在您將員工移至雲端時，保持工作流程不間斷。

使用標籤，您可以按用途、擁有者或環境對AWS資源進行分類。當您有許多相同類型的資源時，這很有用 — 您可以根據指派給該資源的標籤快速識別特定資源。

為靈活的工作室設置

本教學適用於想要設定 Amazon 靈活工作室的管理員使用者。

以下各節將引導您完成在 Nimble Studio 中部署工作室之前需要完成的步驟。

目錄

設定 IAM

開始之前，請先檢閱下列 AWS Identity and Access Management (IAM) 文件。

- IAM 中的安全最佳實務
- 以管理員使用者 AWS 帳戶 身分登入，以完成剩餘的設定。

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

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

建立具有管理權限的使用者

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

保護您的 AWS 帳戶根使用者

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

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

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

建立具有管理權限的使用者

1. 啟用 IAM Identity Center。

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

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

以具有管理權限的使用者身分登入

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

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

指派存取權給其他使用者

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

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

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

相關資源

- IAM 中的安全最佳做法
- AWS 服務 配額- AWS 一般參考

Amazon G入入入入入入入入入入入入門

本章說明如何使用 Nimble Studio 主控台建立工作室的基礎架構、確認、檢閱設定AWS 區域，以及建立您的工作室。您也可以使用其他設定來自訂設定。

對於初次使用的AWS客戶，請參閱為靈活的工作室設置教程。

主題

設定 Nimble S

本指南說明如何設定基礎架構、檢閱設定以及建立工作室。您還可以使用自定義您的工作室其他錄音室設置。

步驟 1：設定 Studio

您 Studio 的基礎設施由以下元件組成的作業：

- Studio 顯示名稱：Studio 顯示名稱是您識別工作室的方式，例如 AnyCompanyStudio。您的工作室名稱也會決定您的 Studio 入口網站網址。您可以在完成設定後隨時變更 Studio 顯示名稱。
- 工作室入口網站網址：您可以使用 Studio 入口網站 URL 存取您的工作室。網址是以工作室的顯示名稱為基礎，例如 https://anycompanystudio.awsapps.com。您可以在完成設定後隨時變更 Studio 入口網站網址。
- AWS 區域：AWS 區域是AWS資料中心集合的實際位置。設置工作室時，「地區」默認為離您最近的位置。您應該變更「地區」，使其位於離您的使用者最近的位置。這樣可以減少延遲並提高數據傳輸速度。

> **Important**
>
> 完成「靈活工作室」的設定後，就無法變更您的地區。

完成本節中的作業，以設定 Studio 的基礎結構。

若要設定工作室的基礎架構

1. 登入AWS Management Console並開啟靈活工作室主控台。
2. 選擇「設定靈活工作室」，然後選擇「下一步」。
3. 輸入 Studio 顯示名稱，例如**AnyCompany Studio**。
4. (選擇性) 若要變更 Studio 入口網站名稱，請選擇 [編輯網址]。
5. （可選）要更改，AWS 區域使其最接近您的工作室用戶，請選擇更改區域。
   a. 請選擇距離使用者最近的區域。
   b. 選擇「套用區域」。
6. (選擇性) 若要進一步自訂您的工作室設定，請選取其他錄音室設置。
7. 若要在建立工作室之前檢閱設定，請選擇「下一步」。

步驟 2：檢閱和建立自己的 Studio

配置工作室的基礎結構後，您可以查看，進行更改和創建工作室。

檢視和建立您的工作室

1. 在 [檢閱和建立] 頁面上，檢閱您的 Studio 基礎結構。
2. 確認最接近您的工作室用戶。AWS 區域
3. (選擇性) 選擇 「編輯」 以變更您的工作室設定。
4. 就緒後，請選擇建立 Studio

其他錄音室設置

靈活的工作室設置包括額外的工作室設置。使用這些設置，您可以查看 Nimble Studio 設置對您的所有更改AWS 帳戶，配置您的工作室用戶角色以及更改加密密鑰類型。您也可以將標籤新增至您的工作室資源。

配置工作室用戶角色

AWS服務可以擔任服務角色來代表您執行動作。靈活的工作室需要一個工作室用戶角色，以使用戶訪問您的工作室中的資源。

您可以將 AWS Identity and Access Management (IAM) 受管政策附加到 Studio 使用者角色。這些策略允許用戶執行某些操作，例如在特定的 Nimble Studio 應用程序中創建作業。由於應用程式取決於受管理原則中的特定條件，因此如果您不使用受管理的原則，應用程式可能無法如預期般執行。

您可以在完成組態後隨時變更 Studio 使用者角色。如需使用者角色的詳細資訊，請參閱 IAM 角色。

下列索引標籤包含兩種不同使用案例的指示。若要建立和使用新的服務角色，請選擇新增服務角色標標籤。若要使用現有的服務角色，請選擇現有的服務角色索引標籤。

New service role

若要建立和使用新的服務角色

1. 選取建立並使用新的服務角色。
2. (選擇性) 輸入服務使用者角色名稱。
3. 如需角色的詳細資訊，請選擇 [檢視權限詳細資料]

Existing service role

若要使用現有的服務角色

1. 選取 [使用現有的服務角色]。
2. 開啟下拉式清單以選擇現有的服務角色。
3. (選擇性) 選擇 IAM 主控台中的檢視，以取得有關該角色的詳細資訊。

AWS IAM Identity Center

AWS IAM Identity Center是用於管理使用者和群組的雲端單一登入服務。IAM 身分中心也可與您的企業單一登入 (SSO) 提供者整合，讓使用者可以使用其公司帳戶登入。

靈活的工作室默認情況下啟用 IAM 身份中心，並且必須設置和使用靈活工作室。如需詳細資訊，請參閱 什麼是 AWS IAM Identity Center。

設定AWS KMS加密金鑰

AWS Key Management Service(AWS KMS) 金鑰為您可以用來加密、解密和重新加密資料。

敏捷工作室包括以下AWS KMS加密密鑰類型：

- AWS擁有的金鑰：AWS擁有的金鑰為AWS 服務擁有和管理以在多個中使用的 KMS 金鑰AWS 帳戶。 AWS擁有的金鑰不在中AWS 帳戶，但 Nimble Studio 可以使用AWS自有的金鑰來保護您帳戶中的資源。

若要使用AWS KMS，您不需要建立或維護金鑰或其金鑰政策。使用AWS擁有的金鑰不收取任何費用，也不會AWS KMS計入您的AWS 帳戶.

- 客戶受管金AWS KMS鑰：客戶受管金鑰為您在中建立、擁AWS 帳戶有和管理的 KMS 金鑰。

  您可以完全控制這些 KMS 金鑰。客戶受管金鑰會產生每月的費用。他們還會針對AWS KMS超出免費方案的每個 API 請求收取費用。如需 AWS KMS 定價的詳細資訊，請參閱 AWS Key Management Service 定價。

完成設定後，無法變更加密金鑰類型。如需有關AWS KMS和加密金鑰類型的詳細資訊，請參閱AWS KMS文件。

選擇不同的加密金鑰類型

1. 選取 [選擇其他AWS KMS按鍵 (進階)]。
2. 選取AWS KMS金鑰或輸入亞馬遜資源編號 (ARN)。
3. 選擇建立AWS KMS金鑰。

組態標標標

標籤可作為組織靈活工作室資源的標籤。您最多可以新增 50 個標標籤來標標標標標、組織、篩選和搜尋資源。

每個標籤由兩個部分組成，您可以定義它們：標籤鍵和一個可選的標籤值-例如，鍵:domain和 value:anycompanystudio.com。

您可以在完成組態標後隨時新增或移除標籤。如需標籤的詳細AWS資訊，請參閱標標標標標標標標標標

將標標標標新增至您的工作室資源

1. 選擇 Add new tag (新增標籤)。
2. 輸入標籤索引鍵。
3. (選擇性) 輸入標籤值。

刪除工作室

您可以刪除不再需要的工作室。刪除工作室時，只會刪除工作室基礎結構。您的其他AWS資源 (例如使用者角色、原則和應用程式資料) 會保持不變。

> **Important**
>
> 一旦刪除工作室便無法復原。

刪除您的工作室

1. 登入AWS Management Console並開啟靈活工作室主控台。
2. 選擇工作室概述。
3. 選擇動作，然後選擇刪除工作室。
4. 輸入**`delete`**，然後選擇刪除。

Amazon Nimble Studio 中的安全性

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 Nimble Studio 的合規計劃，請參閱合規計劃的AWS 服務範圍。
- 雲端中的安全性 — 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。

> **Important**
>
> 強烈建議您閱讀並熟悉安全支柱- AWS Well- Architected 的框架。本文包含保護 AWS 基礎結構的關鍵原則。

本文件有助於您了解如何在使用 Nimble Studio 時套用共同責任模型。下列主題說明如何將 Nimble Studio 設定為達到您的安全及法規遵循目標。您還將學習如何使用其他 AWS 服務來幫助您監控和保護您的Nimble Studio資源。

詳細資訊

- 安全支柱- AWS Well-Architected 的框架
- AWS Cloud Development Kit (AWS CDK) (AWS CDK) 的安全性
- Amazon Virtual Private Cloud 中的安全
- AWS 安全認證
- Amazon EC2 中的安全性
  - Linux
  - Windows

設定 AWS 帳戶 安全性

本指南說明如何設定您在資源遭 AWS 帳戶 到入侵時接收通知，並允許特定 AWS 帳戶 使用者存取它。若要保護您的資源 AWS 帳戶 並追蹤您的資源，請完成以下步驟。

目錄

刪除帳戶的存取金鑰

您可以允許從 AWS Command Line Interface (AWS CLI) 或使用 AWS API 以程式設計方式存取您的 AWS 資源。不過，建 AWS 議您不要建立或使用與根帳戶相關聯的存取金鑰來進行程式設計存取。

如果您仍有存取金鑰，建議您刪除這些金鑰並建立使用者。然後，僅授予該使用者您打算呼叫的 API 所需的權限。您可以使用該使用者發出存取金鑰。

如需詳細資訊，請參閱AWS 一般參考 指南中的管理您 AWS 帳戶的存取金鑰。

啟用多重因素認證

多重要素驗證 (MFA) 是一種安全性功能，除了您的使用者名稱和密碼之外，還提供一層驗證。

MFA 的運作方式如下：使用使用者名稱和密碼登入後，您還必須提供只有您有實際存取權限的其他資訊。此資訊可以來自專用的 MFA 硬體裝置，或來自手機上的應用程式。

您必須從支援的 MFA 裝置清單中選取要使用的 MFA 裝置類型。對於硬體裝置，請將 MFA 裝置放在安全的位置。

如果您使用虛擬 MFA 裝置 (例如手機應用程式)，請考慮手機遺失或損壞時可能會發生什麼情況。一種方法是將您使用的虛擬 MFA 設備保存在安全的地方。另一種選擇是同時激活多個設備，或使用虛擬 MFA 選項進行設備密鑰恢復。

若要深入瞭解 MFA，請參閱啟用虛擬 Multi-Factor Authentication (MFA) 裝置。

相關資源

- 開始使用多重要素驗證

- 保護對 AWS 使用 MFA 的存取

全部 CloudTrail 啟用 AWS 區域

您可以使用追蹤 AWS 資源中的所有活動AWS CloudTrail。我們建議您 CloudTrail 立即開啟。這有助於您 AWS Support 的 AWS 解決方案架構師稍後疑難排解安全性或組態問題。

若要啟用全部 CloudTrail 記錄 AWS 區域，請參閱AWS CloudTrail 更新 — 在所有區域開啟和使用多重追蹤。

若要進一步了解 CloudTrail，請參閱開啟 CloudTrail：在您的 AWS 帳戶. 要了解如何 CloudTrail監控靈活的工作室，請參閱記錄靈活的工作室通話使用 AWS CloudTrail。

設置 Amazon GuardDuty 和通知

Amazon GuardDuty 是一種持續的安全監控服務，可分析並處理以下項目：

- 資料來源
- Amazon VPC 流程日誌
- AWS CloudTrail 管理事件記錄
- CloudTrail S3 資料事件日誌
- DNS 日誌

Amazon 會 GuardDuty 識別您 AWS 環境中的未預期和潛在未經授權的惡意活動。惡意活動可能包括權限提升、使用公開認證，或與惡意 IP 位址或網域通訊等問題。若要識別這些活動，請 GuardDuty 使用威脅情報摘要，例如惡意 IP 位址和網域清單，以及機器學習。例如， GuardDuty 可以偵測服務惡意軟體或採礦比特幣的受感染 Amazon EC2 執行個體。

GuardDuty 也會監控 AWS 帳戶 存取行為是否有入侵跡象。這包括未經授權的基礎結構部署，例如部署在從未 AWS 區域 使用過的執行個體。它還包括不尋常的 API 調用，例如密碼策略更改以降低密碼強度。

GuardDuty 透過產生安全性發現項目，通知您 AWS 環境的狀態。您可以在 GuardDuty 主控台或透過 Amazon CloudWatch 事件檢視這些發現項目。

設定 Amazon SNS 主題和端點

請遵循設定 Amazon SNS 主題和端點教學課程中的指示進行。

設定 GuardDuty 發現項目的 EventBridge 事件

針對 GuardDuty 產生的所有 EventBridge 發現項目建立傳送事件的規則。

若要建立 GuardDuty 發現項目的 EventBridge 事件

1. 登錄到 Amazon 控 EventBridge 制台：https://console.aws.amazon.com/events/
2. 在導覽窗格中，選擇規則。然後，選擇 Create role (建立角色)。
3. 輸入新規則的「名稱」與「摘要」。然後選擇下一步。
4. 保留AWS 為事件來源選取的事件或 EventBridge 合作夥伴事件。
5. 在事件模式中，選擇事件來源的AWS 服務。然後GuardDuty為AWS 服務和GuardDuty 查找事件類型。這是您在中建立的主題設定 Amazon SNS 主題和端點。
6. 選擇下一步。
7. 針對目標 1，選取AWS 服務。在 [選取目標] 下拉式清單中選擇 SNS 主題。然後選擇您的電子GuardDuty郵件主題。
8. 在其他設定區段中：使用 [設定目標輸入] 下拉式清單選擇 [輸入變壓器]。選取設定輸入轉換器。
9. 在「目標輸入變壓器」區段的「輸入路徑」欄位中輸入下列程式碼。

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

10. 若要格式化電子郵件，請在「範本」欄位中輸入下列程式碼。

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type <Finding_Type>
 in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id=<Finding_ID>"
```

11. 選擇建立。然後選擇下一步。
12. (選擇性) 如果您使用標籤來追蹤 AWS 資源，請新增標籤。

13. 選擇下一步。
14. 檢閱您的規則。然後，選擇 Create role (建立角色)。

現在您已設定 AWS 帳戶 安全性，您可以將存取權授予特定使用者，並在資源遭到入侵時收到通知。

Amazon Nimble Studio 中的資料保護

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

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

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

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用主控台、API Nimble Studio 或 AWS SDK 時 AWS 服務 使用或其他使用時。 AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

AWS 共同責任模式適用於 Amazon 敏捷工作室中的資料保護。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您有責任保持對此基礎結構上託管的內容的控制權。此內容包括您使用的安全性組態和管理工作。 AWS 服務

如需有關資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需歐盟資料保護的相關資訊，請造訪 GDPR 中心。

靜態加密

Nimble Studio 通過使用存儲在 AWS Key Management Service （ AWS KMS ）中的加密密鑰對其靜態加密來保護敏感的工作室數據。所有提供靈活工作室的 AWS 區域 地方均可使用靜態加密。我們加密的工作室數據包括所有資源類型的名稱和描述，以及 studio 組件腳本，腳本參數，掛載點，共享名稱和其他數據。

加密資料表示，如果沒有有效金鑰，任何使用者或應用程式都無法讀取儲存在磁碟上的敏感資料。加密的資料可以安全地儲存在靜態位置，而且只能由具有受管理金鑰授權存取權的一方解密。

有關敏捷工作室如何用 AWS KMS 於加密靜態數據的信息，請參閱。Amazon 靈活工作室的密鑰管理

使用授權與 AWS KMS 金鑰

授權是允許AWS 主體在密碼編譯作業中使用 AWS KMS 金鑰的原則工具。它也可以讓他們使用命令檢視 KMS 金鑰`DescribeKey`，以及建立和管理授權。

與整合的授權通 AWS 服務 常用 AWS KMS 於加密靜態資料。服務會代表帳戶中的使用者建立授予、使用其許可，並在其任務完成後立即淘汰授予。

當敏捷工作室創建您的工作室時，我們為靈活的工作室門戶用戶提供了兩個角色：用戶和管理員角色。Nimble Studio 為這些角色創建客戶託管密鑰的贈款，以使他們能夠訪問工作室加密數據。

> **Important**
>
> 如果您刪除授權，則在管理員建立新授權之前，使用者將無法使用 Nimble Studio 入口網站。

如需有關 AWS 服務 使用授權方式的詳細資訊，請參閱服務的 AWS 服務 使用指南 AWS KMS 或開發人員指南中的「如何使用」或「靜態加密」主題。

傳輸中加密

下表提供資料在傳輸過程中如何加密的相關資訊。在適用的情況下，還列出了敏捷工作室的其他數據保護方法。

資料	網路路徑	保護
網頁資產，例如影像和 JavaScript 檔案	網絡路徑是靈活的工作室用戶和靈活的工作室之間。	資料加密使用 TLS 1.2 或更新版本。

像素和相關的串流流量	網絡路徑是靈活的工作室用戶和靈活的工作室之間。	使用 256 位元進階加密標準 (AES-256) 加密，並使用 TLS 1.2 或更新版本進行傳輸。
API 流量	這條路徑是靈活的工作室用戶和靈活的工作室之間。	使用 TLS 1.2 或更新版本進行加密。建立連線的要求會使用 SIGv4 簽署。

Amazon 靈活工作室的密鑰管理

建立新工作室時，您可以選擇下列其中一個金鑰來加密 Studio 資料：

- AWS 擁有的 KMS 金鑰 — 預設加密類型。鑰匙由靈活工作室擁有（不收取額外費用）。
- 客戶管理的 KMS 金鑰 — 金鑰會儲存在您的帳戶中，並由您建立、擁有和管理。您可以完全控制密鑰。 AWS KMS 費用適用。

在 AWS Key Management Service (AWS KMS) 中刪除客戶管理的 KMS 金鑰具有破壞性且具有潛在危險性。它會以不可逆轉的方式刪除金鑰材料以及與金鑰相關聯的所有中繼資料。刪除客戶管理的 KMS 金鑰後，您無法再解密由該金鑰加密的資料。這意味著數據變得不可恢復。

這就是 AWS KMS 為什麼客戶在刪除金鑰之前提供最多 30 天的等待期的原因。預設等待期間為 30 天。

關於等待期

由於刪除客戶管理的 KMS 金鑰具有破壞性且具有潛在危險性，因此我們要求您設定 7 至 30 天的等待期。預設等待期間為 30 天。

不過，實際等待期可能比您排定的等待期長最多 24 小時。要獲取密鑰將被刪除的實際日期和時間，請使用該DescribeKey操作。您也可以在金鑰的詳細資料頁面的 [一般設定] 區段中，在AWS KMS 主控台中查看金鑰的排定刪除日期。請注意時區。

在等待期間，客戶管理的金鑰狀態和金鑰狀態為擱置刪除。

- 待刪除的客戶管理 KMS 金鑰無法用於任何密碼編譯作業。
- AWS KMS 不會輪替待刪除之客戶管理 AWS KMS 金鑰的後備金鑰。

如需有關刪除客戶管理金 AWS KMS 鑰的詳細資訊，請參閱刪除客戶主金鑰。

資料安全措施

基於資料保護目的，我們建議您使用 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別帳戶。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。建議使用 TLS 1.2 或更新版本。
- 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。
- 如果您在透過命令列介面或 API 存取 AWS 時，需要 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。

強烈建議您不要將敏感的識別資訊 (例如客戶帳號) 放入任意格式欄位 (例如「名稱」欄位) 中。這包括當您 AWS 服務 使用主控台、API 或軟體開 AWS 發套件與 Amazon 敏捷工作室或其他工作時。 AWS CLI您輸入 Amazon Nimble Studio 或其他服務的任何資料都可能會被選取，以便包含在診斷日誌中。當您提供外部伺服器的 URL 時，請勿在驗證您對該伺服器請求的 URL 中包含登入資料資訊。

診斷資料和指標

在部署和刪除期間 StudioBuilder，Amazon Nimble Studio 會收集我們用來診斷問題並改善 Nimble Studio 的功能和使用者體驗的某些指標。

收集的指標類型

- 使用資訊 — 執行的一般命令和子命令。
- 錯誤和診斷資訊 — 執行命令的狀態和持續時間，包括結束代碼、內部例外狀況名稱和失敗。
- 系統與環境資訊 — Python 版本、作業系統 (WindowsLinux、或macOS)，以及執行所在 StudioBuilder 的環境。

Amazon 靈活工作室的 Identity and Access Management

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 管理員控制誰可以通過身份驗證 (登入) 和授權 (有權限) 使用 Amazon Nimble Studio 資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

主題

物件

您使用 AWS Identity and Access Management （ IAM ）的方式會有所不同，具體取決於您在靈活工作室中進行的工作。

服務使用者 — 如果您使用敏捷工作室服務來完成工作，那麼您就是服務使用者。在這種情況下，您的管理員將為您提供存取指派資源所需的認證和權限。當您使用更多靈活的 Studio 功能來完成工作時，您可能需要其他權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法在靈活工作室中使用某項功能，請參閱疑難排解 Amazon 敏捷工作室身分和存取。

服務管理員 — 如果您負責公司的靈活工作室資源，您可能可以完全訪問靈活工作室。您的工作就是決定員工應該使用哪些敏捷工作室功能和資源。然後，向您的管理員提交請求，以變更服務使用者的權限。檢閱此頁面上的資訊，了解 IAM 的基本概念。要進一步了解貴公司如何將 IAM 與敏捷工作室搭配使用，請參閱Amazon 靈活工作室如何與 IAM 合作。

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。如需有關使用登入的詳細資訊 AWS Management Console，請參閱 IAM 使用者指南中的「 AWS Management Console 以 IAM 使用者或根使用者身分登入」。

您必須以 AWS 帳戶 root 使用者、使用者或假設 IAM 角色的身分驗證 (登入 AWS)。您還可以使用公司的單一登錄身份驗證，甚至可以使用谷歌或 Facebook 登錄。在上述案例中，您的管理員會使用 IAM 角色預先設定聯合身分。當您 AWS 使用其他公司的憑據訪問時，您將間接擔任角色。

若要直接登入 AWS Management Console，請使用您的密碼與 root 使用者電子郵件地址或您的使用者名稱。您可以使用 root 使用者或使用者存取金鑰以 AWS 程式設計方式存取。

AWS 提供 SDK 和命令行工具，以使用您的憑據對請求進行加密簽名。如果您不使用 AWS 工具，請自行簽署要求。請使用 Signature 第 4 版來執行此作業，它是針對傳入 API 請求進行身分驗證的通訊協定。如需有關驗證要求的詳細資訊，請參閱. AWS 一般參考

無論您使用何種身分驗證方法，您可能還需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。若要進一步了解，請參閱 IAM 使用者指南中 AWS的使用多因素身份驗證 (MFA)。

AWS 帳戶 根使用者

當您第一次建立時 AWS 帳戶，您會從單一登入身分開始，該身分可以完整存取帳戶中的所有資源 AWS 服務 和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。我們強烈建議您不要將 root 使用者用於日常工作，甚至是管理工作。反之，請遵循僅以根使用者建立您第一個 IAM 使用者的最佳實務。接著請妥善鎖定根使用者登入資料，只用來執行少數的帳戶與服務管理作業。

使用者和群組

使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定權限。使用者可以擁有長期認證或一組存取金鑰。若要了解如何產生存取金鑰，請參閱《IAM 使用者指南》中的「管理 IAM 使用者的存取金鑰」。當您為使用者產生存取金鑰時，請檢視並安全地儲存 key pair。您 future 來無法恢復秘密訪問密鑰。而是生成一個新的訪問 key pair。

IAM 群組是指定使用者集合的身分識別。您無法以群組身分登入。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。若要深入了解，請參閱 IAM 使用者指南中的建立使用者的時機 (而非角色)。

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似於使用者，但與特定人員無關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需有關使用角色的方法的詳細資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 暫時使用者許可 - 使用者可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 聯合使用者存取 — 您可以使用企業使用者目錄或 Web 身分 AWS Directory Service提供者的現有身分，而不是建立使用者。這些稱為聯合身分使用者。透過身分提供者身分提供者來請求存取時，AWS 會指派角色給聯合身分使用者。如需聯合身分使用者的詳細資訊，請參閱 IAM 使用者指南中的聯合身分使用者和角色。
  - 成員資格 — Nimble Studio 使用稱為「成員資格」的概念，為用戶提供對特定啟動配置文件的訪問權限。成員資格可讓 Studio 管理員將資源存取權委派給使用者，而無需撰寫或瞭解 IAM 政策。當 Nimble Studio 管理員在啟動設定檔中為使用者建立成員資格時，該使用者將獲授權執行使用啟動設定檔所需的 IAM 動作，例如檢視其屬性以及使用該啟動設定檔啟動串流工作階段。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。服務角色只能在您的帳戶內提供存取權，而且無法用來授與其他帳戶中服務的存取權。管理員可以在 IAM 中建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》 AWS 服務中的建立角色以委派許可給
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。靈活的工作室不支持服務鏈接的角色。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱 IAM 使用者指南中的使用 IAM 角色將許可授與在 Amazon EC2 執行個體上執行的應用程式。

若要了解是使用 IAM 角色還是使用者，請參閱 IAM 使用者指南中的建立 IAM 角色的時機 (而非使用者)。

使用政策管理存取權

您可以透 AWS 過建立政策並將其附加到 IAM 身分或 AWS 資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。您可以以 root 使用者或使用者身分登入，也可以擔任 IAM 角色。當您接著提出要求時， AWS 會評估相關的身分識別或以資源為基礎的政策。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪些主體可以在什麼樣的資源，以及什麼條件執行操作。

每個 IAM 實體 (使用者或角色) 在開始時都沒有許可。換句話說，根據預設，使用者無法執行任何作業，甚至也無法變更他們自己的密碼。若要授予使用者執行動作的許可，管理員必須將許可政策連接到

使用者。或者，管理員可以將使用者新增到具備預定許可的群組。管理員將許可給予群組時，該群組中的所有使用者都會獲得那些許可。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

身分型政策

以身分識別為基礎的原則是 JSON 權限原則文件，您可以附加至身分識別，例如使用者、使用者群組或角色。這些原則控制使用者和角色可以執行哪些動作、哪些資源以及針對哪些條件。若要了解如何建立身分型政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管政策或內嵌政策之間進行選擇，請參閱 IAM 使用者指南中的受管政策和內嵌政策之間進行選擇。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。針對附加原則的資源，此原則會定義指定的主參與者可以對該資源執行的動作，以及針對哪些條件執行。在以資源為基礎的策略中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

敏捷工作室中的訪問控制列表（ACL）

存取控制清單 (ACL) 可控制哪些委託人 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於以資源為基礎的政策，雖然它們不使用 JSON 政策文件格式。

Amazon S3 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF若要進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 權限界限 — 許可界限是一項進階功能，您可以在其中設定以身分為基礎的政策可授予 IAM 實體 (使用者或角色) 的最大許可權。您可以為實體設定許可界限。產生的權限是實體以身分識別為基礎的原則及其權限界限的交集。在`Principal`欄位中指定使用者或角色的資源型策略不受權限界限的限制。所有這類政策中的明確拒絕都會覆寫該允許。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。
- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定組織中組織或組織單位（OU）的最大權限。組 Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的權限，包括每個 AWS 帳戶 root 使用者。如需有關 Organizations 和 SCP 的詳細資訊，請參閱《 AWS Organizations 使用者指南》中的 SCP 如何運作。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Amazon 靈活工作室如何與 IAM 合作

在您使用 IAM 管理敏捷工作室的存取權限之前，請先了解哪些 IAM 功能可與敏捷工作室搭配使用。

您可以與 Amazon 靈活工作室一起使用的 IAM 功能

IAM 功能	靈活的工作室支持
靈活工作室的政策行動	是
靈活工作室的政策資源	是
靈活工作室的政策條件金鑰	是
敏捷工作室中的訪問控制列表（ACL）	否
基於屬性的訪問控制（ABAC）與靈活的工作室	是
透過敏捷工作室使用臨時憑證	是

IAM 功能	靈活的工作室支持
敏捷工作室的跨服務主體權限	是
靈活工作室的服務角色	是
靈活工作室的服務連結角色	否

若要深入了解靈活 AWS 服務 工作室和其他如何與大多數 IAM 功能搭配使用 AWS 服務 ，請參閱 IAM 使用者指南中的 IAM。

敏捷工作室基於身份識別的政策

支援身分型政策	是

以身分識別為基礎的原則是 JSON 權限原則文件，您可以附加至身分識別，例如使用者、使用者群組或角色。這些原則控制使用者和角色可以執行哪些動作、哪些資源以及針對哪些條件。若要了解如何建立身分型政策，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，以及允許或拒絕動作的條件。您無法在以識別為基礎的原則中指定主體，因為它會套用至其所附加的使用者或角色。若要了解可在 JSON 政策中使用的所有元素，請參閱 IAM 使用者指南中的 IAM JSON 政策元素參考資料。

Amazon 敏捷工作室的基於身份的政策示例

要查看靈活工作室基於身份的策略的示例，請參閱。Amazon 敏捷工作室的基於身份的政策示例

靈活工作室內基於資源的政策

支援以資源基礎的政策	否

靈活的工作室不支持基於資源的策略或跨帳戶訪問。資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。針對附加原則的資源，此原則會定義指定的主參與者可以對該資源執行的動作，以及針對哪些條件執行。在以資源為基礎的策略中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

靈活工作室的政策行動

支援政策動作	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪些主體可以在什麼樣的資源，以及什麼條件執行操作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外情況，例如沒有匹配 API 操作的僅限權限操作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

要查看靈活的工作室操作列表，請參閱服務授權參考中由 Amazon 敏捷工作室定義的操作。

敏捷工作室中的策略操作在操作之前使用以下前綴：

```
nimble
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "nimble:action1",
      "nimble:action2"
         ]
```

要查看靈活工作室基於身份的策略的示例，請參閱。Amazon 敏捷工作室的基於身份的政策示例

靈活工作室的政策資源

支援政策資源	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪些主體可以在什麼樣的資源，以及什麼條件執行操作。

`Resource` JSON 政策元素可指定要套用動作的物件。陳述式必須包含 `Resource` 或 `NotResource` 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級權限的動作 (例如列出作業)，請使用萬用字元 (*) 來指出陳述式適用於所有資源。

```
"Resource": "*"
```

要查看靈活工作室基於身份的策略的示例，請參閱。Amazon 敏捷工作室的基於身份的政策示例

靈活工作室的政策條件金鑰

支援政策條件索引鍵	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪些主體可以在什麼樣的資源，以及什麼條件執行操作。

元Condition素 (或Condition`**block**) lets you specify conditions in which a statement is in effect. The `Condition元素是可選的。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。若您為單一條件索引鍵指定多個值， AWS 會使用邏輯 OR 操作評估條件。必須符合所有條件，才能授與陳述式的權限。

您也可以在指定條件時使用預留位置變數。例如，您只能授與使用者存取資源的權限，只有當資源已標記為其使用者名稱時。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看 AWS 全域條件金鑰，請參閱 IAM 使用者指南中的 AWS 全域條件內容金鑰。

要查看靈活工作室基於身份的策略的示例，請參閱。Amazon 敏捷工作室的基於身份的政策示例

敏捷工作室中的訪問控制列表 (ACL)

支援 ACL	否

靈活的工作室不支持訪問控制列表 (ACL)。ACL 控制哪些主體 (帳戶成員、使用者或角色) 具有存取資源的權限。ACL 類似於以資源為基礎的政策，雖然它們不使用 JSON 政策文件格式。

基於屬性的訪問控制（ABAC）與靈活的工作室

支援 ABAC (政策中的標籤)	是

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。然後您設計 ABAC 原則，以便在主體的標籤符合他們嘗試存取的資源上的標籤時允許作業。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如需 ABAC 的詳細資訊，請參閱什麼是 AB AC？ 在 IAM 使用者指南中。若要檢視包含設定 ABAC 步驟的教學課程，請參閱 IAM 使用者指南中的使用以屬性為基礎的存取控制 (ABAC)。

透過敏捷工作室使用臨時憑證

支援臨時憑證	是

當您使用臨時憑據登錄時，有些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需有關切換角色的詳細資訊，請參閱《IAM 使用者指南》中的「切換到角色 (主控台)」。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

敏捷工作室的跨服務主體權限

支援主體許可	是

靈活工作室的服務角色

支援服務角色	是

服務角色是服務擔任的 IAM 角色，可代您執行動作。服務角色只能在您的帳戶內提供存取權，而且無法用來授與其他帳戶中服務的存取權。管理員可以在 IAM 中建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》 AWS 服務中的建立角色以委派許可給

> **Warning**
>
> 變更服務角色的權限可能會中斷「敏捷工作室」功能。只有在敏捷工作室提供指導時，才能編輯服務角色。

靈活工作室的服務連結角色

支援服務連結角色。	否

靈活的工作室不支持服務鏈接的角色。服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的 IAM 帳戶中，並由該服務所擁有。 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服務連結角色的詳細資訊 AWS 服務 ，請參閱使用 IAM。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

Amazon 敏捷工作室的基於身份的政策示例

默認情況下，用戶和角色沒有創建或修改敏捷工作室資源的權限。他們也無法使用 AWS Management Console AWS CLI、或 AWS API 執行工作。管理員必須建立 IAM 政策，以授與使用者和角色對所需資源執行動作的權限。管理員接著必須將這些政策連接至需要這些許可的使用者或群組。

若要了解如何使用這些 JSON 政策文件範例建立 IAM 身分型政策，請參閱 IAM 使用者指南中的 JSON 索引標籤上建立政策。

主題

- 政策最佳實務

政策最佳實務

身分型政策相當強大。他們決定是否有人可以在您的帳戶中創建，訪問或刪除敏捷工作室資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策 — 若要快速開始使用 Nimble Studio，請使用 AWS 受管理的政策為您的員工提供所需的權限。這些政策已在您的帳戶中提供，並由 AWS維護和更新。如需詳細資訊，請參閱 IAM 使用者指南中的 AWS 受管政策開始使用許可。
- 授予最低權限：當您建立自訂政策時，請只授予執行任務所需要的許可。以最小一組許可開始，然後依需要授予額外的許可。這比一開始使用太寬鬆的許可，稍後再嘗試將他們限縮更為安全。如需詳細資訊，請參閱《IAM 使用者指南》中的授予最低權限。
- 針對敏感作業啟用 MFA — 為了提高安全性，使用者必須使用多重要素驗證 (MFA) 來存取敏感資源或 API 作業。如需詳細資訊，請參閱 IAM 使用者指南中 AWS的使用多因素身份驗證 (MFA)。
- 使用策略條件以獲得額外的安全性 — 在可行的範圍內，定義以身份為基礎的策略允許存取資源的條件。例如，您可以撰寫條件，指定請求必須來自一定的允許 IP 地址範圍。您也可以撰寫條件，只在指定的日期或時間範圍內允許請求，或是要求使用 SSL 或 MFA。如需詳細資訊，請參閱 IAM JSON 政策元素：IAM 使用者指南中的條件。

AWS Amazon 靈活工作室的受管政策

若要新增使用者、群組和角色的權限，使用 AWS 受管理的原則比自己撰寫原則更容易。建立 IAM 客戶受管政策需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可以使用我們的 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中使用。如需 AWS 受管政策的詳細資訊，請參閱 IAM 使用者指南中的AWS 受管政策。

AWS 服務會維護和更新 AWS 受管理的策略。您無法變更 AWS 受管理原則中的權限。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管理的政策移除權限，因此政策更新不會破壞您現有的權限。

此外，還 AWS 支援跨多個服務之工作職能的受管理原則。例如，ReadOnlyAccess AWS 受管理的策略提供對所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時， AWS 會為新的操作和資源新增唯讀許可。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中有關任務職能的AWS 受管政策。

您的最終用戶將主要使用靈活工作室門戶訪問 Amazon 敏捷工作室。使用 StudioBuilder 或 Nimble Studio 控制台創建工作室時，會為每個工作室角色創建一個 IAM 角色：工作室管理員和工作室用戶。

每個都附加了各自的 IAM 受管政策。敏捷工作室門戶提供了一種體驗，用戶只能列出和使用他們有權訪問的資源。

Nimble Studio 入口網站提供了一種體驗，使用者只能列出並使用他們有權存取的資源，而入口網站則需視這些政策的內容而定，才能正確運作。靈活的工作室最終用戶將使用門戶訪問他們的雲工作室。因此，當管理員使用建立工作室時 StudioBuilder，會為每個需要存取工作室的人員建立一個 IAM 角色。這包括 Studio 管理員和 Studio 使用者，每個使用者都附加了各自的 IAM 受管政策。

如需工作職能政策的清單和說明，請參閱《IAM 使用者指南》中的AWS 受管工作職能政策。

AWS 受管理的策略：**AmazonNimbleStudio-LaunchProfileWorker**

您可將 AmazonNimbleStudio-LaunchProfileWorker 政策連接到 IAM 身分。

將此政策附加到由靈活工作室構建器創建的 EC2 實例，以授予敏捷工作室啟動配置文件工作者所需資源的訪問權限。

許可詳細資訊

此政策包含以下許可。

- ds-允許 LaunchProfile 工作者發現有 AWS Managed Microsoft AD 關與 LaunchProfile.
- ec2-允許 LaunchProfile 工作者發現安全組和子網信息以連接到 LaunchProfile.
- fsx-允許 LaunchProfile 工作者發現與. LaunchProfile

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
```

```
      },
      "Sid": "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version": "2012-10-17"
}
```

AWS 受管理的策略：**AmazonNimbleStudio-StudioAdmin**

您可將 AmazonNimbleStudio-StudioAdmin 政策連接到 IAM 身分。

將此政策附加到與您的工作室相關聯的管理員角色，以授予與工作室管理員和其他服務中相關工作室資源相關聯的 Amazon Nimble Studio 資源的存取權。

許可詳細資訊

此政策包含以下許可。

- 靈活-允許 Studio 用戶訪問已委託給他們的靈活資源。 StudioAdmins
- SSO-允許工作室用戶查看工作室中其他用戶的名稱的能力。
- 身份存儲-允許工作室用戶查看工作室中其他用戶的姓名的能力。
- ds-允許靈活的工作室虛擬工作站添加到與工作室 AWS Managed Microsoft AD 相關聯。
- ec2-允許靈活的工作室將虛擬工作站連接到您配置的 VPC。
- fsx-允許靈活的工作室將虛擬工作站連接到您配置的 Amazon FSx 卷。
- cloudwatch-允許靈活的工作室檢索 CloudWatch 指標。

```
{
  "Statement": [
    {
      "Sid": "StudioAdminFullAccess",
      "Effect": "Allow",
      "Action": [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:DeleteStreamingSession",
        "nimble:ListStreamingSessionBackups",
```

```
        "nimble:GetStreamingSessionBackup",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetEula",
        "nimble:AcceptEulas",
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListStreamingSessions",
        "nimble:GetStreamingImage",
        "nimble:ListStreamingImages",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents",
        "nimble:ListLaunchProfiles",
        "nimble:GetLaunchProfile",
        "nimble:GetLaunchProfileMember",
        "nimble:ListLaunchProfileMembers",
        "nimble:PutLaunchProfileMembers",
        "nimble:UpdateLaunchProfileMember",
        "nimble:DeleteLaunchProfileMember"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
```

```
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "cloudwatch:GetMetricData",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "AWS/NimbleStudio"
        }
      }
    }
  ],
  "Version": "2012-10-17"
}
```

AWS 受管理的策略：**AmazonNimbleStudio-StudioUser**

您可將 AmazonNimbleStudio-StudioUser 政策連接到 IAM 身分。

將此政策附加到與您的工作室相關聯的使用者角色，以授與工作室使用者和其他服務中相關工作室資源相關聯的 Amazon Nimble Studio 資源的存取權。

許可詳細資訊

此政策包含以下許可。

- 靈活-允許 Studio 用戶訪問已委託給他們的靈活資源。 StudioAdmins
- SSO-允許工作室用戶查看工作室中其他用戶的名稱的能力。
- 身份存儲-允許工作室用戶查看工作室中其他用戶的姓名的能力。

- ds-允許靈活的工作室虛擬工作站添加到與工作室 AWS Managed Microsoft AD 相關聯。
- ec2-允許靈活的工作室將虛擬工作站連接到您配置的 VPC。
- fsx-允許靈活的工作室將虛擬工作站連接到您設定的 Amazon FSx 磁碟區。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
        "*"
      ]
    },
    {
```

```
      "Effect": "Allow",
      "Action": [
        "nimble:ListLaunchProfiles"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "nimble:requesterPrincipalId": "${nimble:principalId}"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:DeleteStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:ListStreamingSessions"
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "nimble:ownedBy": "${nimble:requesterPrincipalId}"
        }
      }
    }
  ],
```

```
  "Version": "2012-10-17"
}
```

敏捷工作室更新 AWS 受管理政策

檢視 Amazon Nimble Studio AWS 受管政策更新的詳細資訊，因為這項服務開始追蹤這些變更。

變更	描述	日期
AWS 受管理的策略：AmazonNimbleStudio-StudioUser - 更新的政策	Amazon 敏捷工作室更新了一項政策，以使用最新版本的身份存儲服務。	2023 年 9 月 22 日
AWS 受管理的策略：AmazonNimbleStudio-StudioAdmin - 更新的政策	Amazon 敏捷工作室更新了一項政策，以使用最新版本的身份存儲服務。	2023 年 9 月 22 日
AWS 受管理的策略：AmazonNimbleStudio-StudioUser - 更新的政策	Amazon 敏捷工作室更新了一項政策，允許工作室用戶查看其工作站備份。	2022 年 12 月 20 日
AWS 受管理的策略：AmazonNimbleStudio-StudioAdmin - 更新的政策	Amazon 敏捷工作室更新了政策，允許工作室管理員查看他們的工作站備份。	2022 年 12 月 20 日
AWS 受管理的策略：AmazonNimbleStudio-StudioUser - 更新的政策	Amazon 敏捷工作室更新了一項政策，允許工作室管理員檢索 CloudWatch指標。	2021 年 11 月 11 日
AWS 受管理的策略：AmazonNimbleStudio-StudioUser - 更新的政策	Amazon 敏捷工作室更新了政策，允許工作室用戶啟動和停止他們的工作站。	2021 年 11 月 1 日
AWS 受管理的策略：AmazonNimbleStudio-StudioAdmin - 更新的政策	Amazon 敏捷工作室更新了政策，允許工作室管理員啟動和停止他們的工作站。	2021 年 11 月 1 日

變更	描述	日期
AWS 受管理的策略：AmazonNimbleStudio-StudioUser - 更新的政策	Amazon 敏捷工作室更新了政策，以有條件地允許基於而不是存取串流工作階段資源。nimble:ownedBy nimble:createdBy	2021 年 8 月 16 日
AWS 受管理的策略：AmazonNimbleStudio-StudioUser – 新政策	Amazon Nimble Studio 新增了一項新政策，允許存取與工作室使用者相關的資源，以及其他服務中的相關工作室資源。	2021 年 4 月 28 日
AWS 受管理的策略：AmazonNimbleStudio-StudioAdmin – 新政策	Amazon Nimble Studio 新增了一項新政策，允許存取與工作室管理員相關聯的資源，以及其他服務中的相關工作室資源。	2021 年 4 月 28 日
AWS 受管理的策略：AmazonNimbleStudio-LaunchProfileWorker – 新政策	Amazon 敏捷工作室添加了一項新政策，允許訪問靈活工作室啟動配置文件工作者所需的資源。	2021 年 4 月 28 日
Amazon 靈活工作室開始跟踪變化	Amazon 敏捷工作室開始追蹤其 AWS 受管政策的變更。	2021 年 4 月 28 日

預防跨服務混淆代理人

混淆的副問題是一個安全性問題，即沒有執行動作權限的實體可能會強制更具權限的實體執行動作。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。調用服務可以被操縱，以其他方式不應該有權限訪問另一個客戶的資源採取行動的權限。為了預防這種情況， AWS 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

我們建議在資源政策中使用aws:SourceArn和aws:SourceAccount全域條件內容金鑰，以限制 Identity and Access Management (IAM) 授予 Amazon Nimble Studio 存取資源的許可。如果您同時使

用全域條件內容索引鍵，則aws:SourceAccount值中的值和帳戶在aws:SourceArn相同的策略陳述式中使用時必須使用相同的帳戶 ID。

的值aws:SourceArn必須是工作室的 ARN，並且aws:SourceAccount必須是您的帳戶 ID。在創建工作室之前，您將不會知道工作室 ID 是什麼，因為它是由靈活工作室生成的。創建您的工作室後，您可以將最終的工作室 ID 設置為更新信任策略aws:SourceArn。

防範混淆代理人問題的最有效方法是使用 aws:SourceArn 全域條件內容索引鍵，以及資源的完整 ARN。如果您不知道資源的完整 ARN，或者您要指定多個資源，請對 ARN 的未知部分使用帶有萬用字元 (*) 的aws:SourceArn全域內容條件索引鍵。例如 arn:aws:nimble::123456789012:*。

您的終端使用者在登入敏捷工作室入口網站時擔任您的工作室角色。當您建立工作室時，請 AWS 設定角色並評估原則。 AWS 每次您的其中一位使用者登入 Nimble Studio 入口網站時，都會評估該政策。建立工作室時，您無法修改aws:SourceArn. 完成創建您的工作室後，您可以使用您的工作室。aws:SourceArn

下列範例是假設角色原則，顯示如何在 Nimble Studio 中使用aws:SourceArn和aws:SourceAccount全域條件內容索引鍵，以防止混淆的副問題。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "identity.nimble.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:nimble:us-west-2:123456789012:studio/*"
        }
      }
    }
  ]
}
```

疑難排解 Amazon 敏捷工作室身分和存取

使用以下資訊協助您診斷和修正使用敏捷工作室和 IAM 時可能會遇到的常見問題。

主題

我沒有在敏捷工作室執行動作的授權。

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 nimble:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 nimble:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 nimble:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 系統管理員。您的管理員提供您的簽署憑證。

我沒有授權執行 iam: PassRole。

如果您收到無權執行iam:PassRole動作的錯誤訊息，請聯絡您的系統管理員以尋求協助。要求他們更新您的政策，以允許您將角色傳遞給靈活工作室。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。若要這麼做，您需要將角色傳遞給服務的權限。

當名為的使用者johndoe嘗試使用主控台在 Nimble Studio 中執行動作時，就會發生下列範例錯誤。但是，動作要求服務具備服務角色授予的許可。John 沒有將角色傳遞給服務的權限。

```
User: arn:aws:iam::123456789012:user/johndoe is not authorized to perform: iam:PassRole
```

在此情況下，John 會要求管理員更新其原則，以授與執行`iam:PassRole`動作的權限。

我想要檢視我的存取金鑰。

Amazon 敏捷工作室不提供訪問密鑰。若要了解秘密存取金鑰，請參閱 IAM 使用者指南中的管理存取金鑰。

> **Important**
>
> 不要向第三方提供您的訪問密鑰，甚至是為了幫助您找到規範的用戶 ID。執行此作業，可能會讓他人能夠永久存取您的帳戶。

當您建立存取 key pair 時，系統會提示您將存取金鑰 ID 和秘密存取金鑰儲存在安全的位置。私密存取金鑰只會在您建立它的時候顯示一次。如果您遺失了密碼存取金鑰，請將新的存取金鑰新增至您的使用者。您最多可以擁有兩個存取金鑰。如果您已有兩個金鑰，請先刪除一個 key pair，然後再建立新金鑰組。若要檢視指示，請參閱《IAM 使用者指南》中的管理存取金鑰。

我是管理員，並希望允許其他人訪問靈活的工作室。

若要允許其他人存取 Nimble Studio，請為需要存取的個人或應用程式建立 IAM 實體 (使用者或角色)。他們將使用該實體的憑證來存取 AWS。然後，將原則附加至授與他們正確權限的實體。

靈活的工作室為您提供了`AmazonNimbleStudio-StudioUser`在 AWS Management Console. 管理主控台的 IT 管理員會使用此原則將 Studio 存取權授予其他人。

如需有關使用管理原則的教學課程，請參閱為靈活的工作室設置指南。若要了解如何將現有政策附加到使用者，例如使用者和啟動設定檔政策，請參閱建立 IAM 使用者 (主控台)。

如需匯入政策的相關資訊，請參閱《IAM 使用者指南》中的「建立第一個 IAM 委派使用者和群組」。

我想允許我以外的人訪問我靈活的工作室資源。 AWS 帳戶

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 要了解靈活工作室是否支持這些功能，請參閱Amazon 靈活工作室如何與 IAM 合作。

- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的提供對外部驗證使用者的存取權 (聯合身分識別)。
- 若要了解跨帳戶存取使用角色和以資源為基礎的政策之間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與以資源為基礎的政策有何不同。

使用敏捷工作室進行安全事件記錄和監控

監控是維持 Amazon Nimble Studio 和您的 AWS 解決方案的可靠性、可用性和效能的重要組成部分。從 AWS 解決方案的所有部分收集監控資料，以便在發生多點故障時，您可以更輕鬆地對多點失敗進行除錯。

AWS 和 Nimble Studio 提供工具，用於監控您的資源並應對潛在事件，包括記錄靈活的工作室通話使用 AWS CloudTrail和AWS CloudFormation 用戶指南。

有 AWS CloudFormation關 Amazon 敏捷工作室如何使用的詳細資訊 (包括 JSON 和 YAML 範本的範例)，請參閱使用者指南中的 Amazon 敏捷工作室資源和屬性參考。 AWS CloudFormation 若要瞭解如何使用 CloudFormation範本，請參閱AWS CloudFormation 概念。

主題

- 記錄靈活的工作室通話使用 AWS CloudTrail

記錄靈活的工作室通話使用 AWS CloudTrail

Amazon 敏捷工作室與服務集成在一起 AWS CloudTrail，該服務可提供用戶，角色或靈活工作室 AWS 服務 中所採取的操作記錄。 CloudTrail 捕獲靈活工作室的所有 API 調用作為事件。擷取的呼叫包括來自靈活工作室主控台的呼叫，以及對 Amazon 敏捷工作室營運的程式碼呼叫。

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 Nimble Studio 的事件。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。使用收集的信息 CloudTrail，您可以確定向 Nimble Studio 提出的請求，提出請求的 IP 地址，提出請求的人員，提出請求的時間以及其他詳細信息。

靈活的工作室信息 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當活動在敏捷工作室中發生時，該活動會與事件歷史記錄中的其他 CloudTrail 事件一起記錄在 AWS 服務 事件中。您可以查看，搜索和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱檢視具有事 CloudTrail 件記錄的事件。

為了持續記錄您的事件 AWS 帳戶，包括敏捷工作室的事件，請創建一個跟踪。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他， AWS 服務 以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。

如需詳細資訊，請參閱下列內容：

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 記錄檔

從多個帳戶接收 CloudTrail 日誌文件

敏捷工作室動作由記錄下來， CloudTrail 並記錄在 Amazon 敏捷工作室 API 參考文獻中。例如，呼叫 GetStudio 和 DeleteStudio 動作會 CreateStudio在 CloudTrail 記錄檔中產生項目。

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

- 要求是使用根使用者登入資料還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項服務提出。

如需詳細資訊，請參閱使CloudTrail 用者識別元素。

了解靈活的工作室日誌文件條目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、

請求參數等資訊。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

此 JSON 範例會顯示三個動作：

- 動作 _1： CreateStudio
- 動作 _2： GetStudio
- 動作 _3： DeleteStudio

```
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:25:49Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:25:49Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "CreateStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "displayName": "Studio Name",
        "studioName": "EXAMPLE-studioName",
```

```
        "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User",
        "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin"
    },
    "responseElements": {},
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:44:25Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:44:25Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "GetStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
```

```
    },
    "responseElements": null,
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:45:14Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:44:14Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "DeleteStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
    },
    "responseElements": {
```

```
        "studio": {
            "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin",
            "displayName": "My New Studio Name",
            "homeRegion": "us-west-2",
            "ssoClientId": "EXAMPLE-ssoClientId",
            "state": "DELETING",
            "statusCode": "DELETING_STUDIO",
            "statusMessage": "Deleting studio",
            "studioEncryptionConfiguration": {
                "keyType": "AWS_OWNED_CMK"
            },
            "studioId": "us-west-2-EXAMPLE-studioId",
            "studioName": "EXAMPLE-studioName",
            "studioUrl": "https://sso111122223333.us-
west-2.portal.nimble.amazonaws.com",
            "tags": {},
            "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User"
        }
    },
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```


在此範例中，您會注意到事件會顯示區域、IP 位址以及其他「requestParameters」(例如「userRoleArn」和「」adminRoleArn)，以協助您識別事件。您可以在「creationDate」中看到時間和日期，以及請求的來源，標記為「事件來源」：「nimble.amazonaws.com」。

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當活動在 IAM 或 AWS STS 中發生時，該活動會與事件歷史記錄中的其他 CloudTrail AWS 服務 事件一起記錄在事件中。您可以查看，搜索和下載最近的事件 AWS 帳戶。

AWS CloudTrail 將 IAM 和 AWS Security Token Service (AWS STS) 的所有 API 呼叫擷取為事件，包括來自主控台和 API 呼叫的呼叫。若要進一步了解如何 CloudTrail 搭配 IAM 使用 AWS STS，請參閱使用記錄 IAM 和 AWS STS API 呼叫 AWS CloudTrail。

若要取得有關的更多資訊 CloudTrail，請參閱AWS CloudTrail 使用指南

如需 Amazon 提供的其他監控服務的相關資訊，請參閱 Amazon CloudWatch 使用者指南。

Amazon 敏捷工作室的合規驗證

Amazon 敏捷工作室遵循共同的責任模式，並與我們的客戶共同合規。 AWS

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 靈活工作室的基礎設施安全

作為一項託管服務，Amazon 敏捷工作室受到 AWS 全球網絡安全的保護。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 已發布的 API 調用通過網絡訪問靈活的工作室。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。

靈活工作室的安全性最佳做法

Amazon Nimble Studio 提供許多安全功能，可在您開發和實作自己的安全政策時考慮。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

監控

監控是維持 Nimble Studio 和您的 AWS 解決方案的可靠性，可用性和性能的重要組成部分。如需監視及回應事件的詳細資訊，請參閱使用敏捷工作室進行安全事件記錄和監控。

資料保護

基於資料保護目的，我們建議您使用 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別帳戶。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。建議使用 TLS 1.2 或更新版本。
- 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 Simple Storage Service (Amazon Simple Storage Service (Amazon S3)) 的個人資料。
- 如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需 FIPS 和 FIPS 端點的詳細資訊，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帳戶號碼等敏感的識別資訊，放在自由格式的欄位中，例如名稱欄位。這包括當您 AWS 服務 使用主控台、API 或軟體開 AWS 發套件與 Amazon 敏捷工作室或其他工作時。 AWS CLI您輸入 Amazon Nimble Studio 或其他服務的任何資料都可能會被選取，以便包含在診斷日誌中。當您提供外部伺服器的 URL 時，請勿在驗證您對該伺服器請求的 URL 中包含登入資料資訊。

許可

使用使用者、IAM 角色管理 AWS 資源存取權，並授予使用者最少的權限。建立憑證管理原則和程序，以建立、散佈、輪換及撤銷 AWS 存取認證。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM 最佳實務。

Support 中心

本節提供了 Nimble Studio 的支持選項，例如在部署或使用服務及其相關應用程序時如何獲得幫助。

目錄

N心 Studio

如果您對靈活工作室有任何疑問，可以訪問靈活工作室論壇。在那裡，您可以從社群和AWS論壇主持人取得有關 Nimble Studio 功能、技術問題和疑難排解說明的解答。

應用支援

敏捷工作室為以下應用程序提供了其他文檔。

AWSThinkboxDeadline

如需彩現農場的說明或瞭解Deadline運作方式，請參閱AWSThinkboxDeadline文件。

N File Transfer

若要瞭解檔案傳輸的運作方式，請參閱靈活的 Studio 檔案傳輸使用者指南。

AWS Support Center

中AWS Support心是建立和管理您的支援案例的中心。它可讓您存取各種資源，包括帳單和技術解決方案、知識中心、知識中心影片、AWS文件，以及訓練與認證。

AWS Support計劃

AWS Support方案可協助您最佳化效能、保持安全、避免停機時間，並控制成本。如需有關AWS Support方案的詳細資訊，請參閱比較AWS Support方案。

有關如何AWS為您提供支持的更多信息，請訪問聯繫我們頁面。

文件歷史紀錄

- API 版本：最新
- 最新文件更新：2023 年 9 月 22 日

下表說明《靈活工作室管理員指南》每個發行版本中的重要變更。

變更	描述	
新的服務與指南	這是亞馬遜敏捷工作室和亞馬遜靈活工作室管理員指南的初始版本。	2023 年 6 月 19 日
AWS 受管政策更新	已更新AmazonNimbleStudio-StudioUser 和AmazonNimbleStudio-StudioAdmin 政策以使用最新版本的AWS IAM Identity Center服務。	2023 年 9 月 22 日

AWS 詞彙表

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

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。