



UNIVERSITY OF
Baguio

SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Arjay V De Leon	DATE PERFORMED: 11/13/24	/50
Section: IDC - 1	DATE SUBMITTED: 11/13/24	

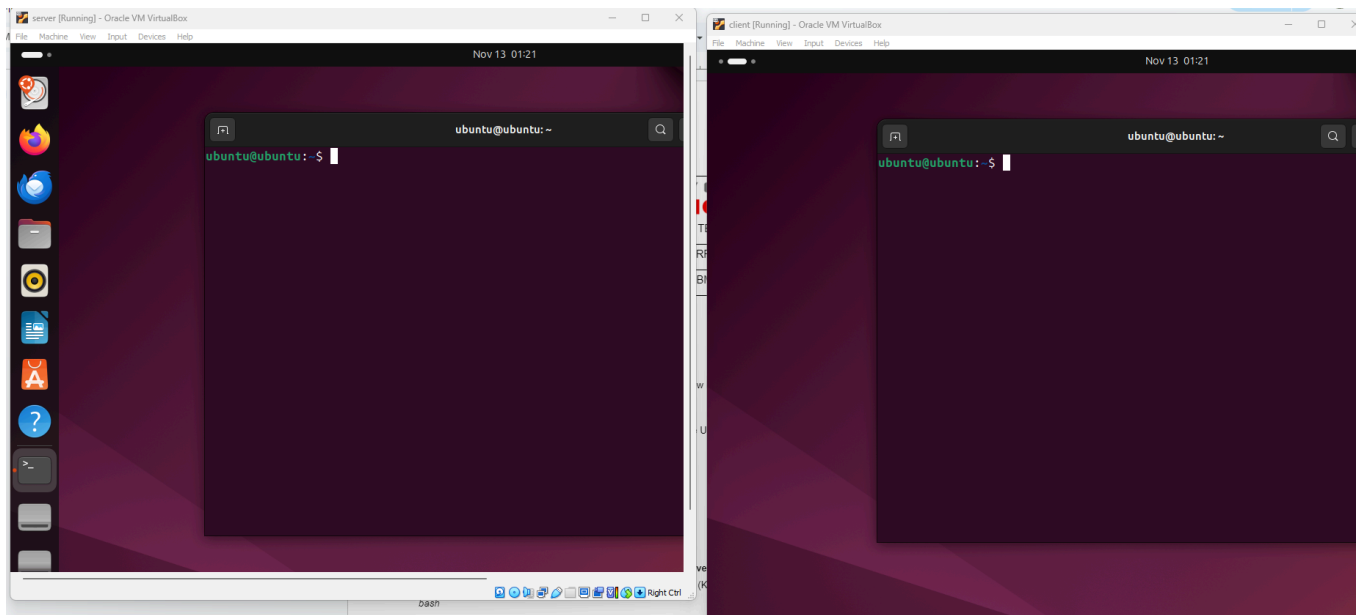
SYSADM1 – Kerberos Lab Activity: A step-by-step Guide

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



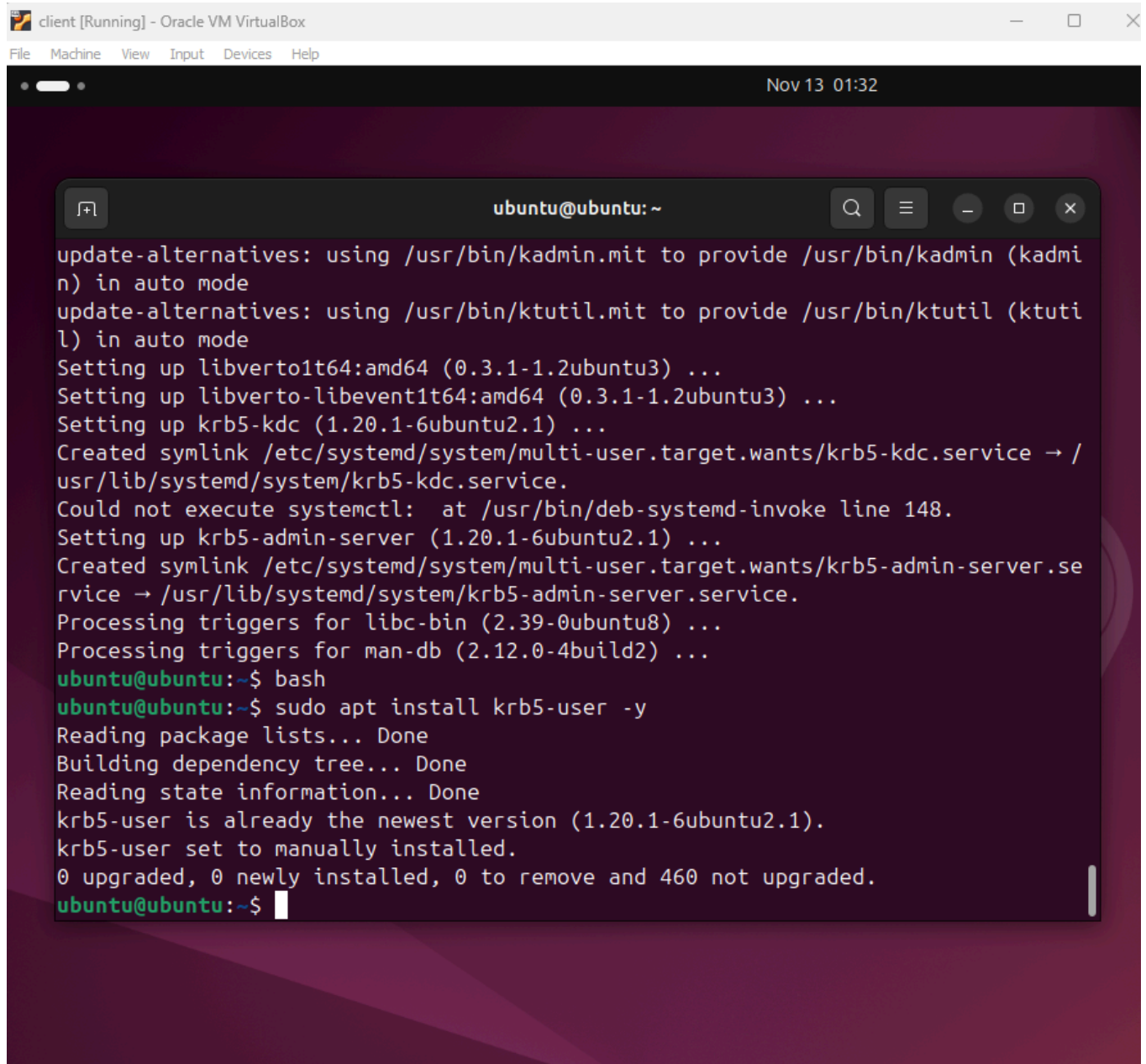
Step 1: Initial Setup and Package Installation

1. Update Packages on Both VMs:

- Open a terminal on each VM and run:

bash

sudo apt update && sudo apt upgrade -y



```
client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Nov 13 01:32

ubuntu@ubuntu: ~
update-alternatives: using /usr/bin/kadmin.mit to provide /usr/bin/kadmin (kadmin) in auto mode
update-alternatives: using /usr/bin/ktutil.mit to provide /usr/bin/ktutil (ktutil) in auto mode
Setting up libverto1t64:amd64 (0.3.1-1.2ubuntu3) ...
Setting up libverto-libevent1t64:amd64 (0.3.1-1.2ubuntu3) ...
Setting up krb5-kdc (1.20.1-6ubuntu2.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/krb5-kdc.service → /usr/lib/systemd/system/krb5-kdc.service.
Could not execute systemctl: at /usr/bin/deb-systemd-invoke line 148.
Setting up krb5-admin-server (1.20.1-6ubuntu2.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/krb5-admin-server.service → /usr/lib/systemd/system/krb5-admin-server.service.
Processing triggers for libc-bin (2.39-0ubuntu8) ...
Processing triggers for man-db (2.12.0-4build2) ...
ubuntu@ubuntu:~$ bash
ubuntu@ubuntu:~$ sudo apt install krb5-user -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
krb5-user is already the newest version (1.20.1-6ubuntu2.1).
krb5-user set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 460 not upgraded.
ubuntu@ubuntu:~$
```

- 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]

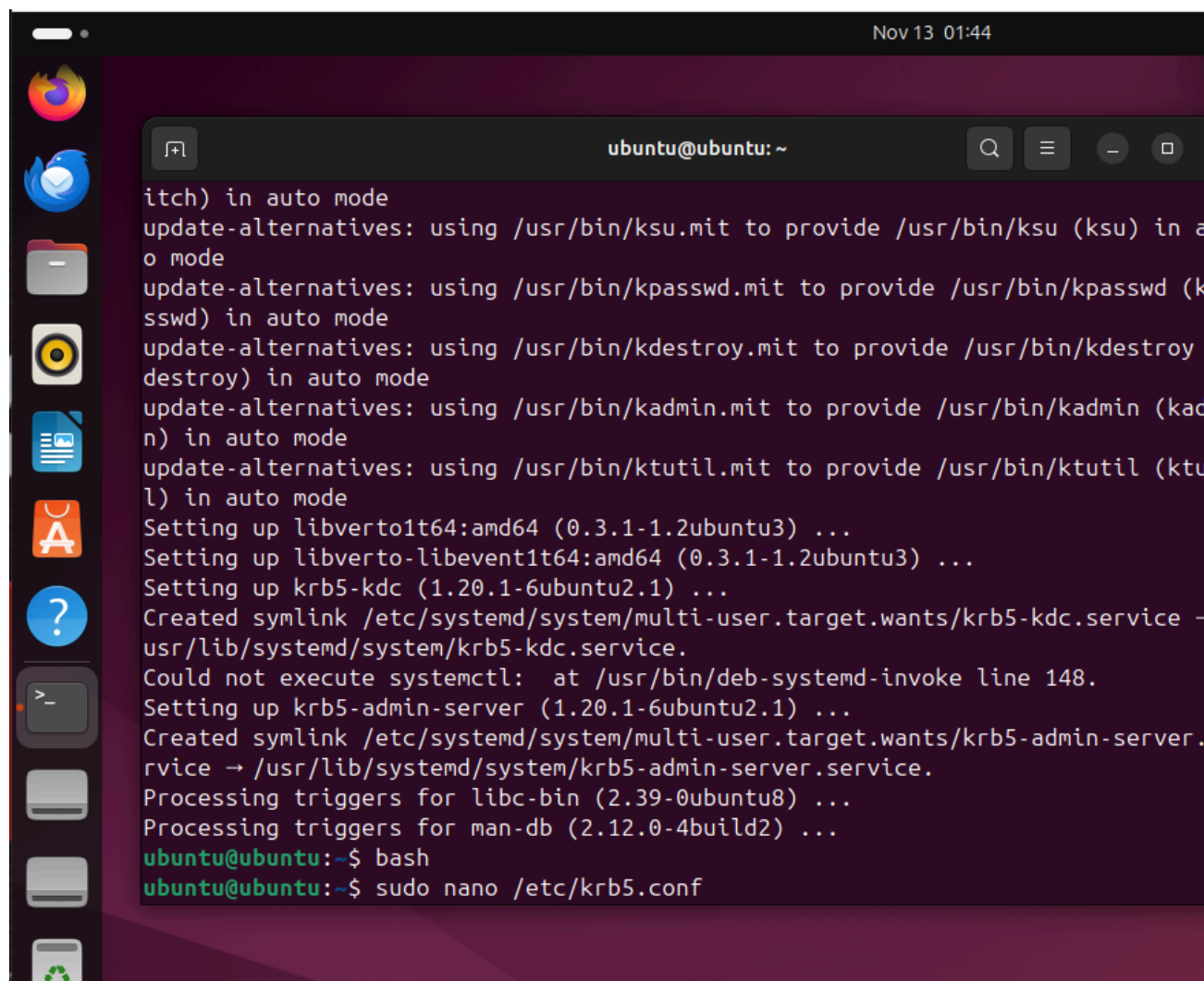
MYLAB.LOCAL = {

kdc = <VM1_IP_or_hostname>

admin_server = <VM1_IP_or_hostname>

}

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



```
Nov 13 01:44
ubuntu@ubuntu: ~
itch) in auto mode
update-alternatives: using /usr/bin/ksu.mit to provide /usr/bin/ksu (ksu) in a
o mode
update-alternatives: using /usr/bin/kpasswd.mit to provide /usr/bin/kpasswd (k
sswd) in auto mode
update-alternatives: using /usr/bin/kdestroy.mit to provide /usr/bin/kdestroy
destroy) in auto mode
update-alternatives: using /usr/bin/kadmin.mit to provide /usr/bin/kadmin (kac
n) in auto mode
update-alternatives: using /usr/bin/ktutil.mit to provide /usr/bin/ktutil (ktu
l) in auto mode
Setting up libverto1t64:amd64 (0.3.1-1.2ubuntu3) ...
Setting up libverto-libevent1t64:amd64 (0.3.1-1.2ubuntu3) ...
Setting up krb5-kdc (1.20.1-6ubuntu2.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/krb5-kdc.service -
usr/lib/systemd/system/krb5-kdc.service.
Could not execute systemctl: at /usr/bin/deb-systemd-invoke line 148.
Setting up krb5-admin-server (1.20.1-6ubuntu2.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/krb5-admin-server
rvice -> /usr/lib/systemd/system/krb5-admin-server.service.
Processing triggers for libc-bin (2.39-0ubuntu8) ...
Processing triggers for man-db (2.12.0-4build2) ...
ubuntu@ubuntu:~$ bash
ubuntu@ubuntu:~$ sudo nano /etc/krb5.conf
```

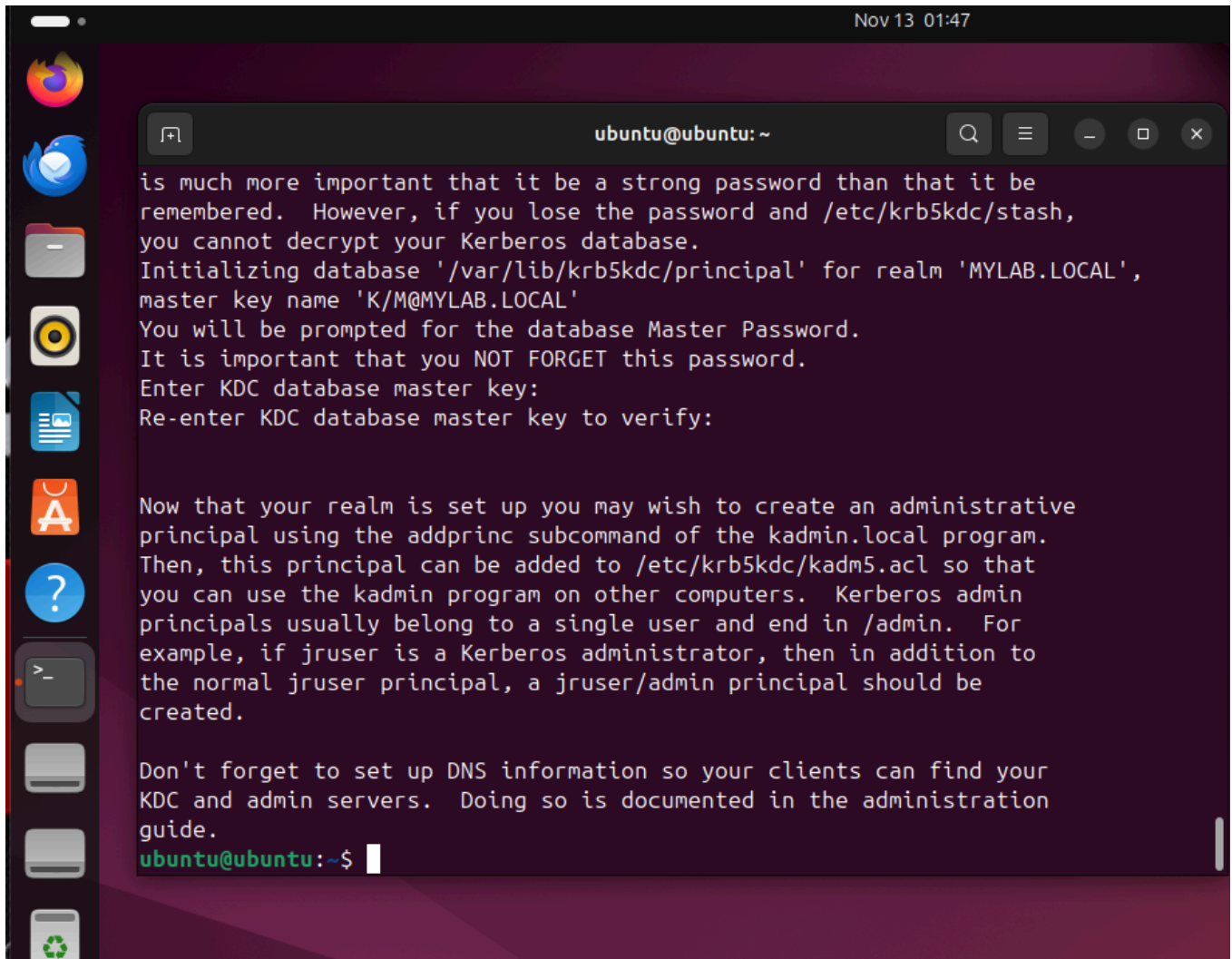
2. Initialize the Kerberos Database:

- Create the database for the Kerberos realm:

bash

sudo krb5_newrealm

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



The screenshot shows a terminal window titled 'ubuntu@ubuntu: ~' with a search icon and window controls. The text in the terminal is as follows:

```
is much more important that it be a strong password than that it be
remembered. However, if you lose the password and /etc/krb5kdc/stash,
you cannot decrypt your Kerberos database.
Initializing database '/var/lib/krb5kdc/principal' for realm 'MYLAB.LOCAL',
master key name 'K/M@MYLAB.LOCAL'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:

Now that your realm is set up you may wish to create an administrative
principal using the addprinc subcommand of the kadmin.local program.
Then, this principal can be added to /etc/krb5kdc/kadm5.acl so that
you can use the kadmin program on other computers. Kerberos admin
principals usually belong to a single user and end in /admin. For
example, if jruser is a Kerberos administrator, then in addition to
the normal jruser principal, a jruser/admin principal should be
created.

Don't forget to set up DNS information so your clients can find your
KDC and admin servers. Doing so is documented in the administration
guide.
ubuntu@ubuntu:~$
```

3. Start and Enable the Kerberos Services:

- Start the KDC and admin server, and ensure they start automatically on boot:

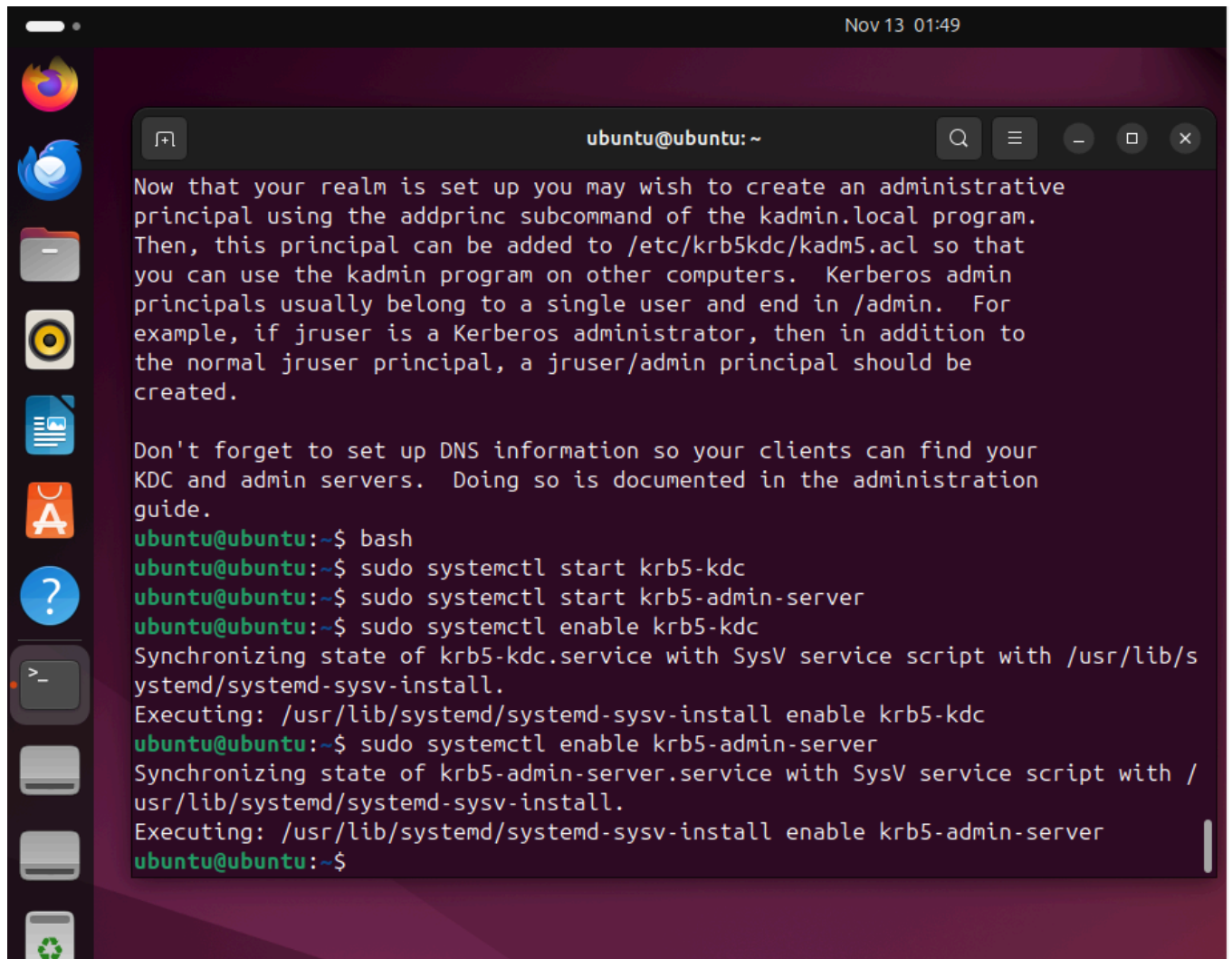
bash

sudo systemctl start krb5-kdc

sudo systemctl start krb5-admin-server

sudo systemctl enable krb5-kdc

sudo systemctl enable krb5-admin-server

A terminal window titled 'ubuntu@ubuntu: ~' with a search bar and window controls. The text inside the terminal provides instructions on creating an administrative principal and setting up DNS information. It then shows a series of commands being executed to start and enable the Kerberos services.

```
Now that your realm is set up you may wish to create an administrative
principal using the addprinc subcommand of the kadmin.local program.
Then, this principal can be added to /etc/krb5kdc/kadm5.acl so that
you can use the kadmin program on other computers.  Kerberos admin
principals usually belong to a single user and end in /admin.  For
example, if jruiser is a Kerberos administrator, then in addition to
the normal jruiser principal, a jruiser/admin principal should be
created.

Don't forget to set up DNS information so your clients can find your
KDC and admin servers.  Doing so is documented in the administration
guide.

ubuntu@ubuntu:~$ bash
ubuntu@ubuntu:~$ sudo systemctl start krb5-kdc
ubuntu@ubuntu:~$ sudo systemctl start krb5-admin-server
ubuntu@ubuntu:~$ sudo systemctl enable krb5-kdc
Synchronizing state of krb5-kdc.service with SysV service script with /usr/lib/s
ystemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable krb5-kdc
ubuntu@ubuntu:~$ sudo systemctl enable krb5-admin-server
Synchronizing state of krb5-admin-server.service with SysV service script with /
usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable krb5-admin-server
ubuntu@ubuntu:~$
```

arjay

Step 3: Set Up a Kerberos User Principal

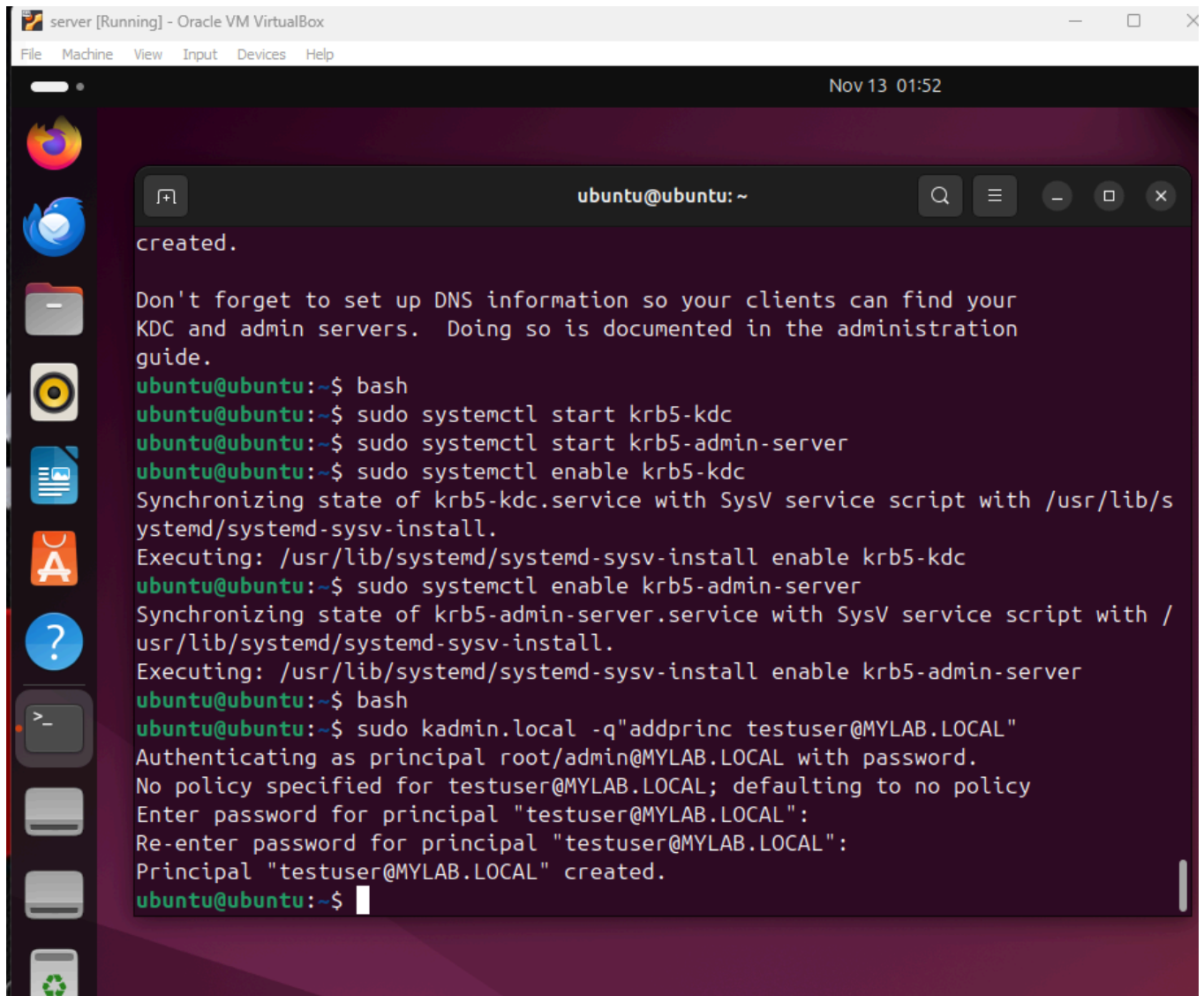
1. Create a New User Principal:

- 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.



The screenshot shows a terminal window titled 'ubuntu@ubuntu: ~' with a search bar and window controls. The terminal output is as follows:

```
created.  
  
Don't forget to set up DNS information so your clients can find your  
KDC and admin servers. Doing so is documented in the administration  
guide.  
ubuntu@ubuntu:~$ bash  
ubuntu@ubuntu:~$ sudo systemctl start krb5-kdc  
ubuntu@ubuntu:~$ sudo systemctl start krb5-admin-server  
ubuntu@ubuntu:~$ sudo systemctl enable krb5-kdc  
Synchronizing state of krb5-kdc.service with SysV service script with /usr/lib/s  
ystemd/systemd-sysv-install.  
Executing: /usr/lib/systemd/systemd-sysv-install enable krb5-kdc  
ubuntu@ubuntu:~$ sudo systemctl enable krb5-admin-server  
Synchronizing state of krb5-admin-server.service with SysV service script with /  
usr/lib/systemd/systemd-sysv-install.  
Executing: /usr/lib/systemd/systemd-sysv-install enable krb5-admin-server  
ubuntu@ubuntu:~$ bash  
ubuntu@ubuntu:~$ sudo kadmin.local -q "addprinc testuser@MYLAB.LOCAL"  
Authenticating as principal root/admin@MYLAB.LOCAL with password.  
No policy specified for testuser@MYLAB.LOCAL; defaulting to no policy  
Enter password for principal "testuser@MYLAB.LOCAL":  
Re-enter password for principal "testuser@MYLAB.LOCAL":  
Principal "testuser@MYLAB.LOCAL" created.  
ubuntu@ubuntu:~$
```

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.

client [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Nov 13 02:02

ubuntu@ubuntu: ~

```
GNU nano 7.2 /etc/krb5.conf
[libdefaults]
    default_realm = MYLAB.LOCAL

# The following krb5.conf variables are only for MIT Kerberos.
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true
    rdns = false

# The following libdefaults parameters are only for Heimdal Kerberos.
    fcc-mit-ticketflags = true

[realms]
    ATHENA.MIT.EDU = {
        kdc = 192.168.1.2
        kdc = kerberos-1.mit.edu
        kdc = kerberos-2.mit.edu:88
        admin_server = 192.168.1.2
    }
[ Read 84 lines ]
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line

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.
```