使用者指南

研究與工程 Studio

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

研究與工程 Studio: 使用者指南

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

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

Table of Contents

概觀 1
功能和優勢 1
概念和定義 2
架構概觀 4
架構圖 4
AWS 此產品中的 服務 5
示範環境 9
建立一鍵式示範堆疊 9
先決條件 9
建立資源和輸入參數 10
部署後步驟 11
規劃您的部署 12
成本 12
安全 12
IAM 角色 13
安全群組 13
資料加密 13
產品安全考量 13
配額 16
此產品中 AWS 服務的配額 16
AWS CloudFormation 配額 16
規劃彈性 16
支援的 AWS 區域 17
部署產品 19
先決條件 19
AWS 帳戶 使用管理使用者建立 19
建立 Amazon EC2 SSH 金鑰對 20
增加服務配額 20
建立自訂網域 （選用） 20
建立網域 （僅限 GovCloud) 21
提供外部資源 21
在您的環境中設定 LDAPS （選用） 22
Microsoft Active Directory 的服務帳戶 23
設定私有 VPC （選用） 24

建立外部資源 ... 35
步驟 1：啟動產品 ... 39
步驟 2：第一次登入 ... 45
更新產品 ... 46
主要版本更新 ... 46
次要版本更新 ... 46
解除安裝產品 ... 48
使用 AWS Management Console ... 48
使用 AWS Command Line Interface ... 48
刪除 shared-storage-security-group ... 48
刪除 Amazon S3 儲存貯體 ... 49
組態指南 ... 50
身分管理 ... 50
Amazon Cognito 身分設定 ... 50
Active Directory 同步 ... 57
使用 IAM Identity Center 設定 SSO ... 65
為 SSO 設定您的身分提供者 ... 69
設定使用者的密碼 ... 78
建立子網域 ... 78
建立 ACM 憑證 ... 79
Amazon CloudWatch Logs ... 80
設定自訂許可界限 ... 81
設定 RES 就緒 AMIs ... 85
準備 IAM 角色以存取 RES 環境 ... 86
建立 EC2 Image Builder 元件 ... 88
準備您的 EC2 Image Builder 配方 ... 92
設定 EC2 Image Builder 基礎設施 ... 94
設定映像建置器映像管道 ... 95
執行映像建置器映像管道 ... 96
在 RES 中註冊新的軟體堆疊 ... 96
管理員指南 ... 97
秘密管理 ... 97
成本監控和控制 ... 99
成本儀表板 ... 104
先決條件 ... 104
具有預算指派圖表的專案 ... 105

時間圖表的成本分析 107
下載 CSV 111
工作階段管理 111
儀表板 113
工作階段 114
軟體堆疊 (AMIs) 117
除錯 127
桌面設定 128
環境管理 130
環境狀態 130
環境設定 131
使用者 132
群組 133
專案 133
許可政策 143
檔案系統 159
快照管理 161
Amazon S3 儲存貯體 168
使用 產品 184
SSH 存取 184
虛擬桌面 184
啟動新的桌面 185
存取您的桌面 186
控制您的桌面狀態 188
修改虛擬桌面 189
擷取工作階段資訊 190
排程虛擬桌面 190
VDI 自動停止 194
共用桌面 196
共用桌面 196
存取共用桌面 198
檔案瀏覽器 198
上傳檔案 (s) 198
刪除 檔案 (s) 199
管理我的最愛 200
編輯檔案 200

傳輸檔案 201
疑難排解 203
一般偵錯和監控 206
有用的日誌和事件資訊來源 206
典型的 Amazon EC2 主控台外觀 211
Windows DCV 偵錯 213
尋找 Amazon DCV 版本資訊 213
發行 RunBooks 214
安裝問題 216
身分管理問題 224
儲存 228
快照 232
基礎設施 233
啟動虛擬桌面 235
虛擬桌面元件 241
Env 刪除 247
示範環境 253
已知問題 255
2024.x 已知問題 256
注意 279
修訂 280
..... cclxxxii

概觀

> **Important**
>
> 此版本的使用者指南涵蓋 2025.03 版的 Research and Engineering Studio AWS。如需目前版本，請參閱《使用者指南》上的 AWS Research and Engineering Studio。

Research and Engineering Studio (RES) 是一種 AWS 支援的開放原始碼產品，可讓 IT 管理員提供 Web 入口網站，供科學家和工程師在其上執行技術運算工作負載 AWS。RES 提供單一窗格，讓使用者啟動安全的虛擬桌面，以執行科學研究、產品設計、工程模擬或資料分析工作負載。使用者可以使用現有的公司登入資料連線到 RES 入口網站，並處理個人或協作專案。

管理員可以為一組特定使用者建立稱為專案的虛擬協同合作空間，以存取共用資源和協同合作。管理員可以建置自己的應用程式軟體堆疊（使用 Amazon Machine Image 或 AMIs)，並允許 RES 使用者啟動 Windows 或 Linux 虛擬桌面，以及透過共用檔案系統存取專案資料。管理員可以指派軟體堆疊和檔案系統，並僅限這些專案使用者存取。管理員可以使用內建遙測來監控環境用量並疑難排解使用者問題。他們也可以為個別專案設定預算，以防止過度耗用資源。由於產品是開放原始碼，客戶也可以自訂 RES 入口網站的使用者體驗，以滿足自己的需求。

RES 可免費使用，您只需為執行應用程式所需的 AWS 資源付費。

本指南概述 上的 Research and Engineering Studio AWS、其參考架構和元件、規劃部署的考量事項，以及將 RES 部署至 Amazon Web Services (AWS) 雲端的組態步驟。

功能和優勢

上的研究和工程 Studio AWS 提供下列功能：

Web 型使用者介面

RES 提供以 Web 為基礎的入口網站，管理員、研究人員和工程師可以使用該入口網站來存取和管理其研究和工程工作區。科學家和工程師不需要具備 AWS 帳戶 或雲端專業知識，即可使用 RES。

專案型組態

使用專案來定義存取許可、配置資源，以及管理一組任務或活動的預算。將特定軟體堆疊（操作系統和核准的應用程式）和儲存資源指派給專案，以確保一致性和合規性。監控和管理每個專案的支出。

協作工具

科學家和工程師可以邀請專案的其他成員與他們合作，設定他們希望這些同事擁有的許可層級。這些人員可以登入 RES 以連線到這些桌面。

與現有身分管理基礎設施整合

與您現有的身分管理和目錄服務基礎設施整合，以使用使用者現有的公司身分啟用與 RES 入口網站的連線，並將許可指派給使用現有使用者和群組成員資格的專案。

持續儲存和存取共用資料

若要讓使用者存取跨虛擬桌面工作階段的共用資料，請連線到 RES 內現有的檔案系統。支援的儲存服務包括適用於 Linux 桌面的 Amazon Elastic File System，以及適用於 Windows 和 Linux 桌面的 Amazon FSx for NetApp ONTAP。

監控和報告

使用分析儀表板來監控執行個體類型、軟體堆疊和作業系統類型的資源使用情況。儀表板也提供依專案的資源用量明細，以供報告。

預算和成本管理

AWS Budgets 連結至您的 RES 專案，以監控每個專案的成本。如果您超過預算，可以限制 VDI 工作階段的啟動。

概念和定義

本節說明關鍵概念，並定義 研究和工程 Studio 的特定術語 AWS：

檔案瀏覽器

檔案瀏覽器是 RES 使用者介面的一部分，目前登入的使用者可以檢視其檔案系統。

檔案系統

檔案系統充當專案資料的容器（通常稱為資料集）。它在專案邊界內提供儲存解決方案，並改善協同合作和資料存取控制。

全域管理員

管理委派代表可存取跨 RES 環境共用的 RES 資源。範圍和許可跨越多個專案。他們可以建立或修改專案並指派專案擁有者。他們可以委派或指派許可給專案擁有者和專案成員。有時，根據組織的大小，同一個人充當 RES 管理員。

專案

專案是應用程式內的邏輯分割區，可做為資料和運算資源的不同界限；這可確保控管資料流程，並防止跨專案共用資料和 VDI 主機。

專案型許可

專案型許可描述系統中資料和 VDI 主機的邏輯分割區，其中可能存在多個專案。使用者對專案內資料和 VDI 主機的存取，取決於其相關聯的角色（角色）。必須為每個使用者需要存取的專案指派存取權（或專案成員資格）。否則，使用者在未獲得成員資格時，無法存取專案資料和 VDIs。

專案成員

RES 資源 (VDI、儲存體等）的最終使用者。範圍和許可僅限於指派給他們的專案。他們無法委派或指派任何許可。

專案擁有者

具有特定專案存取權和所有權的管理委派人。範圍和許可僅限於其擁有的（多個）專案。他們可以為其擁有的專案中的專案成員指派許可。

軟體堆疊

軟體堆疊是具有 RES 特定中繼資料的 Amazon Machine Image (AMI)，以使用者為 VDI 主機選擇佈建的任何作業系統為基礎。

VDI 主機

虛擬桌面執行個體 (VDI) 主機可讓專案成員存取專案特定的資料和運算環境，確保安全且隔離的工作空間。

如需 AWS 術語的一般參考，請參閱《AWS 一般參考》中的AWS 詞彙表。

架構概觀

本節提供與此產品一起部署之元件的架構圖。

架構圖

使用預設參數部署此產品會在您的 中部署下列元件 AWS 帳戶。

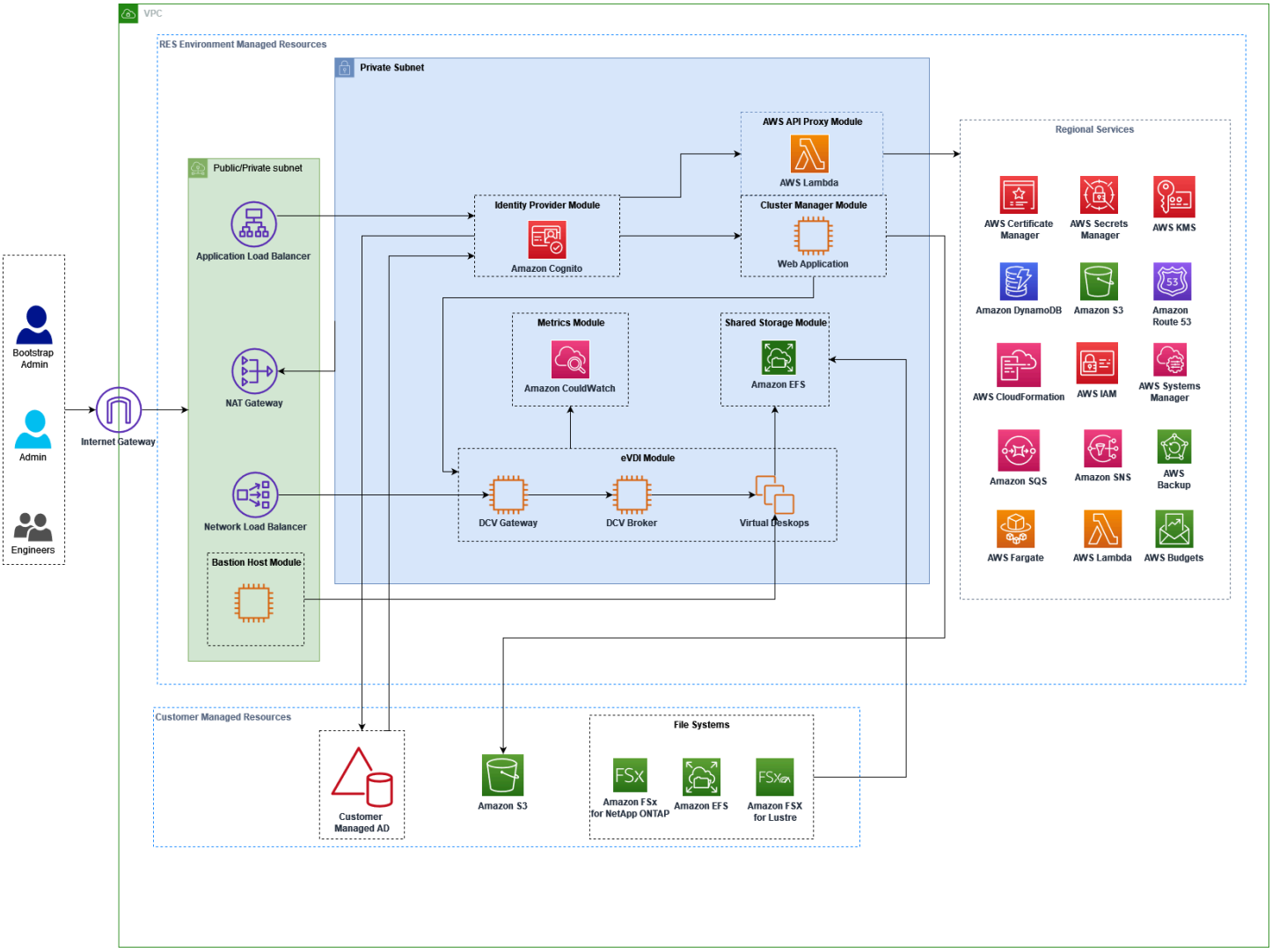


圖 1： AWS 架構上的研究與工程 Studio

> **Note**
>
> AWS CloudFormation 資源是從 AWS Cloud Development Kit (AWS CDK) 建構模組建立的。

搭配 AWS CloudFormation 範本部署之產品元件的高階程序流程如下：

1. RES 會安裝 Web 入口網站的元件，以及：
   a. 適用於互動式工作負載的工程虛擬桌面 (eVDI) 元件
   b. 指標元件

      Amazon CloudWatch 會從 eVDI 元件接收指標。
   c. 堡壘主機元件

      管理員可以使用 SSH 連線到堡壘主機元件來管理基礎基礎設施。
2. RES 會在 NAT 閘道後方的私有子網路中安裝元件。管理員透過 Application Load Balancer (ALB) 或堡壘主機元件存取私有子網路。
3. Amazon DynamoDB 會儲存環境組態。
4. AWS Certificate Manager (ACM) 會產生並存放 Application Load Balancer (ALB) 的公有憑證。

   > **Note**
   >
   > 建議您使用 AWS Certificate Manager 為您的網域產生信任的憑證。

5. Amazon Elastic File System (EFS) 託管安裝在所有適用基礎設施主機和 eVDI Linux 工作階段上的預設/home檔案系統。
6. RES 使用 Amazon Cognito 在 中建立名為「clusteradmin」的初始引導使用者，並將臨時登入資料傳送至安裝期間提供的電子郵件地址。'clusteradmin' 必須在第一次登入時變更密碼。
7. Amazon Cognito 會與您組織的 Active Directory 和使用者身分整合，以進行許可管理。
8. 安全區域可讓管理員根據許可限制對產品內特定元件的存取。

AWS 此產品中的 服務

AWS 服務	Type	描述
Amazon Elastic Compute Cloud	核心	提供基礎運算服務，使用其所選的作業系統和軟體堆疊來建立虛擬桌面。
Elastic Load Balancing	核心	堡壘、叢集管理員和 VDI 主機會在負載平衡器後方的 Auto

AWS 服務	Type	描述
		Scaling 群組中建立。ELB 會平衡來自 Web 入口網站跨 RES 主機的流量。
Amazon Virtual Private Cloud	核心	所有核心產品元件都會在您的 VPC 中建立。
Amazon Cognito	核心	管理使用者身分和身分驗證。Active Directory 使用者會映射至 Amazon Cognito 使用者和群組，以驗證存取層級。
Amazon Elastic File System	核心	提供/home檔案瀏覽器和 VDI 主機的檔案系統，以及共用的外部檔案系統。
Amazon DynamoDB	核心	存放組態資料，例如使用者、群組、專案、檔案系統和元件設定。
AWS Systems Manager	核心	存放執行 VDI 工作階段管理命令的文件。
AWS Lambda	核心	支援產品功能，例如更新 DynamoDB 資料表中的設定、啟動 Active Directory 同步工作流程，以及更新字首清單。
Amazon CloudWatch	支援	提供所有 Amazon EC2 主機和 Lambda 函數的指標和活動日誌。
Amazon Simple Storage Service	支援	存放用於主機引導和組態的應用程式二進位檔。

AWS 服務	Type	描述
AWS Key Management Service	支援	用於搭配 Amazon SQS 佇列、DynamoDB 資料表和 Amazon SNS 主題進行靜態加密。
AWS Secrets Manager	支援	將服務帳戶登入資料儲存在 Active Directory 中，以及 VDIs 的自我簽署憑證中。
AWS CloudFormation	支援	提供產品的部署機制。
AWS Identity and Access Management	支援	限制主機的存取層級。
Amazon Route 53	支援	建立私有託管區域以解析內部負載平衡器和堡壘主機網域名稱。
Amazon Simple Queue Service	支援	建立任務佇列以支援非同步執行。
Amazon Simple Notification Service	支援	支援 VDI 元件之間的發佈訂閱者模型，例如控制器和主機。
AWS Fargate	支援	使用 Fargate 任務安裝、更新和刪除環境。
Amazon FSx 檔案閘道	選用	提供外部共用檔案系統。
Amazon FSx for NetApp ONTAP	選用	提供外部共用檔案系統。
AWS Certificate Manager	選用	為您的自訂網域產生信任的憑證。

AWS 服務	Type	描述
AWS Backup	選用	為 Amazon EC2 主機、檔案系統和 DynamoDB 提供備份功能。

建立示範環境

請依照本節中的步驟來試用 Research and Engineering Studio AWS。此示範使用AWS 示範環境堆疊範本上的 Research and Engineering Studio，部署具有最少參數集的非生產環境。它使用 Keycloak 伺服器進行 SSO。

請注意，部署堆疊之後，您必須先遵循部署後步驟下列操作，在 環境中設定使用者，才能登入。

建立一鍵式示範堆疊

此 AWS CloudFormation 堆疊會建立 Research and Engineering Studio 所需的所有元件。

部署時間：~90 分鐘

先決條件

主題

- AWS 帳戶 使用管理使用者建立
- 建立 Amazon EC2 SSH 金鑰對
- 增加服務配額

AWS 帳戶 使用管理使用者建立

您必須擁有 AWS 帳戶 具有 管理使用者的 ：

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或簡訊，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。

建立 Amazon EC2 SSH 金鑰對

如果您沒有 Amazon EC2 SSH 金鑰對，則需要建立一個。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的使用 Amazon EC2 建立金鑰對。 Amazon EC2

增加服務配額

我們建議增加下列服務配額：

- Amazon VPC
  - 將每個 NAT 閘道的彈性 IP 地址配額從 5 提高到 8
  - 將每個可用區域的 NAT 閘道從 5 個增加到 10 個
- Amazon EC2
  - 將 EC2-VPC 彈性 IPs 從 5 提高到 10

AWS 您的帳戶具有每個 AWS 服務的預設配額，先前稱為限制。除非另有說明，否則每個配額都是區域特定規定。您可以請求提高某些配額，而其他配額無法提高。如需詳細資訊，請參閱the section called “此產品中 AWS 服務的配額”。

建立資源和輸入參數

1. 登入 AWS Management Console 並在 https：//https://console.aws.amazon.com/cloudformation 開啟 AWS CloudFormation 主控台。

   > **Note**
   > 請確定您在管理員帳戶中。

2. 在 主控台中啟動 範本。
3. 在參數下，檢閱此產品範本的參數，並視需要修改。

參數	預設	描述
EnvironmentName	`#res-demo#`	提供給 RES 環境的唯一名稱，開頭為 res-，長度不超過 11 個字元，且不含大寫字母。
AdministratorEmail		使用者完成產品設定的電子郵件地址。如果 Active Directory 單一登入整合失

參數	預設	描述
		敗，此使用者也會充當突破性使用者。
KeyPair		用於連線至基礎設施主機的金鑰對。
ClientIPCidr	<0.0.0.0/0>	IP 地址篩選條件會限制與系統的連線。您可以在部署之後更新 ClientIpCidr。
InboundPrefixList		（選用）為允許直接存取堡壘主機中的 Web UI 和 SSH 的 IPs 提供受管字首清單。

4. 選擇建立堆疊。

部署後步驟

1. 您現在可以使用 clusteradmin 使用者登入示範環境，並將臨時密碼傳送至您在設定期間輸入的管理員電子郵件。系統會提示您在第一次登入時建立新密碼。
2. 如果您想要使用「使用組織 SSO 登入」功能，您必須先為要登入的每個使用者重設密碼。您可以從 AWS Directory Service 重設使用者密碼。示範堆疊會使用使用者名稱建立四個使用者：admin1、user1、admin2 和 user2。
   a. 前往 Directory Service 主控台。
   b. 選取您環境的目錄 ID。您可以從`<StackName>*DirectoryService*`堆疊的輸出取得目錄 ID。
   c. 從右上角的動作下拉式功能表中，選取重設使用者密碼。
   d. 對於您要使用的所有使用者，輸入使用者名稱，輸入您想要的新密碼，然後選擇重設密碼。
3. 重設使用者密碼後，請繼續前往單一登入登入頁面以存取環境。

您的部署現已準備就緒。使用您在電子郵件中收到的 EnvironmentUrl 來存取 UI，或者您也可以從已部署堆疊的輸出中取得相同的 URL。您現在可以使用您在 Active Directory 中為 重設密碼的使用者和密碼登入 Research and Engineering Studio 環境。

規劃您的部署

本節包含成本、安全性、支援區域和配額的相關資訊，可協助您規劃 Research and Engineering Studio 的部署 AWS。

成本

上的研究和工程 Studio AWS 可免費使用，您只需為 AWS 執行應用程式所需的資源付費。如需詳細資訊，請參閱AWS 此產品中的 服務。

> **Note**
>
> 您需負責支付執行此產品時所使用的 AWS 服務成本。
> 我們建議您建立預算表AWS Cost Explorer，以協助管理成本。價格可能變動。如需完整詳細資訊，請參閱此產品中使用的每個 AWS 服務的定價網頁。

安全

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

安全性是 AWS 與您之間的共同責任。共同責任模型將此描述為雲端安全性和雲端安全性：

- 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。在AWS 合規計劃中，第三方稽核人員會定期測試和驗證我們安全的有效性。 若要了解適用於 上的研究和工程 Studio 的合規計劃 AWS，請參閱AWS 合規計劃的 服務範圍。
- 雲端的安全性 – 您的責任取決於您使用 AWS 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。

若要了解如何將共同責任模型套用到 Research and Engineering Studio 所使用的 AWS 服務，請參閱此產品中 服務的安全考量。如需 AWS 安全性的詳細資訊，請參閱AWS 雲端 安全性。

IAM 角色

AWS Identity and Access Management (IAM) 角色可讓客戶將精細存取政策和許可指派給 上的服務和使用者 AWS 雲端。此產品會建立 IAM 角色，授予產品的 AWS Lambda 函數和 Amazon EC2 執行個體建立區域資源的存取權。

RES 支援 IAM 中的身分型政策。部署時，RES 會建立政策來定義管理員許可和存取權。實作產品的管理員會在與 RES 整合的現有客戶 Active Directory 中建立和管理最終使用者和專案領導者。如需詳細資訊，請參閱《 AWS Identity and Access Management 使用者指南》中的建立 IAM 政策。

您組織的管理員可以使用 Active Directory 管理使用者存取。當最終使用者存取 RES 使用者介面時，RES 會向 Amazon Cognito 進行身分驗證。

安全群組

此產品中建立的安全群組旨在控制和隔離 Lambda 函數、EC2 執行個體、檔案系統 CSR 執行個體和遠端 VPN 端點之間的網路流量。建議您檢閱安全群組，並在產品部署後視需要進一步限制存取。

資料加密

根據預設，在 AWS (RES) 上的 Research and Engineering Studio 會使用 RES 擁有的金鑰加密靜態和傳輸中的客戶資料。部署 RES 時，您可以指定 AWS KMS key。RES 使用您的登入資料來授予金鑰存取權。如果您提供客戶擁有和管理的 AWS KMS key，則會使用該金鑰加密靜態客戶資料。

RES 會使用 SSL/TLS 加密傳輸中的客戶資料。我們需要 TLS 1.2，但建議使用 TLS 1.3。

此產品中 服務的安全考量

如需 Research and Engineering Studio 所使用服務之安全性考量的詳細資訊，請遵循下表中的連結：

AWS 服務安全資訊	服務類型	服務在 RES 中的使用方式
Amazon Elastic Compute Cloud	核心	提供基礎運算服務，使用其所選的作業系統和軟體堆疊來建立虛擬桌面。
Elastic Load Balancing	核心	堡壘、叢集管理員和 VDI 主機會在負載平衡器後方的 Auto Scaling 群組中建立。ELB 會

AWS 服務安全資訊	服務類型	服務在 RES 中的使用方式
		平衡來自 Web 入口網站跨 RES 主機的流量。
Amazon Virtual Private Cloud	核心	所有核心產品元件都會在您的 VPC 中建立。
Amazon Cognito	核心	管理使用者身分和身分驗證。Active Directory 使用者會映射至 Amazon Cognito 使用者和群組，以驗證存取層級。
Amazon Elastic File System	核心	提供/home檔案瀏覽器和 VDI 主機的檔案系統，以及共用的外部檔案系統。
Amazon DynamoDB	核心	存放組態資料，例如使用者、群組、專案、檔案系統和元件設定。
AWS Systems Manager	核心	存放執行 VDI 工作階段管理命令的文件。
AWS Lambda	核心	支援產品功能，例如更新 DynamoDB 資料表中的設定、啟動 Active Directory 同步工作流程，以及更新字首清單。
Amazon CloudWatch	支援	提供所有 Amazon EC2 主機和 Lambda 函數的指標和活動日誌。
Amazon Simple Storage Service	支援	存放用於主機引導和組態的應用程式二進位檔。

AWS 服務安全資訊	服務類型	服務在 RES 中的使用方式
AWS Key Management Service	支援	用於搭配 Amazon SQS 佇列、DynamoDB 資料表和 Amazon SNS 主題進行靜態加密。
AWS Secrets Manager	支援	將服務帳戶登入資料儲存在 Active Directory 中，以及 VDIs 的自我簽署憑證中。
AWS CloudFormation	支援	提供產品的部署機制。
AWS Identity and Access Management	支援	限制主機的存取層級。
Amazon Route 53	支援	建立私有託管區域以解析內部負載平衡器和堡壘主機網域名稱。
Amazon Simple Queue Service	支援	建立任務佇列以支援非同步執行。
Amazon Simple Notification Service	支援	支援 VDI 元件之間的發佈訂閱者模型，例如控制器和主機。
AWS Fargate	支援	使用 Fargate 任務安裝、更新和刪除環境。
Amazon FSx 檔案閘道	選用	提供外部共用檔案系統。
Amazon FSx for NetApp ONTAP	選用	提供外部共用檔案系統。
AWS Certificate Manager	選用	為您的自訂網域產生信任的憑證。

AWS 服務安全資訊	服務類型	服務在 RES 中的使用方式
AWS Backup	選用	為 Amazon EC2 主機、檔案系統和 DynamoDB 提供備份功能。

配額

服務配額 (也稱為限制) 是 AWS 帳戶的服務資源或操作的最大數量。

此產品中 AWS 服務的配額

請確定您對此產品中實作的每個服務都有足夠的配額。如需更多相關資訊，請參閱 AWS Service Quotas。

對於此產品，我們建議提高下列服務的配額：

- Amazon Virtual Private Cloud
- Amazon EC2

若要請求增加配額，請參閱 Service Quotas 使用者指南中的請求提高配額。如果 Service Quotas 中尚未提供配額，請使用增加服務配額表單。

AWS CloudFormation 配額

在此產品中啟動堆疊時，您應該注意 AWS 帳戶 的 AWS CloudFormation 配額。透過了解這些配額，您可以避免限制會阻止您成功部署此產品的錯誤。如需詳細資訊，請參閱《 AWS CloudFormation 使用者指南》中的 AWS CloudFormation 配額。

規劃彈性

產品會部署具有 Amazon EC2 執行個體最小數量和大小的預設基礎設施，以操作系統。為了改善大規模生產環境中的彈性，建議您增加基礎設施 Auto Scaling 群組 (ASG) 內的預設最小容量設定。將值從一個執行個體增加到兩個執行個體可提供多個可用區域 (AZ) 的優點，並縮短在發生意外資料遺失時還原系統功能的時間。

ASG 設定可在 Amazon EC2 主控台中自訂，網址為 https：//https://console.aws.amazon.com/ec2/。產品預設會建立四個 ASGs，每個名稱以 結尾`-asg`。您可以將最小值和所需值變更為適合您生產環

境的數量。選取您要修改的群組，然後選擇動作，然後選取編輯。如需 ASGs的詳細資訊，請參閱《Amazon EC2 Auto Scaling 使用者指南》中的擴展 Auto Scaling 群組的大小。 Amazon EC2 Auto Scaling

支援的 AWS 區域

此產品使用目前尚未在所有 中提供的服務 AWS 區域。您必須在可使用 AWS 區域 所有服務的 中啟動此產品。如需 AWS 各區域服務的最新可用性，請參閱 AWS 區域 al Services List。

以下 AWS 支援 上的研究和工程 Studio AWS 區域：

區域名稱	區域	舊版本	最新版本 (2025.03)
美國東部 (維吉尼亞北部)	us-east-1	是	是
美國東部 (俄亥俄)	us-east-2	是	是
美國西部 (加利佛尼亞北部)	us-west-1	是	是
美國西部 (奧勒岡)	us-west-2	是	是
亞太區域 (東京)	ap-northeast-1	是	是
亞太區域 (首爾)	ap-northeast-2	是	是
亞太區域 (孟買)	ap-south-1	是	是
亞太區域 (新加坡)	ap-southeast-1	是	是
亞太區域 (雪梨)	ap-southeast-2	是	是
加拿大 (中部)	ca-central-1	是	是
歐洲 (法蘭克福)	eu-central-1	是	是
歐洲 (米蘭)	eu-south-1	是	是
歐洲 (愛爾蘭)	eu-west-1	是	是

區域名稱	區域	舊版本	最新版本 (2025.03)
歐洲 (倫敦)	eu-west-2	是	是
歐洲 (巴黎)	eu-west-3	是	是
Europe (Stockholm)	eu-north-1	否	是
以色列 (特拉維夫)	il-central-1	是	是
AWS GovCloud（美國西部）	us-gov-west-1	是	是

部署產品

> **Note**
>
> 此產品使用 AWS CloudFormation 範本和堆疊來自動化其部署。CloudFormation 範本說明此產品中包含 AWS 的資源及其屬性。CloudFormation 堆疊會佈建範本中所述的資源。

啟動產品之前，請檢閱本指南先前討論的成本、架構、網路安全和其他考量事項。

主題

- 先決條件
- 建立外部資源
- 步驟 1：啟動產品
- 步驟 2：第一次登入

先決條件

主題

- AWS 帳戶 使用管理使用者建立
- 建立 Amazon EC2 SSH 金鑰對
- 增加服務配額
- 建立自訂網域（選用）
- 建立網域（僅限 GovCloud)
- 提供外部資源
- 在您的環境中設定 LDAPS（選用）
- 設定 Microsoft Active Directory 的服務帳戶
- 設定私有 VPC（選用）

AWS 帳戶 使用管理使用者建立

您必須擁有 AWS 帳戶 具有 管理使用者的 ：

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或簡訊，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。

建立 Amazon EC2 SSH 金鑰對

如果您沒有 Amazon EC2 SSH 金鑰對，則需要建立一個金鑰對。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的使用 Amazon EC2 建立金鑰對。 Amazon EC2

增加服務配額

我們建議增加下列服務配額：

- Amazon VPC
  - 將每個 NAT 閘道的彈性 IP 地址配額從 5 提高到 8。
  - 將每個可用區域的 NAT 閘道從 5 增加到 10。
- Amazon EC2
  - 將 EC2-VPC 彈性 IPs 從 5 提高到 10

AWS 您的帳戶具有每個 AWS 服務的預設配額，先前稱為限制。除非另有說明，否則每個配額都是區域特定規定。您可以請求提高某些配額，而其他配額無法提高。如需詳細資訊，請參閱此產品中 AWS 服務的配額。

建立自訂網域（選用）

建議您為產品使用自訂網域，以擁有易於使用的 URL。您可以提供自訂網域，並選擇性地為其提供憑證。

外部資源堆疊中有一個程序，可為您提供的自訂網域建立憑證。如果您有網域並想要使用外部資源堆疊的憑證產生功能，可以略過此處的步驟。

或者，請依照下列步驟，使用 Amazon Route 53 註冊網域，並使用 匯入網域的憑證 AWS Certificate Manager。

1. 依照指示向 Route53 註冊網域。您應該會收到確認電子郵件。
2. 擷取網域的託管區域。這是由 Route53 自動建立的。
   a. 開啟 Route53 主控台。
   b. 從左側導覽中選擇託管區域。
   c. 開啟為您的網域名稱建立的託管區域，並複製託管區域 ID。
3. 開啟 AWS Certificate Manager 並依照下列步驟請求網域憑證。確定您位於計劃部署解決方案的區域。
4. 從導覽中選擇列出憑證，然後尋找您的憑證請求。請求應處於待定狀態。
5. 選擇您的憑證 ID 以開啟請求。
6. 在網域區段中，選擇在 Route53 中建立記錄。處理請求大約需要十分鐘。
7. 發出憑證後，請從憑證狀態區段複製 ARN。

建立網域（僅限 GovCloud)

如果您要在 AWS GovCloud（美國西部）區域中部署，且正在使用適用於 Research and Engineering Studio 的自訂網域，則需要完成這些先決條件步驟。

1. 在建立公有託管網域的商業分割區 AWS 帳戶中部署憑證 AWS CloudFormation 堆疊。
2. 從憑證 CloudFormation 輸出中，尋找並記下 `CertificateARN`和 `PrivateKeySecretARN`。
3. 在 GovCloud 分割區帳戶中，建立具有`CertificateARN`輸出值的秘密。請注意新的秘密 ARN，並將兩個標籤新增至秘密，以便 `vdc-gateway` 可以存取秘密值：
   a. res：ModuleName = virtual-desktop-controller
   b. res：EnvironmentName = 【環境名稱】（可以是 res-demo。）
4. 在 GovCloud 分割區帳戶中，建立具有`PrivateKeySecretArn`輸出值的秘密。請注意新的秘密 ARN，並將兩個標籤新增至秘密，以便 `vdc-gateway` 可以存取秘密值：
   a. res：ModuleName = virtual-desktop-controller
   b. res：EnvironmentName = 【環境名稱】（可以是 res-demo。）

提供外部資源

上的研究和工程 Studio AWS 預期在部署時存在下列外部資源。

- 網路 (VPC、公有子網路和私有子網路)

  在這裡，您將執行用於託管 RES 環境、Active Directory (AD) 和共用儲存體的 EC2 執行個體。
- 儲存 (Amazon EFS)

  儲存磁碟區包含虛擬桌面基礎設施 (VDI) 所需的檔案和資料。
- 目錄服務 (AWS Directory Service for Microsoft Active Directory)

  目錄服務會將使用者驗證為 RES 環境。
- 秘密，其中包含格式化為鍵/值對的 Active Directory 服務帳戶使用者名稱和密碼 （ 使用者名稱、密碼 ）

  Research and Engineering Studio 會使用 存取您提供的秘密，包括服務帳戶密碼AWS Secrets Manager。

> **Warning**
> 您必須為要同步的所有 Active Directory (AD) 使用者提供有效的電子郵件地址。

> **Tip**
> 如果您正在部署示範環境，但沒有這些外部資源可用，則可以使用 AWS 高效能運算配方來產生外部資源。請參閱下一節 建立外部資源，以在您的帳戶中部署資源。
> 對於 AWS GovCloud （ 美國西部） 區域中的示範部署，您將需要完成 中的先決條件步驟建立網域 （ 僅限 GovCloud)。

在您的環境中設定 LDAPS （ 選用 ）

如果您計劃在環境中使用 LDAPS 通訊，則必須完成以下步驟，才能建立憑證並將其連接至 AWS Managed Microsoft AD (AD) 網域控制器，以提供 AD 和 RES 之間的通訊。

1. 請遵循如何為 啟用伺服器端 LDAPS AWS Managed Microsoft AD中提供的步驟。如果您已啟用 LDAPS，則可以略過此步驟。
2. 確認已在 AD 上設定 LDAPS 後，匯出 AD 憑證：

   a. 前往您的 Active Directory 伺服器。

b. 以管理員身分開啟 PowerShell。

c. 執行 `certmgr.msc` 以開啟憑證清單。

d. 首先開啟信任的根憑證授權機構，然後開啟憑證清單。

e. 選取並按住（或以滑鼠右鍵按一下）與 AD 伺服器同名的憑證，然後選擇所有任務，然後選擇匯出。

f. 選取 Base-64 編碼的 X.509 (.CER)，然後選擇下一步。

g. 選取目錄，然後選擇下一步。

3. 在 中建立秘密 AWS Secrets Manager：

   在 Secrets Manager 中建立機密時，在機密類型下選擇其他類型的機密，並將 PEM 編碼的憑證貼到純文字欄位中。

4. 請注意建立的 ARN，並將其輸入為 中的 `DomainTLSCertificateSecretARN` 參數步驟 1：啟動產品。

設定 Microsoft Active Directory 的服務帳戶

如果您選擇 Microsoft Active Directory (AD) 作為 RES 的身分來源，則 AD 中會有允許程式設計存取的服務帳戶。做為 RES 安裝的一部分，您必須使用服務帳戶的登入資料傳遞秘密。服務帳戶負責下列函數：

- 從 AD 同步使用者：RES 必須從 AD 同步使用者，以允許他們登入 Web 入口網站。同步程序使用服務帳戶查詢使用 LDAP 的 AD（以確定哪些使用者和群組可用）。
- 加入 AD 網域：這是執行個體加入 AD 網域之 Linux 虛擬桌面和基礎設施主機的選用操作。在 RES 中，這會使用 `DisableADJoin` 參數控制。此參數預設為 False，這表示 Linux 虛擬桌面會嘗試在預設組態中加入 AD 網域。
- 連線至 AD：如果 Linux 虛擬桌面和基礎設施主機未加入 AD 網域，則會連線至 AD 網域 (`DisableADJoin` = True)。為了讓此功能正常運作，服務帳戶也需要 `UsersOU`和 中使用者和群組的讀取存取權`GroupsOU`。

服務帳戶需要下列許可：

- 同步使用者並連線至 AD → `UsersOU`和 中使用者和群組的讀取存取權`GroupsOU`。
- 若要加入 AD 網域 → 在 中建立`Computer`物件`ComputersOU`。

https：//https://github.com/aws-samples/aws-hpc-recipes/blob/main/recipes/res/res_demo_env/assets/service_account.ps1 的指令碼提供如何授予適當服務帳戶許可的範例。您可以根據自己的 AD 進行修改。

設定私有 VPC （選用）

在隔離的 VPC 中部署 Research and Engineering Studio 可提供增強的安全性，以滿足組織的合規和管理要求。不過，標準 RES 部署依賴網際網路存取來安裝相依性。若要在私有 VPC 中安裝 RES，您需要滿足下列先決條件：

主題

- 準備 Amazon Machine Image AMIs)
- 設定 VPC 端點
- 在沒有 VPC 端點的情況下連線至 服務
- 設定私有 VPC 部署參數

準備 Amazon Machine Image AMIs)

1. 下載相依性。若要在隔離的 VPC 中部署，RES 基礎設施需要有相依性的可用性，而不需要公有網際網路存取。
2. 使用 Amazon S3 唯讀存取和 Amazon EC2 的受信任身分建立 IAM 角色。
   a. 前往 https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
   b. 從角色中，選擇建立角色。
   c. 在選取信任的實體頁面上：
      - 在信任的實體類型下，選擇 AWS 服務。
      - 針對服務或使用案例下的使用案例，選擇 EC2，然後選擇下一步。
   d. 在新增許可上，選取下列許可政策，然後選擇下一步：
      - AmazonS3ReadOnlyAccess
      - AmazonSSMManagedInstanceCore
      - EC2InstanceProfileForImageBuilder
   e. 新增角色名稱和描述，然後選擇建立角色。
3. 建立 EC2 映像建置器元件：

a. 在 開啟 EC2 Image Builder 主控台https://console.aws.amazon.com/imagebuilder。

b. 在已儲存資源下，選擇元件，然後選擇建立元件。

c. 在建立元件頁面上，輸入下列詳細資訊：

- 針對元件類型，選擇建置。
- 如需元件詳細資訊，請選擇：

參數	使用者項目
Image operating system (OS)	Linux
Compatible OS Versions	Amazon Linux 2, RHEL8, RHEL9, or Windows 10 and 11
Component name	Enter a name such as: *<research-and-engineering-studio-infrastructure>*
Component version	We recommend starting with 1.0.0.
Description	Optional user entry.

d. 在建立元件頁面上，選擇定義文件內容。

i. 在輸入定義文件內容之前，您需要 tar.gz 檔案的檔案 URI。將 RES 提供的 tar.gz 檔案上傳至 Amazon S3 儲存貯體，並從儲存貯體屬性複製檔案的 URI。

ii. 輸入下列資料：

> **Note**
>
> `AddEnvironmentVariables` 是選用的，如果您在基礎設施主機中不需要自訂環境變數，則可以將其移除。
> 如果您要設定 `http_proxy`和 `https_proxy`環境變數，則需要這些`no_proxy`參數，以防止執行個體使用代理來查詢 localhost、執行個體中繼資料 IP 地址，以及支援 VPC 端點的服務。

```
#  Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
#  Licensed under the Apache License, Version 2.0 (the "License"). You may
 not use this file except in compliance
#  with the License. A copy of the License is located at
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
#  or in the 'license' file accompanying this file. This file is
 distributed on an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-infrastructure
description: An RES EC2 Image Builder component to install required RES
 software dependencies for infrastructure hosts.
schemaVersion: 1.0

parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - AWSRegion:
      type: string
      description: RES Environment AWS Region
phases:
  - name: build
    steps:
       - name: DownloadRESInstallScripts
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: '<s3 tar.gz file uri>'
              destination: '/root/bootstrap/res_dependencies/
res_dependencies.tar.gz'
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
```

```
            commands:
                - 'cd /root/bootstrap/res_dependencies'
                - 'tar -xf res_dependencies.tar.gz'
                - 'cd all_dependencies'
                - '/bin/bash install.sh'
        - name: AddEnvironmentVariables
          action: ExecuteBash
          onFailure: Abort
          maxAttempts: 3
          inputs:
            commands:
                - |
                  echo -e "
                  http_proxy=http://<ip>:<port>
                  https_proxy=http://<ip>:<port>

 no_proxy=127.0.0.1,169.254.169.254,169.254.170.2,localhost,
{{ AWSRegion }}.res,{{ AWSRegion }}.vpce.amazonaws.com,
{{ AWSRegion }}.elb.amazonaws.com,s3.
{{ AWSRegion }}.amazonaws.com,s3.dualstack.
{{ AWSRegion }}.amazonaws.com,ec2.{{ AWSRegion }}.amazonaws.com,ec2.
{{ AWSRegion }}.api.aws,ec2messages.{{ AWSRegion }}.amazonaws.com,ssm.
{{ AWSRegion }}.amazonaws.com,ssmmessages.
{{ AWSRegion }}.amazonaws.com,kms.
{{ AWSRegion }}.amazonaws.com,secretsmanager.
{{ AWSRegion }}.amazonaws.com,sqs.
{{ AWSRegion }}.amazonaws.com,elasticloadbalancing.
{{ AWSRegion }}.amazonaws.com,sns.{{ AWSRegion }}.amazonaws.com,logs.
{{ AWSRegion }}.amazonaws.com,logs.
{{ AWSRegion }}.api.aws,elasticfilesystem.
{{ AWSRegion }}.amazonaws.com,fsx.{{ AWSRegion }}.amazonaws.com,dynamodb.
{{ AWSRegion }}.amazonaws.com,api.ecr.
{{ AWSRegion }}.amazonaws.com,.dkr.ecr.
{{ AWSRegion }}.amazonaws.com,kinesis.{{ AWSRegion }}.amazonaws.com,.data-
kinesis.{{ AWSRegion }}.amazonaws.com,.control-
kinesis.{{ AWSRegion }}.amazonaws.com,events.
{{ AWSRegion }}.amazonaws.com,cloudformation.
{{ AWSRegion }}.amazonaws.com,sts.
{{ AWSRegion }}.amazonaws.com,application-autoscaling.
{{ AWSRegion }}.amazonaws.com,monitoring.{{ AWSRegion }}.amazonaws.com,ecs.
{{ AWSRegion }}.amazonaws.com,.execute-api.{{ AWSRegion }}.amazonaws.com
>                   " > /etc/environment
```

e. 選擇建立元件。

4. 建立映像建置器映像配方。

   a. 在建立配方頁面上，輸入下列內容：

章節	參數	使用者項目
配方詳細資訊	名稱	Enter an appropriate name such as res-recipe-linux-x86.
	版本	Enter a version, typically starting with 1.0.0.
	描述	Add an optional description.
基礎映像	選取影像	Select managed images.
	作業系統	Amazon Linux or Red Hat Enterprise Linux (RHEL)
	影像原始伺服器	Quick start (Amazon-managed)
	映像名稱	Amazon Linux 2 x86, Red Hat Enterprise Linux 8 x86, or Red Hat Enterprise Linux 9 x86
	自動版本控制選項	Use latest available OS version.
執行個體組態	–	Keep everything in the default settings, and make sure 在管道執行後移除 SSM 代理程式 is not selected.

章節	參數	使用者項目
工作目錄	工作目錄路徑	/root/bootstrap/res_dependencies
元件	建置元件	搜尋並選取下列項目： • Amazon 受管：aws-cli-version-2-linux • Amazon 受管：amazon-cloudwatch-agent-linux • 由您擁有：先前建立的 Amazon EC2 元件。將您的 AWS 帳戶 ID 和目前 AWS 區域 放在 欄位中。
	測試元件	搜尋並選取： • Amazon 受管：simple-boot-test-linux

b. 選擇建立配方。

5. 建立映像建置器基礎設施組態。

a. 在已儲存資源下，選擇基礎設施組態。

b. 選擇建立基礎設施組態。

c. 在建立基礎設施組態頁面上，輸入下列內容：

章節	參數	使用者項目
一般	名稱	Enter an appropriate name such as res-infra-linux-x86.
	描述	Add an optional description.
	IAM 角色	Select the IAM role created previously.

章節	參數	使用者項目
AWS 基礎設施	執行個體類型	Choose t3.medium.

	VPC、子網路和安全群組	選取允許網際網路存取和存取 Amazon S3 儲存貯體的選項。如果您需要建立安全群組，您可以從 Amazon EC2 主控台使用下列輸入建立安全群組：
		• VPC：選取用於基礎設施組態的相同 VPC。此 VPC 必須具有網際網路存取。
		• 傳入規則：
		  • Type (類型)：SSH
		  • Source (來源)：自訂
		  • CIDR 區塊：0.0.0.0/0

d. 選擇建立基礎設施組態。

6. 建立新的 EC2 Image Builder 管道：

   a. 前往映像管道，然後選擇建立映像管道。

   b. 在指定管道詳細資訊頁面上，輸入以下內容並選擇下一步：

      - 管道名稱和選用描述
      - 對於建置排程，如果您想要手動啟動 AMI 製作程序，請設定排程或選擇手動。

   c. 在選擇配方頁面上，選擇使用現有配方，然後輸入先前建立的配方名稱。選擇下一步。

   d. 在定義映像程序頁面上，選取預設工作流程，然後選擇下一步。

   e. 在定義基礎設施組態頁面上，選擇使用現有的基礎設施組態，然後輸入先前建立的基礎設施組態名稱。選擇下一步。

   f. 在定義分佈設定頁面上，針對您的選擇考慮下列事項：

- 輸出映像必須與部署的 RES 環境位於相同的區域，以便 RES 能夠從中正確啟動基礎設施主機執行個體。使用服務預設值，輸出映像會在使用 EC2 Image Builder 服務的區域中建立。
- 如果您想要在多個區域中部署 RES，您可以選擇建立新的分佈設定，並在該處新增更多區域。

g. 檢閱您的選擇，然後選擇建立管道。

7. 執行 EC2 Image Builder 管道：

   a. 從映像管道中，尋找並選取您建立的管道。

   b. 選擇動作，然後選取執行管道。

   管道可能需要大約 45 分鐘到一小時的時間來建立 AMI 映像。

8. 請注意產生的 AMI 的 AMI ID，並將其用作 中 InfrastructureHostAMI 參數的輸入the section called "步驟 1：啟動產品"。

設定 VPC 端點

若要部署 RES 並啟動虛擬桌面， AWS 服務 需要存取您的私有子網路。您必須設定 VPC 端點以提供必要的存取權，而且您必須為每個端點重複這些步驟。

1. 如果先前尚未設定端點，請遵循AWS 服務 使用介面 VPC 端點存取 中提供的指示。
2. 在兩個可用區域中各選取一個私有子網路。

AWS 服務	服務名稱
Application Auto Scaling	com.amazonaws.*region*.application-autoscaling
AWS CloudFormation	com.amazonaws.*region*.cloudformation
Amazon CloudWatch	com.amazonaws.*region*.monitoring
Amazon CloudWatch Logs	com.amazonaws.*region*.logs
Amazon DynamoDB	com.amazonaws.*region*.dynamodb （需要閘道端點）
Amazon EC2	com.amazonaws.*region*.ec2

AWS 服務	服務名稱
Amazon ECR	com.amazonaws.*region*.ecr.api
	com.amazonaws.*region*.ecr.dkr
Amazon Elastic File System	com.amazonaws.*region*.elasticfilesystem
Elastic Load Balancing	com.amazonaws.*region*.elasticloadbalancing
Amazon EventBridge	com.amazonaws.*region*.events
Amazon FSx	com.amazonaws.*region*.fsx
AWS Key Management Service	com.amazonaws.*region*.kms
Amazon Kinesis Data Streams	com.amazonaws.*region*.kinesis-streams
AWS Lambda	com.amazonaws.*region*.lambda
Amazon Simple Storage Service (Amazon S3)	com.amazonaws.*region*.s3（需要預設在 RES 中建立的閘道端點。） 隔離環境中的跨掛載儲存貯體需要額外的 Amazon S3 介面端點。請參閱存取 Amazon Simple Storage Service 介面端點。
AWS Secrets Manager	com.amazonaws.*region*.secretsmanager
Amazon Elastic Container Service	com.amazonaws.*region*.ecs
Amazon SES	com.amazonaws.*region*.email-smtp（下列可用區域不支援：use-1-az2、use1-az3、use1-az5、usw1-az2、usw2-az4、apne2-az4、cac1-az3 和 cac1-az4。）
AWS Security Token Service	com.amazonaws.*region*.sts
Amazon SNS	com.amazonaws.*region*.sns
Amazon SQS	com.amazonaws.*region*.sqs

AWS 服務	服務名稱
AWS Systems Manager	com.amazonaws.*region*.ec2messages
	com.amazonaws.*region*.ssm
	com.amazonaws.*region*.ssmmessages

在沒有 VPC 端點的情況下連線至 服務

若要與不支援 VPC 端點的服務整合，您可以在 VPC 的公有子網路中設定代理伺服器。請依照下列步驟，使用 AWS 身分中心做為您的身分提供者，建立具有 Research and Engineering Studio 部署所需最低存取權的代理伺服器。

1. 在將用於 RES 部署的 VPC 公有子網路中啟動 Linux 執行個體。
   - Linux 系列 – Amazon Linux 2 或 Amazon Linux 3
   - 架構 – x86
   - 執行個體類型 – t2.micro 或更高版本
   - 安全群組 – 從 0.0.0.0/0 起連接埠 3128 上的 TCP
2. 連線至執行個體以設定代理伺服器。
   a. 開啟 http 連線。
   b. 允許從所有相關子網路連線至下列網域：
      - .amazonaws.com （適用於一般 AWS 服務）
      - .amazoncognito.com （適用於 Amazon Cognito)
      - .awsapps.com （適用於 Identity Center)
      - .signin.aws （適用於 Identity Center)
      - .amazonaws-us-gov.com （適用於 Gov Cloud)
   c. 拒絕所有其他連線。
   d. 啟用並啟動代理伺服器。
   e. 請注意代理伺服器接聽的 PORT。
3. 設定您的路由表以允許存取代理伺服器。
   a. 前往 VPC 主控台，識別您將用於基礎設施主機和 VDI 主機的子網路路由表。

b. 編輯路由表，以允許所有傳入連線前往先前步驟中建立的代理伺服器執行個體。

c. 針對您要用於基礎設施/VDIs 的所有子網路（無網際網路存取）的路由表，執行此操作。

4. 修改代理伺服器 EC2 執行個體的安全群組，並確保其允許代理伺服器接聽之 PORT 上的傳入 TCP 連線。

設定私有 VPC 部署參數

在 中the section called “步驟 1：啟動產品”，您需要在 AWS CloudFormation 範本中輸入特定參數。請務必依照說明設定下列參數，以成功部署到您剛設定的私有 VPC。

參數	輸入
InfrastructureHostAMI	Use the infrastructure AMI ID created in the section called “準備 Amazon Machine Image AMIs)”.
IsLoadBalancerInternetFacing	Set to false.
LoadBalancerSubnets	Choose private subnets without internet access.
InfrastructureHostSubnets	Choose private subnets without internet access.
VdiSubnets	Choose private subnets without internet access.
ClientIP	You can choose your VPC CIDR to allow access for all VPC IP addresses.
HttpProxy	Example: `http://10.1.2.3:123`
HttpsProxy	Example: `http://10.1.2.3:123`
NoProxy	範例： `127.0.0.1,169.254.169.254,169.254.170.2,localhost,us-east-1.res,us-east-1.vpce.amazonaws.com,us-east-1.elb.amazonaws.com,s3.us-east-1.amazonaws.com,s3.dualstack.us-east-1.amazonaws.com,ec2.us-east-1.amazonaws.com,ec2.us-east-1.api.aws,ec2messages.us-ea`

參數	輸入
	`st-1.amazonaws.com,ssm.us-east-1.amazonaws.com,ssmmessages.us-east-1.amazonaws.com,kms.us-east-1.amazonaws.com,secretsmanager.us-east-1.amazonaws.com,sqs.us-east-1.amazonaws.com,elasticloadbalancing.us-east-1.amazonaws.com,sns.us-east-1.amazonaws.com,logs.us-east-1.amazonaws.com,logs.us-east-1.api.aws,elasticfilesystem.us-east-1.amazonaws.com,fsx.us-east-1.amazonaws.com,dynamodb.us-east-1.amazonaws.com,api.ecr.us-east-1.amazonaws.com,.dkr.ecr.us-east-1.amazonaws.com,kinesis.us-east-1.amazonaws.com,.data-kinesis.us-east-1.amazonaws.com,.control-kinesis.us-east-1.amazonaws.com,events.us-east-1.amazonaws.com,cloudformation.us-east-1.amazonaws.com,sts.us-east-1.amazonaws.com,application-autoscaling.us-east-1.amazonaws.com,monitoring.us-east-1.amazonaws.com,ecs.us-east-1.amazonaws.com,.execute-api.us-east-1.amazonaws.com`

建立外部資源

此 CloudFormation 堆疊會建立聯網、儲存體、作用中目錄和網域憑證（如果提供 PortalDomainName)。您必須擁有這些外部資源，才能部署產品。

您可以在部署之前下載配方範本。

部署時間：約 40-90 分鐘

1. 登入 AWS Management Console 並在 https：//https://console.aws.amazon.com/cloudformation 開啟 AWS CloudFormation 主控台。

> **Note**
> 請確定您在管理員帳戶中。

2. 在 主控台中啟動 範本。

   如果您要在 AWS GovCloud （美國西部） 區域中部署 ，請在 GovCloud 分割區帳戶中啟動範本。 GovCloud

3. 輸入範本參數：

參數	預設	描述
DomainName	`corp.res.com`	用於作用中目錄的網域。預設值會在設定引導使用者的`LDIF`檔案中提供。如果您想要使用預設使用者，請將 值保留為預設值。若要變更值，請更新並提供個別`LDIF`的檔案。這不需要符合用於 Active Directory 的網域。
SubDomain （僅限 GovCloud)		此參數對於商業區域為選用，但對於 GovCloud 區域為必要。 如果您提供 SubDomain，則參數會在提供的 DomainName 前綴。提供的 Active Directory 網域名稱將成為子網域。
AdminPassword		Active Directory 管理員的密碼 （使用者名稱 `Admin`)。此使用者會在初始引導階段的作用中目錄中建立，之後不會使用。

參數	預設	描述
		重要：此欄位的格式可以是 (1) 純文字密碼或 (2) 格式化為金鑰/值對之 AWS 秘密的 ARN`{"password":"somepassword"}`。 注意：此使用者的密碼必須符合 Active Directory 的密碼複雜性要求。
ServiceAccountPassword		用來建立服務帳戶的密碼 (`ReadOnlyUser`)。此帳戶用於同步處理。 重要：此欄位的格式可以是 (1) 純文字密碼或 (2) 格式化為金鑰/值對之 AWS 秘密的 ARN`{"password":"somepassword"}`。 注意：此使用者的密碼必須符合 Active Directory 的密碼複雜性要求。
金鑰對		使用 SSH 用戶端連接管理執行個體。 注意：AWS Systems Manager Session Manager 也可以用來連線至執行個體。

參數	預設	描述
LDIFS3Path	`aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res.ldif`	在 Active Directory 設定的引導階段期間匯入的 LDIF 檔案的 Amazon S3 路徑。如需詳細資訊，請參閱 LDIF Support。參數會預先填入檔案，該檔案會在 Active Directory 中建立多個使用者。 若要檢視檔案，請參閱 GitHub 中可用的 res.ldif 檔案。
ClientIpCidr		您將從中存取網站的 IP 地址。例如，您可以選取 IP 地址，並使用 `[IPADDRESS]/32` 僅允許從主機存取。您可以更新此後部署。
ClientPrefixList		輸入字首清單以提供對作用中目錄管理節點的存取。如需建立受管字首清單的資訊，請參閱使用客戶受管字首清單。
EnvironmentName	`res-`*`[environment name]`*	如果`PortalDomainName` 提供 ，此參數會用來將標籤新增至產生的秘密，以便在環境中使用。這需要符合建立 RES 堆疊時使用的`EnvironmentName` 參數。如果您要在帳戶中部署多個環境，這將必須是唯一的。

參數	預設	描述
PortalDomainName		對於 GovCloud 部署，請勿輸入此參數。憑證和秘密是在先決條件期間手動建立的。帳戶在 Amazon Route 53 中的網域名稱。如果提供此功能，則會產生並上傳公有憑證和金鑰檔案 AWS Secrets Manager。如果您有自己的網域和憑證，此參數和 `EnvironmentName` 可以保留空白。

4. 確認功能中的所有核取方塊，然後選擇建立堆疊。

步驟 1：啟動產品

請依照本節中的step-by-step說明，設定並將產品部署至您的帳戶。

部署時間：約 60 分鐘

您可以在部署之前下載此產品的 CloudFormation 範本。

如果您要部署 in AWS GovCloud（美國西部），請使用此範本。

res-stack - 使用此範本啟動產品和所有相關聯的元件。預設組態會部署 RES 主要堆疊和身分驗證、前端和後端資源。

> **Note**
>
> AWS CloudFormation 資源是從 AWS Cloud Development Kit (AWS CDK) (AWS CDK) 建構模組建立的。

AWS CloudFormation 範本會在 AWS 的 上部署 Research and Engineering Studio AWS 雲端。您必須先符合先決條件，才能啟動堆疊。

1. 登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/cloudformation 開啟 AWS CloudFormation 主控台。
2. 啟動範本 。

   若要部署 in AWS GovCloud （美國西部），請啟動此範本。
3. 根據預設，範本會在美國東部（維吉尼亞北部）區域啟動。若要在不同的 中啟動解決方案 AWS 區域，請使用主控台導覽列中的區域選擇器。

> **Note**
>
> 此產品使用 Amazon Cognito 服務，目前尚未在所有 中提供 AWS 區域。您必須在可使用 Amazon Cognito AWS 區域 的 中啟動此產品。如需各區域的最新可用性，請參閱 AWS 區域 al Services List。

4. 在參數下，檢閱此產品範本的參數，並視需要修改。如果您部署了自動化外部資源，您可以在外部資源堆疊的輸出索引標籤中找到這些參數。

參數	預設	描述
EnvironmentName	*#res-demo#*	提供給 RES 環境的唯一名稱，以 res- 開頭，長度不可超過 11 個字元，也不可使用大寫字母。
AdministratorEmail		使用者完成產品設定的電子郵件地址。如果有作用中目錄單一登入整合失敗，此使用者也會充當中斷玻璃使用者。
InfrastructureHostAMI	ami-*########*	（選用）您可以提供用於所有基礎設施主機的自訂 AMI ID。目前支援的OSes為 Amazon Linux 2、RHEL8, RHEL9、Windows Server 2019 和 2022 (x86)，以及 Windows 10 和 11。如需詳

參數	預設	描述
		細資訊，請參閱準備 Amazon Machine Image AMIs)。
SSHKeyPair		用來連線至基礎設施主機的金鑰對。
ClientIP	*x.x.x*.0/24 或 *x.x.x*.0/32	IP 地址篩選條件會限制與系統的連線。您可以在部署之後更新 ClientIpCidr。
ClientPrefixList		（選用）為允許直接存取堡壘主機中的 Web UI 和 SSH 的 IPs 提供受管字首清單。
IAMPermissionBoundary		（選用）您可以提供受管政策 ARN，該政策將做為許可界限連接到 RES 中建立的所有角色。如需詳細資訊，請參閱設定自訂許可界限。
VpcId		執行個體將啟動的 VPC ID。
IsLoadBalancerInternetFacing		選取 true 以部署面向網際網路的負載平衡器（負載平衡器需要公有子網路）。對於需要限制網際網路存取的部署，請選取 false。
LoadBalancerSubnets		在負載平衡器將啟動的不同可用區域中，選取至少兩個子網路。對於需要限制網際網路存取的部署，請選取私有子網路。對於需要網際網路存取的部署，請選取公有子網路。如果外部聯網堆疊建立超過兩個，請選取所有已建立的項目。

參數	預設	描述
InfrastructureHostSubnets		在基礎設施主機將啟動的不同可用區域中，選取至少兩個私有子網路。如果外部聯網堆疊建立超過兩個，請選取所有已建立的項目。
VdiSubnets		在 VDI 執行個體將啟動的不同可用區域中，選取至少兩個私有子網路。如果外部聯網堆疊建立超過兩個，請選取所有已建立的項目。
ActiveDirectoryName	*corp.res.com*	作用中目錄的網域。它不需要符合入口網站網域名稱。
ADShortName	*corp*	作用中目錄的簡短名稱。這也稱為 NetBIOS 名稱。
LDAP 基礎	***DC=corp,DC=res,DC=com***	LDAP 階層中基礎的 LDAP 路徑。
LDAPConnectionURI		可由作用中目錄的主機伺服器到達的單一 ldap：// 路徑。如果您使用預設 AD 網域部署自動化外部資源，則可以使用 ldap：//corp.res.com。
ServiceAccountCredentialsSecretArn		提供秘密 ARN，其中包含 Active Directory ServiceAccount 使用者的使用者名稱和密碼，格式為 username：password key/value 對。
UsersOU		AD 內將同步的使用者的組織單位。

參數	預設	描述
GroupsOU		AD 內將同步之群組的組織單位。
SudoersGroupName	RESAdministrators	群組名稱，其中包含在安裝時執行個體上具有sudoer 存取權的所有使用者，以及在 RES 上具有管理員存取權的所有使用者。
ComputersOU		AD 內執行個體將加入的組織單位。
DomainTLSCertificateSecretARN		（選用）提供網域 TLS 憑證秘密 ARN，以啟用與 AD 的 TLS 通訊。
EnableLdapIDMapping		決定 UID 和 GID 號碼是由 SSSD 產生，還是使用 AD 提供的號碼。設為 True 以使用 SSSD 產生的 UID 和 GID，或設為 False 以使用 AD 提供的 UID 和 GID。在大多數情況下，此參數應該設定為 True。
DisableADJoin	False	若要防止 Linux 主機加入目錄網域，請將 變更為 True。否則，請保留 False 的預設設定。
ServiceAccountUserDN		在目錄中提供服務帳戶使用者的辨別名稱 (DN)。
SharedHomeFilesystemID		用於 Linux VDI 主機之共用主檔案系統的 EFS ID。

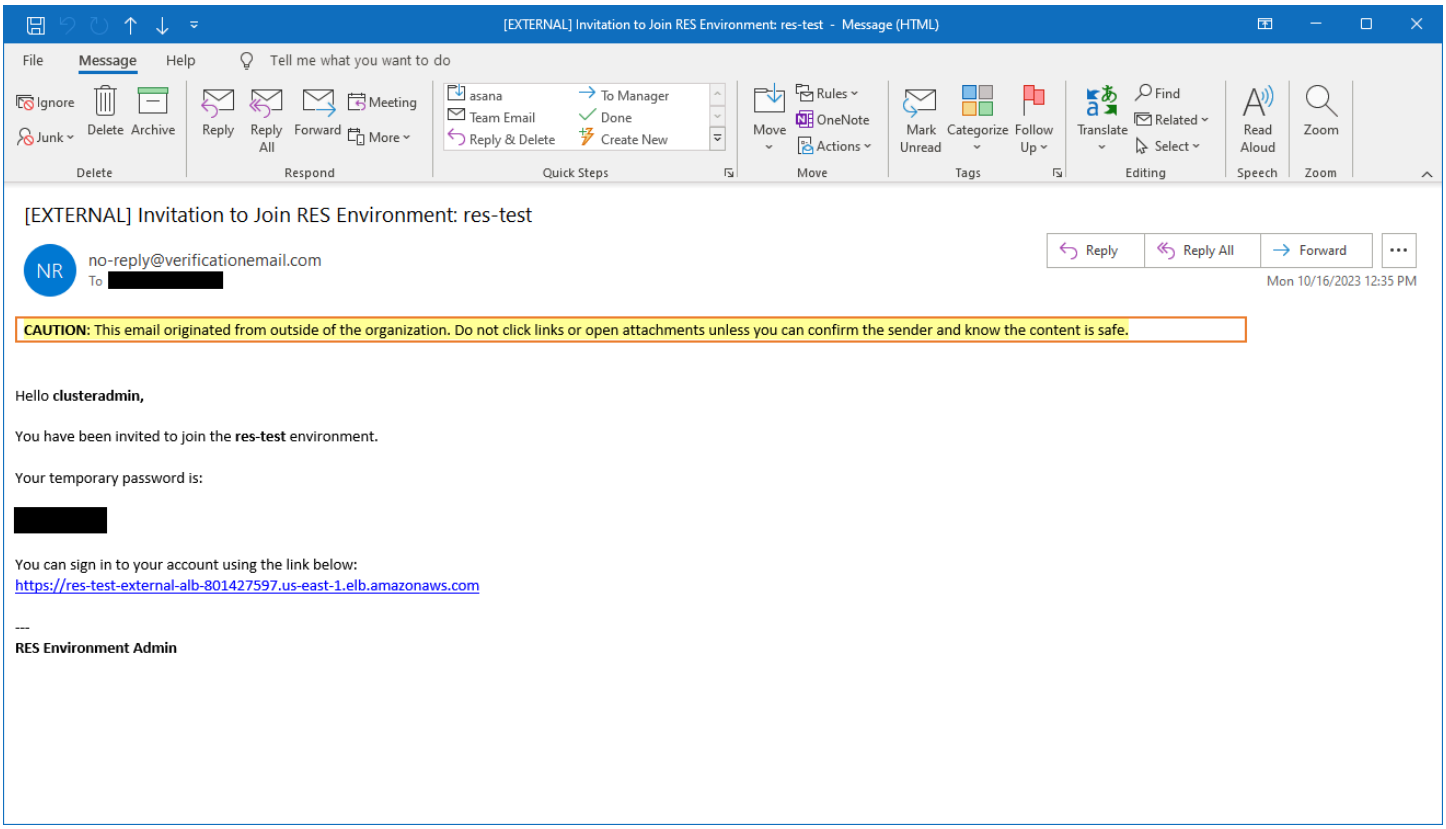
參數	預設	描述
CustomDomainNamefo rWebApp		（選用） Web 入口網站用來提供系統 Web 部分連結的子網域。
CustomDomainNameforVDI		（選用） Web 入口網站用來提供系統 VDI 部分連結的子網域。
ACMCertificateARNf orWebApp		（選用） 使用預設組態時，產品會在網域 amazonaws .com 下託管 Web 應用程式。您可以在網域下託管產品服務。如果您部署了自動化外部資源，則會為您產生此資源，您可以在 res-bi 堆疊的輸出中找到此資訊。如果您需要為 Web 應用程式產生憑證，請參閱 組態指南。
CertificateSecretARNforVDI		（選用） 此 ARN 秘密會儲存 Web 入口網站公有憑證的公有憑證。如果您為自動化外部資源設定入口網站網域名稱，您可以在 res-bi 堆疊的輸出索引標籤下找到此值。
PrivateKeySecretARNforVDI		（選用） 此 ARN 秘密會儲存 Web 入口網站憑證的私有金鑰。如果您為自動化外部資源設定入口網站網域名稱，您可以在 res-bi 堆疊的輸出索引標籤下找到此值。

5. 選擇 Create stack (建立堆疊) 以部署堆疊。

您可以在狀態欄的 AWS CloudFormation 主控台中檢視堆疊的狀態。您應該會在大約 60 分鐘內收到 CREATE_COMPLETE 狀態。

步驟 2：第一次登入

產品堆疊部署到您的帳戶後，您會收到包含登入資料的電子郵件。使用 URL 登入您的帳戶，並為其他使用者設定工作區。



第一次登入後，您可以在 Web 入口網站中設定 設定以連線到 SSO 供應商。如需部署後組態資訊，請參閱 組態指南。請注意， `clusteradmin` 是突破性的帳戶 — 您可以使用它來建立專案，並將使用者或群組成員資格指派給這些專案；它無法自行指派軟體堆疊或部署桌面。

更新產品

Research and Engineering Studio (RES) 有兩種更新產品的方法，取決於版本更新是主要更新還是次要更新。

RES 使用以日期為基礎的版本控制方案。主要版本使用年和月，次要版本會視需要新增序號。例如，2024.01 版已於 2024 年 1 月發行為主要版本；2024.01.01 版是該版本的次要版本更新。

主題

- 主要版本更新
- 次要版本更新

主要版本更新

Research and Engineering Studio 使用快照來支援從先前的 RES 環境遷移至最新的 ，而不會遺失您的環境設定。您也可以在加入使用者之前，使用此程序來測試和驗證您環境的更新。

若要使用最新版本的 RES 更新您的環境：

1. 建立目前環境的快照。請參閱 the section called “建立快照”。
2. 使用新版本重新部署 RES。請參閱 the section called “步驟 1：啟動產品”。
3. 將快照套用至已更新的環境。請參閱 the section called “套用快照”。
4. 驗證所有資料是否成功遷移至新環境。

次要版本更新

對於 RES 的次要版本更新，不需要新的安裝。您可以更新現有 RES 堆疊的 AWS CloudFormation 範本。部署更新 AWS CloudFormation 之前，請先在 中檢查目前 RES 環境的版本。您可以在範本的開頭找到版本編號。

例如：`"Description": "RES_2024.1"`

若要進行次要版本更新：

1. 在 中下載最新的 AWS CloudFormation 範本the section called “步驟 1：啟動產品”。
2. 在 https：//https://console.aws.amazon.com/cloudformation 開啟 AWS CloudFormation 主控台。

3. 從 Stacks 中，尋找並選取主要堆疊。它應該顯示為 `<stack-name>`。
4. 選擇更新。
5. 選擇取代目前範本。
6. 針對 Template source (範本來源)，選擇 Upload a template file (上傳範本檔案)。
7. 選擇選擇檔案並上傳您下載的範本。
8. 在指定堆疊詳細資訊上，選擇下一步。您不需要更新參數。
9. 在設定堆疊選項上，選擇下一步。
10. 在檢閱 <stack-name> 時，選擇提交。

解除安裝產品

您可以從 AWS Management Console 或使用 在 AWS 產品上解除安裝 Research and Engineering Studio AWS Command Line Interface。您必須手動刪除此產品建立的 Amazon Simple Storage Service (Amazon S3) 儲存貯體。如果您有要保留的儲存資料，此產品不會自動刪除 <EnvironmentName>-shared-storage-security-group。

使用 AWS Management Console

1. 登入 AWS CloudFormation 主控台。
2. 在堆疊頁面上，選取此產品的安裝堆疊。
3. 選擇 刪除。

使用 AWS Command Line Interface

判斷 AWS Command Line Interface (AWS CLI) 是否在您的環境中可用。如需安裝說明，請參閱《AWS CLI 使用者指南》中的什麼是 AWS Command Line Interface。確認 AWS CLI 可用且已設定為部署產品所在區域的管理員帳戶後，請執行下列命令。

```
$ aws cloudformation delete-stack --stack-name <RES-stack-name>
```

刪除 shared-storage-security-group

> **Warning**
>
> 產品預設會保留此檔案系統，以防止意外資料遺失。如果您選擇刪除安全群組和相關聯的檔案系統，這些系統內保留的任何資料都會永久刪除。建議您備份資料或將資料重新指派給新的安全群組。

1. 登入 AWS Management Console ，並在 https://console.aws.amazon.com/efs/ ：// 開啟 Amazon EFS 主控台。
2. 刪除與 相關聯的所有檔案系統`<RES-stack-name>-shared-storage-security-group`。或者，您可以將這些檔案系統重新指派給另一個安全群組，以維護資料。

3. 登入 AWS Management Console ，並在 https://console.aws.amazon.com/ec2/：// 開啟 Amazon EC2 主控台。
4. 刪除`<RES-stack-name>`-shared-storage-security-group。

刪除 Amazon S3 儲存貯體

如果您決定刪除 AWS CloudFormation 堆疊以防止意外資料遺失，此產品會設定為保留產品建立的 Amazon S3 儲存貯體（用於在選擇加入區域中部署）。解除安裝產品後，如果您不需要保留資料，您可以手動刪除此 S3 儲存貯體。請依照下列步驟刪除 Amazon S3 儲存貯體。

1. 登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/s3/ 開啟 Amazon S3 主控台。
2. 導覽窗格中的 ChooseBuckets。
3. 找到 S3 儲存`stack-name`貯體。
4. 選取每個 Amazon S3 儲存貯體，然後選擇空白。您必須清空每個儲存貯體。
5. 選取 S3 儲存貯體，然後選擇刪除。

若要使用 刪除 S3 儲存貯體 AWS CLI，請執行下列命令：

```
$ aws s3 rb s3://<bucket-name> --force
```

> **Note**
>
> `--force` 命令會清空其內容的儲存貯體。

組態指南

此組態指南為技術對象提供部署後的指示，說明如何進一步自訂並與 AWS 產品上的 Research and Engineering Studio 整合。

主題

- 身分管理
- 建立子網域
- 建立 ACM 憑證
- Amazon CloudWatch Logs
- 設定自訂許可界限
- 設定 RES 就緒 AMIs

身分管理

Research and Engineering Studio 可以使用任何 SAML 2.0 相容身分提供者。若要使用 Amazon Cognito 做為原生使用者目錄，允許使用者登入具有 Cognito 使用者身分的 Web 入口網站和 Linux 型 VDIs，請參閱 設定 Amazon Cognito 使用者。如果您使用外部資源或計劃使用 IAM Identity Center 部署 RES，請參閱 使用 IAM Identity Center 設定單一登入 (SSO)。如果您有自己的 SAML 2.0 相容身分提供者，請參閱 為單一登入 (SSO) 設定您的身分提供者。

主題

- 設定 Amazon Cognito 使用者
- Active Directory 同步
- 使用 IAM Identity Center 設定單一登入 (SSO)
- 為單一登入 (SSO) 設定您的身分提供者
- 設定使用者的密碼

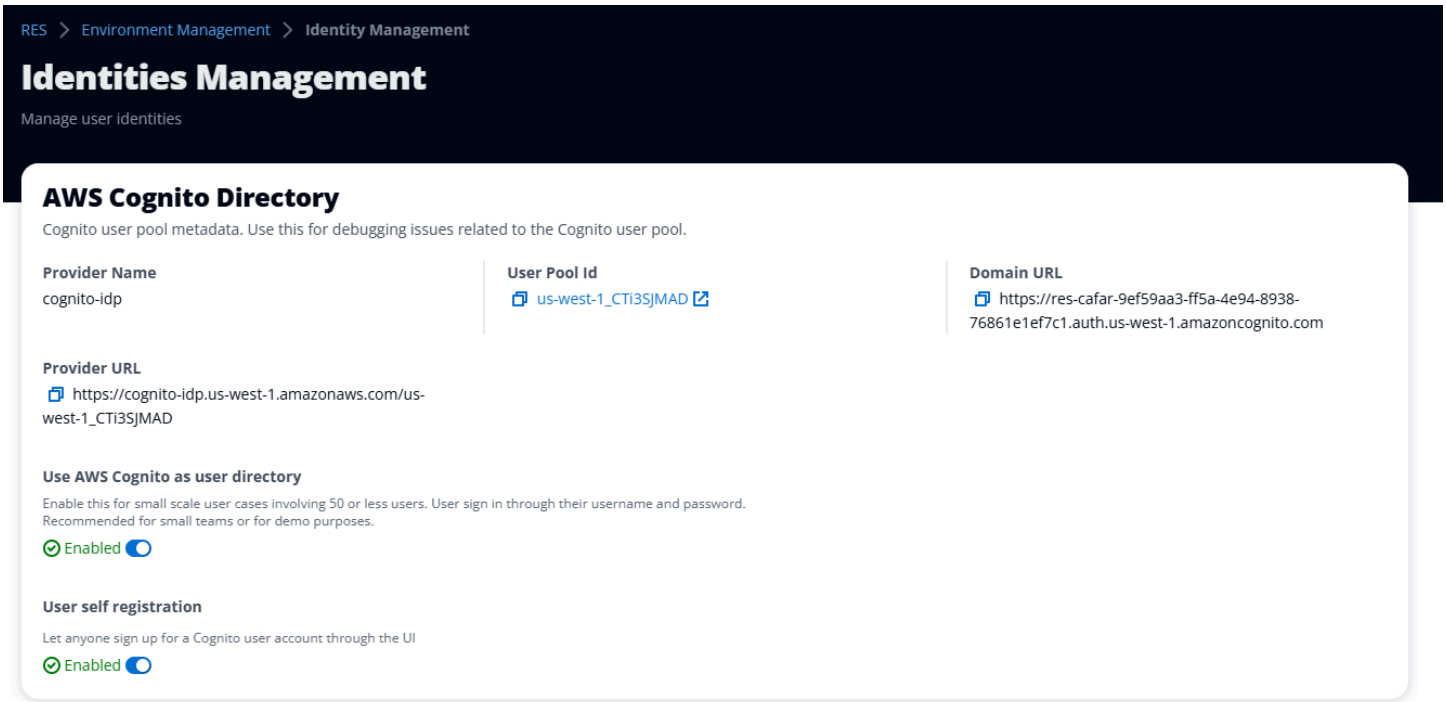
設定 Amazon Cognito 使用者

研究與工程 Studio (RES) 可讓您將 Amazon Cognito 設定為原生使用者目錄。這可讓使用者使用 Amazon Cognito 使用者身分登入 Web 入口網站和 Linux 型 VDIs。管理員可以從 AWS 主控台使用 csv 檔案將多個使用者匯入使用者集區。如需大量使用者匯入的詳細資訊，請參閱《Amazon Cognito

開發人員指南》中的從 CSV 檔案將使用者匯入使用者集區。RES 支援同時使用 Amazon Cognito 型原生使用者目錄和 SSO。

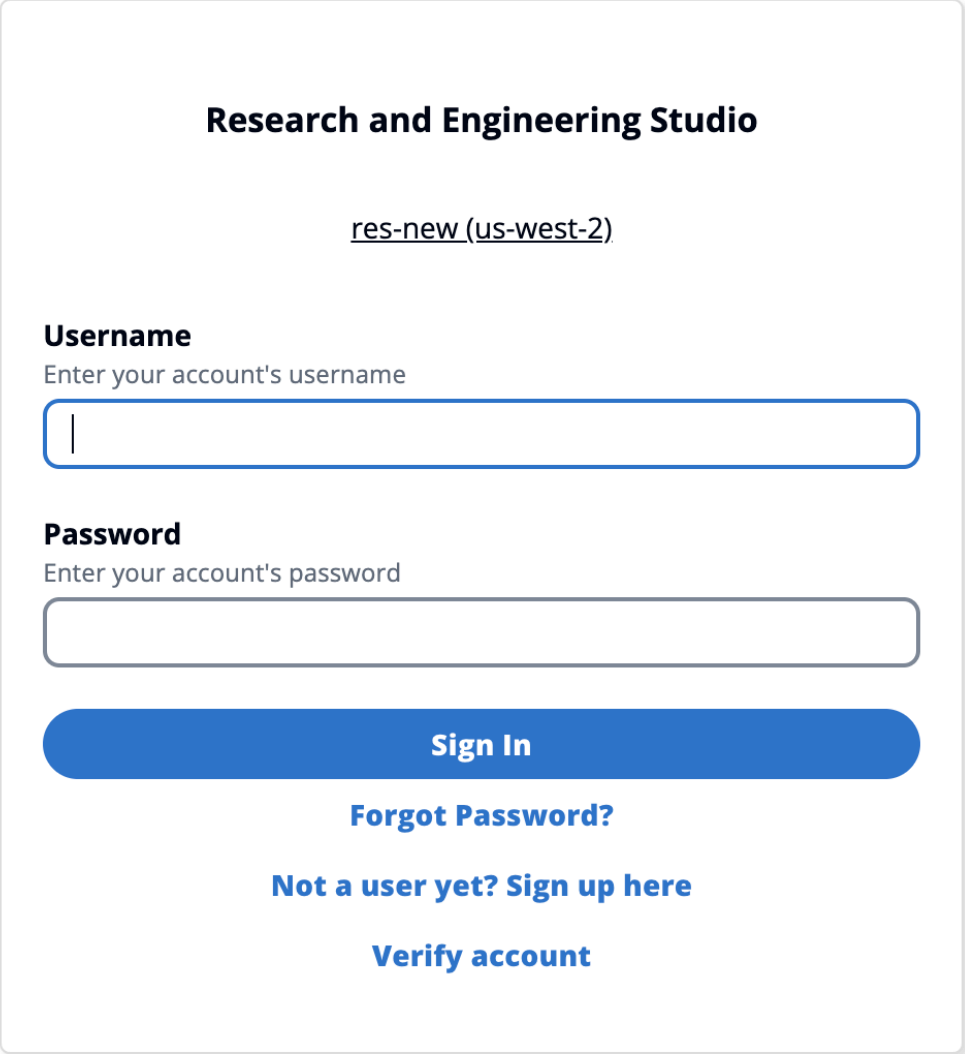
管理設定

身為 RES 管理員，若要將 RES 環境設定為使用 Amazon Cognito 做為使用者目錄，請在可從環境管理頁面存取的身分管理頁面上切換使用 Amazon Cognito 做為使用者目錄按鈕。若要允許使用者自行註冊，請切換相同頁面上的使用者自行註冊按鈕。



使用者在流程中註冊/登入

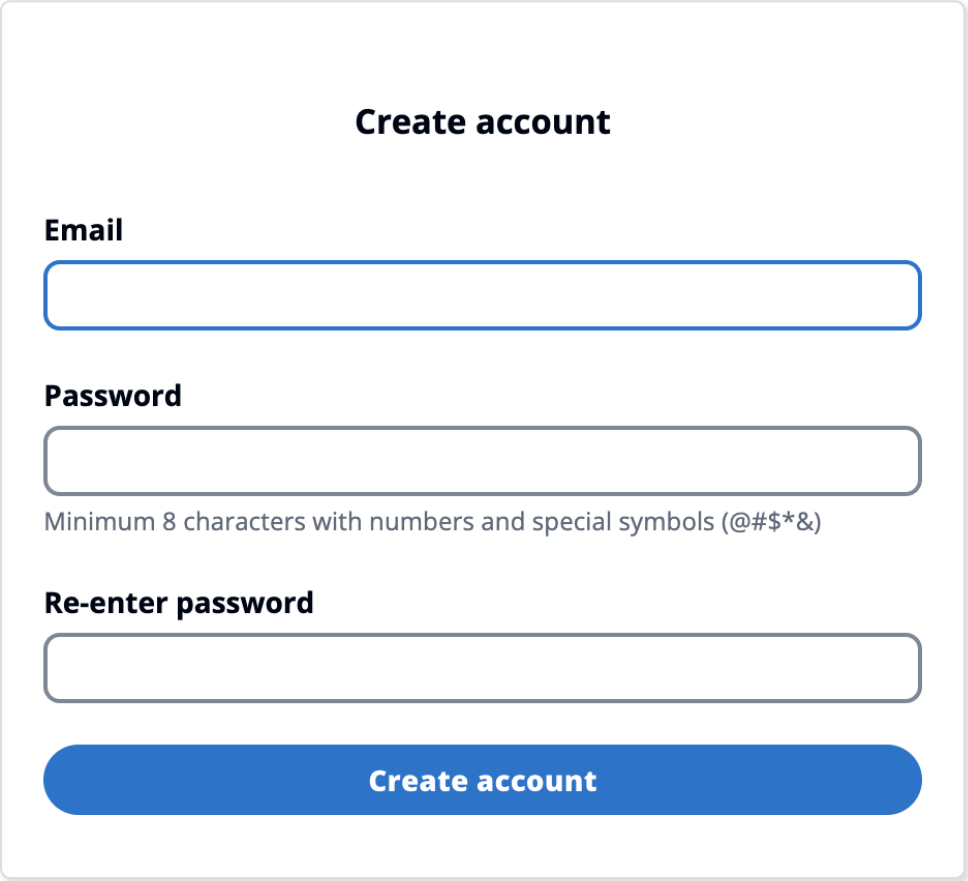
如果已啟用使用者自我註冊，您可以為使用者提供 Web 應用程式的 URL。在那裡，使用者會找到顯示還不是使用者的選項？ 在這裡註冊。



Copyright 2023 Amazon Inc. or its affiliates. All Rights Reserved.

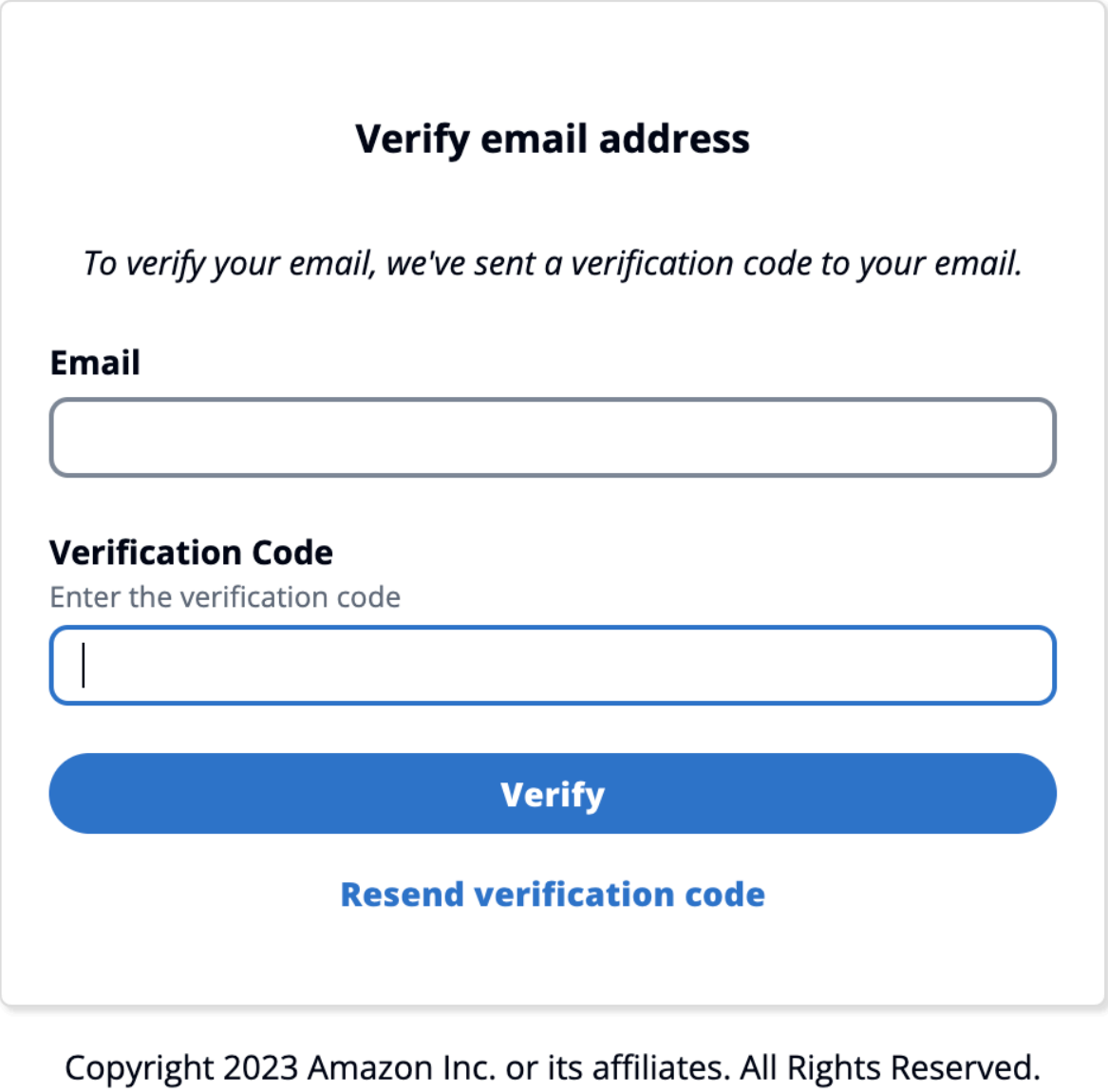
註冊流程

選擇還不是使用者的使用者？ 在此註冊時，系統會要求您輸入其電子郵件和密碼來建立 帳戶。

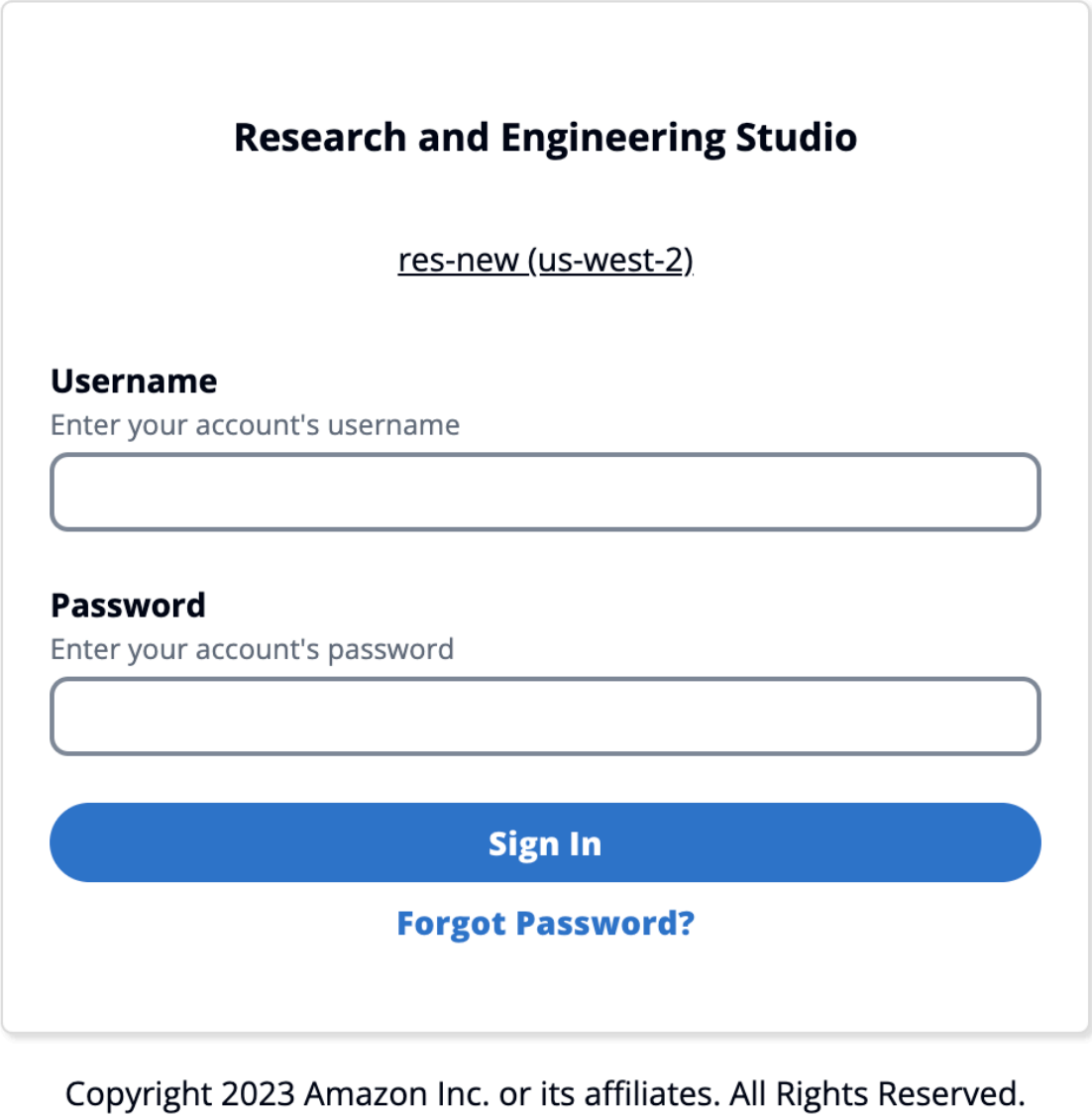


Copyright 2023 Amazon Inc. or its affiliates. All Rights Reserved.

在註冊流程中，系統會要求使用者輸入電子郵件中收到的驗證碼，以完成註冊程序。

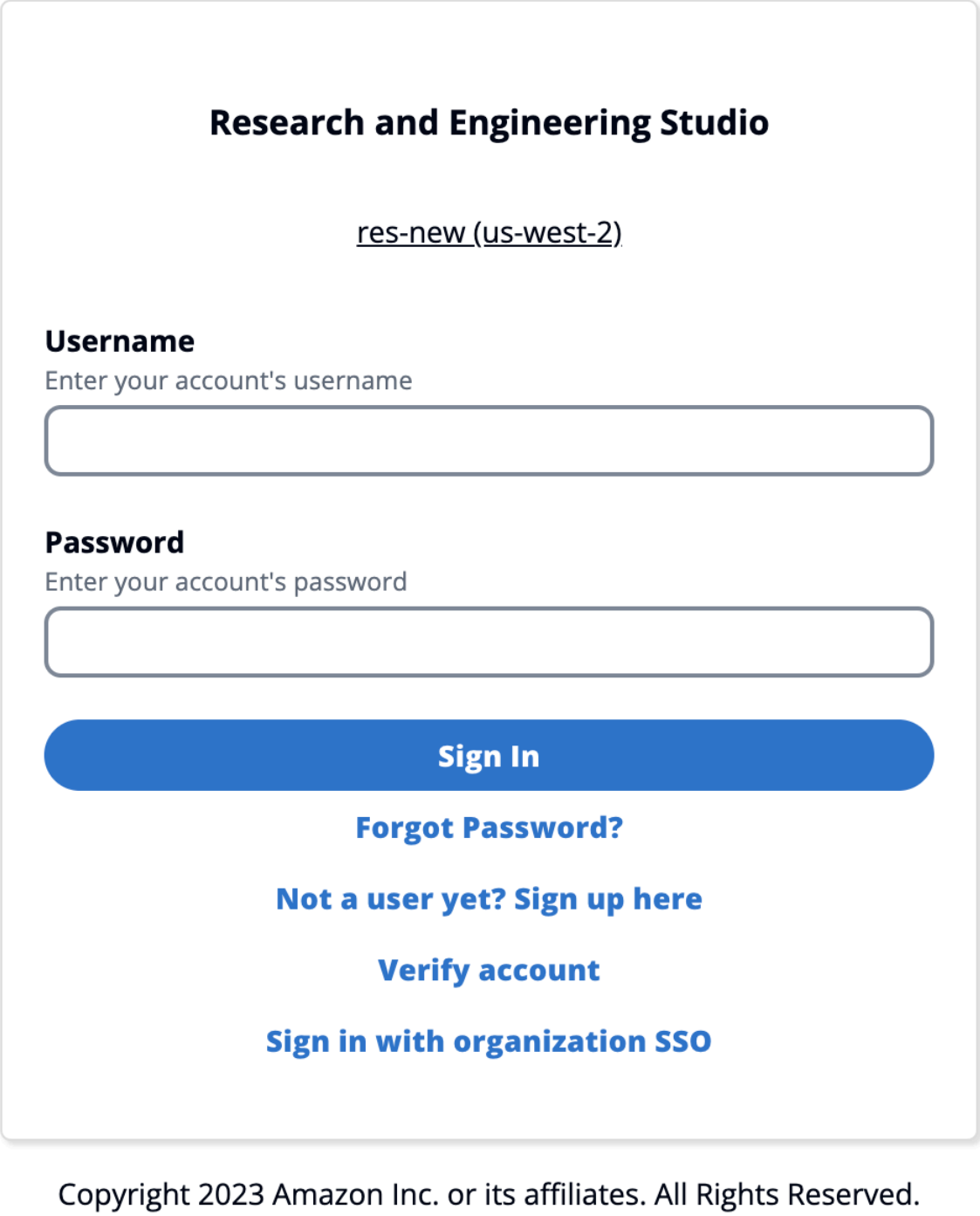


如果停用自我註冊，使用者將不會看到註冊連結。管理員必須在 RES 外部的 Amazon Cognito 中設定使用者。（請參閱《Amazon Cognito 開發人員指南》中的以管理員身分建立使用者帳戶。）



登入頁面選項

如果同時啟用 SSO 和 Amazon Cognito，則會顯示使用組織 SSO 登入的選項。當使用者按一下該選項時，它會將其重新路由至其 SSO 登入頁面。根據預設，如果啟用 Amazon Cognito，使用者將會進行身分驗證。



限制

- 您的 Amazon Cognito 群組名稱最多可有六個字母；只接受小寫字母。
- Amazon Cognito 註冊不允許兩個具有相同使用者名稱但不同網域地址的電子郵件地址。

- 如果同時啟用 Active Directory 和 Amazon Cognito，且系統偵測到重複的使用者名稱，則僅允許 Active Directory 使用者進行身分驗證。管理員應採取步驟，不設定 Amazon Cognito 與其 Active Directory 之間的重複使用者名稱。
- 不允許 Cognito 使用者啟動 Windows 型 VDIs因為 RES 不支援 Windows 執行個體的 Amazon Cognito 型身分驗證。

同步

RES 每小時同步其資料庫與來自 Amazon Cognito 的使用者和群組資訊。屬於群組「管理員」的任何使用者都會在其 VDIs 中獲得 sudo 權限。

您也可以從 Lambda 主控台手動啟動同步。

手動啟動同步程序：

1. 開啟 Lambda 主控台。
2. 搜尋 Cognito 同步 Lambda。此 Lambda 遵循此命名慣
   例：`{RES_ENVIRONMENT_NAME}_cognito-sync-lambda`。
3. 選取測試。
4. 在測試事件區段中，選擇右上角的測試按鈕。事件內文格式並不重要。

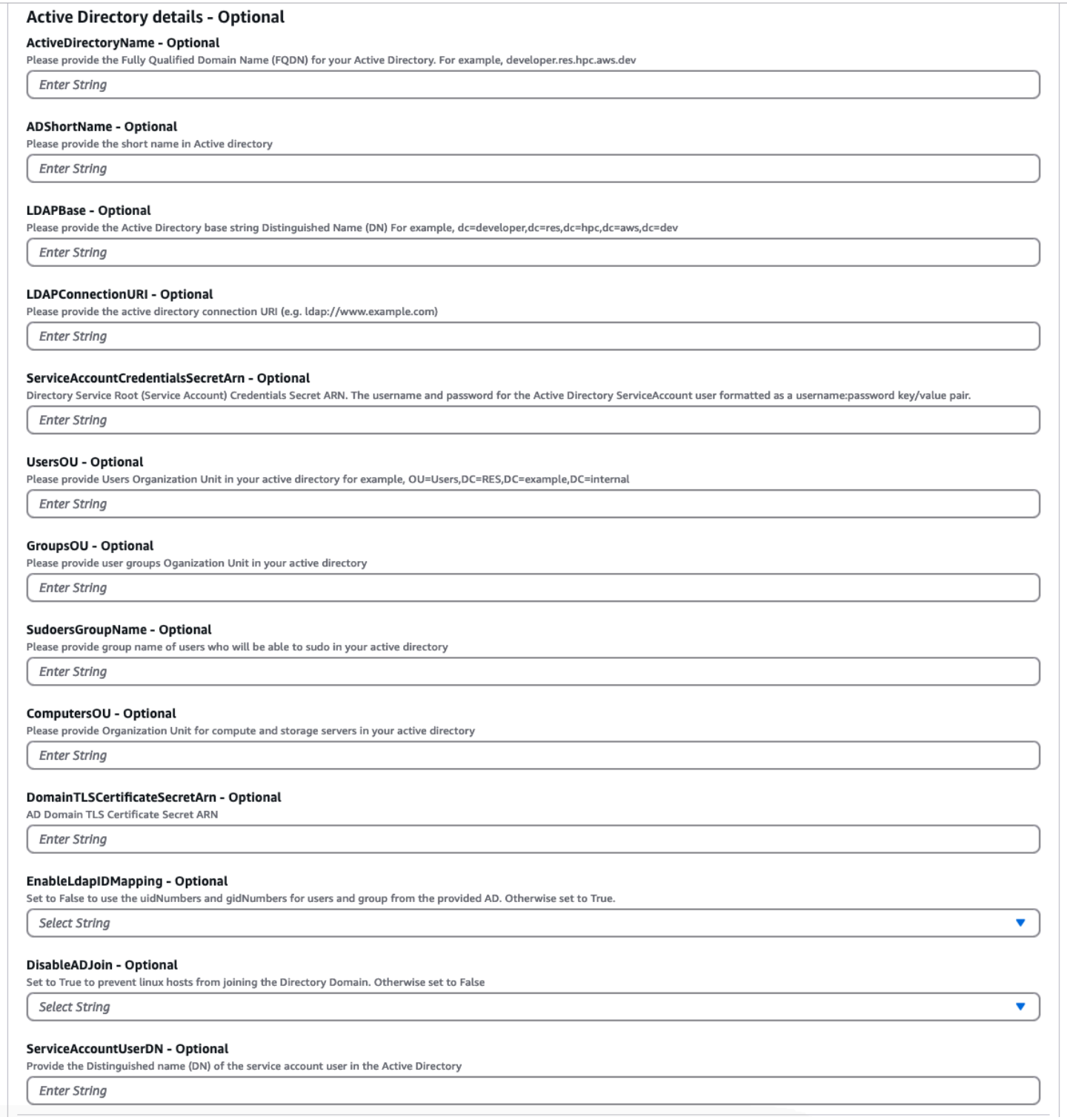
Cognito 的安全考量

在 2024.12 版本之前，預設會啟用使用者活動記錄，這是 Amazon Cognito Plus 計劃功能的一部分。我們從基準部署中移除此項目，為想要嘗試 RES 的客戶節省成本。您可以視需要重新啟用此功能，以符合組織的雲端安全設定。

Active Directory 同步

執行期組態

安裝期間，與 Active Directory (AD) 相關的所有 CFN 參數都是選用的。

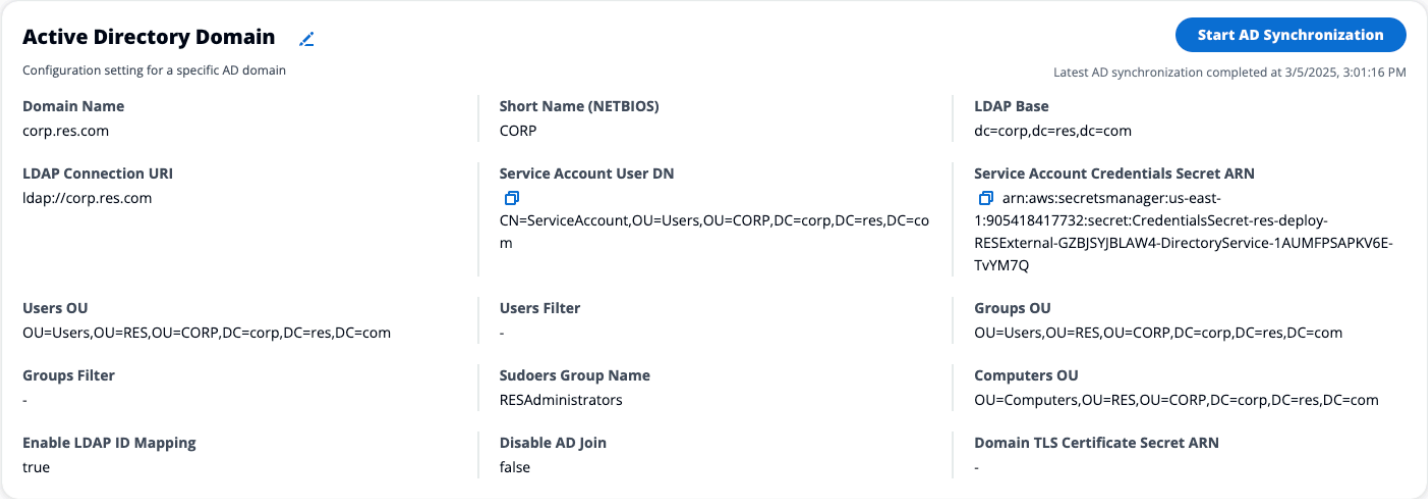


對於執行時間提供的任何秘密 ARN （例如 `ServiceAccountCredentialsSecretArn`或 `DomainTLSCertificateSecretArn`），請務必將下列標籤新增至 RES 的秘密，以取得讀取秘密值的許可：

- 金鑰：`res:EnvironmentName`，值： *`<your RES environment name>`*
- 金鑰：`res:ModuleName`，值： `directoryservice`

Web 入口網站中的任何 AD 組態更新都會在下一次排定的 AD 同步期間自動取得（每小時）。使用者可能需要在變更 AD 組態後重新設定 SSO（例如，如果切換到不同的 AD)。

初次安裝後，管理員可以在身分管理頁面下的 RES Web 入口網站中檢視或編輯 AD 組態：



Active Directory Synchronization

Active Directory Name
Type the name for the Active Directory. It does not need to match the portal domain name.

corp.res.com

Short Name (NETBIOS)
Provide the short name for the Active Directory. This is also called the netBIOS name.

CORP

Service Account User DN
Provide the distinguished name (DN) of the service account user in Directory.

CN=ServiceAccount,OU=Users,OU=CORP,DC=corp,DC=res,DC=com

Service Account Credentials Secret ARN
Provide a Secret ARN which contains the username and password for the Active Directory ServiceAccount user, formatted as a username:password key/value pair.

arn:aws:secretsmanager:us-east-2:992382841930:secret:CredentialsSecret-BI-Dire

The secret should contain the username and password in the format username:password.

LDAP Connection URI
Specify the connection URI for the Active Directory server.

ldap://corp.res.com

LDAP Base
Specify the LDAP path within the directory hierarchy.

dc=corp,dc=res,dc=com

☐ **Disable Active Directory Join**
To prevent Linux hosts from joining the directory domain, check the box. Otherwise, leave in the default setting of unchecked.

☐ **Enable LDAP ID Mapping**
Determines if UID and GID numbers are generated by SSSD or if the numbers provided by the AD are used. Check to use SSSD generated UID and GID, or uncheck to use UID and GID provided by the AD. For most cases this parameter should be checked.

Organizational Units (OU)
Provide the Organizational Unit within AD that will sync.

Users OU

其他設定

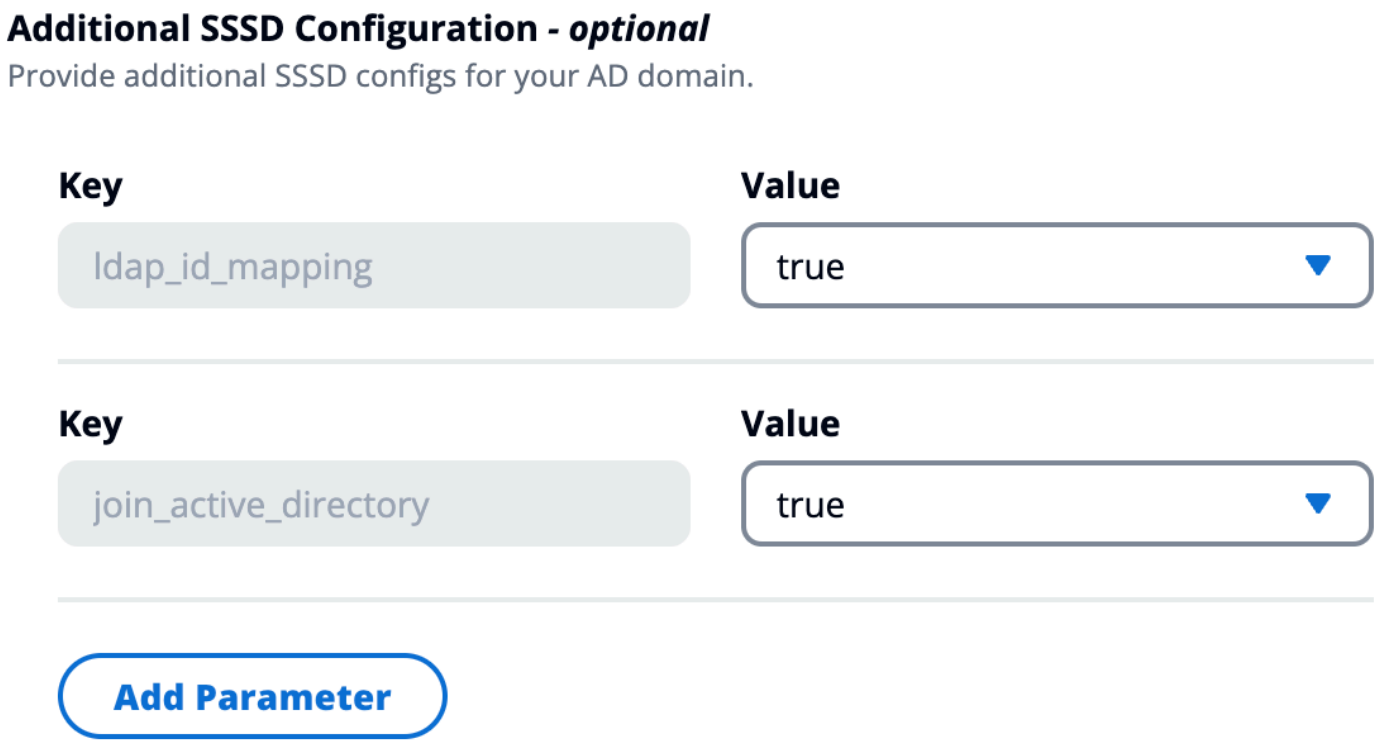
篩選條件

管理員可以使用使用者篩選和群組篩選選項篩選要同步的使用者或群組。篩選條件必須遵循 LDAP 篩選條件語法。範例篩選條件為：

```
(sAMAccountname=<user>)
```

自訂 SSSD 參數

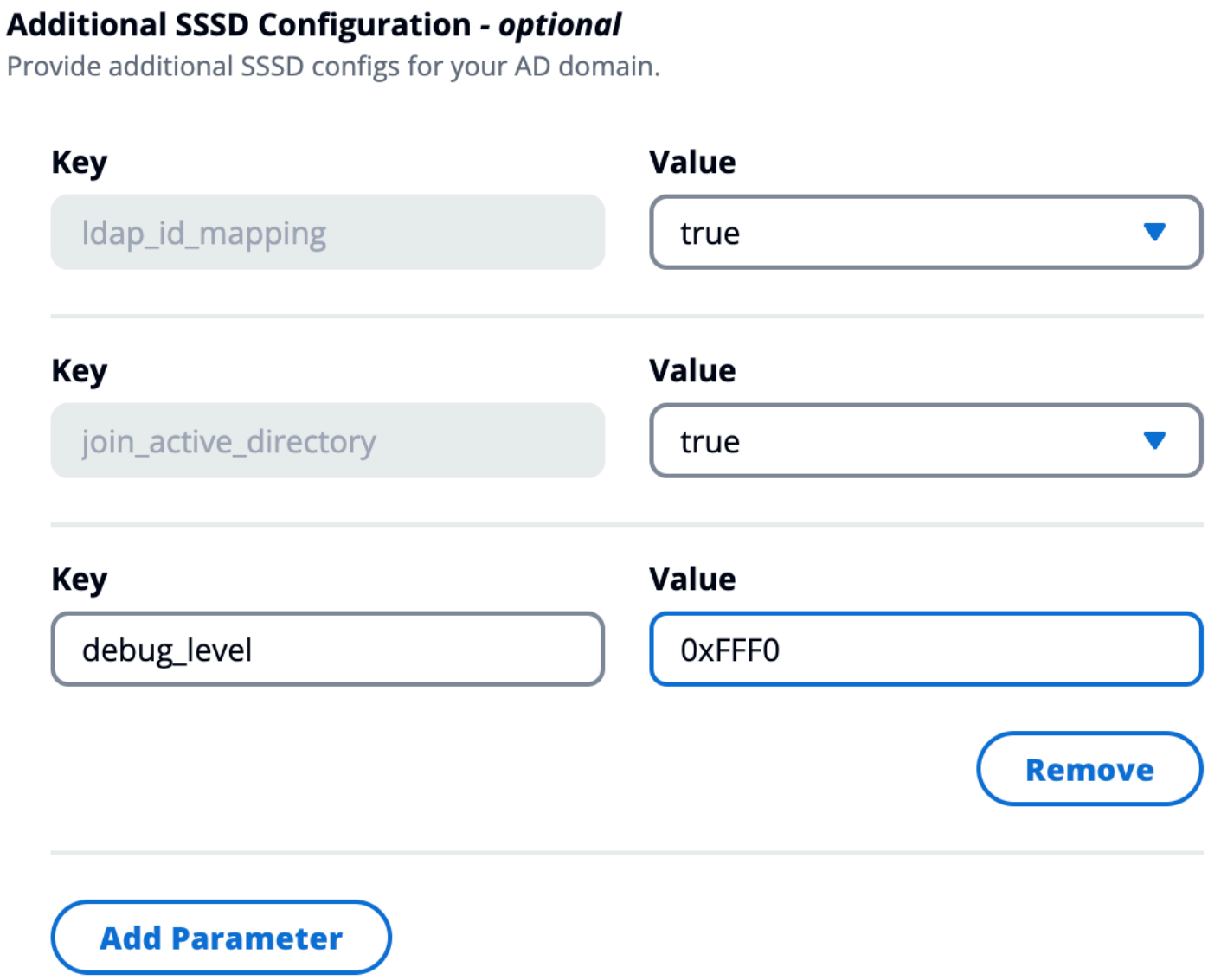
管理員可以提供索引鍵/值對的字典，其中包含要寫入叢集執行個體上 SSSD 組態檔案 `[domain_type/DOMAIN_NAME]` 區段的 SSSD 參數和值。RES 會自動套用 SSSD 更新 – 它會重新啟動叢集執行個體上的 SSSD 服務，並觸發 AD 同步程序。如需 SSSD 組態檔案的完整說明，請參閱的 Linux 手冊頁面SSSD。



SSSD 參數和值必須與 RES SSSD 組態相容，如下所述：

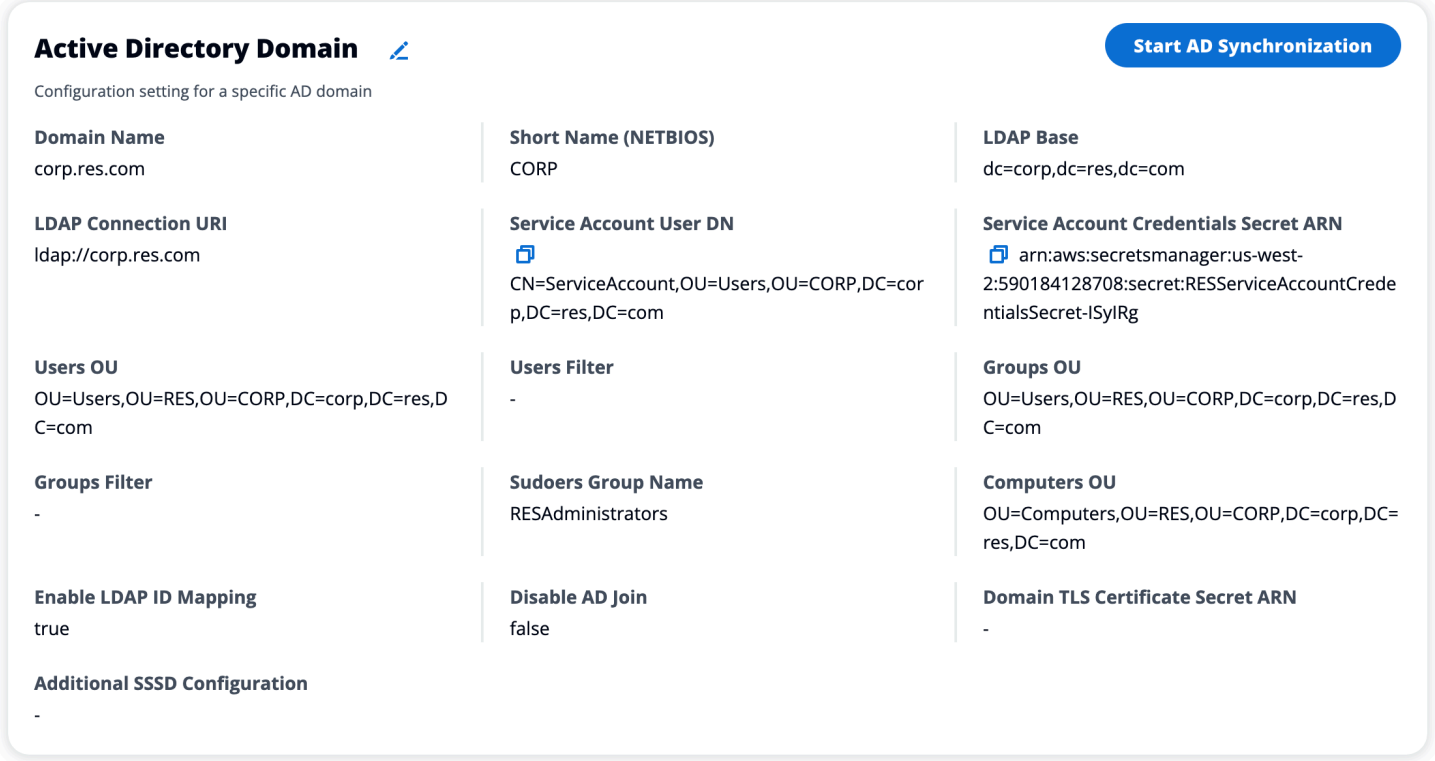
- `id_provider` 由 RES 內部設定，不得修改。
- AD 相關組態，包括 `ldap_uri`、 `ldap_search_base``ldap_default_bind_dn`和 `ldap_default_authtok` 是根據其他提供的 AD 組態設定，不得修改。

下列範例會啟用 SSSD 日誌的偵錯層級：

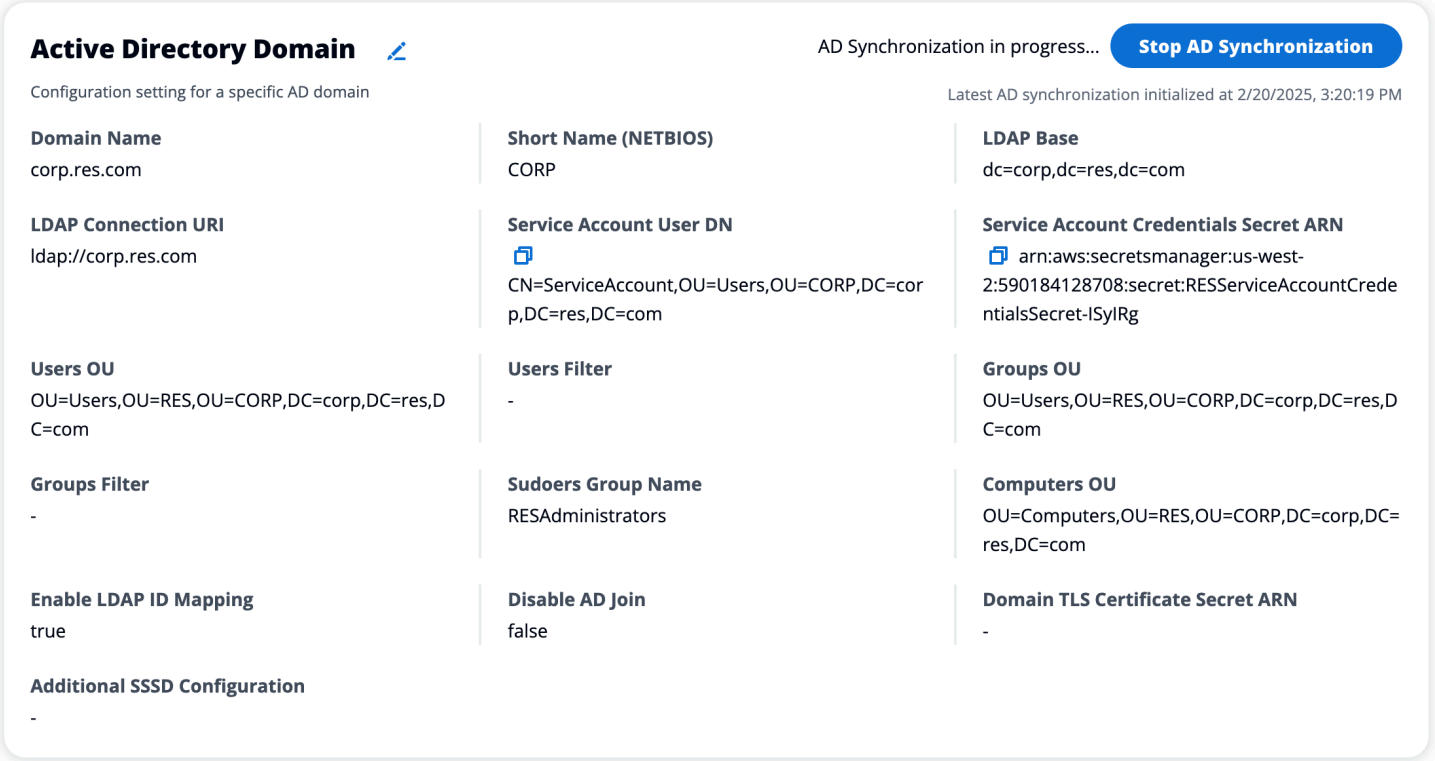


如何手動啟動或停止同步 (2025.03 及更新版本)

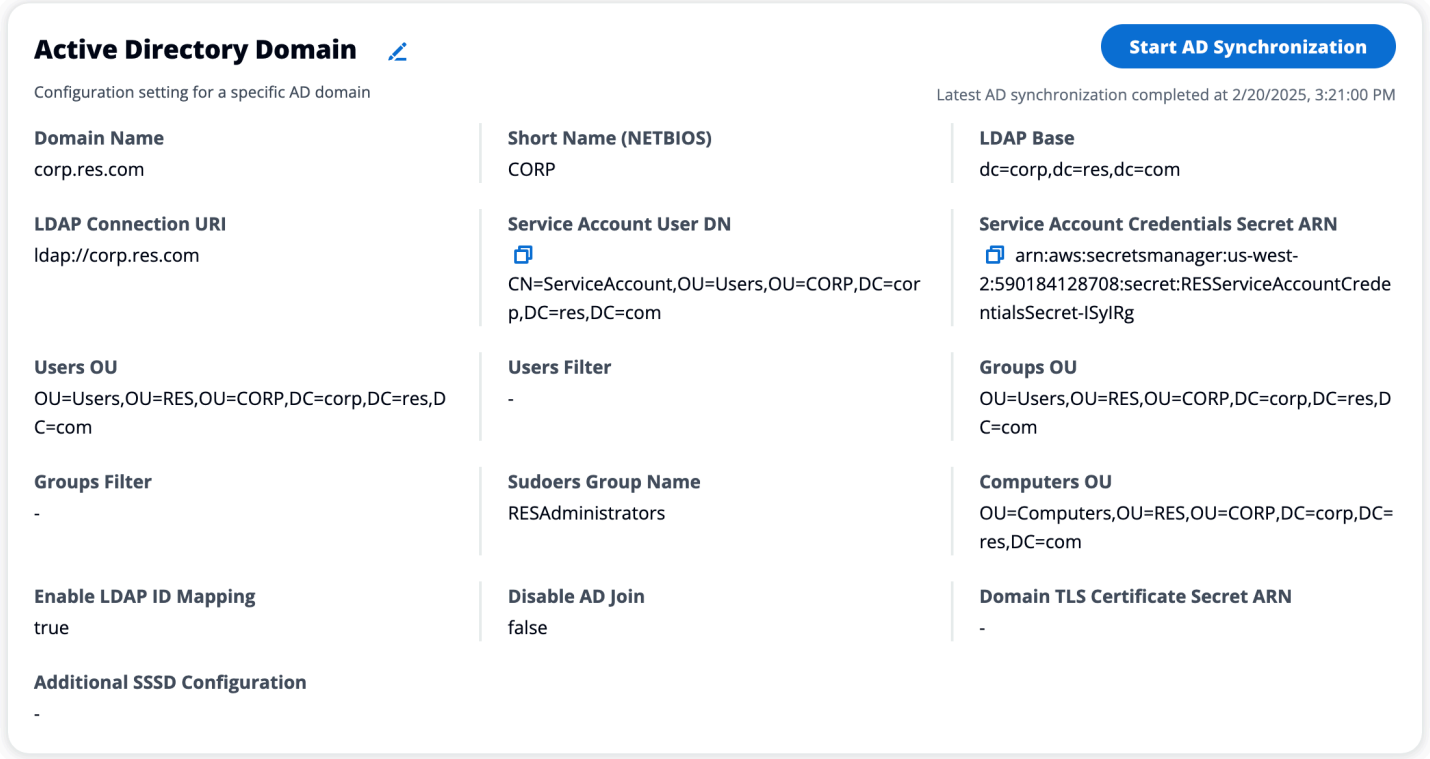
導覽至身分管理頁面，然後選擇 Active Directory 網域容器中的啟動 AD 同步按鈕，以隨需觸發 AD 同步。



若要停止持續的 AD 同步，請選取 Active Directory 網域容器中的停止 AD 同步按鈕。



您也可以在 Active Directory 網域容器中檢查 AD 同步狀態和最新的同步時間。



如何手動執行同步 (2024.12 和 2024.12.01 版)

Active Directory 同步程序已從 Cluster Manager 內部主機移至幕後的一次性 Amazon Elastic Container Service (ECS) 任務。程序排程為每小時執行一次，您可以在`<res-environment-name>-ad-sync-cluster`叢集下的 Amazon ECS 主控台中找到執行中的 ECS 任務。

若要手動啟動它：

1. 導覽至 Lambda 主控台並搜尋稱為 的 lambda`<res-environment>-scheduled-ad-sync`。
2. 開啟 Lambda 函數並前往測試
3. 在事件 JSON 中輸入下列項目：

```
{
    "detail-type": "Scheduled Event"
}
```

4. 選擇測試。
5. 在 CloudWatch 下觀察執行中 AD Sync 任務的日誌 → 日誌群組 → `<environment-name>/ad-sync`。您將看到每個執行中 ECS 任務的日誌。選取最新的 以檢視日誌。

> **Note**
>
> - 如果您變更 AD 參數或新增 AD 篩選條件，RES 會將新使用者新增至新指定的參數，並移除先前已同步且不再包含在 LDAP 搜尋空間中的使用者。
> - RES 無法移除主動指派給專案的使用者/群組。您必須從專案中移除使用者，讓 RES 從環境中移除他們。

SSO 組態

提供 AD 組態後，使用者必須設定單一登入 (SSO)，才能以 AD 使用者身分登入 RES Web 入口網站。SSO 組態已從一般設定頁面移至新的身分管理頁面。如需設定 SSO 的詳細資訊，請參閱 身分管理。

使用 IAM Identity Center 設定單一登入 (SSO)

如果您還沒有連接到受管 Active Directory 的身分中心，請從 開始步驟 1：設定身分中心。如果您已有與受管 Active Directory 連線的身分中心，請從 開始步驟 2：連線至身分中心。

> **Note**
>
> 如果您要部署到 AWS GovCloud （美國西部） 區域，請在 AWS GovCloud (US) 部署 Research and Engineering Studio 的分割區帳戶中設定 SSO。

步驟 1：設定身分中心

啟用 IAM Identity Center

1. 登入 AWS Identity and Access Management 主控台。
2. 開啟 Identity Center。
3. 選擇 啟用 。
4. 選擇使用 啟用 AWS Organizations。
5. 選擇繼續。

> **Note**
> 請確定您位於擁有受管 Active Directory 的相同區域。

將 IAM Identity Center 連線至受管 Active Directory

啟用 IAM Identity Center 之後，請完成以下建議的設定步驟：

1. 在導覽窗格中，選擇設定。
2. 在身分來源下，選擇動作，然後選擇變更身分來源。
3. 在現有目錄下，選取您的目錄。
4. 選擇下一步。
5. 檢閱您的變更**ACCEPT**，然後在確認方塊中輸入 。
6. 選擇變更身分來源。

將使用者和群組同步到身分中心

在 中所做的變更將 IAM Identity Center 連線至受管 Active Directory完成後，會出現綠色確認橫幅。

1. 在確認橫幅中，選擇開始引導設定。
2. 從設定屬性映射中，選擇下一步。
3. 在使用者區段下，輸入您要同步的使用者。
4. 選擇新增。
5. 選擇下一步。
6. 檢閱您的變更，然後選擇儲存組態。
7. 同步程序可能需要幾分鐘的時間。如果您收到有關使用者未同步的警告訊息，請選擇繼續同步。

啟用使用者

1. 從功能表中，選擇使用者。
2. 選取您要為其啟用存取權的 （使用者）。
3. 選擇啟用使用者存取。

步驟 2：連線至身分中心

在 IAM Identity Center 中設定應用程式

1. 開啟 IAM Identity Center 主控台。
2. 選擇 Applications (應用程式)。
3. 選擇新增應用程式。
4. 在設定偏好設定下，選擇我有想要設定的應用程式。
5. 在應用程式類型下，選擇 SAML 2.0。
6. 選擇下一步。
7. 輸入您要使用的顯示名稱和描述。
8. 在 IAM Identity Center 中繼資料下，複製 IAM Identity Center SAML 中繼資料檔案的連結。使用 RES 入口網站設定 IAM Identity Center 時，您將需要此項目。
9. 在應用程式屬性下，輸入您的應用程式啟動 URL。例如 `<your-portal-domain>/sso`。
10. 在應用程式 ACS URL 下，從 RES 入口網站輸入重新導向 URL。若要尋找此項目：
    a. 在環境管理下，選擇一般設定。
    b. 選取身分提供者索引標籤。
    c. 在單一登入下，您會找到 SAML 重新導向 URL。
11. 在應用程式 SAML 對象下，輸入 Amazon Cognito URN。

    若要建立 urn：

    a. 從 RES 入口網站開啟一般設定。
    b. 在身分提供者索引標籤下，找到使用者集區 ID。
    c. 將使用者集區 ID 新增至此字串：

    ```
    urn:amazon:cognito:sp:<user_pool_id>
    ```

12. 輸入 Amazon Cognito URN 之後，請選擇提交。

設定應用程式的屬性映射

1. 從 Identity Center 開啟所建立應用程式的詳細資訊。
2. 選擇動作，然後選擇編輯屬性映射。

3. 在主旨下，輸入 **${user:email}**。
4. 在格式下，選擇 emailAddress。
5. 選擇新增屬性映射。
6. 在應用程式中的使用者屬性下，輸入 'email'。
7. 在 IAM Identity Center 中映射至此字串值或使用者屬性下，輸入 **${user:email}**。
8. 在格式下，輸入「未指定」。
9. 選擇儲存變更。

在 IAM Identity Center 中將使用者新增至應用程式

1. 從 Identity Center 開啟所建立應用程式的指派使用者，然後選擇指派使用者。
2. 選取您要指派應用程式存取權的使用者。
3. 選擇 Assign users (指派使用者)。

在 RES 環境中設定 IAM Identity Center

1. 在環境管理下的研究和工程 Studio 環境中，開啟一般設定。
2. 開啟身分提供者索引標籤。
3. 在單一登入下，選擇編輯 (狀態旁邊) 。
4. 使用下列資訊填寫表單：
   a. 選擇 SAML。
   b. 在提供者名稱下，輸入使用者易記的名稱。
   c. 選擇輸入中繼資料文件端點 URL。
   d. 輸入您在 期間複製的 URL在 IAM Identity Center 中設定應用程式。
   e. 在提供者電子郵件屬性下，輸入 'email'。
   f. 選擇提交。
5. 重新整理頁面並檢查狀態是否顯示為已啟用。

為單一登入 (SSO) 設定您的身分提供者

Research and Engineering Studio 與任何 SAML 2.0 身分提供者整合，以驗證使用者對 RES 入口網站的存取。這些步驟提供與您選擇的 SAML 2.0 身分提供者整合的指示。如果您想要使用 IAM Identity Center，請參閱 使用 IAM Identity Center 設定單一登入 (SSO)。

> **Note**
>
> 使用者的電子郵件必須符合 IDP SAML 聲明和 Active Directory。您需要將身分提供者與 Active Directory 連線，並定期同步使用者。

主題

- 設定您的身分提供者
- 設定 RES 以使用您的身分提供者
- 在非生產環境中設定您的身分提供者
- 偵錯 SAML IdP 問題

設定您的身分提供者

本節提供使用來自 RES Amazon Cognito 使用者集區的資訊來設定身分提供者的步驟。

1. RES 假設您有一個 AD (AWS 受管 AD 或自我佈建 AD)，其使用者身分允許存取 RES 入口網站和專案。將您的 AD 連接至您的身分服務提供者，並同步使用者身分。檢查身分提供者的文件，了解如何連接 AD 和同步使用者身分。例如，請參閱AWS IAM Identity Center 《 使用者指南》中的使用 Active Directory 做為身分來源。
2. 在您的身分提供者 (IdP) 中為 RES 設定 SAML 2.0 應用程式。此組態需要下列參數：
   - SAML 重新導向 URL — IdP 用來傳送 SAML 2.0 回應給服務提供者的 URL。

   > **Note**
   >
   > 根據 IdP，SAML 重新導向 URL 可能有不同的名稱：
   >
   > - 應用程式 URL
   > - 聲明消費者服務 (ACS) URL
   > - ACS POST 繫結 URL

若要取得 URL

1. 以管理員或 clusteradmin 身分登入 RES。
2. 導覽至環境管理 ⇒ 一般設定 ⇒ 身分提供者。
3. 選擇 SAML 重新導向 URL。

- SAML 對象 URI — 服務提供者端 SAML 對象實體的唯一 ID。

> **Note**
>
> 根據 IdP，SAML 對象 URI 可能會有不同的名稱：
>
> - ClientID
> - 應用程式 SAML 對象
> - SP 實體 ID

以下列格式提供輸入。

```
urn:amazon:cognito:sp:user-pool-id
```

尋找您的 SAML 對象 URI

1. 以管理員或 clusteradmin 身分登入 RES。
2. 導覽至環境管理 ⇒ 一般設定 ⇒ 身分提供者。
3. 選擇使用者集區 ID。

3. 張貼到 RES 的 SAML 聲明必須將下列欄位/宣告設定為使用者的電子郵件地址：
   - SAML 主體或 NameID
   - SAML 電子郵件
4. 您的 IdP 會根據組態，將欄位/宣告新增至 SAML 聲明。RES 需要這些欄位。根據預設，大多數供應商會自動填入這些欄位。如果您必須設定，請參閱下列欄位輸入和值。

   - AudienceRestriction — 設定為 `urn:amazon:cognito:sp:`*`user-pool-id`*。使用 Amazon Cognito 使用者集區的 ID 取代 *`user-pool-id`*。

```
<saml:AudienceRestriction>
    <saml:Audience> urn:amazon:cognito:sp:user-pool-id
</saml:AudienceRestriction>
```

- 回應 — InResponseTo設定為 https://*user-pool-domain*/saml2/idpresponse。將 *user-pool-domain* 取代為您的 Amazon Cognito 使用者集區的網域名稱。

```
<saml2p:Response
  Destination="http://user-pool-domain/saml2/idpresponse"
  ID="id123"
  InResponseTo="_dd0a3436-bc64-4679-a0c2-cb4454f04184"
  IssueInstant="Date-time stamp"
  Version="2.0"
  xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:xs="http://www.w3.org/2001/XMLSchema">
```

- SubjectConfirmationData — Recipient設定為您的使用者集區saml2/idpresponse端點和InResponseTo原始 SAML 請求 ID。

```
<saml2:SubjectConfirmationData
  InResponseTo="_dd0a3436-bc64-4679-a0c2-cb4454f04184"
  NotOnOrAfter="Date-time stamp"
  Recipient="https://user-pool-domain/saml2/idpresponse"/>
```

- AuthnStatement — 將 設定為下列項目：

```
<saml2:AuthnStatement AuthnInstant="2016-10-30T13:13:28.152TZ"
  SessionIndex="32413b2e54db89c764fb96ya2k"
 SessionNotOnOrAfter="2016-10-30T13:13:28">
    <saml2:SubjectLocality />
    <saml2:AuthnContext>

 <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</
saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
</saml2:AuthnStatement>
```

5. 如果您的 SAML 應用程式有登出 URL 欄位，請將其設定為：*<domain-url>*/saml2/logout。

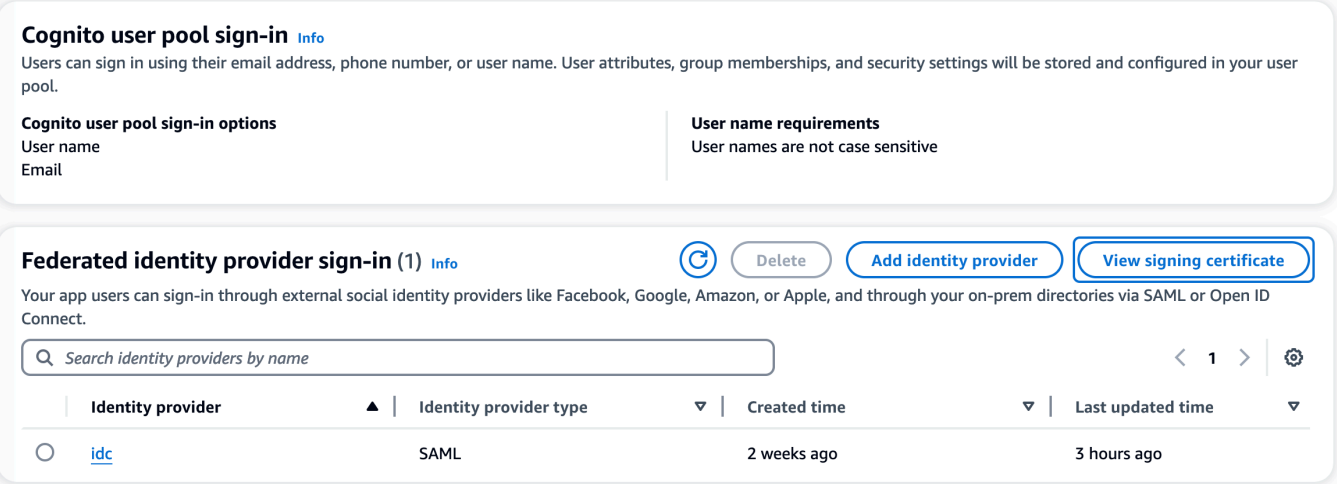
取得網域 URL

1. 以管理員或 clusteradmin 身分登入 RES。
2. 導覽至環境管理 ⇒ 一般設定 ⇒ 身分提供者。
3. 選擇網域 URL。

6. 如果您的 IdP 接受簽署憑證以與 Amazon Cognito 建立信任，請下載 Amazon Cognito 簽署憑證並將其上傳到您的 IdP。

若要取得簽署憑證

1. 在 入門 AWS Management Console中開啟 Amazon Cognito 主控台
2. 選取您的使用者集區。您的使用者集區應該是 `res-<environment name>-user-pool`。
3. 選取登入體驗索引標籤。
4. 在聯合身分提供者登入區段中，選擇檢視簽署憑證。



您可以使用此憑證來設定 Active Directory IDP、新增 `relying party trust`，以及啟用此依賴方的 SAML 支援。

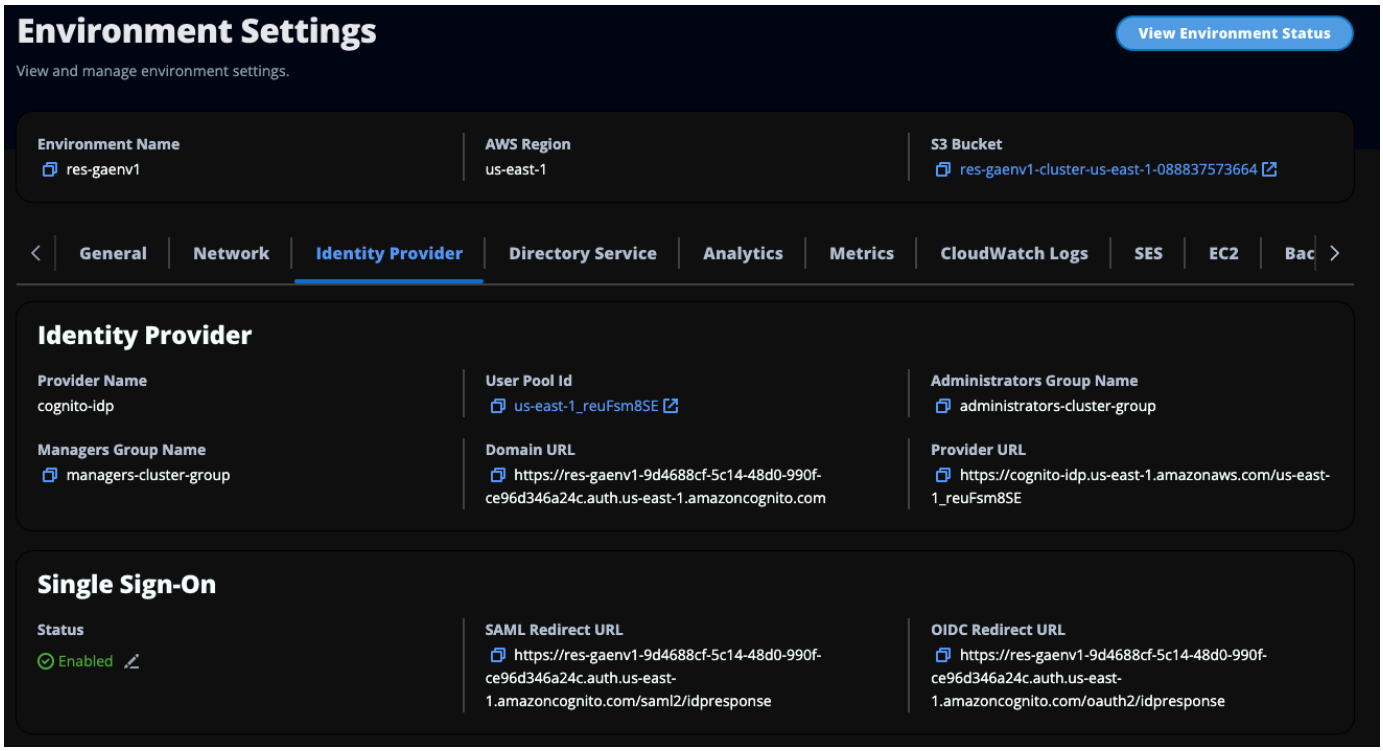
> **Note**
>
> 這不適用於 Keycloak 和 IDC。

5. 應用程式設定完成後，請下載 SAML 2.0 應用程式中繼資料 XML 或 URL。您可以在下一節中使用它。

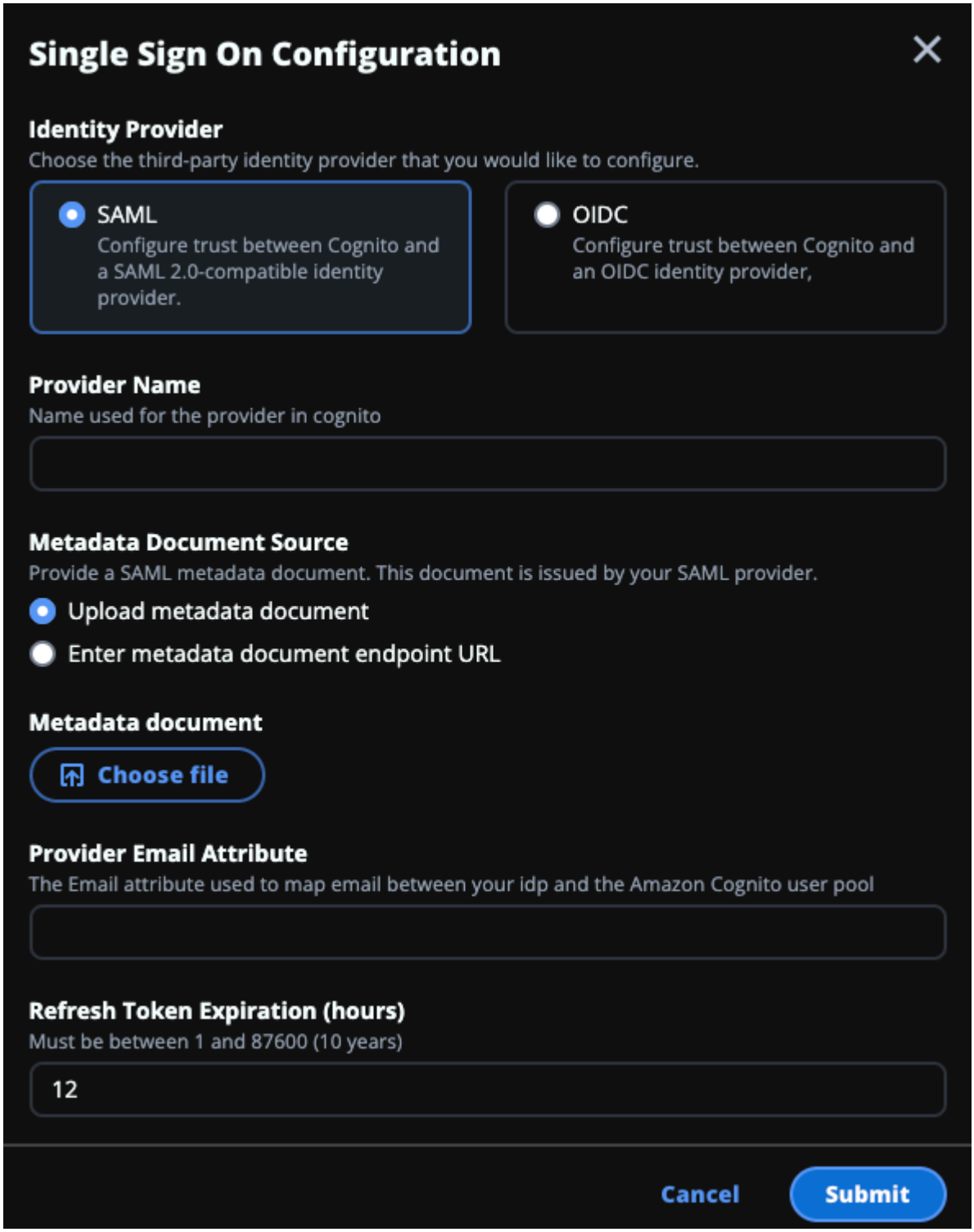
設定 RES 以使用您的身分提供者

完成 RES 的單一登入設定

1. 以管理員或 clusteradmin 身分登入 RES。
2. 導覽至環境管理 ⇒ 一般設定 ⇒ 身分提供者。



3. 在單一登入下，選擇狀態指示燈旁的編輯圖示，以開啟單一登入組態頁面。



a. 針對身分提供者，選擇 SAML。

b. 在提供者名稱中，輸入身分提供者的唯一名稱。

> **Note**
>
> 不允許使用下列名稱：
>
> - Cognito
> - IdentityCenter

c. 在中繼資料文件來源下，選擇適當的選項並上傳中繼資料 XML 文件，或從身分提供者提供 URL。

d. 在提供者電子郵件屬性中，輸入文字值 `email`。

e. 選擇提交。

4. 重新載入環境設定頁面。如果組態正確，則會啟用單一登入。

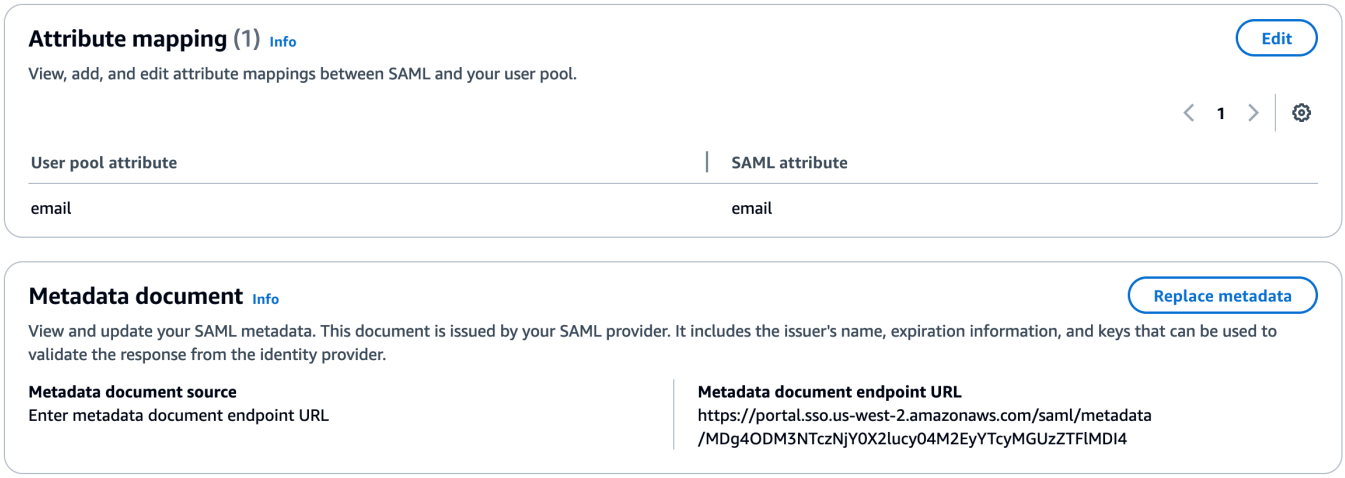
在非生產環境中設定您的身分提供者

如果您使用提供的外部資源來建立非生產 RES 環境，並將 IAM Identity Center 設定為您的身分提供者，您可能想要設定不同的身分提供者，例如 Okta。RES SSO 啟用表單會要求三個組態參數：

1. 供應商名稱 — 無法修改
2. 中繼資料文件或 URL — 可以修改
3. 供應商電子郵件屬性 — 可以修改

若要修改中繼資料文件和提供者電子郵件屬性，請執行下列動作：

1. 前往 Amazon Cognito 主控台。
2. 在導覽中，選擇使用者集區。
3. 選取您的使用者集區以檢視使用者集區概觀。
4. 從登入體驗索引標籤，前往聯合身分提供者登入並開啟您設定的身分提供者。
5. 一般而言，您只需要變更中繼資料，並讓屬性映射保持不變。若要更新屬性映射，請選擇編輯。若要更新中繼資料文件，請選擇取代中繼資料。



6. 如果您編輯屬性映射，則需要更新 DynamoDB 中的`<environment name>.cluster-settings`資料表。

   a. 開啟 DynamoDB 主控台，然後從導覽中選擇資料表。

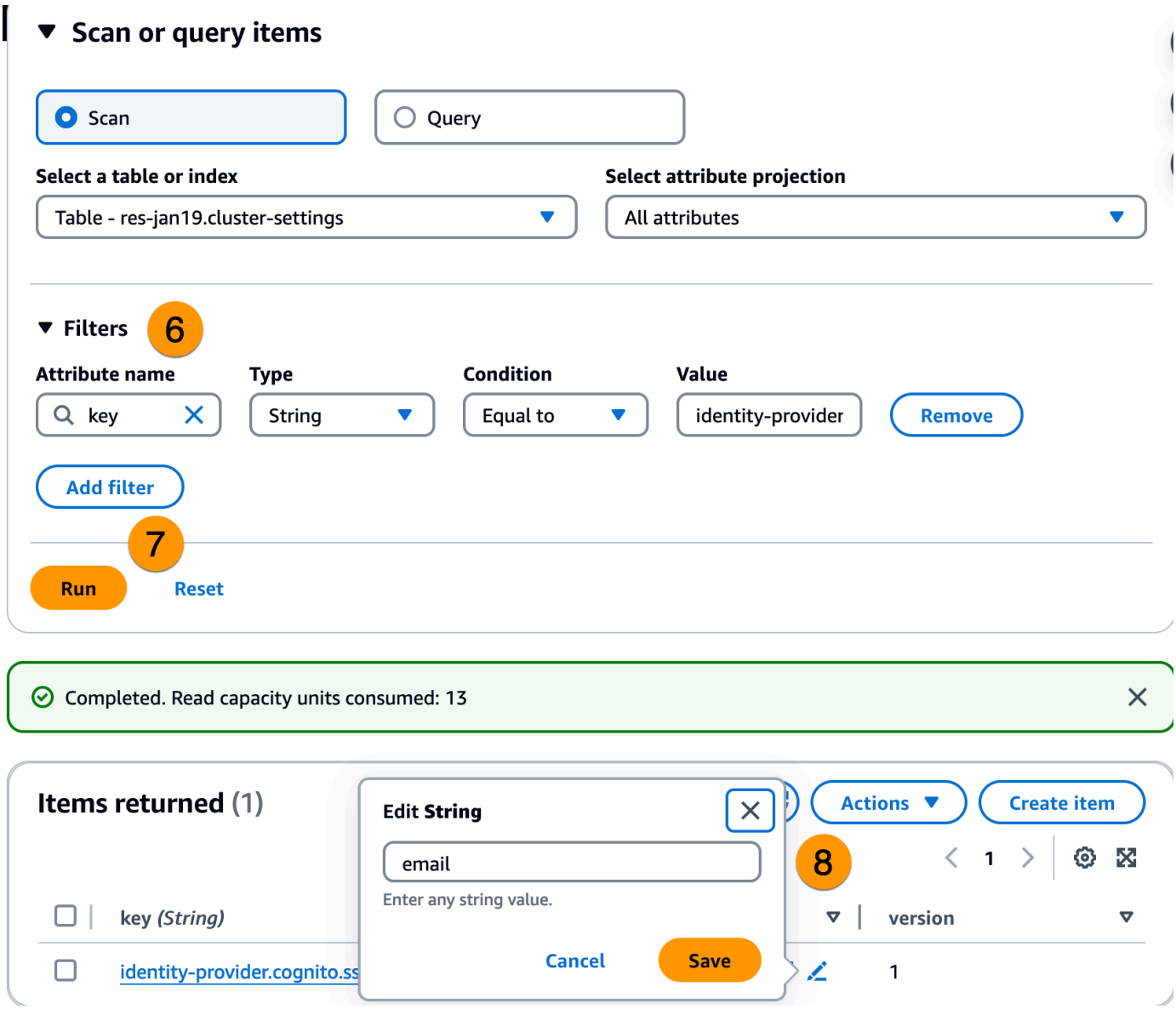
   b. 尋找並選取`<environment name>.cluster-settings`資料表，然後從動作功能表中選取探索項目。

   c. 在掃描或查詢項目下，前往篩選條件並輸入下列參數：

      - 屬性名稱 — `key`
      - 值 — `identity-provider.cognito.sso_idp_provider_email_attribute`

   d. 選擇執行。

7. 在傳回的項目下，尋找`identity-provider.cognito.sso_idp_provider_email_attribute`字串，然後選擇編輯以修改字串，以符合您在 Amazon Cognito 中的變更。



偵錯 SAML IdP 問題

SAML 追蹤器 — 您可以將此延伸模組用於 Chrome 瀏覽器，以追蹤 SAML 請求並檢查 SAML 聲明值。如需詳細資訊，請參閱 Chrome Web Store 中的 SAML 追蹤器。

SAML 開發人員工具 — OneLogin 提供可用於解碼 SAML 編碼值的工具，並檢查 SAML 聲明中的必要欄位。如需詳細資訊，請參閱 OneLogin 網站上的 Base 64 Decode + Inflate。

Amazon CloudWatch Logs — 您可以在 CloudWatch Logs 中檢查 RES 日誌是否有錯誤或警告。您的日誌位於名稱格式為 的日誌群組中`res-environment-name`/`cluster-manager`。

Amazon Cognito 文件 — 如需 SAML 與 Amazon Cognito 整合的詳細資訊，請參閱《Amazon Cognito 開發人員指南》中的將 SAML 身分提供者新增至使用者集區。

設定使用者的密碼

1. 從 AWS Directory Service 主控台中，選取所建立堆疊的目錄。
2. 在動作功能表下，選取重設使用者密碼。
3. 選取使用者並輸入新密碼。
4. 選擇重設密碼。

建立子網域

如果您使用的是自訂網域，則需要設定子網域來支援入口網站的 Web 和 VDI 部分。

> **Note**
>
> 如果您要部署到 AWS GovCloud （美國西部） 區域，請在託管網域公有託管區域的商業分割區帳戶中設定 Web 應用程式和 VDI 子網域。

1. 開啟 Route 53 主控台。
2. 尋找您建立的網域，然後選擇建立記錄。
3. 輸入 'web' 做為記錄名稱。
4. 選取 CNAME 做為記錄類型。
5. 針對值，輸入您在初始電子郵件中收到的連結。
6. 選擇建立記錄。
7. 若要建立 VDC 的記錄，請擷取 NLB 地址。
   a. 開啟 AWS CloudFormation 主控台。
   b. 選擇 `<environment-name>-vdc`。
   c. 選擇資源並開啟 `<environmentname>-vdc-external-nlb`。
   d. 從 NLB 複製 DNS 名稱。
8. 開啟 Route 53 主控台。

9. 尋找您的網域，然後選擇建立記錄。
10. 在記錄名稱下，輸入 `vdc`。
11. 在記錄類型下，選取 CNAME。
12. 針對 NLB，輸入 DNS。
13. 選擇建立記錄。

建立 ACM 憑證

根據預設，RES 會使用網域 amazonaws.com 在應用程式負載平衡器下託管 Web 入口網站。若要使用您自己的網域，您需要設定您提供或從 AWS Certificate Manager (ACM) 請求的公有 SSL/TLS 憑證。如果您使用 ACM，您將會收到需要提供做為參數 AWS 的資源名稱，以加密用戶端和 Web 服務主機之間的 SSL/TLS 通道。

> **Tip**
>
> 如果您要部署外部資源示範套件，則需要在 中部署外部資源堆疊`PortalDomainName`時，在中輸入您選擇的網域建立外部資源。

若要建立自訂網域的憑證：

1. 從 主控台開啟 AWS Certificate Manager 以請求公有憑證。如果您要在 AWS GovCloud（美國西部）中部署，請在 GovCloud 分割區帳戶中建立憑證。
2. 選擇請求公有憑證，然後選擇下一步。
3. 在網域名稱下，請求 `*.PortalDomainName`和 的憑證`PortalDomainName`。
4. 在驗證方法下，選擇 DNS 驗證。
5. 選擇請求。
6. 從憑證清單中，開啟您請求的憑證。每個憑證將具有待定驗證做為狀態。

   > **Note**
   >
   > 如果您沒有看到憑證，請重新整理清單。

7. 執行以下任意一項：
   - 商業部署：

從每個請求憑證的憑證詳細資訊中，選擇在 Route 53 中建立記錄。憑證的狀態應變更為已發行。

- GovCloud 部署：

  如果您要部署 in AWS GovCloud （美國西部），請複製 CNAME 金鑰和值。從商業分割區帳戶，使用 值在公有託管區域中建立新的記錄。憑證的狀態應變更為已發行。

8. 將新憑證 ARN 複製到輸入 做為 的 參數`ACMCertificateARNforWebApp`。

Amazon CloudWatch Logs

Research and Engineering Studio 會在安裝期間於 CloudWatch 中建立下列日誌群組。如需預設保留，請參閱下表：

CloudWatch Log 群組	Retention
/aws/lambda/ *<installation-stack-name>*-cluster-endpoints	永不過期
/aws/lambda/ *<installation-stack-name>*-cluster-manager-scheduled-ad-sync	永不過期
/aws/lambda/ *<installation-stack-name>*-cluster-settings	永不過期
/aws/lambda/ *<installation-stack-name>*-oauth-credentials	永不過期
/aws/lambda/ *<installation-stack-name>*-self-signed-certificate	永不過期
/aws/lambda/ *<installation-stack-name>*-update-cluster-prefix-list	永不過期
/aws/lambda/ *<installation-stack-name>*-vdc-scheduled-event-transformer	永不過期

CloudWatch Log 群組	Retention
/aws/lambda/ <installation-stack-name>-vdc-update-cluster-manager-client-scope	永不過期
/<installation-stack-name> / cluster-manager	3 個月
/<installation-stack-name> /vdc/controller	3 個月
/<installation-stack-name> /vdc/dcv-broker	3 個月
/<installation-stack-name> /vdc/dcv-connection-gateway	3 個月

如果您想要變更日誌群組的預設保留，您可以前往 CloudWatch 主控台，並依照指示在 CloudWatch Logs 中變更日誌資料保留。

設定自訂許可界限

自 2024.04 起，您可以選擇透過連接自訂許可界限來修改 RES 建立的角色。自訂許可界限可以定義為 RES AWS CloudFormation 安裝的一部分，方法是將許可界限的 ARN 作為 IAMPermissionBoundary 參數的一部分。如果此參數保持空白，則不會在任何 RES 角色上設定許可界限。以下是 RES 角色操作所需的動作清單。請確定您計劃使用的任何許可界限明確允許下列動作：

```
[
    {
        "Effect": "Allow",
        "Resource": "*",
        "Sid": "ResRequiredActions",
        "Action": [
            "access-analyzer:*",
            "account:GetAccountInformation",
            "account:ListRegions",
            "acm:*",
            "airflow:*",
```

```
            "amplify:*",
            "amplifybackend:*",
            "amplifyuibuilder:*",
            "aoss:*",
            "apigateway:*",
            "appflow:*",
            "application-autoscaling:*",
            "appmesh:*",
            "apprunner:*",
            "aps:*",
            "athena:*",
            "auditmanager:*",
            "autoscaling-plans:*",
            "autoscaling:*",
            "backup-gateway:*",
            "backup-storage:*",
            "backup:*",
            "batch:*",
            "bedrock:*",
            "budgets:*",
            "ce:*",
            "cloud9:*",
            "cloudformation:*",
            "cloudfront:*",
            "cloudtrail-data:*",
            "cloudtrail:*",
            "cloudwatch:*",
            "codeartifact:*",
            "codebuild:*",
            "codeguru-profiler:*",
            "codeguru-reviewer:*",
            "codepipeline:*",
            "codestar-connections:*",
            "codestar-notifications:*",
            "codestar:*",
            "cognito-identity:*",
            "cognito-idp:*",
            "cognito-sync:*",
            "comprehend:*",
            "compute-optimizer:*",
            "cur:*",
            "databrew:*",
            "datapipeline:*",
            "datasync:*",
```

```
            "dax:*",
            "detective:*",
            "devops-guru:*",
            "dlm:*",
            "dms:*",
            "drs:*",
            "dynamodb:*",
            "ebs:*",
            "ec2-instance-connect:*",
            "ec2:*",
            "ec2messages:*",
            "ecr:*",
            "ecs:*",
            "eks:*",
            "elastic-inference:*",
            "elasticache:*",
            "elasticbeanstalk:*",
            "elasticfilesystem:*",
            "elasticloadbalancing:*",
            "elasticmapreduce:*",
            "elastictranscoder:*",
            "es:*",
            "events:*",
            "firehose:*",
            "fis:*",
            "fms:*",
            "forecast:*",
            "fsx:*",
            "geo:*",
            "glacier:*",
            "glue:*",
            "grafana:*",
            "guardduty:*",
            "health:*",
            "iam:*",
            "identitystore:*",
            "imagebuilder:*",
            "inspector2:*",
            "inspector:*",
            "internetmonitor:*",
            "iot:*",
            "iotanalytics:*",
            "kafka:*",
            "kafkaconnect:*",
```

```
            "kinesis:*",
            "kinesisanalytics:*",
            "kms:*",
            "lambda:*",
            "lightsail:*",
            "logs:*",
            "memorydb:*",
            "mgh:*",
            "mobiletargeting:*",
            "mq:*",
            "neptune-db:*",
            "organizations:DescribeOrganization",
            "osis:*",
            "personalize:*",
            "pi:*",
            "pipes:*",
            "polly:*",
            "qldb:*",
            "quicksight:*",
            "rds-data:*",
            "rds:*",
            "redshift-data:*",
            "redshift-serverless:*",
            "redshift:*",
            "rekognition:*",
            "resiliencehub:*",
            "resource-groups:*",
            "route53:*",
            "route53domains:*",
            "route53resolver:*",
            "rum:*",
            "s3:*",
            "sagemaker:*",
            "scheduler:*",
            "schemas:*",
            "sdb:*",
            "secretsmanager:*",
            "securityhub:*",
            "serverlessrepo:*",
            "servicecatalog:*",
            "servicequotas:*",
            "ses:*",
            "signer:*",
            "sns:*",
```

```
            "sqs:*",
            "ssm:*",
            "ssmmessages:*",
            "states:*",
            "storagegateway:*",
            "sts:*",
            "support:*",
            "tag:GetResources",
            "tag:GetTagKeys",
            "tag:GetTagValues",
            "textract:*",
            "timestream:*",
            "transcribe:*",
            "transfer:*",
            "translate:*",
            "vpc-lattice:*",
            "waf-regional:*",
            "waf:*",
            "wafv2:*",
            "wellarchitected:*",
            "wisdom:*",
            "xray:*"
        ]
    }
]
```

設定 RES 就緒 AMIs

使用 RES-ready Amazon Machine Image (AMIs)，您可以在自訂 AMI 上預先安裝虛擬桌面執行個體 VDIs) 的 RES AMIs 相依性。使用 RES-ready AMIs 可改善使用預先製作映像的 VDI 執行個體開機時間。使用 EC2 Image Builder，您可以將 AMIs 建置並註冊為新的軟體堆疊。如需映像建置器的詳細資訊，請參閱映像建置器使用者指南。

開始之前，您必須部署最新版本的 RES。

主題

- 準備 IAM 角色以存取 RES 環境
- 建立 EC2 Image Builder 元件
- 準備您的 EC2 Image Builder 配方
- 設定 EC2 Image Builder 基礎設施

- 設定映像建置器映像管道
- 執行映像建置器映像管道
- 在 RES 中註冊新的軟體堆疊

準備 IAM 角色以存取 RES 環境

若要從 EC2 Image Builder 存取 RES 環境服務，您必須建立或修改名為 RES-EC2InstanceProfileForImageBuilder 的 IAM 角色。如需有關設定 IAM 角色以在映像建置器中使用的資訊，請參閱《映像建置器使用者指南》中的 AWS Identity and Access Management (IAM)。

您的角色需要：

- 包含 Amazon EC2 服務的信任關係。
- AmazonSSMManagedInstanceCore 和 EC2InstanceProfileForImageBuilder 政策。
- 對部署的 RES 環境具有有限 DynamoDB 和 Amazon S3 存取權的自訂 RES 政策。

  （此政策可以是客戶受管政策或客戶內嵌政策文件。）

1. 首先，建立一個將連接到您的角色的新政策：IAM -> 政策 -> 建立政策
2. 從政策編輯器中選取 JSON。
3. 複製此處顯示的政策並貼到編輯器中，在適用的情況下取代所需的 *{AWS-Region}*、*{AWS-Account-ID}* 和 *{RES-EnvironmentName}*。

   RES 政策：

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RESDynamoDBAccess",
            "Effect": "Allow",
            "Action": "dynamodb:GetItem",
            "Resource": "arn:aws:dynamodb:us-east-1:{AWS-Account-
ID}:table/{RES-EnvironmentName}.cluster-settings",
            "Condition": {
```

```
                "ForAllValues:StringLike": {
                    "dynamodb:LeadingKeys": [
                        "global-settings.gpu_settings.*",
                        "global-settings.package_config.*",
                        "cluster-manager.host_modules.*",
                        "identity-provider.cognito.enable_native_user_login"
                    ]
                }
            }
        },
        {
            "Sid": "RESS3Access",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::{RES-EnvironmentName}-cluster-{AWS-
Region}-{AWS-Account-ID}/idea/vdc/res-ready-install-script-packages/*",
                "arn:aws:s3:::research-engineering-studio-{AWS-Region}/
host_modules/*"
            ]
        }
    ]
}
```

4. 選擇下一步，並提供名稱和選用描述以完成政策建立。
5. 若要建立角色，請先前往 IAM -> 角色 -> 建立角色。
6. 在信任的實體類型下，選取「AWS 服務」。
7. 在服務或使用案例下拉式清單中選取 EC2。
8. 在使用案例區段中，選取 EC2，然後選擇下一步。
9. 搜尋 ，然後選取您先前建立的政策名稱。
10. 選擇下一步，並提供名稱和選用描述以完成角色建立。
11. 選取您的新角色，並確認信任關係符合下列各項：

    信任的關係實體：

    JSON

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

```
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

建立 EC2 Image Builder 元件

遵循《映像建置器使用者指南》中的指示，使用映像建置器主控台建立元件。

輸入您的元件詳細資訊：

1. 針對類型，選擇建置。
2. 針對映像作業系統 (OS)，選擇 Linux 或 Windows。
3. 針對元件名稱，輸入有意義的名稱，例如 **research-and-engineering-studio-vdi-<operating-system>**。
4. 輸入元件的版本編號，並選擇性地新增描述。
5. 在定義文件中，輸入下列定義檔案。如果您遇到任何錯誤，YAML 檔案會區分空間，而且最可能的原因。

   Linux

```
#  Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
#  Licensed under the Apache License, Version 2.0 (the "License"). You may not
 use this file except in compliance
#  with the License. A copy of the License is located at
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
#  or in the 'license' file accompanying this file. This file is distributed on
 an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-vdi-linux
```

```
description: An RES EC2 Image Builder component to install required RES software
 dependencies for Linux VDI.
schemaVersion: 1.0
parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - RESEnvName:
      type: string
      description: RES Environment Name
  - RESEnvRegion:
      type: string
      description: RES Environment Region
  - RESEnvReleaseVersion:
      type: string
      description: RES Release Version

phases:
  - name: build
    steps:
       - name: PrepareRESBootstrap
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - 'mkdir -p /root/bootstrap/logs'
                - 'mkdir -p /root/bootstrap/latest'
       - name: DownloadRESLinuxInstallPackage
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
{{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/linux/
res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
              destination: '/root/bootstrap/
res_linux_install_{{ RESEnvReleaseVersion }}.tar.gz'
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
```

```
            commands:
                - 'tar -xvf
 {{ build.DownloadRESLinuxInstallPackage.inputs[0].destination }} -C /root/
bootstrap/latest'
                - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install.sh -r {{ RESEnvRegion }} -n {{ RESEnvName }} -g NONE'
       - name: FirstReboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
         inputs:
            delaySeconds: 0
       - name: RunInstallPostRebootScript
         action: ExecuteBash
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
                - '/bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
install_post_reboot.sh'
       - name: SecondReboot
         action: Reboot
         onFailure: Abort
         maxAttempts: 3
         inputs:
            delaySeconds: 0
```

Windows

```
#  Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
#
#  Licensed under the Apache License, Version 2.0 (the "License"). You may not
 use this file except in compliance
#  with the License. A copy of the License is located at
#
#      http://www.apache.org/licenses/LICENSE-2.0
#
#  or in the 'license' file accompanying this file. This file is distributed on
 an 'AS IS' BASIS, WITHOUT WARRANTIES
#  OR CONDITIONS OF ANY KIND, express or implied. See the License for the
 specific language governing permissions
#  and limitations under the License.
name: research-and-engineering-studio-vdi-windows
```

```
description: An RES EC2 Image Builder component to install required RES software
 dependencies for Windows VDI.
schemaVersion: 1.0
parameters:
  - AWSAccountID:
      type: string
      description: RES Environment AWS Account ID
  - RESEnvName:
      type: string
      description: RES Environment Name
  - RESEnvRegion:
      type: string
      description: RES Environment Region
  - RESEnvReleaseVersion:
      type: string
      description: RES Release Version

phases:
  - name: build
    steps:
       - name: CreateRESBootstrapFolder
         action: CreateFolder
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - path: 'C:\Users\Administrator\RES\Bootstrap'
              overwrite: true
       - name: DownloadRESWindowsInstallPackage
         action: S3Download
         onFailure: Abort
         maxAttempts: 3
         inputs:
            - source: 's3://{{ RESEnvName }}-cluster-{{ RESEnvRegion }}-
{{ AWSAccountID }}/idea/vdc/res-ready-install-script-packages/windows/
res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
              destination:
 '{{ build.CreateRESBootstrapFolder.inputs[0].path }}\res_windows_install_{{ RESEnvRelea
              expectedBucketOwner: '{{ AWSAccountID }}'
       - name: RunInstallScript
         action: ExecutePowerShell
         onFailure: Abort
         maxAttempts: 3
         inputs:
            commands:
```

```
                - 'cd {{ build.CreateRESBootstrapFolder.inputs[0].path }}'
                - 'Tar -xf
res_windows_install_{{ RESEnvReleaseVersion }}.tar.gz'
                - 'Import-Module .\virtual-desktop-host-windows\Install.ps1'
                - 'Install-WindowsEC2Instance'
      - name: Reboot
        action: Reboot
        onFailure: Abort
        maxAttempts: 3
        inputs:
           delaySeconds: 0
```

6. 建立任何選用標籤，然後選擇建立元件。

準備您的 EC2 Image Builder 配方

EC2 Image Builder 配方會定義基本映像，以做為建立新映像的起點，以及您新增的一組元件來自訂映像，並確認一切如預期般運作。您必須建立或修改配方，以使用必要的 RES 軟體相依性來建構目標 AMI。如需配方的詳細資訊，請參閱管理配方。

RES 支援下列映像作業系統：

- Amazon Linux 2 (x86 和 ARM64)
- Ubuntu 22.04.3 (x86)
- RHEL 8 (x86) 和 9 (x86)
- Windows Server 2019、2022 (x86)
- Windows 10、11 (x86)

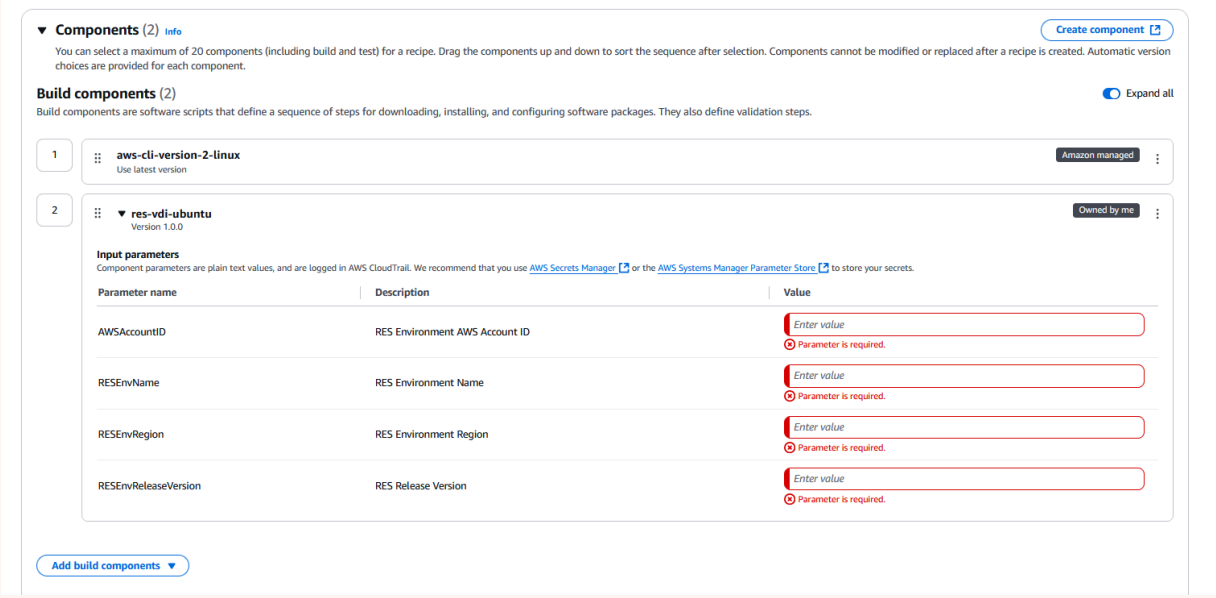
Create a new recipe

1. 在 開啟 EC2 Image Builder 主控台https://console.aws.amazon.com/imagebuilder。
2. 在已儲存資源下，選擇映像配方。
3. 選擇建立映像配方。
4. 輸入唯一的名稱和版本編號。
5. 選取 RES 支援的基礎映像。
6. 在執行個體組態下，如果未預先安裝 SSM 代理程式，請進行安裝。在使用者資料和任何其他所需的使用者資料中輸入資訊。

> **Note**
>
> 如需如何安裝 SSM 代理程式的資訊，請參閱：
>
> - 在 Linux 的 EC2 執行個體上手動安裝 SSM 代理程式。
> - 在適用於 Windows Server 的 EC2 執行個體上手動安裝和解除安裝 SSM Agent。

7. 對於 Linux 型配方，將 Amazon 受管`aws-cli-version-2-linux`建置元件新增至配方。RES 安裝指令碼使用 AWS CLI 提供 DynamoDB 叢集設定組態值的 VDI 存取權。Windows 不需要此元件。
8. 新增為 Linux 或 Windows 環境建立的 EC2 Image Builder 元件，然後輸入任何必要的參數值。下列參數是必要的輸入：AWSAccountID、RESEnvName、RESEnvRegion 和 RESEnvReleaseVersion。

> **Important**
>
> 對於 Linux 環境，您必須依先新增`aws-cli-version-2-linux`建置元件的順序新增這些元件。

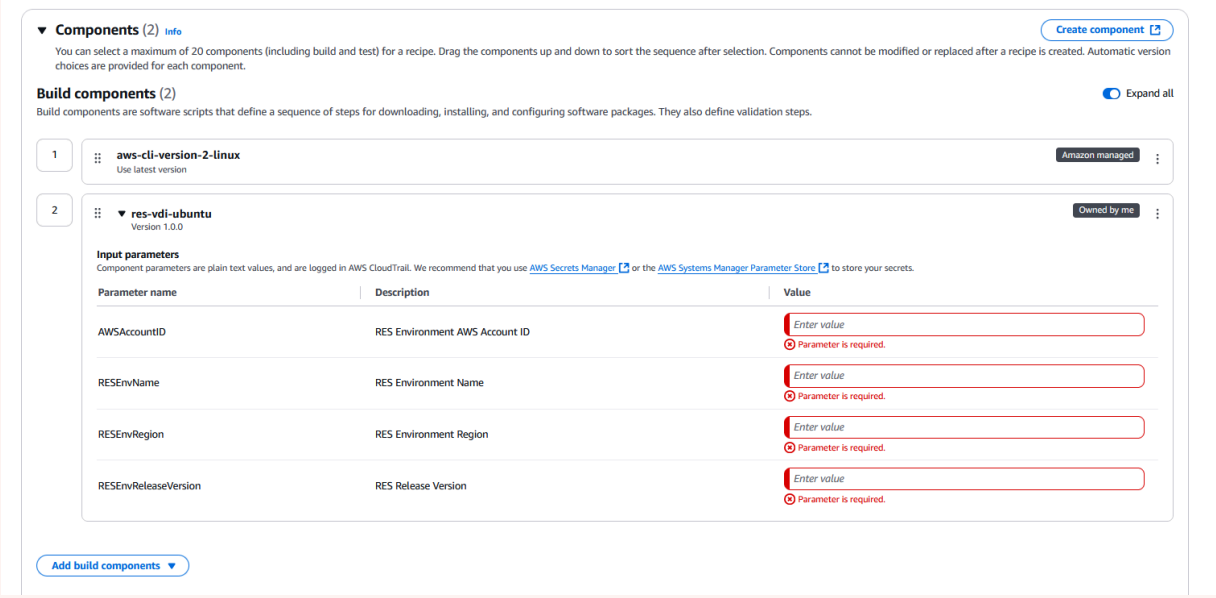


9. （建議）新增 Amazon 受管`simple-boot-test-<linux-or-windows>`測試元件，以確認可以啟動 AMI。這是最低建議。您可以選取其他符合您需求的測試元件。
10. 視需要完成任何選用區段，新增任何其他所需的元件，然後選擇建立配方。

Modify a recipe

如果您有現有的 EC2 Image Builder 配方，您可以新增下列元件來使用它：

1. 對於 Linux 型配方，將 Amazon 受管`aws-cli-version-2-linux`建置元件新增至配方。RES 安裝指令碼使用 AWS CLI 提供 DynamoDB 叢集設定組態值的 VDI 存取權。Windows 不需要此元件。
2. 新增為 Linux 或 Windows 環境建立的 EC2 Image Builder 元件，然後輸入任何必要的參數值。下列參數是必要的輸入：AWSAccountID、RESEnvName、RESEnvRegion 和 RESEnvReleaseVersion。

> **Important**
>
> 對於 Linux 環境，您必須依先新增`aws-cli-version-2-linux`建置元件的順序新增這些元件。
>
> 
>

3. 視需要完成任何選用區段，新增任何其他所需的元件，然後選擇建立配方。

設定 EC2 Image Builder 基礎設施

您可以使用基礎設施組態來指定映像建置器用來建置和測試映像建置器映像的 Amazon EC2 基礎設施。若要搭配 RES 使用，您可以選擇建立新的基礎設施組態，或使用現有的基礎設施組態。

- 若要建立新的基礎設施組態，請參閱建立基礎設施組態。
- 若要使用現有的基礎設施組態，請更新基礎設施組態。

若要設定 Image Builder 基礎設施：

1. 針對 IAM 角色，輸入您先前在 中設定的角色準備 IAM 角色以存取 RES 環境。
2. 針對執行個體類型，選擇至少具有 4 GB 記憶體的類型，並支援您選擇的基本 AMI 架構。請參閱 Amazon EC2 執行個體類型。
3. 對於 VPC、子網路和安全群組，您必須允許網際網路存取以下載軟體套件。還必須允許存取 RES 環境的 `cluster-settings` DynamoDB 資料表和 Amazon S3 叢集儲存貯體。

設定映像建置器映像管道

映像建置器映像管道會組合基礎映像、用於建置和測試的元件、基礎設施組態和分發設定。若要為 RES 就緒 AMIs 設定映像管道，您可以選擇建立新的管道，或使用現有的管道。如需詳細資訊，請參閱《映像建置器使用者指南》中的建立和更新 AMI 映像管道。

Create a new Image Builder pipeline

1. 在 開啟映像建置器主控台https://console.aws.amazon.com/imagebuilder。
2. 從導覽窗格中，選擇映像管道。
3. 選擇建立映像管道。
4. 輸入唯一名稱、選用描述、排程和頻率來指定管道詳細資訊。
5. 針對選擇配方，選擇使用現有配方，然後選取在 中建立的配方準備您的 EC2 Image Builder 配方。確認您的配方詳細資訊正確無誤。
6. 針對定義映像建立程序，根據使用案例選擇預設或自訂工作流程。在大多數情況下，預設工作流程已足夠。如需詳細資訊，請參閱為您的 EC2 Image Builder 管道設定映像工作流程。
7. 針對定義基礎設施組態，選擇選擇現有的基礎設施組態，然後選取在 中建立的基礎設施組態設定 EC2 Image Builder 基礎設施。確認您的基礎設施詳細資訊正確無誤。
8. 針對定義分佈設定，選擇使用服務預設值建立分佈設定。輸出映像必須位於與您的 RES 環境 AWS 區域 相同的 中。使用服務預設值，會在使用映像建置器的區域中建立映像。
9. 檢閱管道詳細資訊，然後選擇建立管道。

Modify an existing Image Builder pipeline

1. 若要使用現有的管道，請修改詳細資訊以使用在 中建立的配方準備您的 EC2 Image Builder 配方。
2. 選擇儲存變更。

執行映像建置器映像管道

若要產生設定的輸出映像，您必須啟動映像管道。建置程序可能需要長達一小時的時間，具體取決於映像配方中的元件數量。

若要執行映像管道：

1. 從映像管道中，選取在 中建立的管道設定映像建置器映像管道。
2. 在動作中，選擇執行管道。

在 RES 中註冊新的軟體堆疊

1. 遵循 中的指示the section called “軟體堆疊 (AMIs)”來註冊軟體堆疊。
2. 針對 AMI ID，輸入內建於 之輸出映像的 AMI ID執行映像建置器映像管道。

管理員指南

此管理員指南為技術對象提供有關如何進一步自訂並與 AWS 產品上的 Research and Engineering Studio 整合的其他說明。

主題

- 秘密管理
- 成本監控和控制
- 成本分析儀表板
- 工作階段管理
- 環境管理

秘密管理

Research and Engineering Studio 會使用 維護下列秘密 AWS Secrets Manager。RES 會在環境建立期間自動建立秘密。管理員在環境建立期間輸入的秘密會輸入為參數。

秘密名稱	描述	產生的 RES	管理員已輸入
`<envname> -sso-client-secret`	環境的單一登入 OAuth2 用戶端秘密	✓	
`<envname> -vdc-client-secret`	vdc ClientSecret	✓	
`<envname> -vdc-client-id`	vdc ClientId	✓	
`<envname> -vdc-gateway-certificate-private-key`	網域的自我簽署憑證私有金鑰	✓	
`<envname> -vdc-gateway-`	網域的自我簽署憑證	✓	

秘密名稱	描述	產生的 RES	管理員已輸入
certificate-certificate			
<envname> -cluster-manager-client-secret	cluster-manager ClientSecret	✓	
<envname> -cluster-manager-client-id	cluster-manager ClientId	✓	
<envname> -external-private-key	網域的自我簽署憑證私有金鑰	✓	
<envname> -external-certificate	網域的自我簽署憑證	✓	
<envname> -internal-private-key	網域的自我簽署憑證私有金鑰	✓	
<envname> -internal-certificate	網域的自我簽署憑證	✓	
<envname> -directoryservice-ServiceAccountUserDN	ServiceAccount 使用者的辨別名稱 (DN) 屬性。	✓	

下列秘密 ARN 值包含在 DynamoDB 的 <envname>-cluster-settings資料表中：

金鑰	來源
identity-provider.cognito.sso_client_secret	
vdc.dcv_connection_gateway.certificate.certificate_secret_arn	堆疊
vdc.dcv_connection_gateway.certificate.private_key_secret_arn	堆疊
cluster.load_balancers.internal_alb.certificates.private_key_secret_arn	堆疊
directoryservice.root_username_secret_arn	
vdc.client_secret	堆疊
cluster.load_balancers.external_alb.certificates.certificate_secret_arn	堆疊
cluster.load_balancers.internal_alb.certificates.certificate_secret_arn	堆疊
directoryservice.root_password_secret_arn	
cluster.secretsmanager.kms_key_id	
cluster.load_balancers.external_alb.certificates.private_key_secret_arn	堆疊
cluster-manager.client_secret	

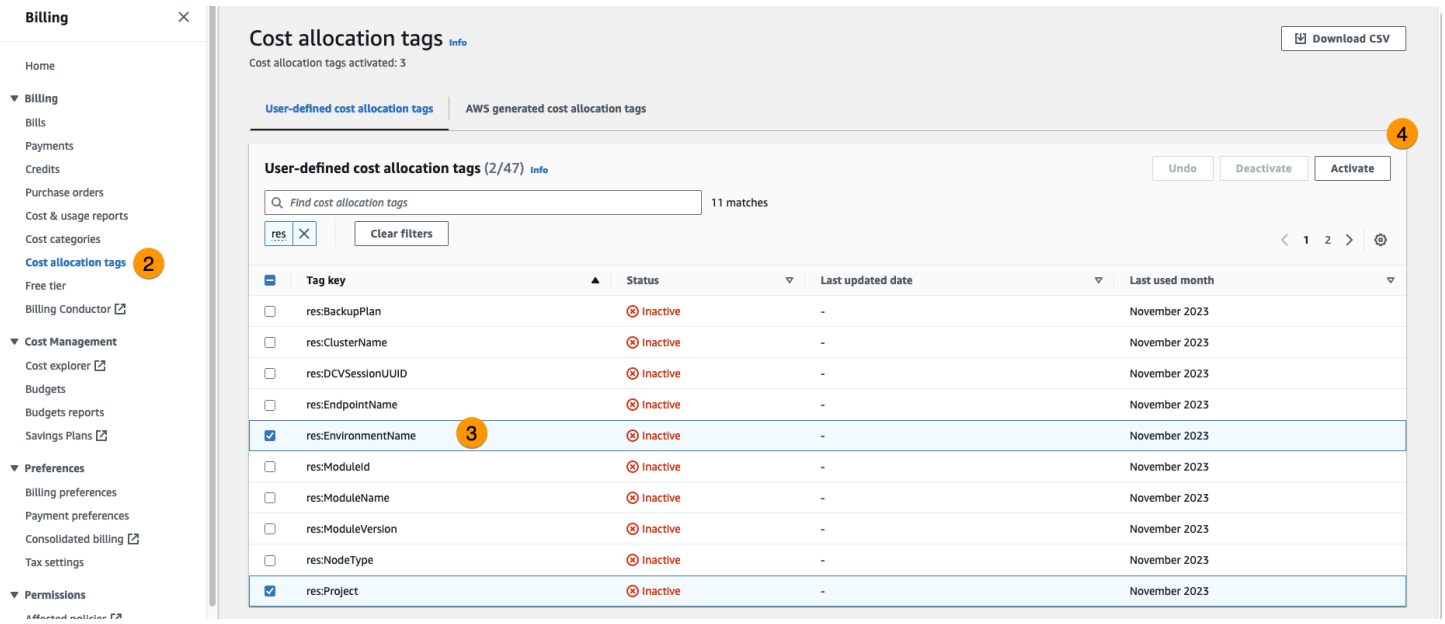
成本監控和控制

> **Note**
>
> AWS Budgets 不支援將 Research and Engineering Studio 專案與 建立關聯 AWS GovCloud (US)。

我們建議您透過 AWS Cost Explorer 建立預算，以協助管理成本。價格可能變動。如需完整詳細資訊，請參閱每個 的定價網頁the section called “AWS 此產品中的 服務”。

若要協助追蹤成本，您可以將 RES 專案與其中建立的預算建立關聯 AWS Budgets。您必須先啟用帳單成本分配標籤內的環境標籤。

1. 登入 AWS Management Console ，並在 https：//https://console.aws.amazon.com/costmanagement/ 開啟 AWS 帳單與成本管理 主控台。
2. 選擇成本分配標籤。
3. 搜尋並選取 `res:Project`和 `res:EnvironmentName`標籤。
4. 選擇 Activate (啟用)。

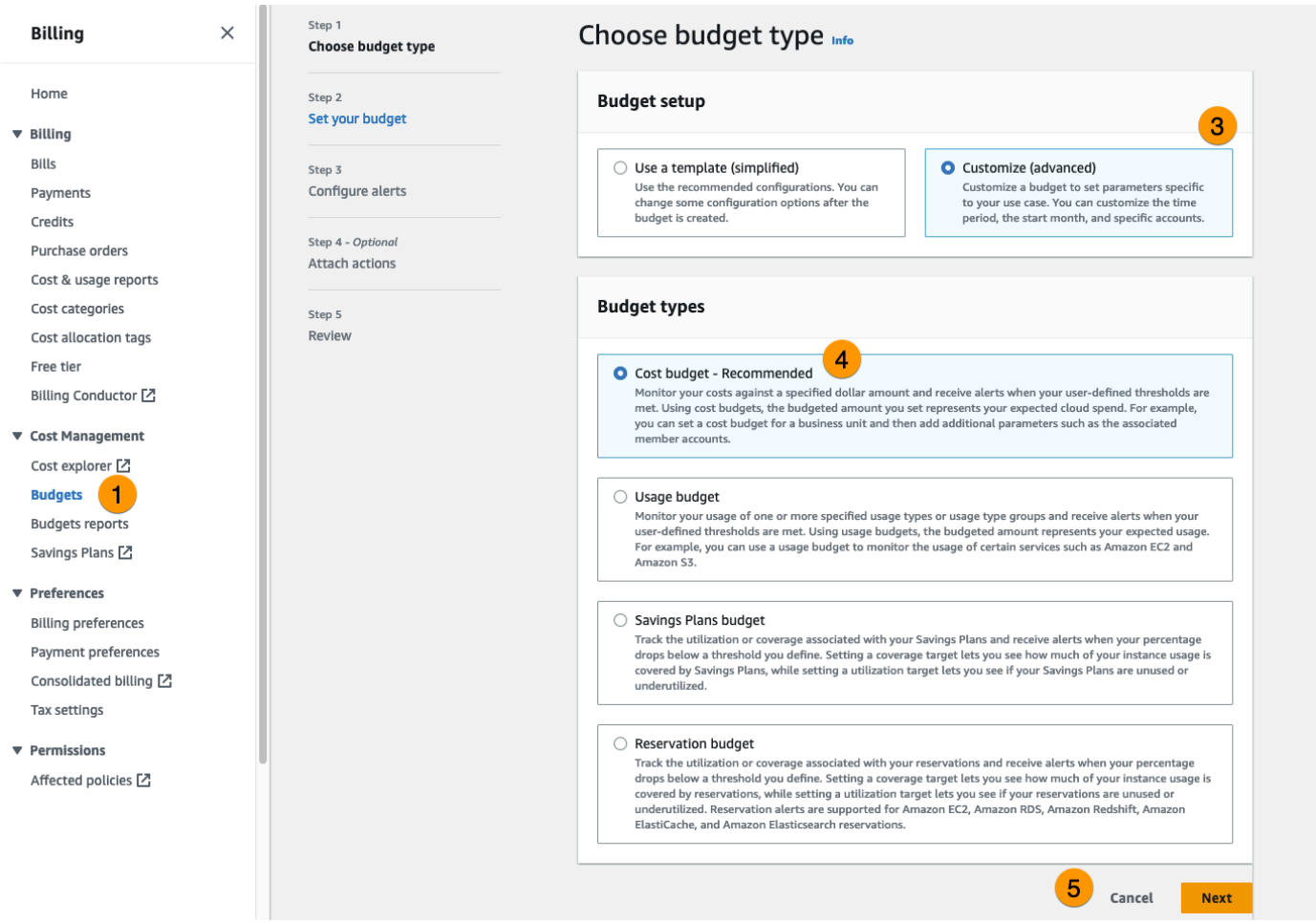


> **Note**
>
> 部署後，RES 標籤最多可能需要一天的時間才會出現。

若要建立 RES 資源的預算：

1. 從帳單主控台中，選擇預算。
2. 選擇建立預算。
3. 在預算設定下，選擇自訂（進階）。

4. 在預算類型下，選擇成本預算 - 建議。
5. 選擇下一步。

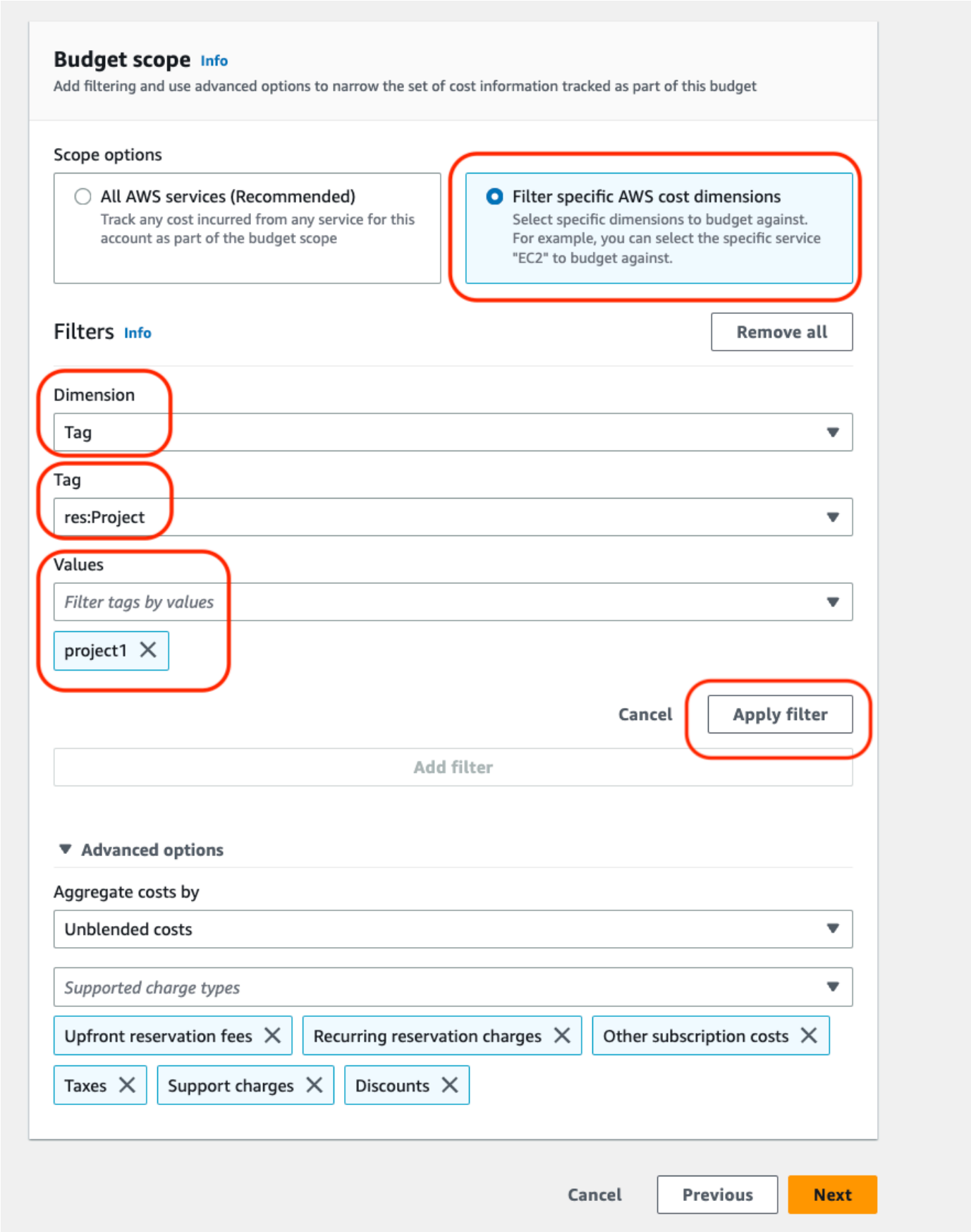


6. 在詳細資訊下，為您的預算輸入有意義的預算名稱，以將其與您帳戶中的其他預算區分開來。例如 *<EnvironmentName>-<ProjectName>-<BudgetName>*。
7. 在設定預算金額下，輸入專案的預算金額。
8. 在預算範圍內，選擇篩選特定 AWS 成本維度。
9. 選擇新增篩選條件。
10. 在維度下，選擇標籤。
11. 在標籤下，選取 res：Project。

> **Note**
>
> 標籤和值可能需要兩天的時間才能使用。您可以在專案名稱變成可用時建立預算。

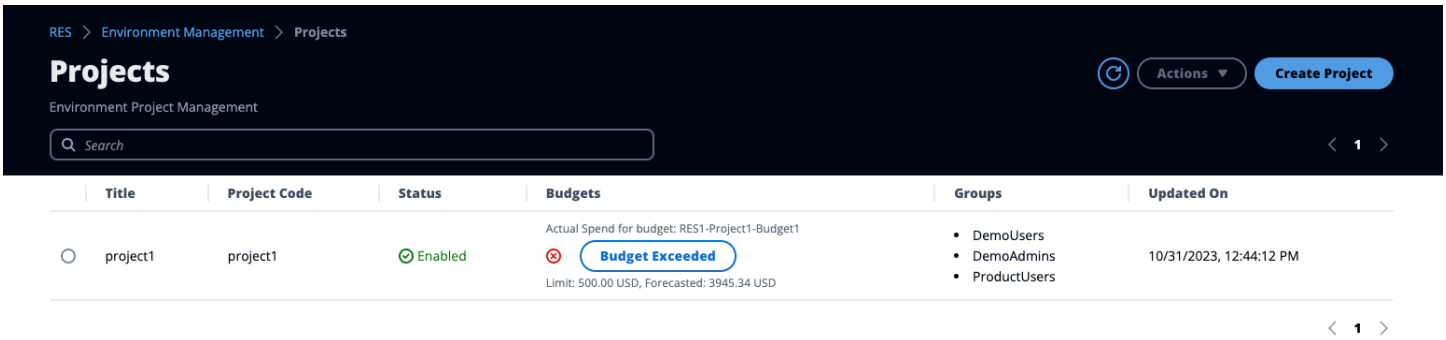
12. 在值下，選取專案名稱。

13. 選擇套用篩選條件，將專案篩選條件連接至預算。
14. 選擇下一步。


Budget scope Info
Add filtering and use advanced options to narrow the set of cost information tracked as part of this budget
Scope options
All AWS services (Recommended)
Track any cost incurred from any service for this account as part of the budget scope
Filter specific AWS cost dimensions
Select specific dimensions to budget against. For example, you can select the specific service "EC2" to budget against.
Filters Info
Remove all
Dimension
Tag
Tag
res:Project
Values
Filter tags by values
project1
Cancel
Apply filter
Add filter
Advanced options
Aggregate costs by
Unblended costs
Supported charge types
Upfront reservation fees
Recurring reservation charges
Other subscription costs
Taxes
Support charges
Discounts
Cancel
Previous
Next

15. （選用。）新增提醒閾值。
16. 選擇下一步。
17. （選用。）如果已設定提醒，請使用連接動作來設定具有提醒的所需動作。
18. 選擇下一步。
19. 檢閱預算組態，並確認已在其他預算參數下設定正確的標籤。
20. 選擇建立預算。

現在預算已建立，您可以啟用專案的預算。若要開啟專案的預算，請參閱 the section called “編輯專案”。如果超過預算，虛擬桌面將無法啟動。如果在啟動桌面時超過預算，桌面將繼續運作。



如果您需要變更預算，請返回主控台編輯預算金額。變更在 RES 中最多可能需要 15 分鐘才會生效。或者，您可以編輯專案以停用預算。

成本分析儀表板

成本分析儀表板可讓 RES 管理員從 RES 入口網站監控專案預算和一段時間內的專案成本。您可以在專案層級篩選成本。

主題

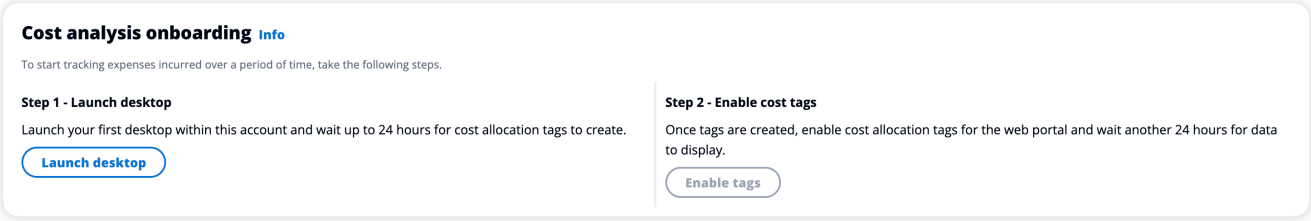
- 先決條件
- 具有預算指派圖表的專案
- 時間圖表的成本分析
- 下載 CSV

先決條件

若要使用 Research and Engineering Studio 的成本儀表板，您必須先：

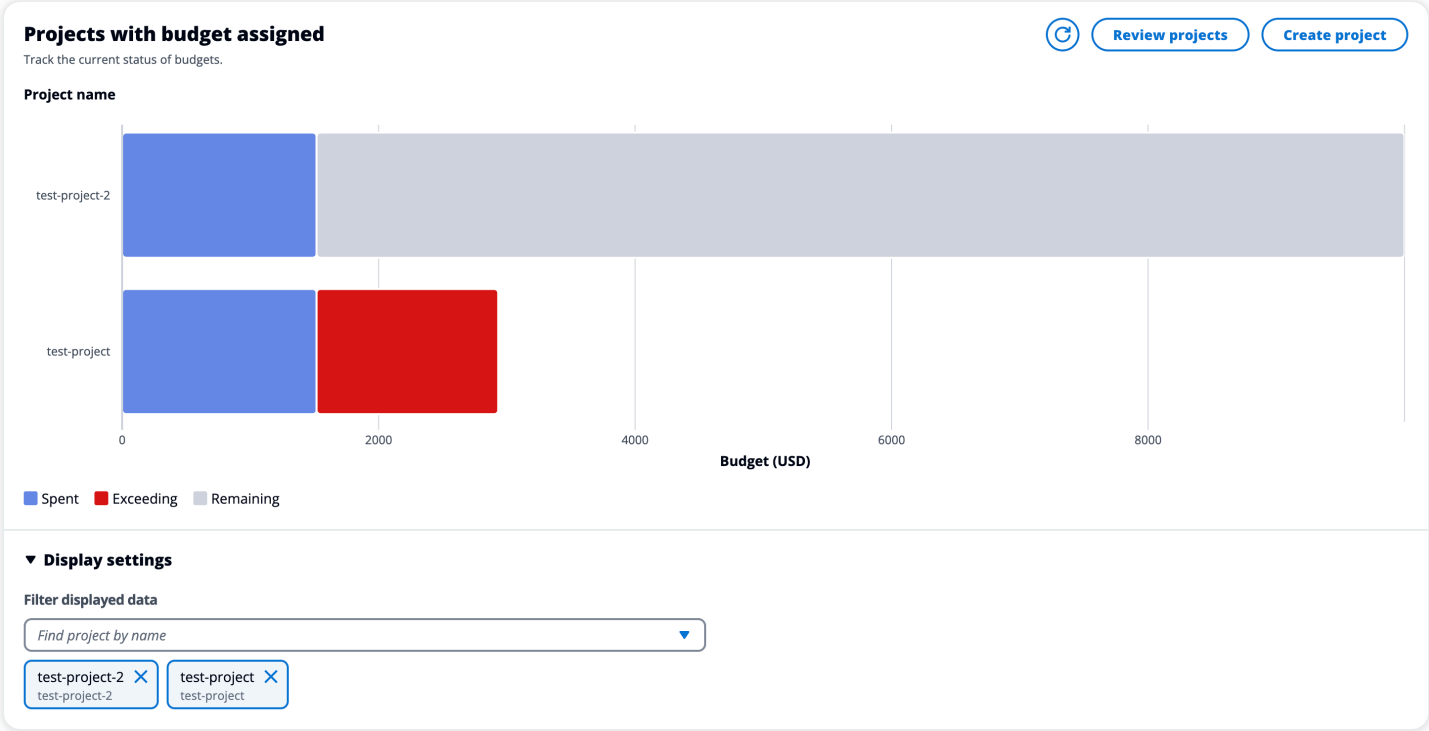
- 建立專案.
- 在 AWS Billing and Cost Management 主控台中建立預算。
- 將預算連接至專案（請參閱 編輯專案)。
- 為具有新 RES 部署的帳戶啟用成本分析圖表。若要這麼做，請依照下列步驟進行：

  1. 為您建立的專案部署 VDI。這會在 AWS Cost Explorer 中佈建`res:Project`標籤，最多可能需要 24 小時。
  2. 建立標籤後，啟用標籤按鈕會啟動。選擇按鈕以在 Cost Explorer 中啟用標籤。此程序可能需要額外 24 小時。



具有預算指派圖表的專案

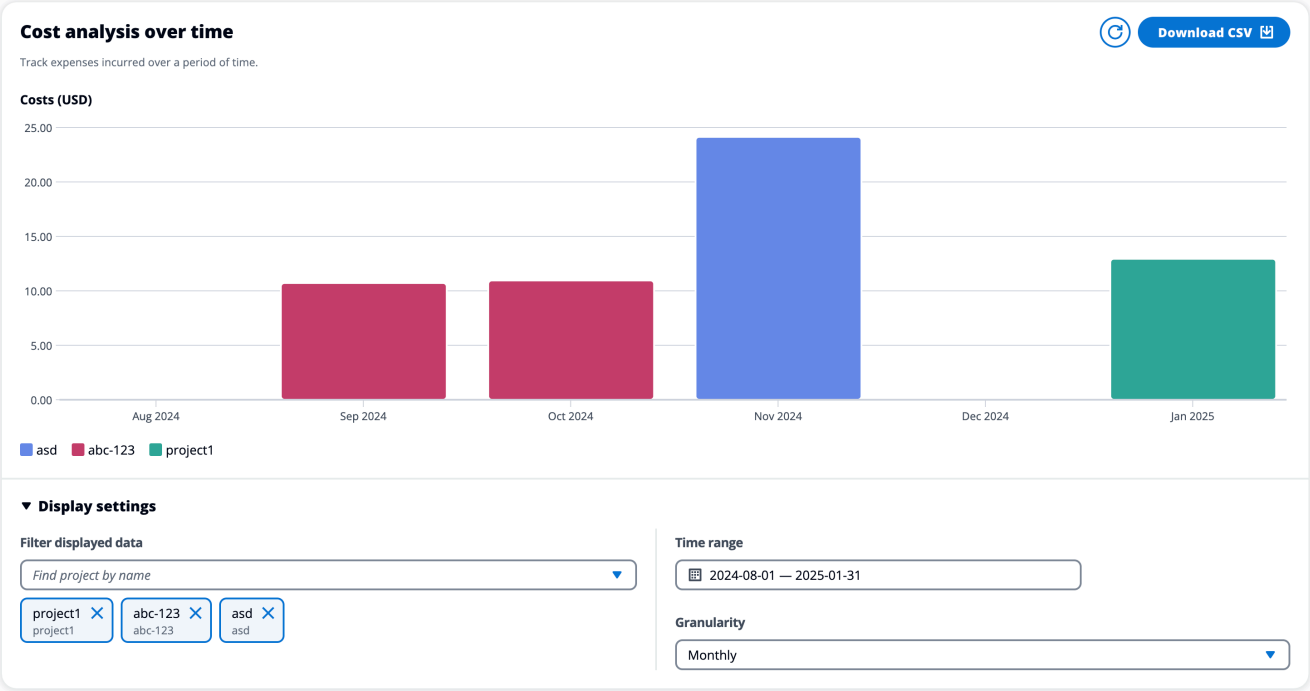
已指派預算的專案圖表會顯示 RES 環境中已指派預算的專案預算狀態。根據預設，圖表會依預算金額顯示前 5 個專案。您可以在篩選顯示的資料下拉式清單中選取特定專案，載入預算指派專案的完整清單。



圖表會以 USD 貨幣顯示每個預算的花費、剩餘和超出金額。將滑鼠游標移至長條上，以顯示每個類別的確切 USD 金額。您也可以分別選擇右上角的檢閱專案和建立專案按鈕，以開啟專案和建立專案頁面。

時間圖表的成本分析

隨時間推移的成本分析圖表會顯示指定期間內專案的成本明細。根據預設，圖表會顯示過去 6 個月的每個資料。它會使用您選取的精細度，依所選時間範圍的總成本顯示前 5 個專案。除了前 5 個項目外，所有其他選取的專案都會彙總到其他類別下。

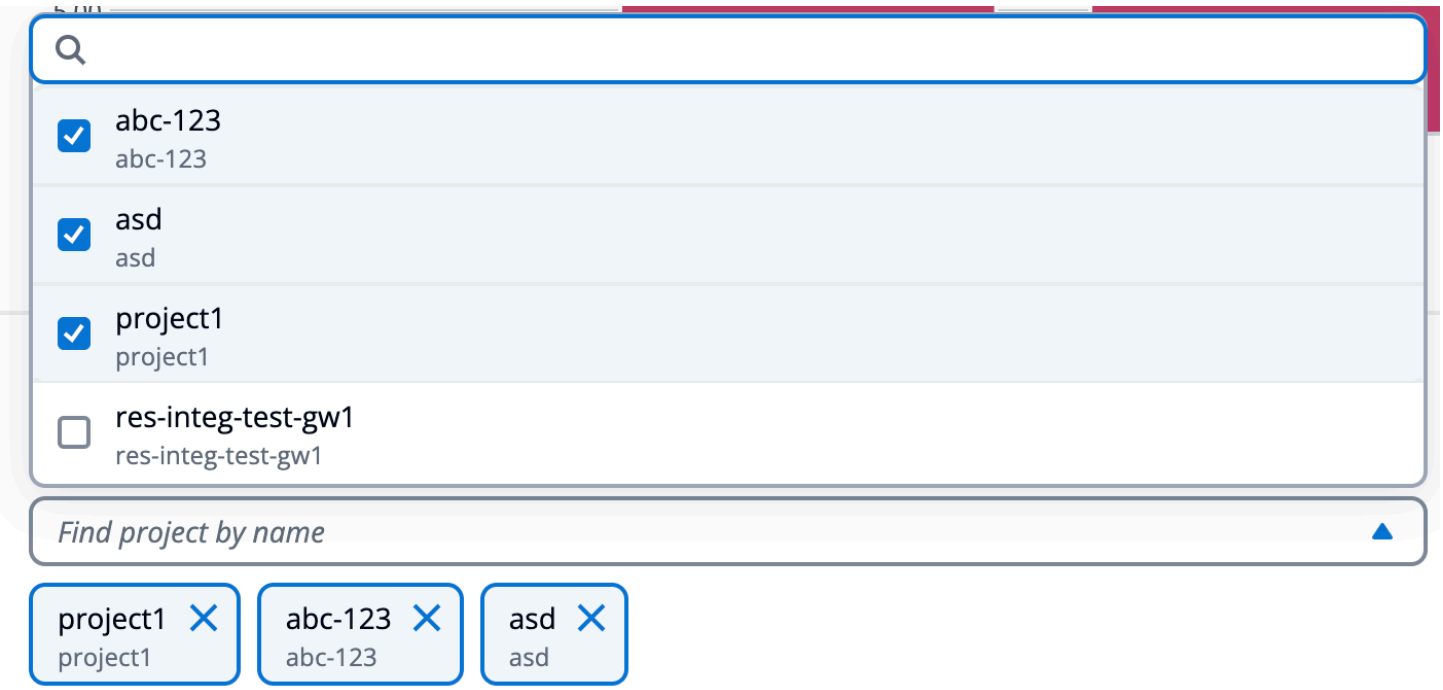


篩選條件

您可以依專案、時間範圍和精細程度進行篩選，以自訂時間圖表檢視的成本分析。如果選取任何無效的篩選條件組合，則會彈出一個模態視窗，讓您選擇還原至先前的組態，或接受更新篩選條件組合的建議。

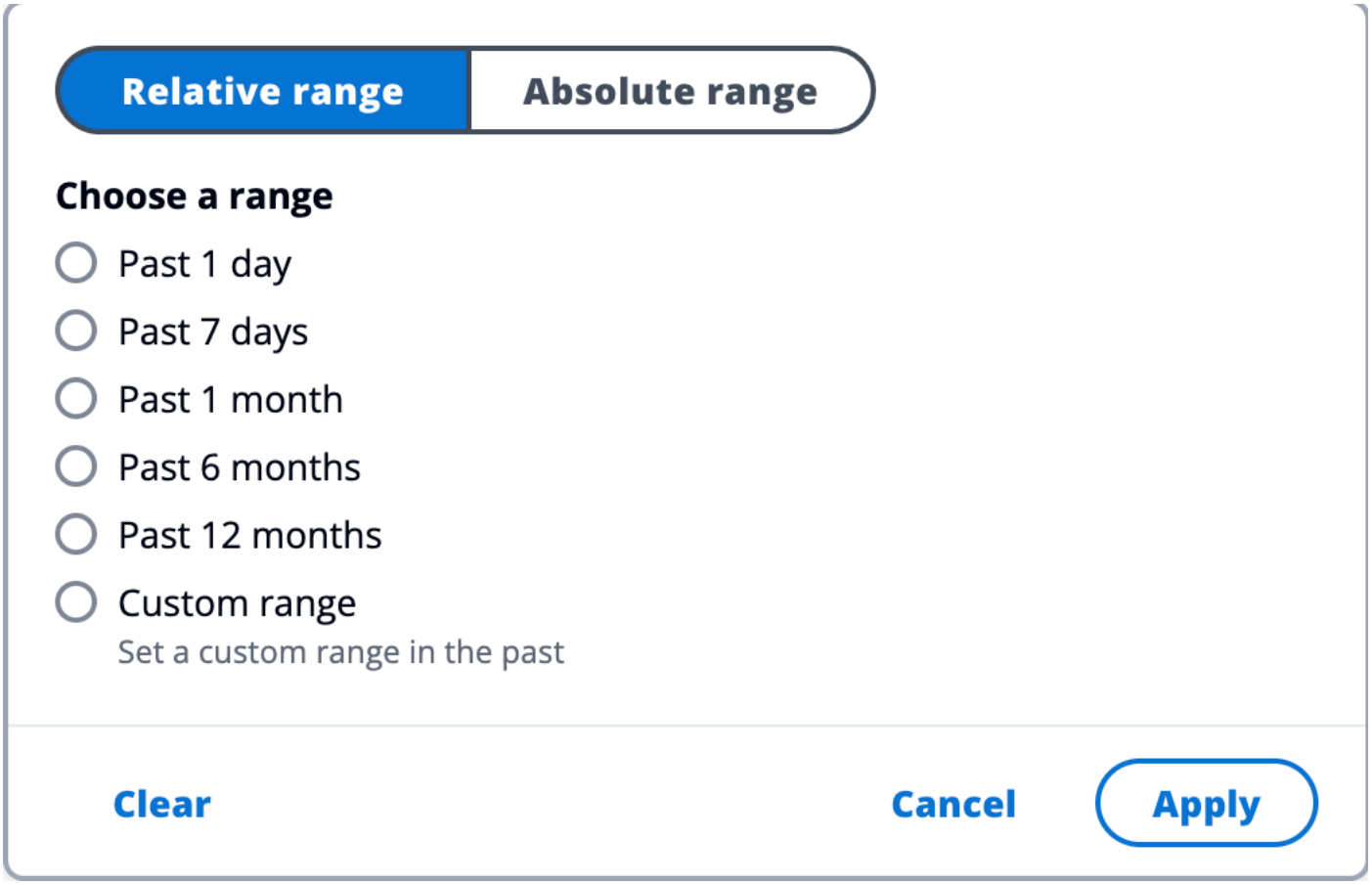
專案

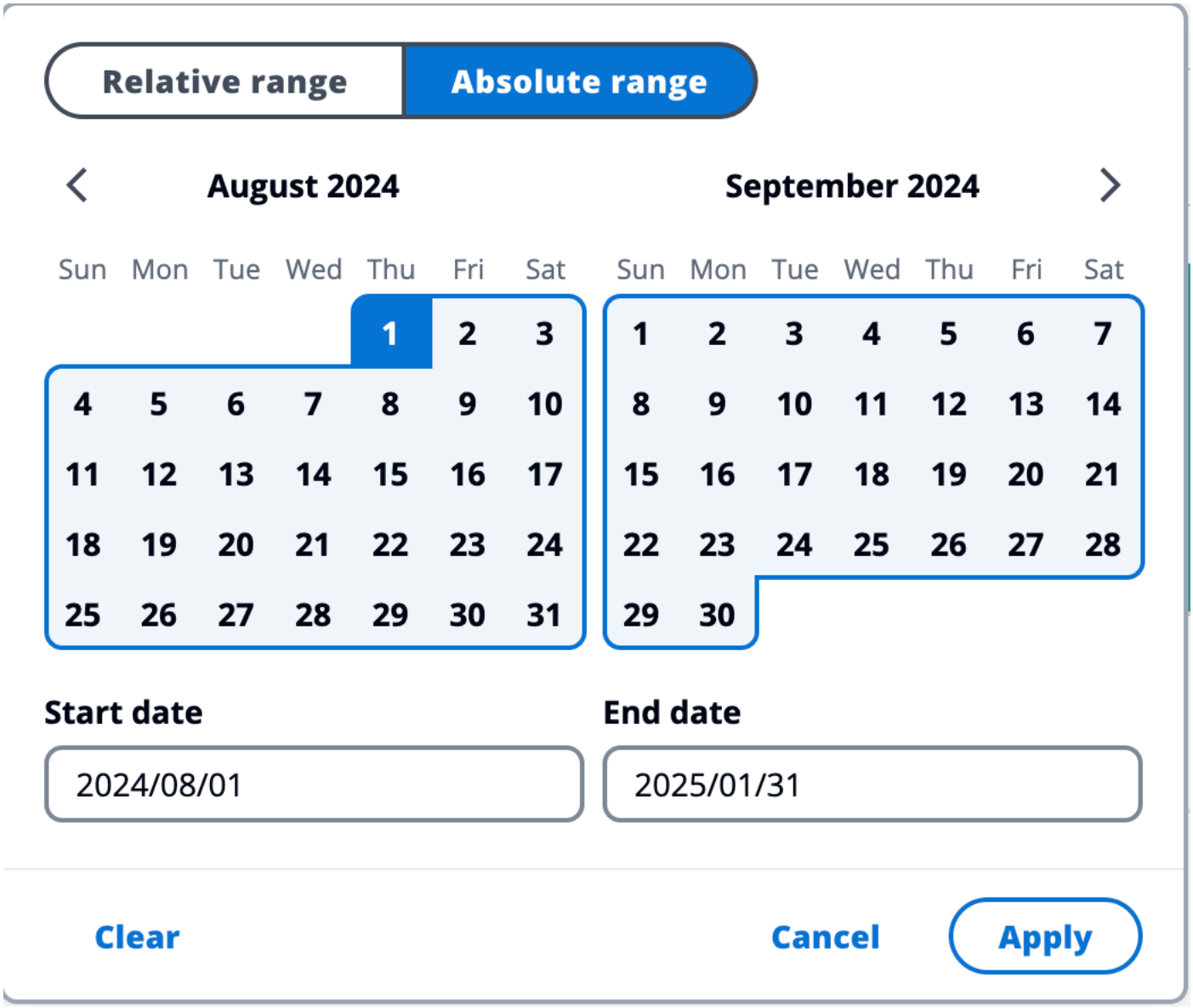
當您選擇篩選顯示的資料下拉式清單時，您會在目前的 RES 環境中看到專案的完整清單。您會看到專案名稱，並在下面顯示專案代碼。



指定時間範圍

當您指定日期範圍時，可以選擇使用絕對範圍或相對範圍。當您選取相對範圍時，會使用完整的時間單位來計算日期。例如，如果您在 2025 年 2 月選取過去 6 個月選項，這將導致時間範圍為 8/1/25 - 1/31/25。


Relative range
Absolute range
Choose a range
Past 1 day
Past 7 days
Past 1 month
Past 6 months
Past 12 months
Custom range
Set a custom range in the past
Clear
Cancel
Apply

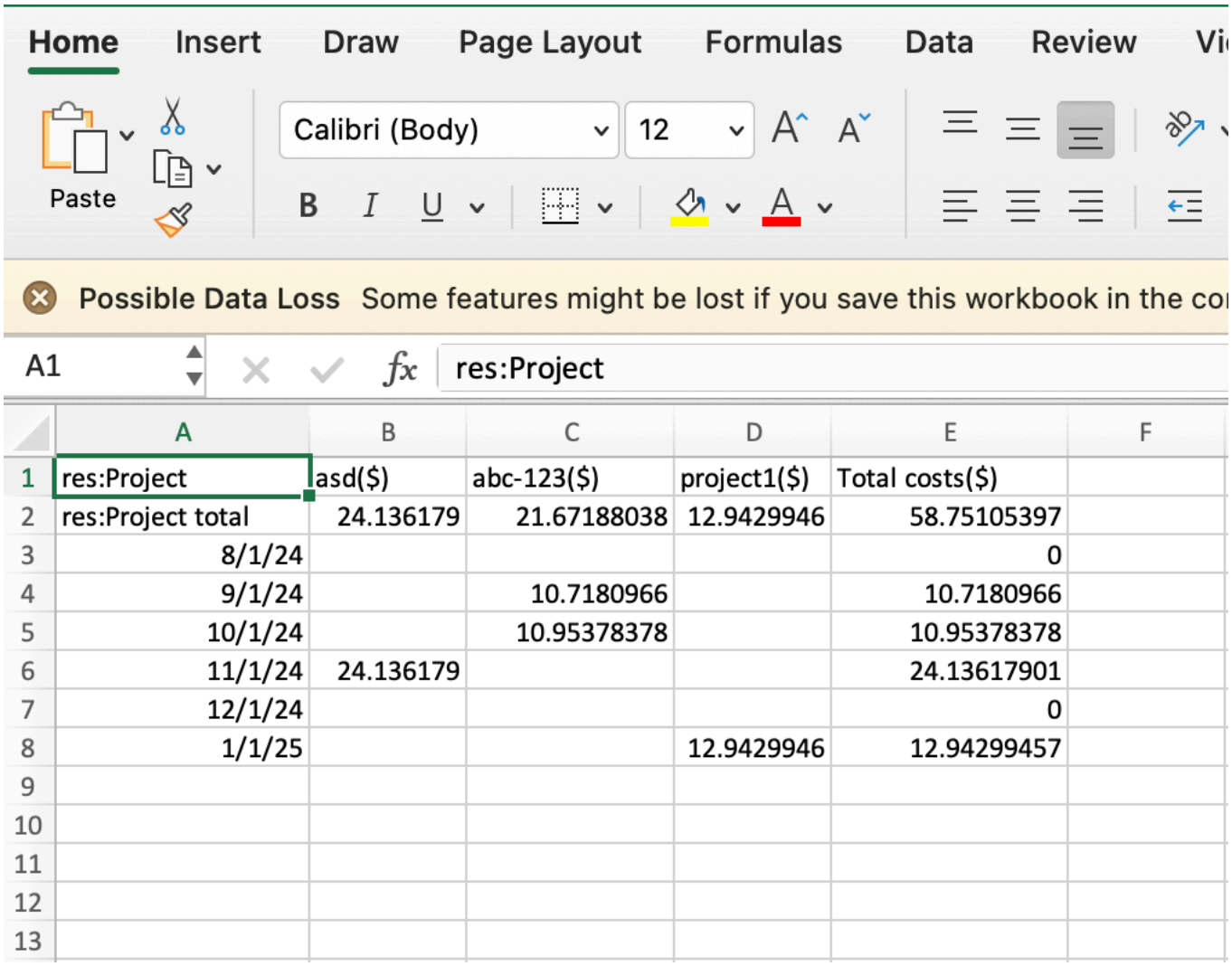


精細程度

您可以選擇檢視每月、每日或每小時精細程度的資料。每小時精細程度僅支援最多 14 天的日期範圍。每日精細程度僅支援最長 14 個月的日期範圍。

下載 CSV

若要匯出目前的成本分析檢視，請選擇時間圖表成本分析右上角的下載 CSV。下載的 CSV 包含指定期間內每個所選專案的成本資訊，以及依專案和依時段的成本總計。



	A	B	C	D	E	F
1	res:Project	asd($)	abc-123($)	project1($)	Total costs($)	
2	res:Project total	24.136179	21.67188038	12.9429946	58.75105397	
3	8/1/24				0	
4	9/1/24		10.7180966		10.7180966	
5	10/1/24		10.95378378		10.95378378	
6	11/1/24	24.136179			24.13617901	
7	12/1/24				0	
8	1/1/25			12.9429946	12.94299457	
9						
10						
11						
12						
13						

工作階段管理

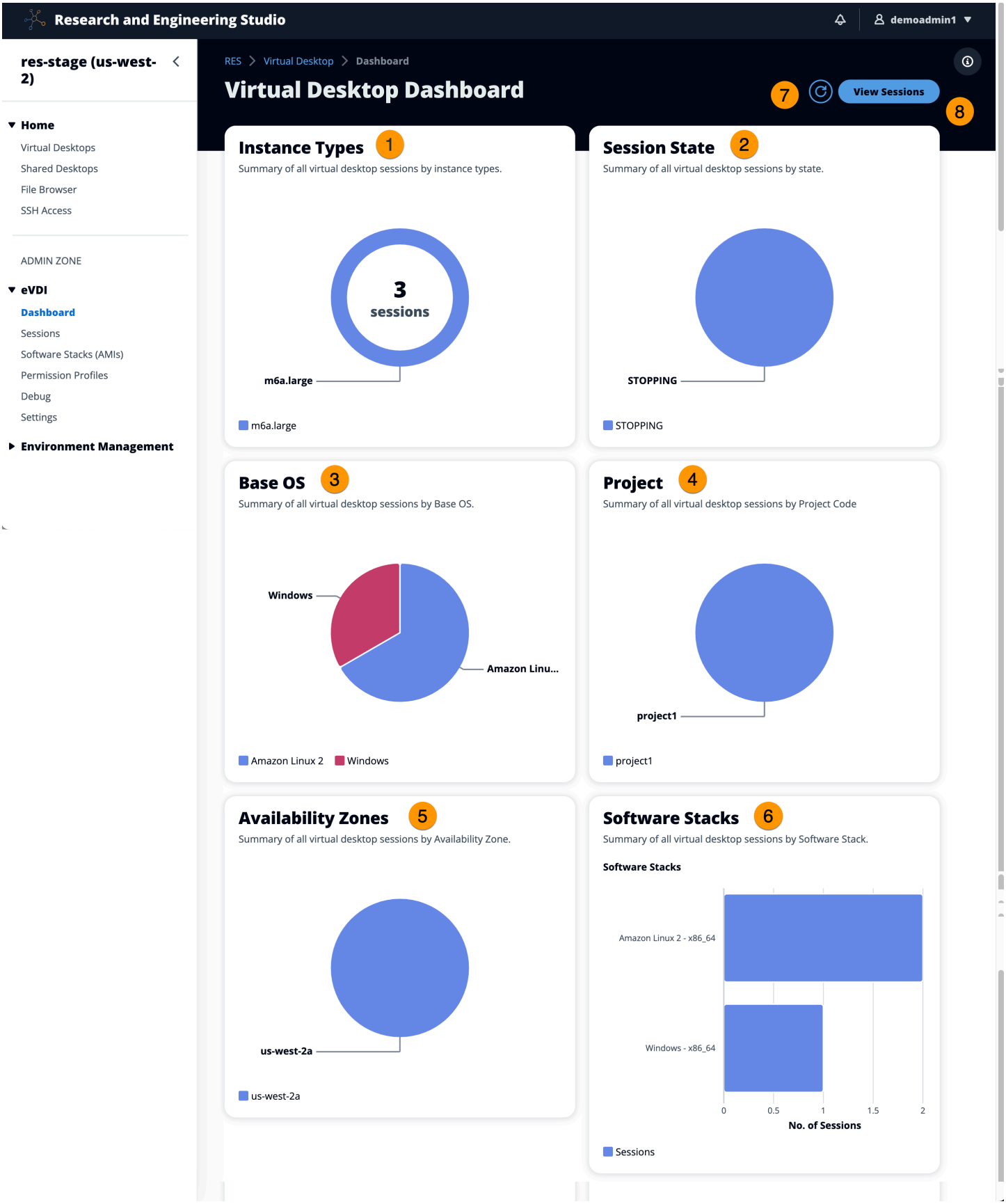
工作階段管理為開發和測試工作階段提供靈活且互動式的環境。身為管理使用者，您可以允許使用者在其專案環境中建立和管理互動式工作階段。

主題

- 儀表板
- 工作階段
- 軟體堆疊 (AMIs)

- 除錯
- 桌面設定

儀表板


Research and Engineering Studio
demoadmin1
res-stage (us-west-2)
Home
Virtual Desktops
Shared Desktops
File Browser
SSH Access
ADMIN ZONE
eVDI
Dashboard
Sessions
Software Stacks (AMIs)
Permission Profiles
Debug
Settings
Environment Management
RES > Virtual Desktop > Dashboard
Virtual Desktop Dashboard
7
View Sessions
8
Instance Types
1
Summary of all virtual desktop sessions by instance types.
3
sessions
m6a.large
m6a.large
Session State
2
Summary of all virtual desktop sessions by state.
STOPPING
STOPPING
Base OS
3
Summary of all virtual desktop sessions by Base OS.
Windows
Amazon Linu...
Amazon Linux 2
Windows
Project
4
Summary of all virtual desktop sessions by Project Code
project1
project1
Availability Zones
5
Summary of all virtual desktop sessions by Availability Zone.
us-west-2a
us-west-2a
Software Stacks
6
Summary of all virtual desktop sessions by Software Stack.
Software Stacks
Amazon Linux 2 - x86_64
Windows - x86_64
0
0.5
1
1.5
2
No. of Sessions
Sessions

工作階段管理儀表板可讓管理員快速檢視：

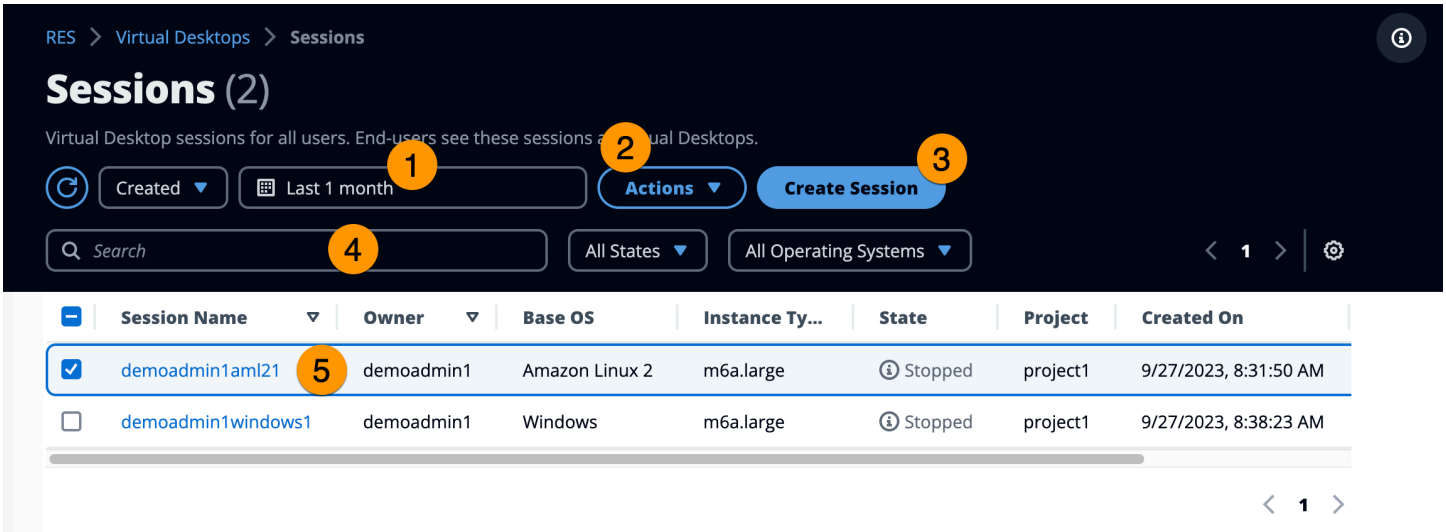
1. 執行個體類型
2. 工作階段狀態
3. 基礎作業系統
4. 專案
5. 可用區域
6. 軟體堆疊

此外，管理員可以：

7. 重新整理儀表板以更新資訊。
8. 選擇檢視工作階段以導覽至工作階段。

工作階段

工作階段會顯示所有在 Research and Engineering Studio 中建立的虛擬桌面。從工作階段頁面，您可以篩選和檢視工作階段資訊或建立新的工作階段。



1. 使用選單，依在指定時間範圍內建立或更新的工作階段篩選結果。
2. 選取工作階段並使用動作功能表來：
   a. 繼續工作階段 (s)
   b. 停止/休眠工作階段 (s)

c. 強制停止/休眠工作階段 (s)

d. 終止工作階段 (s)

e. 強制終止工作階段 (s)

f. Session(s) 運作狀態

g. 建立軟體堆疊

3. 選擇建立工作階段以建立新的工作階段。
4. 依名稱搜尋工作階段，並依狀態和作業系統篩選。
5. 選取工作階段名稱以檢視更多詳細資訊。

建立工作階段

1. 選擇建立工作階段。啟動新的虛擬桌面模態隨即開啟。
2. 輸入新工作階段的詳細資訊。
3. （選用。) 開啟顯示進階選項，以提供其他詳細資訊，例如子網路 ID 和 DCV 工作階段類型。
4. 選擇提交。

Launch New Virtual Desktop

Session Name

Enter a name for the virtual desktop

Session Name is required. Use any characters and form a name of length between 3 and 24 characters, inclusive.

User

Select the user to create the session for

Project

Select the project under which the session will get created

Operating System

Select the operating system for the virtual desktop

Amazon Linux 2

Software Stack

Select the software stack for your virtual desktop

Enable Instance Hibernation

Hibernation saves the contents from the instance memory (RAM) to your Amazon Elastic Block Store (Amazon EBS) root volume. You can not change instance type if you enable this option.

Virtual Desktop Size

Select a virtual desktop instance type

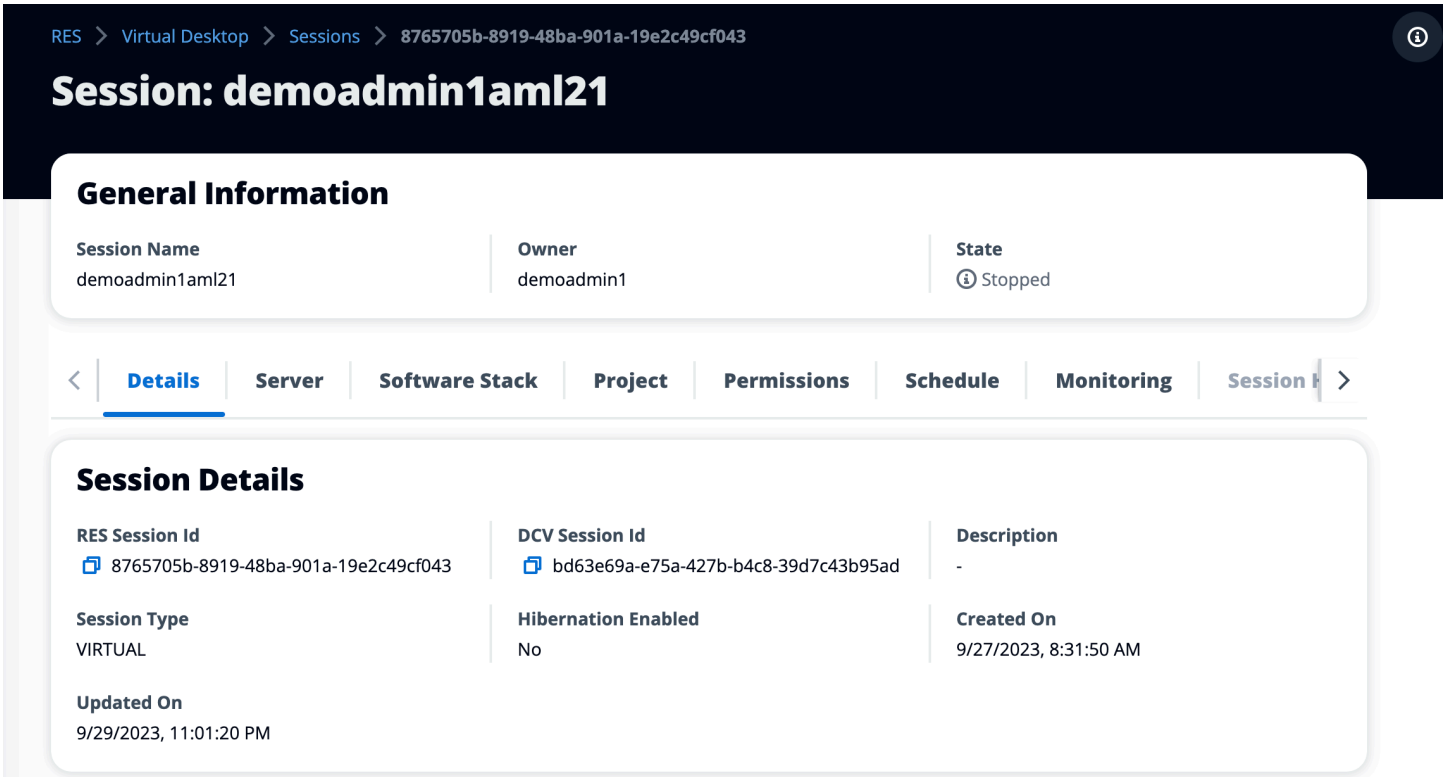
Storage Size (GB)

Enter the storage size for your virtual desktop in GBs

10

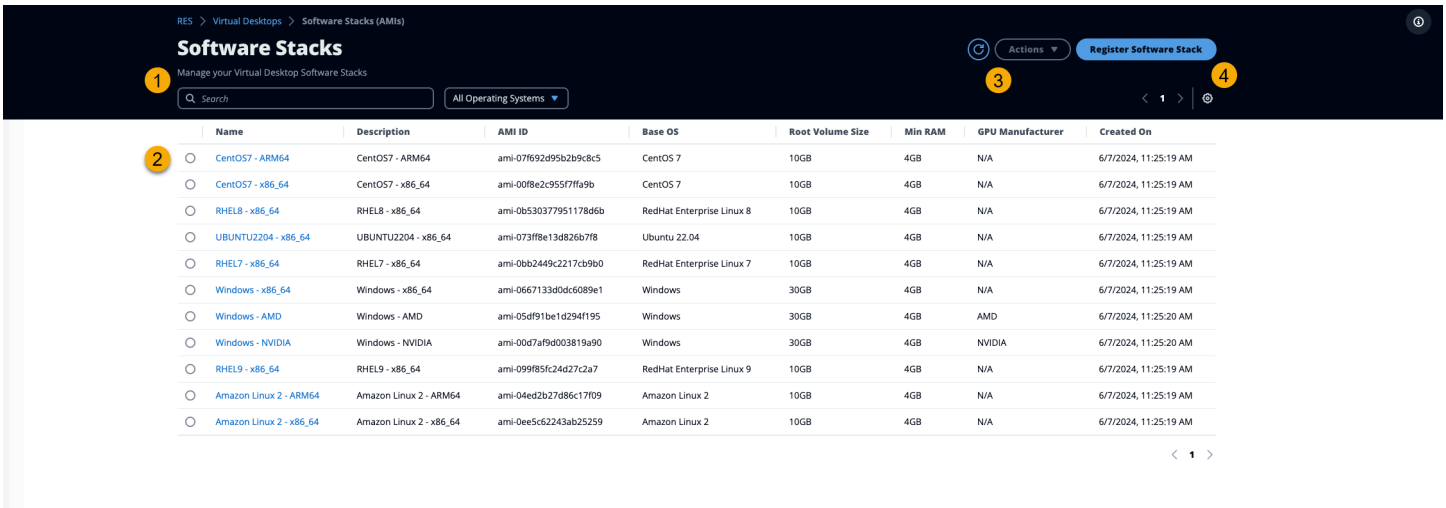
工作階段詳細資訊

從工作階段清單中，選取工作階段名稱以檢視工作階段詳細資訊。



軟體堆疊 (AMIs)

從軟體堆疊頁面，您可以設定 Amazon Machine Image (AMIs) 或管理現有的映像。



1. 若要搜尋現有的軟體堆疊，請使用作業系統下拉式清單依作業系統篩選。
2. 選取軟體堆疊的名稱，以檢視堆疊的詳細資訊。

3. 選擇軟體堆疊旁的選項按鈕，然後使用動作功能表來編輯堆疊，並將堆疊指派給專案。
4. 選擇註冊軟體堆疊按鈕來建立新的堆疊。

註冊新的軟體堆疊

註冊軟體堆疊按鈕可讓您建立新的堆疊：

1. 選擇註冊軟體堆疊。
2. 輸入新軟體堆疊的詳細資訊。
3. 選擇提交。

Register new Software Stack

Name

Enter a name for the software stack

Use any characters and form a name of length between 3 and 24 characters, inclusive.

Description

Enter a user friendly description for the software stack

AMI Id

Enter the AMI Id

AMI Id must start with ami-xxx

Operating System

Select the operating system for the software stack

Amazon Linux 2

GPU Manufacturer

Select the GPU Manufacturer for the software stack

N/A

Min. Storage Size (GB)

Enter the min. storage size for your virtual desktop in GBs

10

Min. RAM (GB)

Enter the min. ram for your virtual desktop in GBs

10

Projects

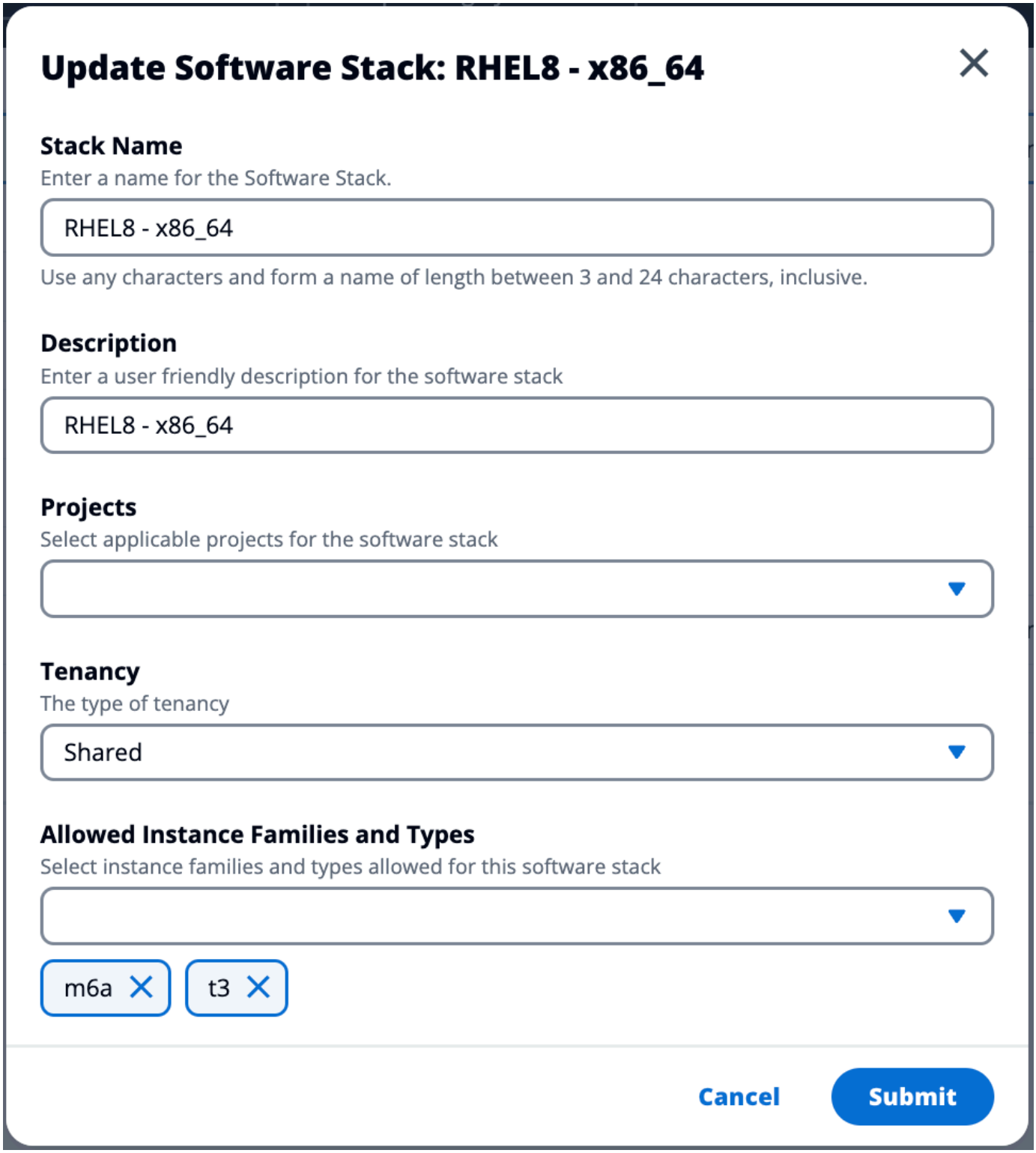
Select applicable projects for the software stack

將軟體堆疊指派給專案

當您建立新的軟體堆疊時，您可以將堆疊指派給專案。但是，如果您需要在初始建立之後將堆疊新增至專案，請執行下列動作：

> **Note**
>
> 您只能將軟體堆疊指派給您為成員的專案。

1. 在軟體堆疊頁面上，選取您要新增至專案之軟體堆疊的選項按鈕。
2. 選擇動作。
3. 選擇編輯。
4. 使用專案下拉式清單選取專案。

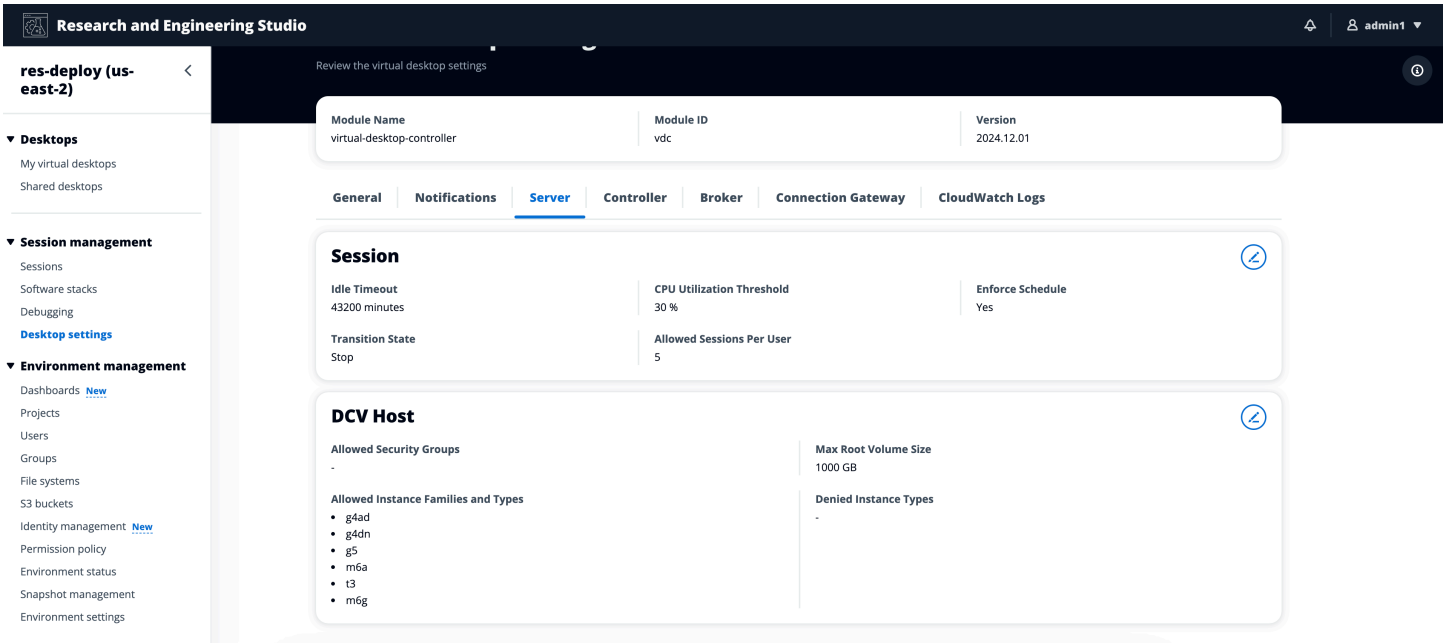


5. 選擇提交。

您也可以從堆疊詳細資訊頁面編輯軟體堆疊。

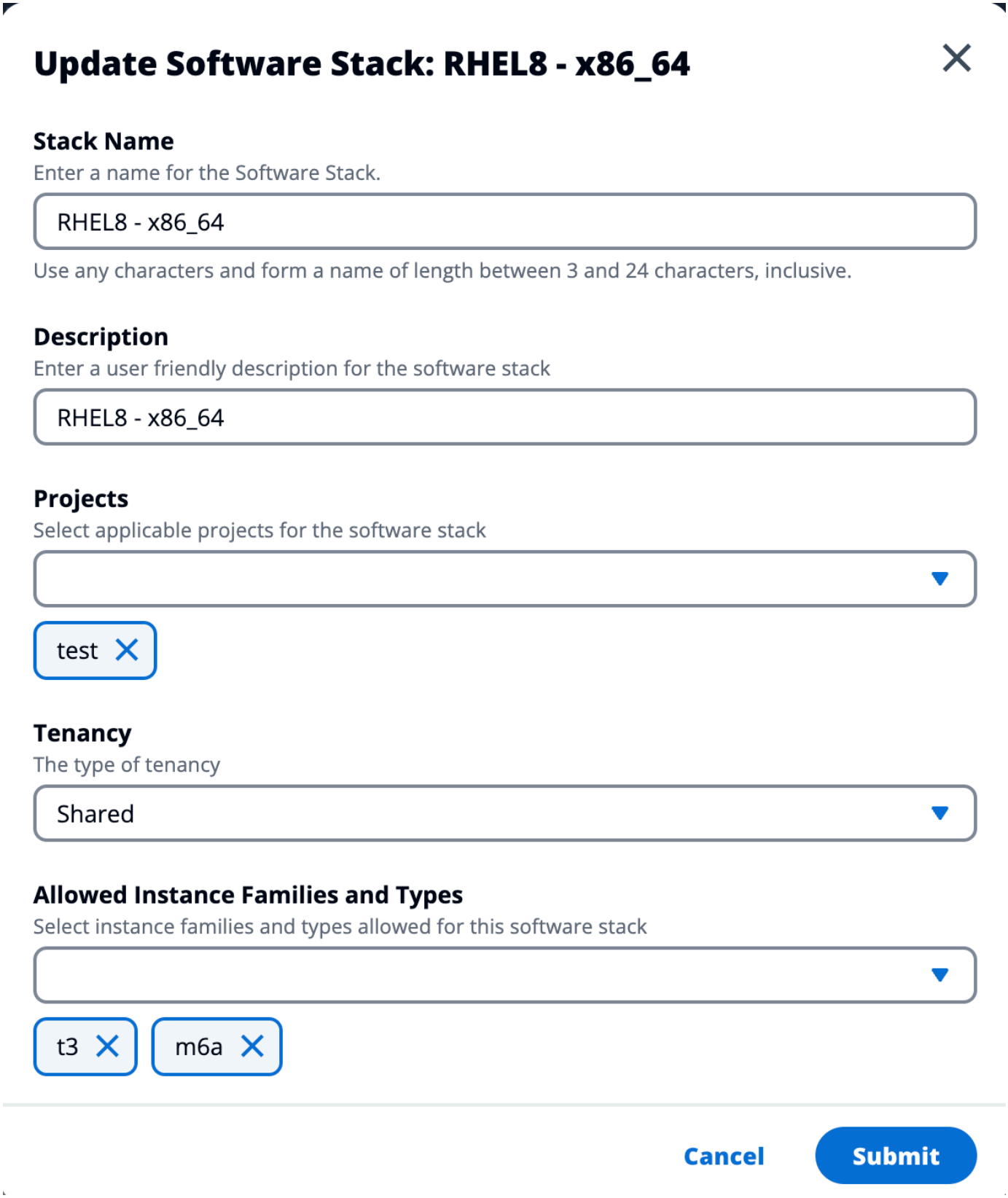
修改軟體堆疊的 VDI 執行個體清單

對於每個已註冊的軟體堆疊，您可以選擇允許的執行個體系列和類型。每個軟體堆疊的選項清單會依桌面設定中定義的選項進行篩選。您可以在該處找到和修改全域允許的執行個體系列和類型。



若要編輯軟體堆疊的允許執行個體系列和類型屬性：

1. 在軟體堆疊頁面上，選擇軟體堆疊的選項按鈕。
2. 選擇動作，然後選取編輯堆疊。
3. 從允許執行個體系列和類型下的下拉式清單中選擇所需的執行個體系列和類型。


Update Software Stack: RHEL8 - x86_64
Stack Name
Enter a name for the Software Stack.
RHEL8 - x86_64
Use any characters and form a name of length between 3 and 24 characters, inclusive.
Description
Enter a user friendly description for the software stack
RHEL8 - x86_64
Projects
Select applicable projects for the software stack
test
Tenancy
The type of tenancy
Shared
Allowed Instance Families and Types
Select instance families and types allowed for this software stack
t3
m6a
Cancel
Submit

4. 選取提交。

> **Note**
>
> 如果允許的執行個體系列和類型全域集包含執行個體系列和該系列內的執行個體類型（例如 `t3`和 `t3.large`），則軟體堆疊的允許執行個體系列和類型屬性的可用選項只會包含執行個體系列。

> **Important**
>
> - 從環境層級的允許清單中刪除執行個體類型/系列時，應該會自動從所有軟體堆疊中移除。
> - 在環境層級新增的執行個體類型/系列不會自動新增至軟體堆疊。

檢視軟體堆疊詳細資訊

從軟體堆疊頁面，選取軟體堆疊名稱以檢視其詳細資訊。您也可以選取軟體堆疊的選項按鈕，選擇動作，然後選取編輯以編輯軟體堆疊。

VDI 租用支援

當您註冊新的軟體堆疊或編輯現有的軟體堆疊時，您可以為從此軟體堆疊啟動VDIs 選取租用。支援以下三個租用：

- 共用（預設）- 使用共用硬體執行個體執行 VDIs
- 專用執行個體 - 使用專用執行個體執行 VDIs
- 專用主機 - 使用專用主機執行 VDIs

Register new Software Stack

Name

Enter a name for the software stack

Use any characters and form a name of length between 3 and 24 characters, inclusive.

Description

Enter a user friendly description for the software stack

AMI ID

Enter the AMI ID

AMI ID must start with ami-xxx

Operating System

Select the operating system for the software stack

Amazon Linux 2

GPU Manufacturer

Select the GPU Manufacturer for the software stack

N/A

Min. Storage Size (GB)

Enter the min. storage size for your virtual desktop in GBs

50

Min. RAM (GB)

Enter the min. ram for your virtual desktop in GBs

10

Projects

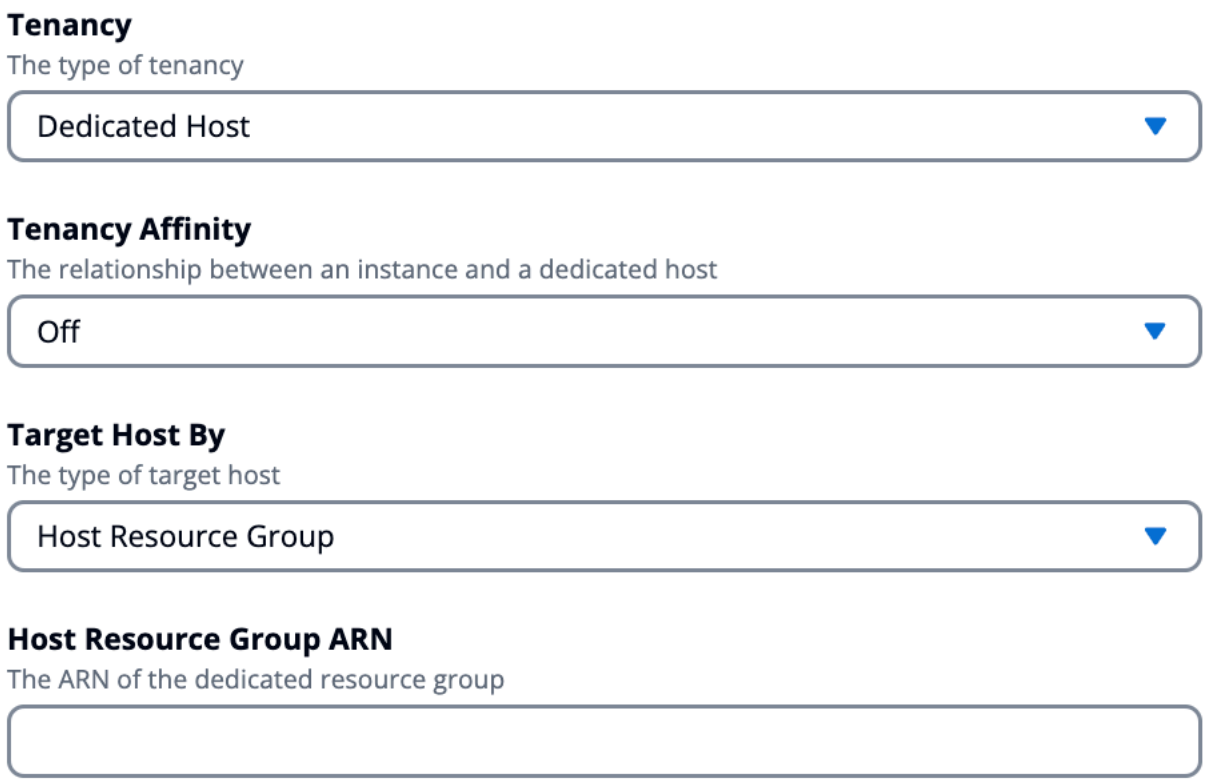
Select applicable projects for the software stack

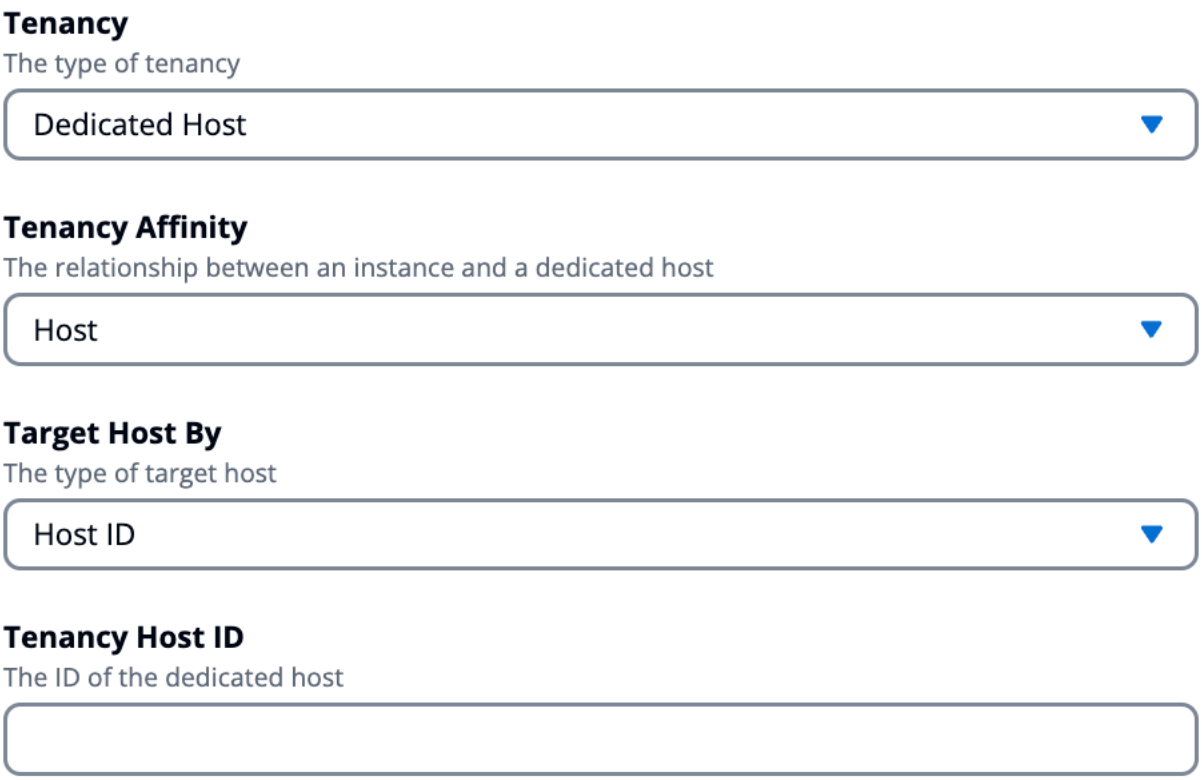
Tenancy

The type of tenancy

選取專用主機租用類型時，您還必須選取租用親和性與目標主機類型。支援下列目標主機類型：

- 主機資源群組 - 在 AWS License Manager 中建立的主機資源群組
- 主機 ID - 特定主機 ID

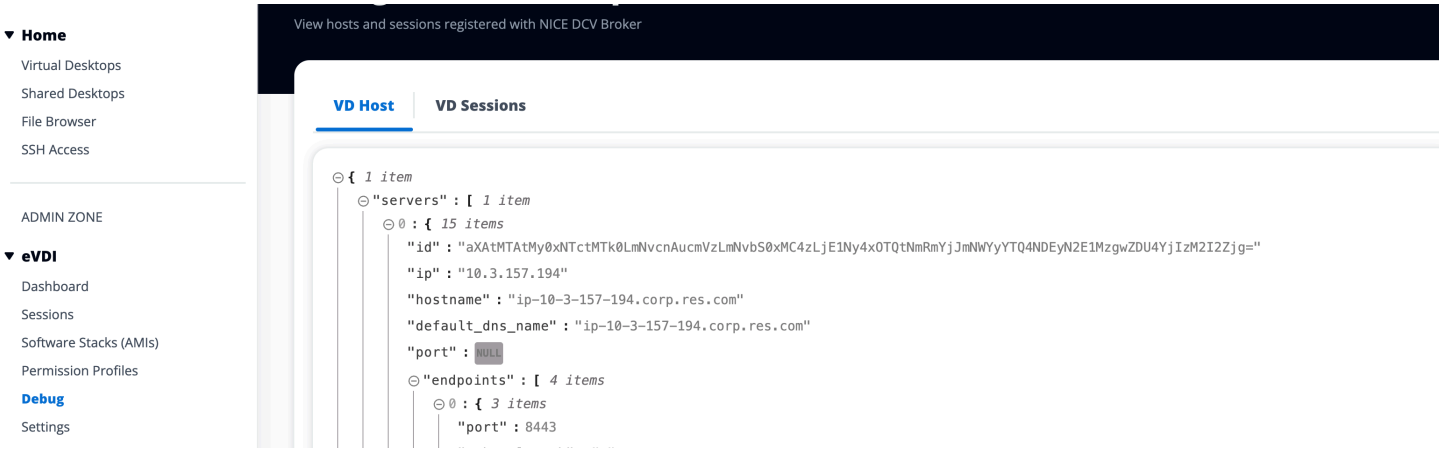




若要在啟動 VDIs 時指定 VDI 所需的任何自我管理授權與專用主機租用，請依照《 License AWS Manager 使用者指南》中的建立自我管理授權和 AMIs 的關聯，將授權與 AMI 建立關聯。

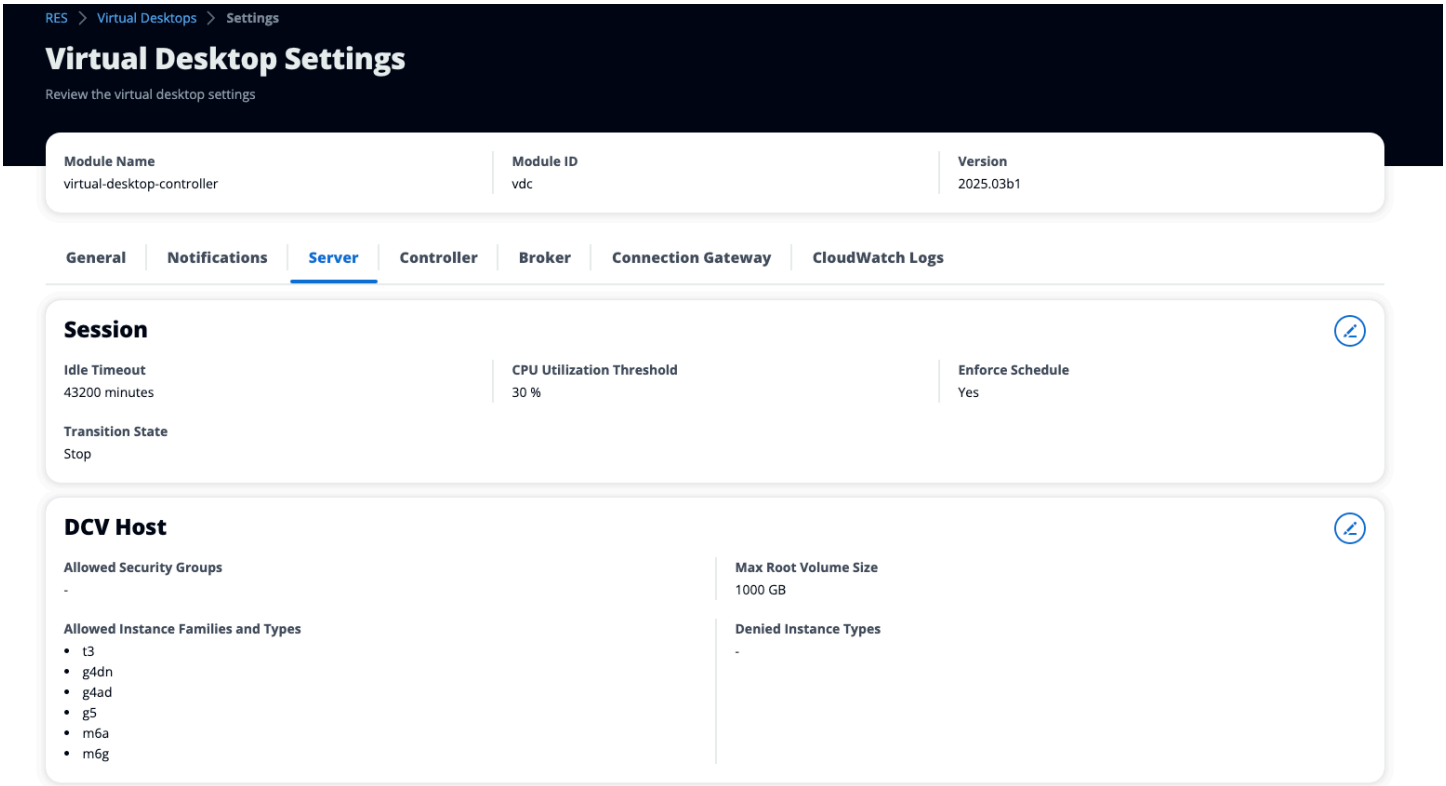
除錯

除錯面板會顯示與虛擬桌面相關聯的訊息流量。您可以使用此面板來觀察主機之間的活動。VD 主機索引標籤會顯示執行個體特定活動，而 VD 工作階段索引標籤會顯示進行中工作階段活動。



桌面設定

您可以使用桌面設定頁面來設定與虛擬桌面相關聯的資源。



一般

一般索引標籤可讓您存取設定，例如：

QUIC

啟用 QUIC 以偏好 TCP 做為所有虛擬桌面的預設串流通訊協定。

預設 DCV 工作階段類型

用於所有虛擬桌面的預設 DCV 工作階段類型。此設定不適用於先前建立的桌面。這僅適用於執行個體類型和作業系統支援虛擬或主控台工作階段類型的情況。

每個專案每個使用者的預設允許工作階段數

每個專案每個使用者允許的 VDI 工作階段數量的預設值。

伺服器

伺服器索引標籤可讓您存取設定，例如：

DCV 工作階段閒置逾時

之後 DCV 工作階段會自動中斷連線的時間。這不會變更桌面工作階段的狀態，只會從 DCV 用戶端或 Web 瀏覽器關閉工作階段。

閒置逾時警告

閒置警告之後會提供給用戶端的時間。

CPU 使用率閾值

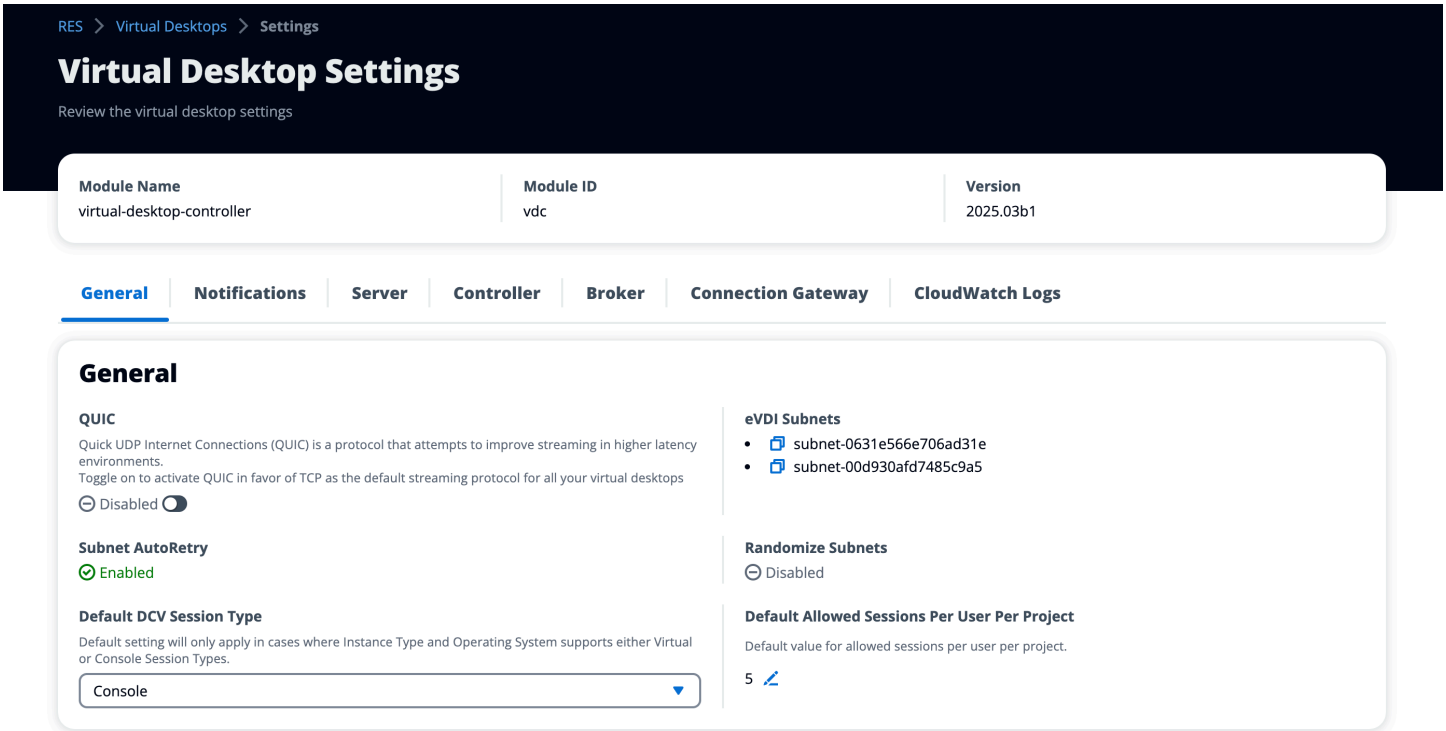
要視為閒置的 CPU 使用率。

根磁碟區大小上限

虛擬桌面工作階段上根磁碟區的預設大小。

允許的執行個體類型

可為此 RES 環境啟動的執行個體系列和大小清單。同時接受執行個體系列和執行個體大小組合。例如，如果您指定 'm7a'，則 m7a 系列的所有大小都可以作為 VDI 工作階段啟動。如果您指定 'm7a.24xlarge'，則只有 m7a.24xlarge 可供做為 VDI 工作階段啟動。此清單會影響環境中的所有專案。



環境管理

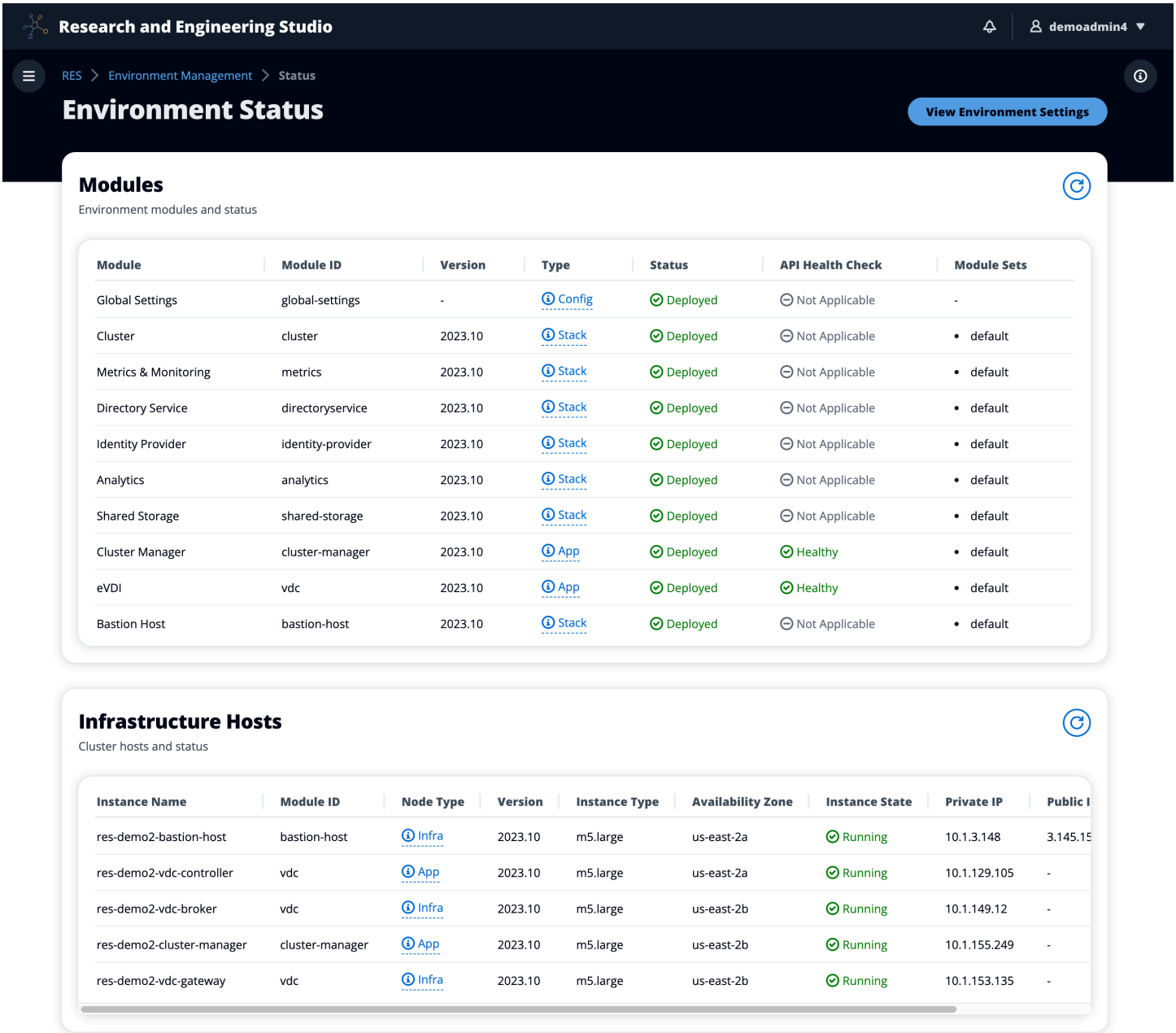
從 Research and Engineering Studio 的環境管理區段中，管理使用者可以為其研究和工程專案建立和管理隔離的環境。這些環境可以包含運算資源、儲存和其他必要的元件，全都在安全的環境中進行。使用者可以設定和自訂這些環境，以滿足其專案的特定需求，從而更輕鬆地實驗、測試和迭代其解決方案，而不會影響其他專案或環境。

主題

- 環境狀態
- 環境設定
- 使用者
- 群組
- 專案
- 許可政策
- 檔案系統
- 快照管理
- Amazon S3 儲存貯體

環境狀態

環境狀態頁面會顯示產品內已部署的軟體和主機。它包含軟體版本、模組名稱和其他系統資訊等資訊。



環境設定

環境設定頁面會顯示產品組態詳細資訊，例如：

- 一般

  顯示佈建產品的使用者的管理員使用者名稱和電子郵件等資訊。您可以編輯 Web 入口網站標題和著作權文字。

- 身分提供者

顯示資訊，例如單一登入狀態。

- 網路

  顯示 VPC ID、用於存取的字首清單 IDs。

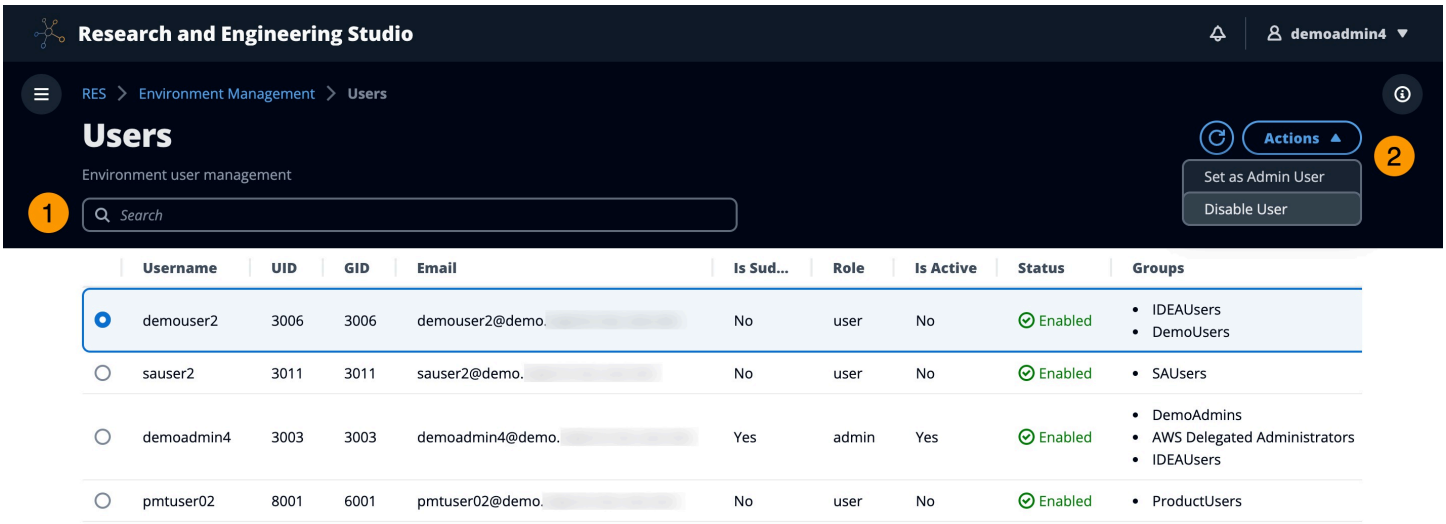
- Directory Service

  顯示使用者名稱和密碼的作用中目錄設定和服務帳戶秘密管理員 ARN。

使用者

從作用中目錄同步的所有使用者都會顯示在使用者頁面上。叢集管理員使用者會在產品組態期間同步使用者。如需初始使用者組態的詳細資訊，請參閱 組態指南。

> **Note**
>
> 管理員只能為作用中使用者建立工作階段。根據預設，所有使用者都會處於非作用中狀態，直到他們登入產品環境為止。如果使用者處於非作用中狀態，請他們先登入，再為其建立工作階段。



在使用者頁面中，您可以：

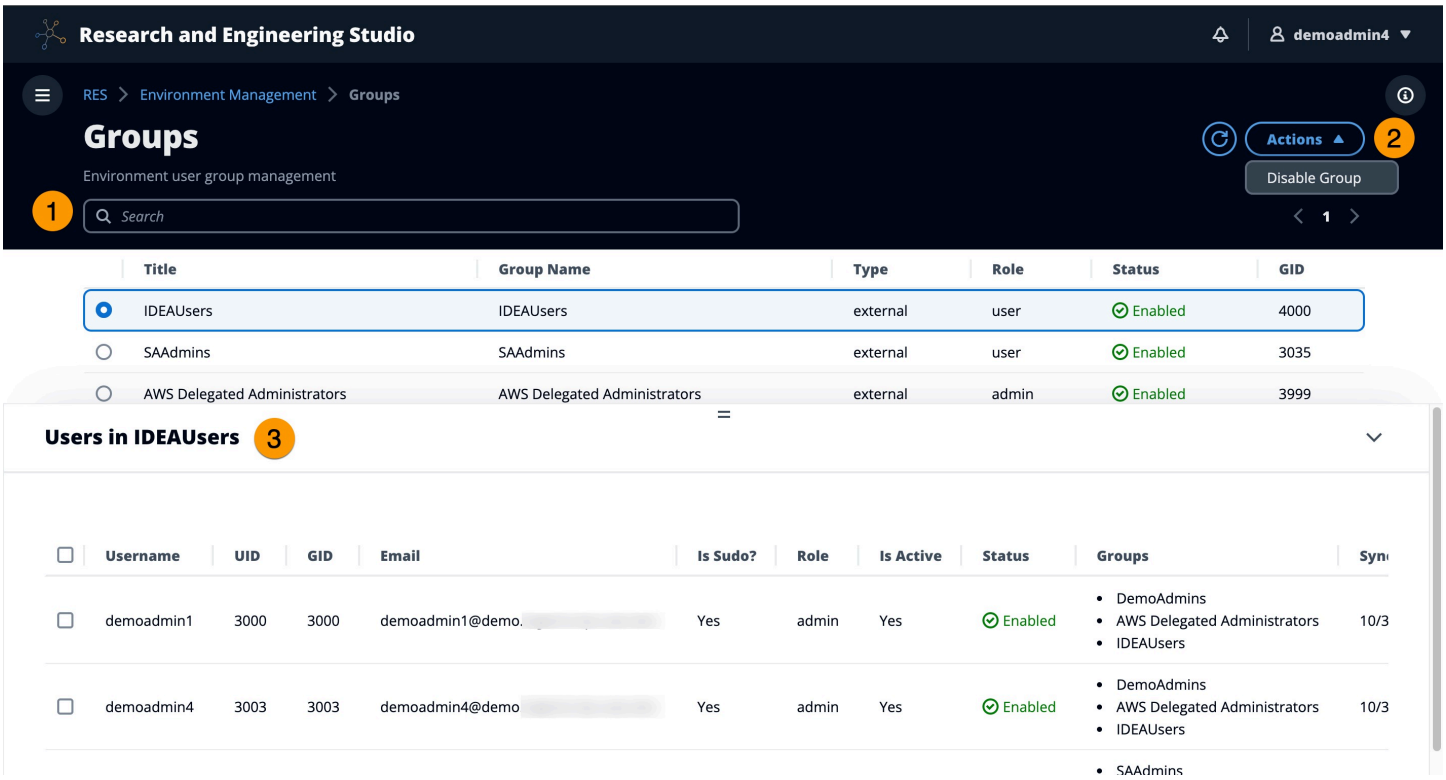
1. 搜尋使用者。
2. 選取使用者名稱時，請使用動作功能表來：

a. 設定為管理員使用者

b. 停用使用者

群組

從作用中目錄同步的所有群組都會出現在群組頁面上。如需群組組態和管理的詳細資訊，請參閱 組態指南。



在群組頁面中，您可以：

1. 搜尋使用者群組。
2. 選取使用者群組時，請使用動作功能表來停用或啟用群組。
3. 選取使用者群組時，您可以展開畫面底部的使用者窗格，以檢視群組中的使用者。

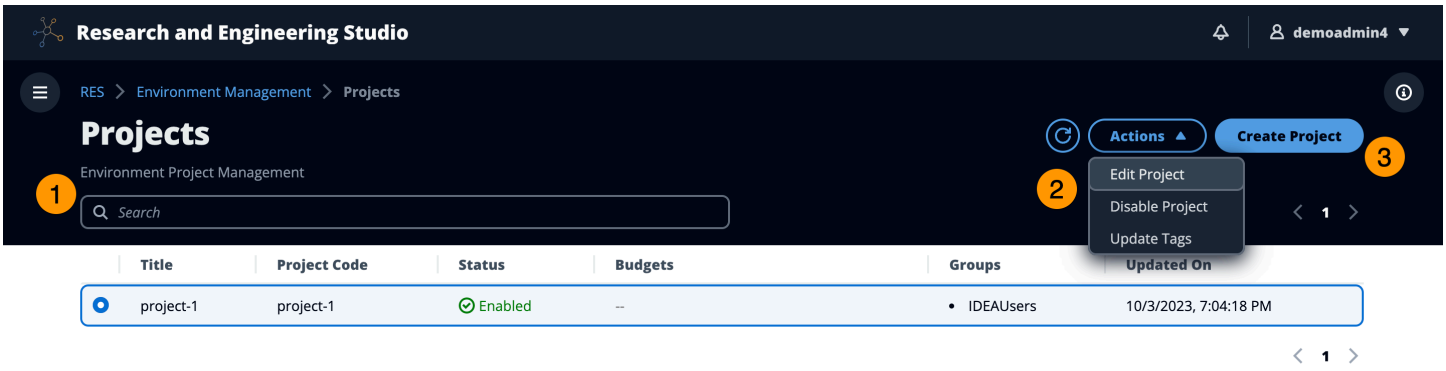
專案

專案形成虛擬桌面、團隊和預算的界限。建立專案時，您可以定義其設定，例如名稱、描述和環境組態。專案通常包含一或多個環境，可自訂以符合專案的特定需求，例如運算資源的類型和大小、軟體堆疊和聯網組態。

主題

- 檢視專案
- 建立專案
- 編輯專案
- 停用專案
- 刪除專案
- 從專案新增或移除標籤
- 檢視與專案相關聯的檔案系統
- 新增啟動範本

檢視專案



專案儀表板提供您可用的專案清單。從專案儀表板，您可以：

1. 您可以使用搜尋欄位來尋找專案。
2. 選取專案時，您可以使用動作功能表來：
   a. 編輯專案
   b. 停用或啟用專案
   c. 更新專案標籤
   d. 刪除專案
3. 您可以選擇建立專案來建立新的專案。

建立專案

1. 選擇建立專案。

2. 輸入專案詳細資訊。

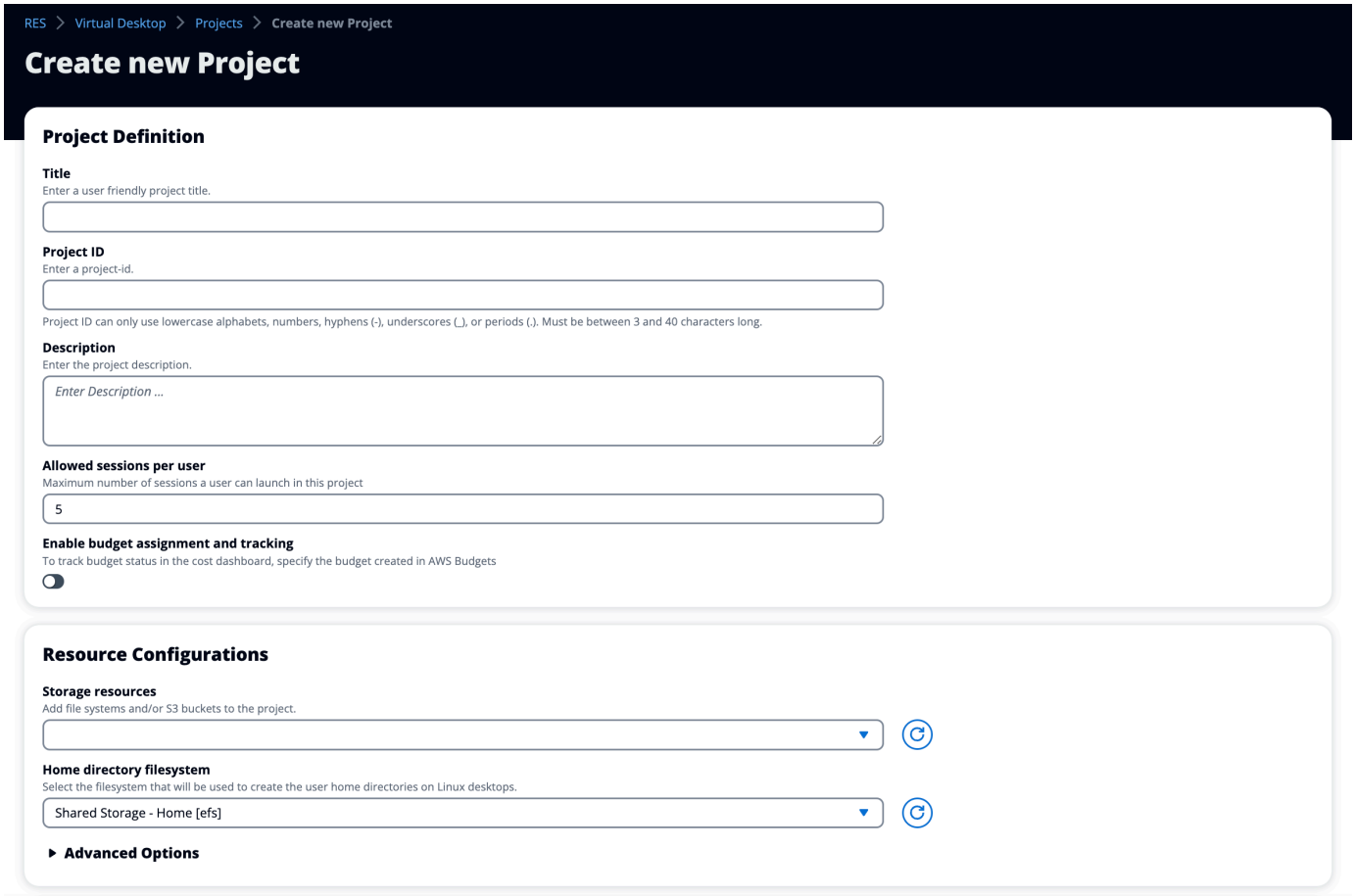
   專案 ID 是可用來追蹤 中成本分配的資源標籤 AWS Cost Explorer Service。如需詳細資訊，請參閱啟用使用者定義的成本分配標籤。

   > **Important**
   >
   > 專案 ID 無法在建立後變更。

   如需進階選項的詳細資訊，請參閱 新增啟動範本。

3. （選用）開啟專案的預算。如需預算的詳細資訊，請參閱 成本監控和控制。
4. 主目錄檔案系統可以使用共用主檔案系統（預設）、EFS、FSx for Lustre、FSx NetApp ONTAP 或 EBS 磁碟區儲存。

   請務必注意，共用的主檔案系統、EFS、FSx for Lustre 和 FSx NetApp ONTAP 可以跨多個專案和 VDIs 共用。不過，EBS 磁碟區儲存選項會要求該專案中的每個 VDI 擁有自己的主目錄，這些目錄不會在其他 VDIs 或專案之間共用。



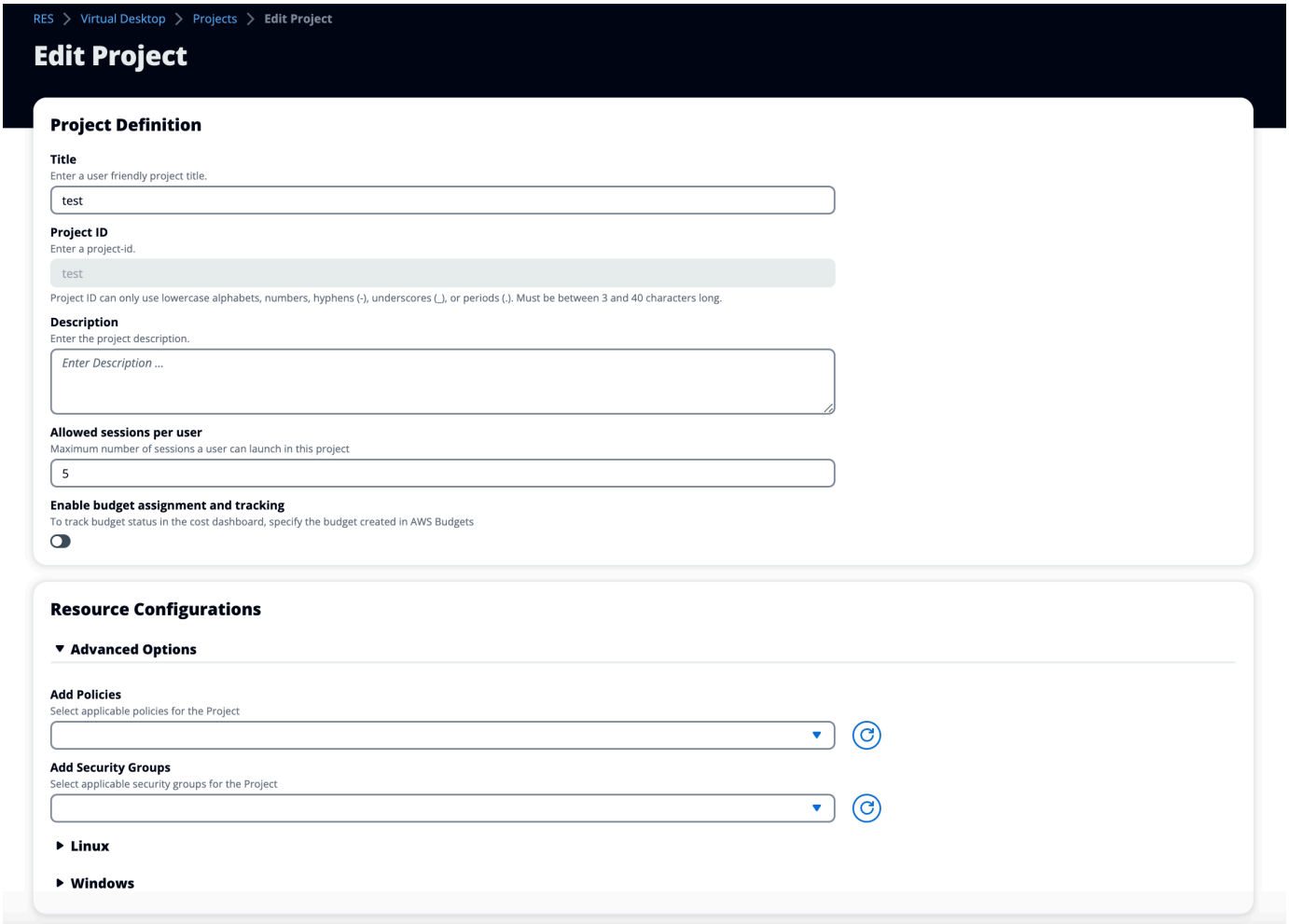
5. 指派使用者和/或群組適當的角色 (「專案成員」或「專案擁有者」)。如需每個角色可以採取的動作預設許可設定檔，請參閱 。
6. 選擇提交。

編輯專案

1. 在專案清單中選取專案。
2. 從動作功能表中，選擇編輯專案。
3. 輸入您的更新。

   如果您想要啟用預算，請參閱 成本監控和控制 以取得詳細資訊。當您選擇專案的預算時，預算下拉式清單選項可能會有幾秒鐘的載入延遲，如果您看不到剛建立的預算，請選取下拉式清單旁的重新整理按鈕。

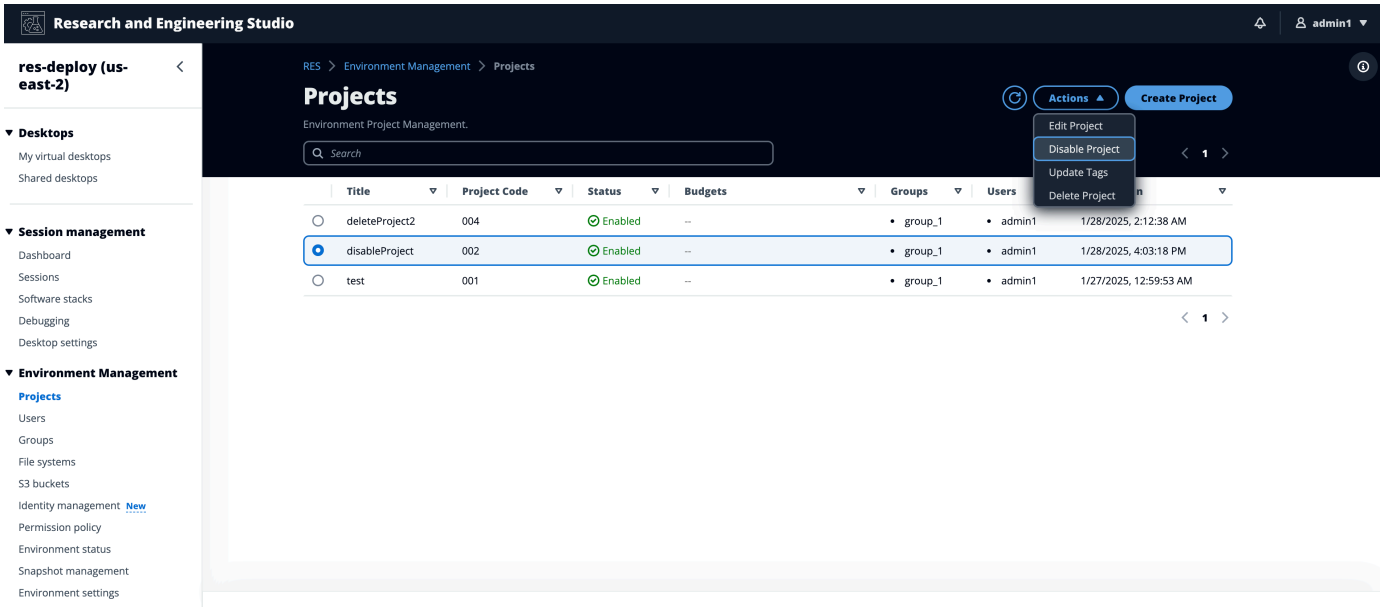
   如需進階選項的詳細資訊，請參閱 新增啟動範本。
4. 選擇提交。



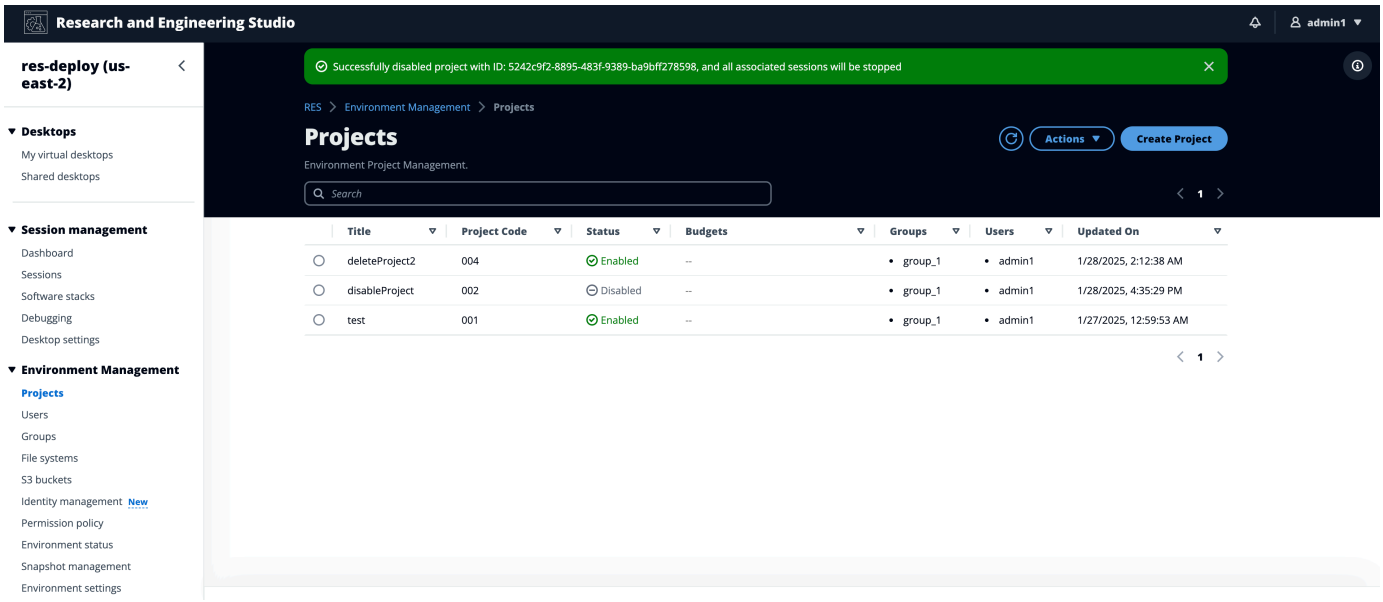
停用專案

若要停用專案：

1. 在專案清單中選取專案。
2. 從動作功能表中，選擇停用專案。



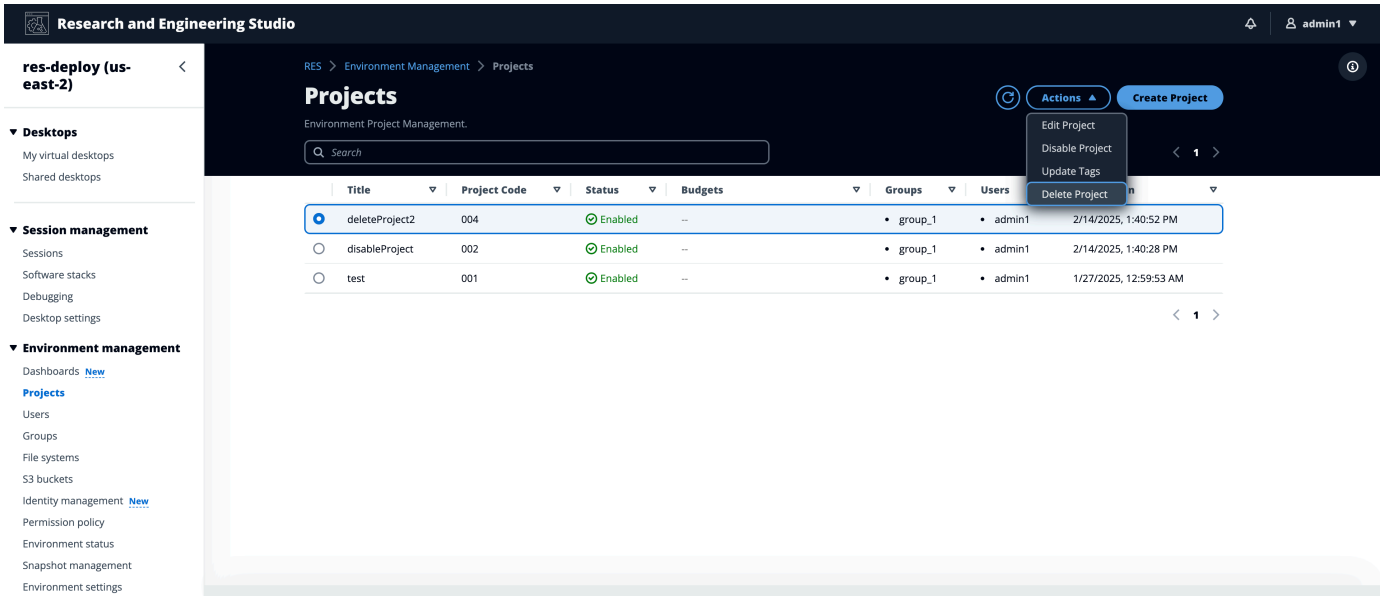
3. 如果專案已停用，與該專案相關聯的所有 VDI 工作階段都會停止。這些工作階段無法在專案停用時重新啟動。



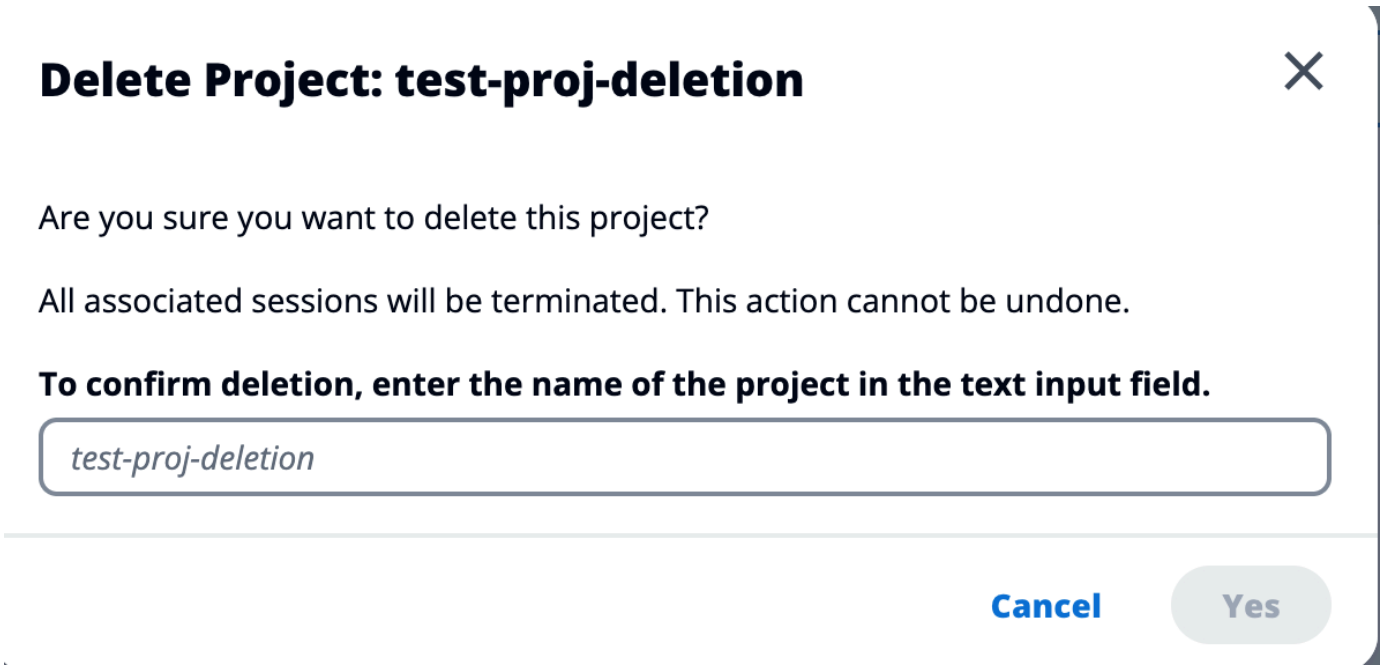
刪除專案

若要刪除專案：

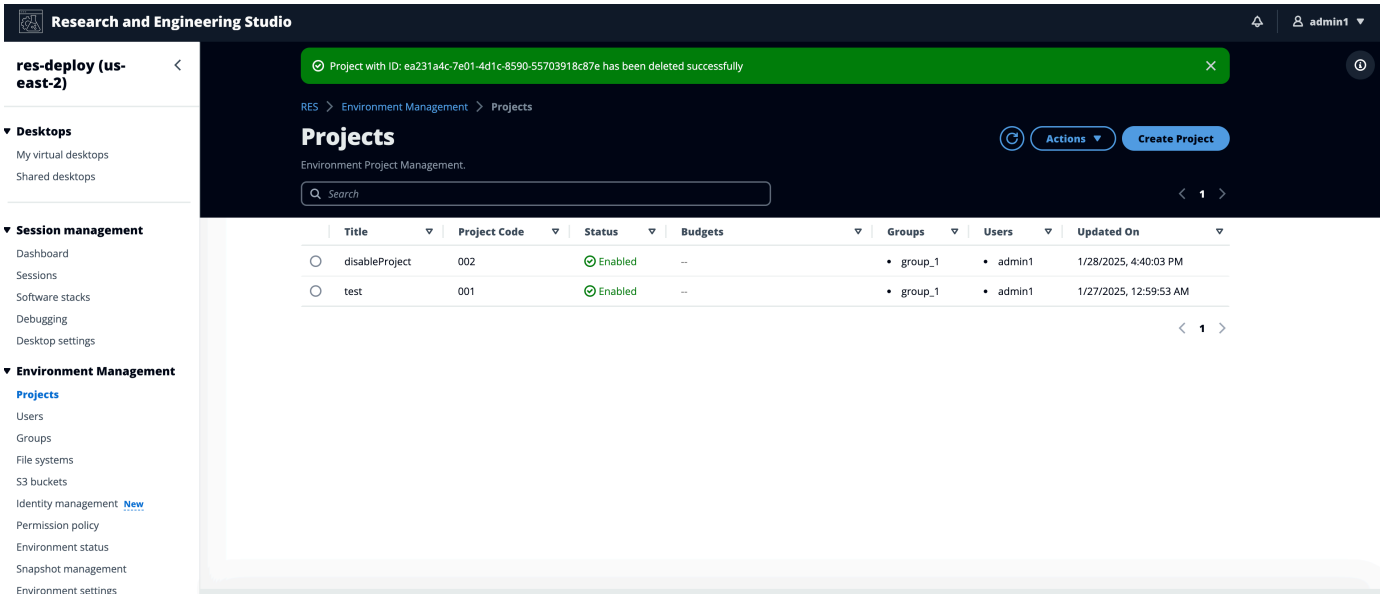
1. 在專案清單中選取專案。
2. 從動作功能表中，選擇刪除專案。



3. 確認快顯視窗隨即出現。輸入專案的名稱，然後選擇是來刪除專案。



4. 如果刪除專案，與該專案相關聯的所有 VDI 工作階段都會終止。



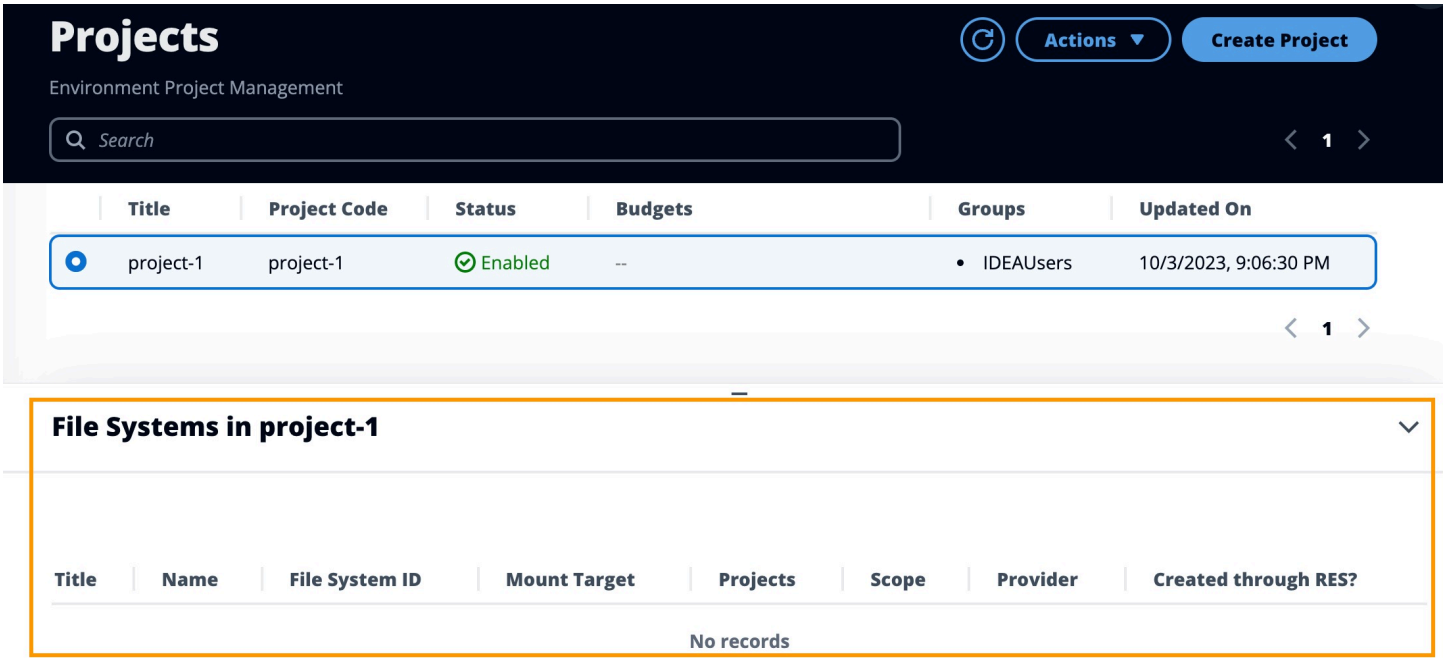
從專案新增或移除標籤

專案標籤會將標籤指派給在該專案下建立的所有執行個體。

1. 在專案清單中選取專案。
2. 從動作功能表中，選擇更新標籤。
3. 選擇新增標籤，然後輸入金鑰的值。
4. 若要移除標籤，請選擇您要移除之標籤旁的移除。

檢視與專案相關聯的檔案系統

選取專案時，您可以展開畫面底部的檔案系統窗格，以檢視與專案相關聯的檔案系統。



新增啟動範本

建立或編輯專案時，您可以使用專案組態中的進階選項來新增啟動範本。啟動範本為專案中的所有 VDI 執行個體提供額外的組態，例如安全群組、IAM 政策和啟動指令碼。

新增政策

您可以新增 IAM 政策來控制專案下部署之所有執行個體的 VDI 存取。若要加入政策，請使用下列鍵值對標記政策：

```
res:Resource/vdi-host-policy
```

如需 IAM 角色的詳細資訊，請參閱 IAM 中的政策和許可。

新增安全群組

您可以新增安全群組來控制專案下所有 VDI 執行個體的輸出和輸入資料。若要加入安全群組，請使用下列鍵值對標記安全群組：

```
res:Resource/vdi-security-group
```

如需安全群組的詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用安全群組控制資源 AWS 的流量。

新增啟動指令碼

您可以新增啟動指令碼，這些指令碼將在專案中的所有 VDI 工作階段上啟動。RES 支援 Linux 和 Windows 的指令碼啟動。對於指令碼啟動，您可以選擇：

VDI 啟動時執行指令碼

此選項會在執行任何 RES 組態或安裝之前，在 VDI 執行個體的開頭啟動指令碼。

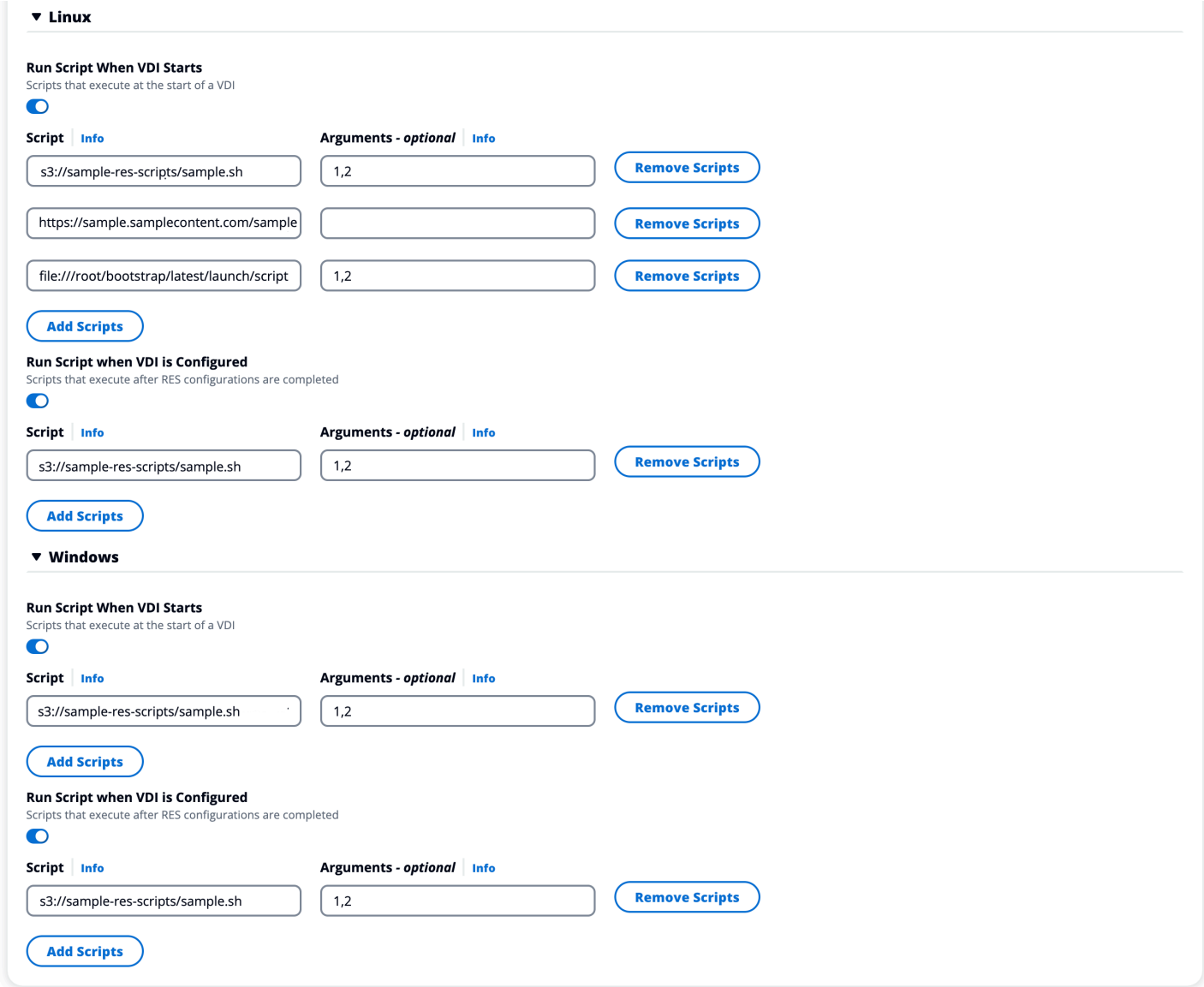
設定 VDI 時執行指令碼

此選項會在 RES 組態完成後啟動指令碼。

指令碼支援下列選項：

指令碼組態	範例
S3 URI	s3：//bucketname/script.sh
HTTPS URL (HTTPS URL)	https://sample.samplecontent.com/sample
本機檔案	file：///user/scripts/example.sh

對於引數，請提供以逗號分隔的任何引數。



專案組態的範例

許可政策

Research and Engineering Studio (RES) 允許管理使用者建立自訂許可設定檔，以授予所選使用者管理其所屬專案的額外許可。每個專案都有兩個預設許可設定檔：「專案成員」和「專案擁有者」，可在部署後自訂。

目前，管理員可以使用許可設定檔授予兩個許可集合：

1. 專案管理許可包含「更新專案成員資格」，可讓指定的使用者將其他使用者和群組新增至專案，或從中移除，以及「更新專案狀態」，以允許指定的使用者啟用或停用專案。

2. VDI 工作階段管理許可包含「建立工作階段」，允許指定的使用者在其專案中建立 VDI 工作階段，以及「建立/終止另一個使用者的工作階段」，允許指定的使用者建立或終止專案中其他使用者的工作階段。

透過這種方式，管理員可以將專案型許可委派給其環境中的非管理員。

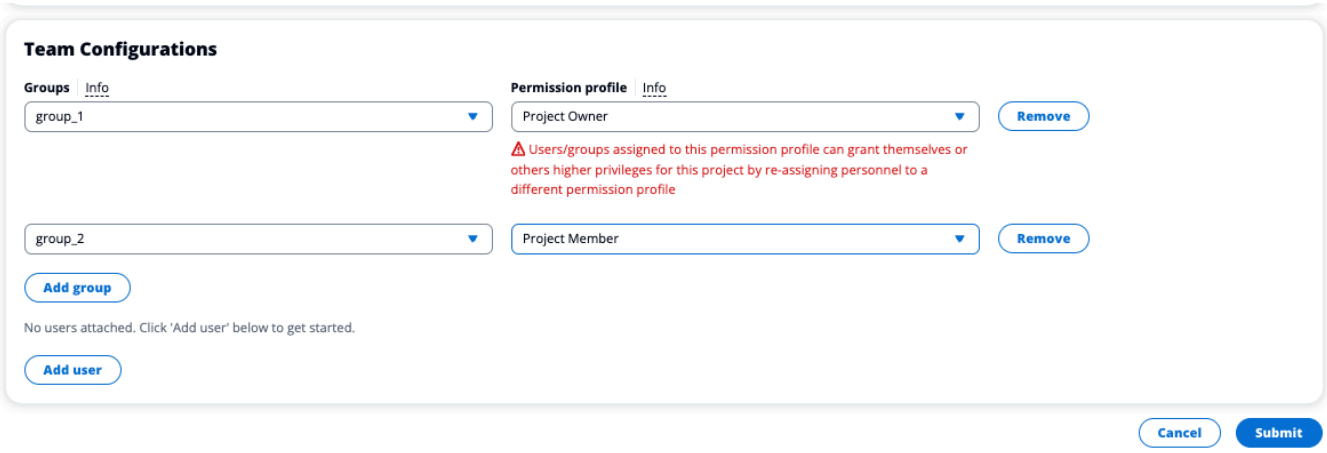
主題

- 專案管理許可
- VDI 工作階段管理許可
- 管理許可設定檔
- 預設許可設定檔
- 環境界限
- 桌面共用設定檔

專案管理許可

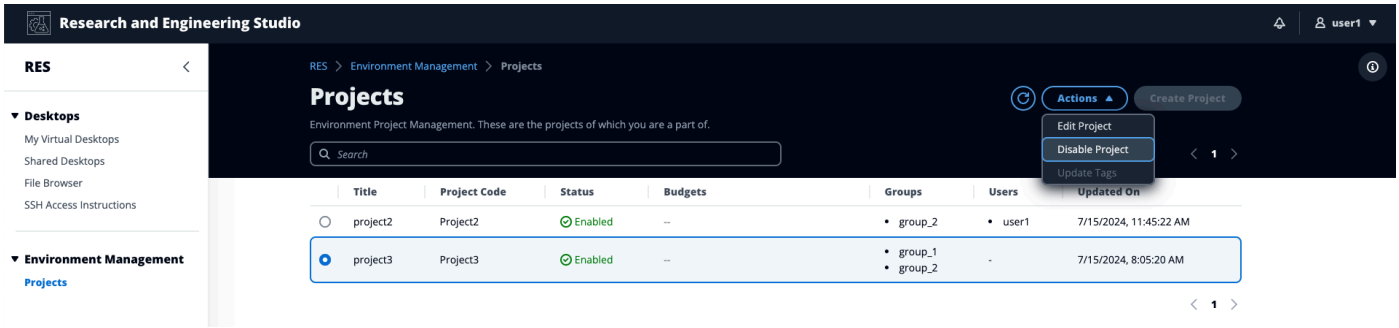
更新專案成員資格

此許可允許獲得授予的非管理員使用者從專案中新增和移除使用者或群組。它還允許他們設定許可設定檔，並決定該專案所有其他使用者和群組的存取層級。



更新專案狀態

此許可允許獲得授予的非管理員使用者使用專案頁面上的動作按鈕啟用或停用專案。

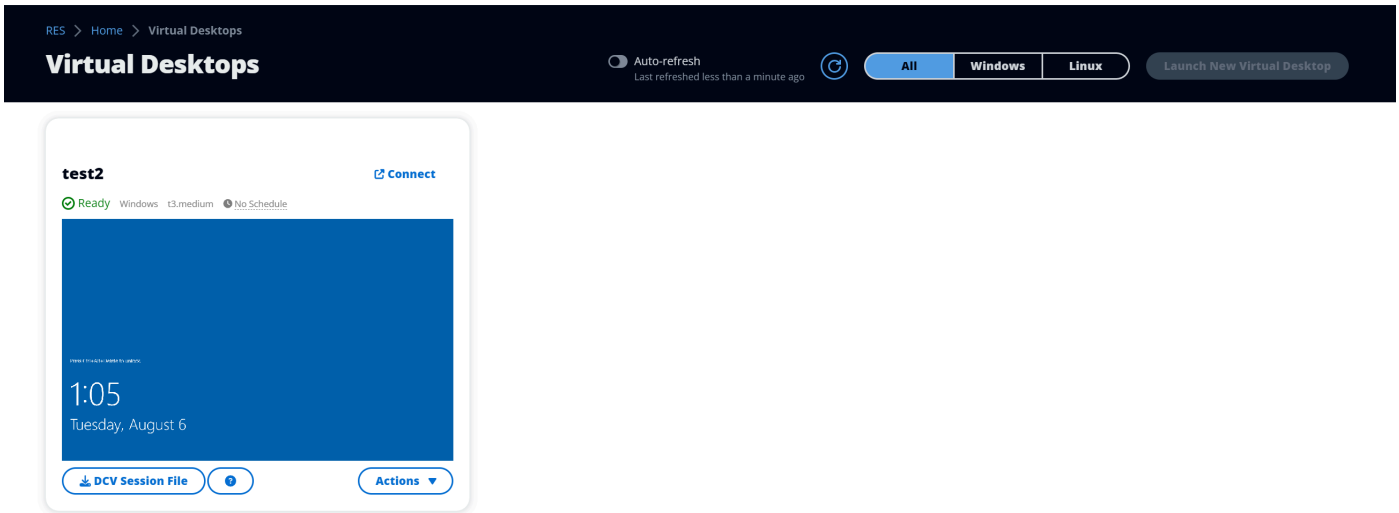


VDI 工作階段管理許可

建立工作階段

控制是否允許使用者從我的虛擬桌面頁面啟動自己的 VDI 工作階段。停用此選項可拒絕非管理員使用者啟動自己的 VDI 工作階段。使用者一律可以停止和終止自己的 VDI 工作階段。

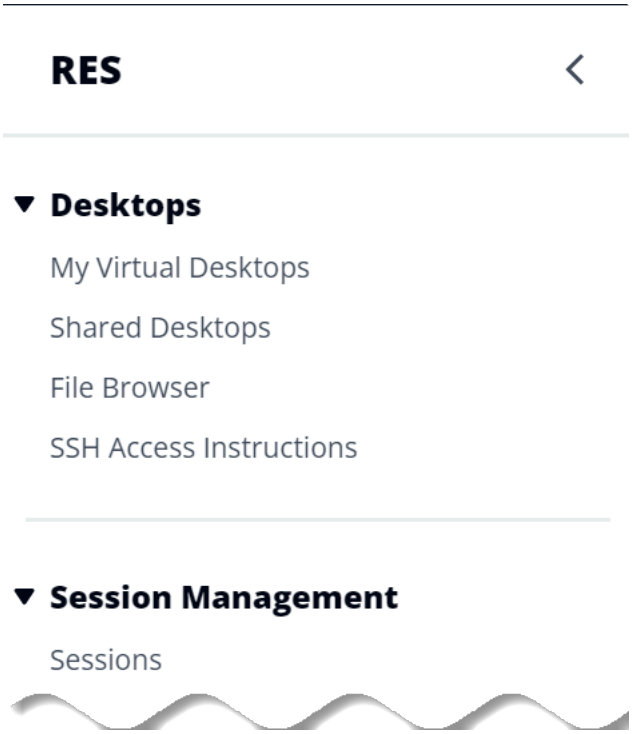
如果非管理員使用者沒有建立工作階段的許可，則會為他們停用啟動新的虛擬桌面按鈕，如下所示：



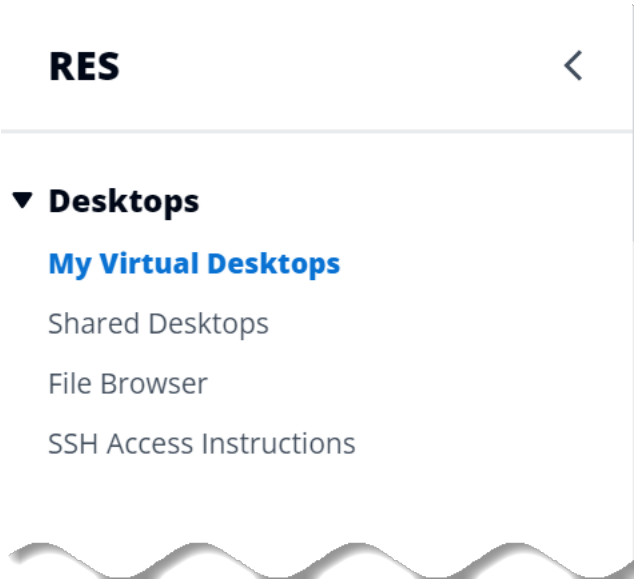
建立或終止其他人的工作階段

允許非管理員使用者從左側導覽窗格存取工作階段頁面。這些使用者將能夠在獲得此許可的專案中為其他使用者啟動 VDI 工作階段。

如果非管理員使用者具有為其他使用者啟動工作階段的許可，其左側導覽窗格將顯示工作階段管理下的工作階段連結，如下所示：



如果非管理員使用者沒有為其他人建立工作階段的許可，其左側導覽窗格將不會顯示工作階段管理，如下所示：

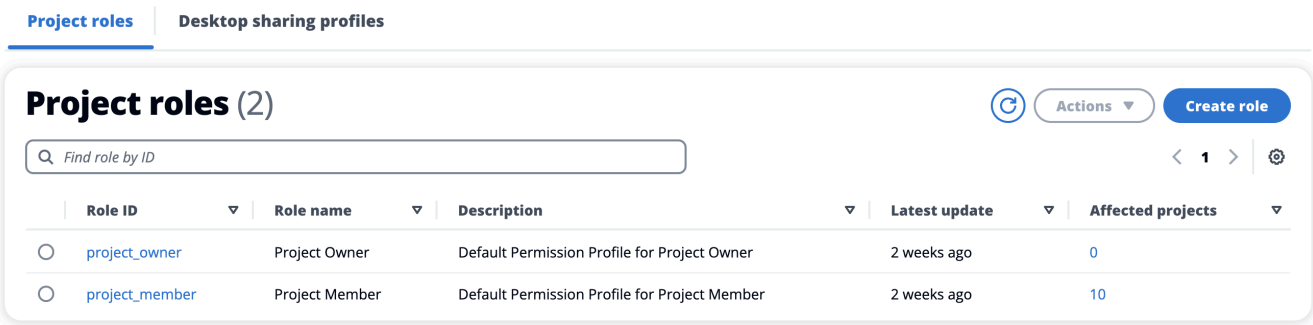


管理許可設定檔

身為 RES 管理員，您可以執行下列動作來管理許可設定檔。

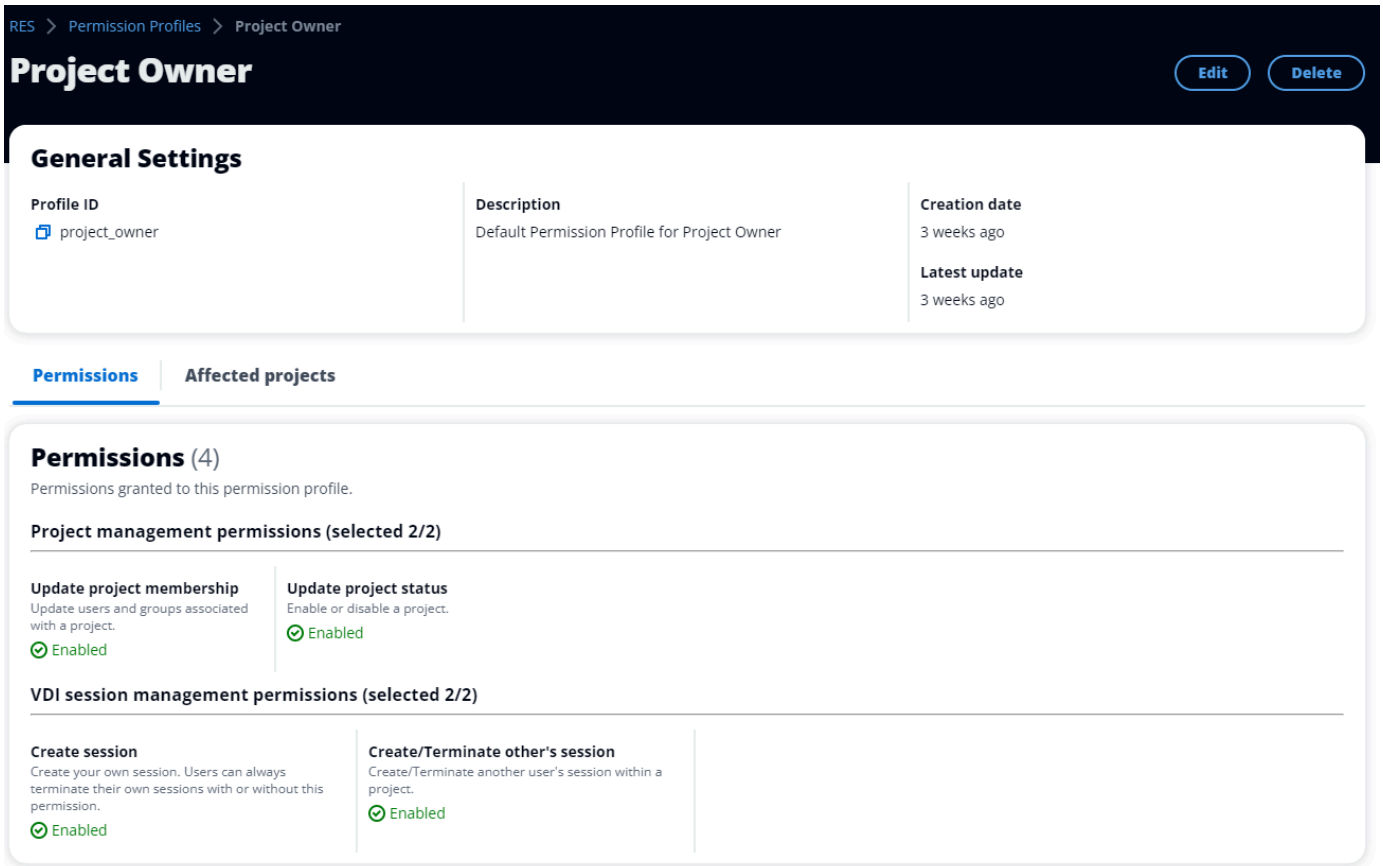
列出許可設定檔

- 從研究和工程 Studio 主控台頁面，選擇左側導覽窗格中的許可政策。在此頁面上，您可以建立、更新、列出、檢視和刪除許可設定檔。

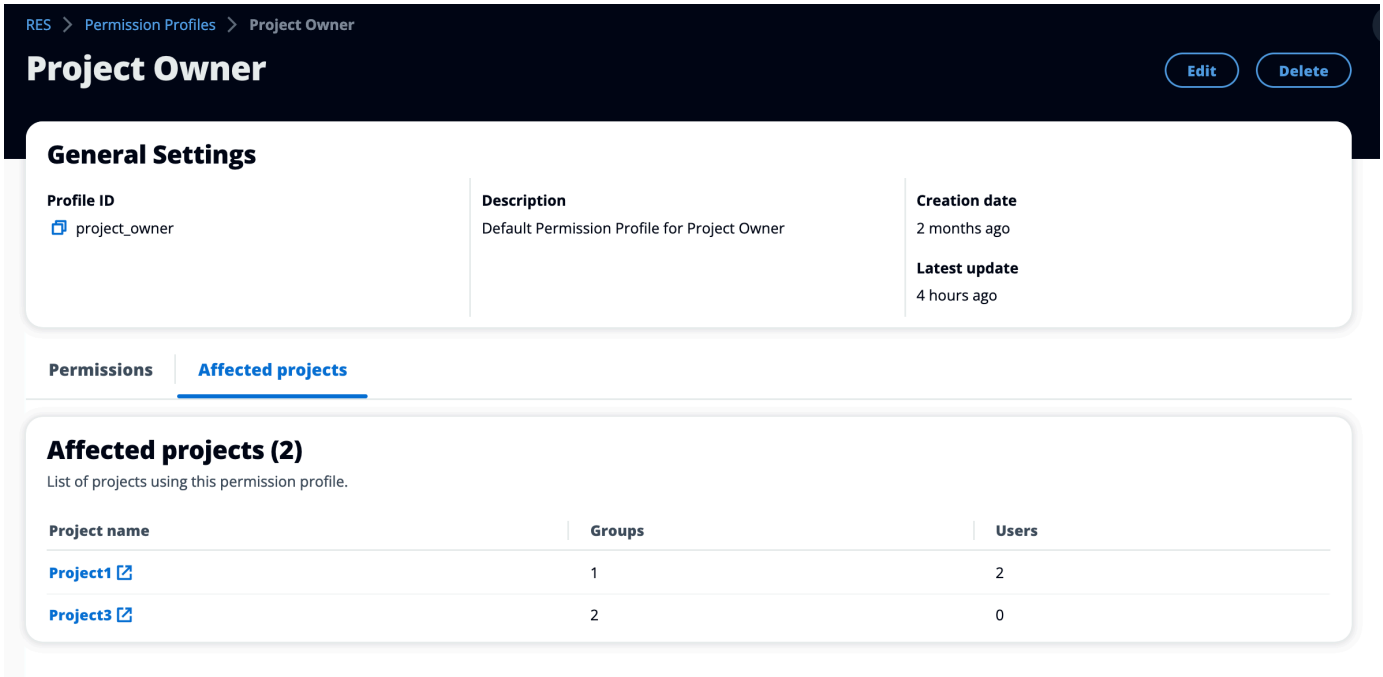


檢視許可設定檔

1. 在主要許可設定檔頁面上，選取您要檢視的許可設定檔名稱。在此頁面上，您可以編輯或刪除選取的許可設定檔。

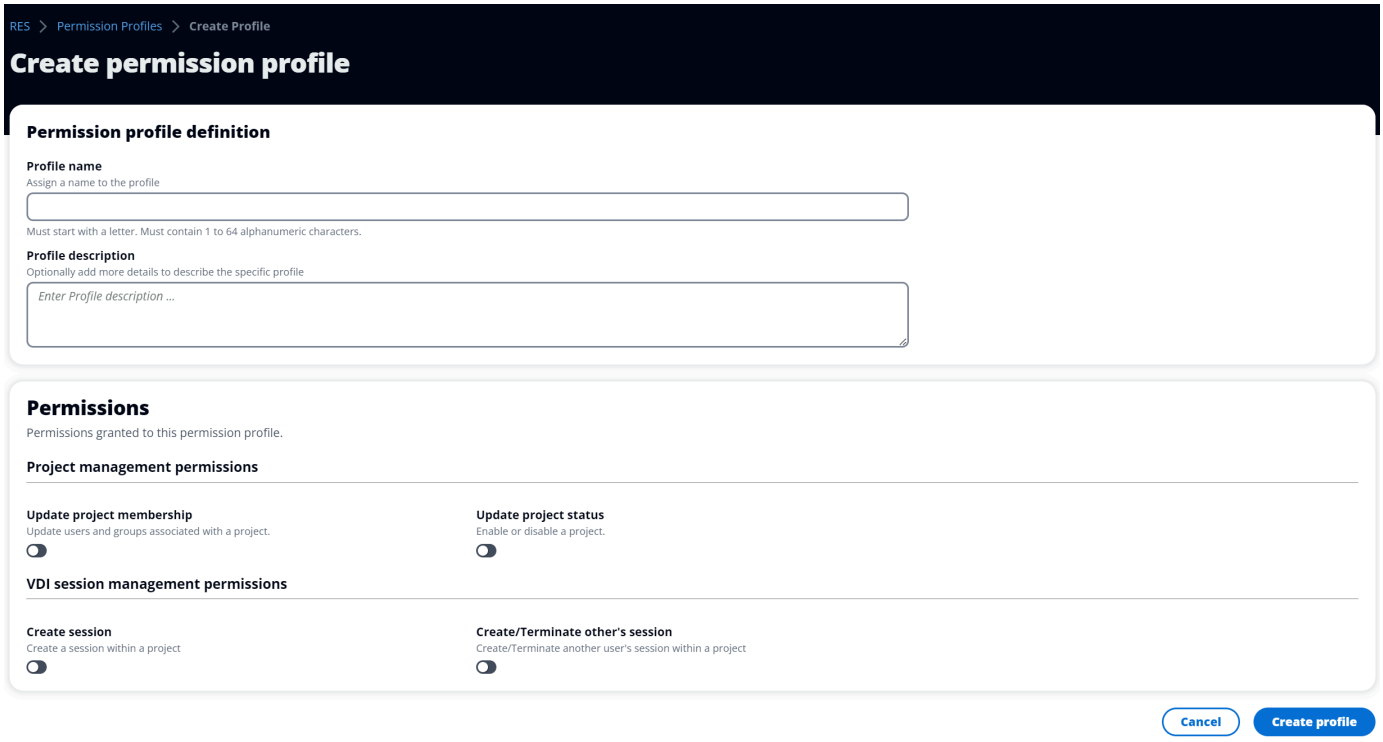


2. 選取受影響的專案索引標籤，以檢視目前使用許可設定檔的專案。



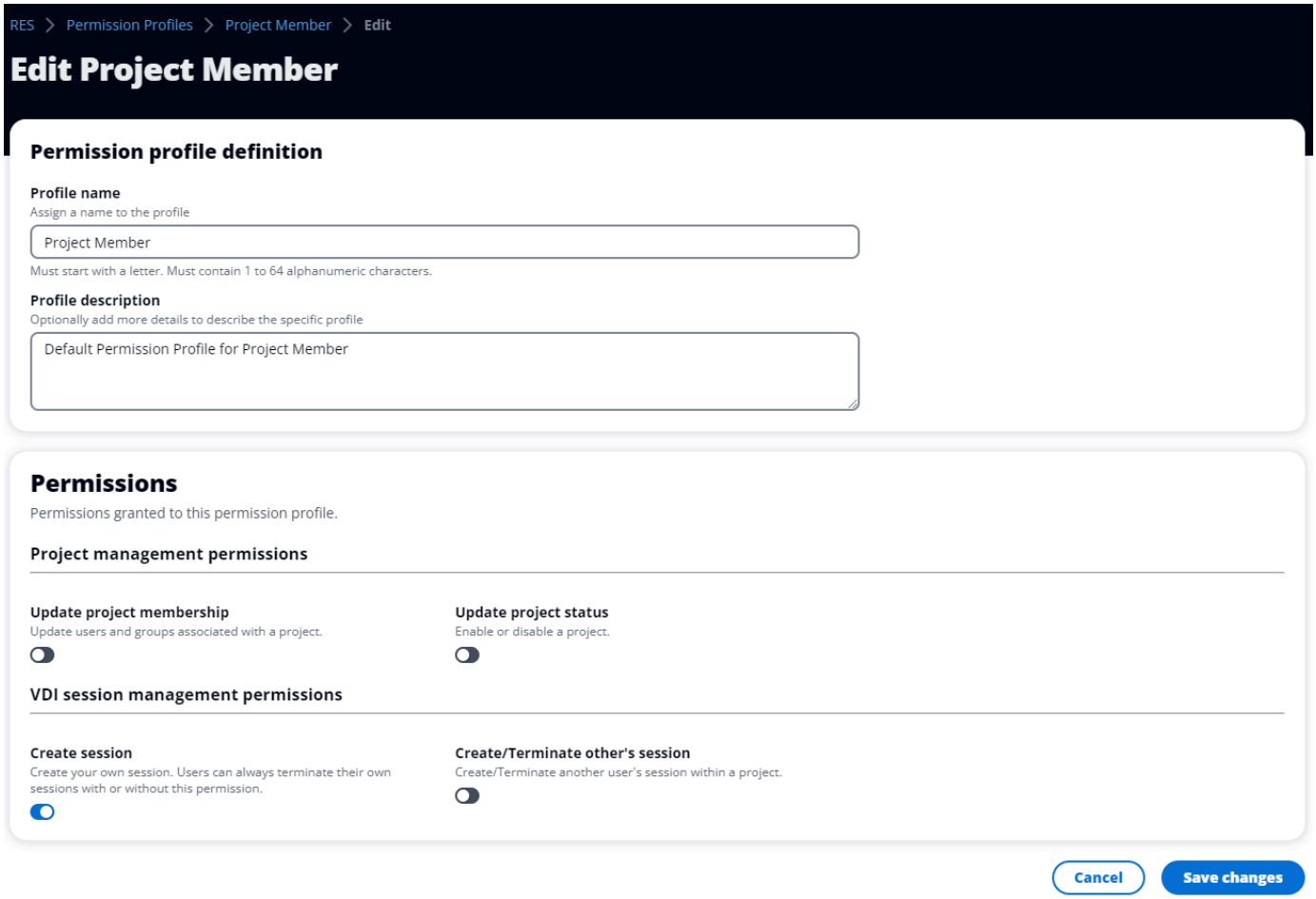
建立許可設定檔

1. 在主要許可設定檔頁面上，選擇建立設定檔以建立許可設定檔。
2. 輸入許可設定檔名稱和描述，然後選取要授予您指派給此設定檔之使用者或群組的許可。



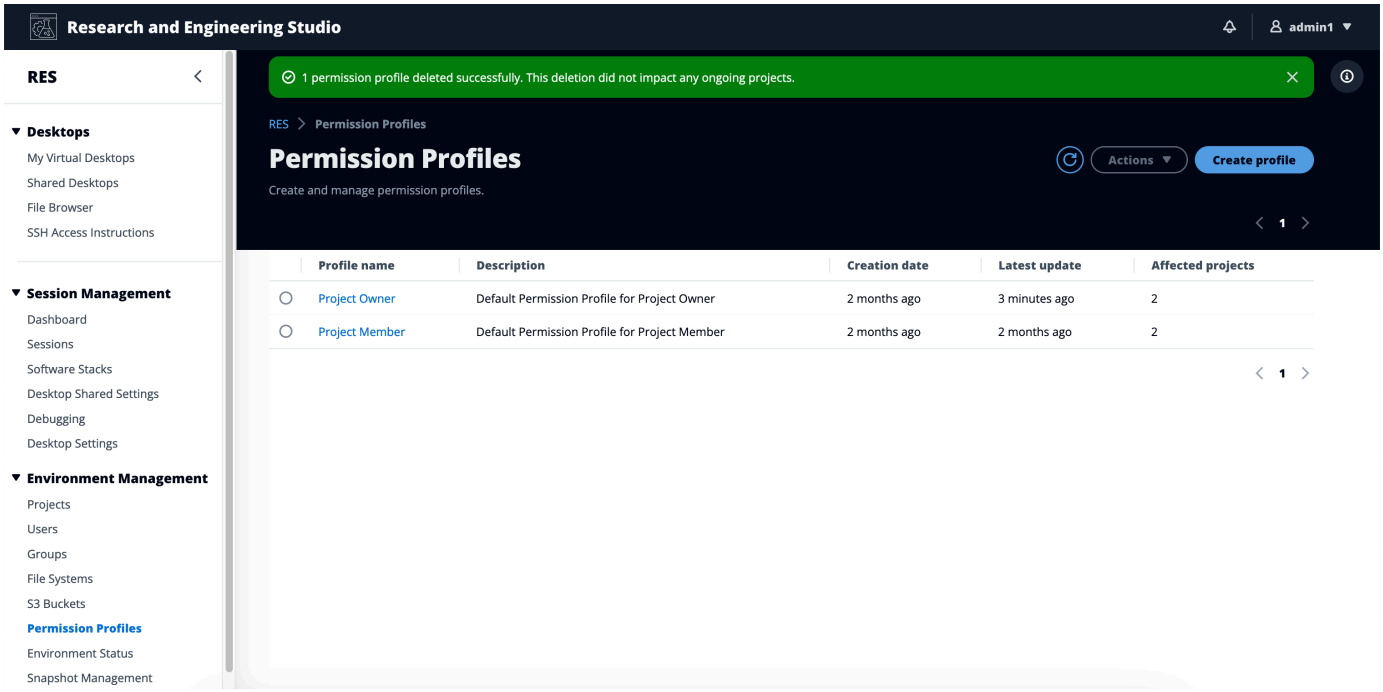
編輯許可設定檔

- 在主要許可設定檔頁面上，按一下其旁邊的圓圈來選取設定檔，選擇動作，然後選擇編輯設定檔以更新該許可設定檔。



刪除許可設定檔

- 在主要許可設定檔頁面上，按一下其旁邊的圓圈來選取設定檔，選擇動作，然後選擇刪除設定檔。您無法刪除任何現有專案所使用的許可設定檔。



預設許可設定檔

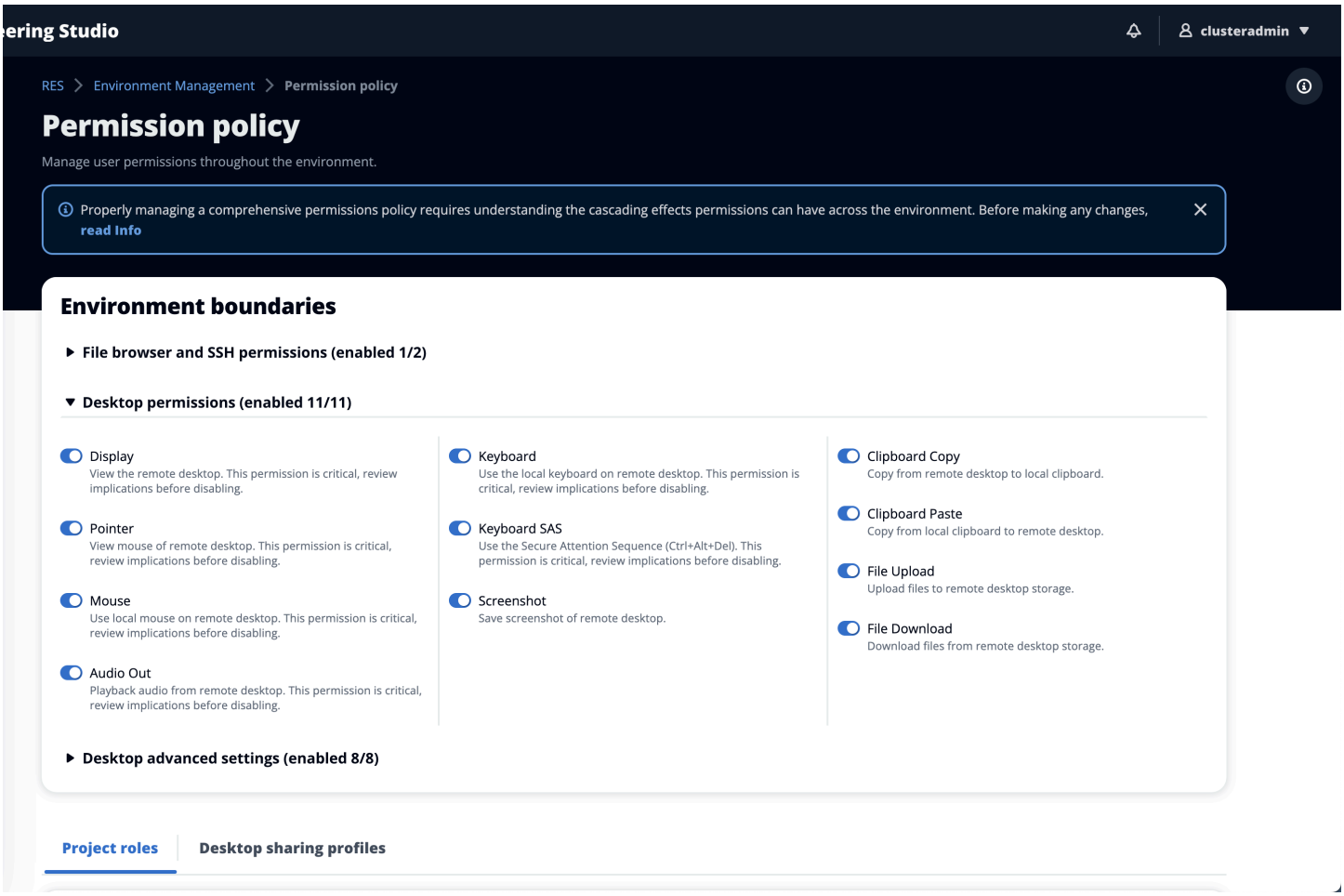
每個 RES 專案都隨附兩個預設許可設定檔，可供全球管理員設定。（此外，全域管理員可以建立和修改專案的新許可設定檔。）下表顯示預設許可設定檔的允許許可：「專案成員」和「專案擁有者」。許可設定檔及其授予選取專案使用者的許可，僅適用於其所屬的專案；全球管理員是跨所有專案擁有以下所有許可的超級使用者。

許可	描述	專案成員	專案擁有者	
建立工作階段	建立您自己的工作階段。使用者一律可以使用或不使用此許可來停止和終止自己的工作階段。	X	X	
建立/終止其他人的工作階段	在專案中建立或終止其他使用者的工作階段。		X	

許可	描述	專案成員	專案擁有者	
更新專案成員資格	更新與專案相關聯的使用者和群組。		X	
更新專案狀態	啟用或停用專案。		X	

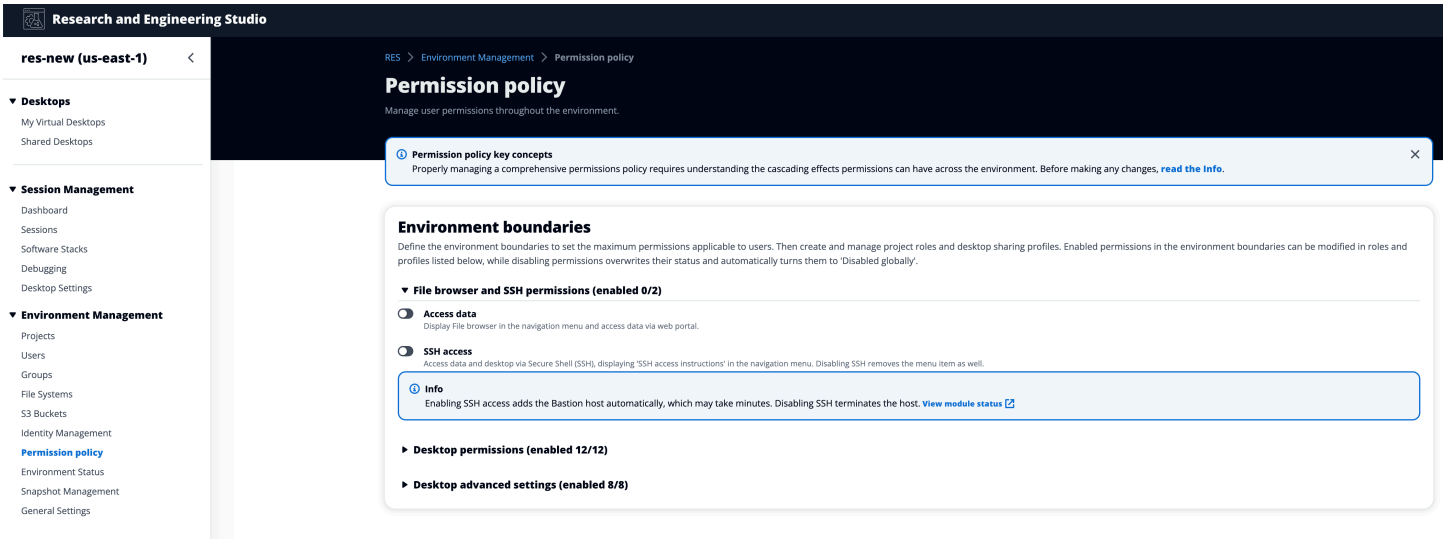
環境界限

環境界限可讓 Research and Engineering Studio (RES) 管理員設定全域對所有使用者生效的許可。這包括檔案瀏覽器和 SSH 許可、桌面許可和桌面進階設定等許可。



設定檔案瀏覽器存取

RES 管理員可以在檔案瀏覽器許可下開啟或關閉存取資料。如果關閉存取資料，使用者將無法在其 Web 入口網站中看到檔案瀏覽器導覽，也無法上傳或下載連接至其全域檔案系統的資料。啟用存取資料時，使用者可以在其 Web 入口網站中存取檔案瀏覽器導覽，以允許他們上傳或下載連接到其全域檔案系統的資料。



開啟存取資料功能並稍後關閉時，已登入 Web 入口網站的使用者將無法上傳或下載檔案，即使他們位於對應的頁面上。此外，導覽功能表會在重新整理頁面時消失。

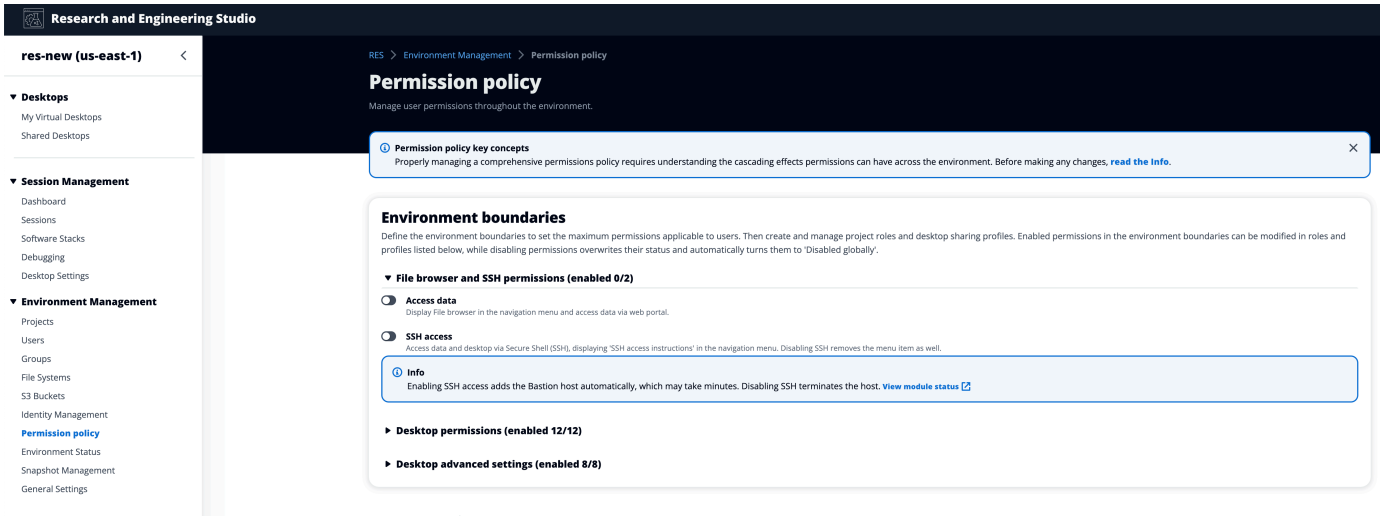
設定 SSH 存取

管理員可以從環境邊界區段啟用或停用 RES 環境的 SSH。SSH 存取 VDIs 是透過堡壘主機來促進。當您啟用此切換時，RES 會部署堡壘主機，並讓使用者可以看到 SSH 存取指示頁面。當您停用切換時，RES 會停用 SSH 存取、終止堡壘主機，並移除使用者的 SSH 存取指示頁面。此切換預設為停用。

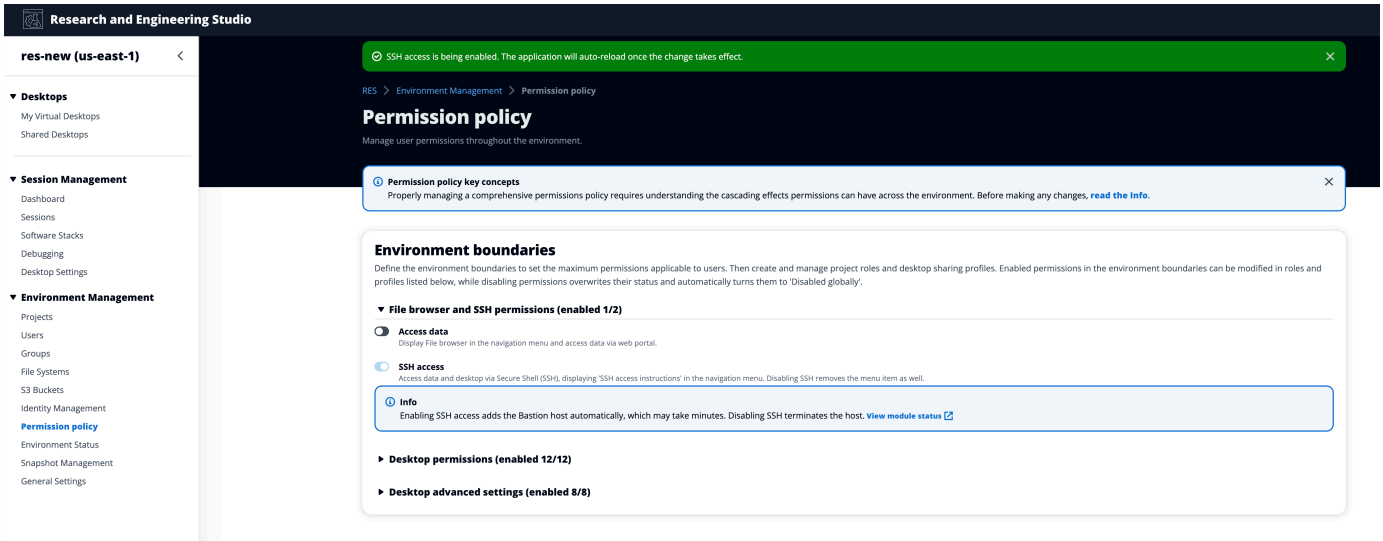
> **Note**
>
> 當 RES 部署堡壘主機時，會在您的帳戶中新增 `t3.medium` Amazon EC2 執行個體 AWS 。您需負責支付與此執行個體相關的所有費用。如需詳細資訊，請參閱 Amazon EC2 定價頁面。

啟用 SSH 存取

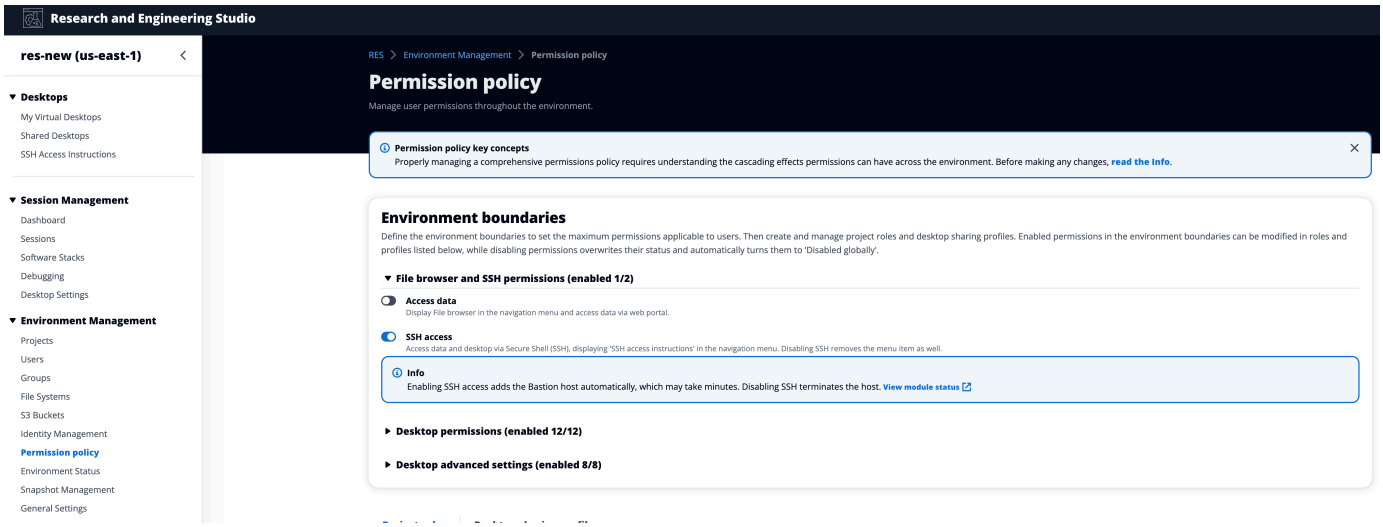
1. 在 RES 主控台的左側導覽窗格中，選擇環境管理，然後選擇許可政策。在環境邊界下，選取 SSH 存取切換。



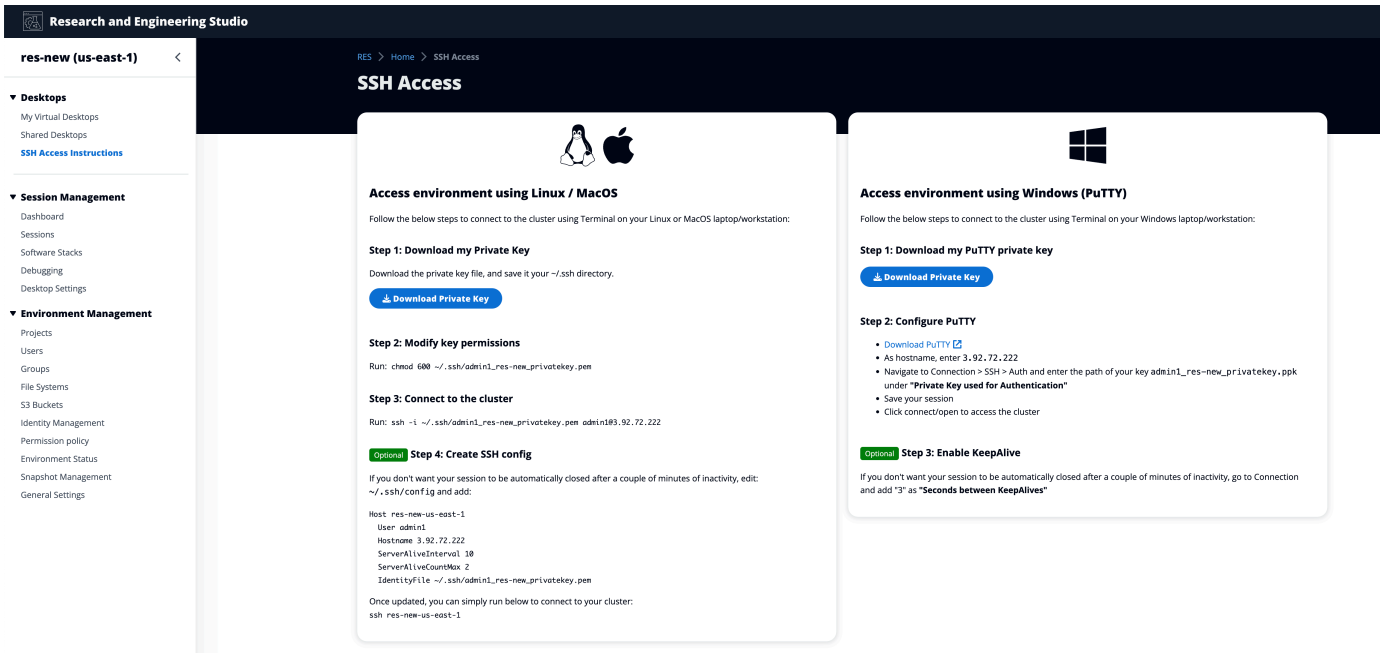
2. 等待啟用 SSH 存取。



3. 新增堡壘主機後，即會啟用 SSH 存取。

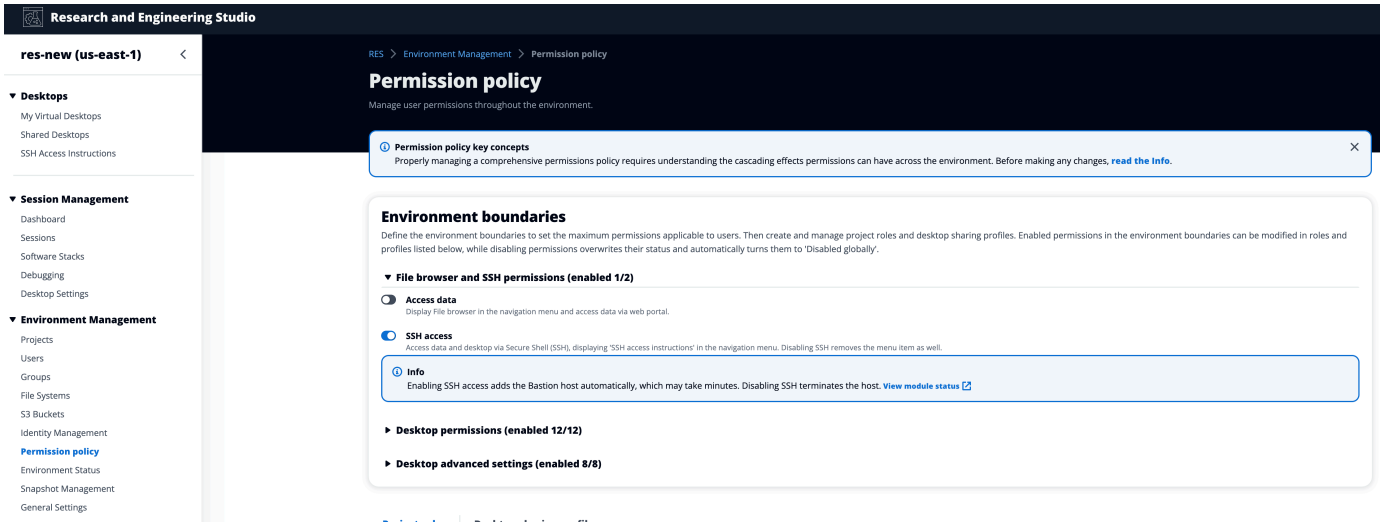


使用者可從左側導覽窗格看到 SSH 存取指示頁面。

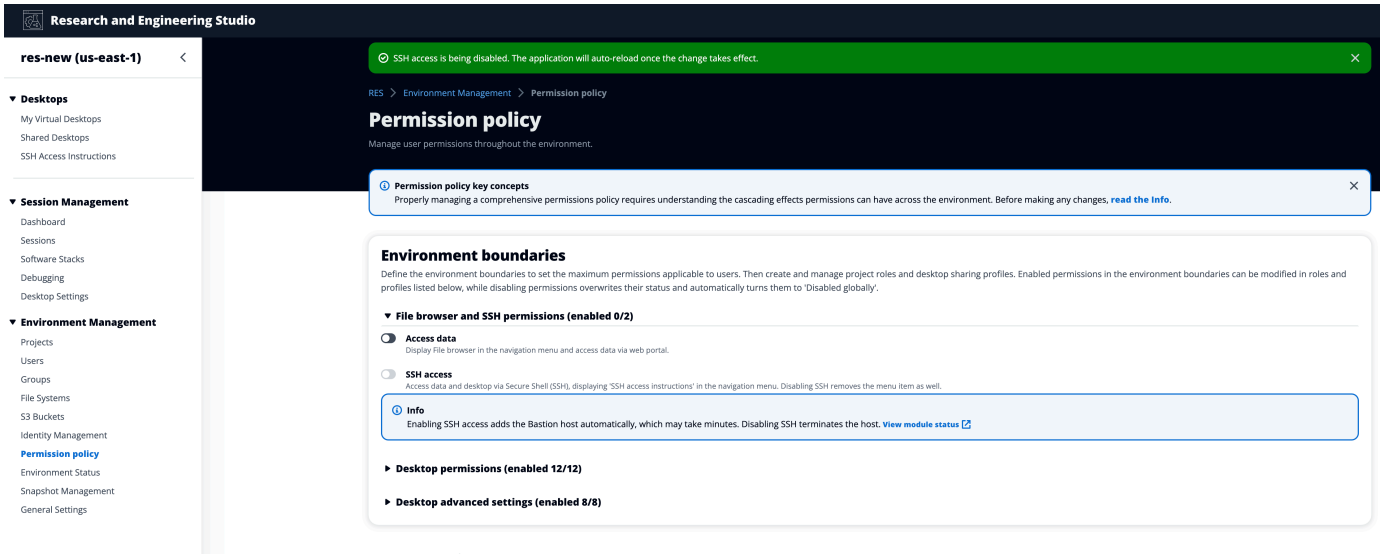


停用 SSH 存取

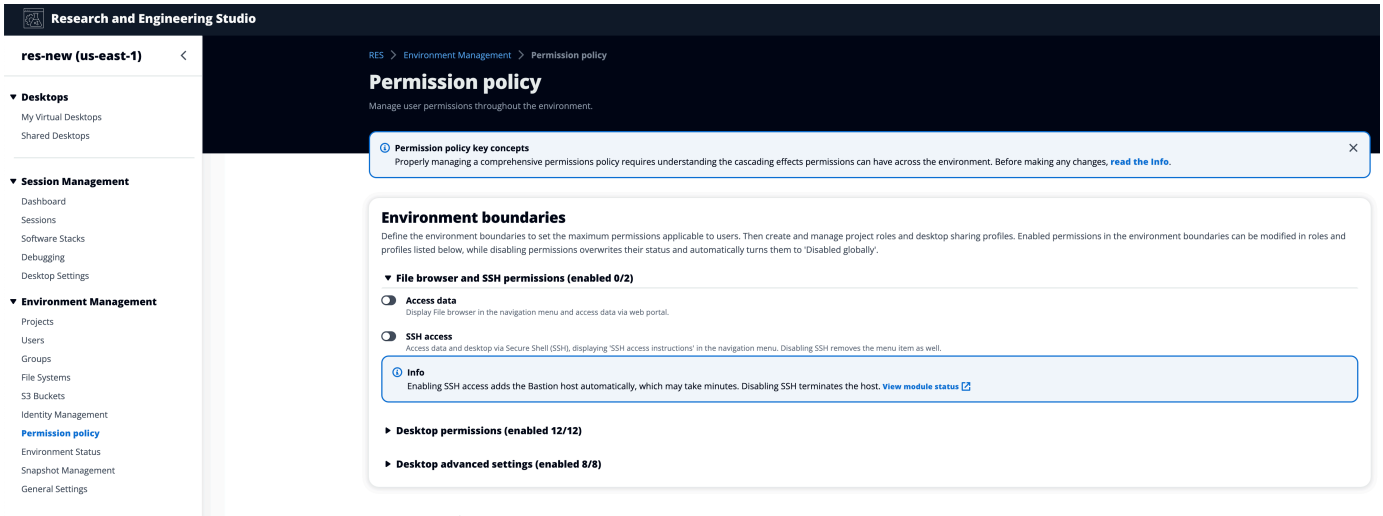
1. 在 RES 主控台的左側導覽窗格中，選擇環境管理，然後選擇許可政策。在環境邊界下，選取 SSH 存取切換。



2. 等待停用 SSH 存取。

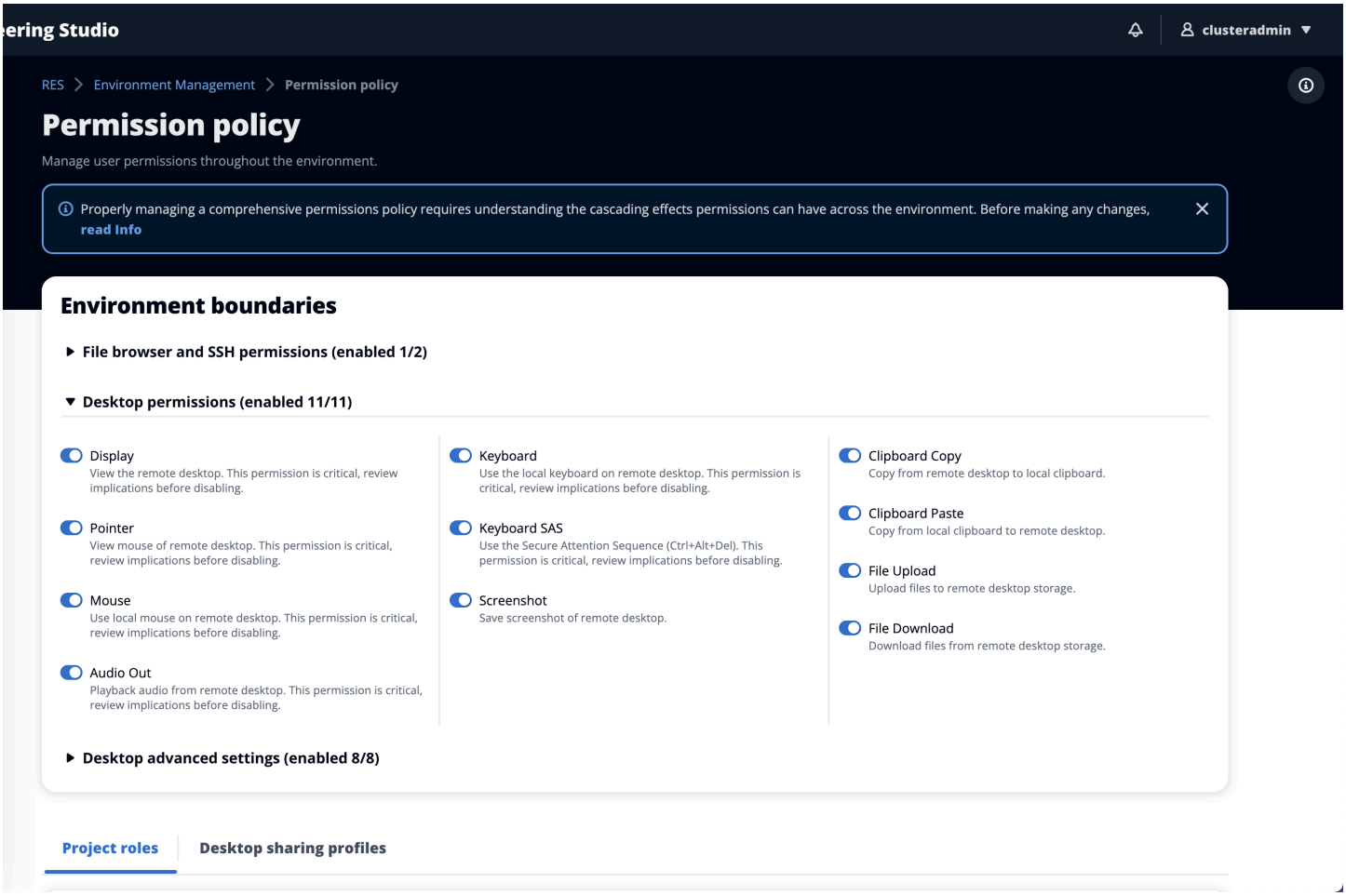


3. 程序完成後，會停用 SSH 存取。



設定桌面許可

管理員可以開啟或關閉桌面許可，以全域管理所有工作階段擁有者的 VDI 功能。所有這些許可或子集都可用來建立桌面共用設定檔，以決定與桌面共用的使用者可執行哪些動作。如果停用任何桌面許可，這會自動停用桌面共用設定檔中的對應許可。這些許可會標記為「全域停用」。即使管理員再次啟用此桌面許可，桌面共用設定檔中的許可仍會保持停用狀態，直到管理員手動啟用為止。

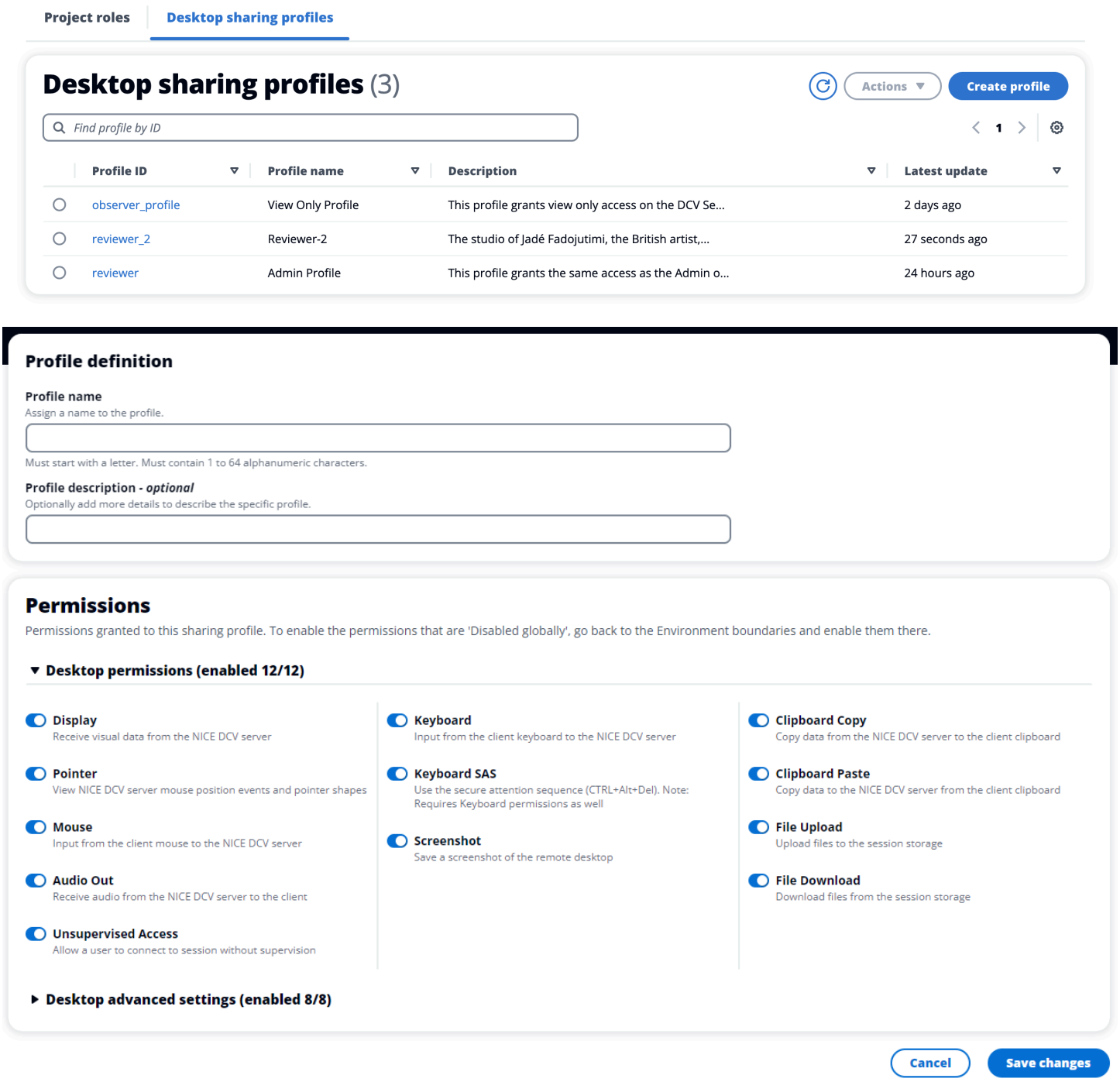


桌面共用設定檔

管理員可以建立新的設定檔並自訂它們。所有使用者都可以存取這些設定檔，並在與他人共用工作階段時使用。這些設定檔中授予的最大許可不能超過全域允許的桌面許可。

建立設定檔

管理員可以選擇建立設定檔來建立新的設定檔。然後，他們可以輸入設定檔名稱、設定檔描述、設定所需的許可，以及儲存其變更。



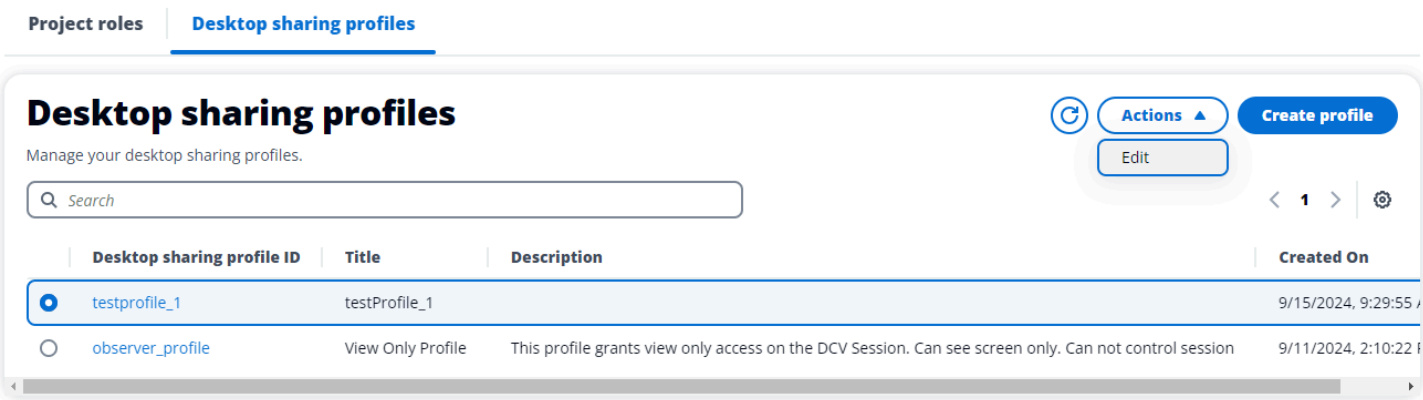
編輯設定檔

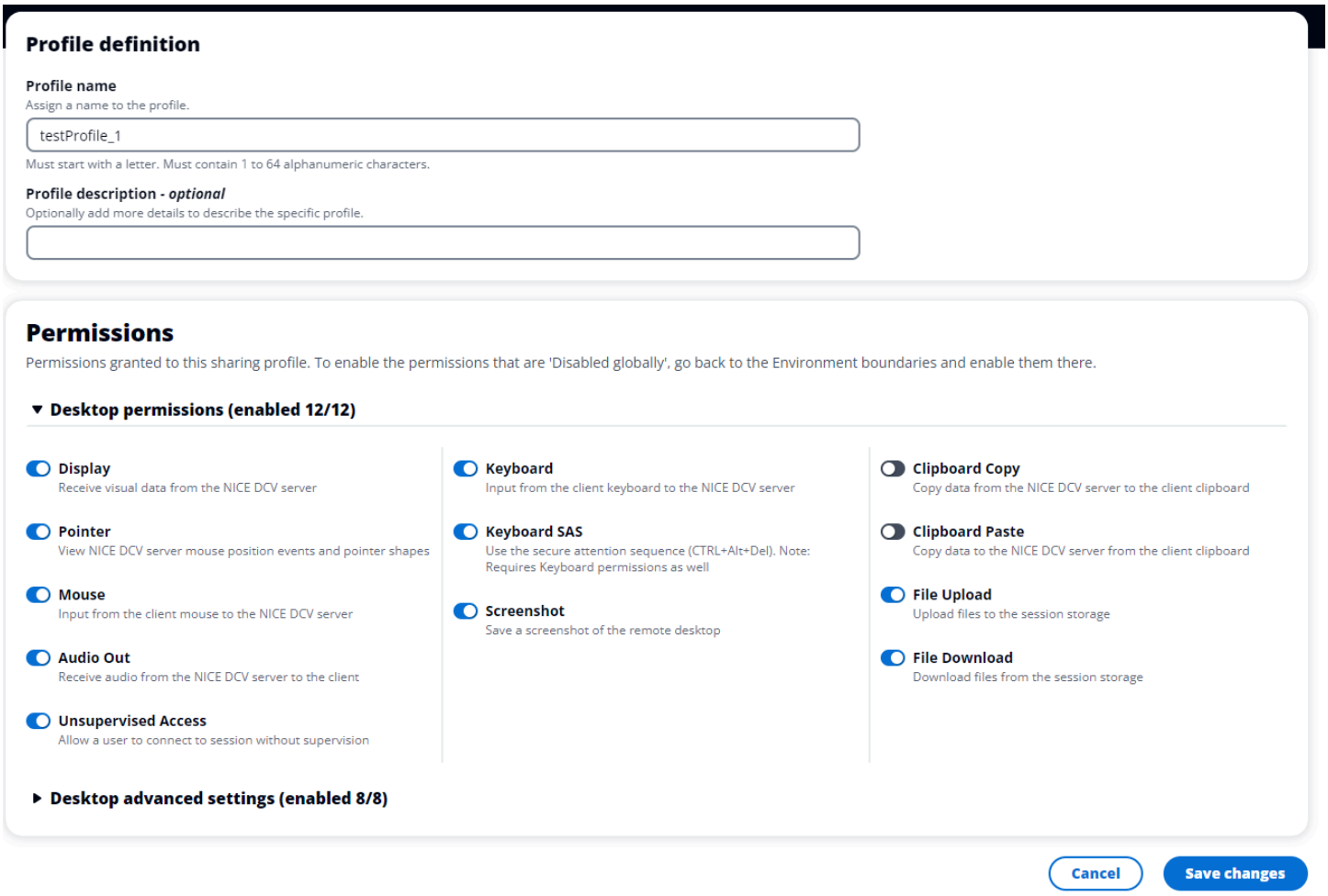
若要編輯設定檔：

1. 選取所需的設定檔。
2. 選擇動作，然後選取編輯以修改設定檔。

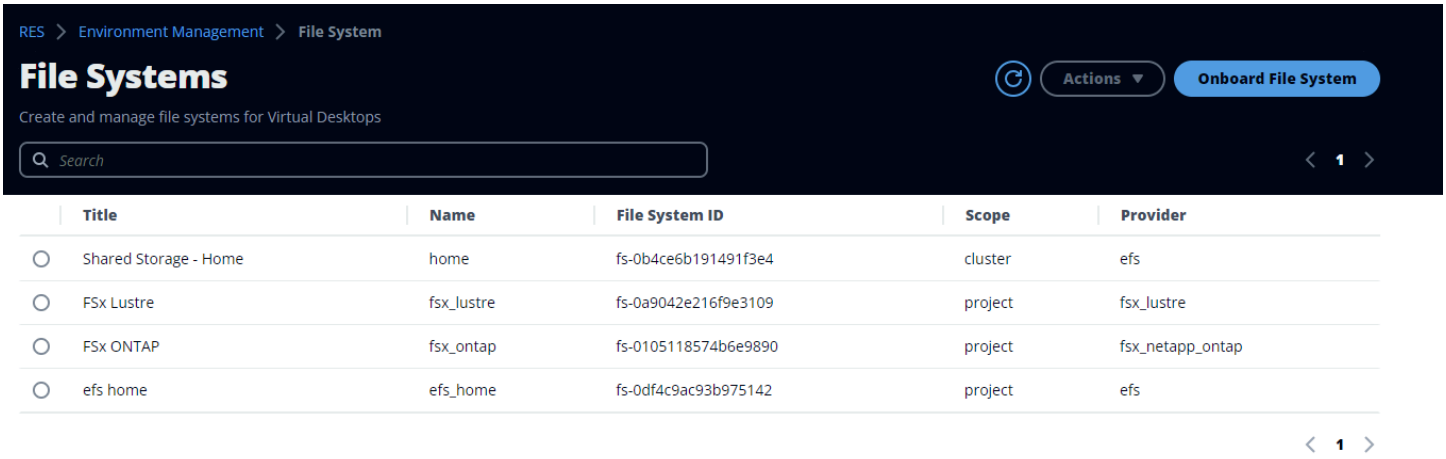
3. 視需要調整許可。
4. 選擇儲存變更。

對設定檔所做的任何變更都會立即套用至目前開啟的工作階段。





檔案系統



從檔案系統頁面，您可以：

1. 搜尋檔案系統。
2. 選取檔案系統時，請使用動作功能表來：
   a. 將檔案系統新增至專案。
   b. 從專案移除檔案系統
3. 加入新的檔案系統。
4. 選取檔案系統時，您可以展開畫面底部的窗格，以檢視檔案系統詳細資訊。

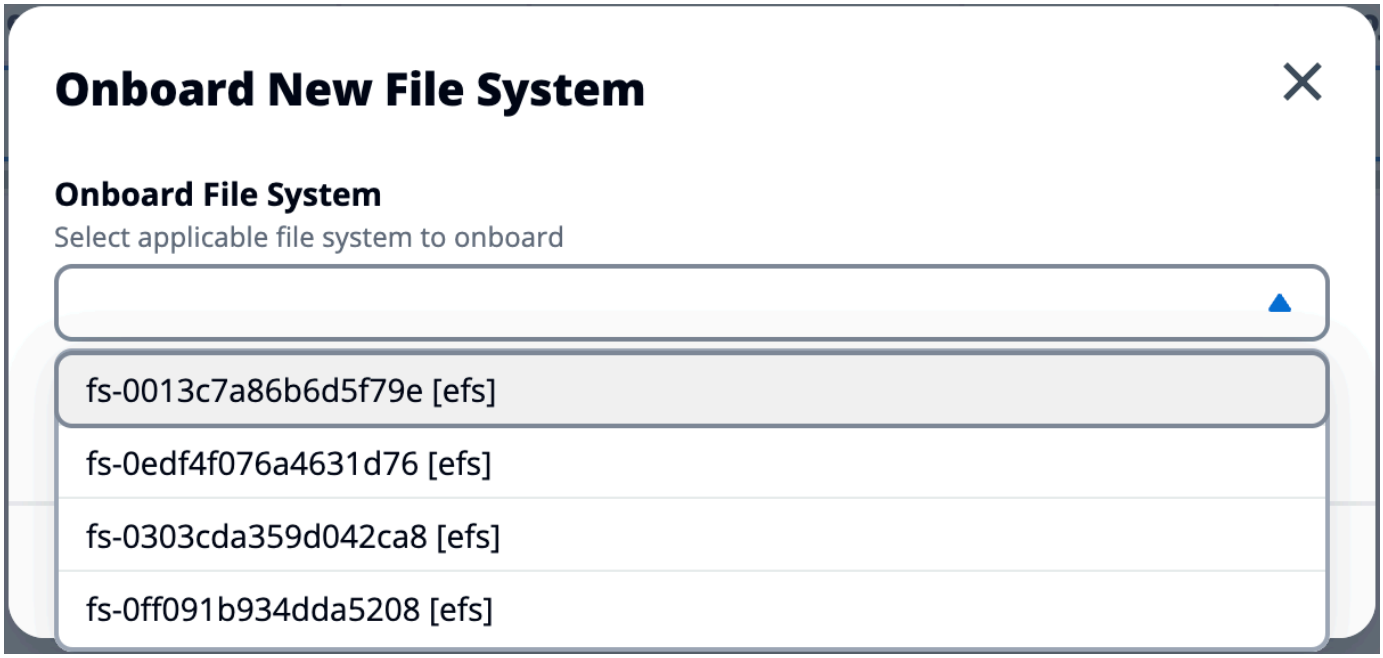
主題

- 加入檔案系統

加入檔案系統

> **Note**
> 若要成功加入檔案系統，它必須共用相同的 VPC 和至少一個 RES 子網路。您還必須確保已正確設定安全群組，以便您的 VDIs 可以存取檔案系統的內容。

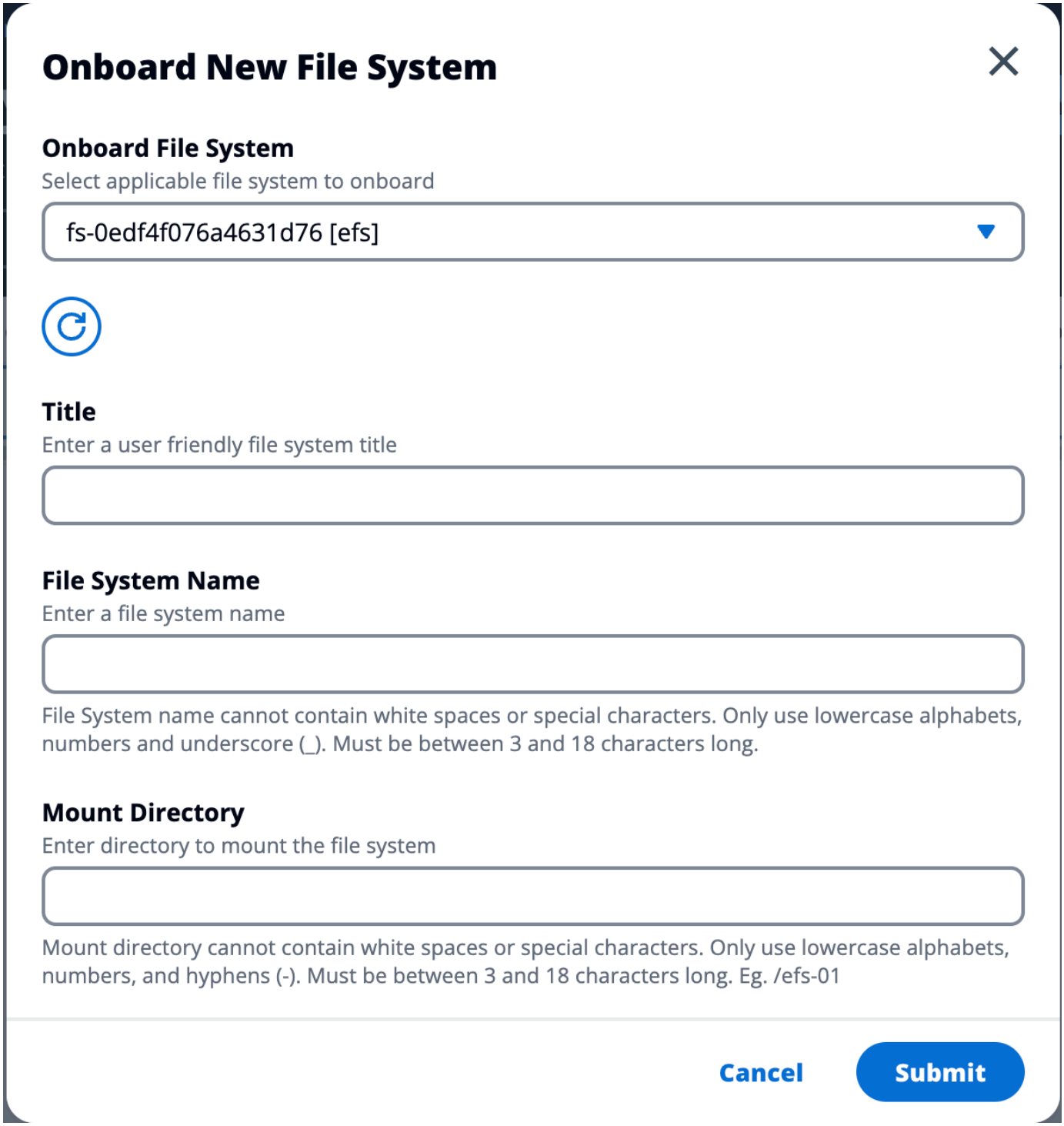
1. 選擇加入檔案系統。
2. 從下拉式清單中選取檔案系統。模態將以其他詳細資訊項目展開。



3. 輸入檔案系統詳細資訊。

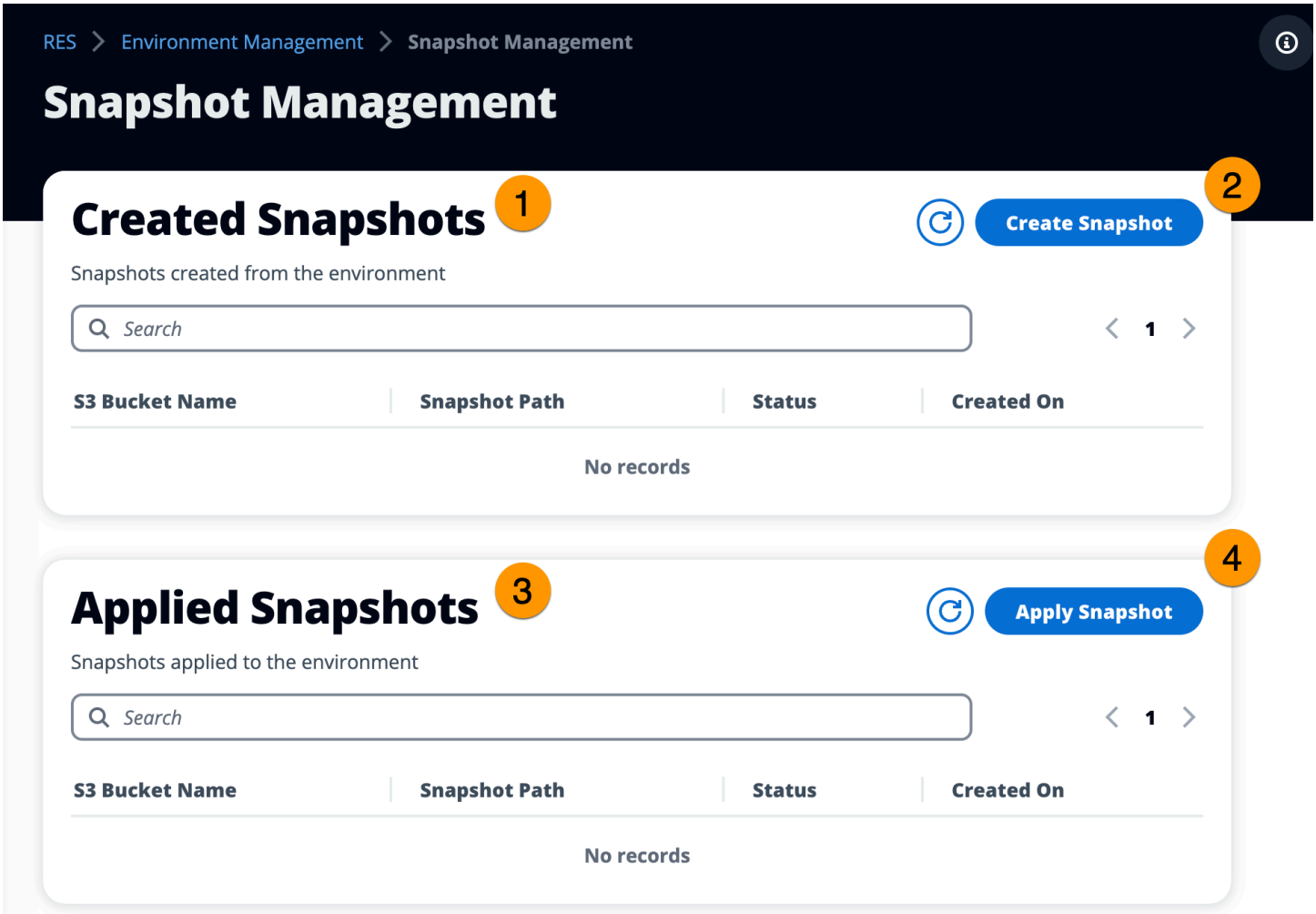
> **Note**
>
> 根據預設，管理員和專案擁有者可以在建立新專案時選擇主檔案系統，之後就無法編輯。旨在用作專案上主目錄的檔案系統必須透過將其掛載目錄路徑設定為 來加入/home。這將在主目錄檔案系統下拉式清單選項上填入加入的檔案系統。此功能有助於隔離跨專案的資料，因為只有與專案相關聯的使用者才能透過其 VDIs 存取檔案系統。VDIs會將檔案系統掛載在檔案系統加入期間選取的掛載點。

4. 選擇提交。



快照管理

快照管理可簡化在環境之間儲存和遷移資料的程序，確保一致性和準確性。透過快照，您可以儲存環境狀態，並將資料遷移至具有相同狀態的新環境。



從快照管理頁面，您可以：

1. 檢視所有建立的快照及其狀態。
2. 建立快照。您必須先建立具有適當許可的儲存貯體，才能建立快照。
3. 檢視所有套用的快照及其狀態。
4. 套用快照。

主題

- 建立快照
- 套用快照

建立快照

您必須先提供具備必要許可的 Amazon S3 儲存貯體，才能建立快照。如需與建立儲存貯體相關的資訊，請參閱建立儲存貯體。我們建議您啟用儲存貯體版本控制和伺服器存取記錄。佈建後，可以從儲存貯體的屬性索引標籤啟用這些設定。

> **Note**
>
> 此 Amazon S3 儲存貯體的生命週期將不會在產品中管理。您需要從 主控台管理儲存貯體生命週期。

若要將許可新增至儲存貯體：

1. 從儲存貯體清單中選取您建立的儲存貯體。
2. 選取許可索引標籤。
3. 在 Bucket policy (儲存貯體政策) 下方，選擇 Edit (編輯)。
4. 將下列陳述式新增至儲存貯體政策。以您自己的值取代這些值：
   - AWS_ACCOUNT_ID
   - RES_ENVIRONMENT_NAME
   - AWS_REGION
   - S3_BUCKET_NAME

   > **Important**
   >
   > 支援的版本字串有限 AWS。如需詳細資訊，請參閱https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_version.html。

   JSON

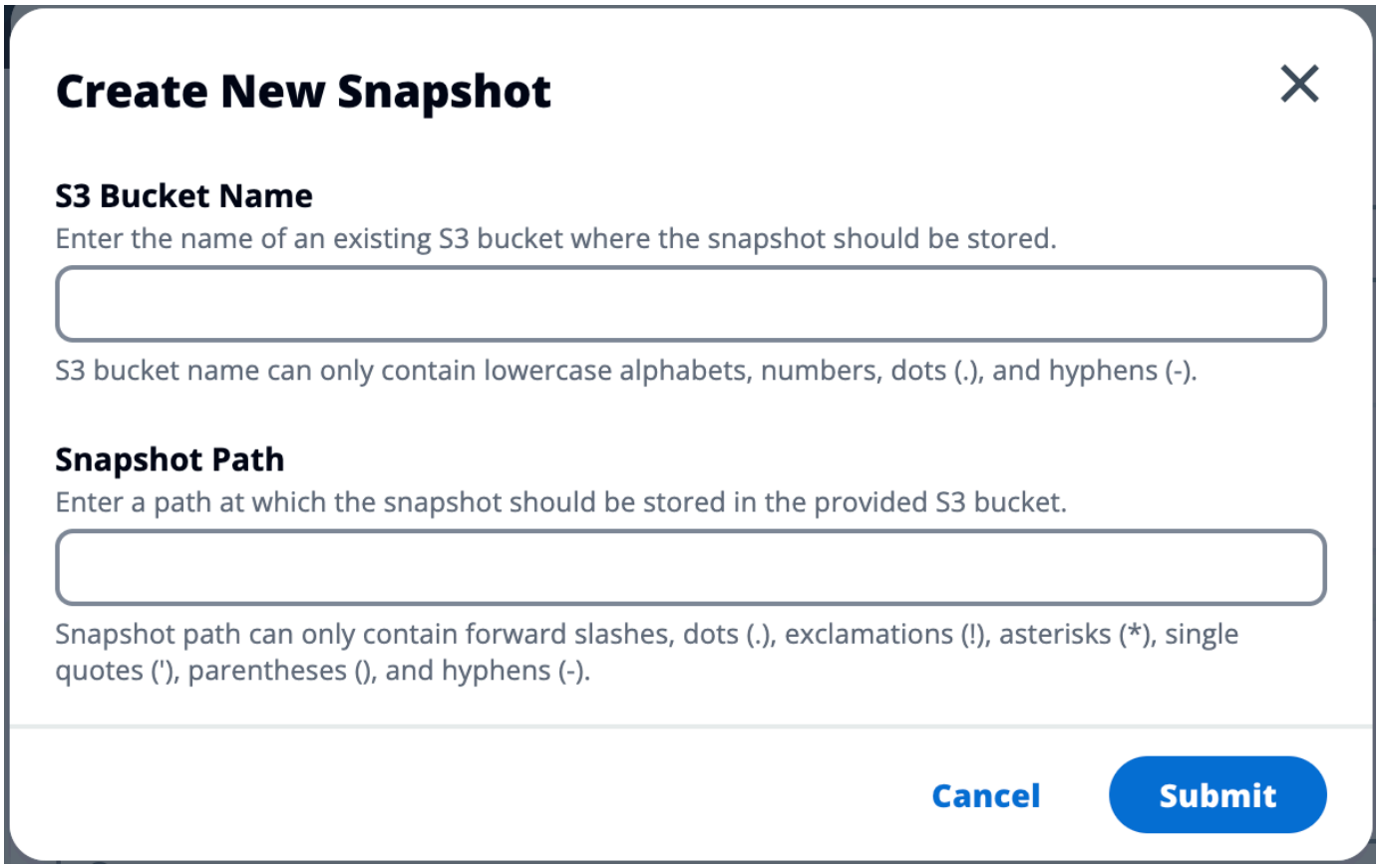
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-
role-{AWS_REGION}}"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ]
        },
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
    ]
}
```

若要建立快照：

1. 選擇 Create Snapshot (建立快照)。
2. 輸入您建立的 Amazon S3 儲存貯體名稱。
3. 輸入您希望快照存放在儲存貯體中的路徑。例如 **`october2023/23`**。

4. 選擇提交。



5. 5 到 10 分鐘後，在快照頁面上選擇重新整理以檢查狀態。在狀態從 IN_PROGRESS 變更為 COMPLETED 之前，快照將無效。

套用快照

建立環境快照後，您可以將該快照套用至新環境以遷移資料。您將需要將新的政策新增至儲存貯體，允許環境讀取快照。

套用快照會複製資料，例如使用者許可、專案、軟體堆疊、許可設定檔和檔案系統與其與新環境的關聯。使用者工作階段將不會複寫。套用快照時，它會檢查每個資源記錄的基本資訊，以判斷它是否已存在。對於重複的記錄，快照會略過在新環境中建立資源。對於類似 的記錄，例如共用名稱或金鑰，但其他基本資源資訊會有所不同，它會使用以下慣例建立具有修改名稱和金鑰的新記錄：`RecordName_SnapshotRESVersion_ApplySnapshotID`。`ApplySnapshotID` 看起來像時間戳記，並識別每次嘗試套用快照。

在快照應用程式期間，快照會檢查資源的可用性。新環境無法使用的資源將不會建立。對於具有相依資源的資源，快照會檢查相依資源的可用性。如果相依資源無法使用，則會在沒有相依資源的情況下建立主要資源。

如果新環境不如預期或失敗，您可以檢查日誌群組中找到的 CloudWatch 日誌`/res-<env-name>/cluster-manager`以取得詳細資訊。每個日誌都會有 【套用快照】 標籤。套用快照後，您可以從 the section called “快照管理”頁面檢查其狀態。

若要將許可新增至儲存貯體：

1. 從儲存貯體清單中選取您建立的儲存貯體。
2. 選取許可索引標籤。
3. 在 Bucket policy (儲存貯體政策) 下方，選擇 Edit (編輯)。
4. 將下列陳述式新增至儲存貯體政策。以您自己的值取代這些值：

   - AWS_ACCOUNT_ID
   - RES_ENVIRONMENT_NAME
   - AWS_REGION
   - S3_BUCKET_NAME

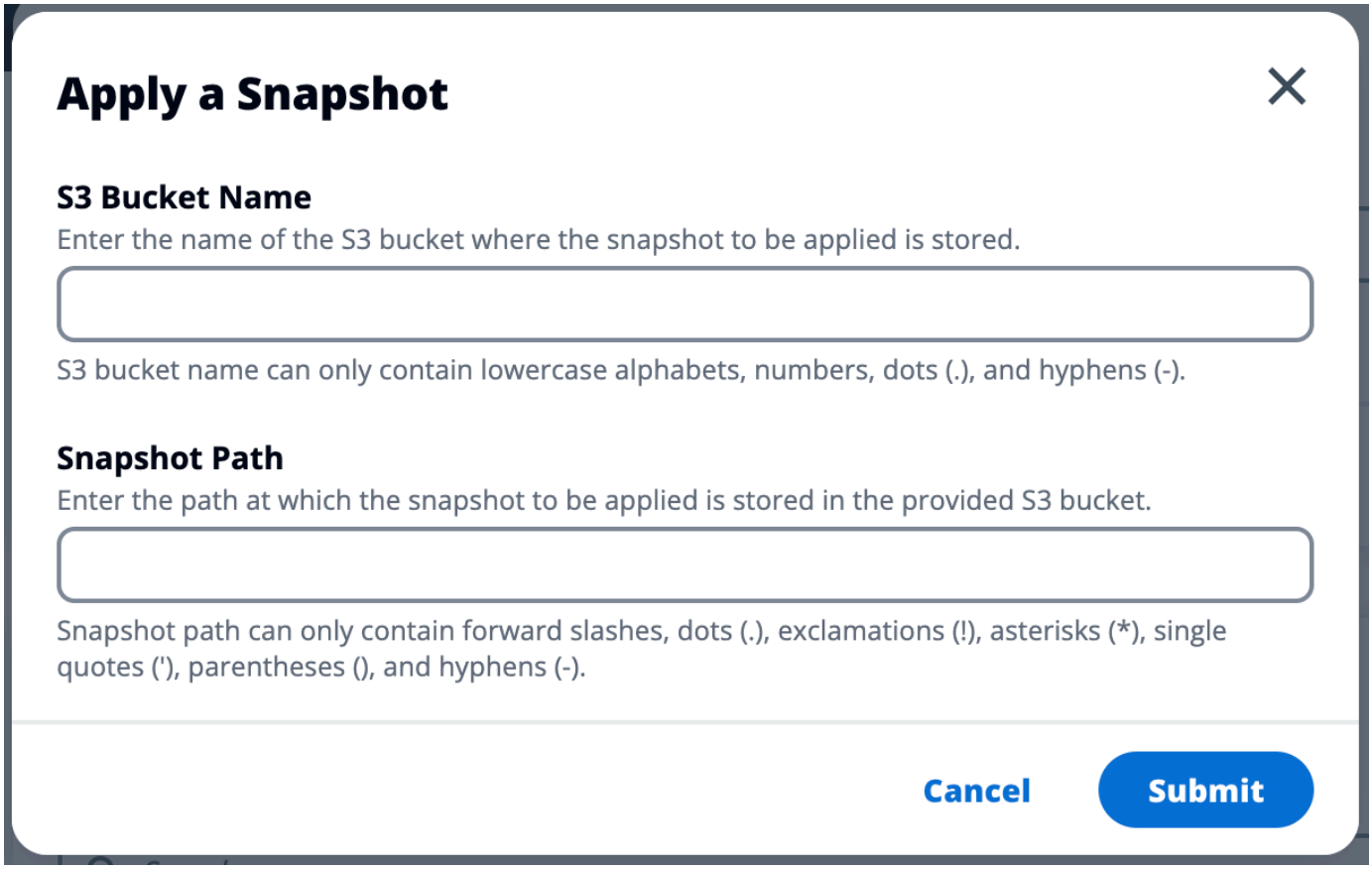
   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Export-Snapshot-Policy",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/{RES_ENVIRONMENT_NAME}-cluster-manager-
role-{AWS_REGION}}"
            },
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ]
        },
        {
```

```
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::{S3_BUCKET_NAME}",
                "arn:aws:s3:::{S3_BUCKET_NAME}/*"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            },
            "Principal": "*"
        }
    ]
}
```

若要套用快照：

1. 選擇套用快照。
2. 輸入包含快照的 Amazon S3 儲存貯體名稱。
3. 輸入儲存貯體中快照的檔案路徑。
4. 選擇提交。



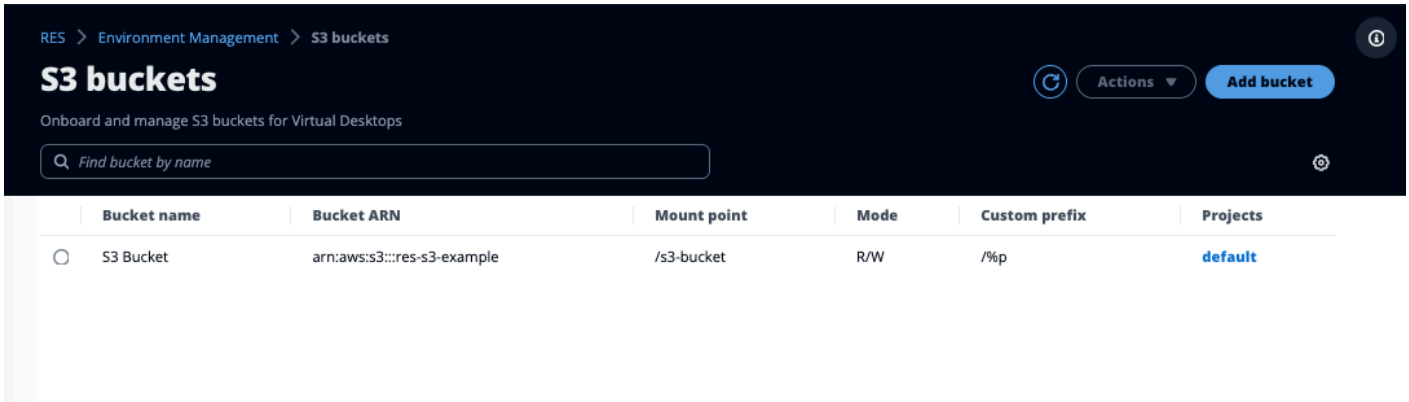
5. 5 到 10 分鐘後，在快照管理頁面上選擇重新整理以檢查狀態。

Amazon S3 儲存貯體

Research and Engineering Studio (RES) 支援將 Amazon S3 儲存貯體掛載到 Linux Virtual Desktop Infrastructure (VDI) 執行個體。RES 管理員可以將 S3 儲存貯體加入 RES、將其連接至專案、編輯其組態，以及移除環境管理下 S3 儲存貯體索引標籤中的儲存貯體。

S3 儲存貯體儀表板提供您可使用的已加入 S3 儲存貯體清單。從 S3 儲存貯體儀表板，您可以：

1. 使用新增儲存貯體將 S3 儲存貯體加入 RES。
2. 選取 S3 儲存貯體並使用動作功能表來：
   - 編輯儲存貯體
   - 移除儲存貯體
3. 使用搜尋欄位依儲存貯體名稱搜尋，並尋找加入的 S3 儲存貯體。



下列各節說明如何在 RES 專案中管理 Amazon S3 儲存貯體。

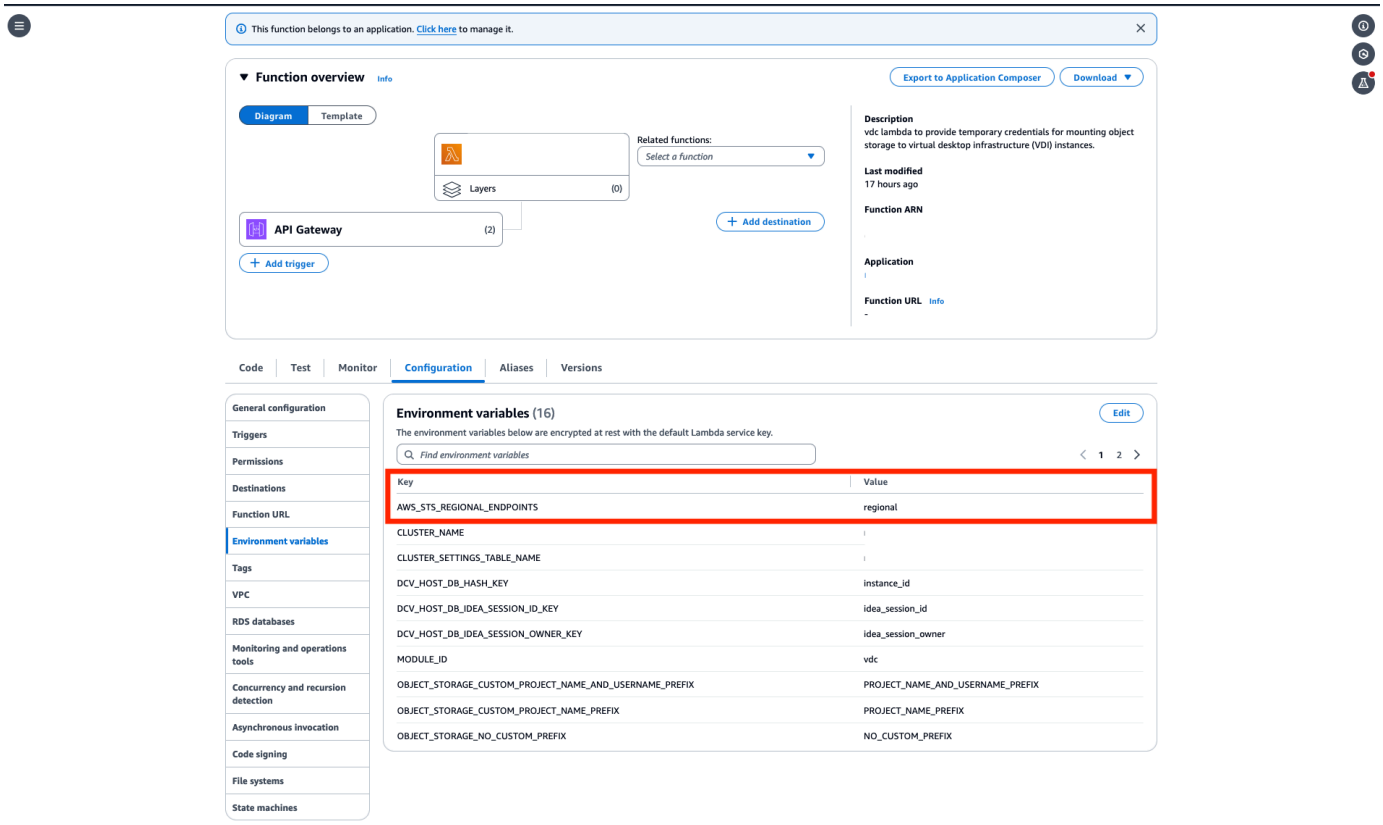
主題

- 隔離 VPC 部署的 Amazon S3 儲存貯體先決條件
- 新增 Amazon S3 儲存貯體
- 編輯 Amazon S3 儲存貯體
- 移除 Amazon S3 儲存貯體
- 資料隔離
- 跨帳戶儲存貯體存取
- 防止私有 VPC 中的資料外洩
- 故障診斷
- 啟用 CloudTrail

隔離 VPC 部署的 Amazon S3 儲存貯體先決條件

如果您要在隔離的 VPC 中部署 Research and Engineering Studio，請在 AWS 帳戶中部署 RES 之後，依照下列步驟更新 lambda 組態參數。

1. 登入部署 Research and Engineering Studio 之 AWS 帳戶的 Lambda 主控台。
2. 尋找並導覽至名為 的 Lambda 函數`<RES-EnvironmentName>-vdc-custom-credential-broker-lambda`。
3. 選取 函數的組態索引標籤。



4. 在左側，選擇環境變數以檢視該區段。
5. 選擇編輯，並將下列新環境變數新增至函數：
   - 索引鍵：`AWS_STS_REGIONAL_ENDPOINTS`
   - 值：`regional`
6. 選擇儲存。

新增 Amazon S3 儲存貯體

若要將 S3 儲存貯體新增至您的 RES 環境：

1. 選擇新增儲存貯體。
2. 輸入儲存貯體詳細資訊，例如儲存貯體名稱、ARN 和掛載點。

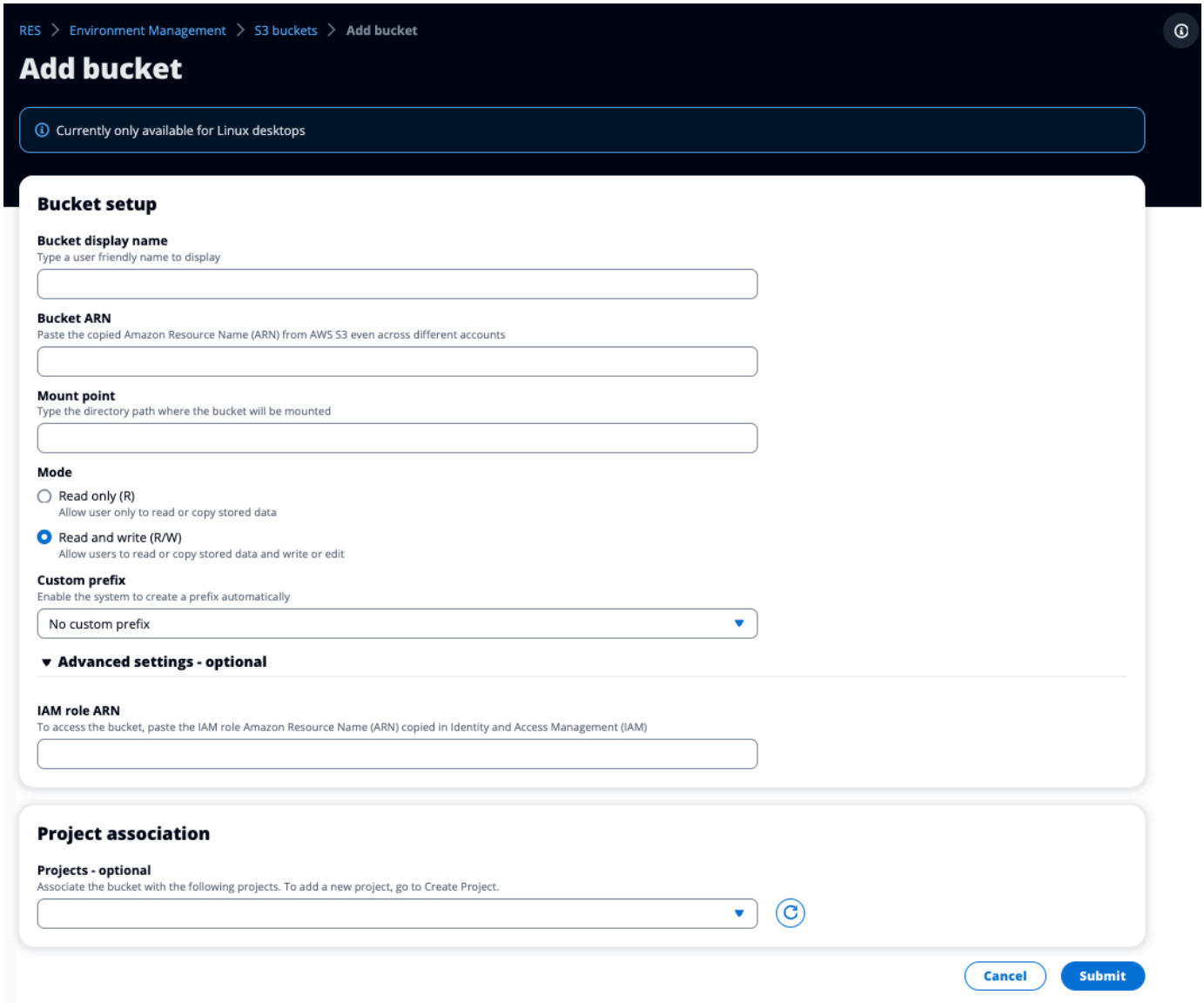
> **Important**
>
> - 提供的儲存貯體 ARN、掛載點和模式無法在建立後變更。

- 儲存貯體 ARN 可以包含一個字首，將加入的 S3 儲存貯體與該字首隔離。

3. 選取要加入儲存貯體的模式。

> **Important**
>
> - 資料隔離 如需使用特定模式隔離資料的詳細資訊，請參閱 。

4. 在進階選項下，您可以提供 IAM 角色 ARN 來掛載儲存貯體以進行跨帳戶存取。請依照 中的步驟跨帳戶儲存貯體存取建立跨帳戶存取所需的 IAM 角色。
5. （選用）將儲存貯體與專案建立關聯，稍後可以變更。不過，S3 儲存貯體無法掛載到專案的現有 VDI 工作階段。只有專案與儲存貯體建立關聯之後啟動的工作階段，才會掛載儲存貯體。
6. 選擇提交。

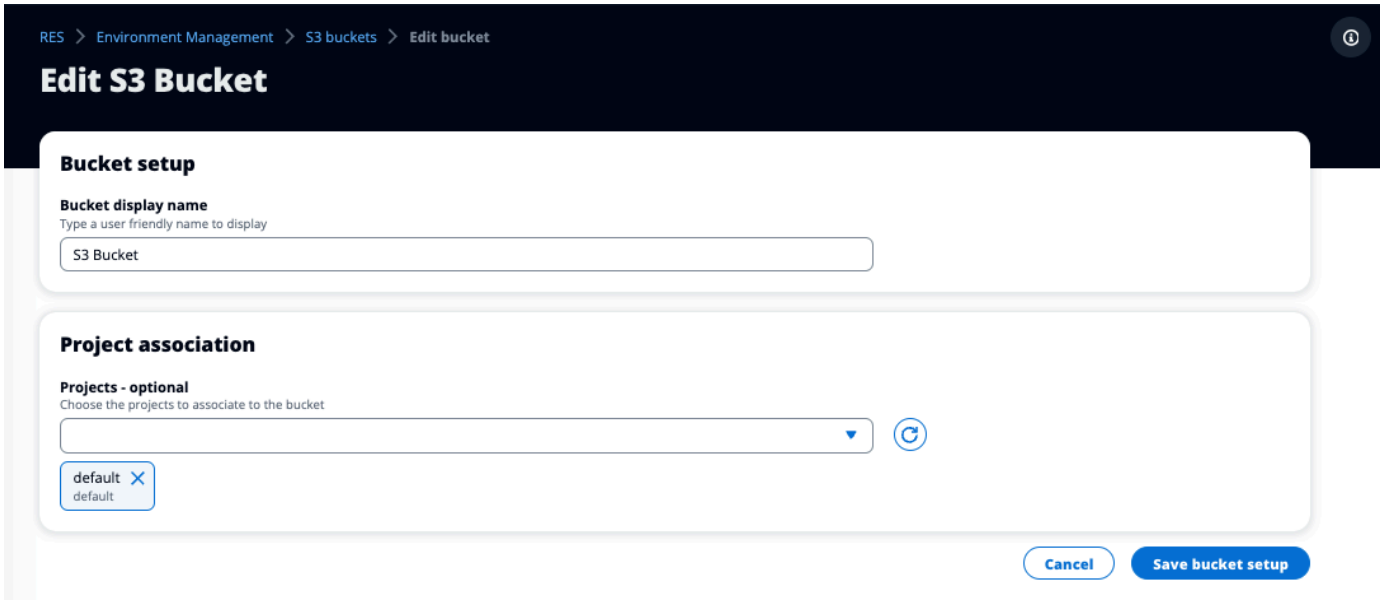


編輯 Amazon S3 儲存貯體

1. 在 S3 儲存貯體清單中選取 S3 儲存貯體。
2. 從動作功能表中，選取編輯。
3. 輸入您的更新。

> **Important**
>
> - 將專案與 S3 儲存貯體建立關聯不會將儲存貯體掛載到該專案的現有虛擬桌面基礎設施 (VDI) 執行個體。只有在儲存貯體與該專案建立關聯之後，儲存貯體才會掛載到專案中啟動的 VDI 工作階段。
> - 取消專案與 S3 儲存貯體的關聯不會影響 S3 儲存貯體中的資料，但會導致桌面使用者無法存取該資料。

4. 選擇儲存儲存貯體設定。



移除 Amazon S3 儲存貯體

1. 在 S3 儲存貯體清單中選取 S3 儲存貯體。
2. 從動作功能表中，選取移除。

> **Important**
>
> - 您必須先從儲存貯體中移除所有專案關聯。
> - 移除操作不會影響 S3 儲存貯體中的資料。它只會移除 S3 儲存貯體與 RES 的關聯。
> - 移除儲存貯體會導致現有的 VDI 工作階段在該工作階段的登入資料過期時 (~1 小時) 無法存取該儲存貯體的內容。

資料隔離

當您將 S3 儲存貯體新增至 RES 時，您可以選擇將儲存貯體中的資料隔離給特定專案和使用者。在新增儲存貯體頁面上，您可以選擇唯讀 (R) 或讀寫 (R/W) 模式。

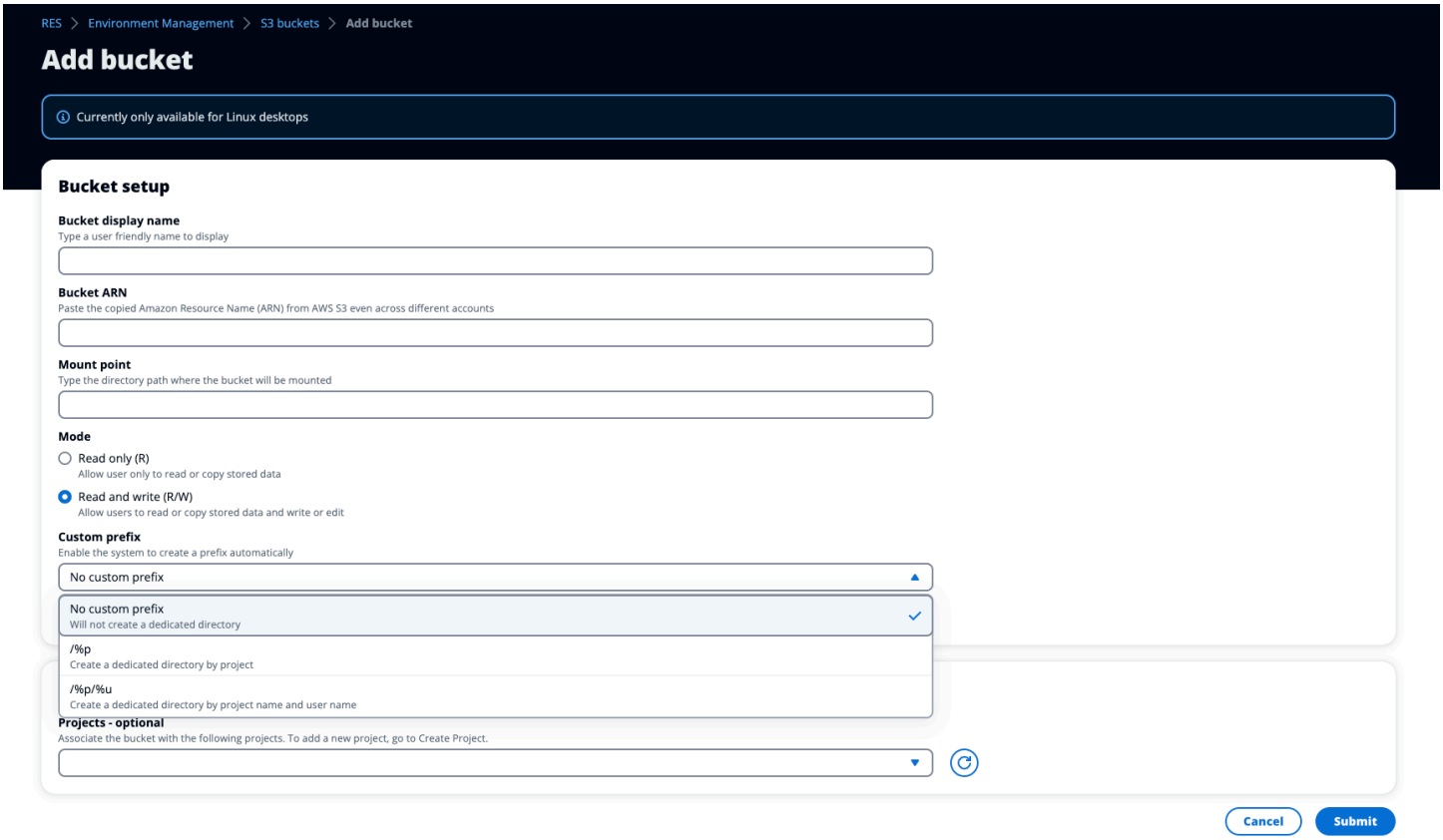
唯讀

`Read Only (R)` 如果選取 ，則會根據儲存貯體 ARN (Amazon Resource Name) 的字首強制執行資料隔離。例如，如果管理員使用 ARN 將儲存貯體新增至 RES，`arn:aws:s3:::`*`bucket-name/example-data`*`/`並將此儲存貯體與專案 A 和專案 B 建立關聯，則從專案 A 和專案 B 內啟動 VDIs 的使用者只能讀取路徑 *`bucket-name`*下位於 中的資料*`/example-data`*。他們將無法存取該路徑以外的資料。如果沒有字首附加到儲存貯體 ARN，則整個儲存貯體將提供給與其相關聯的任何專案。

讀取和寫入

如果選取 `Read and Write (R/W)` ，仍會根據儲存貯體 ARN 的字首強制執行資料隔離，如上所述。此模式有其他選項，可讓管理員為 S3 儲存貯體提供以變數為基礎的字首。`Read and Write (R/W)` 選取 時，自訂字首區段會變成可用，提供具有下列選項的下拉式功能表：

- 沒有自訂字首
- /%p
- /%p/%u



無自訂資料隔離

為自訂字首選取 No custom prefix 時，會新增儲存貯體，而沒有任何自訂資料隔離。這可讓與儲存貯體相關聯的任何專案具有讀取和寫入存取權。例如，如果管理員使用arn:aws:s3:::*bucket-name*No custom prefix選取的 ARN 將儲存貯體新增至 RES，並將此儲存貯體與專案 A 和專案 B 建立關聯，則從專案 A 和專案 B 內啟動 VDIs 的使用者將擁有儲存貯體的無限制讀取和寫入存取權。

每個專案層級的資料隔離

為自訂字首選取 /%p 時，儲存貯體中的資料會隔離至與其相關聯的每個特定專案。%p 變數代表專案程式碼。例如，如果管理員使用arn:aws:s3:::*bucket-name*具有/%p所選 的 ARN 和 */ ###*體的掛載點將儲存貯體新增至 RES，並將此儲存貯體與專案 A 和專案 B 建立關聯，則專案 A 中的使用者 A 可以將檔案寫入 */ ####*。專案 A 中的使用者 B 也可以查看使用者 A 在 */ ###*體中撰寫的檔案。不過，如果使用者 B 在專案 B 中啟動 VDI 並在 */ ###*體中尋找，他們將不會看到使用者 A 所撰寫的檔案，因為資料是由專案隔離。檔案 使用者 A 寫入位於 S3 儲存貯體的字首下，/ProjectA而使用者 B 只能在從專案 B 使用其 VDIs/ProjectB時存取 。

每個專案、每個使用者層級的資料隔離

為自訂字首選取 /%p/%u 時，儲存貯體中的資料會與該專案相關聯的每個特定專案和使用者隔離。%p 變數代表專案程式碼，而 %u代表使用者名稱。例如，管理員使用 `arn:aws:s3:::bucket-name` ARN 搭配/%p/%u選取的 和 / ####的掛載點，將儲存貯體新增至 RES。此儲存貯體與專案 A 和專案 B 相關聯。專案 A 中的使用者 A 可以將檔案寫入 / ####。與先前僅隔離的情況不同%p，在此情況下，使用者 B 不會看到使用者 A 在 / ###體的專案 A 中寫入的檔案，因為資料是由專案和使用者所隔離。檔案 使用者 A 寫入位於 S3 儲存貯體的字首下，/ ProjectA/UserA而使用者 B 只能在專案 A 中使用其 VDIs/ProjectA/UserB時存取 。

跨帳戶儲存貯體存取

RES 能夠從其他 AWS 帳戶掛載儲存貯體，前提是這些儲存貯體具有適當的許可。在下列案例中，帳戶 A 中的 RES 環境想要在帳戶 B 中掛載 S3 儲存貯體。

步驟 1：在部署 RES 的帳戶中建立 IAM 角色（這將稱為帳戶 A)：

1. 登入需要存取 S3 儲存貯體（帳戶 A) 之 RES 帳戶的 AWS 管理主控台。
2. 開啟 IAM 主控台：
   a. 導覽至 IAM 儀表板。
   b. 在導覽窗格中，選擇政策。
3. 建立政策：
   a. 選擇建立政策。
   b. 選取 JSON 標籤。
   c. 貼上下列 JSON 政策 (*<BUCKET-NAME>*以帳戶 B 中的 S3 儲存貯體名稱取代）：

      JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
```

```
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload"
            ],
            "Resource": [
                "arn:aws:s3:::<BUCKET-NAME>",
                "arn:aws:s3:::<BUCKET-NAME>/*"
            ]
        }
    ]
}
```

d. 選擇下一步。

4. 檢閱並建立政策：

   a. 提供政策的名稱（例如，「S3AccessPolicy」)。

   b. 新增選用的描述來解釋政策的目的。

   c. 檢閱政策，然後選擇建立政策。

5. 開啟 IAM 主控台：

   a. 導覽至 IAM 儀表板。

   b. 在導覽窗格中，選擇角色。

6. 建立角色：

   a. 選擇建立角色。

   b. 選擇自訂信任政策作為信任實體的類型。

   c. 貼上下列 JSON 政策 (*<ACCOUNT_ID>*將 取代為帳戶 A 的實際帳戶 ID、*<ENVIRONMENT_NAME>*將 取代為 RES 部署的環境名稱，*<REGION>*並將 RES 部署為 AWS 區域）：

      JSON

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

```
                "AWS":
 "arn:aws:iam::<ACCOUNT_ID>:role/<ENVIRONMENT_NAME>-custom-credential-
broker-lambda-role-<REGION>"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

d. 選擇下一步。

7. 連接許可政策：

   a. 搜尋並選取您先前建立的政策。

   b. 選擇下一步。

8. 標記、檢閱和建立角色：

   a. 輸入角色名稱（例如，「S3AccessRole」)。

   b. 在步驟 3 下，選擇新增標籤，然後輸入下列索引鍵和值：

      - 索引鍵：`res:Resource`
      - 值：`s3-bucket-iam-role`

   c. 檢閱角色，然後選擇建立角色。

9. 在 RES 中使用 IAM 角色：

   a. 複製您建立的 IAM 角色 ARN。

   b. 登入 RES 主控台。

   c. 在左側導覽窗格中，選擇 S3 儲存貯體。

   d. 選擇新增儲存貯體，並使用跨帳戶 S3 儲存貯體 ARN 填寫表單。

   e. 選擇進階設定 - 選用下拉式清單。

   f. 在 IAM 角色 ARN 欄位中輸入角色 ARN。

   g. 選擇新增儲存貯體。

步驟 2：修改帳戶 B 中的儲存貯體政策

1. 登入帳戶 B 的 AWS 管理主控台。

2. 開啟 S3 主控台：

a. 導覽至 S3 儀表板。

b. 選取您要授予存取權的儲存貯體。

3. 編輯儲存貯體政策：

a. 選取許可索引標籤，然後選擇儲存貯體政策。

b. 新增下列政策，以授予帳戶 A 對儲存貯體的 IAM 角色存取權（將 *<AccountA_ID>* 取代為帳戶 A 的實際帳戶 ID，並將 *<BUCKET-NAME>* 取代為 S3 儲存貯體的名稱）：

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/S3AccessRole"
            },
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:AbortMultipartUpload"
            ],
            "Resource": [
                "arn:aws:s3:::<BUCKET-NAME>",
                "arn:aws:s3:::<BUCKET-NAME>/*"
            ]
        }
    ]
}
```

c. 選擇儲存。

防止私有 VPC 中的資料外洩

若要防止使用者將資料從安全的 S3 儲存貯體滲透到其帳戶中自己的 S3 儲存貯體，您可以連接 VPC 端點來保護您的私有 VPC。下列步驟說明如何為 S3 服務建立 VPC 端點，以支援存取您帳戶中的 S3 儲存貯體，以及具有跨帳戶儲存貯體的任何其他帳戶。

1. 開啟 Amazon VPC 主控台：
   a. 登入 AWS 管理主控台。
   b. 開啟位於 https：//https://console.aws.amazon.com/vpc/ 的 Amazon VPC 主控台。
2. 建立 S3 的 VPC 端點：
   a. 在左側導覽窗格中選擇 Endpoints (端點)。
   b. 選擇建立端點。
   c. 請確定在 Service category (服務類別) 欄位，您已選擇 AWS services (AWS 服務)。
   d. 在服務名稱欄位中，輸入 `com.amazonaws.<region>.s3`(`<region>`取代您的 AWS 區域） 或搜尋 "S3"。
   e. 從清單中選擇 S3 服務。
3. 設定端點設定：
   a. 針對 VPC，選取您要建立端點的 VPC。
   b. 針對子網路，選取部署期間用於 VDI 子網路的兩個私有子網路。
   c. 針對啟用 DNS 名稱，請確定已勾選 選項。這可讓私有 DNS 主機名稱解析為端點網路介面。
4. 設定政策以限制存取：
   a. 在政策下，選擇自訂。
   b. 在政策編輯器中，輸入限制存取您帳戶或特定帳戶內資源的政策。以下是範例政策 （將 *mybucket* 取代為您的 S3 儲存貯體名稱，並將 *111122223333* 和 *444455556666* 取代為您想要存取的適當 AWS 帳戶 IDs)：

      JSON

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

```
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::mybucket",
                "arn:aws:s3:::mybucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "111122223333",   // Your Account ID
                        "444455556666"    // Another Account ID
                    ]
                }
            }
        }
    ]
}
```

5. 建立端點：
   a. 檢閱您的設定。
   b. 選擇建立端點。
6. 驗證端點：
   a. 建立端點後，導覽至 VPC 主控台中的端點區段。
   b. 選取新建立的端點。
   c. 驗證狀態是否可用。

遵循這些步驟，您可以建立 VPC 端點，允許 S3 存取僅限於您帳戶或指定帳戶 ID 內的資源。

故障診斷

如何檢查儲存貯體是否無法在 VDI 上掛載

如果儲存貯體無法在 VDI 上掛載，有幾個位置可讓您檢查錯誤。請依照下列步驟進行。

1. 檢查 VDI 日誌：
   a. 登入 AWS 管理主控台。
   b. 開啟 EC2 主控台並導覽至執行個體。
   c. 選取您啟動的 VDI 執行個體。

d. 透過 Session Manager 連線至 VDI。

e. 執行下列命令：

```
sudo su
cd ~/bootstrap/logs
```

在這裡，您會找到引導日誌。任何失敗的詳細資訊都會位於 `configure.log.{time}` 檔案中。

此外，請檢查`/etc/message`日誌以取得更多詳細資訊。

2. 檢查自訂登入資料中介裝置 Lambda CloudWatch Logs：

   a. 登入 AWS 管理主控台。

   b. 開啟 CloudWatch 主控台並導覽至日誌群組。

   c. 搜尋日誌群組 `/aws/lambda/<stack-name>-vdc-custom-credential-broker-lambda`。

   d. 檢查第一個可用的日誌群組，並在日誌中找到任何錯誤。這些日誌將包含有關提供臨時自訂登入資料以掛載 S3 儲存貯體的潛在問題的詳細資訊。

3. 檢查自訂登入資料中介裝置 API Gateway CloudWatch Logs：

   a. 登入 AWS 管理主控台。

   b. 開啟 CloudWatch 主控台並導覽至日誌群組。

   c. 搜尋日誌群組 `<stack-name>-vdc-custom-credential-broker-lambdavdccustomcredentialbrokerapigatewayaccesslogs<nonce>`。

   d. 檢查第一個可用的日誌群組，並在日誌中找到任何錯誤。這些日誌將包含任何請求和 API Gateway 回應的詳細資訊，以取得掛載 S3 儲存貯體所需的自訂登入資料。

如何在加入後編輯儲存貯體的 IAM 角色組態

1. 登入 AWS DynamoDB 主控台。

2. 選取資料表：

   a. 在左側導覽窗格中，選擇 Tables (資料表)。

   b. 尋找並選取 `<stack-name>.cluster-settings`。

3. 掃描資料表：

a. 選擇 探索資料表項目 。
b. 確定已選取掃描。

4. 新增篩選條件：

a. 選擇篩選條件以開啟篩選條件項目區段。
b. 設定篩選條件以符合您的金鑰 -

- 屬性：輸入 金鑰。
- 條件：選取開頭。
- 值：輸入 以需要修改的檔案系統值`shared-storage.<filesystem_id>.s3_bucket.iam_role_arn`取代 `<filesystem_id>`。

5. 執行掃描：

選擇執行以使用篩選條件執行掃描。

6. 檢查 值：

如果項目存在，請確保使用正確的 IAM 角色 ARN 正確設定值。

如果項目不存在：

a. 選擇建立項目。
b. 輸入項目詳細資訊：

- 針對金鑰屬性，輸入 `shared-storage.<filesystem_id>.s3_bucket.iam_role_arn`。
- 新增正確的 IAM 角色 ARN。

c. 選擇儲存以新增項目。

7. 重新啟動 VDI 執行個體：

重新啟動執行個體，以確保再次掛載受不正確 IAM 角色 ARN 影響VDIs。

啟用 CloudTrail

若要使用 CloudTrail 主控台在您的帳戶中啟用 CloudTrail，請遵循 AWS CloudTrail 使用者指南中的使用 CloudTrail 主控台建立追蹤中提供的指示。CloudTrail 將透過記錄存取 S3 儲存貯體的 IAM 角色來記錄對 S3 儲存貯體的存取。這可以連結回連結至專案或使用者的執行個體 ID。

使用 產品

本節提供使用者使用虛擬桌面與其他使用者協作的指導。

主題

- SSH 存取
- 虛擬桌面
- 共用桌面
- 檔案瀏覽器

SSH 存取

若要使用 SSH 存取堡壘主機：

1. 從 RES 功能表中，選擇 SSH 存取。
2. 依照畫面上的指示，使用 SSH 或 PuTTY 進行存取。

虛擬桌面

虛擬桌面界面 (VDI) 模組可讓使用者建立和管理 Windows 或 Linux 虛擬桌面 AWS。使用者可以使用其偏好的工具和預先安裝並設定的應用程式來啟動 Amazon EC2 執行個體。

支援的作業系統

RES 目前支援使用下列作業系統啟動虛擬桌面：

- Amazon Linux 2 (x86 和 ARM64)
- Ubuntu 22.04.03 (x86)
- RHEL 8 (x86) 和 9 (x86)
- Windows Server 2019、2022 (x86)
- Windows 10、11 (x86)

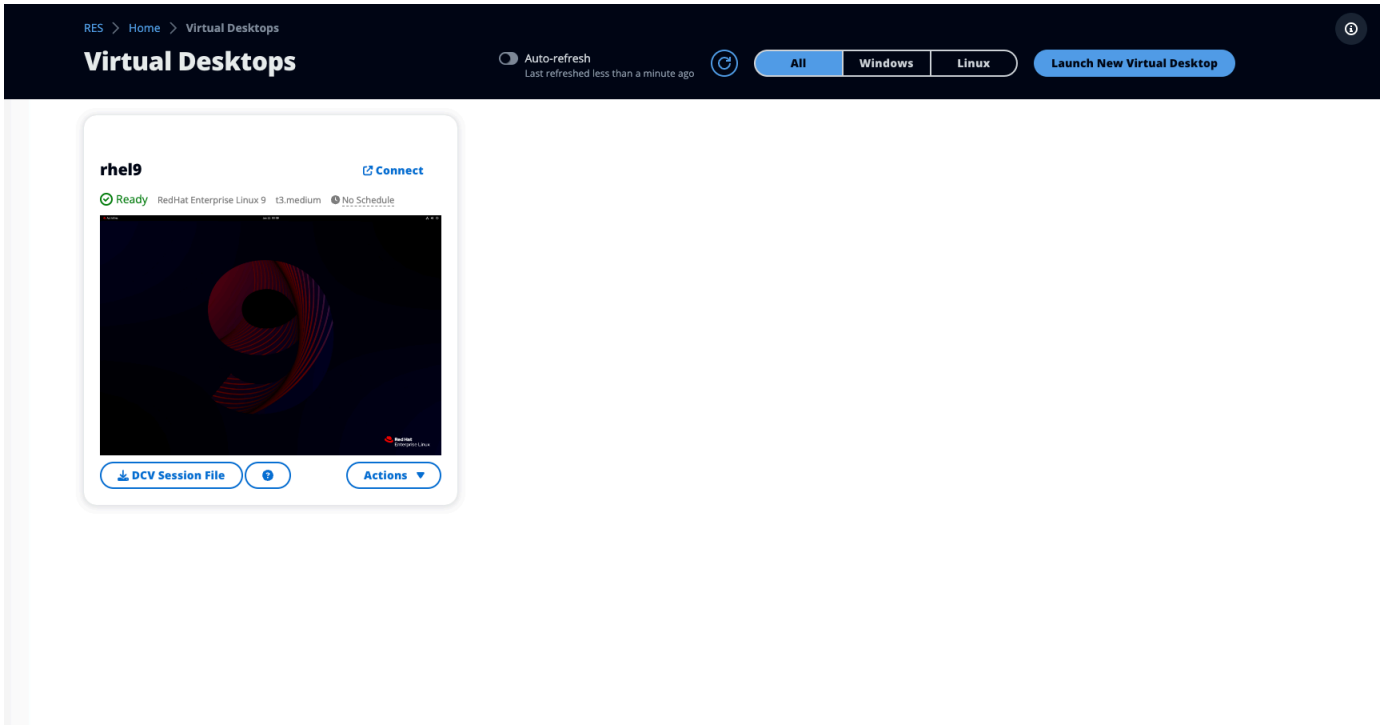
主題

- 啟動新的桌面

- 存取您的桌面
- 控制您的桌面狀態
- 修改虛擬桌面
- 擷取工作階段資訊
- 排程虛擬桌面
- 虛擬桌面界面自動停止

啟動新的桌面

1. 從功能表中，選擇我的虛擬桌面。
2. 選擇啟動新的虛擬桌面。



3. 輸入新桌面的詳細資訊。
4. 選擇提交。

包含您桌面資訊的新卡會立即顯示，您的桌面將在 10-15 分鐘內可供使用。啟動時間取決於選取的映像。RES 會偵測 GPU 執行個體並安裝相關的驅動程式。

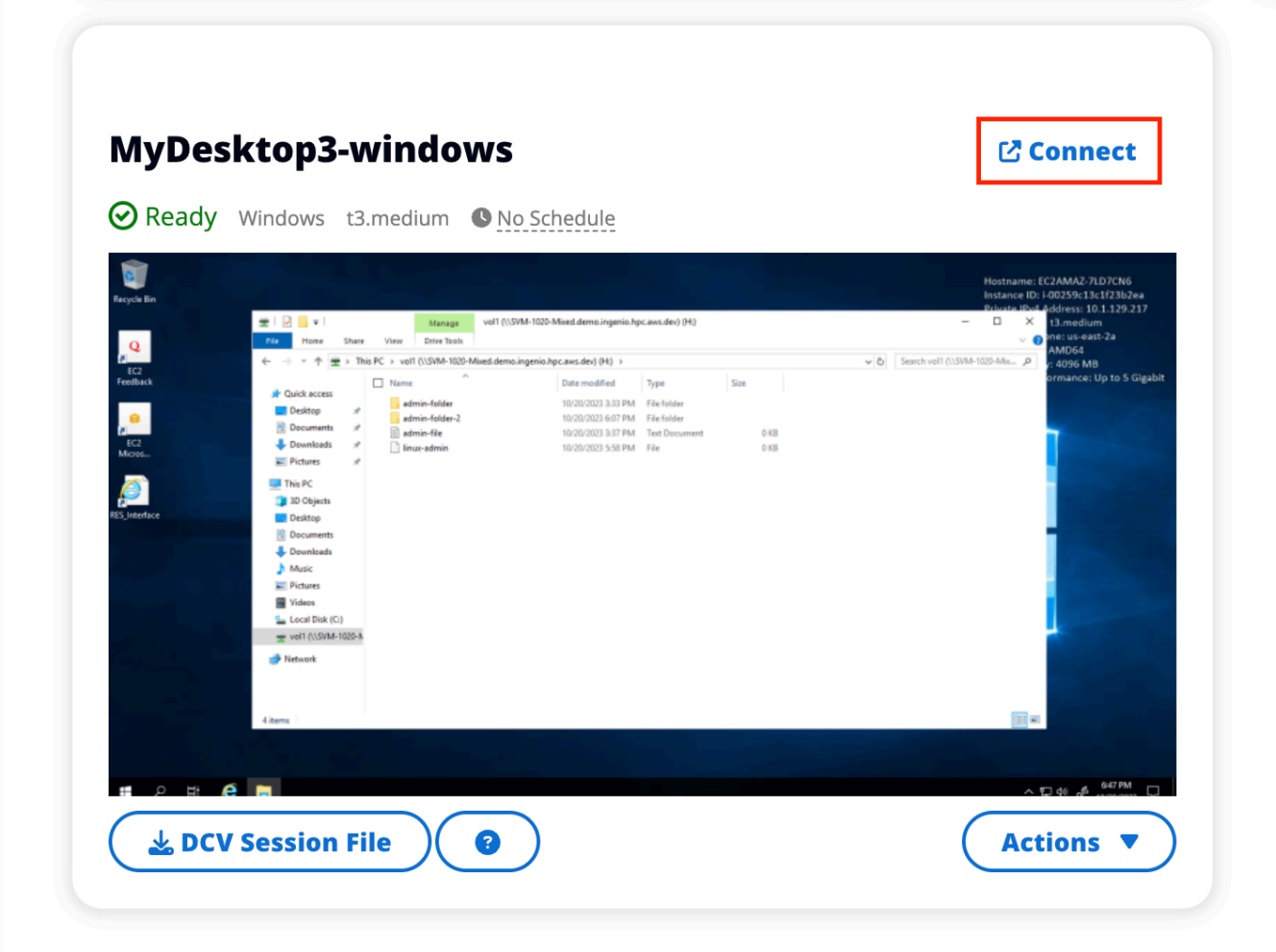
存取您的桌面

若要存取虛擬桌面，請選擇桌面的卡片，並使用 Web 或 DCV 用戶端進行連線。

Web connection

透過 Web 瀏覽器存取桌面是最簡單的連線方法。

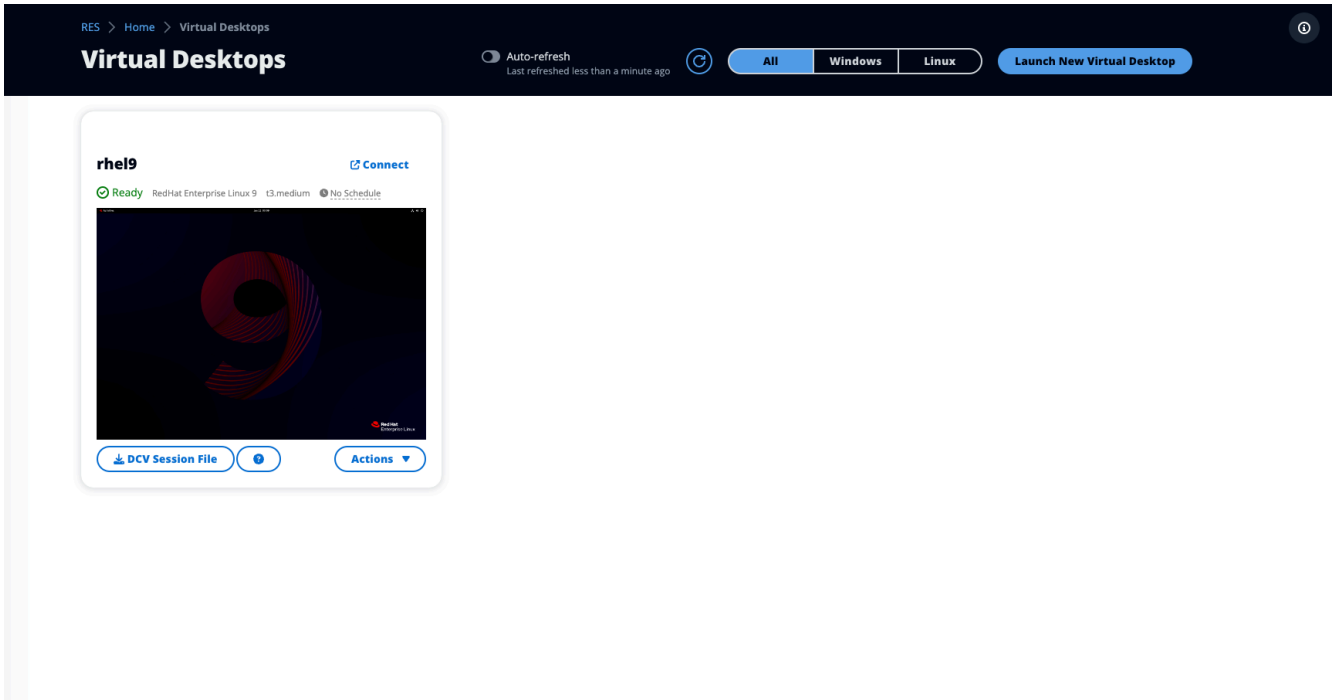
- 選擇連線，或選擇縮圖，直接透過瀏覽器存取您的桌面。



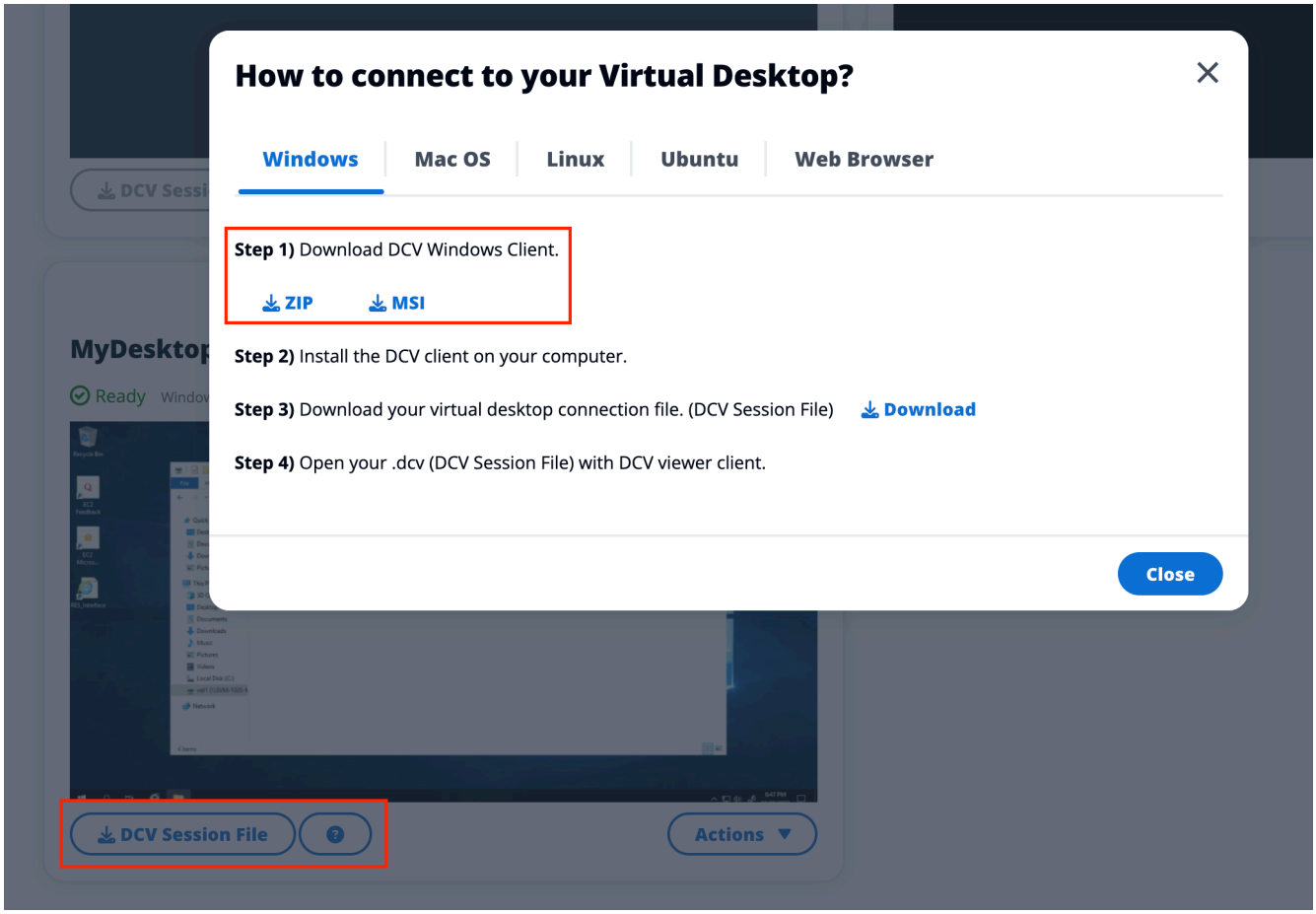
DCV connection

透過 DCV 用戶端存取您的桌面可提供最佳效能。若要透過 DCV 存取：

1. 選擇 DCV 工作階段檔案以下載`.dcv`檔案。您需要在系統上安裝 DCV 用戶端。



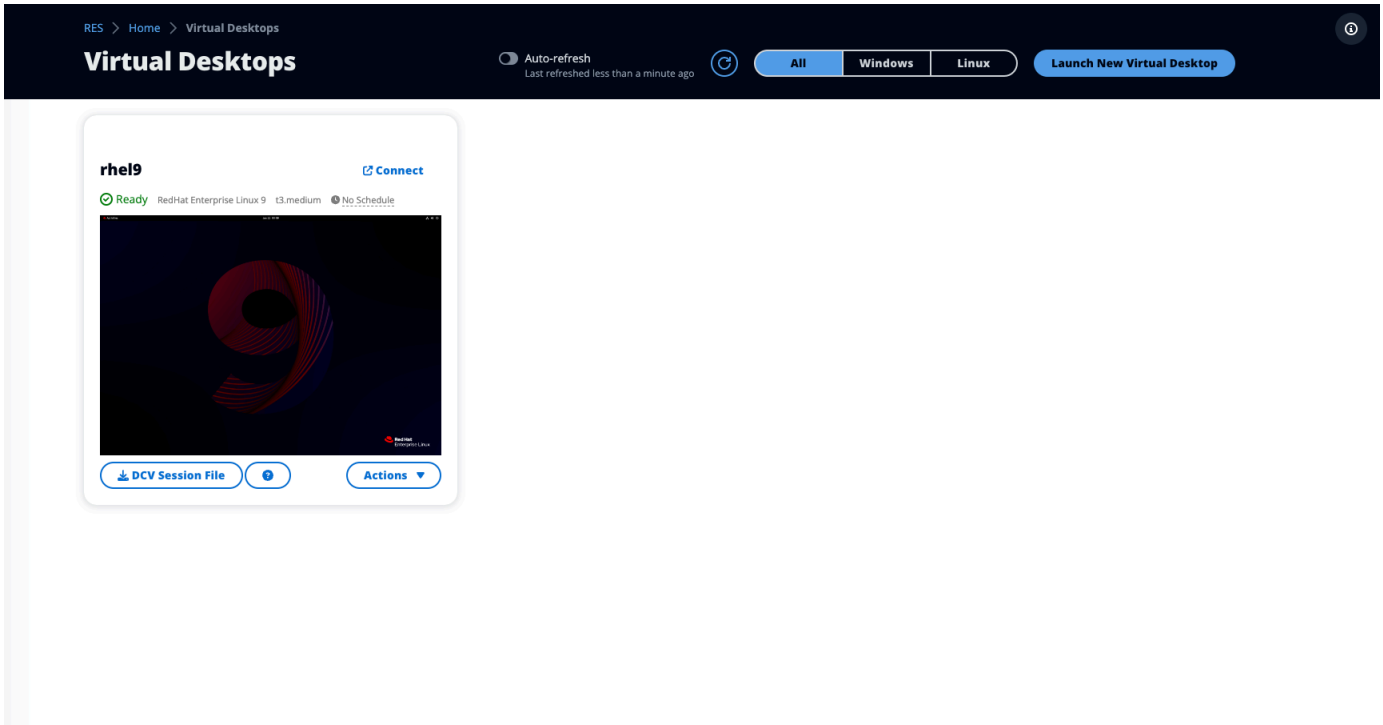
2. 如需安裝說明，請選擇 ? 圖示。



控制您的桌面狀態

若要控制桌面的狀態：

1. 選擇動作。



2. 選擇虛擬桌面狀態。您有四種狀態可供選擇：

   - 停止

     停止的工作階段不會導致資料遺失，而且您可以隨時重新啟動停止的工作階段。

   - 重新啟動

     重新啟動目前的工作階段。

   - 終止

     永久結束工作階段。如果您使用暫時性儲存，終止工作階段可能會導致資料遺失。在終止之前，您應該將資料備份到 RES 檔案系統。

   - 休眠

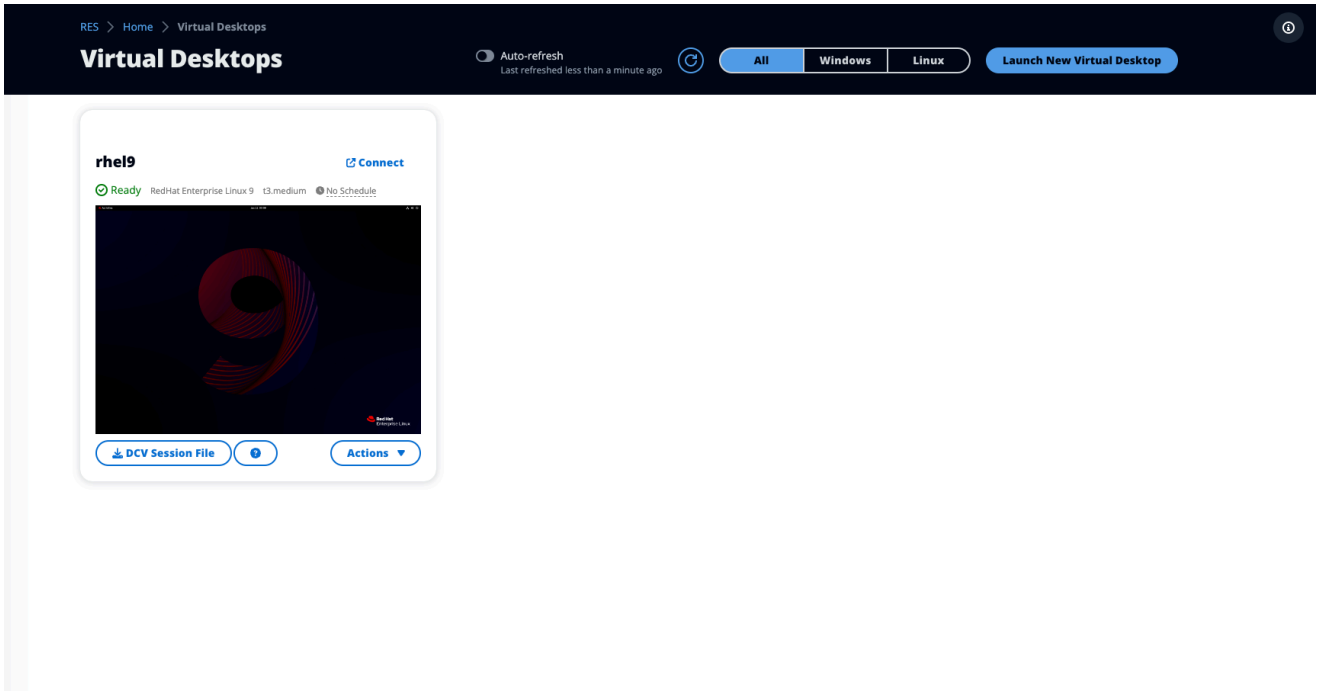
     您的桌面狀態將儲存在記憶體中。當您重新啟動桌面時，您的應用程式會繼續，但任何遠端連線都可能遺失。並非所有執行個體都支援休眠，而且只有在執行個體建立期間啟用時，才能使用選項。若要驗證執行個體是否支援此狀態，請參閱休眠先決條件。

修改虛擬桌面

您可以更新虛擬桌面的硬體或變更工作階段名稱。

1. 在變更執行個體大小之前，您必須停止工作階段：

   a. 選擇動作。



   b. 選擇虛擬桌面狀態。

   c. 選擇停止。

> **Note**
> 您無法更新休眠工作階段的桌面大小。

2. 一旦您確認桌面已停止，請選擇動作，然後選擇更新工作階段。
3. 變更工作階段名稱，或選擇您想要的桌面大小。
4. 選擇提交。
5. 執行個體更新後，請重新啟動桌面：

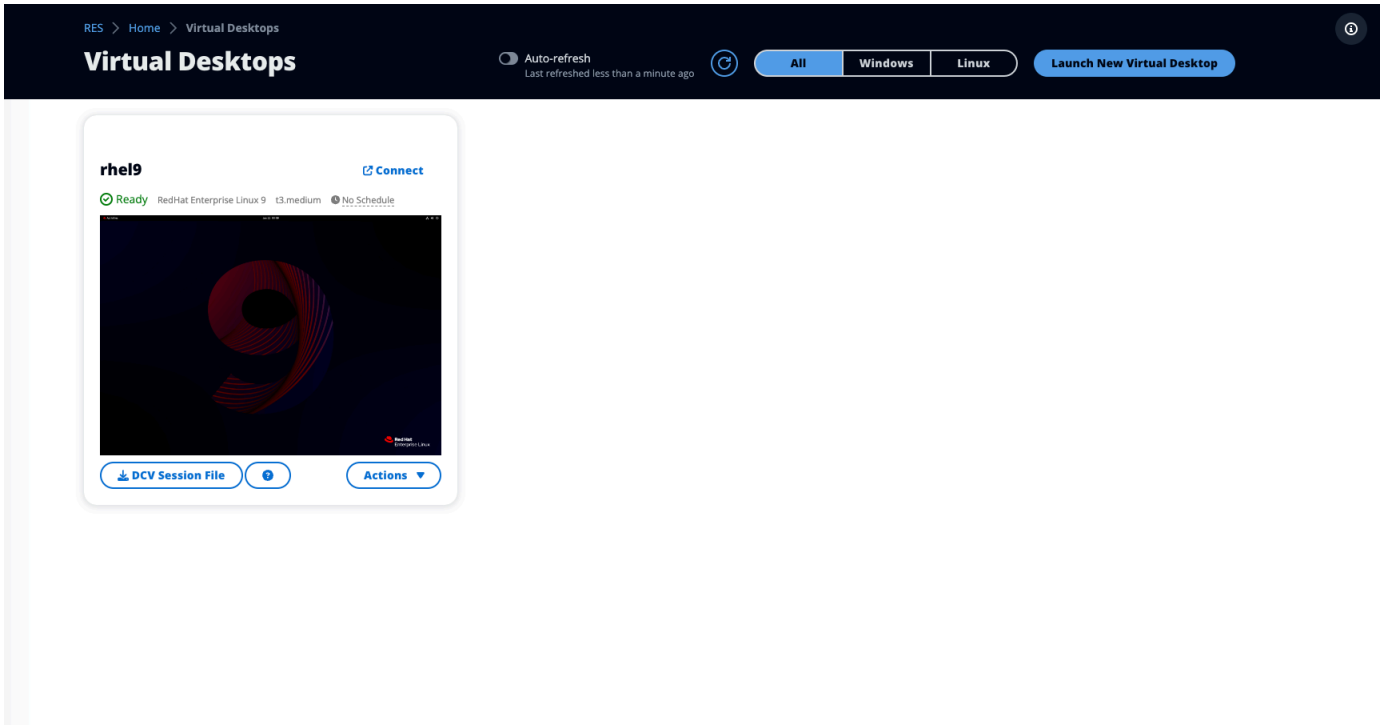
   a. 選擇動作。

   b. 選擇虛擬桌面狀態。

c. 選擇 開始使用。

擷取工作階段資訊

1. 選擇動作。



2. 選擇顯示資訊。

排程虛擬桌面

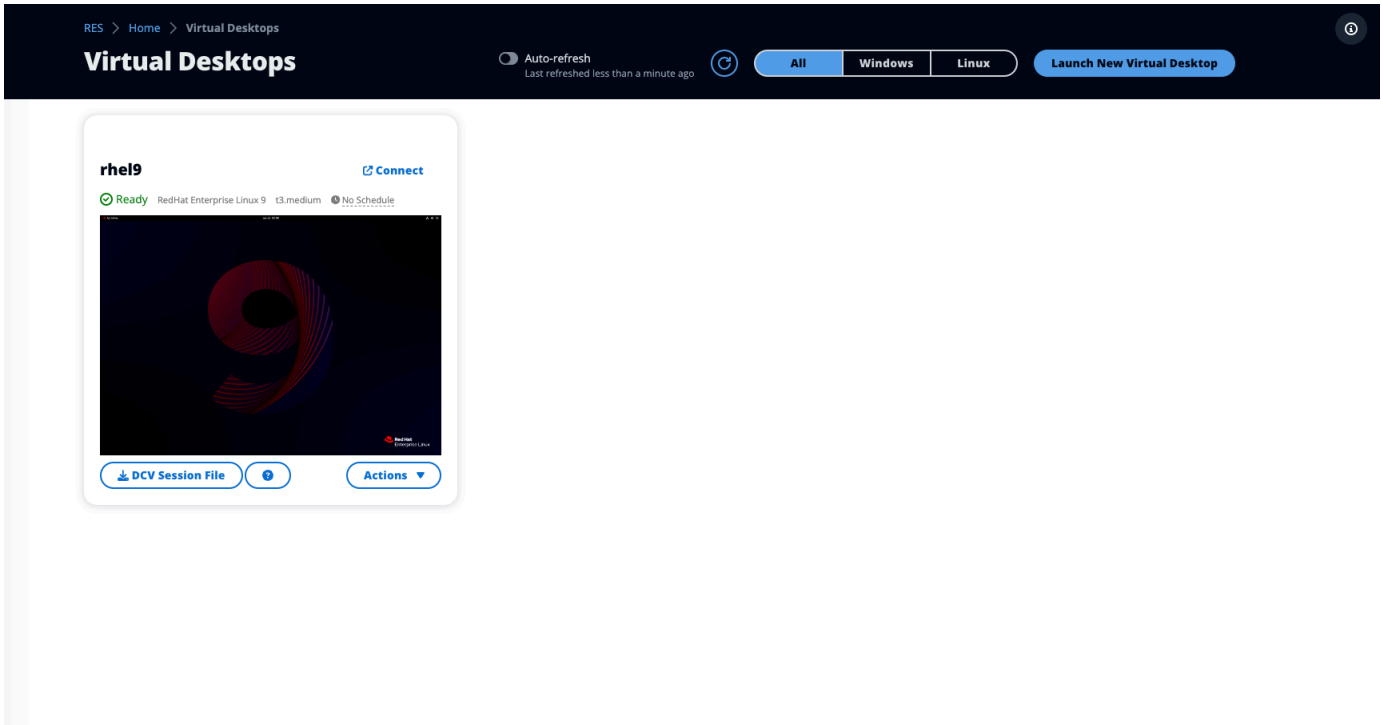
根據預設，虛擬桌面會排程在週六和週日自動停止。您可以使用從個別桌面上的動作功能表存取的排程視窗來調整個別桌面的排程，如下一節所示。若要進一步了解，在整個環境中設定預設排程請參閱該章節。桌面也可以在閒置時停止，以協助降低成本。請參閱 虛擬桌面界面自動停止 以進一步了解 VDI Autostop。

主題

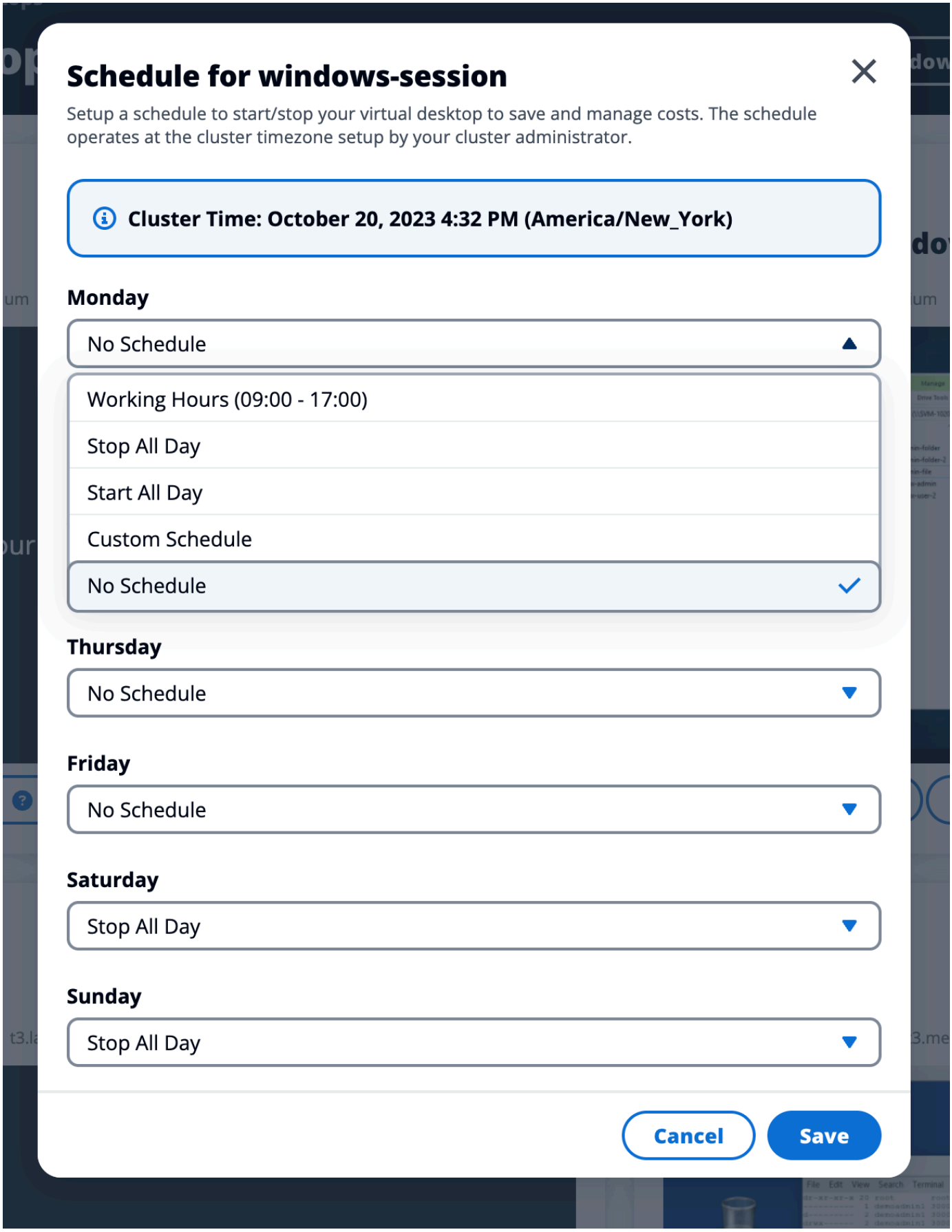
- 設定個別桌面排程
- 在整個環境中設定預設排程

設定個別桌面排程

1. 選擇動作。



2. 選擇 Schedule (排程)。
3. 設定您每天的排程。
4. 選擇儲存。


Schedule for windows-session
Setup a schedule to start/stop your virtual desktop to save and manage costs. The schedule operates at the cluster timezone setup by your cluster administrator.
Cluster Time: October 20, 2023 4:32 PM (America/New_York)
Monday
No Schedule
Working Hours (09:00 - 17:00)
Stop All Day
Start All Day
Custom Schedule
No Schedule
Thursday
No Schedule
Friday
No Schedule
Saturday
Stop All Day
Sunday
Stop All Day
Cancel
Save

在整個環境中設定預設排程

可以在 DynamoDB 中更新預設排程：

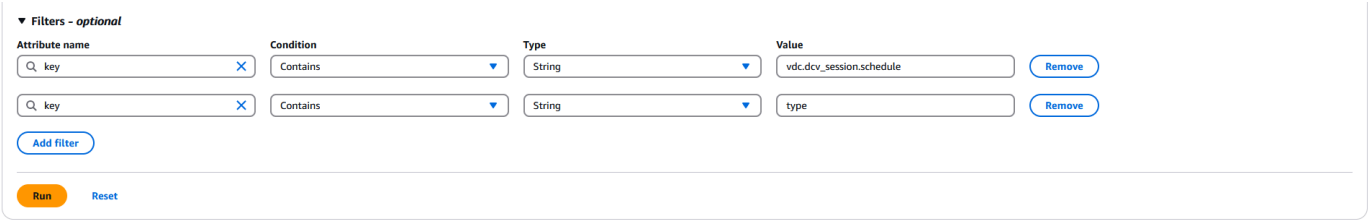
1. 搜尋您環境的叢集設定資料表：`<env-name>.cluster-settings`。
2. 選取探索項目。
3. 在篩選條件下，輸入下列兩個篩選條件：

   篩選條件 1

   - 屬性名稱 = **key**
   - 條件 = **Contains**
   - 類型 = **String**
   - 值 = **vdc.dcv_session.schedule**

   篩選條件 2

   - 屬性名稱 = **key**
   - 條件 = **Contains**
   - 類型 = **String**
   - 值 = **type**



   這會顯示七個項目，這些項目代表表單 每天的預設排程類型`vdc.dcv_session.schedule.<day>.type`。有效值為：

   - `NO_SCHEDULE`
   - `STOP_ALL_DAY`
   - `START_ALL_DAY`
   - `WORKING_HOURS`

- CUSTOM_SCHEDULE

4. 如果CUSTOM_SCHEDULE已設定 ，您必須提供自訂的開始和停止時間。若要這樣做，請在叢集設定資料表中使用下列篩選條件：

   - 屬性名稱 = **key**
   - 條件 = **Contains**
   - 類型 = **String**
   - 值 = **vdc.dcv_session.schedule**

5. 搜尋您要設定自訂排程之個別天數的格式化為 `vdc.dcv_session.schedule.<day>.start_up_time`和 `vdc.dcv_session.schedule.<day>.shut_down_time` 的項目。在項目內，刪除 Null 項目，並將其取代為字串項目，如下所示：

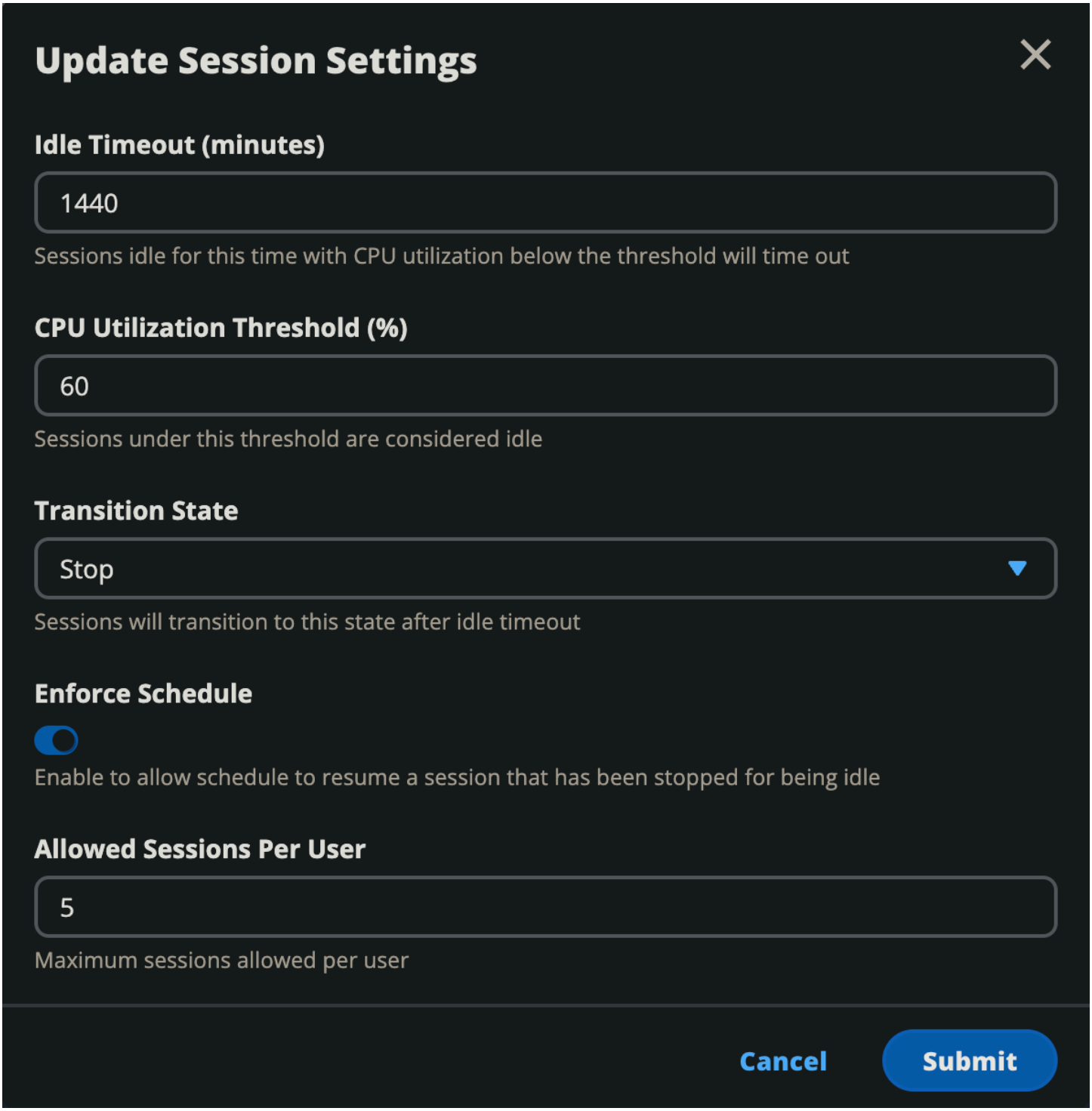
   - 屬性名稱 = **value**
   - 值 = ***<The time>***
   - 類型 = **String**

   時間值必須使用 24 小時制格式化為 XX：XX。例如，上午 9 點為 09：00，下午 5 點為 17：00。輸入的時間一律對應至 RES 環境部署所在 AWS 區域的當地時間。

虛擬桌面界面自動停止

管理員可以設定 設定，以允許停止或終止閒置VDIs。有 4 個可設定的設定：

1. 閒置逾時：CPU 使用率低於閾值的目前工作階段閒置將會逾時。
2. CPU 使用率閾值：沒有互動且低於此閾值的工作階段會被視為閒置。如果將此設為 0，則工作階段永遠不會被視為閒置。
3. 轉換狀態：閒置逾時後，工作階段將轉換為此狀態（已停止或終止）。
4. 強制執行排程：如果選取此選項，則已因閒置而停止的工作階段可由其每日排程繼續。

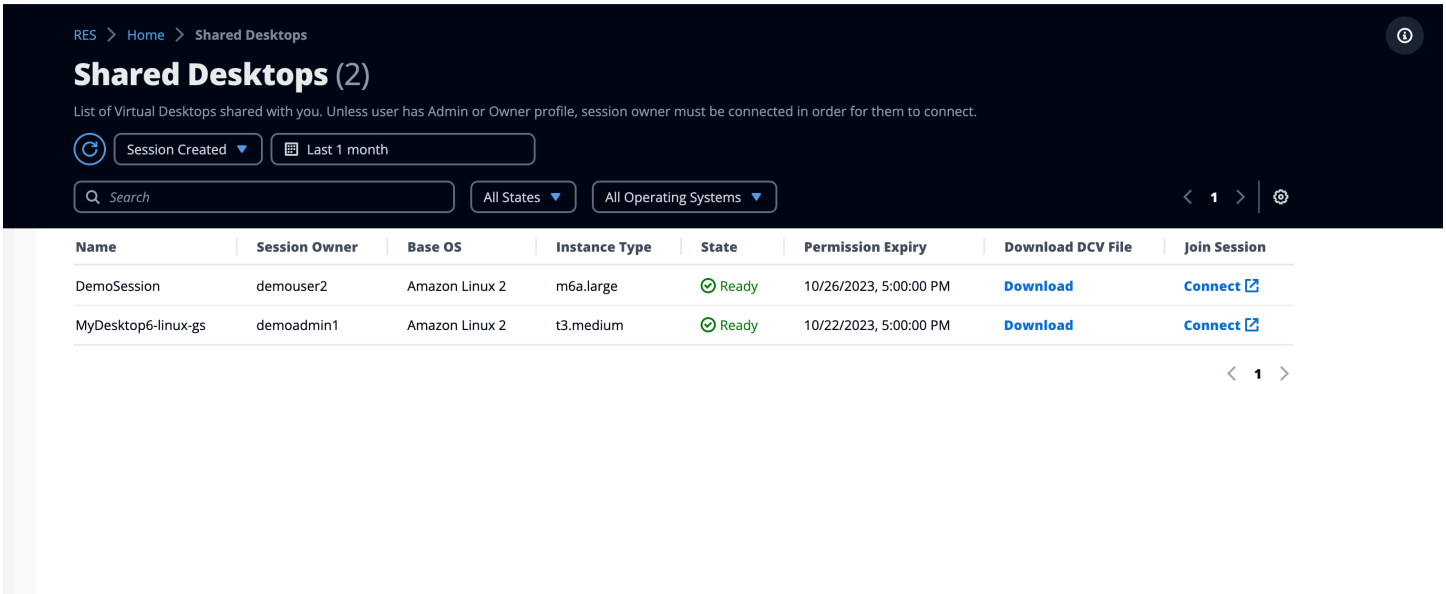


這些設定會顯示在伺服器索引標籤下的桌面設定頁面上。根據您的需求更新設定後，請按一下提交以儲存設定。新工作階段將使用更新的設定，但請注意，現有工作階段仍會使用啟動時擁有的設定。

逾時後，工作階段會根據其組態終止或轉換為 STOPPED_IDLE 狀態。使用者將能夠從 UI 啟動STOPPED_IDLE工作階段。

共用桌面

在共用桌面上，您可以看到已與您共用的桌面。若要連線至桌面，除非您是管理員或擁有者，否則工作階段擁有者也必須連線。



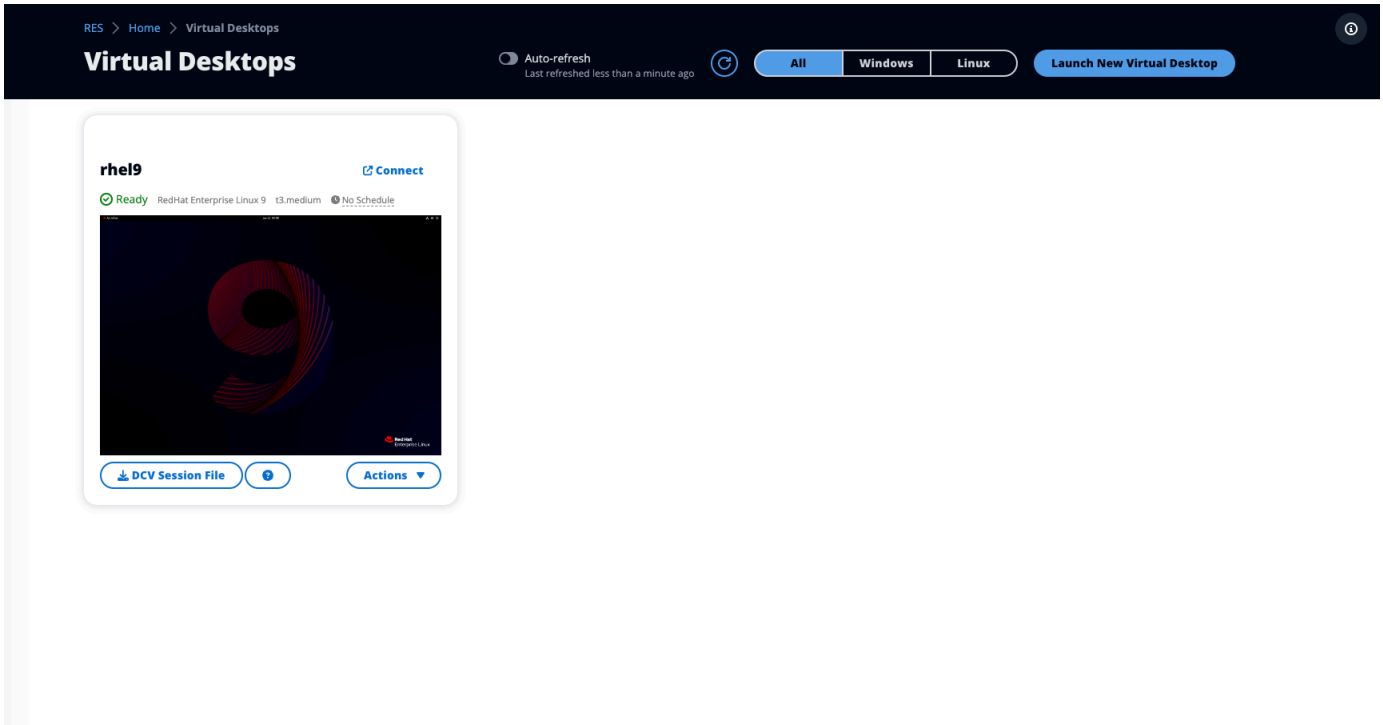
共用工作階段時，您可以設定協作者的許可。例如，您可以將唯讀存取權授予與您合作的團隊成員。

主題

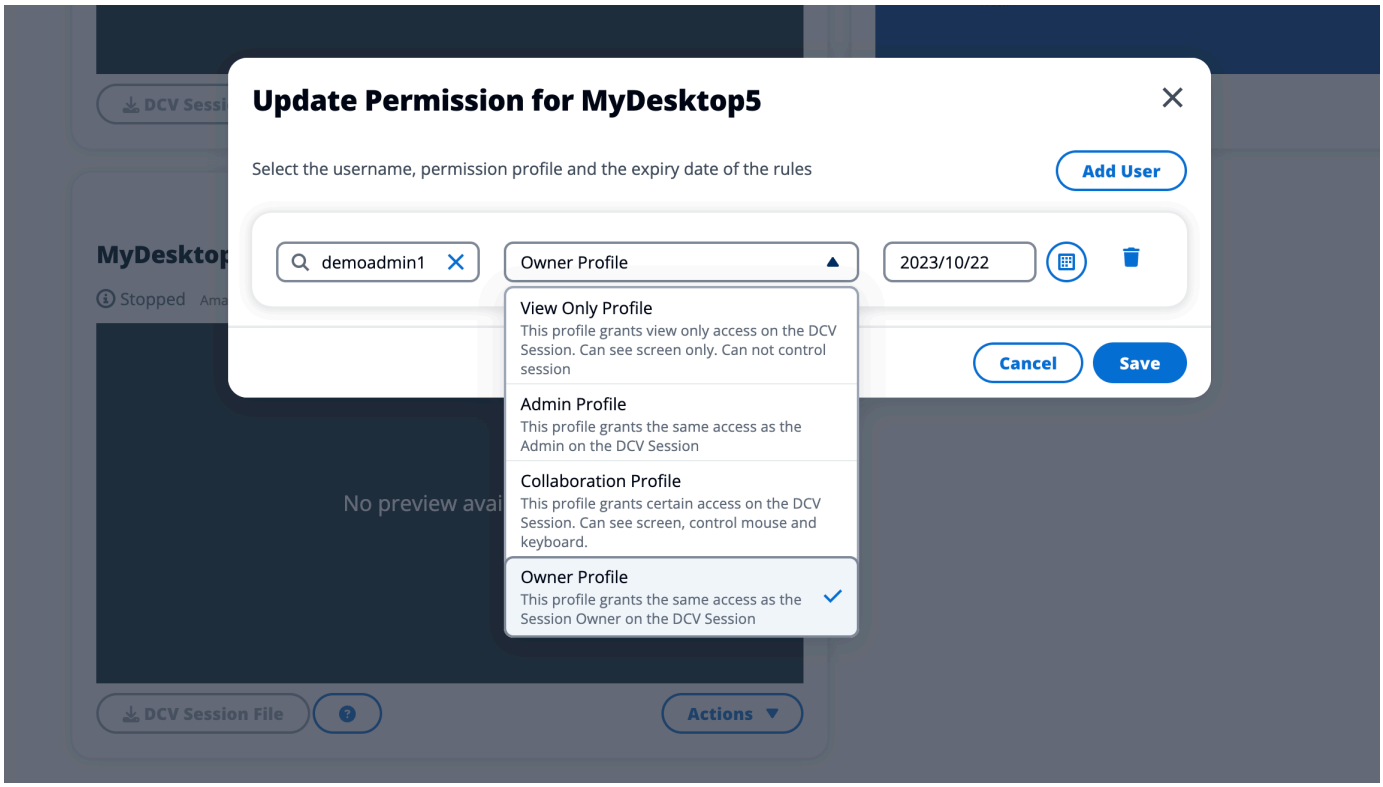
- 共用桌面
- 存取共用桌面

共用桌面

1. 在桌面工作階段中，選擇動作。



2. 選取工作階段許可。
3. 選取使用者和許可層級。您也可以設定過期時間。
4. 選擇儲存。



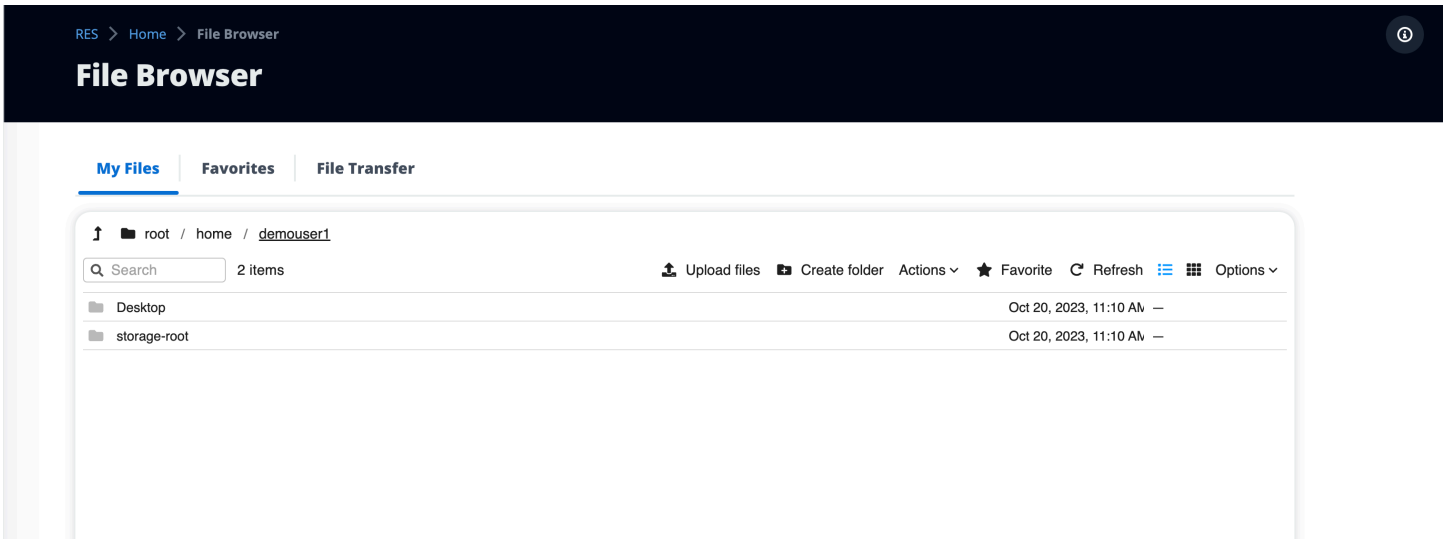
如需許可的詳細資訊，請參閱 the section called “許可政策”。

存取共用桌面

從共用桌面，您可以檢視與您共用的桌面並連線至執行個體。您可以透過 Web 瀏覽器或 DCV 加入。若要連線，請遵循 中的指示存取您的桌面。

檔案瀏覽器

檔案瀏覽器可讓您透過 Web 入口網站存取全域共用 EFS 檔案系統。您可以管理您在基礎檔案系統上具有存取許可的所有可用檔案。這是 Linux 虛擬桌面共用的相同檔案系統。更新虛擬桌面上的檔案與透過終端機或 Web 檔案瀏覽器更新檔案相同。

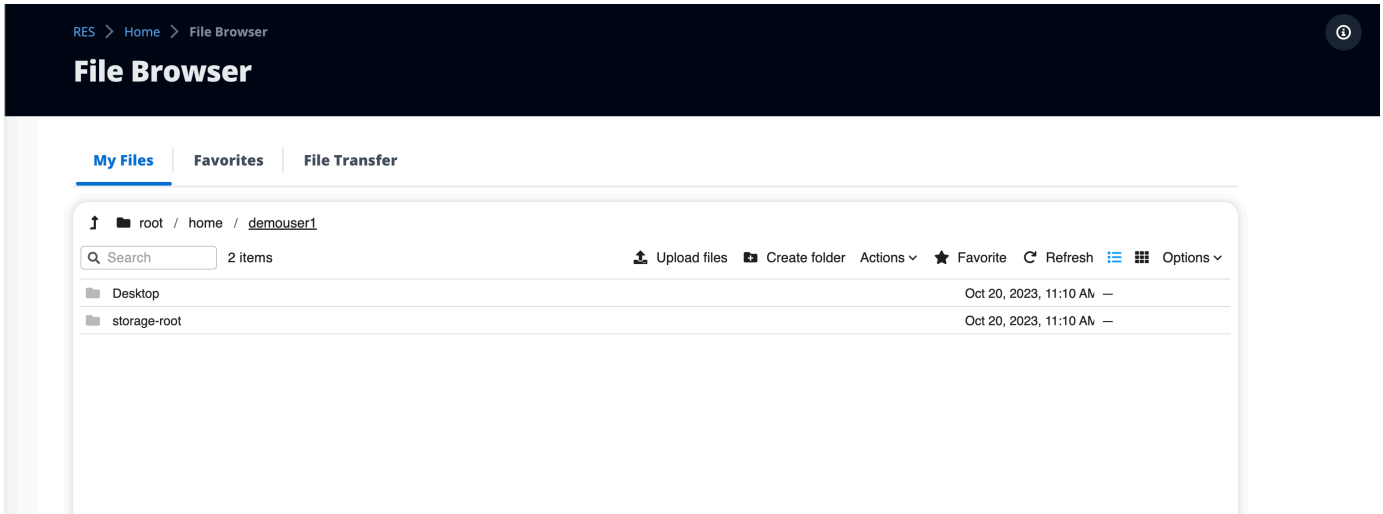


主題

- 上傳檔案 (s)
- 刪除 檔案 (s)
- 管理我的最愛
- 編輯檔案
- 傳輸檔案

上傳檔案 (s)

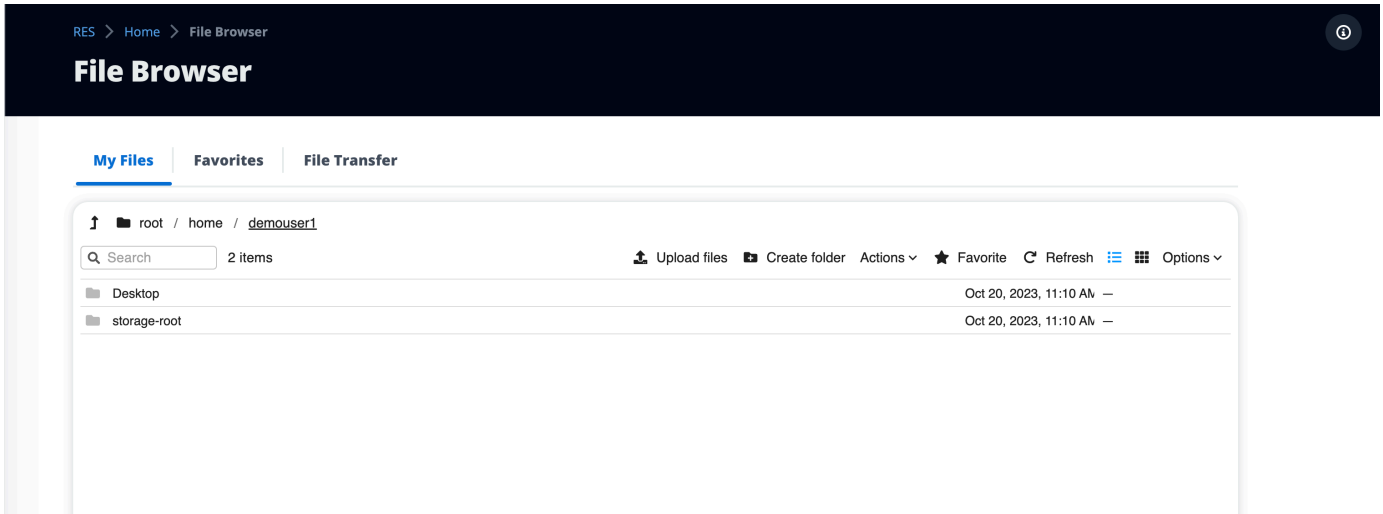
1. 選擇上傳檔案。



2. 捨棄檔案或瀏覽要上傳的檔案。
3. 選擇上傳 (n) 檔案。

刪除 檔案 (s)

1. 選取您要刪除的檔案（檔案）。



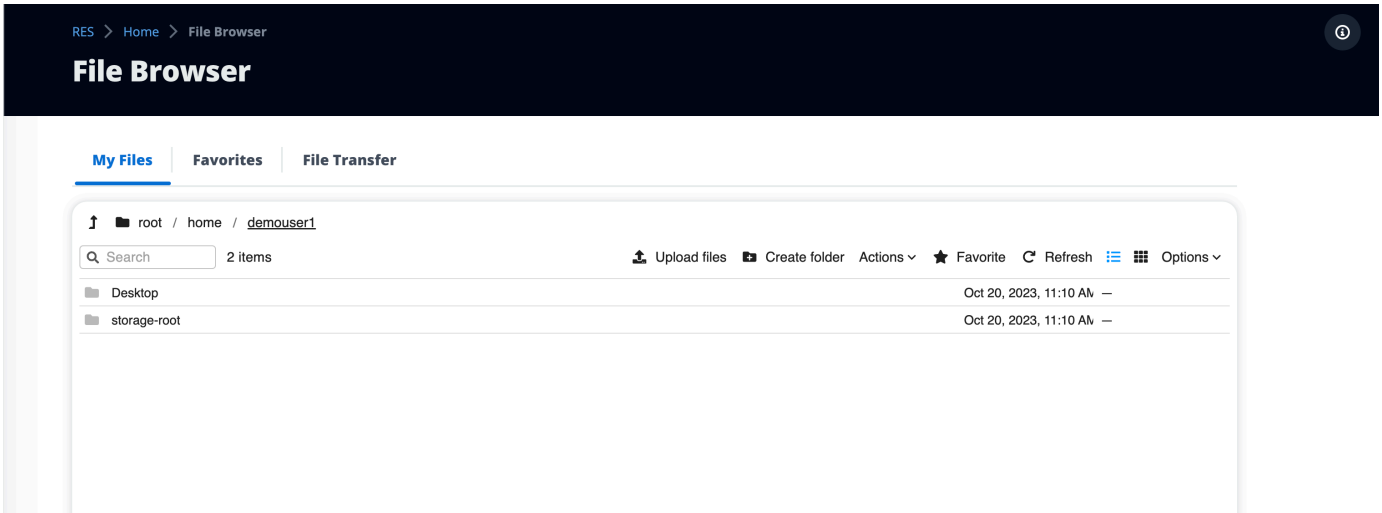
2. 選擇動作。
3. 選取刪除檔案。

或者，您也可以在任何檔案或資料夾上按一下滑鼠右鍵，然後選取刪除檔案。

管理我的最愛

若要鎖定重要的檔案和資料夾，您可以將它們新增至我的最愛。

1. 選取檔案或資料夾。



2. 選擇我的最愛。

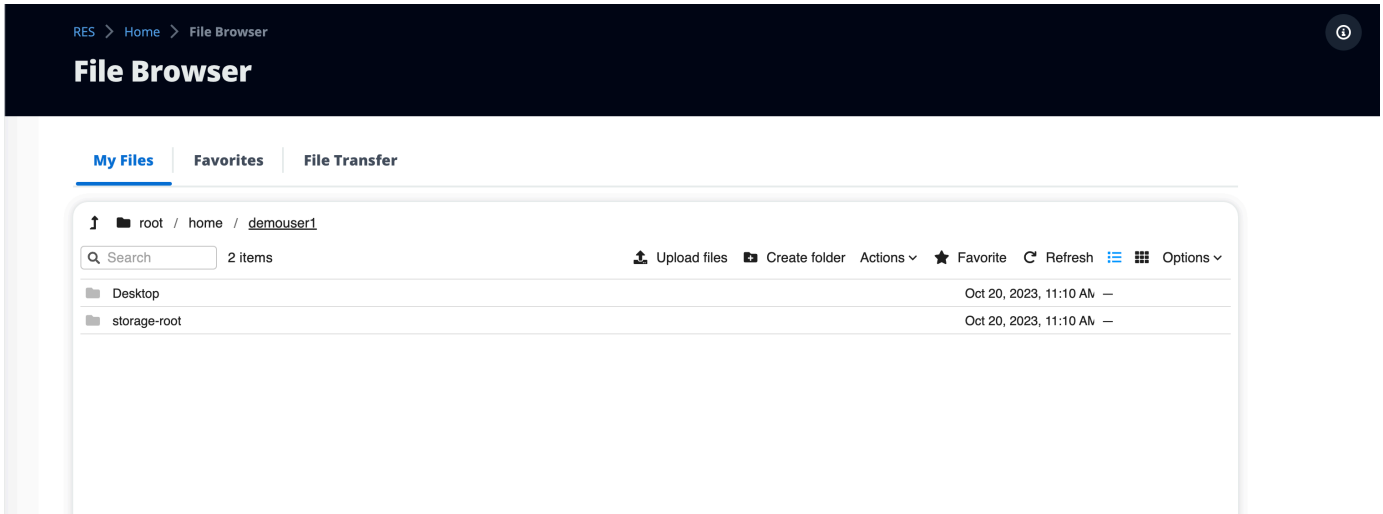
或者，您可以在任何檔案或資料夾上按一下滑鼠右鍵，然後選取我的最愛。

> **Note**
> 我的最愛會儲存到本機瀏覽器。如果您變更瀏覽器或清除快取，您將需要重新鎖定我的最愛。

編輯檔案

您可以在 Web 入口網站中編輯文字型檔案的內容。

1. 選取您要更新的檔案。模態將會開啟，其中包含檔案的內容。



2. 進行更新，然後選擇儲存。

傳輸檔案

使用檔案傳輸來使用外部檔案傳輸應用程式來傳輸檔案。您可以從下列應用程式中選取 ，並依照畫面上的指示傳輸檔案。

- FileZilla (Windows、MacOS、Linux)
- WinSCP (Windows)
- AWS Transfer for FTP (Amazon EFS)

RES > Home > File Browser

File Browser

My Files | Favorites | File Transfer

File Transfer Method

We recommend using below methods to transfer large files to your RES environment. Select an option below.

- (●) **FileZilla** — Available for download on Windows, MacOS and Linux
- ( ) **WinSCP** — Available for download on Windows Only
- ( ) **AWS Transfer** — Your RES environment must be using Amazon EFS to use AWS Transfer

FileZilla

Step 1: Download FileZilla

- Download FileZilla (MacOS)
- Download FileZilla (Windows)
- Download FileZilla (Linux)

Step 2: Download Key File

Download Key File [*.pem] (MacOS / Linux) | Download Key File [*.ppk] (Windows)

Step 3: Configure FileZilla

Open FileZilla and select **File > Site Manager** to create a new Site using below options:

Host	**Port**
Protocol SFTP	**Logon Type** Key File
User demouser3	**Key File** /path/to/key-file (downloaded in Step 2)

Save the settings and click **Connect**

Step 4: Connect and transfer file to FileZilla

During your first connection, you will be asked whether or not you want to trust . Check "Always Trust this Host" and Click "Ok".

Once connected, simply drag & drop to upload/download files.

疑難排解

本節包含如何監控系統以及如何疑難排解可能發生之特定問題的相關資訊。

主題

- 一般偵錯和監控
- 發行 RunBooks
- 已知問題

詳細內容：

- 一般偵錯和監控
  - 有用的日誌和事件資訊來源
    - 尋找環境變數的位置
    - 環境 Amazon EC2 執行個體上的日誌檔案
    - CloudFormation 堆疊
    - 因問題而發生系統故障，並由 Amazon EC2 Auto Scaling 群組活動反映
  - 典型的 Amazon EC2 主控台外觀
    - 基礎設施主機
    - 基礎設施主機和虛擬桌面
    - 處於終止狀態的主機
    - 實用的 Active Directory (AD) 相關命令以供參考
  - Windows DCV 偵錯
  - 尋找 Amazon DCV 版本資訊
- 發行 RunBooks
  - 安裝問題
    - 我想要在安裝 RES 之後設定自訂網域
    - AWS CloudFormation 堆疊無法建立 ，並顯示訊息「WaitCondition 收到失敗的訊息。Error：States.TaskFailed"
    - 堆疊建立成功後 AWS CloudFormation 未收到電子郵件通知
    - 執行個體循環或處於失敗狀態的 vdc-controller
    - 由於相依物件錯誤，環境 CloudFormation 堆疊無法刪除

- 環境建立期間 CIDR 區塊參數發生錯誤
- 環境建立期間的 CloudFormation 堆疊建立失敗
- 使用 AdDomainAdminNode CREATE_FAILED 建立外部資源（示範）堆疊失敗
- 身分管理問題
  - 我未獲得執行 iam:PassRole 的授權
  - 我想要允許 AWS 帳戶外的人員存取我的 Research and Engineering Studio on AWS 資源
  - 登入環境時，我立即返回登入頁面
  - 嘗試登入時發生「找不到使用者」錯誤
  - 在 Active Directory 中新增的使用者，但 RES 中遺失
  - 建立工作階段時無法使用使用者
  - CloudWatch cluster-manager 日誌中超出大小限制的錯誤
- 儲存
  - 我透過 RES 建立檔案系統，但未掛載在 VDI 主機上
  - 我透過 RES 加入檔案系統，但未掛載在 VDI 主機上
  - 我無法從 VDI 主機讀取/寫入
    - 處理使用案例的許可範例
  - 我從 RES 建立 Amazon FSx for NetApp ONTAP，但未加入我的網域
- 快照
  - 快照的狀態為失敗
  - 快照無法套用至表示無法匯入資料表的日誌。
- 基礎設施
  - 沒有運作狀態良好執行個體的負載平衡器目標群組
- 啟動虛擬桌面
  - Windows 虛擬桌面的登入帳戶設定為管理員
  - 使用外部資源 CertificateRenewalNode 時，憑證過期
  - 先前運作中的虛擬桌面無法再成功連線
  - 我只能啟動 5 個虛擬桌面
  - 桌面 Windows 連線嘗試失敗，並顯示「連線已關閉。傳輸錯誤"
  - VDIs停滯在佈建狀態

  - 啟動後，VDIs會進入錯誤狀態

- 虛擬桌面元件
  - Amazon EC2 執行個體在主控台中重複顯示已終止
  - vdc-controller 執行個體正在循環中，因為無法加入 AD/eVDI 模組，顯示 API 運作狀態檢查失敗
  - 編輯軟體堆疊以新增專案時，專案不會出現在下拉式清單中
  - cluster-manager Amazon CloudWatch 日誌顯示「<user-home-init> 帳戶尚無法使用。正在等待使用者同步」（其中帳戶是使用者名稱）
  - Windows 桌面登入嘗試時顯示「您的帳戶已停用。請洽詢您的管理員"
  - 外部/客戶 AD 組態的 DHCP 選項問題
  - Firefox 錯誤 MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING
- Env 刪除
  - res-xxx-cluster 堆疊處於「DELETE_FAILED」狀態，無法手動刪除，因為「角色無效或無法擔任」錯誤
  - 收集日誌
  - 下載 VDI 日誌
  - 從 Linux EC2 執行個體下載日誌
  - 從 Windows EC2 執行個體下載日誌
  - 收集 WaitCondition 錯誤的 ECS 日誌
- 示範環境
  - 處理身分提供者的身分驗證請求時發生示範環境登入錯誤
  - 示範堆疊 keycloak 無法運作
- 2024.x 已知問題
  - 2024.x 已知問題
    - (2024.12 和 2024.12.01) 註冊新 Cognito 使用者時發生 Regex 失敗
    - (2024.12.01 及更早版本） 使用自訂網域連線至 VDI 時出現無效的憑證錯誤
    - (2024.12 和 2024.12.01) Active Directory 使用者無法 SSH 到堡壘主機
    - (2024.10) 針對部署在隔離 VPCs 中的 RES 環境，VDI 自動停止中斷
    - (2024.10 及更早版本） 無法啟動 VDI for Graphic 增強型執行個體類型
    - (2024.08) 準備基礎設施 AMI 失敗
    - (2024.08) 虛擬桌面無法掛載具有根儲存貯體 ARN 和自訂字首的讀取/寫入 Amazon S3 儲存貯體
    - (2024.06) 當 AD 群組名稱包含空格時，套用快照失敗

- (2024.06 及更早版本） AD 同步期間未同步至 RES 的群組成員
- (2024.06 及更早版本） CVE-2024-6387、RegreSSHion、RHEL9 和 Ubuntu VDIs中的安全漏洞
- (2024.04-2024.04.02) 提供未連接至 VDI 執行個體角色的 IAM 許可界限
- (2024.04.02 及更早版本） ap-southeast-2 （雪梨） 中的 Windows NVIDIA 執行個體無法啟動
- (2024.04 和 2024.04.01) GovCloud 中的 RES 刪除失敗
- (2024.04 - 2024.04.02) 重新啟動時，Linux 虛擬桌面可能卡在「繼續」狀態
- (2024.04.02 及更早版本） 無法同步 SAMAccountName 屬性包含大寫字母或特殊字元的 AD 使用者
- (2024.04.02 及更早版本） 用於存取堡壘主機的私有金鑰無效

一般偵錯和監控

本節包含可在 RES 中找到的資訊。

- 有用的日誌和事件資訊來源
  - 尋找環境變數的位置
  - 環境 Amazon EC2 執行個體上的日誌檔案
  - CloudFormation 堆疊
  - 因問題而發生系統故障，並由 Amazon EC2 Auto Scaling 群組活動反映
- 典型的 Amazon EC2 主控台外觀
  - 基礎設施主機
  - 基礎設施主機和虛擬桌面
  - 處於終止狀態的主機
  - 實用的 Active Directory (AD) 相關命令以供參考
- Windows DCV 偵錯
- 尋找 Amazon DCV 版本資訊

有用的日誌和事件資訊來源

保留了各種資訊來源，可用於故障診斷和監控用途。

尋找環境變數的位置

根據預設，您可以在下列位置找到環境變數，例如工作階段擁有者使用者名稱：

- Linux：`/etc/environment`
- Windows：`C:\Users\Administrator\RES\Bootstrap\virtual-desktop-host-windows\environment_variables.json`

環境 Amazon EC2 執行個體上的日誌檔案

日誌檔案存在於 RES 使用的 Amazon EC2 執行個體上。SSM Session Manager 可用來開啟執行個體的工作階段，以檢查這些檔案。

在叢集管理員和 vdc-controller 等基礎設施執行個體上，可在下列位置找到應用程式和其他日誌。

- /opt/idea/app/logs/application.log
- /root/bootstrap/logs/
- /var/log/
- /var/log/sssd/
- /var/log/messages
- /var/log/user-data.log
- /var/log/cloud-init.log
- /var/log/cloud-init-output.log

在 Linux 虛擬桌面上，以下包含有用的日誌檔案

- /var/log/dcv/
- /root/bootstrap/logs/userdata.log
- /var/log/messages

在 Windows 虛擬桌面執行個體上，日誌位於

- PS C：\ProgramData\nice\dcv\log
- PS C：\ProgramData\nice\DCVSessionManagerAgent\log

在 Windows 上，某些應用程式記錄可在以下位置找到：

- PS C：\Program Files\NICE\DCV\Server\bin

在 Windows 上，您可以在以下位置找到 NICE DCV 憑證檔案：

- C：\Windows\System32\config\systemprofile\AppData\Local\NICE\dcv\

Amazon CloudWatch 日誌群組

Amazon EC2 和 AWS Lambda 運算資源會將資訊記錄到 Amazon CloudWatch Log Groups。其中的日誌項目可在疑難排解潛在問題或取得一般資訊時提供有用的資訊。

這些群組的名稱如下：

- `/aws/lambda/<envname>-/ - lambda related`
- `/<envname>/`
  - `cluster-manager/ - main infrastructure host`
  - `vdc/ - virtual desktop related`
    - `dcv-broker/ - desktop related`
    - `dcv-connection-gateway/ - desktop related`
    - `controller/ - main desktop controller host`
    - `dcv-session/ - desktop session related`

檢查日誌群組時，使用如下的大寫和小寫字串進行篩選會很有幫助。這只會輸出包含記下字串的訊息。

```
?"ERROR" ?"error"
```

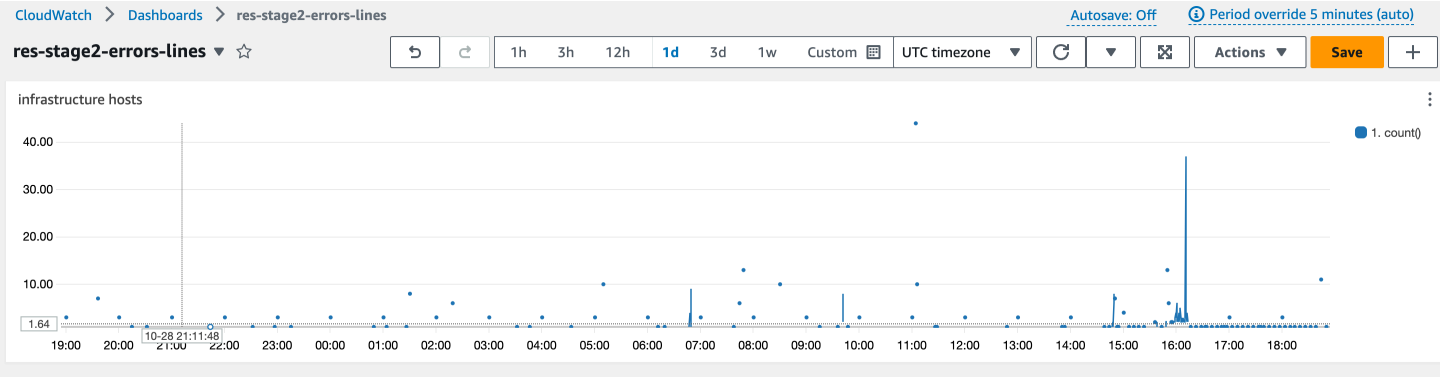
監控問題的另一個方法是建立 Amazon CloudWatch Dashboards，其中包含顯示感興趣資料的小工具。

例如，建立一個小工具，計算字串錯誤和 ERROR 的出現，並將其繪製為行。此方法可讓您更輕鬆地偵測潛在問題的發生，或指出已發生模式變更的趨勢。

以下是 基礎設施主機的範例。若要使用此功能，請將查詢行串連，並以適當的值取代 `<envname>`和 `<region>` 屬性。

```
{
    "widgets": [
        {
            "type": "log",
            "x": 0,
            "y": 0,
            "width": 24,
            "height": 6,
            "properties": {
                "query": "SOURCE '/<envname>/vdc/controller' |
                    SOURCE '/<envname>/cluster-manager' |
                    SOURCE '/<envname>/vdc/dcv-broker' |
                   SOURCE '/<envname>/vdc/dcv-connection-gateway' |
                    fields @timestamp, @message, @logStream, @log\n|
                    filter @message like /(?i)(error|ERROR)/\n|
                    sort @timestamp desc|
                    stats count() by bin(30s)",
                "region": "<region>",
                "title": "infrastructure hosts",
                "view": "timeSeries",
                "stacked": false
            }
        }
    ]
}
```

儀表板的範例可能會出現如下：



CloudFormation 堆疊

在環境建立期間建立的 CloudFormation 堆疊包含與環境組態相關聯的資源、事件和輸出資訊。

對於每個堆疊，如需堆疊的相關資訊，可以參考事件、資源和輸出索引標籤。

RES 堆疊：

- <envname>-bootstrap
- <envname>-cluster
- <envname>-metrics
- <envname>-directoryservice
- <envname>-identity-provider
- <envname>-shared-storage
- <envname>-cluster-manager
- <envname>-vdc
- <envname>-bastion-host

示範環境堆疊（如果您正在部署示範環境，但沒有這些外部資源可用，您可以使用 AWS 高效能運算配方來產生示範環境的資源。）

- <envname>
- <envname>-Networking
- <envname>-DirectoryService
- <envname>-Storage
- <envname>-WindowsManagementHost

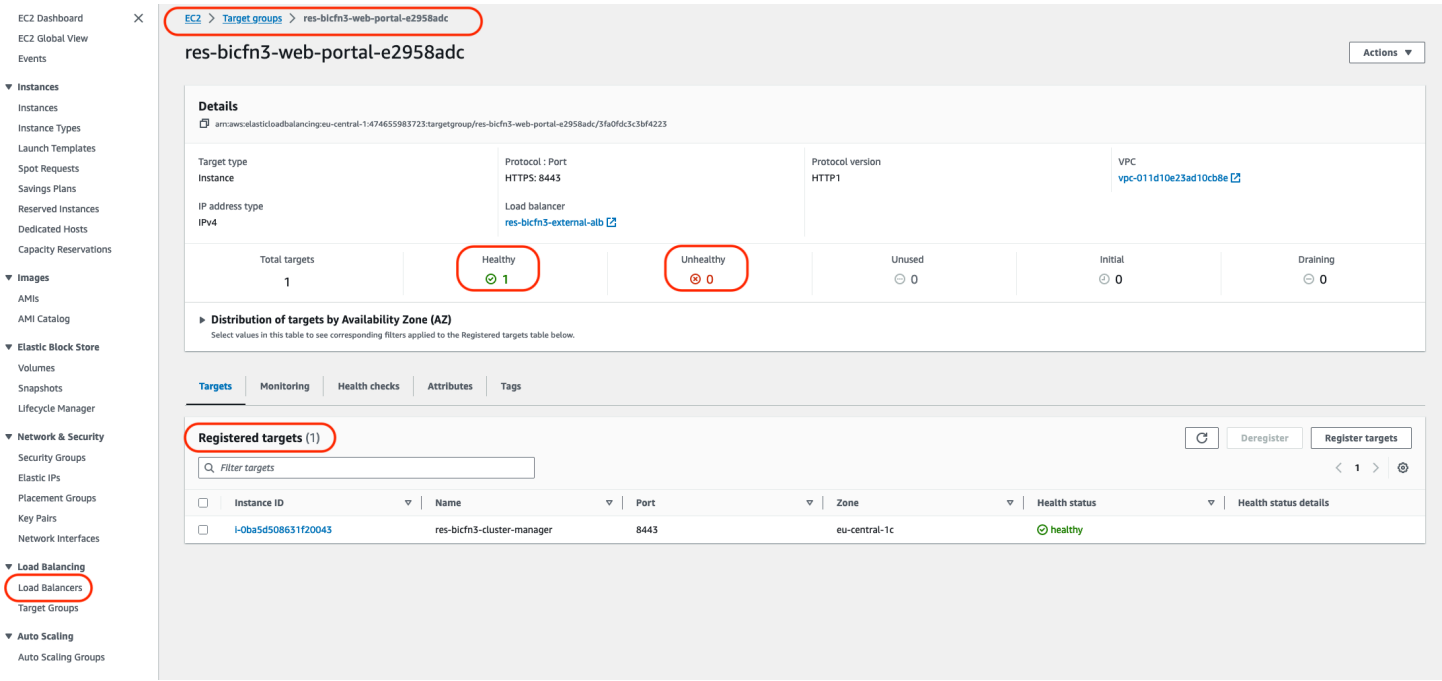
因問題而發生系統故障，並由 Amazon EC2 Auto Scaling 群組活動反映

如果 RES UIs 指出伺服器錯誤，原因可能是應用程式軟體或其他問題。

每個基礎設施 Amazon EC2 執行個體自動擴展群組 (ASGs) 都包含一個活動索引標籤，可用於偵測執行個體的擴展活動。如果 UI 頁面注意到任何錯誤或無法存取，請檢查 Amazon EC2 主控台是否有多個終止的執行個體，並檢查 Auto Scaling 群組活動索引標籤是否有相關的 ASG，以判斷 Amazon EC2 執行個體是否正在循環。

如果是這樣，請使用執行個體的相關 Amazon CloudWatch 日誌群組來判斷是否記錄錯誤，這可能表示問題的原因。您也可以使用 SSM 工作階段主控台開啟該類型執行中執行個體的工作階段，並檢查執行個體上的日誌檔案以判斷原因，再將執行個體標示為運作狀態不佳，並由 ASG 終止。

如果發生此問題，ASG 主控台可能會顯示類似下列的活動。

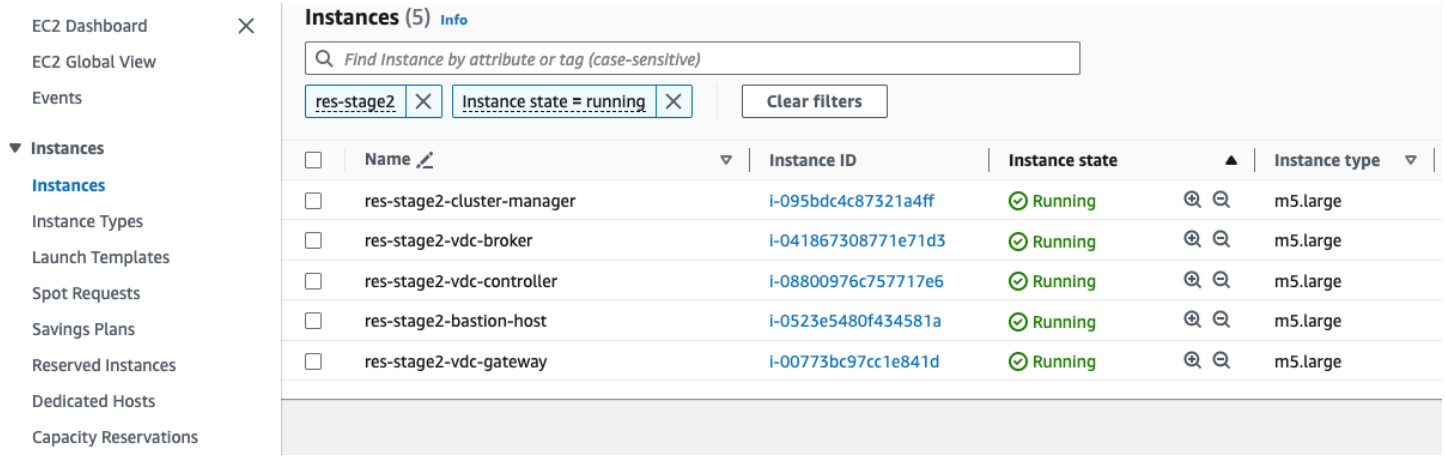


典型的 Amazon EC2 主控台外觀

本節包含在各種狀態下操作的系統螢幕擷取畫面。

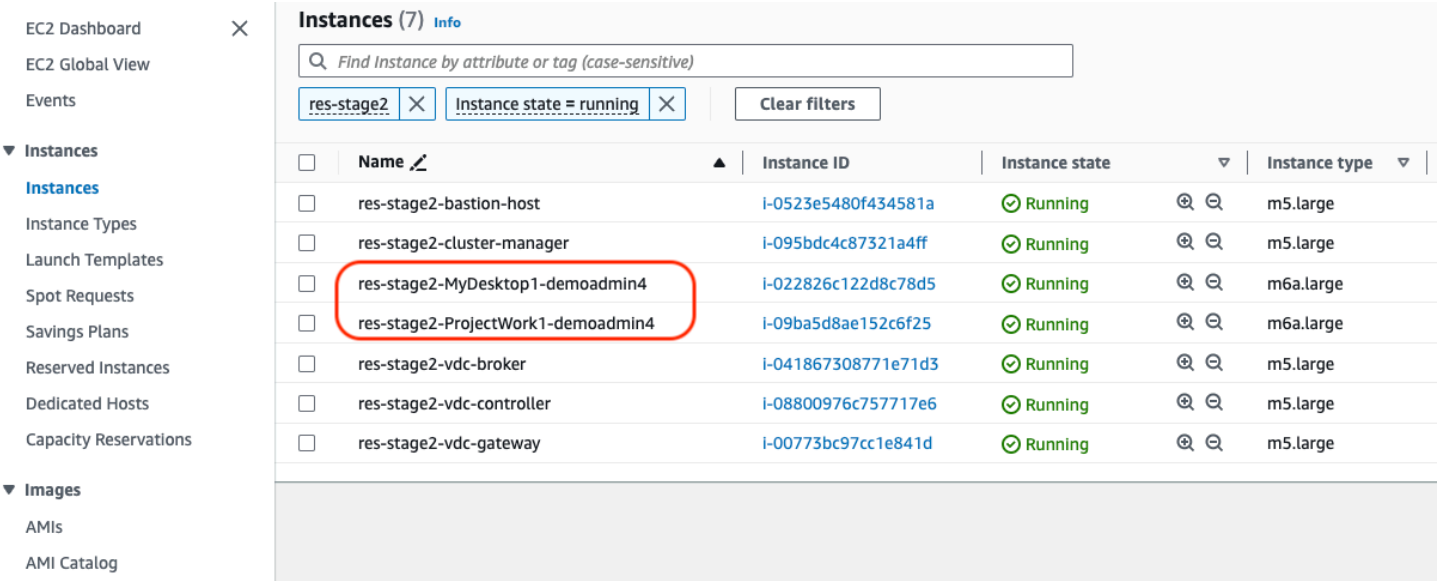
基礎設施主機

當沒有桌面執行時，Amazon EC2 主控台通常看起來類似以下內容。顯示的執行個體是 RES 基礎設施 Amazon EC2 主機。執行個體名稱中的字首是 RES 環境名稱。



基礎設施主機和虛擬桌面

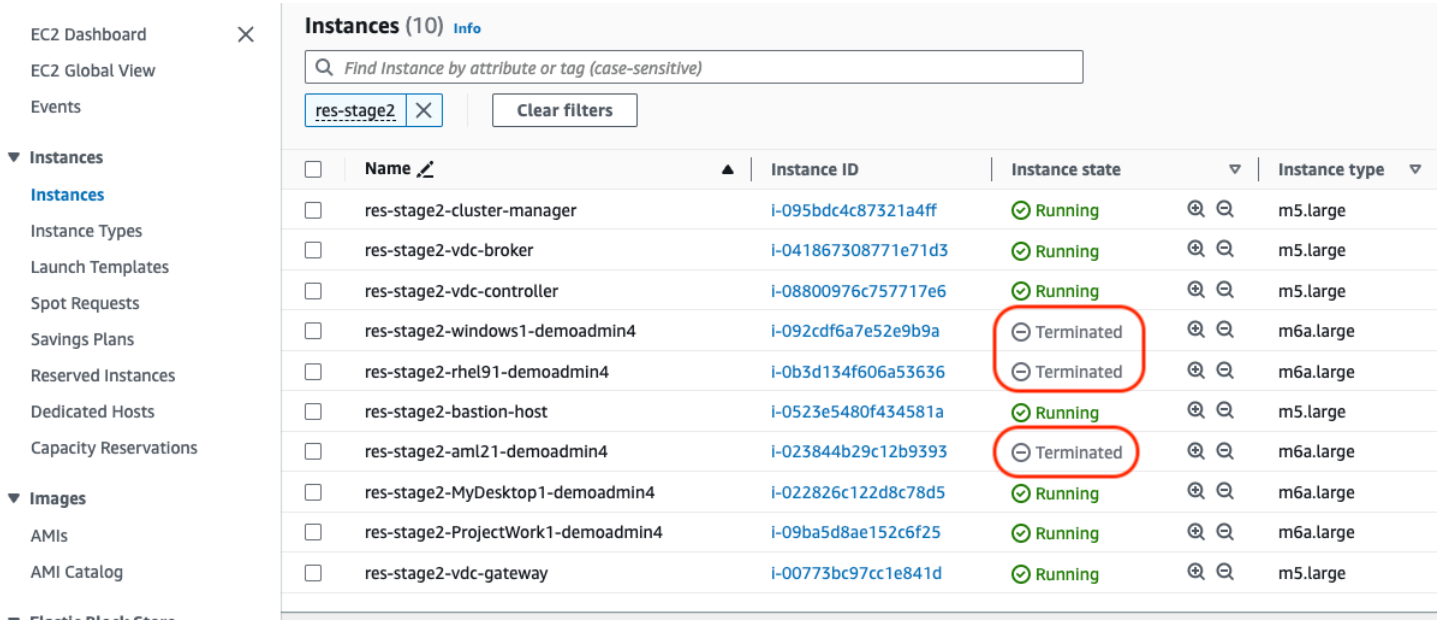
在 Amazon EC2 主控台中，當虛擬桌面執行時，它們看起來與以下內容類似。在此情況下，虛擬桌面會以紅色標示。執行個體名稱的尾碼是建立桌面的使用者。中間的名稱是啟動時設定的工作階段名稱，可以是預設的「MyDesktop」或使用者設定的名稱。



處於終止狀態的主機

當 Amazon EC2 主控台顯示已終止的執行個體時，它們通常是已終止的桌面主機。如果主控台包含處於終止狀態的基礎設施主機，特別是有多個相同類型的主機，這可能表示系統正在進行中。

下圖顯示已終止的桌面執行個體。



實用的 Active Directory (AD) 相關命令以供參考

以下是可在基礎設施主機上輸入的 ldap 相關命令範例，以檢視 AD 組態相關資訊。使用的網域和其他參數應該反映在環境建立時輸入的參數。

```
ldapsearch "(cn=AWS Delegated Add Workstations To Domain Users)" -x -h corp.res.com
    -b "DC=corp,DC=res,DC=com" -D "CN=Admin,OU=Users,OU=CORP,DC=corp,DC=res,DC=com"
    -w <password>

ldapsearch "(&(objectClass=group))" -x -h corp.res.com
    -b "DC=corp,DC=res,DC=com" -D "CN=Admin,OU=Users,OU=CORP,DC=corp,DC=res,DC=com"
    -w <password>
```

Windows DCV 偵錯

在 Windows 桌面上，您可以使用下列方式列出與其相關聯的工作階段：

```
PS C:\Windows\System32\config\systemprofile\AppData\Local\NICE\dcv> & 'C:\Program Files
\NICE\DCV\Server\bin\dcv.exe'list-sessions
Session: 'a7953489-9dbf-492b-8135-7709dccc4cab' (owner:admin2 type:console
 name:windows1)
```

尋找 Amazon DCV 版本資訊

Amazon DCV 用於虛擬桌面工作階段。AWS Amazon DCV。下列範例示範如何判斷已安裝的 DCV 軟體版本。

Linux

```
[root@ip-10-3-157-194 ~]# /usr/bin/dcv version

Amazon DCV 2023.0 (r14852)
Copyright (C) 2010-2023 NICE s.r.l.
All rights reserved.

This product is protected by copyright and
licenses restricting use, copying, distribution, and decompilation.
```

Windows

```
PS C:\Windows\System32\config\systemprofile\AppData\Local\NICE\dcv> & 'C:\Program Files
\NICE\DCV\Server\bin\dcv.exe' version

Amazon DCV 2023.0 (r15065)
Copyright (C) 2010-2023 NICE s.r.l.
All rights reserved.

This product is protected by copyright and
licenses restricting use, copying, distribution, and decompilation.
```

發行 RunBooks

下一節包含可能發生的問題、如何偵測問題，以及如何解決問題的建議。

- 安裝問題
  - 我想要在安裝 RES 之後設定自訂網域
  - AWS CloudFormation 堆疊無法建立 ，並顯示訊息「WaitCondition 收到失敗的訊息。Error：States.TaskFailed"
  - 堆疊建立成功後 AWS CloudFormation 未收到電子郵件通知
  - 執行個體循環或處於失敗狀態的 vdc-controller
  - 由於相依物件錯誤，環境 CloudFormation 堆疊無法刪除
  - 環境建立期間 CIDR 區塊參數發生錯誤
  - 環境建立期間的 CloudFormation 堆疊建立失敗
  - 使用 AdDomainAdminNode CREATE_FAILED 建立外部資源 （示範） 堆疊失敗
- 身分管理問題
  - 我未獲得執行 iam:PassRole 的授權
  - 我想要允許 AWS 帳戶外的人員存取我的 Research and Engineering Studio on AWS 資源
  - 登入環境時，我立即返回登入頁面
  - 嘗試登入時發生「找不到使用者」錯誤
  - 在 Active Directory 中新增的使用者，但 RES 中遺失
  - 建立工作階段時無法使用使用者
  - CloudWatch cluster-manager 日誌中超出大小限制的錯誤
- 儲存
  - 我透過 RES 建立檔案系統，但未掛載在 VDI 主機上

- 我透過 RES 加入檔案系統，但未掛載在 VDI 主機上
- 我無法從 VDI 主機讀取/寫入
  - 處理使用案例的許可範例
- 我從 RES 建立 Amazon FSx for NetApp ONTAP，但未加入我的網域
- 快照
  - 快照的狀態為失敗
  - 快照無法套用至表示無法匯入資料表的日誌。
- 基礎設施
  - 沒有運作狀態良好執行個體的負載平衡器目標群組
- 啟動虛擬桌面
  - Windows 虛擬桌面的登入帳戶設定為管理員
  - 使用外部資源 CertificateRenewalNode 時，憑證過期
  - 先前運作中的虛擬桌面無法再成功連線
  - 我只能啟動 5 個虛擬桌面
  - 桌面 Windows 連線嘗試失敗，並顯示「連線已關閉。傳輸錯誤"
  - VDIs停滯在佈建狀態
  - 啟動後，VDIs會進入錯誤狀態
- 虛擬桌面元件
  - Amazon EC2 執行個體在主控台中重複顯示已終止
  - vdc-controller 執行個體正在循環中，因為無法加入 AD/eVDI 模組，顯示 API 運作狀態檢查失敗
  - 編輯軟體堆疊以新增專案時，專案不會出現在下拉式清單中
  - cluster-manager Amazon CloudWatch 日誌顯示「<user-home-init> 帳戶尚無法使用。正在等待使用者同步」（其中帳戶是使用者名稱）
  - Windows 桌面登入嘗試時顯示「您的帳戶已停用。請洽詢您的管理員"
  - 外部/客戶 AD 組態的 DHCP 選項問題
  - Firefox 錯誤 MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING
- Env 刪除
  - res-xxx-cluster 堆疊處於「DELETE_FAILED」狀態，無法手動刪除，因為「角色無效或無法擔任」錯誤
  - 收集日誌
  - 下載 VDI 日誌

- 從 Linux EC2 執行個體下載日誌
- 從 Windows EC2 執行個體下載日誌
- 收集 WaitCondition 錯誤的 ECS 日誌
- 示範環境
  - 處理身分提供者的身分驗證請求時發生示範環境登入錯誤
  - 示範堆疊 keycloak 無法運作

安裝問題

主題

- 我想要在安裝 RES 之後設定自訂網域
- AWS CloudFormation 堆疊無法建立 ，並顯示訊息「WaitCondition 收到失敗的訊息。Error：States.TaskFailed"
- 堆疊建立成功後 AWS CloudFormation 未收到電子郵件通知
- 執行個體循環或處於失敗狀態的 vdc-controller
- 由於相依物件錯誤，環境 CloudFormation 堆疊無法刪除
- 環境建立期間 CIDR 區塊參數發生錯誤
- 環境建立期間的 CloudFormation 堆疊建立失敗
- 使用 AdDomainAdminNode CREATE_FAILED 建立外部資源 （ 示範 ） 堆疊失敗

.....

我想要在安裝 RES 之後設定自訂網域

> **Note**
>
> 先決條件：您必須先將 Certificate 和 PrivateKey 內容存放在 Secrets Manager 秘密中，才能執行這些步驟。

將憑證新增至 Web 用戶端

1. 更新連接至外部-alb 負載平衡器接聽程式的憑證：

a. 導覽至 AWS 主控台中 EC2 > Load Balancing > Load Balancer 下的 RES 外部負載平衡器。

b. 搜尋遵循命名慣例 的負載平衡器`<env-name>-external-alb`。

c. 檢查連接至負載平衡器的接聽程式。

d. 更新具有與新憑證詳細資訊連接之預設 SSL/TLS 憑證的接聽程式。

e. 儲存您的變更。

2. 在叢集設定資料表中：

   a. 在 DynamoDB -> Tables -> 中尋找叢集設定資料表`<env-name>.cluster-settings`。

   b. 前往探索項目並依屬性篩選 – 名稱 "key"、類型 "string"、條件 "contains" 和值 "external_alb"。

   c. `cluster.load_balancers.external_alb.certificates.provided` 設定為 True。

   d. 更新 的 值`cluster.load_balancers.external_alb.certificates.custom_dns_name`。這是 Web 使用者介面的自訂網域名稱。

   e. 更新 的 值`cluster.load_balancers.external_alb.certificates.acm_certificate_arn`。這是存放在 Amazon Certificate Manager (ACM) 中對應憑證的 Amazon Resource Name (ARN)。

3. 更新您為 Web 用戶端建立的對應 Route53 子網域記錄，以指向外部 alb 負載平衡器的 DNS 名稱`<env-name>-external-alb`。

4. 如果已在環境中設定 SSO，請使用與 RES Web 入口網站中環境管理 > 身分管理 > 單一登入 > 狀態 > 編輯按鈕中最初使用的相同輸入來重新設定 SSO。

將憑證新增至 VDIs

1. 將下列標籤新增至秘密，授予 RES 應用程式對秘密執行 GetSecret 操作的許可：

   - `res:EnvironmentName`：`<env-name>`
   - `res:ModuleName`：`virtual-desktop-controller`

2. 在叢集設定資料表中：

   a. 在 DynamoDB -> Tables -> 中尋找叢集設定資料表`<env-name>.cluster-settings`。

   b. 前往探索項目並依屬性篩選 – 名稱 "key"、類型 "string"、條件 "contains" 和值 "dcv_connection_gateway"。

c. `vdc.dcv_connection_gateway.certificate.provided` 設定為 True。

d. 更新 的值`vdc.dcv_connection_gateway.certificate.custom_dns_name`。這是 VDI 存取的自訂網域名稱。

e. 更新 的值`vdc.dcv_connection_gateway.certificate.certificate_secret_arn`。這是存放憑證內容之秘密的 ARN。

f. 更新 的值`vdc.dcv_connection_gateway.certificate.private_key_secret_arn`。這是存放私有金鑰內容之秘密的 ARN。

3. 更新用於閘道執行個體的啟動範本：

   a. 在 AWS 主控台的 EC2 > Auto Scaling > Auto Scaling 群組下開啟 Auto Scaling 群組。

   b. 選取對應至 RES 環境的閘道自動擴展群組。名稱遵循命名慣例 `<env-name>-vdc-gateway-asg`。

   c. 在詳細資訊區段中尋找並開啟啟動範本。

   d. 在詳細資訊 > 動作 > 選擇修改範本 （建立新版本）。

   e. 向下捲動至進階詳細資訊。

   f. 捲動至最底部，至使用者資料。

   g. 尋找單字 `CERTIFICATE_SECRET_ARN`和 `PRIVATE_KEY_SECRET_ARN`。使用提供給存放憑證 （請參閱步驟 2.ARNs 更新這些值。

   h. 確定 Auto Scaling 群組已設定為使用最近建立的啟動範本版本 （從 Auto Scaling 群組頁面）。

4. 更新您為虛擬桌面建立的對應 Route53 子網域記錄，以指向外部 nlb 負載平衡器的 DNS 名稱：`<env-name>-external-nlb`。

5. 終止現有的 dcv-gateway 執行個體： `<env-name>-vdc-gateway`並等待新的執行個體啟動。

.....

AWS CloudFormation 堆疊無法建立 ，並顯示訊息「WaitCondition 收到失敗的訊息。Error：States.TaskFailed"

若要識別問題，請檢查名為 的 Amazon CloudWatch 日誌群組`<stack-name>-InstallerTasksCreateTaskDefCreateContainerLogGroup<nonce>-<nonce>`。如果有多個

具有相同名稱的日誌群組，請檢查第一個可用的日誌群組。日誌中的錯誤訊息將提供有關問題的詳細資訊。

> **Note**
>
> 確認參數值沒有空格。

.....

堆疊建立成功後 AWS CloudFormation 未收到電子郵件通知

如果在成功建立 AWS CloudFormation 堆疊後未收到電子郵件邀請，請確認下列事項：

1. 確認電子郵件地址參數輸入正確。

   如果電子郵件地址不正確或無法存取，請刪除並重新部署 Research and Engineering Studio 環境。

2. 檢查 Amazon EC2 主控台是否有循環執行個體的證據。

   如果有字`<envname>`首顯示為已終止的 Amazon EC2 執行個體，然後以新的執行個體取代，則網路或 Active Directory 組態可能會出現問題。

3. 如果您已部署 AWS 高效能運算配方來建立外部資源，請確認堆疊已建立 VPC、私有和公有子網路，以及其他選取的參數。

   如果任何參數不正確，您可能需要刪除並重新部署 RES 環境。如需詳細資訊，請參閱解除安裝產品。

4. 如果您使用自己的外部資源部署產品，請確認聯網和 Active Directory 符合預期的組態。

   確認基礎設施執行個體成功加入 Active Directory 至關重要。嘗試 中的步驟the section called “執行個體循環或處於失敗狀態的 vdc-controller”來解決問題。

.....

執行個體循環或處於失敗狀態的 vdc-controller

此問題最可能的原因是資源無法連線或加入 Active Directory (Active Directory)。

若要驗證問題：

1. 從命令列，在 vdc-controller 的執行中執行個體上使用 SSM 啟動工作階段。
2. 執行 `sudo su -`。
3. 執行 `systemctl status sssd`。

如果狀態為非作用中、失敗或您在日誌中看到錯誤，則執行個體無法加入 Active Directory。

```
[root@ip-                ]# systemctl status sssd
● sssd.service - System Security Services Daemon
   Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2023-11-14 12:12:19 UTC; 1 weeks 0 days ago
 Main PID: 31248 (sssd)
   CGroup: /system.slice/sssd.service
           ├─31248 /usr/sbin/sssd -i --logger=files
           ├─31249 /usr/libexec/sssd/sssd_be --domain corp.res.com --uid 0 --gid 0 --logger=files
           ├─31251 /usr/libexec/sssd/sssd_nss --uid 0 --gid 0 --logger=files
           └─31252 /usr/libexec/sssd/sssd_pam --uid 0 --gid 0 --logger=files

Nov 21 15:27:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:27:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 2
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:42:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 2
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 1
Nov 21 15:57:19 ip-10-3-144-194.ec2.internal sssd_be[31249]: GSSAPI client step 2
```

Might see “inactive”/“failed” here

Might see errors highlighted in RED here

SSM 錯誤日誌

若要解決問題：

- 從相同的命令列執行個體執行 `cat /root/bootstrap/logs/userdata.log` 以調查日誌。

此問題可能有三種可能的根本原因之一。

根本原因 1：輸入的 ldap 連線詳細資訊不正確

檢閱日誌。如果您看到下列重複多次，則執行個體無法加入 Active Directory。

```
+ local AD_AUTHORIZATION_ENTRY=
+ [[ -z '' ]]
+ [[ 0 -le 180 ]]
+ local SLEEP_TIME=34
+ log_info '(0 of 180) waiting for AD authorization, retrying in 34 seconds ...'
++ date '+%Y-%m-%d %H:%M:%S,%3N'
```

```
+ echo '[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization,
 retrying in 34 seconds ...'
[2024-01-16 22:02:19,802] [INFO] (0 of 180) waiting for AD authorization, retrying in
 34 seconds ...
+ sleep 34
+ (( ATTEMPT_COUNT++ ))
```

1. 確認 RES 堆疊建立期間已正確輸入下列項目的參數值。
   - directoryservice.ldap_connection_uri
   - directoryservice.ldap_base
   - directoryservice.users.ou
   - directoryservice.groups.ou
   - directoryservice.sudoers.ou
   - directoryservice. computers.ou
   - directoryservice.name
2. 更新 DynamoDB 資料表中的任何不正確值。資料表可在 DynamoDB 主控台的資料表下找到。資料表名稱應為 `<stack name>.cluster-settings`。
3. 更新資料表後，請刪除目前執行環境執行個體的 cluster-manager 和 vdc-controller。自動擴展將使用來自 DynamoDB 資料表的最新值啟動新執行個體。

根本原因 2：輸入的 ServiceAccount 使用者名稱不正確

如果日誌傳回 `Insufficient permissions to modify computer account`，則在堆疊建立期間輸入的 ServiceAccount 名稱可能不正確。

1. 從 AWS 主控台開啟 Secrets Manager。
2. 搜尋 `directoryserviceServiceAccountUsername`。秘密應為 `<stack name>-directoryservice-ServiceAccountUsername`。
3. 開啟秘密以檢視詳細資訊頁面。在秘密值下，選擇擷取秘密值，然後選擇純文字。
4. 如果該值已更新，請刪除目前執行環境的 cluster-manager 和 vdc-controller 執行個體。自動擴展將使用 Secrets Manager 的最新值啟動新執行個體。

根本原因 3：輸入的 ServiceAccount 密碼不正確

如果日誌顯示 `Invalid credentials`，則在堆疊建立期間輸入的 ServiceAccount 密碼可能不正確。

1. 從 AWS 主控台開啟 Secrets Manager。
2. 搜尋 `directoryserviceServiceAccountPassword`。秘密應為 `<stack name>-directoryservice-ServiceAccountPassword`。
3. 開啟秘密以檢視詳細資訊頁面。在秘密值下，選擇擷取秘密值，然後選擇純文字。
4. 如果您忘記密碼，或不確定輸入的密碼是否正確，您可以在 Active Directory 和 Secrets Manager 中重設密碼。
   a. 若要在 中重設密碼 AWS Managed Microsoft AD：
      i. 開啟 AWS 主控台並前往 AWS Directory Service。
      ii. 選取 RES 目錄的目錄 ID，然後選擇動作。
      iii. 選取重設使用者密碼。
      iv. 輸入 ServiceAccount 使用者名稱。
      v. 輸入新密碼，然後選擇重設密碼。
   b. 若要在 Secrets Manager 中重設密碼：
      i. 開啟 AWS 主控台並前往 Secrets Manager。
      ii. 搜尋 `directoryserviceServiceAccountPassword`。秘密應為 `<stack name>-directoryservice-ServiceAccountPassword`。
      iii. 開啟秘密以檢視詳細資訊頁面。在秘密值下，選擇擷取秘密值，然後選擇純文字。
      iv. 選擇編輯。
      v. 為 ServiceAccount 使用者設定新密碼，然後選擇儲存。
5. 如果您更新了 值，請刪除目前執行環境的 cluster-manager 和 vdc-controller 執行個體。自動擴展將使用最新的值啟動新的執行個體。

.....

由於相依物件錯誤，環境 CloudFormation 堆疊無法刪除

如果 `<env-name>-vdc` CloudFormation 堆疊的刪除因相依物件錯誤而失敗，例如 `vdcdcvhostsecuritygroup`，這可能是因為使用主控台在 RES 建立的子網路或安全群組中啟動的 Amazon EC2 AWS 執行個體所致。

若要解決此問題，請尋找並終止以這種方式啟動的所有 Amazon EC2 執行個體。然後，您可以繼續刪除環境。

.....

環境建立期間 CIDR 區塊參數發生錯誤

建立環境時，回應狀態為 【FAILED】 的 CIDR 區塊參數會出現錯誤。

錯誤範例：

```
Failed to update cluster prefix list:
        An error occurred (InvalidParameterValue) when calling the
 ModifyManagedPrefixList operation:
        The specified CIDR (52.94.133.132/24) is not valid. For example, specify a CIDR
 in the following form: 10.0.0.0/16.
```

若要解決問題，預期的格式為 x.x.x.0/24 或 x.x.x.0/32。

.....

環境建立期間的 CloudFormation 堆疊建立失敗

建立環境涉及一系列的資源建立操作。在某些區域中，可能會發生容量問題，導致 CloudFormation 堆疊建立失敗。

如果發生這種情況，請刪除環境並重試建立。或者，您可以在不同的區域中重試建立。

.....

使用 AdDomainAdminNode CREATE_FAILED 建立外部資源 （示範） 堆疊失敗

如果示範環境堆疊建立失敗並出現下列錯誤，可能是因為執行個體啟動後佈建期間意外發生 Amazon EC2 修補。

```
AdDomainAdminNode CREATE_FAILED  Failed to receive 1 resource signal(s) within the
 specified duration
```

若要判斷失敗的原因：

1. 在 SSM 狀態管理員中，檢查是否已設定修補，以及是否已針對所有執行個體設定修補。
2. 在 SSM RunCommand/Automation 執行歷史記錄中，檢查修補相關 SSM 文件的執行是否與執行個體啟動一致。
3. 在環境 Amazon EC2 執行個體的日誌檔案中，檢閱本機執行個體日誌，以判斷執行個體是否在佈建期間重新啟動。

如果問題是由修補造成，請在啟動後至少 15 分鐘延遲 RES 執行個體的修補。

.....

身分管理問題

單一登入 (SSO) 和身分管理的大多數問題都是因為組態錯誤而發生。如需設定 SSO 組態的資訊，請參閱：

- the section called “使用 IAM Identity Center 設定 SSO”
- the section called “為 SSO 設定您的身分提供者”

若要疑難排解與身分管理相關的其他問題，請參閱下列疑難排解主題：

主題

- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 AWS 帳戶外的人員存取我的 Research and Engineering Studio on AWS 資源
- 登入環境時，我立即返回登入頁面
- 嘗試登入時發生「找不到使用者」錯誤
- 在 Active Directory 中新增的使用者，但 RES 中遺失
- 建立工作階段時無法使用使用者
- CloudWatch cluster-manager 日誌中超出大小限制的錯誤

.....

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 iam：PassRole 動作，您的政策必須更新，以允許您將角色傳遞給 RES。

有些 AWS 服務可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 marymajor 的 IAM 使用者嘗試使用主控台在 RES 中執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

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

在這種情況下，Mary 的政策必須更新，以允許她執行 iam：PassRole 動作。如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

.....

我想要允許 AWS 帳戶外的人員存取我的 Research and Engineering Studio on AWS 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：

- 若要了解如何在您擁有 AWS 的帳戶中提供資源的存取權，請參閱《IAM 使用者指南》中的為您擁有的另一個 AWS 帳戶中的 IAM 使用者提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方擁有 AWS 的帳戶。
- 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。

.....

登入環境時，我立即返回登入頁面

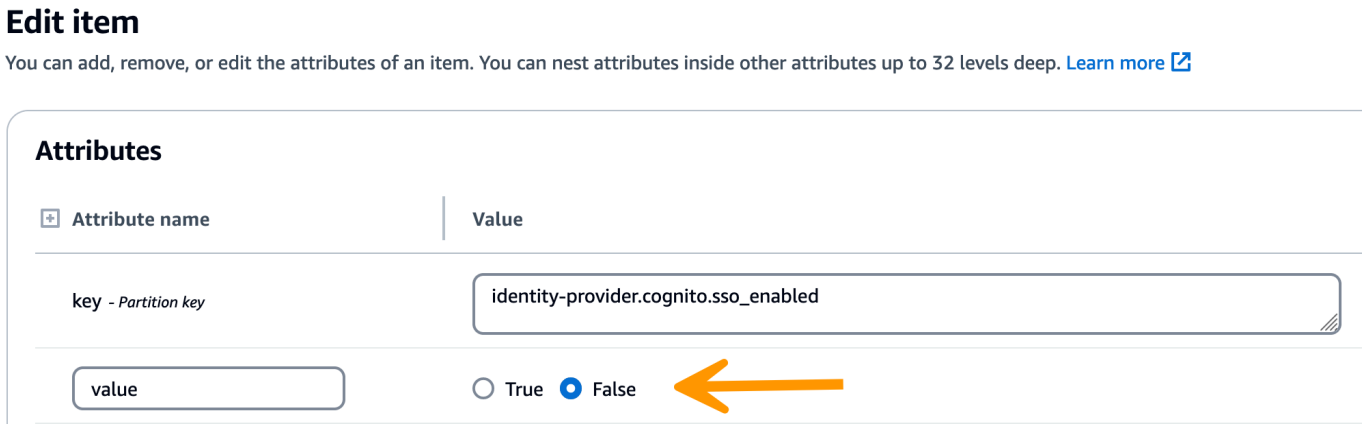
當您的 SSO 整合設定錯誤時，就會發生此問題。若要判斷問題，請檢查控制器執行個體日誌並檢閱組態設定是否有錯誤。

若要檢查日誌：

1. 開啟 CloudWatch 主控台。
2. 從日誌群組中，尋找名為 的群組/*<environment-name>*/cluster-manager。
3. 開啟日誌群組以搜尋日誌串流中的任何錯誤。

若要檢查組態設定：

1. 開啟 DynamoDB 主控台
2. 從資料表中，尋找名為 的資料表*<environment-name>*.cluster-settings。
3. 開啟資料表，然後選擇探索資料表項目。
4. 展開篩選條件區段，然後輸入下列變數：
   - 屬性名稱 – 索引鍵
   - 條件 – 包含
   - 值 – sso
5. 選擇執行。
6. 在傳回的字串中，驗證 SSO 組態值是否正確。如果不正確，請將 sso_enabled 金鑰的值變更為 False。



7. 返回 RES 使用者介面以重新設定 SSO。

.....

嘗試登入時發生「找不到使用者」錯誤

如果使用者嘗試登入 RES 介面時收到錯誤「找不到使用者」，且使用者出現在 Active Directory 中：

- 如果使用者不存在於 RES 中，且您最近將使用者新增至 AD
  - 使用者可能尚未同步到 RES。RES 每小時同步一次，因此您可能需要等待，並檢查使用者是否在下一次同步後新增。若要立即同步，請遵循中的步驟在 Active Directory 中新增的使用者，但 RES 中遺失。
- 如果使用者存在於 RES 中：
  1. 確定屬性映射已正確設定。如需詳細資訊，請參閱為單一登入 (SSO) 設定您的身分提供者。
  2. 確保 SAML 主旨和 SAML 電子郵件都對應到使用者的電子郵件地址。

.....

在 Active Directory 中新增的使用者，但 RES 中遺失

> **Note**
>
> 本節適用於 RES 2024.10 及更早版本。如需 RES 2024.12 及更新版本，請參閱 如何手動執行同步 (2024.12 和 2024.12.01 版) 。如需 RES 2025.03 及更新版本，請參閱 如何手動啟動或停止同步 (2025.03 及更新版本) 。

如果您已將使用者新增至 Active Directory，但在 RES 中缺少使用者，則需要觸發 AD 同步。AD 同步是由將 AD 項目匯入 RES 環境的 Lambda 函數每小時執行。有時候，在您新增使用者或群組之後，會延遲到下一個同步程序執行為止。您可以從 Amazon Simple Queue Service 手動啟動同步。

手動啟動同步程序：

1. 開啟 Amazon SQS 主控台。
2. 從佇列中，選取 `<environment-name>-cluster-manager-tasks.fifo`。
3. 選擇傳送及接收訊息。
4. 在訊息內文中，輸入：

```
{ "name": "adsync.sync-from-ad", "payload": {} }
```

5. 針對訊息群組 ID，輸入： **adsync.sync-from-ad**
6. 針對訊息重複資料刪除 ID，輸入隨機的英數字元字串。此項目必須與過去五分鐘內進行的所有呼叫不同，否則將會忽略請求。

.....

建立工作階段時無法使用使用者

如果您是建立工作階段的管理員，但發現在建立工作階段時無法使用 Active Directory 中的使用者，則使用者可能需要第一次登入。只能為作用中使用者建立工作階段。作用中使用者必須至少登入環境一次。

.....

CloudWatch cluster-manager 日誌中超出大小限制的錯誤

```
2023-10-31T18:03:12.942-07:00 ldap.SIZELIMIT_EXCEEDED: {'msgtype': 100, 'msgid': 11,
 'result': 4, 'desc': 'Size limit exceeded', 'ctrls': []}
```

如果您在 CloudWatch cluster-manager 日誌中收到此錯誤，ldap 搜尋可能已傳回太多使用者記錄。若要修正此問題，請提高 IDP 的 ldap 搜尋結果限制。

.....

儲存

主題

- 我透過 RES 建立檔案系統，但未掛載在 VDI 主機上
- 我透過 RES 加入檔案系統，但未掛載在 VDI 主機上
- 我無法從 VDI 主機讀取/寫入
- 我從 RES 建立 Amazon FSx for NetApp ONTAP，但未加入我的網域

.....

我透過 RES 建立檔案系統，但未掛載在 VDI 主機上

檔案系統必須處於「可用」狀態，才能由 VDI 主機掛載。請依照下列步驟，驗證檔案系統是否處於必要狀態。

Amazon EFS

1. 前往 Amazon EFS 主控台。
2. 檢查檔案系統狀態是否可用。
3. 如果檔案系統狀態不可用，請等待 再啟動 VDI 主機。

Amazon FSx ONTAP

1. 前往 Amazon FSx 主控台。
2. 檢查狀態是否可用。
3. 如果狀態不可用，請等待 再啟動 VDI 主機。

.....

我透過 RES 加入檔案系統，但未掛載在 VDI 主機上

在 RES 上加入的檔案系統應設定必要的安全群組規則，以允許 VDI 主機掛載檔案系統。由於這些檔案系統是在 RES 外部建立，RES 不會管理相關聯的安全群組規則。

與加入的檔案系統相關聯的安全群組應允許下列傳入流量：

- 來自 linux VDC 主機的 NFS 流量（連接埠：2049)
- 來自 Windows VDC 主機的 SMB 流量（連接埠：445)

.....

我無法從 VDI 主機讀取/寫入

ONTAP 支援磁碟區的 UNIX、NTFS 和 MIXED 安全樣式。安全樣式決定 ONTAP 用於控制資料存取的許可類型，以及哪些用戶端類型可以修改這些許可。

例如，如果磁碟區使用 UNIX 安全樣式，由於 ONTAP 的多協定性質，SMB 用戶端仍然可以存取資料（前提是他們正確驗證和授權）。不過，ONTAP 使用 UNIX 許可，只有 UNIX 用戶端可以使用原生工具修改。

處理使用案例的許可範例

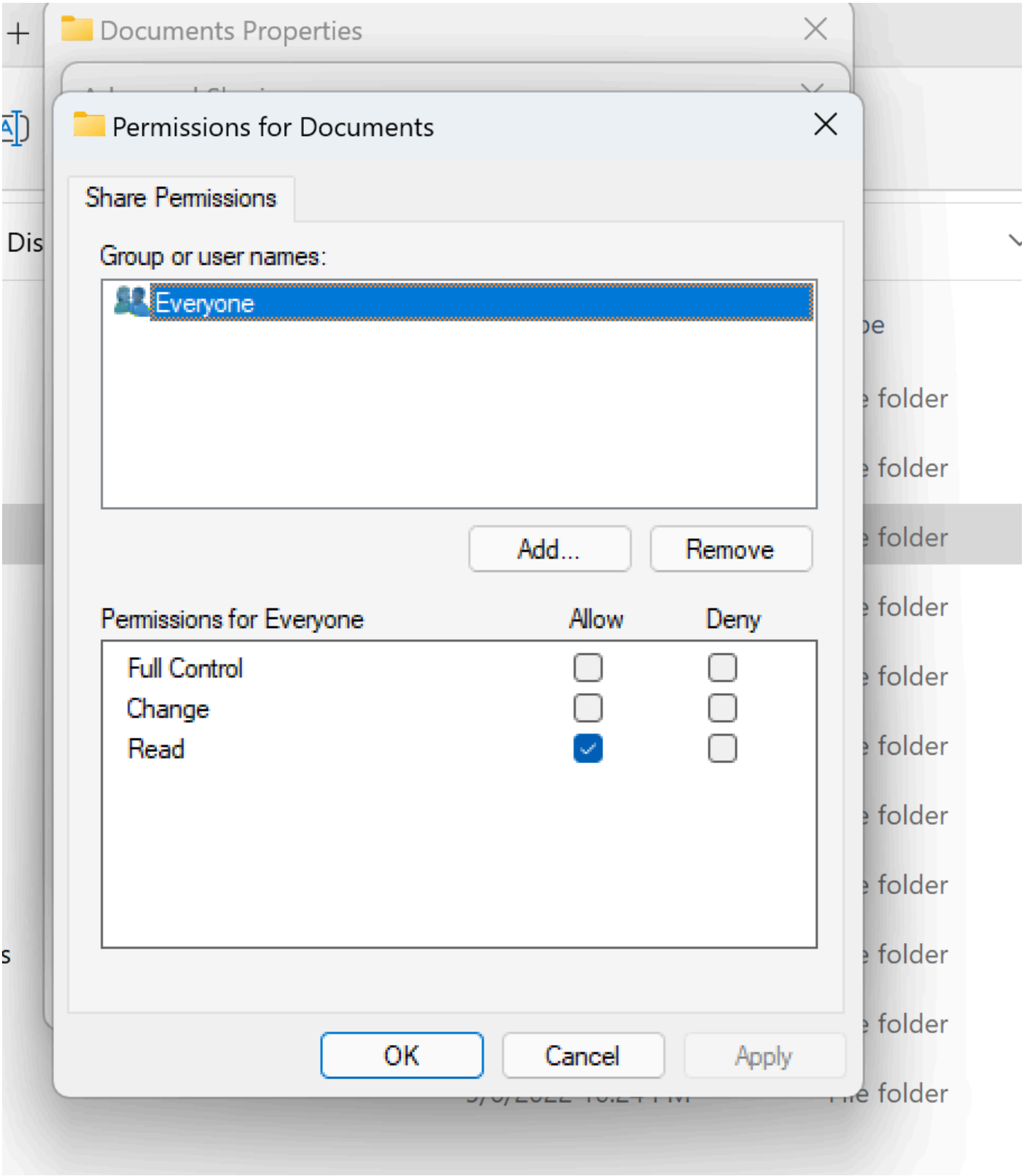
搭配 Linux 工作負載使用 UNIX 樣式磁碟區

sudoer 可以為其他使用者設定許可。例如，以下內容會授予/<project-name>目錄上所有<group-ID>完整讀取/寫入許可的成員：

```
sudo chown root:<group-ID> /<project-name>
sudo chmod 770 /<project-name>
```

搭配 Linux 和 Windows 工作負載使用 NTFS 樣式磁碟區

您可以使用特定資料夾的共用屬性來設定共用許可。例如，指定使用者user_01和資料夾myfolder，您可以將 Full Control、 Change或 的許可設定為 ReadAllow或 Deny：


Documents Properties
Permissions for Documents
Share Permissions
Group or user names:
Everyone
Add...
Remove
Permissions for Everyone
Allow
Deny
Full Control
Change
Read
OK
Cancel
Apply

如果 Linux 和 Windows 用戶端都會使用磁碟區，我們需要在 SVM 上設定名稱映射，該映射會將任何 Linux 使用者名稱與相同使用者名稱與 domain\username 的 NetBIOS 網域名稱格式建立關聯。這在 Linux 和 Windows 使用者之間進行翻譯時需要用到。如需參考，請參閱使用 Amazon FSx for NetApp ONTAP 啟用多協定工作負載。

.....

我從 RES 建立 Amazon FSx for NetApp ONTAP，但未加入我的網域

目前，當您從 RES 主控台建立 Amazon FSx for NetApp ONTAP 時，系統會佈建檔案系統，但不會加入網域。若要將建立的 ONTAP 檔案系統 SVM 加入您的網域，請參閱將 SVMs 加入 Microsoft Active Directory 並遵循 Amazon FSx 主控台上的步驟。確定必要的許可委派給 AD 中的 Amazon FSx Service 帳戶。一旦 SVM 成功加入網域，請前往 SVM 摘要 > 端點 > SMB DNS 名稱，然後複製 DNS 名稱，因為稍後會需要它。

加入網域後，請在叢集設定 DynamoDB 資料表中編輯 SMB DNS 組態金鑰：

1. 前往 Amazon DynamoDB 主控台。
2. 選擇資料表，然後選擇 `<stack-name>-cluster-settings`。
3. 在探索資料表項目下，展開篩選條件，然後輸入下列篩選條件：
   - 屬性名稱 - 索引鍵
   - 條件 - 等於
   - 值 - `shared-storage.<file-system-name>.fsx_netapp_ontap.svm.smb_dns`
4. 選取傳回的項目，然後選取動作、編輯項目。
5. 使用您先前複製的 SMB DNS 名稱更新值。
6. 選擇儲存與關閉。

此外，請確保與檔案系統相關聯的安全群組允許 Amazon VPC 檔案系統存取控制中建議的流量。使用檔案系統的新 VDI 主機現在將能夠掛載加入 SVM 和檔案系統的網域。

或者，您可以使用 RES 加入檔案系統功能加入現有的檔案系統 - 從環境管理選擇檔案系統、加入檔案系統。

.....

快照

主題

- 快照的狀態為失敗
- 快照無法套用至表示無法匯入資料表的日誌。

.....

快照的狀態為失敗

在 RES 快照頁面上，如果快照的狀態為失敗，則可以前往叢集管理員的 Amazon CloudWatch 日誌群組來判斷錯誤發生的時間。

```
[2023-11-19 03:39:20,208] [INFO] [snapshots-service] creating snapshot in S3 Bucket:
  asdf at path s31
[2023-11-19 03:39:20,381] [ERROR] [snapshots-service] An error occurred while
  creating the snapshot: An error occurred (TableNotFoundException)
  when calling the UpdateContinuousBackups operation:
  Table not found: res-demo.accounts.sequence-config
```

.....

快照無法套用至表示無法匯入資料表的日誌。

如果從上一個 env 擷取的快照無法在新的 env 中套用，請查看叢集管理員的 CloudWatch 日誌以識別問題。如果問題提及未匯入必要的資料表雲端，請確認快照處於有效狀態。

1. 下載 metadata.json 檔案，並確認各種資料表的 ExportStatus 具有 COMPLETED 狀態。確保各種資料表都有 `ExportManifest` 欄位集。如果您找不到上述欄位集，快照會處於無效狀態，且無法與套用快照功能搭配使用。
2. 啟動快照建立後，請確保快照狀態在 RES 中變為 COMPLETED。快照建立程序最多需要 5 到 10 分鐘。重新載入或重新檢視快照管理頁面，以確保快照已成功建立。這將確保建立的快照處於有效狀態。

.....

基礎設施

主題

- 沒有運作狀態良好執行個體的負載平衡器目標群組

.....

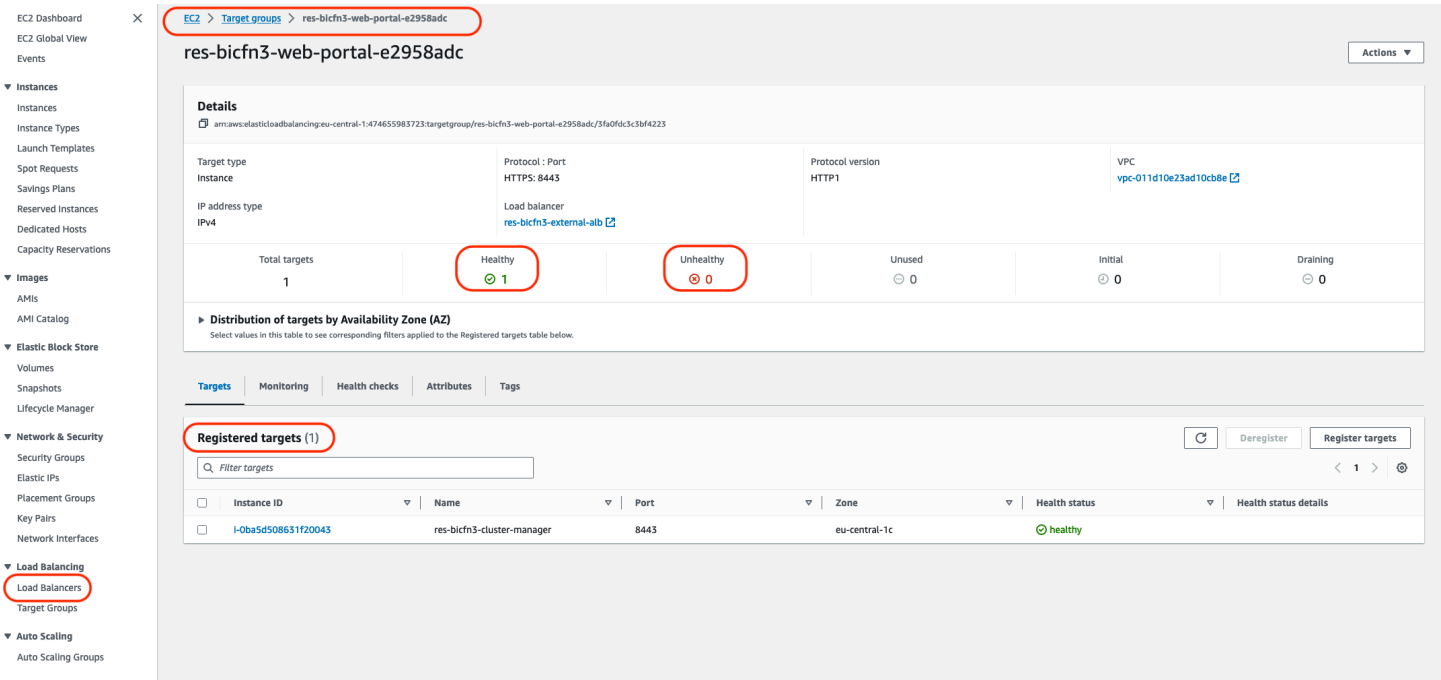
沒有運作狀態良好執行個體的負載平衡器目標群組

如果 UI 中出現伺服器錯誤訊息等問題，或桌面工作階段無法連線，這可能表示基礎設施 Amazon EC2 執行個體發生問題。

判斷問題來源的方法，是先檢查 Amazon EC2 主控台是否有任何 Amazon EC2 執行個體重複終止，並以新執行個體取代。如果是這種情況，檢查 Amazon CloudWatch logs可能會決定原因。

另一種方法是檢查系統中的負載平衡器。如果 Amazon EC2 主控台上發現任何負載平衡器未顯示任何運作狀態良好的執行個體，則表示系統可能有問題。

正常外觀的範例如下所示：



如果運作狀態項目為 0，表示沒有 Amazon EC2 執行個體可用於處理請求。

如果運作狀態不佳的項目為非 0，表示 Amazon EC2 執行個體可能正在循環。這可能是因為已安裝的應用程式軟體未通過運作狀態檢查。

如果運作狀態良好和運作狀態不佳的項目都是 0，表示潛在的網路組態錯誤。例如，公有和私有子網路可能沒有對應的 AZs。如果發生這種情況，主控台上可能會有額外的文字，指出網路狀態存在。

.....

啟動虛擬桌面

主題

- Windows 虛擬桌面的登入帳戶設定為管理員
- 使用外部資源 CertificateRenewalNode 時，憑證過期
- 先前運作中的虛擬桌面無法再成功連線
- 我只能啟動 5 個虛擬桌面
- 桌面 Windows 連線嘗試失敗，並顯示「連線已關閉。傳輸錯誤"
- VDIs停滯在佈建狀態
- 啟動後，VDIs會進入錯誤狀態

.....

Windows 虛擬桌面的登入帳戶設定為管理員

如果您能夠在 RES Web 入口網站中啟動 Windows 虛擬桌面，但其登入帳戶在您連線時設定為管理員，則您的 Windows VDI 可能尚未成功加入 Active Directory。

若要驗證，請從 Amazon EC2 主控台連線至 Windows 執行個體，並檢查 下的引導日誌`C:\Users\Administrator\RES\Bootstrap\virtual-desktop-host-windows\`。以 開頭的錯誤訊息`[Join AD] authorization failed:`表示執行個體無法加入 AD。如需失敗`<res-environment-name>/cluster-manager`的詳細資訊，請參閱日誌群組名稱下 CloudWatch 中的 Cluster Manager 日誌：

- `Insufficient permissions to modify computer account`
  - 此錯誤表示您的服務帳戶沒有將電腦新增至 AD 的適當許可。檢查 設定 Microsoft Active Directory 的服務帳戶區段以取得服務帳戶所需的許可。
- `Invalid Credentials`
  - 您在 AD 中的服務帳戶登入資料已過期，或您提供的登入資料不正確。若要檢查或更新您的服務帳戶登入資料，請存取在 Secrets Manager 主控台中存放密碼的秘密。請確定此秘密的 ARN 在 RES 環境身分管理頁面的 Active Directory 網域下的服務帳戶登入資料秘密 ARN 欄位中正確無誤。

.....

使用外部資源 CertificateRenewalNode 時，憑證過期

如果您部署了外部資源配方，並在連線至 Linux VDIs "The connection has been closed. Transport error"時遇到 錯誤，最可能的原因是憑證過期，因為 Linux 上的 pip 安裝路徑不正確而未自動重新整理。憑證會在 3 個月後過期。

Amazon CloudWatch 日誌群組*<envname>*/vdc/dcv-connection-gateway可能會使用類似以下內容的訊息記錄連線嘗試錯誤：

```
| 2024-07-29T21:46:02.651Z | Jul 29 21:46:01.702  WARN HTTP:Splicer Connection{id=341
 client_address="x.x.x.x:50682"}: Error in connection task: TLS handshake error:
 received fatal alert: CertificateUnknown | redacted:/res-demo/vdc/dcv-connection-
gateway | dcv-connection-gateway_10.3.146.195 |
| 2024-07-29T21:46:02.651Z | Jul 29 21:46:01.702  WARN HTTP:Splicer Connection{id=341
 client_address="x.x.x.x:50682"}: Certificate error: AlertReceived(CertificateUnknown)
 | redacted:/res-demo/vdc/dcv-connection-gateway | dcv-connection-gateway_10.3.146.195
 |
```

要解決問題：

1. 在您的帳戶中 AWS ，前往 EC2。如果有名為 `*-CertificateRenewalNode-*` 的執行個體，請終止執行個體。
2. 前往 Lambda。您應該會看到名為 `*-CertificateRenewalLambda-*` 的 Lambda 函數，請檢查 Lambda 程式碼是否有類似如下的內容：

```
export HOME=/tmp/home
mkdir -p $HOME

cd /tmp
wget https://bootstrap.pypa.io/pip/3.7/get-pip.py
python3 ./get-pip.py
pip3 install boto3
eval $(python3 -c "from botocore.credentials import
 InstanceMetadataProvider, InstanceMetadataFetcher; provider =
 InstanceMetadataProvider(iam_role_fetcher=InstanceMetadataFetcher(timeout=1000,
 num_attempts=2)); c = provider.load().get_frozen_credentials();
 print(f'export AWS_ACCESS_KEY_ID={c.access_key}'); print(f'export
 AWS_SECRET_ACCESS_KEY={c.secret_key}'); print(f'export
 AWS_SESSION_TOKEN={c.token}')")

mkdir certificates
```

```
cd certificates
git clone https://github.com/Neilpang/acme.sh.git
cd acme.sh
```

3. 在這裡尋找最新的外部資源 Certs 堆疊範本。在範本中尋找 Lambda 程式碼：資源 → CertificateRenewalLambda → 屬性 → 程式碼。您可能會找到類似如下的內容：

```
sudo yum install -y wget
export HOME=/tmp/home
mkdir -p $HOME
cd /tmp
wget https://bootstrap.pypa.io/pip/3.7/get-pip.py
mkdir -p pip
python3 ./get-pip.py --target $PWD/pip
$PWD/pip/bin/pip3 install boto3
eval $(python3 -c "from botocore.credentials import
 InstanceMetadataProvider, InstanceMetadataFetcher; provider =
 InstanceMetadataProvider(iam_role_fetcher=InstanceMetadataFetcher(timeout=1000,
 num_attempts=2)); c = provider.load().get_frozen_credentials();
 print(f'export AWS_ACCESS_KEY_ID={c.access_key}'); print(f'export
 AWS_SECRET_ACCESS_KEY={c.secret_key}'); print(f'export
 AWS_SESSION_TOKEN={c.token}')")

mkdir certificates
cd certificates
VERSION=3.1.0
wget https://github.com/acmesh-official/acme.sh/archive/refs/tags/$VERSION.tar.gz -
O acme-$VERSION.tar.gz
tar -xvf acme-$VERSION.tar.gz
cd acme.sh-$VERSION
```

4. 將 `*-CertificateRenewalLambda-*` Lambda 函數中步驟 2 的 區段取代為步驟 3 的程式碼。選取部署並等待程式碼變更生效。
5. 若要手動觸發 Lambda 函數，請前往測試索引標籤，然後選取測試。不需要額外的輸入。這應該會建立憑證 EC2 執行個體，以更新 Secret Manager 中的憑證和 PrivateKey 秘密。
6. 終止現有的 dcv-gateway 執行個體：`<env-name>-vdc-gateway`並等待自動擴展群組自動部署新的執行個體。

.....

先前運作中的虛擬桌面無法再成功連線

如果桌面連線關閉或您無法再與其連線，問題可能是因為基礎 Amazon EC2 執行個體故障，或 Amazon EC2 執行個體可能在 RES 環境之外終止或停止。管理員 UI 狀態可能會繼續顯示就緒狀態，但嘗試連線失敗。

應使用 Amazon EC2 主控台來判斷執行個體是否已終止或停止。如果停止，請嘗試再次啟動。如果狀態終止，則必須建立另一個桌面。使用者主目錄上存放的任何資料，在新執行個體啟動時仍應可供使用。

如果先前失敗的執行個體仍顯示在 Admin UI 上，則可能需要使用 Admin UI 將其終止。

.....

我只能啟動 5 個虛擬桌面

使用者可以啟動的虛擬桌面數量預設限制為 5。管理員可以使用 Admin UI 進行變更，如下所示：

- 前往桌面設定。
- 選取一般索引標籤。
- 選取每個專案每個使用者預設允許工作階段右側的編輯圖示，並將值變更為所需的新值。
- 選擇提交。
- 重新整理頁面以確認新的設定已就位。

.....

桌面 Windows 連線嘗試失敗，並顯示「連線已關閉。傳輸錯誤"

如果 Windows 桌面連線失敗，並顯示 UI 錯誤「連線已關閉。傳輸錯誤"，原因可能是在 Windows 執行個體上建立憑證相關的 DCV 伺服器軟體發生問題。

Amazon CloudWatch 日誌群組`<envname>/vdc/dcv-connection-gateway`可能會使用類似以下內容的訊息記錄連線嘗試錯誤：

```
Nov 24 20:24:27.631 DEBUG HTTP:Splicer Connection{id=9}:
Websocket{session_id="1291e75f-7816-48d9-bbb2-7371b3b911cd"}:
Resolver lookup{client_ip=Some(52.94.36.19)
session_id="1291e75f-7816-48d9-bbb2-7371b3b911cd"
 protocol_type=WebSocket extension_data=None}:NoStrictCertVerification:
 Additional stack certificate (0): [s/n: 0E9E9C4DE7194B37687DC4D2C0F5E94AF0DD57E]
```

```
Nov 24 20:25:15.384  INFO HTTP:Splicer Connection{id=21}:Websocket{
session_id="d1d35954-f29d-4b3f-8c23-6a53303ebc3f"}:
Connection initiated error: unreachable, server io error Custom {
kind: InvalidData, error:
General("Invalid certificate: certificate has expired (code: 10)") }

Nov 24 20:25:15.384  WARN HTTP:Splicer Connection{id=21}:
Websocket{session_id="d1d35954-f29d-4b3f-8c23-6a53303ebc3f"}:
Error in websocket connection: Server unreachable: Server error: IO error:
unexpected error: Invalid certificate: certificate has expired (code: 10)
```

如果發生這種情況，解決方法是使用 SSM Session Manager 開啟與 Windows 執行個體的連線，並移除下列 2 個憑證相關檔案：

```
PS C:\Windows\system32\config\systemprofile\AppData\Local\NICE\dcv> dir

    Directory: C:\Windows\system32\config\systemprofile\AppData\Local\NICE\dcv


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         8/4/2022  12:59 PM           1704 dcv.key
-a----         8/4/2022  12:59 PM           1265 dcv.pem
```

這些檔案應該會自動重新建立，且後續的連線嘗試可能會成功。

如果此方法解決問題，而且如果 Windows 桌面的新啟動產生相同的錯誤，請使用建立軟體堆疊函數，使用重新產生的憑證檔案來建立固定執行個體的新 Windows 軟體堆疊。這可能會產生 Windows 軟體堆疊，可用於成功的啟動和連線。

.....

VDIs停滯在佈建狀態

如果桌面啟動在 Admin UI 中仍處於佈建狀態，這可能是由於幾個原因所致。

若要判斷原因，請檢查桌面執行個體上的日誌檔案，並尋找可能導致問題的錯誤。本文件包含日誌檔案和 Amazon CloudWatch 日誌群組的清單，其中包含標記為實用日誌和事件資訊來源一節中的相關資訊。

以下是此問題的潛在原因。

- 使用的 AMI ID 已註冊為軟體堆疊，但 RES 不支援。

引導佈建指令碼無法完成，因為 Amazon Machine Image (AMI) 沒有所需的預期組態或工具。執行個體上的日誌檔案，例如 `/root/bootstrap/logs/` Linux 執行個體，可能包含與此相關的實用資訊。從 AWS Marketplace 取得的 AMIs ID 可能無法用於 RES 桌面執行個體。它們需要測試以確認是否支援。

- 從自訂 AMI 啟動 Windows 虛擬桌面執行個體時，不會執行使用者資料指令碼。

  根據預設，當 Amazon EC2 執行個體啟動時，使用者資料指令碼會執行一次。如果您從現有的虛擬桌面執行個體建立 AMI，然後向 AMI 註冊軟體堆疊，並嘗試使用此軟體堆疊啟動另一個虛擬桌面，則使用者資料指令碼將不會在新的虛擬桌面執行個體上執行。

  若要修正此問題，請在您用來建立 AMI 的原始虛擬桌面執行個體上，以管理員身分開啟 PowerShell 命令視窗，然後執行下列命令：

  ```
  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
  ```

  然後從執行個體建立新的 AMI。您可以使用新的 AMI 來註冊軟體堆疊，並在之後啟動新的虛擬桌面。請注意，您也可以在保持佈建狀態的執行個體上執行相同的命令，並重新啟動執行個體以修正虛擬桌面工作階段，但當您從設定錯誤的 AMI 啟動另一個虛擬桌面時，將會再次遇到相同的問題。

.....

啟動後，VDIs會進入錯誤狀態

可能的問題 1：主檔案系統的 目錄適用於具有不同 POSIX 許可的使用者。

如果下列案例成立，這可能是您面臨的問題：

1. 部署的 RES 版本為 2024.01 或更新版本。
2. 在部署 RES 堆疊期間， 的 屬性`EnableLdapIDMapping`設定為 `True`。
3. 在 RES 堆疊部署期間指定的主檔案系統用於 RES 2024.01 之前的版本，或在先前環境中使用，並將 `EnableLdapIDMapping`設定為 `False`。

解決步驟：刪除 檔案系統中的使用者目錄。

1. SSM 至叢集管理員主機。
2. `cd /home`.
3. `ls` - 應列出目錄名稱符合使用者名稱的目錄，例如 `admin1`、`admin2`.. 等。
4. 刪除目錄 `sudo rm -r 'dir_name'`。請勿刪除 ssm-user 和 ec2-user 目錄。

5. 如果使用者已同步到新的 env，請從使用者的 DDB 資料表刪除使用者的 (clusteradmin 除外)。
6. 啟動 AD 同步 - 在叢集管理員 Amazon EC2 `sudo /opt/idea/python/3.9.16/bin/resctl ldap sync-from-ad`中執行。
7. 從 RES 網頁以 `Error` 狀態重新啟動 VDI 執行個體。驗證 VDI 是否在大約 20 分鐘內轉換為 `Ready` 狀態。

.....

虛擬桌面元件

主題

- Amazon EC2 執行個體在主控台中重複顯示已終止
- vdc-controller 執行個體正在循環中，因為無法加入 AD/eVDI 模組，顯示 API 運作狀態檢查失敗
- 編輯軟體堆疊以新增專案時，專案不會出現在下拉式清單中
- cluster-manager Amazon CloudWatch 日誌顯示「<user-home-init> 帳戶尚無法使用。正在等待使用者同步」（其中帳戶是使用者名稱）
- Windows 桌面登入嘗試時顯示「您的帳戶已停用。請洽詢您的管理員"
- 外部/客戶 AD 組態的 DHCP 選項問題
- Firefox 錯誤 MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING

.....

Amazon EC2 執行個體在主控台中重複顯示已終止

如果基礎設施執行個體在 Amazon EC2 主控台中重複顯示為已終止，原因可能與其組態有關，並取決於基礎設施執行個體類型。以下是判斷原因的方法。

如果 vdc-controller 執行個體在 Amazon EC2 主控台中顯示重複終止狀態，這可能是由於不正確的秘密標籤所致。RES 維護的秘密具有標籤，做為連接到基礎設施 Amazon EC2 執行個體的 IAM 存取控制政策的一部分。如果 vdc-controller 正在循環，且 CloudWatch 日誌群組中出現下列錯誤，原因可能是秘密未正確標記。請注意，秘密需要標記下列項目：

```
{
    "res:EnvironmentName": "<envname>" # e.g. "res-demo"
    "res:ModuleName": "virtual-desktop-controller"
}
```

此錯誤的 Amazon CloudWatch 日誌訊息將如下所示：

```
An error occurred (AccessDeniedException) when calling the GetSecretValue
operation: User: arn:aws:sts::160215750999:assumed-role/<envname>-vdc-gateway-role-us-
east-1/i-043f76a2677f373d0
is not authorized to perform: secretsmanager:GetSecretValue on resource:
arn:aws:secretsmanager:us-east-1:160215750999:secret:Certificate-res-bi-
Certs-5W9SPUXF08IB-F1sNRv
because no identity-based policy allows the secretsmanager:GetSecretValue action
```

檢查 Amazon EC2 執行個體上的標籤，並確認它們符合上述清單。

.....

vdc-controller 執行個體正在循環中，因為無法加入 AD/eVDI 模組，顯示 API 運作狀態檢查失敗

如果 eVDI 模組運作狀態檢查失敗，則會在環境狀態區段中顯示下列項目。

Modules

Environment modules and status

Module	Module ID	Version	Type	Status	API Health Check	Module Sets
Global Settings	global-settings	-	Config	Deployed	Not Applicable	-
Cluster	cluster	2023.10b1	Stack	Deployed	Not Applicable	• default
Metrics & Monitoring	metrics	2023.10b1	Stack	Deployed	Not Applicable	• default
Directory Service	directoryservice	2023.10b1	Stack	Deployed	Not Applicable	• default
Identity Provider	identity-provider	2023.10b1	Stack	Deployed	Not Applicable	• default
Analytics	analytics	2023.10b1	Stack	Deployed	Not Applicable	• default
Shared Storage	shared-storage	2023.10b1	Stack	Deployed	Not Applicable	• default
Cluster Manager	cluster-manager	2023.10b1	App	Deployed	Healthy	• default
eVDI	vdc	2023.10b1	App	Deployed	Failed	• default
Bastion Host	bastion-host	2023.10b1	Stack	Deployed	Not Applicable	• default

在這種情況下，除錯的一般路徑是查看叢集管理員 CloudWatch 日誌。（尋找名為 的日誌群組`<env-name>/cluster-manager`。）

可能的問題：

- 如果日誌包含文字 `Insufficient permissions`，請確定建立 res 堆疊時提供的 ServiceAccount 使用者名稱拼寫正確。

  日誌行範例：

  ```
  Insufficient permissions to modify computer account:
   CN=IDEA-586BD25043,OU=Computers,OU=RES,OU=CORP,DC=corp,DC=res,DC=com:
   000020E7: AtrErr: DSID-03153943, #1: 0: 000020E7: DSID-03153943, problem 1005
   (CONSTRAINT_ATT_TYPE), data 0, Att 90008 (userAccountControl):len 4 >> 432 ms -
   request will be retried in 30 seconds
  ```

  - 您可以從 SecretsManager 主控台存取 RES 部署期間提供的 ServiceAccount 使用者名稱。在 Secrets Manager 中尋找對應的秘密，然後選擇擷取純文字。如果使用者名稱不正確，請選擇編輯以更新秘密值。終止目前的叢集管理員和 vdc-controller 執行個體。新的執行個體將進入穩定狀態。
  - 如果您使用由提供的外部資源堆疊建立的資源，使用者名稱必須是「ServiceAccount」。如果在部署 RES 期間將 `DisableADJoin` 參數設定為 False，請確定 "ServiceAccount" 使用者具有在 AD 中建立電腦物件的許可。
- 如果使用的使用者名稱正確，但日誌包含文字 `Invalid credentials`，則您輸入的密碼可能錯誤或已過期。

  日誌行範例：

  ```
  {'msgtype': 97, 'msgid': 1, 'result': 49, 'desc': 'Invalid credentials', 'ctrls': [],
   'info': '80090308: LdapErr: DSID-0C090569, comment: AcceptSecurityContext error,
   data 532, v4563'}
  ```

  - 您可以透過存取在 Secrets Manager 主控台中存放密碼的秘密，讀取您在建立 env 期間輸入的密碼。選取秘密（例如 `<env_name>directoryserviceServiceAccountPassword`），然後選擇擷取純文字。
  - 如果秘密中的密碼不正確，請選擇編輯以更新秘密中的值。終止目前的叢集管理員和 vdc-controller 執行個體。新執行個體將使用更新的密碼，並進入穩定狀態。
  - 如果密碼正確，可能是已連線 Active Directory 中的密碼已過期。您必須先重設 Active Directory 中的密碼，然後更新秘密。您可以從 Directory Service 主控台在 Active Directory 中重設使用者的密碼：

    1. 選擇適當的目錄 ID

2. 選擇動作、重設使用者密碼，然後使用使用者名稱（例如「ServiceAccount」）和新密碼填寫表單。
3. 如果新設定的密碼與先前的密碼不同，請在對應的 Secret Manager 秘密中更新密碼（例如 `<env_name>directoryserviceServiceAccountPassword`。
4. 終止目前的叢集管理員和 vdc-controller 執行個體。新執行個體將進入穩定狀態。

.....

編輯軟體堆疊以新增專案時，專案不會出現在下拉式清單中

此問題可能與下列與將使用者帳戶與 AD 同步相關的問題有關。如果出現此問題，請檢查叢集管理員 Amazon CloudWatch 日誌群組是否有錯誤「`<user-home-init> account not available yet. waiting for user to be synced`」，以判斷原因是否相同或相關。

.....

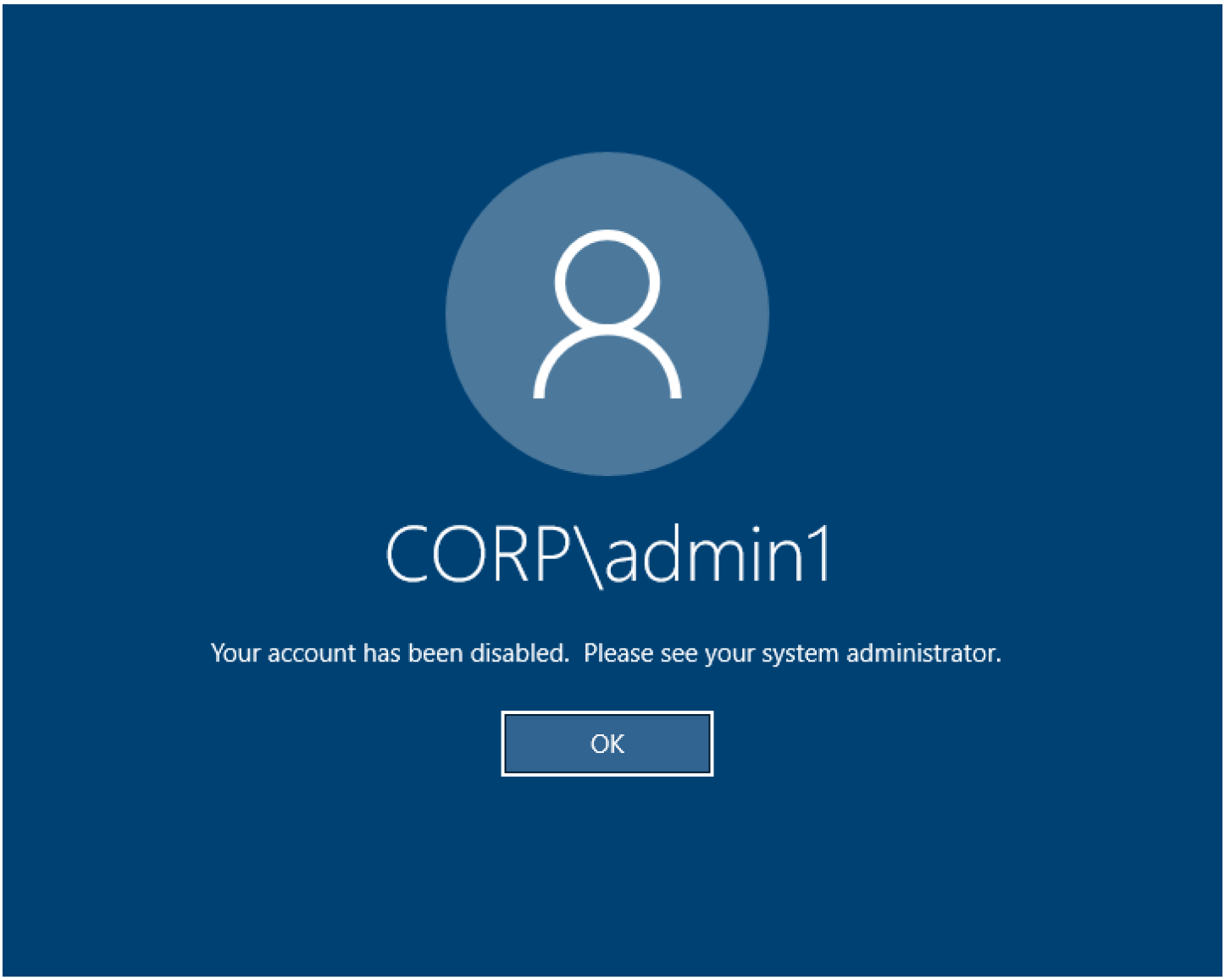
cluster-manager Amazon CloudWatch 日誌顯示「<user-home-init> 帳戶尚無法使用。正在等待使用者同步」（其中帳戶是使用者名稱）

SQS 訂閱者忙碌且卡在無限迴圈中，因為它無法到達使用者帳戶。在使用者同步期間嘗試為使用者建立主檔案系統時，會觸發此程式碼。

無法到達使用者帳戶的原因可能是 RES 未正確設定 AD 使用中。例如，在 BI/RES 環境建立中使用的 `ServiceAccountCredentialsSecretArn` 參數不是正確的值。

.....

Windows 桌面登入嘗試時顯示「您的帳戶已停用。請洽詢您的管理員"



如果使用者無法登入鎖定的畫面，這可能表示使用者在透過 SSO 成功登入後，已在針對 RES 設定的 AD 中停用。

如果使用者帳戶已在 AD 中停用，SSO 登入應該會失敗。

.....

外部/客戶 AD 組態的 DHCP 選項問題

如果您在`"The connection has been closed. Transport error"`將 RES 與您自己的 Active Directory 搭配使用時遇到使用 Windows 虛擬桌面的錯誤，請檢查 dcv-connection-gateway Amazon CloudWatch 日誌是否有類似如下的內容：

```
Oct 28 00:12:30.626  INFO HTTP:Splicer Connection{id=263}:
Websocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Connection initiated
 error: unreachable, server io error Custom { kind: Uncategorized, error: "failed to
 lookup address information: Name or service not known" }

Oct 28 00:12:30.626  WARN HTTP:Splicer Connection{id=263}:
 Websocket{session_id="96cffa6e-cf2e-410f-9eea-6ae8478dc08a"}: Error in websocket
 connection: Server unreachable: Server error: IO error: failed to lookup address
 information: Name or service not known

Oct 28 00:12:30.627 DEBUG HTTP:Splicer Connection{id=263}: ConnectionGuard dropped
```

如果您針對自己的 VPC 使用 DHCP 選項的 AD 網域控制器，則需要：

1. 將 AmazonProvidedDNS 新增至兩個網域控制站 IPs。
2. 將網域名稱設定為 ec2.internal。

此處顯示範例。如果沒有此組態，Windows 桌面會為您提供傳輸錯誤 ，因為 RES/DCV 會尋找 ip-10-0-x-xx.ec2.internal hostname。

.....

Firefox 錯誤 MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING

當您使用 Firefox Web 瀏覽器時，當您嘗試連線到虛擬桌面時，可能會遇到 MOZILLA_PKIX_ERROR_REQUIRED_TLS_FEATURE_MISSING 錯誤訊息類型。

原因是 RES Web 伺服器已使用 TLS + Stapling On 設定，但未使用 Stapling Validation 回應 （請參閱 https://support.mozilla.org/en-US/questions/1372483：//。

您可以依照 https：//https://really-simple-ssl.com/mozilla_pkix_error_required_tls_feature_missing 的指示來修正此問題。

.....

Env 刪除

主題

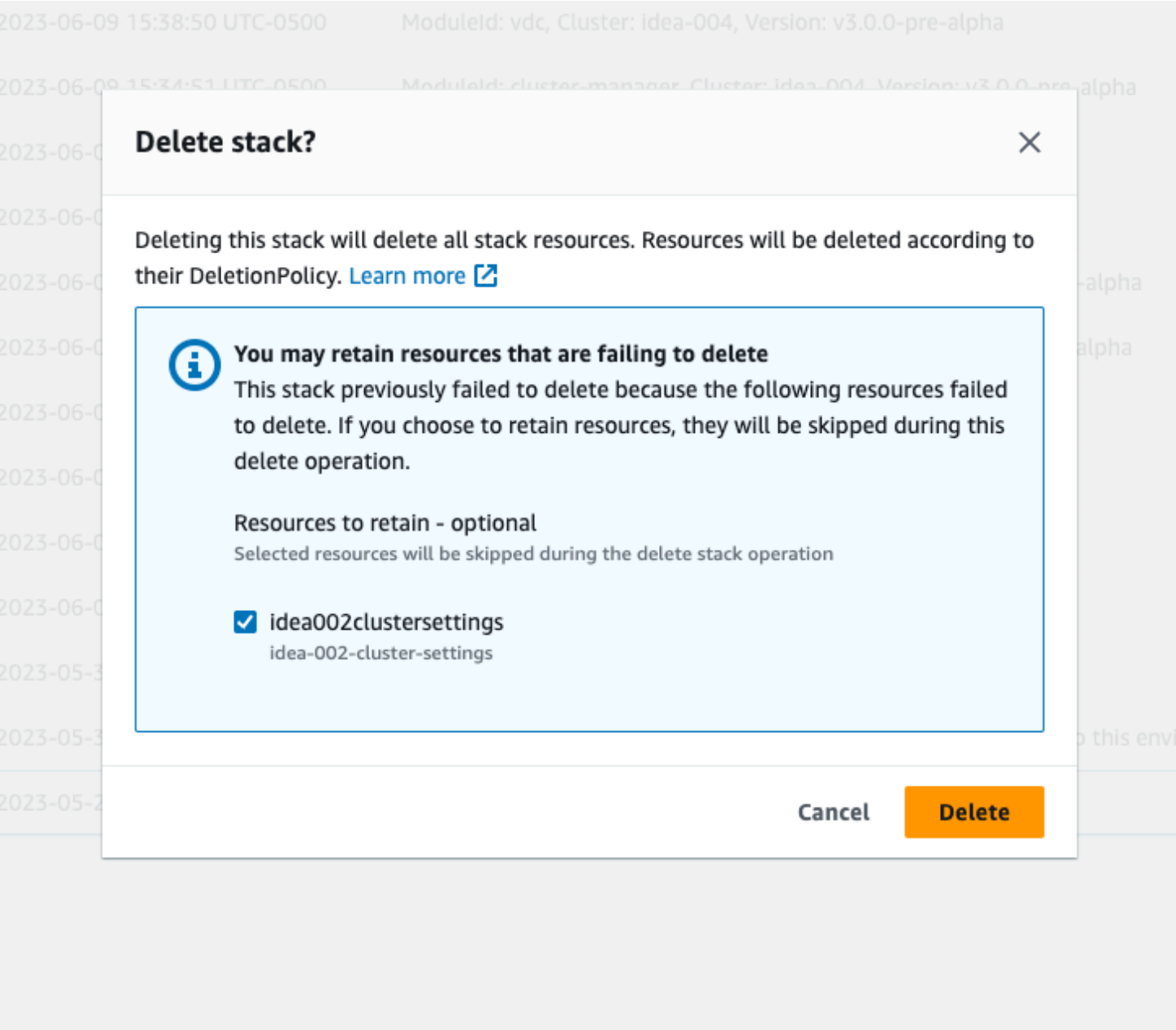
- res-xxx-cluster 堆疊處於「DELETE_FAILED」狀態，無法手動刪除，因為「角色無效或無法擔任」錯誤
- 收集日誌
- 下載 VDI 日誌
- 從 Linux EC2 執行個體下載日誌
- 從 Windows EC2 執行個體下載日誌
- 收集 WaitCondition 錯誤的 ECS 日誌

.....

res-xxx-cluster 堆疊處於「DELETE_FAILED」狀態，無法手動刪除，因為「角色無效或無法擔任」錯誤

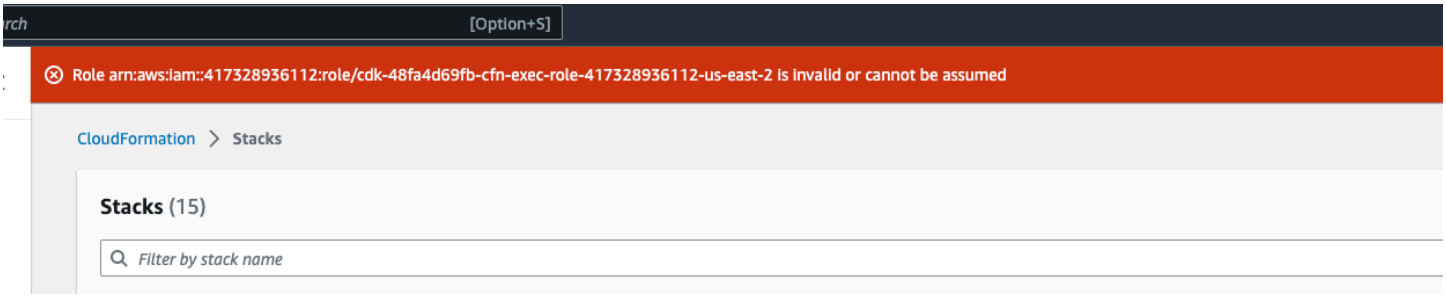
如果您注意到 "res-xxx-cluster" 堆疊處於 "DELETE_FAILED" 狀態，且無法手動刪除，您可以執行下列步驟將其刪除。

如果您看到堆疊處於「DELETE_FAILED」狀態，請先嘗試手動將其刪除。它可能會彈出一個對話方塊，確認刪除堆疊。選擇 刪除。



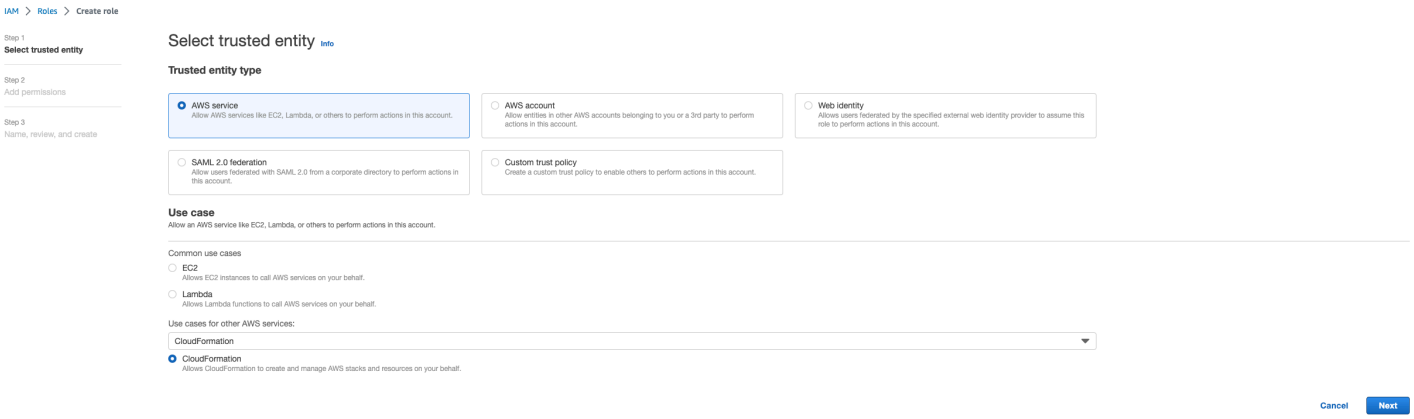
有時候，即使您刪除所有必要的堆疊資源，您仍可能會看到訊息來選取要保留的資源。在這種情況下，請選取所有資源做為「要保留的資源」，然後選擇刪除。

您可能會看到類似 的錯誤 `Role: arn:aws:iam::... is Invalid or cannot be assumed`

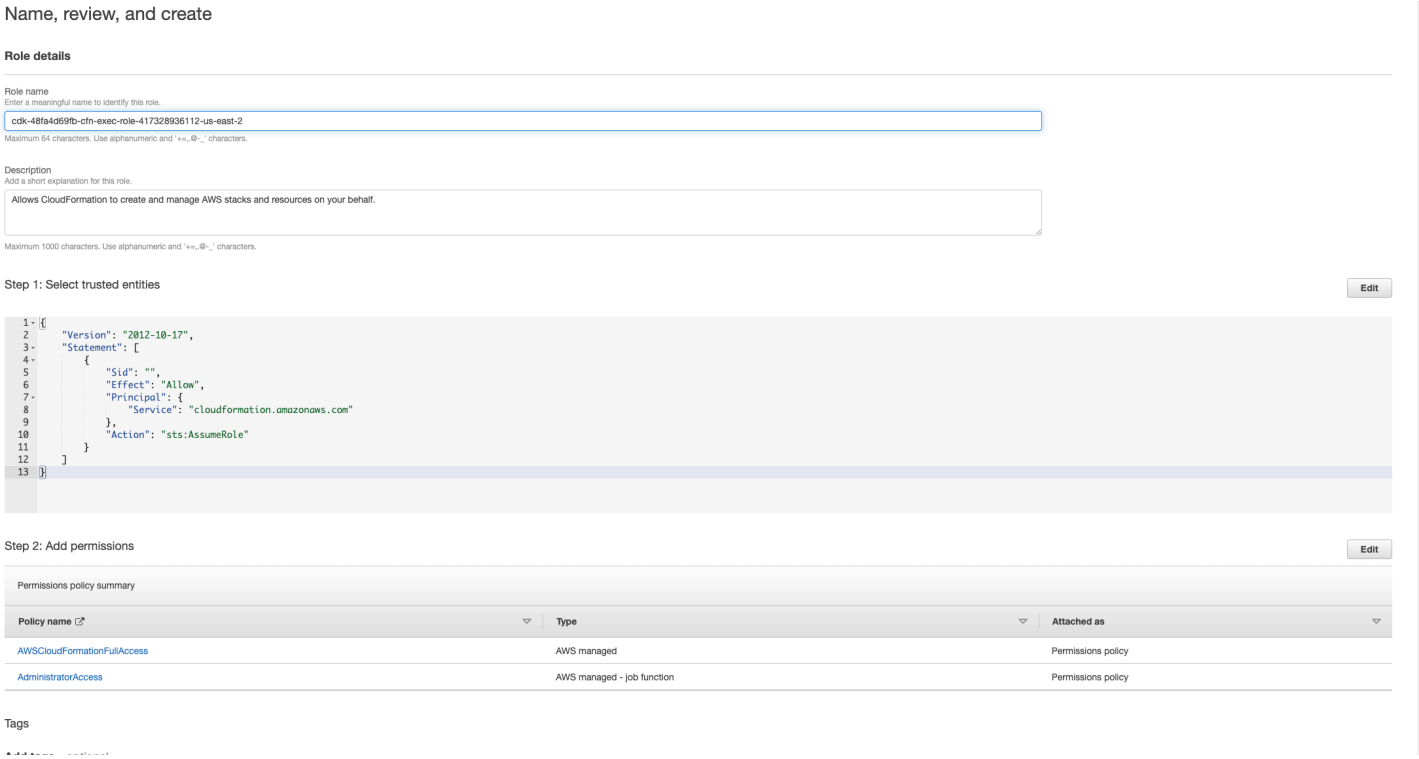


這表示刪除堆疊所需的角色會在堆疊之前先刪除。若要解決此問題，請複製角色的名稱。前往 IAM 主控台，並使用如下所示的參數建立具有該名稱的角色，如下所示：

- 針對信任的實體類型，選擇 AWS 服務。
- 針對使用案例，在 下`Use cases for other AWS services`選擇 `CloudFormation`。



選擇下一步。請務必提供角色 `'AWSCloudFormationFullAccess'` 和 `'AdministratorAccess'` 許可。您的檢閱頁面看起來應該如下所示：



然後返回 CloudFormation 主控台並刪除堆疊。您現在應該可以在建立角色後將其刪除。最後，前往 IAM 主控台並刪除您建立的角色。

.....

收集日誌

從 EC2 主控台登入 EC2 執行個體

- 請依照這些指示登入您的 Linux EC2 執行個體。
- 請依照這些指示登入您的 Windows EC2 執行個體。然後開啟 Windows PowerShell 以執行任何命令。

收集基礎設施主機日誌

1. Cluster-manager：從下列位置取得叢集管理員的日誌，並將其連接到票證。
   a. 來自 CloudWatch 日誌群組 的所有日誌`<env-name>/cluster-manager`。
   b. `<env-name>-cluster-manager` EC2 執行個體上 `/root/bootstrap/logs`目錄下的所有日誌。遵循本節開頭從「從 EC2 主控台登入 EC2 執行個體」連結到 的指示，以登入您的執行個體。

2. Vdc-controller：從下列位置取得 vdc-controller 的日誌，並將其連接至票證。
   a. 來自 CloudWatch 日誌群組 的所有日誌`<env-name>/vdc-controller`。
   b. `<env-name>-vdc-controller` EC2 執行個體上 `/root/bootstrap/logs`目錄下的所有日誌。遵循本節開頭從「從 EC2 主控台登入 EC2 執行個體」連結到 的指示，以登入您的執行個體。

輕鬆取得日誌的其中一種方法是遵循 從 Linux EC2 執行個體下載日誌一節中的指示。模組名稱會是執行個體名稱。

收集 VDI 日誌

識別對應的 Amazon EC2 執行個體

如果使用者以工作階段名稱 啟動 VDIVDI1，Amazon EC2 主控台上的執行個體對應名稱將為 `<env-name>-VDI1-<user name>`。

收集 Linux VDI 日誌

遵循本節開頭「從 Amazon EC2 主控台登入 EC2 執行個體」中連結至 的指示，從 Amazon EC2 主控台登入對應的 Amazon EC2 執行個體。取得 VDI Amazon EC2 執行個體上 `/root/bootstrap/logs`和 `/var/log/dcv/`目錄下的所有日誌。

取得日誌的其中一種方法是將日誌上傳至 s3，然後從該處下載日誌。為此，您可以依照下列步驟，從一個目錄取得所有日誌，然後上傳它們：

1. 請依照下列步驟，在 `/root/bootstrap/logs`目錄下複製 dcv 日誌：

```
sudo su -
cd /root/bootstrap
mkdir -p logs/dcv_logs
cp -r /var/log/dcv/* logs/dcv_logs/
```

2. 現在，請依照下一節列出的步驟下載 VDI 日誌，下載日誌。

收集 Windows VDI 日誌

遵循本節開頭「從 Amazon EC2 主控台登入 EC2 執行個體」中連結至 的指示，從 Amazon EC2 主控台登入對應的 Amazon EC2 執行個體。在 VDI EC2 執行個體的 `$env:SystemDrive\Users\Administrator\RES\Bootstrap\Log\`目錄下取得所有日誌。

取得日誌的其中一種方法是將它們上傳到 S3，然後從那裡下載它們。若要這樣做，請依照下一節列出的步驟進行：下載 VDI 日誌。

.....

下載 VDI 日誌

1. 更新 VDI EC2 執行個體 IAM 角色以允許 S3 存取。
2. 前往 EC2 主控台，然後選取您的 VDI 執行個體。
3. 選取其正在使用的 IAM 角色。
4. 在新增許可下拉式功能表的許可政策區段中，選擇連接政策，然後選取 AmazonS3FullAccess 政策。
5. 選擇新增許可以連接該政策。
6. 之後，根據您的 VDI 類型，依照下列步驟下載日誌。模組名稱會是執行個體名稱。
   a. 從 Linux EC2 執行個體下載日誌 適用於 Linux。
   b. 從 Windows EC2 執行個體下載日誌 適用於 Windows 的 。
7. 最後，編輯角色以移除`AmazonS3FullAccess`政策。

> **Note**
>
> 所有 VDIs 都使用相同的 IAM 角色， `<env-name>-vdc-host-role-<region>`

.....

從 Linux EC2 執行個體下載日誌

登入您要從中下載日誌的 EC2 執行個體，並執行下列命令，將所有日誌上傳至 s3 儲存貯體：

```
sudo su -
ENV_NAME=<environment_name>
REGION=<region>
ACCOUNT=<aws_account_number>
MODULE=<module_name>

cd /root/bootstrap
tar -czvf ${MODULE}_logs.tar.gz logs/ --overwrite
aws s3 cp ${MODULE}_logs.tar.gz s3://${ENV_NAME}-cluster-${REGION}-${ACCOUNT}/
${MODULE}_logs.tar.gz
```

之後，請前往 S3 主控台，選取名稱為 的儲存貯體，`<environment_name>-cluster-<region>-<aws_account_number>`然後下載先前上傳`<module_name>_logs.tar.gz`的檔案。

.....

從 Windows EC2 執行個體下載日誌

登入您要從中下載日誌的 EC2 執行個體，並執行下列命令，將所有日誌上傳至 S3 儲存貯體：

```
$ENV_NAME="<environment_name>"
$REGION="<region>"
$ACCOUNT="<aws_account_number>"
$MODULE="<module_name>"

$logDirPath = Join-Path -Path $env:SystemDrive -ChildPath "Users\Administrator\RES
\Bootstrap\Log"
$zipFilePath = Join-Path -Path $env:TEMP -ChildPath "logs.zip"
Remove-Item $zipFilePath
Compress-Archive -Path $logDirPath -DestinationPath $zipFilePath
$bucketName = "${ENV_NAME}-cluster-${REGION}-${ACCOUNT}"
$keyName = "${MODULE}_logs.zip"
Write-S3Object -BucketName $bucketName -Key $keyName -File $zipFilePath
```

之後，請前往 S3 主控台，選取名稱為 的儲存貯體，`<environment_name>-cluster-<region>-<aws_account_number>`然後下載先前上傳`<module_name>_logs.zip`的檔案。

.....

收集 WaitCondition 錯誤的 ECS 日誌

1. 前往部署的堆疊，然後選取資源索引標籤。
2. 展開部署 → ResearchAndEngineeringStudio → 安裝程式 → 任務 → CreateTaskDef → CreateContainer → LogGroup，然後選取日誌群組以開啟 CloudWatch 日誌。
3. 從此日誌群組中擷取最新的日誌。

.....

示範環境

主題

- 處理身分提供者的身分驗證請求時發生示範環境登入錯誤
- 示範堆疊 keycloak 無法運作

.....

處理身分提供者的身分驗證請求時發生示範環境登入錯誤

問題

如果您嘗試登入並在處理身分提供者的身分驗證請求時收到「非預期的錯誤」，您的密碼可能已過期。這可能是您嘗試以 身分登入的使用者的密碼，或是您的 Active Directory 服務帳戶。

緩解

1. 在目錄服務主控台中重設使用者和服務帳戶密碼。
2. 在 Secrets Manager 中更新服務帳戶密碼，以符合您在上面輸入的新密碼：
   - 適用於 Keycloak 堆疊：PasswordSecret-...-RESExternal-...-DirectoryService-... 與描述：Microsoft Active Directory 的密碼
   - for RES： res-ServiceAccountPassword-... with Description： Active Directory Service 帳戶密碼
3. 前往 EC2 主控台並終止叢集管理員執行個體。Auto Scaling 規則會自動觸發新執行個體的部署。

.....

示範堆疊 keycloak 無法運作

問題

如果您的 keycloak 伺服器當機，且當您重新啟動伺服器時，執行個體的 IP 已變更，這可能會導致 keycloak 中斷 – RES 入口網站的登入頁面無法載入或卡在從未解析的載入狀態。

緩解

您需要刪除現有的基礎設施，並重新部署 Keycloak 堆疊，將 Keycloak 還原至運作狀態良好。請遵循下列步驟：

1. 前往 Cloudformation。您應該會在那裡看到兩個與 keycloak 相關的堆疊：
   - `<env-name>-RESSsoKeycloak-<random characters>` (堆疊 1)

`<env-name>-RESSsoKeycloak-<random characters>-RESSsoKeycloak-*` (Stack2)

2. 刪除 Stack1。如果系統提示您刪除巢狀堆疊，請選取是來刪除巢狀堆疊。

   確定堆疊已完全刪除。

3. 在此下載 RES SSO Keycloak 堆疊範本https://s3.amazonaws.com/aws-hpc-recipes/main/recipes/res/res_demo_env/assets/res-sso-keycloak.yaml。
4. 使用與已刪除堆疊完全相同的參數值手動部署此堆疊。從 CloudFormation 主控台部署它，方法是前往建立堆疊 → 使用新資源（標準）→ 選擇現有範本 → 上傳範本檔案。使用與已刪除堆疊相同的輸入填入必要的參數。您可以在 CloudFormation 主控台上變更篩選條件並前往參數索引標籤，在已刪除的堆疊中找到這些輸入。請確定環境名稱、金鑰對和其他參數符合原始堆疊參數。
5. 部署堆疊後，您的環境即可再次使用。您可以在已部署堆疊的輸出索引標籤中找到 ApplicationUrl。

.....

已知問題

- 2024.x 已知問題
  - (2024.12 和 2024.12.01) 註冊新 Cognito 使用者時發生 Regex 失敗
  - (2024.12.01 及更早版本）使用自訂網域連線至 VDI 時出現無效的憑證錯誤
  - (2024.12 和 2024.12.01) Active Directory 使用者無法 SSH 到堡壘主機
  - (2024.10) 針對部署在隔離 VPCs 中的 RES 環境，VDI 自動停止中斷
  - (2024.10 及更早版本）無法啟動 VDI for Graphic 增強型執行個體類型
  - (2024.08) 準備基礎設施 AMI 失敗
  - (2024.08) 虛擬桌面無法掛載具有根儲存貯體 ARN 和自訂字首的讀取/寫入 Amazon S3 儲存貯體
  - (2024.06) 當 AD 群組名稱包含空格時，套用快照失敗
  - (2024.06 及更早版本）AD 同步期間未同步至 RES 的群組成員
  - (2024.06 及更早版本）CVE-2024-6387、RegreSSHion、RHEL9 和 Ubuntu VDIs中的安全漏洞
  - (2024.04-2024.04.02) 提供未連接至 VDI 執行個體角色的 IAM 許可界限
  - (2024.04.02 及更早版本）ap-southeast-2（雪梨）中的 Windows NVIDIA 執行個體無法啟動
  - (2024.04 和 2024.04.01) GovCloud 中的 RES 刪除失敗
  - (2024.04 - 2024.04.02) 重新啟動時，Linux 虛擬桌面可能卡在「繼續」狀態

- (2024.04.02 及更早版本） 無法同步 SAMAccountName 屬性包含大寫字母或特殊字元的 AD 使用者
- (2024.04.02 及更早版本） 用於存取堡壘主機的私有金鑰無效

2024.x 已知問題

.....

(2024.12 和 2024.12.01) 註冊新 Cognito 使用者時發生 Regex 失敗

錯誤描述

如果您嘗試透過 Web 入口網站註冊電子郵件字首包含 "." 的 AWS Cognito 使用者，例如 `<firstname>.<lastname>@<company>.com`，這將導致錯誤，指出 Cognito 使用者名稱不符合定義的 regex 模式。

> Invalid parameters: Username doesn't match the regex pattern ^[a-z][-a-z0-9_]{0,31}$. Username may only contain lower case ASCII letters (a-z), numbers (0-9),and the following special characters: underscore (_), and hypen (-).The maximum length of username is 32.

此錯誤是由 RES 從使用者的電子郵件字首自動產生使用者名稱所造成。不過，在 RES 支援的特定 Linux 發行版本中，具有 "." 的使用者名稱不是 VDIs 的有效使用者。此修正會在產生使用者名稱時移除電子郵件字首中的任何 "."，讓使用者名稱在 RES Linux VDIs上有效。

受影響的版本

RES 2024.12 和 2024.12.01 版

緩解

1. 執行下列命令來下載 2024.12 `cognito_sign_up_email_fix.patch`版或 2024.12.01 版`cognito_sign_up_email_fix.patch`的 `patch.py`和 ，`<output-directory>`將 取代為您要下載修補程式指令碼和修補程式檔案的目錄，並將 `<environment-name>`取代為 RES 環境的名稱：

   a. 此修補程式適用於 RES 2024.12 和 2024.12.01。

   b. 修補程式指令碼需要 AWS CLI v2、Python 3.9.16 或更新版本，以及 Boto3。

c. 為部署 AWS RES 的帳戶和區域設定 CLI，並確保您具有寫入 RES 所建立儲存貯體的 S3 許可。

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>
RES_VERSION=<res-version> # either 2024.12 or 2024.12.01

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patches/cognito_sign_up_email_fix.patch --output
 ${OUTPUT_DIRECTORY}/cognito_sign_up_email_fix.patch
```

2. 導覽至下載修補程式指令碼和修補程式檔案的目錄。執行下列修補程式命令：

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --
res-version ${RES_VERSION} --module cluster-manager --patch ${OUTPUT_DIRECTORY}/
cognito_sign_up_email_fix.patch
```

3. 為您的環境重新啟動 Cluster Manager 執行個體。您也可以從 Amazon EC2 管理主控台終止執行個體。

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

4. 檢查以名稱 開頭的自動擴展群組活動，以驗證 Cluster Manager 執行個體狀態`<RES-EnvironmentName>-cluster-manager-asg`。等待新執行個體成功啟動。

.....

(2024.12.01 及更早版本） 使用自訂網域連線至 VDI 時出現無效的憑證錯誤

錯誤描述

當您使用自訂入口網站網域名稱部署外部資源配方和 RES 時，CertificateRenewalNode 無法在 中重新整理 VDI 連線的 TLS 憑證，並顯示下列錯誤`/var/log/user-data.log`：

```
{
  "type": "urn:ietf:params:acme:error:unauthorized",
  "detail": "Error finalizing order :: OCSP must-staple extension is no longer
 available: see https://letsencrypt.org/2024/12/05/ending-ocsp",
  "status": 403
}
```

因此，當您在 RES Web 入口網站中連線至 VDIs 時，將會遇到 (`net::ERR_CERT_DATE_INVALID`Chrome) 或 `Error code: SSL_ERROR_BAD_CERT_DOMAIN`(FireFox) 的錯誤。

受影響的版本

2024.12.01 及更早版本

緩解

1. 導覽至 EC2 主控台。如果有名為 的執行個體`CertificateRenewalNode-`，請終止執行個體。
2. 導覽至 Lambda 主控台。開啟名為 之 Lambda 函數的原始程式碼`-CertificateRenewalLambda-`。識別注視 的行，`./acme.sh --issue --dns dns_aws --ocsp-must-staple --keylength 4096`並移除`--ocsp-must-staple`引數。
3. 選取部署並等待程式碼變更生效。
4. 若要手動觸發 Lambda 函數：請前往測試索引標籤，然後選取測試。不需要額外的輸入。這應該會建立憑證 EC2 執行個體，以更新 Secret Manager 中的憑證和 PrivateKey 秘密。秘密更新後，執行個體會自動終止。
5. 終止現有的 dcv-gateway 執行個體：`<env-name>-vdc-gateway`並等待自動擴展群組自動部署新的執行個體。

錯誤詳細資訊

Let's Encrypt 將於 2025 年結束 OCSP 支援。從 2025 年 1 月 30 日開始，除非請求帳戶先前已發行包含 OCSP 必須取代延伸的憑證，否則 OCSP 必須取代請求將會失敗。如需詳細資訊，請參閱 https://letsencrypt.org/2024/12/05/ending-ocsp/：//。

.....

(2024.12 和 2024.12.01) Active Directory 使用者無法 SSH 到堡壘主機

錯誤描述

Active Directory 使用者在依照 RES Web 入口網站的指示連線至堡壘主機時，會收到許可遭拒的錯誤。

由於缺少環境變數，在堡壘主機上執行的 Python 應用程式無法啟動 SSSD 服務。因此，AD 使用者對作業系統未知，無法登入。

受影響的版本

2024.12 和 2024.12.01

緩解

1. 從 EC2 主控台連線至堡壘主機執行個體。
2. 在 IDEA_CLUSTER_NAME 下編輯`/etc/environment`並新增 `environment_name=<res-environment-name>` 作為新行。
3. 在執行個體上執行下列命令：

```
source /etc/environment
sudo service supervisord restart
sudo systemctl restart supervisord
```

4. 請依照 RES Web 入口網站的指示，嘗試再次連線至堡壘主機。

.....

(2024.10) 針對部署在隔離 VPCs 中的 RES 環境，VDI 自動停止中斷

錯誤描述

在 2024.10 RES 版本中，已為閒置一段時間的 VDIs 自動停止。此設定可在桌面設定 → 伺服器 → 工作階段中設定。

部署在隔離 VPCs 中的 RES 環境目前不支援 VDI 自動停止。

受影響的版本

2024.10

緩解

我們目前正在處理將包含在未來版本中的修正。不過，仍然可以在 RES 環境中手動停止部署在隔離 VPCs中的 VDIs。

.....

(2024.10 及更早版本） 無法啟動 VDI for Graphic 增強型執行個體類型

錯誤描述

在圖形增強型執行個體類型 (g4、g5) 上啟動 Amazon Linux 2 - x86_64、RHEL 8 - x86_64 或 RHEL 9 x86_64 VDI 時，執行個體會卡在佈建狀態。這表示執行個體永遠不會進入「就緒」狀態，且可供連線使用。

這是因為 X Server 無法在執行個體上正確執行個體化。套用此修補程式之後，我們也建議您將圖形執行個體的軟體堆疊根磁碟區大小增加到 50gb，以確保有足夠的空間安裝所有相依性。

受影響的版本

所有 RES 2024.10 版或更早版本。

緩解

1. 下載 patch.py 和 graphic_enhanced_instance_types_fix.patch，方法是將 取代`<output-directory>`為您要下載修補程式指令碼和修補程式檔案的目錄，並將 `<environment-name>`取代為下列命令中的 RES 環境名稱：

   a. 修補程式僅適用於 RES 2024.10。
   b. 修補程式指令碼需要 AWS CLI v2、Python 3.9.16 或更新版本，以及 Boto3。
   c. 為部署 AWS RES 的帳戶和區域設定 CLI，並確保您具有寫入 RES 所建立儲存貯體的 S3 許可。

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.10/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
```

```
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.10/patch_scripts/patches/graphic_enhanced_instance_types_fix.patch --
output ${OUTPUT_DIRECTORY}/graphic_enhanced_instance_types_fix.patch
```

2. 導覽至下載修補程式指令碼和修補程式檔案的目錄。執行下列修補程式命令：

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.10 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
graphic_enhanced_instance_types_fix.patch
```

3. 若要終止您環境的虛擬桌面控制器 (vdc-controller) 執行個體，請執行下列命令，取代顯示的 RES 環境名稱。

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

4. 在名稱開頭為 的目標群組`<RES-EnvironmentName>-vdc-ext`正常運作後，啟動新的執行個體。我們建議您為圖形執行個體註冊的任何新軟體堆疊至少要有 50GB 的儲存空間。

.....

(2024.08) 準備基礎設施 AMI 失敗

錯誤描述

當您根據先決條件文件中列出的指示使用 EC2 Image Builder 準備 AMIs 時，建置程序會失敗，並顯示下列錯誤訊息：

```
CmdExecution: [ERROR] Command execution has resulted in an error
```

這是因為文件中提供的相依性檔案中的錯誤。

受影響的版本

2024.08

緩解

建立新的 EC2 Image Builder 資源：

（如果您從未為 RES 執行個體準備 AMIs請遵循以下步驟）

1. 下載更新的 res-infra-dependencies.tar.gz 檔案。
2. 請遵循先決條件頁面上準備 Amazon Machine Image AMIs) 中列出的步驟。

重複使用先前的 EC2 Image Builder 資源：

（如果您已為 RES 執行個體準備 AMIs請遵循以下步驟）

1. 下載更新的 res-infra-dependencies.tar.gz 檔案。
2. 導覽至 EC2 Image Builder → 元件 → 按一下為準備 RES AMIs元件。
3. 請注意內容 → DownloadRESInstallScripts 步驟 → 輸入 → 來源下列出的 S3 位置。
4. 上面找到的 S3 位置包含先前使用的相依性檔案，請將此檔案取代為第一個步驟中下載的檔案。

.....

(2024.08) 虛擬桌面無法掛載具有根儲存貯體 ARN 和自訂字首的讀取/寫入 Amazon S3 儲存貯體

錯誤描述

研究和工程 Studio 2024.08 在使用根儲存貯體 ARN（即）和自訂字首（專案名稱或專案名稱和使用者名稱）時，無法在虛擬桌面基礎設施 (VDI`arn:aws:s3:::example-bucket`) 執行個體上掛載讀取/寫入 S3 儲存貯體。

不受此問題影響的儲存貯體組態包括：

- 唯讀儲存貯體
- 具有字首做為儲存貯體 ARN（即 `arn:aws:s3:::example-bucket/example-folder-prefix`) 和自訂字首（專案名稱或專案名稱和使用者名稱）一部分的讀取/寫入儲存貯體
- 具有根儲存貯體 ARN 但沒有自訂字首的讀取/寫入儲存貯體

佈建 VDI 執行個體之後，該 S3 儲存貯體的指定掛載目錄將不會掛載儲存貯體。雖然 VDI 上的掛載目錄將存在，但目錄將為空，且不會包含儲存貯體的目前內容。當您使用終端機將檔案寫入目錄

時，`Permission denied, unable to write a file`將會擲回錯誤，而且檔案內容不會上傳到對應的 S3 儲存貯體。

受影響的版本

2024 年 8 月

緩解

1. 若要下載修補程式指令碼和修補程式檔案 (`patch.py` 和 `s3_mount_custom_prefix_fix.patch`)，請執行下列命令，將 取代`<output-directory>`為您要下載修補程式指令碼和修補程式檔案的目錄，並將 `<environment-name>`取代為 RES 環境的名稱：

   a. 此修補程式僅適用於 RES 2024.08。
   b. 修補程式指令碼需要 AWS CLI v2、Python 3.9.16 或更新版本，以及 Boto3。
   c. 為部署 RES 的帳戶和區域設定 AWS CLI，並確保您具有 Amazon S3 寫入 RES 建立之儲存貯體的許可。

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.08/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.08/patch_scripts/patches/s3_mount_custom_prefix_fix.patch --output
 ${OUTPUT_DIRECTORY}/s3_mount_custom_prefix_fix.patch
```

2. 導覽至下載修補程式指令碼和修補程式檔案的目錄。執行下列修補程式命令：

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.08 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
s3_mount_custom_prefix_fix.patch
```

3. 若要終止您環境的虛擬桌面控制器 (vdc-controller) 執行個體，請執行下列命令。（您已在第一個步驟中將`ENVIRONMENT_NAME`變數設定為 RES 環境的名稱。）

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
```

```
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

> **Note**
>
> 對於私有 VPC 設定，如果您尚未這麼做，則對於 `<RES-EnvironmentName>-vdc-custom-credential-broker-lambda`函數，請務必新增名稱為 `AWS_STS_REGIONAL_ENDPOINTS`且值`Environment variable`為 的 `regional`。如需詳細資訊，請參閱隔離 VPC 部署的 Amazon S3 儲存貯體先決條件。

4. 以名稱開頭的目標群組*`<RES-EnvironmentName>`*`-vdc-ext`運作狀態良好後，將需要啟動新的 VDIs，其將具有已正確掛載根儲存貯體 ARN 和自訂字首的讀取/寫入 S3 儲存貯體。

.....

(2024.06) 當 AD 群組名稱包含空格時，套用快照失敗

問題

如果 AD 群組名稱中包含空格，RES 2024.06 無法套用先前版本的快照。

在 AD 同步期間，叢集管理員 CloudWatch 日誌（在`<environment-name>/cluster-manager`日誌群組下）將包含下列錯誤：

```
[apply-snapshot] authz.role-assignments/<Group name with
 spaces>:group#<projectID>:project FAILED_APPLY because: [INVALID_PARAMS] Actor key
 doesn't match the regex pattern ^[a-zA-Z0-9_.][a-zA-Z0-9_.-]{1,20}:(user|group)$
```

RES 產生的錯誤僅接受符合下列要求的群組名稱：

- 它只能包含小寫和大寫 ASCII 字母、數字、破折號 (-)、句點 (.) 和底線 (_)
- 不允許破折號 (-) 做為第一個字元
- 其中不可含有空格。

受影響的版本

2024.06

緩解

1. 若要下載修補程式指令碼和修補程式檔案 (https：//patch.py 和 groupname_regex.patch)，請執行下列命令，<output-directory>將 取代為您要放置檔案的目錄，並將 <environment-name>取代為 RES 環境的名稱：

   a. 此修補程式僅適用於 RES 2024.06

   b. 修補程式指令碼需要 AWS CLI v2、Python 3.9.16 或更新版本，以及 Boto3。

   c. 為部署 RES 的帳戶和區域設定 AWS CLI，並確保您具有寫入 RES 建立之儲存貯體的 S3 許可：

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

mkdir -p ${OUTPUT_DIRECTORY}
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py
curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patches/groupname_regex.patch --output
 ${OUTPUT_DIRECTORY}/groupname_regex.patch
```

2. 導覽至下載修補程式指令碼和修補程式檔案的目錄。執行下列修補程式命令：

```
python3 patch.py --environment-name ${ENVIRONMENT_NAME} --res-version 2024.06 --
module cluster-manager --patch ${OUTPUT_DIRECTORY}/groupname_regex.patch
```

3. 若要重新啟動您環境的 Cluster Manager 執行個體，請執行下列命令：您也可以從 Amazon EC2 管理主控台終止執行個體。

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

> **Note**
>
> 修補程式允許 AD 群組名稱包含大小寫 ASCII 字母、數字、破折號 (-)、句點 (.)、底線 (_) 和總長度介於 1 到 30 之間的空格。

.....

(2024.06 及更早版本） AD 同步期間未同步至 RES 的群組成員

錯誤描述

如果 GroupOU 與 UserOU 不同，群組成員將無法正確同步至 RES。

RES 會在嘗試從 AD 群組同步使用者時建立 ldapsearch 篩選條件。目前的篩選條件不正確地使用 UserOU 參數，而不是 GroupOU 參數。結果是搜尋無法傳回任何使用者。此行為只會發生在 UsersOU 和 GroupOU 不同的執行個體中。

受影響的版本

所有 RES 2024.06 版或更早版本

緩解

請依照下列步驟來解決問題：

1. 若要下載 patch.py 指令碼和 group_member_sync_bug_fix.patch 檔案，請執行下列命令，`<output-directory>`將 取代為您要下載檔案的本機目錄，並將 `<res_version>`取代為您要修補的 RES 版本：

   > **Note**
   >
   > - 修補程式指令碼需要 AWS CLI v2、Python 3.9.16 或更新版本，以及 Boto3。
   > - 為部署 AWS RES 的帳戶和區域設定 CLI，並確保您擁有寫入 RES 建立之儲存貯體的 S3 許可。
   > - 此修補程式僅支援 RES 2024.04.02 和 2024.06 版。如果您使用的是 2024.04 或 2024.04.01，您可以遵循 中列出的步驟次要版本更新，先將環境更新為 2024.04.02，然後再套用修補程式。
   > - RES 版本：RES 2024.04.02

修補程式下載連結：2024.04.02_group_member_sync_bug_fix.patch

- RES 版本：RES 2024.06

  修補程式下載連結：2024.06_group_member_sync_bug_fix.patch

```
OUTPUT_DIRECTORY=<output-directory>
RES_VERSION=<res_version>
mkdir -p ${OUTPUT_DIRECTORY}

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/releases/
${RES_VERSION}/patch_scripts/patches/${RES_VERSION}_group_member_sync_bug_fix.patch
 --output ${OUTPUT_DIRECTORY}/${RES_VERSION}_group_member_sync_bug_fix.patch
```

2. 導覽至下載修補程式指令碼和修補程式檔案的目錄。執行下列修補程式命令，`<environment-name>`將 取代為您的 RES 環境名稱：

```
cd ${OUTPUT_DIRECTORY}
ENVIRONMENT_NAME=<environment-name>

python3 patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version ${RES_VERSION} --module cluster-manager --patch $PWD/
${RES_VERSION}_group_member_sync_bug_fix.patch
```

3. 若要重新啟動您環境的 cluster-manager 執行個體，請執行下列命令：

```
INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.06 及更早版本） CVE-2024-6387、RegreSSHion、RHEL9 和 Ubuntu VDIs中的安全漏洞

錯誤描述

OpenSSH 伺服器中已識別稱為 regreSSHion 的 CVE-2024-6387。此漏洞可讓未驗證的遠端攻擊者在目標伺服器上執行任意程式碼，為利用 OpenSSH 進行安全通訊的系統帶來嚴重風險。

對於 RES，標準組態是透過堡壘主機進入 SSH 進入虛擬桌面，而堡壘主機不受此漏洞影響。不過，我們在所有 RES 版本中為 RHEL9 和 Ubuntu2024 VDIs（虛擬桌面基礎設施）提供的預設 AMI (Amazon Machine Image) 會使用易受安全威脅影響的 OpenSSH 版本。

這表示現有的 RHEL9 和 Ubuntu2024 VDIs 可以利用，但攻擊者需要存取堡壘主機。

如需問題的詳細資訊，請參閱此處。

受影響的版本

所有 RES 2024.06 版或更早版本。

緩解

RHEL9 和 Ubuntu 都已針對 OpenSSH 發行修補程式，以修正安全性漏洞。您可以使用平台各自的套件管理員提取這些套件。

如果您有現有的 RHEL9 或 Ubuntu VDIs，建議您遵循以下 PATCH EXISTING VDIs說明。若要修補未來的 VDIs，建議您遵循 PATCH FUTURE VDIs指示。這些指示說明如何執行指令碼，在您的 VDIs 上套用平台更新。

修補現有的 VDIs

1. 執行下列命令來修補所有現有的 Ubuntu 和 RHEL9 VDIs：

   a. 修補程式指令碼需要 AWS CLI v2。
   b. 為部署 AWS RES 的帳戶和區域設定 CLI，並確保您具有傳送 AWS Systems Manager Run Command 的 Systems Manager 許可。

```
aws ssm send-command \
    --document-name "AWS-RunRemoteScript" \
    --targets "Key=tag:res:NodeType,Values=virtual-desktop-dcv-host" \
    --parameters '{"sourceType":["S3"],"sourceInfo":["{\"path\":\"https://
research-engineering-studio-us-east-1.s3.amazonaws.com/releases/2024.06/
```

```
patch_scripts/scripts/patch_openssh.sh\"}"],"commandLine":["bash
 patch_openssh.sh"]}'
```

2. 您可以在執行命令頁面上驗證指令碼是否成功執行。按一下命令歷史記錄索引標籤，選取最新的命令 ID，並確認所有執行個體 IDs都有 SUCCESS 訊息。

修補未來 VDIs

1. 若要下載修補程式指令碼和修補程式檔案 (https：//patch.py 和 update_openssh.patch)，請執行下列命令，<output-directory>將 取代為您要下載檔案的目錄，並將 <environment-name>取代為 RES 環境的名稱：

> **Note**
>
> - 此修補程式僅適用於 RES 2024.06。
> - 修補程式指令碼需要 AWS CLI v2、Python 3.9.16 或更新版本，以及 Boto3。
> - 為部署 AWS RES 的帳戶和區域設定 CLI 複本，並確保您擁有寫入 RES 所建立儲存貯體的 S3 許可。

```
OUTPUT_DIRECTORY=<output-directory>
ENVIRONMENT_NAME=<environment-name>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.06/patch_scripts/patches/update_openssh.patch --output
 ${OUTPUT_DIRECTORY}/update_openssh.patch
```

2. 執行下列修補程式命令：

```
python3 ${OUTPUT_DIRECTORY}/patch.py --environment-name ${ENVIRONMENT_NAME} --res-
version 2024.06 --module virtual-desktop-controller --patch ${OUTPUT_DIRECTORY}/
update_openssh.patch
```

3. 使用下列命令重新啟動您環境的 VDC 控制器執行個體：

```
INSTANCE_ID=$(aws ec2 describe-instances \
```

```
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

> **Important**
>
> 只有 RES 2024.06 版和更新版本才支援修補未來的 VDIs。若要在 RES 環境中使用早於 2024.06 的版本修補未來的 VDIs，請先使用下列指示將 RES 環境升級至 2024.06：主要版本更新。

.....

(2024.04-2024.04.02) 提供未連接至 VDI 執行個體角色的 IAM 許可界限

問題

虛擬桌面工作階段未正確繼承其專案的許可界限組態。這是 IAMPermissionBoundary 參數定義的許可界限在建立專案期間未正確指派給專案的結果。

受影響的版本

2024.04 - 2024.04.02

緩解

請依照下列步驟，允許 VDIs 正確繼承指派給專案的許可界限：

1. 若要下載修補程式指令碼和修補程式檔案 (patch.py 和 vdi_host_role_permission_boundary.patch)，請執行下列命令，`<output-directory>`將 取代為您要放置檔案的本機目錄：

   a. 修補程式僅適用於 RES 2024.04.02。如果您使用的是 2024.04 或 2024.04.01 版，您可以依照公有文件中列出的步驟進行次要版本更新，將環境更新至 2024.04.02。

   b. 修補程式指令碼需要 AWS CLI v2、Python 3.9.16 或更新版本，以及 Boto3。

c. 為部署 AWS RES 的帳戶和區域設定 CLI，並確保您具有寫入 RES 所建立儲存貯體的 S3 許可。

```
OUTPUT_DIRECTORY=<output-directory>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_host_role_permission_boundary.patch
 --output ${OUTPUT_DIRECTORY}/vdi_host_role_permission_boundary.patch
```

2. 導覽至下載修補程式指令碼和修補程式檔案的目錄。執行下列修補程式命令，`<environment-name>`將 取代為您的 RES 環境名稱：

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch vdi_host_role_permission_boundary.patch
```

3. 執行此命令以 RES 環境`<environment-name>`的名稱取代 ，以重新啟動您環境中的 cluster-manager 執行個體。您也可以從 Amazon EC2 管理主控台終止執行個體。

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.04.02 及更早版本） ap-southeast-2（雪梨） 中的 Windows NVIDIA 執行個體無法啟動

問題

Amazon Machine Image AMIs) 用於在具有特定組態的 RES 中啟動虛擬桌面 (VDIs)。每個 AMI 都有每個區域的關聯 ID。在 RES 中設定為在 ap-southeast-2（雪梨）中啟動 Windows Nvidia 執行個體的 AMI ID 目前不正確。

這類執行個體組態`ami-0e190f8939a996caf`的 AMI-ID 錯誤地列在 ap-southeast-2（雪梨）中。`ami-027cf6e71e2e442f4` 應該改用 AMI ID。

嘗試使用預設 `ami-0e190f8939a996caf` AMI 啟動執行個體時，使用者會收到下列錯誤。

```
An error occured (InvalidAMIID.NotFound) when calling the RunInstances operation: The
 image id ‘[ami-0e190f8939a996caf]’ does not exist
```

重現錯誤的步驟，包括範例組態檔案：

- 在 ap-southeast-2 區域中部署 RES。
- 使用 Windows-NVIDIA 預設軟體堆疊 (AMI ID `ami-0e190f8939a996caf`) 啟動執行個體。

受影響的版本

所有 RES 2024.04.02 版或更早版本都會受到影響

緩解

RES 2024.01.01 版已測試下列緩解措施：

- 使用下列設定註冊新的軟體堆疊
  - AMI ID：`ami-027cf6e71e2e442f4`
  - 作業系統：Windows
  - GPU 製造商：NVIDIA
  - 最小值 儲存大小 (GB)：30
  - 最小值 RAM (GB)：4
- 使用此軟體堆疊來啟動 Windows-NVIDIA 執行個體

.....

(2024.04 和 2024.04.01) GovCloud 中的 RES 刪除失敗

問題

在 RES 刪除工作流程期間，`UnprotectCognitoUserPoolLambda` 會停用稍後將刪除的 Cognito 使用者集區的刪除保護。Lambda 執行由 啟動`InstallerStateMachine`。

由於商業和 GovCloud AWS 區域之間的預設 CLI 版本差異，Lambda 中的`update_user_pool`呼叫會在 GovCloud 區域失敗。

嘗試刪除 GovCloud 區域中的 RES 時，客戶會收到下列錯誤：

```
Parameter validation failed: Unknown parameter in input: \"DeletionProtection
\", must be one of: UserPoolId, Policies, LambdaConfig, AutoVerifiedAttributes,
 SmsVerificationMessage, EmailVerificationMessage, EmailVerificationSubject,
 VerificationMessageTemplate, SmsAuthenticationMessage, MfaConfiguration,
 DeviceConfiguration, EmailConfiguration, SmsConfiguration, UserPoolTags,
 AdminCreateUserConfig, UserPoolAddOns, AccountRecoverySetting
```

重現錯誤的步驟：

- 在 GovCloud 區域中部署 RES
- 刪除 RES 堆疊

受影響的版本

RES 2024.04 和 2024.04.01 版

緩解

RES 2024.04 版已測試下列緩解措施：

- 開啟 `UnprotectCognitoUserPool` Lambda
  - 命名慣例： `<env-name>-InstallerTasksUnprotectCognitoUserPool-...`
- 執行時間設定 -> 編輯 -> 選取執行時間 `Python 3.11` -> 儲存。
- 開啟 CloudFormation。
- 刪除 RES 堆疊 -> 保留保留安裝程式資源 UNCHECKED -> 刪除。

.....

(2024.04 - 2024.04.02) 重新啟動時，Linux 虛擬桌面可能卡在「繼續」狀態

問題

在手動或排程停止之後重新啟動時，Linux 虛擬桌面可能會卡在「恢復」狀態。

重新啟動執行個體後， AWS Systems Manager 不會執行任何遠端命令來建立新的 DCV 工作階段，而且 vdc-controller CloudWatch 日誌中缺少下列日誌訊息 (`<environment-name>/vdc/controller`在 CloudWatch 日誌群組下）：

```
Handling message of type DCV_HOST_REBOOT_COMPLETE_EVENT
```

受影響的版本

2024.04 - 2024.04.02

緩解

若要復原卡在「恢復」狀態的虛擬桌面：

1. 從 EC2 主控台 SSH 進入問題執行個體。
2. 在執行個體上執行下列命令：

   ```
   sudo su -
   /bin/bash /root/bootstrap/latest/virtual-desktop-host-linux/
   configure_post_reboot.sh
   sudo reboot
   ```

3. 等待執行個體重新啟動。

若要防止新的虛擬桌面執行到相同的問題：

1. 若要下載修補程式指令碼和修補程式檔案 (patch.py 和 vdi_stuck_in_resuming_status.patch)，請執行下列命令，`<output-directory>`將 取代為您要放置檔案的目錄：

   > **Note**
   >
   > - 修補程式僅適用於 RES 2024.04.02。
   > - 修補程式指令碼需要 AWS CLI v2、Python 3.9.16 或更新版本，以及 Boto3。
   > - 為部署 AWS RES 的帳戶和區域設定 CLI，並確保您具有寫入 RES 所建立儲存貯體的 S3 許可。

```
OUTPUT_DIRECTORY=<output-directory>

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
releases/2024.04.02/patch_scripts/patches/vdi_stuck_in_resuming_status.patch --
output ${OUTPUT_DIRECTORY}/vdi_stuck_in_resuming_status.patch
```

2. 導覽至下載修補程式指令碼和修補程式檔案的目錄。執行下列修補程式命令，<environment-name>將 取代為您的 RES 環境名稱，並將 <aws-region>取代為部署 RES 的區域：

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02
 --module virtual-desktop-controller --patch vdi_stuck_in_resuming_status.patch --
region <aws-region>
```

3. 若要重新啟動您環境的 VDC 控制器執行個體，請執行下列命令，<environment-name>將 取代為您的 RES 環境名稱：

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-vdc-controller \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.04.02 及更早版本） 無法同步 SAMAccountName 屬性包含大寫字母或特殊字元的 AD 使用者

問題

SSO 設定至少兩個小時後（兩個 AD 同步週期），RES 無法同步 AD 使用者。叢集管理員 CloudWatch 日誌（在`<environment-name>/cluster-manager`日誌群組下）在 AD 同步期間包含下列錯誤：

```
Error: [INVALID_PARAMS] Invalid params: user.username must match regex: ^(?=.{3,20}$)
(?![_.])(?!.*[_.]{2})[a-z0-9._]+(?<![_.])$
```

RES 產生的錯誤僅接受符合下列要求的 SAMAccount 使用者名稱：

- 它只能包含小寫 ASCII 字母、數字、句點 (.)、底線 (_)。
- 句點或底線不允許做為第一個或最後一個字元。
- 它不能包含兩個連續的句點或底線（例如 ..、__、._、_.)。

受影響的版本

2024.04.02 及更早版本

緩解

1. 若要下載修補程式指令碼和修補程式檔案 (patch.py 和 samaccountname_regex.patch)，請執行下列命令，`<output-directory>`將 取代為您要放置檔案的目錄：

   > **Note**
   >
   > - 修補程式僅適用於 RES 2024.04.02。
   > - 修補程式指令碼需要 AWS CLI v2、Python 3.9.16 或更新版本，以及 Boto3。
   > - 為部署 AWS RES 的帳戶和區域設定 CLI，並確保您具有寫入 RES 所建立儲存貯體的 S3 許可。

   ```
   OUTPUT_DIRECTORY=<output-directory>

   curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
   releases/2024.04.02/patch_scripts/patch.py --output ${OUTPUT_DIRECTORY}/patch.py

   curl https://research-engineering-studio-us-east-1.s3.amazonaws.com/
   releases/2024.04.02/patch_scripts/patches/samaccountname_regex.patch --output
    ${OUTPUT_DIRECTORY}/samaccountname_regex.patch
   ```

2. 導覽至下載修補程式指令碼和修補程式檔案的目錄。執行下列修補程式命令，<environment-name>將 取代為您的 RES 環境名稱：

```
python3 patch.py --environment-name <environment-name> --res-version 2024.04.02 --
module cluster-manager --patch samaccountname_regex.patch
```

3. 若要重新啟動您環境的 Cluster Manager 執行個體，請執行下列命令，<environment-name>將取代為您的 RES 環境名稱。您也可以從 Amazon EC2 管理主控台終止執行個體。

```
ENVIRONMENT_NAME=<environment-name>

INSTANCE_ID=$(aws ec2 describe-instances \
    --filters \
    Name=tag:Name,Values=${ENVIRONMENT_NAME}-cluster-manager \
    Name=tag:res:EnvironmentName,Values=${ENVIRONMENT_NAME}\
    --query "Reservations[0].Instances[0].InstanceId" \
    --output text)

aws ec2 terminate-instances --instance-ids ${INSTANCE_ID}
```

.....

(2024.04.02 及更早版本） 用於存取堡壘主機的私有金鑰無效

問題

當使用者從 RES Web 入口網站下載私有金鑰以存取堡壘主機時，金鑰格式不正確 – 多行下載為單行，這會使金鑰無效。當使用者嘗試使用下載的金鑰存取堡壘主機時，會收到下列錯誤：

```
Load key "<downloaded-ssh-key-path>": error in libcrypto
<user-name>@<bastion-host-public-ip>: Permission denied (publickey,gssapi-keyex,gssapi-
with-mic)
```

受影響的版本

2024.04.02 及更早版本

緩解

我們建議您使用 Chrome 下載金鑰，因為此瀏覽器不受影響。

或者，可以透過在 後面建立新行-----BEGIN PRIVATE KEY-----，然後在 前面建立新行來重新格式化金鑰檔案-----END PRIVATE KEY-----。

.....

注意

每個 Amazon EC2 執行個體都隨附兩個遠端桌面服務（終端服務）授權，以供管理之用。此資訊可協助您為管理員佈建這些授權。您也可以使用 AWS Systems Manager Session Manager，這可讓 在沒有 RDP 的情況下遠端登入 Amazon EC2 執行個體，而不需要 RDP 授權。如果需要額外的遠端桌面服務授權，則應向 Microsoft 或 Microsoft 授權經銷商購買遠端桌面使用者 CALs。具有有效軟體保證的遠端桌面使用者 CALs 具有授權行動性優勢，並可帶入 AWS 預設（共用）租用戶環境。如需有關在沒有軟體保證或授權行動性利益的情況下取得授權的資訊，請參閱 常見問答集的本節。

客戶有責任對本文件中的資訊進行自己的獨立評定。本文件： (a) 僅供參考， (b) 代表 AWS 目前的產品產品和實務， 可能隨時變更，恕不另行通知。 和 (c) 不會從 AWS 及其附屬公司建立任何承諾或保證， 供應商或 licensors. AWS products 或服務會以「原樣」方式提供，不做任何保證， 表示法、 或任何類型的條件， 無論明示還是暗示。 對客戶 AWS 的責任和責任都由 AWS 協議控制， 本文件不屬於 也不會修改 AWS 與其客戶之間的任何協議。

上的研究和工程 Studio AWS 是根據 Apache Software Foundation 提供的 Apache License 2.0 版條款進行授權。

修訂

如需詳細資訊，請參閱 GitHub 儲存庫中的 CHANGELOG.md 檔案。

日期	變更
2025 年 3 月	• 發行版本 2025.03 新增章節 — • 停用專案. • 刪除專案. • 成本分析儀表板. 已變更的區段 — • 虛擬桌面. • 軟體堆疊 (AMIs). • 設定 RES 就緒 AMIs. • 桌面設定. • 設定 SSH 存取. • Active Directory 同步.
2024 年 12 月	• 發行版本 2024.12 新增章節 — • Active Directory 同步. • 設定桌面許可. • 設定檔案瀏覽器存取. • 設定 SSH 存取. • 設定 Amazon Cognito 使用者. 已變更的區段 — • 環境界限. • 設定私有 VPC （選用）.
2024 年 10 月	• 2024.10 版：新增對 的支援：

日期	變更
	• 環境界限. • 桌面共用設定檔. • 虛擬桌面界面自動停止.

2024 年 8 月	• 2024.08 版：新增對 的支援：
	  • 將 Amazon S3 儲存貯體掛載到 Linux Virtual Desktop Infrastructure (VDI) 執行個體。請參閱 Amazon S3 儲存貯體。
	  • 自訂專案許可，一種增強型許可模型，允許自訂現有角色和新增自訂角色。請參閱 許可政策。
	• 使用者指南：已展開 疑難排解區段。

2024 年 6 月	• 2024.06 版 — Ubuntu 支援、專案擁有者許可。 • 使用者指南：已新增 建立示範環境
2024 年 4 月	2024.04 版 — RES 就緒 AMIs和專案啟動範本
2024 年 3 月	其他疑難排解主題、CloudWatch Logs 保留、解除安裝次要版本
2024 年 2 月	版 2024.01.01 — 更新的部署範本
2024 年 1 月	發行版本 2024.01
2023 年 12 月	已新增 GovCloud 方向和範本
2023 年 11 月	初始版本

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。