

# Foreword

This document contains initial setup instructions along with solutions to all of the lab exercises in the SEC495 *Leveraging LLMs: Building & Securing RAG, Contextual RAG, and Agentic RAG* course. This course was created to rapidly provide you with all of the key knowledge and hands-on experience necessary to build useful RAG solutions in an enterprise without the need to consume paid APIs or send your sensitive information out of the enterprise to an API. The goal is to provide information security professionals with all of the information necessary to implement these types of solutions, whether for a chatbot sitting in a Slack or Teams channel, a more effective helpdesk/knowledgebase solution, or any other application where your organization can benefit from using a generative AI solution for knowledge retrieval.

## Getting Started

All of the lab exercises in this course assume that you are using the provided containerized environment with all of the necessary servers, data, and Jupyter notebooks. While you can pull these pieces apart (and you may want to do this sometime *after* completing all of the labs, especially if you wish to build a production solution that leverages GPUs or that can leverage the scalability of Kubernetes or another container platform), we strongly recommend that you use them within Docker or Rancher as delivered to you. These notebooks will also work in other environments that support IPython, like Visual Studio Code and others, but will require changes to connect to the containers. All of the instructions in the book will assume that you are using Rancher Desktop with the provided containers. If you choose to use something else and run into trouble, you are welcome to write in for support, but please do not be offended if the suggestion comes back that you use the provided containers to run the labs. If you are looking for assistance for a possible production deployment, feel free to reach out to me directly and I will assist you if possible: dhoelzer@enclaveforensics.com.

## Objectives

- Install and prepare your system for class.
- Install Rancher Desktop
- Convince Rancher to pull all of the required containers from Docker Hub.

## Lab Preparation

### Download and Copy Course Files

1. Download the ISO image containing lab exercises and supporting data from your SANS Portal by navigating to <https://www.sans.org/account/course-materials>, selecting **SEC495: Leveraging LLMs: Building & Securing RAG, Contextual RAG, and Agentic RAG**, and clicking on the ISO file link (e.g., SEC495.25.1.iso) under **Media / Lab Files**.

2. Mount the ISO file on your local system by double-clicking it.
3. You will find a folder called **Exercises** in the mounted ISO file. This folder contains all of the exercises, solutions, and data files for the lab exercises throughout the course. There is also a **Solutions** subfolder within that has completed and functional Jupyter notebooks for every lab in the class.
4. If you choose to work through any of the labs on your own, we would recommend that you have this PDF. While you can certainly open the solution notebooks at any time, there is the potential risk that you inadvertently edit something, breaking the notebook. Also, it can be tempting to just use the completed notebook as-is, rather than working through the problem yourself.
5. To force yourself to work through the problem, follow along with your instructor or, if you are challenging yourself, work through each lab with this volume handy so that you can refer to it for hints only as needed. Since this course is only offered through OnDemand, you have the opportunity to pause the video after each discussion leading to the creation of code for a cell and can test yourself, working through the code either immediately before or immediately after the instructor demonstrates the solution.
6. You will want to copy this folder to your local system by right-clicking on the folder name (1), choosing **Copy** (2), and then pasting the folder somewhere on your local system. We recommend the path to your Desktop so that everything is easy to find.

## Install Rancher Desktop

7. The root directory of the mounted ISO contains Rancher Desktop installation packages for MacOS (Intel and ARM) and Windows (x86\_64 only). Locate the installer that matches your operating system and start it by double-clicking.

Rancher Desktop is also fully supported on x86\_64 hosts running Linux, but you will need to visit <https://docs.rancherdesktop.io/getting-started/installation/#linux> and follow the directions that apply to your type of Linux system.

If you are using MacOS, continue on. If you are working on a Windows system, proceed to the *Windows Instructions* and step 16.

## MacOS Instructions

8. After mounting the Rancher Desktop installer by double-clicking, it should automatically open the following window. If it doesn't, locate the Rancher Desktop icon on your desktop and double-click on it to reveal the following:

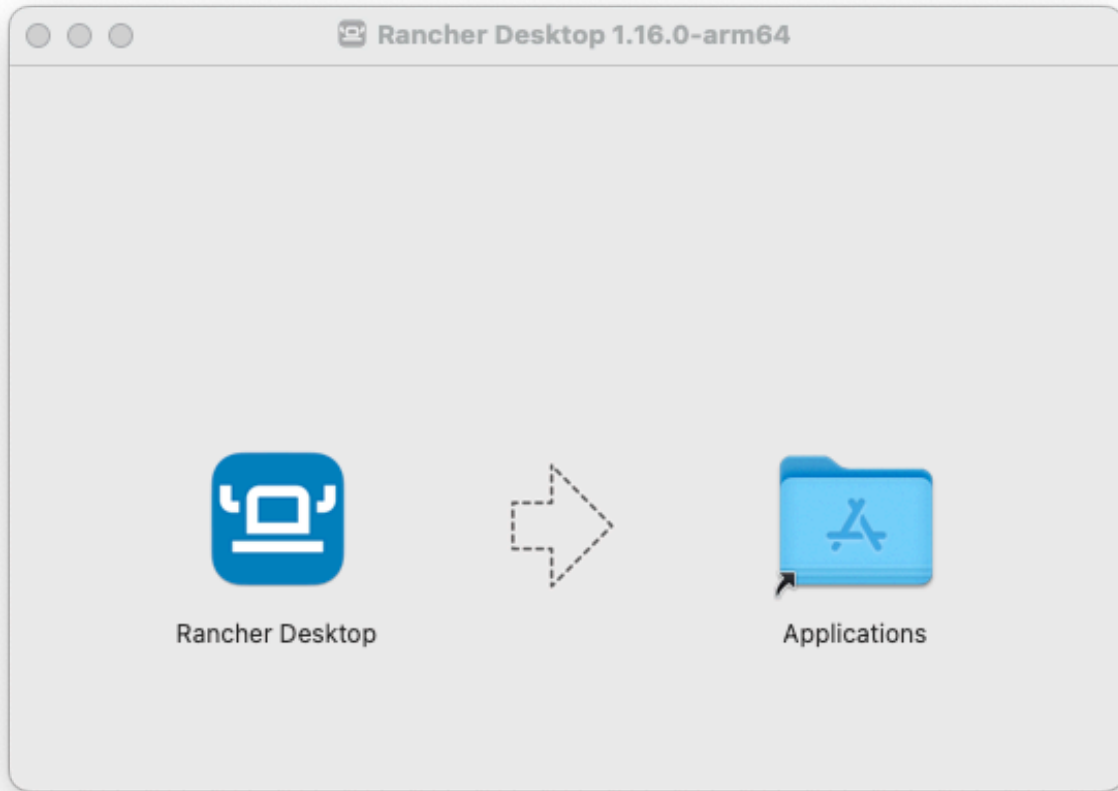


Figure 1: Rancher Installation

9. Click and drag the Rancher Desktop icon in the Rancher Desktop installer package into your Applications folder.
10. Hold down the Command key and press the space bar to open the Spotlight search. Search for Rancher Desktop. Press the Enter key to open it.

11. The Rancher Desktop interface will open. Be patient. It will take it some time to get all of the required pieces up and running. You will likely be prompted to allow Rancher to access the folder where the exercises are located. Please permit this. Eventually, you will see an interface very similar to this:

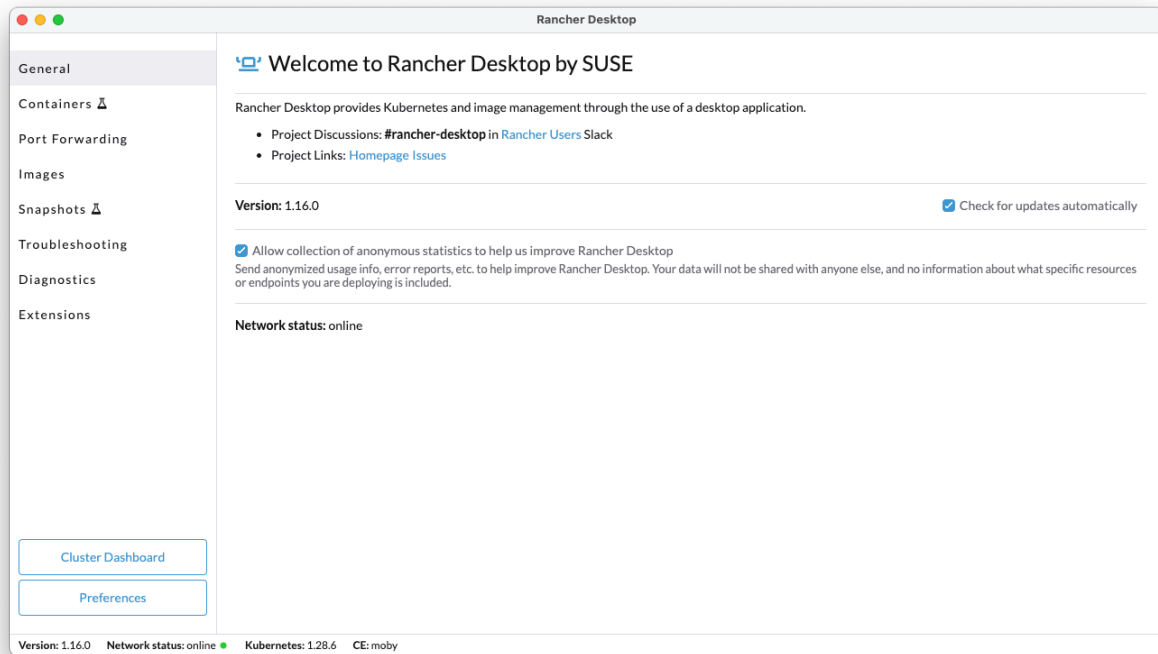


Figure 2: Rancher Desktop Interface

12. At some point, you will be asked to allow Rancher to discover devices on the network. Please permit this. Rancher on the Mac will run a VM under the hood. The default settings for the VM are not sufficient for our class. We also want to ensure that the other options are correct. Click on the **Preferences** button on the main Rancher Desktop interface:

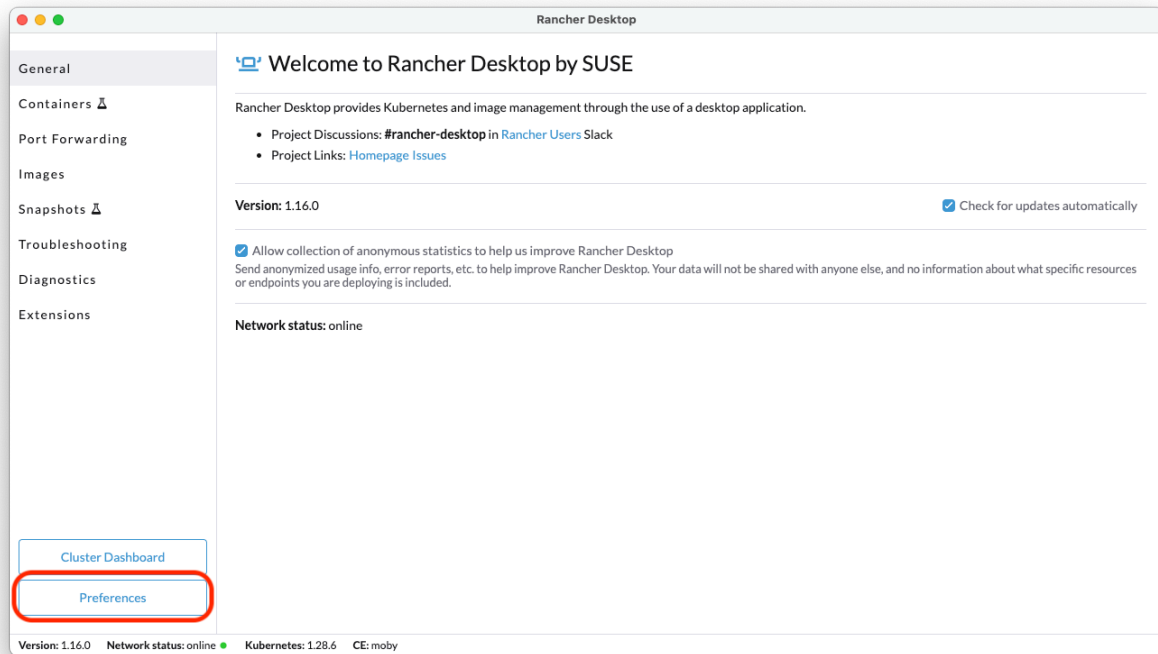


Figure 3: Rancher Preferences Button

13. Verify that the options in your preferences panel match those in the image below:

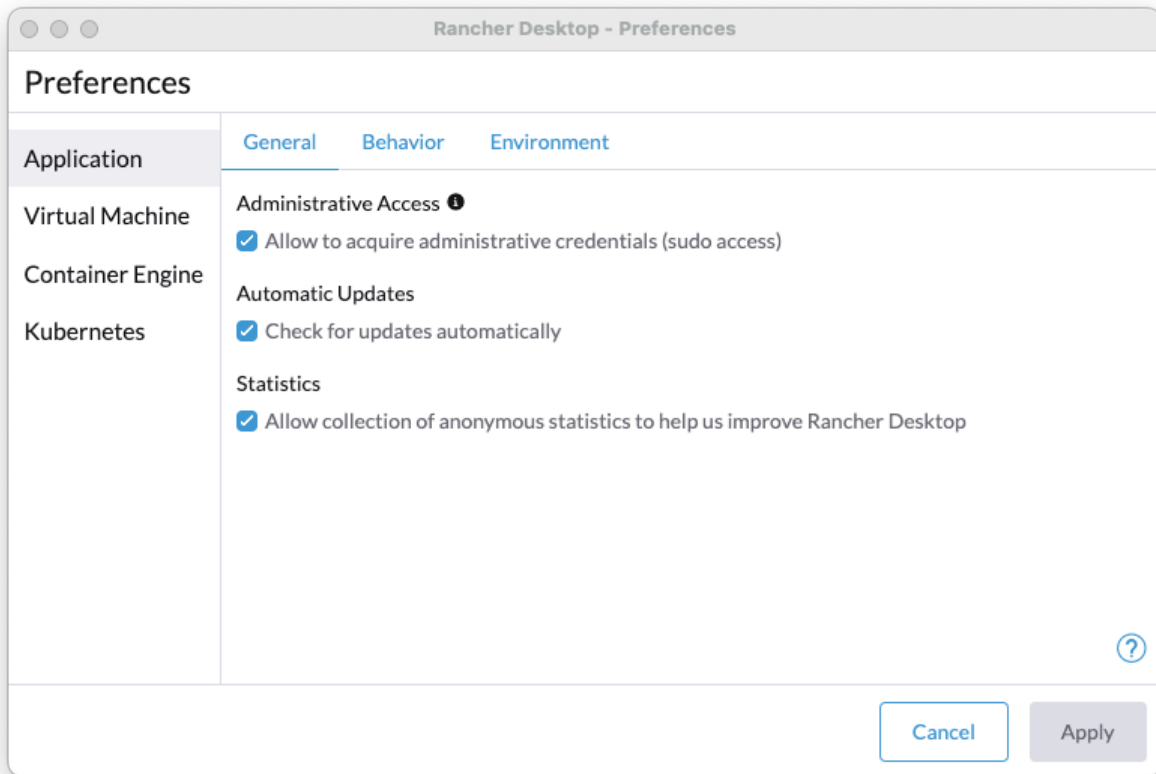


Figure 4: Rancher Options

- Click on the Virtual Machine section of the preferences panel. Adjust the virtual machine memory and CPU count to match the following:

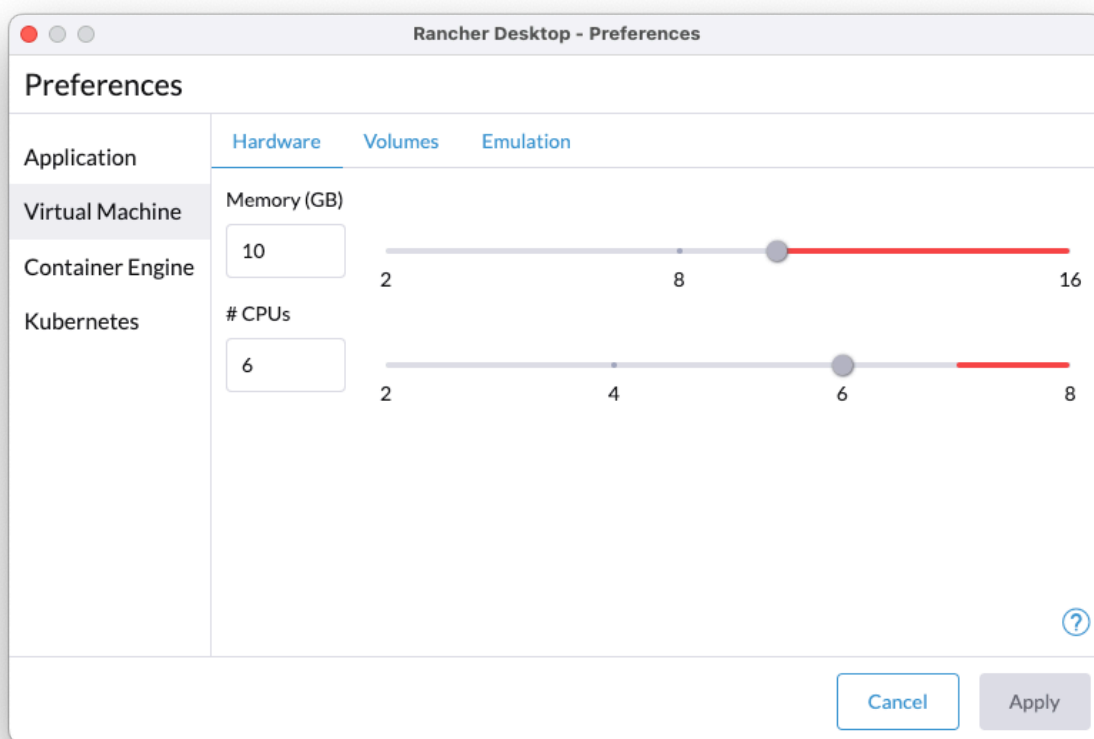


Figure 5: Rancher VM Settings

- Proceed to step 25.

## Windows Instructions

16. Double-click the Rancher Desktop installer. It is named Rancher.Desktop.Installer with a version number.
17. Shortly after starting the installer, you will be prompted to accept the software license agreement:

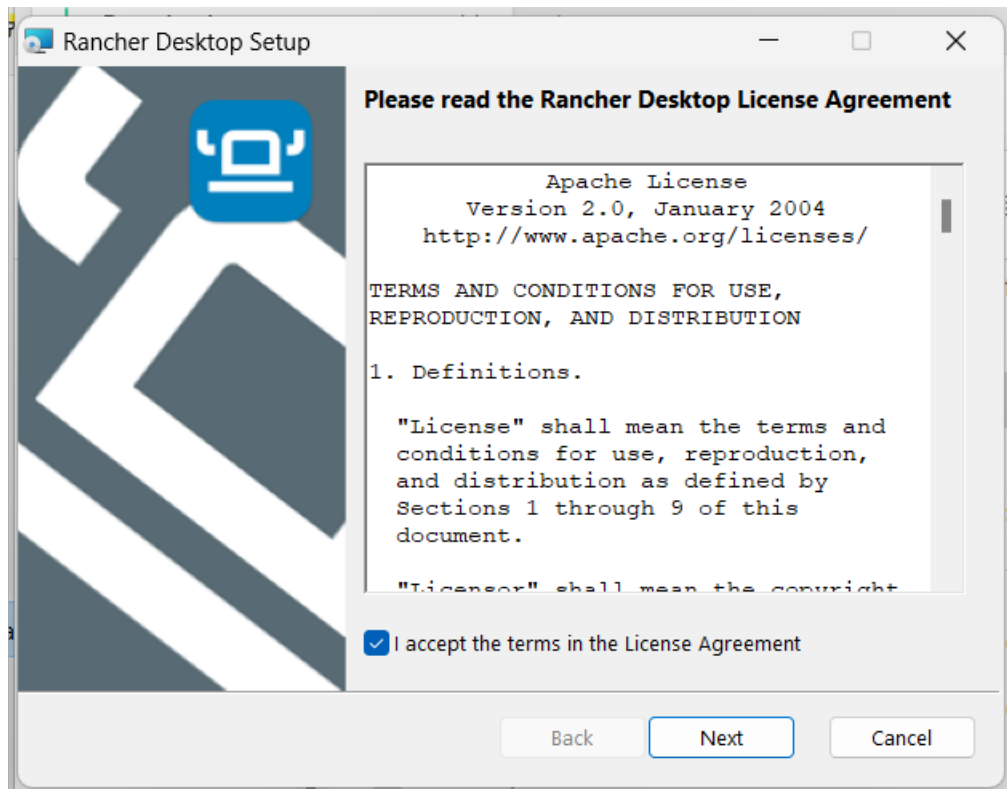


Figure 6: Rancher License



18. Click on the **Install** button to allow Rancher Desktop to install. Be aware that you will likely receive a security prompt asking you to allow the installation to occur. At times, this prompt does not come to the fore. If nothing happens after 10 or more seconds, try using Alt-Tab to see if there is an Allow window hiding somewhere.

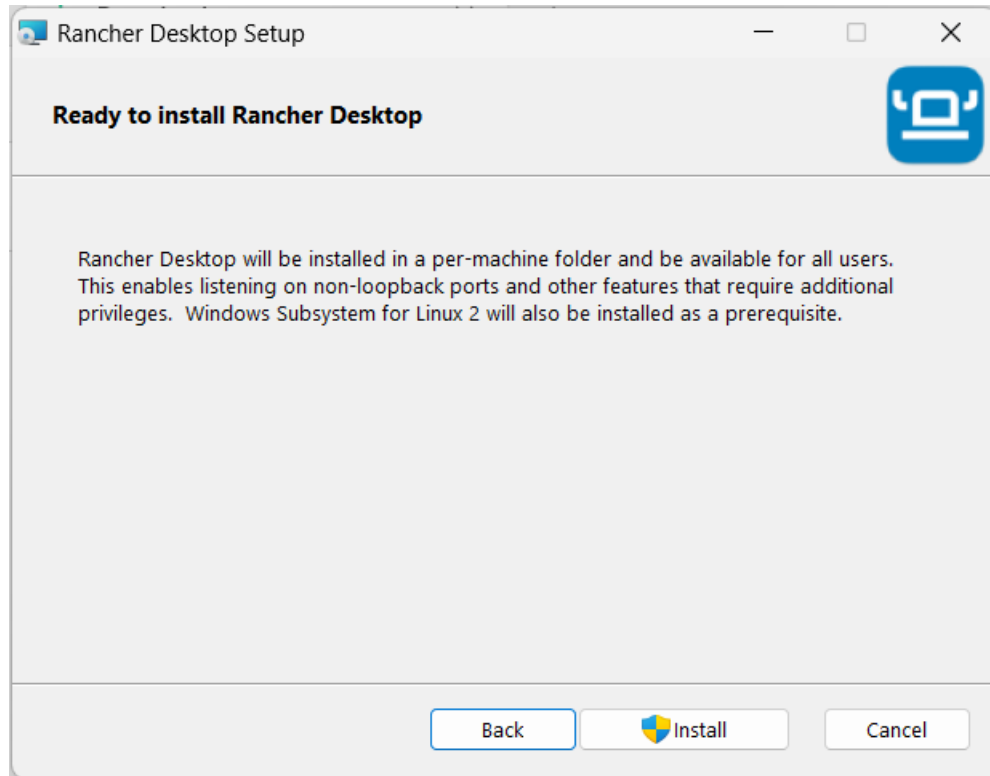


Figure 7: Installation

19. The installation will now proceed:

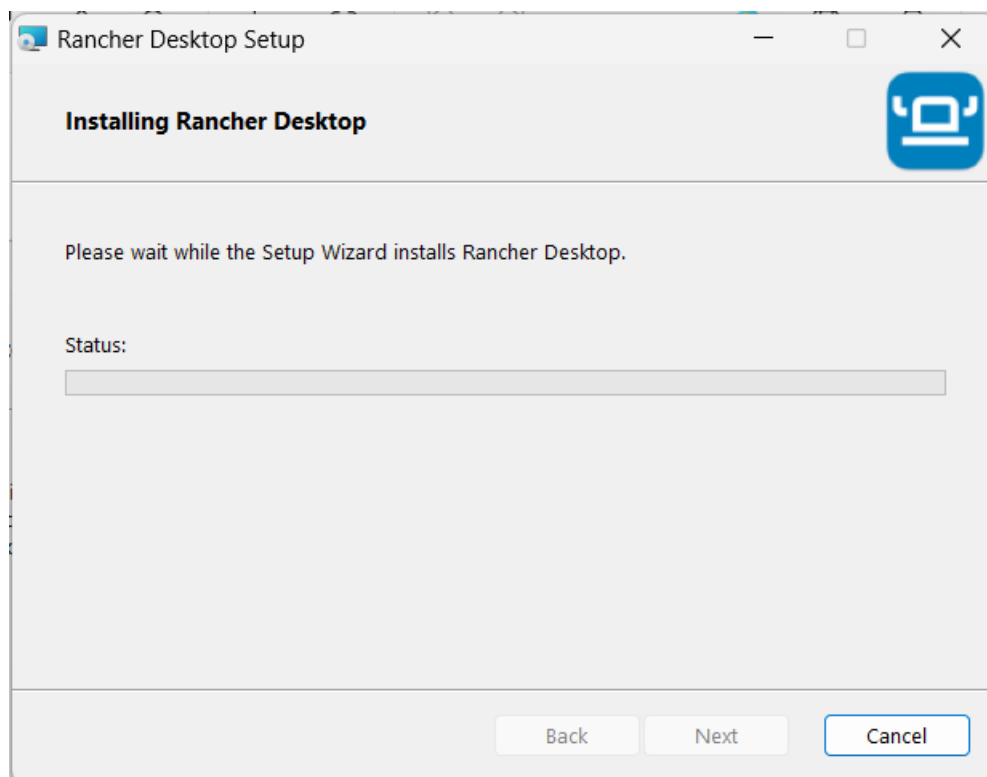


Figure 8: Installation Prompt

At some point, you may be prompted to allow the WSL (Windows Subsystem for Linux) to be installed and enabled. Allow this action. It may also proceed silently.

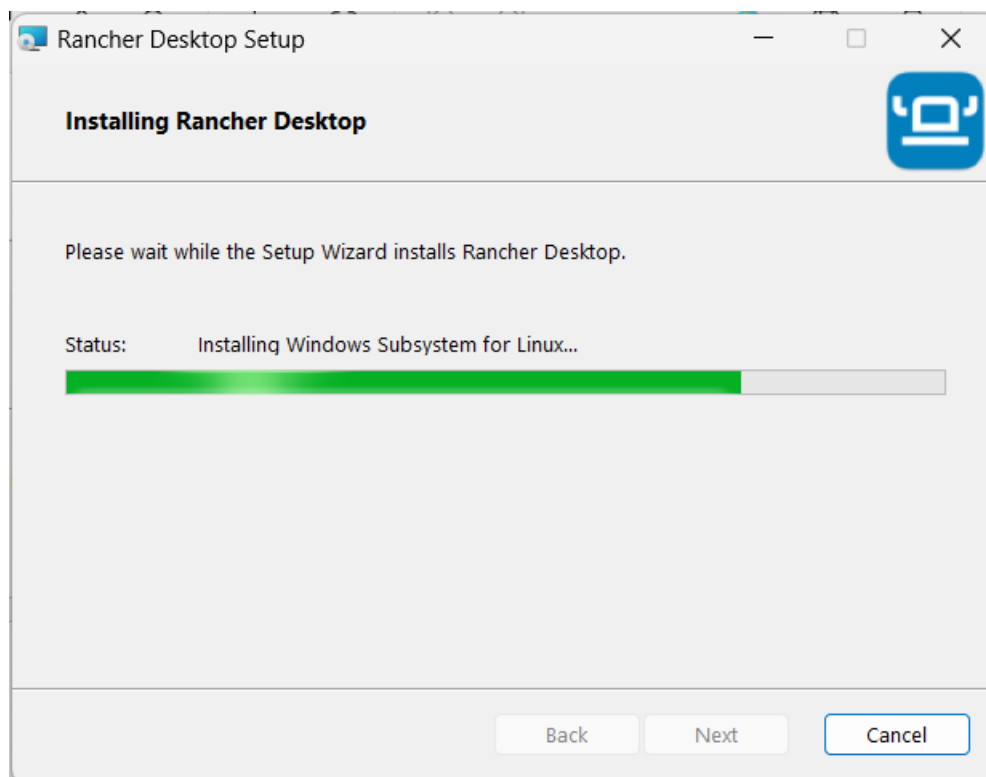


Figure 9: WSL Being Installed

20. When the installation completes, click **Finish**.

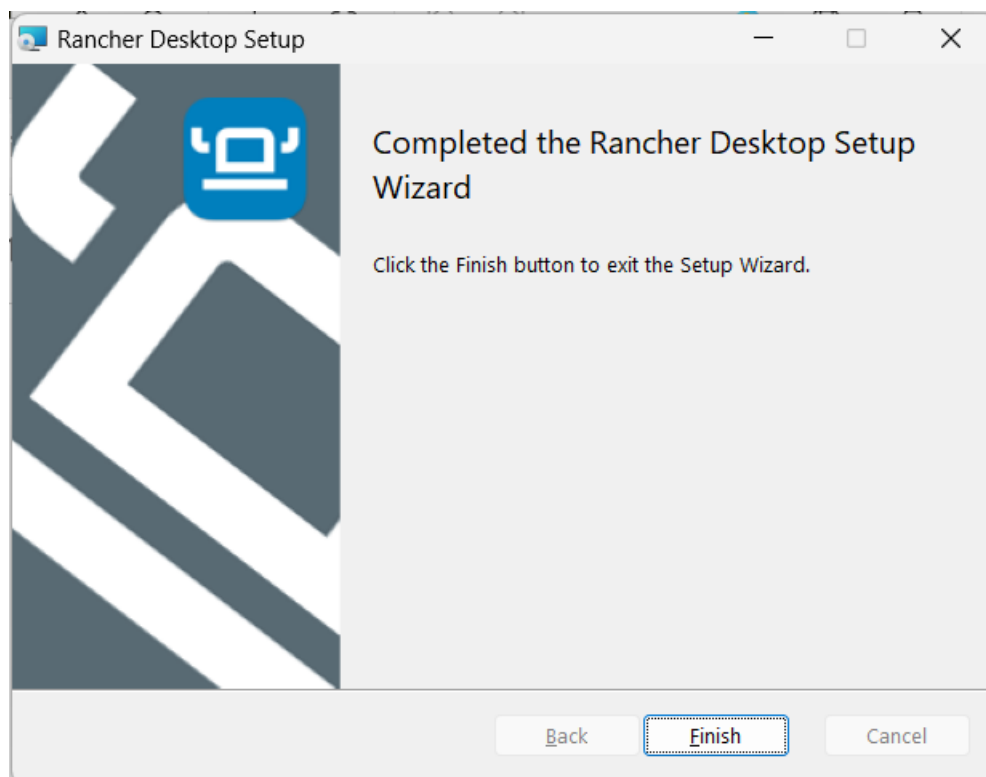


Figure 10: Installation Finished

21. You will now be prompted to restart your computer. Before doing so, please open a Windows command prompt and execute the command `wsl --update`. This may not always be required, but if you previously had the WSL installed, it might need updating. Please do this now. Also, even if Rancher does not prompt you to restart, please reboot your computer now.

•

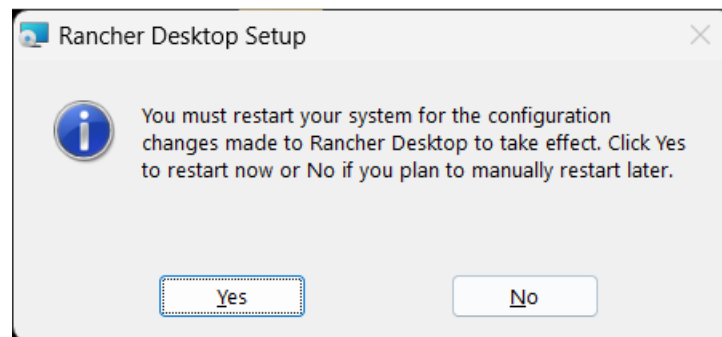


Figure 11: Restart Computer

22. Locate the Rancher Desktop icon on your desktop. Double-click this icon to start Rancher.

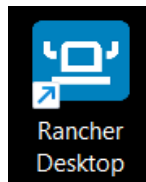


Figure 12: Rancher Icon

23. After a few seconds, a welcome dialog will open. Ensure that Enable Kubernetes is checked and that the Container Engine is set to “dockerd (moby)”. Please note that the Kubernetes version displayed on your system might be higher since newer releases may be available.

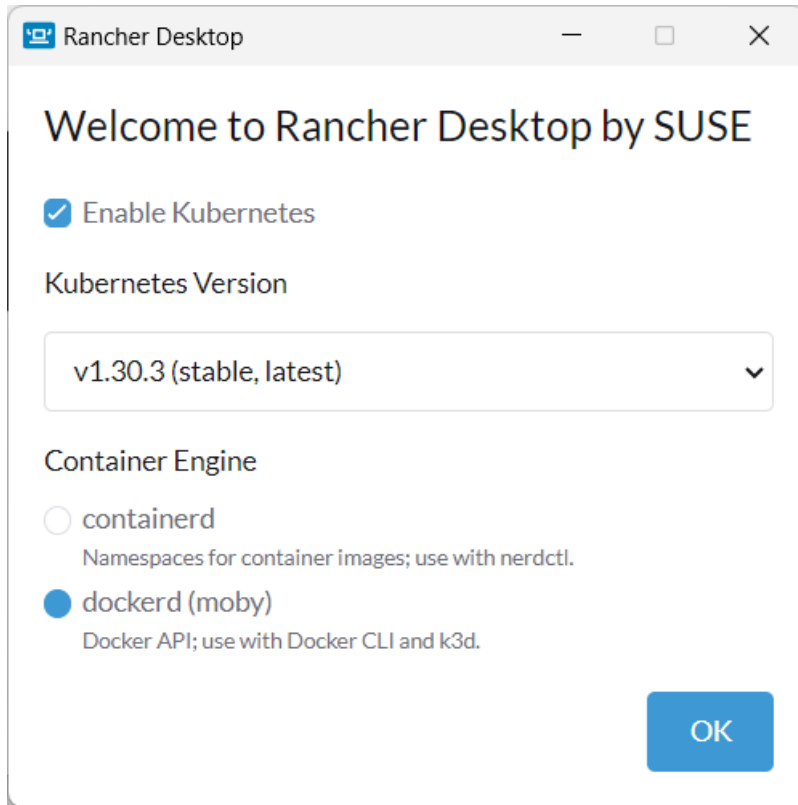


Figure 13: Rancher Welcome

24. The Rancher Desktop interface will now open. Please wait patiently while all of the supporting services are started. You will see a progress bar in the lower right-hand corner of the panel:

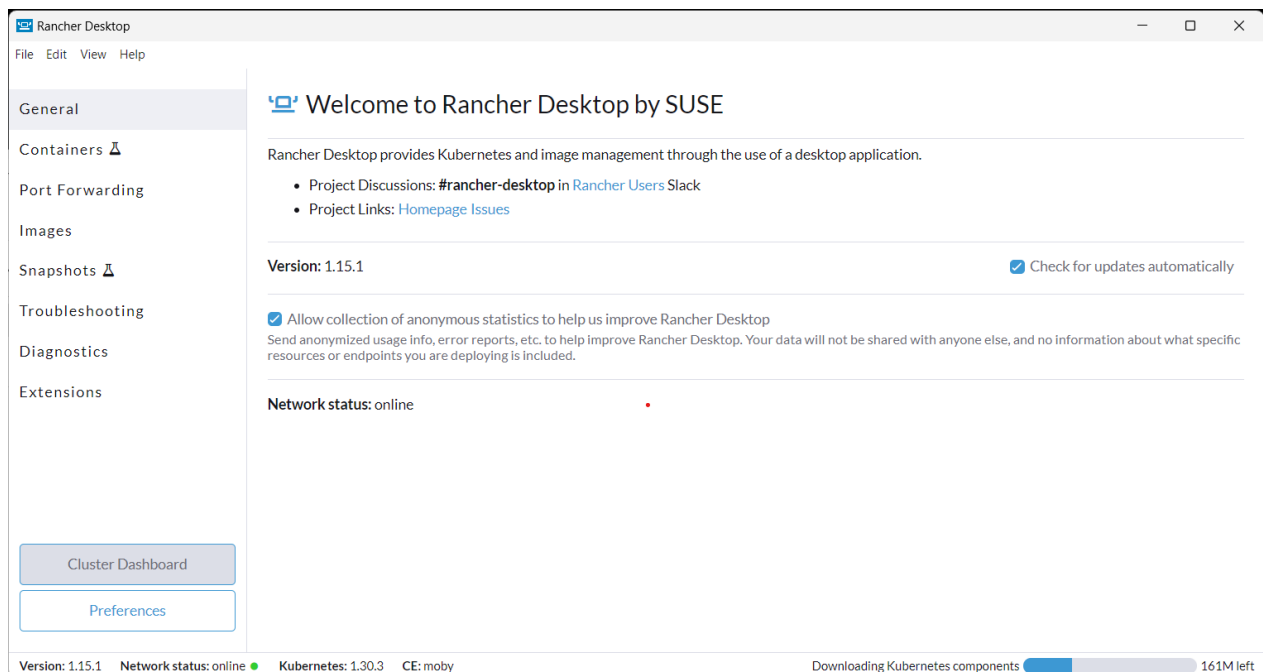


Figure 14: Rancher Desktop Starting

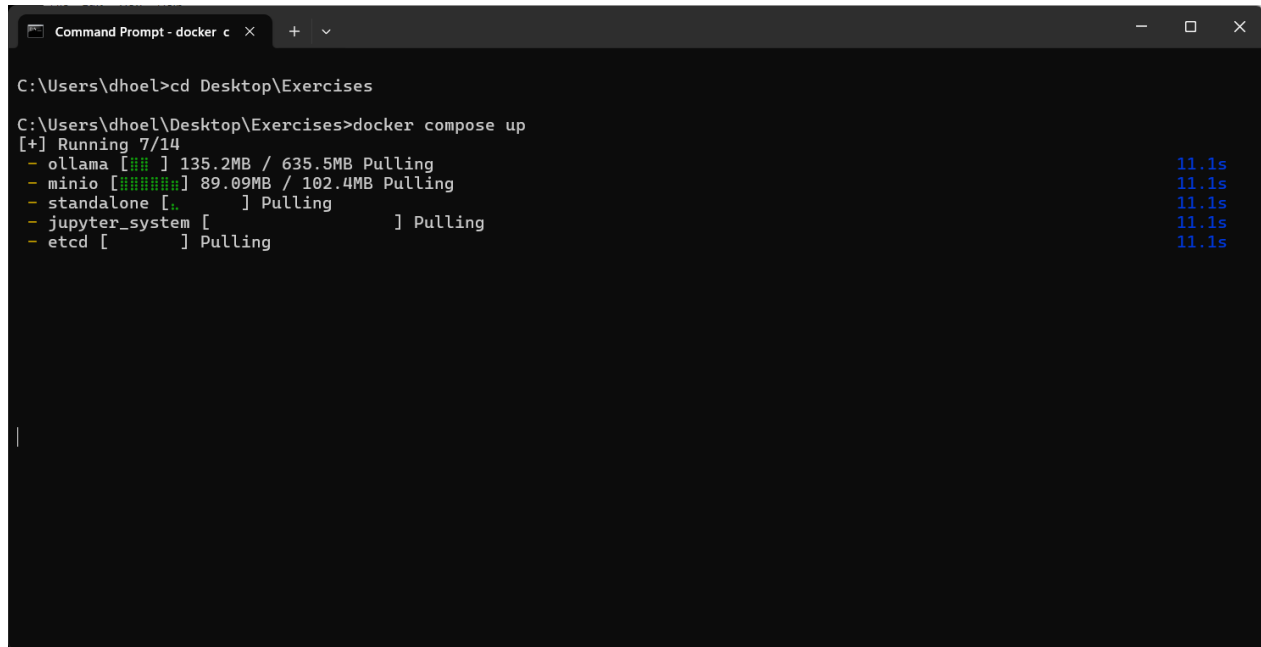
## All Systems: Pulling and Starting the Containers

25. Now that Rancher Desktop is running, open a command prompt. If you are on Windows, use your Windows start menu button and type “cmd” and press the Enter key. On a Macintosh, hold down the Command key and press the space bar. Type the word “terminal” and press Enter. On Linux, start a terminal.
26. Using your command line, change to the directory where you copied the contents of the ISO file. For example, on all operating systems your command prompt will open in your user home directory. If you copied the Exercises folder to your Desktop, you can likely navigate there with the command:

```
cd Desktop/Exercises
```

This is also true on Linux and MacOS. If you are using Windows with Microsoft OneDrive synching your desktop, you may need to spend some time determining exactly what the correct file path is for your Desktop folder.

27. Inside of the Exercises folder, type `docker compose up`:



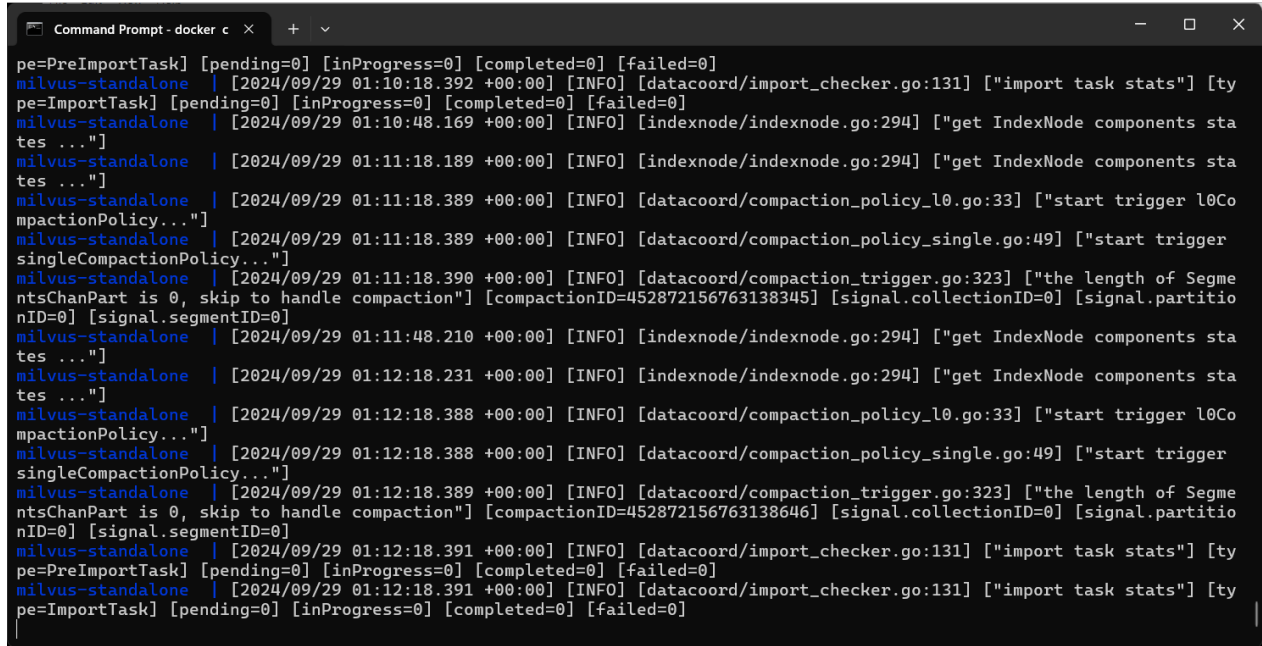
The screenshot shows a Windows Command Prompt window titled "Command Prompt - docker c". The user has navigated to the "C:\Users\dhoel\Desktop\Exercises" directory and executed the command "docker compose up". The output shows the progress of pulling Docker images for five services: ollama, minio, standalone, jupyter\_system, and etcd. Each service is shown with a progress bar, the amount of data pulled, and the time taken. The time for each service is 11.1s.

```
C:\Users\dhoel>cd Desktop\Exercises
C:\Users\dhoel\Desktop\Exercises>docker compose up
[+] Running 7/14
- ollama [### ] 135.2MB / 635.5MB Pulling 11.1s
- minio [#####] 89.09MB / 102.4MB Pulling 11.1s
- standalone [.] Pulling 11.1s
- jupyter_system [ ] Pulling 11.1s
- etcd [ ] Pulling 11.1s
```

Figure 15: Running 'docker compose up'



28. Wait patiently while all of the images for the containers are downloaded. Once this completes, the containers will start. You will see something similar to (but not the same as!) the following:



```
pe=PreImportTask] [pending=0] [inProgress=0] [completed=0] [failed=0]
milvus-standalone | [2024/09/29 01:10:18.392 +00:00] [INFO] [datacoord/import_checker.go:131] ["import task stats"] [ty
pe=ImportTask] [pending=0] [inProgress=0] [completed=0] [failed=0]
milvus-standalone | [2024/09/29 01:10:48.169 +00:00] [INFO] [indexnode/indexnode.go:294] ["get IndexNode components sta
tes ..."]
milvus-standalone | [2024/09/29 01:11:18.189 +00:00] [INFO] [indexnode/indexnode.go:294] ["get IndexNode components sta
tes ..."]
milvus-standalone | [2024/09/29 01:11:18.389 +00:00] [INFO] [datacoord/compaction_policy_l0.go:33] ["start trigger l0Co
mpactionPolicy..."]
milvus-standalone | [2024/09/29 01:11:18.389 +00:00] [INFO] [datacoord/compaction_policy_single.go:49] ["start trigger
singleCompactionPolicy..."]
milvus-standalone | [2024/09/29 01:11:18.390 +00:00] [INFO] [datacoord/compaction_trigger.go:323] ["the length of Segme
ntsChanPart is 0, skip to handle compaction"] [compactionID=452872156763138345] [signal.collectionID=0] [signal.partitionID=0] [signal.segmentID=0]
milvus-standalone | [2024/09/29 01:11:48.210 +00:00] [INFO] [indexnode/indexnode.go:294] ["get IndexNode components sta
tes ..."]
milvus-standalone | [2024/09/29 01:12:18.231 +00:00] [INFO] [indexnode/indexnode.go:294] ["get IndexNode components sta
tes ..."]
milvus-standalone | [2024/09/29 01:12:18.388 +00:00] [INFO] [datacoord/compaction_policy_l0.go:33] ["start trigger l0Co
mpactionPolicy..."]
milvus-standalone | [2024/09/29 01:12:18.388 +00:00] [INFO] [datacoord/compaction_policy_single.go:49] ["start trigger
singleCompactionPolicy..."]
milvus-standalone | [2024/09/29 01:12:18.389 +00:00] [INFO] [datacoord/compaction_trigger.go:323] ["the length of Segme
ntsChanPart is 0, skip to handle compaction"] [compactionID=452872156763138646] [signal.collectionID=0] [signal.partitionID=0] [signal.segmentID=0]
milvus-standalone | [2024/09/29 01:12:18.391 +00:00] [INFO] [datacoord/import_checker.go:131] ["import task stats"] [ty
pe=PreImportTask] [pending=0] [inProgress=0] [completed=0] [failed=0]
milvus-standalone | [2024/09/29 01:12:18.391 +00:00] [INFO] [datacoord/import_checker.go:131] ["import task stats"] [ty
pe=ImportTask] [pending=0] [inProgress=0] [completed=0] [failed=0]
```

Figure 16: Compose Completed

29. Once the containers are up and running, open your web browser and connect to the following URL: `http://127.0.0.1:8888`.

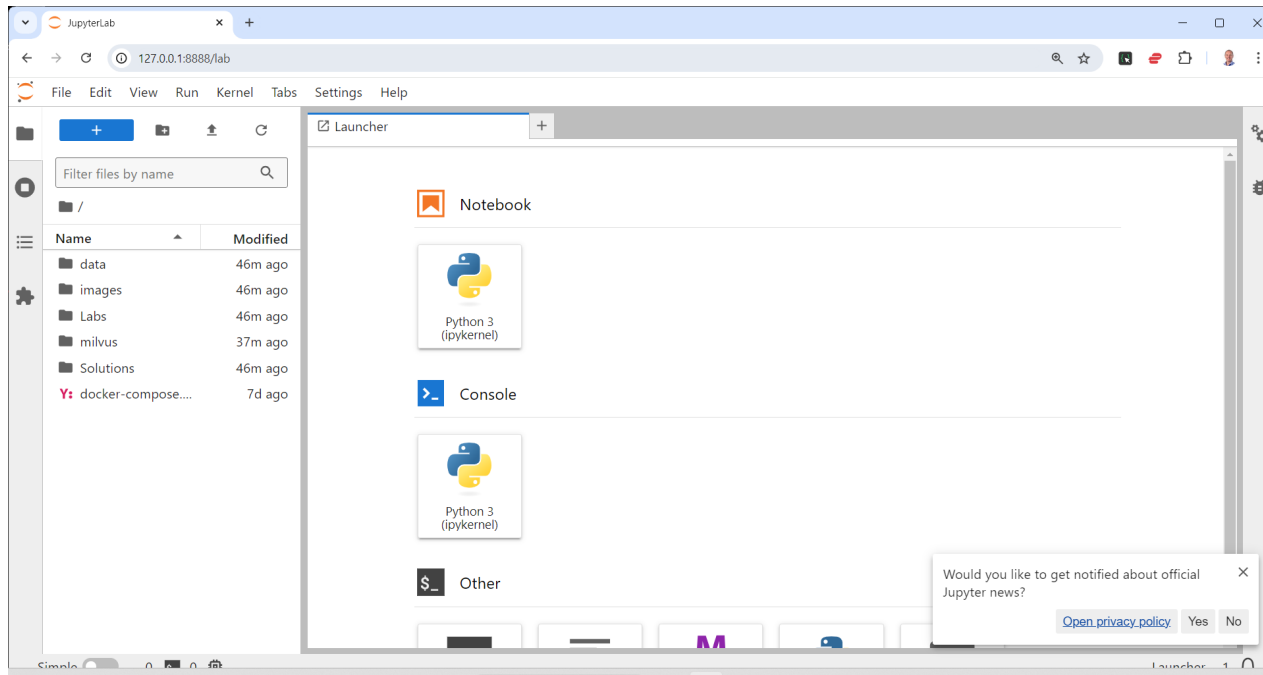


Figure 17: Connecting to Jupyter

Congratulations! You are now ready to start the class!