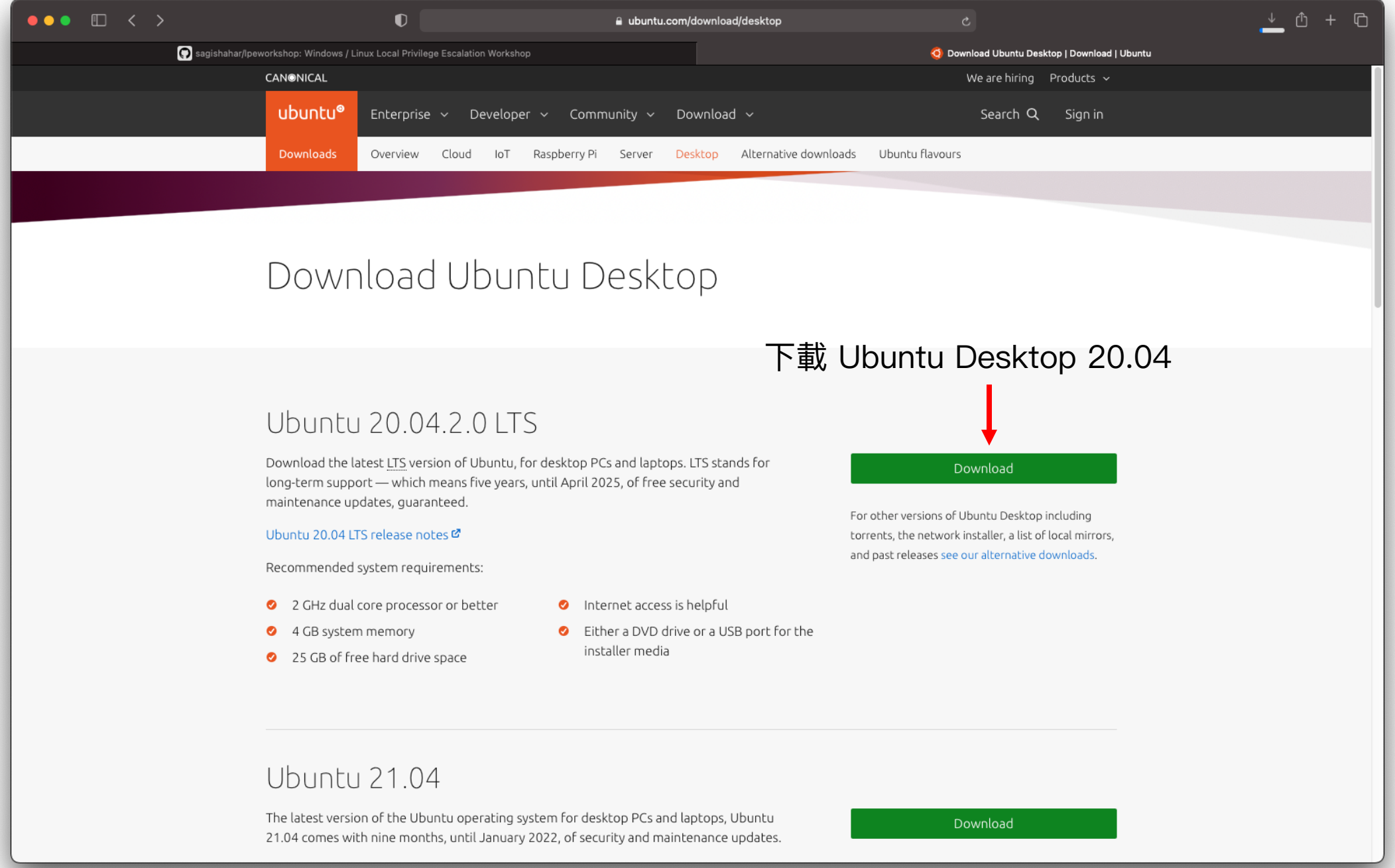
安裝 HELK

下載 Ubuntu ISO

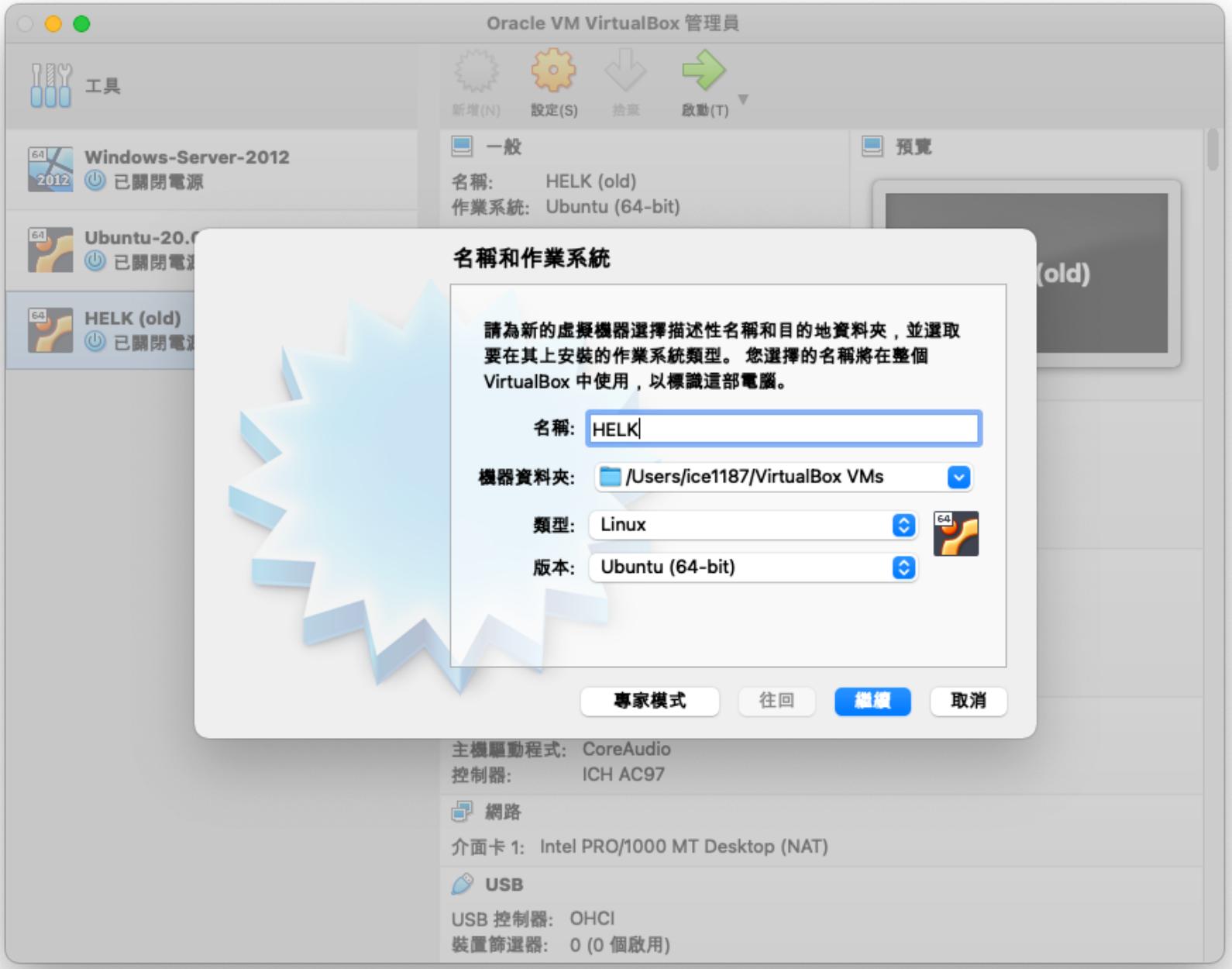


https://ubuntu.com/download/desktop

新增 VM

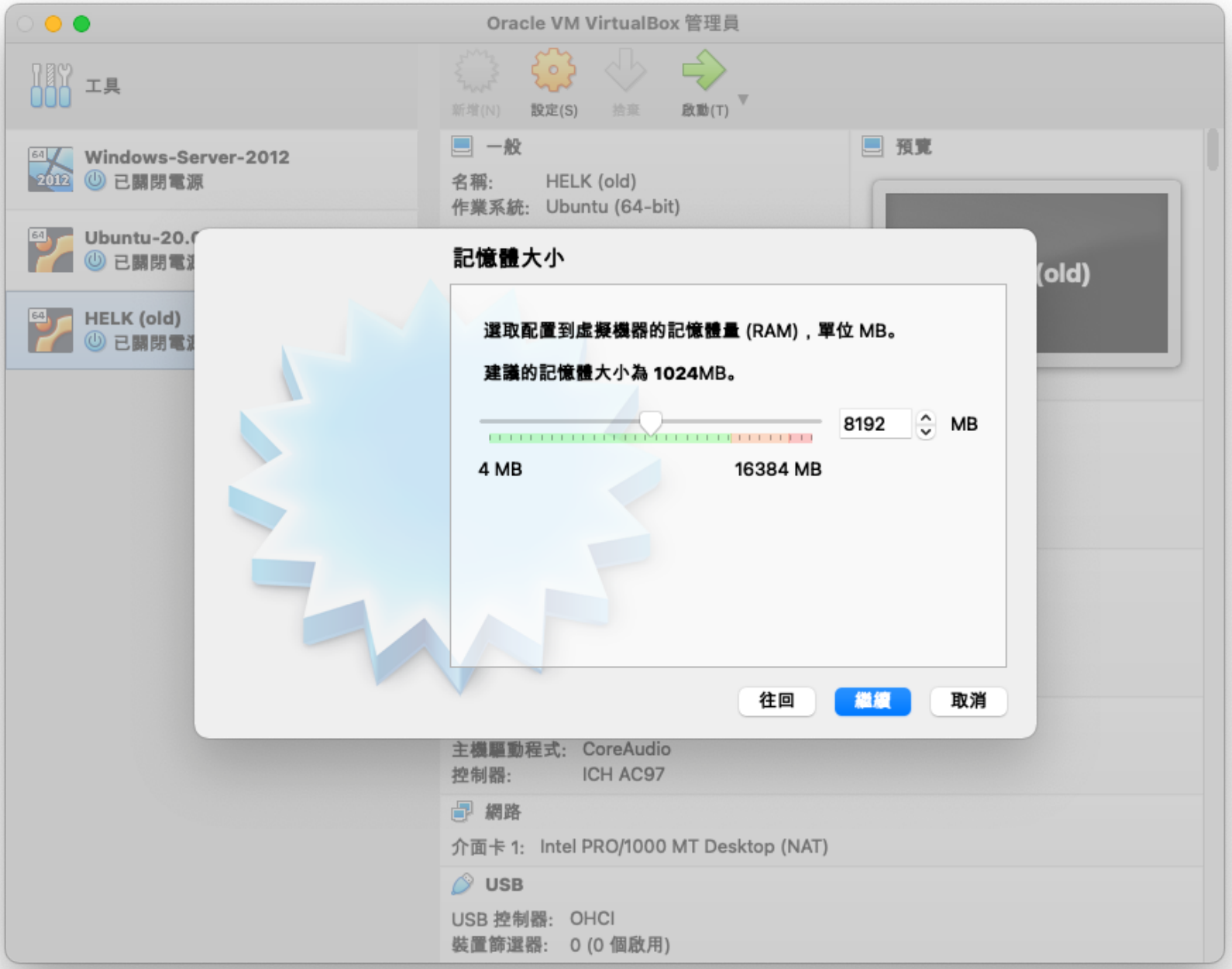
新增 VM

- 名稱：HELK
- 類型：Linux
- 版本：Ubuntu (64 bit)



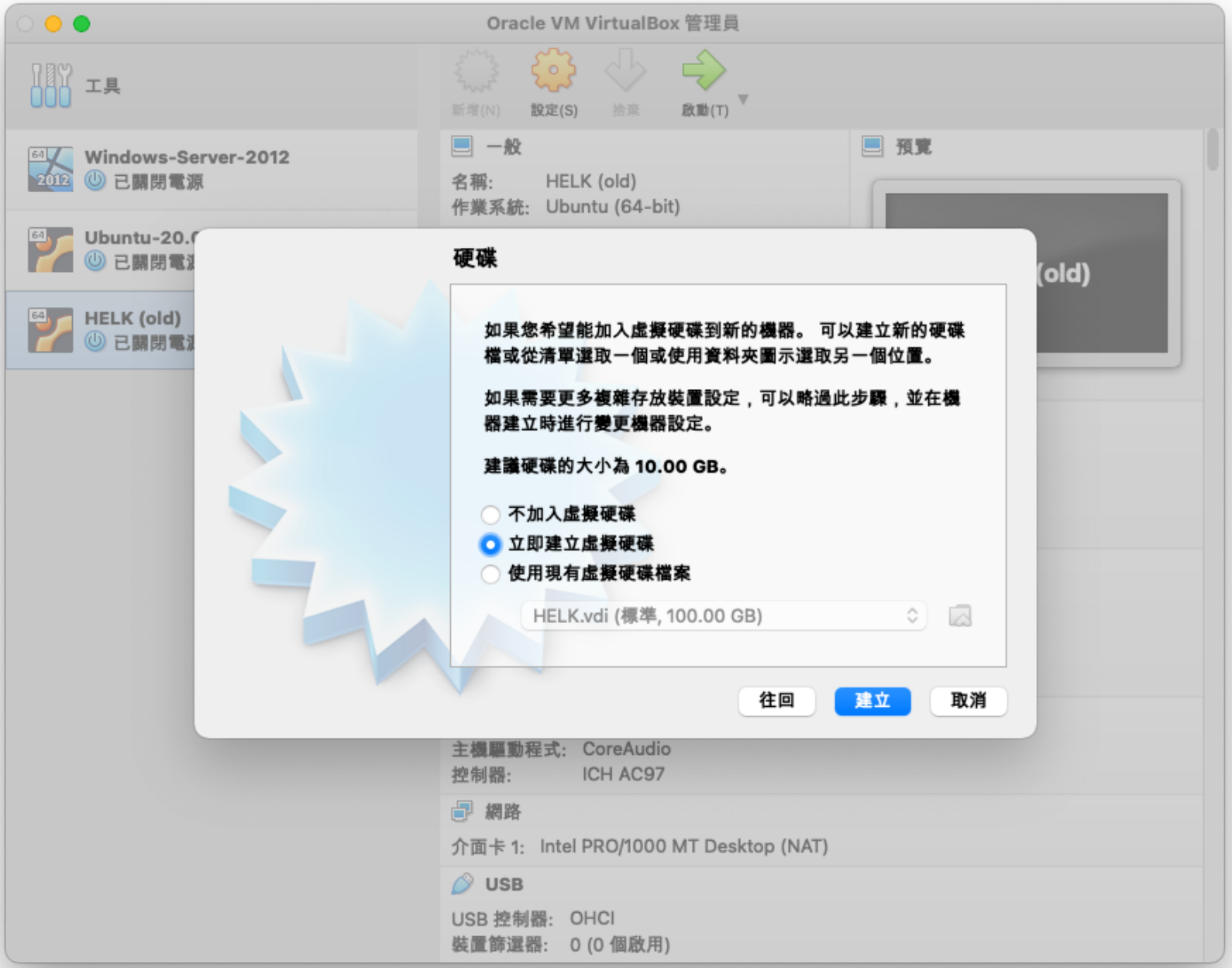
設定 RAM

- 實測至少需大於 6400 MB
- 建議開到 8192 MB 以上較能順暢執行



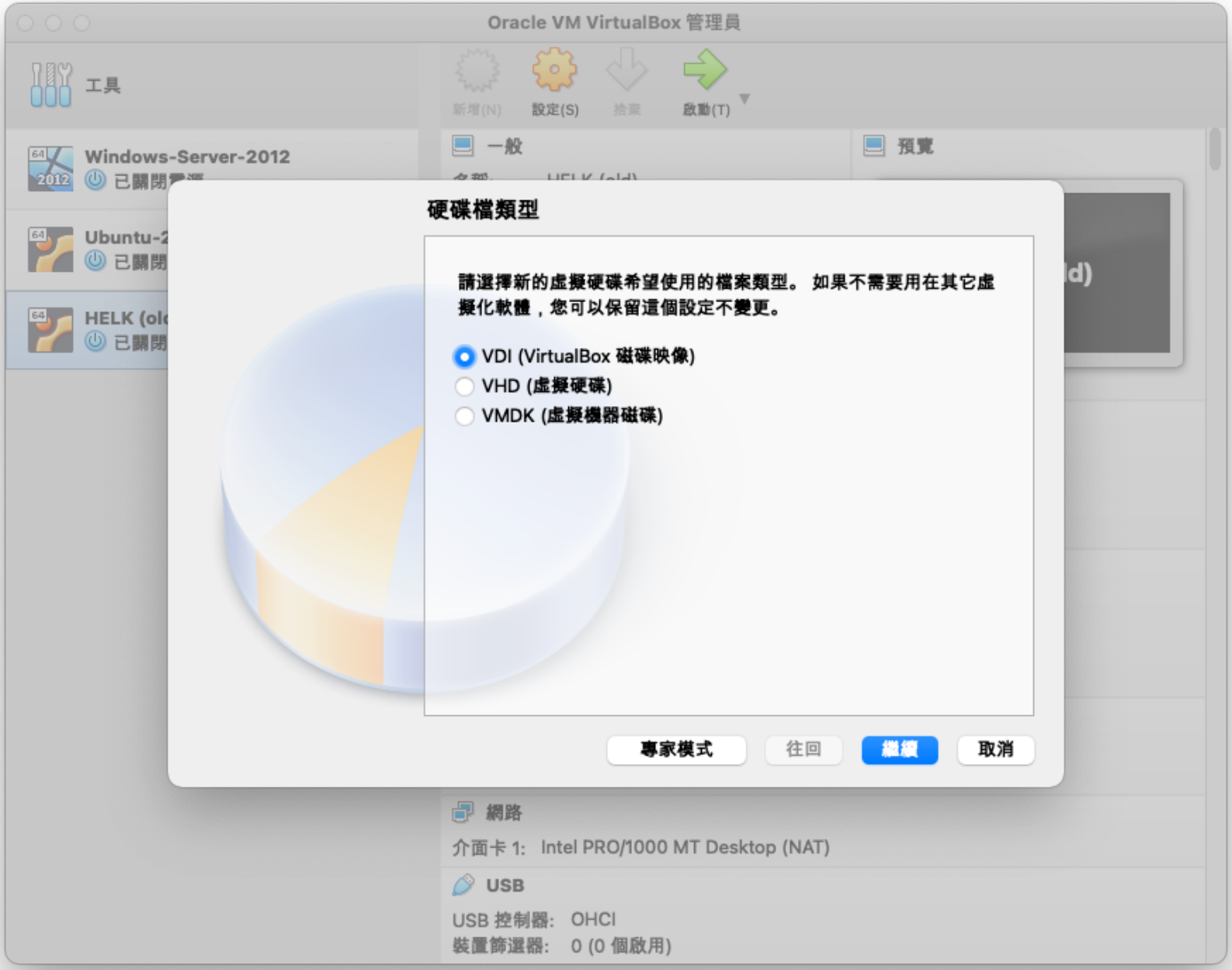
設定 Disk

- 選擇「立即建立虛擬硬碟」



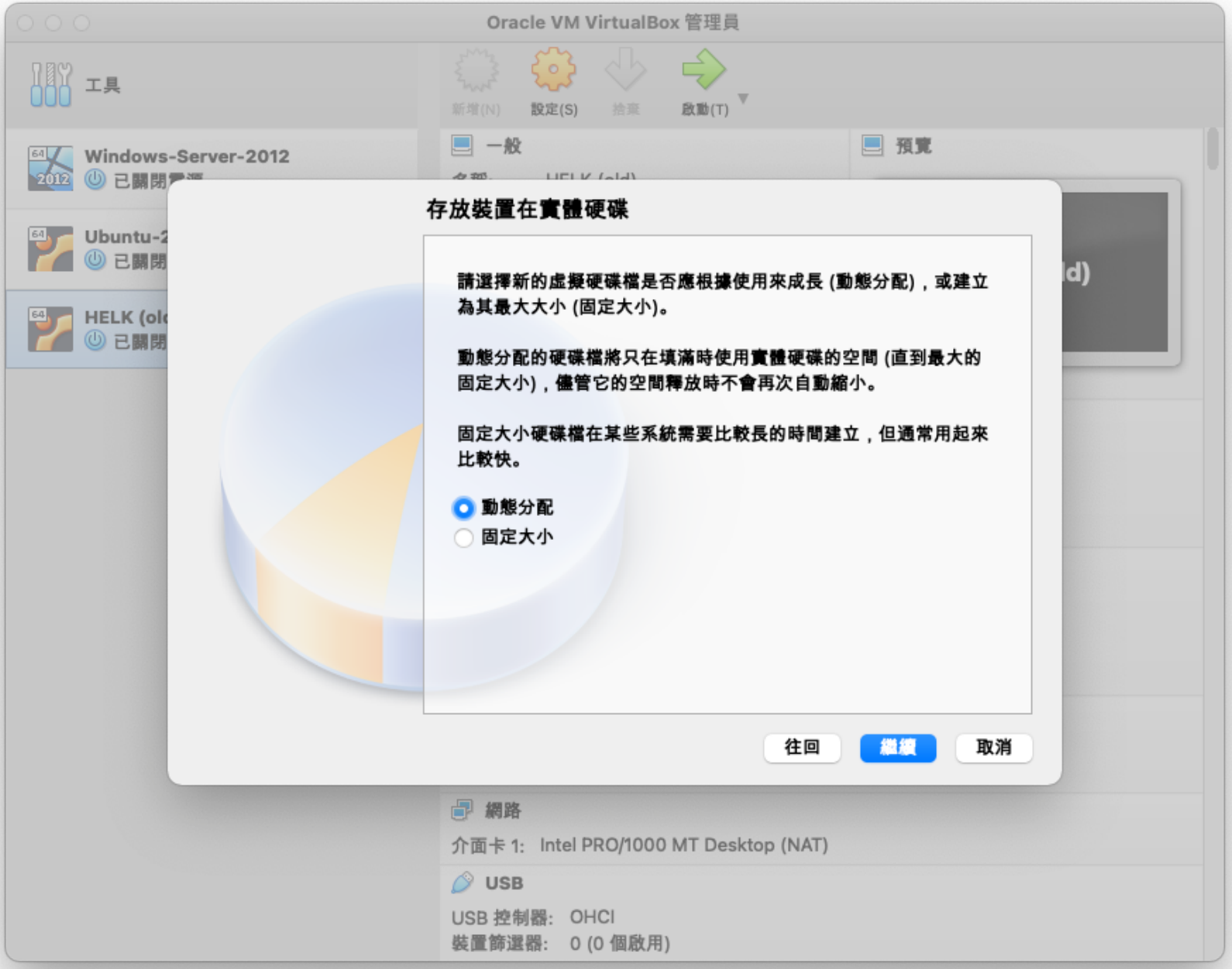
設定 Disk

- 選擇「立即建立虛擬硬碟」
- 選擇「VDI」



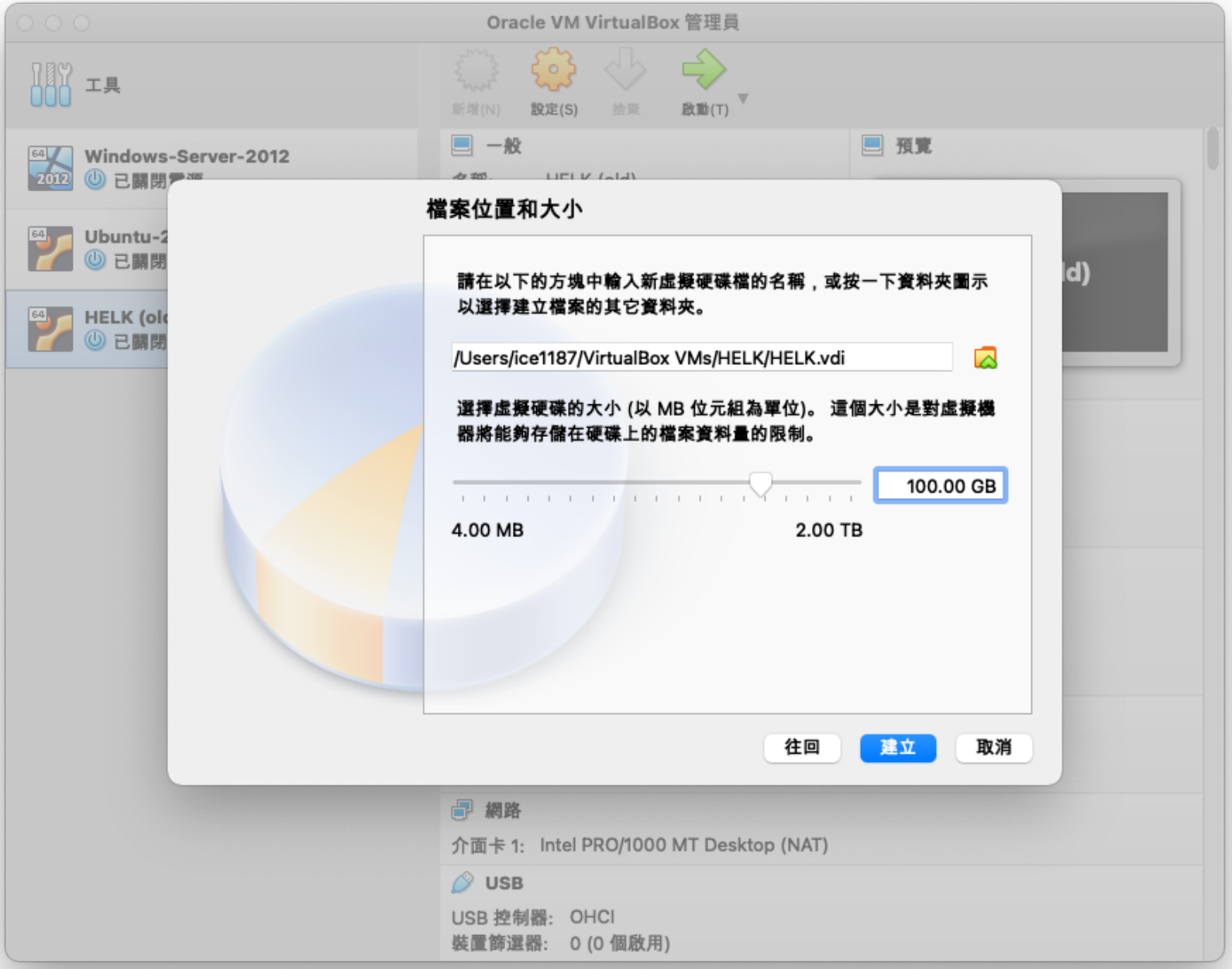
設定 Disk

- 選擇「立即建立虛擬硬碟」
- 選擇「VDI」
- 選擇「動態分配」



設定 Disk

- 選擇「立即建立虛擬硬碟」
- 選擇「VDI」
- 選擇「動態分配」
- 選擇 60 ~ 100 GB



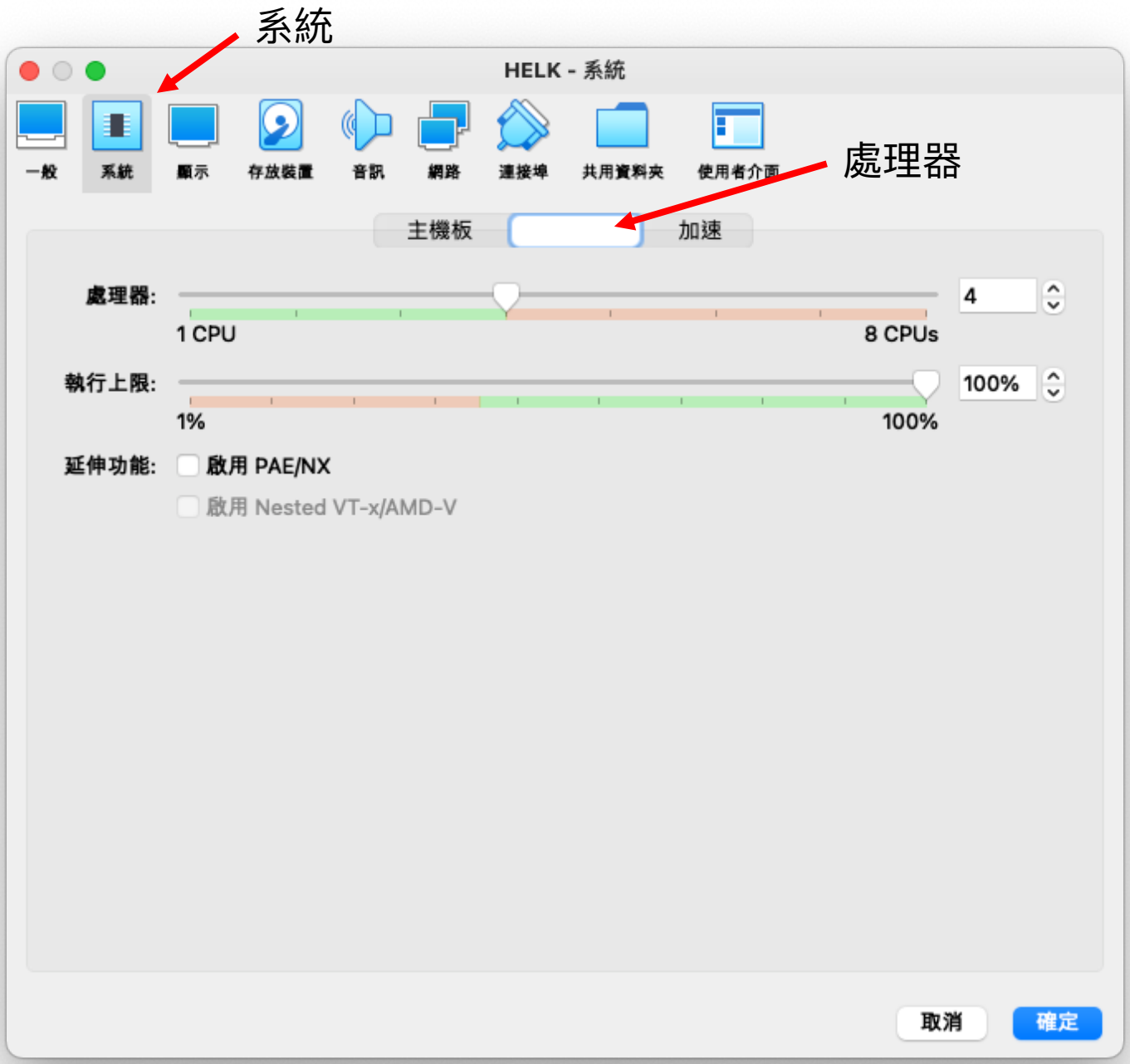
設定硬體

- 選擇「設定」


設定
Oracle VM VirtualBox 管理員
工具
新增(N)
設定(S)
捨棄
啟動(T)
Windows-Server-2012
已關閉電源
Ubuntu-20.04 (Time done.)
已關閉電源
HELK (old)
已關閉電源
HELK
已關閉電源
剛剛設定的 VM
一般
名稱: HELK
作業系統: Ubuntu (64-bit)
系統
基礎記憶體: 8192 MB
開機順序: 軟碟, 光碟, 硬碟
加速: VT-x/AMD-V, 巢式分頁, KVM 半虛擬化
預覽
HELK
顯示
視訊記憶體: 16 MB
圖形控制器: VMSVGA
遠端桌面伺服器: 停用
錄製: 停用
存放裝置
控制器: IDE
IDE Secondary Device 0: [光碟機] 空的
控制器: SATA
SATA 埠 0: HELK.vdi (標準, 100.00 GB)
音訊
主機驅動程式: CoreAudio
控制器: ICH AC97
網路
介面卡 1: Intel PRO/1000 MT Desktop (NAT)
USB
USB 控制器: OHCI
裝置篩選器: 0 (0 個啟用)

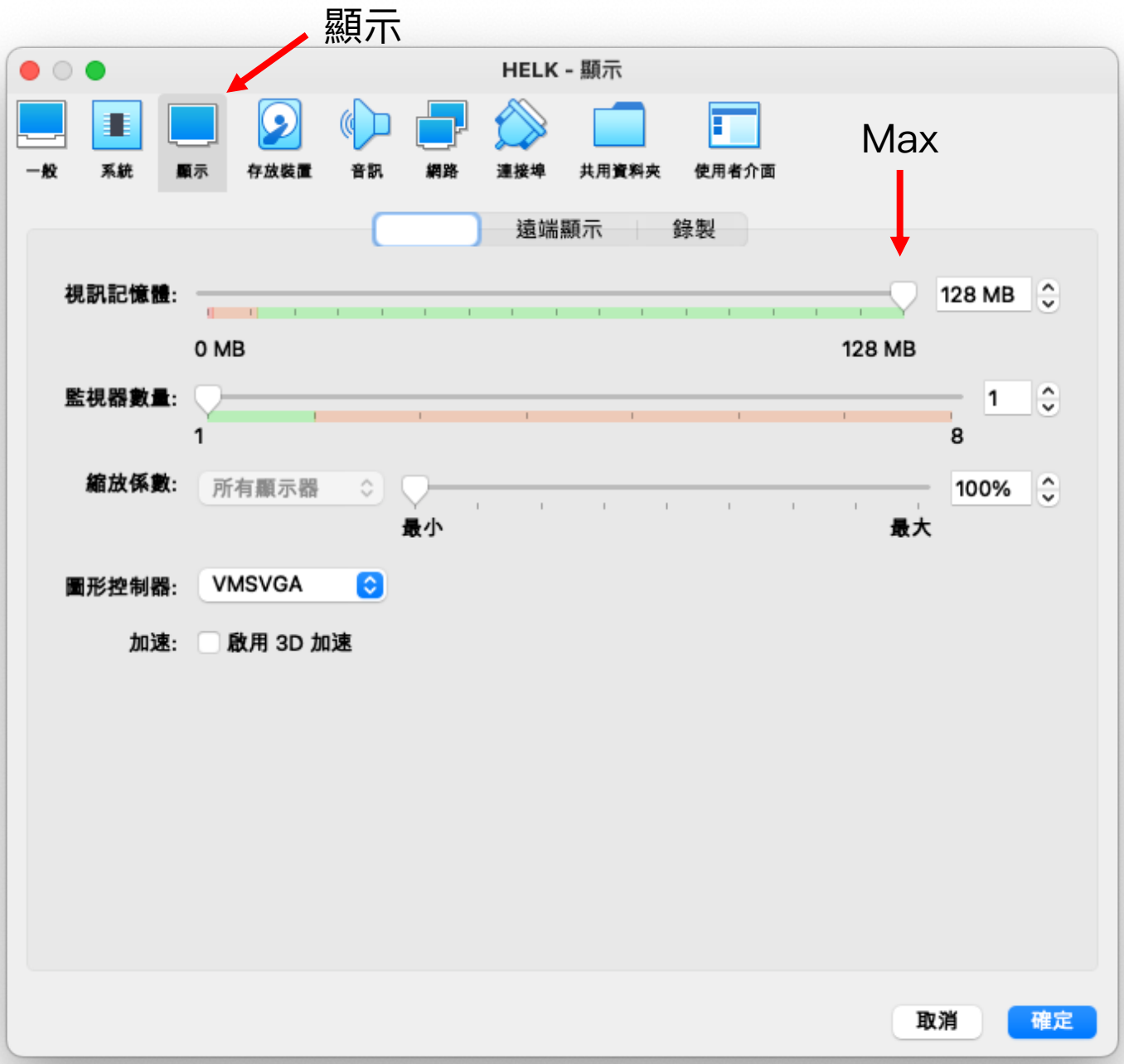
設定硬體

- 選擇「設定」
- 選擇「系統」–> 「處理器」 –> 「4 CPU」



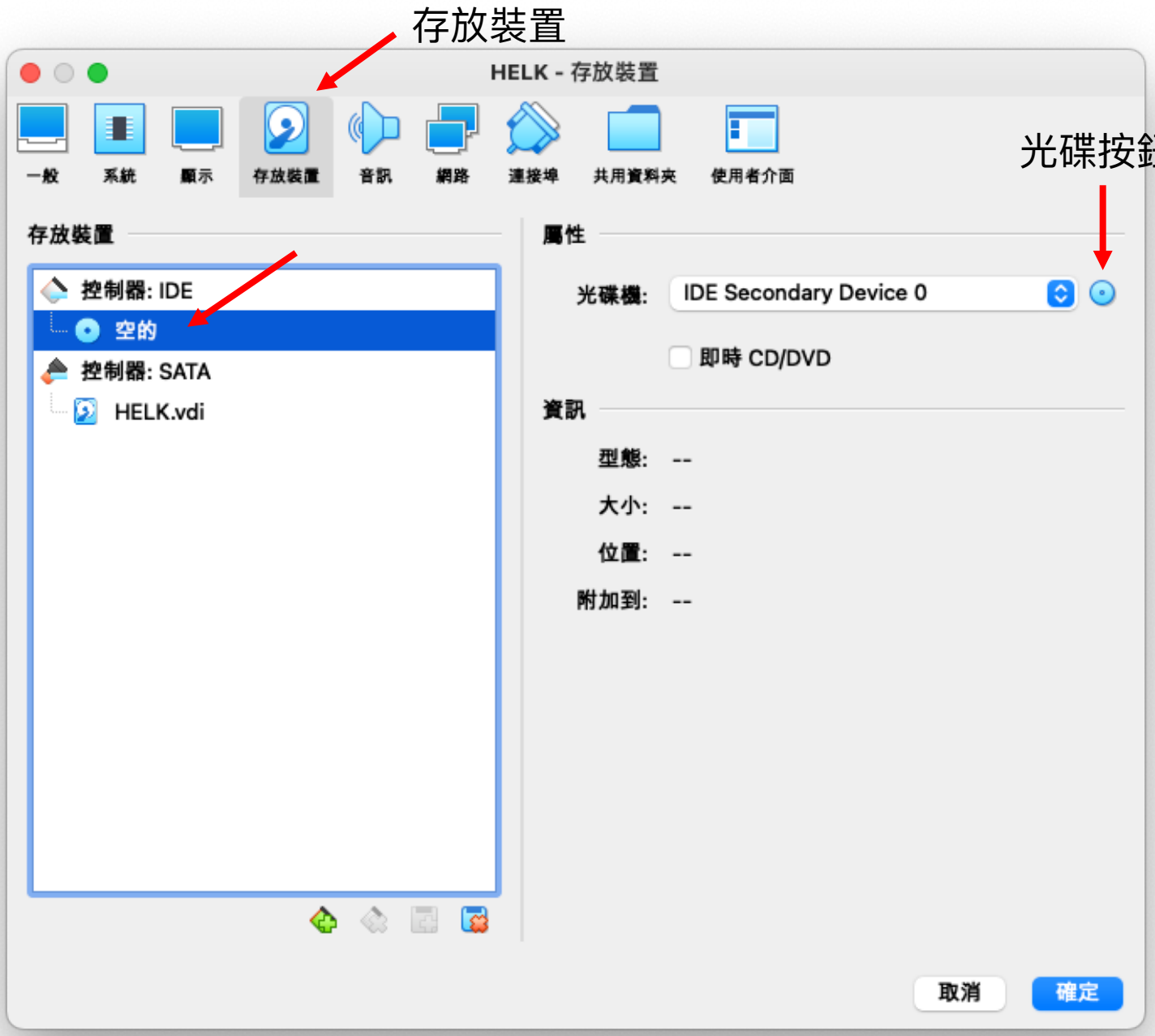
設定硬體

- 選擇「設定」
- 選擇「系統」–> 「處理器」–> 「4 CPU」
- 選擇「顯示」–> 「視訊記憶體」拉到 Max



設定硬體：ISO

- 選擇「存放裝置」–> IDE 下的「空的」–> 右方光碟按鈕

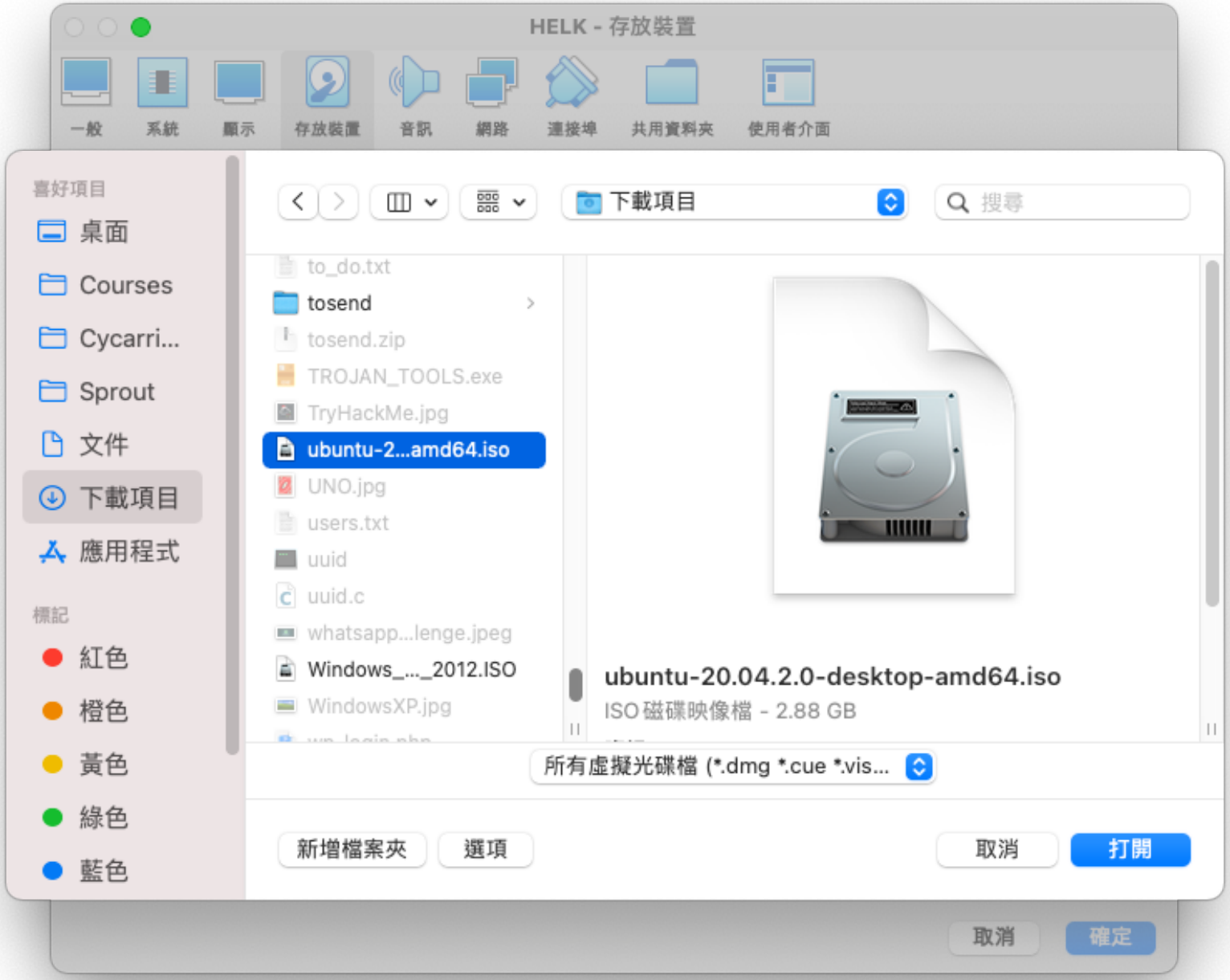


設定硬體：ISO

- 選擇「存放裝置」–> IDE 下的「空的」–> 右方光碟按鈕
- 選擇「選擇磁碟檔...」

設定硬體：ISO

- 選擇「存放裝置」–> IDE 下的「空的」–> 右方光碟按鈕
- 選擇「選擇磁碟檔...」
- 選擇下載好的 Ubuntu .iso 檔



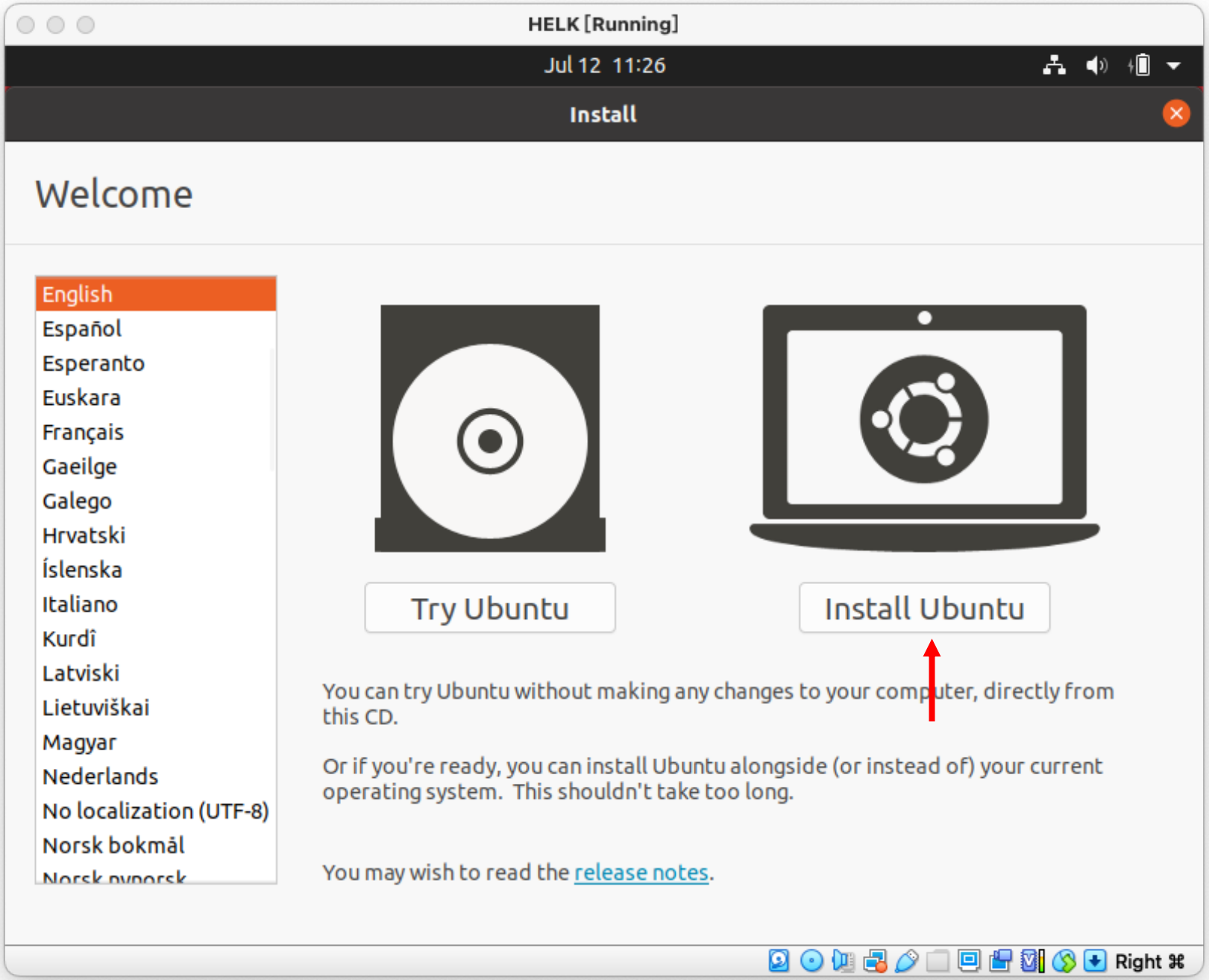
安裝 Ubuntu

- 點兩下「HELK」開機

安裝 Ubuntu

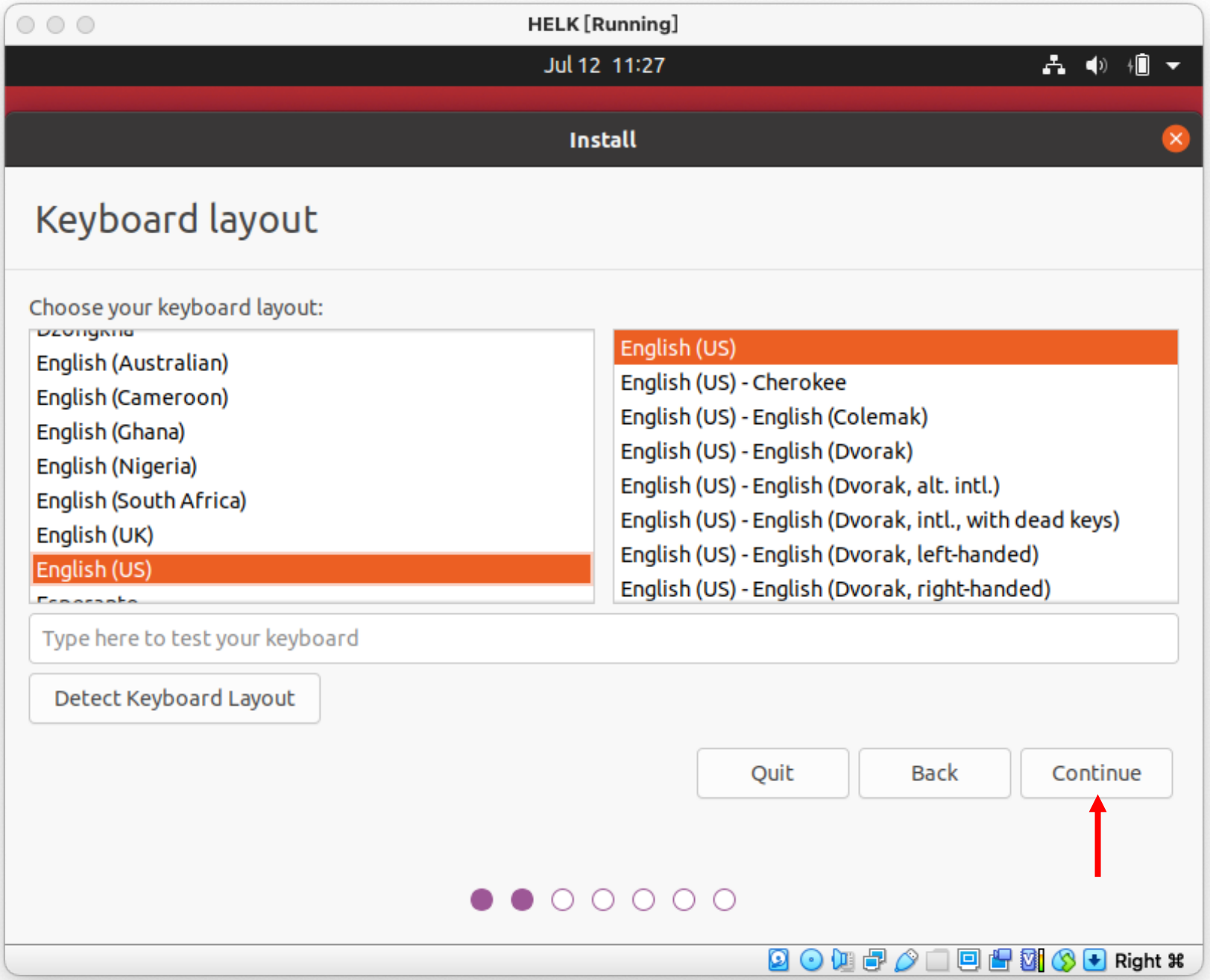
安裝 Ubuntu

- 點兩下「HELK」開機
- 選擇「Install Ubuntu」



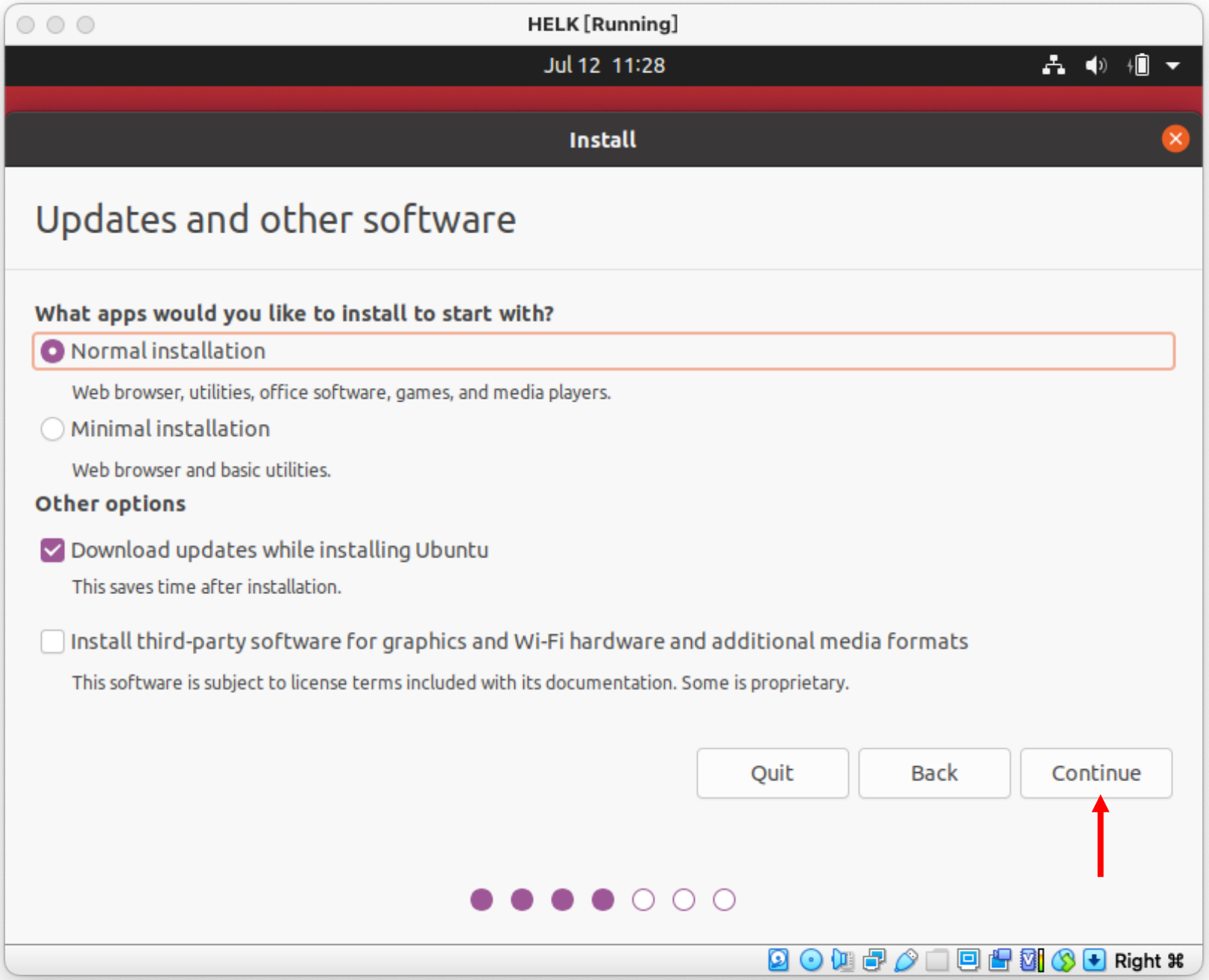
安裝 Ubuntu

- 點兩下「HELK」開機
- 選擇「Install Ubuntu」
- 選擇「Continue」



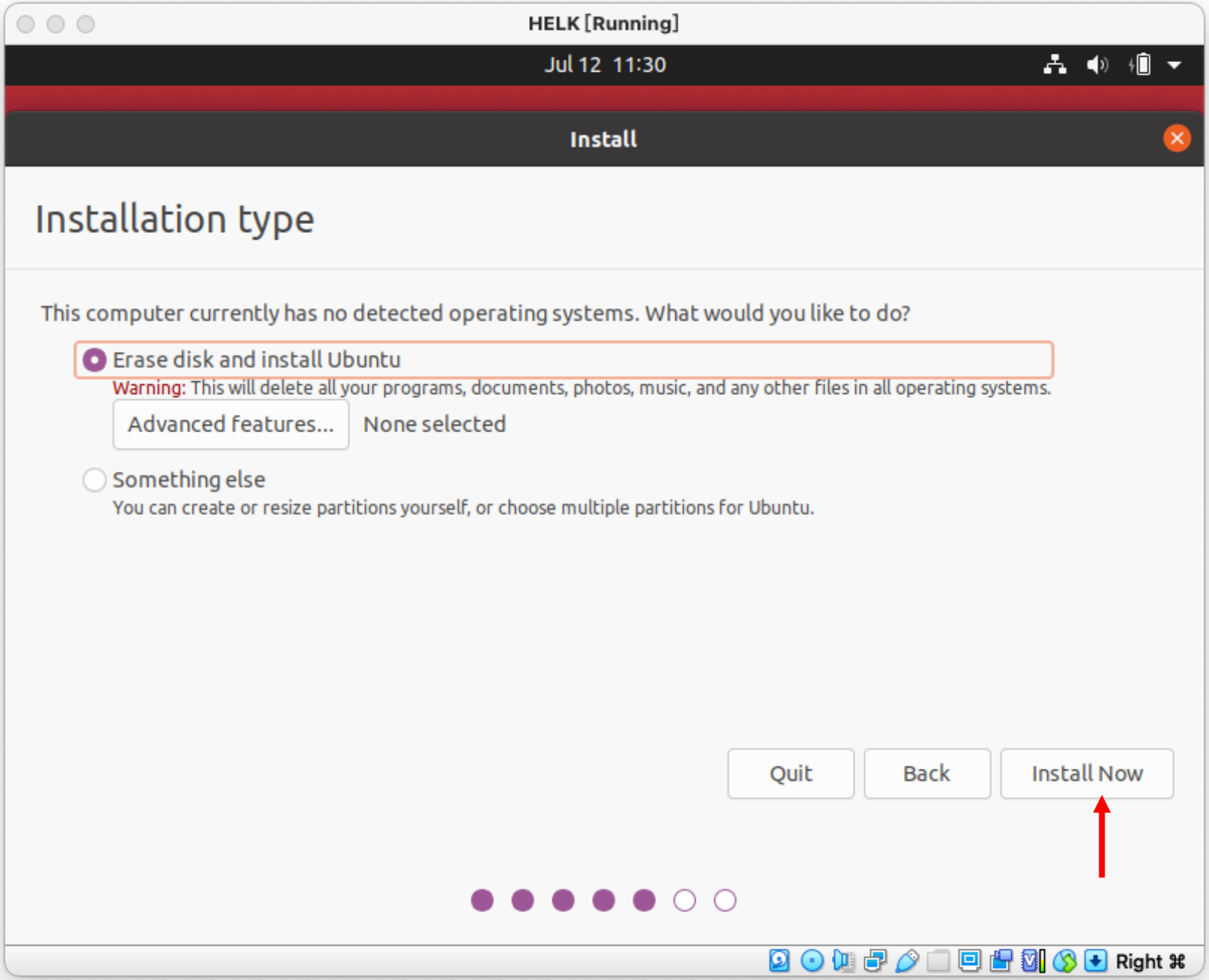
安裝 Ubuntu

- 點兩下「HELK」開機
- 選擇「Install Ubuntu」
- 選擇「Continue」
- 選擇「Continue」



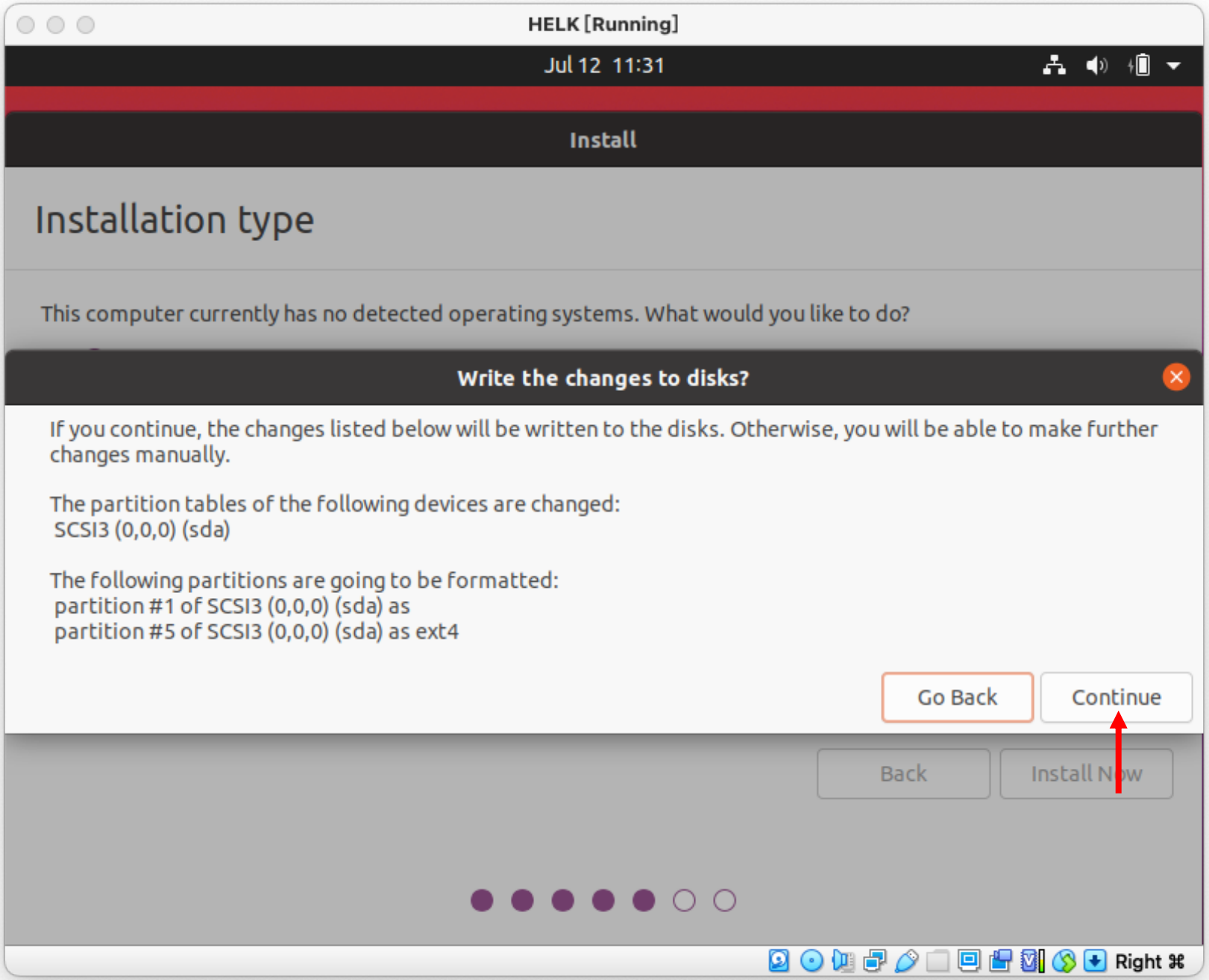
安裝 Ubuntu

- 點兩下「HELK」開機
- 選擇「Install Ubuntu」
- 選擇「Continue」
- 選擇「Continue」
- 選擇「Install Now」



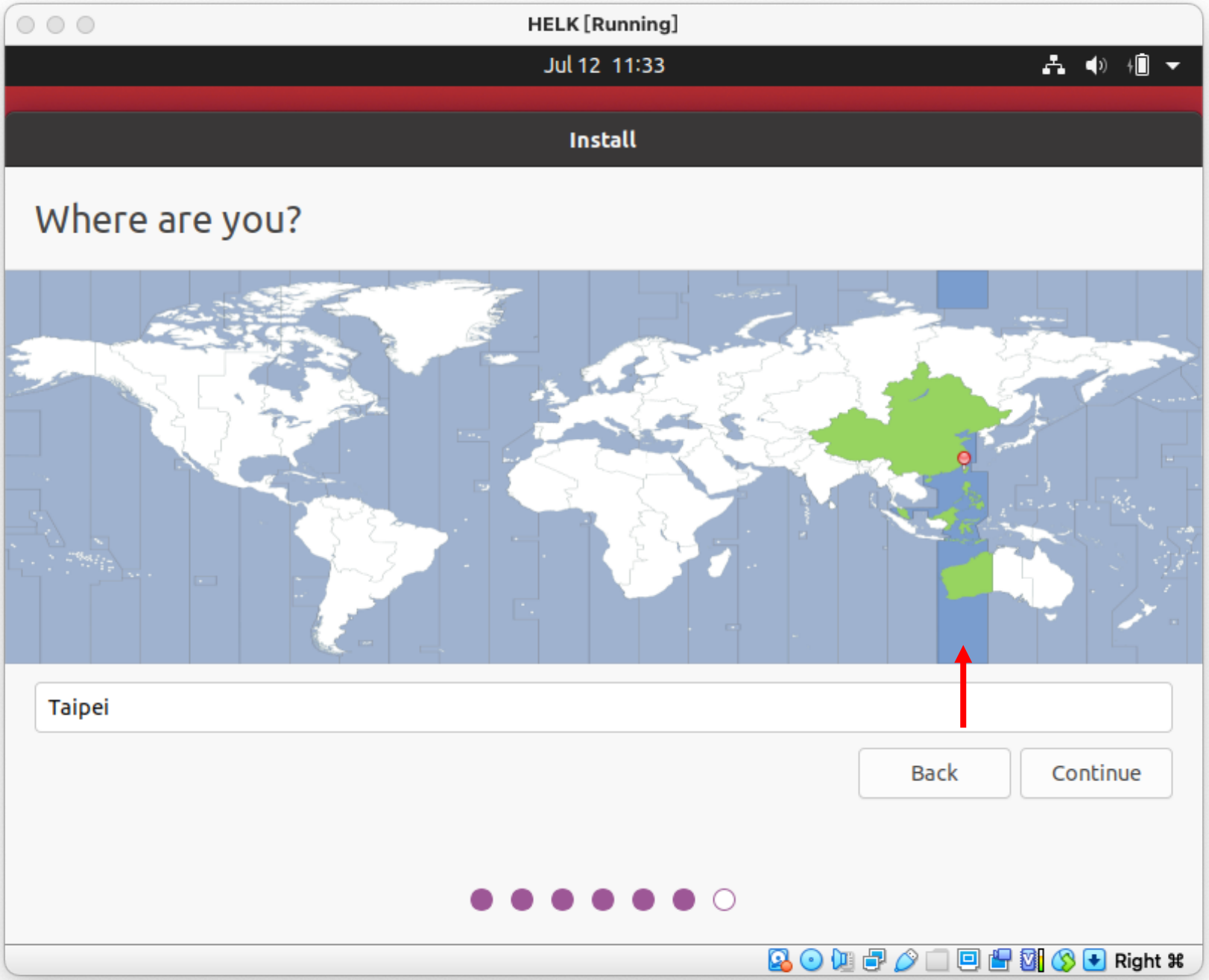
安裝 Ubuntu

- 點兩下「HELK」開機
- 選擇「Install Ubuntu」
- 選擇「Continue」
- 選擇「Continue」
- 選擇「Install Now」
- 選擇「Continue」



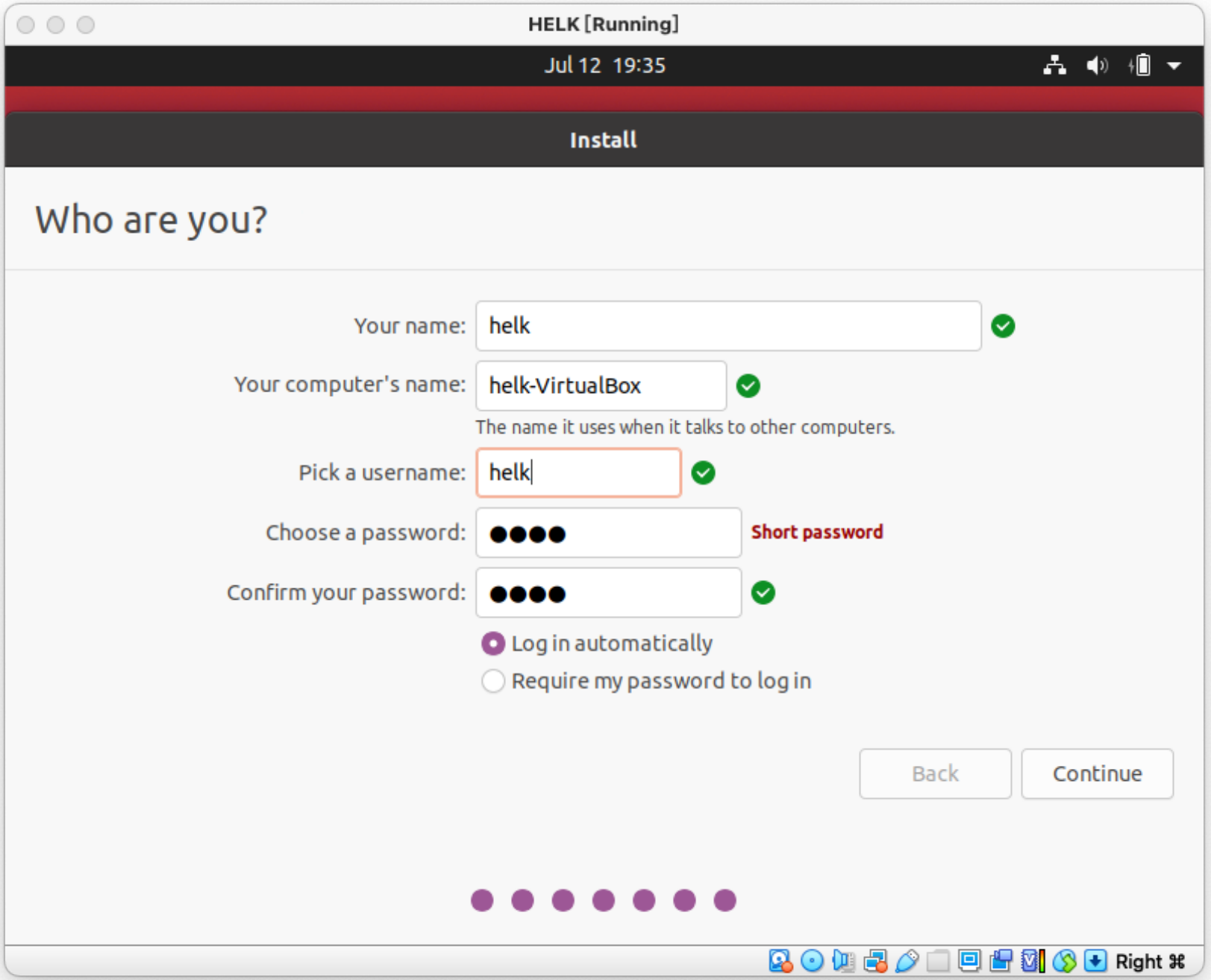
安裝 Ubuntu

- 點兩下「HELK」開機
- 選擇「Install Ubuntu」
- 選擇「Continue」
- 選擇「Continue」
- 選擇「Install Now」
- 選擇「Continue」
- 選擇「Taipei」



安裝 Ubuntu

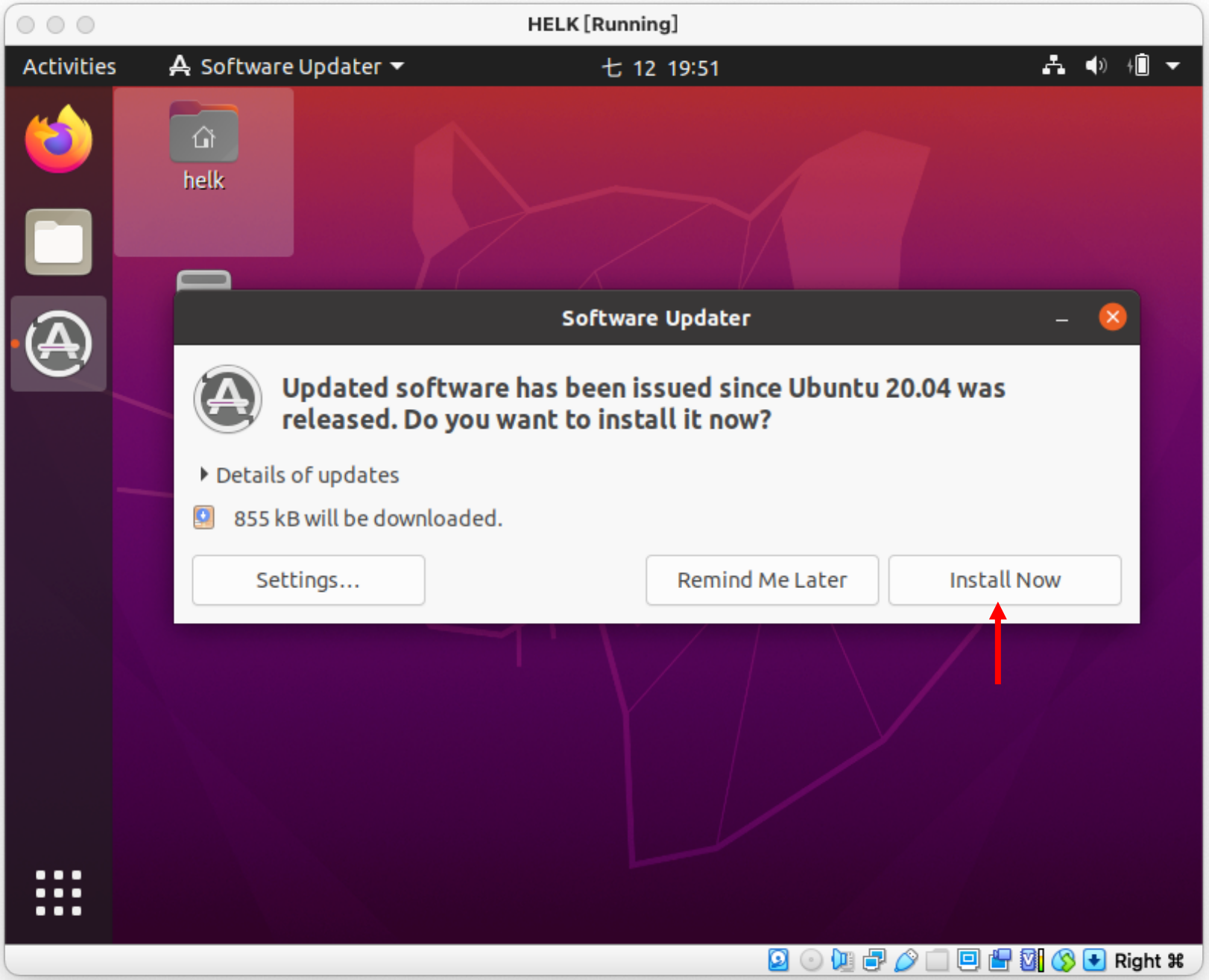
- 點兩下「HELK」開機
- 選擇「Install Ubuntu」
- 選擇「Continue」
- 選擇「Continue」
- 選擇「Install Now」
- 選擇「Continue」
- 選擇「Taipei」
- 設定 user、password



設定 Ubuntu

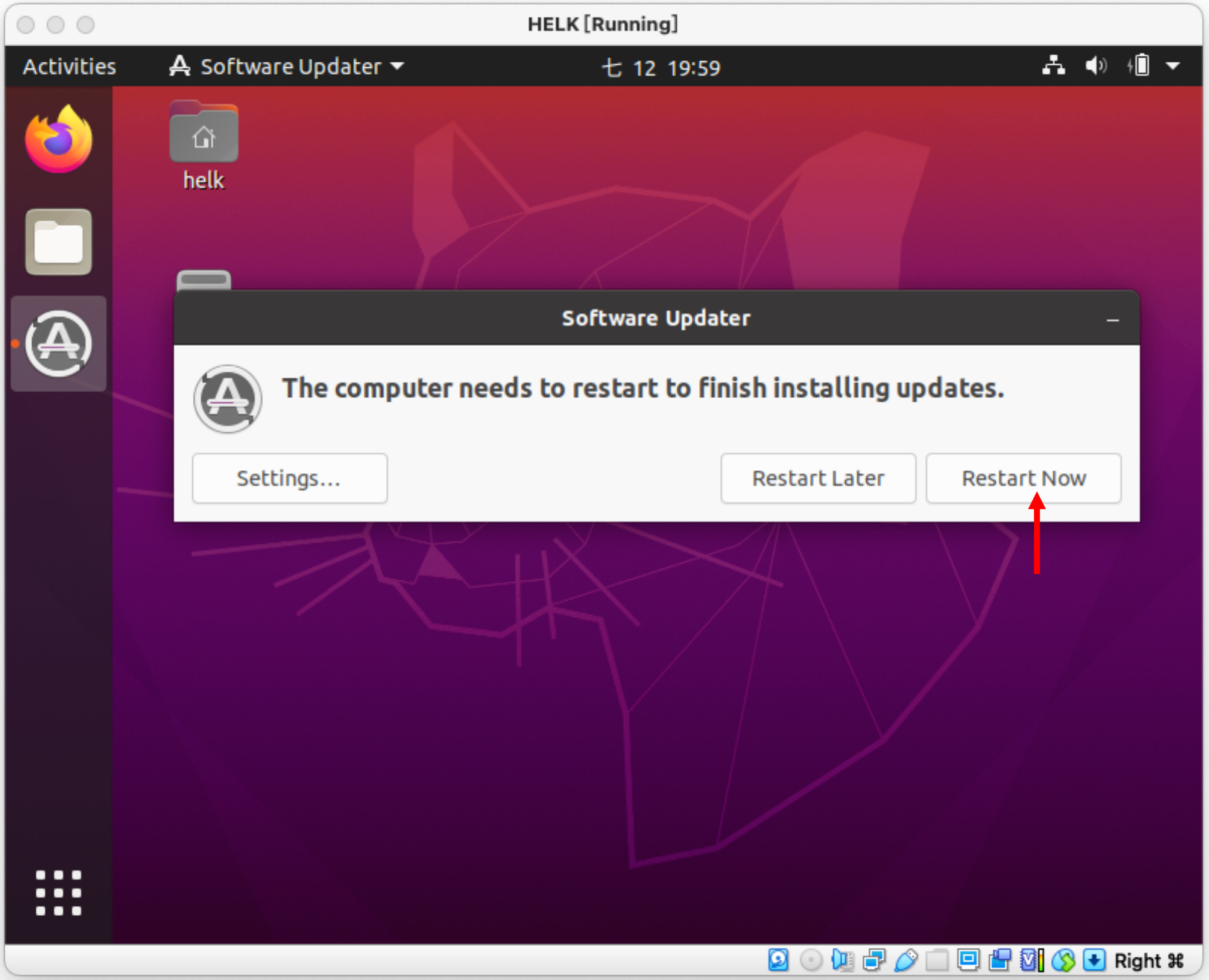
設定 Ubuntu

- 選擇「Install Now」



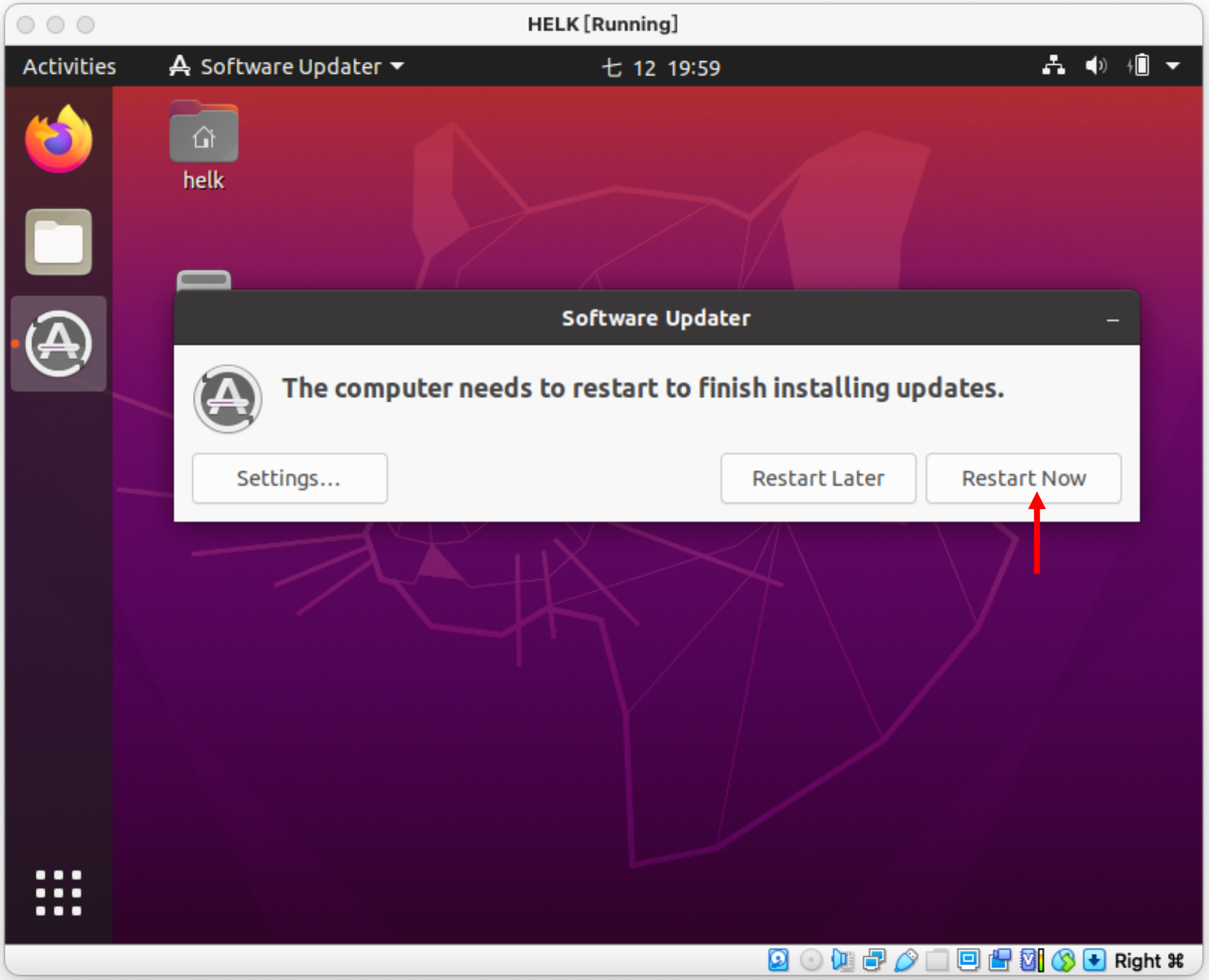
設定 Ubuntu

- 選擇「Install Now」
- 等跑完，選擇「Restart Now」



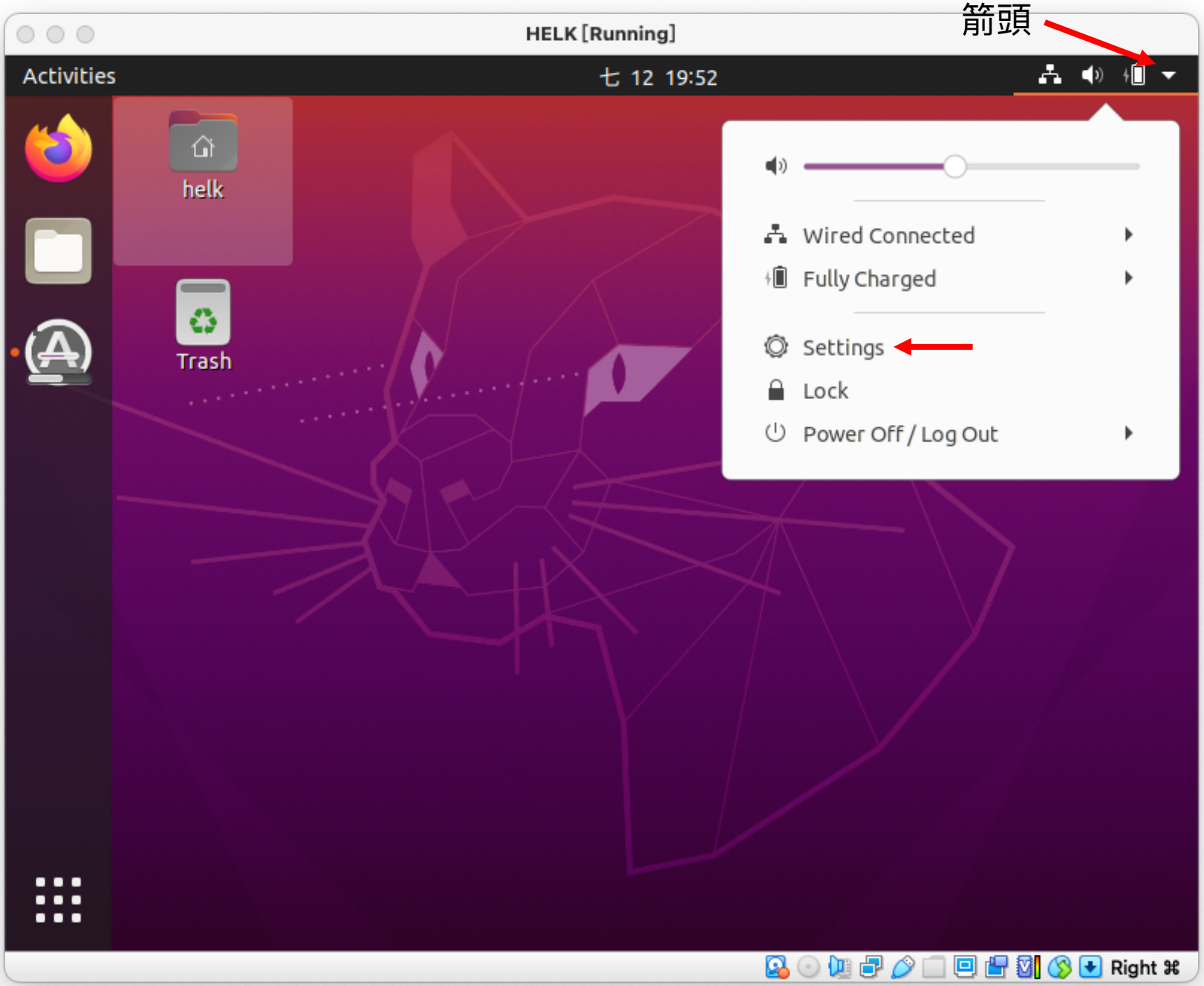
設定 Ubuntu

- 選擇「Install Now」
- 等跑完，選擇「Restart Now」



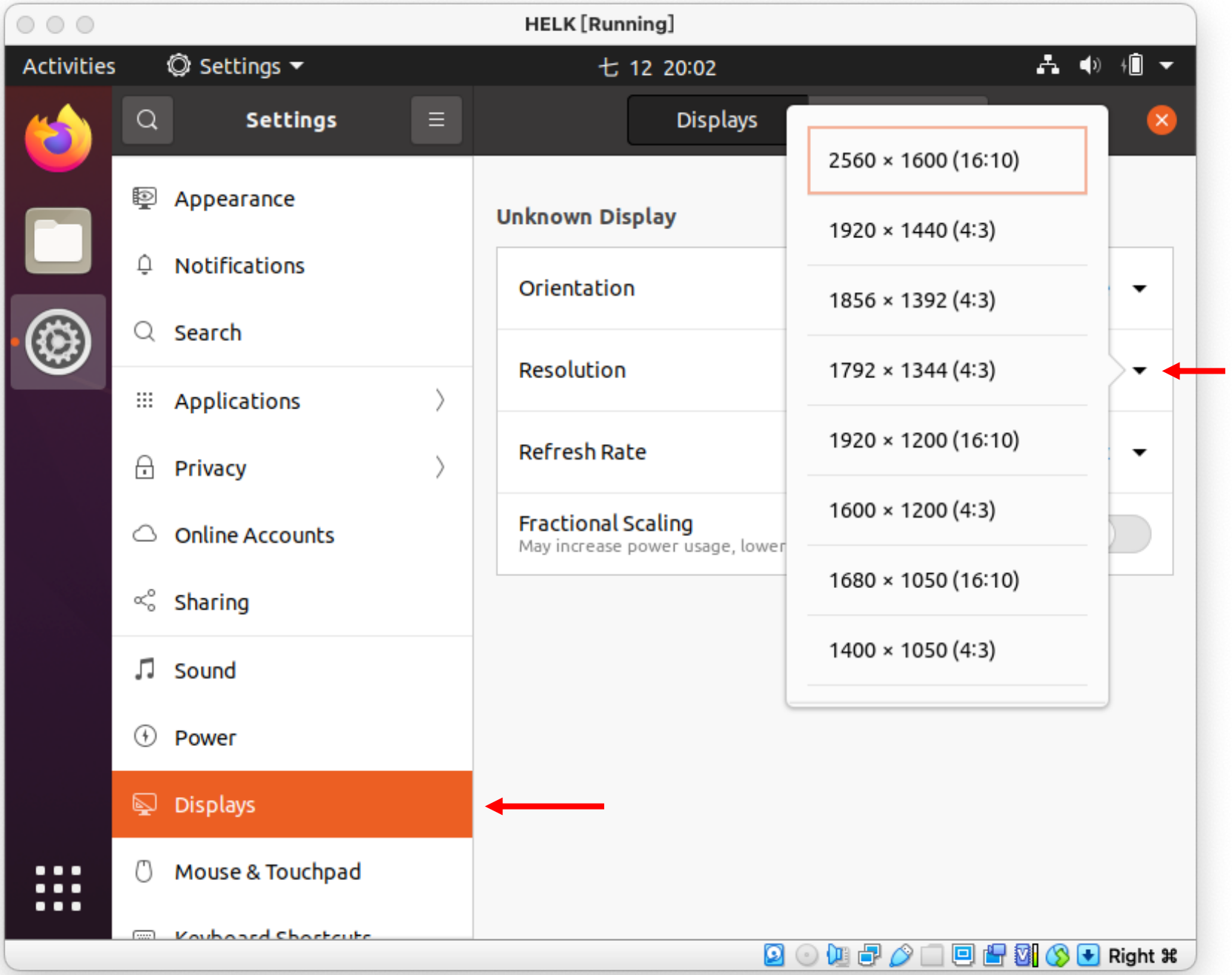
設定 Ubuntu

- 選擇「Install Now」
- 等跑完，選擇「Restart Now」
- 點選「箭頭」 –> 「Settings」



設定 Ubuntu

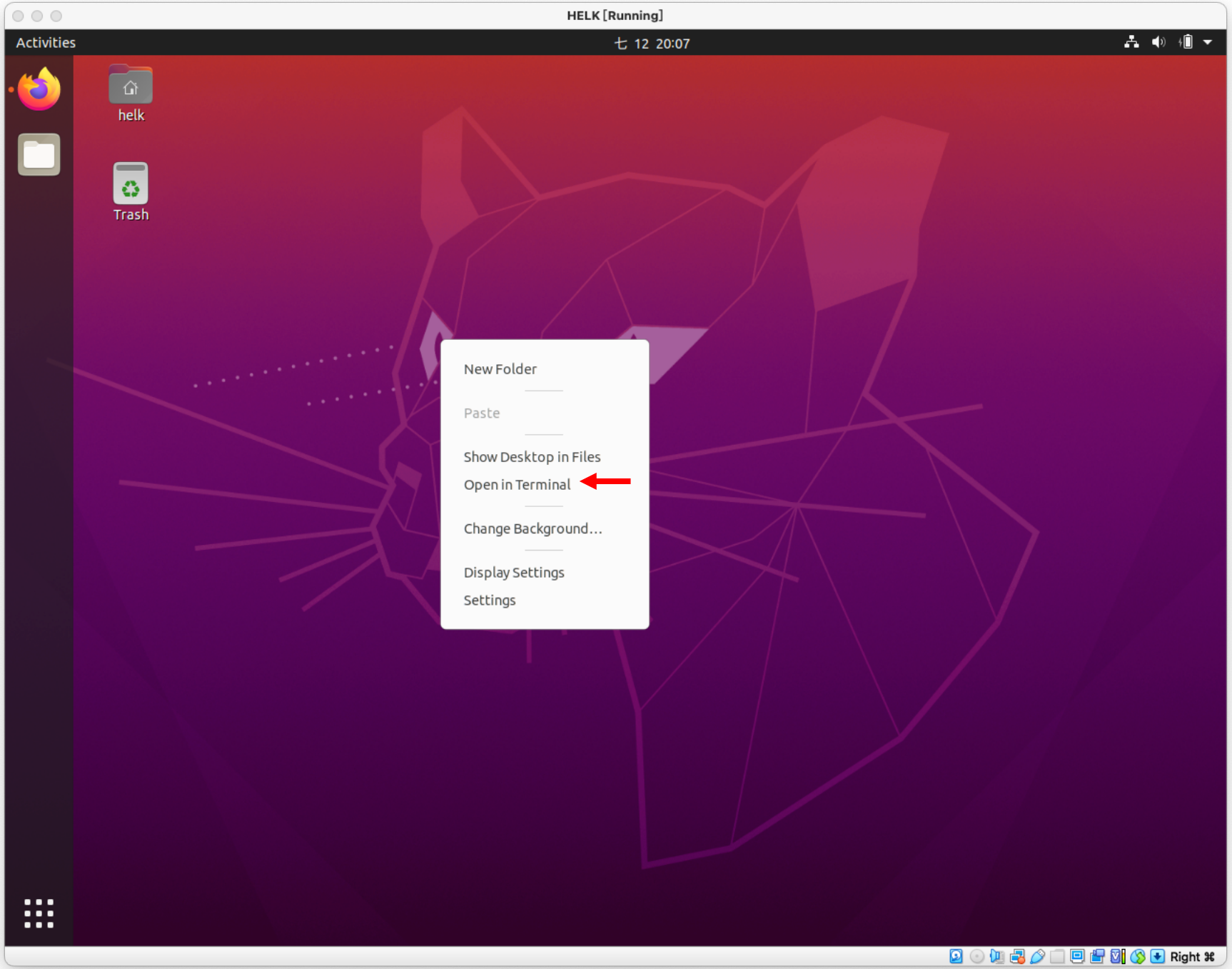
- 選擇「Install Now」
- 等跑完，選擇「Restart Now」
- 點選「箭頭」 –> 「Settings」
- 選擇「Displays」–> 「Resolution」，然後調整到適當的視窗大小



安裝 Lab 環境

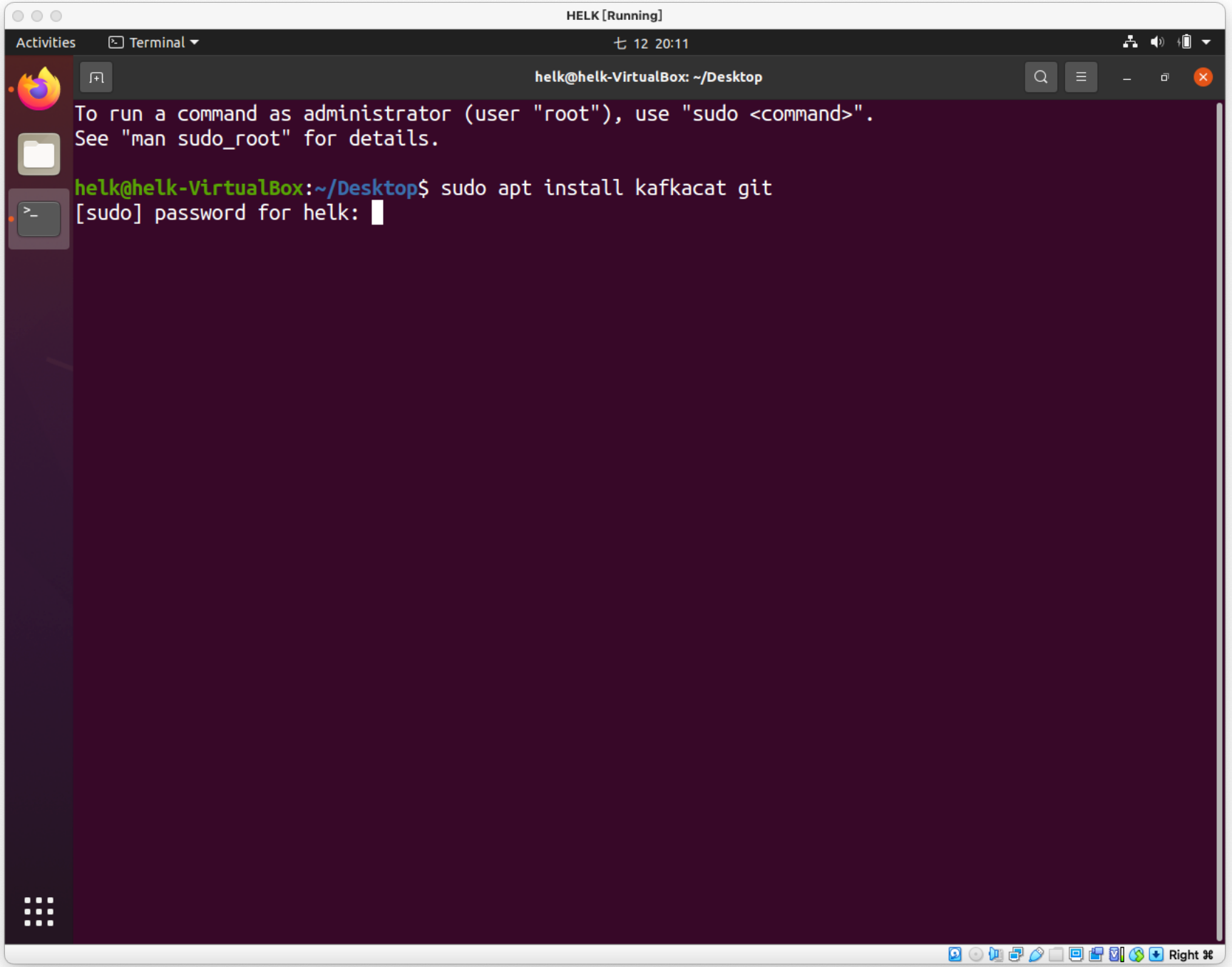
安裝 Kafkacat

- 在桌面「右鍵」–>「Open in Terminal」



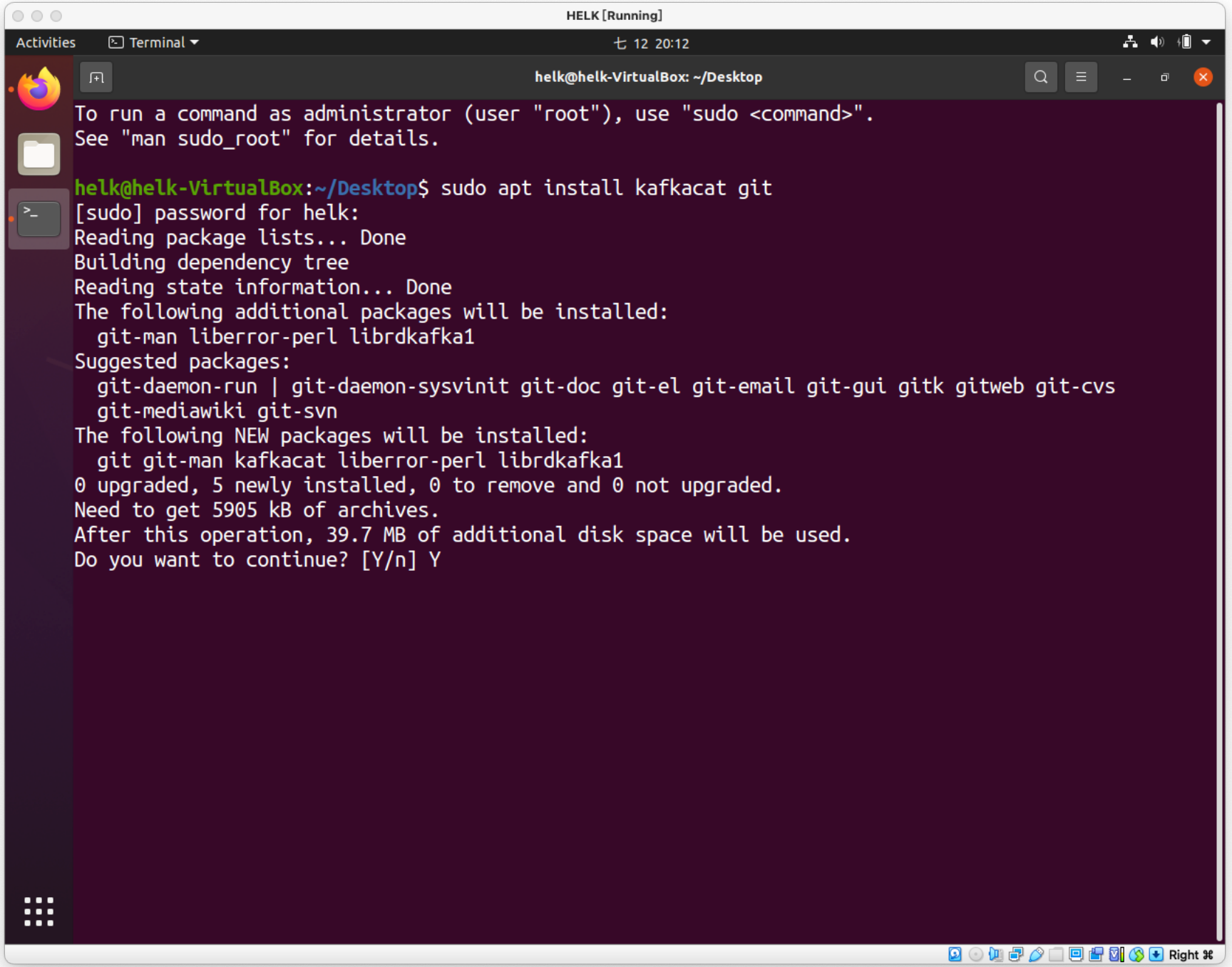
安裝 Kafkacat

- 在桌面「右鍵」–>「Open in Terminal」
- 輸入「sudo apt install kafkacat git」–> 輸入密碼



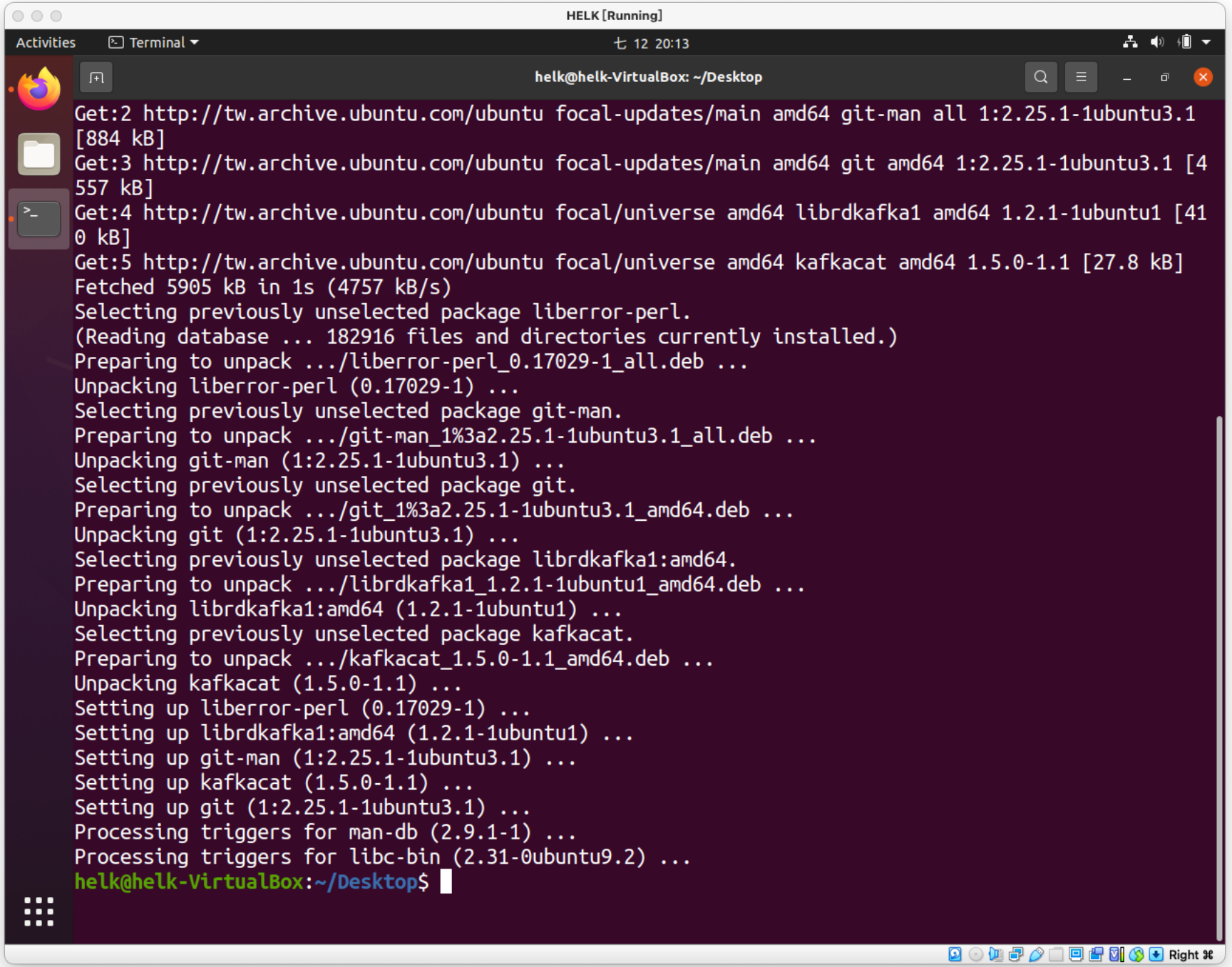
安裝 Kafkacat

- 在桌面「右鍵」–>「Open in Terminal」
- 輸入「sudo apt install kafkacat git」–> 輸入密碼
- 輸入「Y」



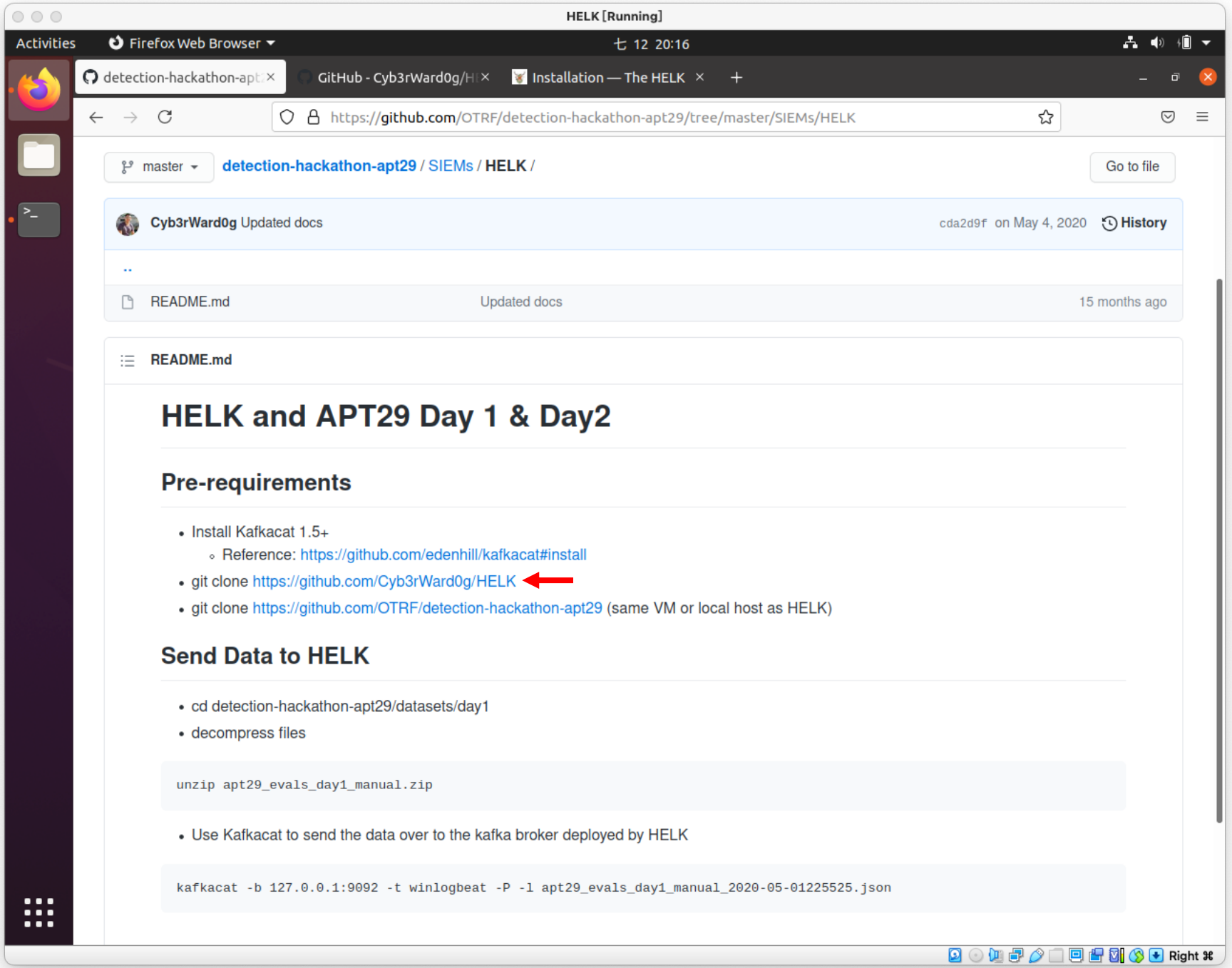
安裝 Kafkacat

- 在桌面「右鍵」–>「Open in Terminal」
- 輸入「sudo apt install kafkacat git」–> 輸入密碼
- 輸入「Y」
- 若沒有出現錯誤，應該就是沒有問題



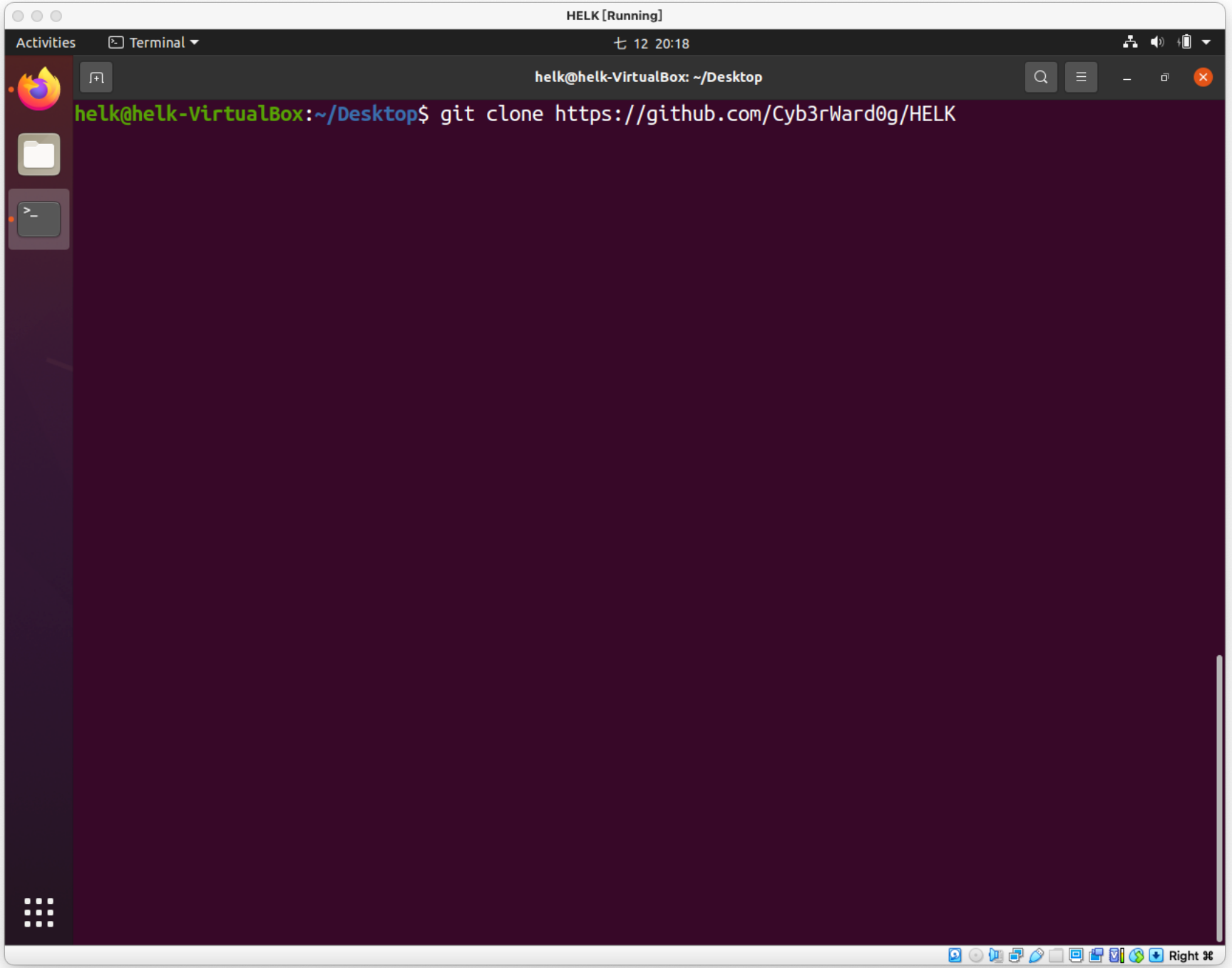
安裝 HELK

- 打開連結 –> 複製 HELK 網址



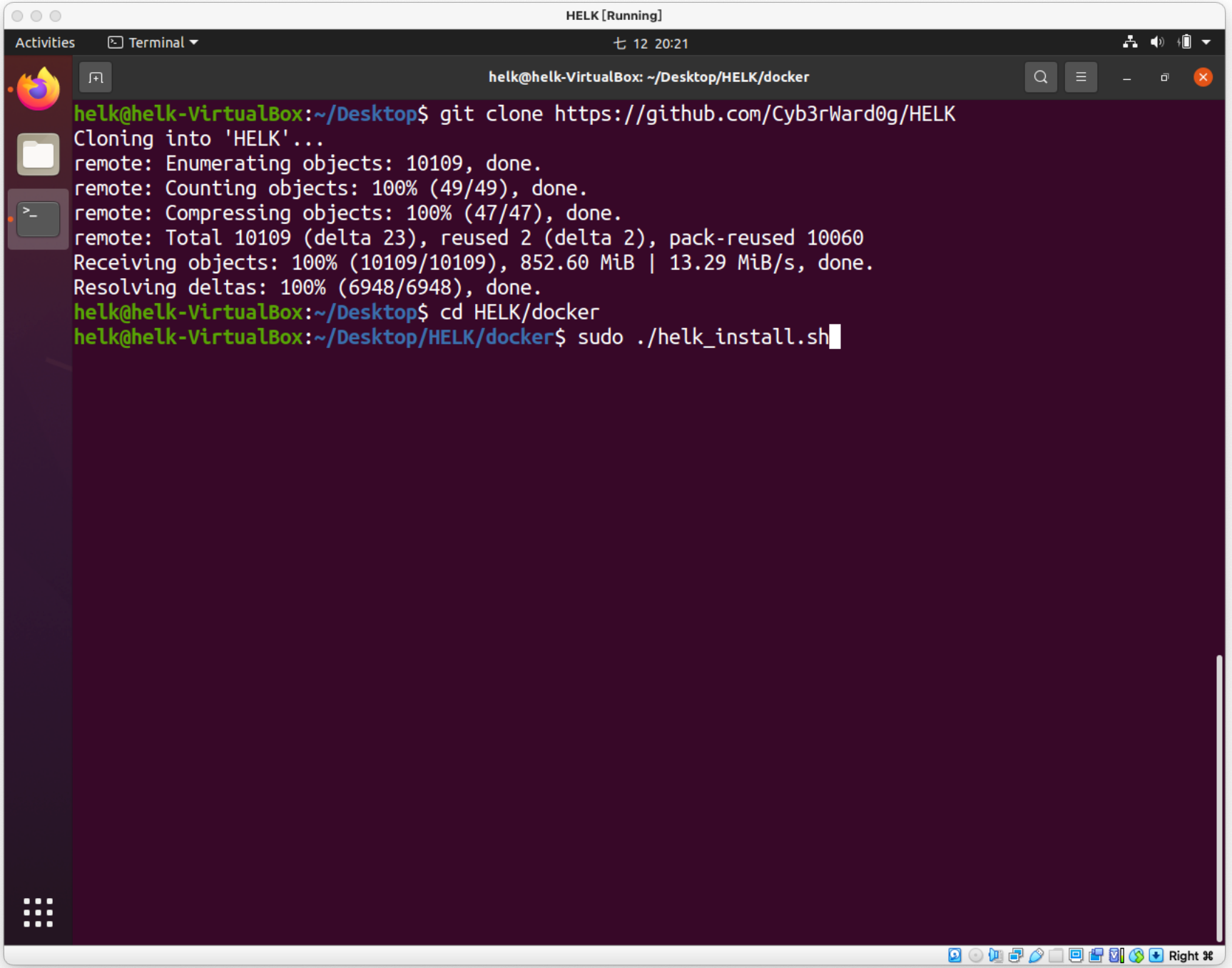
安裝 HELK

- 打開連結 –> 複製 HELK 網址
- 輸入「git clone <網址>」



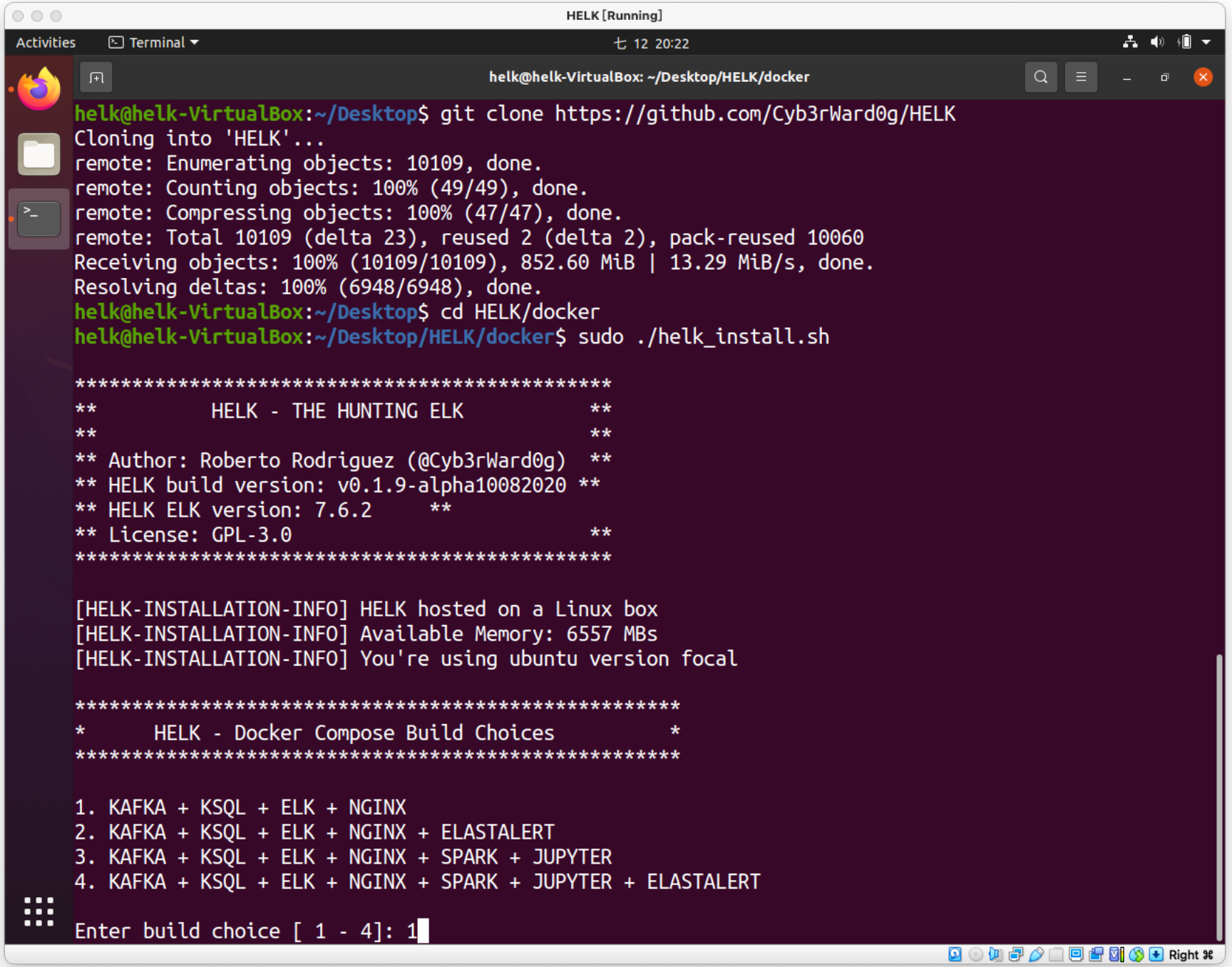
安裝 HELK

- 打開連結 -> 複製 HELK 網址
- 輸入「git clone <網址>」
- 輸入「cd HELK/docker」->
  「sudo ./helk_install.sh」



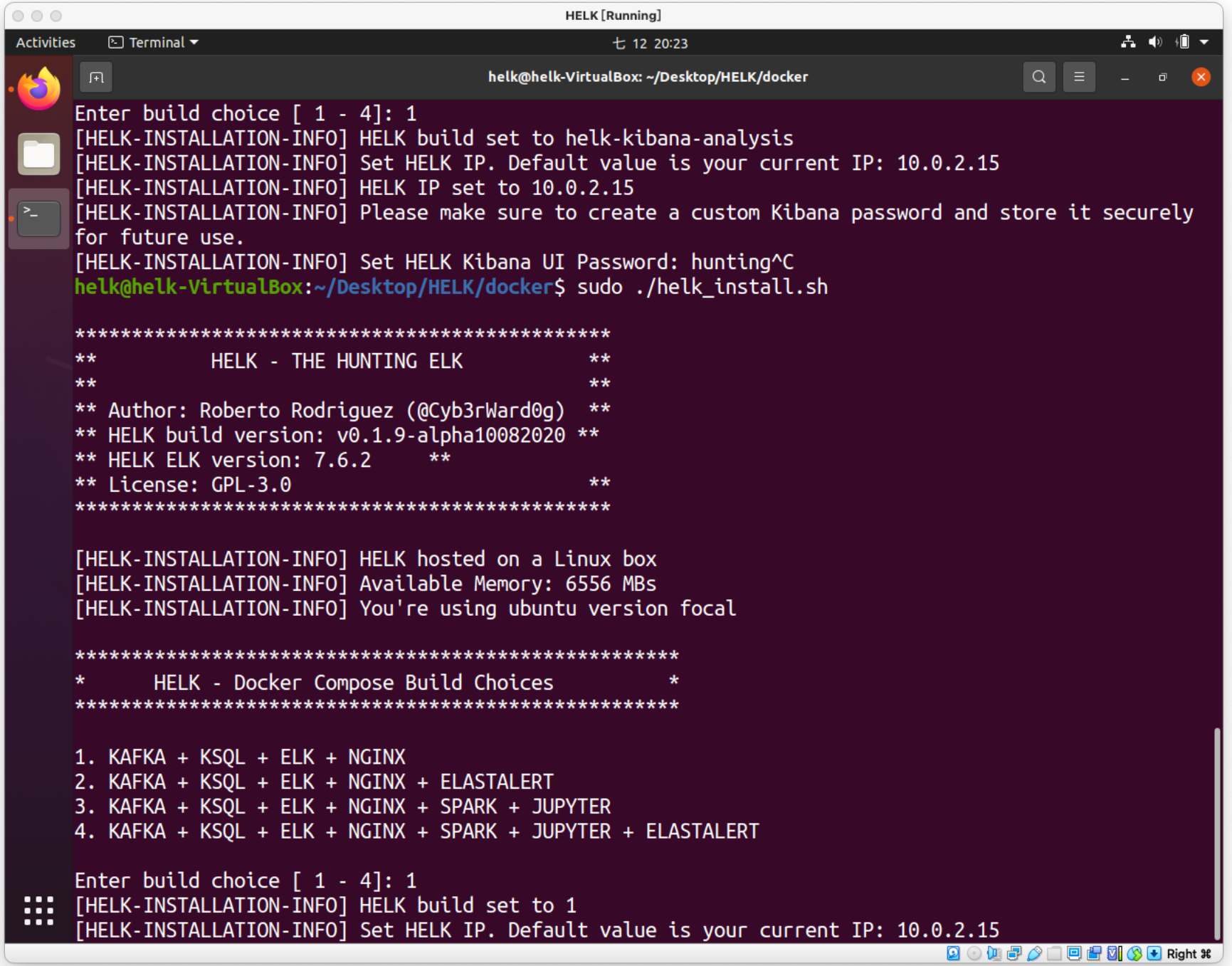
安裝 HELK

- 打開連結 -> 複製 HELK 網址
- 輸入「git clone <網址>」
- 輸入「cd HELK/docker」->
  「sudo ./helk_install.sh」
- Builde choice 輸入「1」



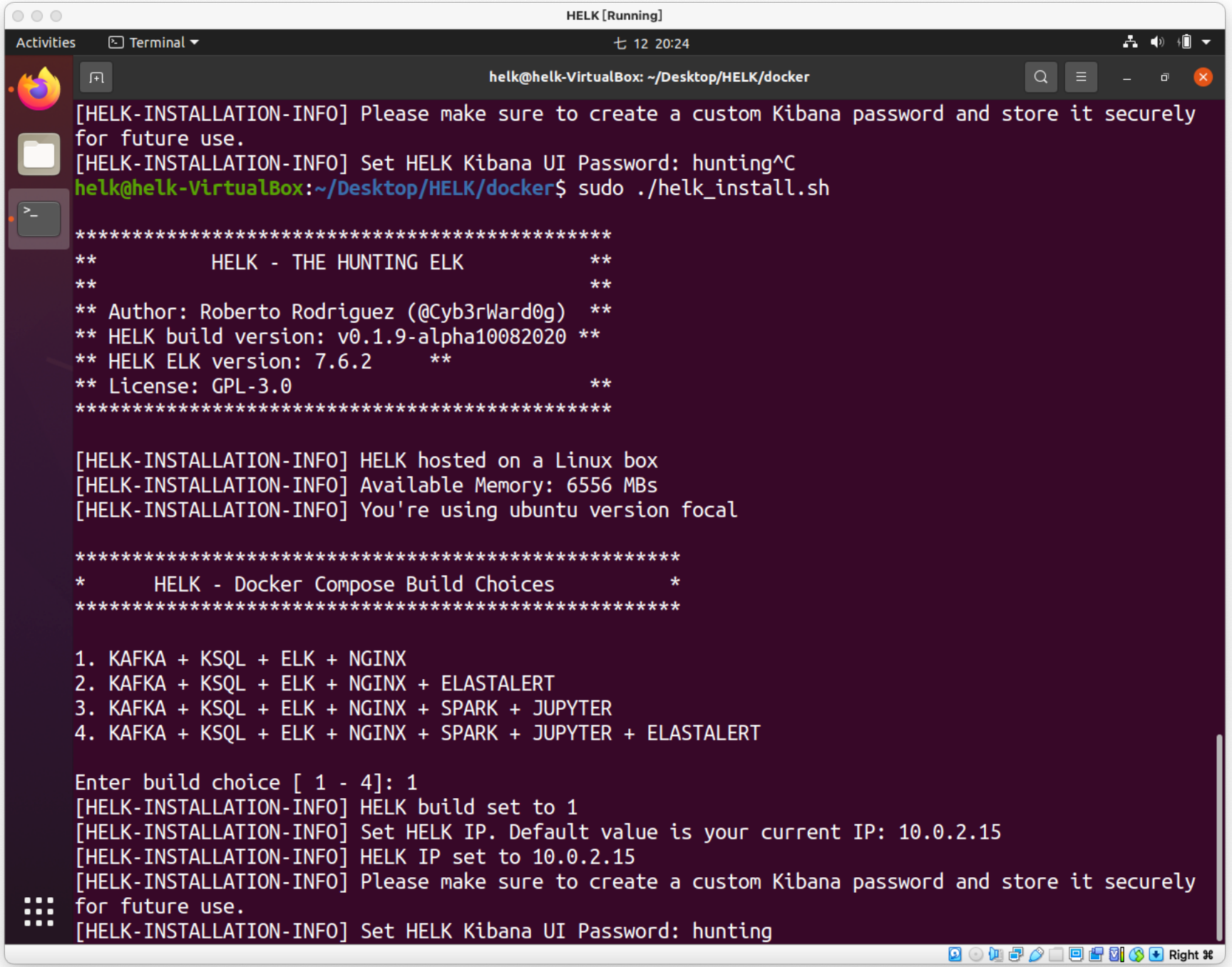
安裝 HELK

- 打開連結 -> 複製 HELK 網址
- 輸入「git clone <網址>」
- 輸入「cd HELK/docker」->
  「sudo ./helk_install.sh」
- Builde choice 輸入「1」
- HELK IP 直接「Enter」



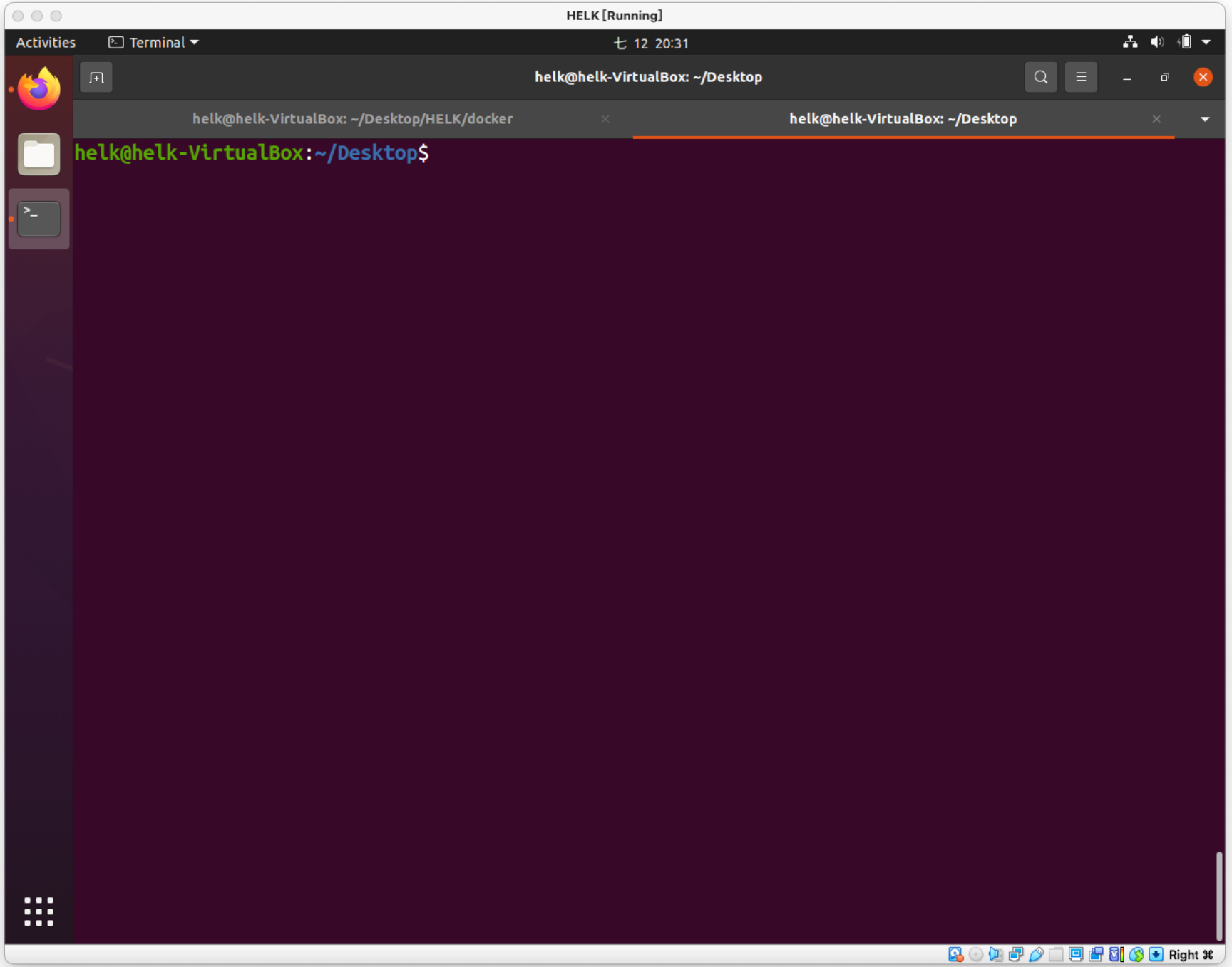
安裝 HELK

- 打開連結 -> 複製 HELK 網址
- 輸入「git clone <網址>」
- 輸入「cd HELK/docker」->
  「sudo ./helk_install.sh」
- Builde choice 選擇「1」
- HELK IP 直接「Enter」
- 設定 Kibana password



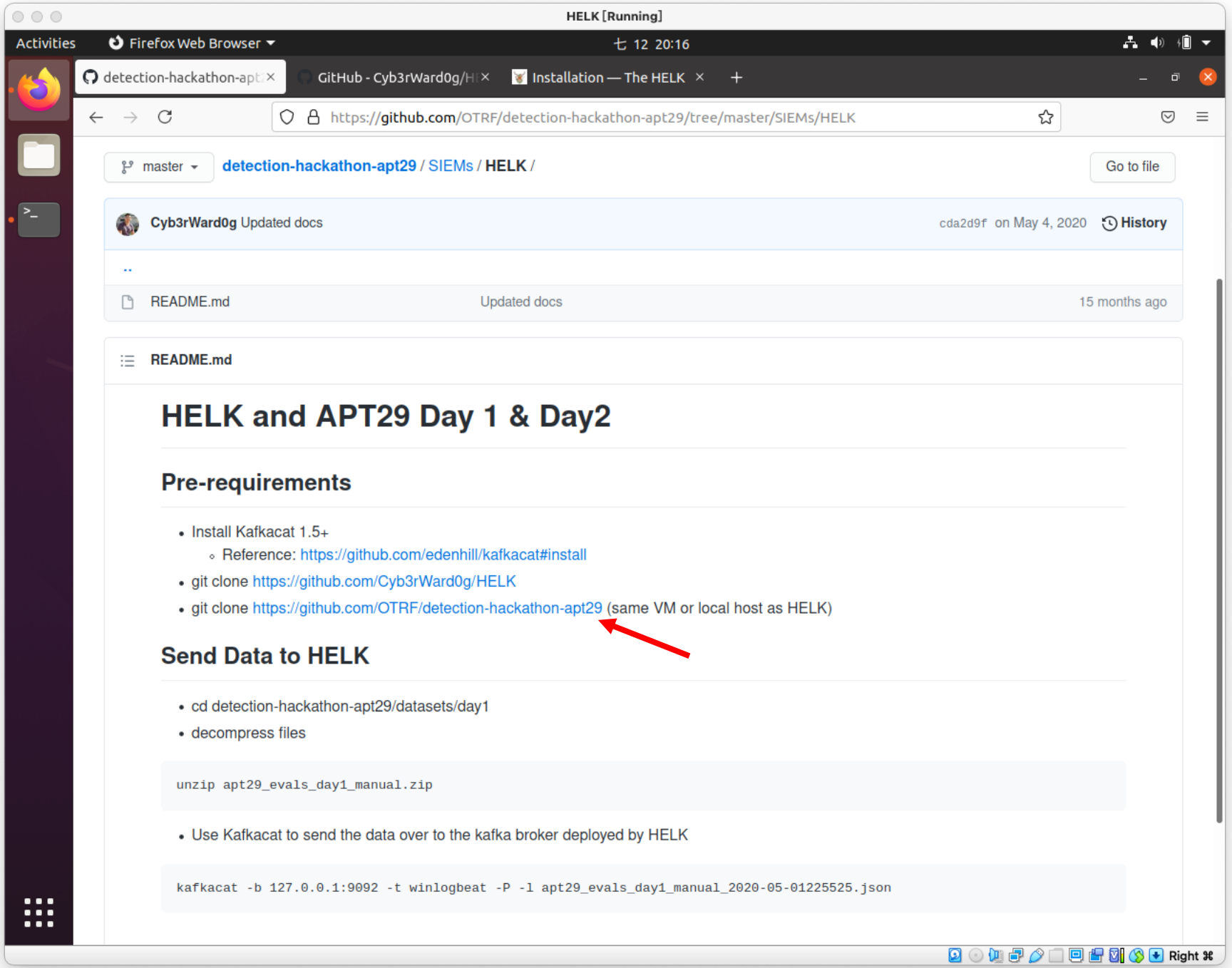
下載 datasets

- 輸入「Ctrl+Shift+t」打開 tab



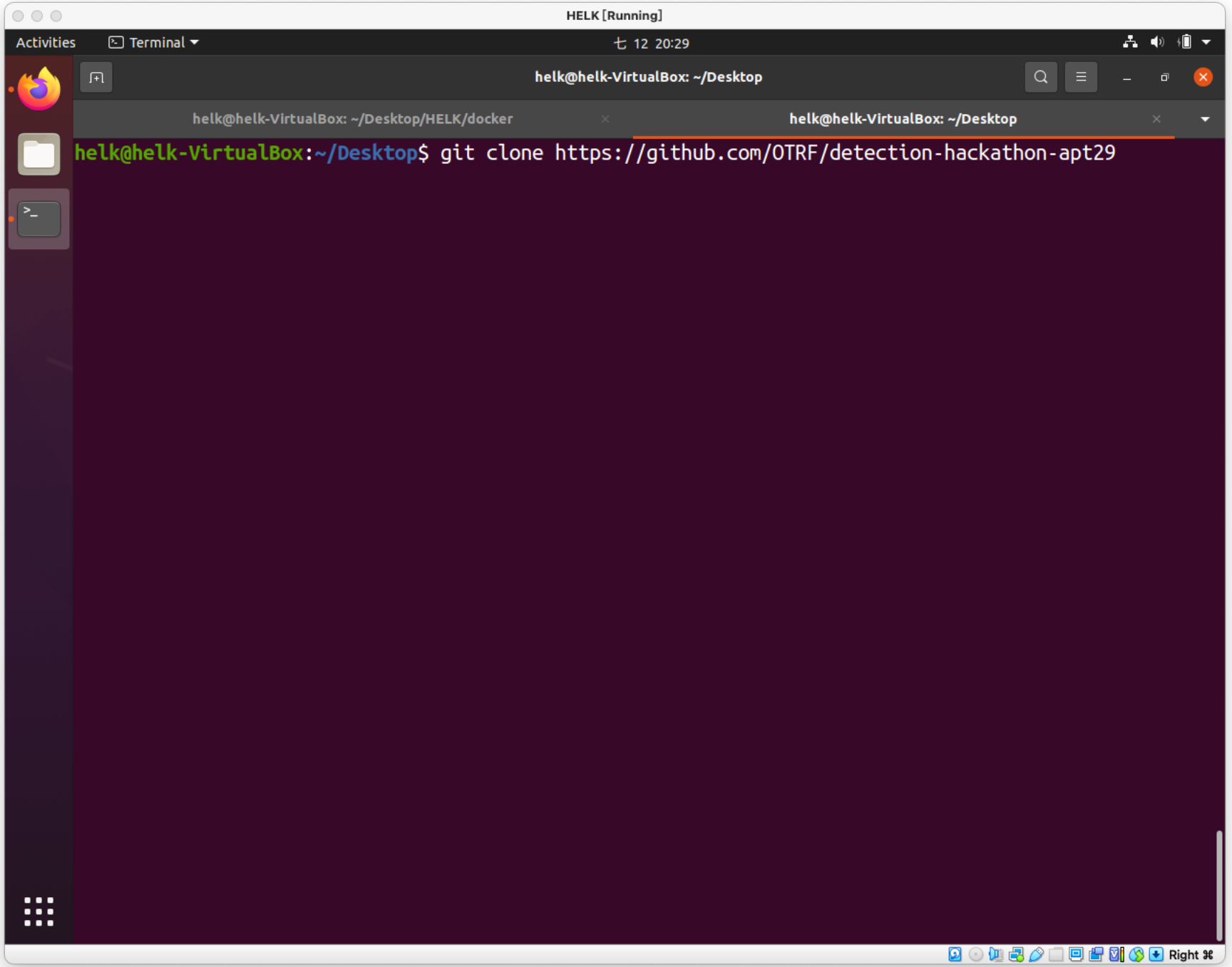
下載 datasets

- 輸入「Ctrl+Shift+t」打開 tab
- 打開連結 –> 複製第三個網址



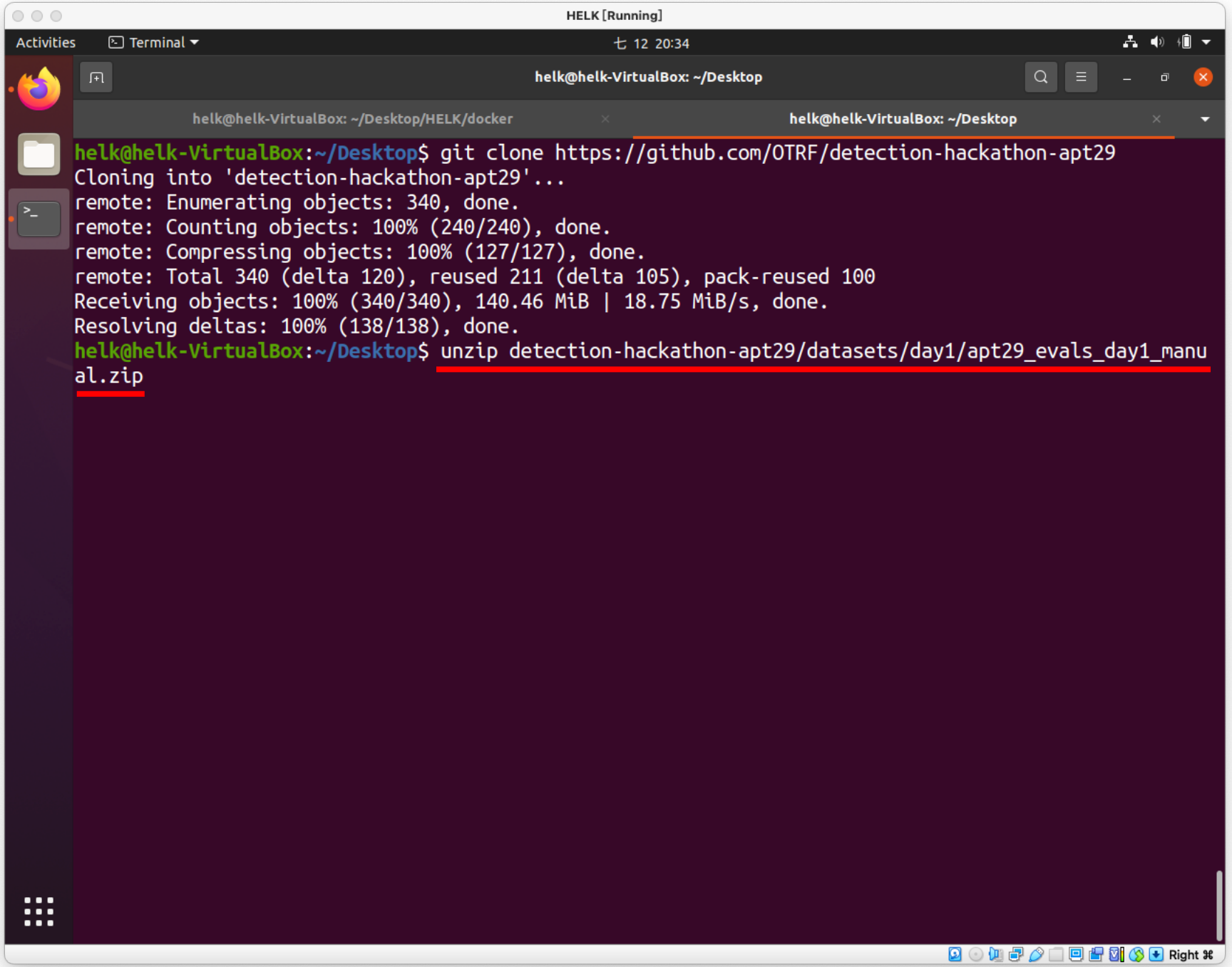
下載 datasets

- 輸入「Ctrl+Shift+t」打開 tab
- 打開連結 -> 複製第三個網址
- 輸入「git clone <網址>」



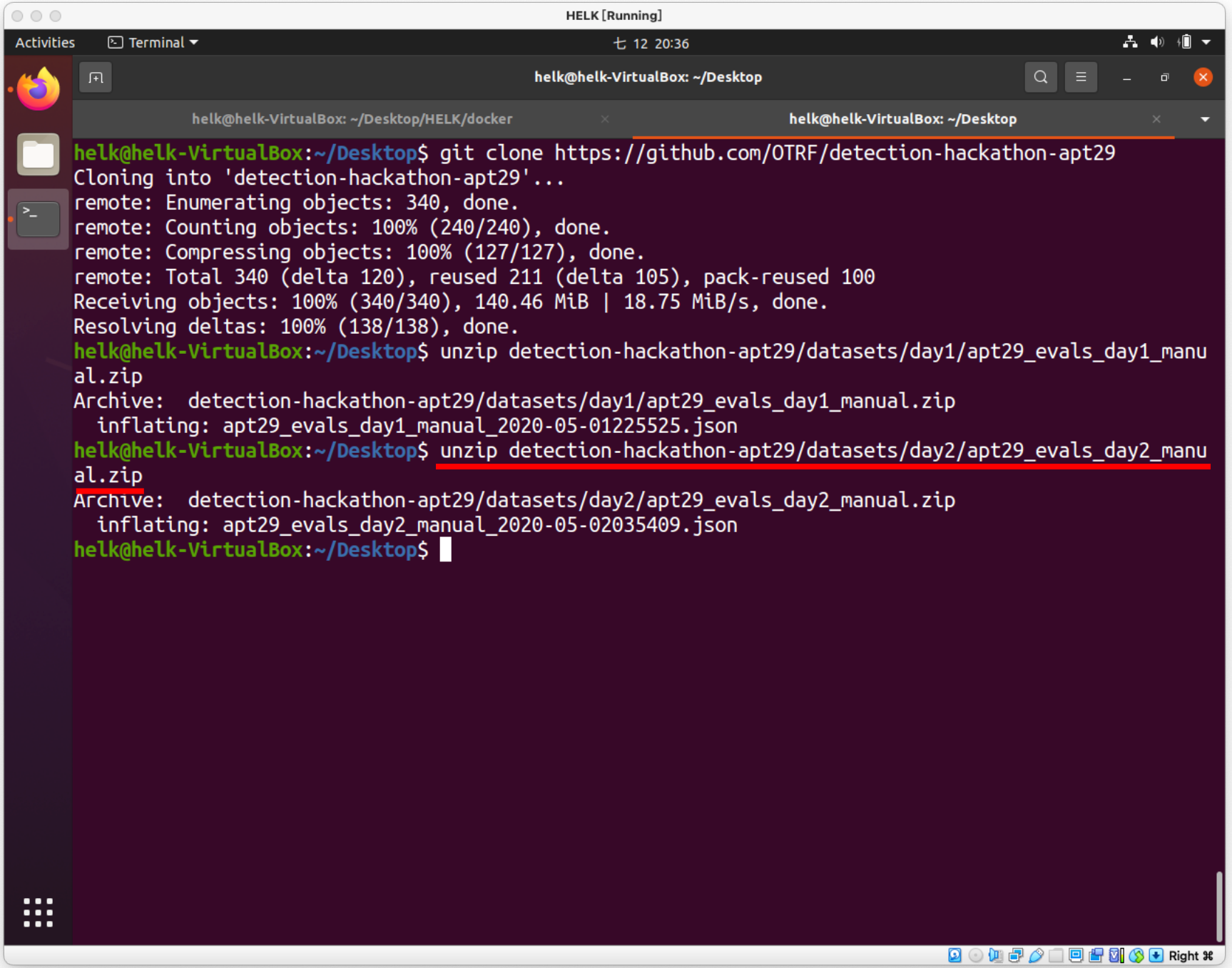
下載 datasets

- 輸入「Ctrl+Shift+t」打開 tab
- 打開連結 -> 複製第三個網址
- 輸入「git clone <網址>」
- 輸入「unzip …day1…」



下載 datasets

- 輸入「Ctrl+Shift+t」打開 tab
- 打開連結 -> 複製第三個網址
- 輸入「git clone <網址>」
- 輸入「unzip …day1…」
- 輸入「unzip …day2…」

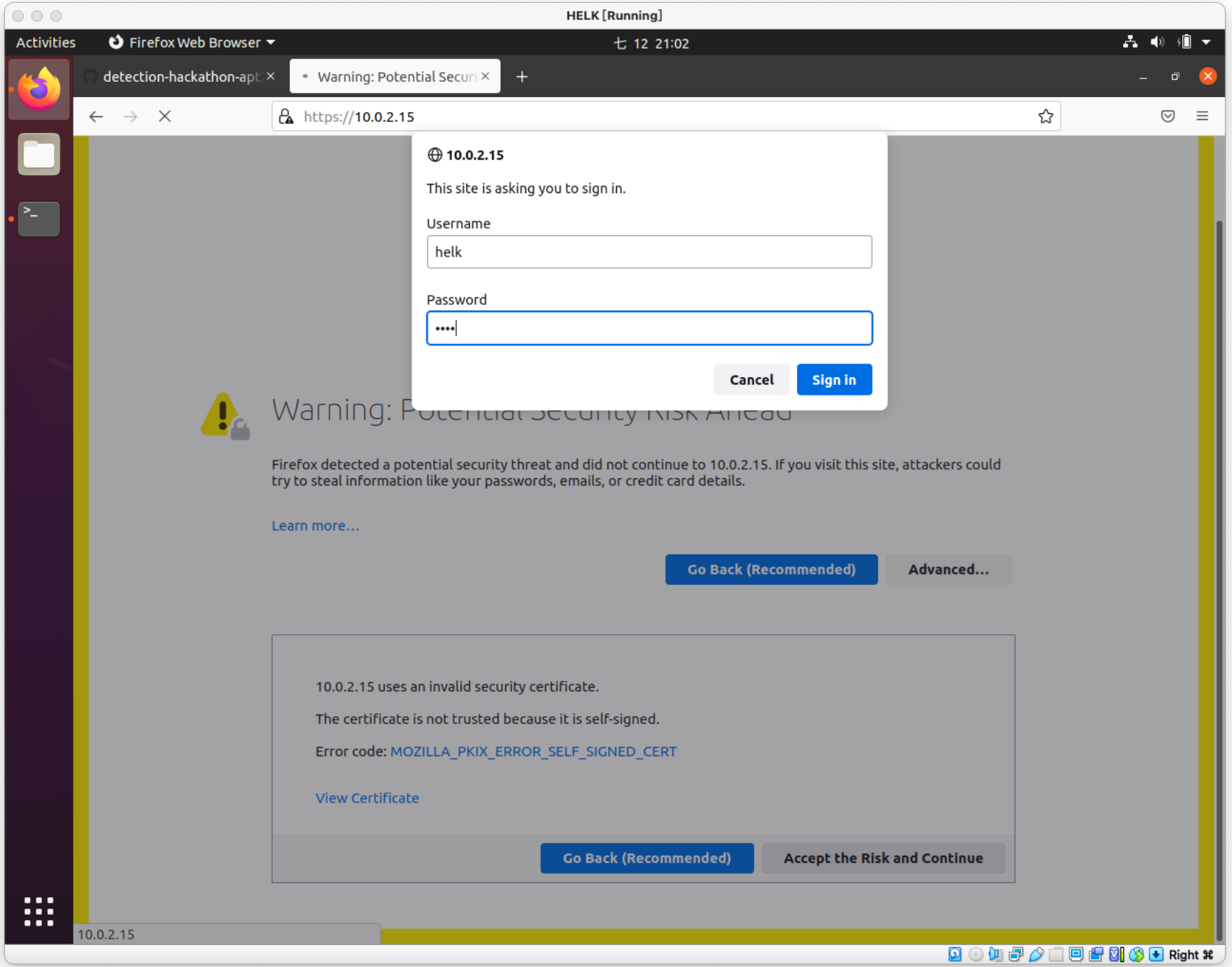


HELK 資訊

```
HELK KIBANA URL: https://10.0.2.15
HELK KIBANA USER: helk
HELK KIBANA PASSWORD: helk
HELK ZOOKEEPER: 10.0.2.15:2181
HELK KSQL SERVER: 10.0.2.15:8088
```

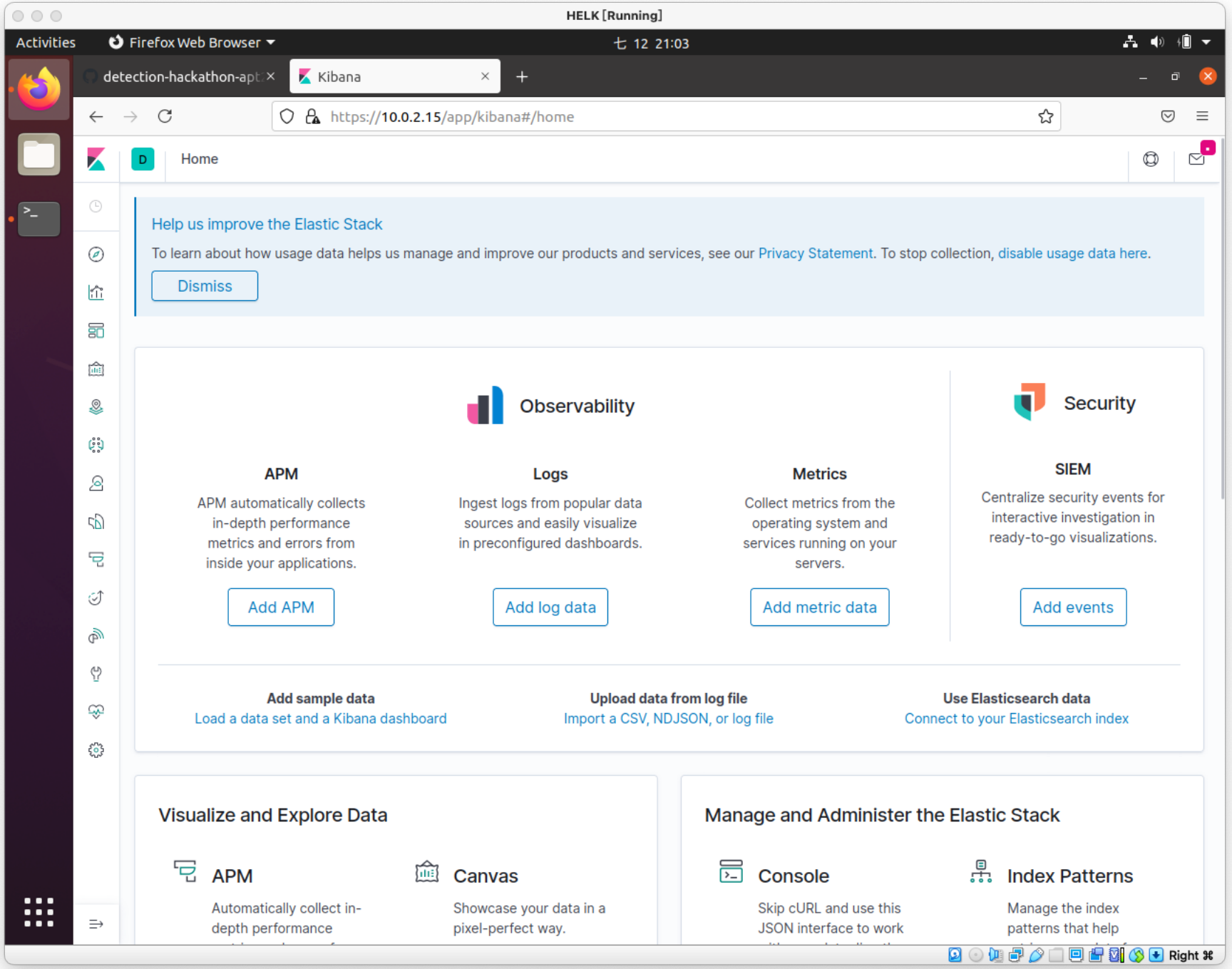
啟動 HELK

- 打開「https://<ip>」–> 「Advanced…」–>「Accept the Risk and Continue」，然後輸入 user、password



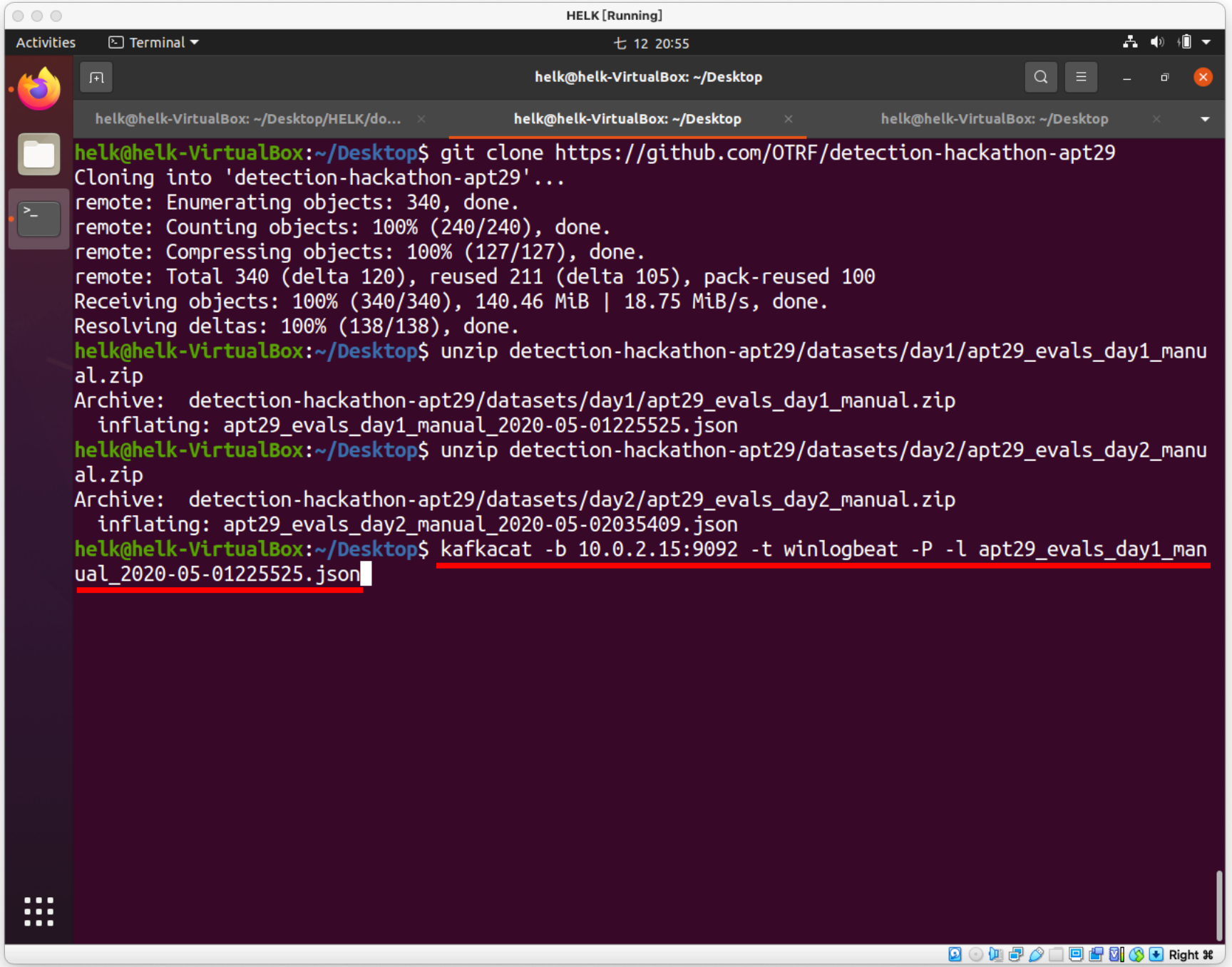
啟動 HELK

- 打開「https://<ip>」–> 「Advanced...」–>「Accept the Risk and Continue」，然後輸入 user、password
- 若出現 502 Bad Gateway 表示還在啟動中，直到出現 Kibana 畫面表示啟動完成



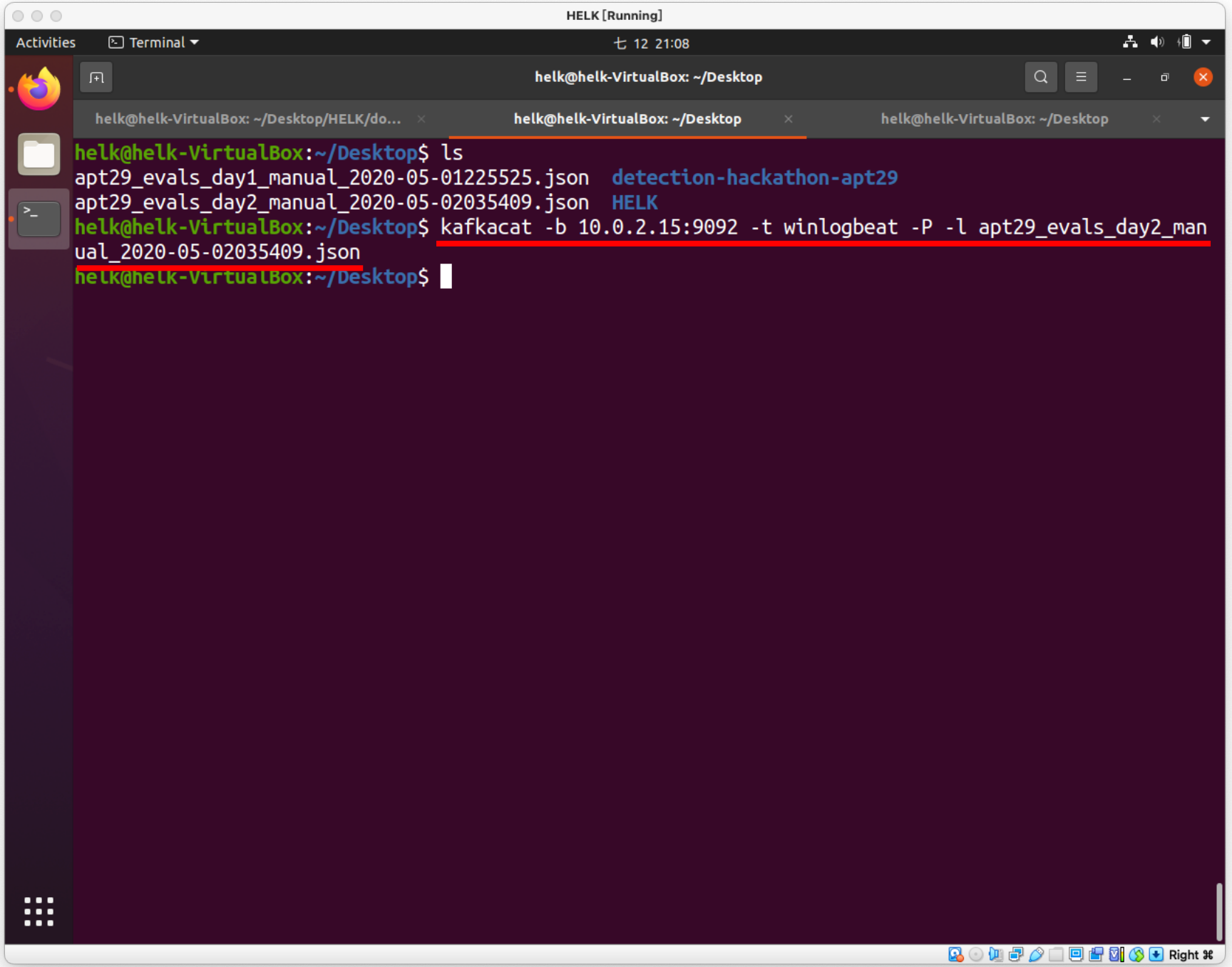
匯入 dataset

- 輸入「... <ip>:9092 ...day1...」



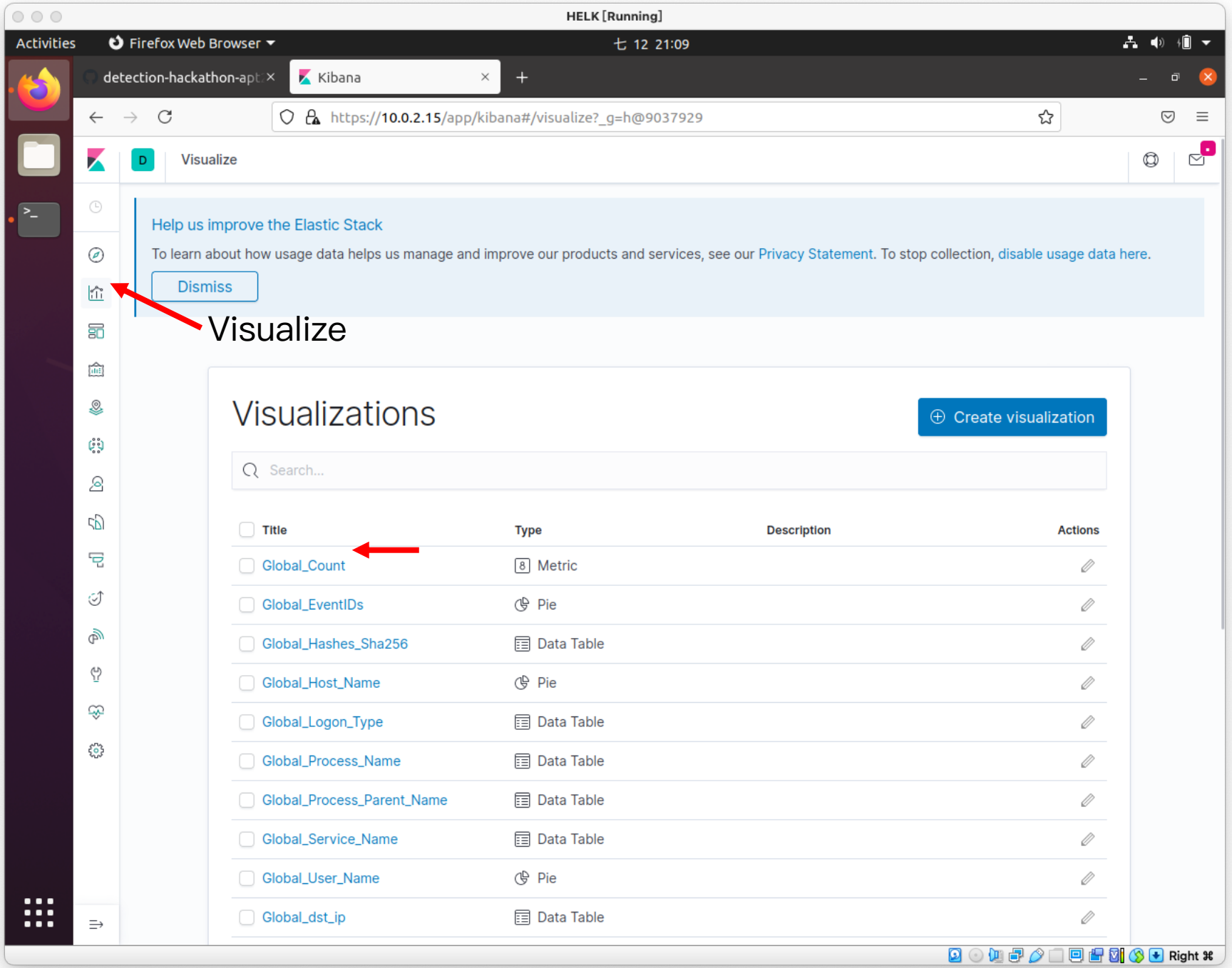
匯入 dataset

- 輸入「... <ip>:9092 …day1…」
- 輸入「... <ip>:9092 …day2…」



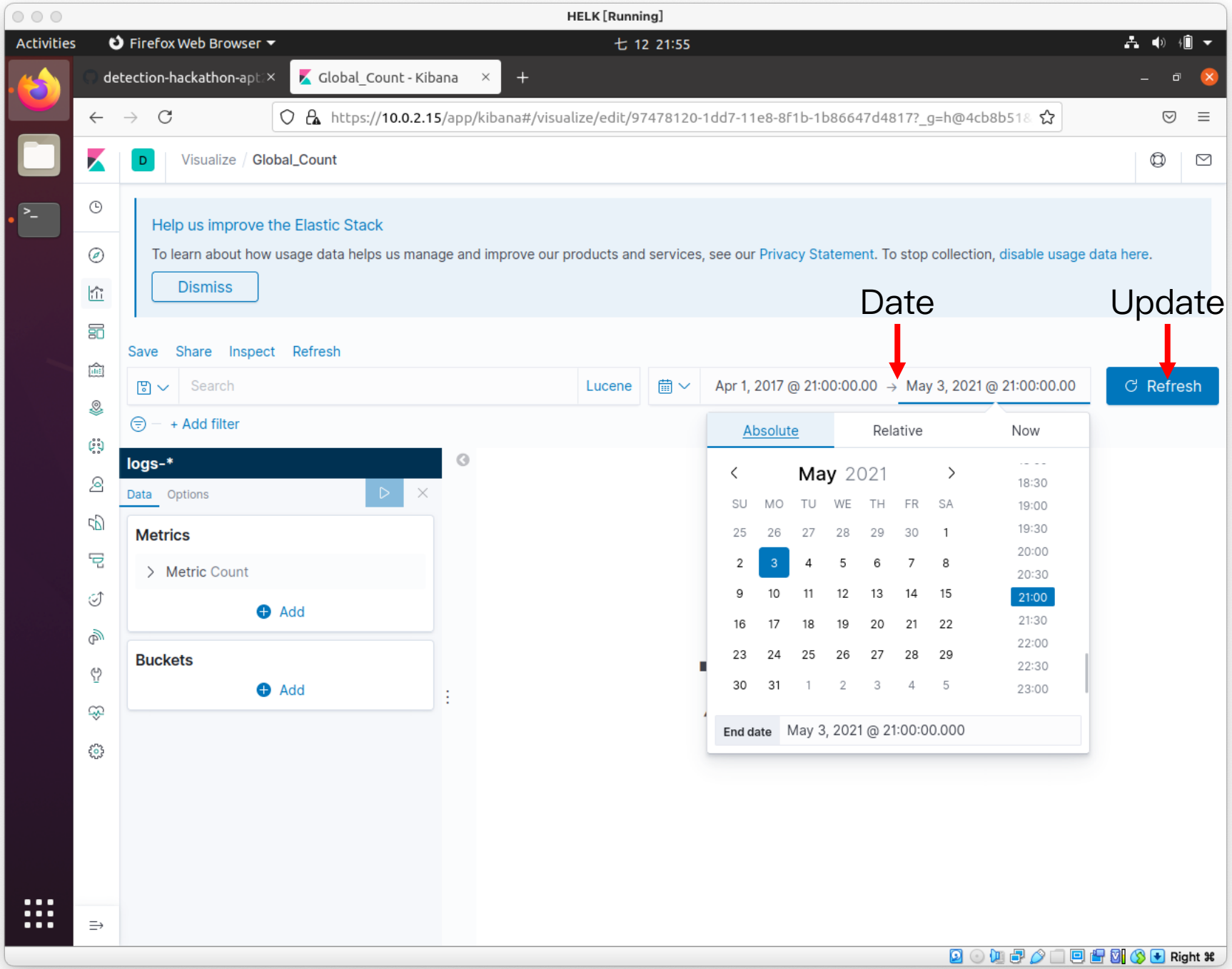
匯入 dataset

- 輸入「... <ip>:9092 ...day1...」
- 輸入「... <ip>:9092 ...day2...」
- 打開 Kibana，點選「Visualize」
  –>「Global_Count」



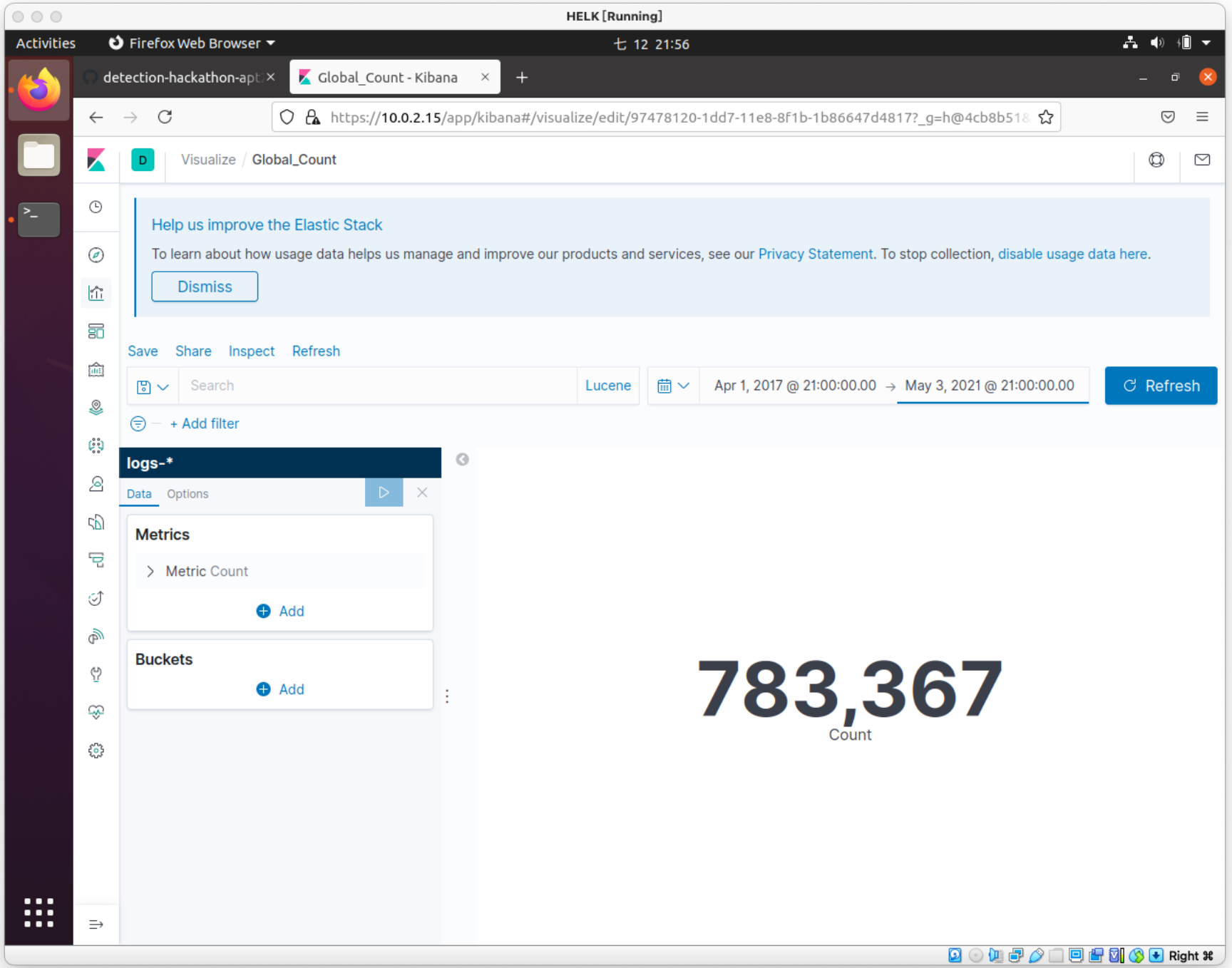
匯入 dataset

- 輸入「... <ip>:9092 ...day1...」
- 輸入「... <ip>:9092 ...day2...」
- 打開 Kibana，點選「Visualize」–>「Global_Count」
- 設定 Date 至「2020/04/30 ~ 2020/05/03」–>「Update」



匯入 dataset

- 輸入「... <ip>:9092 …day1…」
- 輸入「... <ip>:9092 …day2…」
- 打開 Kibana，點選「Visualize」–>「Global_Count」
- 設定 Date 至「2020/04/30 ~ 2020/05/03」–>「Update」
- 點選「Update」，等到數值為 783,367，應該就是匯入完成



啟動、關閉 HELK

- 下次開機會需要使用右方的 start 指令啟動 HELK

```
sudo docker-compose -f /home/helk/Desktop/HELK/docker/helk-kibana-analysis-basic.yml start
sudo docker-compose -f /home/helk/Desktop/HELK/docker/helk-kibana-analysis-basic.yml stop
```