aws

사용자 가이드

연구용 Amazon Lightsail

연구용 Amazon Lightsail: 사용자 가이드

Table of Contents

연구용 Amazon Lightsail이란 무엇입니까?

연구자와 연구자는 Amazon Lightsail for Research를 사용하여 Amazon Web Services () 클라우드에서 강력한 가상 컴퓨터를 만들 수 있습니다.AWS이러한 가상 컴퓨터에는 Scilab과 같은 연구 애플리케이션이 사전 설치되어 있습니다. RStudio

Lightsail for Research를 사용하면 웹 브라우저에서 직접 데이터를 업로드하여 작업을 시작할 수 있습니다. 언제든지 가상 컴퓨터를 만들고 삭제할 수 있으므로 강력한 컴퓨팅 리소스에 온디맨드 방식으로 액세스할 수 있습니다.

가상 컴퓨터가 필요한 기간 동안만 비용을 지불하면 됩니다. Lightsail for Research는 사전 구성된 비용 한도에 도달하면 컴퓨터를 자동으로 중지할 수 있는 예산 관리 기능을 제공하므로 초과 요금에 대해 걱정할 필요가 없습니다.

Lightsail for Research 콘솔에서 수행하는 모든 작업은 공개적으로 사용 가능한 자료를 통해 지원됩니다. API Amazon APILightsail용 AWS CLI및 를 설치하고 사용하는 방법을 알아보십시오.

요금

Lightsail for Research를 사용하면 생성하고 사용한 리소스에 대해서만 비용을 지불하면 됩니다. 자세한 내용은 연구용 Lightsail 요금을 참조하십시오.

가용성

연구용 Lightsail은 미국 동부 (버지니아 북부) 지역을 제외하고 Amazon Lightsail과 AWS 동일한 지역에서 사용할 수 있습니다. 연구용 Lightsail도 Lightsail과 동일한 엔드포인트를 사용합니다. Lightsail에 대해 현재 지원되는 AWS 지역 및 엔드포인트를 보려면 일반 참조의 Lightsail 엔드포인트 및 할당량을 참조하십시오.AWS

연구용 Amazon Lightsail 설정하기

신규 AWS 고객인 경우 Amazon Lightsail for Research를 사용하기 전에 이 페이지에 나열된 설정 사전 요구 사항을 완료하십시오.

가입하여 다음을 수행하십시오. AWS 계정

계정이 없는 경우 다음 단계를 완료하여 계정을 만드세요. AWS 계정

가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/등록 열기.
2. 온라인 지시 사항을 따릅니다.

   등록 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   에 가입하면 AWS 계정 루트 사용자팬이 생성됩니다. AWS 계정루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 가입 절차가 완료된 후 확인 이메일을 보냅니다. 언제라도 https://aws.amazon.com/로 이동하여 내 계정을 선택하여 현재 계정 활동을 확인하고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

가입한 AWS 계정후에는 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 보호하고 AWS IAM Identity Center활성화하고 생성하십시오. AWS 계정 루트 사용자

보안을 유지하세요. AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 AWS Management Console소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 User Guide의 루트 사용자로 로그인을 참조하십시오.
2. 루트 사용자에 대한 다단계 인증 (MFA) 을 켜십시오.

지침은 사용 설명서의 AWS 계정 IAM루트 사용자 (콘솔) 용 가상 MFA 기기 활성화를 참조하십시오.

관리자 액세스 권한이 있는 사용자 생성

1. IAMID 센터를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAMID 센터에서 사용자에게 관리 액세스 권한을 부여하십시오.

   를 ID 소스로 사용하는 방법에 대한 자습서는 사용 설명서의 기본값으로 IAM Identity Center 디렉터리AWS IAM Identity Center 사용자 액세스 구성을 참조하십시오. IAM Identity Center 디렉터리

관리 액세스 권한이 있는 사용자로 로그인

- IAMIdentity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 URL 로그인을 사용하십시오.

  IAMIdentity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 사용 설명서의 AWS 액세스 포털에 로그인을 참조하십시오.AWS 로그인

추가 사용자에게 액세스 권한 할당

1. IAMIdentity Center에서 최소 권한 권한 적용의 모범 사례를 따르는 권한 집합을 생성하십시오.

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.
2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

튜토리얼: 연구용 Lightsail 가상 컴퓨터 시작하기

이 자습서를 사용하여 연구용 Amazon Lightsail 가상 컴퓨터를 시작하십시오. 가상 컴퓨터를 만들고 연결하며 사용하는 방법을 배울 수 있습니다. Lightsail for Research에서 가상 컴퓨터는 사용자가 만들고 관리하는 연구용 워크스테이션입니다. AWS 클라우드가상 컴퓨터는 우분투 운영 체제가 설치된 Lightsail Linux 인스턴스를 기반으로 합니다. 가상 컴퓨터에서,, Scilab 등과 같은 JupyterLab 연구 애플리케이션을 미리 구성할 수 있습니다. RStudio

이 자습서에서 생성하는 가상 컴퓨터에는 가상 컴퓨터를 생성한 시점부터 삭제할 때까지 사용 요금이 부과됩니다. 삭제는 이 자습서의 마지막 단계입니다. 요금에 대한 자세한 내용은 연구용 Lightsail 요금을 참조하십시오.

주제

1단계: 필수 구성 요소 완성

신규 AWS 고객인 경우 Amazon Lightsail for Research를 사용하기 전에 설정 사전 요구 사항을 완료하십시오. 자세한 내용은 연구용 Amazon Lightsail 설정하기 단원을 참조하십시오.

2단계: 가상 컴퓨터 생성

다음 절차에 설명된 대로 Lightsail for Research 콘솔을 사용하여 가상 컴퓨터를 만들 수 있습니다. 이 자습서는 첫 번째 가상 컴퓨터를 빠르게 시작하도록 돕기 위한 것입니다. 또한 사용 가능한 애플리케이션과 하드웨어 플랜을 살펴보는 것이 좋습니다. 자세한 내용은 연구용 Lightsail의 애플리케이션 이미지 및 하드웨어 플랜 선택 및 연구용 Lightsail 가상 컴퓨터 만들기 단원을 참조하세요.

1. 연구용 Lightsail 콘솔에 로그인합니다.

2. 홈페이지에서 가상 컴퓨터 만들기를 선택합니다.
3. 가상 AWS 리전 컴퓨터용으로 선택하세요.

   대기 시간을 줄이려면 실제 위치와 가장 가까운 위치를 선택하세요. AWS 리전
4. APILightsail에서 블루프린트라고도 하는 애플리케이션을 선택하십시오.

   선택한 애플리케이션은 가상 컴퓨터를 만들 때 가상 컴퓨터에 설치 및 구성됩니다.
5. APILightsail에서는 번들이라고도 하는 하드웨어 플랜을 선택하십시오.

   하드웨어 요금제는 CPU v코어, 메모리, 스토리지, 월별 데이터 전송을 포함하여 다양한 양의 처리 능력을 제공합니다. 연구용 Lightsail은 가상 컴퓨터에 대한 표준 GPU 요금제와 요금제를 제공합니다. 작업에 필요한 계산 요구 사항이 낮을 때는 표준 플랜을 선택합니다. 기계 학습 모델이나 기타 계산 집약적인 작업을 실행하는 경우와 같이 요구 사항이 높을 때는 GPU 요금제를 선택하십시오.
6. 가상 컴퓨터의 이름을 입력합니다.
7. 요약 패널에서 가상 컴퓨터 만들기를 선택합니다.

새 가상 컴퓨터를 설치하고 실행한 후 이 자습서의 다음 단계를 계속 진행하여 컴퓨터 애플리케이션을 시작하는 방법을 알아봅니다.

3단계: 가상 컴퓨터 애플리케이션 시작

가상 컴퓨터를 만들고 실행 중 상태가 되면 웹 브라우저에서 가상 세션을 시작할 수 있습니다. 세션을 통해 가상 컴퓨터에 설치된 애플리케이션과 상호 작용하고 해당 애플리케이션을 관리할 수 있습니다.

1. 연구용 Lightsail 콘솔의 탐색 창에서 가상 컴퓨터를 선택합니다.
2. 1단계에서 만든 가상 컴퓨터의 이름을 찾은 다음 애플리케이션 시작을 선택합니다. 예를 들어, 실행. JupyterLab 새 웹 브라우저 창에 애플리케이션 세션이 열립니다.

> **Important**
>
> 웹 브라우저에 팝업 차단기가 설치되어 있는 경우 세션을 열기 전에 aws.amazon.com 도메인의 팝업을 허용해야 할 수 있습니다.

가상 컴퓨터에 연결하는 방법에 대해 알아보려면 이 자습서의 다음 단계를 계속 진행합니다.

4단계: 가상 컴퓨터에 연결

다음 방법을 사용하여 가상 컴퓨터에 연결하는 것이 가능합니다.

- 연구용 Lightsail 콘솔에서 사용할 수 있는 브라우저 기반 NICE DCV 클라이언트를 사용하십시오. 에서는 그래픽 사용자 인터페이스 (GUI) 를 사용하여 연구 응용 프로그램 및 가상 컴퓨터의 운영 체제와 상호 작용할 수 있습니다. NICE DCV

  또한 브라우저 기반 NICE DCV 클라이언트를 사용하여 가상 컴퓨터의 명령줄 인터페이스에 액세스하고 파일을 전송할 수 있습니다.
- Open SSHTTY, Pu 또는 Linux용 Windows 서브시스템과 같은 보안 셸 (SSH) 클라이언트를 사용하여 가상 컴퓨터의 명령줄 인터페이스에 액세스하십시오. SSH클라이언트를 사용하여 스크립트와 구성 파일을 편집할 수 있습니다.
- Secure Copy (SCP) 를 사용하여 로컬 컴퓨터와 가상 컴퓨터 간에 파일을 안전하게 전송할 수 있습니다. 를 사용하면 로컬에서 작업을 시작한 후 가상 컴퓨터에서 작업을 계속할 수 있습니다. SCP 또한 가상 컴퓨터에서 파일을 다운로드하여 작업을 로컬 컴퓨터에 복사할 수 있습니다.

를 사용하여 가상 컴퓨터에 SSH 연결하거나 를 사용하여 파일을 전송하려면 가상 컴퓨터의 키 쌍을 제공해야 SCP 합니다. 키 페어는 Lightsail for Research 가상 컴퓨터에 연결할 때 ID를 증명하는 데 사용하는 보안 자격 증명 세트입니다. 키 페어는 프라이빗 키와 퍼블릭 키를 구성됩니다.

가상 컴퓨터에 연결하는 방법에 대한 자세한 내용은 다음 설명서를 참조하세요.

- 원격 디스플레이 프로토콜 연결 설정:
  - 연구용 Lightsail 가상 컴퓨터 애플리케이션에 액세스
  - 연구용 Lightsail 가상 컴퓨터의 운영 체제에 액세스
- 다음을 사용하여 SSH 연결을 설정하거나 파일을 전송하십시오. SCP
  - 연구용 Lightsail 가상 컴퓨터용 키 페어를 구매하세요
  - 보안 셸을 사용하여 연구용 Lightsail 가상 컴퓨터에 연결
  - 보안 복사를 사용하여 연구용 Lightsail 가상 컴퓨터로 파일 전송

가상 컴퓨터 스토리지에 대해 알아보려면 이 자습서의 다음 단계를 계속 진행합니다.

5단계: 가상 컴퓨터에 스토리지 추가

Lightsail for Research는 가상 컴퓨터에 연결할 수 있는 블록 수준의 스토리지 볼륨 (디스크) 을 제공합니다. 가상 컴퓨터에 시스템 디스크가 함께 제공되더라도 스토리지 요구 사항이 변경되면 가상 컴퓨터에 추가 디스크를 연결할 수 있습니다. 가상 컴퓨터에서 디스크를 분리한 다음 이 디스크를 다른 가상 컴퓨터에 연결하는 것도 가능합니다.

콘솔을 사용하여 가상 컴퓨터에 디스크를 연결하면 Lightsail for Research가 자동으로 디스크를 포맷하고 운영 체제에 마운트합니다. 이 프로세스는 몇 분 정도 걸리므로 사용하기 전에 디스크가 마운트된 상태인지 확인해야 합니다.

디스크 생성, 연결, 관리에 대한 자세한 내용은 다음 설명서를 참조하세요.

- 연구용 Lightsail 콘솔에서 스토리지 디스크 만들기
- 연구용 Lightsail 콘솔에서 스토리지 디스크 세부 정보 보기
- 연구용 Lightsail에서 가상 컴퓨터에 스토리지 추가
- 연구용 Lightsail의 가상 컴퓨터에서 디스크 분리하기
- 연구용 Lightsail에서 사용하지 않는 스토리지 디스크 삭제

가상 컴퓨터 백업에 대해 알아보려면 이 자습서의 다음 단계를 계속 진행합니다.

6단계: 스냅샷 생성

스냅샷은 데이터의 point-in-time 복사본입니다. 가상 컴퓨터의 스냅샷을 생성하고 이를 기준으로 사용하여 새 컴퓨터를 생성하거나 데이터 백업을 할 수 있습니다. 스냅샷은 스냅샷을 생성한 시점부터 컴퓨터를 복원하는 데 필요한 모든 데이터를 포함합니다.

스냅샷 생성 및 관리에 대한 자세한 내용은 다음 설명서를 참조하세요.

- 연구용 Lightsail 가상 컴퓨터 또는 디스크의 스냅샷 생성
- 연구용 Lightsail에서 가상 컴퓨터 및 디스크 스냅샷 보기 및 관리
- 스냅샷에서 가상 컴퓨터 또는 디스크 만들기
- 연구용 Lightsail 콘솔에서 스냅샷을 삭제합니다.

가상 컴퓨터 리소스 정리에 대해 알아보려면 이 자습서의 다음 단계를 계속 진행합니다.

7단계: 정리

이 자습서용으로 생성한 가상 컴퓨터 작업을 마친 후에는 가성 컴퓨터를 삭제할 수 있습니다. 이렇게 하면 필요하지 않은 가상 컴퓨터에 대한 요금이 더 이상 부과되지 않습니다.

가상 컴퓨터를 삭제해도 관련 스냅샷이나 연결된 디스크는 삭제되지 않습니다. 스냅샷과 디스크를 생성한 경우 해당 스냅샷과 디스크를 수동으로 삭제하여 요금이 부과되지 않도록 해야 합니다.

나중에 사용할 수 있도록 가상 컴퓨터를 저장하되 표준 시간당 요금으로 요금이 부과되지 않도록 하려면 가상 컴퓨터를 삭제하는 대신 중지하면 됩니다. 그런 다음 나중에 다시 시작할 수 있습니다. 자세한 내용은 연구용 Lightsail 가상 컴퓨터 세부 정보 보기 단원을 참조하십시오. 요금에 대한 자세한 내용은 연구용 Lightsail 요금을 참조하십시오.

> **Important**
>
> 연구용 Lightsail 리소스 삭제는 영구적인 조치입니다. 삭제된 데이터는 복구할 수 없습니다. 나중에 데이터가 필요할 수 있는 경우 삭제하기 전에 가상 컴퓨터의 스냅샷을 생성합니다. 자세한 내용은 스냅샷 생성을 참조하세요..

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 가상 컴퓨터를 선택합니다.
3. 삭제할 가상 컴퓨터를 선택합니다.
4. 작업을 선택한 다음 가상 컴퓨터 삭제를 선택합니다.
5. 텍스트 블록에 확인을 입력합니다. 그런 다음 가상 컴퓨터 삭제를 선택합니다

연구용 Lightsail에서 데이터 과학 애플리케이션을 시작해 보세요.

다음 자습서에서는 Lightsail for Research에서 사용할 수 있는 특정 응용 프로그램을 시작하는 방법에 대한 추가 정보를 제공합니다.

주제

- 연구용 JupyterLab Lightsail에서 실행 및 사용
- 연구용 RStudio Lightsail에서 실행 및 사용

> **Note**
>
> Lightsail for Research를 시작하기 위한 심층 자습서가 공공 부문 블로그에 RStudio AWS 게시되어 있습니다. 자세한 내용은 연구용 Amazon Lightsail 시작하기: 를 사용하는 자습서를 참조하십시오. RStudio

연구용 JupyterLab Lightsail에서 실행 및 사용

이 자습서에서는 Amazon Lightsail for Research에서 JupyterLab 가상 컴퓨터를 관리하고 사용하는 방법을 보여줍니다.

주제

- 1단계: 필수 구성 요소 완성
- 2단계: (옵션) 스토리지 스페이스 추가
- 3단계: 파일 업로드 및 다운로드
- 4단계: JupyterLab 애플리케이션 실행
- 5단계: JupyterLab 설명서 읽기
- 6단계: (옵션) 사용량 및 비용 모니터링
- 7단계: (옵션) 비용 관리 규칙 생성
- 8단계: (옵션) 스냅샷 생성
- 9단계: (옵션) 가상 컴퓨터 중지 또는 삭제

1단계: 필수 구성 요소 완성

아직 만들지 않았다면 JupyterLab 애플리케이션을 사용하여 가상 컴퓨터를 만드십시오. 자세한 내용은 연구용 Lightsail 가상 컴퓨터 만들기 단원을 참조하십시오.

새 가상 컴퓨터를 설치하고 실행한 후에는 이 자습서의 JupyterLab 응용 프로그램 섹션을 계속 실행하십시오.

2단계: (옵션) 스토리지 스페이스 추가

가상 컴퓨터는 시스템 디스크와 함께 제공됩니다. 그러나 스토리지 요구 사항이 변경되면 가상 컴퓨터에 추가 디스크를 연결하여 스토리지 스페이스를 늘릴 수 있습니다.

작업 파일을 연결된 디스크에 저장할 수도 있습니다. 그런 다음 디스크를 분리하고 다른 가상 컴퓨터에 연결하여 한 컴퓨터에서 다른 컴퓨터로 파일을 빠르게 이동할 수 있습니다.

또는 작업 파일이 있는 연결된 디스크의 스냅샷을 만든 다음 스냅샷에서 복제 디스크를 만들 수 있습니다. 그런 다음 새 복제 디스크를 다른 컴퓨터에 연결하여 여러 가상 컴퓨터에 작업을 복제할 수 있습니다. 자세한 내용은 연구용 Lightsail 콘솔에서 스토리지 디스크 만들기 및 연구용 Lightsail에서 가상 컴퓨터에 스토리지 추가 단원을 참조하세요.

> **Note**
>
> 콘솔을 사용하여 가상 컴퓨터에 디스크를 연결하면 Lightsail for Research가 자동으로 디스크를 포맷하고 마운트합니다. 이 프로세스는 몇 분 정도 걸리므로 사용하기 전에 디스크가 Mounted 마운팅 상태에 도달했는지 확인해야 합니다. 기본적으로 연구용 Lightsail은 디렉터리에 디스크를 마운트합니다. `/home/lightsail-user/<disk-name>` `<disk-name>`디스크에 지정한 이름입니다.

3단계: 파일 업로드 및 다운로드

JupyterLab 가상 컴퓨터에 파일을 업로드하고 가상 컴퓨터에서 파일을 다운로드할 수 있습니다. 이렇게 하려면 다음 단계를 완료합니다.

1. Amazon Lightsail에서 키 페어를 구하십시오. 자세한 내용은 연구용 Lightsail 가상 컴퓨터용 키 페어를 구매하세요 단원을 참조하십시오.

2. 키 페어를 확보한 후에는 Secure Copy (SCP) 유틸리티를 사용하여 연결을 설정할 수 있습니다. SCP명령 프롬프트 또는 터미널을 사용하여 파일을 업로드하고 다운로드할 수 있습니다. 자세한 내용은 보안 복사를 사용하여 연구용 Lightsail 가상 컴퓨터로 파일 전송 단원을 참조하십시오.
3. (선택 사항) 키 페어를 사용하여 가상 컴퓨터에 연결할 수도 SSH 있습니다. 자세한 내용은 보안 셸을 사용하여 연구용 Lightsail 가상 컴퓨터에 연결 단원을 참조하십시오.

> **Note**
>
> 브라우저 기반 NICE DCV 클라이언트를 사용하여 가상 컴퓨터의 명령줄 인터페이스에 액세스하고 파일을 전송할 수도 있습니다. NICEDCV연구용 Lightsail 콘솔에서 사용할 수 있습니다. 자세한 내용은 연구용 Lightsail 가상 컴퓨터 애플리케이션에 액세스 및 연구용 Lightsail 가상 컴퓨터의 운영 체제에 액세스 단원을 참조하세요.

연결된 스토리지 디스크에서 프로젝트 파일을 관리하려면 해당 파일을 첨부 디스크의 올바른 마운트 디렉터리에 업로드해야 합니다. 콘솔을 사용하여 가상 컴퓨터에 디스크를 연결하면 Lightsail for Research가 자동으로 디스크를 포맷하고 디렉터리에 마운트합니다. `/home/lightsail-user/<disk-name>` `<disk-name>`디스크에 부여한 이름입니다.

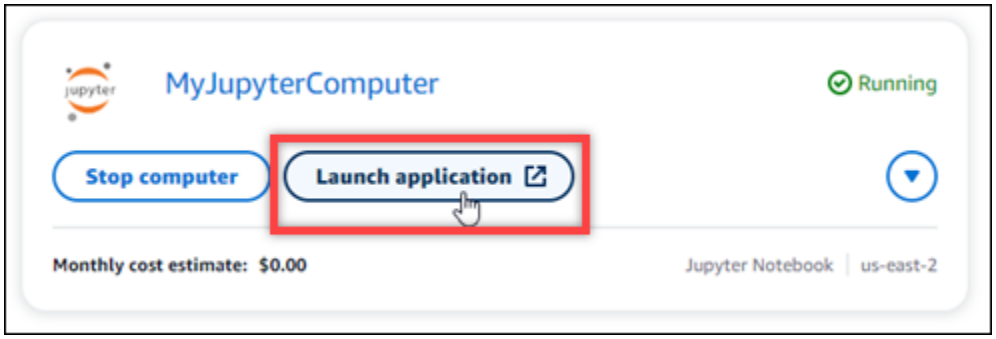
4단계: JupyterLab 애플리케이션 실행

다음 절차를 완료하여 새 가상 컴퓨터에서 JupyterLab 애플리케이션을 실행합니다.

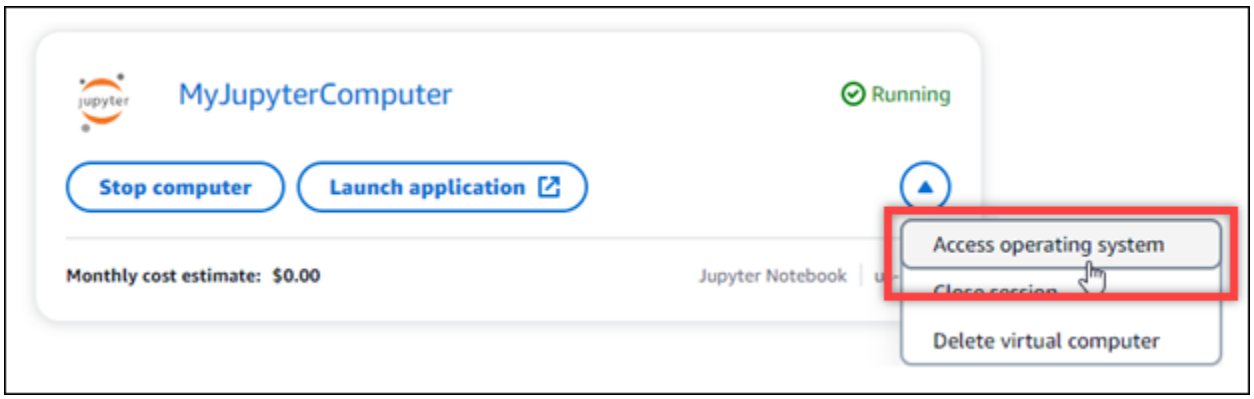
> **Important**
>
> 운영 체제나 JupyterLab 애플리케이션을 업데이트하라는 메시지가 표시되더라도 업데이트하지 마십시오. 대신 해당 프롬프트를 닫거나 무시하는 옵션을 선택합니다. 또한 /home/lightsail-admin/ 디렉터리에 있는 파일은 수정하지 마세요. 이러한 작업으로 인해 가상 컴퓨터를 사용할 수 없게 될 수 있습니다.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 계정에서 사용할 수 있는 가상 컴퓨터를 보려면 탐색 창에서 가상 컴퓨터를 선택합니다.
3. 가상 컴퓨터 페이지에서 가상 컴퓨터를 찾고 다음 옵션 중 하나를 선택하여 가상 컴퓨터에 연결합니다.

a. (권장) 집중 모드에서 애플리케이션을 실행하려면 JupyterLab 애플리케이션 시작을 선택합니다. 최근에 가상 컴퓨터에 연결하지 않은 경우 Lightsail for Research에서 세션을 준비하는 동안 몇 분 정도 기다려야 할 수 있습니다.



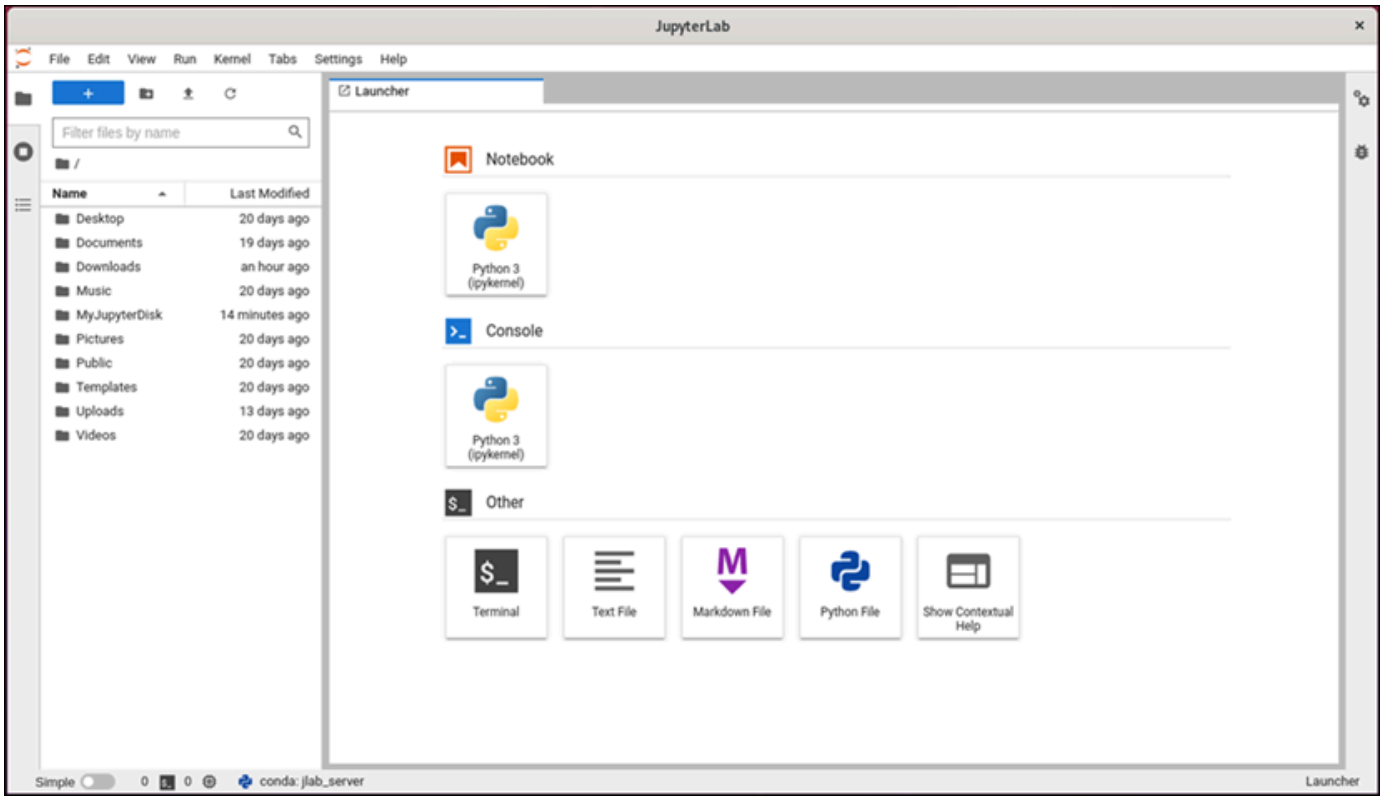
b. 컴퓨터의 드롭다운 메뉴를 선택한 다음 운영 체제 액세스를 선택하여 가상 컴퓨터의 데스크톱에 접근합니다.



연구용 Lightsail은 몇 가지 명령을 실행하여 원격 디스플레이 프로토콜 연결을 시작합니다. 잠시 후 가상 컴퓨터에 가상 데스크톱 연결이 설정된 새 브라우저 탭 창이 열립니다. 애플리케이션 실행 옵션을 선택한 경우 이 절차의 다음 단계를 계속 진행하여 애플리케이션에서 파일을 엽니다. JupyterLab 운영 체제 액세스 옵션을 선택한 경우 Ubuntu 데스크톱을 통해 다른 애플리케이션을 열 수 있습니다.

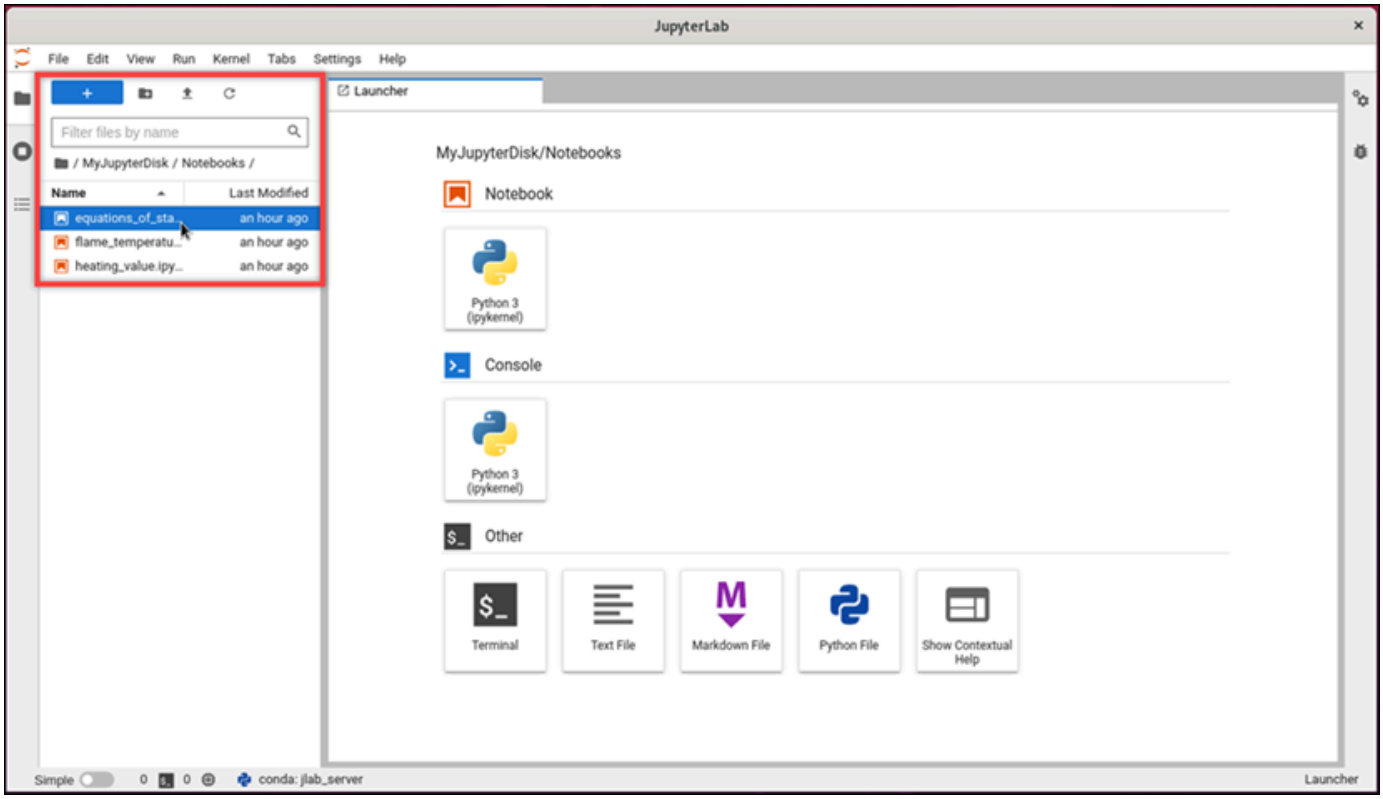
> **Note**
>
> 브라우저에서 클립보드 공유를 승인하라는 메시지가 표시될 수 있습니다. 이렇게 하면 로컬 컴퓨터와 가상 컴퓨터 간에 복사하여 붙여넣을 수 있습니다.
> Ubuntu에서 초기 설정을 묻는 메시지가 표시될 수도 있습니다. 지시에 따라 설정을 완료하고 운영 체제를 사용할 수 있습니다.

4. JupyterLab 애플리케이션이 열립니다. 런처 메뉴에서 새 노트북을 만들고, 콘솔을 시작하고, 터미널을 시작하고, 다양한 파일을 만들 수 있습니다.

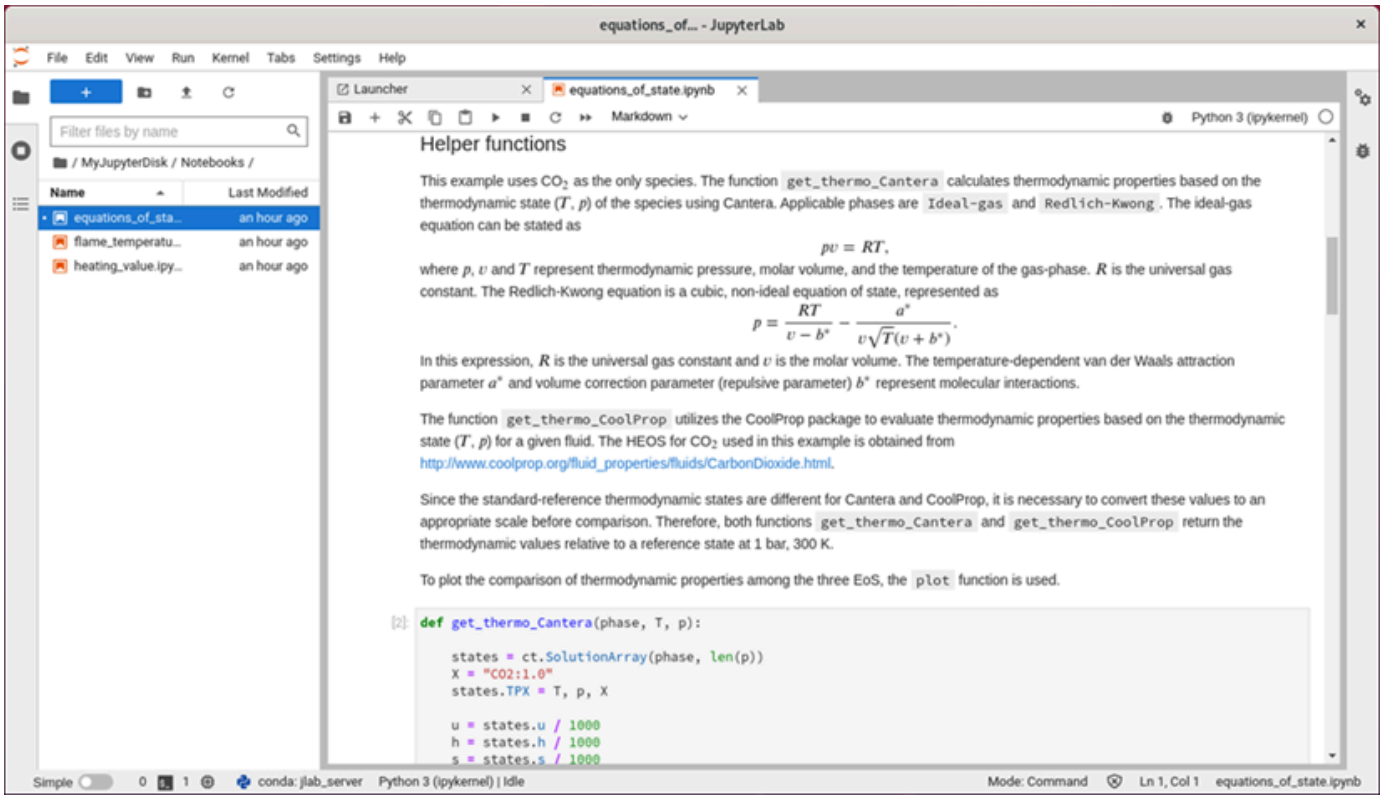


5. 에서 JupyterLab 파일을 열려면 파일 브라우저 창에서 프로젝트 파일이 저장되어 있는 디렉토리나 폴더를 선택합니다. 그런 후 파일을 선택하여 엽니다.

   연결된 디스크에 프로젝트 파일을 업로드한 경우 디스크가 마운트된 디렉터리를 찾습니다. 기본적으로 연구용 Lightsail은 디렉터리에 디스크를 마운트합니다. `/home/lightsail-user/<disk-name>` `<disk-name>`디스크에 지정한 이름입니다. 다음 예제에서 `MyJupyterDisk` 디렉터리는 마운트된 디스크를 나타내며, `Notebooks` 하위 디렉터리에는 Jupyter Notebook 파일이 들어 있습니다.



다음 예제에서는 `equations_of_state.ipynb` Jupyter Notebook 파일을 열었습니다.



시작 방법에 대한 자세한 내용은 이 자습서의 5단계: JupyterLab 설명서 읽기 섹션을 참조하세요.

5단계: JupyterLab 설명서 읽기

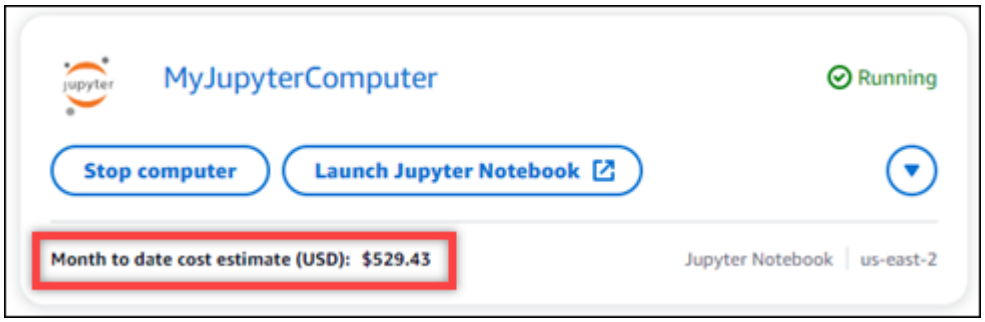
JupyterLab익숙하지 않은 경우 공식 설명서를 읽어 보는 것이 좋습니다. 다음과 같은 JupyterLab 온라인 리소스를 이용할 수 있습니다.

- JupyterLab문서
- Jupyter 담론 포럼
- JupyterLab ... 에 StackOverflow
- JupyterLab ... 에 GitHub

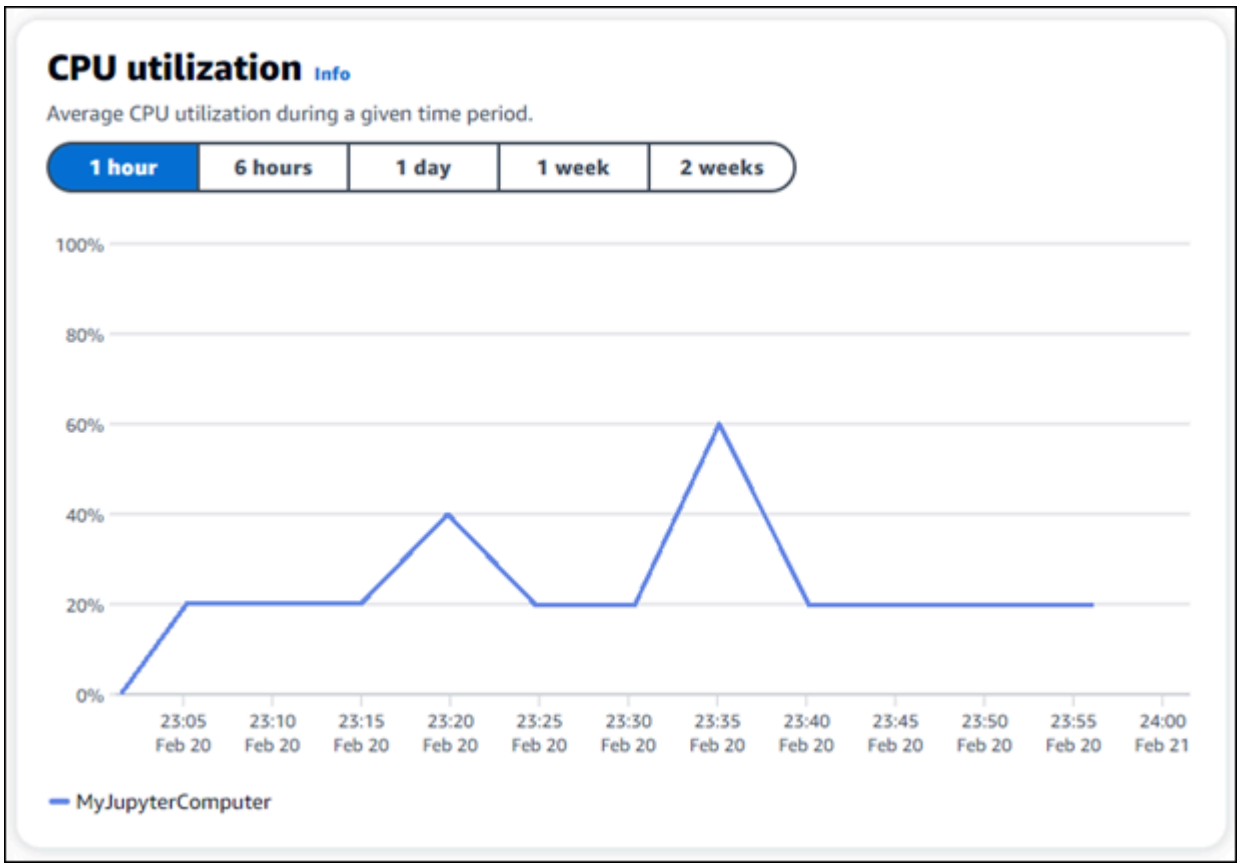
6단계: (옵션) 사용량 및 비용 모니터링

연구용 Lightsail 리소스의 월간 누계 비용 및 사용량 추정치는 연구용 Lightsail 콘솔의 다음 영역에 표시됩니다.

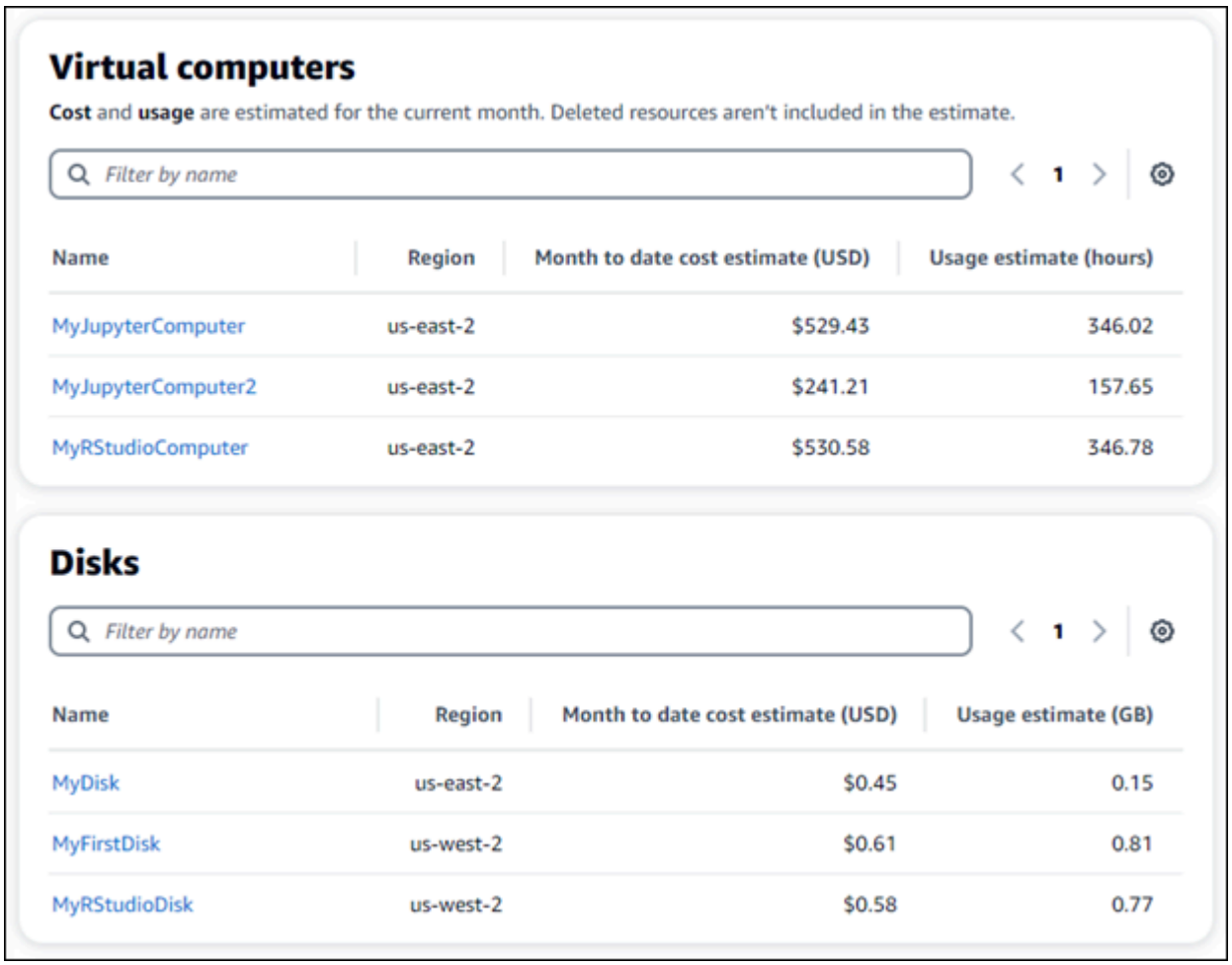
1. 연구용 Lightsail 콘솔의 탐색 창에서 가상 컴퓨터를 선택합니다. 실행 중인 각 가상 컴퓨터 아래에 가상 컴퓨터의 월 누계 예상 비용이 나열됩니다.



2. 가상 컴퓨터의 CPU 사용률을 보려면 가상 컴퓨터의 이름을 선택한 다음 대시보드 탭을 선택합니다.



3. 모든 Lightsail for Research 리소스의 월간 누계 비용 및 예상 사용량을 보려면 탐색 창에서 사용량을 선택합니다.



7단계: (옵션) 비용 관리 규칙 생성

비용 관리 규칙을 생성하여 가상 컴퓨터의 사용량과 비용을 관리합니다. 지정된 기간 동안 CPU 사용률이 지정된 비율에 도달하면 실행 중인 컴퓨터를 중지하는 유휴 상태에서 가상 컴퓨터 중지 규칙을 만들 수 있습니다. 예를 들어, 규칙은 30분 동안 특정 컴퓨터의 CPU 사용률이 5% 이하일 때 자동으로 중지할 수 있습니다. 이는 컴퓨터가 유휴 상태이고 Lightsail for Research가 컴퓨터를 중지하여 유휴 리소스에 대한 요금이 발생하지 않음을 의미할 수 있습니다.

> **Important**
>
> 유휴 상태인 가상 컴퓨터를 중지하는 규칙을 만들기 전에 며칠 동안 사용률을 CPU 모니터링하는 것이 좋습니다. 가상 컴퓨터의 부하가 서로 다를 때의 CPU 사용률을 기록해 두십시오. 예를 들어, 코드를 컴파일하고, 작업을 처리하고, 유휴 상태인 경우가 있습니다. 이렇게 하면 규칙의 정확한 임계값을 결정하는 데 도움이 됩니다. 자세한 내용은 이 자습서의 6단계: (옵션) 사용량 및 비용 모니터링 섹션을 참조하세요.

CPU사용률 임계값이 워크로드보다 높은 규칙을 만들면 규칙으로 인해 가상 컴퓨터가 연속적으로 중지될 수 있습니다. 예를 들어, 규칙에 의해 중지된 후 바로 가상 컴퓨터를 시작하면 규칙이 다시 활성화되고 컴퓨터가 다시 중지됩니다.

비용 관리 규칙의 생성 및 관리에 대한 자세한 지침은 다음 가이드에서 확인할 수 있습니다.

- 연구용 Lightsail에서 비용 관리 규칙을 관리합니다.
- 연구용 Lightsail 가상 컴퓨터에 대한 비용 관리 규칙 생성
- 연구용 Lightsail 가상 컴퓨터의 비용 관리 규칙을 삭제합니다.

8단계: (옵션) 스냅샷 생성

스냅샷은 데이터의 point-in-time 복사본입니다. 가상 컴퓨터의 스냅샷을 생성하고 이를 기준으로 사용하여 새 컴퓨터를 생성하거나 데이터 백업을 할 수 있습니다. 스냅샷은 스냅샷을 생성한 시점부터 컴퓨터를 복원하는 데 필요한 모든 데이터를 포함합니다.

스냅샷 생성 및 관리에 대한 자세한 지침은 다음 가이드에서 확인할 수 있습니다.

- 연구용 Lightsail 가상 컴퓨터 또는 디스크의 스냅샷 생성
- 연구용 Lightsail에서 가상 컴퓨터 및 디스크 스냅샷 보기 및 관리
- 스냅샷에서 가상 컴퓨터 또는 디스크 만들기
- 연구용 Lightsail 콘솔에서 스냅샷을 삭제합니다.

9단계: (옵션) 가상 컴퓨터 중지 또는 삭제

이 자습서용으로 생성한 가상 컴퓨터 작업을 마친 후에는 가성 컴퓨터를 삭제할 수 있습니다. 이렇게 하면 필요하지 않은 가상 컴퓨터에 대한 요금이 더 이상 부과되지 않습니다.

가상 컴퓨터를 삭제해도 관련 스냅샷이나 연결된 디스크는 삭제되지 않습니다. 스냅샷과 디스크를 생성한 경우 해당 스냅샷과 디스크를 수동으로 삭제하여 요금이 부과되지 않도록 해야 합니다.

나중에 사용할 수 있도록 가상 컴퓨터를 저장하되 표준 시간당 요금으로 요금이 부과되지 않도록 하려면 가상 컴퓨터를 삭제하는 대신 중지하면 됩니다. 그런 다음 나중에 다시 시작할 수 있습니다. 자세한 내용은 연구용 Lightsail 가상 컴퓨터 세부 정보 보기 단원을 참조하십시오. 요금에 대한 자세한 내용은 연구용 Lightsail 요금을 참조하십시오.

> **Important**
>
> 연구용 Lightsail 리소스 삭제는 영구적인 조치입니다. 삭제된 데이터는 복구할 수 없습니다. 나중에 데이터가 필요할 수 있는 경우 삭제하기 전에 가상 컴퓨터의 스냅샷을 생성합니다. 자세한 내용은 스냅샷 생성을 참조하세요..

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 가상 컴퓨터를 선택합니다.
3. 삭제할 가상 컴퓨터를 선택합니다.
4. 작업을 선택한 다음 가상 컴퓨터 삭제를 선택합니다.
5. 텍스트 블록에 확인을 입력합니다. 그런 다음 가상 컴퓨터 삭제를 선택합니다

연구용 RStudio Lightsail에서 실행 및 사용

이 자습서에서는 Amazon Lightsail for Research에서 RStudio 가상 컴퓨터를 관리하고 사용하는 방법을 보여줍니다.

> **Note**
>
> Lightsail for Research를 시작하기 위한 심층 자습서가 공공 부문 블로그에 RStudio AWS 게시되어 있습니다. 자세한 내용은 연구용 Amazon Lightsail 시작하기: 를 사용하는 자습서를 참조하십시오. RStudio

주제

1단계: 필수 구성 요소 완성

아직 만들지 않았다면 RStudio 애플리케이션을 사용하여 가상 컴퓨터를 만드십시오. 자세한 내용은 연구용 Lightsail 가상 컴퓨터 만들기 단원을 참조하십시오.

2단계: (옵션) 스토리지 스페이스 추가

가상 컴퓨터는 시스템 디스크와 함께 제공됩니다. 그러나 스토리지 요구 사항이 변경되면 가상 컴퓨터에 추가 디스크를 연결하여 스토리지 스페이스를 늘릴 수 있습니다.

작업 파일을 연결된 디스크에 저장할 수도 있습니다. 그런 다음 디스크를 분리하고 다른 가상 컴퓨터에 연결하여 한 컴퓨터에서 다른 컴퓨터로 파일을 빠르게 이동할 수 있습니다.

또는 작업 파일이 있는 연결된 디스크의 스냅샷을 만든 다음 스냅샷에서 복제 디스크를 만들 수 있습니다. 그런 다음 새 복제 디스크를 다른 컴퓨터에 연결하여 여러 가상 컴퓨터에 작업을 복제할 수 있습니다. 자세한 내용은 연구용 Lightsail 콘솔에서 스토리지 디스크 만들기 및 연구용 Lightsail에서 가상 컴퓨터에 스토리지 추가 단원을 참조하세요.

> **Note**
>
> 콘솔을 사용하여 가상 컴퓨터에 디스크를 연결하면 Lightsail for Research가 자동으로 디스크를 포맷하고 마운트합니다. 이 프로세스는 몇 분 정도 걸리므로 사용하기 전에 디스크가 Mounted 마운팅 상태에 도달했는지 확인해야 합니다. 기본적으로 Lightsail for Research는 사용자가 지정한 디스크 이름의 *<disk-name>* 디렉토리에 디스크를 마운트합니다. `/home/lightsail-user/`*<disk-name>*

3단계: 파일 업로드 및 다운로드

가상 컴퓨터에 파일을 업로드하고 RStudio 가상 컴퓨터에서 파일을 다운로드할 수 있습니다. 이렇게 하려면 다음 단계를 완료합니다.

1. Amazon Lightsail에서 키 페어를 구하십시오. 자세한 내용은 연구용 Lightsail 가상 컴퓨터용 키 페어를 구매하세요 단원을 참조하십시오.

2. 키 페어를 확보한 후에는 Secure Copy (SCP) 유틸리티를 사용하여 연결을 설정할 수 있습니다. SCP명령 프롬프트 또는 터미널을 사용하여 파일을 업로드하고 다운로드할 수 있습니다. 자세한 내용은 보안 복사를 사용하여 연구용 Lightsail 가상 컴퓨터로 파일 전송 단원을 참조하십시오.
3. (선택 사항) 키 페어를 사용하여 가상 컴퓨터에 연결할 수도 SSH 있습니다. 자세한 내용은 보안 셸을 사용하여 연구용 Lightsail 가상 컴퓨터에 연결 단원을 참조하십시오.

> **Note**
>
> 브라우저 기반 NICE DCV 클라이언트를 사용하여 가상 컴퓨터의 명령줄 인터페이스에 액세스하고 파일을 전송할 수도 있습니다. NICEDCV연구용 Lightsail 콘솔에서 사용할 수 있습니다. 자세한 내용은 연구용 Lightsail 가상 컴퓨터 애플리케이션에 액세스 및 연구용 Lightsail 가상 컴퓨터의 운영 체제에 액세스 단원을 참조하세요.

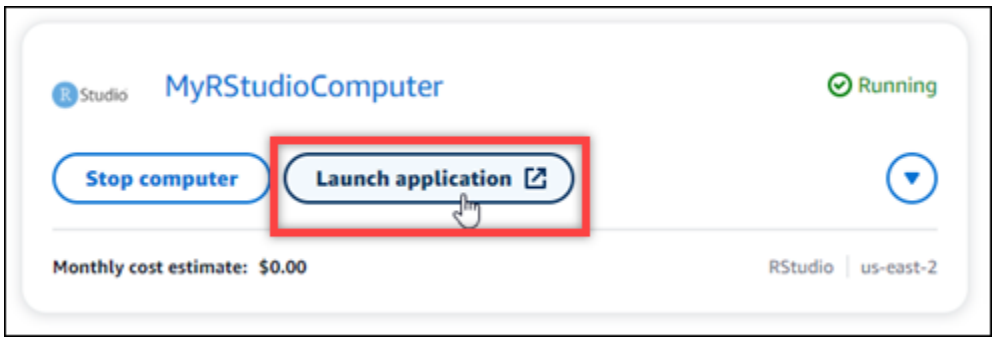
4단계: 애플리케이션 실행 RStudio

다음 절차를 완료하여 새 가상 컴퓨터에서 RStudio 애플리케이션을 실행합니다.

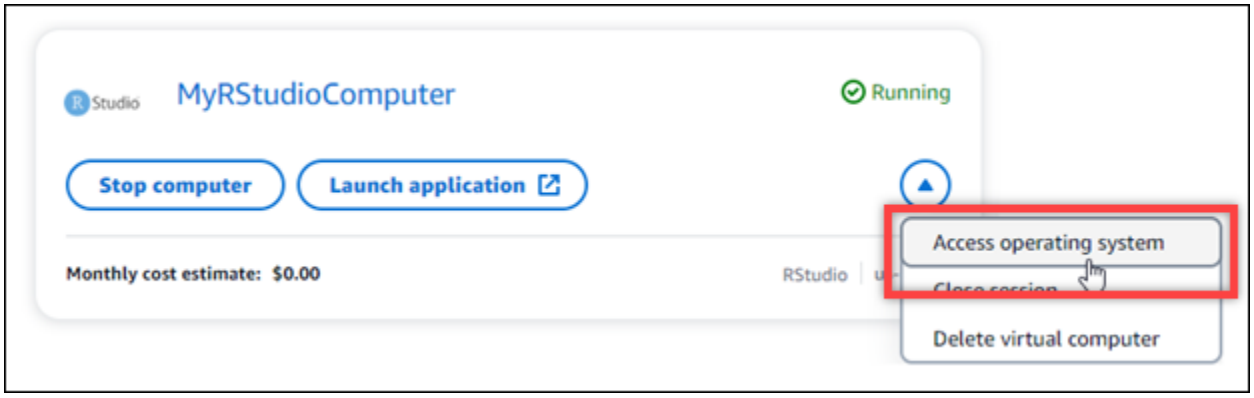
> **Important**
>
> 운영 체제나 RStudio 애플리케이션을 업데이트하라는 메시지가 표시되더라도 업데이트하지 마십시오. 대신 해당 프롬프트를 닫거나 무시하는 옵션을 선택합니다. 또한 /home/lightsail-admin/ 디렉터리에 있는 파일은 수정하지 마세요. 이러한 작업으로 인해 가상 컴퓨터를 사용할 수 없게 될 수 있습니다.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 계정에서 사용할 수 있는 가상 컴퓨터를 보려면 탐색 창에서 가상 컴퓨터를 선택합니다.
3. 가상 컴퓨터 페이지에서 가상 컴퓨터를 찾고 다음 옵션 중 하나를 선택하여 가상 컴퓨터에 연결합니다.

   a. (권장) 집중 모드에서 애플리케이션을 실행하려면 RStudio애플리케이션 시작을 선택합니다. 최근에 가상 컴퓨터에 연결하지 않은 경우 Lightsail for Research에서 세션을 준비하는 동안 몇 분 정도 기다려야 할 수 있습니다.



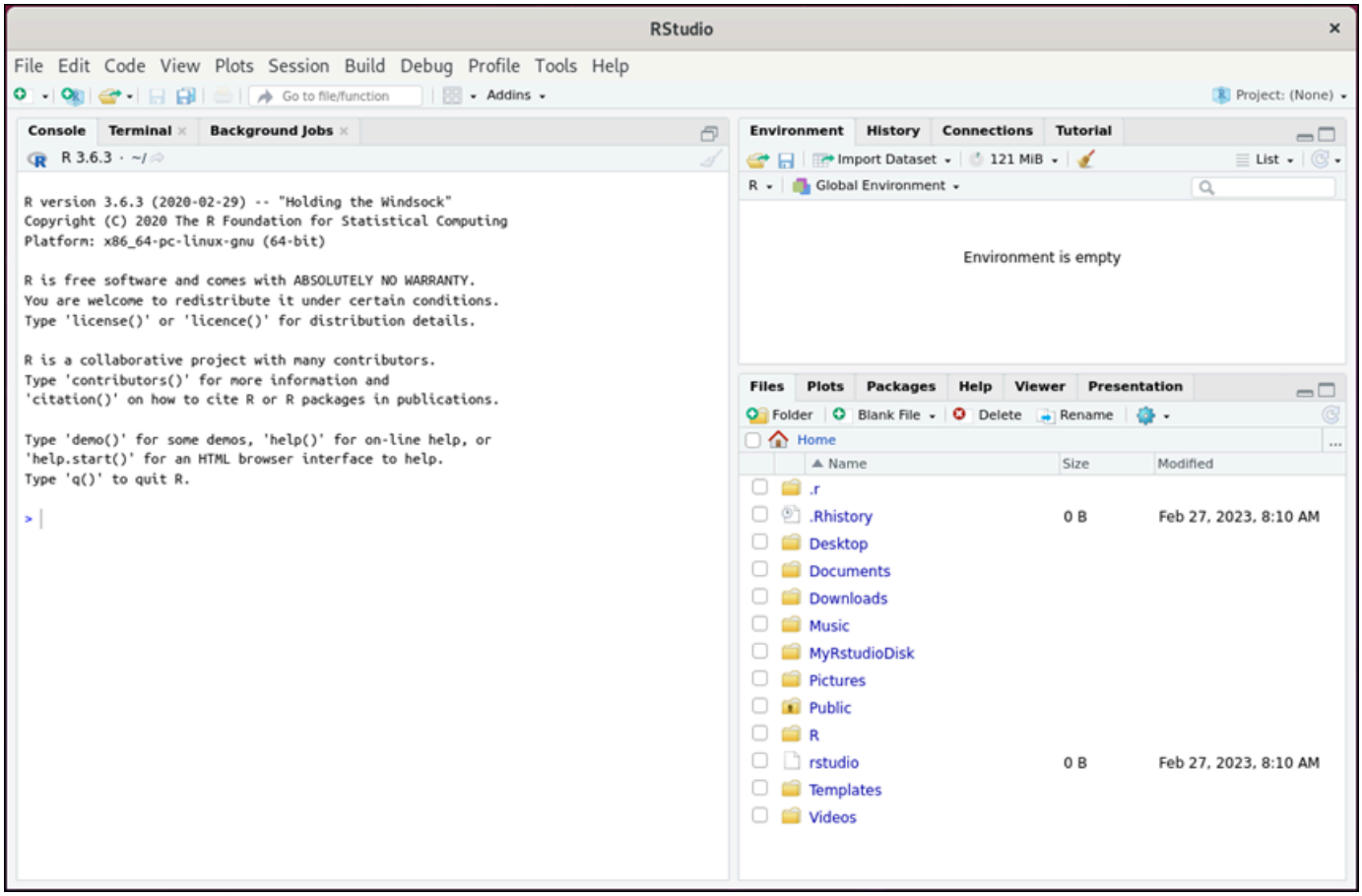
b. 컴퓨터의 드롭다운 메뉴를 선택한 다음 운영 체제 액세스를 선택하여 가상 컴퓨터의 데스크톱에 접근합니다. 운영 체제에 다른 애플리케이션을 설치하려면 이렇게 하세요.



연구용 Lightsail은 몇 가지 명령을 실행하여 원격 디스플레이 프로토콜 연결을 시작합니다. 잠시 후 가상 컴퓨터에 가상 데스크톱 연결이 설정된 새 브라우저 탭 창이 열립니다. 애플리케이션 실행 옵션을 선택한 경우 이 절차의 다음 단계를 계속 진행하여 애플리케이션에서 파일을 엽니다. RStudio 운영 체제 액세스 옵션을 선택한 경우 Ubuntu 데스크톱을 통해 다른 애플리케이션을 열 수 있습니다.

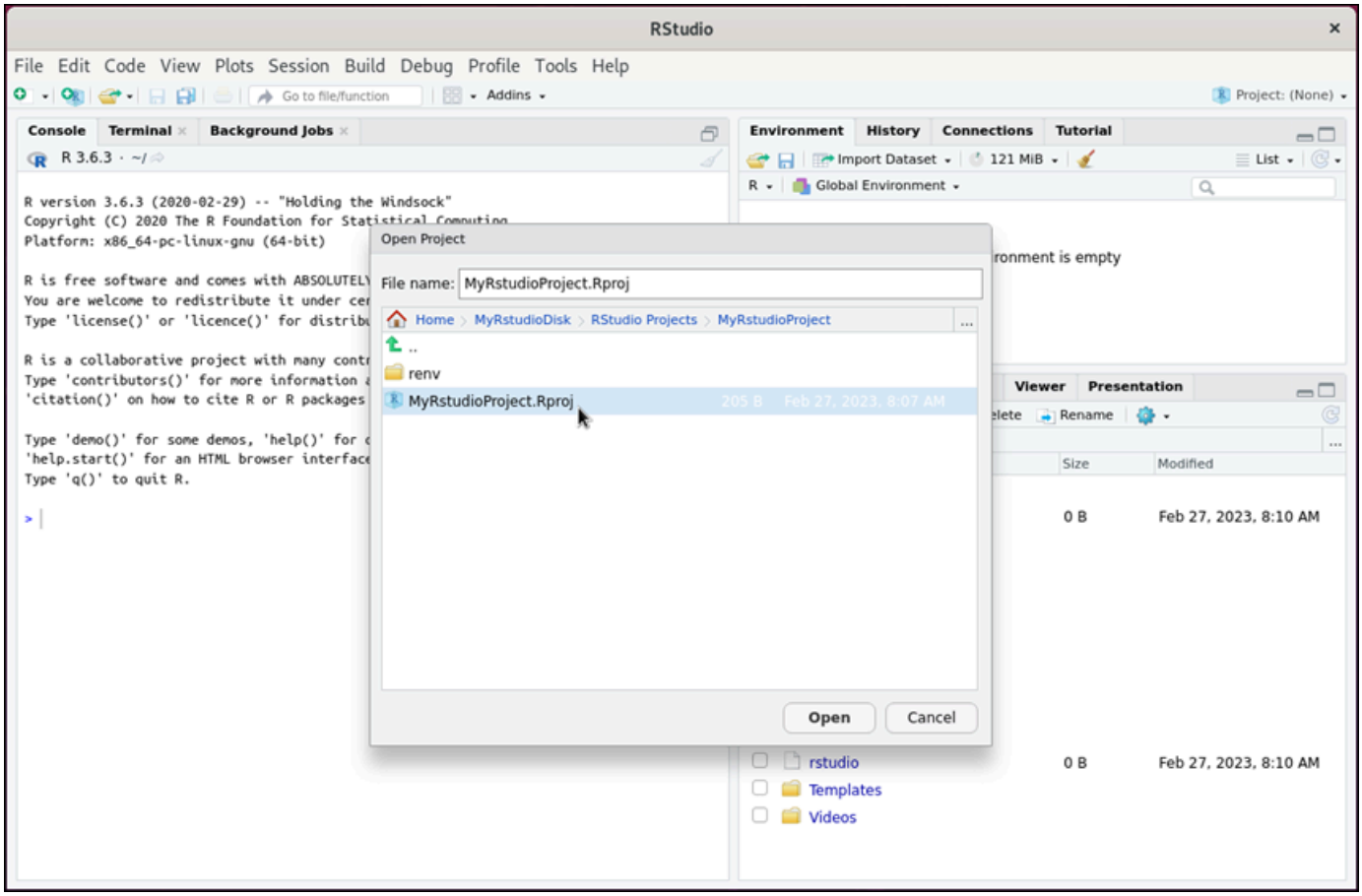
> **Note**
>
> 브라우저에서 클립보드 공유를 승인하라는 메시지가 표시될 수 있습니다. 이렇게 하면 로컬 컴퓨터와 가상 컴퓨터 간에 복사하여 붙여넣을 수 있습니다.
> Ubuntu에서 초기 설정을 묻는 메시지가 표시될 수도 있습니다. 지시에 따라 설정을 완료하고 운영 체제를 사용할 수 있습니다.

4. RStudio애플리케이션이 열립니다.

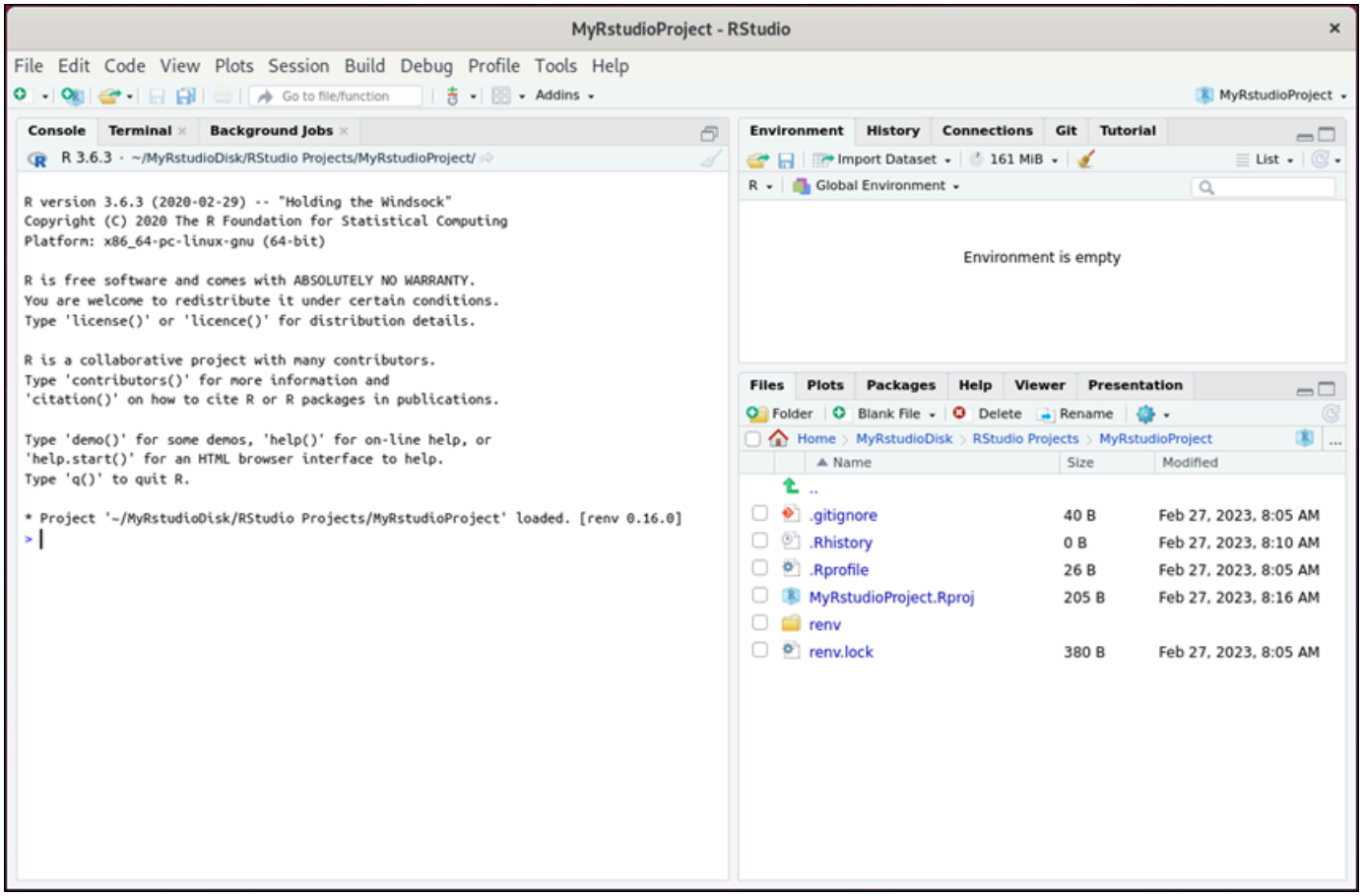


5. 에서 RStudio 프로젝트를 열려면 파일 메뉴를 선택한 다음 프로젝트 열기를 선택합니다. 프로젝트 파일이 저장된 디렉터리 또는 폴더를 탐색합니다. 그런 후 파일을 선택하여 엽니다.

   연결된 디스크에 프로젝트 파일을 업로드한 경우 디스크가 마운트된 디렉터리를 찾습니다. 기본적으로 연구용 Lightsail은 디렉터리에 디스크를 마운트합니다. `/home/lightsail-user/<disk-name>` `<disk-name>`디스크에 지정한 이름입니다. 다음 예제에서 `MyRstudioDisk` 디렉토리는 마운트된 디스크를 나타내며, `Projects` 하위 디렉토리는 RStudio 프로젝트 파일을 포함합니다.



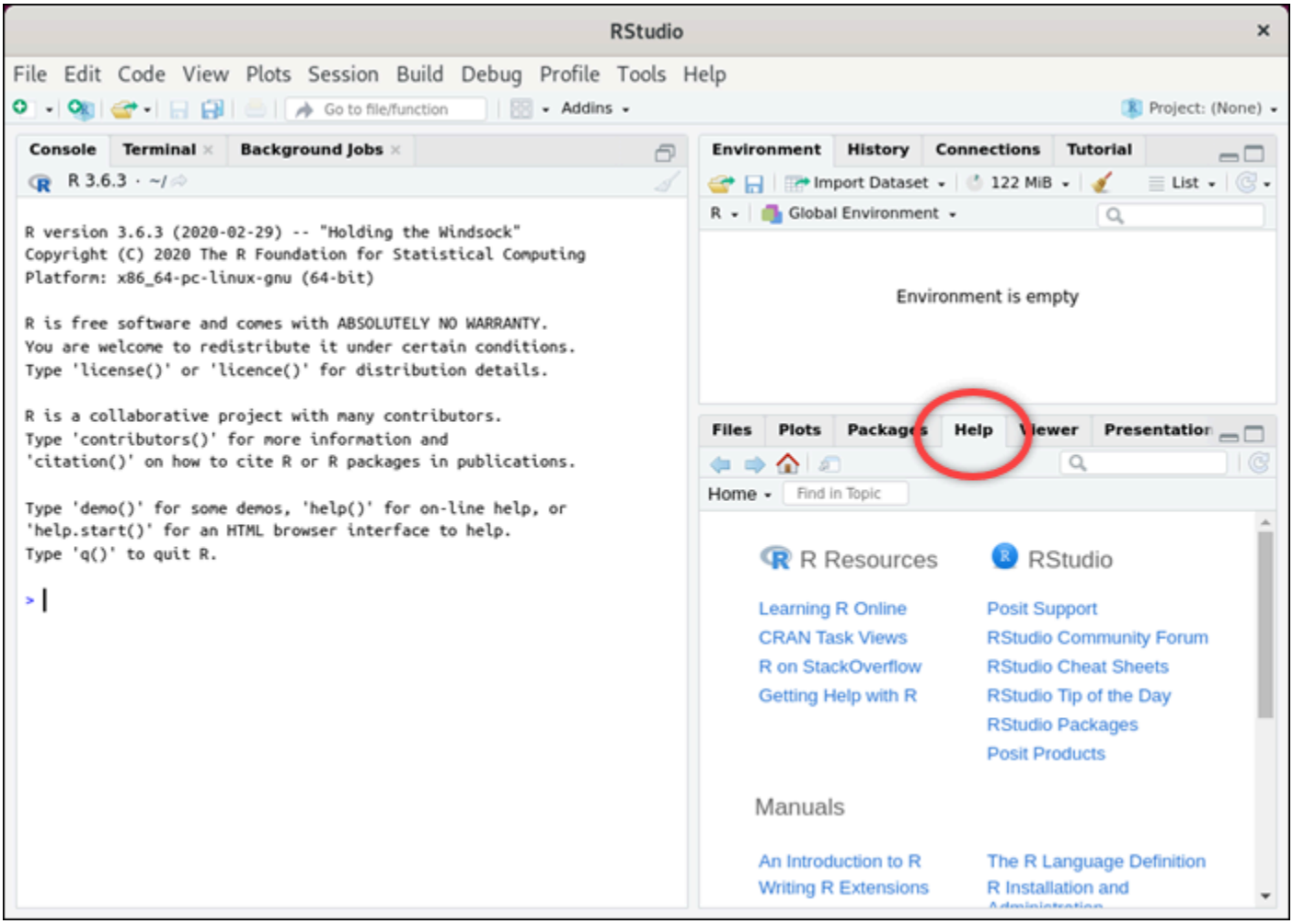
다음 예제에서는 `MyRstudioProject.Rproj` 프로젝트 파일을 열었습니다.



시작하는 RStudio 방법에 대한 자세한 내용은 이 튜토리얼의 5단계: RStudio 설명서 읽기 섹션을 계속 참조하십시오.

5단계: RStudio 설명서 읽기

RStudio애플리케이션은 포괄적인 설명서 패키지와 함께 번들로 제공됩니다. 학습을 RStudio 시작하려면 다음 예제와 RStudio 같이 도움말 탭에 액세스하는 것이 좋습니다.



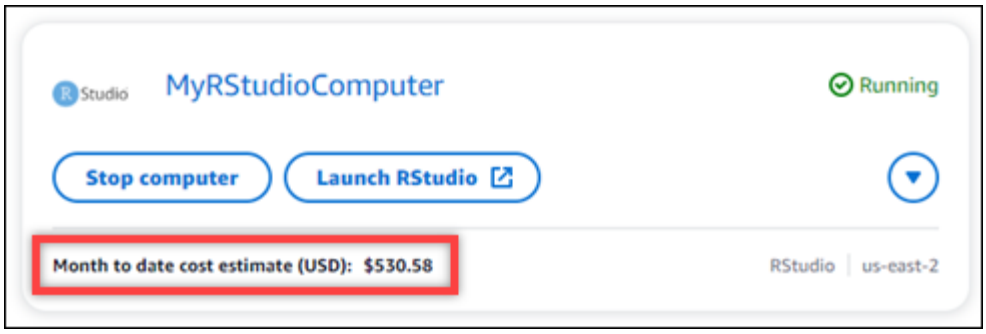
다음과 같은 RStudio 온라인 리소스도 사용할 수 있습니다.

- R 온라인 학습
- R on StackOverflow
- R로 도움말 보기
- Posit 지원
- RStudio커뮤니티 포럼
- RStudio치트 시트
- RStudio팁 오브 더 데이 (트위터)
- RStudio패키지

6단계: (옵션) 사용량 및 비용 모니터링

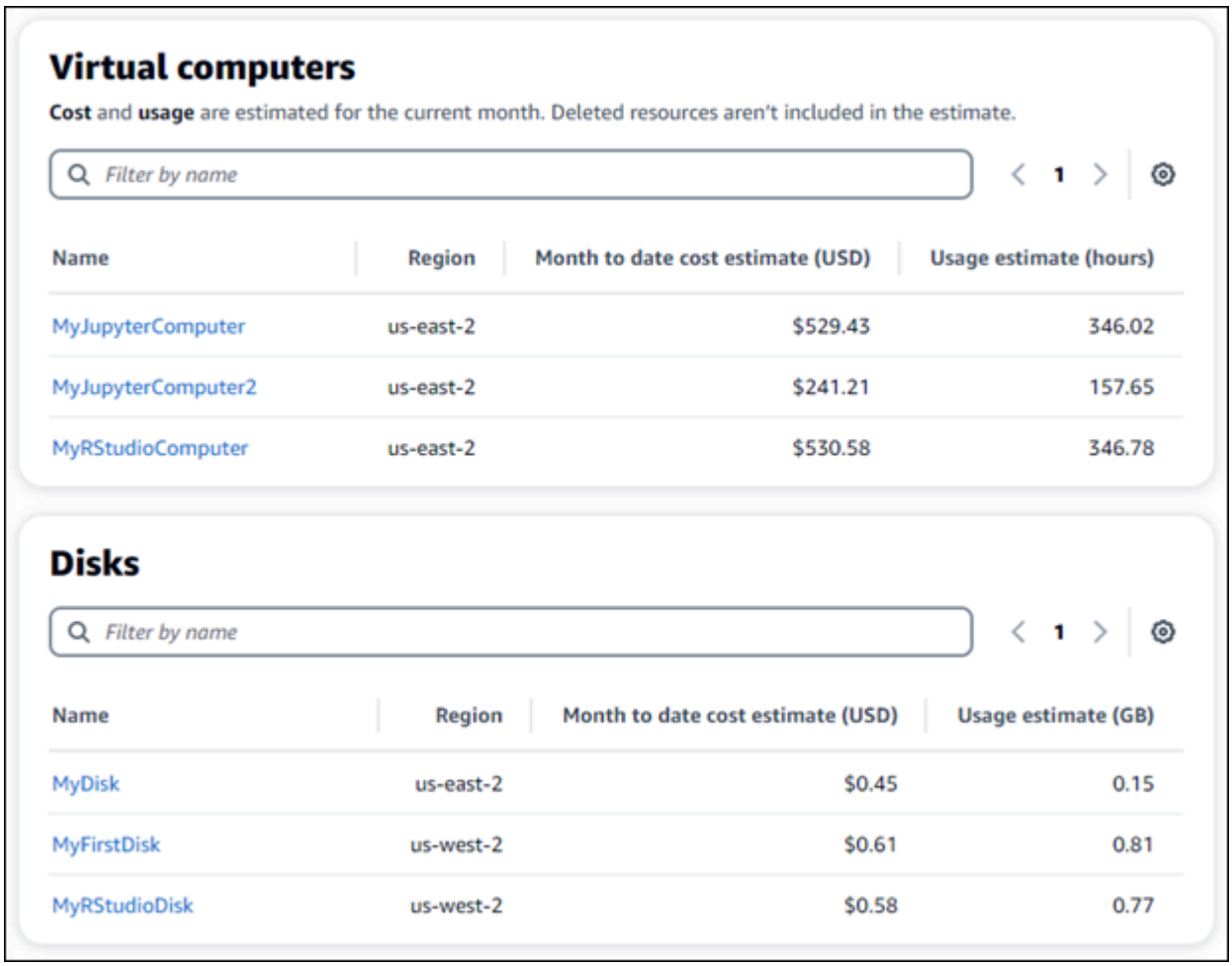
연구용 Lightsail 리소스의 월간 누계 비용 및 사용량 추정치는 연구용 Lightsail 콘솔의 다음 영역에 표시됩니다.

1. 연구용 Lightsail 콘솔의 탐색 창에서 가상 컴퓨터를 선택합니다. 실행 중인 각 가상 컴퓨터 아래에 가상 컴퓨터의 월 누계 예상 비용이 나열됩니다.



2. 가상 컴퓨터의 CPU 사용률을 보려면 가상 컴퓨터의 이름을 선택한 다음 대시보드 탭을 선택합니다.

3. 모든 Lightsail for Research 리소스의 월간 누계 비용 및 예상 사용량을 보려면 탐색 창에서 사용량을 선택합니다.



7단계: (옵션) 비용 관리 규칙 생성

비용 관리 규칙을 생성하여 가상 컴퓨터의 사용량과 비용을 관리합니다. 지정된 기간 동안 CPU 사용률이 지정된 비율에 도달하면 실행 중인 컴퓨터를 중지하는 유휴 상태에서 가상 컴퓨터 중지 규칙을 만들 수 있습니다. 예를 들어, 규칙은 30분 동안 특정 컴퓨터의 CPU 사용률이 5% 이하일 때 자동으로 중지할 수 있습니다. 이는 컴퓨터가 유휴 상태이고 Lightsail for Research가 컴퓨터를 중지하여 유휴 리소스에 대한 요금이 발생하지 않음을 의미할 수 있습니다.

> **Important**
>
> 유휴 상태인 가상 컴퓨터를 중지하는 규칙을 만들기 전에 며칠 동안 사용률을 CPU 모니터링하는 것이 좋습니다. 가상 컴퓨터의 부하가 서로 다를 때의 CPU 사용률을 기록해 두십시오. 예를 들어, 코드를 컴파일하고, 작업을 처리하고, 유휴 상태인 경우가 있습니다. 이렇게 하면 규칙의 정확한 임계값을 결정하는 데 도움이 됩니다. 자세한 내용은 이 자습서의 6단계: (옵션) 사용량 및 비용 모니터링 섹션을 참조하세요.

CPU사용률 임계값이 워크로드보다 높은 규칙을 만들면 규칙으로 인해 가상 컴퓨터가 연속적으로 중지될 수 있습니다. 예를 들어, 규칙에 의해 중지된 후 바로 가상 컴퓨터를 시작하면 규칙이 다시 활성화되고 컴퓨터가 다시 중지됩니다.

비용 관리 규칙의 생성 및 관리에 대한 자세한 지침은 다음 가이드에서 확인할 수 있습니다.

- 연구용 Lightsail에서 비용 관리 규칙을 관리합니다.
- 연구용 Lightsail 가상 컴퓨터에 대한 비용 관리 규칙 생성
- 연구용 Lightsail 가상 컴퓨터의 비용 관리 규칙을 삭제합니다.

8단계: (옵션) 스냅샷 생성

스냅샷은 데이터의 point-in-time 복사본입니다. 가상 컴퓨터의 스냅샷을 생성하고 이를 기준으로 사용하여 새 컴퓨터를 생성하거나 데이터 백업을 할 수 있습니다. 스냅샷은 스냅샷을 생성한 시점부터 컴퓨터를 복원하는 데 필요한 모든 데이터를 포함합니다.

스냅샷 생성 및 관리에 대한 자세한 지침은 다음 가이드에서 확인할 수 있습니다.

- 연구용 Lightsail 가상 컴퓨터 또는 디스크의 스냅샷 생성
- 연구용 Lightsail에서 가상 컴퓨터 및 디스크 스냅샷 보기 및 관리
- 스냅샷에서 가상 컴퓨터 또는 디스크 만들기
- 연구용 Lightsail 콘솔에서 스냅샷을 삭제합니다.

9단계: (옵션) 가상 컴퓨터 중지 또는 삭제

이 자습서용으로 생성한 가상 컴퓨터 작업을 마친 후에는 가성 컴퓨터를 삭제할 수 있습니다. 이렇게 하면 필요하지 않은 가상 컴퓨터에 대한 요금이 더 이상 부과되지 않습니다.

가상 컴퓨터를 삭제해도 관련 스냅샷이나 연결된 디스크는 삭제되지 않습니다. 스냅샷과 디스크를 생성한 경우 해당 스냅샷과 디스크를 수동으로 삭제하여 요금이 부과되지 않도록 해야 합니다.

나중에 사용할 수 있도록 가상 컴퓨터를 저장하되 표준 시간당 요금으로 요금이 부과되지 않도록 하려면 가상 컴퓨터를 삭제하는 대신 중지하면 됩니다. 그런 다음 나중에 다시 시작할 수 있습니다. 자세한 내용은 연구용 Lightsail 가상 컴퓨터 세부 정보 보기 단원을 참조하십시오. 요금에 대한 자세한 내용은 연구용 Lightsail 요금을 참조하십시오.

> **Important**
>
> 연구용 Lightsail 리소스 삭제는 영구적인 조치입니다. 삭제된 데이터는 복구할 수 없습니다. 나중에 데이터가 필요할 수 있는 경우 삭제하기 전에 가상 컴퓨터의 스냅샷을 생성합니다. 자세한 내용은 스냅샷 생성을 참조하세요..

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 가상 컴퓨터를 선택합니다.
3. 삭제할 가상 컴퓨터를 선택합니다.
4. 작업을 선택한 다음 가상 컴퓨터 삭제를 선택합니다.
5. 텍스트 블록에 확인을 입력합니다. 그런 다음 가상 컴퓨터 삭제를 선택합니다

연구용 Lightsail에서 가상 컴퓨터를 만들고 관리합니다.

연구용 Amazon Lightsail을 사용하면 가상 컴퓨터를 만들 수 있습니다. AWS 클라우드

가상 컴퓨터를 만들 때는 사용할 애플리케이션과 하드웨어 요금제를 선택합니다. 가상 컴퓨터에 대한 지출 한도를 설정하고 가상 컴퓨터가 해당 한도에 도달했을 때 어떤 일이 발생할지 선택할 수 있습니다. 예를 들어, 구성된 예산을 초과하여 요금이 부과되지 않도록 가상 컴퓨터를 자동으로 중지하도록 선택할 수 있습니다.

> **Important**
>
> 2024년 3월 22일부터 연구용 Lightsail 가상 컴퓨터가 기본적으로 적용됩니다. IMDSv2

주제

연구용 Lightsail의 애플리케이션 이미지 및 하드웨어 플랜 선택

Amazon Lightsail for Research 가상 컴퓨터를 생성할 때는 애플리케이션과 이에 대한 하드웨어 플랜(플랜) 을 선택합니다.

애플리케이션은 소프트웨어 구성(예: 애플리케이션 및 운영 체제)을 제공합니다. 플랜은 개수, 메모리, 스토리지 공간, 월별 데이터 전송 vCPUs 허용량 등 가상 컴퓨터의 하드웨어를 제공합니다. 애플리케이션과 플랜이 함께 가상 컴퓨터 구성을 구성합니다.

> **Note**
>
> 가상 컴퓨터를 생성한 후에는 가상 컴퓨터의 애플리케이션 또는 플랜을 변경할 수 없습니다. 하지만 가상 컴퓨터의 스냅샷을 만든 다음 스냅샷에서 새 가상 컴퓨터를 만들 때 새 요금제를 선택할 수 있습니다. 스냅샷 복사에 대한 자세한 내용은 연구용 Lightsail 스냅샷을 사용하여 가상 컴퓨터 및 디스크를 백업합니다. 섹션을 참조하십시오

주제

애플리케이션

Amazon Lightsail for Research는 가상 컴퓨터를 시작하는 데 필요한 애플리케이션과 운영 체제가 포함된 머신 이미지를 제공하고 관리합니다. Lightsail for Research에서 가상 컴퓨터를 만들 때 응용 프로그램 목록에서 원하는 응용 프로그램을 선택합니다. 모든 Lightsail for Research 애플리케이션 이미지는 우분투 (Linux) 운영 체제를 사용합니다.

연구용 Lightsail에서 사용할 수 있는 응용 프로그램은 다음과 같습니다.

- JupyterLab— 노트북, 코드 및 데이터를 위한 웹 기반 통합 개발 환경 (IDE) JupyterLab 입니다. 유연한 인터페이스를 통해 데이터 과학, 과학 컴퓨팅, 컴퓨터 저널리즘 및 기계 학습의 워크플로를 구성하고 정렬할 수 있습니다. 자세한 내용은 Jupyter Project 설명서를 참조하세요.
- RStudio— 통계 컴퓨팅 및 그래픽을 위한 프로그래밍 언어인 R과 Python을 위한 오픈 소스 통합 개발 환경 (IDE) RStudio 입니다. 소스 코드 편집기, 빌드 자동화 도구, 디버거 뿐만 아니라 플로팅 및 작업 공간 관리를 위한 도구도 결합합니다. 자세한 내용은 를 참조하십시오. RStudioIDE
- VSCodium— VSCodium Microsoft 에디터 VS Code의 커뮤니티 기반 바이너리 배포판입니다. 자세한 내용은 VSCodium를 참조하세요.
- Scilab - Scilab은 오픈 소스 수치 계산 패키지이자 높은 수준의 수치 지향 프로그래밍 언어입니다. 자세한 내용은 Scilab. 섹션을 참조하세요.
- 우분투 20.04 LTS — 우분투는 데비안 기반의 오픈소스 리눅스 배포판입니다. 간결하고 빠르며 강력한 Ubuntu Server는 안정적이고 예측 가능하며 경제적으로 서비스를 제공합니다. 가상 컴퓨터를 구축할 수 있는 훌륭한 기반입니다. 자세한 내용은 Ubuntu 릴리스를 참조하세요.

계획

플랜은 하드웨어 사양을 제공하고 Lightsail for Research 가상 컴퓨터의 가격을 결정합니다. 요금제에는 고정된 양의 메모리 (RAM), 컴퓨팅 (vCPUs), SSD 기반 스토리지 볼륨 (디스크) 공간 및 월별 데이터 전송 허용량이 포함됩니다. 플랜은 시간당 온디맨드 기준으로 청구되므로 가상 컴퓨터가 실행되는 시간에 대해서만 비용을 지불하면 됩니다.

선택한 플랜은 워크로드에 필요한 리소스에 따라 다를 수 있습니다. 연구용 Lightsail은 다음과 같은 플랜 유형을 제공합니다.

- 표준 – 표준 플랜은 컴퓨팅에 최적화되어 있으며 고성능 프로세서의 이점을 활용하는 컴퓨팅 기반 애플리케이션에 적합합니다.
- GPU— GPU 플랜은 범용 GPU 컴퓨팅을 위한 비용 효율적인 고성능 플랫폼을 제공합니다. 이러한 플랜을 사용하여 과학, 공학, 렌더링 애플리케이션 및 워크로드를 가속화할 수 있습니다.

표준 플랜

다음은 연구용 Lightsail에서 사용할 수 있는 표준 플랜의 하드웨어 사양입니다.

플랜 이름	vCPUs	메모리	스토리지 공간	월간 데이터 전송 허용량
표준 XL	4	8GB	50GB	512GB
표준 2XL	8	16 GB	50GB	512GB
표준 4XL	16	32GB	50GB	512GB

GPU플랜

다음은 연구용 Lightsail에서 사용할 수 있는 GPU 플랜의 하드웨어 사양입니다.

플랜 이름	vCPUs	메모리	스토리지 공간	월간 데이터 전송 허용량
GPUXL	4	16 GB	50GB	1TB

GPU2XL	8	32GB	50GB	1TB
GPU4XL	16	64GB	50GB	1TB

연구용 Lightsail 가상 컴퓨터 만들기

애플리케이션을 실행하는 Lightsail for Research 가상 컴퓨터를 만들려면 다음 단계를 완료하십시오.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 홈페이지에서 가상 컴퓨터 만들기를 선택합니다.
3. 실제 위치 근처에 있는 가상 AWS 리전 컴퓨터용 서버를 선택하십시오.
4. 애플리케이션 및 하드웨어 플랜을 선택합니다. 자세한 내용은 연구용 Lightsail의 애플리케이션 이미지 및 하드웨어 플랜 선택 단원을 참조하십시오.
5. 가상 컴퓨터의 이름을 입력합니다. 유효한 문자에는 영숫자, 숫자, 마침표, 하이픈, 밑줄이 포함됩니다.

   가상 컴퓨터 이름은 다음 요구 사항도 충족해야 합니다.

   - 연구용 Lightsail AWS 리전 계정에서 각 계정마다 고유해야 합니다.
   - 2–255자로 구성되어야 합니다.
   - 영숫자 문자 또는 숫자로 시작하고 끝나야 합니다.
6. 요약 패널에서 가상 컴퓨터 만들기를 선택합니다.

몇 분 안에 Lightsail for Research 가상 컴퓨터가 준비되고 그래픽 사용자 인터페이스 GUI () 세션을 통해 연결할 수 있습니다. 연구용 Lightsail 가상 컴퓨터에 연결하는 방법에 대한 자세한 내용은 을 참조하십시오. 연구용 Lightsail 가상 컴퓨터 애플리케이션에 액세스

> **Important**
>
> 새로 만든 가상 컴퓨터에는 기본적으로 방화벽 포트 집합이 열려 있습니다. 이러한 포트에 대한 자세한 내용은 연구용 Lightsail 가상 컴퓨터의 방화벽 포트 관리 섹션을 참조하세요.

연구용 Lightsail 가상 컴퓨터 세부 정보 보기

다음 단계를 완료하여 Lightsail for Research 계정에서 가상 컴퓨터 목록과 세부 정보를 확인하십시오.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 가상 컴퓨터를 선택하면 계정의 가상 컴퓨터 목록이 표시됩니다.

가상 컴퓨터의 이름을 선택하여 해당 관리 페이지로 이동합니다. 관리 페이지에서 제공하는 정보는 다음과 같습니다.

- 가상 컴퓨터 이름 - 가상 컴퓨터의 이름입니다.
- 상태 - 가상 컴퓨터에는 다음 상태 코드 중 하나가 있을 수 있습니다.
  - [생성 중]
  - 실행 중
  - Stopping(중지 중)
  - Stopped(중지됨)
  - 알 수 없음
- AWS 리전— 가상 AWS 리전 컴퓨터가 에서 생성되었습니다.
- 애플리케이션 및 하드웨어 - 가상 컴퓨터의 애플리케이션 및 하드웨어 플랜입니다.
- 월별 예상 사용량 - 현재 청구 주기 동안 이 가상 컴퓨터의 시간당 예상 사용량입니다.
- 월간 누계 예상 비용 — 이번 청구 주기 동안의 가상 컴퓨터 예상 비용 (인치USD) 입니다.
- 대시보드 - 대시보드 탭에서 세션을 시작하여 가상 컴퓨터의 애플리케이션에 액세스할 수 있습니다. CPU사용률도 볼 수 있습니다. CPU사용률은 가상 컴퓨터 응용 프로그램에서 사용하는 처리 능력을 식별합니다. 그래프에 표시된 각 데이터 포인트는 일정 기간 동안의 평균 CPU 사용률을 나타냅니다.
- 비용 관리 규칙 - 가상 컴퓨터의 사용 및 비용을 관리하는 데 도움이 되도록 정의하는 규칙입니다.
- 가상 컴퓨터 사용 - 지정된 청구 주기의 예상 비용 및 사용량 추정치입니다. 날짜 및 시간을 기준으로 필터링할 수 있습니다.
- 스토리지 - 스토리지 탭에서 가상 컴퓨터 디스크를 생성, 연결 및 분리합니다. 디스크는 가상 컴퓨터에 연결하고 하드 드라이브로 마운트할 수 있는 스토리지 볼륨입니다.
- 태그 - 태그 탭에서 가상 컴퓨터 태그를 관리합니다. 태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 키와 값(선택 사항)으로 구성됩니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 AWS 비용을 추적할 수 있습니다.

연구용 Lightsail 가상 컴퓨터 애플리케이션에 액세스

다음 단계를 완료하여 Lightsail for Research 가상 컴퓨터에서 실행 중인 애플리케이션을 시작하십시오.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 가상 컴퓨터를 선택합니다.
3. 애플리케이션을 실행하려는 가상 컴퓨터의 이름을 찾습니다.

> **Note**
>
> 가상 컴퓨터가 중지된 경우 먼저 컴퓨터 시작 버튼을 선택하여 켭니다.

4. 애플리케이션 시작을 선택합니다. 예: 실행. JupyterLab 애플리케이션 세션이 새 웹 브라우저 창에서 열립니다.

> **Important**
>
> 웹 브라우저에 팝업 차단기가 설치되어 있는 경우 세션을 열기 전에 aws.amazon.com 도메인의 팝업을 허용해야 할 수 있습니다.

연구용 Lightsail 가상 컴퓨터의 운영 체제에 액세스

다음 단계를 완료하여 Lightsail for Research 가상 컴퓨터의 운영 체제에 액세스하십시오.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 가상 컴퓨터를 선택합니다.
3. 가상 컴퓨터의 이름을 찾은 다음 컴퓨터 상태 아래에 있는 작업 버튼 드롭다운을 선택합니다.

> **Note**
>
> 가상 컴퓨터가 중지된 경우 먼저 시작 버튼을 선택하여 켭니다.

4. Access 운영 체제를 선택합니다. 새 브라우저 창에 운영 체제 세션이 열립니다.

> **Important**
>
> 웹 브라우저에 팝업 차단기가 설치되어 있는 경우 세션을 열기 전에 aws.amazon.com 도메인에서 팝업을 허용해야 할 수 있습니다.

연구용 Lightsail 가상 컴퓨터의 방화벽 포트 관리

Amazon Lightsail for Research의 방화벽은 가상 컴퓨터에 연결할 수 있는 트래픽을 제어합니다. 프로토콜, 포트, 연결이 허용된 소스 IPv4 또는 IPv6 주소를 지정하는 규칙을 가상 컴퓨터의 방화벽에 추가합니다. 방화벽 규칙은 항상 허용적입니다. 따라서 액세스를 거부하는 규칙을 생성할 수 없습니다. 가상 컴퓨터의 방화벽에 규칙을 추가하여 트래픽이 가상 컴퓨터에 도달하도록 허용합니다. 각 가상 컴퓨터에는 두 개의 방화벽이 있습니다. 하나는 IPv4 주소용이고 다른 하나는 IPv6 주소용입니다. 두 방화벽은 서로 독립적이며 인스턴스로 들어오는 트래픽을 필터링하는 사전 구성된 규칙 세트를 포함합니다.

프로토콜

프로토콜은 두 컴퓨터 간에 데이터가 전송되는 형식입니다. 방화벽 규칙에 다음 프로토콜을 지정할 수 있습니다.

- 전송 제어 프로토콜 (TCP) 은 주로 클라이언트와 가상 컴퓨터에서 실행되는 응용 프로그램 간의 연결을 설정하고 유지하는 데 사용됩니다. 이 프로토콜은 널리 사용되는 프로토콜이며 방화벽 규칙에서 자주 지정할 수 있습니다.
- 사용자 데이터그램 프로토콜 (UDP) 은 주로 클라이언트와 가상 컴퓨터에서 실행되는 응용 프로그램 간에 지연 시간이 짧고 손실 허용 가능한 연결을 설정하는 데 사용됩니다. 게임, 음성 및 비디오 통신과 같이 인식되는 지연 시간이 중요한 네트워크 애플리케이션에 적합합니다.
- 인터넷 제어 메시지 프로토콜 (ICMP) 은 데이터가 적시에 의도한 목적지에 도달하고 있는지 확인하는 등 네트워크 통신 문제를 진단하는 데 주로 사용됩니다. 로컬 컴퓨터와 가상 컴퓨터 간의 연결 속도를 테스트하는 데 사용할 수 있는 Ping 유틸리티에 적합합니다. 데이터가 가상 컴퓨터에 도달한 후 로컬 컴퓨터로 돌아오는 데 걸리는 시간을 보고합니다.
- 모두는 모든 프로토콜 트래픽이 가상 컴퓨터로 유입되도록 허용하는 데 사용됩니다. 지정할 프로토콜을 잘 모르는 경우 이 프로토콜을 지정합니다. 여기에서 지정된 프로토콜뿐만 아니라 모든 인터넷 프로토콜이 포함됩니다. 자세한 내용은 Internet Assigned Numbers Authority 웹 사이트의 Protocol Numbers를 참조하세요.

포트

컴퓨터가 키보드 및 포인트와 같은 주변 장치와 통신할 수 있는 컴퓨터의 물리적 포트와 마찬가지로, 방화벽 포트는 가상 컴퓨터의 인터넷 통신 엔드포인트 역할을 합니다. 클라이언트가 가상 컴퓨터에 연결하려고 할 때 통신을 설정하기 위해 포트를 노출합니다.

방화벽 규칙에서 지정할 수 있는 포트의 범위는 0에서 65535 사이입니다. 클라이언트가 가상 컴퓨터와 연결할 수 있도록 하는 방화벽 규칙을 만들 경우 사용할 프로토콜을 지정합니다. 또한 연결을 설정할 때 사용하는 포트 번호와 연결을 설정할 수 있는 IP 주소를 지정합니다.

새로 만든 가상 컴퓨터에는 기본적으로 다음 포트가 열립니다.

- TCP
  - 22 - 보안 셸 (SSH) 에 사용됩니다.
  - 80 - 하이퍼텍스트 전송 프로토콜 (HTTP) 에 사용됩니다.
  - 443 - 하이퍼텍스트 전송 프로토콜 보안 () 에 사용됩니다. HTTPS
  - 8443 - 하이퍼텍스트 전송 프로토콜 보안 () 에 사용됩니다. HTTPS

포트를 열고 닫는 이유

포트를 열면 클라이언트가 가상 컴퓨터와 연결을 설정할 수 있습니다. 포트를 닫으면 가상 컴퓨터에 대한 연결이 차단됩니다. 예를 들어 SSH 클라이언트가 가상 컴퓨터에 연결할 수 있도록 하려면 연결을 설정해야 하는 컴퓨터의 IP 주소에서만 포트 22를 TCP 통한 연결을 허용하는 방화벽 규칙을 구성합니다. 이 경우에는 어떤 IP 주소로도 가상 컴퓨터에 SSH 연결되도록 허용하지 않는 것이 좋습니다. 연결을 허용하면 보안 위험이 발생할 수 있습니다. 인스턴스의 방화벽에 이 규칙이 이미 구성되어 있는 경우 이를 삭제하여 SSH 클라이언트가 가상 컴퓨터에 연결하는 것을 차단할 수 있습니다.

다음 절차는 가상 컴퓨터에 현재 열려 있는 포트를 가져오고, 새 포트를 열고, 포트를 닫는 방법을 보여줍니다.

주제

사전 조건 완료

시작하기 전에 다음 사전 조건을 완료합니다.

- 연구용 Lightsail에서 가상 컴퓨터를 만드세요. 자세한 내용은 연구용 Lightsail 가상 컴퓨터 만들기 단원을 참조하십시오.
- AWS Command Line Interface ()AWS CLI를 다운로드하고 설치합니다. 자세한 내용은 AWS Command Line Interface 버전 2 사용 설명서의 AWS CLI최신 버전의 설치 또는 업데이트를 참조하세요.
- 에 AWS CLI 액세스하도록 구성합니다 AWS 계정. 자세한 내용은 AWS Command Line Interface 버전 2 사용 설명서의 구성 기초 섹션을 참조하세요.

가상 컴퓨터의 포트 상태를 가져옵니다.

가상 컴퓨터의 포트 상태를 가져오려면 다음 절차를 완료합니다. 이 절차에서는 `get-instance-port-states` AWS CLI 명령을 사용하여 특정 Lightsail for Research 가상 컴퓨터의 방화벽 포트 상태, 포트를 통해 가상 컴퓨터에 연결할 수 있는 IP 주소 및 프로토콜을 확인합니다. 자세한 내용은 AWS CLI 명령 get-instance-port-states참조를 참조하십시오.

1. 이 단계는 로컬 컴퓨터의 운영 체제에 따라 결정됩니다.
   - 로컬 컴퓨터에서 Windows 운영 체제를 사용하는 경우 명령 프롬프트 창을 엽니다.
   - 로컬 컴퓨터에서 Linux 또는 Unix 기반 운영 체제(macOS 포함)를 사용하는 경우 터미널 창을 엽니다.
2. 다음 명령을 입력하여 방화벽 포트 상태와 허용된 IP 주소 및 프로토콜을 가져옵니다. 명령에서 가상 컴퓨터를 만든 AWS 리전의 코드(예: `us-east-2`)로 *REGION*을 바꿉니다. 가상 컴퓨터의 이름으로 *NAME*을 바꿉니다.

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

   예

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

   응답에는 열린 포트와 프로토콜, 가상 컴퓨터에 연결할 수 있는 IP CIDR 범위가 표시됩니다.

```
[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
```

포트를 여는 방법에 대한 자세한 내용은 다음 섹션을 참조하세요.

가상 컴퓨터용 포트 열기

가상 컴퓨터용 포트를 열려면 다음 절차를 완료합니다. 이 절차에서는 `open-instance-public-ports` AWS CLI 명령을 사용합니다. 방화벽 포트를 열어 신뢰할 수 있는 IP 주소 또는 IP 주소 범위에서 연결을 구성하도록 합니다. 예를 들어, IP 주소 `192.0.2.44`를 허용하려면 `192.0.2.44` 또는 `192.0.2.44/32`를 지정합니다. IP 주소 `192.0.2.0~192.0.2.255`를 허용하려면 `192.0.2.0/24`를 지정합니다. 자세한 내용은 AWS CLI 명령 참조서를 참조하십시오 open-instance-public-ports.

1. 이 단계는 로컬 컴퓨터의 운영 체제에 따라 결정됩니다.
   - 로컬 컴퓨터에서 Windows 운영 체제를 사용하는 경우 명령 프롬프트 창을 엽니다.
   - 로컬 컴퓨터에서 Linux 또는 Unix 기반 운영 체제(macOS 포함)를 사용하는 경우 터미널 창을 엽니다.
2. 다음 명령을 입력하여 포트를 엽니다.

   명령에서 다음 항목을 바꿉니다.

   - 가상 컴퓨터를 만든 AWS 지역의 코드 (예:) *REGION* 로 `us-east-2` 바꾸십시오.
   - 가상 컴퓨터의 이름으로 *NAME*을 바꿉니다.
   - 열려는 포트 범위의 첫 번째 포트로 *FROM-PORT*을 바꿉니다.
   - IP 프로토콜 이름으로 *PROTOCOL*을 바꿉니다. 예를 들어,TCP.
   - 열려는 포트 범위의 마지막 포트로 *TO-PORT*을 바꿉니다.
   - 가상 컴퓨터에 연결할 수 있도록 허용하려는 IP 주소 또는 IP 주소 범위로 *IP*을 바꿉니다.

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

예

```
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
```

응답에는 가상 컴퓨터에 연결할 수 있는 새로 추가된 포트, 프로토콜 및 IP CIDR 범위가 표시됩니다.

```
[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"
    }
}
```

포트를 닫는 방법에 대한 자세한 내용은 다음 섹션을 참조하세요.

가상 컴퓨터용 포트 닫기

가상 컴퓨터용 포트를 닫으려면 다음 절차를 완료합니다. 이 절차에서는 `close-instance-public-ports` AWS CLI 명령을 사용합니다. 자세한 내용은 AWS CLI 명령 참조서를 참조하십시오 close-instance-public-ports.

1. 이 단계는 로컬 컴퓨터의 운영 체제에 따라 결정됩니다.
   - 로컬 컴퓨터에서 Windows 운영 체제를 사용하는 경우 명령 프롬프트 창을 엽니다.
   - 로컬 컴퓨터에서 Linux 또는 Unix 기반 운영 체제(macOS 포함)를 사용하는 경우 터미널 창을 엽니다.
2. 포트를 닫으려면 다음 명령을 입력합니다.

명령에서 다음 항목을 바꿉니다.

- 가상 컴퓨터를 만든 AWS 지역의 코드 (예:) *REGION* 로 us-east-2 바꾸십시오.
- 가상 컴퓨터의 이름으로 *NAME*을 바꿉니다.
- 닫으려는 포트 범위의 첫 번째 포트로 *FROM-PORT*을 바꿉니다.
- IP 프로토콜 이름으로 *PROTOCOL*을 바꿉니다. 예를 들어,TCP.
- 닫으려는 포트 범위의 마지막 포트로 *TO-PORT*을 바꿉니다.
- 제거하려는 IP 주소 또는 IP 주소 범위로 *IP*을 바꿉니다.

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

예

```
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
```

응답에는 닫혀 더 이상 가상 컴퓨터에 연결할 수 없는 포트, 프로토콜 및 IP CIDR 범위가 표시됩니다.

```
[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"
    }
}
```

다음 단계로 이동합니다.

가상 컴퓨터의 방화벽 포트를 성공적으로 관리한 후 다음 추가 단계를 완료할 수 있습니다.

- 가상 컴퓨터의 키 페어를 가져옵니다. 키 페어를 사용하면 Open SSHTTY, Pu 및 Linux용 Windows 하위 시스템과 같은 다양한 SSH 클라이언트를 사용하여 연결을 설정할 수 있습니다. 자세한 내용은 연구용 Lightsail 가상 컴퓨터용 키 페어를 구매하세요 단원을 참조하십시오.
- 명령줄을 사용하여 가상 컴퓨터를 관리하는 SSH 데 사용합니다. 자세한 내용은 보안 복사를 사용하여 연구용 Lightsail 가상 컴퓨터로 파일 전송 단원을 참조하십시오.
- 를 사용하여 SCP 가상 컴퓨터에 연결하여 파일을 안전하게 전송합니다. 자세한 내용은 보안 복사를 사용하여 연구용 Lightsail 가상 컴퓨터로 파일 전송 단원을 참조하십시오.

연구용 Lightsail 가상 컴퓨터용 키 페어를 구매하세요

공개 키와 개인 키로 구성된 키 쌍은 Amazon Lightsail for Research 가상 컴퓨터에 연결할 때 신원을 증명하는 데 사용하는 보안 자격 증명 세트입니다. 공개 키는 Lightsail for Research의 각 가상 컴퓨터에 저장되며 개인 키는 로컬 컴퓨터에 보관됩니다. 개인 키를 사용하면 가상 컴퓨터에 보안 셸 프로토콜 (SSH) 을 안전하게 설정할 수 있습니다. 프라이빗 키를 소유하는 사람은 누구나 가상 컴퓨터에 연결할 수 있으므로 보안된 위치에 프라이빗 키를 저장해 두는 것이 중요합니다.

Amazon Lightsail 기본 키 쌍 DKP () 은 Lightsail 인스턴스 또는 연구용 Lightsail 가상 컴퓨터를 처음 생성할 때 자동으로 생성됩니다. 인스턴스 DKP 또는 가상 컴퓨터를 생성하는 각 AWS 지역마다 다릅니다. 예를 들어 미국 동부 (오하이오) 지역용 DKP Lightsail (us-east-2) 은 미국 동부 (오하이오) 에서 Lightsail 및 Lightsail for Research로 만든 컴퓨터 중 생성 당시 를 사용하도록 구성된 모든 컴퓨터에 적용됩니다. DKP Lightsail for Research는 사용자가 생성한 가상 컴퓨터에 DKP 의 공개 키를 자동으로 저장합니다. Lightsail 서비스에 API 전화를 걸어 DKP 언제든지 의 개인 키를 다운로드할 수 있습니다.

이 문서에서는 가상 DKP 컴퓨터용 코드를 구하는 방법을 보여줍니다. 를 설치한 후에는 Open DKP SSHTTY, Pu 및 Linux용 Windows 하위 시스템과 같은 다양한 SSH 클라이언트를 사용하여 연결을 설정할 수 있습니다. 또한 Secure Copy (SCP) 를 사용하여 로컬 컴퓨터에서 가상 컴퓨터로 파일을 안전하게 전송할 수 있습니다.

> **Note**
>
> 브라우저 기반 NICE DCV 클라이언트를 사용하여 가상 컴퓨터에 원격 디스플레이 프로토콜 연결을 설정할 수도 있습니다. NICEDCV연구용 Lightsail 콘솔에서 사용할 수 있습니다. 해당 RDP 클라이언트에서는 컴퓨터의 키 페어를 받을 필요가 없습니다. 자세한 내용은 연구용 Lightsail 가상 컴퓨터 애플리케이션에 액세스 및 연구용 Lightsail 가상 컴퓨터의 운영 체제에 액세스 단원을 참조하세요.

주제

사전 조건 완료

시작하기 전에 다음 사전 조건을 완료합니다.

- 연구용 Lightsail에서 가상 컴퓨터를 만드세요. 자세한 내용은 연구용 Lightsail 가상 컴퓨터 만들기 단원을 참조하십시오.
- AWS Command Line Interface ()AWS CLI를 다운로드하고 설치합니다. 자세한 내용은 AWS Command Line Interface 버전 2 사용 설명서의 AWS CLI최신 버전의 설치 또는 업데이트를 참조하세요.
- 에 AWS CLI 액세스하도록 구성합니다 AWS 계정. 자세한 내용은 AWS Command Line Interface 버전 2 사용 설명서의 구성 기초 섹션을 참조하세요.
- jq를 다운로드하여 설치합니다. 다음 절차에서 JSON 출력에서 키 쌍 세부 정보를 추출하는 데 사용되는 가볍고 유연한 명령줄 JSON AWS CLI프로세서입니다. jq 다운로드 및 설치에 대한 자세한 내용은 jq 웹 사이트의 jq 다운로드를 참조하세요.

가상 컴퓨터용 키 페어 가져오기

연구용 DKP Lightsail에서 가상 컴퓨터용 Lightsail을 다운로드하려면 다음 절차 중 하나를 완료하십시오.

Windows 로컬 컴퓨터를 사용하는 가상 컴퓨터의 키 페어 가져오기

이 절차는 로컬 컴퓨터에서 Windows 운영 체제를 사용하는 경우에 적용됩니다. 이 절차에서는 `download-default-key-pair` AWS CLI 명령을 사용하여 지역에 대한 DKP Lightsail을 가져옵니다. AWS 자세한 내용은 AWS CLI 명령 download-default-key-pair참조서를 참조하십시오.

1. 명령 프롬프트 창을 엽니다.
2. 특정 지역의 DKP Lightsail을 가져오려면 다음 명령을 입력합니다. AWS 이 명령은 정보를 `dkp-details.json` 파일에 저장합니다. 명령에서 가상 컴퓨터가 생성된 AWS 지역의 코드 (예:) *`region-code`* 로 바꿉니다. `us-east-2`

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

예

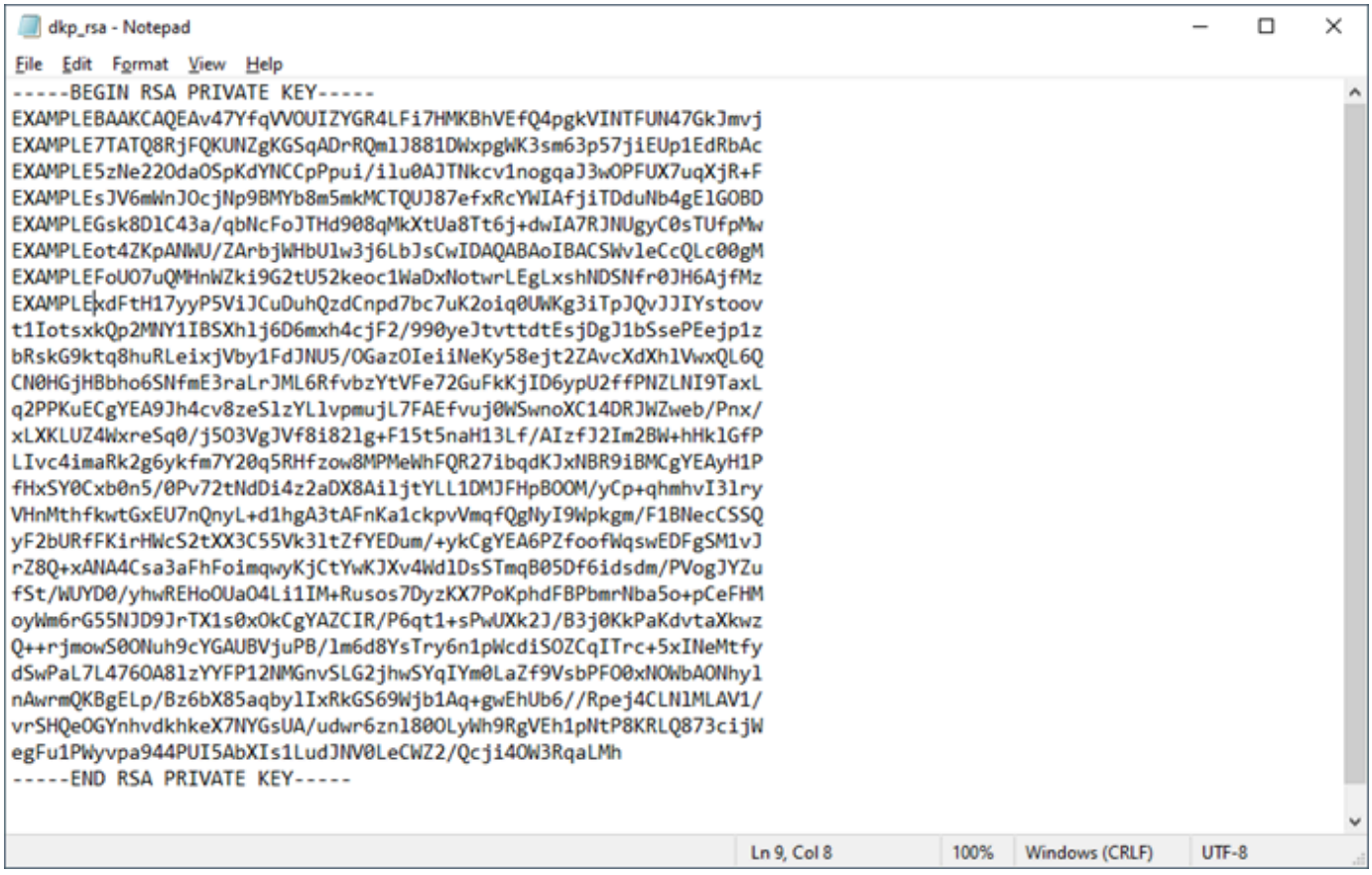
```
aws lightsail download-default-key-pair --region us-east-2 > dkp-details.json
```

명령에 대한 응답이 없습니다. dkp-details.json파일을 열고 DKP Lightsail 정보가 저장되었는지 확인하여 명령이 성공했는지 확인할 수 있습니다. dkp-details.json 파일 내용은 다음 예제와 같은 형식으로 보입니다. 파일이 비어 있어 명령이 실패했습니다.

3. 다음 명령을 입력하여 dkp-details.json 파일에서 프라이빗 키 정보를 추출하여 새 dkp_rsa 프라이빗 키 파일에 추가합니다.

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

명령에 대한 응답이 없습니다. dkp_rsa 파일을 열고 정보가 들어 있는지 확인하여 명령이 제대로 실행되었는지 확인할 수 있습니다. dkp_rsa 파일 내용은 다음 예제와 같은 형식으로 보입니다. 파일이 비어 있어 명령이 실패했습니다.



이제 가상 컴퓨터에 SSH OR SCP 연결을 설정하는 데 필요한 개인 키가 생겼습니다. 다음 추가 단계를 보려면 다음 섹션을 계속 진행합니다.

Linux, Unix 또는 macOS 로컬 컴퓨터를 사용하는 가상 컴퓨터의 키 페어 가져오기

이 절차는 로컬 컴퓨터가 Linux, Unix 또는 macOS 운영 체제를 사용하는 경우에 적용됩니다. 이 절차에서는 `download-default-key-pair` AWS CLI 명령을 사용하여 지역에 대한 DKP Lightsail을 가져옵니다. AWS 자세한 내용은 AWS CLI 명령 download-default-key-pair참조서를 참조하십시오.

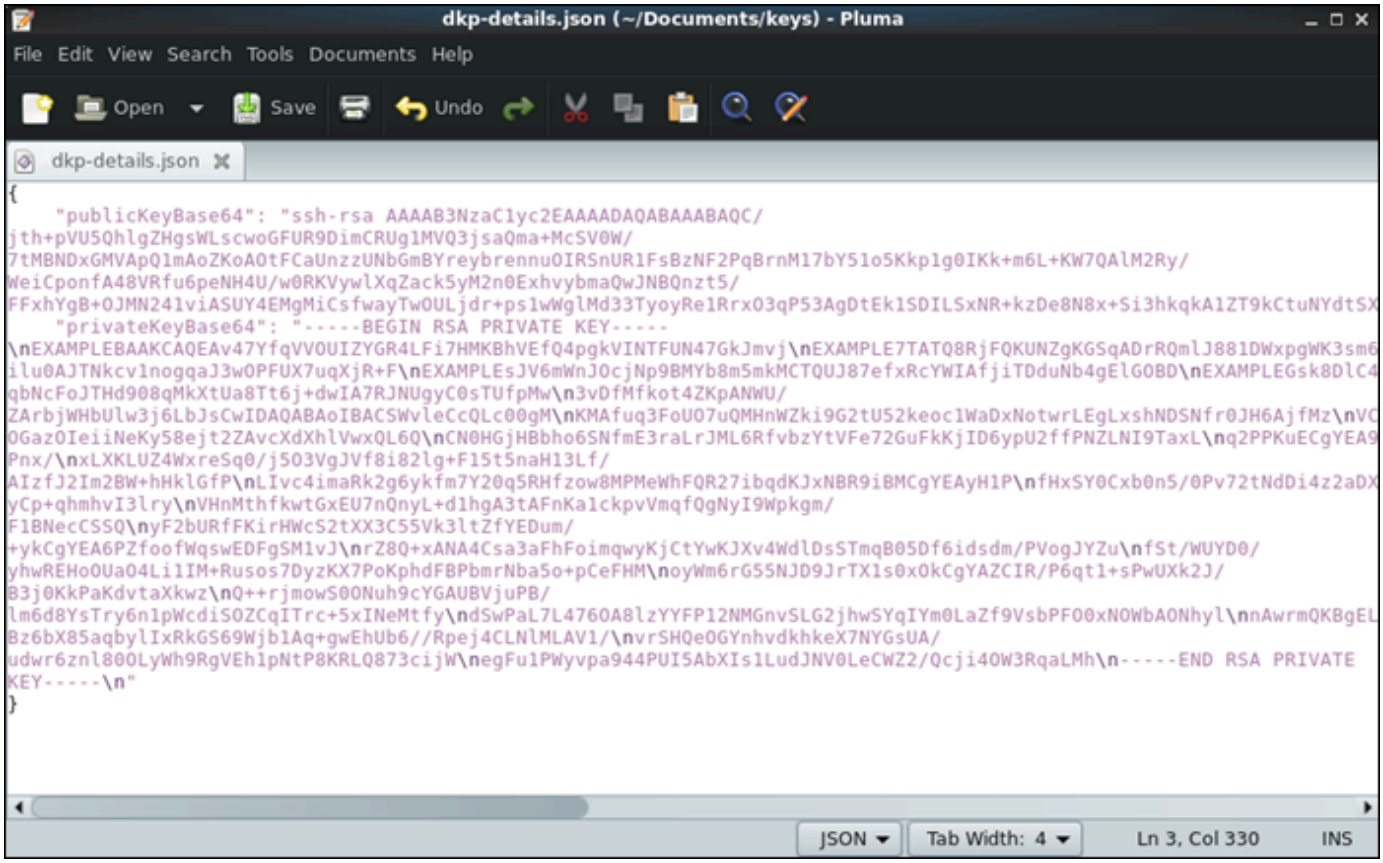
1. 터미널 창을 엽니다.
2. 특정 지역의 DKP Lightsail을 가져오려면 다음 명령을 입력합니다. AWS 이 명령은 정보를 `dkp-details.json` 파일에 저장합니다. 명령에서 가상 컴퓨터가 생성된 AWS 지역의 코드 (예:) *`region-code`* 로 바꿉니다. `us-east-2`

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

   예

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

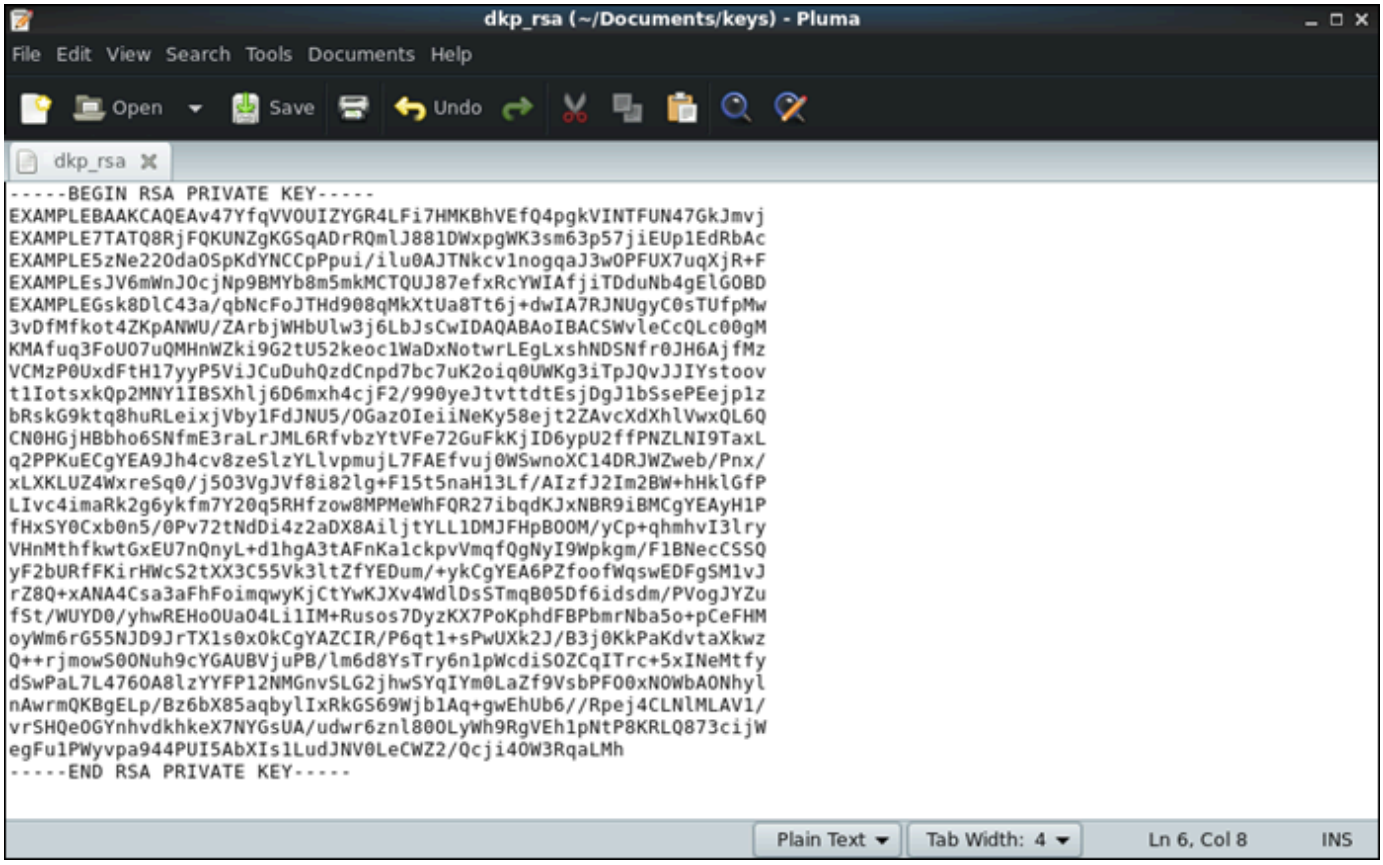
명령에 대한 응답이 없습니다. dkp-details.json파일을 열고 DKP Lightsail 정보가 저장되었는지 확인하여 명령이 성공했는지 확인할 수 있습니다. dkp-details.json 파일 내용은 다음 예제와 같은 형식으로 보입니다. 파일이 비어 있어 명령이 실패했습니다.



3. 다음 명령을 입력하여 dkp-details.json 파일에서 프라이빗 키 정보를 추출하여 새 dkp_rsa 프라이빗 키 파일에 추가합니다.

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

명령에 대한 응답이 없습니다. dkp_rsa 파일을 열고 정보가 들어 있는지 확인하여 명령이 제대로 실행되었는지 확인할 수 있습니다. dkp_rsa 파일 내용은 다음 예제와 같은 형식으로 보입니다. 파일이 비어 있어 명령이 실패했습니다.



4. dkp_rsa 파일에 대한 권한을 설정하려면 다음 명령을 입력합니다.

```
chmod 600 dkp_rsa
```

이제 가상 컴퓨터에 SSH OR SCP 연결을 설정하는 데 필요한 개인 키가 생겼습니다. 다음 추가 단계를 보려면 다음 섹션을 계속 진행합니다.

다음 단계로 이동합니다.

가상 컴퓨터의 키 페어를 성공적으로 확보한 후 다음 추가 단계를 완료할 수 있습니다.

- 명령줄을 사용하여 가상 컴퓨터를 SSH 관리하려면 를 사용하여 가상 컴퓨터에 연결합니다. 자세한 내용은 보안 셸을 사용하여 연구용 Lightsail 가상 컴퓨터에 연결 단원을 참조하십시오.
- 를 사용하여 SCP 가상 컴퓨터에 연결하여 파일을 안전하게 전송합니다. 자세한 내용은 보안 복사를 사용하여 연구용 Lightsail 가상 컴퓨터로 파일 전송 단원을 참조하십시오.

보안 셸을 사용하여 연구용 Lightsail 가상 컴퓨터에 연결

보안 셸 프로토콜 () 을 사용하여 연구용 Amazon Lightsail의 가상 컴퓨터에 연결할 수 있습니다. SSH SSH를 사용하면 인터넷을 통해 컴퓨터에 로그인하고 명령을 실행할 수 있도록 가상 컴퓨터를 원격으로 관리할 수 있습니다.

> **Note**
>
> 브라우저 기반 NICE DCV 클라이언트를 사용하여 가상 컴퓨터에 대한 원격 디스플레이 프로토콜 연결을 설정할 수도 있습니다. NICEDCV연구용 Lightsail 콘솔에서 사용할 수 있습니다. 자세한 내용은 연구용 Lightsail 가상 컴퓨터의 운영 체제에 액세스 단원을 참조하십시오.

주제

사전 조건 완료

시작하기 전에 다음 사전 조건을 완료합니다.

- 연구용 Lightsail에서 가상 컴퓨터를 만드세요. 자세한 내용은 연구용 Lightsail 가상 컴퓨터 만들기 단원을 참조하십시오.
- 연결할 가상 컴퓨터가 실행 상태인지 확인합니다. 또한 가상 컴퓨터의 이름과 가상 컴퓨터가 생성된 AWS 지역을 기록해 두십시오. 이 정보는 이 프로세스 후반부에 필요합니다. 자세한 내용은 연구용 Lightsail 가상 컴퓨터 세부 정보 보기 단원을 참조하십시오.
- 연결할 가상 컴퓨터에 포트 22가 열려 있는지 확인합니다. 이 포트가 사용되는 기본 SSH 포트입니다. 기본적으로 열립니다. 하지만 포트를 닫았으면 계속하기 전에 다시 열어야 합니다. 자세한 내용은 연구용 Lightsail 가상 컴퓨터의 방화벽 포트 관리 단원을 참조하십시오.
- 가상 컴퓨터의 Lightsail 기본 키 페어 DKP () 를 가져옵니다. 자세한 내용은 가상 컴퓨터용 키 페어 가져오기 단원을 참조하십시오.

> **Tip**
>
> 를 사용하여 가상 컴퓨터에 AWS CloudShell 연결하려는 를 사용하여 가상 컴퓨터에 연결 AWS CloudShell 경우 다음 섹션을 참조하십시오. 자세한 내용은 Whatis를 참조하십시오 AWS CloudShell. 그렇지 않으면 다음 사전 요구 사항을 계속 진행하십시오.

- AWS Command Line Interface ()AWS CLI를 다운로드하고 설치합니다. 자세한 내용은 AWS Command Line Interface 버전 2 사용 설명서의 AWS CLI최신 버전의 설치 또는 업데이트를 참조하세요.
- 에 AWS CLI 액세스하도록 구성합니다 AWS 계정. 자세한 내용은 AWS Command Line Interface 버전 2 사용 설명서의 구성 기초 섹션을 참조하세요.
- jq를 다운로드하여 설치합니다. 다음 절차에서 키 쌍 세부 정보를 추출하는 데 사용되는 가볍고 유연한 명령줄 JSON 프로세서입니다. jq 다운로드 및 설치에 대한 자세한 내용은 jq 웹 사이트의 jq 다운로드를 참조하세요.

를 사용하여 가상 컴퓨터에 연결 SSH

다음 절차 중 하나를 완료하여 Lightsail for Research에서 가상 컴퓨터에 대한 SSH 연결을 설정합니다.

를 사용하여 가상 컴퓨터에 연결 AWS CloudShell

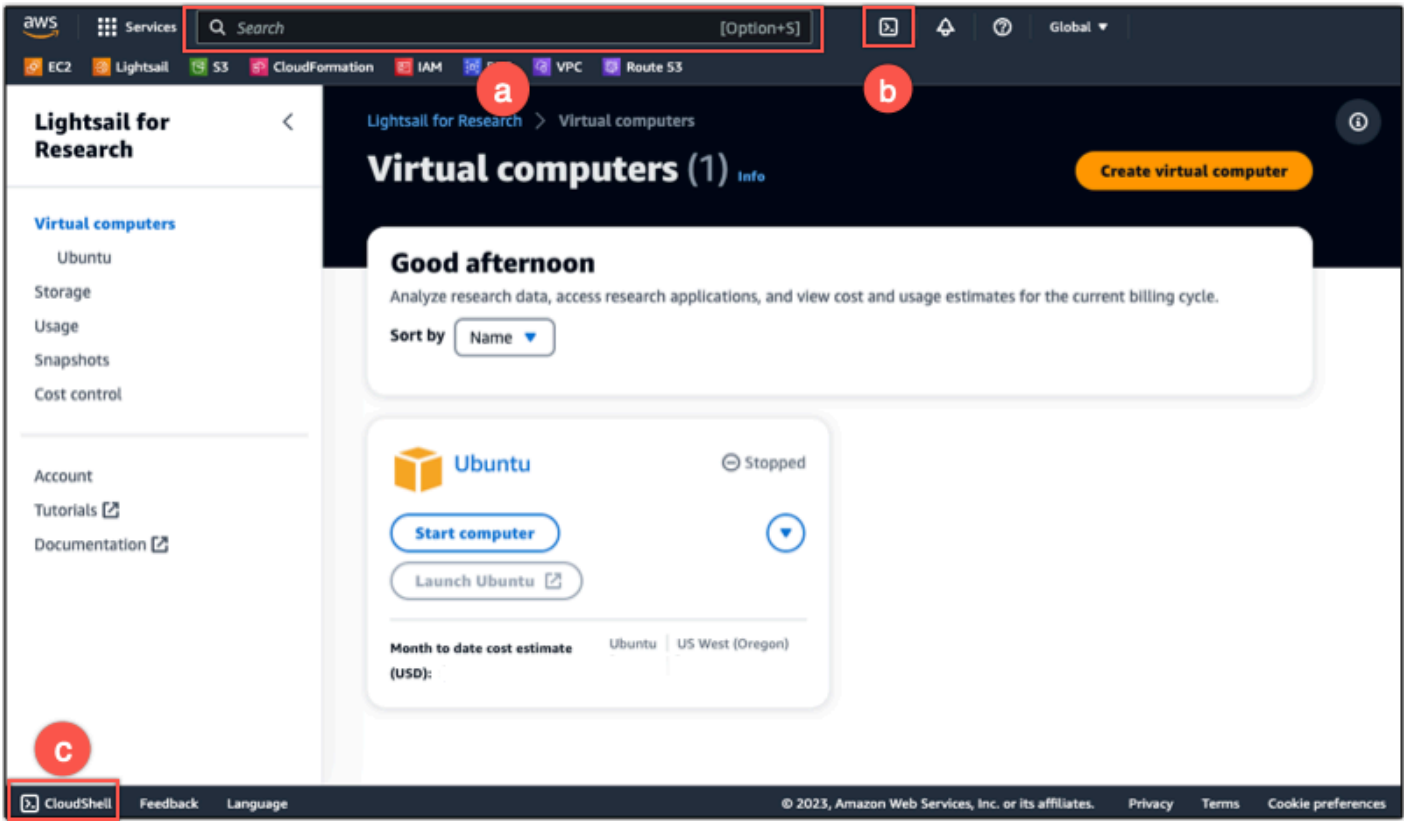
이 절차는 가상 컴퓨터에 연결하기 위한 최소 설정을 선호하는 경우에 적용됩니다. AWS CloudShell 에서 직접 실행할 수 있는 브라우저 기반의 사전 인증된 셸을 사용합니다. AWS Management Console Bash, PowerShell 또는 Z 셸과 같은 원하는 셸을 사용하여 AWS CLI 명령을 실행할 수 있습니다. 명령줄 도구를 다운로드하거나 설치할 필요 없이 이 작업을 수행할 수 있습니다. 자세한 내용은 AWS CloudShell 사용 설명서의 AWS CloudShell시작하기를 참조하세요.

> **Important**
>
> 시작하기 전에 연결하려는 가상 컴퓨터의 Lightsail 기본 키 페어 DKP () 를 가져와야 합니다. 자세한 내용은 연구용 Lightsail 가상 컴퓨터용 키 페어를 구매하세요 단원을 참조하십시오.

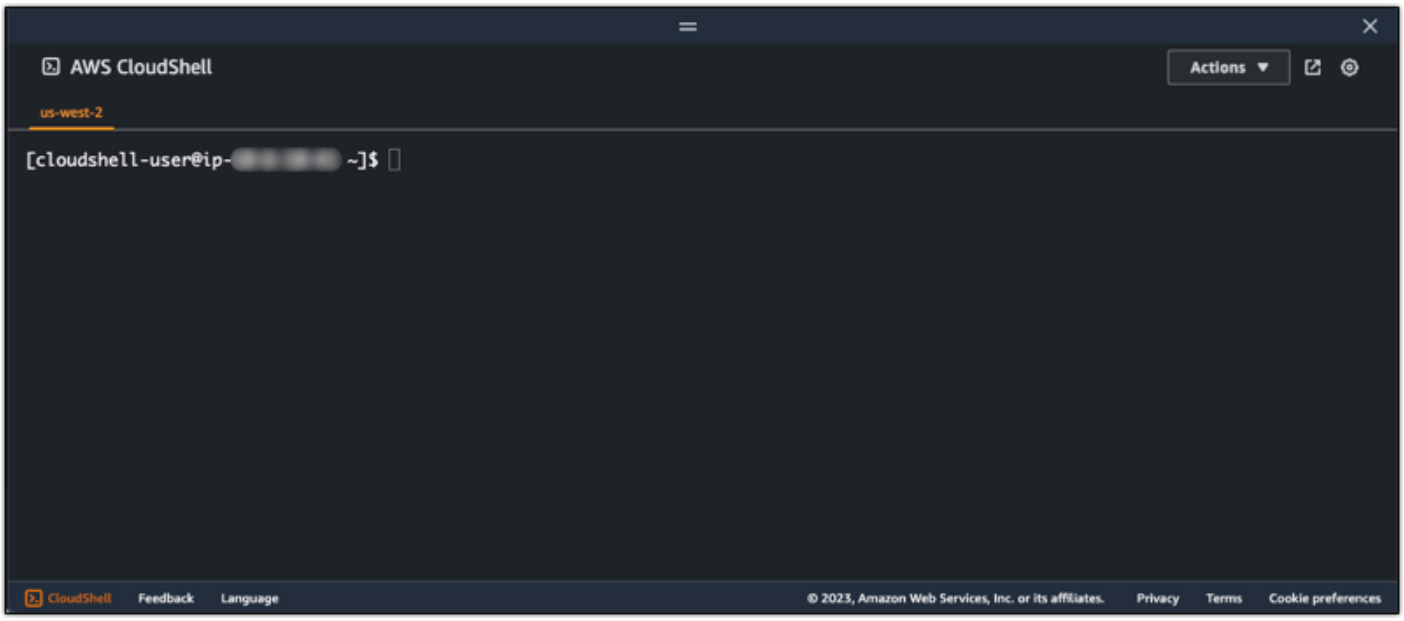
1. 연구용 Lightsail 콘솔에서 다음 옵션 중 하나를 선택하여 CloudShell 실행합니다.
   a. 검색 상자에 "CloudShell“를 입력한 다음 선택합니다. CloudShell

b. 탐색 막대에서 CloudShell아이콘을 선택합니다.

c. 콘솔 CloudShell왼쪽 아래에 있는 콘솔 툴바에서 선택합니다.



명령 프롬프트가 표시되면 셸이 상호 작용할 준비가 된 것입니다.



2. 사용할 사전 설치된 셸을 선택합니다. 기본 셸을 변경하려면 명령줄 프롬프트에 다음 프로그램 이름 중 하나를 입력합니다. Bash시작할 때 실행되는 기본 AWS CloudShell셸입니다.

   Bash

   ```
   bash
   ```

   Bash(으)로 전환하면 명령 프롬프트의 기호가 $(으)로 업데이트됩니다.

   PowerShell

   ```
   pwsh
   ```

   로 PowerShell 전환하면 명령 프롬프트의 기호가 로 PS> 업데이트됩니다.

   Z shell

   ```
   zsh
   ```

   Z shell(으)로 전환하면 명령 프롬프트의 기호가 %(으)로 업데이트됩니다.

3. CloudShell 터미널 창에서 가상 컴퓨터에 연결하려면 을 참조하십시오Linux, Unix 또는 macOS 로컬 SSH 컴퓨터에서 사용하여 가상 컴퓨터에 연결.

CloudShell환경에 사전 설치된 소프트웨어에 대한 자세한 내용은 AWS CloudShell 사용 설명서의AWS CloudShell 컴퓨팅 환경을 참조하십시오.

Windows 로컬 SSH 컴퓨터에서 를 사용하여 가상 컴퓨터에 연결

이 절차는 로컬 컴퓨터에서 Windows 운영 체제를 사용하는 경우에 적용됩니다. 이 절차에서는 `get-instance` AWS CLI 명령을 사용하여 연결하려는 인스턴스의 사용자 이름과 퍼블릭 IP 주소를 얻습니다. 자세한 내용은 AWS CLI 명령 참조에서 get-instance를 참조하세요.

> **Important**
>
> 이 절차를 시작하기 전에 연결하려는 가상 컴퓨터의 Lightsail 기본 키 쌍 DKP () 을 가져왔는지 확인하십시오. 자세한 내용은 연구용 Lightsail 가상 컴퓨터용 키 페어를 구매하세요 단원을 참조하십시오. 이 프로시저는 DKP Lightsail의 프라이빗 키를 다음 명령 `dkp_rsa` 중 하나에 사용되는 파일에 출력합니다.

1. 명령 프롬프트 창을 엽니다.

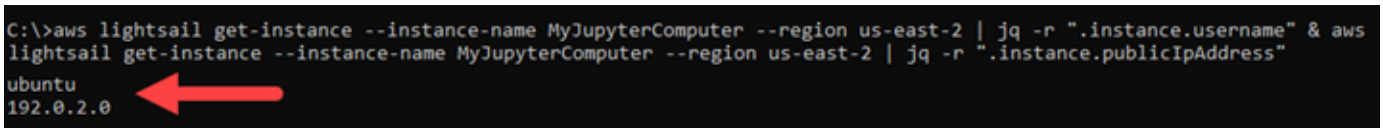
2. 다음 명령을 입력하여 가상 컴퓨터의 퍼블릭 IP 주소와 사용자 이름을 표시합니다. 명령에서 가상 컴퓨터가 생성된 코드 (예:) *region-code* 로 바꿉니다. AWS 리전 us-east-2 *computer-name*을 연결하려는 가상 컴퓨터의 이름으로 바꿉니다.

```
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"
```

예

```
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"
```

응답에는 다음 예제와 같이 가상 컴퓨터의 사용자 이름과 퍼블릭 IP 주소가 표시됩니다. 이 절차의 다음 단계에서 필요하므로 이 값을 기록해 둡니다.



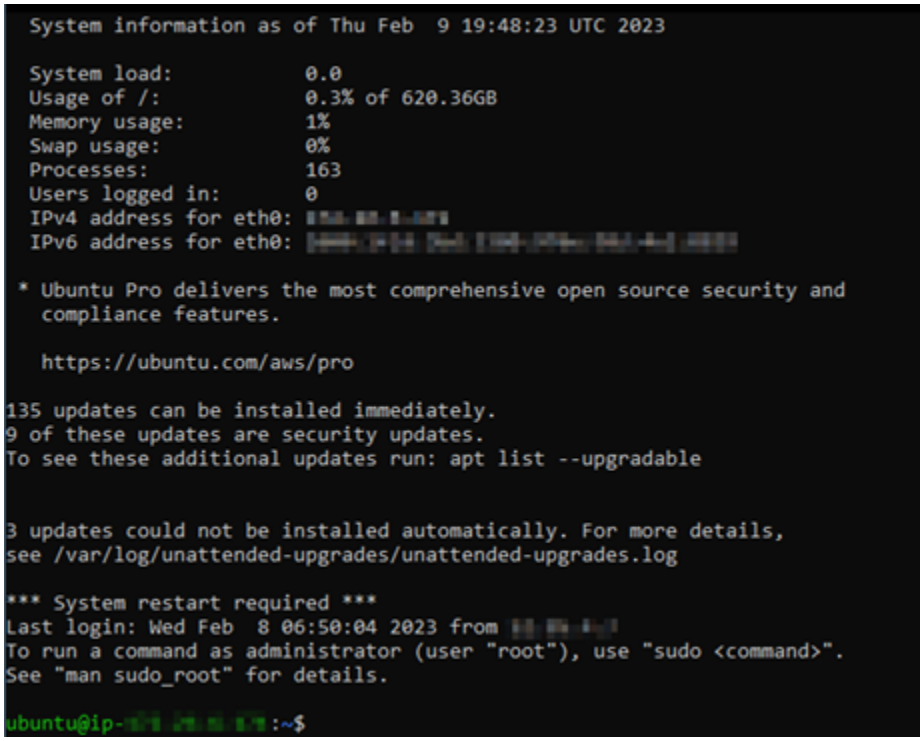
3. 다음 명령을 입력하여 가상 컴퓨터와의 SSH 연결을 설정합니다. 명령에서 *user-name*을 로그인 사용자 이름으로 바꾸고 *public-ip-address*를 가상 컴퓨터의 퍼블릭 IP 주소로 바꿉니다.

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

예

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

Lightsail for Research에서 Ubuntu 가상 컴퓨터에 설정된 SSH 연결을 보여주는 다음 예와 비슷한 응답이 표시되어야 합니다.



이제 가상 컴퓨터에 성공적으로 SSH 연결되었으므로 다음 섹션을 계속 진행하여 다음 단계를 추가로 진행하십시오.

Linux, Unix 또는 macOS 로컬 SSH 컴퓨터에서 사용하여 가상 컴퓨터에 연결

이 절차는 로컬 컴퓨터가 Linux, Unix 또는 macOS 운영 체제를 사용하는 경우에 적용됩니다. 이 절차에서는 `get-instance` AWS CLI 명령을 사용하여 연결하려는 인스턴스의 사용자 이름과 퍼블릭 IP 주소를 얻습니다. 자세한 내용은 AWS CLI 명령 참조에서 get-instance를 참조하세요.

> **Important**
>
> 이 절차를 시작하기 전에 연결하려는 가상 컴퓨터의 Lightsail 기본 키 쌍 DKP () 을 가져왔는지 확인하십시오. 자세한 내용은 연구용 Lightsail 가상 컴퓨터용 키 페어를 구매하세요 단원을 참조하십시오. 이 프로시저는 DKP Lightsail의 프라이빗 키를 다음 명령 `dkp_rsa` 중 하나에 사용되는 파일에 출력합니다.

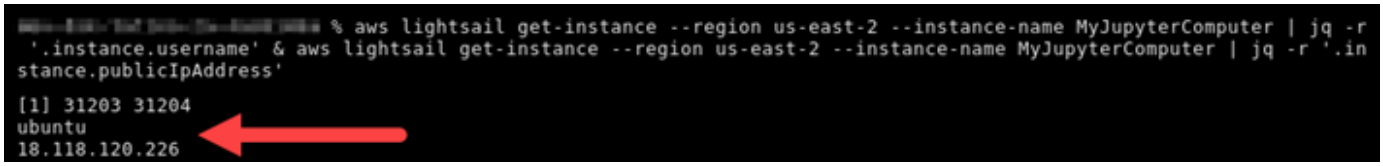
1. 터미널 창을 엽니다.
2. 다음 명령을 입력하여 가상 컴퓨터의 퍼블릭 IP 주소와 사용자 이름을 표시합니다. 명령에서 가상 컴퓨터가 생성된 AWS 지역의 코드 (예:) *`region-code`* 로 대체하십시오. `us-east-2` *`computer-name`*을 연결하려는 가상 컴퓨터의 이름으로 바꿉니다.

```
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'
```

예

```
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'
```

응답에는 다음 예제와 같이 가상 컴퓨터의 사용자 이름과 퍼블릭 IP 주소가 표시됩니다. 이 절차의 다음 단계에서 필요하므로 이 값을 기록해 둡니다.



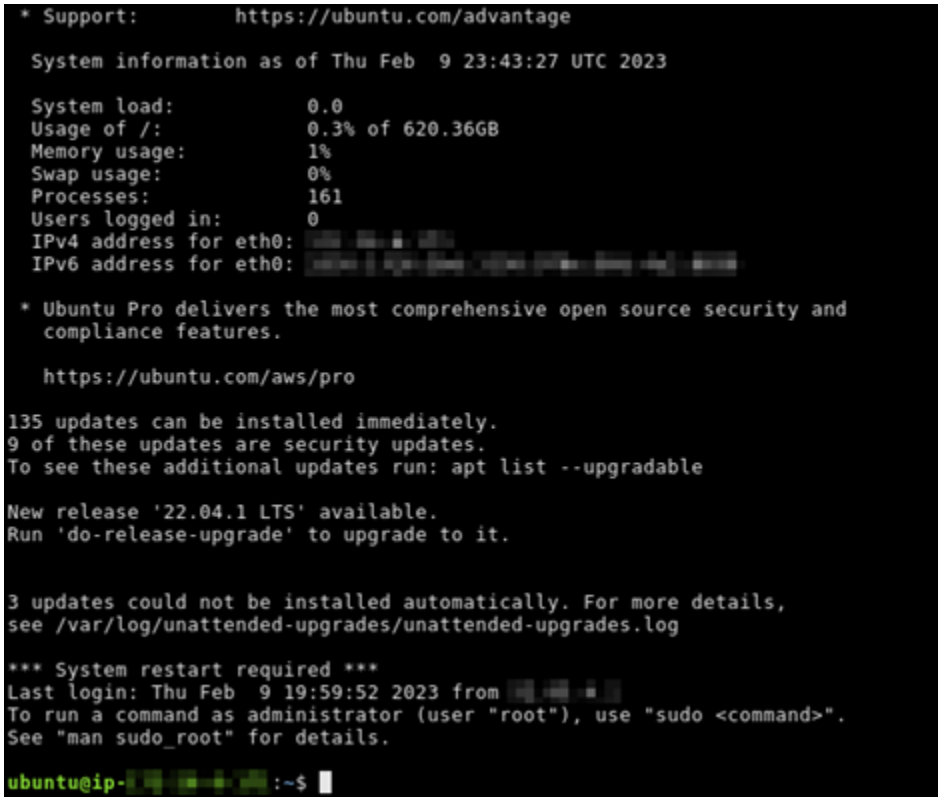
3. 다음 명령을 입력하여 가상 컴퓨터와의 SSH 연결을 설정합니다. 명령에서 *user-name*을 로그인 사용자 이름으로 바꾸고 *public-ip-address*를 가상 컴퓨터의 퍼블릭 IP 주소로 바꿉니다.

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

예

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

Lightsail for Research에서 Ubuntu 가상 컴퓨터에 설정된 SSH 연결을 보여주는 다음 예와 비슷한 응답이 표시되어야 합니다.



이제 가상 컴퓨터에 성공적으로 SSH 연결되었으므로 다음 섹션을 계속 진행하여 다음 단계를 추가로 진행하십시오.

다음 단계로 이동합니다.

가상 컴퓨터에 성공적으로 SSH 연결되면 다음 추가 단계를 완료할 수 있습니다.

- 를 사용하여 SCP 가상 컴퓨터에 연결하여 파일을 안전하게 전송합니다. 자세한 내용은 보안 복사를 사용하여 연구용 Lightsail 가상 컴퓨터로 파일 전송 단원을 참조하십시오.

보안 복사를 사용하여 연구용 Lightsail 가상 컴퓨터로 파일 전송

보안 복사 () 를 사용하여 로컬 컴퓨터의 파일을 연구용 Amazon Lightsail의 가상 컴퓨터로 전송할 수 있습니다. SCP 이 프로세스를 통해 한 번에 여러 파일 또는 전체 디렉터리를 전송할 수 있습니다.

> **Note**
>
> Lightsail for Research 콘솔에서 사용할 수 있는 브라우저 기반 NICE DCV 클라이언트를 사용하여 가상 컴퓨터에 대한 원격 디스플레이 프로토콜 연결을 설정할 수도 있습니다. NICEDCV

클라이언트를 사용하면 개별 파일을 빠르게 전송할 수 있습니다. 자세한 내용은 연구용 Lightsail 가상 컴퓨터의 운영 체제에 액세스 단원을 참조하십시오.

주제

사전 조건 완료

시작하기 전에 다음 사전 조건을 완료합니다.

- 연구용 Lightsail에서 가상 컴퓨터를 만드세요. 자세한 내용은 연구용 Lightsail 가상 컴퓨터 만들기 단원을 참조하십시오.
- 연결할 가상 컴퓨터가 실행 상태인지 확인합니다. 또한 가상 컴퓨터의 이름과 가상 컴퓨터를 만든 AWS 리전을 기록해 둡니다. 이 정보는 이 절차의 뒷부분에서 필요합니다. 자세한 내용은 연구용 Lightsail 가상 컴퓨터 세부 정보 보기 단원을 참조하십시오.
- AWS Command Line Interface ()AWS CLI를 다운로드하고 설치합니다. 자세한 내용은 AWS Command Line Interface 버전 2 사용 설명서의 AWS CLI최신 버전의 설치 또는 업데이트를 참조하세요.
- 에 AWS CLI 액세스하도록 구성합니다 AWS 계정. 자세한 내용은 AWS Command Line Interface 버전 2 사용 설명서의 구성 기초 섹션을 참조하세요.
- jq를 다운로드하여 설치합니다. 다음 절차에서 키 쌍 세부 정보를 추출하는 데 사용되는 가볍고 유연한 명령줄 JSON 프로세서입니다. jq 다운로드 및 설치에 대한 자세한 내용은 jq 웹 사이트의 jq 다운로드를 참조하세요.
- 연결할 가상 컴퓨터에 포트 22가 열려 있는지 확인합니다. 이 포트가 사용되는 기본 SSH 포트입니다. 기본적으로 열립니다. 하지만 포트를 닫았으면 계속하기 전에 다시 열어야 합니다. 자세한 내용은 연구용 Lightsail 가상 컴퓨터의 방화벽 포트 관리 단원을 참조하십시오.
- 가상 컴퓨터의 Lightsail 기본 키 페어 DKP () 를 가져옵니다. 자세한 내용은 연구용 Lightsail 가상 컴퓨터 만들기 단원을 참조하십시오.

를 사용하여 가상 컴퓨터에 연결 SCP

다음 절차 중 하나를 완료하여 Lightsail for Research에서 가상 컴퓨터에 연결합니다. SCP

Windows 로컬 SCP 컴퓨터에서 를 사용하여 가상 컴퓨터에 연결

이 절차는 로컬 컴퓨터에서 Windows 운영 체제를 사용하는 경우에 적용됩니다. 이 절차에서는 `get-instance` AWS CLI 명령을 사용하여 연결하려는 인스턴스의 사용자 이름과 퍼블릭 IP 주소를 얻습니다. 자세한 내용은 AWS CLI 명령 참조에서 get-instance를 참조하세요.

> **Important**
>
> 이 절차를 시작하기 전에 연결하려는 가상 컴퓨터의 Lightsail 기본 키 쌍 DKP () 을 가져왔는지 확인하십시오. 자세한 내용은 연구용 Lightsail 가상 컴퓨터용 키 페어를 구매하세요 단원을 참조하십시오. 이 프로시저는 DKP Lightsail의 프라이빗 키를 다음 명령 `dkp_rsa` 중 하나에 사용되는 파일에 출력합니다.

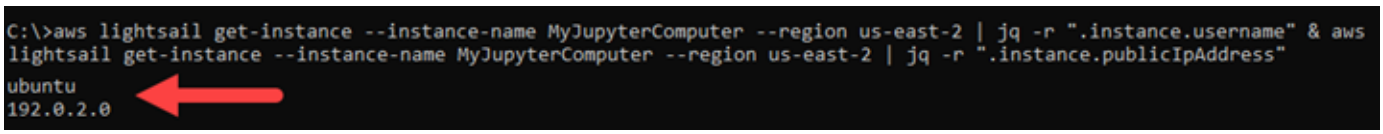
1. 명령 프롬프트 창을 엽니다.
2. 다음 명령을 입력하여 가상 컴퓨터의 퍼블릭 IP 주소와 사용자 이름을 표시합니다. 명령에서 가상 컴퓨터가 생성된 AWS 지역의 코드 (예:) *region-code* 로 대체하십시오. `us-east-2` *computer-name*을 연결하려는 가상 컴퓨터의 이름으로 바꿉니다.

   ```
   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"
   ```

   예

   ```
   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"
   ```

   응답에는 다음 예제와 같이 가상 컴퓨터의 사용자 이름과 퍼블릭 IP 주소가 표시됩니다. 이 절차의 다음 단계에서 필요하므로 이 값을 기록해 둡니다.

3. 다음 명령을 입력하여 가상 컴퓨터와의 SCP 연결을 설정하고 가상 컴퓨터로 파일을 전송합니다.

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

명령에서 다음과 같이 바꿉니다.

- 전송하려는 파일이 들어 있는 로컬 컴퓨터의 폴더를 포함한 *source-folder*.
- 이 절차의 이전 단계에서 사용한 사용자 이름(예:ubuntu)을 포함한 *user-name*.
- 이 절차의 이전 단계에서 사용한 가상 컴퓨터의 퍼블릭 IP 주소를 포함한 *public-ip-address*.
- 파일을 복사할 가상 컴퓨터의 디렉터리 경로를 포함한 *destination-directory*.

다음 예제에서는 로컬 컴퓨터의 `C:\Files` 폴더에 있는 모든 파일을 원격 가상 컴퓨터의 `/home/lightsail-user/Uploads/` 디렉터리로 복사합니다.

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

다음 예와 비슷한 응답이 나타나는 것을 볼 수 있습니다. 원본 폴더에서 대상 디렉터리로 전송된 각 파일이 표시됩니다. 이제 가상 컴퓨터에서 해당 파일에 액세스할 수 있습니다.

```
C:\>scp -i dkp_rsa -r "C:\Files" ubuntu@192.0.2.0:/home/lightsail-user/Uploads/
myfile.txt                                    100%   11     0.2KB/s   00:00
myfile1.txt                                   100%    9     0.2KB/s   00:00
myfile10.txt                                  100%    7     0.1KB/s   00:00
myfile11.txt                                  100%    4     0.1KB/s   00:00
myfile12.txt                                  100%   13     0.2KB/s   00:00
myfile2.txt                                   100%   10     0.2KB/s   00:00
myfile3.txt                                   100%   10     0.2KB/s   00:00
myfile4.txt                                   100%    9     0.1KB/s   00:00
myfile5.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
myfile8.txt                                   100%    9     0.2KB/s   00:00
myfile9.txt                                   100%    9     0.2KB/s   00:00
```

Linux, Unix 또는 macOS 로컬 SCP 컴퓨터에서 사용하여 가상 컴퓨터에 연결

이 절차는 로컬 컴퓨터가 Linux, Unix 또는 macOS 운영 체제를 사용하는 경우에 적용됩니다. 이 절차에서는 `get-instance` AWS CLI 명령을 사용하여 연결하려는 인스턴스의 사용자 이름과 퍼블릭 IP 주소를 얻습니다. 자세한 내용은 AWS CLI 명령 참조에서 get-instance를 참조하세요.

> **Important**
>
> 이 절차를 시작하기 전에 연결하려는 가상 컴퓨터의 Lightsail 기본 키 쌍 DKP () 을 가져왔는지 확인하십시오. 자세한 내용은 연구용 Lightsail 가상 컴퓨터용 키 페어를 구매하세요 단원을 참

조하십시오. 이 프로시저는 DKP Lightsail의 프라이빗 키를 다음 명령 dkp_rsa 중 하나에 사용되는 파일에 출력합니다.

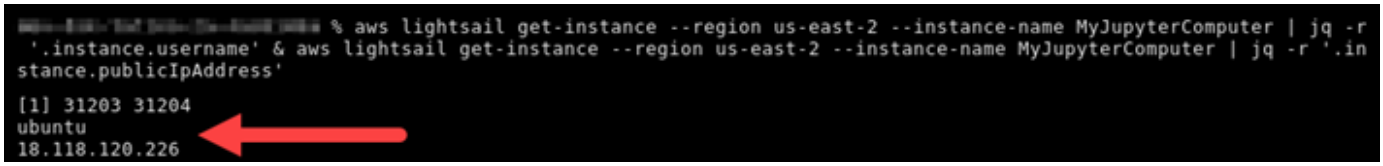
1. 터미널 창을 엽니다.
2. 다음 명령을 입력하여 가상 컴퓨터의 퍼블릭 IP 주소와 사용자 이름을 표시합니다. 명령에서 가상 컴퓨터가 생성된 AWS 지역의 코드 (예:) *region-code* 로 대체하십시오. us-east-2 *computer-name*을 연결하려는 가상 컴퓨터의 이름으로 바꿉니다.

```
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'
```

예

```
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'
```

응답에는 다음 예제와 같이 가상 컴퓨터의 사용자 이름과 퍼블릭 IP 주소가 표시됩니다. 이 절차의 다음 단계에서 필요하므로 이 값을 기록해 둡니다.



3. 다음 명령을 입력하여 가상 컴퓨터와의 SCP 연결을 설정하고 가상 컴퓨터로 파일을 전송합니다.

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

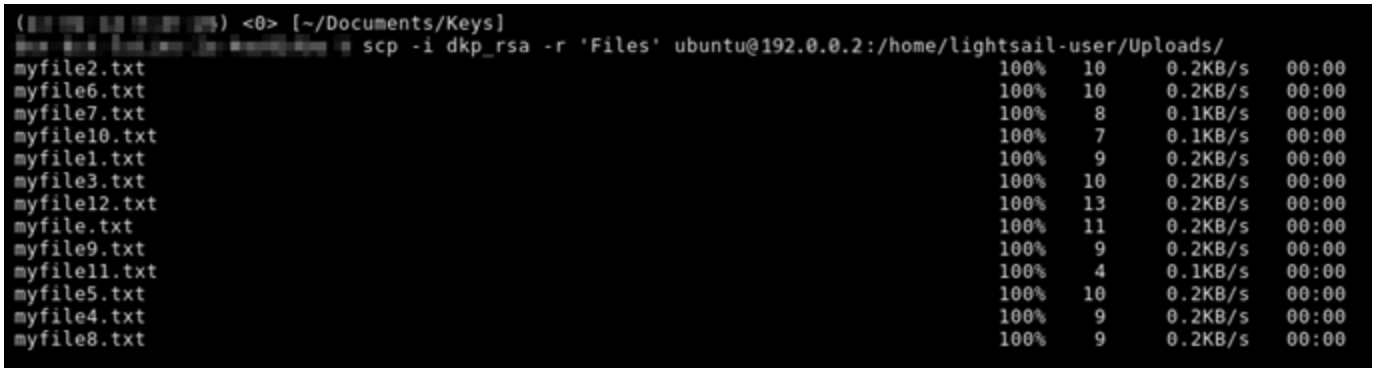
명령에서 다음과 같이 바꿉니다.

- 전송하려는 파일이 들어 있는 로컬 컴퓨터의 폴더를 포함한 *source-folder*.
- 이 절차의 이전 단계에서 사용한 사용자 이름(예:ubuntu)을 포함한 *user-name*.
- 이 절차의 이전 단계에서 사용한 가상 컴퓨터의 퍼블릭 IP 주소를 포함한 *public-ip-address*.
- 파일을 복사할 가상 컴퓨터의 디렉터리 경로를 포함한 *destination-directory*.

다음 예제에서는 로컬 컴퓨터의 C:\Files 폴더에 있는 모든 파일을 원격 가상 컴퓨터의 /home/lightsail-user/Uploads/ 디렉터리로 복사합니다.

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

다음 예와 비슷한 응답이 나타나는 것을 볼 수 있습니다. 원본 폴더에서 대상 디렉터리로 전송된 각 파일이 표시됩니다. 이제 가상 컴퓨터에서 해당 파일에 액세스할 수 있습니다.



연구용 Lightsail 가상 컴퓨터 삭제

더 이상 필요하지 않은 경우 다음 단계를 완료하여 Lightsail for Research 가상 컴퓨터를 삭제하십시오. 삭제하는 즉시 가상 컴퓨터에 대한 요금 발생이 중지됩니다. 스냅샷과 같이 삭제된 컴퓨터에 연결된 리소스에는 삭제할 때까지 계속 요금이 부과됩니다.

> **Important**
>
> 가상 컴퓨터 삭제는 영구적인 작업이므로 컴퓨터를 복구할 수 없습니다. 나중에 데이터가 필요할 수 있는 경우 삭제하기 전에 가상 컴퓨터의 스냅샷을 생성하세요. 자세한 내용은 스냅샷 생성을 참조하세요..

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 가상 컴퓨터를 선택합니다.
3. 삭제할 가상 컴퓨터를 선택합니다.
4. 작업을 선택한 다음 가상 컴퓨터 삭제를 선택합니다.
5. 텍스트 블록에 확인을 입력합니다. 그런 다음 가상 컴퓨터 삭제를 선택합니다

연구용 Lightsail 볼륨으로 데이터 보호 및 저장

연구용 Amazon Lightsail 가상 컴퓨터에 연결할 수 있는 블록 수준의 스토리지 볼륨 (디스크) 을 제공합니다. 이 볼륨 (디스크) 은 실행 중인 Lightsail for Research 가상 컴퓨터에 연결할 수 있습니다. 세분화된 업데이트를 자주 수행하는 데이터의 경우 기본 스토리지 디바이스로 스토리를 사용할 수 있습니다. 예를 들어, Lightsail for Research 가상 컴퓨터에서 데이터베이스를 실행할 때는 디스크를 사용하는 것이 좋습니다.

디스크는 단일 가상 컴퓨터에 연결하는 형식이 지정되지 않은 외부 블록 디바이스와 같은 방식으로 동작합니다. 볼륨은 컴퓨터의 실행 수명과 독립적으로 유지됩니다. 디스크를 컴퓨터에 연결한 후에는 다른 물리적 하드 드라이브처럼 사용할 수 있습니다.

컴퓨터에 여러 디스크를 연결할 수 있습니다. 한 컴퓨터에서 분리한 다음 이 디스크를 다른 컴퓨터에 연결하는 것도 가능합니다.

데이터의 백업 복사본을 유지하려면 디스크의 스냅샷을 생성합니다. 스냅샷에서 새 디스크를 생성하여 다른 컴퓨터에 연결할 수 있습니다.

주제

연구용 Lightsail 콘솔에서 스토리지 디스크 만들기

다음 단계를 완료하여 Lightsail for Research 가상 컴퓨터용 디스크를 만드십시오.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 스토리지를 선택합니다.
3. 디스크 생성을 선택합니다.
4. 디스크의 이름을 입력합니다. 유효한 문자에는 영숫자, 숫자, 마침표, 하이픈, 밑줄이 포함됩니다.

   디스크 이름은 다음 요구 사항을 충족해야 합니다.

- 연구용 Lightsail AWS 리전 계정에서 각 계정마다 고유해야 합니다.
- 2–255자로 구성되어야 합니다.
- 영숫자 문자 또는 숫자로 시작하고 끝나야 합니다.

5. 디스크에 AWS 리전 맞는 것을 선택하세요.

   디스크는 이 디스크를 연결하는 가상 컴퓨터와 동일한 리전에 있어야 합니다.
6. 디스크 크기(GB)를 선택합니다.
7. 가상 컴퓨터에 디스크를 연결하는 방법에 대한 자세한 내용은 디스크 연결 섹션을 계속 참조하세요.

연구용 Lightsail 콘솔에서 스토리지 디스크 세부 정보 보기

다음 단계를 완료하여 Lightsail for Research 계정의 디스크와 해당 세부 정보를 확인하십시오.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 스토리지를 선택합니다.

   스토리지 페이지에서는 Lightsail for Research 계정의 디스크를 종합적으로 볼 수 있습니다.

   다음 정보가 페이지에 표시됩니다.

   - 이름 - 스토리지 디스크의 이름.
   - 크기 - 디스크 크기(GB).
   - AWS 리전 - 디스크가 생성된 AWS 리전 .
   - 연결 대상 - 디스크가 연결된 Lightsail 컴퓨터입니다.
   - 만든 날짜 - 디스크를 만든 날짜.

연구용 Lightsail에서 가상 컴퓨터에 스토리지 추가

연구용 Lightsail에서 가상 컴퓨터에 디스크를 연결하려면 다음 단계를 완료하십시오. 가상 컴퓨터에는 최대 15개의 디스크를 연결할 수 있습니다. Lightsail for Research 콘솔을 사용하여 가상 컴퓨터에 디스크를 연결하면 서비스가 디스크를 자동으로 포맷하고 마운트합니다. 이 프로세스는 몇 분 정도 걸리므로 사용하기 전에 디스크가 Mounted 마운팅 상태에 도달했는지 확인해야 합니다. 기본적으로 Lightsail for Research는 디렉터리에 디스크를 마운트합니다. *<disk-name>* 여기서 은 사용자가 지정한 디스크 이름입니다. `/home/lightsail-user/`*<disk-name>*

> **Important**
>
> 가상 컴퓨터에 디스크를 연결하려면 먼저 가상 컴퓨터가 실행 중 상태여야 합니다. 중지된 상태일 때 가상 컴퓨터에 디스크를 연결하면 디스크는 연결되지만 마운트되지 않습니다. 디스크의 마운트 상태가 실패인 경우 가상 컴퓨터가 실행 중일 때 디스크를 분리했다가 다시 연결해야 합니다.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 가상 컴퓨터를 선택합니다.
3. 디스크를 연결할 컴퓨터를 선택합니다.
4. 스토리지 탭을 선택합니다.
5. 디스크 연결을 선택합니다.
6. 컴퓨터에 연결할 디스크 이름을 선택합니다.
7. 연결을 선택합니다.

연구용 Lightsail의 가상 컴퓨터에서 디스크 분리하기

다음 단계에 따라 컴퓨터에서 디스크를 분리합니다.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 스토리지를 선택합니다.
3. 분리할 디스크를 찾습니다. 연결 대상 열에서 디스크가 연결된 컴퓨터 이름을 선택합니다.
4. 컴퓨터를 중지하려면 중지를 선택합니다. 디스크를 분리하려면 먼저 컴퓨터를 중지해야 합니다.
5. 컴퓨터를 중지할 것인지 확인한 다음 컴퓨터 중지를 선택합니다.
6. 스토리지 탭을 선택합니다.
7. 분리할 디스크를 선택한 다음 분리를 선택합니다.
8. 컴퓨터에서 디스크를 분리할 것인지 확인한 다음 분리를 선택합니다.

연구용 Lightsail에서 사용하지 않는 스토리지 디스크 삭제

스토리지 디스크가 더 이상 필요하지 않은 경우 삭제하세요. 디스크가 삭제되는 즉시 디스크에 대한 요금 발생이 중지됩니다.

디스크가 컴퓨터에 연결되어 있는 경우 디스크를 분리해야 디스크를 삭제할 수 있습니다. 자세한 내용은 연구용 Lightsail의 가상 컴퓨터에서 디스크 분리하기 단원을 참조하십시오.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 스토리지를 선택합니다.
3. 삭제할 디스크를 찾아 선택합니다.
4. 디스크 삭제를 선택합니다.
5. 디스크를 삭제하려 한다는 것을 확인합니다. 그런 다음 삭제를 선택합니다.

연구용 Lightsail 스냅샷을 사용하여 가상 컴퓨터 및 디스크를 백업합니다.

스냅샷은 데이터의 point-in-time 사본입니다. Amazon Lightsail for Research 가상 컴퓨터 및 스토리지 디스크의 스냅샷을 생성하고 이를 기준으로 사용하여 새 컴퓨터를 만들거나 데이터를 백업할 수 있습니다.

스냅샷은 스냅샷을 생성한 시점부터 컴퓨터를 복원하는 데 필요한 모든 데이터를 포함합니다. 스냅샷에서 새 가상 컴퓨터를 생성하면 스냅샷을 생성하는 데 사용된 원래 컴퓨터의 정확한 복제본으로 시작됩니다.

언제든지 리소스에 장애가 발생할 수 있으므로 영구적인 데이터 손실을 방지하려면 스냅샷을 자주 만드는 것이 좋습니다.

주제

연구용 Lightsail 가상 컴퓨터 또는 디스크의 스냅샷 생성

다음 단계를 완료하여 Lightsail for Research 가상 컴퓨터 또는 디스크의 스냅샷을 만드십시오.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 스냅샷을 선택합니다.
3. 다음 단계 중 하나를 완료합니다.

   - 가상 컴퓨터 스냅샷에서 스냅샷을 만들려는 컴퓨터의 이름을 찾은 다음 스냅샷 만들기를 선택합니다.
   - 디스크 스냅샷에서 스냅샷하려는 디스크의 이름을 찾은 다음 스냅샷 만들기를 선택합니다.
4. 스냅샷 복사본 이름을 입력합니다. 유효한 문자에는 영숫자, 숫자, 마침표, 하이픈, 밑줄이 포함됩니다.

   스냅샷 이름은 다음 요구 사항을 충족해야 합니다.

- 연구용 Lightsail AWS 리전 계정에서 각 계정마다 고유해야 합니다.
- 2–255자로 구성되어야 합니다.
- 영숫자 문자 또는 숫자로 시작하고 끝나야 합니다.

5. 스냅샷 생성(Create snapshot)을 선택합니다.

연구용 Lightsail에서 가상 컴퓨터 및 디스크 스냅샷 보기 및 관리

가상 컴퓨터 및 디스크의 스냅샷을 보려면 다음 단계를 완료합니다.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 스냅샷을 선택합니다.

   스냅샷 페이지에는 사용자가 만든 가상 컴퓨터 및 디스크 스냅샷이 표시됩니다.

   보관된 스냅샷은 이 페이지에도 있습니다. 보관된 스냅샷은 계정에서 삭제된 리소스의 스냅샷입니다.

스냅샷에서 가상 컴퓨터 또는 디스크 만들기

스냅샷에서 새 Lightsail for Research 가상 컴퓨터 또는 디스크를 만들려면 다음 단계를 완료하십시오.

스냅샷으로 가상 컴퓨터를 만들 때는 원래 컴퓨터에 사용한 것과 크기가 같거나 더 큰 플랜을 사용합니다. 원래 가상 컴퓨터보다 작은 플랜은 사용할 수 없습니다.

스냅샷에서 디스크를 만들 때는 원본 디스크보다 큰 디스크 크기를 선택합니다. 원본 디스크보다 작은 디스크는 사용할 수 없습니다.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 스냅샷을 선택합니다.
3. 스냅샷 페이지에서 새 컴퓨터 또는 디스크를 만드는 데 사용할 컴퓨터 또는 디스크 스냅샷의 이름을 찾습니다. 스냅샷 드롭다운 메뉴를 선택하면 해당 리소스에 사용할 수 있는 스냅샷 목록을 볼 수 있습니다.
4. 가상 컴퓨터를 생성하는 데 사용할 스냅샷을 선택합니다.
5. 작업 드롭다운 메뉴를 선택합니다. 그런 다음 가상 컴퓨터 만들기 또는 디스크 생성을 선택합니다.

연구용 Lightsail 콘솔에서 스냅샷을 삭제합니다.

스냅샷을 삭제하려면 다음 단계를 완료합니다.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 스냅샷을 선택합니다.
3. 스냅샷 페이지에서 삭제하려는 컴퓨터 또는 디스크 스냅샷의 이름을 찾습니다. 스냅샷 드롭다운 메뉴를 선택하면 해당 리소스에 사용할 수 있는 스냅샷 목록을 볼 수 있습니다.
4. 삭제하고 싶은 스냅샷을 선택합니다.
5. 작업 드롭다운 메뉴를 선택합니다. 그런 다음 스냅샷 삭제를 선택합니다.
6. 스냅샷 이름이 올바른지 확인합니다. 그런 다음 스냅샷 삭제를 선택합니다.

연구용 Lightsail의 비용 및 사용량 추정치

연구용 Amazon Lightsail은 리소스에 대한 예상 비용 및 사용량을 제공합니다. AWS 이 추정치를 사용하여 Lightsail for Research를 사용할 때 지출 계획을 세우고, 비용 절감 기회를 찾고, 정보에 입각한 결정을 내릴 수 있습니다.

가상 컴퓨터나 디스크를 만들면 해당 리소스에 대한 예상 비용 및 사용량이 표시됩니다. 예상 비용 및 사용량은 리소스가 생성되고 사용 가능 또는 실행 중 상태가 되는 즉시 추적을 시작합니다. 예상치는 리소스가 생성된 후 15분 이내에 AWS 관리 콘솔에 표시됩니다. 삭제된 리소스는 포함되지 않습니다.

> **Important**
>
> 예상 비용이란 리소스 사용량을 기준으로 계산한 예상 비용입니다. 실제 비용은 Lightsail for Research 콘솔에 표시된 예상 비용이 아니라 실제 리소스 사용량을 기준으로 합니다. 실제 비용은 AWS Billing 계정 명세서에 표시됩니다.
> 에서 AWS Management Console 로그인하고 AWS Billing 콘솔을 엽니다 https://console.aws.amazon.com/billing/.

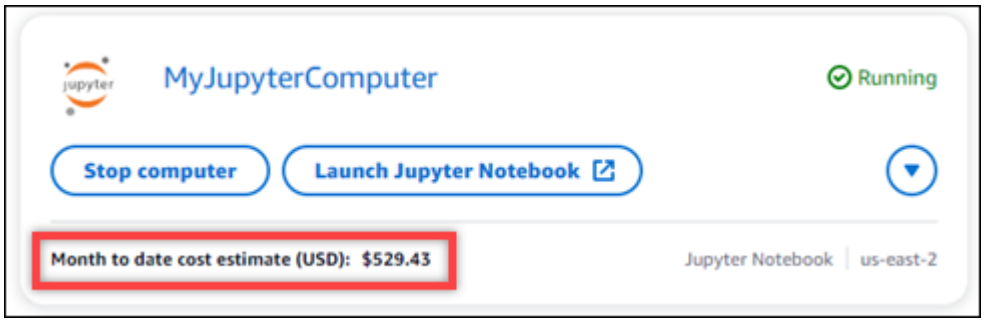
주제

- 연구용 Lightsail에서 리소스의 예상 비용 및 사용량을 확인하십시오.

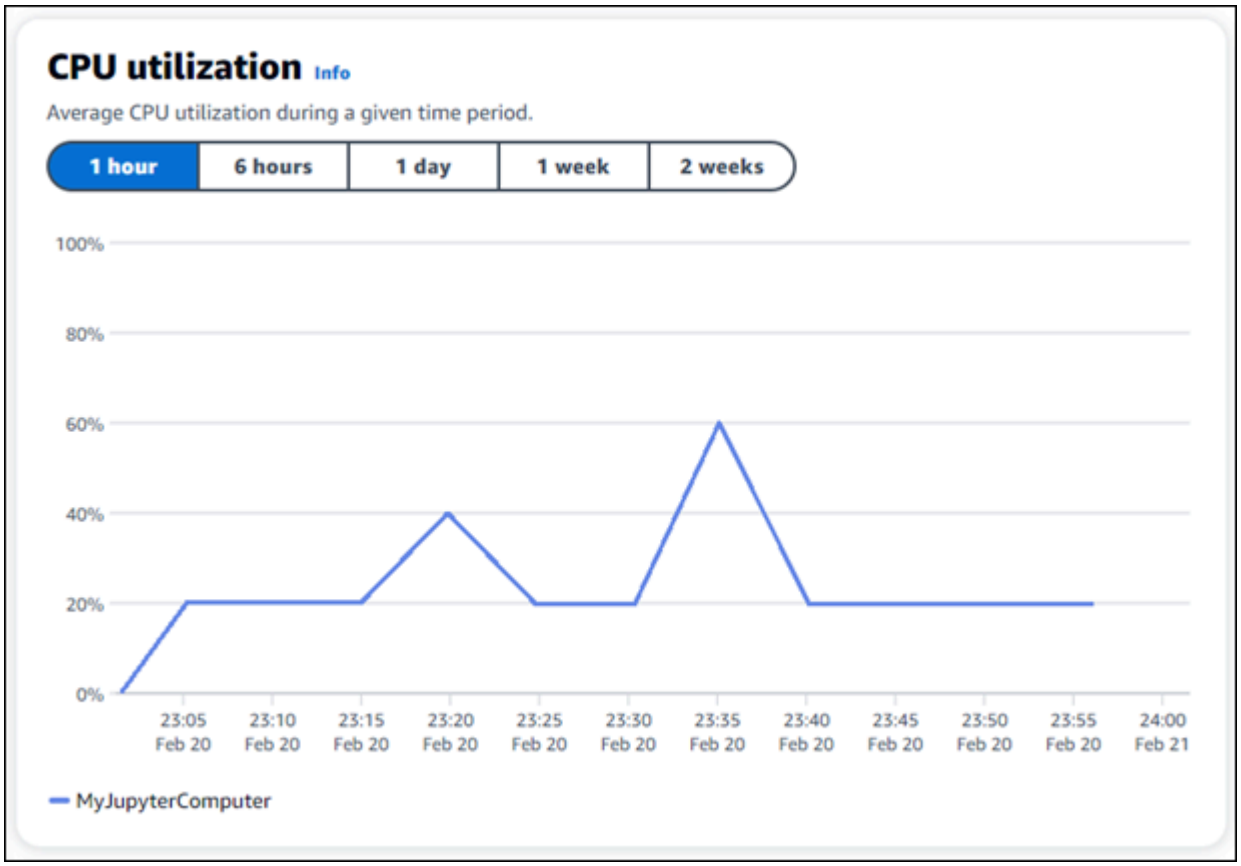
연구용 Lightsail에서 리소스의 예상 비용 및 사용량을 확인하십시오.

연구용 Lightsail 리소스의 월간 누계 비용 및 사용량 추정치는 연구용 Lightsail 콘솔의 다음 영역에 표시됩니다.

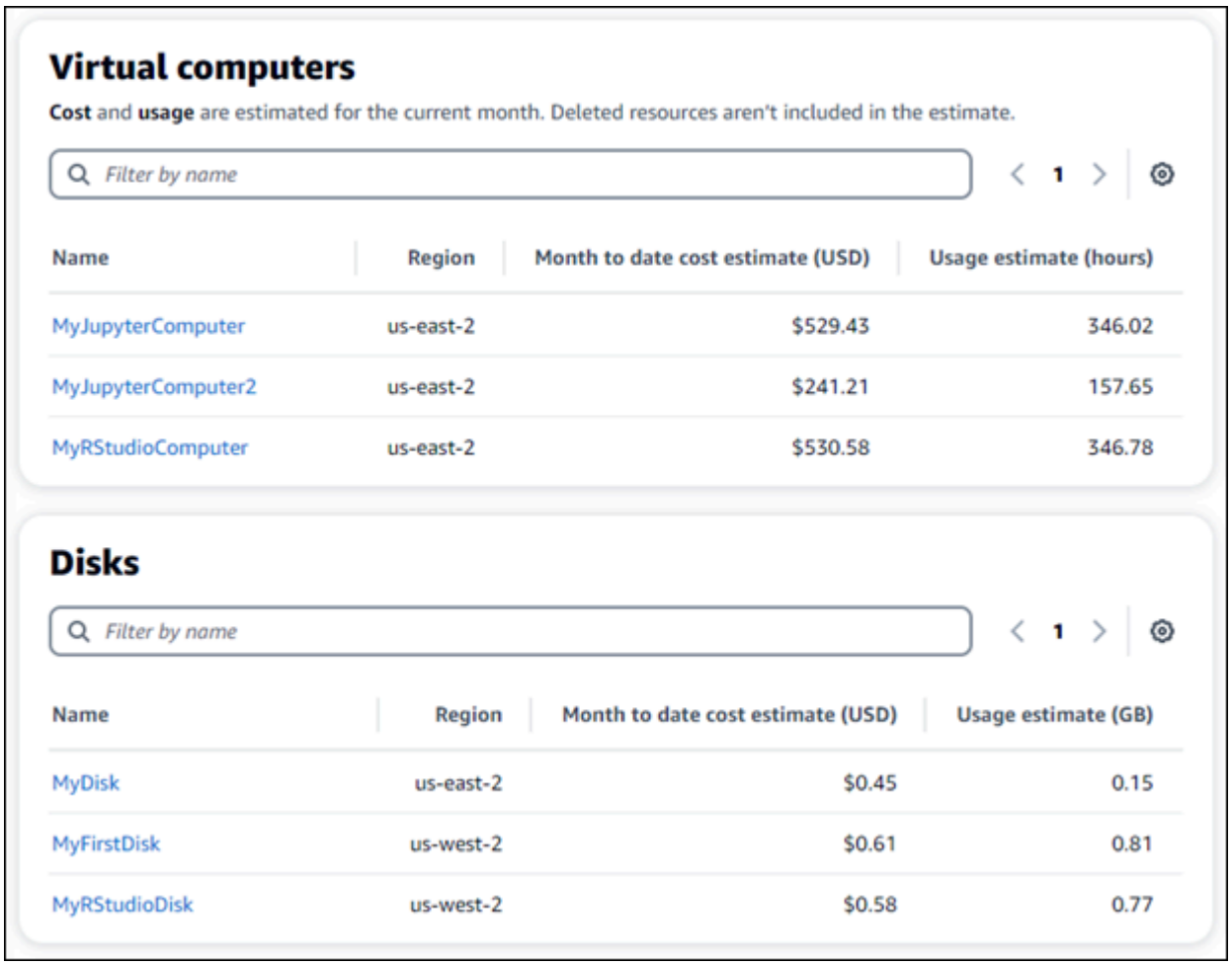
1. 연구용 Lightsail 콘솔의 탐색 창에서 가상 컴퓨터를 선택합니다. 실행 중인 각 가상 컴퓨터 아래에 가상 컴퓨터의 월 누계 예상 비용이 나열됩니다.



2. 가상 컴퓨터의 CPU 사용률을 보려면 가상 컴퓨터의 이름을 선택한 다음 대시보드 탭을 선택합니다.



3. 모든 Lightsail for Research 리소스의 월간 누계 비용 및 예상 사용량을 보려면 탐색 창에서 사용량을 선택합니다.



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

연구용 Lightsail에서 비용 관리 규칙을 관리합니다.

비용 관리에서는 사용자가 정의한 규칙을 사용하여 Lightsail for Research 가상 컴퓨터의 사용 및 비용을 관리할 수 있습니다.

일정 기간 동안 CPU 사용률이 지정된 비율에 도달하면 실행 중인 컴퓨터를 중지하는 유휴 상태에서 가상 컴퓨터 중지 규칙을 만들 수 있습니다. 예를 들어, 규칙은 30분 동안 특정 컴퓨터의 CPU 사용률이 5% 이하일 때 자동으로 중지할 수 있습니다. 이는 컴퓨터가 유휴 상태이고 Lightsail for Research가 컴퓨터를 중지함을 나타냅니다. 가상 컴퓨터가 중지된 후에는 더 이상 표준 시간당 요금이 발생하지 않습니다.

주제

연구용 Lightsail 가상 컴퓨터에 대한 비용 관리 규칙 생성

연구용 Lightsail 가상 컴퓨터에 대한 규칙을 만들려면 다음 단계를 완료하십시오.

> **Note**
>
> 현재 지원되는 유일한 규칙 동작은 가상 컴퓨터를 중지하는 것입니다. CPU사용률은 현재 규칙에 의해 모니터링되는 유일한 지표이며 지원되는 유일한 작업은 다음과 같거나 작습니다.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 비용 관리를 선택합니다.
3. Create rule을 선택합니다.
4. 규칙을 적용할 리소스를 선택합니다.
5. 규칙을 실행해야 하는 CPU 사용률과 기간을 지정합니다.

   예를 들어 5%와 30분을 지정할 수 있습니다. 연구용 Lightsail for Research는 30분 동안 컴퓨터 사용률이 5% 이하인 경우 CPU 컴퓨터를 자동으로 중지합니다.
6. Create rule을 선택합니다.
7. 새 규칙의 정보가 정확한지 확인한 다음 확인을 선택합니다.

연구용 Lightsail 가상 컴퓨터의 비용 관리 규칙을 삭제합니다.

연구용 Lightsail 가상 컴퓨터에 대한 규칙을 삭제하려면 다음 단계를 완료하십시오.

1. 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 비용 관리를 선택합니다.
3. 삭제할 규칙을 선택합니다.
4. Delete(삭제)를 선택합니다.
5. 규칙을 삭제할지 확인한 다음 삭제를 선택합니다.

태그를 사용하여 연구용 Lightsail 리소스를 정리하세요

연구용 Amazon Lightsail을 사용하면 리소스에 태그를 할당할 수 있습니다. 각 태그는 리소스를 효율적으로 관리할 수 있는 키와 선택적 값으로 구성된 레이블입니다. 값이 없는 키는 키 전용 태그라고 하고, 값이 있는 키는 키-값 태그라고 합니다. 고유한 태그 유형은 없지만 목적, 소유자, 환경 또는 기타 기준에 따라 리소스를 분류할 수 있습니다. 이는 동일한 유형의 리소스가 많을 때 유용합니다. 지정한 태그를 기반으로 특정 리소스를 신속하게 식별할 수 있습니다. 예를 들어, 각 리소스의 프로젝트 또는 우선순위를 추적하는 데 도움이 되는 태그 세트를 정의할 수 있습니다.

연구용 Amazon Lightsail 콘솔에서 다음 리소스를 태깅할 수 있습니다.

- 가상 컴퓨터
- 스토리지 디스크
- 스냅샷

태그에 적용되는 제한은 다음과 같습니다.

- 리소스당 최대 태그 수는 50개입니다.
- 각 리소스에 대해 각 태그 키는 고유해야 합니다. 각 태그 키는 하나의 값만 가질 수 있습니다.
- 최대 키 길이는 -8자의 유니코드 문자 128자입니다. UTF
- 최대 값 길이는 -8의 유니코드 문자 256자입니다. UTF
- 태깅 스키마를 여러 서비스와 리소스에서 사용하는 경우, 다른 서비스에서는 허용되는 문자에 제한이 있을 수 있다는 점에 주의하세요. 일반적으로 허용되는 문자는 문자, 숫자, 공백 및 `+ - = . _ : / @`입니다.
- 태그 키와 값은 대/소문자를 구분합니다.
- 키 또는 값에 `aws:` 접두사는 사용하지 않습니다. 해당 접두사는 사용하도록 예약되어 있습니다. AWS

주제

- 태그: 연구용 Lightsail 리소스
- 연구용 Lightsail 리소스에서 태그 제거

태그: 연구용 Lightsail 리소스

연구용 Lightsail 가상 컴퓨터용 태그를 만들려면 다음 단계를 완료하십시오. 연구용 Lightsail 디스크 및 스냅샷의 단계는 비슷합니다.

1. 연구용 Lightsail 콘솔에서 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 가상 컴퓨터를 선택합니다.
3. 태그를 생성할 가상 컴퓨터를 선택합니다.
4. 태그 탭을 선택합니다.
5. 태그 관리를 선택합니다.
6. 새 태그 추가를 선택합니다.
7. 키 필드에 키 이름을 입력합니다. 예: 프로젝트.
8. (선택 사항) 값 필드에 값 이름을 입력합니다. 예: 블로그.
9. 변경 내용 저장을 선택하여 키를 가상 컴퓨터에 저장합니다.

연구용 Lightsail 리소스에서 태그 제거

연구용 Lightsail 가상 컴퓨터에서 태그를 삭제하려면 다음 단계를 완료하십시오. 연구용 Lightsail 디스크 및 스냅샷의 단계는 비슷합니다.

1. 연구용 Lightsail 콘솔에서 연구용 Lightsail 콘솔에 로그인합니다.
2. 탐색 창에서 가상 컴퓨터를 선택합니다.
3. 태그를 삭제할 가상 컴퓨터를 선택합니다.
4. 태그 탭을 선택합니다.
5. 태그 관리를 선택합니다.
6. 리소스에서 태그를 삭제하려면 제거를 선택합니다.

> **Note**
>
> 태그의 값만 제거하려는 경우 값을 찾은 다음 옆에 있는 X 아이콘을 선택합니다.

7. 변경 사항 저장(Save changes)을 선택합니다.

연구용 Amazon Lightsail의 보안

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 기업과 귀사 간의 공동 책임입니다. AWS 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. Amazon Lightsail for Research에 적용되는 규정 준수 프로그램에 대해 자세히 알아보려면 규정 준수 프로그램별 범위 내 서비스 규정 준수 참조하십시오.
- 클라우드에서의 보안 — 사용하는 AWS 서비스에 따라 책임이 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Lightsail for Research를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 충족하도록 Lightsail for Research를 구성하는 방법을 보여줍니다. 또한 Lightsail for Research 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

연구용 Amazon Lightsail에서의 데이터 보호

AWS 공동 책임 모델 공동 책임 모델 이 모델에 설명된 대로, AWS 는 모든 모델을 실행하는 글로벌 인프라를 보호하는 역할을 합니다. AWS 클라우드사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터

프라이버시에 대한 자세한 내용은 데이터 프라이버시를 참조하십시오FAQ. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 공동 책임 모델 및AWS 보안 GDPR 블로그의 블로그 게시물을 참조하십시오.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 개별 사용자에게 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM) 를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정마다 다단계 인증 (MFA) 을 사용하십시오.
- SSLTLS/를 사용하여 AWS 리소스와 통신하세요. TLS1.2가 필요하고 TLS 1.3을 권장합니다.
- API를 사용하여 사용자 활동 로깅을 설정합니다 AWS CloudTrail.
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API an을 AWS 통해 액세스할 때 FIPS 140-3개의 검증된 암호화 모듈이 필요한 경우 엔드포인트를 사용하십시오. FIPS 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준 () 140-3을 참조하십시오. FIPS

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 Lightsail for Research 또는 AWS 서비스 다른 콘솔을 사용하여 작업하는 경우 또는 기타 API 콘솔을 사용하는 경우가 포함됩니다. AWS CLI AWS SDKs 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL a를 제공하는 경우 해당 서버에 대한 요청을 URL 검증하기 위해 자격 증명 정보를 에 포함하지 않는 것이 좋습니다.

연구용 Amazon Lightsail의 ID 및 Access 관리

AWS Identity and Access Management (IAM) 는 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. AWS IAM관리자는 Lightsail for Research 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. IAM추가 비용 없이 사용할 AWS 서비스 수 있습니다.

> **Note**
>
> Amazon Lightsail과 연구용 Lightsail은 동일한 정책 파라미터를 공유합니다. IAM 연구용 Lightsail 정책에 대한 변경 사항은 Lightsail 정책에도 영향을 미칩니다. 예를 들어 사용자가 Lightsail for Research에서 디스크를 만들 수 있는 권한을 가지고 있는 경우 같은 사용자가 Lightsail에서도 디스크를 만들 수 있습니다.

주제

고객

AWS Identity and Access Management (IAM) 를 사용하는 방법은 연구용 Lightsail에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - Lightsail for Research 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 Lightsail for Research 기능을 사용하여 작업을 수행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. 연구용 Lightsail의 기능에 액세스할 수 없는 경우 을 참조하십시오. 연구용 자격 증명 및 액세스를 위한 Amazon Lightsail 문제 해결

서비스 관리자 — 회사에서 연구용 Lightsail 리소스를 담당하고 있다면 연구용 Lightsail에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 사용자가 액세스해야 하는 Lightsail for Research 기능 및 리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음 IAM 관리자에게 서비스 사용자의 권한을 변경해 달라는 요청을 제출해야 합니다. 이 페이지의 정보를 검토하여 의 기본 개념을 IAM 이해하십시오. 회사에서 Lightsail을 연구용으로 사용하는 IAM 방법에 대해 자세히 알아보려면 을 참조하십시오. 연구용 Amazon Lightsail은 다음과 함께 작동하는 방식 IAM

IAM관리자 - 관리자인 경우 IAM Lightsail for Research에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대해 자세히 알아보는 것이 좋습니다. 에서 사용할 수 있는 Lightsail for Research ID 기반 정책의 예를 보려면 을 참조하십시오. IAM 연구용 Amazon Lightsail의 ID 기반 정책 예제

ID를 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM사용자로서 또는 역할을 위임하여 인증 (로그인 AWS) 을 받아야 합니다. AWS 계정 루트 사용자 IAM

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAMID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인하는 경우 관리자는 이전에 역할을 사용하여 ID 페더레이션을 설정했습니다. IAM 페더레이션을 AWS 사용하여 액세스하는 경우 간접적으로 역할을 수임하는 것입니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호로 서명할 수 있는 소프트웨어 개발 키트 (SDKCLI) 와 명령줄 인터페이스 () 가 AWS 제공됩니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 사용 IAM설명서의 AWS API요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, 계정 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 AWS 것을 권장합니다. 자세한 내용은 사용 설명서의 다단계 인증 및 사용 AWS IAM Identity Center 설명서의 다단계 인증 사용 (MFA) 을 IAM 참조하십시오. AWS

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 작업의 전체 목록은 사용 설명서의 루트 사용자 자격 증명이 필요한 작업을 참조하십시오. IAM

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS

Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAMIdentity Center에서 사용자 및 그룹을 만들거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 AWS 계정 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. ID 센터에 대한 자세한 내용은 IAM ID 센터란 IAM 무엇입니까? 를 참조하십시오. AWS IAM Identity Center 사용 설명서에서

IAM 사용자 및 그룹

IAM사용자란 단일 사용자 또는 애플리케이션에 대한 특정 권한을 가진 사용자 내의 ID입니다. AWS 계정 가능하면 암호 및 액세스 키와 같은 장기 자격 증명을 가진 IAM 사용자를 만드는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 특정 사용 사례에서 IAM 사용자의 장기 자격 증명이 필요한 경우에는 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 사용 설명서의 장기 자격 증명이 필요한 사용 사례에 대한 정기적인 액세스 키 IAM 교체를 참조하십시오.

IAM그룹은 IAM 사용자 컬렉션을 지정하는 ID입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어 이름을 지정한 IAMAdmins그룹을 만들고 해당 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세히 알아보려면 사용 설명서의 역할 대신 IAM 사용자를 만드는 시기를 참조하십시오. IAM

IAM역할

IAM역할은 특정 권한을 AWS 계정 가진 사용자 내의 ID입니다. IAM사용자와 비슷하지만 특정인과 관련이 있는 것은 아닙니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI or AWS API 작업을 호출하거나 사용자 지정을 사용하여 역할을 수임할 수 URL 있습니다. 역할 사용 방법에 대한 자세한 내용은 사용 IAM설명서의 IAM역할 사용을 참조하십시오.

IAM임시 자격 증명이 있는 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션을 위한 역할에 대한 자세한 내용은 IAM사용 설명서의 타사 ID 제공자를 위한 역할 생성을 참조하십시오. IAMIdentity Center를 사용하는 경우 권한 집합을 구성합니다. ID가 인증된 후 액세스할

수 있는 대상을 제어하기 위해 IAM Identity Center는 권한 집합을 역할의 상관 관계와 연결합니다. IAM 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.

- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할이 역할을 맡아 특정 작업에 대해 일시적으로 다른 권한을 부여받을 수 있습니다. IAM
- 계정 간 액세스 - IAM 역할을 사용하여 다른 계정의 사용자 (신뢰할 수 있는 사용자) 가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 하지만 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 계정 간 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 사용 설명서의 교차 계정 리소스 액세스를 참조하십시오. IAM IAM
- 서비스 간 액세스 — 일부는 다른 기능을 AWS 서비스 사용합니다. AWS 서비스예를 들어, 서비스를 호출하면 해당 서비스가 Amazon에서 애플리케이션을 EC2 실행하거나 Amazon S3에 객체를 저장하는 것이 일반적입니다. 서비스는직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS요청 시 적용되는 정책 세부 정보는 전달 액세스 세션을 참조하십시오.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 간주하는 IAM 역할입니다. IAM관리자는 내부에서 IAM 서비스 역할을 만들고, 수정하고, 삭제할 수 있습니다. 자세한 내용은 사용 설명서의 역할 만들기를 참조하여 권한을 위임하십시오IAM. AWS 서비스
  - 서비스 연결 역할 - 서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.
- Amazon에서 실행 중인 애플리케이션 EC2 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS API 요청을 보내는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS CLI EC2인스턴스 내에 액세스 키를 저장하는 것보다 이 방법이 더 좋습니다. EC2인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 만들어야 합니다. 인스턴스 프로필에는 역할이 포함되며, 이를 통해 EC2 인스턴스에서 실행 중인 프로그램이 임시 자격 증명을 얻을 수 있습니다. 자세한 내용은 사용 설명서의 IAM역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 IAM 참조하십시오.

IAM역할을 사용할지 IAM 사용자를 사용할지 알아보려면 사용 설명서의 IAM 역할 생성 시기 (사용자 대신) 를 IAM참조하십시오.

정책을 사용한 액세스 관리

정책을 만들고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON정책 문서의 구조 및 내용에 대한 자세한 내용은 IAM사용 설명서의 JSON 정책 개요를 참조하십시오.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. IAM관리자는 IAM 정책을 생성하여 필요한 리소스에서 작업을 수행할 수 있는 권한을 사용자에게 부여할 수 있습니다. 그러면 관리자가 역할에 IAM 정책을 추가할 수 있으며, 사용자는 역할을 수임할 수 있습니다.

IAM정책은 작업을 수행하는 데 사용하는 방법에 관계없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 에서 역할 정보를 가져올 수 AWS API 있습니다.

보안 인증 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. ID 기반 정책을 만드는 방법을 알아보려면 사용 설명서의 IAM정책 생성을 참조하십시오. IAM

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책과 인라인 정책 중에서 선택하는 방법을 알아보려면 IAM사용 설명서의 관리형 정책과 인라인 정책 중 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리

자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 IAM 정책에서는 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록 () ACLs

액세스 제어 목록 (ACLs) 은 리소스에 액세스할 수 있는 권한을 가진 주체 (계정 구성원, 사용자 또는 역할) 를 제어합니다. ACLs정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 JSON 비슷합니다.

지원하는 서비스의 VPC 예로는 Amazon S3와 Amazon이 ACLs 있습니다. AWS WAF자세한 내용은 Amazon 심플 스토리지 서비스 개발자 안내서의 액세스 제어 목록 (ACL) 개요를 참조하십시오. ACLs

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 - 권한 경계는 ID 기반 정책이 IAM 엔티티 (IAM사용자 또는 역할) 에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 사용 IAM설명서의 IAM 엔티티의 권한 경계를 참조하십시오.
- 서비스 제어 정책 (SCPs) - SCPs 조직 또는 OU (조직 단위) 에 대한 최대 권한을 지정하는 JSON AWS Organizations정책입니다. AWS Organizations 기업이 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직의 모든 기능을 사용하도록 설정하면 일부 또는 모든 계정에 서비스 제어 정책 (SCPs) 을 적용할 수 있습니다. 각 항목을 포함하여 구성원 계정의 엔티티에 대한 권한을 SCP AWS 계정 루트 사용자제한합니다. Organizations 및 SCPs 에 대한 자세한 내용은 AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하십시오.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM사용 설명서의 세션 정책을 참조하십시오.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련된 경우 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM사용 설명서의 정책 평가 로직을 참조하십시오.

연구용 Amazon Lightsail은 다음과 함께 작동하는 방식 IAM

Lightsail for Research에 대한 액세스를 관리하는 IAM 데 사용하기 전에 Lightsail for Research에서 사용할 수 있는 기능에 IAM 대해 알아보십시오.

IAM연구용 Amazon Lightsail과 함께 사용할 수 있는 기능

IAM특징:	연구 지원을 위한 Lightsail
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACLs	아니요
ABAC(정책의 태그)	부분
임시 보안 인증	예
보안 주체 권한	아니요
서비스 역할	아니요
서비스 연결 역할	아니요

Lightsail for Research 및 AWS 기타 서비스가 IAM 대부분의 기능과 어떻게 작동하는지 자세히 알아보려면 사용 설명서에서 IAM 함께 작동하는 서비스를AWS 참조하십시오. IAM

연구용 Lightsail의 ID 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. ID 기반 정책을 만드는 방법을 알아보려면 사용 설명서의 IAM정책 생성을 참조하십시오. IAM

IAMID 기반 정책을 사용하면 허용 또는 거부된 작업 및 리소스는 물론 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 사용 IAM설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

연구용 Lightsail의 ID 기반 정책 예제

연구용 Lightsail ID 기반 정책의 예를 보려면 을 참조하십시오. 연구용 Amazon Lightsail의 ID 기반 정책 예제

연구용 Lightsail 내의 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

계정 간 액세스를 활성화하려면 다른 계정의 전체 계정 또는 IAM 엔티티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM사용 설명서의 계정 간 리소스 액세스를 참조하십시오. IAM

연구용 Lightsail의 정책 조치

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

정책 `Action` 요소는 JSON 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 작업이 없는 권한 전용 작업과 같은 몇 가지 예외가 있습니다. API 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

연구용 Lightsail 작업 목록을 보려면 서비스 승인 참조의 Amazon Lightsail 연구용으로 정의한 작업을 참조하십시오.

연구용 Lightsail의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
lightsail
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

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

연구용 Lightsail ID 기반 정책의 예를 보려면 을 참조하십시오. 연구용 Amazon Lightsail의 ID 기반 정책 예제

연구용 Lightsail을 위한 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource`JSON정책 요소는 작업이 적용되는 하나 또는 여러 개의 객체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. Amazon 리소스 이름 (ARN) 을 사용하여 리소스를 지정하는 것이 가장 좋습니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

연구용 Lightsail 리소스 유형 및 ARNs 해당 유형의 목록을 보려면 서비스 인증 참조의 Amazon Lightsail 연구용으로 정의한 리소스를 참조하십시오. 각 리소스에 어떤 작업을 지정할 수 있는지 알아보려면 Amazon Lightsail for Research에서 정의한 작업을 참조하십시오. ARN

연구용 Lightsail ID 기반 정책의 예를 보려면 을 참조하십시오. 연구용 Amazon Lightsail의 ID 기반 정책 예제

연구용 Lightsail의 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어 리소스에 IAM 사용자 이름이 태그가 지정된 경우에만 리소스에 대한 액세스 권한을 IAM 사용자에게 부여할 수 있습니다. 자세한 내용은 IAM사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM사용 설명서의AWS 글로벌 조건 컨텍스트 키를 참조하십시오.

연구용 Lightsail 조건 키 목록을 보려면 서비스 승인 참조의 연구용 Amazon Lightsail 조건 키를 참조하십시오. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 Amazon Lightsail for Research에서 정의한 작업을 참조하십시오.

연구용 Lightsail ID 기반 정책의 예를 보려면 을 참조하십시오. 연구용 Amazon Lightsail의 ID 기반 정책 예제

ACLs연구용 Lightsail에서

지원 ACLs: 아니요

액세스 제어 목록 (ACLs) 은 리소스에 액세스할 수 있는 권한을 가진 주체 (계정 구성원, 사용자 또는 역할) 를 제어합니다. ACLs정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 JSON 비슷합니다.

ABAC연구용 Lightsail 사용

지원 ABAC (정책의 태그): 부분

속성 기반 액세스 제어 (ABAC) 는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM엔티티 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. 의 ABAC 첫 번째 단계는 엔티티와 리소스에 태그를 지정하는 것입니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC빠르게 성장하는 환경에서 유용하며 정책 관리가 복잡해지는 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

에 대한 자세한 내용은 What is ABAC? 를 참조하십시오. ABAC IAM사용 설명서에서. 설정 ABAC 단계가 포함된 자습서를 보려면 사용 IAM설명서의 속성 기반 액세스 제어 사용 (ABAC) 을 참조하십시오.

연구용 Lightsail에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명을 사용하여 로그인하면 일부 자격 증명이 AWS 서비스 작동하지 않습니다. 임시 자격 증명을 사용하는 AWS 서비스 방법을 비롯한 추가 정보는 IAM사용 설명서의 AWS 서비스 해당 자격 증명을 참조하십시오. IAM

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하는 경우 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 Single Sign-On (SSO) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그

인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM사용 설명서의 역할 전환 (콘솔) 을 참조하십시오.

AWS CLI 또는 를 사용하여 임시 자격 증명을 수동으로 생성할 수 AWS API 있습니다. 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 내용은 의 임시 보안 자격 증명을 참조하십시오. IAM

연구용 Lightsail에 대한 크로스 서비스 주체 권한

순방향 액세스 세션 지원 (): 아니요 FAS

에서 IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 사용자는 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS를 호출하는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. AWS 서비스 FAS요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS요청 시 적용되는 정책 세부 정보는 전달 액세스 세션을 참조하십시오.

연구용 Lightsail의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 IAM역할을 말합니다. IAM관리자는 내부에서 IAM 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 사용 설명서의 역할 만들기를 참조하여 권한을 위임하십시오IAM. AWS 서비스

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 Lightsail for Research 기능이 작동하지 않을 수 있습니다. Lightsail for Research가 이에 대한 지침을 제공하는 경우에만 서비스 역할을 편집하십시오.

연구용 Lightsail의 서비스 연계 역할

서비스 링크 역할 지원: 아니요

서비스 연결 역할은 다음과 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되

며 해당 서비스가 소유합니다. IAM관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

서비스 연결 역할을 만들거나 관리하는 방법에 대한 자세한 내용은 함께 작동하는 AWS 서비스를 참조하십시오. IAM 서비스 연결 역할 열에서 Yes(이)가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

연구용 Amazon Lightsail의 ID 기반 정책 예제

기본적으로 사용자와 역할에는 Lightsail for Research 리소스를 만들거나 수정할 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 를 사용하여 작업을 수행할 수 없습니다. AWS API IAM관리자는 IAM 정책을 생성하여 필요한 리소스에서 작업을 수행할 수 있는 권한을 사용자에게 부여할 수 있습니다. 그러면 관리자가 역할에 IAM 정책을 추가할 수 있으며, 사용자는 역할을 수임할 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 만드는 방법을 알아보려면 사용 IAM설명서에서 IAM 정책 생성을 참조하십시오.

각 리소스 유형의 형식을 비롯하여 Lightsail for Research에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 인증 참조의 Amazon Lightsail for Research용 작업, 리소스 및 조건 키를 참조하십시오. ARNs

주제

- 정책 모범 사례
- 연구용 Lightsail 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

정책 모범 사례

ID 기반 정책에 따라 계정에서 Lightsail for Research 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책으로 시작하고 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하십시오. 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 내용은 IAM사용 설명서의 AWS 관리형 정책 또는 작업 기능에 대한AWS 관리형 정책을 참조하십시오.

- 최소 권한 적용 — IAM 정책으로 권한을 설정하는 경우 작업 수행에 필요한 권한만 부여하십시오. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. 를 사용하여 권한을 IAM 적용하는 방법에 대한 자세한 내용은 사용 설명서의 정책 및 권한을 참조하십시오. IAM IAM
- IAM정책의 조건을 사용하여 액세스를 추가로 제한 - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, 를 사용하여 모든 요청을 전송하도록 지정하는 정책 조건을 작성할 수 SSL 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 내용은 IAM사용 설명서의 IAMJSON정책 요소: 조건을 참조하십시오.
- IAMAccess Analyzer를 사용하여 IAM 정책을 검증하여 안전하고 기능적인 권한을 보장합니다. IAM Access Analyzer는 새 정책과 기존 정책을 검증하여 정책이 IAM 정책 언어 (JSON) 및 IAM 모범 사례를 준수하는지 확인합니다. IAMAccess Analyzer는 안전하고 기능적인 정책을 작성하는 데 도움이 되는 100개 이상의 정책 검사와 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 사용 설명서의 IAMAccess Analyzer 정책 검증을 참조하십시오. IAM
- 다단계 인증 필요 (MFA) - 사용자 또는 루트 IAM 사용자가 필요한 시나리오가 있는 경우 보안을 강화하려면 이 기능을 MFA 켜십시오. AWS 계정 API작업 호출 MFA 시기를 요구하려면 정책에 MFA 조건을 추가하세요. 자세한 내용은 IAM사용 설명서의 MFA -보호된 API 액세스 구성을 참조하십시오.

의 모범 사례에 IAM 대한 자세한 내용은 IAM사용 설명서의 보안 모범 사례를 참조하십시오. IAM

연구용 Lightsail 콘솔 사용

Amazon Lightsail for Research 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 Lightsail for Research 리소스의 세부 정보를 나열하고 볼 수 있어야 합니다. AWS 계정최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 에만 전화를 거는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. AWS API 대신 수행하려는 작업과 일치하는 API 작업에만 액세스를 허용하세요.

사용자와 역할이 연구용 Lightsail 콘솔을 계속 사용할 수 있도록 하려면 연구용 Lightsail 또는 관리형 정책도 엔티티에 `ConsoleAccess` 연결하십시오. `ReadOnly` AWS 자세한 내용은 사용 설명서의 사용자에게 권한 추가를 참조하십시오. IAM

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제에서는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 만드는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 OR를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 AWS CLI 권한이 포함됩니다. 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": "*"
        }
    ]
}
```

연구용 자격 증명 및 액세스를 위한 Amazon Lightsail 문제 해결

다음 정보를 사용하면 Lightsail for Research 및 을 (를) 사용할 때 발생할 수 있는 일반적인 문제를 진단하고 해결하는 데 도움이 됩니다. IAM

주제

- 연구용 Lightsail에서 작업을 수행할 권한이 없습니다.
- 외부 사용자가 Lightsail for Research AWS 계정 리소스에 액세스할 수 있도록 허용하고 싶습니다.

연구용 Lightsail에서 작업을 수행할 권한이 없습니다.

작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 권한이 없는 경우 발생합니다. `lightsail:`*`GetWidget`*

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

이 경우 `lightsail:`*`GetWidget`*작업을 사용하여 *`my-example-widget`*리소스에 액세스할 수 있도록 `mateojackson`사용자 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

외부 사용자가 Lightsail for Research AWS 계정 리소스에 액세스할 수 있도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록 (ACLs) 을 지원하는 서비스의 경우 해당 정책을 사용하여 사용자에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- 연구용 Lightsail이 이러한 기능을 지원하는지 알아보려면 을 참조하십시오. 연구용 Amazon Lightsail은 다음과 함께 작동하는 방식 IAM
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 사용 설명서에서 소유한 다른 IAM AWS 계정 사용자의 액세스 권한 제공을 IAM 참조하십시오.

- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM사용 설명서의 제3자가 AWS 계정 소유한 리소스에 대한 액세스 제공을 참조하십시오. AWS 계정
- ID 페더레이션을 통해 액세스를 제공하는 방법을 알아보려면 사용 설명서의 외부 인증된 사용자에게 액세스 제공 (ID 페더레이션) 을 IAM 참조하십시오.
- 계정 간 액세스에 대한 역할 사용과 리소스 기반 정책의 차이점을 알아보려면 사용 설명서의 계정 간 리소스 액세스를 참조하십시오. IAM IAM

연구용 Amazon Lightsail에 대한 규정 준수 검증

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 적합한 애플리케이션을 만드는 AWS HIPAA 데 사용할 수 있는 방법을 설명합니다.

> **Note**
>
> 모든 AWS 서비스 사람이 자격이 있는 것은 아닙니다. HIPAA 자세한 내용은 HIPAA적격 서비스 참조를 참조하십시오.

- AWS 규정AWS 준수 리소스 — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (국립 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (), 국제 표준화 기구 ()) 를 포함한PCI) 전반의 보안 제어에 대한 지침을 매핑합니다. ISO

- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하는 PCI DSS 등 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

연구용 Amazon Lightsail의 레질리언스

AWS 글로벌 인프라는 가용 영역을 중심으로 구축됩니다. AWS 리전 AWS 리전 물리적으로 분리되고 격리된 여러 가용 영역을 제공합니다. 이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

가용 영역에 대한 AWS 리전 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

Lightsail for Research는 AWS 글로벌 인프라 외에도 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 여러 기능을 제공합니다. 자세한 내용은 연구용 Lightsail 스냅샷을 사용하여 가상 컴퓨터 및 디스크를 백업합니다. 및 연구용 Lightsail 가상 컴퓨터 또는 디스크의 스냅샷 생성 단원을 참조하세요.

연구용 Amazon Lightsail의 인프라 보안

연구용 Amazon Lightsail은 관리형 서비스로서 글로벌 네트워크 보안의 보호를 받습니다 AWS . AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 Lightsail for Research에 액세스할 수 있습니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안 ()TLS. TLS1.2가 필요하고 TLS 1.3을 권장합니다.
- (임시 디피-헬만) 또는 (타원 곡선 임시 디피-헬만PFS) 와 같이 완벽한 순방향 기밀성 DHE () 을 갖춘 암호 제품군. ECDHE Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 액세스 키 ID와 보안 주체와 연결된 비밀 액세스 키를 사용하여 요청에 서명해야 합니다. IAM 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

연구용 Amazon Lightsail의 구성 및 취약성 분석

구성 및 IT 제어는 귀하와 당사 고객 간의 AWS 공동 책임입니다. 자세한 내용은 AWS 공동 책임 모델을 참조하십시오.

연구용 Amazon Lightsail의 보안 모범 사례

Lightsail for Research는 자체 보안 정책을 개발하고 구현할 때 고려할 수 있는 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 참고용으로만 사용해 주십시오.

Lightsail for Research 사용과 관련된 잠재적 보안 이벤트를 방지하려면 다음 모범 사례를 따르십시오.

- 첫 번째 콘솔에 인증하여 Lightsail for Research 콘솔에 액세스하십시오. AWS Management Console 개인 콘솔 자격 증명을 공유하지 마세요. 인터넷을 사용하는 모든 사용자는 콘솔을 탐색할 수 있지만 콘솔에 대한 유효한 자격 증명이 없으면 로그인하거나 세션을 시작할 수 없습니다.

Lightsail for Research 사용 설명서에 대한 문서 이력

다음 표에서는 Lightsail for Research에 대한 문서 릴리스를 소개합니다.

변경 사항	설명	날짜
최초 릴리스	Lightsail for Research 사용 설명서의 최초 릴리스입니다.	2023년 2월 28일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.