aws

使用者指南

Amazon Lightsail for Research

Amazon Lightsail for Research: 使用者指南

Table of Contents

什麼是 Amazon Lightsail 的研究？ 1
定價 1
可用性 1
設定 2
註冊 AWS 帳戶 2
建立具有管理存取權的使用者 2
入門教學課程 4
步驟 1：完成先決條件 4
步驟2：建立虛擬電腦 4
步驟3：啟動虛擬電腦的應用程式 5
步驟 4：連線至虛擬電腦 5
步驟 5：將儲存新增至您的虛擬電腦 6
步驟 6：建立快照 7
步驟 7：清除 7
教學課程 9
開始使用 JupyterLab 9
步驟 1：完成先決條件 9
步驟 2：(選用) 新增儲存空間 10
步驟 3：上傳並下載檔案 10
步驟 4：啟動 JupyterLab應用程式 11
步驟 5：閱讀 JupyterLab文件 15
步驟 6：(選用) 監控用量和成本 15
步驟 7：(選用) 建立成本控制規則 17
步驟 8：(選用) 建立快照 18
步驟 9：(選用) 停止或刪除您的虛擬電腦 18
開始使用 RStudio 19
步驟 1：完成先決條件 20
步驟 2：(選用) 新增儲存空間 20
步驟 3：上傳並下載檔案 20
步驟 4：啟動RStudio應用程式 21
步驟 5：閱讀RStudio文件 25
步驟 6：(選用) 監控用量和成本 27
步驟 7：(選用) 建立成本控制規則 28
步驟 8：(選用) 建立快照 29

步驟 9：(選用) 停止或刪除您的虛擬電腦 29
虛擬電腦 31
應用程式和硬體方案 31
應用程式 32
計畫 33
建立虛擬電腦 34
檢視虛擬電腦詳細資訊 34
啟動虛擬電腦的應用程式 35
存取虛擬電腦的作業系統 36
防火牆連接埠 37
通訊協定 37
連接埠 37
為何要開啟和關閉連接埠 38
完成先決條件 38
取得虛擬電腦的連接埠狀態 38
開啟虛擬電腦的連接埠 39
關閉虛擬電腦的連接埠 41
繼續後續步驟 42
取得虛擬電腦的金鑰對 42
完成先決條件 43
取得虛擬電腦的金鑰對 43
繼續後續步驟 48
使用 連線至虛擬電腦 SSH 49
完成先決條件 49
使用 連線至虛擬電腦 SSH 50
繼續後續步驟 56
使用 將檔案傳輸至虛擬電腦 SCP 56
完成先決條件 57
使用 連線至虛擬電腦 SCP 57
刪除虛擬電腦 61
儲存 62
建立磁碟 62
檢視磁碟 63
將磁碟連接至虛擬電腦 63
將磁碟與虛擬電腦分離 64
刪除磁碟 64

快照 65
建立快照 65
檢視快照 66
從快照建立虛擬電腦或磁碟 66
刪除快照 66
成本和用量 68
檢視成本和用量 68
成本控制規則 71
建立規則 71
刪除規則 72
標籤 73
建立標籤 73
刪除標籤 74
安全 75
資料保護 75
身分和存取權管理 76
物件 77
使用身分驗證 77
使用政策管理存取權 80
Amazon Lightsail for Research 如何與 搭配使用 IAM 82
身分型政策範例 87
故障診斷 90
法規遵循驗證 91
恢復能力 92
基礎架構安全 92
組態與漏洞分析 93
安全最佳實務 93
文件進版記錄 94
..... xcv

什麼是 Amazon Lightsail 的研究？

透過 Amazon Lightsail 研究用，學者和研究人員可以在 Amazon Web Services (AWS) 雲端中建立功能強大的虛擬電腦。這些虛擬計算機帶有預先安裝的研究應用程序，例如RStudio和 Scilab。

有了 Lightsail 研究版，您可以直接從網頁瀏覽器上傳資料以開始您的工作。您隨時可以建立和刪除虛擬電腦，讓您隨需存取強大的運算資源。

您只需在您需要虛擬電腦時支付費用。Lightsail 為研究提供預算控制功能，可在電腦達到預先設定的成本限制時自動停止運作，因此您不必擔心超額費用。

您在 Lightsail 適用於研究的主控台中所做的一切都是由公開提供API的支援。了解如何安裝AWS CLI和使API用 Amazon Lightsail。

定價

使用 Lightsail 研究版，您只需為您建立和使用的資源付費。如需詳細資訊，請參閱 Lightsail 適用於研究的定價。

可用性

適用於研究的 Lightsail 可在與 Amazon Lightsail 相同的 AWS 區域使用，但美國東部 (維吉尼亞北部) 區域除外。適用於研究的 Lightsail 也使用與 Lightsail 相同的端點。若要檢視 Lightsail 目前支援的 AWS 區域和端點，請參閱AWS 一般參考中的 Lightsail 端點和配額。

設定 Amazon Lightsail for Research

如果您是新 AWS 客戶，請先完成此頁面列出的設定先決條件，再開始使用 Amazon Lightsail for Research。

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟以建立 。

若要註冊 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

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

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時前往 https://aws.amazon.com/ 並選擇我的帳戶 來檢視目前的帳戶活動和管理帳戶。

建立具有管理存取權的使用者

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

保護您的 AWS 帳戶根使用者

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

   如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的以根使用者身分登入。
2. 為您的根使用者開啟多重要素驗證 （MFA）。

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

建立具有管理存取權的使用者

1. 啟用IAM身分中心。

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

   如需使用 IAM Identity Center 目錄 作為身分來源的教學課程，請參閱 AWS IAM Identity Center 使用者指南 中的使用 設定使用者存取權 IAM Identity Center 目錄。

以具有管理存取權的使用者身分登入

- 若要使用 IAM Identity Center 使用者登入，請使用您建立 IAM Identity Center 使用者時URL傳送到您電子郵件地址的登入。

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

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立遵循套用最低權限許可最佳實務的許可集。

   如需指示，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。
2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

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

教學課程：Lightsail for Research 虛擬電腦入門

使用此教學課程來開始使用 Amazon Lightsail for Research 虛擬電腦。您將學習如何建立虛擬電腦、連線至虛擬電腦，以及使用虛擬電腦。在 Lightsail for Research 中，虛擬電腦是您在 中建立和管理的研究工作站 AWS 雲端。虛擬電腦是以具有 Ubuntu 作業系統的 Lightsail Linux 執行個體為基礎。在虛擬電腦上，您可以預先設定研究應用程式，例如 JupyterLab、RStudio、Scilab 等。

您在本教學課程中建立的虛擬電腦從建立之時起即會產生使用費用，直到您將其刪除為止。刪除是本教學課程的最後一個步驟。如需定價的詳細資訊，請參閱 Lightsail for Research 定價。

主題

- 步驟 1：完成先決條件
- 步驟2：建立虛擬電腦
- 步驟3：啟動虛擬電腦的應用程式
- 步驟 4：連線至虛擬電腦
- 步驟 5：將儲存新增至您的虛擬電腦
- 步驟 6：建立快照
- 步驟 7：清除

步驟 1：完成先決條件

如果您是新 AWS 客戶，請先完成設定先決條件，再開始使用 Amazon Lightsail for Research。如需詳細資訊，請參閱設定 Amazon Lightsail for Research。

步驟2：建立虛擬電腦

您可以使用 Lightsail for Research 主控台來建立虛擬電腦，如下列程序所述。本教學課程旨在協助快速啟動您的第一個虛擬電腦。我們也建議探索可用的應用程式和硬體方案。如需詳細資訊，請參閱 選擇 Lightsail for Research 的應用程式映像和硬體計劃 和 建立 Lightsail for Research 虛擬電腦。

1. 登入 Lightsail for Research 主控台 。
2. 在首頁上，選擇建立虛擬電腦。
3. AWS 區域 為您的虛擬電腦選取 。

   選擇最接近您實體位置 AWS 區域 的 ，以減少延遲。

4. 選擇應用程式，也稱為 Lightsail 中的藍圖API。

   您選擇的應用程式會在您建立虛擬電腦時安裝並進行設定。

5. 選擇硬體計劃，也稱為 Lightsail 中的套件API。

   硬體計劃提供不同量的處理能力，包括 vCPU 核心、記憶體、儲存體和每月資料傳輸。Lightsail for Research GPU 提供虛擬電腦的標準計劃。當您工作的運算需求很低時，請選擇標準方案。當需求很高時選擇GPU計劃，例如執行機器學習模型或其他運算密集型任務時。

6. 輸入虛擬電腦的名稱。
7. 在摘要面板中，選擇建立虛擬電腦。

在您的新虛擬電腦上線且運行之後，繼續本教學課程的下一節，了解如何啟動電腦的應用程式。

步驟3：啟動虛擬電腦的應用程式

當虛擬電腦建立完成並處於執行中狀態後，您可以在 Web 瀏覽器中啟動虛擬工作階段。透過工作階段，您可以與虛擬電腦上安裝的應用程式互動並進行管理。

1. 在 Lightsail for Research 主控台的導覽窗格中選擇虛擬電腦。
2. 找出您在步驟 1 中建立的虛擬電腦名稱，然後選擇啟動應用程式。例如，啟動 JupyterLab。應用程式工作階段會在新的 Web 瀏覽器視窗中開啟。

   > **Important**
   >
   > 如果您的 Web 瀏覽器有安裝彈出視窗封鎖程式，則在開啟工作階段之前，您可能需要允許來自 aws.amazon.com 網域的彈出視窗。

若要學習如何連接到虛擬電腦，請繼續本教學課程下一個步驟。

步驟 4：連線至虛擬電腦

您可以使用以下方法連線至您的虛擬電腦：

- 使用 Lightsail for Research 主控台中提供的瀏覽器型 Amazon DCV用戶端。透過 Amazon DCV，您可以使用圖形化使用者介面 （GUI） 與研究應用程式和虛擬電腦的作業系統互動。

  您也可以使用瀏覽器型 Amazon DCV用戶端存取虛擬電腦的命令列介面並傳輸檔案。

- 使用 Open SSH、Pu TTY或 Windows Subsystem for Linux 等安全 shell （SSH） 用戶端來存取虛擬電腦的命令列介面。使用SSH用戶端，您可以編輯指令碼和組態檔案。
- 使用安全複製 （SCP） 安全地在本機電腦和虛擬電腦之間傳輸檔案。使用 SCP，您可以在本機啟動工作，並在虛擬電腦上繼續工作。您也可以從虛擬電腦下載檔案，將工作複製到本機電腦。

您必須提供虛擬電腦的金鑰對，才能使用 SSH或 連線到它，才能使用 傳輸檔案SCP。金鑰對是一組安全憑證，用於在連線至 Lightsail for Research 虛擬電腦時證明您的身分。金鑰對包含公有金鑰和私有金鑰。

如需連線至虛擬電腦的詳細資訊，請參閱以下文件：

- 建立遠端顯示協定連線：
  - 存取 Lightsail for Research 虛擬電腦應用程式
  - 存取 Lightsail for Research 虛擬電腦的作業系統
- 使用 建立SSH連線或傳輸檔案SCP：
  - 取得 Lightsail for Research 虛擬電腦的金鑰對
  - 使用 Secure Shell 連線至 Lightsail for Research 虛擬電腦
  - 使用 Secure Copy 將檔案傳輸至 Lightsail for Research 虛擬電腦

若要了解虛擬電腦的儲存，請繼續本教學課程的下一個步驟。

步驟 5：將儲存新增至您的虛擬電腦

Lightsail for Research 提供區塊層級儲存磁碟區 （磁碟），您可以連接至虛擬電腦。即使您的虛擬電腦隨附有系統磁碟，也可以在需求變化時附接額外的儲存磁碟。您也可以將磁碟與虛擬電腦分離，然後連接至另一台虛擬電腦。

當您使用主控台將磁碟連接至虛擬電腦時，Lightsail for Research 會自動格式化並在作業系統中掛載磁碟。此過程需要幾分鐘的時間，因此您應該先確認磁碟處於掛載狀態，然後再開始使用。

如需有關建立、附接和管理磁碟的詳細資訊，請參閱以下文件：

- 在適用於研究的 Lightsail 主控台中建立儲存磁碟
- 在 Lightsail 進行研究的主控台中檢視儲存磁碟詳細資料
- 在 Lightsail 進行研究的虛擬電腦中新增儲存空間
- 在 Lightsail 中將磁碟從虛擬電腦中卸離以進行研究

- 刪除研究用的 Lightsail 中未使用的儲存磁碟

若要了解如何備份虛擬電腦，請繼續本教學課程的下一個步驟。

步驟 6：建立快照

快照是 point-in-time資料的副本。可建立虛擬電腦的快照，並用來作為建立新電腦或資料備份的基準。快照包含還原電腦所需的所有資料 (從建立快照的那一刻開始)。

如需有關建立和管理快照的詳細資訊，請參閱以下文件：

- 建立適用於研究人員的 Lightsail 虛擬電腦或磁碟快照
- 在研究專用 Lightsail 中檢視和管理虛擬電腦和磁碟快照
- 從快照建立虛擬電腦或磁碟
- 在適用於研究的 Lightsail 主控台中刪除快照

若要了解如何清除虛擬電腦資源，請繼續本教學課程的下一個步驟。

步驟 7：清除

如果不再使用為此教學課程建立的虛擬電腦，可將其刪除。如果不再需要，這樣做可停止虛擬電腦產生費用。

刪除虛擬電腦並不會刪除其關聯的快照或連接的磁碟。如果您已建立快照和磁碟，則應手動刪除這些快照和磁碟，以免產生費用。

若要儲存您的虛擬電腦以供日後使用，但又想要避免依標準的每小時價格計費，則可以停止虛擬電腦而不用刪除。然後，您可之後再次將其啟動。如需詳細資訊，請參閱檢視 Lightsail for Research 虛擬電腦詳細資訊。如需定價的詳細資訊，請參閱 Lightsail for Research 定價。

> **Important**
>
> 刪除 Lightsail for Research 資源是永久動作。刪除的資料無法復原。如果之後可能需要該資料，請在刪除之前建立虛擬電腦的快照。如需詳細資訊，請參閱建立快照。

1. 登入 Lightsail for Research 主控台 。

2. 在導覽窗格中，選擇虛擬電腦。
3. 選擇要刪除的虛擬電腦。
4. 選擇動作，然後選擇刪除虛擬電腦。
5. 在文字區塊中鍵入確認。然後，選擇刪除虛擬電腦。

Lightsail for Research 上的資料科學應用程式入門

下列教學課程提供有關如何開始使用 Lightsail for Research 中提供的特定應用程式的其他資訊。

主題

- 在 Lightsail for Research JupyterLab 上啟動和使用
- 在 Lightsail for Research RStudio上啟動和使用

> **Note**
>
> 開始使用 Lightsail for Research 的深入教學課程RStudio，並發佈至 AWS 公部門部落格。如需詳細資訊，請參閱開始使用 Amazon Lightsail for Research：使用 的教學RStudio課程。

在 Lightsail for Research JupyterLab 上啟動和使用

在本教學課程中，我們將示範如何在 Amazon Lightsail for Research 中開始管理和使用 JupyterLab 虛擬電腦。

主題

- 步驟 1：完成先決條件
- 步驟 2：(選用) 新增儲存空間
- 步驟 3：上傳並下載檔案
- 步驟 4：啟動 JupyterLab應用程式
- 步驟 5：閱讀 JupyterLab文件
- 步驟 6：(選用) 監控用量和成本
- 步驟 7：(選用) 建立成本控制規則
- 步驟 8：(選用) 建立快照
- 步驟 9：(選用) 停止或刪除您的虛擬電腦

步驟 1：完成先決條件

如果您尚未使用 JupyterLab 應用程式建立虛擬電腦。如需詳細資訊，請參閱建立 Lightsail for Research 虛擬電腦。

新虛擬電腦啟動並執行後，請繼續本教學課程的應用程式 JupyterLab 區段的啟動。

步驟 2：(選用) 新增儲存空間

您的虛擬電腦隨附系統磁碟。但是，隨著您儲存需求的變更，您可以將另外的磁碟連接至虛擬電腦，以增加儲存空間。

您還可以將工作檔案存儲到相連的磁碟上。然後，您可以分離磁碟並將其連接至不同的虛擬電腦，以快速將檔案從一台電腦移動到另一台電腦。

或者，您可以為具有工作檔案的連接磁碟建立快照，然後從快照建立複製磁碟。然後，您可以將新的複製磁碟連接至另一台電腦，以在不同的虛擬電腦之間複製您的工作。如需詳細資訊，請參閱 在適用於研究的 Lightsail 主控台中建立儲存磁碟 和 在 Lightsail 進行研究的虛擬電腦中新增儲存空間。

> **Note**
>
> 當您使用主控台將磁碟連接至虛擬電腦時，Lightsail for Research 會自動格式化並掛載磁碟。此過程需要幾分鐘的時間，因此您應該先確認磁碟已達到掛載狀態，然後再開始使用。根據預設，Lightsail for Research 會將磁碟掛載到 `/home/lightsail-user/<disk-name>` 目錄。 *<disk-name>* 是您提供磁碟的名稱。

步驟 3：上傳並下載檔案

您可以將檔案上傳到 JupyterLab 虛擬電腦，並從中下載檔案。若要這樣做，必須先完成以下步驟：

1. 從 Amazon Lightsail 取得金鑰對。如需詳細資訊，請參閱取得 Lightsail for Research 虛擬電腦的金鑰對。
2. 擁有金鑰對後，您可以使用它來使用安全複製（SCP）公用程式建立連線。SCP 可讓您使用命令提示字元或終端機上傳和下載檔案。如需詳細資訊，請參閱使用 Secure Copy 將檔案傳輸至 Lightsail for Research 虛擬電腦。
3. （選用）您也可以使用金鑰對，透過 連線至虛擬電腦SSH。如需詳細資訊，請參閱使用 Secure Shell 連線至 Lightsail for Research 虛擬電腦。

> **Note**
>
> 您也可以使用瀏覽器型 Amazon DCV用戶端存取虛擬電腦的命令列介面並傳輸檔案。Amazon DCV 可在 Lightsail for Research 主控台中使用。如需詳細資訊，請參閱 存取

Lightsail for Research 虛擬電腦應用程式 和 存取 Lightsail for Research 虛擬電腦的作業系統。

若要管理連接至儲存磁碟中的專案檔案，請務必將這些檔案上傳至相連磁碟的正確掛載目錄。當您使用主控台將磁碟連接至虛擬電腦時，Lightsail for Research 會自動格式化磁碟並將其掛載至/home/lightsail-user/*<disk-name>*目錄。 *<disk-name>* 是您提供磁碟的名稱。

步驟 4：啟動 JupyterLab應用程式

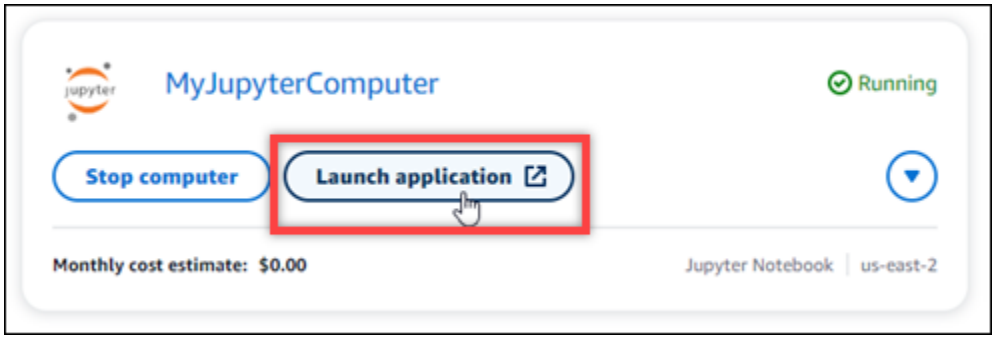
完成下列程序，在新的虛擬電腦上啟動 JupyterLab 應用程式。

Important

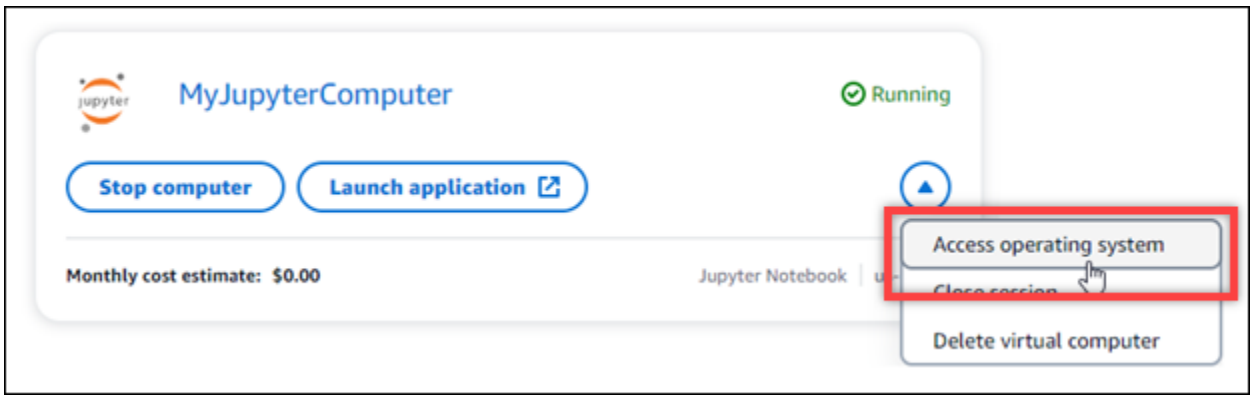
請勿更新作業系統或 JupyterLab 應用程式，即使系統提示您這麼做。請選擇關閉或忽略這些提示的選項。此外，請勿修改 /home/lightsail-admin/ 目錄中的任何檔案。這些動作可能會導致虛擬電腦無法使用。

1. 登入 Lightsail for Research 主控台 。
2. 在導覽窗格中選擇虛擬電腦，以檢視帳戶中可用的虛擬電腦。
3. 在虛擬電腦頁面中，尋找您的虛擬電腦，然後選擇以下其中一個選項來連線至虛擬電腦：

   a. （建議）選擇啟動應用程式以聚焦模式啟動 JupyterLab 應用程式。如果您最近尚未連線至虛擬電腦，您可能需要等待幾分鐘，Lightsail for Research 會準備您的工作階段。



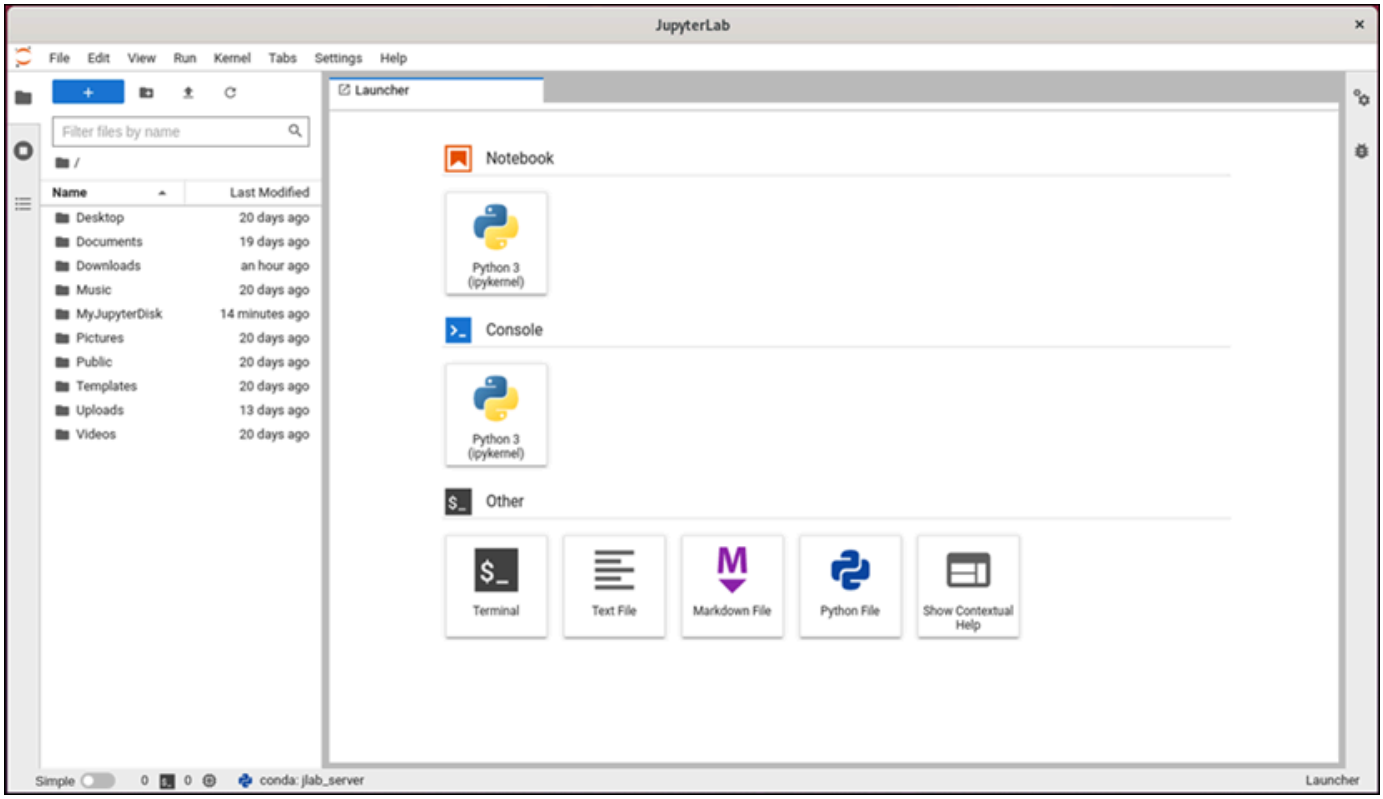
   b. 選擇電腦的下拉式選單，然後選擇存取作業系統以存取虛擬電腦的桌面。



Lightsail for Research 會執行一些命令來啟動遠端顯示通訊協定連線。經過一段時間後，將開啟一個新的瀏覽器分頁視窗，其中包含與虛擬電腦建立的虛擬桌面連線。如果您選擇啟動應用程式選項，請繼續執行此程序的下一個步驟，以在 JupyterLab 應用程式中開啟檔案。如果您選擇存取作業系統選項，則可以透過 Ubuntu 桌面開啟其他應用程式。

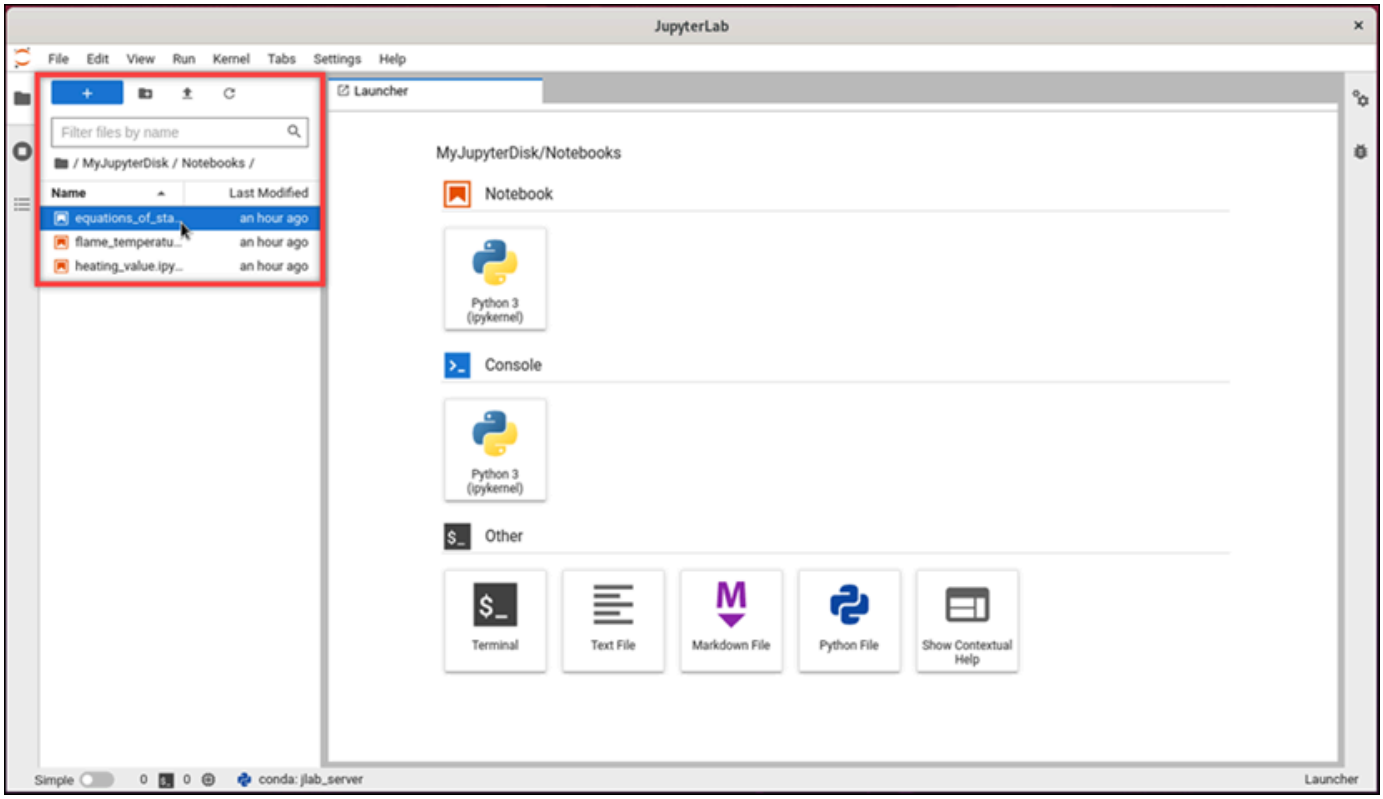
> **Note**
>
> 您的瀏覽器可能會提示您授權共用剪貼簿。允許此選項可讓您在本機電腦與虛擬電腦之間進行複製和貼上。
>
> Ubuntu 可能還會提示您進行初始設置。按照提示操作，直到完成設置且可以使用作業系統。

4. JupyterLab 應用程式會開啟。在啟動程式選單中，您可以建立一個新的筆記本、啟動主控台、啟動終端並建立各種檔案。

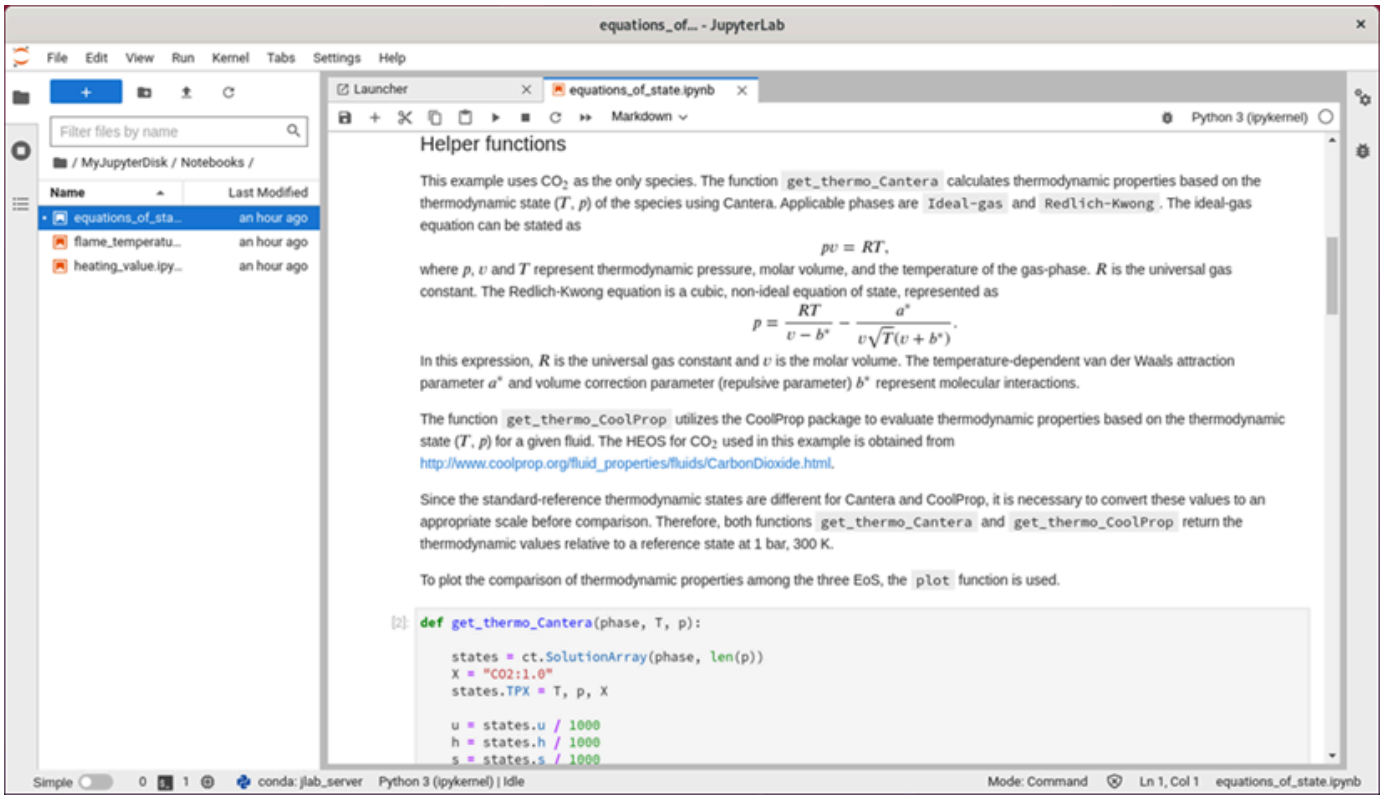


5. 若要在 中開啟檔案 JupyterLab，請在檔案瀏覽器窗格中，選擇存放專案檔案的目錄或資料夾。然後選擇要開啟的檔案。

   如果您將專案檔案上傳至連接的磁碟，請尋找掛載磁碟的目錄。根據預設，Lightsail for Research 會將磁碟掛載到/home/lightsail-user/*<disk-name>*目錄。 *<disk-name>*是您為磁碟提供的名稱。在以下範例中，MyJupyterDisk 目錄代表掛載的磁碟，Notebooks 子目錄內含我們的 Jupyter 筆記本檔案。



在以下範例中，我們開啟了一個 `equations_of_state.ipynb` Jupyter 筆記本檔案。



若要取得有關如何開始使用的詳細資訊，請繼續本教學課程的 步驟 5：閱讀 JupyterLab文件 章節。

步驟 5：閱讀 JupyterLab文件

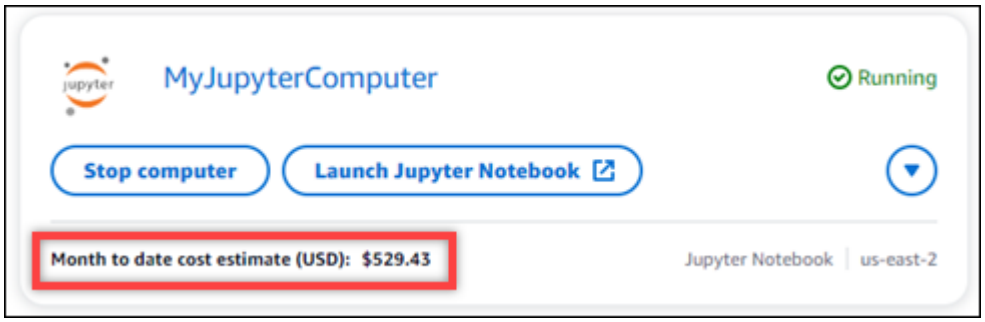
如果您不熟悉 JupyterLab，建議您閱讀其正式文件。下列 JupyterLab 線上資源可供使用：

- JupyterLab 文件
- Jupyter Discourse 論壇
- JupyterLab 在 上 StackOverflow
- JupyterLab 在 上 GitHub

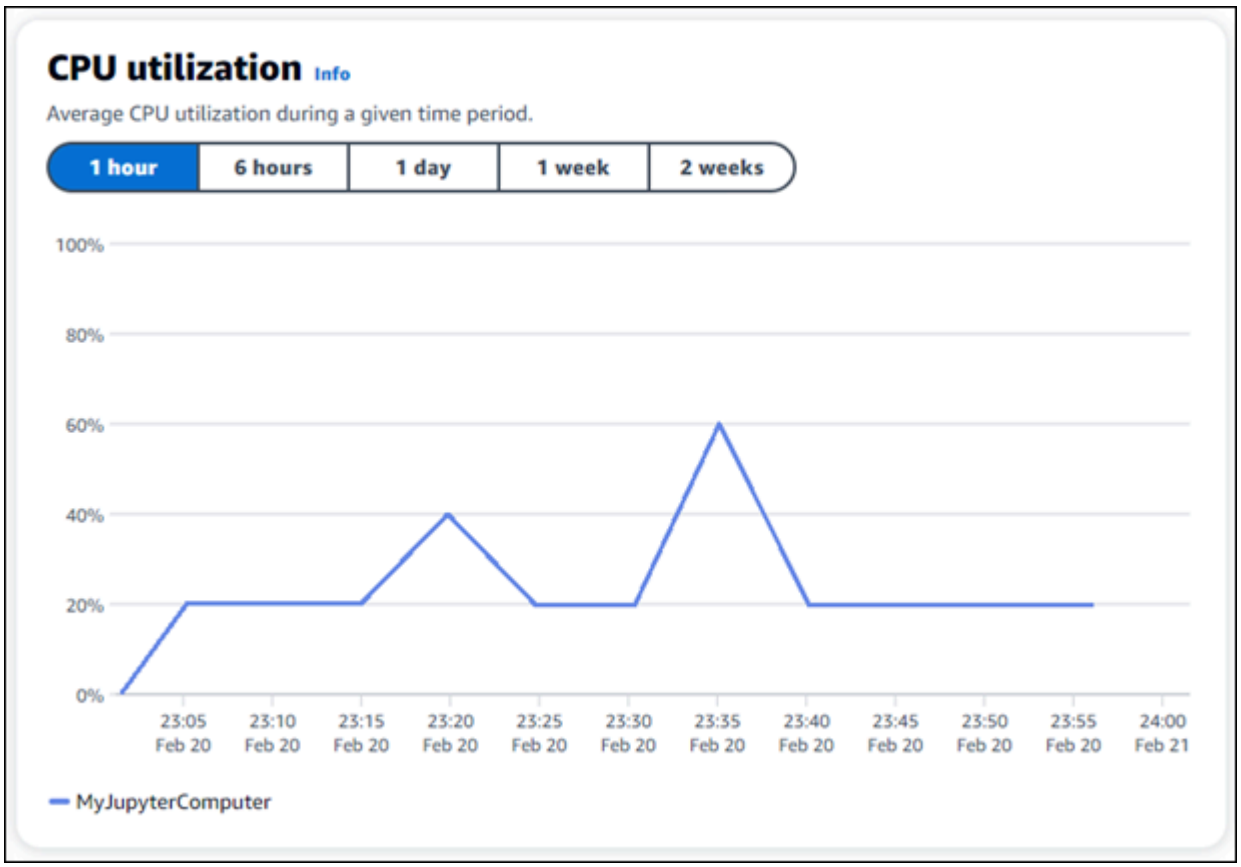
步驟 6：(選用) 監控用量和成本

Lightsail for Research 資源的本月迄今成本和用量估算會顯示在 Lightsail for Research 主控台的下列區域中。

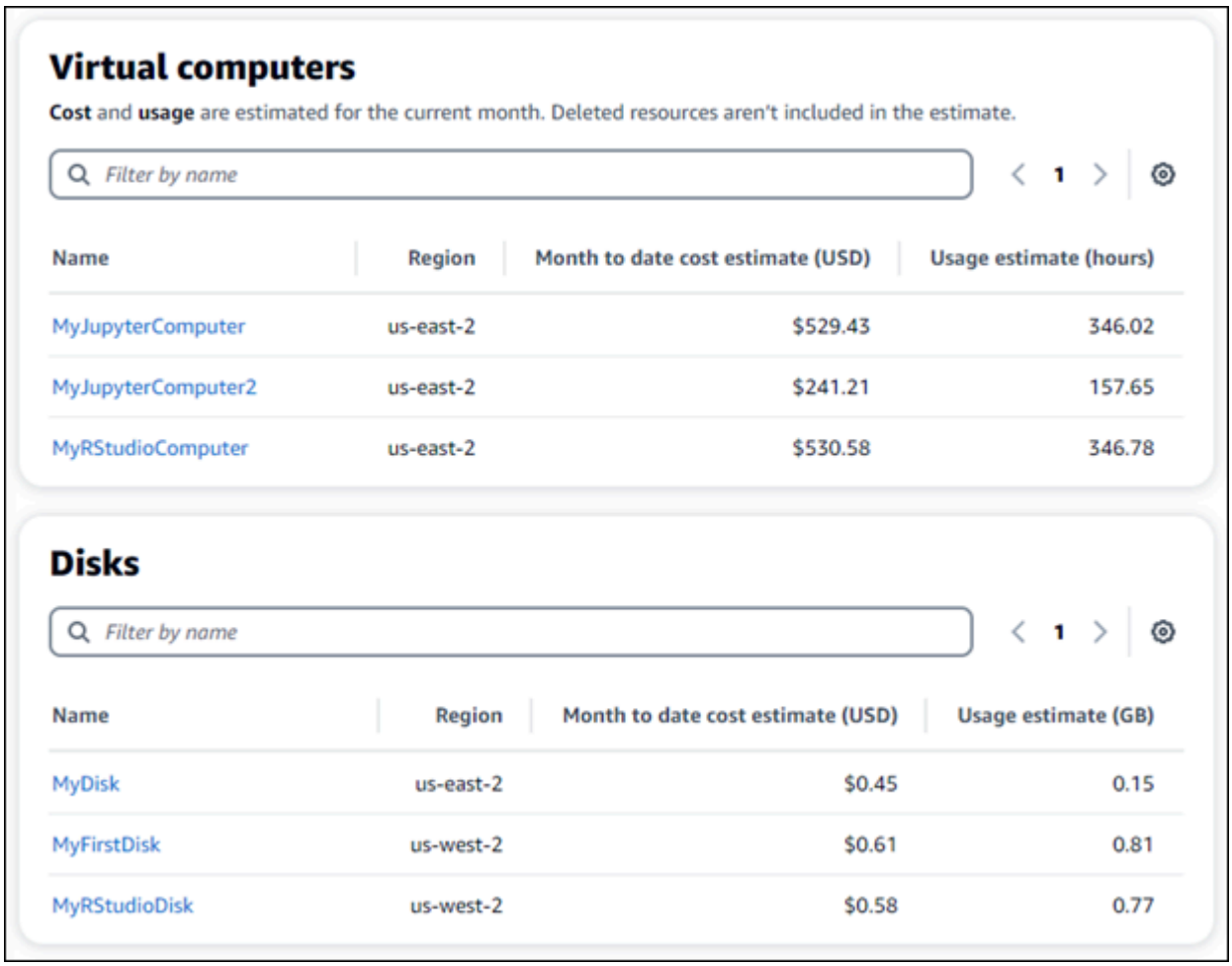
1. 在 Lightsail for Research 主控台的導覽窗格中選擇虛擬電腦。每台運行中虛擬電腦的下方，會列出該虛擬電腦當月至今的成本估算。



2. 若要檢視虛擬電腦的使用CPU率，請選擇虛擬電腦的名稱，然後選擇儀表板索引標籤。



3. 若要檢視所有 Lightsail for Research 資源的本月迄今成本和用量估算，請在導覽窗格中選擇用量。



步驟 7：(選用) 建立成本控制規則

透過建立成本控制規則，管理虛擬電腦的用量和成本。您可以在閒置規則上建立停止虛擬電腦，當電腦在指定期間內達到其CPU使用率的指定百分比時，就會停止執行中的電腦。例如，當特定電腦在 30 分鐘期間內的使用CPU率等於或低於 5% 時，規則會自動停止。這可能表示電腦處於閒置狀態，Lightsail for Research 會停止電腦，讓您不會產生閒置資源的費用。

> **Important**
>
> 在您建立規則以在閒置時停止虛擬電腦之前，建議您監控其CPU使用率幾天。記下虛擬電腦處於不同負載時的CPU使用率。例如，當電腦在編譯程式碼時、處理操作時和閒置時。這可協助您判斷規則的準確門檻值。如需詳細資訊，請參閱本教學課程的 步驟 6：(選用) 監控用量和成本 章節。

如果您建立的規則CPU使用率閾值高於工作負載，則規則可以連續停止您的虛擬電腦。例如，如果您在規則停止虛擬電腦之後立即啟動該電腦，則規則會重新啟動，電腦會再次停止。

可在以下指南中找到建立及管理成本控制規則的詳細說明：

- 管理研究用 Lightsail 中的成本控制規則
- 為您的研究用 Lightsail 虛擬電腦建立成本控制規則
- 刪除適用於研究成本的 Lightsail 虛擬電腦的成本控制規則

步驟 8：(選用) 建立快照

快照是 point-in-time資料的副本。可建立虛擬電腦的快照，並用來作為建立新電腦或資料備份的基準。快照包含還原電腦所需的所有資料 (從建立快照的那一刻開始)。

可在以下指南中找到建立及管理快照的詳細說明：

- 建立適用於研究人員的 Lightsail 虛擬電腦或磁碟快照
- 在研究專用 Lightsail 中檢視和管理虛擬電腦和磁碟快照
- 從快照建立虛擬電腦或磁碟
- 在適用於研究的 Lightsail 主控台中刪除快照

步驟 9：(選用) 停止或刪除您的虛擬電腦

如果不再使用為此教學課程建立的虛擬電腦，可將其刪除。如果不再需要，這樣做可停止虛擬電腦產生費用。

刪除虛擬電腦並不會刪除其關聯的快照或連接的磁碟。如果您已建立快照和磁碟，則應手動刪除這些快照和磁碟，以免產生費用。

若要儲存您的虛擬電腦以供日後使用，但又想要避免依標準的每小時價格計費，則可以停止虛擬電腦而不用刪除。然後，您可之後再次將其啟動。如需詳細資訊，請參閱檢視 Lightsail for Research 虛擬電腦詳細資訊。如需定價的詳細資訊，請參閱 Lightsail for Research 定價。

> **Important**
>
> 刪除 Lightsail for Research 資源是永久動作。刪除的資料無法復原。如果之後可能需要該資料，請在刪除之前建立虛擬電腦的快照。如需詳細資訊，請參閱建立快照。

1. 登入 Lightsail for Research 主控台 。
2. 在導覽窗格中，選擇虛擬電腦。
3. 選擇要刪除的虛擬電腦。
4. 選擇動作，然後選擇刪除虛擬電腦。
5. 在文字區塊中鍵入確認。然後，選擇刪除虛擬電腦。

在 Lightsail for Research RStudio上啟動和使用

在本教學課程中，我們將示範如何在 Amazon Lightsail for Research 中開始管理及使用RStudio虛擬電腦。

> **Note**
>
> 開始使用 Lightsail for Research 的深入教學課程RStudio，並發佈至 AWS 公部門部落格。如需詳細資訊，請參閱開始使用 Amazon Lightsail for Research：使用 的教學RStudio課程。

主題

- 步驟 1：完成先決條件
- 步驟 2：(選用) 新增儲存空間
- 步驟 3：上傳並下載檔案
- 步驟 4：啟動RStudio應用程式
- 步驟 5：閱讀RStudio文件
- 步驟 6：(選用) 監控用量和成本
- 步驟 7：(選用) 建立成本控制規則
- 步驟 8：(選用) 建立快照
- 步驟 9：(選用) 停止或刪除您的虛擬電腦

步驟 1：完成先決條件

如果您尚未使用 RStudio 應用程式建立虛擬電腦。如需詳細資訊，請參閱建立 Lightsail for Research 虛擬電腦。

步驟 2：(選用) 新增儲存空間

您的虛擬電腦隨附系統磁碟。但是，隨著您儲存需求的變更，您可以將另外的磁碟連接至虛擬電腦，以增加儲存空間。

您還可以將工作檔案存儲到相連的磁碟上。然後，您可以分離磁碟並將其連接至不同的虛擬電腦，以快速將檔案從一台電腦移動到另一台電腦。

或者，您可以為具有工作檔案的連接磁碟建立快照，然後從快照建立複製磁碟。然後，您可以將新的複製磁碟連接至另一台電腦，以在不同的虛擬電腦之間複製您的工作。如需詳細資訊，請參閱 在適用於研究的 Lightsail 主控台中建立儲存磁碟 和 在 Lightsail 進行研究的虛擬電腦中新增儲存空間。

> **Note**
>
> 當您使用主控台將磁碟連接至虛擬電腦時，Lightsail for Research 會自動格式化並掛載磁碟。此過程需要幾分鐘的時間，因此您應該先確認磁碟已達到掛載狀態，然後再開始使用。依預設，Lightsail for Research 會將磁碟掛載到/home/lightsail-user/*<disk-name>*目錄*<disk-name>*是您為磁碟提供的名稱。

步驟 3：上傳並下載檔案

您可以將檔案上傳到RStudio虛擬電腦，並從中下載檔案。若要這樣做，必須先完成以下步驟：

1. 從 Amazon Lightsail 取得金鑰對。如需詳細資訊，請參閱取得 Lightsail for Research 虛擬電腦的金鑰對。
2. 擁有金鑰對後，您可以使用它來使用安全複製（SCP）公用程式建立連線。SCP 可讓您使用命令提示字元或終端機上傳和下載檔案。如需詳細資訊，請參閱使用 Secure Copy 將檔案傳輸至 Lightsail for Research 虛擬電腦。
3. （選用）您也可以使用金鑰對，透過 連線至虛擬電腦SSH。如需詳細資訊，請參閱使用 Secure Shell 連線至 Lightsail for Research 虛擬電腦。

> **Note**
>
> 您也可以使用瀏覽器型 Amazon DCV用戶端存取虛擬電腦的命令列介面並傳輸檔案。Amazon DCV 可在 Lightsail for Research 主控台中使用。如需詳細資訊，請參閱 存取 Lightsail for Research 虛擬電腦應用程式 和 存取 Lightsail for Research 虛擬電腦的作業系統。

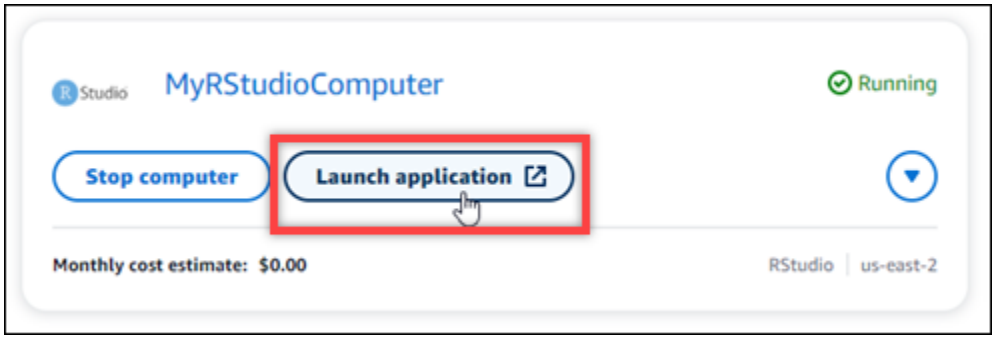
步驟 4：啟動RStudio應用程式

完成下列程序，在新的虛擬電腦上啟動RStudio應用程式。

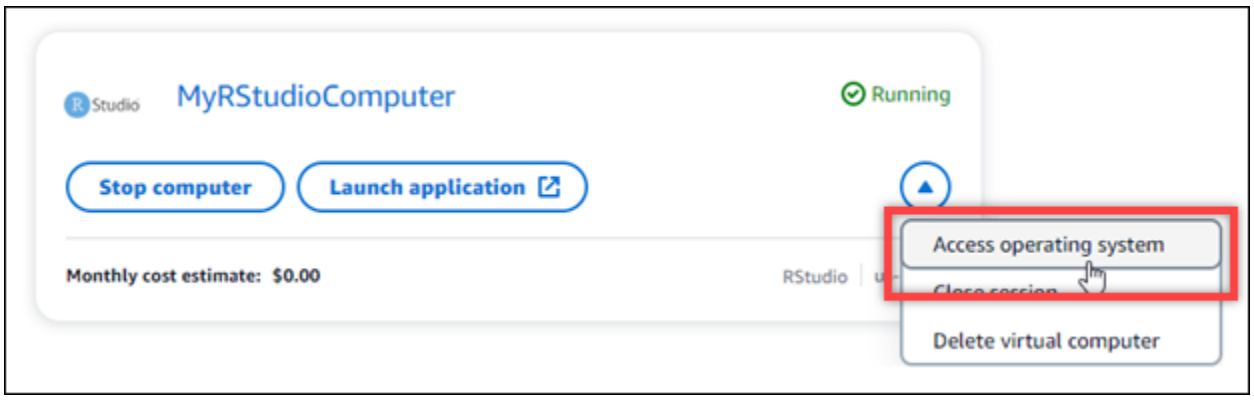
> **Important**
>
> 請勿更新作業系統或RStudio應用程式，即使系統提示您這麼做。請選擇關閉或忽略這些提示的選項。此外，請勿修改 /home/lightsail-admin/ 目錄中的任何檔案。這些動作可能會導致虛擬電腦無法使用。

1. 登入 Lightsail for Research 主控台 。
2. 在導覽窗格中選擇虛擬電腦，以檢視帳戶中可用的虛擬電腦。
3. 在虛擬電腦頁面中，尋找您的虛擬電腦，然後選擇以下其中一個選項來連線至虛擬電腦：

   a. （建議）選擇啟動應用程式以聚焦模式啟動RStudio應用程式。如果您最近尚未連線至虛擬電腦，您可能需要等待幾分鐘，Lightsail for Research 會準備您的工作階段。

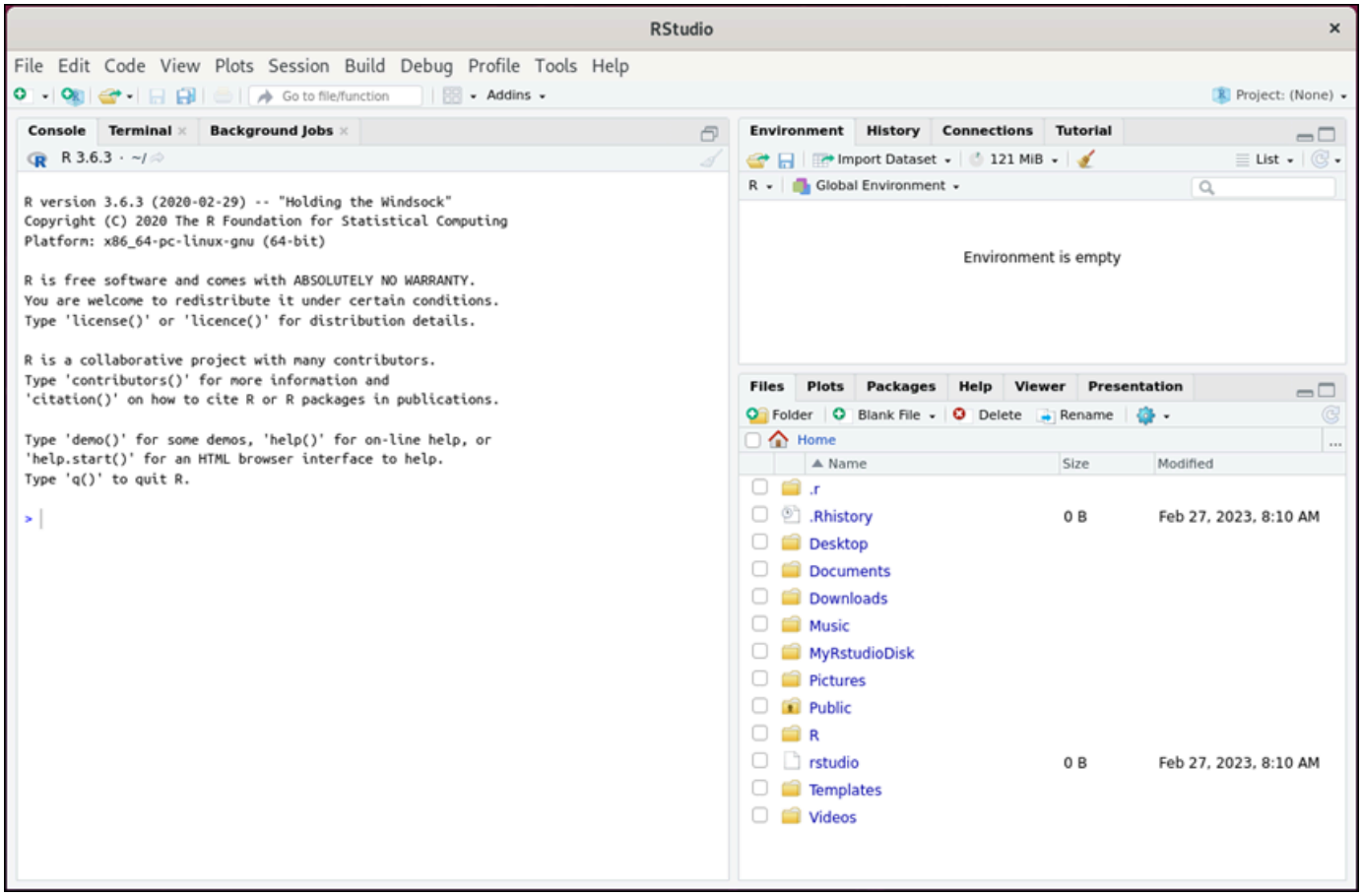
   b. 選擇電腦的下拉式選單，然後選擇存取作業系統以存取虛擬電腦的桌面。如果您要在作業系統上安裝其他應用程式，請執行此動作。



Lightsail for Research 會執行一些命令來啟動遠端顯示通訊協定連線。經過一段時間後，將開啟一個新的瀏覽器分頁視窗，其中包含與虛擬電腦建立的虛擬桌面連線。如果您選擇啟動應用程式選項，請繼續此程序的下一個步驟，在RStudio應用程式中開啟檔案。如果您選擇存取作業系統選項，則可以透過 Ubuntu 桌面開啟其他應用程式。

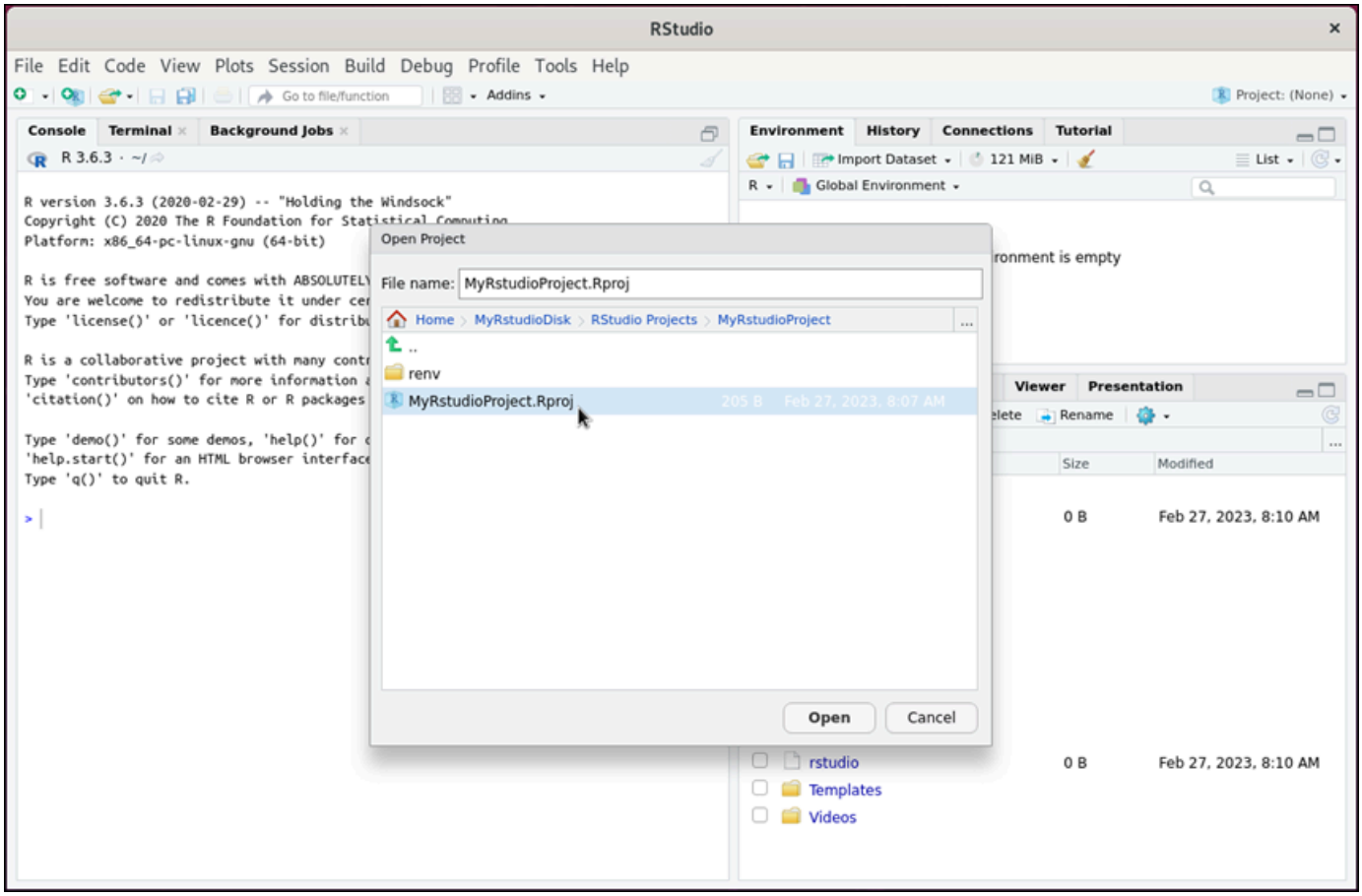
> **Note**
>
> 您的瀏覽器可能會提示您授權共用剪貼簿。允許此選項可讓您在本機電腦與虛擬電腦之間進行複製和貼上。
>
> Ubuntu 可能還會提示您進行初始設置。按照提示操作，直到完成設置且可以使用作業系統。

4. RStudio 應用程式會開啟。

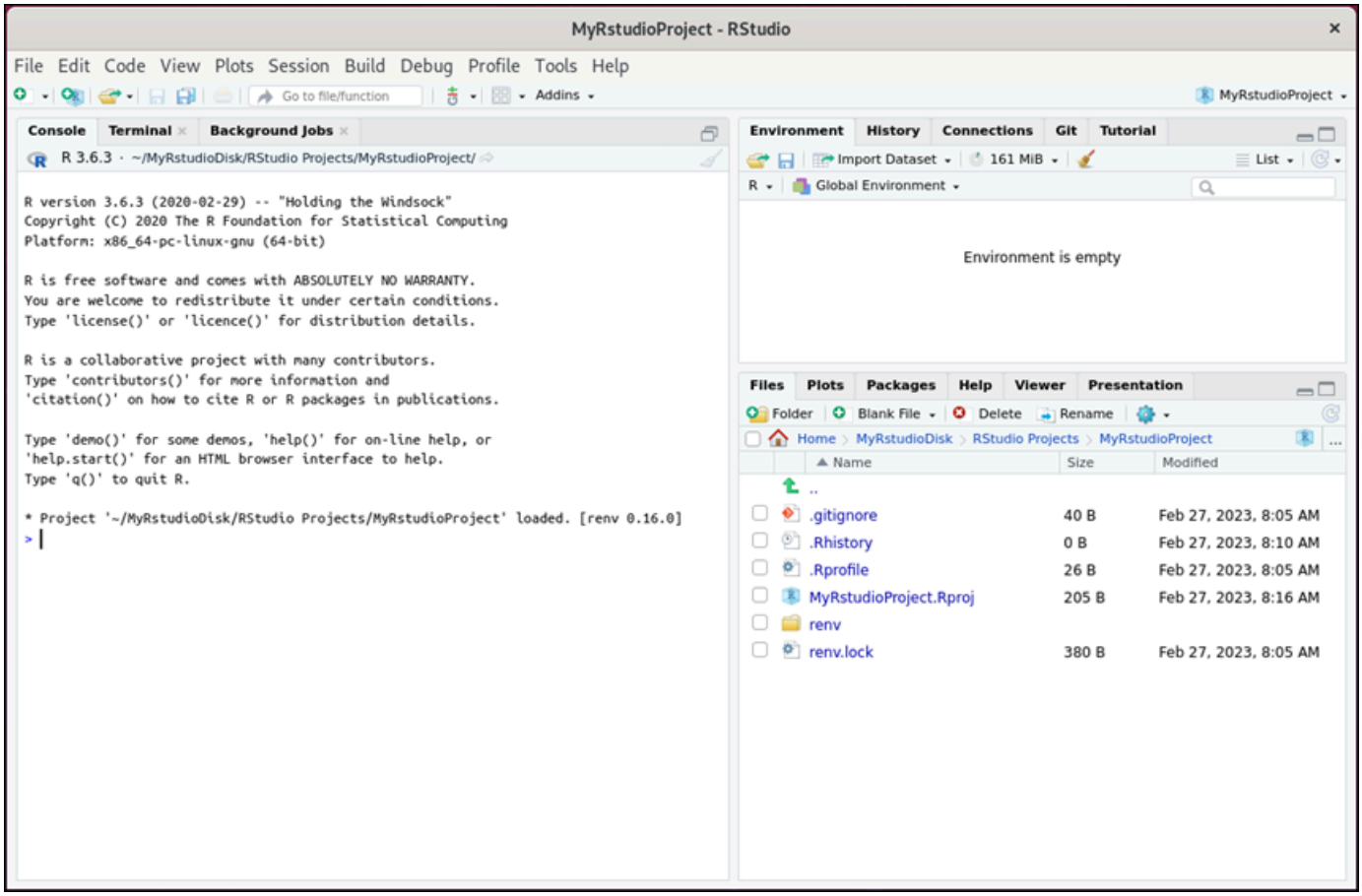


5. 若要在 中開啟專案RStudio，請選擇檔案選單，然後選擇開啟專案 。瀏覽至存放專案檔案的目錄或資料夾。然後選擇要開啟的檔案。

   如果您將專案檔案上傳至連接的磁碟，請尋找掛載磁碟的目錄。根據預設，Lightsail for Research會將磁碟掛載到/home/lightsail-user/*<disk-name>*目錄。 *<disk-name>*是您為磁碟提供的名稱。在下列範例中，MyRstudioDisk目錄代表掛載的磁碟，而Projects子目錄包含我們的RStudio專案檔案。



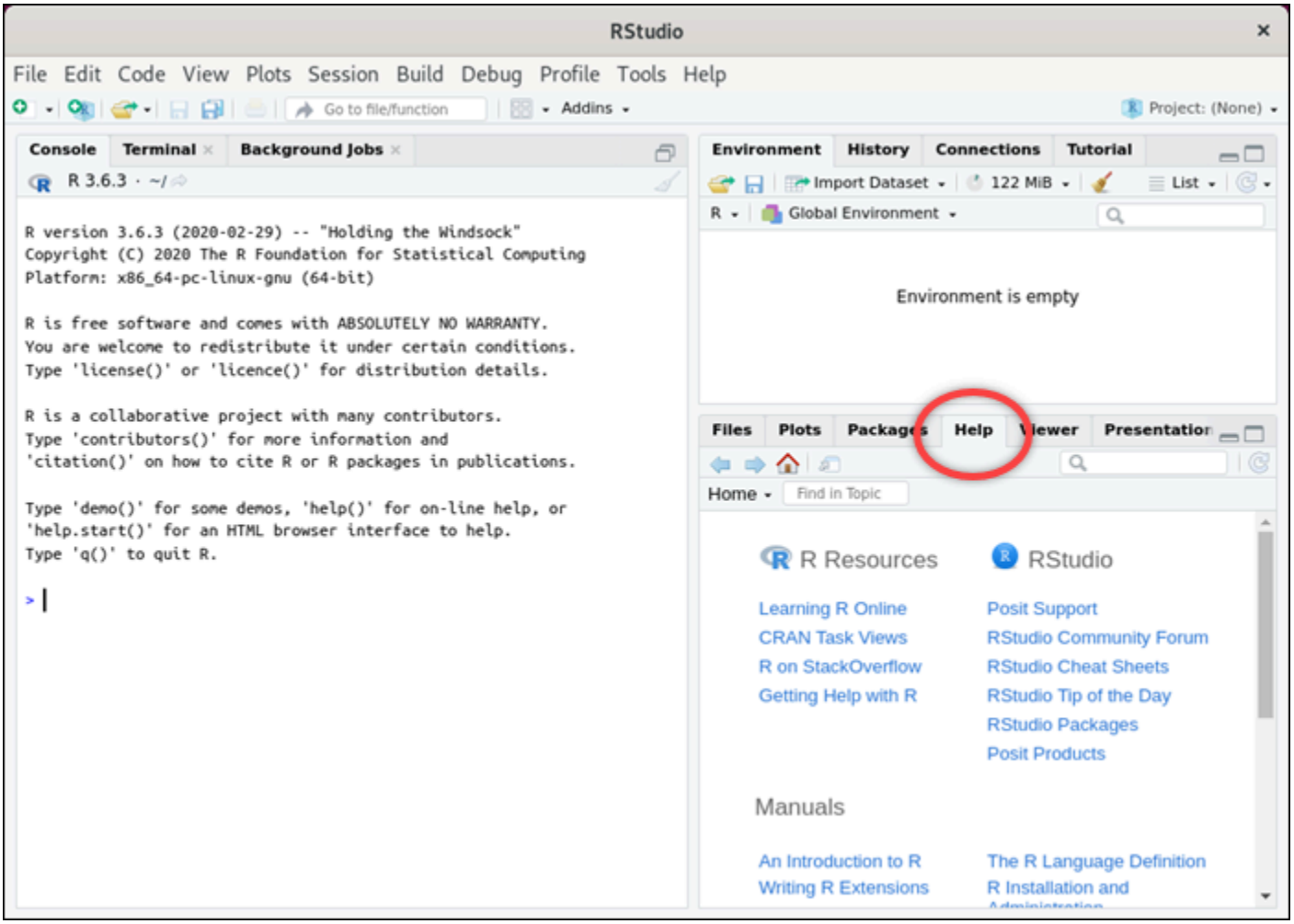
在以下範例中，我們開啟了 `MyRstudioProject.Rproj` 專案檔案。



如需有關如何開始使用 的資訊RStudio，請繼續本教學課程的 步驟 5：閱讀RStudio文件章節。

步驟 5：閱讀RStudio文件

RStudio 應用程式會搭配全面的文件套件。若要開始學習 RStudio，建議您存取 中的說明索引標籤 RStudio，如下列範例所示。



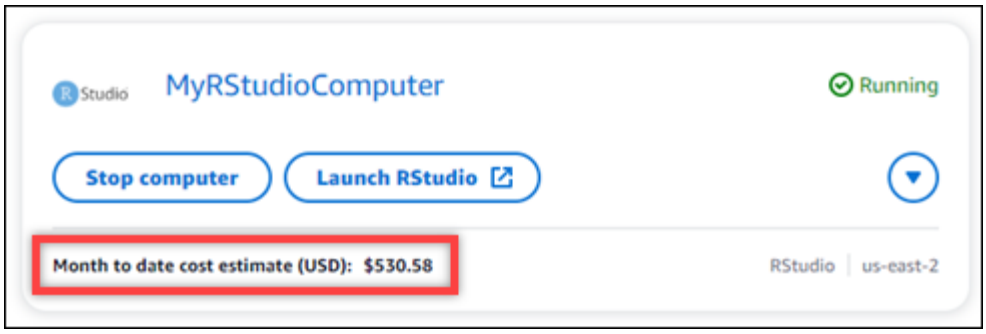
也提供下列RStudio線上資源：

- 線上學習 R
- R 開啟 StackOverflow
- 取得 R 的說明
- Posit 支援
- RStudio 社群論壇
- RStudio Cheat Sheets
- RStudio 當日秘訣（Twitter）
- RStudio 套件

步驟 6：(選用) 監控用量和成本

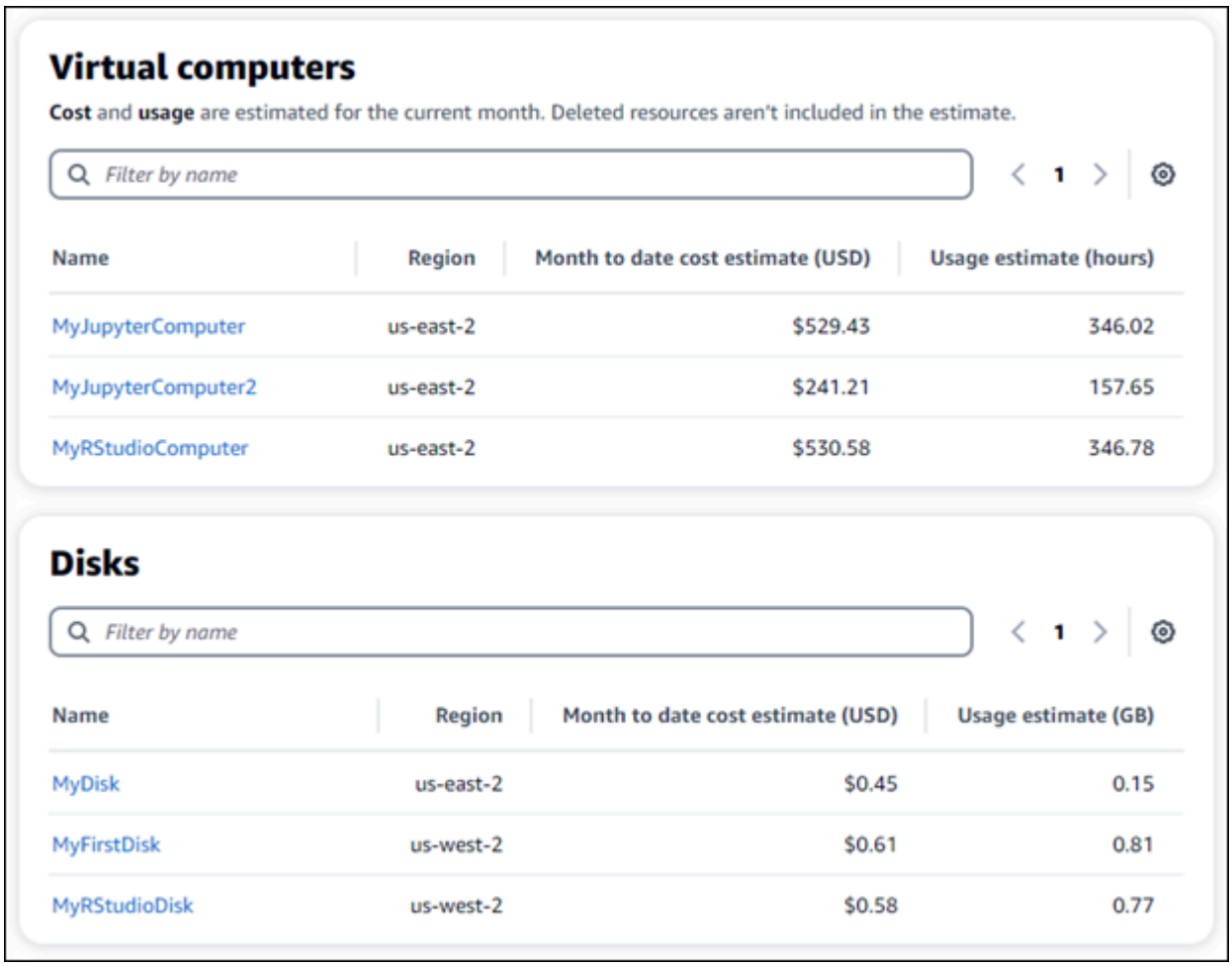
Lightsail for Research 資源的本月迄今成本和用量估算會顯示在 Lightsail for Research 主控台的下列區域中。

1. 在 Lightsail for Research 主控台的導覽窗格中選擇虛擬電腦。每台運行中虛擬電腦的下方，會列出該虛擬電腦當月至今的成本估算。



2. 若要檢視虛擬電腦的使用CPU率，請選擇虛擬電腦的名稱，然後選擇儀表板索引標籤。

3. 若要檢視所有 Lightsail for Research 資源的本月迄今成本和用量估算，請在導覽窗格中選擇用量。



步驟 7：(選用) 建立成本控制規則

透過建立成本控制規則，管理虛擬電腦的用量和成本。您可以建立在閒置規則上停止虛擬電腦，當執行中的電腦在指定期間內達到其CPU使用率的指定百分比時，就會停止該電腦。例如，當特定電腦在 30 分鐘期間內的使用CPU率等於或低於 5% 時，規則會自動停止。這可能表示電腦處於閒置狀態，Lightsail for Research 會停止電腦，讓您不會產生閒置資源的費用。

> **Important**
>
> 在您建立規則以在閒置時停止虛擬電腦之前，建議您監控其CPU使用率幾天。記下虛擬電腦處於不同負載時的CPU使用率。例如，當電腦在編譯程式碼時、處理操作時和閒置時。這可協助您判斷規則的準確門檻值。如需詳細資訊，請參閱本教學課程的 步驟 6：(選用) 監控用量和成本 章節。

如果您建立的規則CPU使用率閾值高於工作負載，則規則可以連續停止您的虛擬電腦。例如，如果您在規則停止虛擬電腦之後立即啟動該電腦，則規則會重新啟動，電腦會再次停止。

可在以下指南中找到建立及管理成本控制規則的詳細說明：

- 管理研究用 Lightsail 中的成本控制規則
- 為您的研究用 Lightsail 虛擬電腦建立成本控制規則
- 刪除適用於研究成本的 Lightsail 虛擬電腦的成本控制規則

步驟 8：(選用) 建立快照

快照是 point-in-time資料的副本。可建立虛擬電腦的快照，並用來作為建立新電腦或資料備份的基準。快照包含還原電腦所需的所有資料 (從建立快照的那一刻開始)。

可在以下指南中找到建立及管理快照的詳細說明：

- 建立適用於研究人員的 Lightsail 虛擬電腦或磁碟快照
- 在研究專用 Lightsail 中檢視和管理虛擬電腦和磁碟快照
- 從快照建立虛擬電腦或磁碟
- 在適用於研究的 Lightsail 主控台中刪除快照

步驟 9：(選用) 停止或刪除您的虛擬電腦

如果不再使用為此教學課程建立的虛擬電腦，可將其刪除。如果不再需要，這樣做可停止虛擬電腦產生費用。

刪除虛擬電腦並不會刪除其關聯的快照或連接的磁碟。如果您已建立快照和磁碟，則應手動刪除這些快照和磁碟，以免產生費用。

若要儲存您的虛擬電腦以供日後使用，但又想要避免依標準的每小時價格計費，則可以停止虛擬電腦而不用刪除。然後，您可之後再次將其啟動。如需詳細資訊，請參閱檢視 Lightsail for Research 虛擬電腦詳細資訊。如需定價的詳細資訊，請參閱 Lightsail for Research 定價。

> **Important**
>
> 刪除 Lightsail for Research 資源是永久動作。刪除的資料無法復原。如果之後可能需要該資料，請在刪除之前建立虛擬電腦的快照。如需詳細資訊，請參閱建立快照。

1. 登入 Lightsail for Research 主控台 。
2. 在導覽窗格中，選擇虛擬電腦。
3. 選擇要刪除的虛擬電腦。
4. 選擇動作，然後選擇刪除虛擬電腦。
5. 在文字區塊中鍵入確認。然後，選擇刪除虛擬電腦。

在 Lightsail for Research 上建立和管理虛擬電腦

透過 Amazon Lightsail for Research，您可以在 中建立虛擬電腦 AWS 雲端。

建立虛擬電腦時，您可以選擇要使用的應用程式和硬體方案。您可以為虛擬電腦設定支出限制，並選擇虛擬電腦達到該限制時會發生的情況。例如，您可以選擇自動停止虛擬電腦，這樣您就不會被收取超過設定預算的費用。

> **Important**
>
> 截至 2024 年 3 月 22 日，Lightsail for Research 虛擬電腦預設會IMDSv2強制執行。

主題

- 選擇 Lightsail for Research 的應用程式映像和硬體計劃
- 建立 Lightsail for Research 虛擬電腦
- 檢視 Lightsail for Research 虛擬電腦詳細資訊
- 存取 Lightsail for Research 虛擬電腦應用程式
- 存取 Lightsail for Research 虛擬電腦的作業系統
- 管理 Lightsail for Research 虛擬電腦的防火牆連接埠
- 取得 Lightsail for Research 虛擬電腦的金鑰對
- 使用 Secure Shell 連線至 Lightsail for Research 虛擬電腦
- 使用 Secure Copy 將檔案傳輸至 Lightsail for Research 虛擬電腦
- 刪除 Lightsail for Research 虛擬電腦

選擇 Lightsail for Research 的應用程式映像和硬體計劃

當您建立 Amazon Lightsail for Research 虛擬電腦時，您需要為其選取應用程式和硬體計劃（計劃）。

應用程式提供軟體組態 (例如，應用程式和作業系統)。計劃提供虛擬電腦的硬體，例如 的數量 vCPUs、記憶體、儲存空間和每月資料傳輸額度。應用程式和方案共同構成了虛擬電腦組態。

> **Note**
>
> 建立虛擬電腦之後，就無法變更虛擬電腦的應用程式或方案。但是，您可以建立虛擬電腦的快照，然後在從快照建立新的虛擬電腦時選擇新的方案。如需快照的相關資訊，請參閱 使用 Lightsail 進行研究快照 Backup 虛擬電腦和磁碟。

主題

- 應用程式
- 計畫

應用程式

Amazon Lightsail for Research 提供和管理機器映像，其中包含啟動虛擬電腦所需的應用程式和作業系統。當您在 Lightsail for Research 中建立虛擬電腦時，您可以從應用程式清單中選擇。所有 Lightsail for Research 應用程式映像都使用 Ubuntu （Linux） 作業系統。

Lightsail for Research 提供下列應用程式：

- JupyterLab – JupyterLab 是適用於筆記本、程式碼和資料的 Web 型整合式開發環境 （IDE）。憑藉其靈活的介面，您可以配置和安排資料科學、科學運算、計算新聞學和機器學習中的工作流程。如需詳細資訊，請參閱 Jupyter 專案文件。
- RStudio – RStudio 是 R 的開放原始碼整合式開發環境 （IDE），也是統計運算和圖形的程式設計語言，以及 Python。結合了原始碼編輯器、構建自動化工具和除錯程式，以及用於繪圖和工作空間管理的工具。如需詳細資訊，請參閱 RStudio IDE。
- VSCodium – VSCodium 是 Microsoft 編輯器 VS 程式碼的社群驅動二進位分佈。如需詳細資訊，請參閱 VSCodium。
- Scilab – Scilab 為一開放原始碼的數值運算套件，也是一種高階、數值導向的程式語言。如需詳細資訊，請參閱 Scilab。
- Ubuntu 20.04 LTS – Ubuntu 是以 Debian 為基礎的開放原始碼 Linux 發行版本。精簡、快速且強大的 Ubuntu 伺服器提供可靠、可預測且經濟實惠的服務。這是用來建立虛擬電腦的優異基礎。如需詳細資訊，請參閱 Ubuntu 發行版本。

計畫

計劃提供硬體規格，並決定 Lightsail for Research 虛擬電腦的定價。計劃包含固定數量的記憶體（RAM）、運算（vCPUs）、SSD以 為基礎的儲存磁碟區（磁碟）空間，以及每月資料傳輸額度。方案為按小時隨需收費，因此您只需支付虛擬電腦運行時間的費用。

您選擇的方案可能取決於您的工作負載所需的資源。Lightsail for Research 提供下列計劃類型：

- 標準 – 標準方案經過運算最佳化，非常適合將因高效能處理器而受惠的運算密集型應用程式。
- GPU – GPU計劃為一般用途GPU運算提供具成本效益的高效能平台。您可以使用這些方案來加速科學、工程和轉譯等應用程式與工作負載。

標準方案

以下是 Lightsail for Research 中提供的標準計劃的硬體規格。

方案名稱	vCPUs	記憶體	儲存空間	每月資料傳輸限額
標準 XL	4	8 GB	50 GB	512 GB
標準 2XL	8	16 GB	50 GB	512 GB
標準 4XL	16	32 GB	50 GB	512 GB

GPU 計劃

以下是 Lightsail for Research 中提供的GPU計劃硬體規格。

方案名稱	vCPUs	記憶體	儲存空間	每月資料傳輸限額
GPU XL	4	16 GB	50 GB	1 TB
GPU 2XL	8	32 GB	50 GB	1 TB
GPU 4XL	16	64 GB	50 GB	1 TB

建立 Lightsail for Research 虛擬電腦

請完成下列步驟，以建立執行應用程式的 Lightsail for Research 虛擬電腦。

1. 登入 Lightsail for Research 主控台 。
2. 在首頁上，選擇建立虛擬電腦。
3. AWS 區域 為實體位置附近的虛擬電腦選取 。
4. 選擇應用程式和硬體方案。如需詳細資訊，請參閱選擇 Lightsail for Research 的應用程式映像和硬體計劃。
5. 輸入虛擬電腦的名稱。有效字元包括英數字元、數字、句點、連字符和底線。

   虛擬電腦名稱也必須符合以下要求：

   - 在您的 Lightsail for Research 帳戶中的每個 AWS 區域 中都是唯一的。
   - 含有 2–255 個字元。
   - 開頭和結尾為英數字元或數字。
6. 在摘要面板中，選擇建立虛擬電腦。

在幾分鐘內，您的 Lightsail for Research 虛擬電腦已準備就緒，您可以透過圖形化使用者介面（GUI）工作階段與其連線。如需連線至 Lightsail for Research 虛擬電腦的詳細資訊，請參閱 存取 Lightsail for Research 虛擬電腦應用程式。

> **Important**
>
> 新建立的虛擬電腦預設會開啟一組防火牆連接埠。如需這些連接埠的詳細資訊，請參閱 管理 Lightsail for Research 虛擬電腦的防火牆連接埠。

檢視 Lightsail for Research 虛擬電腦詳細資訊

請完成下列步驟，以檢視您 Lightsail for Research 帳戶中的虛擬電腦清單及其詳細資訊。

1. 登入 Lightsail for Research 主控台 。
2. 在瀏覽窗格中選擇虛擬電腦，以查看帳戶中的虛擬電腦。

選擇虛擬電腦的名稱以瀏覽至其管理頁面。以下是管理頁面提供的資訊：

- 虛擬電腦名稱 – 虛擬電腦的名稱。
- 狀態 – 您的虛擬電腦可能具有以下其中一種狀態代碼：
  - 正在建立
  - 執行中
  - 正在停止
  - 已停止
  - 不明
- AWS 區域 – AWS 區域 您的虛擬電腦是在 中建立的。
- 應用程式與硬體 – 虛擬電腦的應用程式與硬體方案。
- 每月用量估算 – 此虛擬電腦目前計費週期的預估每小時用量。
- 本月至今成本估算 – 此帳單週期的虛擬電腦預估成本 （ 以 為單位USD ）。
- 儀表板 – 您可以從儀表板分頁啟動工作階段，以存取虛擬電腦的應用程式。您也可以檢視CPU使用率。CPU 使用率會識別虛擬電腦應用程式使用的處理能力。圖表中顯示的每個資料點代表一段時間內的平均CPU使用率。
- 成本控制規則 – 您定義的規則，用以協助管理虛擬電腦的用量和成本。
- 虛擬電腦用量 – 指定計費週期的成本和用量估算。您可以按日期與時間篩選。
- 儲存空間 – 從儲存索引標籤建立、連接和分離虛擬電腦磁碟。磁碟是您可以連接至虛擬電腦並掛載為硬碟的儲存磁碟區。
- 標籤 — 從標籤分頁管理您的虛擬電腦標籤。標籤是您指派給 AWS 資源的標籤。每個標籤皆包含索引鍵與選用值。您可以使用標籤來搜尋和篩選資源，或追蹤您的 AWS 成本。

存取 Lightsail for Research 虛擬電腦應用程式

請完成下列步驟，以啟動正在 Lightsail for Research 虛擬電腦上執行的應用程式。

1. 登入 Lightsail for Research 主控台 。
2. 在導覽窗格中，選擇虛擬電腦。
3. 找到您要從中啟動應用程式的虛擬電腦名稱。

> **Note**
>
> 如果虛擬電腦已停止，請先選擇啟動電腦按鈕將其開啟。

4. 選擇啟動應用程式。例如，啟動 JupyterLab。應用程式工作階段會在新的 Web 瀏覽器視窗中開啟。

> **Important**
>
> 如果您的 Web 瀏覽器有安裝彈出視窗封鎖程式，則在開啟工作階段之前，您可能需要允許來自 aws.amazon.com 網域的彈出視窗。

存取 Lightsail for Research 虛擬電腦的作業系統

請完成下列步驟，以存取 Lightsail for Research 虛擬電腦的作業系統。

1. 登入 Lightsail for Research 主控台 。
2. 在導覽窗格中，選擇虛擬電腦。
3. 找到虛擬電腦的名稱，然後選擇電腦狀態下的動作按鈕下拉式選單。

> **Note**
>
> 如果虛擬電腦已停止，請先選擇啟動按鈕將其開啟。

4. 選擇存取作業系統。作業系統工作階段會在新的瀏覽器視窗中開啟。

> **Important**
>
> 如果您的 Web 瀏覽器有安裝彈出視窗封鎖程式，則在開啟工作階段之前，您可能需要允許來自 aws.amazon.com 網域的彈出視窗。

管理 Lightsail for Research 虛擬電腦的防火牆連接埠

Amazon Lightsail for Research 中的防火牆會控制允許連線至您虛擬電腦的流量。您可以將規則新增至虛擬電腦的防火牆，以指定通訊協定、連接埠，以及允許與其連線的來源IPv4或IPv6地址。防火牆規則一律為許可制。您無法建立拒絕存取的規則。您可以新增虛擬電腦防火牆的規則，以允許流量到達虛擬電腦。每個虛擬電腦有兩個防火牆；一個用於IPv4地址，另一個用於IPv6地址。兩個防火牆彼此獨立，且含有一組預先設定的規則，用來篩選要進入執行個體的流量。

通訊協定

通訊協定是指在兩部電腦之間傳輸資料時所採用的格式。您可以在防火牆規則中指定以下通訊協定：

- 傳輸控制通訊協定（TCP）主要用於建立和維護用戶端與虛擬電腦上執行的應用程式之間的連線。這是廣泛使用的通訊協定，而且是您通常可能會在防火牆規則中指定的通訊協定。
- 使用者資料包通訊協定（UDP）主要用於在用戶端與虛擬電腦上執行的應用程式之間建立低延遲和容損連線。非常適合用於將感知延遲視為至關重要的網路應用程式，例如遊戲、語音和影像通訊。
- 網路控制訊息通訊協定（ICMP）主要用於診斷網路通訊問題，例如判斷資料是否及時到達其預期目的地。非常適合用於 Ping 公用程式，可用來測試本機電腦與虛擬電腦之間的連線速度。會回報資料到達虛擬電腦並返回本機電腦所需的時間。
- 全部可用來允許所有通訊協定流量流入虛擬電腦。當您不確定要指定哪個通訊協定時，請指定此通訊協定。這包含所有網際網路通訊協定；不只是此處指定的通訊協定。如需詳細資訊，請參閱 Internet Assigned Numbers Authority 網站上的通訊協定號碼。

連接埠

類似於電腦上的實體連接埠，可讓電腦與鍵盤和滑鼠等周邊裝置進行通訊，防火牆連接埠可做為虛擬電腦的網際網路通訊端點。當用戶端想要與虛擬電腦連線時，會開放一個連接埠以建立通訊。

您可在防火牆規則中指定的連接埠可能介於 0 至 65535。當您建立防火牆規則以允許用戶端建立與虛擬電腦的連線時，您要指定要使用的通訊協定。您也可以指定可建立連線的連接埠號編號，以及允許建立連線的 IP 地址。

根據預設，新建立的虛擬電腦會開啟以下連接埠。

- TCP
  - 22 - 用於安全殼層（SSH）。
  - 80 - 用於超文字傳輸通訊協定（HTTP）。

- 443 - 用於 Hypertext Transfer Protocol Secure （HTTPS）。
- 8443 - 用於 Hypertext Transfer Protocol Secure （HTTPS）。

為何要開啟和關閉連接埠

當您開啟連接埠時，會允許用戶端與您的虛擬電腦建立連線。當您關閉連接埠時，會封鎖與虛擬電腦的連線。例如，若要允許SSH用戶端連線至您的虛擬電腦，您可以設定防火牆規則，僅允許從需要建立連線的電腦 IP 地址TCP透過連接埠 22。在此情況下，您不想允許任何 IP 地址建立與虛擬電腦的SSH連線。這樣做可能會導致安全風險。如果此規則已在執行個體的防火牆上設定，則可以將其刪除，以封鎖SSH用戶端連線至您的虛擬電腦。

以下程序說明如何取得虛擬電腦上目前開啟的連接埠、如何開啟新的連接埠，以及如何關閉連接埠。

主題

- 完成先決條件
- 取得虛擬電腦的連接埠狀態
- 開啟虛擬電腦的連接埠
- 關閉虛擬電腦的連接埠
- 繼續後續步驟

完成先決條件

開始之前，請先完成以下先決條件：

- 在 Lightsail for Research 中建立虛擬電腦。如需詳細資訊，請參閱建立 Lightsail for Research 虛擬電腦。
- 下載並安裝 AWS Command Line Interface （AWS CLI）。如需詳細資訊，請參閱《AWS Command Line Interface 第 2 版使用者指南》中的安裝或更新最新版的 AWS CLI。
- 設定 AWS CLI 以存取您的 AWS 帳戶。如需詳細資訊，請參閱《AWS Command Line Interface 第 2 版使用者指南》中的組態基礎概念。

取得虛擬電腦的連接埠狀態

完成以下程序，取得虛擬電腦的連接埠狀態。此程序使用 `get-instance-port-states` AWS CLI 命令來取得特定 Lightsail for Research 虛擬電腦的防火牆連接埠狀態、允許透過連接埠連線至虛擬電

腦的 IP 地址，以及通訊協定。如需詳細資訊，請參閱 命令參考 get-instance-port-states 中的 。 AWS CLI

1. 此步驟取決於本機電腦的作業系統。

   - 如果您的本機電腦使用 Windows 作業系統，請開啟「命令提示」視窗。
   - 如果您的本機電腦使用 Linux 或 UNIX 作業系統 (包括 macOS)，請開啟「終端機」視窗。

2. 輸入以下命令，取得防火牆連接埠狀態及其允許的 IP 地址與通訊協定。在命令中，將 *REGION* 換成在其中建立虛擬電腦的 AWS 區域代碼，例如 us-east-2。將 *NAME* 換成虛擬電腦的名稱。

   ```
   aws lightsail get-instance-port-states --region REGION --instance-name NAME
   ```

   範例

   ```
   aws lightsail get-instance-port-states --region us-east-2 --instance-name MyUbuntu
   ```

   回應會顯示開啟的連接埠和通訊協定，以及允許連線至您虛擬電腦的 IP CIDR範圍。

   ```
   [redacted] % aws lightsail get-instance-port-states --region us-east-2 --instance
   -name MyUbuntu
   PORTSTATES      80      tcp     open    80
   CIDRS   0.0.0.0/0
   IPV6CIDRS       ::/0
   PORTSTATES      22      tcp     open    22
   CIDRS   0.0.0.0/0
   IPV6CIDRS       ::/0
   PORTSTATES      8443    tcp     open    8443
   CIDRS   0.0.0.0/0
   IPV6CIDRS       ::/0
   PORTSTATES      443     tcp     open    443
   CIDRS   0.0.0.0/0
   IPV6CIDRS       ::/0
   ```

   如需如何開啟連接埠的詳細資訊，請繼續下一節。

開啟虛擬電腦的連接埠

完成以下程序，開啟虛擬電腦的連接埠。此程序使用 open-instance-public-ports AWS CLI 命令。開啟防火牆連接埠，允許從受信任的 IP 地址或受信任的 IP 地址範圍建立連線。例如，若要允許 IP 地址 192.0.2.44，請指定 192.0.2.44 或 192.0.2.44/32。要允許 IP 地址 192.0.2.0 至 192.0.2.255，請指定 192.0.2.0/24。如需詳細資訊，請參閱 命令參考 open-instance-public-ports 中的 。 AWS CLI

1. 此步驟取決於本機電腦的作業系統。

- 如果您的本機電腦使用 Windows 作業系統，請開啟「命令提示」視窗。
- 如果您的本機電腦使用 Linux 或 UNIX 作業系統 (包括 macOS)，請開啟「終端機」視窗。

2. 然後輸入以下命令以開啟連接埠。

在命令中，替換以下項目：

- *REGION* 將 取代為虛擬電腦建立所在 AWS 區域的程式碼，例如 us-east-2。
- 將 *NAME* 換成虛擬電腦的名稱。
- 將 *FROM-PORT* 換成您想要開啟的連接埠範圍中的第一個連接埠。
- 將 *PROTOCOL* 換成 IP 通訊協定名稱。例如，TCP。
- 將 *TO-PORT* 換成您想要開啟的連接埠範圍中的最後一個連接埠。
- 將 *IP* 換成您想要允許連線至虛擬電腦的 IP 地址或 IP 地址範圍。

```
aws lightsail open-instance-public-ports --region REGION --instance-name NAME --
port-info fromPort=FROM-PORT, protocol=PROTOCOL, toPort=TO-PORT,cidrs=IP
```

範例

```
aws lightsail open-instance-public-ports --region us-east-2 --instance-
name MyUbuntu --port-info fromPort=22, protocol=TCP, toPort=22,cidrs=192.0.2.0/24
```

回應會顯示允許連線至您虛擬電腦的新新增連接埠、通訊協定和 IP CIDR範圍。

```
[redacted] % aws lightsail open-instance-public-ports --instance-name MyUbuntu -
-port-info fromPort=22,protocol=TCP,toPort=22,cidrs=192.0.2.0/24
{
    "operation": {
        "id": "0789ead5-6996-4277-97b6-0cc7fad55daf",
        "resourceName": "MyUbuntu",
        "resourceType": "Instance",
        "createdAt": "2023-02-15T16:41:50.048000-08:00",
        "location": {
            "availabilityZone": "us-east-2a",
            "regionName": "us-east-2"
        },
        "isTerminal": true,
        "operationDetails": "22/tcp(192.0.2.0/24)",
        "operationType": "OpenInstancePublicPorts",
        "status": "Succeeded",
        "statusChangedAt": "2023-02-15T16:41:50.048000-08:00"
    }
}
```

如需如何關閉連接埠的詳細資訊，請繼續下一節。

關閉虛擬電腦的連接埠

完成以下程序，關閉虛擬電腦的連接埠。此程序使用 `close-instance-public-ports` AWS CLI 命令。如需詳細資訊，請參閱 命令參考 close-instance-public-ports 中的 。 AWS CLI

1. 此步驟取決於本機電腦的作業系統。
   - 如果您的本機電腦使用 Windows 作業系統，請開啟「命令提示」視窗。
   - 如果您的本機電腦使用 Linux 或 UNIX 作業系統 (包括 macOS)，請開啟「終端機」視窗。
2. 輸入以下命令以關閉連接埠。

   在命令中，替換以下項目：

   - *REGION* 將 取代為虛擬電腦建立所在 AWS 區域的程式碼，例如 `us-east-2`。
   - 將 *NAME* 換成虛擬電腦的名稱。
   - 將 *FROM-PORT* 換成您想要關閉的連接埠範圍中的第一個連接埠。
   - 將 *PROTOCOL* 換成 IP 通訊協定名稱。例如，TCP。
   - 將 *TO-PORT* 換成您想要關閉的連接埠範圍中的最後一個連接埠。
   - 將 *IP* 換成您想要移除的 IP 地址或 IP 地址範圍。

   ```
   aws lightsail close-instance-public-ports --region REGION --instance-name NAME --
   port-info fromPort=FROM-PORT, protocol=PROTOCOL, toPort=TO-PORT,cidrs=IP
   ```

   範例

   ```
   aws lightsail close-instance-public-ports --region us-east-2 --instance-
   name MyUbuntu --port-info fromPort=22, protocol=TCP, toPort=22,cidrs=192.0.2.0/24
   ```

   回應會顯示已關閉且不再被允許連線至您虛擬電腦的連接埠、通訊協定和 IP CIDR範圍。

```
[redacted] % aws lightsail close-instance-public-ports --instance-name MyUbuntu
--port-info fromPort=22,protocol=TCP,toPort=22,cidrs=192.0.2.0/24
{
    "operation": {
        "id": "a7f3191a-e9ea-497d-b662-4428121f127c",
        "resourceName": "MyUbuntu",
        "resourceType": "Instance",
        "createdAt": "2023-02-15T16:48:42.459000-08:00",
        "location": {
            "availabilityZone": "us-east-2a",
            "regionName": "us-east-2"
        },
        "isTerminal": true,
        "operationDetails": "22/tcp(192.0.2.0/24)",
        "operationType": "CloseInstancePublicPorts",
        "status": "Succeeded",
        "statusChangedAt": "2023-02-15T16:48:42.459000-08:00"
    }
}
```

繼續後續步驟

成功管理虛擬電腦的防火牆連接埠後，您可以完成以下其他後續步驟：

- 取得虛擬電腦的金鑰對。使用金鑰對，您可以使用許多SSH用戶端建立連線，例如 Open SSH、PuTTY和 Windows Subsystem for Linux。如需詳細資訊，請參閱取得 Lightsail for Research 虛擬電腦的金鑰對。
- 使用 連線至您的虛擬電腦SSH，以使用命令列來管理它。如需詳細資訊，請參閱使用 Secure Copy 將檔案傳輸至 Lightsail for Research 虛擬電腦。
- 使用 連線至您的虛擬電腦SCP，以安全地傳輸檔案。如需詳細資訊，請參閱使用 Secure Copy 將檔案傳輸至 Lightsail for Research 虛擬電腦。

取得 Lightsail for Research 虛擬電腦的金鑰對

金鑰對包含公有金鑰和私有金鑰，是一組安全憑證，用於在連線至 Amazon Lightsail for Research 虛擬電腦時證明您的身分。公有金鑰會儲存在 Lightsail for Research 中的每個虛擬電腦上，而且您會在本機電腦上保留私有金鑰。私有金鑰可讓您使用虛擬機器安全地建立安全 Shell 通訊協定 （SSH）。任何擁有私有金鑰的人都可以連線到您的虛擬電腦，因此請務必將私有金鑰存放在安全的位置。

當您第一次建立 Lightsail 執行個體或 Lightsail for Research 虛擬電腦時，會自動建立 Amazon Lightsail 預設金鑰對 （DKP）。DKP 專屬於您在其中建立執行個體或虛擬電腦的每個 AWS 區域。例如，美國東部 DKP （俄亥俄） 區域的 Lightsail （us-east-2） 適用於您在美國東部 （俄亥俄） 建立的所有電腦，這些電腦設定為在建立DKP時使用 。Lightsail for Research 會自動將 的公有金鑰存放在您建立DKP的虛擬電腦上。DKP 您可以隨時API呼叫 Lightsail 服務來下載 的私有金鑰。

在本文件中，我們會示範如何取得虛擬電腦DKP的 。擁有 之後DKP，您可以使用許多SSH用戶端建立連線，例如 Open SSH、Pu TTY和 Windows Subsystem for Linux。您也可以使用 Secure Copy（SCP）將檔案從本機電腦安全地傳輸至虛擬電腦。

> **Note**
>
> 您也可以使用瀏覽器型 Amazon DCV用戶端，建立遠端顯示通訊協定連線至虛擬電腦。Amazon DCV 可在 Lightsail for Research 主控台中使用。該RDP用戶端不需要您為電腦取得金鑰對。如需詳細資訊，請參閱 存取 Lightsail for Research 虛擬電腦應用程式 和 存取 Lightsail for Research 虛擬電腦的作業系統。

主題

- 完成先決條件
- 取得虛擬電腦的金鑰對
- 繼續後續步驟

完成先決條件

開始之前，請先完成以下先決條件：

- 在 Lightsail for Research 中建立虛擬電腦。如需詳細資訊，請參閱建立 Lightsail for Research 虛擬電腦。
- 下載並安裝 AWS Command Line Interface（AWS CLI）。如需詳細資訊，請參閱《AWS Command Line Interface 第 2 版使用者指南》中的安裝或更新最新版的 AWS CLI。
- 設定 AWS CLI 以存取您的 AWS 帳戶。如需詳細資訊，請參閱《AWS Command Line Interface 第 2 版使用者指南》中的組態基礎概念。
- 下載並安裝 jq。它是一種輕量且靈活的命令列JSON處理器，用於下列程序，從 的JSON輸出擷取金鑰對詳細資訊 AWS CLI。如需有關下載和安裝 jq 的詳細資訊，請參閱 jq 網站上的下載 jq。

取得虛擬電腦的金鑰對

完成下列其中一個程序，以取得 Lightsail for Research 中虛擬電腦DKP的 Lightsail。

使用 Windows 本機電腦取得虛擬電腦的金鑰對

如果您的本機電腦使用 Windows 作業系統，則此程序適用。此程序使用 `download-default-key-pair` AWS CLI 命令來取得 DKP AWS 區域的 Lightsail。如需詳細資訊，請參閱 命令參考 download-default-key-pair 中的 。 AWS CLI

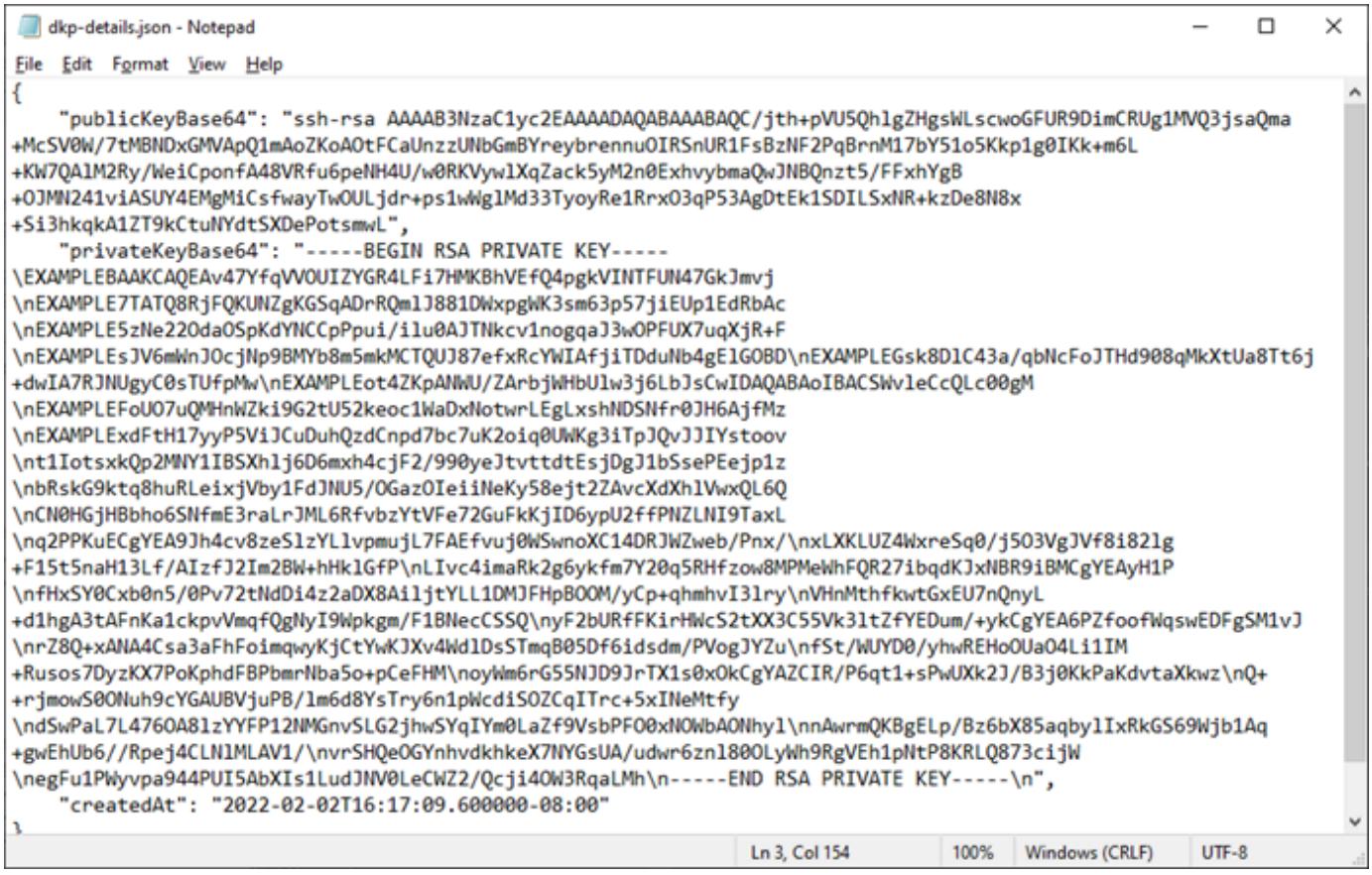
1. 開啟命令提示視窗。
2. 輸入下列命令以取得DKP特定 AWS 區域的 Lightsail。此命令會將資訊儲存到 `dkp-details.json` 檔案中。在 命令中，*`region-code`*將 取代為虛擬電腦建立所在 AWS 區域的程式碼，例如 `us-east-2`。

   ```
   aws lightsail download-default-key-pair --region region-code > dkp-details.json
   ```

   範例

   ```
   aws lightsail download-default-key-pair --region us-east-2 > dkp-details.json
   ```

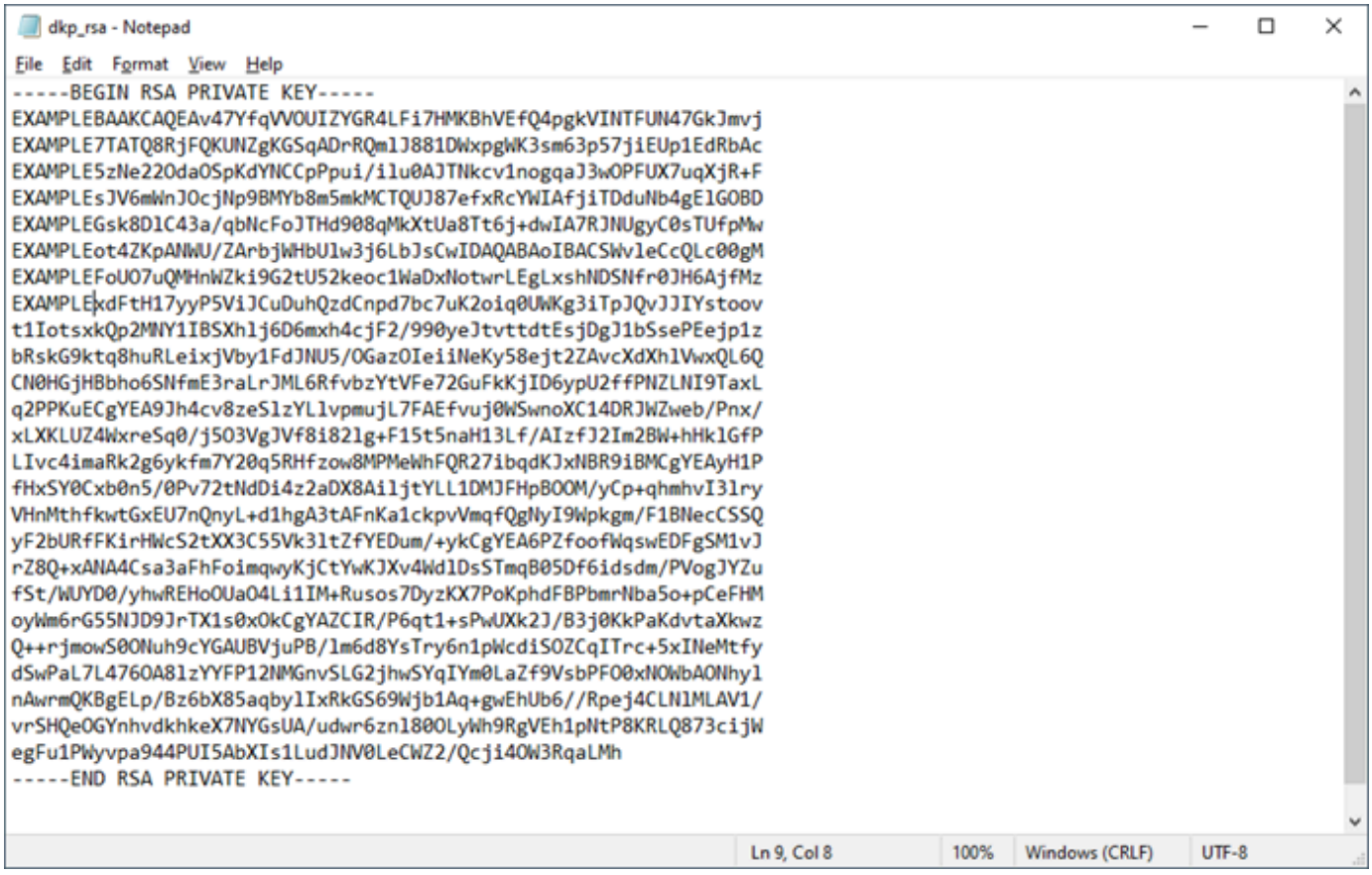
   沒有對命令的回應。您可以開啟`dkp-details.json`檔案並查看 Lightsail DKP資訊是否已儲存，以確認命令是否成功。`dkp-details.json` 檔案的內容應如以下範例所示：如果檔案為空白，表示命令失敗。



3. 輸入以下命令，從 dkp-details.json 檔案中提取私有金鑰資訊，並將其新增至新的 dkp_rsa 私有金鑰檔案。

```
type dkp-details.json | jq -r ".privateKeyBase64" > dkp_rsa
```

沒有對命令的回應。您可以藉由開啟 dkp_rsa 檔案並查看是否含有資訊，來確認命令是否成功。dkp_rsa 檔案的內容應如以下範例所示：如果檔案為空白，表示命令失敗。



您現在擁有建立 SSH或 SCP連線至虛擬電腦所需的私有金鑰。繼續下一節，進行其他後續步驟。

使用 Linux、Unix 或 macOS 本機電腦取得虛擬電腦的金鑰對

如果您的本機電腦使用 Linux、Unix 或 macOS 作業系統，則此程序適用。此程序使用 `download-default-key-pair` AWS CLI 命令來取得 DKP AWS 區域的 Lightsail。如需詳細資訊，請參閱 命令參考 download-default-key-pair 中的 。 AWS CLI

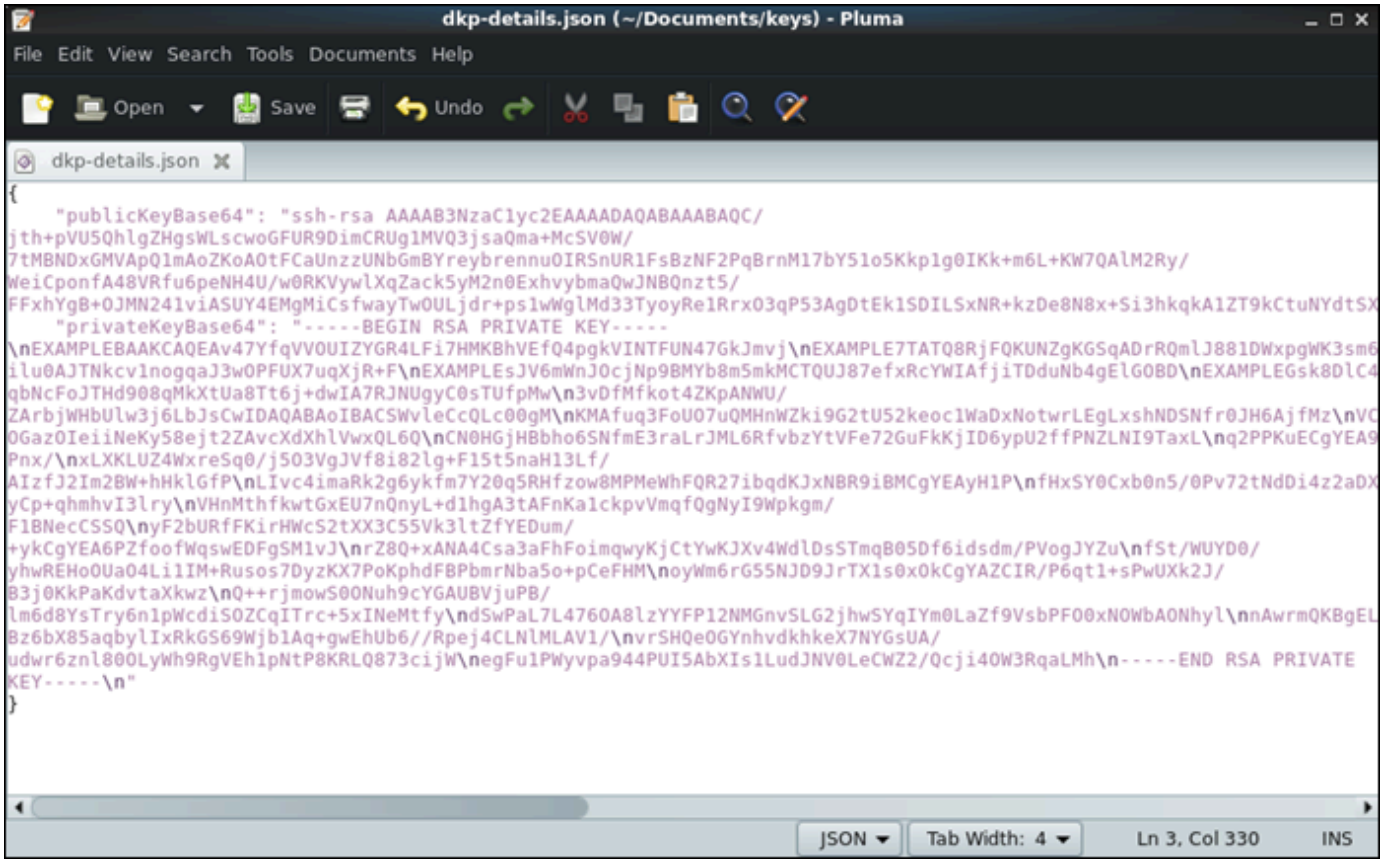
1. 開啟「終端機」視窗。
2. 輸入下列命令以取得DKP特定 AWS 區域的 Lightsail。此命令會將資訊儲存到 `dkp-details.json` 檔案中。在 命令中，*`region-code`*將 取代為虛擬電腦建立所在 AWS 區域的程式碼，例如 `us-east-2`。

```
aws lightsail download-default-key-pair --region region-code > dkp-details.json
```

範例

```
aws lightsail download-default-key-pair --region us-east-2 > dkp-details.json
```

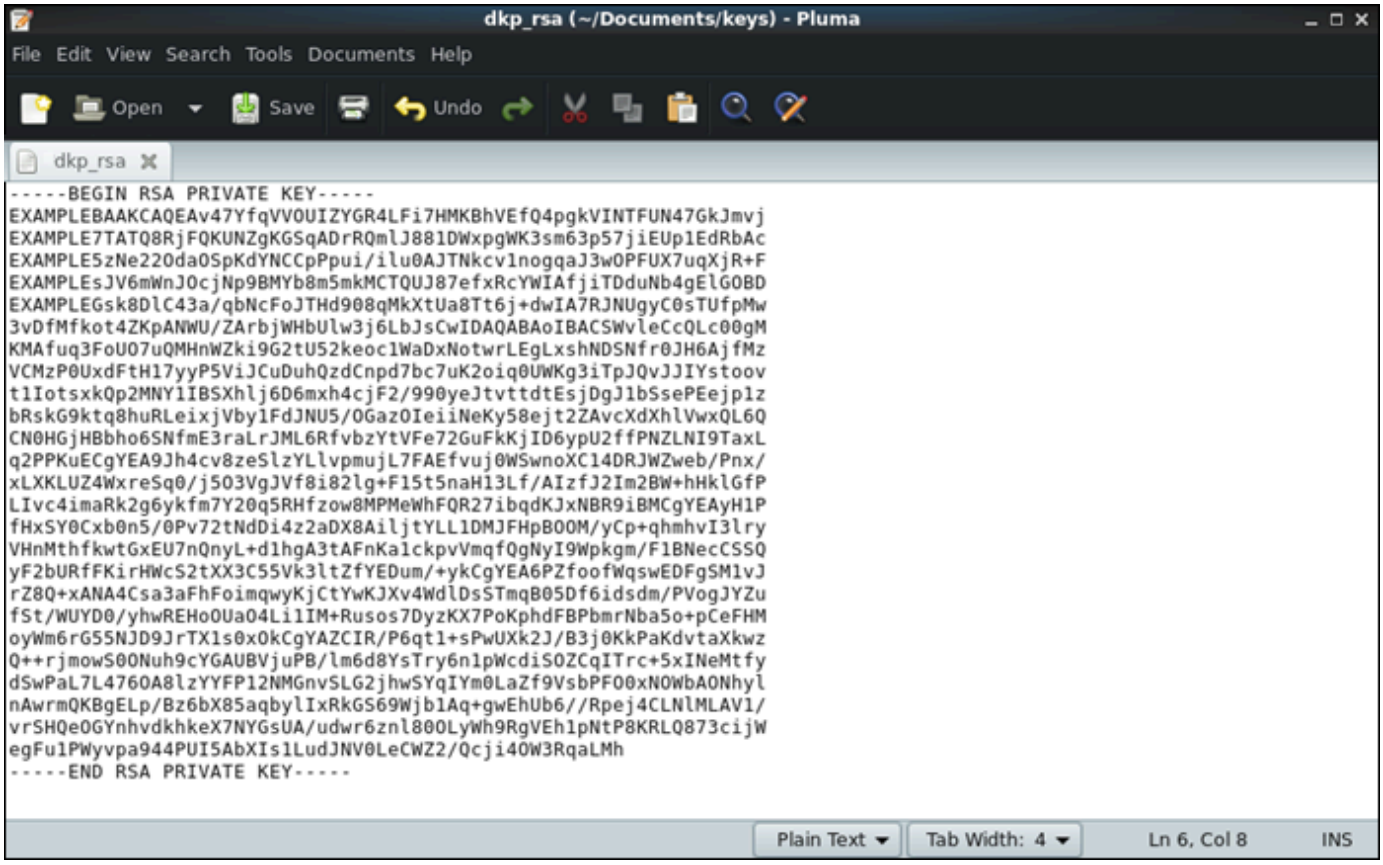
沒有對命令的回應。您可以開啟dkp-details.json檔案並查看 Lightsail DKP資訊是否已儲存，以確認命令是否成功。dkp-details.json 檔案的內容應如以下範例所示：如果檔案為空白，表示命令失敗。



3. 輸入以下命令，從 dkp-details.json 檔案中提取私有金鑰資訊，並將其新增至新的 dkp_rsa 私有金鑰檔案。

```
cat dkp-details.json | jq -r '.privateKeyBase64' > dkp_rsa
```

沒有對命令的回應。您可以藉由開啟 dkp_rsa 檔案並查看是否含有資訊，來確認命令是否成功。dkp_rsa 檔案的內容應如以下範例所示：如果檔案為空白，表示命令失敗。



4. 輸入以下命令以設定 dkp_rsa 檔案的許可：

```
chmod 600 dkp_rsa
```

您現在擁有建立 SSH或 SCP連線至虛擬電腦所需的私有金鑰。繼續下一節，進行其他後續步驟。

繼續後續步驟

成功取得虛擬電腦的金鑰對後，可以完成以下其他後續步驟：

- 使用 連線至您的虛擬電腦SSH，以使用命令列管理它。如需詳細資訊，請參閱使用 Secure Shell 連線至 Lightsail for Research 虛擬電腦。
- 使用 連線至您的虛擬電腦SCP，以安全地傳輸檔案。如需詳細資訊，請參閱使用 Secure Copy 將檔案傳輸至 Lightsail for Research 虛擬電腦。

使用 Secure Shell 連線至 Lightsail for Research 虛擬電腦

您可以使用 Secure Shell 通訊協定 （ ） 連線至 Amazon Lightsail for Research 中的虛擬電腦SSH。您可以使用 SSH 遠端管理虛擬電腦，以便透過網際網路登入電腦並執行命令。

> **Note**
>
> 您也可以使用瀏覽器型 Amazon DCV用戶端，建立遠端顯示通訊協定連線至虛擬電腦。Amazon DCV 可在 Lightsail for Research 主控台中使用。如需詳細資訊，請參閱存取 Lightsail for Research 虛擬電腦的作業系統。

主題

- 完成先決條件
- 使用 連線至虛擬電腦 SSH
- 繼續後續步驟

完成先決條件

開始之前，請先完成以下先決條件：

- 在 Lightsail for Research 中建立虛擬電腦。如需詳細資訊，請參閱建立 Lightsail for Research 虛擬電腦。
- 確認您想連線的虛擬電腦處於運行中狀態。此外，請注意虛擬電腦的名稱及其建立所在的 AWS 區域。稍後在這個程序中，您需要此資訊。如需詳細資訊，請參閱檢視 Lightsail for Research 虛擬電腦詳細資訊。
- 確認您想要連線的虛擬電腦上連接埠 22 已開啟。這是 使用的預設連接埠SSH。預設為開啟 但如果您已將其關閉，則必須重新開啟，然後再繼續。如需詳細資訊，請參閱管理 Lightsail for Research 虛擬電腦的防火牆連接埠。
- 取得虛擬電腦的 Lightsail 預設金鑰對 （DKP）。如需詳細資訊，請參閱取得虛擬電腦的金鑰對。

> **Tip**
>
> 如果您打算使用 AWS CloudShell 連線到您的虛擬電腦，請參閱下一節使用 連線至虛擬電腦 AWS CloudShell中的 。如需詳細資訊，請參閱什麼是 AWS CloudShell。否則，請繼續下一個先決條件。

- 下載並安裝 AWS Command Line Interface （ AWS CLI ）。如需詳細資訊，請參閱《AWS Command Line Interface 第 2 版使用者指南》中的安裝或更新最新版的 AWS CLI。
- 設定 AWS CLI 以存取您的 AWS 帳戶。如需詳細資訊，請參閱《AWS Command Line Interface 第 2 版使用者指南》中的組態基礎概念。
- 下載並安裝 jq。它是一種輕量且靈活的命令列JSON處理器，用於下列程序，以擷取金鑰對詳細資訊。如需有關下載和安裝 jq 的詳細資訊，請參閱 jq 網站上的下載 jq。

使用 連線至虛擬電腦 SSH

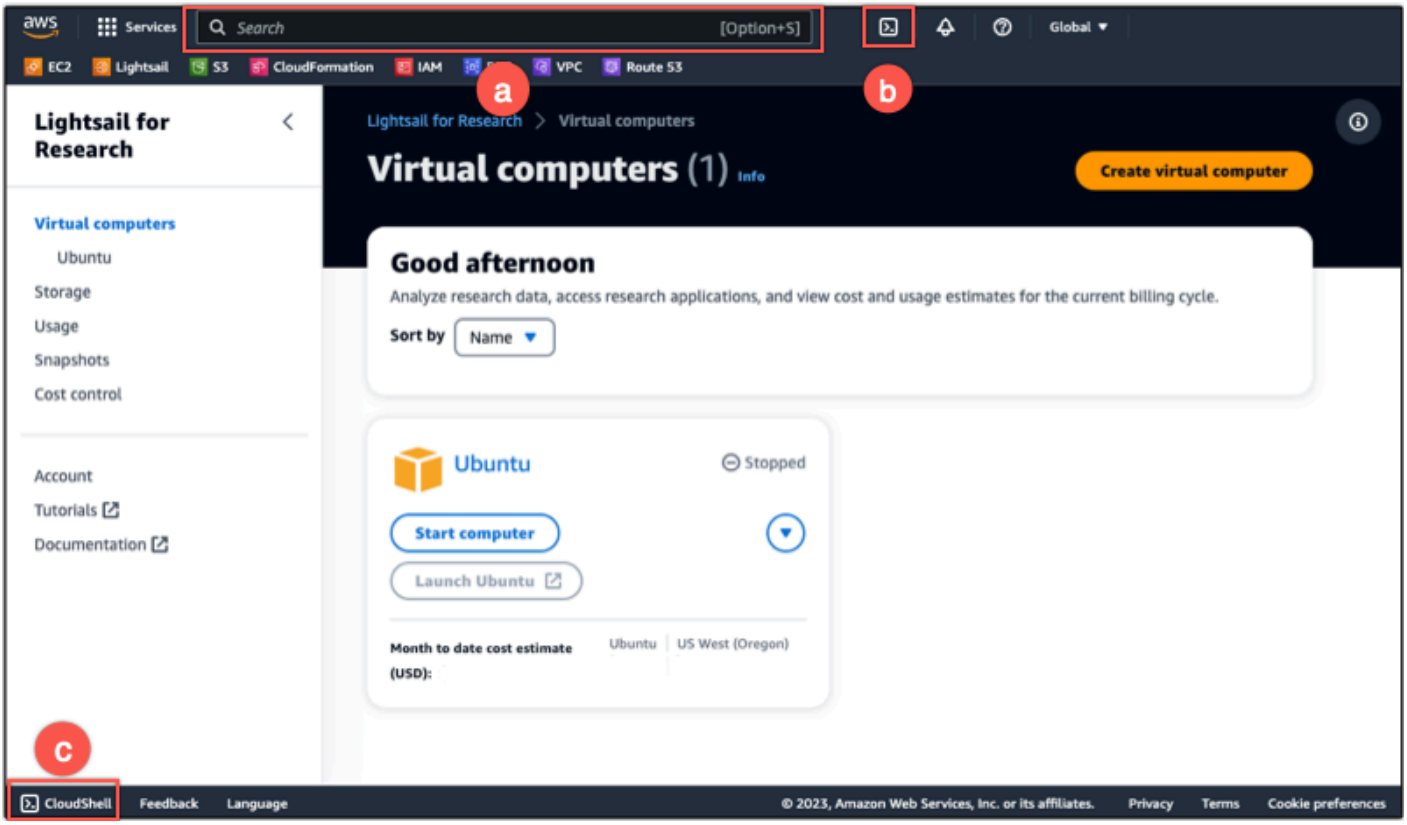
完成下列其中一個程序，在 Lightsail for Research 中建立與虛擬電腦的SSH連線。

使用 連線至虛擬電腦 AWS CloudShell

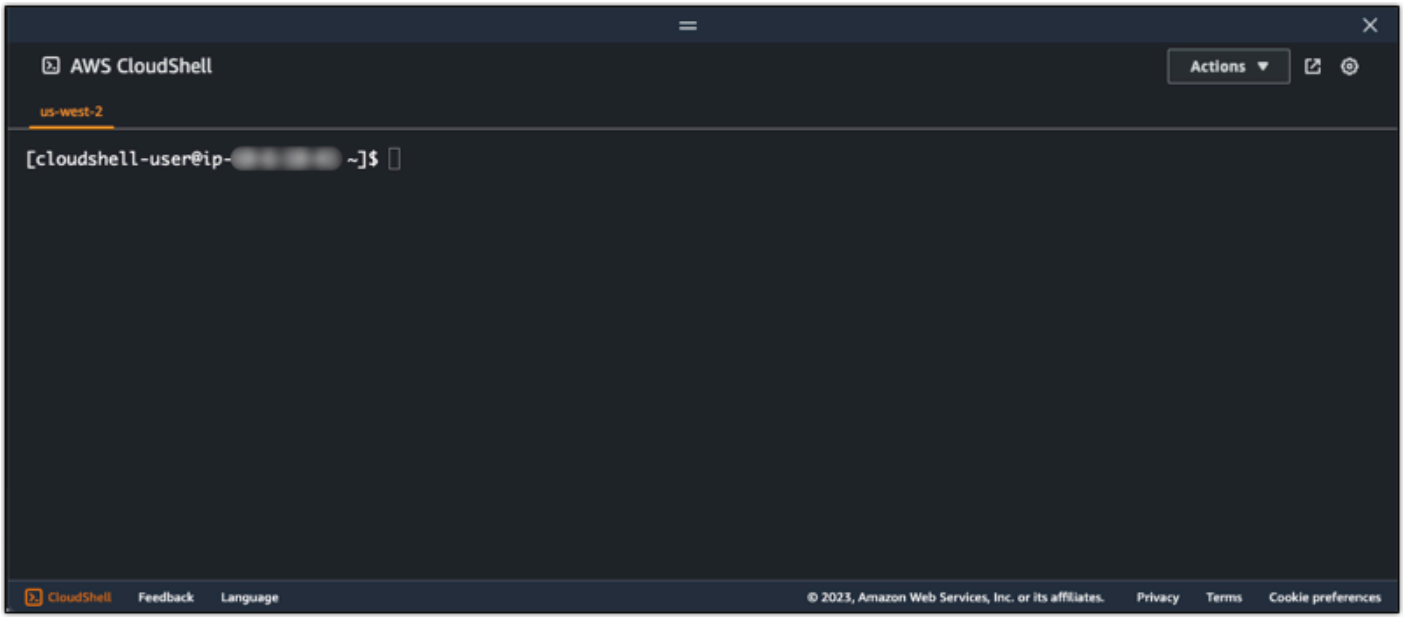
如果您偏好最低設定連線到虛擬電腦，則此程序適用。 AWS CloudShell 會使用瀏覽器型預先驗證的 Shell，您可以直接從 啟動 AWS Management Console。您可以使用您偏好的 shell 執行 AWS CLI 命令，例如 Bash PowerShell或 Z Shell。無需下載或安裝命令列工具即可執行此操作。如需詳細資訊，請參閱《AWS CloudShell 使用者指南》中的 AWS CloudShell入門

> **Important**
>
> 開始之前，請務必取得您要連線之虛擬電腦的 Lightsail 預設金鑰對 （ DKP ）。如需詳細資訊，請參閱取得 Lightsail for Research 虛擬電腦的金鑰對。

1. 從 Lightsail for Research 主控台 中，選擇下列其中一個選項 CloudShell 來啟動：
   a. 在搜尋方塊中，輸入 "CloudShell"，然後選擇 CloudShell。
   b. 在導覽列上，選擇 CloudShell 圖示。
   c. CloudShell 在主控台左下角的主控台工具列上選擇 。



出現命令提示時，表示 Shell 已準備好開始互動。



2. 選擇要使用的預先安裝 Shell。若要變更預設 Shell，請在命令列提示中輸入下列其中一個程式名稱。Bash 是啟動 時執行的預設 Shell AWS CloudShell。

Bash

```
bash
```

如果您切換至 Bash，命令提示字元的 符號會更新為 $。

PowerShell

```
pwsh
```

如果您切換至 PowerShell，命令提示字元的 符號會更新為 PS>。

Z shell

```
zsh
```

如果您切換至 Z shell，命令提示字元的 符號會更新為 %。

3. 若要從 CloudShell 終端機視窗連線至虛擬電腦，請參閱 在 SSH Linux、Unix 或 macOS 本機電腦上使用 連線至虛擬電腦。

如需環境中 CloudShell預先安裝軟體的相關資訊，請參閱 AWS CloudShell 使用者指南 中的AWS CloudShell 運算環境。

在 SSH Windows 本機電腦上使用 連線至虛擬電腦

如果您的本機電腦使用 Windows 作業系統，則此程序適用。此程序使用 `get-instance` AWS CLI 命令來取得您要連線之執行個體的使用者名稱和公有 IP 地址。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 get-instance。

> **Important**
>
> 在開始此程序之前，請確定您取得要連線之虛擬電腦的 Lightsail 預設金鑰對 （DKP）。如需詳細資訊，請參閱取得 Lightsail for Research 虛擬電腦的金鑰對。該程序會將 Lightsail 的私有金鑰輸出DKP至下列其中一個命令中使用的`dkp_rsa`檔案。

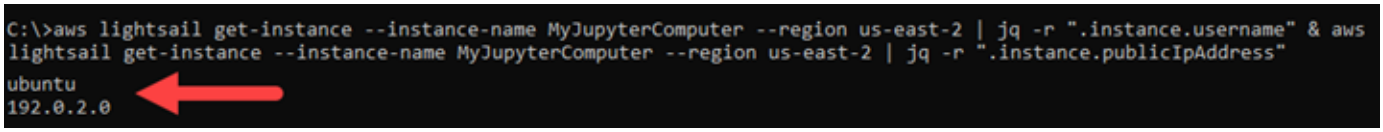
1. 開啟命令提示視窗。
2. 輸入以下命令以顯示虛擬電腦的公有 IP 地址和使用者名稱。在 命令中，*`region-code`*將 取代為建立 AWS 區域 虛擬電腦的 程式碼，例如 `us-east-2`。將 *`computer-name`* 換成您想要連線的虛擬電腦的名稱。

```
aws lightsail get-instance --region region-code --instance-name computer-name |
 jq -r ".instance.username" & aws lightsail get-instance --region region-code --
instance-name computer-name | jq -r ".instance.publicIpAddress"
```

範例

```
aws lightsail get-instance --region us-east-2 --instance-name MyJupyterComputer
 | jq -r ".instance.username" & aws lightsail get-instance --region us-east-2 --
instance-name MyJupyterComputer | jq -r ".instance.publicIpAddress"
```

回應會顯示虛擬電腦的使用者名稱和公有 IP 地址，如以下範例所示。記下這些值，因為在此程序的下一步中會用到。



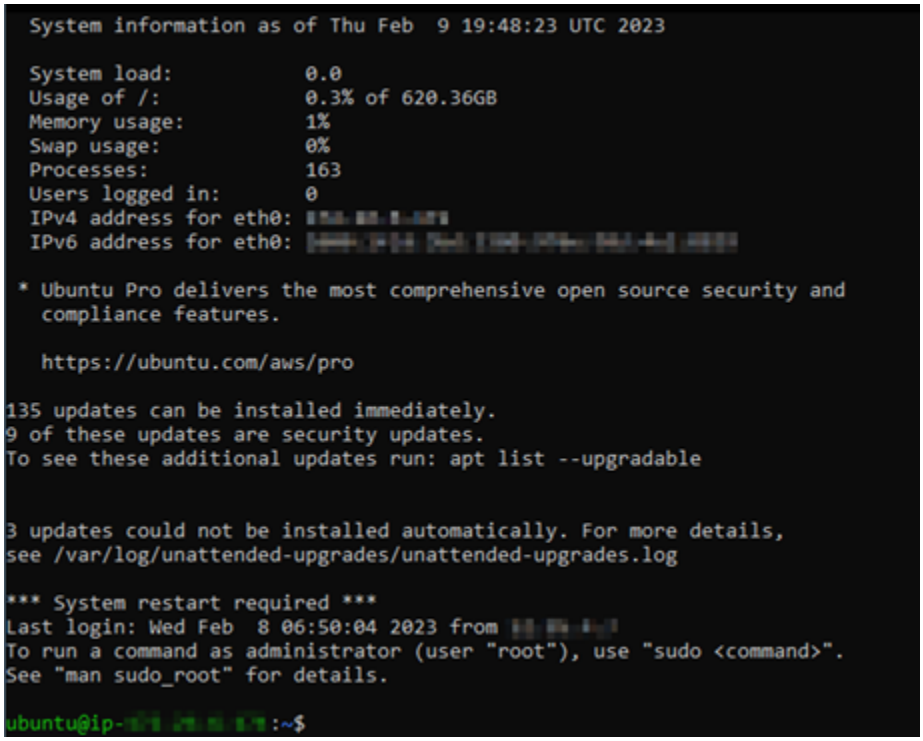
3. 輸入下列命令以建立與虛擬電腦的SSH連線。在命令中，將 *user-name* 換成登入的使用者名稱，並將 *public-ip-address* 換成虛擬電腦的公有 IP 地址。

```
ssh -i dkp_rsa user-name@public-ip-address
```

範例

```
ssh -i dkp_rsa ubuntu@192.0.2.0
```

您應該會看到類似下列範例的回應，顯示與 Lightsail for Research 中的 Ubuntu 虛擬電腦建立的SSH連線。



現在您已成功建立與虛擬電腦的SSH連線，請繼續前往下一節以取得其他後續步驟。

在 SSH Linux、Unix 或 macOS 本機電腦上使用 連線至虛擬電腦

如果您的本機電腦使用 Linux、Unix 或 macOS 作業系統，則此程序適用。此程序使用 `get-instance` AWS CLI 命令來取得您要連線之執行個體的使用者名稱和公有 IP 地址。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 get-instance。

> **Important**
>
> 在開始此程序之前，請確定您取得要連線之虛擬電腦的 Lightsail 預設金鑰對（DKP）。如需詳細資訊，請參閱取得 Lightsail for Research 虛擬電腦的金鑰對。該程序會將 Lightsail 的私有金鑰輸出DKP至下列其中一個命令中使用的`dkp_rsa`檔案。

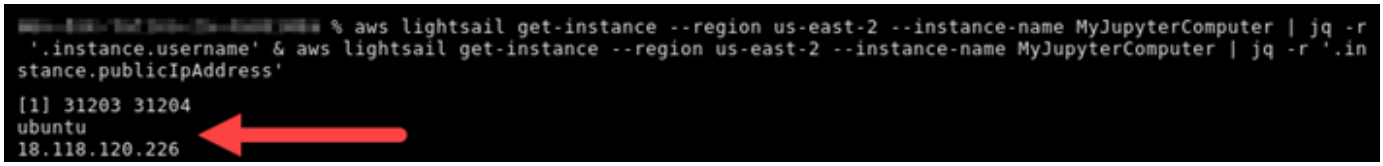
1. 開啟「終端機」視窗。
2. 輸入以下命令以顯示虛擬電腦的公有 IP 地址和使用者名稱。在 命令中，*`region-code`*將 取代為虛擬電腦建立所在 AWS 區域的程式碼，例如 `us-east-2`。將 *`computer-name`* 換成您想要連線的虛擬電腦的名稱。

```
aws lightsail get-instance --region region-code --instance-name computer-name |
 jq -r '.instance.username' && aws lightsail get-instance --region region-code --
instance-name computer-name | jq -r '.instance.publicIpAddress'
```

範例

```
aws lightsail get-instance --region us-east-2 --instance-name MyJupyterComputer
 | jq -r '.instance.username' && aws lightsail get-instance --region us-east-2 --
instance-name MyJupyterComputer | jq -r '.instance.publicIpAddress'
```

回應會顯示虛擬電腦的使用者名稱和公有 IP 地址，如以下範例所示。記下這些值，因為在此程序的下一步中會用到。



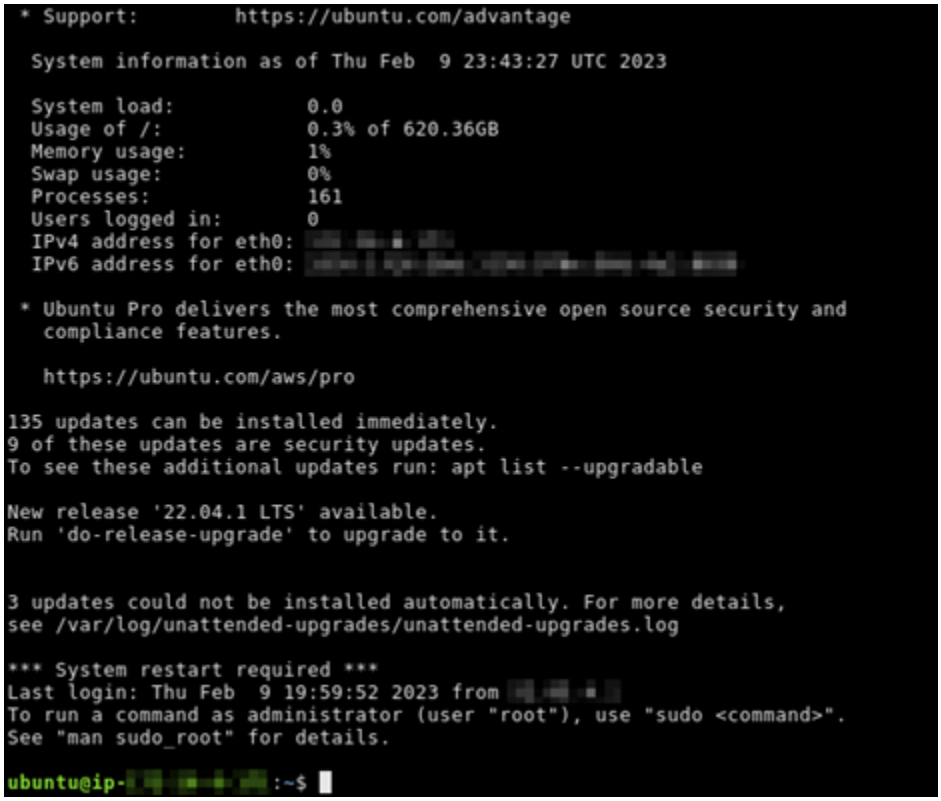
3. 輸入下列命令以建立與虛擬電腦的SSH連線。在命令中，將 *user-name* 換成登入的使用者名稱，並將 *public-ip-address* 換成虛擬電腦的公有 IP 地址。

```
ssh -i dkp_rsa user-name@public-ip-address
```

範例

```
ssh -i dkp_rsa ubuntu@192.0.2.0
```

您應該會看到類似下列範例的回應，顯示與 Lightsail for Research 中的 Ubuntu 虛擬電腦建立的SSH連線。



現在您已成功建立與虛擬電腦的SSH連線，請繼續前往下一節以取得其他後續步驟。

繼續後續步驟

您可以在成功建立與虛擬電腦的SSH連線之後，完成下列其他後續步驟：

- 使用 連線至您的虛擬電腦SCP，以安全地傳輸檔案。如需詳細資訊，請參閱使用 Secure Copy 將檔案傳輸至 Lightsail for Research 虛擬電腦。

使用 Secure Copy 將檔案傳輸至 Lightsail for Research 虛擬電腦

您可以使用 Secure Copy （ ），將檔案從本機電腦傳輸到 Amazon Lightsail for Research 中的虛擬電腦SCP。利用此程序，您可以一次傳輸多個檔案或整個目錄。

> **Note**
>
> 您也可以使用 Lightsail for Research 主控台中提供的瀏覽器型 Amazon DCV用戶端，建立與虛擬電腦的遠端顯示通訊協定連線。使用 Amazon DCV用戶端，您可以快速傳輸個別檔案。如需詳細資訊，請參閱存取 Lightsail for Research 虛擬電腦的作業系統。

主題

- 完成先決條件
- 使用 連線至虛擬電腦 SCP

完成先決條件

開始之前，請先完成以下先決條件：

- 在 Lightsail for Research 中建立虛擬電腦。如需詳細資訊，請參閱建立 Lightsail for Research 虛擬電腦。
- 確認您想連線的虛擬電腦處於運行中狀態。此外，請記下虛擬電腦的名稱和在其中建立該虛擬電腦的 AWS 區域。您在此程序的後續步驟中會需要此資訊。如需詳細資訊，請參閱檢視 Lightsail for Research 虛擬電腦詳細資訊。
- 下載並安裝 AWS Command Line Interface （ AWS CLI ）。如需詳細資訊，請參閱《AWS Command Line Interface 第 2 版使用者指南》中的安裝或更新最新版的 AWS CLI。
- 設定 AWS CLI 以存取您的 AWS 帳戶。如需詳細資訊，請參閱《AWS Command Line Interface 第 2 版使用者指南》中的組態基礎概念。
- 下載並安裝 jq。它是一種輕量且靈活的命令列JSON處理器，用於下列程序，以擷取金鑰對詳細資訊。如需有關下載和安裝 jq 的詳細資訊，請參閱 jq 網站上的下載 jq。
- 確認您想要連線的虛擬電腦上連接埠 22 已開啟。這是 使用的預設連接埠SSH。預設為開啟 但如果您已將其關閉，則必須重新開啟，然後再繼續。如需詳細資訊，請參閱管理 Lightsail for Research 虛擬電腦的防火牆連接埠。
- 取得虛擬電腦的 Lightsail 預設金鑰對 （ DKP ）。如需詳細資訊，請參閱建立 Lightsail for Research 虛擬電腦。

使用 連線至虛擬電腦 SCP

完成下列其中一個程序，使用 連線至 Lightsail for Research 中的虛擬電腦SCP。

在 SCP Windows 本機電腦上使用 連線至虛擬電腦

如果您的本機電腦使用 Windows 作業系統，則此程序適用。此程序使用 `get-instance` AWS CLI 命令來取得您要連線之執行個體的使用者名稱和公有 IP 地址。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 get-instance。

> **Important**
>
> 在開始此程序之前，請確定您取得要連線之虛擬電腦的 Lightsail 預設金鑰對 （DKP）。如需詳細資訊，請參閱取得 Lightsail for Research 虛擬電腦的金鑰對。該程序會將 Lightsail 的私有金鑰輸出DKP至下列其中一個命令中使用的`dkp_rsa`檔案。

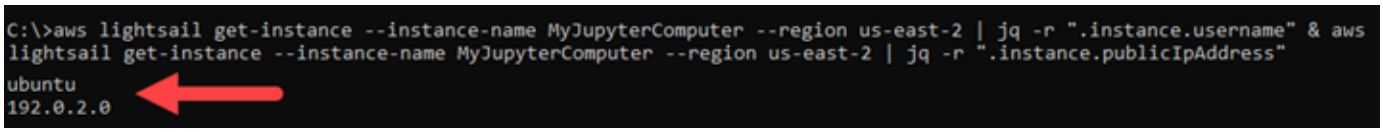
1. 開啟命令提示視窗。
2. 輸入以下命令以顯示虛擬電腦的公有 IP 地址和使用者名稱。在 命令中，*`region-code`*將 取代為虛擬電腦建立所在 AWS 區域的程式碼，例如 `us-east-2`。將 *`computer-name`* 換成您想要連線的虛擬電腦的名稱。

   ```
   aws lightsail get-instance --region region-code --instance-name computer-name |
    jq -r ".instance.username" & aws lightsail get-instance --region region-code --
   instance-name computer-name | jq -r ".instance.publicIpAddress"
   ```

   範例

   ```
   aws lightsail get-instance --region us-east-2 --instance-name MyJupyterComputer
    | jq -r ".instance.username" & aws lightsail get-instance --region us-east-2 --
   instance-name MyJupyterComputer | jq -r ".instance.publicIpAddress"
   ```

   回應會顯示虛擬電腦的使用者名稱和公有 IP 地址，如以下範例所示。記下這些值，因為在此程序的下一步中會用到。

3. 輸入下列命令，以建立與虛擬電腦的SCP連線，並將檔案傳輸至其中。

   ```
   scp -i dkp_rsa -r "source-folder" user-name@public-ip-address:destination-directory
   ```

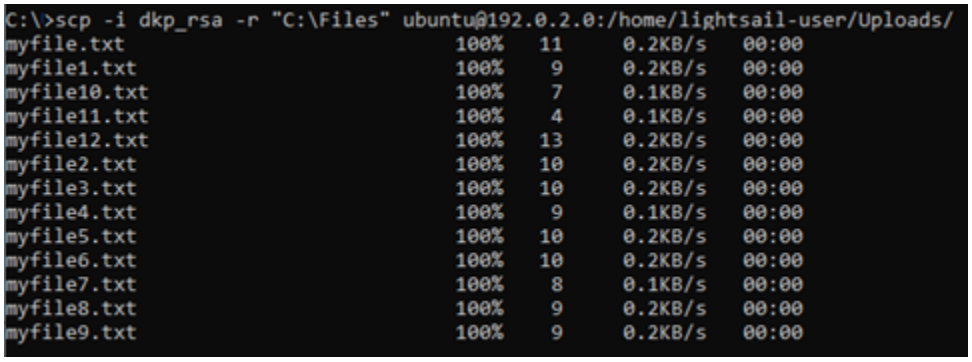
   在命令中：

- 將 *source-folder* 換成本機電腦上含有要傳輸的檔案的資料夾。
- 將 *user-name* 換成此程序先前步驟的使用者名稱 (例如 ubuntu)。
- 將 *public-ip-address* 換成此程序先前步驟的虛擬電腦公有 IP 地址。
- 將 *destination-directory* 換成您想要複製檔案的虛擬電腦上的目錄路徑。

以下範例會將本機電腦上 C:\Files 資料夾中的所有檔案複製到遠端虛擬電腦上的 /home/lightsail-user/Uploads/ 目錄。

```
scp -i dkp_rsa -r "C:\Files" ubuntu@192.0.2.0:/home/lightsail-user/Uploads/
```

您應該會看到類似於以下範例的回應。顯示從原始資料夾傳輸到目的地目錄的每個檔案。現在，您應該可以在虛擬電腦上存取這些檔案。



在 SCP Linux、Unix 或 macOS 本機電腦上使用 連線至虛擬電腦

如果您的本機電腦使用 Linux、Unix 或 macOS 作業系統，則此程序適用。此程序使用 get-instance AWS CLI 命令來取得您要連線之執行個體的使用者名稱和公有 IP 地址。如需詳細資訊，請參閱《AWS CLI 命令參考》中的 get-instance。

> **Important**
>
> 在開始此程序之前，請確定您取得要連線之虛擬電腦的 Lightsail 預設金鑰對 （DKP）。如需詳細資訊，請參閱取得 Lightsail for Research 虛擬電腦的金鑰對。該程序會將 Lightsail 的私有金鑰輸出DKP至下列其中一個命令中使用的dkp_rsa檔案。

1. 開啟「終端機」視窗。

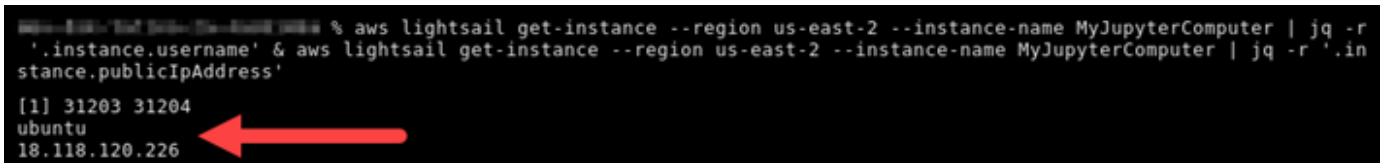
2. 輸入以下命令以顯示虛擬電腦的公有 IP 地址和使用者名稱。在 命令中，*region-code*將 取代為虛擬電腦建立所在 AWS 區域的程式碼，例如 us-east-2。將 *computer-name* 換成您想要連線的虛擬電腦的名稱。

```
aws lightsail get-instance --region region-code --instance-name computer-name |
 jq -r '.instance.username' & aws lightsail get-instance --region region-code --
instance-name computer-name | jq -r '.instance.publicIpAddress'
```

範例

```
aws lightsail get-instance --region us-east-2 --instance-name MyJupyterComputer
 | jq -r '.instance.username' & aws lightsail get-instance --region us-east-2 --
instance-name MyJupyterComputer | jq -r '.instance.publicIpAddress'
```

回應會顯示虛擬電腦的使用者名稱和公有 IP 地址，如以下範例所示。記下這些值，因為在此程序的下一步中會用到。



3. 輸入下列命令，以建立與虛擬電腦的SCP連線，並將檔案傳輸至其中。

```
scp -i dkp_rsa -r 'source-folder' user-name@public-ip-address:destination-directory
```

在命令中：

- 將 *source-folder* 換成本機電腦上含有要傳輸的檔案的資料夾。
- 將 *user-name* 換成此程序先前步驟的使用者名稱 (例如 ubuntu)。
- 將 *public-ip-address* 換成此程序先前步驟的虛擬電腦公有 IP 地址。
- 將 *destination-directory* 換成您想要複製檔案的虛擬電腦上的目錄路徑。

以下範例會將本機電腦上 C:\Files 資料夾中的所有檔案複製到遠端虛擬電腦上的 /home/lightsail-user/Uploads/ 目錄。

```
scp -i dkp_rsa -r 'Files' ubuntu@192.0.2.0:/home/lightsail-user/Uploads/
```

您應該會看到類似於以下範例的回應。顯示從原始資料夾傳輸到目的地目錄的每個檔案。現在，您應該可以在虛擬電腦上存取這些檔案。

```
([redacted]) <0> [~/Documents/Keys]
[redacted] # scp -i dkp_rsa -r 'Files' ubuntu@192.0.0.2:/home/lightsail-user/Uploads/
myfile2.txt                                   100%   10     0.2KB/s   00:00
myfile6.txt                                   100%   10     0.2KB/s   00:00
myfile7.txt                                   100%    8     0.1KB/s   00:00
myfile10.txt                                  100%    7     0.1KB/s   00:00
myfile1.txt                                   100%    9     0.2KB/s   00:00
myfile3.txt                                   100%   10     0.2KB/s   00:00
myfile12.txt                                  100%   13     0.2KB/s   00:00
myfile.txt                                    100%   11     0.2KB/s   00:00
myfile9.txt                                   100%    9     0.2KB/s   00:00
myfile11.txt                                  100%    4     0.1KB/s   00:00
myfile5.txt                                   100%   10     0.2KB/s   00:00
myfile4.txt                                   100%    9     0.2KB/s   00:00
myfile8.txt                                   100%    9     0.2KB/s   00:00
```

刪除 Lightsail for Research 虛擬電腦

當您不再需要 Lightsail for Research 虛擬電腦時，請完成下列步驟以將其刪除。一旦刪除虛擬電腦後，您即無須再支付其費用。連接至已刪除電腦的資源，例如快照，仍會持續產生費用，直到您將其刪除為止。

> **Important**
>
> 刪除虛擬電腦是永久性的動作，而且無法將電腦復原。如果之後可能需要資料，請在刪除之前建立虛擬電腦的快照。如需詳細資訊，請參閱建立快照。

1. 登入 Lightsail for Research 主控台 。
2. 在導覽窗格中，選擇虛擬電腦。
3. 選擇要刪除的虛擬電腦。
4. 選擇動作，然後選擇刪除虛擬電腦。
5. 在文字區塊中鍵入確認。然後，選擇刪除虛擬電腦。

使用 Lightsail 保護和儲存資料，適用於研究資料

適用於研究的 Amazon Lightsail 提供區塊層級儲存磁碟區 (磁碟)，您可以將這些磁碟連接到執行中的 Lightsail 用於研究虛擬電腦。您可以使用磁碟做為需要頻繁和精細更新之資料的主要儲存裝置。例如，當您在 Lightsail 研究用虛擬電腦上執行資料庫時，建議使用磁碟選項。

磁碟的行為類似於未格式化的外部區塊型儲存裝置，您可以將其連接至單一虛擬電腦。磁碟區的存續與電腦的運行壽命無關。將磁碟連接至電腦後，您就能像使用任何其他實體硬碟一樣的使用。

您可以將多個磁碟連接至一台電腦。您也可以將磁碟與某台電腦分離，然後連接至另一台電腦。

若要保留資料的備份副本，請建立磁碟的快照。您可以從快照建立新的磁碟，然後連接至另一台電腦。

主題

- 在適用於研究的 Lightsail 主控台中建立儲存磁碟
- 在 Lightsail 進行研究的主控台中檢視儲存磁碟詳細資料
- 在 Lightsail 進行研究的虛擬電腦中新增儲存空間
- 在 Lightsail 中將磁碟從虛擬電腦中卸離以進行研究
- 刪除研究用的 Lightsail 中未使用的儲存磁碟

在適用於研究的 Lightsail 主控台中建立儲存磁碟

請完成下列步驟，為您的 Lightsail 研究用虛擬電腦建立磁碟。

1. 登入適用於研究的 Lightsail 主控台。
2. 在導覽窗格中，選擇儲存。
3. 選擇 Create disk (建立磁碟)。
4. 輸入磁碟的名稱。有效字元包括英數字元、數字、句點、連字符和底線。

   磁碟名稱必須符合以下要求：

   - AWS 區域 在您的 Lightsail 研究帳戶中，每個項目都是獨一無二的。
   - 含有 2–255 個字元。
   - 開頭和結尾為英數字元或數字。
5. AWS 區域 為您的磁碟選擇一個。

磁碟必須位於和您要連接之虛擬電腦相同的區域。

6. 選擇磁碟大小，單位為 GB。
7. 如需將磁碟連接至虛擬電腦的資訊，請繼續磁碟連接章節。

在 Lightsail 進行研究的主控台中檢視儲存磁碟詳細資料

請完成下列步驟，以檢視 Lightsail 用於研究帳戶中的磁碟及其詳細資料。

1. 登入適用於研究的 Lightsail 主控台。
2. 在導覽窗格中，選擇儲存。

   [儲存空間] 頁面提供您 Lightsail 研究帳戶中磁碟的完整檢視。

   頁面上會顯示以下資訊：

   - 名稱 – 儲存磁碟的名稱。
   - 大小 – 磁碟的大小 (單位為 GB)。
   - AWS 區域 – 在其中建立磁碟的 AWS 區域 。
   - 附加至 — 您的磁碟所連接的 Lightsail 電腦。
   - 建立日期 – 建立磁碟的日期。

在 Lightsail 進行研究的虛擬電腦中新增儲存空間

請完成下列步驟，將磁碟附加至 Lightsail 進行研究用的虛擬電腦。您最多可以將 15 個磁碟連接至虛擬電腦。當您使用 Lightsail 進行研究控制台將磁碟連接到虛擬電腦時，該服務會自動格式化和掛載該磁碟。此過程需要幾分鐘的時間，因此您應該先確認磁碟已達到掛載狀態，然後再開始使用。根據預設，研究專用 Lightsail 會將磁碟掛接到/home/lightsail-user/*<disk-name>*目錄；其中*<disk-name>*是您為磁碟提供的名稱。

> **Important**
>
> 虛擬電腦必須處於執行中狀態，才能將磁碟連接至虛擬電腦。如果您在虛擬電腦處於已停止狀態時連接磁碟，則磁碟將會連接但無法掛載。如果磁碟的掛載狀態為失敗，您必須先分離磁碟，然後在虛擬電腦處於運行中狀態時重新連接磁碟。

1. 登入適用於研究的 Lightsail 主控台。
2. 在導覽窗格中，選擇虛擬電腦。
3. 選擇磁碟要連接的電腦。
4. 選擇儲存分頁。
5. 選擇連接磁碟。
6. 選取要連接至電腦的磁碟名稱。
7. 選擇 Attach (連接)。

在 Lightsail 中將磁碟從虛擬電腦中卸離以進行研究

完成以下步驟，以將磁碟與電腦分離。

1. 登入適用於研究的 Lightsail 主控台。
2. 在導覽窗格中，選擇儲存。
3. 找到您想要分離的磁碟。在連接至欄位下，選擇與磁碟相連的電腦名稱。
4. 選擇停止以停止電腦。您必須先停止電腦，才能分離磁碟。
5. 確認您要停止電腦，然後選擇停止電腦電腦。
6. 選擇儲存分頁。
7. 選取要分離的磁碟，然後選擇分離。
8. 確認您要將磁碟與電腦分離，然後選擇分離。

刪除研究用的 Lightsail 中未使用的儲存磁碟

當您不再需要儲存磁碟時，完成以下步驟以刪除磁碟。一旦刪除磁碟後，您即無須再支付其費用。

如果磁碟連接至電腦，您必須先將其分離才能刪除。如需詳細資訊，請參閱在 Lightsail 中將磁碟從虛擬電腦中卸離以進行研究。

1. 登入適用於研究的 Lightsail 主控台。
2. 在導覽窗格中，選擇儲存。
3. 尋找並選取您要刪除的磁碟。
4. 選擇刪除磁碟。
5. 確認您要刪除磁碟。再選擇 Delete (刪除)。

使用 Lightsail 進行研究快照 Backup 虛擬電腦和磁碟

快照是資料的 point-in-time 副本。您可以建立 Amazon Lightsail 用於研究虛擬電腦和儲存磁碟的快照，並將其用作基準以建立新電腦或進行資料備份。

快照包含還原電腦所需的所有資料 (從建立快照的那一刻開始)。當您以快照為基礎建立新虛擬電腦時，其開始成為用來建立快照之原始電腦的確切複本。

由於您的資源隨時可能發生問題，因此建議您定期建立快照，以免資料遺失永久遺失。

主題

- 建立適用於研究人員的 Lightsail 虛擬電腦或磁碟快照
- 在研究專用 Lightsail 中檢視和管理虛擬電腦和磁碟快照
- 從快照建立虛擬電腦或磁碟
- 在適用於研究的 Lightsail 主控台中刪除快照

建立適用於研究人員的 Lightsail 虛擬電腦或磁碟快照

請完成下列步驟，以建立 Lightsail 研究用虛擬電腦或磁碟的快照。

1. 登入適用於研究的 Lightsail 主控台。
2. 在導覽窗格中，選擇 Snapshots (快照)。
3. 完成以下其中一個步驟：
   - 在虛擬電腦快照之下，找到您要製做快照的電腦名稱，然後選擇建立快照。
   - 在磁照快照之下，找到您要製做快照的磁碟名稱，然後選擇建立快照。
4. 輸入快照的名稱。有效字元包括英數字元、數字、句點、連字符和底線。

   快照名稱必須符合以下要求：
   - AWS 區域 在您的 Lightsail 研究帳戶中，每個項目都是獨一無二的。
   - 含有 2–255 個字元。
   - 開頭和結尾為英數字元或數字。
5. 選擇建立快照。

在研究專用 Lightsail 中檢視和管理虛擬電腦和磁碟快照

完成以下步驟，檢視虛擬電腦和磁碟的快照。

1. 登入適用於研究的 Lightsail 主控台。
2. 在導覽窗格中，選擇 Snapshots (快照)。

   快照頁面會顯示您已建立的虛擬電腦和磁碟快照。

   封存的快照也在此頁面上。封存的快照是已從您的帳戶中刪除之資源的快照。

從快照建立虛擬電腦或磁碟

完成下列步驟，即可從快照建立新的 Lightsail 適用於研究的虛擬電腦或磁碟。

當您從快照建立虛擬電腦時，使用與原始電腦大小相同或更大的方案。您無法使用小於原始虛擬電腦的方案。

當您從快照建立磁碟時，選擇原始磁碟大的磁碟大小。您無法使用比原始磁碟小的磁碟。

1. 登入適用於研究的 Lightsail 主控台。
2. 在導覽窗格中，選擇 Snapshots (快照)。
3. 在快照頁面上，找到要用來建立新電腦或磁碟的電腦或磁碟快照名稱。選擇快照下拉式選單，檢視該資源的可用快照清單。
4. 選取您想要用來建立虛擬電腦的快照。
5. 選擇動作下拉式選單。然後，選擇建立虛擬電腦或建立磁碟。

在適用於研究的 Lightsail 主控台中刪除快照

完成以下步驟以刪除快照。

1. 登入適用於研究的 Lightsail 主控台。
2. 在導覽窗格中，選擇 Snapshots (快照)。
3. 在快照頁面上，找到要刪除的電腦或磁碟快照的名稱。選擇快照下拉式選單，檢視該資源的可用快照清單。
4. 選取想要刪除的快照。

5. 選擇動作下拉式選單。然後選擇刪除快照。
6. 確認快照名稱正確無誤。然後選擇刪除快照。

研究用 Lightsail 中的成本和使用量估算

適用於研究的 Amazon Lightsail 可為您的 AWS 資源提供成本和用量估算。使用 Lightsail for Research 時，您可以使用這些估算值來協助您規劃支出方式、尋找節省成本的機會，以及做出明智的決定。

當您建立虛擬電腦或磁碟時，會顯示該資源的成本和用量估算。成本和用量估算會在資源建立後並處於可用或執行中狀態時立即開始追蹤。資源建立後 15 分鐘內，估算值會顯示在AWS管理主控台中。估算不會包含已刪除的資源。

> **Important**
>
> 估算是以資源用量為基礎的預估成本。您的實際成本將根據資源的實際使用情況而定，而不是 Lightsail for Research 主控台中顯示的估計值。實際費用會顯示在您的帳 AWS Billing 戶對帳單上。
>
> 登入 AWS Management Console 並開啟 AWS Billing 主控台，位於https://console.aws.amazon.com/billing/。

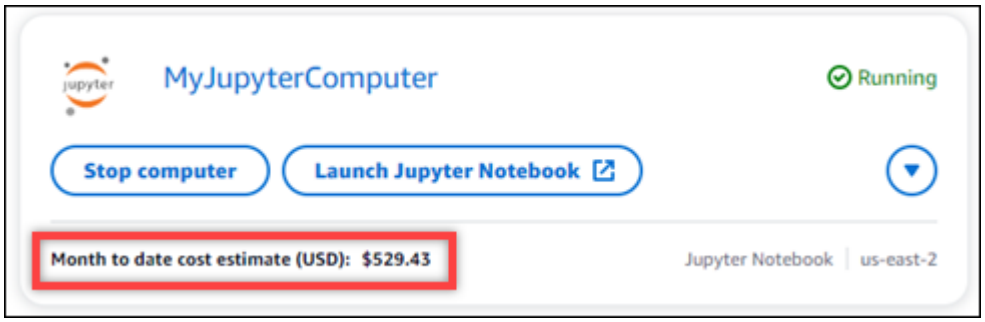
主題

- 在研究用 Lightsail 中檢視資源的成本和使用量預估

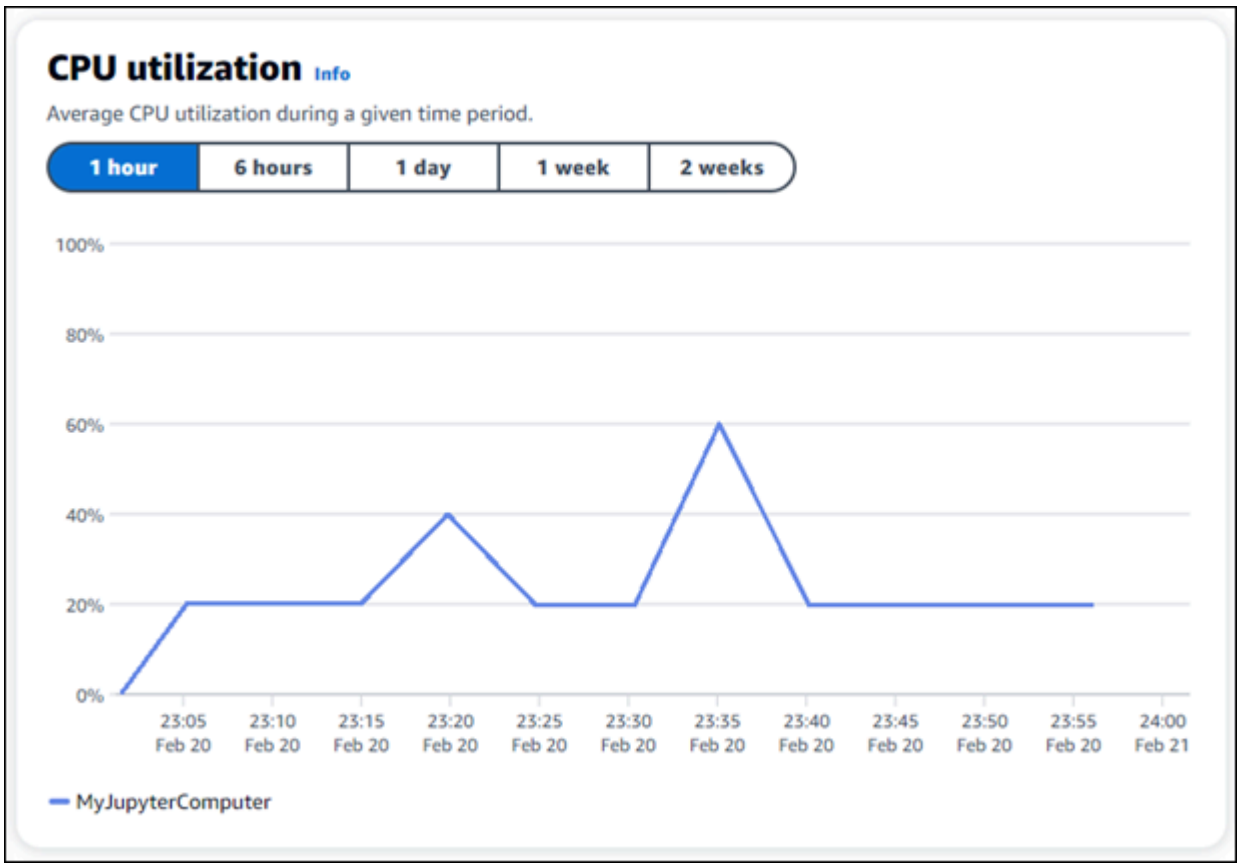
在研究用 Lightsail 中檢視資源的成本和使用量預估

Lightsail 研究用資源的每月迄今成本和使用量估算會顯示在 Li ghtsail 用於研究主控台的下列區域中。

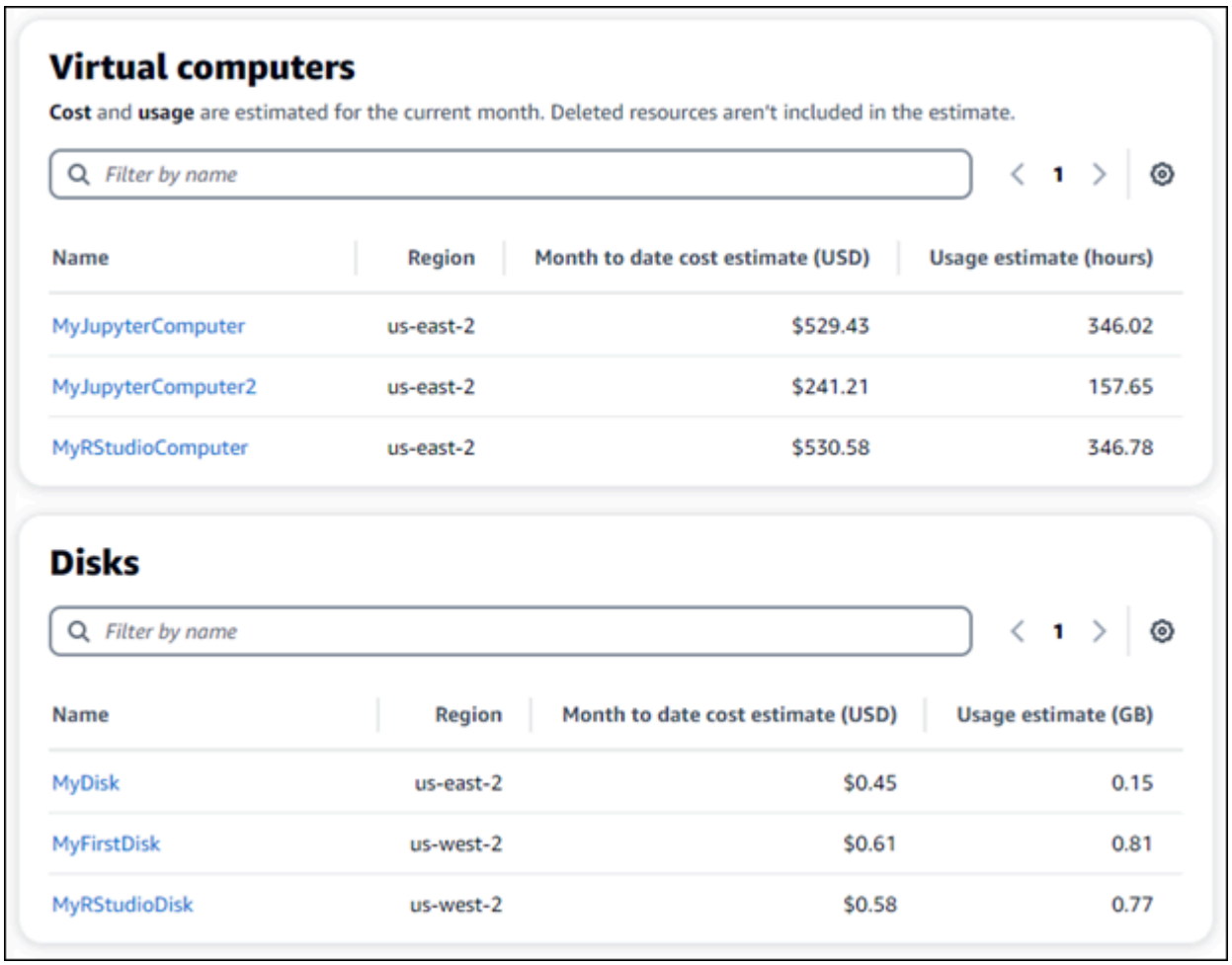
1. 在適用於研究的 Lightsail 主控台的導覽窗格中選擇虛擬電腦。每台運行中虛擬電腦的下方，會列出該虛擬電腦當月至今的成本估算。



2. 若要檢視虛擬電腦的CPU使用率，請選擇虛擬電腦的名稱，然後選擇 [儀表板] 索引標籤。



3. 若要檢視所有 Lightsail for Research 資源的每月迄今成本和使用量預估，請在導覽窗格中選擇「使用量」。


Virtual computers
Cost and usage are estimated for the current month. Deleted resources aren't included in the estimate.
Filter by name
1
Name
Region
Month to date cost estimate (USD)
Usage estimate (hours)
MyJupyterComputer
us-east-2
$529.43
346.02
MyJupyterComputer2
us-east-2
$241.21
157.65
MyRStudioComputer
us-east-2
$530.58
346.78
Disks
Filter by name
1
Name
Region
Month to date cost estimate (USD)
Usage estimate (GB)
MyDisk
us-east-2
$0.45
0.15
MyFirstDisk
us-west-2
$0.61
0.81
MyRStudioDisk
us-west-2
$0.58
0.77

管理研究用 Lightsail 中的成本控制規則

成本控制會使用您定義的規則來協助管理 Lightsail 用於研究虛擬電腦的使用量和成本。

您可以建立閒置時停止虛擬電腦規則，在指定期間內達到CPU使用率的指定百分比時，停止執行中的電腦。例如，當特定電腦的CPU使用率在 30 分鐘的期間內等於或小於 5% 時，規則可以自動停止。這表示電腦處於閒置狀態，而研究用 Lightsail 會停止電腦。虛擬電腦停止後，您就不需要支付標準的小時費用。

主題

- 為您的研究用 Lightsail 虛擬電腦建立成本控制規則
- 刪除適用於研究成本的 Lightsail 虛擬電腦的成本控制規則

為您的研究用 Lightsail 虛擬電腦建立成本控制規則

請完成下列步驟，為您的 Lightsail 研究用虛擬電腦建立規則。

> **Note**
>
> 此時唯一支援的規則動作是停止虛擬電腦。CPU使用率是目前唯一受規則監督的測量結果，而唯一支援的作業小於或等於。

1. 登入適用於研究的 Lightsail 主控台。
2. 在導覽窗格中，選擇成本控制。
3. 選擇建立規則。
4. 選取要套用規則的資源。
5. 指定應執行規則的CPU使用率百分比和期間。

   例如，您可以指定 5% 和 30 分鐘。Lightsail 適用於研究的電腦會在 30 分鐘的期間內，當電腦的CPU使用率低於或等於 5% 時，自動停止電腦。
6. 選擇建立規則。
7. 確認新規則的資訊正確無誤，然後選擇確認。

刪除適用於研究成本的 Lightsail 虛擬電腦的成本控制規則

請完成下列步驟，以刪除 Lightsail 研究用虛擬電腦的規則。

1. 登入適用於研究的 Lightsail 主控台。
2. 在導覽窗格中，選擇成本控制。
3. 選取要刪除的規則。
4. 選擇刪除。
5. 確認您要刪除規則，然後選擇刪除。

使用標籤整理用於研究資源的 Lightsail

使用亞馬遜研究用 Lightsail，您可以為資源指派標籤。每個標籤都是由索引鍵和選用值組成的標示，能夠有效率的管理您的資源。沒有值的索引鍵稱為僅索引鍵標籤，而具有值的索引鍵稱為鍵值標籤。雖然沒有固有的標籤類型，但能讓您依用途、擁有者、環境或其他條件將資源分類。這在您擁有許多相同類型的資源時很有用。您可以根據您指派給資源的標籤快速識別特定資源。例如，您可以定義一組能夠協助您追蹤每個資源之專案或優先順序的標籤。

您可以在適用於研究的亞馬遜 Lightsail 主控台中標記下列資源：

- 虛擬電腦
- 儲存磁碟
- 快照

以下限制適用於標籤：

- 每一資源標籤數最多為 50。
- 每個資源的每個標籤索引鍵都必須是唯一的。每個標籤索引鍵只能有一個值。
- 最大密鑰長度是 128 碼字符 UTF -8。
- 最大值長度為 UTF -8 中 256 個萬國碼字元。
- 如果您的標記結構描述是跨多項服務和資源使用，請記得其他服務可能會有字元使用限制。通常允許的字元為：字母、數字和空格，以及以下字元：`+ - = . _ : / @`。
- 標籤金鑰與值皆區分大小寫。
- 索引鍵或值請勿使用 `aws:` 字首。該前綴保留供 AWS 使用。

主題

- 標籤 Lightsail 的研究資源
- 移除研究資 Lightsail 的標籤

標籤 Lightsail 的研究資源

請完成下列步驟，為您的 Lightsail 研究用虛擬電腦建立標籤。Lightsail 研究專用磁碟和快照集的步驟類似。

1. 在適用於研究的 Lightsail 主控台上登入適用於研究的 Lightsail 主控台。
2. 在導覽窗格中，選擇虛擬電腦。
3. 選擇您要為其建立標籤的虛擬電腦。
4. 選擇 Tags (標籤) 索引標籤。
5. 選擇管理標籤。
6. 選擇 Add new tag (新增標籤)。
7. 在索引鍵欄位中輸入標籤名稱。例如，專案。
8. (選用) 在值欄位中輸入值名稱。例如，部落格。
9. 選擇儲存變更，將索引鍵儲存至虛擬電腦。

移除研究資 Lightsail 的標籤

完成下列步驟，即可從 Lightsail 研究用虛擬電腦刪除標籤。Lightsail 研究專用磁碟和快照集的步驟類似。

1. 在適用於研究的 Lightsail 主控台上登入適用於研究的 Lightsail 主控台。
2. 在導覽窗格中，選擇虛擬電腦。
3. 選擇您要刪除標籤的虛擬電腦。
4. 選擇 Tags (標籤) 索引標籤。
5. 選擇管理標籤。
6. 選擇移除，以刪除資源的標籤。

> **Note**
>
> 如果您只想移除標籤的值，找到該值，然後選擇旁邊的 X 圖示。

7. 選擇 Save changes (儲存變更)。

Amazon Lightsail for Research 的安全性

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

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

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。 AWS 也提供您可以安全使用的服務。第三方稽核人員會定期測試和驗證我們安全的有效性，這是AWS 合規計畫 的一部分。若要了解適用於 Amazon Lightsail for Research 的合規計劃，請參閱合規計劃AWS 範圍內的合規計劃。
- 雲端安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 Lightsail for Research 時套用共同責任模型。下列主題說明如何設定 Lightsail for Research 以符合您的安全性和合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Lightsail for Research 資源。

主題

- Amazon Lightsail for Research 中的資料保護
- 適用於 Amazon Lightsail for Research 的身分和存取管理
- Amazon Lightsail for Research 的合規驗證
- Amazon Lightsail for Research 中的復原能力
- Amazon Lightsail for Research 中的基礎設施安全性
- Amazon Lightsail for Research 中的組態和漏洞分析
- Amazon Lightsail for Research 的安全最佳實務

Amazon Lightsail for Research 中的資料保護

AWS 共同責任模型適用於 Amazon Lightsail for Research 中的資料保護。如本模型所述， AWS 負責保護執行所有 的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權。FAQ如需歐洲資料保護的相關資訊，請參閱AWS 安全部落格 上的AWS 共同責任模型和GDPR部落格文章。

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

- 對每個帳戶使用多重要素驗證 （MFA）。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 和 建議 TLS 1.3。
- 使用 設定 API 和使用者活動日誌 AWS CloudTrail。如需使用 CloudTrail 線索擷取 AWS 活動的資訊，請參閱 AWS CloudTrail 使用者指南 中的使用 CloudTrail 線索。
- 使用 AWS 加密解決方案，以及 中的所有預設安全控制項 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列介面或 FIPS 存取 時需要 140-3 個經過驗證的密碼編譯模組API，請使用FIPS端點。如需可用FIPS端點的詳細資訊，請參閱聯邦資訊處理標準 （FIPS） 140-3。

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

適用於 Amazon Lightsail for Research 的身分和存取管理

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

> **Note**
>
> Amazon Lightsail 和 Lightsail for Research 共用相同的IAM政策參數。Lightsail for Research 政策的變更也會影響 Lightsail 政策。例如，如果使用者擁有在 Lightsail for Research 中建立磁碟的許可，則該相同使用者也可以在 Lightsail 中建立磁碟。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- Amazon Lightsail for Research 如何與 搭配使用 IAM
- Amazon Lightsail for Research 的身分型政策範例
- 對 Amazon Lightsail for Research 身分和存取權進行故障診斷

物件

使用 AWS Identity and Access Management （ IAM ） 的方式會有所不同，取決於您在 Lightsail for Research 中執行的工作。

服務使用者 – 如果您使用 Lightsail for Research 服務來執行您的任務，則您的管理員會為您提供所需的憑證和許可。當您使用更多 Lightsail for Research 功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 Lightsail for Research 中的功能，請參閱 對 Amazon Lightsail for Research 身分和存取權進行故障診斷。

服務管理員 – 如果您在公司負責 Lightsail for Research 資源，您可能可以完整存取 Lightsail for Research。您的任務是判斷您的服務使用者應存取哪些 Lightsail for Research 功能和資源。然後，您必須向IAM管理員提交請求，以變更服務使用者的許可。請檢閱此頁面上的資訊，以了解 的基本概念 IAM。若要進一步了解您的公司如何IAM搭配 Lightsail for Research 使用，請參閱 Amazon Lightsail for Research 如何與 搭配使用 IAM。

IAM 管理員 – 如果您是IAM管理員，您可能想要了解如何撰寫政策以管理 Lightsail for Research 存取的詳細資訊。若要檢視您可以在 中使用的 Lightsail for Research 身分型政策範例IAM，請參閱 Amazon Lightsail for Research 的身分型政策範例。

使用身分驗證

驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者身分、IAM使用者身分或擔任IAM角色來驗證 （ 登入 AWS ）。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分登入 。 AWS IAM Identity Center （ IAM Identity Center ） 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 憑證，都是聯合身分的範例。當您以聯合身分登入時，您的管理員先前會使用 IAM角色設定身分聯合。當您 AWS 使用聯合來存取 時，您會間接擔任 角色。

根據您身分的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱 使用者指南 中的如何登入 AWS 帳戶您的 。 AWS 登入

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 （ SDK ） 和命令列介面 （ CLI ），以使用您的 憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南 中的簽署 AWS API請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多因素身分驗證 （ MFA ） 來提高帳戶的安全性。若要進一步了解，請參閱AWS IAM Identity Center 使用者指南中的多重要素驗證，以及IAM使用者指南中的使用多重要素驗證 （ MFA ） AWS。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個登入身分開始，該身分可完全存取 帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 根使用者，透過您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以根使用者身分登入的任務完整清單，請參閱 IAM 使用者指南 中的需要根使用者憑證的任務。

聯合身分

最佳實務是， 要求人類使用者，包括需要管理員存取權的使用者，使用 AWS 服務 臨時憑證與身分提供者聯合來存取 。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、 AWS Directory Service、身分中心目錄，或使用透過身分來源提供的 AWS 服務 憑證存取的任何使用者。當聯合身分存取 時 AWS 帳戶，它們會擔任 角色，而角色會提供臨時憑證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，或者您可以連線並同步到您身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有 和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱 AWS IAM Identity Center 使用者指南 中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是 中具有單一個人或應用程式特定許可 AWS 帳戶 的身分。在可能的情況下，我們建議依賴臨時憑證，而不是建立具有密碼和存取金鑰等長期憑證IAM的使用者。不過，如果您有特定的使用案例需要IAM使用者長期憑證，建議您輪換存取金鑰。如需詳細資訊，請參閱 IAM 使用者指南 中的定期輪換需要長期憑證的使用案例存取金鑰。

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

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。若要進一步了解，請參閱 IAM 使用者指南 中的何時建立IAM使用者（而非角色）。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似於IAM使用者，但與特定人員無關。您可以透過 AWS Management Console 切換IAM角色 暫時在 中擔任角色。 https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html您可以透過呼叫 AWS CLI 或 AWS API 操作，或使用自訂 來擔任角色URL。如需使用角色方法的詳細資訊，請參閱 IAM 使用者指南 中的擔任角色的方法。

IAM 具有臨時憑證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱 IAM 使用者指南 中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，您可以設定許可集。若要控制身分在身分驗證後可存取的內容，IAMIdentity Center 會將許可集與 中的角色相關聯IAM。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 臨時IAM使用者許可 – IAM使用者或角色可以擔任IAM角色，暫時接受特定任務的不同許可。
- 跨帳戶存取 – 您可以使用 IAM角色，允許不同帳戶中的某人（受信任的主體）存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。不過，使用部分 AWS 服務，您可以將政策直接連接至資源（而不是使用角色作為代理）。若要了解跨帳戶存取的角色與資源型政策之間的差異，請參閱 IAM 使用者指南 中的跨帳戶資源存取IAM。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在 服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式EC2或在 Amazon S3 中儲存物件。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉送存取工作階段（FAS）– 當您使用IAM使用者或角色在 中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，並結合請求向下游服務 AWS 服務 提出請求。FAS 只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出FAS請求時的政策詳細資訊，請參閱轉送存取工作階段 。

- 服務角色 – 服務角色是服務代表您執行動作時擔任IAM的角色。IAM 管理員可以從 內部建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 使用者指南 中的建立角色以將許可委派給 AWS 服務 。 IAM
- 服務連結角色 – 服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的 中 AWS 帳戶 ，並由 服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

- 在 Amazon 上執行的應用程式 EC2 – 您可以使用 IAM角色來管理在EC2執行個體上執行的應用程式的臨時憑證，以及提出 AWS CLI 或 AWS API請求。最好將存取金鑰存放在EC2執行個體中。若要將 AWS 角色指派給EC2執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體設定檔。執行個體設定檔包含 角色，並啟用在EC2執行個體上執行的程式，以取得臨時憑證。如需詳細資訊，請參閱 IAM 使用者指南 中的使用 IAM角色將許可授予在 Amazon EC2執行個體上執行的應用程式。

若要了解如何使用IAM角色或IAM使用者，請參閱 IAM 使用者指南 中的建立IAM角色 （ 而非使用者 ）的時機。

使用政策管理存取權

您可以透過建立政策並將其連接至 AWS 身分或資源 AWS 來控制 中的存取。政策是 AWS 其中的物件，當與身分或資源相關聯時， 會定義其許可。當主體 （ 使用者、根使用者或角色工作階段 ） 發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策會以JSON文件 AWS 形式儲存在 中。如需JSON政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南 中的JSON政策概觀。

管理員可以使用 AWS JSON政策來指定誰可以存取什麼。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對所需資源執行動作的許可，IAM管理員可以建立IAM政策。然後，管理員可以將IAM政策新增至角色，使用者可以擔任角色。

IAM 無論您用來執行操作的方法為何，政策都會定義動作的許可。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console、 AWS CLI或 AWS 取得角色資訊API。

身分型政策

身分型政策是您可以連接到身分的JSON許可政策文件，例如IAM使用者、使用者群組或角色。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分型政策，請參閱 IAM 使用者指南 中的建立IAM政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。若要了解如何在受管政策或內嵌政策之間進行選擇，請參閱 IAM 使用者指南 中的在受管政策與內嵌政策之間進行選擇。

資源型政策

資源型政策是您連接至資源JSON的政策文件。資源型政策的範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策 。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主體可以包括帳戶、使用者、角色、聯合使用者或 AWS 服務。

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

存取控制清單 （ACLs）

存取控制清單 （ACLs） 控制哪些主體 （帳戶成員、使用者或角色） 具有存取 資源的許可。ACLs 類似於資源型政策，雖然它們不使用JSON政策文件格式。

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

其他政策類型

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

- 許可界限 – 許可界限是一項進階功能，您可以在其中設定身分型政策可授予IAM實體 （IAM使用者或角色） 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南 中的IAM實體許可界限。
- 服務控制政策 （SCPs） – SCPs是在 中指定組織或組織單位 （OU） 最大許可JSON的政策 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶 的多個

的服務。如果您啟用組織中的所有功能，則可以將服務控制政策（SCPs）套用至任何或所有帳戶。SCP 限制成員帳戶中實體的許可，包括每個 AWS 帳戶根使用者。如需 Organizations 和 的詳細資訊SCPs，請參閱 AWS Organizations 使用者指南 中的服務控制政策。

- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南 中的工作階段政策。

多種政策類型

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

Amazon Lightsail for Research 如何與 搭配使用 IAM

在您使用 IAM 管理 Lightsail for Research 的存取權之前，請先了解哪些IAM功能可與 Lightsail for Research 搭配使用。

IAM 您可以與 Amazon Lightsail for Research 搭配使用的功能

IAM 功能	Lightsail for Research 支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACLs	否
ABAC （政策中的標籤）	部分
臨時憑證	是
主體許可	否

IAM 功能	Lightsail for Research 支援
服務角色	否
服務連結角色	否

若要取得 Lightsail for Research 和其他 AWS 服務如何與大多數 IAM 功能搭配使用的高階檢視，請參閱 IAM 使用者指南 中的AWS 使用 的服務IAM。

Lightsail for Research 的身分型政策

支援身分型政策：是

身分型政策是您可以連接到身分的JSON許可政策文件，例如IAM使用者、使用者群組或角色。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分型政策，請參閱 IAM 使用者指南 中的建立IAM政策。

透過身分IAM型政策，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要了解您可以在JSON政策中使用的所有元素，請參閱 IAM 使用者指南 中的IAMJSON政策元素參考。

Lightsail for Research 的身分型政策範例

若要檢視 Lightsail for Research 身分型政策的範例，請參閱 Amazon Lightsail for Research 的身分型政策範例。

Lightsail for Research 中的資源型政策

支援資源型政策：否

資源型政策是您連接至資源JSON的政策文件。資源型政策的範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策 。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主體可以包括帳戶、使用者、角色、聯合使用者或 AWS 服務。

若要啟用跨帳戶存取，您可以將另一個帳戶中的整個帳戶或IAM實體指定為資源型政策中的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同的 時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授予主體實體 （使用者或角色） 存取資源的許可。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱 IAM 使用者指南 中的跨帳戶資源存取權IAM。

Lightsail for Research 的政策動作

支援政策動作：是

管理員可以使用 AWS JSON政策來指定誰可以存取什麼。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

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

政策會使用動作來授予執行相關聯動作的許可。

若要查看 Lightsail for Research 動作的清單，請參閱服務授權參考 中的 Amazon Lightsail for Research 定義的動作。

Lightsail for Research 中的政策動作在動作之前使用下列字首：

```
lightsail
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

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

若要檢視 Lightsail for Research 身分型政策的範例，請參閱 Amazon Lightsail for Research 的身分型政策範例。

Lightsail for Research 的政策資源

支援政策資源：是

管理員可以使用 AWS JSON政策來指定誰可以存取什麼。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

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

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

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

若要查看 Lightsail for Research 資源類型及其 的清單ARNs，請參閱服務授權參考 中的 Amazon Lightsail for Research 定義的資源。若要了解您可以使用哪些動作指定每個資源ARN的 ，請參閱 Amazon Lightsail for Research 定義的動作。

若要檢視 Lightsail for Research 身分型政策的範例，請參閱 Amazon Lightsail for Research 的身分型政策範例。

Lightsail for Research 的政策條件金鑰

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON政策來指定誰可以存取什麼。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

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

您也可以在指定條件時使用預留位置變數。例如，只有在使用者使用其IAM使用者名稱加上標籤時，您才能授予IAM使用者存取資源的許可。如需詳細資訊，請參閱 IAM 使用者指南 中的IAM政策元素：變數和標籤。

AWS 支援全域條件索引鍵和服務特定條件索引鍵。若要查看所有 AWS 全域條件索引鍵，請參閱 IAM 使用者指南 中的AWS 全域條件內容索引鍵。

若要查看 Lightsail for Research 條件金鑰清單，請參閱服務授權參考 中的 Amazon Lightsail for Research 條件金鑰。若要了解您可以使用條件金鑰的動作和資源，請參閱 Amazon Lightsail for Research 定義的動作。

若要檢視 Lightsail for Research 身分型政策的範例，請參閱 Amazon Lightsail for Research 的身分型政策範例。

ACLs 在 Lightsail for Research 中

支援 ACLs：否

存取控制清單（ACLs）控制哪些主體（帳戶成員、使用者或角色）具有存取 資源的許可。ACLs 類似於資源型政策，雖然它們不使用JSON政策文件格式。

ABAC 搭配 Lightsail for Research

支援 ABAC（政策中的標籤）：部分

屬性型存取控制（ABAC）是一種根據屬性定義許可的授權策略。在 中 AWS，這些屬性稱為標籤。您可以將標籤連接至IAM實體（使用者或角色）和許多 AWS 資源。標記實體和資源是 的第一步 ABAC。然後，您可以設計ABAC政策，以便在主體的標籤與其嘗試存取的資源上的標籤相符時允許操作。

ABAC 有助於快速成長的環境，並有助於處理政策管理變得繁瑣的情況。

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

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 的詳細資訊ABAC，請參閱 使用者指南 中的什麼是 ABAC？。 IAM 若要檢視包含設定 之步驟的教學課程ABAC，請參閱 IAM 使用者指南 中的使用屬性型存取控制（ABAC）。

搭配 Lightsail for Research 使用臨時憑證

支援臨時憑證：是

當您使用臨時憑證登入時，有些 AWS 服務 無法使用。如需詳細資訊，包括 AWS 服務 使用哪些臨時憑證，請參閱 使用者指南 中的 AWS 服務 使用 IAM 。 IAM

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

您可以使用 AWS CLI 或 手動建立臨時憑證 AWS API。然後，您可以使用這些臨時憑證來存取 AWS. AWS recommends，讓您動態產生臨時憑證，而不是使用長期存取金鑰。如需詳細資訊，請參閱 中的臨時安全憑證IAM。

Lightsail for Research 的跨服務主體許可

支援轉送存取工作階段（FAS）：否

當您使用IAM使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，並結合請求向下游服務 AWS 服務 提出請求的 。FAS 只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出FAS請求的政策詳細資訊，請參閱轉送存取工作階段 。

Lightsail for Research 的服務角色

支援服務角色：否

服務角色是服務代表您執行動作時擔任IAM的角色。IAM 管理員可以從 內部建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 使用者指南 中的建立角色以將許可委派給 AWS 服務 。 IAM

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

Lightsail for Research 的服務連結角色

支援服務連結角色：否

服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的 中 AWS 帳戶 ，並由 服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

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

Amazon Lightsail for Research 的身分型政策範例

根據預設，使用者和角色沒有建立或修改 Lightsail for Research 資源的許可。他們也無法使用 AWS Management Console、 AWS Command Line Interface（AWS CLI）或 來執行任務 AWS API。若要授予使用者對所需資源執行動作的許可，IAM管理員可以建立IAM政策。然後，管理員可以將IAM政策新增至角色，使用者可以擔任角色。

若要了解如何使用這些範例政策文件來建立以IAM身分為基礎的JSON政策，請參閱 IAM 使用者指南 中的建立IAM政策。

如需 Lightsail for Research 定義之動作和資源類型的詳細資訊，包括ARNs每種資源類型的 格式，請參閱服務授權參考 中的 Amazon Lightsail for Research 的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 使用 Lightsail for Research 主控台
- 允許使用者檢視他們自己的許可

政策最佳實務

身分型政策會判斷是否有人可以在您的帳戶中建立、存取或刪除 Lightsail for Research 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用針對許多常見使用案例授予許可的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需詳細資訊，請參閱 IAM 使用者指南 中的 AWS 受管政策或 AWS 任務功能的受管政策。
- 套用最低權限許可 – 當您使用IAM政策設定許可時， 只會授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的詳細資訊，請參閱 IAM 使用者指南 中的政策和許可IAM。
- 使用IAM政策中的條件來進一步限制存取：您可以將條件新增至政策，以限制對動作和資源的存取。例如，您可以撰寫政策條件來指定所有請求都必須使用 傳送SSL。如果透過特定 使用服務動作，例如 AWS 服務，您也可以使用 條件來授予其存取權 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南 中的IAMJSON政策元素：條件。
- 使用 IAM Access Analyzer 驗證您的IAM政策以確保安全且功能許可 – IAM Access Analyzer 會驗證新的和現有的政策，讓政策遵循IAM政策語言 （JSON） 和IAM最佳實務。IAM Access Analyzer 提供超過 100 個政策檢查和可操作的建議，協助您撰寫安全且實用的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的IAM存取分析器政策驗證。
- 需要多重要素身分驗證 （MFA） – 如果您有需要IAM使用者或 根使用者的案例 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫API操作MFA時要求 ，請將MFA條件新增至您的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的設定 MFA受保護的API存取。

如需 中最佳實務的詳細資訊IAM，請參閱 IAM 使用者指南 中的安全最佳實務IAM。

使用 Lightsail for Research 主控台

若要存取 Amazon Lightsail for Research 主控台，您必須具有一組最低許可。這些許可必須允許您列出和檢視 中 Lightsail for Research 資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅對 AWS CLI 或 進行呼叫的使用者，您不需要允許最低主控台許可 AWS API。相反地，僅允許存取與其嘗試執行API的操作相符的動作。

為了確保使用者和角色仍然可以使用 Lightsail for Research 主控台，也請將 Lightsail for Research *ConsoleAccess*或*ReadOnly* AWS 受管政策連接至實體。如需詳細資訊，請參閱 IAM 使用者指南中的新增許可給使用者。

允許使用者檢視他們自己的許可

此範例示範如何建立政策，允許使用者檢視連接至其IAM使用者身分的內嵌和受管政策。此政策包含在主控台上完成此動作或使用 或 AWS CLI 以程式設計方式完成此動作的許可 AWS API。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
```

```
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

對 Amazon Lightsail for Research 身分和存取權進行故障診斷

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

主題

- 我無權在 Lightsail for Research 中執行動作
- 我想要允許 以外的人員 AWS 帳戶 存取我的 Lightsail for Research 資源

我無權在 Lightsail for Research 中執行動作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

當mateojacksonIAM使用者嘗試使用主控台檢視虛構*my-example-widget*資源的詳細資訊，但沒有虛構lightsail:*GetWidget*許可時，會發生下列錯誤範例。

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

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

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 以外的人員 AWS 帳戶 存取我的 Lightsail for Research 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。對於支援資源型政策或存取控制清單 （ACLs） 的服務，您可以使用這些政策來授予人員對資源的存取權。

如需進一步了解，請參閱以下內容：

- 若要了解 Lightsail for Research 是否支援這些功能，請參閱 Amazon Lightsail for Research 如何與搭配使用 IAM。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱 IAM 使用者指南 中的在您擁有 AWS 帳戶 的另一個資源中為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 使用者指南 中的提供存取權給第三方 AWS 帳戶 擁有。 IAM
- 若要了解如何透過身分聯合提供存取權，請參閱 IAM 使用者指南 中的為外部驗證的使用者提供存取權（身分聯合）。
- 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 中的跨帳戶資源存取IAM。

Amazon Lightsail for Research 的合規驗證

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

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

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

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

> **Note**
>
> 並非所有 AWS 服務 都HIPAA符合資格。如需詳細資訊，請參閱HIPAA合格服務參考 。

- AWS 合規資源 – 此工作手冊和指南集可能適用於您的產業和位置。
- AWS 客戶合規指南 – 透過合規的角度了解共同的責任模型。本指南摘要說明跨多個架構（包括國家標準和技術研究所（）NIST、支付卡產業安全標準委員會（PCI）和國際標準化組織（ISO））保護指南 AWS 服務 並映射至安全控制的最佳實務。
- AWS Config 開發人員指南中的使用規則評估資源 – AWS Config 服務會評估資源組態是否符合內部實務、產業準則和法規。

- AWS Security Hub – 這 AWS 服務 提供 內安全狀態的全面檢視 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty – 這會監控環境是否有可疑和惡意活動，藉此 AWS 服務 偵測 AWS 帳戶、工作負載、容器和資料的潛在威脅。 GuardDuty 可以透過滿足某些合規架構強制要求的入侵偵測需求，協助您解決各種合規要求DSS，例如 PCI 。
- AWS Audit Manager – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及遵守法規和產業標準的方式。

Amazon Lightsail for Research 中的復原能力

AWS 全域基礎設施是以 AWS 區域 和 可用區域為基礎建置。 AWS 區域 提供多個實體隔離和隔離的可用區域，這些區域與低延遲、高輸送量和高度冗餘聯網連接。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎設施 。

除了 AWS 全球基礎設施之外，Lightsail for Research 還提供數種功能，以協助支援您的資料復原能力和備份需求。如需詳細資訊，請參閱 使用 Lightsail 進行研究快照 Backup 虛擬電腦和磁碟 和 建立適用於研究人員的 Lightsail 虛擬電腦或磁碟快照。

Amazon Lightsail for Research 中的基礎設施安全性

作為受管服務，Amazon Lightsail for Research 受到 AWS 全球網路安全的保護。如需有關 AWS 安全服務以及如何 AWS 保護基礎設施的資訊，請參閱 AWS Cloud Security 。若要使用基礎設施安全的最佳實務來設計您的 AWS 環境，請參閱 Security Pillar AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 已發佈的API呼叫，透過網路存取 Lightsail for Research。使用者端必須支援下列專案：

- Transport Layer Security （ TLS ）。我們需要 TLS 1.2 和 建議 TLS 1.3。
- 具有完美前向秘密 （ PFS ） 的加密套件，例如 DHE（ Ephemeral Diffie-Hellman ） 或 ECDHE（ Elliptic Curve Ephemeral Diffie-Hellman ）。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，必須使用與IAM委託人相關聯的存取金鑰 ID 和秘密存取金鑰來簽署請求。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

Amazon Lightsail for Research 中的組態和漏洞分析

組態和 IT 控制是 AWS 和您，也就是我們的客戶之間的共同責任。如需詳細資訊，請參閱 AWS 共同責任模型 。

Amazon Lightsail for Research 的安全最佳實務

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

為了防止與您使用 Lightsail for Research 相關的潛在安全事件，請遵循下列最佳實務：

- 透過驗證 AWS Management Console 第一個 來存取 Lightsail for Research 主控台。請勿共用您的個人主機憑證。網際網路上的任何人都可以瀏覽到主控台，但除非他們擁有主控台的有效憑證，否則無法登入或開始工作階段。

Lightsail for Research 使用者指南的文件進版記錄

下表說明 Lightsail for Research 的文件版本。

變更	描述	日期
初始版本	Lightsail for Research 使用者指南的初始版本。	2023 年 2 月 28 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。