UNIVERSITY OF Baguio SCHOOL OF INFORMATION AND TECHNOLOGY		
NAME: Arjay V De Leon	DATE PERFORMED: 11/13/24	
Section: IDC - 1	DATE SUBMITTED: 11/13/24	/50

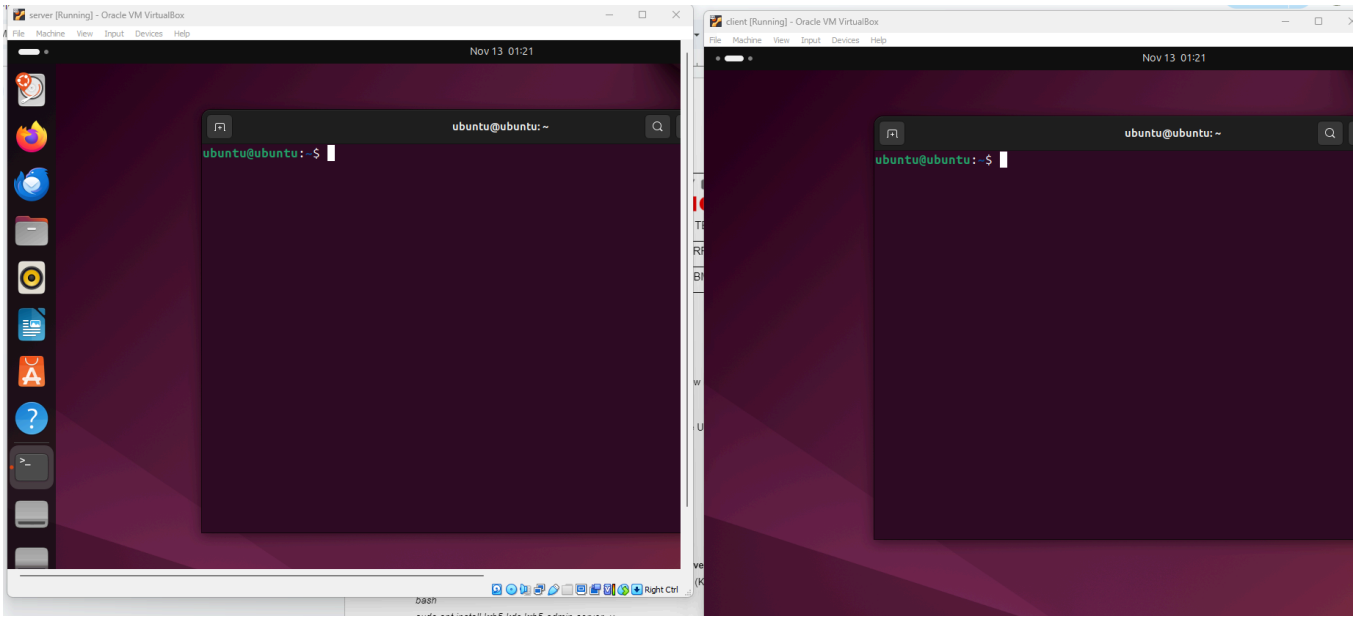
SYSADM1 – Kerberos Lab Activity: A step-by-step Guide

Objective:

Set up a basic Kerberos authentication system to understand how Kerberos manages secure logins through ticket-based access.

Setup Requirements:

- Two VMs in Oracle VM, both running a Linux distribution like Ubuntu or CentOS.
- VM1: Kerberos Server
- VM2: Kerberos Client

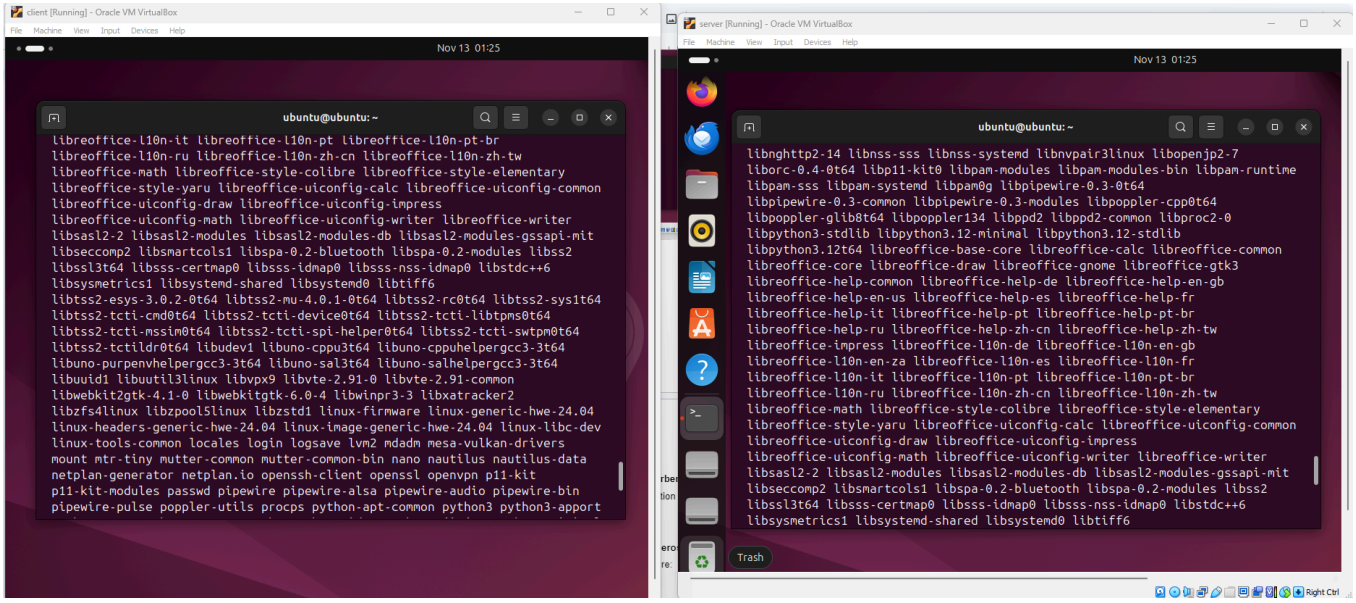


Step 1: Initial Setup and Package Installation

1. **Update Packages on Both VMs:**
    - Open a terminal on each VM and run:

bash

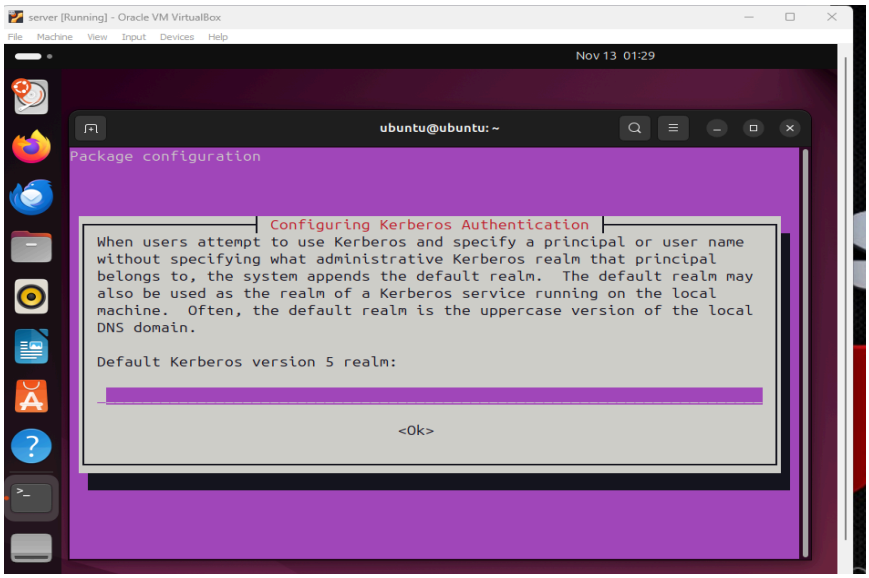
sudo apt update && sudo apt upgrade -y



2. **Install Kerberos Server Packages on VM1 (Kerberos Server):**
   - In VM1, install the Kerberos Key Distribution Center (KDC) and admin server:

bash

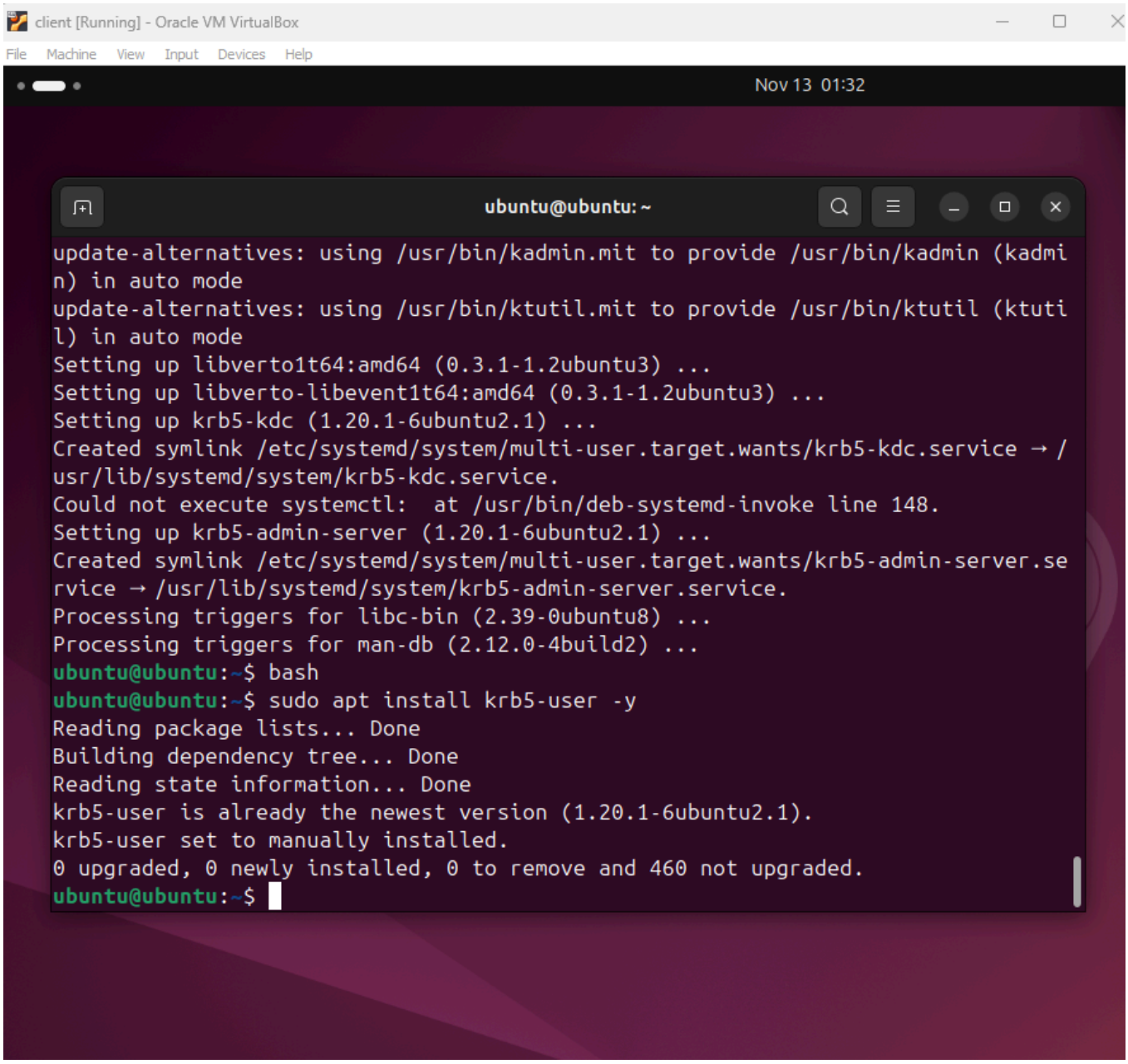
sudo apt install krb5-kdc krb5-admin-server -y



3. **Install Kerberos Client Package on VM2 (Kerberos Client):**
   - In VM2, install the Kerberos client software:

bash

sudo apt install krb5-user -y



- During installation, when prompted, enter the Kerberos realm you plan to set up, e.g., MYLAB.LOCAL.

Step 2: Configure the Kerberos Server (VM1)

1. **Edit the Kerberos Configuration File:**
   - Open /etc/krb5.conf for editing:

bash

sudo nano /etc/krb5.conf

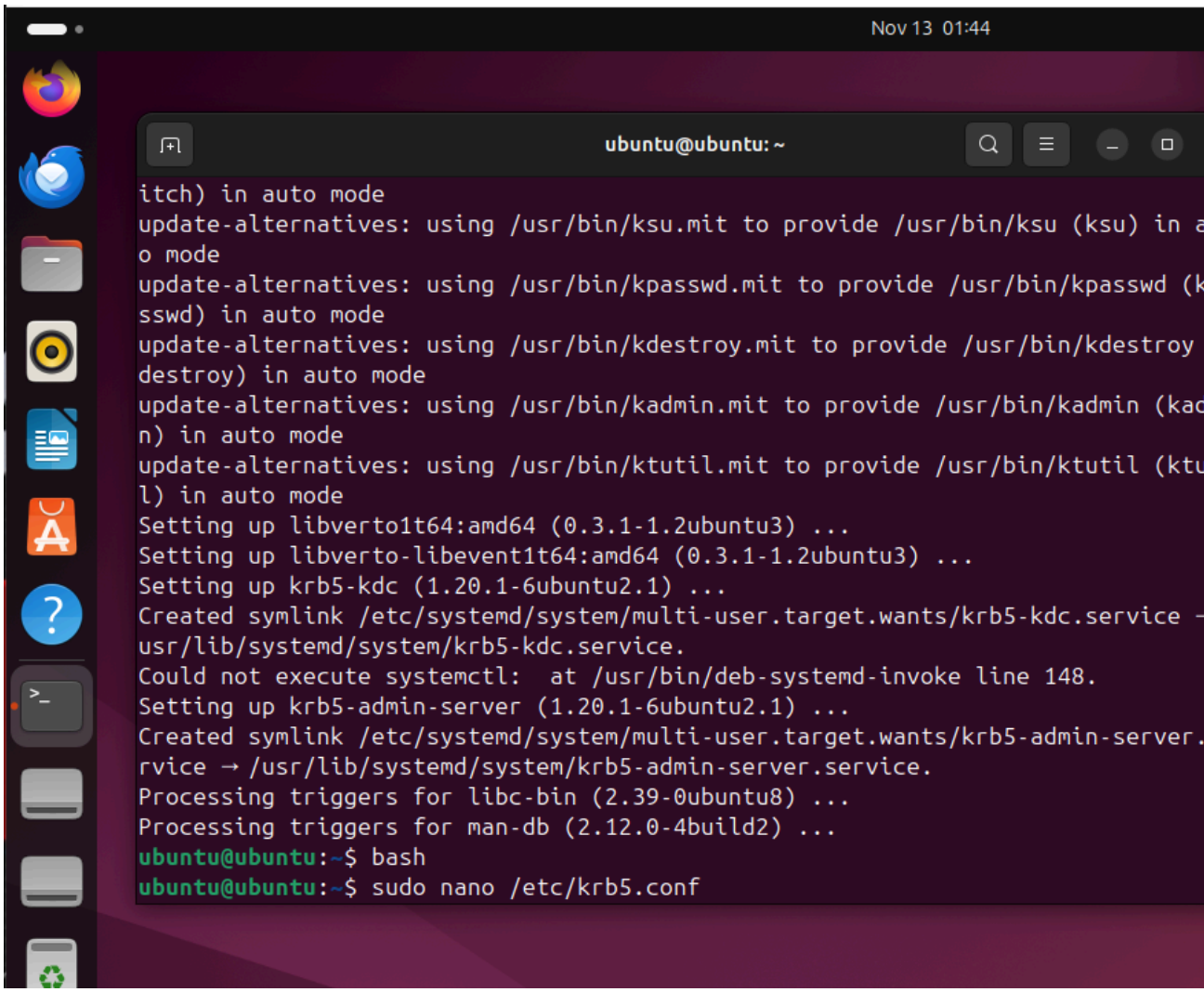
- Set the realm as MYLAB.LOCAL. You should also specify the KDC and admin server as VM1's hostname or IP address:

ini

```
[libdefaults]
    default_realm = MYLAB.LOCAL

[realms]
    MYLAB.LOCAL = {
        kdc = <VM1_IP_or_hostname>
        admin_server = <VM1_IP_or_hostname>
    }
```

- Save and close the file (Ctrl+X, then Y, and Enter to confirm).

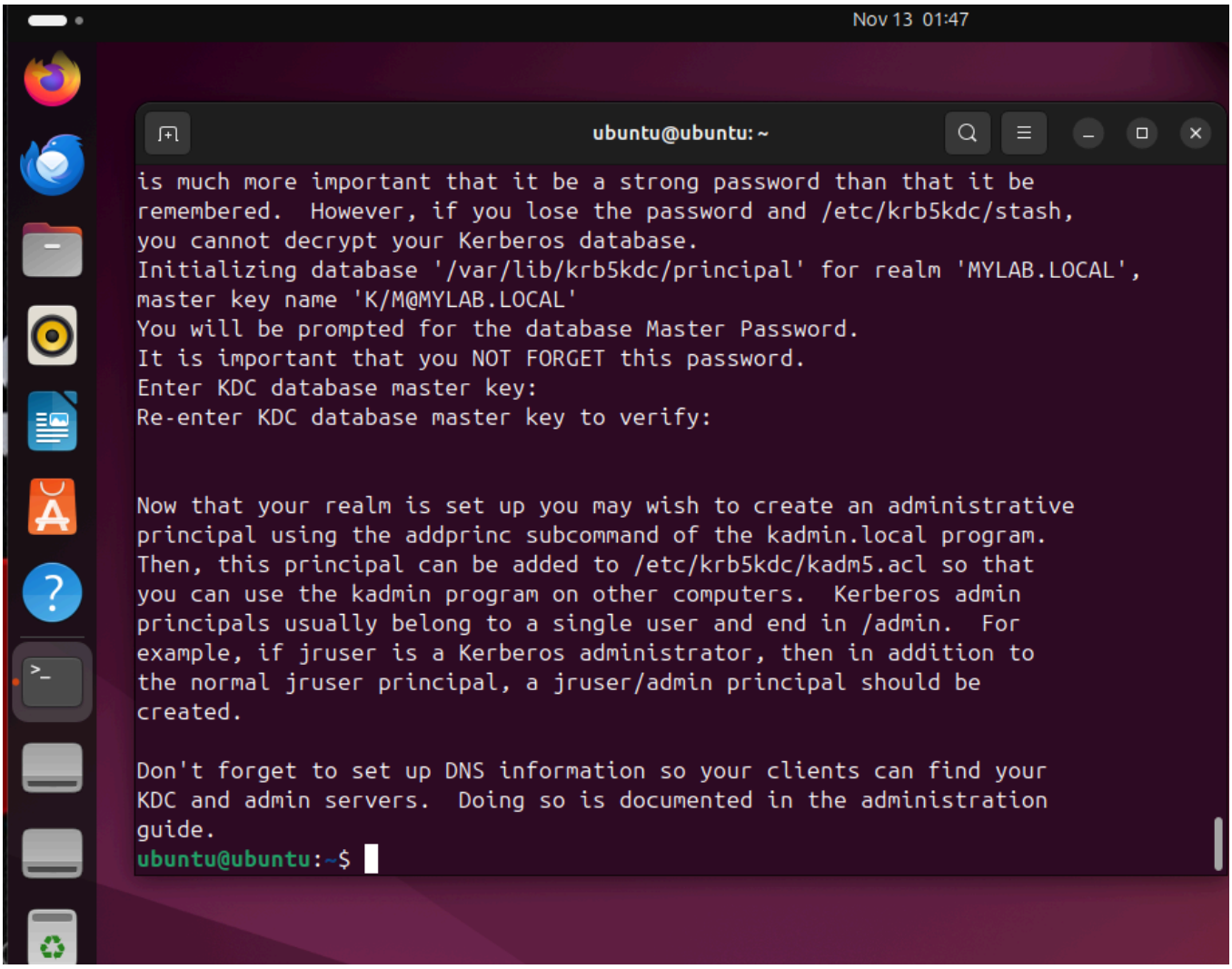


2. **Initialize the Kerberos Database:**
    - Create the database for the Kerberos realm:

bash

sudo krb5_newrealm

- You will be prompted to set a password for the Kerberos database.



3. **Start and Enable the Kerberos Services:**
   - Start the KDC and admin server, and ensure they start automatically on boot:

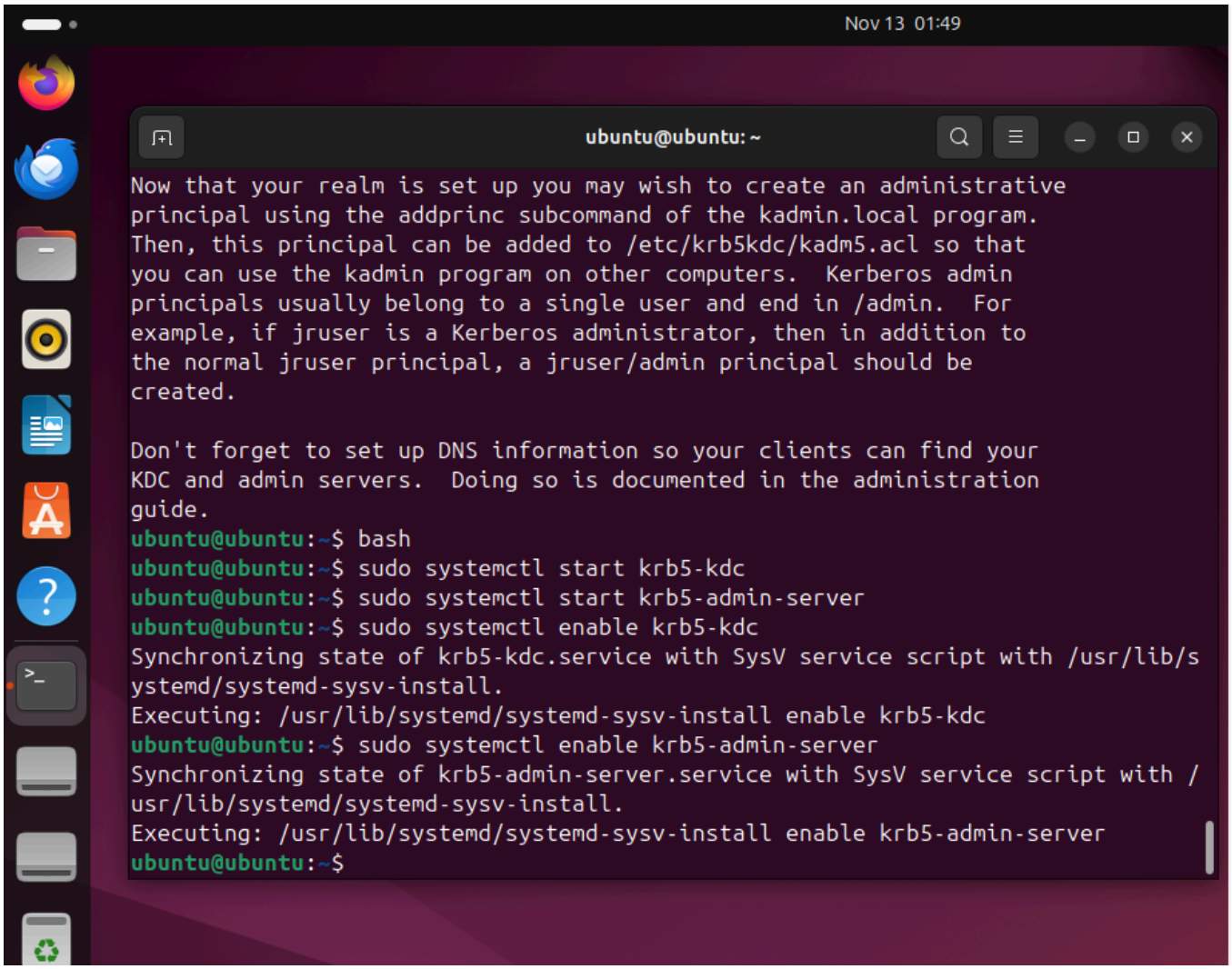
bash

sudo systemctl start krb5-kdc

sudo systemctl start krb5-admin-server

sudo systemctl enable krb5-kdc

sudo systemctl enable krb5-admin-server



arjay

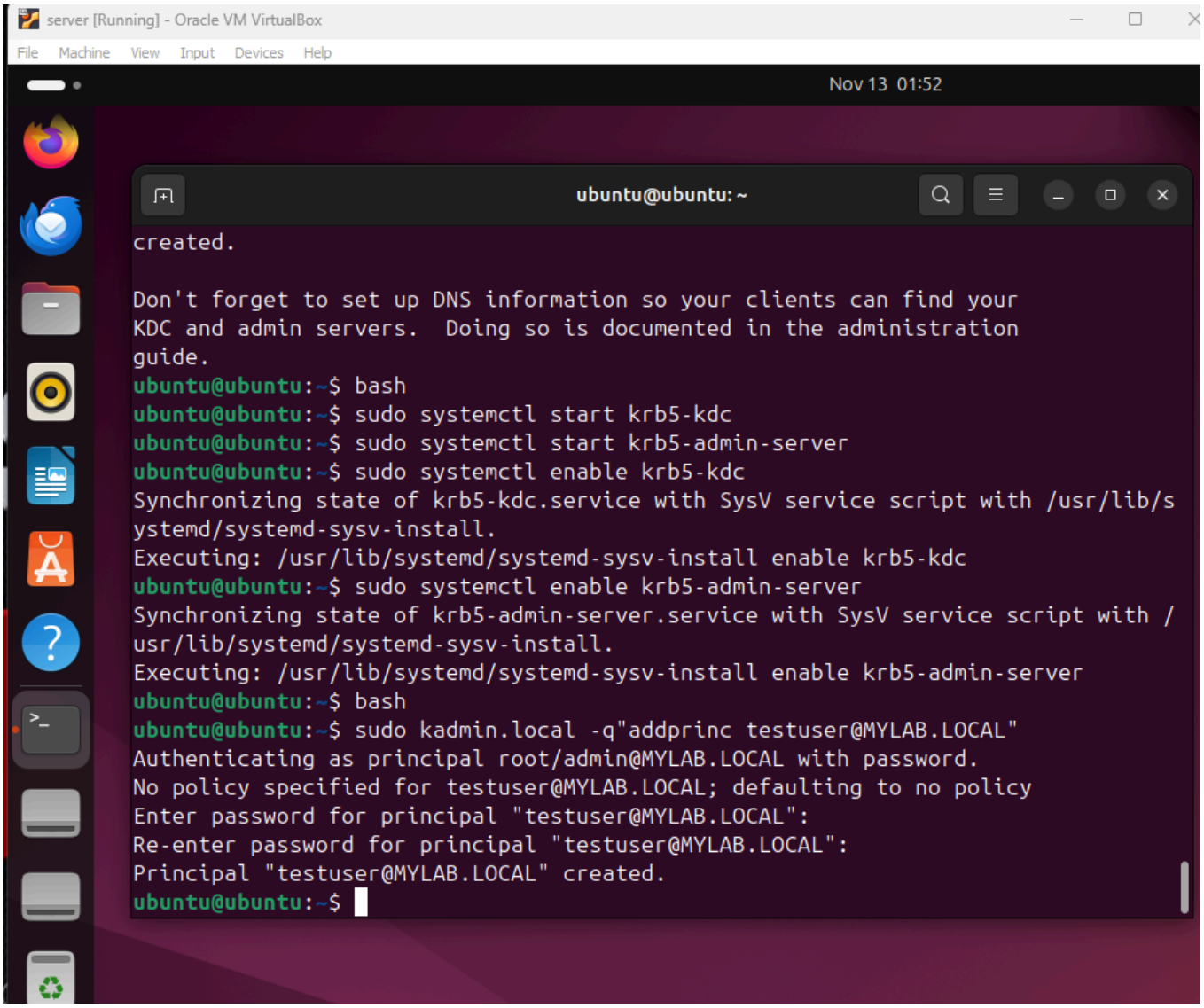
Step 3: Set Up a Kerberos User Principal

1. **Create a New User Principal:**
    - Run the following command to create a test user in the Kerberos realm:

bash

sudo kadmin.local -q "addprinc testuser@MYLAB.LOCAL"

    - Set a password for testuser.



2. **Verify the User Principal:**
   - To confirm the principal is created, list all principals:

bash

sudo kadmin.local -q "listprincs"

```
ubuntu@ubuntu:~$ bash
ubuntu@ubuntu:~$ sudo kadmin.local -q "listprincs"
Authenticating as principal root/admin@MYLAB.LOCAL with password.
K/M@MYLAB.LOCAL
kadmin/admin@MYLAB.LOCAL
kadmin/changepw@MYLAB.LOCAL
krbtgt/MYLAB.LOCAL@MYLAB.LOCAL
testuser@MYLAB.LOCAL
```

su

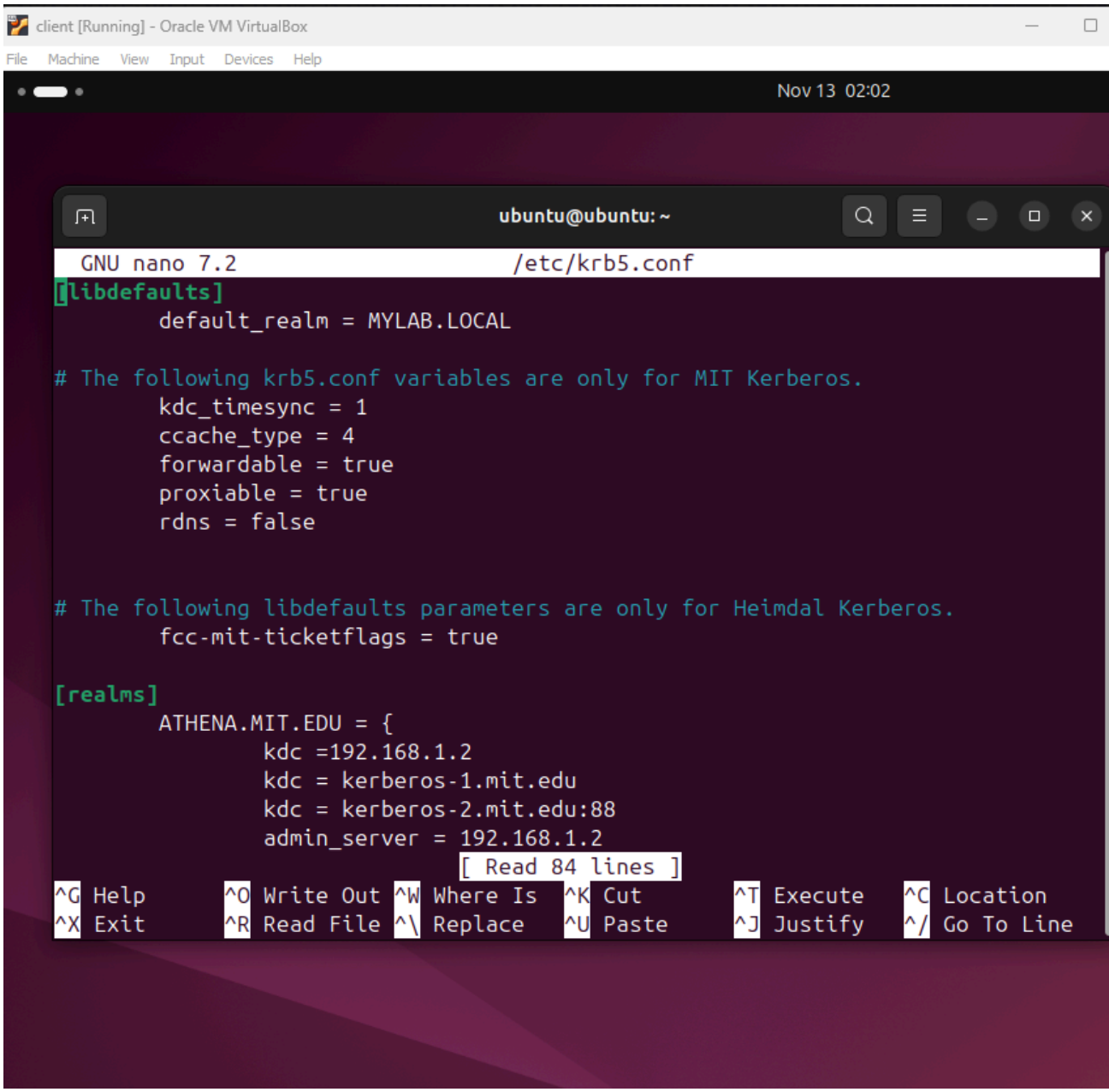
Step 4: Configure the Kerberos Client (VM2)

1. **Edit the Kerberos Configuration File on VM2:**
    - Open /etc/krb5.conf for editing on VM2:

bash

sudo nano /etc/krb5.conf

- Set the default realm to MYLAB.LOCAL and point to the KDC and admin server on VM1. The configuration should match what you set on VM1.



Step 5: Test Kerberos Authentication

1. **Request a Kerberos Ticket for the User on VM2:**
   - In the terminal on VM2, request a ticket for testuser:

bash

kinit testuser@MYLAB.LOCAL

   - Enter the password you set for testuser.

```
ubuntu@ubuntu:~$ bash
ubuntu@ubuntu:~$ sudo nano /etc/krb5.conf
ubuntu@ubuntu:~$ bash
ubuntu@ubuntu:~$ kinit testuser@MYLAB.LOCAL
kinit: Cannot find KDC for realm "MYLAB.LOCAL" while getting initial credentials
```

2. **Verify the Ticket:**
    - Check if the ticket was issued by listing active Kerberos tickets:

ticket is not verified for that reason cannot find KDC for realm “MYLAB.LOCAL”

bash

list

- You should see details about the ticket, such as the principal and expiration time, confirming successful Kerberos authentication.

```
ubuntu@ubuntu:~$ bash
ubuntu@ubuntu:~$ list
Command 'list' not found, but there are 22 similar ones.
```