管理員指南

Amazon Nimble Studio

Amazon Nimble Studio: 管理員指南

Table of Contents

支援終止通知：在 2024 年 10 月 22 日， AWS 將停止對 Amazon Nimble Studio 的支援。2024 年 10 月 22 日之後，您將無法再存取 Nimble Studio 主控台或 Nimble Studio 資源。

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。

什麼是 Amazon Nimble Studio？

Nimble Studio 為一組應用程式和服務提供基礎設施和集中式管理，讓藝術家可以用來在雲端產生視覺效果、動畫和遊戲內容。

使用 Nimble Studio，您可以取得使用者和群組管理的必要工具。您也可以新增和管理應用程式，包括 AWS Thinkbox 和 Nimble Studio File Transfer。

Nimble Studio 具有統一的界面，可將您所有的 Studio 資源放在一個位置。您可以加入使用者、指派應用程式，以及連接其任務函數特定的許可。Nimble Studio 不需要 AWS 任何體驗，您可以在大約五分鐘內設定。

目錄

功能和優勢

以下是您透過 Nimble Studio 獲得的一些功能和好處：

- 免費使用 Nimble Studio；只需為您的應用程式使用的 Studio 資源付費。
- 集中管理您的工作室、檢查其狀態，並深入了解其操作。
- 新增和管理 Nimble Studio 應用程式、使用者和群組，並連接許可。
- 使用 AWS Identity and Access Management (IAM) 政策和角色安全地管理對 Studio 資源的存取。
- 使用 AWS IAM Identity Center (IAM Identity Center) 管理 Studio 使用者和外部身分提供者的安全登入。
- 使用 Studio 資源的標籤來整理並輕鬆尋找 Studio 資源。

相關應用程式

Nimble Studio 為數位內容創作者提供應用程式，以操作雲端型工作室來產生視覺效果 (VFX)、動畫和互動式內容。

您可以使用 Amazon Elastic Compute Cloud (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 Simple Storage Service (Amazon S3) 安全地傳輸和存放數位媒體資產。這表示您可以使用 Nimble Studio 來降低實體基礎設施、設備和技術人員的成本。

Nimble Studio 目前提供下列應用程式：

- AWS Thinkbox：Thinkbox軟體包含轉譯陣列管理員Thinkbox截止日期，以及 3D 外掛程式 Thinkbox Krakatoa。您可以使用 Thinkbox 軟體來協助您增加現場部署、使用 Amazon EC2 在雲端或兩者的組合中工作室的創意輸出。如需詳細資訊，請參閱AWS Thinkbox產品。
- Nimble Studio File Transfer：File Transfer加速數位媒體資產往返 Amazon S3 的媒體資產傳輸。File Transfer提供圖形化使用者介面，可用來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。

Nimble Studio 的定價

設定 Nimble Studio 並使用它來管理您的 Studio 基礎設施、使用者、安全性和服務無需付費。

不過，如果您在工作室中設定服務和應用程式，您可能需要支付儲存和其他工作室資源的費用。如需 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。

Nimble Studio 入門

Nimble Studio 設定和部署大約需要五分鐘。

熟悉 Nimble Studio 概念和術語後，請參閱 Amazon Nimble Studio 入門。您可以在其中找到部署 Studio 的step-by-step說明。

Amazon Nimble Studio 的概念和術語

為了協助您開始使用 Amazon Nimble Studio，並了解其運作方式，您可以參閱本指南中的關鍵概念和術語。

主要功能

Amazon Nimble Studio

Amazon Nimble Studio 是一種 AWS 服務 ，可讓創意工作室在從故事板草圖到最終交付項目的雲端中產生完全視覺效果、動畫和互動式內容。

Amazon Nimble Studio 主控台

Nimble Studio 主控台是 的一部分AWS Management Console，專門用於我們的管理 IT 客戶。此主控台可讓管理員建立雲端工作室和管理許多設定。例如，Studio 管理員頁面可讓您新增或移除資源、新增應用程式，以及將許可授予使用者和群組。

Amazon Nimble Studio 入口網站

Nimble Studio 入口網站提供與 Nimble Studio 應用程式和服務day-to-day互動的使用者介面。使用者使用其使用者名稱和密碼直接登入入口網站，而不必與 互動AWS Management Console。

Nimble Studio File Transfer

File Transfer 加速數位媒體資產往返 Amazon Simple Storage Service (Amazon S3) 的媒體資產傳輸。File Transfer提供圖形化使用者介面，可讓您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 軟體包含轉譯陣列管理員Thinkbox截止日期，以及 3D 外掛程式 Thinkbox Krakatoa。您可以使用 Thinkbox 軟體，協助您增加工作室在內部部署、使用 Amazon EC2 的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 受管政策

AWS 受管政策是由 建立和管理的獨立政策 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：aws：iam：：aws：policy/IAMReadOnlyAccess 是 AWS 受管政策。如需 ARN 的詳細資訊，請參閱 IAM ARN。

AWS 受管政策用於將許可授予常見任務函數。引入新的服務和 API 操作 AWS 時， 會維護和更新任務函數政策。例如，AdministratorAccess 工作職能提供對 AWS中的每個服務和資源的完整存取權和許可委派。但 AmazonMobileAnalyticsWriteOnlyAccess 和 AmazonEC2ReadOnlyAccess 等部分存取 AWS 受管政策可以提供特定層級的存取， AWS 服務 而無需允許完整存取。如需存取政策的詳細資訊，請參閱了解政策摘要中的存取層級摘要。

AWS Management Console

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

每個服務也包含自己的主控台。這些主控台提供雲端運算的各種工具。甚至還有一項服務可協助計費和成本管理。

AWS IAM Identity Center (IAM Identity Center)

IAM Identity Center 是一項 AWS 服務，可讓您輕鬆集中管理對多個 AWS 帳戶 和 商業應用程式的存取。透過 IAM Identity Center，您可以從單一位置提供使用者所有指派帳戶和應用程式的單一登入存取權。您也可以集中管理 中所有帳戶的多帳戶存取和使用者許可 AWS Organizations。如需詳細資訊，請參閱AWS IAM Identity Center FAQs。

AWS PrivateLink

AWS PrivateLink 可在 VPCs AWS 服務和內部部署網路之間提供私有連線，而不會將您的流量暴露到公有網際網路。 AWS PrivateLink 可讓您輕鬆地跨不同帳戶和 VPCs 連接服務。 AWS PrivateLink 可按月收費，費用由 支付 AWS 帳戶。

數位內容建立 (DCC)

數位內容建立 (DCC) 是指用於產生創意內容的應用程式類別，包括 Blender、Nuke、 Maya和 Houdini。

區域

Nimble Studio 提供 11 AWS 區域 個選擇部署您的 Studio 的選項。區域是必要 Studio 基礎設施的存在，例如您的資料和應用程式。

該區域應位於最接近您 Studio 使用者的位置。這可降低延遲並改善資料傳輸速度。

Studio

Studio 是其他 Nimble Studio 相關資源的最上層容器。您的雲端工作室會管理 Nimble Studio Web 入口網站，以及與 中基本資源的連線， AWS 帳戶 例如 VPC、使用者目錄和儲存加密金鑰。

Studio 應用程式

Studio 元件是客戶 Nimble Studio 內的組態，告知服務如何存取 檔案系統、授權伺服器和 中的轉譯陣列等資源 AWS 帳戶。

Nimble Studio 包含許多 Studio 元件的子類型，包括共用檔案系統、運算陣列、Active Directory 和授權元件。這些子類型說明您希望工作室使用的資源。

Studio 資源

Studio 資源一詞會封裝 Studio 在日常操作中需要的物件。當描述資源如何融入雲端工作室的基礎設施時，它們也可能稱為工作室元件。

Tags (標籤)

標籤是您指派給 AWS 資源的標籤。每個標籤都包含您定義的金鑰和選用值。

標籤可讓您以不同的方式分類 AWS 資源。例如，您可以為帳戶的 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體定義一組標籤，協助您追蹤每個執行個體的擁有者和堆疊層級。標籤也可讓您整合組織的共用檔案系統，並將陣列轉譯為 Nimble Studio，讓您在將人力資源移至雲端時，工作流程不會中斷。

使用標籤，您可以依用途、擁有者或環境來分類 AWS 資源。當您有許多相同類型的資源時，這會很有用，您可以根據您指派給該資源的標籤快速識別特定資源。

設定 Nimble Studio

本教學課程適用於想要設定 Amazon Nimble Studio 的管理員使用者。

以下各節將引導您在 Nimble Studio 部署 Studio 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 身分登入您的 ，以完成剩餘的設定。

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個 。

註冊 AWS 帳戶

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

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

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

建立具有管理存取權的使用者

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

保護您的 AWS 帳戶根使用者

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

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

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

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的啟用 AWS IAM Identity Center。

2. 在 IAM Identity Center 中，將管理存取權授予使用者。

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

以具有管理存取權的使用者身分登入

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

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

指派存取權給其他使用者

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

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

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

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

相關資源

- IAM 中的安全最佳實務
- AWS 服務 配額 - AWS 一般參考

Amazon Nimble Studio 入門

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

如需初次 AWS 使用的客戶，請參閱設定 Nimble Studio教學課程。

主題

- 設定 Nimble Studio
- 其他 Studio 設定

設定 Nimble Studio

本指南說明如何設定您的基礎設施、檢閱您的設定，以及建立您的工作室。您也可以使用 自訂您的 Studio其他 Studio 設定。

步驟 1：設定 Studio 基礎設施

您工作室的基礎設施包含下列元件：

- Studio 顯示名稱：Studio 顯示名稱是您識別 Studio 的方式，例如 AnyCompany Studio。您的 Studio 名稱也會決定您的 Studio 入口網站 URL。完成設定後，您可以隨時變更 Studio 顯示名稱。
- Studio 入口網站 URL：您可以使用 Studio 入口網站 URL 存取您的 Studio。URL 是以 Studio 顯示名稱為基礎，例如 https://anycompanystudio.awsapps.com。完成設定後，您可以隨時變更 Studio 入口網站 URL。
- AWS 區域： AWS 區域是 AWS 資料中心集合的實體位置。當您設定 Studio 時，區域預設為離您最近的位置。您應該變更 區域，讓它距離您的使用者最接近。這可降低延遲並改善資料傳輸速度。

> **Important**
>
> 在完成設定 Nimble Studio 之後，您無法變更您的區域。

完成本節中的任務，以設定您工作室的基礎設施。

設定 Studio 的基礎設施

1. 登入 AWS Management Console並開啟 Nimble Studio 主控台。
2. 選擇設定 Nimble Studio，然後選擇下一步。
3. 輸入 Studio 顯示名稱 - 例如 **AnyCompany Studio**。
4. （選用）若要變更 Studio 入口網站名稱，請選擇編輯 URL。
5. （選用）若要變更AWS 區域最接近您 Studio 使用者的 ，請選擇變更區域。
   a. 選取最接近您使用者的 區域。
   b. 選擇套用區域。
6. （選用）若要進一步自訂您的 Studio 設定，請選取 其他 Studio 設定。
7. 若要在建立工作室之前檢閱設定，請選擇下一步。

步驟 2：檢閱和建立您的工作室

設定工作室的基礎設施後，您可以檢閱、變更和建立工作室。

若要檢閱和建立您的 Studio

1. 在檢閱和建立頁面上，檢閱您的 Studio 基礎設施。
2. 確認 AWS 區域 最接近您的 Studio 使用者。
3. （選用）選擇編輯以變更您的 Studio 設定。
4. 當您準備好時，請選擇建立工作室。

其他 Studio 設定

Nimble Studio 設定包含其他 Studio 設定。透過這些設定，您可以檢視 Nimble Studio 設定對 所做的所有變更 AWS 帳戶、設定您的 Studio 使用者角色，以及變更加密金鑰類型。您也可以將選用標籤新增至您的 Studio 資源。

設定 Studio 使用者角色

AWS 服務可以擔任服務角色來代表您執行動作。Nimble Studio 需要 Studio 使用者角色，才能讓使用者存取您 Studio 中的資源。

您可以將 AWS Identity and Access Management (IAM) 受管政策連接至 Studio 使用者角色。這些政策允許使用者執行特定動作，例如在特定 Nimble Studio 應用程式中建立任務。由於應用程式取決於受管政策中的特定條件，因此如果您不使用受管政策，應用程式可能無法如預期般執行。

完成設定後，您可以隨時變更 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個不同使用案例的說明。若要建立和使用新的服務角色，請選擇新增服務角色索引標籤。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

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. （選用）輸入服務使用者角色名稱。
3. 選擇檢視許可詳細資訊以取得角色的詳細資訊。

Existing service role

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. （選用）選擇 IAM 主控台中的檢視，以取得角色的詳細資訊。

AWS IAM Identity Center

AWS IAM Identity Center 是以雲端為基礎的單一登入服務，用於管理使用者和群組。IAM Identity Center 也可以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。

Nimble Studio 預設會啟用 IAM Identity Center，而且必須設定和使用 Nimble Studio。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) 金鑰是 KMS 金鑰的主要類型，可用來加密、解密和重新加密您的資料。

Nimble Studio 包含下列 AWS KMS 加密金鑰類型：

- AWS 擁有的金鑰 - AWS 擁有的金鑰是 AWS 服務 擁有和管理的 KMS 金鑰，用於多個 AWS 帳戶。AWS 擁有的金鑰並不位於您的 中 AWS 帳戶，但 Nimble Studio 可以使用 AWS 擁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 擁有的金鑰是免費的，它們不會計入 AWS KMS 您 的配額 AWS 帳戶。

- 客戶受管 AWS KMS 金鑰 – 客戶受管金鑰是您建立、擁有和管理的 中的 KMS AWS 帳戶 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費用。對於 AWS KMS 超出免費方案的每個 API 請求，也會產生費用。如需 AWS KMS 定價的詳細資訊，請參閱AWS Key Management Service 定價。

加密金鑰類型無法在您完成設定後變更。如需 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. 選取選擇不同的 AWS KMS 金鑰 （進階）。
2. 選取 AWS KMS 金鑰或輸入 Amazon 資源號碼 (ARN)。
3. 選擇建立 AWS KMS 金鑰。

設定標籤

標籤可做為組織 Nimble Studio 資源的標籤。您最多可以新增 50 個標籤來識別、組織、篩選和搜尋資源。

每個標籤都包含兩個部分，您定義：標籤索引鍵和選用的標籤值 — 例如索引鍵： `domain`和值：`anycompanystudio.com`。

您可以在完成設定後，隨時新增或移除標籤。如需標籤的詳細資訊，請參閱標記您的 AWS 資源。

將標籤新增至您的 Studio 資源

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

刪除工作室

如果您不再需要 Studio，則可以將其刪除。當您刪除工作室時，只會刪除工作室基礎設施。您的其他 AWS 資源，例如使用者角色、政策和應用程式資料，都保持不變。

> **Important**
>
> 刪除 Studio 之後，就無法還原它。

刪除您的 Studio

1. 登入 AWS Management Console 並開啟 Nimble Studio 主控台。
2. 選取 Studio 概觀。
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

的雲端安全 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了滿足最安全敏感組織的需求而建置。

安全是 AWS 和 之間的共同責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。第三方稽核人員會定期測試和驗證我們安全的有效性，做為AWS 合規計畫的一部分。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。
- 雲端安全性 – 您的責任取決於您使用 AWS 的服務。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 Security Pillar - AWS Well-Architected Framework。本文包含保護 AWS 基礎設施的重要原則。

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。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Nimble Studio資源。

詳細資訊

- Security Pillar - AWS Well-Architected Framework
- AWS Cloud Development Kit (AWS CDK) (AWS CDK) 的安全性
- Amazon Virtual Private Cloud 的安全性
- AWS 安全登入資料
- 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 AWS 帳戶 ，以便在資源遭到入侵時接收通知，並允許特定 AWS 帳戶 使用者存取。若要保護您的 AWS 帳戶 並追蹤您的 資源，請完成下列步驟。

目錄

刪除您帳戶的存取金鑰

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

如果您仍然有存取金鑰，我們建議您刪除這些金鑰並建立使用者。然後，僅授予該使用者您計劃呼叫 APIs 所需的許可。您可以使用該使用者來發行存取金鑰。

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

啟用多重因素認證

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

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能夠實際存取的額外資訊。此資訊可能來自專用 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 裝置存放在安全的位置。

如果您使用虛擬 MFA 裝置 （例如手機應用程式），請考慮如果手機遺失或損壞，可能會發生什麼情況。其中一種方法是將您使用的虛擬 MFA 裝置存放在安全的地方。另一個選項是同時啟用多個裝置，或使用虛擬 MFA 選項進行裝置金鑰復原。

若要進一步了解 MFA，請參閱啟用虛擬Multi-Factor Authentication (MFA) 裝置。

相關資源

- 多重要素驗證入門

- AWS 使用 MFA 保護對 的存取

在所有 中啟用 CloudTrail AWS 區域

您可以使用 追蹤 AWS 資源中的所有活動AWS CloudTrail。建議您現在開啟 CloudTrail。這有助於 支援 和您的 AWS 解決方案架構師稍後對安全或組態問題進行故障診斷。

若要在所有區域中啟用 CloudTrail 記錄 AWS 區域，請參閱AWS CloudTrail 更新 – 在所有區域中開啟並使用多個線索。

若要進一步了解 CloudTrail，請參閱在您的 中開啟 CloudTrail：記錄 API 活動 AWS 帳戶。若要了解 CloudTrail 如何監控 Nimble Studio，請參閱 使用 記錄 Nimble Studio 呼叫 AWS CloudTrail。

設定 Amazon GuardDuty 和通知

Amazon GuardDuty 是一種持續的安全監控服務，可分析和處理下列項目：

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

Amazon GuardDuty 可識別您 AWS 環境中的非預期和可能未經授權的惡意活動。惡意活動可能包括權限提升、使用公開憑證，或與惡意 IP 地址或網域通訊等問題。為了識別這些活動，GuardDuty 會使用威脅情報摘要，例如惡意 IP 地址和網域清單，以及機器學習。例如，GuardDuty 可以偵測遭入侵的 Amazon EC2 執行個體，提供惡意軟體或挖礦比特幣。

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設施部署，例如在中部署 AWS 區域 且從未使用的執行個體。它還包括不尋常的 API 呼叫，例如密碼政策變更，以減少密碼強度。

GuardDuty 透過產生安全調查結果，通知您 AWS 環境的狀態。您可以在 GuardDuty 主控台或透過 Amazon CloudWatch 事件檢視這些調查結果。

設定 Amazon SNS 主題和端點

請遵循設定 Amazon SNS 主題和端點教學中的指示。

為 GuardDuty 調查結果設定 EventBridge 事件

為 EventBridge 建立規則，以傳送 GuardDuty 產生之所有調查結果的事件。

為 GuardDuty 調查結果建立 EventBridge 事件

1. 登入 Amazon EventBridge 主控台：https：//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. 輸入新規則的名稱和描述。然後選擇下一步。
4. 保留為事件來源選取的事件AWS 或 EventBridge 合作夥伴事件。
5. 在事件模式中，選擇事件來源AWS 的服務。然後， AWS 服務的 GuardDuty 和事件類型的 GuardDuty Finding。這是您在 中建立的主題設定 Amazon SNS 主題和端點。
6. 選擇 Next (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 GuardDuty_to_Email 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轉換器。選取設定輸入轉換器。
9. 在目標輸入轉換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 Create (建立)。然後選擇下一步。
12. （選用）如果您使用標籤來追蹤 AWS 資源，請新增標籤。

13. 選擇 Next (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，您可以授予特定使用者的存取權，並在資源遭到入侵時收到通知。

Amazon Nimble Studio 中的資料保護

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

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

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Nimble Studio 或其他 AWS 服務 使用 主控台、API AWS CLI或 AWS SDKs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。

AWS 共同責任模型適用於 Amazon Nimble Studio 中的資料保護。如此模型所述， AWS 負責保護執行所有 的全域基礎設施 AWS 雲端。您需負責控制在此基礎設施上託管的內容。此內容包含 AWS 服務您使用之 的安全組態和管理任務。

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。如需有關歐盟資料保護的資訊，請造訪 GDPR 中心。

靜態加密

Nimble Studio 使用存放在 AWS Key Management Service (AWS KMS) 中的加密金鑰，透過靜態加密來保護敏感的 Studio 資料。所有可使用 Nimble Studio AWS 區域 的 都可以使用靜態加密。我們加密的 Studio 資料包含所有資源類型的名稱和描述，以及 Studio 元件指令碼、指令碼參數、掛載點、共用名稱和其他資料。

加密資料表示在沒有有效金鑰的情況下，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靜態存放，而且只能由有權存取受管金鑰的一方解密。

如需 Nimble Studio 如何使用 AWS KMS 加密靜態資料的資訊，請參閱 Amazon Nimble Studio 的金鑰管理。

將授予與 AWS KMS 金鑰搭配使用

授予是允許AWS 主體在密碼編譯操作中使用 AWS KMS 金鑰的政策工具。它也可以讓他們使用命令檢視 KMS 金鑰`DescribeKey`，並建立和管理授予。

與 整合 AWS 服務 的 通常使用 授予 AWS KMS 來加密靜態資料。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 Nimble Studio 建立您的 Studio 時，我們為 Nimble Studio 入口網站使用者提供兩個角色：使用者和管理員角色。Nimble Studio 會為這些角色建立客戶受管金鑰的授予，讓他們能夠存取 Studio 加密資料。

> **Important**
>
> 如果您刪除授予，Nimble Studio 入口網站將無法使用於使用者，直到管理員建立新的授予為止。

如需 AWS 服務 如何使用授與的詳細資訊，請參閱服務使用者指南或開發人員指南中的 AWS 服務 如何使用 AWS KMS 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。如適用，也會列出 Nimble Studio 的其他資料保護方法。

資料	網路路徑	保護

Web 資產，例如映像和 JavaScript 檔案	網路路徑介於 Nimble Studio 使用者和 Nimble Studio 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	網路路徑介於 Nimble Studio 使用者和 Nimble Studio 之間。	使用 256 位元進階加密標準 (AES-256) 加密，並使用 TLS 1.2 或更新版本傳輸。
API 流量	路徑介於 Nimble Studio 使用者和 Nimble Studio 之間。	使用 TLS 1.2 或更新版本加密。建立連線的請求會使用 SigV4 簽署。

Amazon Nimble Studio 的金鑰管理

建立新的 Studio 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。金鑰由 Nimble Studio 擁有 （不收取額外費用）。
- 客戶受管 KMS 金鑰 – 金鑰存放在您的帳戶中，由您建立、擁有和管理。您可以完全控制 key. AWS KMS charges。

在 AWS Key Management Service (AWS KMS) 中刪除客戶受管的 KMS 金鑰具有破壞性且可能危險。它會不可逆地刪除與金鑰相關聯的金鑰材料和所有中繼資料。刪除客戶受管 KMS 金鑰後，您無法再解密該金鑰加密的資料。這表示資料無法復原。

這就是為什麼在刪除金鑰之前， AWS KMS 會給予客戶最多 30 天的等待期。預設等待期間為 30 天。

關於等待期

由於刪除客戶受管 KMS 金鑰具有破壞性和潛在危險性，因此我們會要求您設定 7 – 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。若要取得要刪除金鑰的實際日期和時間，請使用 DescribeKey 操作。您也可以在金鑰的詳細資訊頁面的 AWS KMS 主控台中，於一般組態區段中查看金鑰的排程刪除日期。請注意時區。

在等待期間，客戶受管金鑰的狀態和金鑰狀態為待刪除。

- 待刪除的客戶受管 KMS 金鑰無法用於任何密碼編譯操作。

- AWS KMS 不會輪換待刪除之客戶受管金鑰的後端 AWS KMS 金鑰。

如需刪除客戶受管 AWS KMS 金鑰的詳細資訊，請參閱刪除客戶主金鑰。

資料安全措施

基於資料保護目的，建議您保護 AWS 帳戶 登入資料，並使用 AWS Identity and Access Management (IAM) 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 中的所有預設安全控制 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。

我們強烈建議您絕對不要將敏感的識別資訊，例如客戶帳戶號碼，放入任意格式欄位，例如名稱欄位。這包括當您使用 Amazon Nimble Studio 或其他 AWS 服務 使用 主控台、API、 AWS CLI或 AWS SDKs 時。您在 Amazon Nimble Studio 或其他 服務中輸入的任何資料都可能被挑選納入診斷日誌中。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 StudioBuilder 期間，Amazon Nimble Studio 會收集特定指標，用於診斷問題並改善 Nimble Studio 的功能和使用者體驗。

收集的指標類型

- 用量資訊 – 執行的一般命令和子命令。
- 錯誤和診斷資訊 – 執行中命令的狀態和持續時間，包括結束代碼、內部例外名稱和失敗。
- 系統和環境資訊 – Python 版本、作業系統 (Linux、 Windows或 macOS)，以及執行 StudioBuilder 的環境。

Amazon Nimble Studio 的身分和存取管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。管理員可控制誰可以進行身分驗證 （ 登入 ） 和授權 （ 具有許可 ） 來使用 Amazon Nimble Studio 資源。IAM 是 AWS 服務 您可以免費使用的 。

主題

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，取決於您在 Nimble Studio 中執行的工作。

服務使用者 – 如果您使用 Nimble Studio 服務來執行任務，則您是服務使用者。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登入資料和許可。當您使用更多 Nimble Studio 功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 Nimble Studio 中的功能，請參閱 對 Amazon Nimble Studio 身分和存取進行故障診斷。

服務管理員 – 如果您在公司負責 Nimble Studio 資源，您可能可以完整存取 Nimble Studio。您的任務是判斷員工應存取哪些 Nimble Studio 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許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何搭配 Nimble Studio 使用 IAM，請參閱Amazon Nimble Studio 如何與 IAM 搭配使用。

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。如需使用 登入的詳細資訊 AWS Management Console，請參閱《IAM 使用者指南》中的以 IAM 使用者或根使用者 AWS Management Console 身分登入 。

您需要以 AWS 帳戶 根使用者、使用者或擔任 IAM 角色身分進行身分驗證 （ 登入 AWS)。您也可以使用公司的單一登入身分驗證，甚至使用 Google 或 Facebook 登入。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 使用其他公司的登入資料存取 時，您會間接擔任 角色。

若要直接登入 AWS Management Console，請使用您的密碼搭配您的根使用者電子郵件地址或使用者名稱。您可以使用根使用者或使用者存取 AWS 金鑰，以程式設計方式存取 。

AWS 提供 SDK 和命令列工具，以密碼編譯方式使用您的登入資料簽署請求。如果您不使用 AWS 工具，請自行簽署請求。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。如需驗證請求的詳細資訊，請參閱 中的簽章第 4 版簽署程序 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) 來提高帳戶的安全性。若要進一步了解，請參閱《IAM 使用者指南》中的使用多重要素驗證 (MFA) AWS。

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，該身分可完整存取 帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 Theroot 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要將根使用者用於日常任務，即使是管理任務。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 中具有單一人員或應用程式特定許可 AWS 帳戶 的身分。使用者可以擁有長期憑證或一組存取金鑰。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金鑰對。您未來無法復原秘密存取金鑰。反之，會產生新的存取金鑰對。

IAM 群組是指定使用者集合的身分。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，但角色僅提供臨時憑證。若要進一步了解，請參閱《IAM 使用者指南》中的何時建立使用者 （ 而非角色 ）。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似於使用者，但與特定人員沒有關聯。您可以 AWS Management Console 切換角色，暫時在 中擔任 IAM 角色。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色方法的詳細資訊，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。
- 聯合身分使用者存取 – 您可以使用來自 AWS Directory Service企業使用者目錄或 Web 身分提供者的現有身分，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 使用名為 'membership' 的概念，為使用者提供特定啟動設定檔的存取權。成員資格可讓 Studio 管理員將資源存取權委派給使用者，而不必撰寫或了解 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，該使用者有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。服務角色只會在您的 帳戶中提供存取權，無法用來授予其他帳戶中服務的存取權。管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以將許可委派給 AWS 服務 。
  - 服務連結角色 – 服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。Nimble Studio 不支援服務連結角色。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體，並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色將許可授予在 Amazon EC2 執行個體上執行的應用程式。

若要了解如何使用 IAM 角色或使用者，請參閱《IAM 使用者指南》中的何時建立 IAM 角色 （ 而非使用者 ）。

使用政策管理存取權

您可以透過建立政策並將其連接至 IAM 身分或 AWS 資源 AWS 來控制 中的存取。政策是 中的物件， AWS 當與身分或資源建立關聯時， 會定義其許可。您可以以根使用者身分登入，也可以擔任 IAM 角

色。然後，當您提出請求時， 會 AWS 評估相關的身分型或資源型政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個委託人可以對哪些資源以及哪些條件執行動作。

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。具有該政策的使用者可以從 AWS Management Console AWS CLI、 或 AWS API 取得角色資訊。

身分型政策

以身分為基礎的政策是 JSON 許可政策文件，您可以連接到身分，例如使用者、使用者群組或角色。這些政策控制使用者和角色可以執行的動作、資源以及條件。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。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。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》中的在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。對於附加政策的資源，政策會定義指定主體可以對該資源執行的動作，以及針對哪些條件執行的動作。在資源型政策中指定委託人。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

Nimble Studio 中的存取控制清單 (ACLs)

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACLs 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 AWS WAF和 Amazon VPC 是支援 ACLs的服務範例。如需進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

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

- 許可界限 – 許可界限是一種進階功能，您可以在其中設定身分型政策可授予 IAM 實體 （使用者或角色） 的最大許可。您可以為實體設定許可界限。產生的許可是實體身分型政策及其許可界限的交集。在 `Principal` 欄位中指定使用者或角色的資源型政策不受許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱《IAM 使用者指南》中的 IAM 實體的許可界限。
- 服務控制政策 SCPs) – SCPs是 JSON 政策，可在 Organizations 中指定組織或組織單位 (OU) 的最大許可。Organizations 是一項服務，用於分組和集中管理企業擁有 AWS 帳戶 的多個 。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個 AWS 帳戶 根使用者。如需 Organizations 和 SCPs的詳細資訊，請參閱 AWS Organizations 使用者指南中的 SCPs運作方式。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱《IAM 使用者指南》中的工作階段政策。

多種政策類型

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

Amazon Nimble Studio 如何與 IAM 搭配使用

使用 IAM 管理 Nimble Studio 的存取權之前，請先了解哪些 IAM 功能可與 Nimble Studio 搭配使用。

您可以搭配 Amazon Nimble Studio 使用的 IAM 功能

IAM 功能	Nimble Studio 支援
Nimble Studio 的政策動作	是
Nimble Studio 的政策資源	是

IAM 功能	Nimble Studio 支援
Nimble Studio 的政策條件索引鍵	是
Nimble Studio 中的存取控制清單 (ACLs)	否
使用 Nimble Studio 的屬性型存取控制 (ABAC)	是
搭配 Nimble Studio 使用臨時憑證	是
Nimble Studio 的跨服務主體許可	是
Nimble Studio 的服務角色	是
Nimble Studio 的服務連結角色	否

若要深入了解 Nimble Studio 和其他 如何與大多數 IAM 功能 AWS 服務 搭配使用，請參閱《AWS 服務 IAM 使用者指南》中的 與 IAM 搭配使用。

Nimble Studio 的身分型政策

支援身分型政策	是

以身分為基礎的政策是 JSON 許可政策文件，您可以連接到身分，例如使用者、使用者群組或角色。這些政策控制使用者和角色可以執行的動作、資源以及條件。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。

透過 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。您無法在身分型政策中指定委託人，因為它適用於其連接的使用者或角色。若要了解您可以在 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。

Amazon Nimble Studio 的身分型政策範例

若要檢視 Nimble Studio 身分型政策的範例，請參閱 Amazon Nimble Studio 的身分型政策範例。

Nimble Studio 中的資源型政策

支援以資源基礎的政策	否

Nimble Studio 不支援以資源為基礎的政策或跨帳戶存取。資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定主體可以對該資源執行的動作，以及針對哪些條件執行的動作。在資源型政策中指定委託人。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

Nimble Studio 的政策動作

支援政策動作	是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個委託人可以對哪些資源以及哪些條件執行動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API 操作相同的名稱。有一些例外狀況，例如沒有相符 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 Nimble Studio 動作清單，請參閱服務授權參考中的 Amazon Nimble Studio 定義的動作。

Nimble Studio 中的政策動作在動作之前使用下列字首：

```
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"
         ]
```

若要檢視 Nimble Studio 身分型政策的範例，請參閱 Amazon Nimble Studio 的身分型政策範例。

Nimble Studio 的政策資源

支援政策資源	是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個委託人可以對哪些資源以及哪些條件執行動作。

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

對於不支援資源層級許可的動作，例如列出操作，請使用萬用字元 (*) 表示陳述式適用於所有資源。

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

若要檢視 Nimble Studio 身分型政策的範例，請參閱 Amazon Nimble Studio 的身分型政策範例。

Nimble Studio 的政策條件索引鍵

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內容。也就是說，哪個委託人可以對哪些資源以及哪些條件執行動作。

Condition 元素 （或 Condition`**block**) lets you specify conditions in which a statement is in effect. The `Condition元素是選用的。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。在授予陳述式的許可之前，必須符合所有條件。

您也可以在指定條件時使用預留位置變數。例如，只有在使用者使用使用者名稱標記時，您才能授予使用者存取資源的許可。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 支援全域條件索引鍵和服務特定條件索引鍵。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。

若要檢視 Nimble Studio 身分型政策的範例，請參閱 Amazon Nimble Studio 的身分型政策範例。

Nimble Studio 中的存取控制清單 (ACLs)

支援 ACL	否

Nimble Studio 不支援存取控制清單 ACLs)。ACLs控制哪些主體 （帳戶成員、使用者或角色） 具有存取資源的許可。ACLs 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。

使用 Nimble Studio 的屬性型存取控制 (ABAC)

支援 ABAC (政策中的標籤)	是

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在 中 AWS，這些屬性稱為標籤。您可以將標籤連接至 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，您可以設計 ABAC 政策，以便在主體的標籤符合其嘗試存取之資源上的標籤時允許操作。

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《IAM 使用者指南》中的什麼是 ABAC？。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》中的使用屬性型存取控制 (ABAC)。

搭配 Nimble Studio 使用臨時憑證

支援臨時憑證	是

當您使用臨時登入資料登入時，有些 AWS 服務 無法使用。如需詳細資訊，包括哪些 AWS 服務 使用臨時登入資料，請參閱《AWS 服務 IAM 使用者指南》中的 使用 IAM。

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入 ，則會使用臨時登入資料。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取 時，該程序會自動建立臨時登入資料。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的切換到角色 （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。

Nimble Studio 的跨服務主體許可

支援主體許可	是

Nimble Studio 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。服務角色只會在您的 帳戶中提供存取權，無法用來授予其他帳戶中服務的存取權。管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以將許可委派給 AWS 服務 。

> **Warning**
>
> 變更服務角色的許可可能會中斷 Nimble Studio 功能。只有在 Nimble Studio 提供指引時，才能編輯服務角色。

Nimble Studio 的服務連結角色

支援服務連結角色。	否

Nimble Studio 不支援服務連結角色。服務連結角色是連結至 的服務角色類型 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，請參閱 AWS 服務 與 IAM 搭配使用。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 Nimble Studio 的身分型政策範例

根據預設，使用者和角色沒有建立或修改 Nimble Studio 資源的許可。他們也無法使用 AWS Management Console AWS CLI或 AWS API 來執行任務。管理員必須建立 IAM 政策，授予使用者和角色對所需資源執行動作的許可。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範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的在 JSON 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。他們會判斷是否有人可以在您的帳戶中建立、存取或刪除 Nimble Studio 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 受管政策為您的員工提供所需的許可。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》中的使用許可搭配 AWS 受管政策。
- 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。
- 為敏感操作啟用 MFA – 為了提高安全性， 要求使用者使用多重要素驗證 (MFA) 來存取敏感資源或 API 操作。如需詳細資訊，請參閱《IAM 使用者指南》中的在 中使用多重要素驗證 (MFA) AWS。
- 使用政策條件來提高安全性 – 在實際可行的範圍內，定義以身分為基礎的政策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 使用者指南》中的 IAM JSON 政策元素：條件。

AWS Amazon Nimble Studio 的 受管政策

若要將許可新增至使用者、群組和角色，使用 AWS 受管政策比自行撰寫政策更容易。建立 IAM 客戶受管政策需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可以使用我們的 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中使用。如需受 AWS 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 受管政策。您無法變更 AWS 受管政策中的許可。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管政策中移除許可，因此政策更新不會破壞現有的許可。

此外， AWS 支援跨多個 服務之任務函數的受管政策。例如，ReadOnlyAccess AWS 受管政策提供所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時， 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。

您的最終使用者將主要使用 Nimble Studio 入口網站存取 Amazon Nimble Studio。使用 StudioBuilder 或 Nimble Studio 主控台建立您的 Studio 時，會為每個 Studio 角色建立一個 IAM 角色：Studio 管理員

和 Studio 使用者。每個 都已連接各自的 IAM 受管政策。Nimble Studio 入口網站提供一種體驗，使用者只能列出和使用他們有權存取的資源。

Nimble Studio 入口網站提供一種體驗，使用者只能列出和使用他們有權存取的資源，而入口網站取決於這些政策的內容來正確運作。Nimble Studio 最終使用者將使用 入口網站存取其雲端工作室。因此，當管理員使用 StudioBuilder 建立其工作室時，每個需要存取工作室的人員都會建立一個 IAM 角色。這包括 Studio 管理員和 Studio 使用者，每個都連接各自的 IAM 受管政策。

如需任務函數政策的清單和說明，請參閱《IAM 使用者指南》中的AWS 任務函數的受管政策。

AWS 受管政策： **AmazonNimbleStudio-LaunchProfileWorker**

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

將此政策連接至 Nimble Studio Builder 建立的 EC2 執行個體，以授予 Nimble Studio 啟動描述檔工作者所需資源的存取權。

許可詳細資訊

此政策包含以下許可。

- ds - 允許 LaunchProfile 工作者探索與 LaunchProfile AWS Managed Microsoft AD 相關聯的 連線資訊。
- ec2 - 允許 LaunchProfile 工作者探索安全群組和子網路資訊，以連線至 LaunchProfile。
- fsx - 允許 LaunchProfile 工作者探索與 LaunchProfile 相關聯的 Amazon FSx 磁碟區的連線資訊。

```
{
  "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 受管政策： **AmazonNimbleStudio-StudioAdmin**

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

將此政策附加至與您 Studio 相關聯的管理員角色，以授予與 Studio 管理員相關聯的 Amazon Nimble Studio 資源和其他 服務中的相關 Studio 資源的存取權。

許可詳細資訊

此政策包含以下許可。

- nimble - 允許 Studio 使用者存取 StudioAdmins 委派給他們的 Nimble 資源。
- sso - 允許 Studio 使用者檢視 Studio 中其他使用者的名稱。
- identitystore - 允許 Studio 使用者檢視 Studio 中其他使用者的名稱。
- ds - 允許 Nimble Studio 將虛擬工作站新增至與 Studio AWS Managed Microsoft AD 相關聯的 。
- ec2 - 允許 Nimble Studio 將虛擬工作站連接到您設定的 VPC。
- fsx - 允許 Nimble Studio 將虛擬工作站連接到您設定的 Amazon FSx 磁碟區。
- cloudwatch - 允許 Nimble Studio 擷取 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 受管政策： **AmazonNimbleStudio-StudioUser**

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

將此政策附加至與您 Studio 相關聯的使用者角色，以授予與其他服務中 Studio 使用者和相關 Studio 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。

- nimble - 允許 Studio 使用者存取 StudioAdmins 委派給他們的 Nimble 資源。

- sso - 允許 Studio 使用者檢視 Studio 中其他使用者的名稱。
- identitystore - 允許 Studio 使用者檢視 Studio 中其他使用者的名稱。
- ds - 允許 Nimble Studio 將虛擬工作站新增至與 Studio AWS Managed Microsoft AD 相關聯的 。
- ec2 - 允許 Nimble Studio 將虛擬工作站連接到您設定的 VPC。
- fsx - 允許 Nimble Studio 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"
}
```

受管政策的 AWS Nimble Studio 更新

檢視自此服務開始追蹤這些變更以來，Amazon Nimble Studio AWS 受管政策更新的詳細資訊。

變更	描述	日期
AWS 受管政策： AmazonNimbleStudio-StudioUser - 更新的政策	Amazon Nimble Studio 已更新政策，以使用最新版本的 Identity Store 服務。	2023 年 9 月 22 日
AWS 受管政策： AmazonNimbleStudio-StudioAdmin - 更新的政策	Amazon Nimble Studio 已更新政策，以使用最新版本的 Identity Store 服務。	2023 年 9 月 22 日
AWS 受管政策： AmazonNimbleStudio-StudioUser - 更新的政策	Amazon Nimble Studio 已更新政策，以允許 Studio 使用者檢視其工作站備份。	2022 年 12 月 20 日
AWS 受管政策： AmazonNimbleStudio-StudioAdmin - 更新的政策	Amazon Nimble Studio 已更新政策，允許 Studio 管理員檢視其工作站備份。	2022 年 12 月 20 日
AWS 受管政策： AmazonNimbleStudio-StudioUser - 更新的政策	Amazon Nimble Studio 已更新政策，允許 Studio 管理員擷取 CloudWatch 指標。	2021 年 11 月 11 日
AWS 受管政策： AmazonNimbleStudio-StudioUser - 更新的政策	Amazon Nimble Studio 已更新政策，以允許 Studio 使用者啟動和停止其工作站。	2021 年 11 月 1 日
AWS 受管政策： AmazonNimbleStudio-StudioAdmin - 更新的政策	Amazon Nimble Studio 已更新政策，允許 Studio 管理員啟動和停止其工作站。	2021 年 11 月 1 日

變更	描述	日期
AWS 受管政策： AmazonNimbleStudio-StudioUser - 更新的政策	Amazon Nimble Studio 已更新政策，以有條件允許根據 nimble:ownedBy 而非 存取串流工作階段資源nimble:createdBy 。	2021 年 8 月 16 日
AWS 受管政策： AmazonNimbleStudio-StudioUser – 新政策	Amazon Nimble Studio 新增了一項新政策，允許存取與 Studio 使用者相關的資源和其他 服務中的相關 Studio 資源。	2021 年 4 月 28 日
AWS 受管政策： AmazonNimbleStudio-StudioAdmin – 新政策	Amazon Nimble Studio 新增了一項新政策，允許存取與 Studio 管理員相關的資源和其他 服務中的相關 Studio 資源。	2021 年 4 月 28 日
AWS 受管政策： AmazonNimbleStudio-LaunchProfileWorker – 新政策	Amazon Nimble Studio 新增了一項新政策，允許存取 Nimble Studio 啟動描述檔工作者所需的資源。	2021 年 4 月 28 日
Amazon Nimble Studio 開始追蹤變更	Amazon Nimble Studio 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

混淆代理人問題是一種安全問題，其中沒有執行動作許可的實體可能會迫使更特權的實體執行動作。在中 AWS，跨服務模擬可能會導致混淆代理人問題。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。呼叫服務可以被操縱，以使用其許可來對其他客戶的資源採取不應具有存取許可的方式。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，則值中的 aws:SourceAccount 值和 帳戶在使用相同的政策陳述式時，aws:SourceArn必須使用相同的帳戶 ID。

的值aws:SourceArn必須是 Studio 的 ARN，而且aws:SourceAccount必須是您的帳戶 ID。在建立 Studio 之前，您不會知道 Studio ID 是什麼，因為它是由 Nimble Studio 產生。建立 Studio 後，您可以使用最終 Studio ID 設定為 來更新信任政策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，或如果您指定多個資源，請針對 ARN 的未知部分使用aws:SourceArn全域內容條件索引鍵搭配萬用字元 (*)。例如：arn:aws:nimble::123456789012:*。

您的最終使用者在登入 Nimble Studio 入口網站時擔任您的 Studio 角色。當您建立 Studio 時， 會 AWS 設定角色並評估政策。 AWS 會在您的其中一位使用者登入 Nimble Studio 入口網站後，評估政策。建立 Studio 時，您無法修改 aws:SourceArn。建立 Studio 之後，您可以使用 studioArn 進行 aws:SourceArn。

下列範例是擔任角色政策，示範如何使用 Nimble Studio 中的 aws:SourceArn和 aws:SourceAccount全域條件內容索引鍵來防止混淆代理人問題。

```
{
  "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/*"
        }
      }
    }
  ]
}
```

對 Amazon Nimble Studio 身分和存取進行故障診斷

使用下列資訊來協助您診斷和修正使用 Nimble Studio 和 IAM 時可能遇到的常見問題。

主題

我無權在 Nimble Studio 中執行動作。

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 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 管理員。您的管理員提供您的簽署憑證。

我無權執行 iam：PassRole。

如果您收到錯誤，表示您無權執行iam:PassRole動作，請聯絡您的管理員尋求協助。請他們更新您的政策，以允許您將角色傳遞給 Nimble Studio。

有些 AWS 服務 可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。若要這樣做，您需要許可才能將角色傳遞給 服務。

當名為 johndoe 的使用者嘗試使用主控台在 Nimble Studio 中執行動作時，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許可。

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

在這種情況下，John 要求管理員更新其政策，以授予執行`iam:PassRole`動作的許可。

我想要檢視我的存取金鑰。

Amazon Nimble Studio 不提供存取金鑰。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**
>
> 不要將您的存取金鑰提供給第三方，即使是協助尋找您的正式使用者 ID。執行此作業，可能會讓他人能夠永久存取您的帳戶。

當您建立存取金鑰對時，系統會提示您將存取金鑰 ID 和私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。如果您遺失秘密存取金鑰，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對，請先刪除一個金鑰對，再建立新的金鑰對。若要檢視說明，請參閱《IAM 使用者指南》中的管理存取金鑰。

我是管理員，想要允許其他人存取 Nimble Studio。

若要允許其他人存取 Nimble Studio，請為需要存取的人員或應用程式建立 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，將政策連接到授予其正確許可的實體。

Nimble Studio 會在`AmazonNimbleStudio-StudioUser`中為您提供 AWS Management Console。管理主控台的 IT 管理員使用此政策將 Studio 存取權授予其他人。

如需使用 管理政策的教學課程，請檢視 設定 Nimble Studio指南。若要了解如何將現有政策連接至使用者，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）。

如需有關匯入政策的資訊，請參閱《IAM 使用者指南》中的建立您的第一個 IAM 委派使用者和群組。

我想要允許 以外的人員 AWS 帳戶 存取我的 Nimble Studio 資源。

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

如需進一步了解，請參閱以下內容：

- 若要了解 Nimble Studio 是否支援這些功能，請參閱 Amazon Nimble Studio 如何與 IAM 搭配使用。

- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個資源中提供存取權給 IAM 使用者。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的提供存取權給第三方 AWS 帳戶 擁有。
- 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》中的提供存取權給外部驗證的使用者 （ 聯合身分 ）。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策的差異。

使用 Nimble Studio 記錄和監控安全事件

監控是維護 Amazon Nimble Studio 和您的 AWS 解決方案可靠性、可用性和效能的重要部分。從 AWS 解決方案的所有部分收集監控資料，以便在發生多點失敗時更輕鬆地偵錯。

AWS 和 Nimble Studio 提供工具來監控您的資源和回應潛在事件，包括 使用 記錄 Nimble Studio 呼叫 AWS CloudTrail和 AWS CloudFormation 使用者指南。

如需有關 Amazon Nimble Studio 如何使用 的詳細資訊 AWS CloudFormation，包括 JSON 和 YAML 範本的範例，請參閱 AWS CloudFormation 《 使用者指南》中的 Amazon Nimble Studio 資源和屬性參考。若要了解如何使用 CloudFormation 範本，請參閱 AWS CloudFormation 概念。

主題

- 使用 記錄 Nimble Studio 呼叫 AWS CloudTrail

使用 記錄 Nimble Studio 呼叫 AWS CloudTrail

Amazon Nimble Studio 已與 整合 AWS CloudTrail，此服務提供使用者、角色或 Nimble Studio AWS 服務 中 所採取動作的記錄。CloudTrail 會將 Nimble Studio 的所有 API 呼叫擷取為事件。擷取的呼叫包括從 Nimble Studio 主控台的呼叫，以及對 Amazon Nimble Studio 操作的程式碼呼叫。

如果您建立追蹤，則可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Nimble Studio 的事件。如果您未設定追蹤，仍然可以在 CloudTrail 主控台的事件歷史記錄中檢視最新的事件。使用 CloudTrail 收集的資訊，您可以判斷向 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，以及其他詳細資訊。

CloudTrail 中的 Nimble Studio 資訊

建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當活動在 Nimble Studio 中發生時，該活動會與事件歷史記錄中的其他 AWS 服務 事件一起記錄在 CloudTrail 事件中。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱《使用 CloudTrail 事件歷史記錄檢視事件》https://docs.aws.amazon.com/awscloudtrail/latest/userguide/view-cloudtrail-events.html。

若要持續記錄 中的事件 AWS 帳戶，包括 Nimble Studio 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤會記錄 AWS 分割區中所有 區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務 來進一步分析 CloudTrail 日誌中收集的事件資料，並對其採取行動。

如需詳細資訊，請參閱下列內容：

建立追蹤的概觀

CloudTrail 支援的服務和整合

設定 CloudTrail 的 Amazon SNS 通知

從多個區域接收 CloudTrail 日誌檔案

從多個帳戶接收 CloudTrail 日誌檔案

Nimble Studio 動作由 CloudTrail 記錄，並記錄在 Amazon Nimble Studio API 參考中。例如，呼叫 CreateStudio、GetStudio 和 DeleteStudio 動作會在 CloudTrail 日誌檔案中產生項目。

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

- 請求是使用根還是 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 CloudTrail userIdentity 元素。

了解 Nimble Studio 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時

間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

此 JSON 範例顯示三個動作：

- ACTION_1：CreateStudio
- ACTION_2：GetStudio
- ACTION_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，您會注意到事件顯示區域、IP 地址和其他「requestParameters」，例如「userRoleArn」和「adminRoleArn」，這將協助您識別事件。您可以在「creationDate」中看到時間和日期，以及請求發起的來源，標示為「eventSource」：「nimble.amazonaws.com」。

建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。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 AWS 服務 事件一起記錄在 CloudTrail 事件中。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。

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

如需 CloudTrail 的詳細資訊，請參閱 AWS CloudTrail 使用者指南 。

如需有關 Amazon 提供的其他監控服務的資訊，請參閱 Amazon CloudWatch 使用者指南。

Amazon Nimble Studio 的合規驗證

Amazon Nimble Studio 遵循共同的責任模型，且合規由 AWS 和 客戶共同分享。

若要了解 是否 AWS 服務 在特定合規計劃的範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 AWS Compliance Programs。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 中下載報告 AWS Artifact。

使用 時的合規責任 AWS 服務 取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源以協助合規：

- 安全與合規快速入門指南 – 這些部署指南討論架構考量，並提供以 AWS 安全與合規為重心的基準環境部署步驟。
- Amazon Web Services 上的 HIPAA 安全與合規架構 – 此白皮書說明公司如何使用 AWS 來建立符合 HIPAA 資格的應用程式。

> **Note**
>
> 並非所有 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 – 此工作手冊和指南的集合可能適用於您的產業和位置。
- AWS 客戶合規指南 – 透過合規的角度了解共同責任模型。本指南摘要說明保護 的最佳實務， AWS 服務 並將指南映射到跨多個架構的安全控制 （ 包括國家標準和技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO))。
- AWS Config 開發人員指南中的使用規則評估資源 – AWS Config 服務會評估資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub – 這 AWS 服務 可讓您全面檢視其中的安全狀態 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱「Security Hub 控制參考」。
- Amazon GuardDuty – 這可透過監控您的環境是否有可疑和惡意活動，來 AWS 服務 偵測對您 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可滿足特定合規架構所規定的入侵偵測需求，以協助您因應 PCI DSS 等各種不同的合規需求。
- AWS Audit Manager – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和產業標準的方式。

Amazon Nimble Studio 中的基礎設施安全性

Amazon Nimble Studio 是受管服務，受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及如何 AWS 保護基礎設施的相關資訊，請參閱AWS 雲端安全。若要使用基礎設施安全的最佳實務設計您的 AWS 環境，請參閱 Security Pillar AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 已發佈的 API 呼叫，透過網路存取 Nimble Studio。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。

Nimble Studio 的安全最佳實務

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

監控

監控是維護 Nimble Studio 和 AWS 解決方案可靠性、可用性和效能的重要部分。如需監控和回應事件的詳細資訊，請參閱使用 Nimble Studio 記錄和監控安全事件。

資料保護

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS Identity and Access Management (IAM) 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 中的所有預設安全控制項 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。這包括當您使用 Amazon Nimble Studio 或其他 AWS 服務 使用主控台 AWS CLI、API 或 AWS SDKs。您在 Amazon Nimble Studio 或其他 服務中輸入的任何資料都可能被挑選納入診斷日誌中。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 角色和將最低權限授予使用者，來管理對 AWS 資源的存取。建立憑證管理政策和程序，以建立、分發、輪換和撤銷 AWS 存取憑證。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM 最佳實務。

支援 Nimble Studio

本節提供 Nimble Studio 的支援選項，例如如何在部署或使用服務及其相關應用程式時取得協助。

目錄

Nimble Studio 論壇

如果您對 Nimble Studio 有任何疑問，可以造訪 Nimble Studio 論壇。您可以在此取得社群和 AWS 論壇主持人對 Nimble Studio 功能、技術問題和故障診斷協助的解答。

應用程式支援

Nimble Studio 為下列應用程式提供額外的文件。

AWSThinkboxDeadline

如需渲染陣列的協助或了解Deadline運作方式，請參閱 AWSThinkboxDeadline 文件。

Nimble Studio File Transfer

若要了解檔案傳輸的運作方式，請參閱 Nimble Studio 檔案傳輸使用者指南。

支援 中心

支援 中心是建立和管理支援案例的中樞。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，以及訓練和認證。

支援 計劃

支援 計劃可協助您最佳化效能、保持安全、避免停機時間，以及控制成本。如需 支援 計劃的詳細資訊，請參閱比較 支援 計劃。

如需 AWS 如何支援您的詳細資訊，請造訪聯絡我們頁面。

文件歷史記錄

- API 版本：最新
- 文件最近更新時間：2024 年 10 月 2 日

下表說明 Nimble Studio 管理員指南每個版本的重要變更。

變更	描述	
支援結束通知	支援終止通知：在 2024 年 10 月 22 日， AWS 將停止對 Amazon Nimble Studio 的支援。2024 年 10 月 22 日之後，您將無法再存取 Nimble Studio 主控台或 Nimble Studio 資源。	2024 年 10 月 2 日
AWS 受管政策更新	已更新 `AmazonNimbleStudio-StudioUser` 和 `AmazonNimbleStudio-StudioAdmin` 政策，以使用最新版本的服務 AWS IAM Identity Center 。	2023 年 9 月 22 日
新的服務與指南	這是 Amazon Nimble Studio 和 Amazon Nimble Studio 管理員指南的初始版本。	2023 年 6 月 19 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。