aws

使用者指南

Amazon Lightsail 進行研究

Amazon Lightsail 進行研究: 使用者指南

Table of Contents

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。這些虛擬電腦隨附有預先安裝的研究應用程式，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由公開可用的 API 提供支援。了解如何安裝和使用適用於亞馬遜的AWS CLI和 API。

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。

設置 Amazon Lightsail 進行研究

如果您是新 AWS 客戶，請先完成本頁面上列出的設定先決條件，然後再開始使用 Amazon Lightsail 進行研究。對於這些設定程序，您可以使用 AWS Identity and Access Management (IAM) 服務。如需 IAM 的完整資訊，請參閱《IAM 使用者指南》。

主題

註冊成為 AWS

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

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

建立 IAM 使用者

若要建立管理員使用者，請選擇下列其中一個選項。

選擇一種管理管理員的方式	到	By	您也可以
在 IAM Identity Center (建議)	使用短期憑證存取 AWS。 這與安全性最佳實務一致。有關最佳實務的資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。	請遵循 AWS IAM Identity Center 使用者指南的入門中的說明。	AWS IAM Identity Center 在《使用AWS Command Line Interface 者指南》中設定 AWS CLI 要使用的，以設定程式設計方式存取。
在 IAM 中 (不建議使用)	使用長期憑證存取 AWS。	請遵循 IAM 使用者指南中建立您的第一個 IAM 管理員使用者和使用者群組的說明。	請參閱 IAM 使用者指南中的管理 IAM 使用者的存取金鑰，設定程式設計存取。

教學課程：Lightsail for Research 虛擬電腦入門

使用此教學課程以開始使用 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 AWS 雲端中建立和管理的研究工作站。虛擬電腦是以具有 Ubuntu 作業系統的 Lightsail 執行個體為基礎。在您的虛擬電腦上，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。如需關於定價的詳細資訊，請參閱 Lightsail for Research 定價。

主題

步驟 1：完成先決條件

如果您是 AWS 的新客戶，請先完成設定先決條件，然後再開始使用 Amazon Lightsail for Research。如需更多詳細資訊，請參閱 設置 Amazon Lightsail 進行研究。

步驟2：建立虛擬電腦

可以使用 Lightsail for Research 主控台建立虛擬電腦，如以下程序所述。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，請參閱應用程式和硬體方案及建立虛擬電腦。

1. 登入 Lightsail for Research 主控台。
2. 在首頁上，選擇建立虛擬電腦。
3. 為您的虛擬電腦選取一個 AWS 區域。

   請選擇距離您實體位置最近的區域，以改善延遲。

4. 選擇一個應用程式，在 Lightsail API 中亦稱為藍圖。

   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. 選擇硬體方案，在 Lightsail API 中亦稱為的套裝組合。

   硬體方案提供不同數量的處理能力，包括 vCPU 核心、記憶體、儲存和每月資料傳輸。Lightsail for Research 提供虛擬電腦的標準方案和 GPU 方案。當您工作的運算需求很低時，請選擇標準方案。如果需求很高，例如運行機器學習模型或其他運算密集型工作時，請選擇 GPU 方案。

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

建立虛擬電腦並其處於運行中狀態後，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 主控台中提供的以瀏覽器為基礎的 NICE DCV 用戶端。使用 NICE DCV，您可以使用圖形使用者介面 (GUI) 與您的研究應用程式和虛擬電腦的作業系統互動。

- 使用 Secure Shell (SSH) 用戶端，例如 OpenSSH、PuTTY 或 Windows Subsystem for Linux 來存取虛擬電腦的命令行介面。使用 SSH 客戶端，您可以編輯指令碼和組態檔案。
- 使用 Secure Copy (SCP) 在您的本機電腦和虛擬電腦之間安全地傳輸檔案。使用 SCP，您可以在本機開始工作，然後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。

> **Note**
>
> 您還可以使用以瀏覽器為基礎的 NICE DCV 用戶端存取虛擬電腦的命令行介面和傳輸檔案。

您必須提供虛擬電腦的金鑰對，才能使用 SSH 連線至虛擬電腦，或使用 SCP 傳輸檔案。金鑰對是在連線至 Lightsail for Research 虛擬電腦時用來證明身分的一組安全憑證。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：
  - 啟動虛擬電腦的應用程式
  - 存取虛擬電腦的作業系統
- 使用 SCP 建立 SSH 連線或傳輸檔案：
  - 取得虛擬電腦的金鑰對
  - 使用 Secure Shell 連線至虛擬電腦
  - 使用 Secure Copy 將檔案傳輸至虛擬電腦

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 提供區塊層級儲存體磁碟區 (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 會自動在您的作業系統中將磁碟格式化並掛載。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：

- 建立磁碟
- 檢視磁碟
- 將磁碟連接至虛擬電腦
- 將磁碟與虛擬電腦分離
- 刪除磁碟

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

快照是資料的時間點副本。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：

- 建立快照
- 檢視快照
- 從快照建立虛擬電腦或磁碟
- 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。如需更多詳細資訊，請參閱 檢視虛擬電腦詳細資訊。如需關於定價的詳細資訊，請參閱 Lightsail for Research 定價。

> **Important**
>
> 刪除 Lightsail for Research 資源是永久性動作。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。

亞馬遜研究專用的開始教學課程

下列教學課程提供有關如何開始使用 Lightsail 進行研究專用之特定應用程式的其他資訊。

主題

- 開始使用 JupyterLab
- RStudio 入門

> **Note**
>
> 有關開始使用 Lightsail 進行研究和 RStudio 的深入教學課程已發佈至 AWS 公共部門部落格。如需詳細資訊，請參閱使用亞馬遜 Lightsail 進行研究：使用 RStudio 的教學課程。

開始使用 JupyterLab

在本教學中，我們將向您展示如何開始在 Amazon Lightsail 進行研究用的 JupyterLab 虛擬電腦管理和使用。

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應用程序
- 步驟 5：閱讀文 JupyterLab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

如果您還沒有，請使用該 JupyterLab 應用程序創建一台虛擬計算機。如需詳細資訊，請參閱 建立虛擬電腦。

在新的虛擬電腦啟動並執行之後，請繼續啟動本教學課程的 JupyterLab 應用程式一節。

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 建立磁碟 及 將磁碟連接至虛擬電腦。

> **Note**
>
> 當您使用主控台將磁碟連接到虛擬電腦時，Lightsail 研究報告會自動格式化並掛接磁碟。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 會將磁碟掛接至目/home/lightsail-user/*<disk-name>*錄。 *<disk-name>*是您給磁盤的名稱。

步驟 3：上傳並下載檔案

您可以將文件上傳到 JupyterLab 虛擬計算機，然後從中下載文件。若要這樣做，必須先完成以下步驟：

1. 從 Amazon Lightsail 獲得一 key pair。如需詳細資訊，請參閱 取得虛擬電腦的金鑰對。
2. 得到金鑰對後，您可以使用金鑰對並利用 Secure Copy (SCP) 公用程式來建立連線。SCP 讓您能使用命令提示字元或終端來上傳和下載文件。如需詳細資訊，請參閱 使用 Secure Copy 將檔案傳輸至虛擬電腦。
3. (選用) 您也可以使用金鑰對透過 SSH 連線至虛擬電腦。如需詳細資訊，請參閱 使用 Secure Shell 連線至虛擬電腦。

> **Note**
>
> 您還可以使用以瀏覽器為基礎的 NICE DCV 用戶端存取虛擬電腦的命令行介面和傳輸檔案。適用於研究的 Lightsail 主控台中提供了 NICE DCV。如需詳細資訊，請參閱 啟動虛擬電腦的應用程式 及 存取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附加到虛擬電腦時，Lightsail 進行研究會自動格式化並將該磁碟掛載到/home/lightsail-user/*<disk-name>*目錄中。 *<disk-name>*是您給磁盤的名稱。

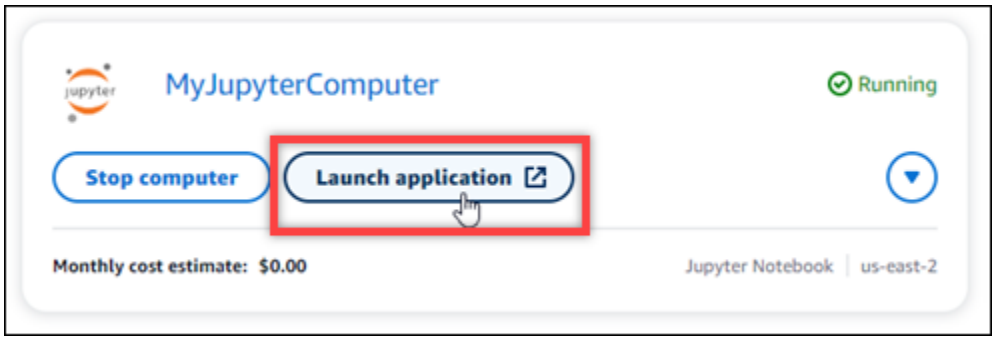
步驟 4：啟動 JupyterLab應用程序

請完成下列程序，在新的虛擬電腦上啟動 JupyterLab 應用程式。

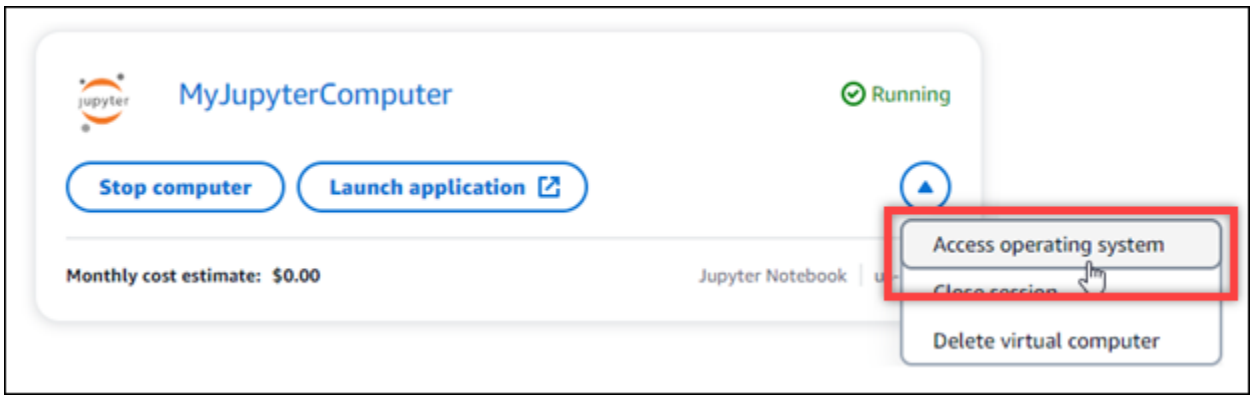
> **Important**
>
> 即使系統提示您這樣做，也 JupyterLab 請勿更新作業系統或應用程式。請選擇關閉或忽略這些提示的選項。此外，請勿修改任何位於 /home/lightsail-admin/ 目錄中的檔案。這些動作可能會導致虛擬電腦無法使用。

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，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。如果您最近沒有連線到虛擬電腦，則可能需要等待幾分鐘，Lightsail 進行研究報告準備工作階段。



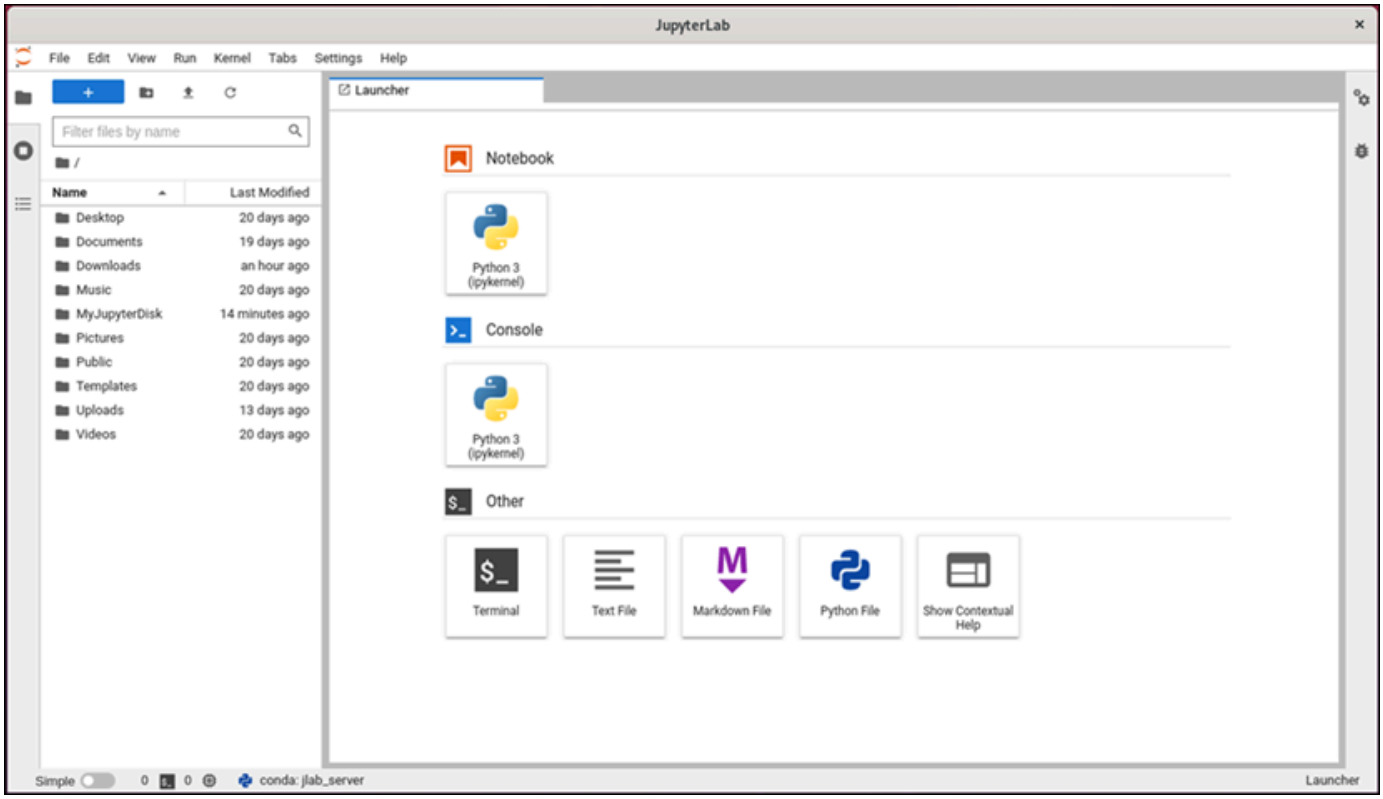
   b. 選擇電腦的下拉式選單，然後選擇存取作業系統以存取虛擬電腦的桌面。



Lightsail 研究報告版會執行一些指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。

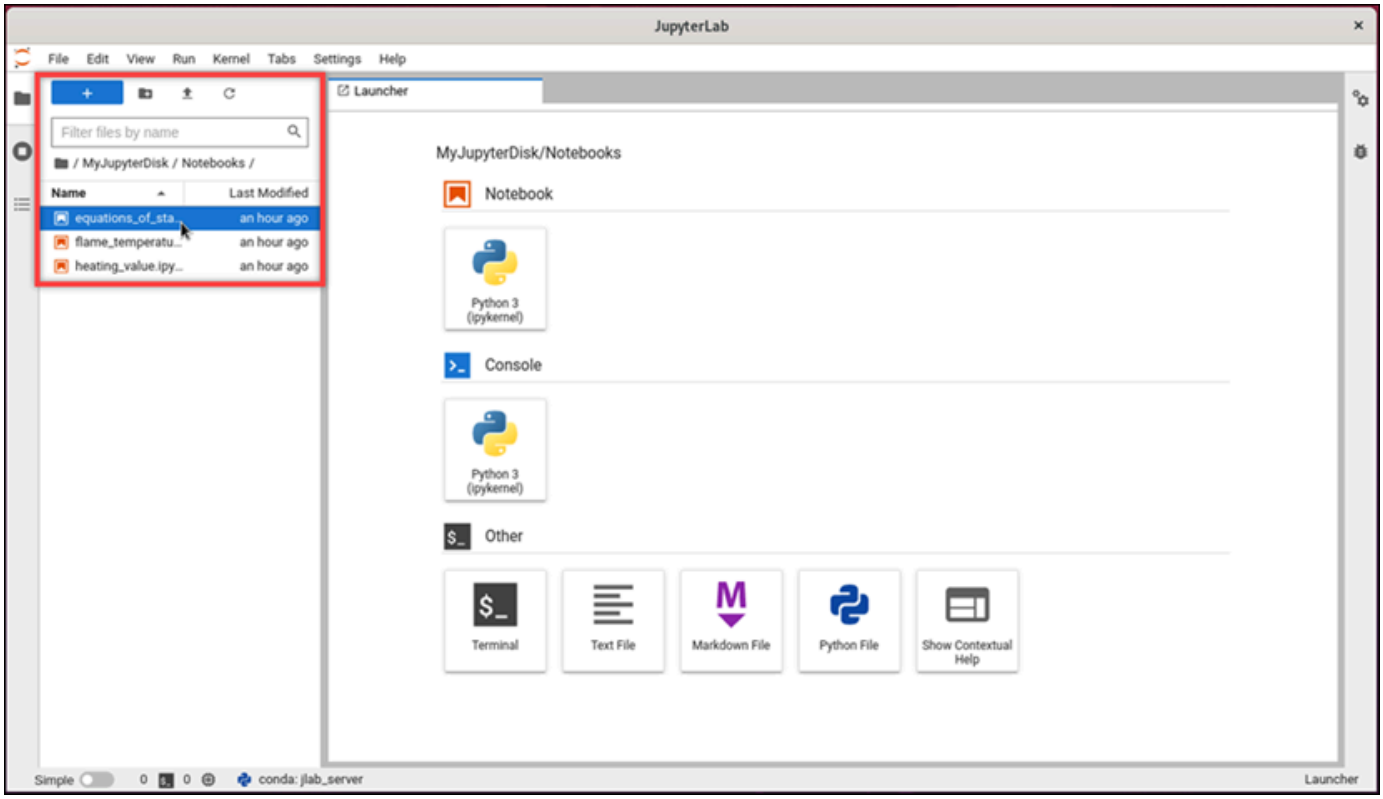
> **Note**
>
> 您的瀏覽器可能會提示您授權共用剪貼簿。允許此選項可讓您在本機電腦與虛擬電腦之間進行複製和貼上。
>
> Ubuntu 可能還會提示您進行初始設置。按照提示操作，直到完成設置且可以使用作業系統。

4. JupyterLab 應用程式隨即開啟。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。

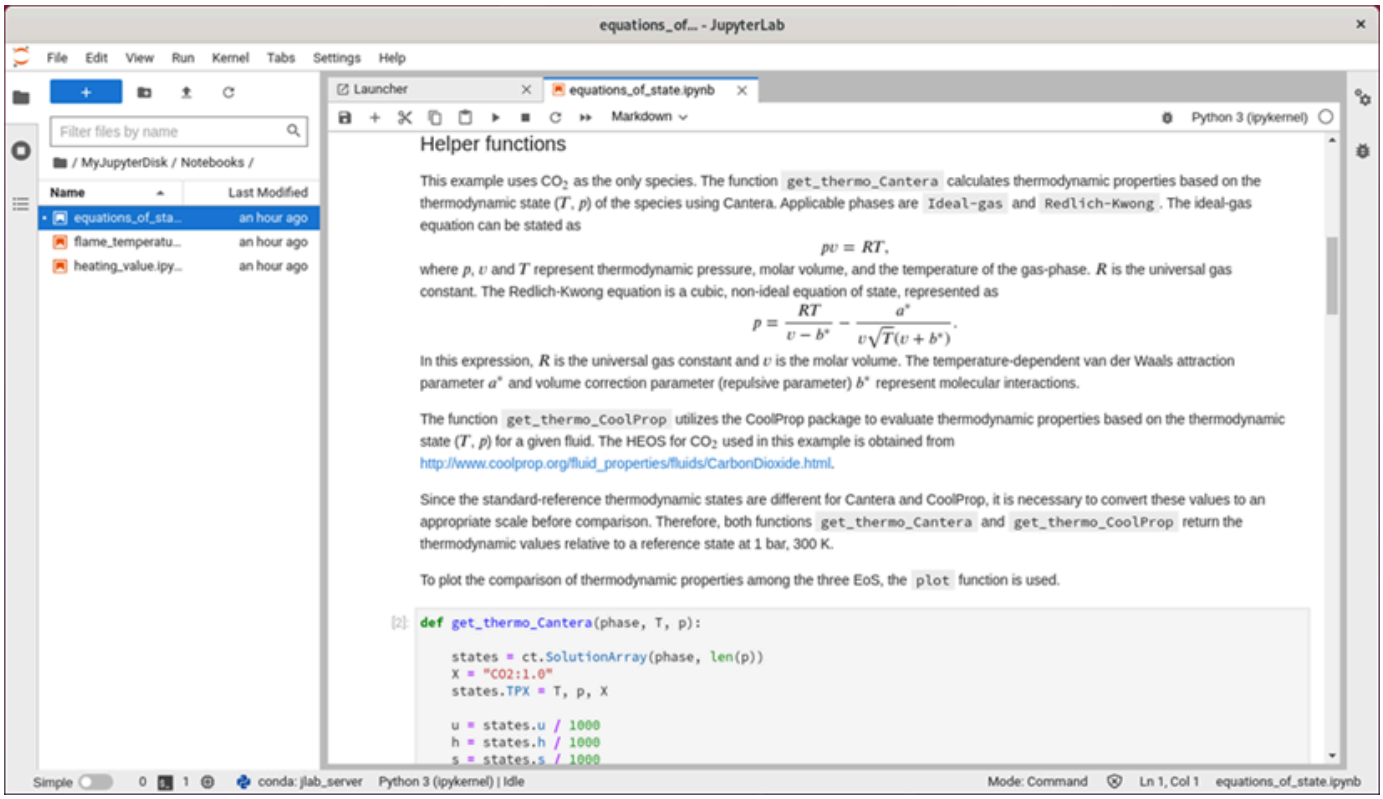


5. 若要在中開啟檔案 JupyterLab，請在「檔案瀏覽器」窗格中，選擇儲存專案檔案的目錄或資料夾。然後選擇要開啟的檔案。

   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，研究專用 Lightsail 會將磁碟掛接至目/home/lightsail-user/*<disk-name>*錄。 *<disk-name>*是您給磁盤的名稱。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：閱讀文 JupyterLab件 章節。

步驟 5：閱讀文 JupyterLab件

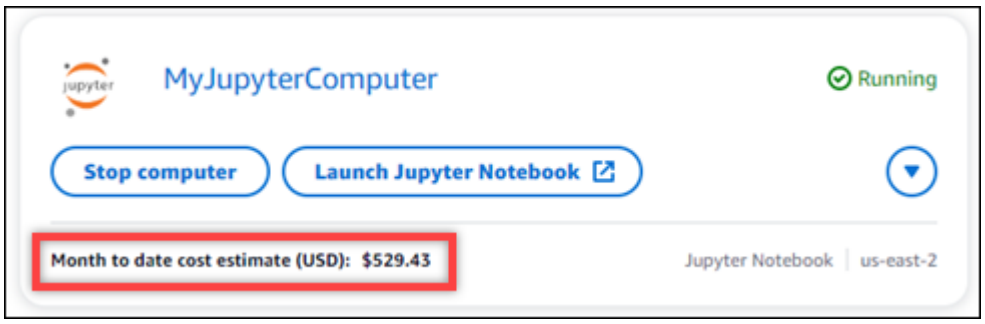
如果您不熟悉 JupyterLab，我們建議您閱讀他們的官方文檔。以下是可用的 JupyterLab 線上資源：

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

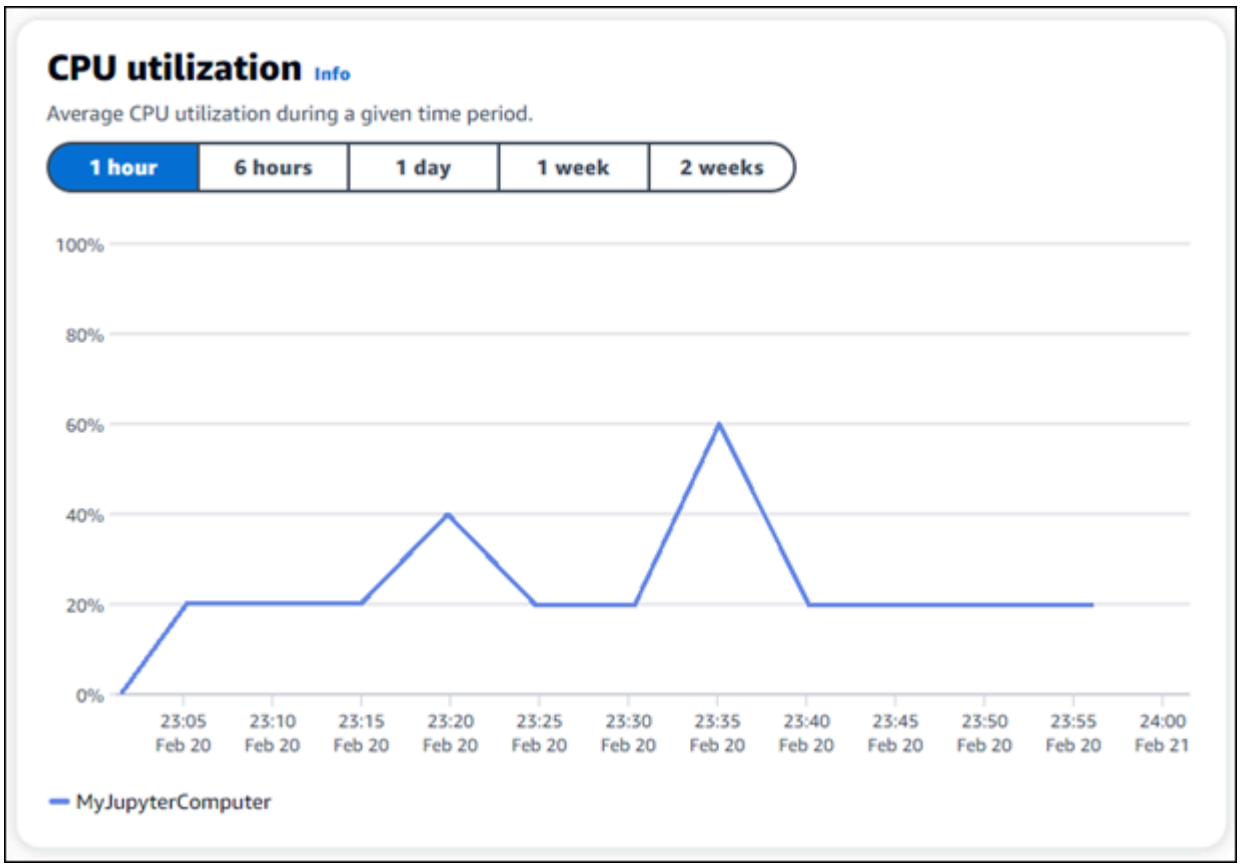
步驟 6：(選用) 監控用量和成本

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

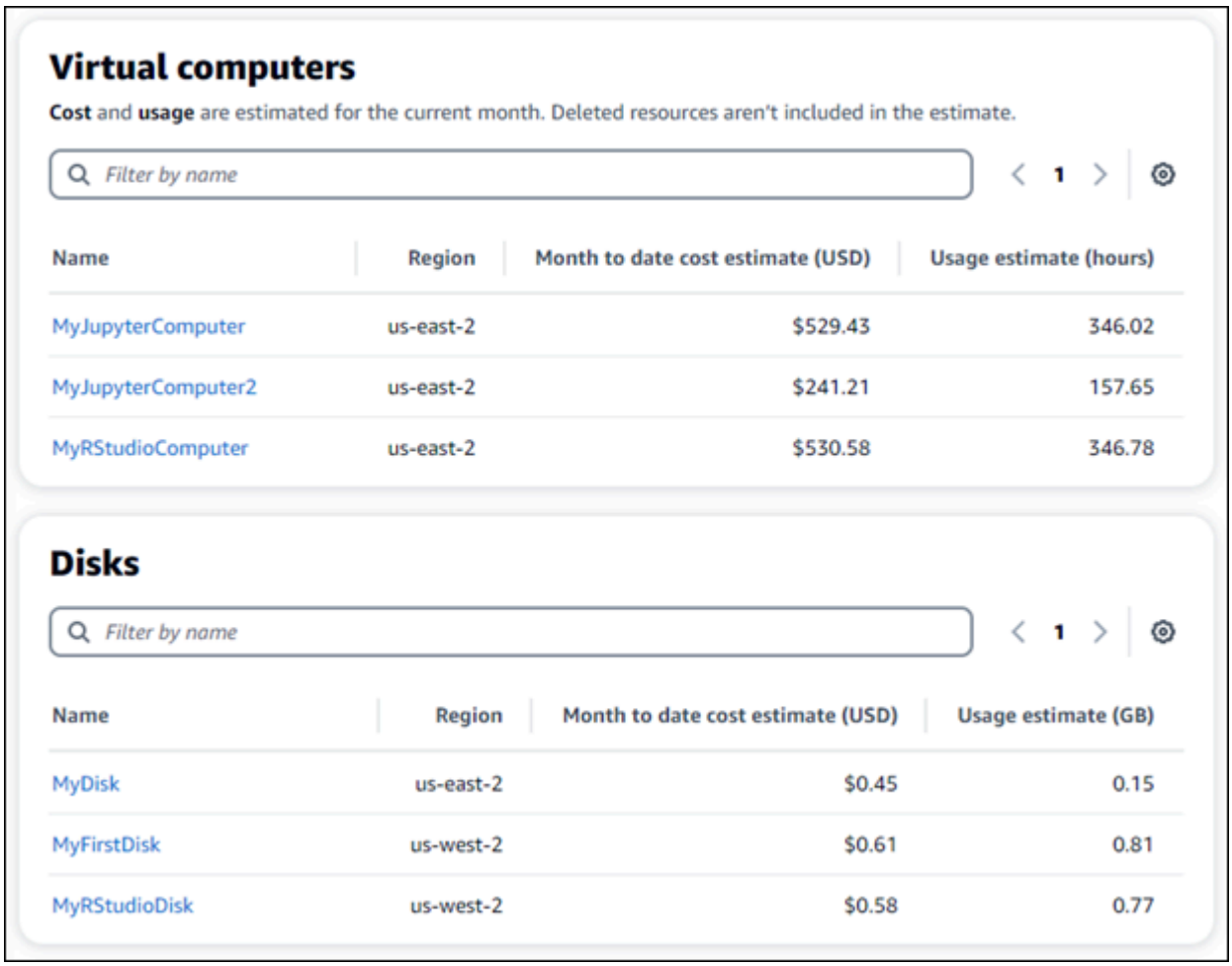
1. 在適用於研究的 Lightsail 主控台的導覽窗格中選擇虛擬電腦。每台運行中虛擬電腦的下方，會列出該虛擬電腦當月至今的成本估算。



2. 若要檢視虛擬電腦的 CPU 使用率，請選擇虛擬電腦的名稱，然後選擇儀表板分頁。



3. 若要檢視所有 Lightsail 用於研究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」。



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。您可以建立停止閒置虛擬電腦規則，則當在給定的時間段內達到指定的 CPU 使用率百分比時，即會停止運行中的電腦。例如，當某台電腦的 CPU 使用率在 30 分鐘的期間內等於或小於 5% 時，規則可以自動停止該電腦。這表示電腦可能處於閒置狀態，而 Lightsail 研究用會停止電腦，讓您不會因閒置資源而產生費用。

> **Important**
>
> 建立規則以停止閒置的虛擬電腦之前，建議您先利用幾天的時間監控虛擬電腦的 CPU 使用率。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。

如果您建立一個 CPU 使用率門檻值高於工作負載的規則，則該規則可能會不斷地停止您的虛擬電腦。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：

- 成本控制
- 建立規則
- 刪除規則

步驟 8：(選用) 建立快照

快照是資料的 point-in-time 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：

- 建立快照
- 檢視快照
- 從快照建立虛擬電腦或磁碟
- 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 檢視虛擬電腦詳細資訊。如需有關定價的詳細資訊，請參閱 Lightsail 適用於研究的定價。

> **Important**
>
> 刪除 Lightsail 進行研究資源是一項永久性的動作。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。

RStudio 入門

在本教學中，我們將向您展示如何開始在 Amazon Lightsail 進行研究專用的 RStudio 虛擬電腦管理和使用。

> **Note**
>
> 有關開始使用 Lightsail 進行研究和 RStudio 的深入教學課程已發佈至 AWS 公共部門部落格。如需詳細資訊，請參閱使用亞馬遜 Lightsail 進行研究：使用 RStudio 的教學課程。

主題

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，請先建立。如需詳細資訊，請參閱 建立虛擬電腦。

在新的虛擬電腦啟動並處於執行中狀態之後，請前往本教學課程的步驟 4。

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 建立磁碟 及 將磁碟連接至虛擬電腦。

> **Note**
>
> 當您使用主控台將磁碟連接到虛擬電腦時，Lightsail 研究報告會自動格式化並掛接磁碟。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，適用於研究的 Lightsail 會將磁碟掛接到`/home/lightsail-user/<disk-name>`目錄中，*<disk-name>*就是您為磁碟提供的名稱。

步驟 3：上傳並下載檔案

您可以將檔案上傳至您的 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 獲得一 key pair。如需詳細資訊，請參閱 取得虛擬電腦的金鑰對。
2. 得到金鑰對後，您可以使用金鑰對並利用 Secure Copy (SCP) 公用程式來建立連線。SCP 讓您能使用命令提示字元或終端來上傳和下載文件。如需詳細資訊，請參閱 使用 Secure Copy 將檔案傳輸至虛擬電腦。
3. (選用) 您也可以使用金鑰對透過 SSH 連線至虛擬電腦。如需詳細資訊，請參閱 使用 Secure Shell 連線至虛擬電腦。

> **Note**
>
> 您還可以使用以瀏覽器為基礎的 NICE DCV 用戶端存取虛擬電腦的命令行介面和傳輸檔案。適用於研究的 Lightsail 主控台中提供了 NICE DCV。如需詳細資訊，請參閱 啟動虛擬電腦的應用程式 及 存取虛擬電腦的作業系統。

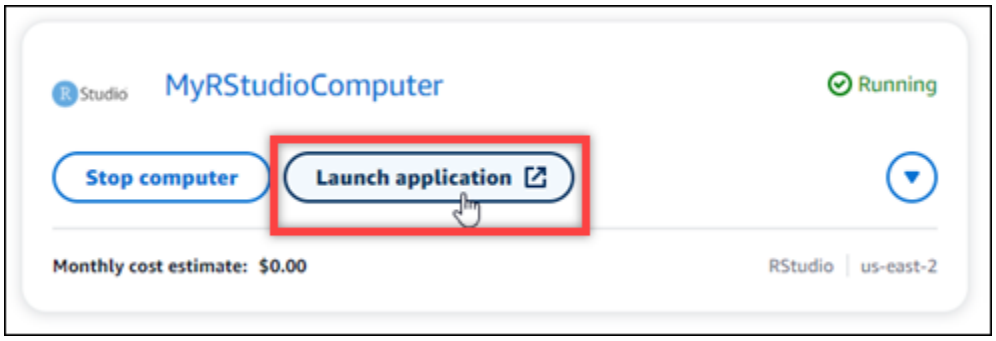
步驟 4：啟動 RStudio 應用程式

完成以下程序以啟動新虛擬電腦上的 RStudio 應用程式。

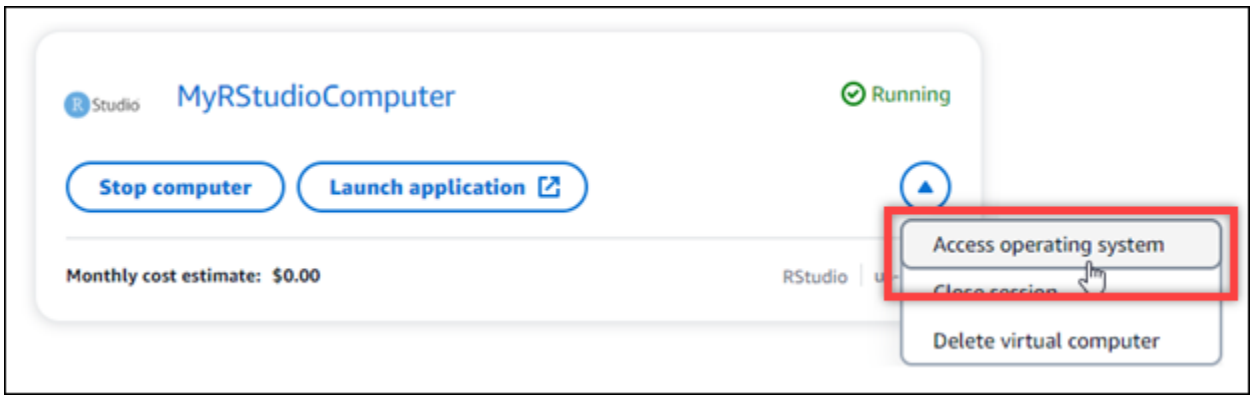
> **Important**
>
> 即使系統提示您更新作業系統或 RStudio 應用程式，也請不要更新。請選擇關閉或忽略這些提示的選項。此外，請勿修改任何位於 /home/lightsail-admin/ 目錄中的檔案。這些動作可能會導致虛擬電腦無法使用。

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，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。如果您最近沒有連線到虛擬電腦，則可能需要等待幾分鐘，Lightsail 進行研究報告準備工作階段。

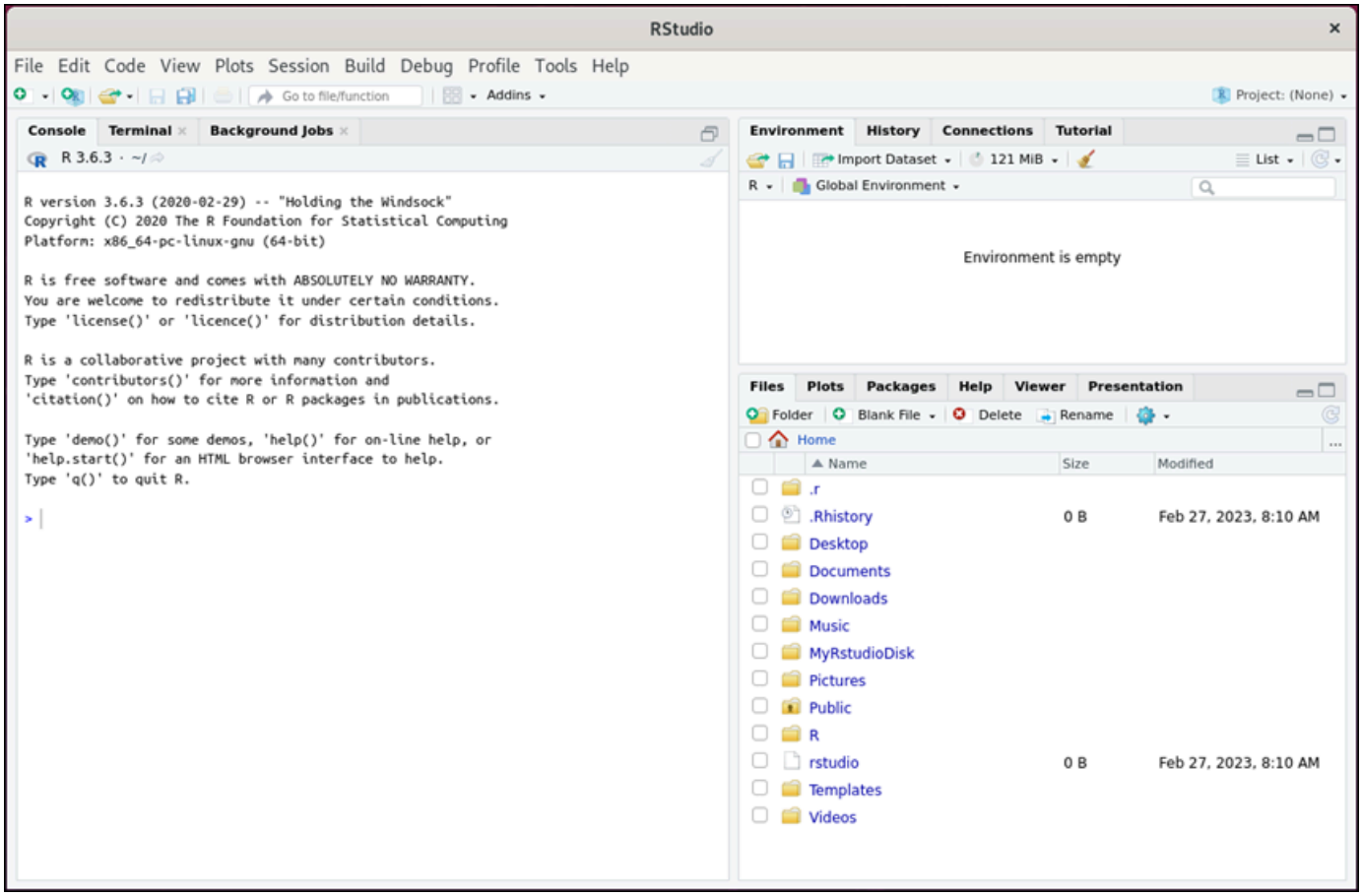
   b. 選擇電腦的下拉式選單，然後選擇存取作業系統以存取虛擬電腦的桌面。如果您要在作業系統上安裝其他應用程式，請執行此動作。



Lightsail 研究報告版會執行一些指令來啟動遠端顯示通訊協定連線。幾分鐘後，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 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。

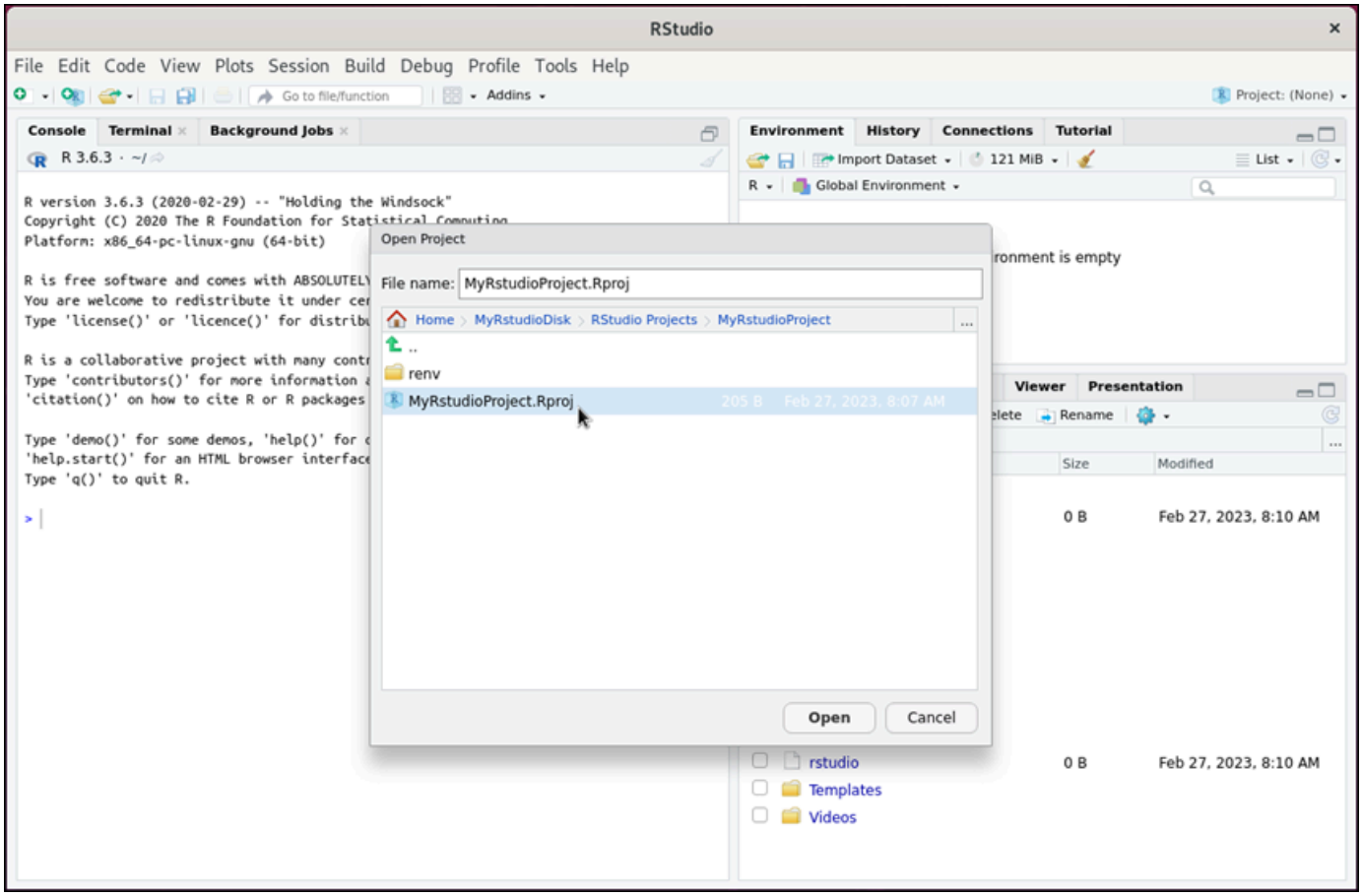
> **Note**
>
> 您的瀏覽器可能會提示您授權共用剪貼簿。允許此選項可讓您在本機電腦與虛擬電腦之間進行複製和貼上。
>
> Ubuntu 可能還會提示您進行初始設置。按照提示操作，直到完成設置且可以使用作業系統。

4. RStudio 應用程式開啟。

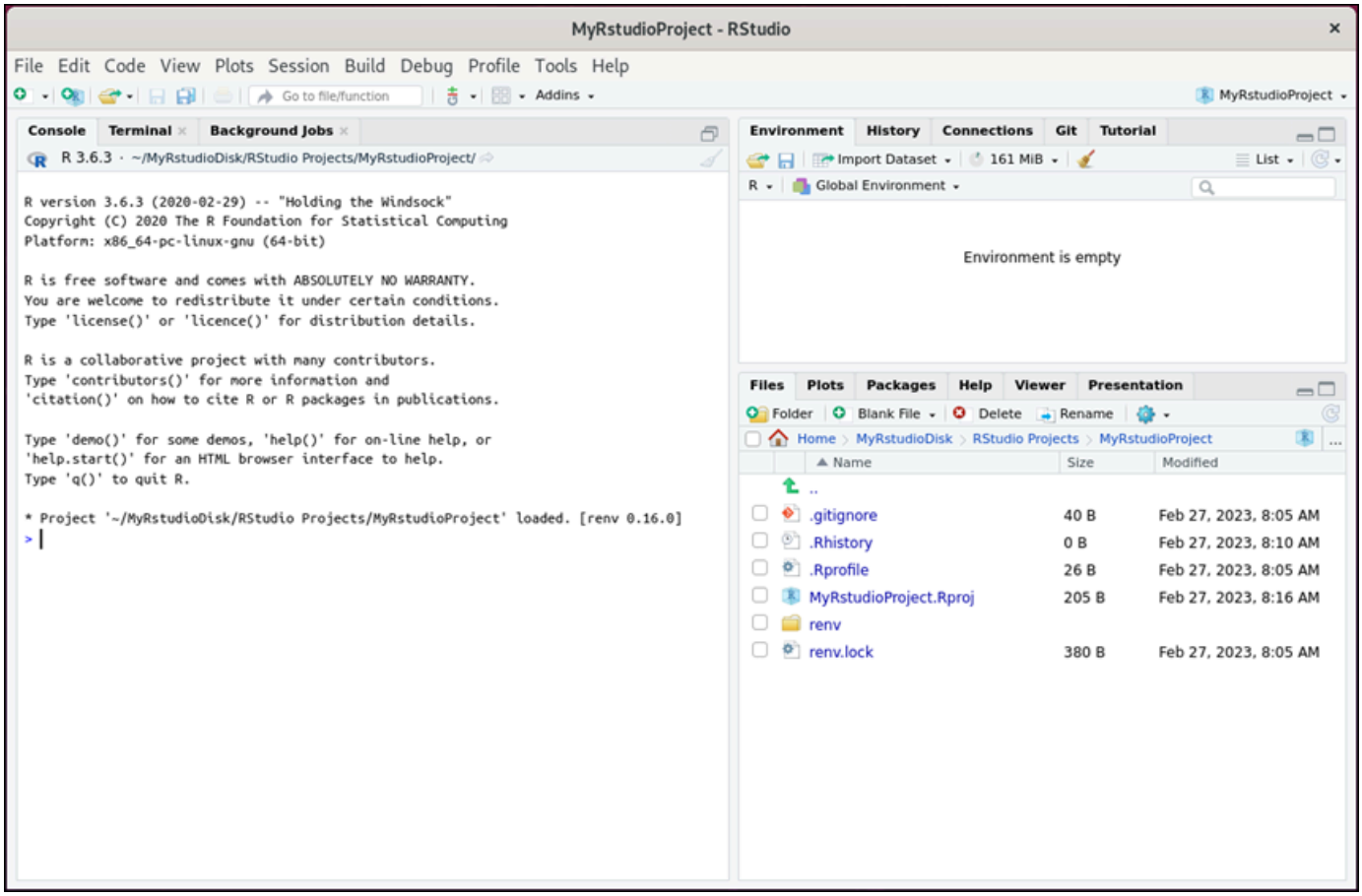


5. 若要在 RStudio 中開啟專案，選擇檔案選單，然後選擇開啟專案。瀏覽至存放專案檔案的目錄或資料夾。然後選擇要開啟的檔案。

   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，研究專用 Lightsail 會將磁碟掛接至目/home/lightsail-user/*<disk-name>*錄。 *<disk-name>*是您給磁盤的名稱。在以下範例中，MyRstudioDisk 目錄代表掛載的磁碟，Projects 子目錄內含我們的 RStudio 專案檔案。



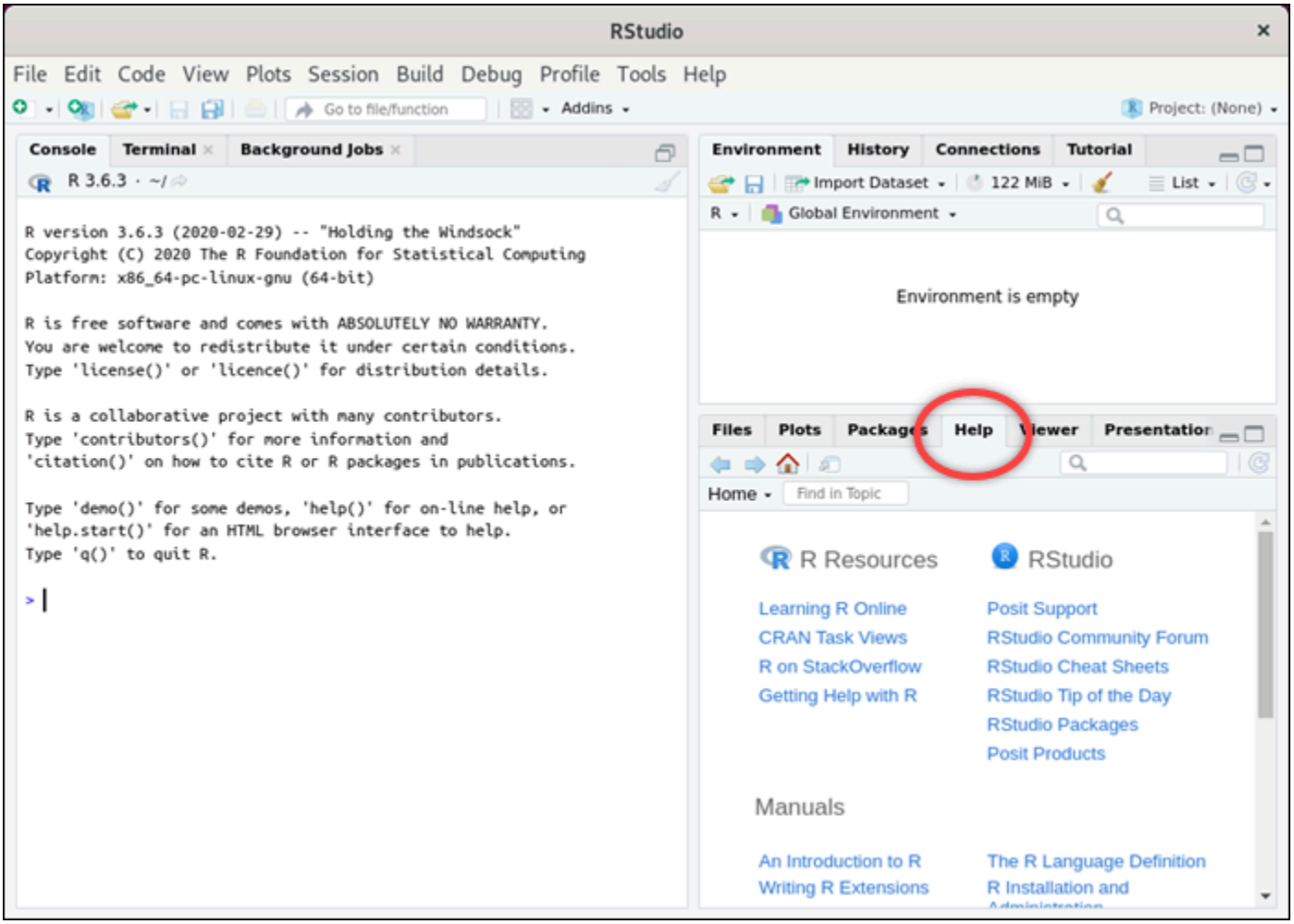
在以下範例中，我們開啟了 `MyRstudioProject.Rproj` 專案檔案。



若要取得有關如何開始使用 RStudio 的詳細資訊，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 應用程式隨附全面的套裝文件。若要開始學習 RStudio，我們建議您存取 RStudio 中的說明分頁，如以下範例所示。



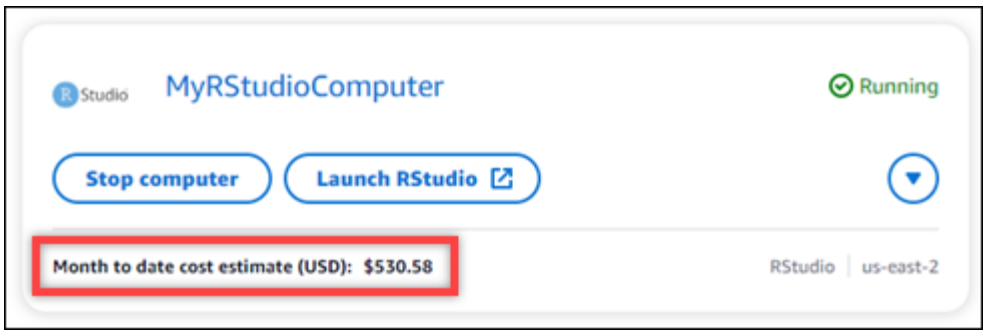
另外還可以取得以下 RStudio 線上資源：

- 線上學習 R
- R 在上 StackOverflow
- 取得 R 的說明
- Posit 支援
- RStudio 社群論壇
- RStudio 速查表
- RStudio 每日一帖 (推特)
- RStudio 套件

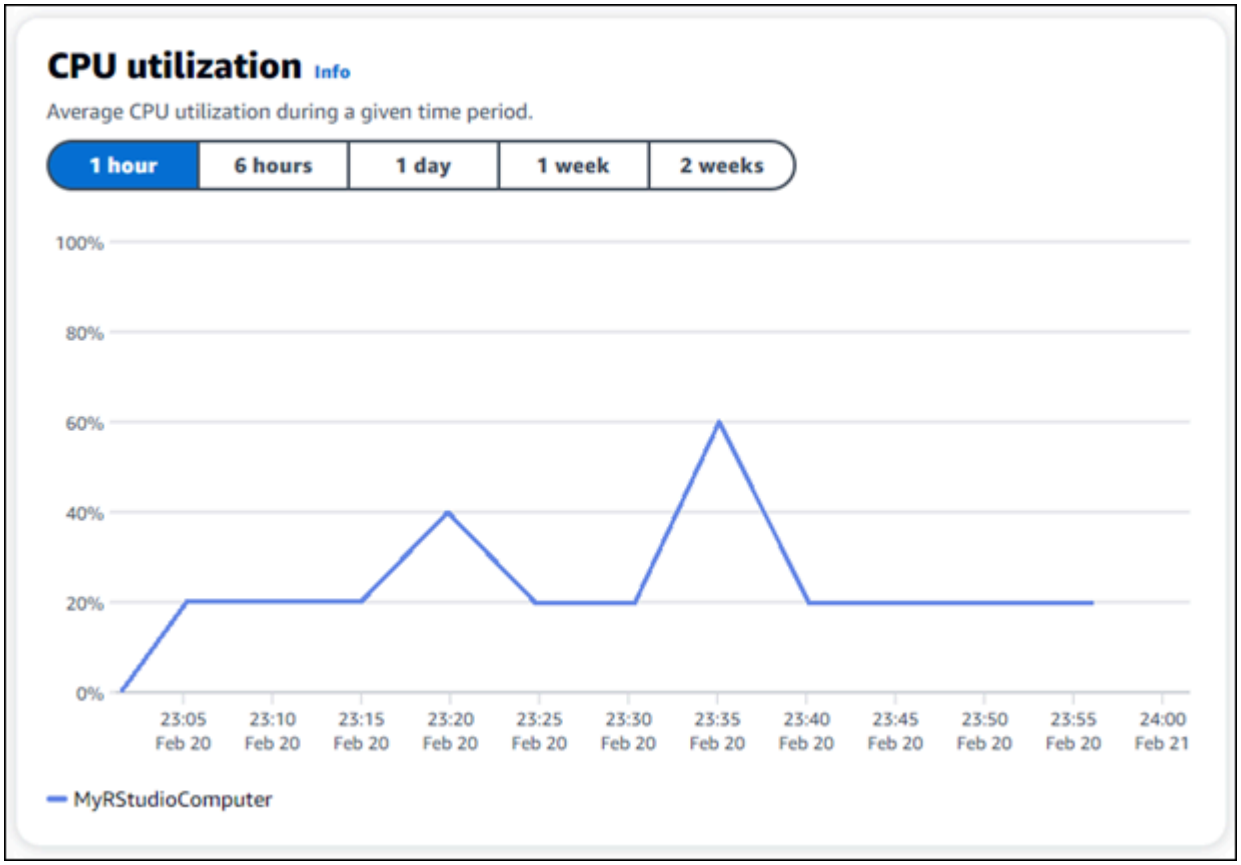
步驟 6：(選用) 監控用量和成本

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

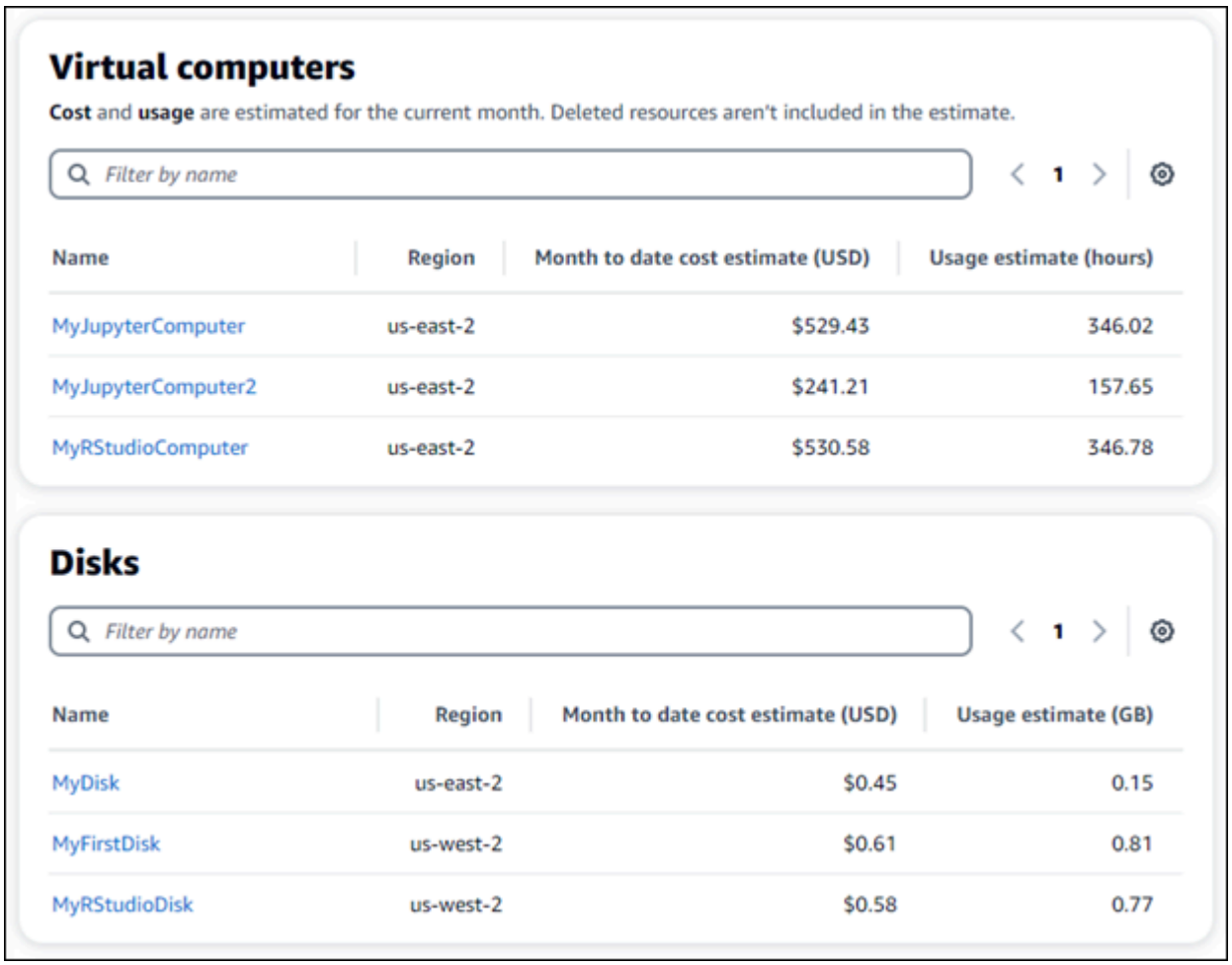
1. 在適用於研究的 Lightsail 主控台的導覽窗格中選擇虛擬電腦。每台運行中虛擬電腦的下方，會列出該虛擬電腦當月至今的成本估算。



2. 若要檢視虛擬電腦的 CPU 使用率，請選擇虛擬電腦的名稱，然後選擇儀表板分頁。



3. 若要檢視所有 Lightsail 用於研究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」。



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。您可以建立停止閒置虛擬電腦規則，則當在給定的時間段內達到指定的 CPU 使用率百分比時，即會停止運行中的電腦。例如，當某台電腦的 CPU 使用率在 30 分鐘的期間內等於或小於 5% 時，規則可以自動停止該電腦。這表示電腦可能處於閒置狀態，而 Lightsail 研究用會停止電腦，讓您不會因閒置資源而產生費用。

> **Important**
>
> 建立規則以停止閒置的虛擬電腦之前，建議您先利用幾天的時間監控虛擬電腦的 CPU 使用率。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。

如果您建立一個 CPU 使用率門檻值高於工作負載的規則，則該規則可能會不斷地停止您的虛擬電腦。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：

- 成本控制
- 建立規則
- 刪除規則

步驟 8：(選用) 建立快照

快照是資料的 point-in-time 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：

- 建立快照
- 檢視快照
- 從快照建立虛擬電腦或磁碟
- 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 檢視虛擬電腦詳細資訊。如需有關定價的詳細資訊，請參閱 Lightsail 適用於研究的定價。

> **Important**
>
> 刪除 Lightsail 進行研究資源是一項永久性的動作。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。

虛擬電腦

有了 AWS 雲端亞馬遜研究用 Lightsail，您可以在中建立虛擬電腦。

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**
>
> 自 2024 年 3 月 22 日起，研究用 Lightsail 虛擬電腦預設會強制執行 ImDSv2。

主題

應用程式和硬體方案

當您建立適用於研究的 Amazon Lightsail 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)。方案提供虛擬電腦的硬體，例如 vCPU 的數量、記憶體、儲存空間和每月資料傳輸限額。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 快照。

主題

應用程式

Amazon Lightsail 研究版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 進行研究用的虛擬電腦時，您可以從應用程式清單中選擇。所有 Lightsail 程式映像都使用 Ubuntu (Linux) 作業系統。

下列應用程式適 Lightsail 研究用：

- JupyterLab— JupyterLab 是用於筆記本電腦，代碼和數據的基於 Web 的集成開發環境（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 是針對 R (是一種用於統計運算與圖形的程式語言) 和 Python 的開放原始碼整合式開發環境 (IDE)。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 是社群推動的微軟編輯器 VS Code 的二進位發行版。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 為以 Debian 為基礎的開放原始碼 Linux 發行版。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

方案會提供硬體規格，並決定 Lightsail 用於研究虛擬電腦的價格。方案包括固定數量的記憶體 (RAM)、運算能力 (vCPU)、SSD 型儲存磁碟區 (磁碟) 空間，以及每月資料傳輸限額。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。適用於研究的 Lightsail 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 方案為一般用途 GPU 運算提供符合成本效益且高效能的平台。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

以下是適用於研究的 Lightsail 標準計劃的硬體規格。

方案名稱	vCPU	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 方案

以下是研究用 Lightsail 中可用的 GPU 計劃的硬體規格。

方案名稱	vCPU	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

建立虛擬電腦

完成下列步驟，以建立執行應用程式的 Lightsail 適用於研究的虛擬電腦。

1. 登入適用於研究的 Lightsail 主控台。
2. 在首頁上，選擇建立虛擬電腦。
3. AWS 區域 為您的實際位置附近的虛擬電腦選取一個。
4. 選擇應用程式和硬體方案。如需詳細資訊，請參閱 應用程式和硬體方案。
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：

   - 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。
6. 在摘要面板中，選擇建立虛擬電腦。

只需幾分鐘，您的 Lightsail 研究虛擬電腦就已準備就緒，您可以透過圖形化使用者介面 (GUI) 工作階段連線至該虛擬電腦。如需有關連線至 Lightsail 進行研究專用虛擬電腦的詳細資訊，請參閱啟動虛擬電腦的應用程式。

> **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 管理虛擬電腦的防火牆連接埠。

檢視虛擬電腦詳細資訊

完成下列步驟，即可在您的 Lightsail 用於研究帳戶中檢視虛擬電腦的清單及其詳細資料。

1. 登入適用於研究的 Lightsail 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
  - Stopping (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。
- 當月至今成本估算 – 虛擬電腦在此計費週期的預估成本 (以美元計)。
- 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 使用率可識別虛擬電腦應用程式所使用的處理能力。圖形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 AWS 成本。

啟動虛擬電腦的應用程式

完成下列步驟，以啟動 Lightsail 進行研究用虛擬電腦上執行的應用程式。

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. 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。

存取虛擬電腦的作業系統

請完成下列步驟，以存取 Lightsail 用於研究型虛擬電腦的作業系統。

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. 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。

管理虛擬電腦的防火牆連接埠

適用於研究的 Amazon Lightsail 防火牆可控制允許連接到虛擬電腦的流量。您可以新增虛擬電腦防火牆的規則，指定允許連接至虛擬電腦的通訊協定、連接埠和來源 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。每個虛擬電腦均具有兩個防火牆；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運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。
- 使用者資料報通訊協定 (UDP) 主要用於在用戶端與虛擬電腦上運行的應用程式之間建立低延遲和容忍遺失的連線。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。
- 網際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觸達其預定的目的地。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 Secure Shell (SSH)。

- 80 - 用於超文件傳送協定 (HTTP)。
- 443 – 用於超文本傳輸協定安全 (HTTPS)。
- 8443 – 用於超文本傳輸協定安全 (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 用戶端能夠連線至虛擬電腦，您可以設定一個防火牆規則，僅允許來自需要建立連線之電腦的 IP 地址透過連接埠 22 進行 TCP。在此情況下，您不會想要允許任何 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。如果已在執行個體的防火牆上設定此規則，則您可以將其刪除，以封鎖 SSH 用戶端連線至虛擬電腦。

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

開始之前，請先完成以下先決條件：

- 在 Lightsail 中建立虛擬電腦以供研究使用。如需詳細資訊，請參閱 建立虛擬電腦。
- 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。此程序會使用此`get-instance-port-states` AWS CLI 命令來取得特定 Lightsail 用於研究專用虛擬電腦的防火牆連接埠狀態、允許透過連接埠連線到虛

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

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，以及允許連線到虛擬電腦的 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。此程序會使用open-instance-public-ports AWS CLI 指令。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 AWS CLI 命令參考中的 open-instance-public-ports。

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*以建立虛擬電腦所在 AWS 地區的程式碼取代，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
```

回應會顯示新增的連接埠、通訊協定，以及允許連線到虛擬電腦的 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。此程序會使用`close-instance-public-ports` AWS CLI 指令。如需詳細資訊，請參閱 AWS CLI 命令參考中的 close-instance-public-ports。

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*以建立虛擬電腦所在 AWS 地區的程式碼取代，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
   ```

   回應會顯示已經關閉且不再允許連線至虛擬電腦]的連接埠、通訊協定以及 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。透過金鑰對，您可以使用各種 SSH 用戶端來建立連線，例如 OpenSSH、PuTTY 以及 Windows Subsystem for Linux。如需詳細資訊，請參閱 取得虛擬電腦的金鑰對。
- 使用 SSH 連線至虛擬電腦以使用命令行對進行管理。如需詳細資訊，請參閱 使用 Secure Copy 將檔案傳輸至虛擬電腦。
- 使用 SCP 連線至虛擬電腦以安全地傳輸檔案。如需詳細資訊，請參閱 使用 Secure Copy 將檔案傳輸至虛擬電腦。

取得虛擬電腦的金鑰對

key pair (包含公開金鑰和私密金鑰) 是一組安全登入資料，可在連線至 Amazon Lightsail 用於研究虛擬電腦時用來證明您的身分。公開金鑰會儲存在 Lightsail 進行研究用的每部虛擬電腦上，而且您會將私密金鑰保留在本機電腦上。私有金鑰讓您能與虛擬電腦安全地建立 Secure 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 執行個體或研究專用的 Lightsail 虛擬電腦時，系統會自動建立 Amazon Lightsail 預設 key pair (DKP)。DKP 是特定於您在其中建立執行個體或虛擬電腦的每個 AWS 區域。例如，適用於美國東部 (俄亥俄) 區域 (us-east-2) 的 Lightsail DKP 適用於您在美國東部 (俄亥俄州) Lightsail 和 Lightsail 進行研究所建立且設定為在建立 DKP 時使用的所有電腦。適用於研究的 Lightsail 會自動將 DKP 的公開金鑰儲存在您建立的虛擬電腦上。您可以透過對 Lightsail 服務進行 API 呼叫，隨時下載 DKP 的私密金鑰。

在本文件中，我們會向您展示如何取得虛擬電腦的 DKP。擁有金鑰對後，您可以使用各種 SSH 用戶端來建立連線，例如 OpenSSH、PuTTY 以及 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到虛擬電腦。

> **Note**
>
> 您還可以使用以瀏覽器為基礎的 NICE DCV 用戶端，建立與虛擬電腦的遠端顯示通訊協定連線。適用於研究的 Lightsail 主控台中提供了 NICE DCV。該 RDP 用戶端不需要您取得電腦的金鑰對。如需詳細資訊，請參閱 啟動虛擬電腦的應用程式 及 存取虛擬電腦的作業系統。

主題

完成先決條件

開始之前，請先完成以下先決條件：

- 在 Lightsail 中建立虛擬電腦以供研究使用。如需詳細資訊，請參閱 建立虛擬電腦。
- 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。這是一個輕量且靈活的命令行 JSON 處理器，在以下程序中用來從 AWS CLI的 JSON 輸出提取金鑰對詳細資訊。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。

取得虛擬電腦的金鑰對

完成下列其中一個程序，即可在 Lightsail 研究用中取得虛擬電腦的 Lightsail DKP。

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。此程序會使用`download-default-key-pair` AWS CLI 指令來取得區域的 Lightsail DKP。 AWS 如需詳細資訊，請參閱 AWS CLI 命令參考中的 download-default-key-pair。

1. 開啟命令提示視窗。
2. 輸入下列指令以取得特定 AWS 區域的 Lightsail DKP。此命令會將資訊儲存到 dkp-details.json 檔案中。在命令中，替換*region-code*為在其中創建虛擬計算機的 AWS 區域的代碼，例如us-east-2。

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

範例

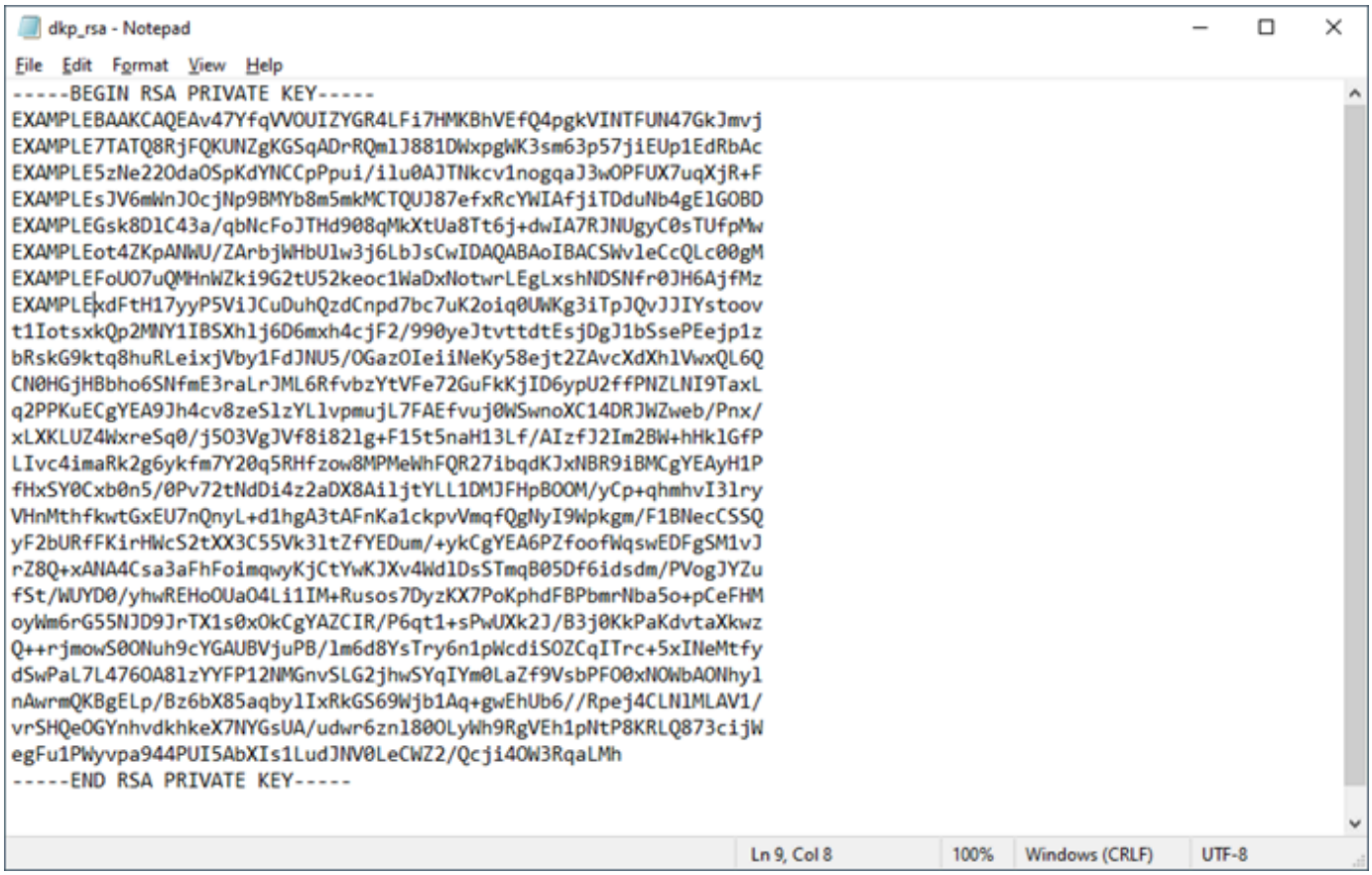
```
aws lightsail download-default-key-pair --region us-east-2 > dkp-details.json
```

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。



您現在擁有必要的私有金鑰，可以建立與虛擬電腦的 SSH 或 SCP 連線。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。此程序會使用download-default-key-pair AWS CLI 指令來取得區域的 Lightsail DKP。 AWS 如需詳細資訊，請參閱 AWS CLI 命令參考中的 download-default-key-pair。

1. 開啟「終端機」視窗。

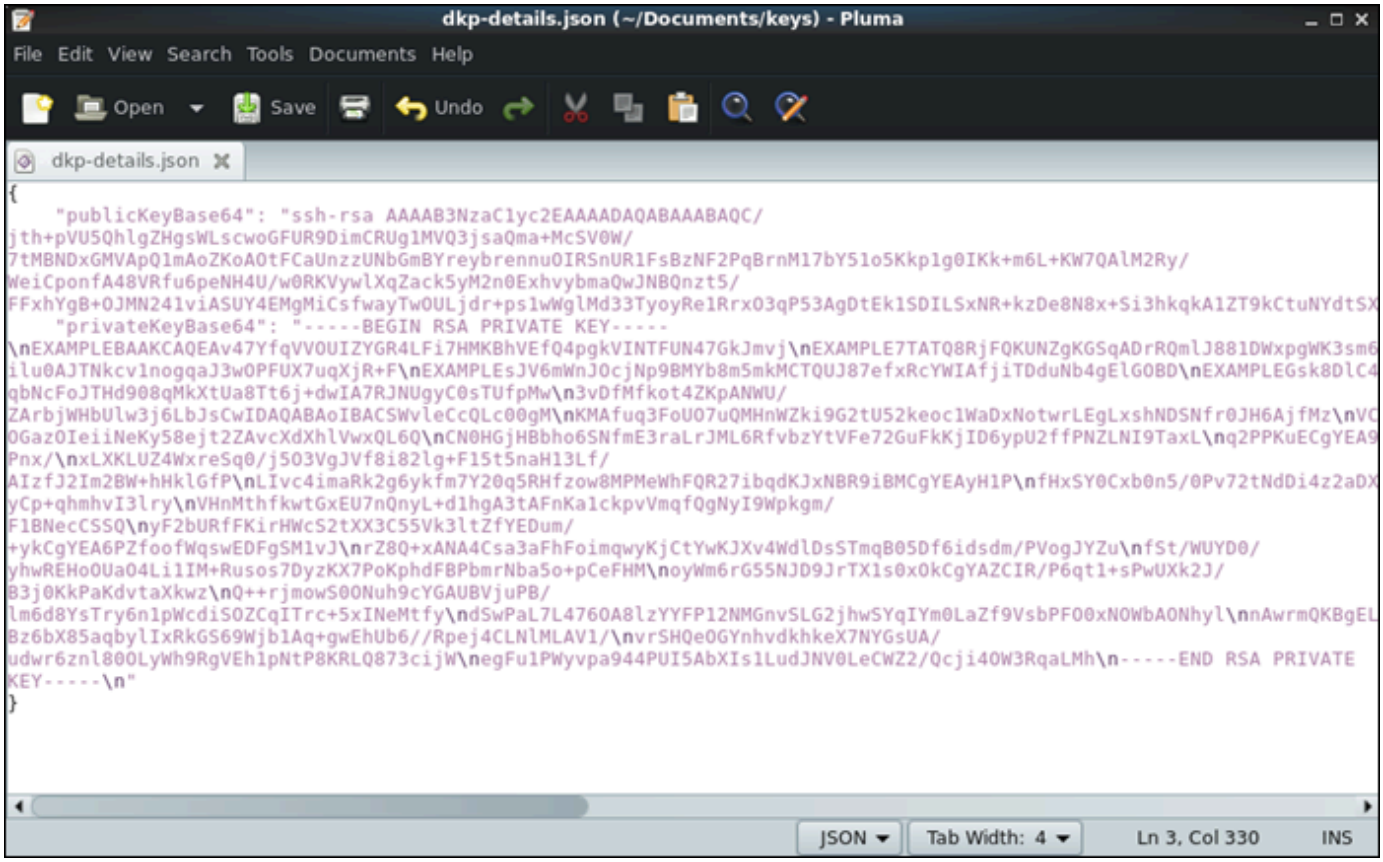
2. 輸入下列指令以取得特定 AWS 區域的 Lightsail DKP。此命令會將資訊儲存到 dkp-details.json 檔案中。在命令中，替換*region-code*為在其中創建虛擬計算機的 AWS 區域的代碼，例如us-east-2。

```
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
```

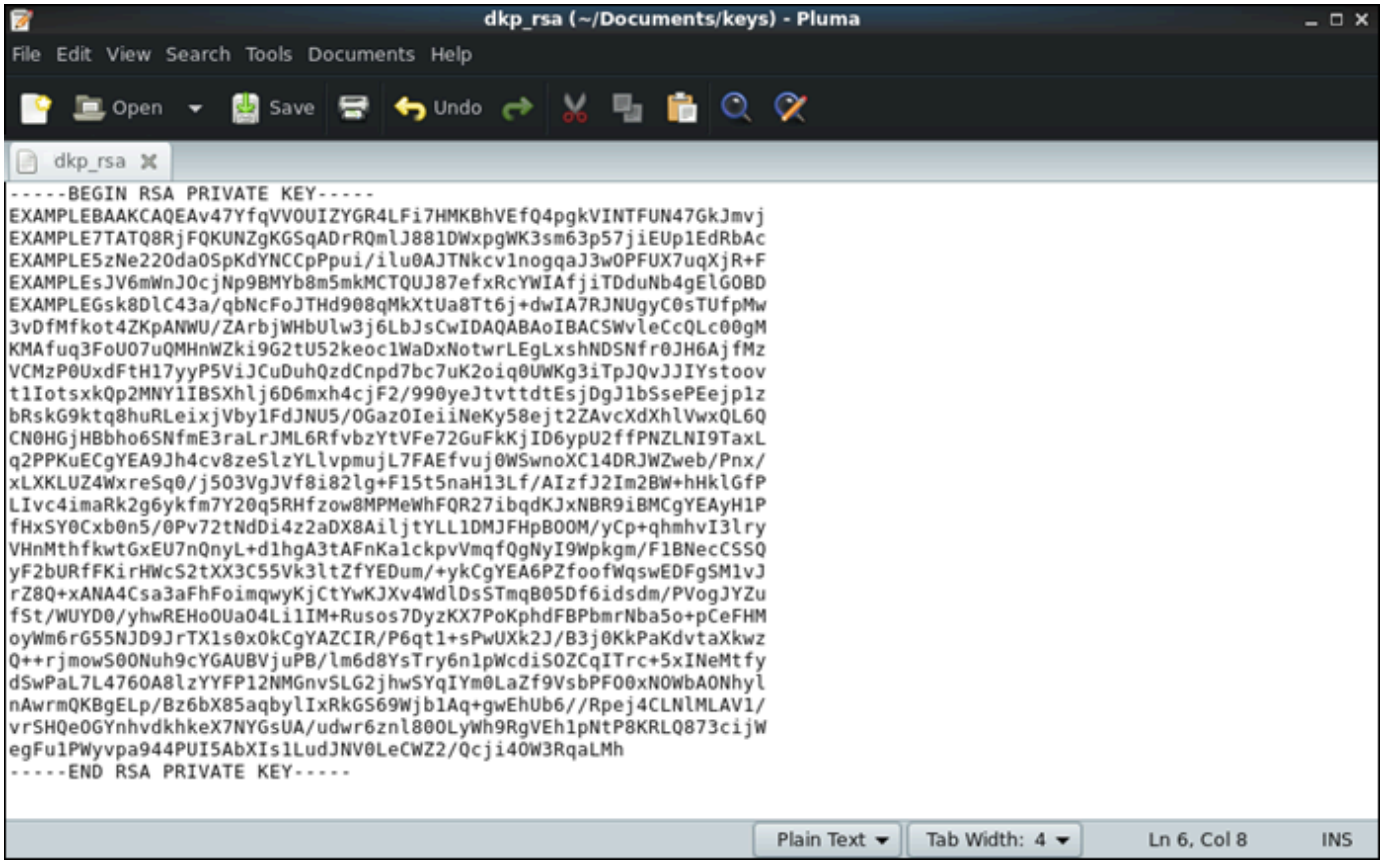
沒有對命令的回應。您可以開啟dkp-details.json檔案並查看 Lightsail DKP 資訊是否已儲存，以確認命令是否成功。dkp-details.json 檔案的內容應如以下範例所示：如果檔案為空白，表示命令失敗。



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
```

您現在擁有必要的私有金鑰，可以建立與虛擬電腦的 SSH 或 SCP 連線。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 SSH 連線至虛擬電腦以使用命令行進行管理。如需詳細資訊，請參閱 使用 Secure Shell 連線至虛擬電腦。
- 使用 SCP 連線至虛擬電腦以安全地傳輸檔案。如需詳細資訊，請參閱 使用 Secure Copy 將檔案傳輸至虛擬電腦。

使用 Secure Shell 連線至虛擬電腦

您可以使用安全殼層通訊協定 (SSH) 連線到 Amazon Lightsail 進行研究的虛擬電腦。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**
>
> 您還可以使用以瀏覽器為基礎的 NICE DCV 用戶端，建立與虛擬電腦的遠端顯示通訊協定連線。適用於研究的 Lightsail 主控台中提供了 NICE DCV。如需詳細資訊，請參閱 存取虛擬電腦的作業系統。

主題

完成先決條件

開始之前，請先完成以下先決條件：

- 在 Lightsail 中建立虛擬電腦以供研究使用。如需詳細資訊，請參閱 建立虛擬電腦。
- 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建立虛擬電腦的 AWS 區域。在此過程中，您將需要此信息。如需詳細資訊，請參閱 檢視虛擬電腦詳細資訊。
- 確認您想要連線的虛擬電腦上連接埠 22 已開啟。這是 SSH 使用的預設連接埠。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 管理虛擬電腦的防火牆連接埠。
- 取得虛擬電腦的預設 key pair (DKP)。如需詳細資訊，請參閱 取得虛擬電腦的金鑰對。

> **Tip**
>
> 如果您打算使用連線 AWS CloudShell 至虛擬電腦，請使用 Connect 至虛擬電腦 AWS CloudShell參閱下一節。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。這是一個輕量且靈活的命令行 JSON 處理器，在以下程序中用來提取金鑰對詳細資訊。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 SSH 連線至虛擬電腦

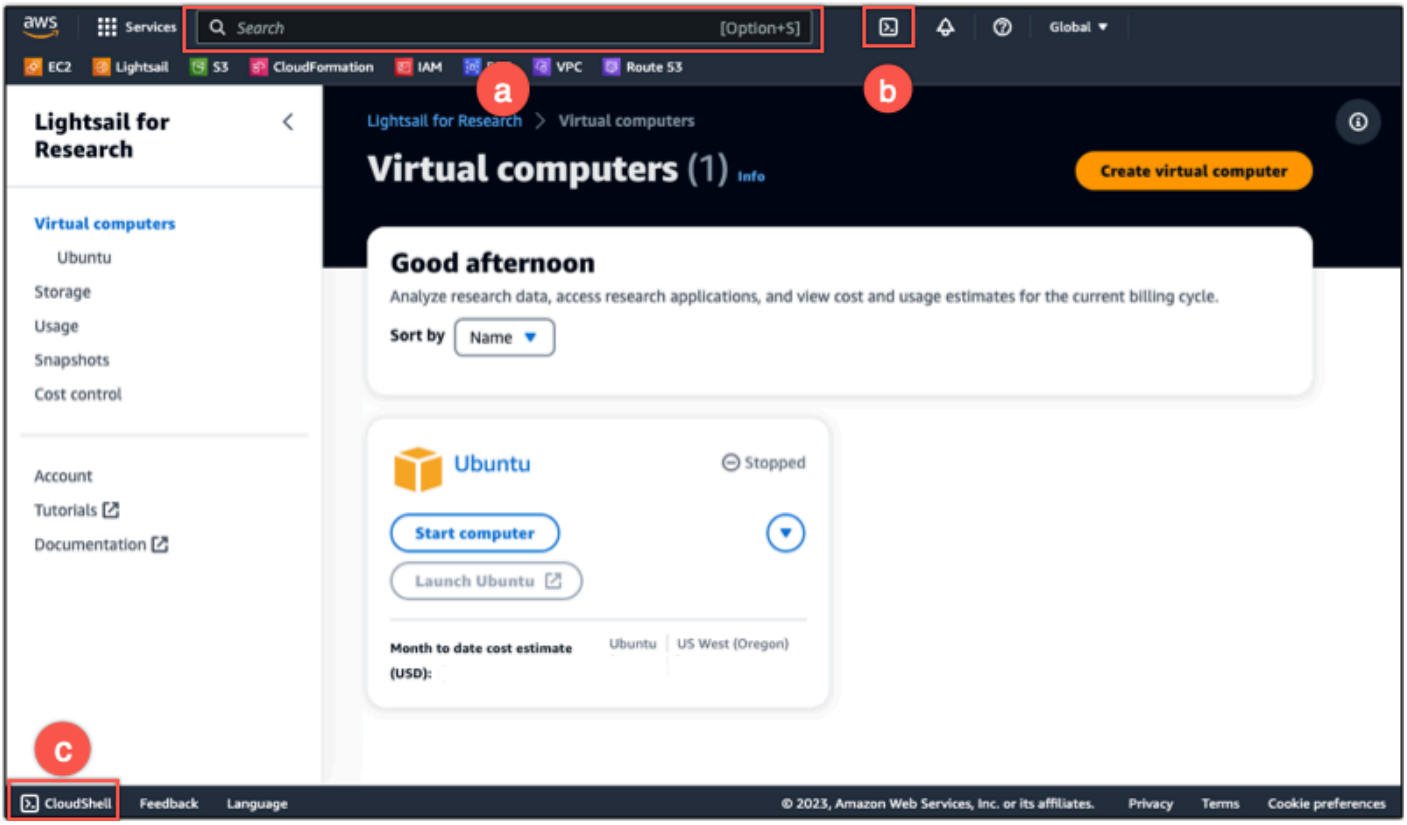
完成下列其中一個程序，即可在 Lightsail 進行研究用中建立與虛擬電腦的 SSH 連線。

使用 Connect 至虛擬電腦 AWS CloudShell

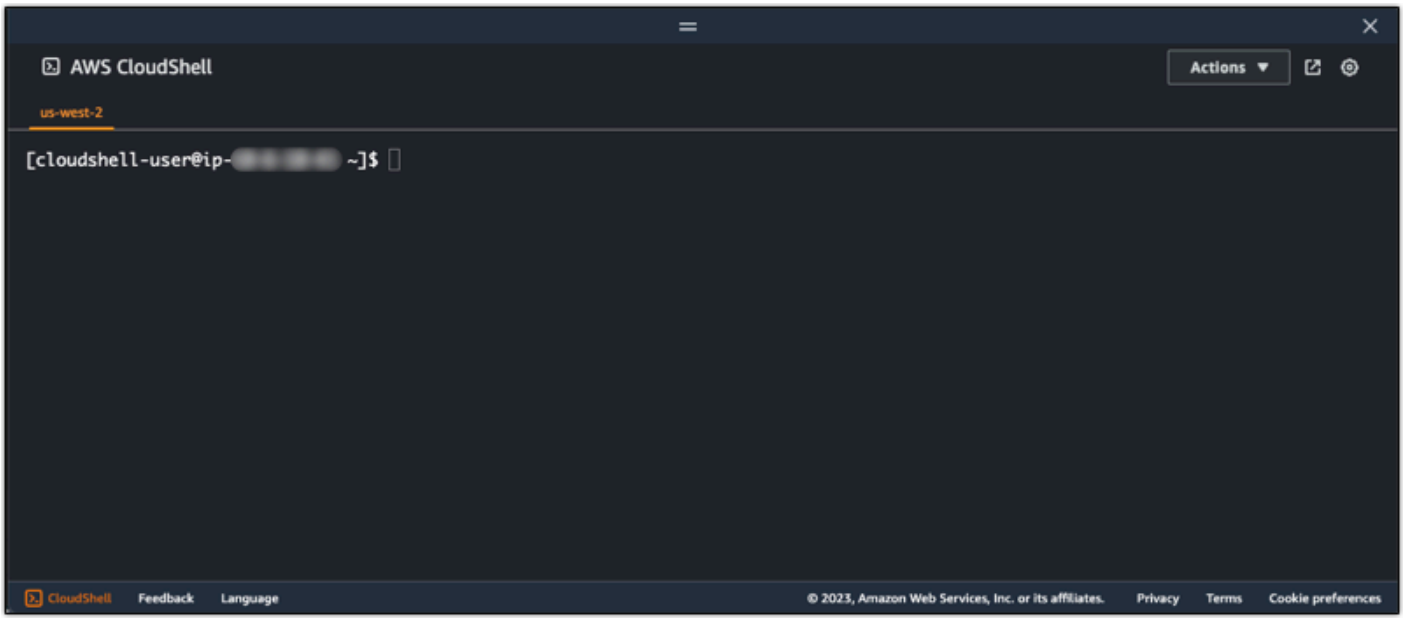
如果您偏好最低限度的設定來連線到虛擬電腦，則適用此程序。 AWS CloudShell 使用以瀏覽器為基礎的預先驗證殼層，您可以直接從. AWS Management Console您可以使用偏好的外殼程序來執行 AWS CLI 命令 PowerShell，例如 Bash 或 Z 殼層。無需下載或安裝命令列工具即可執行此操作。如需詳細資訊，請參閱《AWS CloudShell 使用者指南》中的 AWS CloudShell入門

> **Important**
>
> 在開始之前，請確定已取得要連線之虛擬電腦的 Lightsail 預設 key pair (DKP)。如需詳細資訊，請參閱 取得虛擬電腦的金鑰對。

1. 從 Lightsail 適用於研究的主控台中，選擇下列其中一個選項來啟動 CloudShell ：
   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. 在主控台左下方的 [主控台] 工具列CloudShell上選擇。



出現命令提示時，表示 Shell 已準備好開始互動。



2. 選擇預先安裝的外殼來使用。若要變更預設 shell，請在指令行提示下輸入下列其中一個程式名稱。Bash是啟動時執行的預設殼層 AWS CloudShell。

Bash

```
bash
```

如果切換至Bash，則指令提示下的符號會更新為$。

PowerShell

```
pwsh
```

如果切換至 PowerShell，則指令提示下的符號會更新為PS>。

Z shell

```
zsh
```

如果切換至Z shell，則指令提示下的符號會更新為%。

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

如需有關 CloudShell環境中預先安裝軟體的資訊，請參閱《AWS CloudShell 使用指南》中的AWS CloudShell 計算環境。

在 Windows 本機電腦上使用 SSH 連線至虛擬電腦

如果您的本機電腦使用 Windows 作業系統，則適用此程序。此程序會使用`get-instance` AWS CLI 命令來取得要連線之執行個體的使用者名稱和公用 IP 位址。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，請確定您已取得您嘗試連線之虛擬電腦的 Lightsail 預設 key pair (DKP)。如需詳細資訊，請參閱 取得虛擬電腦的金鑰對。該程序會將 Lightsail DKP 的私密金鑰輸出至下列其中一個指令中使用的`dkp_rsa`檔案。

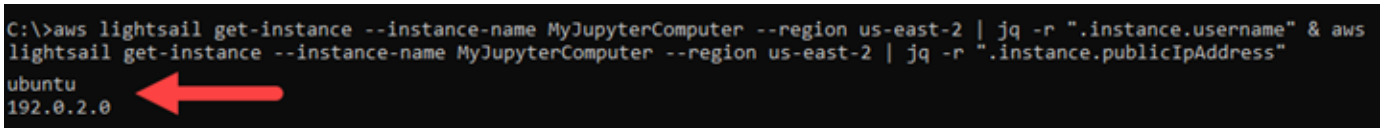
1. 開啟命令提示視窗。
2. 輸入以下命令以顯示虛擬電腦的公有 IP 地址和使用者名稱。在命令中，*`region-code`*以建立虛擬電腦的程式碼取代，例如`us-east-2`。 AWS 區域 將 *`computer-name`* 換成您想要連線的虛擬電腦的名稱。

```
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。



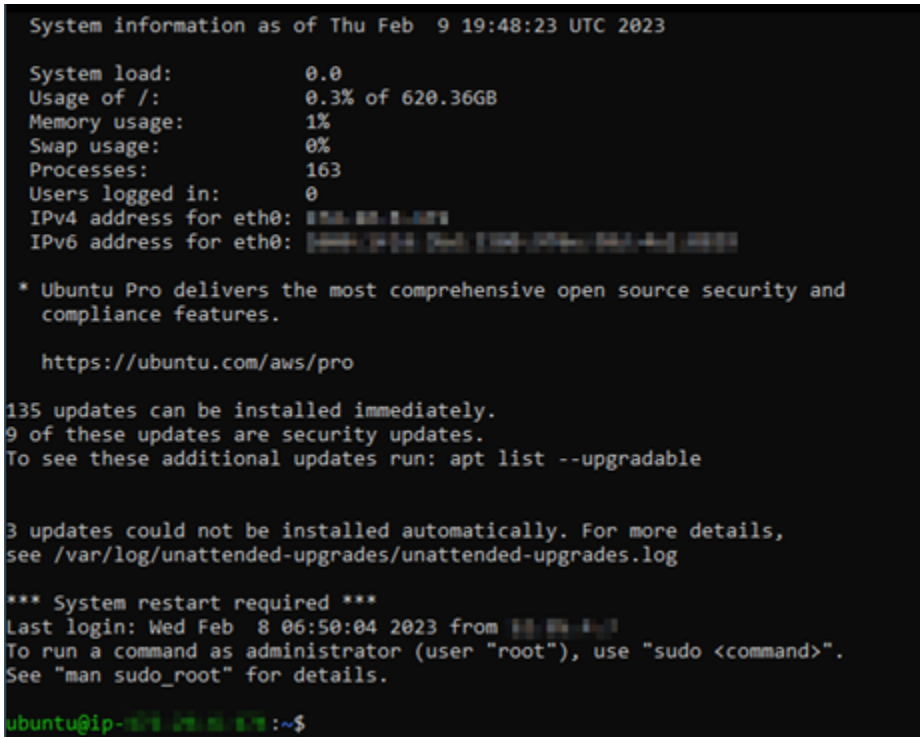
3. 輸入以下命令，建立與虛擬電腦的 SSH 連線。在命令中，將 *user-name* 換成登入的使用者名稱，並將 *public-ip-address* 換成虛擬電腦的公有 IP 地址。

```
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，該回應會顯示與 Lightsail 進行研究用的 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，請繼續下一節以進行其他後續步驟。

在 Linux、Unix 或 macOS 本機電腦上使用 SSH 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，則適用此程序。此程序會使用`get-instance` AWS CLI 命令來取得要連線之執行個體的使用者名稱和公用 IP 位址。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，請確定您已取得您嘗試連線之虛擬電腦的 Lightsail 預設 key pair (DKP)。如需詳細資訊，請參閱 取得虛擬電腦的金鑰對。該程序會將 Lightsail DKP 的私密金鑰輸出至下列其中一個指令中使用的`dkp_rsa`檔案。

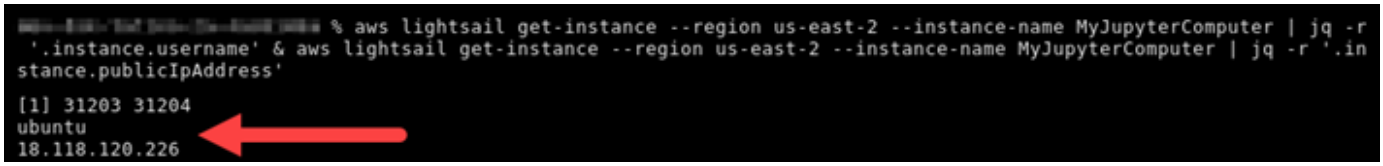
1. 開啟「終端機」視窗。
2. 輸入以下命令以顯示虛擬電腦的公有 IP 地址和使用者名稱。在命令中，替換*`region-code`*為在其中創建虛擬計算機的 AWS 區域的代碼，例如`us-east-2`。將 *`computer-name`* 換成您想要連線的虛擬電腦的名稱。

```
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。



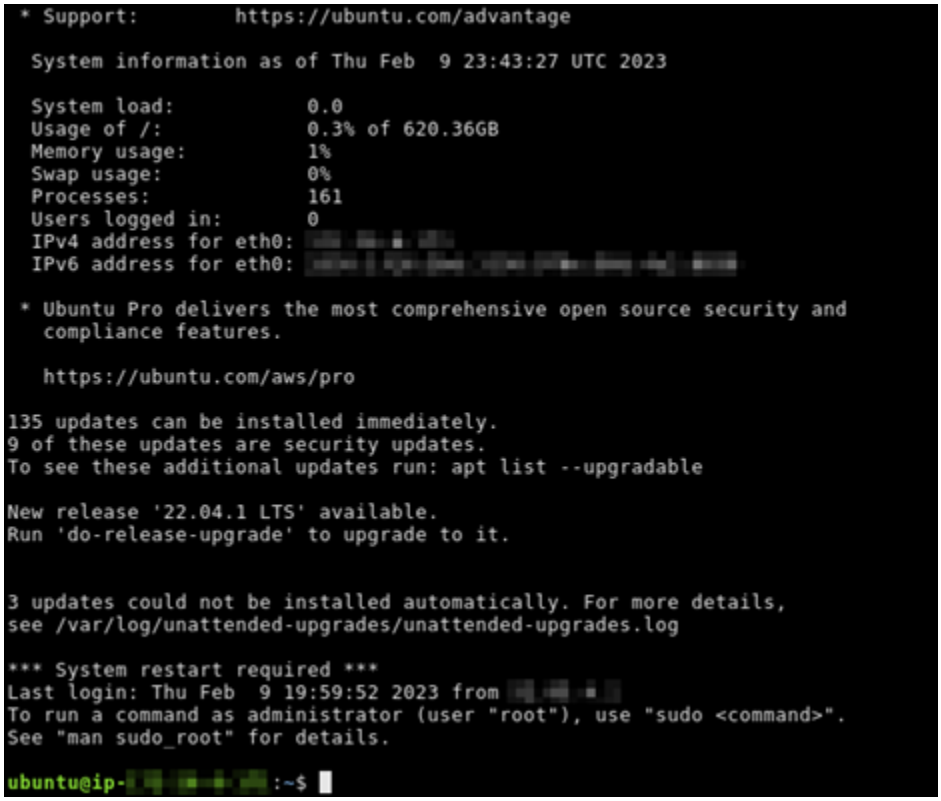
3. 輸入以下命令，建立與虛擬電腦的 SSH 連線。在命令中，將 *user-name* 換成登入的使用者名稱，並將 *public-ip-address* 換成虛擬電腦的公有 IP 地址。

```
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，該回應會顯示與 Lightsail 進行研究用的 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，請繼續下一節以進行其他後續步驟。

繼續後續步驟

成功建立與虛擬電腦的 SSH 連線後，可以完成以下其他後續步驟：

- 使用 SCP 連線至虛擬電腦以安全地傳輸檔案。如需詳細資訊，請參閱 使用 Secure Copy 將檔案傳輸至虛擬電腦。

使用 Secure Copy 將檔案傳輸至虛擬電腦

您可以使用安全複製 (SCP)，將檔案從本機電腦傳輸到用於研究的 Amazon Lightsail 中的虛擬電腦。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 用於研究主控台的瀏覽器式 NICE DCV 用戶端，建立與虛擬電腦的遠端顯示通訊協定連線。利用 NICE DCV 用戶端，您可以快速地傳輸個別檔案。如需詳細資訊，請參閱 存取虛擬電腦的作業系統。

主題

完成先決條件

開始之前，請先完成以下先決條件：

- 在 Lightsail 中建立虛擬電腦以供研究使用。如需詳細資訊，請參閱 建立虛擬電腦。
- 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。這是一個輕量且靈活的命令行 JSON 處理器，在以下程序中用來提取金鑰對詳細資訊。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 SSH 使用的預設連接埠。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 管理虛擬電腦的防火牆連接埠。
- 取得虛擬電腦的預設 key pair (DKP)。如需詳細資訊，請參閱 建立虛擬電腦。

使用 SCP 連線至虛擬電腦

完成下列其中一個程序，以使用 SCP 連線至 Lightsail 進行研究的虛擬電腦。

在 Windows 本機電腦上使用 SCP 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。此程序會使用`get-instance` AWS CLI 命令來取得要連線之執行個體的使用者名稱和公用 IP 位址。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，請確定您已取得您嘗試連線之虛擬電腦的 Lightsail 預設 key pair (DKP)。如需詳細資訊，請參閱 取得虛擬電腦的金鑰對。該程序會將 Lightsail DKP 的私密金鑰輸出至下列其中一個指令中使用的`dkp_rsa`檔案。

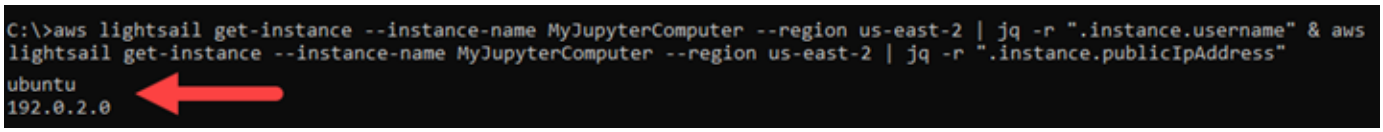
1. 開啟命令提示視窗。
2. 輸入以下命令以顯示虛擬電腦的公有 IP 地址和使用者名稱。在命令中，替換*`region-code`*為在其中創建虛擬計算機的 AWS 區域的代碼，例如`us-east-2`。將 *`computer-name`* 換成您想要連線的虛擬電腦的名稱。

   ```
   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. 輸入以下命令，建立與虛擬電腦的 SCP 連線並傳輸檔案。

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

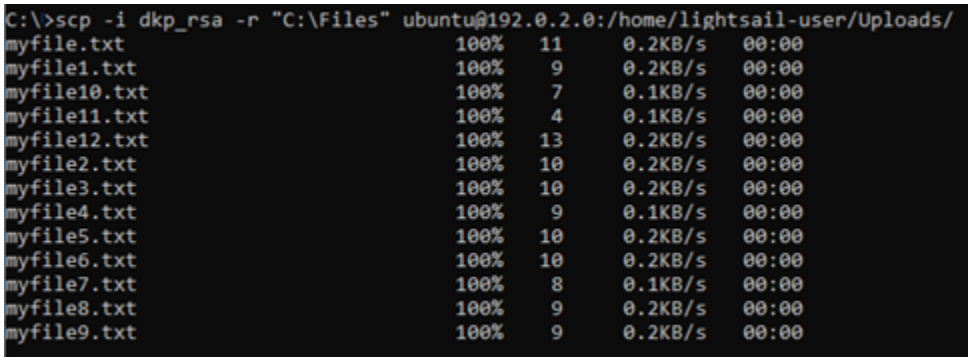
   在命令中：

- 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 Linux、Unix 或 macOS 本機電腦上使用 SCP 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。此程序會使用get-instance AWS CLI 命令來取得要連線之執行個體的使用者名稱和公用 IP 位址。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，請確定您已取得您嘗試連線之虛擬電腦的 Lightsail 預設 key pair (DKP)。如需詳細資訊，請參閱 取得虛擬電腦的金鑰對。該程序會將 Lightsail DKP 的私密金鑰輸出至下列其中一個指令中使用的dkp_rsa檔案。

1. 開啟「終端機」視窗。

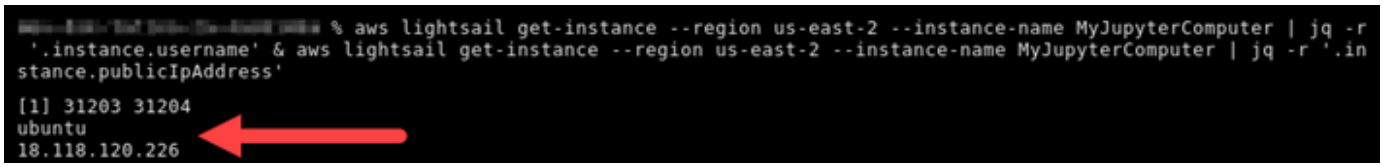
2. 輸入以下命令以顯示虛擬電腦的公有 IP 地址和使用者名稱。在命令中，替換*region-code*為在其中創建虛擬計算機的 AWS 區域的代碼，例如us-east-2。將 *computer-name* 換成您想要連線的虛擬電腦的名稱。

```
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. 輸入以下命令，建立與虛擬電腦的 SCP 連線並傳輸檔案。

```
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
```

刪除虛擬電腦

完成下列步驟，以在您不再需要 Lightsail 研究用虛擬電腦時刪除它。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。

儲存

Amazon Lightsail for Research 提供區塊層級儲存體磁碟區 (磁碟)，您可以連接至運行中的 Lightsail for Research 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 for Research 虛擬電腦上執行資料庫時，磁碟是建議的儲存選項。

磁碟的行為類似未格式化的外部區塊型儲存裝置，您可以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

建立磁碟

完成以下步驟，以建立一個 Lightsail for Research 虛擬電腦的磁碟。

1. 登入 Lightsail for Research 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：

   - 在您 Lightsail for Research 帳戶的每個 AWS 區域 內必須為唯一。
   - 含有 2–255 個字元。
   - 開頭和結尾為英數字元或數字。
5. 為您的磁碟選擇一個 AWS 區域。

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。

檢視磁碟

完成以下步驟，即可在檢視您 Lightsail for Research 帳戶中的磁碟及其詳細資訊。

1. 登入 Lightsail for Research 主控台。
2. 在導覽窗格中，選擇儲存。

   儲存頁面提供您 Lightsail for Research 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。
   - 連接至 – 磁碟所連接的 Lightsail 電腦。
   - 建立日期 – 建立磁碟的日期。

將磁碟連接至虛擬電腦

完成以下步驟，以在 Lightsail for Research 中將磁碟連接至虛擬電腦。您最多可以將 15 個磁碟連接至虛擬電腦。當您使用 Lightsail for Research 主控台將磁碟連接至虛擬電腦時，服務會自動將其格式化並掛載。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 會將磁碟掛載至 `/home/lightsail-user/<disk-name>` 目錄，而 `<disk-name>` 是您指定的磁碟機名稱。

> **Important**
>
> 虛擬電腦必須處於運行中狀態，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 Lightsail for Research 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)。

將磁碟與虛擬電腦分離

完成以下步驟，以將磁碟與電腦分離。

1. 登入 Lightsail for Research 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。如需更多詳細資訊，請參閱 將磁碟與虛擬電腦分離。

1. 登入 Lightsail for Research 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)。

快照

快照是資料的時間點副本。可建立 Amazon Lightsail for Research 虛擬電腦的快照，並將它們用作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)。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，因此建議您頻繁的建立快照，以免資料遺失永久遺失。

主題

建立快照

完成以下步驟，以建立 Lightsail for Research 虛擬電腦或磁碟的快照。

1. 登入 Lightsail for Research 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：
   - 在您 Lightsail for Research 帳戶的每個 AWS 區域 內必須為唯一。
   - 含有 2–255 個字元。
   - 開頭和結尾為英數字元或數字。
5. 選擇 Create snapshot (建立快照)。

檢視快照

完成以下步驟，檢視虛擬電腦和磁碟的快照。

1. 登入 Lightsail for Research 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

完成以下步驟，以從快照建立一個新的 Lightsail for Research 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 Lightsail for Research 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。

刪除快照

完成以下步驟以刪除快照。

1. 登入 Lightsail for Research 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。

Amazon Lightsail 研究用的成本和用量估算

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。估算會在資源建立後 15 分鐘內顯示在 AWS 管理主控台中。估算不會包含已刪除的資源。

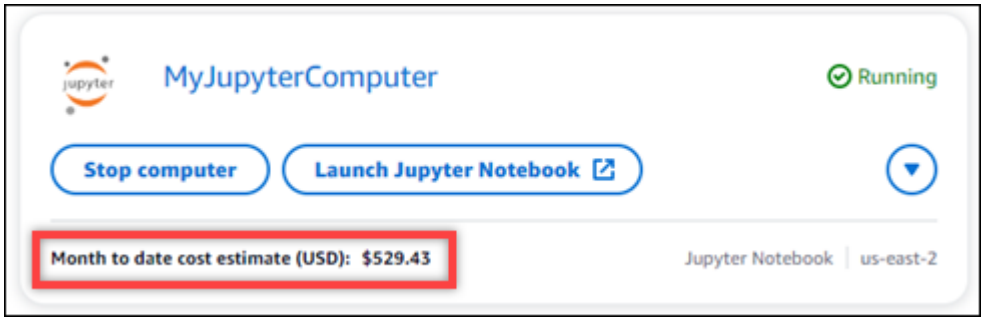
> **Important**
>
> 估算是以資源用量為基礎的預估成本。您的實際成本將根據資源的實際使用情況而定，而不是 Lightsail for Research 主控台中顯示的估計值。實際費用會顯示在您的帳 AWS Billing 戶對帳單上。
>
> 請登入 AWS Management Console 並開啟 AWS Billing 主控台，網址為 https://console.aws.amazon.com/billing/。

主題

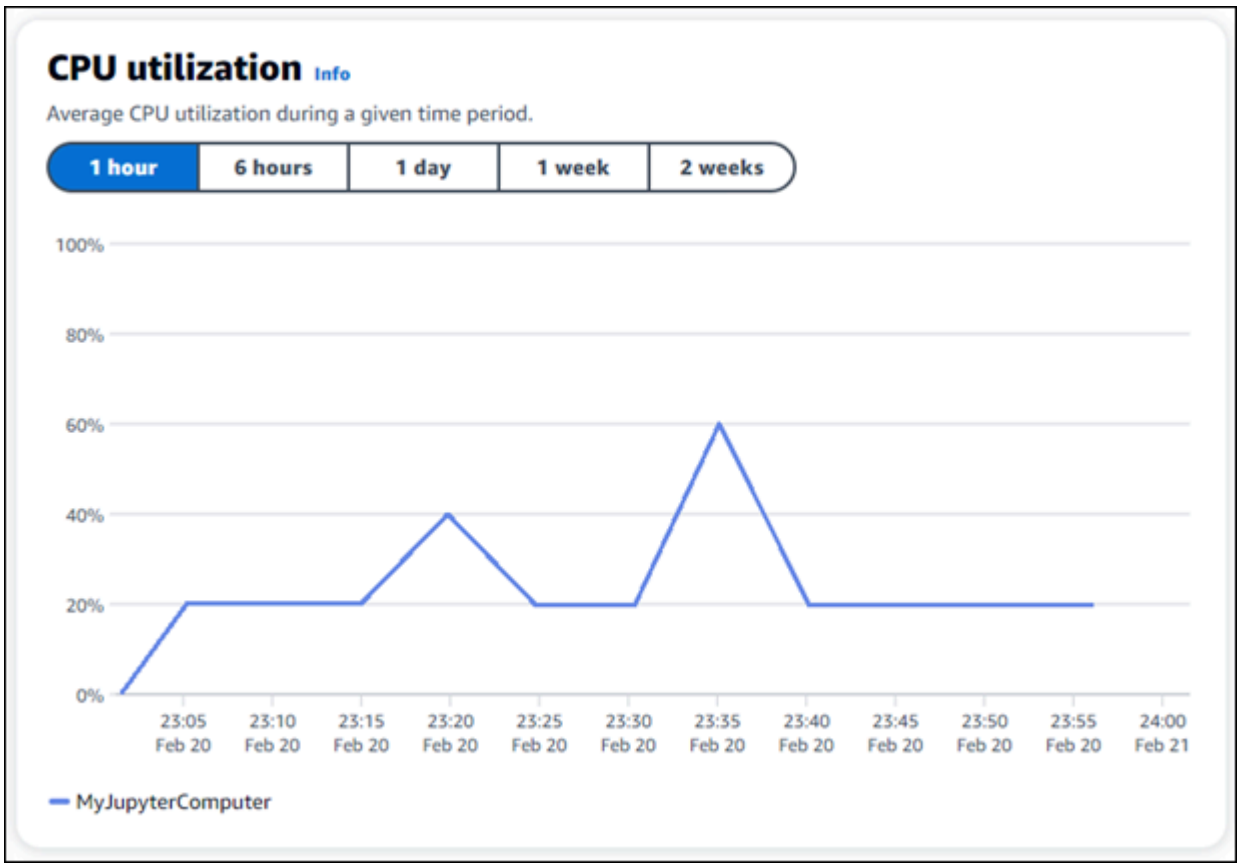
監控成本和用量估算。

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。

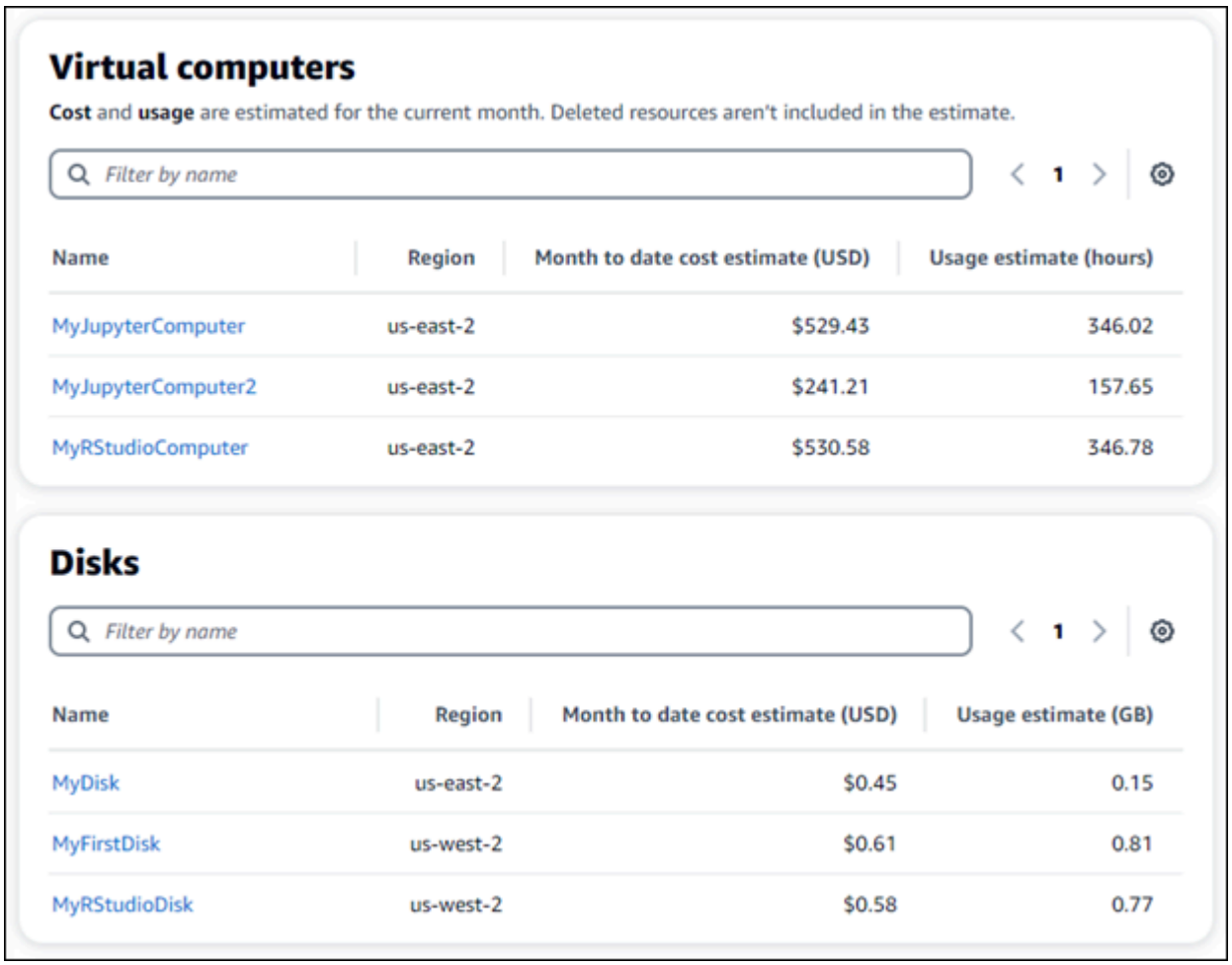
1. 在適用於研究的 Lightsail 主控台的導覽窗格中選擇 [虛擬電腦]。每台運行中虛擬電腦的下方，會列出該虛擬電腦當月至今的成本估算。



2. 若要檢視虛擬電腦的 CPU 使用率，請選擇虛擬電腦的名稱，然後選擇儀表板分頁。



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

成本控制

成本控制使用您定義的規則，協助管理 Lightsail for Research 虛擬電腦的用量和成本。

您可以建立停止閒置虛擬電腦規則，則當在給定的時間段內達到指定的 CPU 使用率百分比時，即會停止運行中的電腦。例如，當某台電腦的 CPU 使用率在 30 分鐘的期間內等於或小於 5% 時，規則可以自動停止該電腦。這表示電腦處於閒置狀態，Lightsail for Research 會停止該電腦。虛擬電腦停止後，您就不需要支付標準的小時費用。

主題

建立規則

完成以下步驟，以建立一個 Lightsail for Research 虛擬電腦的規則。

> **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控的指標，而唯一支援的運算是小於或等於。

1. 登入 Lightsail for Research 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 使用率百分比和持續時間。

   例如，您可以指定 5% 和 30 分鐘。當某台電腦的 CPU 使用率在 30 分鐘的期間內等於或小於 5% 時，Lightsail for Research 會自動停止該電腦。
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。

刪除規則

完成以下步驟，以刪除 Lightsail for Research 虛擬電腦的規則。

1. 登入 Lightsail for Research 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。

標籤

使用 Amazon Lightsail for Research，您可以為您的資源指派標籤。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。

以下資源可在 Amazon Lightsail for Research 主控台中加上標籤：

- 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。
- 索引鍵的長度上限為 128 個 Unicode 字元 (UTF-8)。
- 值的長度上限則為 256 個 Unicode 字元 (UTF-8)。
- 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。該字首保留供 AWS 使用。

主題

建立標籤

完成以下步驟，以建立一個 Lightsail for Research 虛擬電腦的標籤。與 Lightsail for Research 磁碟和快照的步驟類似。

1. 登入位於 Lightsail for Research 主控台的 Lightsail for Research 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 Manage tags (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。

刪除標籤

完成以下步驟，以刪除 Lightsail for Research 虛擬電腦的標籤。與 Lightsail for Research 磁碟和快照的步驟類似。

1. 登入位於 Lightsail for Research 主控台的 Lightsail for Research 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 Manage tags (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)。

用於研究的 Amazon Lightsail 中的安全性

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

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

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

本文件可協助您瞭解如何在使用 Lightsail 進行研究報告時套用共同的責任模型。下列主題說明如何設定 Lightsail 進行研究報告，以符合您的安全性和合規性目標。您也會學到如何使用其他可 AWS 協助您監控及保護 Lightsail 研究用資源的服務。

主題

- Amazon Lightsail 研究中的資料保護
- 適用於研究的 Amazon Lightsail Identity and Access Management
- 適用於研究的 Amazon Lightsail 合規驗證
- Amazon Lightsail 的研究彈性
- 用於研究的亞 Amazon Lightsail 基礎設施安全
- 亞馬遜研究專用中的組態和漏洞分析
- 適用於研究的 Amazon Lightsail 的安全最佳實務

Amazon Lightsail 研究中的資料保護

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

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

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

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

適用於研究的 Amazon Lightsail Identity and Access Management

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員可控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 Lightsail 用於研究資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

> **Note**
>
> 適用於研究的亞馬遜 Lightsail 和 Lightsail 共用相同的 IAM 政策參數。對 Lightsail 進行的研究政策所做的變更也會影響 Lightsail 政策。例如，如果使用者具有在 Lightsail 研究用中建立磁碟的權限，該使用者也可以在 Lightsail 中建立磁碟。

主題

- 使用政策管理存取權
- 用於研究的 Amazon Lightsail 如何與 IAM 搭配使用
- 適用於研究的 Amazon Lightsail 基於身份識別的政策示例
- 針對研究的身分識別和存取權進 Amazon Lightsail 疑難排解

物件

您使用 AWS Identity and Access Management (IAM) 的方式會根據您在 Lightsail 進行的研究工作而有所不同。

服務使用者 — 如果您使用 Lightsail 進行研究用服務，則管理員會為您提供所需的認證和權限。當您使用更多 Lightsail 研究用功能來完成工作時，您可能需要其他權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法在 Lightsail 進行研究版中存取某項功能，請參閱針對研究的身分識別和存取權進 Amazon Lightsail 疑難排解。

服務管理員 — 如果您負責公司的 Lightsail 研究用資源，您可能擁有 Lightsail 研究版的完整存取權。您的工作就是決定服務使用者應存取哪些 Lightsail 適用於研究的功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要深入了解貴公司如何將 IAM 與 Lightsail 進行研究版使用，請參閱用於研究的 Amazon Lightsail 如何與 IAM 搭配使用。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要瞭解如何撰寫政策以管理 Lightsail for Research 的存取權限的詳細資訊。若要檢視可在 IAM 中使用的 Lightsail 以身分識別為基礎的政策範例，請參閱。適用於研究的 Amazon Lightsail 基於身份識別的政策示例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需有關登入的詳細資訊 AWS，請參閱《AWS 登入 使用指南》 AWS 帳戶中的如何登入您的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署您的要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的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 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的多重要素驗證和 IAM 使用者指南中的在 AWS中使用多重要素驗證 (MFA)。

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，該身分可完整存取該帳戶中的所有資源 AWS 服務和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。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。如需這些任務的完整清單，了解需以根使用者登入的任務，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

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時登入資料進行存取 AWS 服務 。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

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，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 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 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 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，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

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

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法更多相關資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 – 若要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。如需有關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，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。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。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 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。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取權角色和資源型政策間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源類型政策的差異。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。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。
  - 轉寄存取工作階段 (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 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 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《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需更多資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

若要了解是否要使用 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 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的更多相關資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪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。若要授予使用者對其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，使用者便能擔任這些角色。

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

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

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

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定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。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

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

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些委託人 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

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

其他政策類型

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

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 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。如需許可範圍的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 實體許可範圍。
- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需組織和 SCP 的更多相關資訊，請參閱 AWS Organizations 使用者指南中的 SCP 運作方式。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過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。如需更多資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

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

用於研究的 Amazon Lightsail 如何與 IAM 搭配使用

在您使用 IAM 管理適用於研究的 Lightsail 存取權限之前，請先了解哪些 IAM 功能可與研究版 Lightsail 搭配使用。

您可以與亞馬遜研究專用的 IAM 功能搭配使用

IAM 功能	Lightsail 提供研究支援
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
ACL	否
ABAC(政策中的標籤)	部分
臨時憑證	是
主體許可	否
服務角色	否
服務連結角色	否

若要深入瞭解 Lightsail 研究版和其他 AWS 服務如何搭配大多數 IAM 功能搭配使用，請參閱 IAM 使用者指南中的適用於 IAM 的AWS 服務。

適用於研究的 Lightsail 基於身分識別的政策

支援身分型政策	是

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

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

適用於研究之 Lightsail 的身分識別原則範例

若要檢視 Lightsail 適用於研究人員身分識別型原則的範例，請參閱。適用於研究的 Amazon Lightsail 基於身份識別的政策示例

Lightsail 進行研究的基於資源的政策

支援以資源基礎的政策	否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定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。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的主體。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時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。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 IAM 角色與資源型政策有何差異。

Lightsail 進行研究的政策行動

支援政策動作	是

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

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 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。

若要查看適用於研究的 Lightsail 動作清單，請參閱服務授權參考資料中的 Amazon Lightsail 為研究定義的動作。

Lightsail 適用於研究的政策動作在動作前使用下列前置詞：

```
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 適用於研究人員身分識別型原則的範例，請參閱。適用於研究的 Amazon Lightsail 基於身份識別的政策示例

適用於 Lightsail 研究的政策資源

支援政策資源	是

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

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

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

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

若要查看適用於研究的 Lightsail 資源類型及其 ARN 清單，請參閱服務授權參考資料中由 Amazon Lightsail 定義的研究資源。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 Amazon Lightsail 為研究所定義的動作。

若要檢視 Lightsail 適用於研究人員身分識別型原則的範例，請參閱。適用於研究的 Amazon Lightsail 基於身份識別的政策示例

適用於研究用的 Lightsail 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哪些內容。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，請使用邏輯OR運算來 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，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

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

若要查看適用於研究的 Lightsail 條件金鑰清單，請參閱服務授權參考資料中的適用於研究的 Amazon Lightsail 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 為研究定義的動作。

若要檢視 Lightsail 適用於研究人員身分識別型原則的範例，請參閱。適用於研究的 Amazon Lightsail 基於身份識別的政策示例

用於研究的應用於 Lightsail 的 ACL

支援 ACL	否

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

ABAC 與 Lightsail 進行研究

支援 ABAC (政策中的標籤)	部分

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，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 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC?。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

使用臨時登入資 Lightsail 搭配研究用

支援臨時憑證	是

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

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

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

適用於研究的 Lightsail 跨服務主體權限

支援轉寄存取工作階段 (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 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 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《轉發存取工作階段》。

Lightsail 進行研究的服務角色

支援服務角色	否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。

> **Warning**
>
> 變更服務角色的權限可能會中斷 Lightsail 用於研究的功能。只有當 Lightsail 用於研究人員提供指引時，才能編輯服務角色。

適用於研究用的 Lightsail 務連結角色

支援服務連結角色。	否

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。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，請參閱可搭配 IAM 運作的AWS 服務。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。

適用於研究的 Amazon Lightsail 基於身份識別的政策示例

根據預設，使用者和角色沒有建立或修改 Lightsail 用於研究資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其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，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

如需 Lightsail 進行研究所定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱服務授權參考中的適用於 Amazon Lightsail 研究的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 使用適用 Lightsail 究的主控台
- 允許使用者檢視他們自己的許可

政策最佳實務

以身分識別為基礎的原則會決定某人是否可以建立、存取或刪除您帳戶中的 Lightsail 用於研究資源。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 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。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 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。

- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

使用適用 Lightsail 究的主控台

若要存取適用於研究的 Amazon Lightsail 主控台，您必須擁有最低限度的許可集。這些權限必須允許您列出並檢視有關 Lightsail 的研究用資源的詳細資 AWS 帳戶料。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。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

若要確保使用者和角色仍可使用 Lightsail 進行研究主控台，請同時將 Lightsail 進行研究*ConsoleAccess*或*ReadOnly* AWS 受管理的原則附加至實體。如需詳細資訊，請參閱《IAM 使用者指南》中的新增許可到使用者。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "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": "*"
        }
    ]
}
```

針對研究的身分識別和存取權進 Amazon Lightsail 疑難排解

使用下列資訊可協助您診斷並修正使用 Lightsail 研究版和 IAM 時可能會遇到的常見問題。

主題

- 我沒有在 Lightsail 進行研究用的動作的授權
- 我想要允許我以外的人員存 AWS 帳戶 取我的 Lightsail 研究用資源

我沒有在 Lightsail 進行研究用的動作的授權

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

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

```
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 系統管理員。您的管理員提供您的簽署憑證。

我想要允許我以外的人員存 AWS 帳戶 取我的 Lightsail 研究用資源

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：

- 若要瞭解研究版 Lightsail 是否支援這些功能，請參閱用於研究的 Amazon Lightsail 如何與 IAM 搭配使用。
- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱 IAM 使用者指南中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (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。

適用於研究的 Amazon Lightsail 合規驗證

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。

- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

Amazon Lightsail 的研究彈性

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎結構。

除了 AWS 全球基礎架構外，Lightsail for Research 還提供多種功能，協助支援您的資料恢復能力和備份需求。如需詳細資訊，請參閱 快照 及 建立快照。

用於研究的亞 Amazon Lightsail 基礎設施安全

作為一項受管服務，適用於研究的 Amazon Lightsail 受到 AWS 全球網路安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫，透過網路存取適用於研究的 Lightsail。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

亞馬遜研究專用中的組態和漏洞分析

配置和 IT 控制是與您（我們的客戶）AWS 之間的共同責任。如需詳細資訊，請參閱 AWS 共用的責任模型。

適用於研究的 Amazon Lightsail 的安全最佳實務

Lightsail 研究版提供許多安全性功能，可在您開發和實作自己的安全性原則時考量。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。

若要防止與您使用 Lightsail 進行研究相關的潛在安全性事件，請遵循下列最佳做法：

- 透過驗證第一個控制台，存取 Lightsail 進行研究專用主控台。 AWS Management Console 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。