



HACETTEPE
University

Computer Science and Engineering Department

Group Name&Surname: Mehmet Taha USTA & Burcu ÖZTAŞ

Identity Numbers: 21527472 & 21483435

Course: BBM-465 Information Security Lab.

Experiment: Assignment 4

Subject: Kerberos Authentication System

Due Date: 24/12/2019 - 23:59

Advisor: Dr. Ahmet Selman BOZKIR

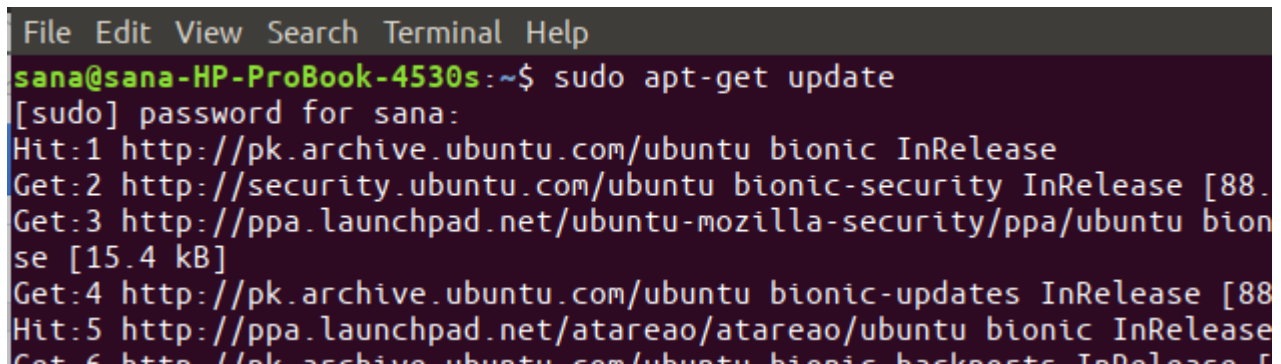
1. Syncing Times

Since time is an important parameter for this connection. Server and the users computers time's need to be synchronized for this ntp service is used.

1.1 Update Repository Index

In order to install the latest available version of software from the Internet repositories, your local repository index needs to be in line with them. Run the following command as sudo in order to update your local repository index:

```
$ sudo apt-get update
```

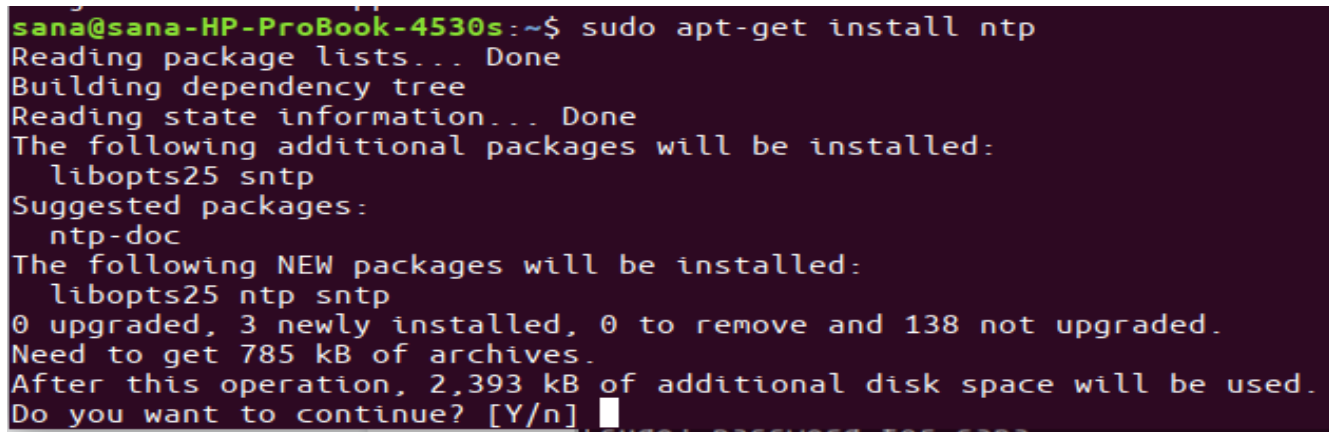


```
File Edit View Search Terminal Help
sana@sana-HP-ProBook-4530s:~$ sudo apt-get update
[sudo] password for sana:
Hit:1 http://pk.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.4 kB]
Get:3 http://ppa.launchpad.net/ubuntu-mozilla-security/ppa/ubuntu bionic InRelease [15.4 kB]
Get:4 http://pk.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.4 kB]
Hit:5 http://ppa.launchpad.net/atareaao/atareaao/ubuntu bionic InRelease [15.4 kB]
Get:6 http://pk.archive.ubuntu.com/ubuntu bionic-backports InRelease [15.4 kB]
```

1.2 Install NTP Server With Apt-get

Please run the following command as sudo in order to install NTP server daemon from the APT repositories:

```
$ sudo apt-get install ntp
```



```
File Edit View Search Terminal Help
sana@sana-HP-ProBook-4530s:~$ sudo apt-get install ntp
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libopts25 sntp
Suggested packages:
  ntp-doc
The following NEW packages will be installed:
  libopts25 ntp sntp
0 upgraded, 3 newly installed, 0 to remove and 138 not upgraded.
Need to get 785 kB of archives.
After this operation, 2,393 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

1.3 Verify Installation (optional)

You can verify your NTP installation and also check the version number by running the following command in your Terminal:

```
$ sntp --version
```

```
sana@sana-HP-ProBook-4530s:~$ sntp --version
sntp 4.2.8p10@1.3728-o (1)
sana@sana-HP-ProBook-4530s:~$
```

1.4 Restart the NTP server

In order for the above changes to take effect, you need to restart the NTP server. Run the following command as sudo in order to do so:

```
$ sudo service ntp restart
```

1.5 Verify That The NTP Server Is Running

```
$ sudo service ntp status
```

```
File Edit View Search Terminal Help
● ntp.service - Network Time Service
   Loaded: loaded (/lib/systemd/system/ntp.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2019-03-25 12:44:04 PKT; 1min 20s ago
     Docs: man:ntpd(8)
  Process: 25468 ExecStart=/usr/lib/ntp/ntp-systemd-wrapper (code=exited, status=0/SUCCESS)
 Main PID: 25476 (ntpd)
    Tasks: 2 (limit: 4583)
   CGroup: /system.slice/ntp.service
           └─25476 /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 124:129

Mar 25 12:44:08 sana-HP-ProBook-4530s ntpd[25476]: Soliciting pool server 45.43.30.59
Mar 25 12:44:08 sana-HP-ProBook-4530s ntpd[25476]: Soliciting pool server 69.164.198.192
Mar 25 12:44:08 sana-HP-ProBook-4530s ntpd[25476]: Soliciting pool server 45.79.1.70
Mar 25 12:44:09 sana-HP-ProBook-4530s ntpd[25476]: Soliciting pool server 204.11.201.10
Mar 25 12:44:09 sana-HP-ProBook-4530s ntpd[25476]: Soliciting pool server 69.10.161.7
Mar 25 12:44:09 sana-HP-ProBook-4530s ntpd[25476]: Soliciting pool server 45.76.244.202
Mar 25 12:44:09 sana-HP-ProBook-4530s ntpd[25476]: Soliciting pool server 91.189.94.4
Mar 25 12:44:10 sana-HP-ProBook-4530s ntpd[25476]: Soliciting pool server 91.189.91.157
Mar 25 12:44:10 sana-HP-ProBook-4530s ntpd[25476]: Soliciting pool server 69.164.202.202
Mar 25 12:44:10 sana-HP-ProBook-4530s ntpd[25476]: Soliciting pool server 108.61.73.244
```

2. OpenSSH Server

Server and client must be installed to provide SSH Connection.

2.1 Update Repository Index

In order to install the latest available version of software from the Internet repositories, your local repository index needs to be in line with them. Run the following command as sudo in order to update your local repository index:

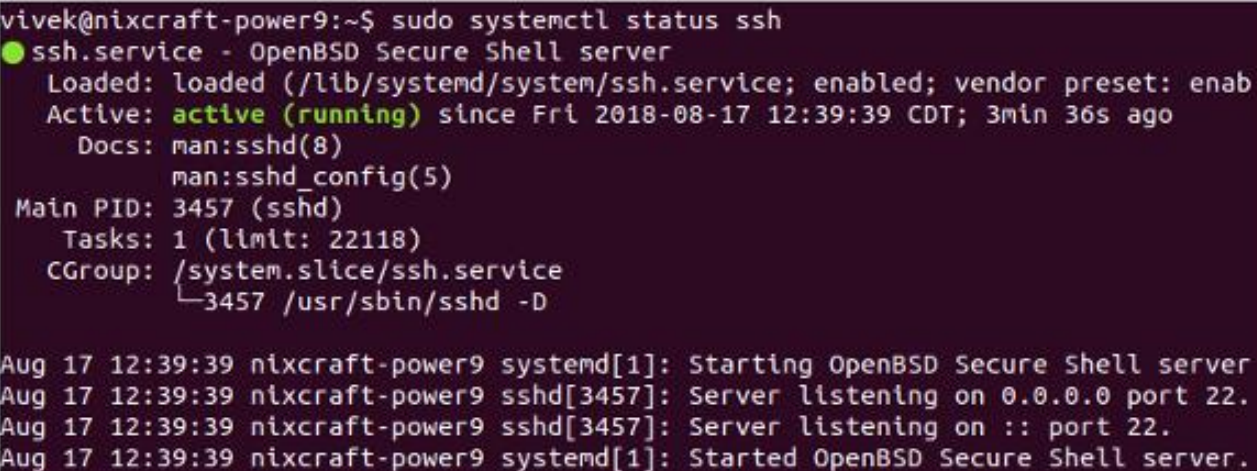
```
$ sudo apt-get update
```

2.2 Install OpenSSH-Server

```
$ sudo apt install openssh-server
```

2.3 Verify That SSH Service Running

```
$ sudo systemctl status ssh
```

A terminal window with a dark background showing the output of the command 'sudo systemctl status ssh'. The output indicates that the 'ssh.service' is 'active (running)'. It provides details such as the loaded path, vendor preset, active time, documentation, main PID, tasks, and CGroup. At the bottom, there are four log entries showing the service being started and listening on port 22.

```
vivek@nixcraft-power9:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Fri 2018-08-17 12:39:39 CDT; 3min 36s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 3457 (sshd)
      Tasks: 1 (limit: 22118)
   CGroup: /system.slice/ssh.service
           └─3457 /usr/sbin/sshd -D

Aug 17 12:39:39 nixcraft-power9 systemd[1]: Starting OpenBSD Secure Shell server
Aug 17 12:39:39 nixcraft-power9 sshd[3457]: Server listening on 0.0.0.0 port 22.
Aug 17 12:39:39 nixcraft-power9 sshd[3457]: Server listening on :: port 22.
Aug 17 12:39:39 nixcraft-power9 systemd[1]: Started OpenBSD Secure Shell server.
```

If not running enable the ssh server and start it as follows by typing the systemctl command:

```
$ sudo systemctl enable ssh
```

```
$ sudo systemctl start ssh
```

3. KERBEROS

3.1 Setup FQDN

Change the FQDN(fully qualified domain name) of the Kerberos server using the following command.

```
Hostname set-hostname krb5.group.io
```

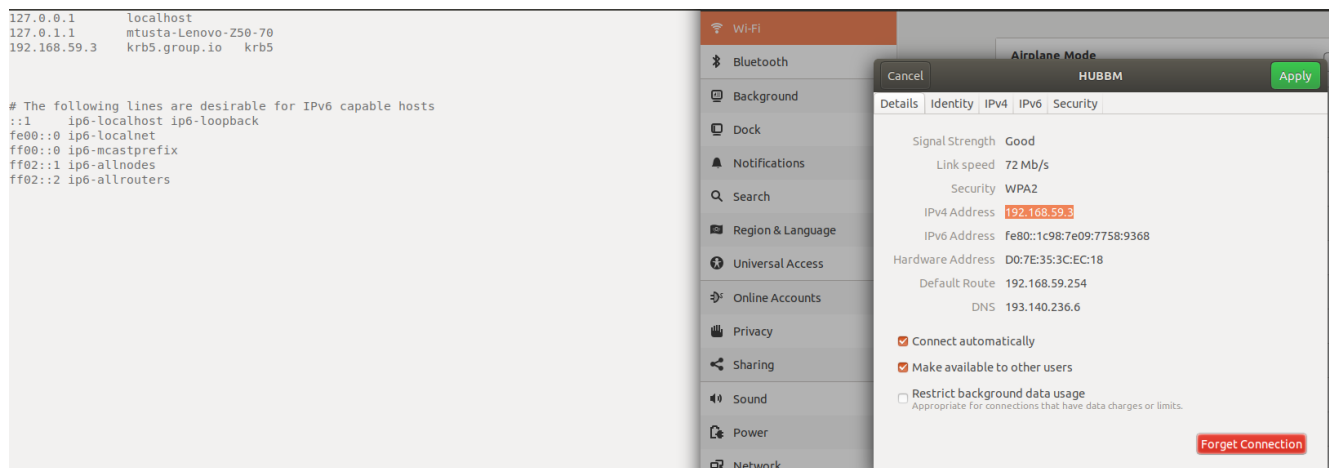
```
mtusta@krb5:~$ hostname
mehmettahausta
mtusta@krb5:~$ hostnamectl set-hostname krb5.group.io
mtusta@krb5:~$ hostname
```

After that, edit the '/etc/hosts' file.

```
sudo gedit /etc/hosts
```

```
mtusta@krb5:~$ sudo gedit /etc/hosts
```

Add the IP address and FQDN with your own and paste into it.



Save and close.

Now test using the 'ping' command below and make sure the FQDN is resolved to the right IP address.

```
Ping -c 3 $(hostname -f)
```

```
mtusta@krb5:~$ ping -c 3 $(hostname -f)
PING krb5.group.io (192.168.59.3) 56(84) bytes of data.
64 bytes from krb5.group.io (192.168.59.3): icmp_seq=1 ttl=64 time=0.026 ms
64 bytes from krb5.group.io (192.168.59.3): icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from krb5.group.io (192.168.59.3): icmp_seq=3 ttl=64 time=0.049 ms
```

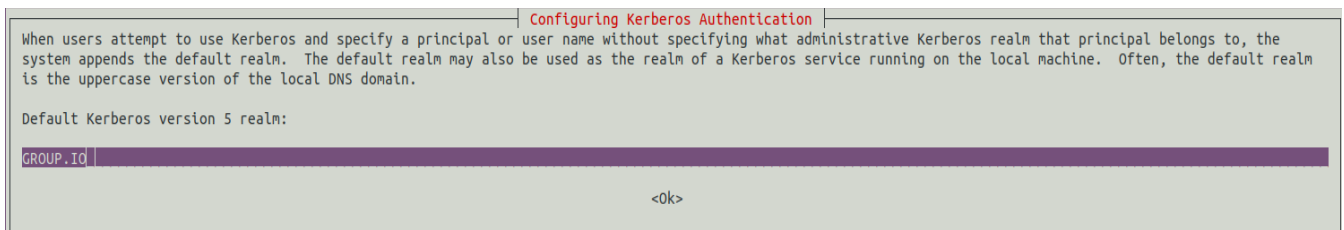
3.2 Install KDC Kerberos Server

Install Kerberos server using the following apt command.

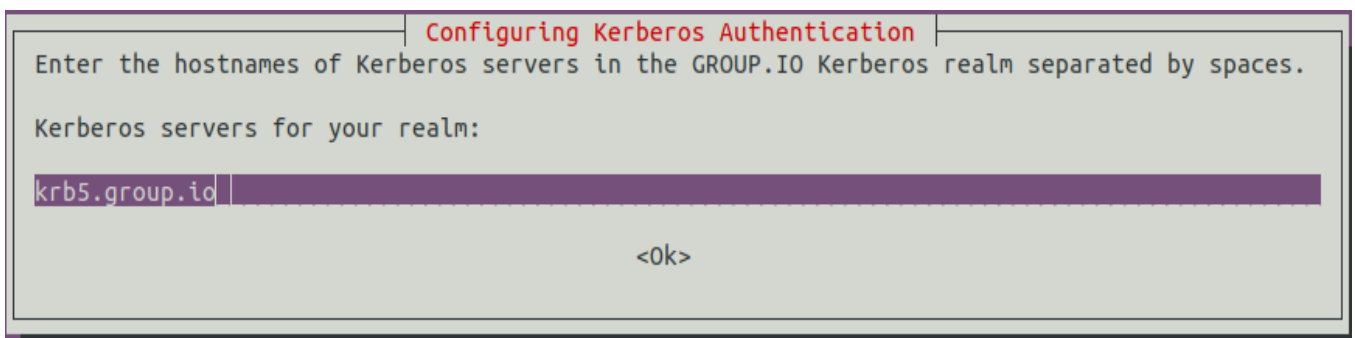
```
sudo apt install krb5-kdc krb5-admin-server krb5-config -y
```

During the installation, you will be asked about the Kerberos Realm, the Kerberos server of the Realm, and the Admin server.

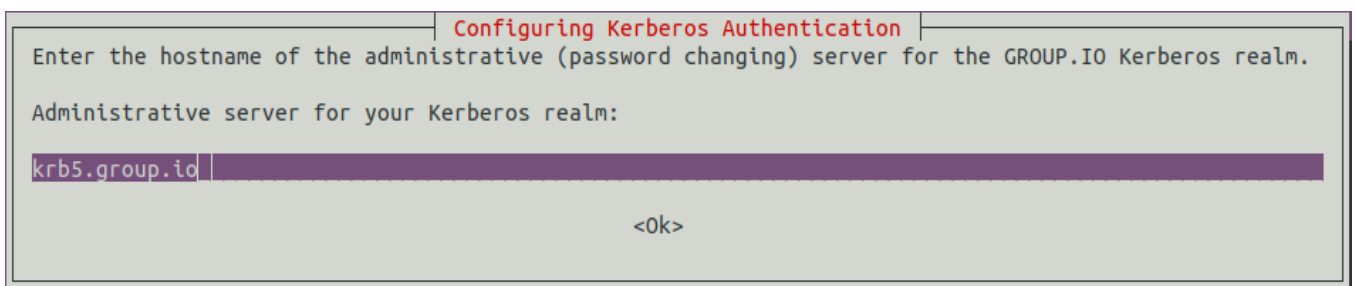
By default, the Kerberos will use the Kerberos server domain name as a REALM, '**GROUP.IO**'.



The Kerberos server is '**krb5.group.io**'.



And the Admin server same as the Kerberos server '**krb5.group.io**'.



3.3 Configure KDC Kerberos Server

Now generate a new strong master password for the Kerberos REALM using the following command.

```
Sudo krb5_newrealm
```


Type your strong password and the REALM password will be generated at the '/etc/krb5kdc/stash' file.

```
mtusta@krb5:~$ sudo krb5_newrealm
This script should be run on the master KDC/admin server to initialize
a Kerberos realm. It will ask you to type in a master key password.
This password will be used to generate a key that is stored in
/etc/krb5kdc/stash. You should try to remember this password, but it
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.
Loading random data
Initializing database '/var/lib/krb5kdc/principal' for realm 'GROUP.IO',
master key name 'K/M@GROUP.IO'
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:
```

After that, we need to create the admin user (admin principal) for the KDC Kerberos server, add the Kerberos server hostname to the database, and then create the keytab for the Kerberos server.

Run the 'kadmin.local' command-line interface for Kerberos administration command below.

```
sudo kadmin.local
```

Create a new admin user principal called 'root'.

```
addprinc root/admin
```

```
mtusta@krb5:~$ sudo kadmin.local
Authenticating as principal root/admin@GROUP.IO with password.
kadmin.local: addprinc root/admin
WARNING: no policy specified for root/admin@GROUP.IO; defaulting to no policy
Enter password for principal "root/admin@GROUP.IO":
Re-enter password for principal "root/admin@GROUP.IO":
Principal "root/admin@GROUP.IO" created.
```

Type the strong password for the 'root' admin principal.

Add the KDC Kerberos server to the database and create the keytab file for the KDC host.

```
addprinc -randkey host/krb5.group.io
```

```
ktadd host/krb5.group.io
```

Then close the 'kadmin.local' utility.

```
quit
```

```
kadmin.local: addprinc -randkey host/krb5.group.io
WARNING: no policy specified for host/krb5.group.io@GROUP.IO; defaulting to no policy
Principal "host/krb5.group.io@GROUP.IO" created.
kadmin.local: ktadd host/krb5.group.io
Entry for principal host/krb5.group.io with kvno 2, encryption type aes256-cts-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab.
Entry for principal host/krb5.group.io with kvno 2, encryption type aes128-cts-hmac-sha1-96 added to keytab FILE:/etc/krb5.keytab.
kadmin.local: quit
```

Next, we need to add the 'root' admin principle to the access control list by editing the '/etc/krb5kdc/kadm5.acl' file.

```
sudo gedit /etc/krb5kdc/kadm5.acl
```

```
mtusta@krb5:~$ sudo gedit /etc/krb5kdc/kadm5.acl
```

Change the following configuration.

```
# This file is the access control list for krb5 administration.
# When this file is edited run service krb5-admin-server restart to activate
# One common way to set up Kerberos administration is to allow any principal
# ending in /admin is given full administrative rights.
# To enable this, uncomment the following line:
*root/admin@GROUP.IO *
```

Save and close the configuration, then restart the Kerberos service.

```
sudo systemctl restart krb5-admin-server.service
```



```
mtusta@krb5:~$ sudo systemctl restart krb5-admin-server.service
mtusta@krb5:~$ systemctl status krb5-admin-server.service
● krb5-admin-server.service - Kerberos 5 Admin Server
   Loaded: loaded (/lib/systemd/system/krb5-admin-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2019-12-24 18:59:52 +03; 12s ago
     Main PID: 6577 (kadmind)
        Tasks: 1 (limit: 4915)
       CGroup: /system.slice/krb5-admin-server.service
               └─6577 /usr/sbin/kadmind -nofork

Ara 24 18:59:52 krb5.group.io kadmind[6577]: Setting up TCP socket for address 0.0.0.0.464
Ara 24 18:59:52 krb5.group.io kadmind[6577]: Setting up TCP socket for address ::.464
Ara 24 18:59:52 krb5.group.io kadmind[6577]: setsockopt(12,IPV6_V6ONLY,1) worked
Ara 24 18:59:52 krb5.group.io kadmind[6577]: Setting up RPC socket for address 0.0.0.0.749
Ara 24 18:59:52 krb5.group.io kadmind[6577]: Setting up RPC socket for address ::.749
Ara 24 18:59:52 krb5.group.io kadmind[6577]: setsockopt(14,IPV6_V6ONLY,1) worked
Ara 24 18:59:52 krb5.group.io kadmind[6577]: set up 6 sockets
Ara 24 18:59:52 krb5.group.io kadmind[6577]: Seeding random number generator
Ara 24 18:59:52 krb5.group.io kadmind[6577]: starting
Ara 24 18:59:52 krb5.group.io kadmind[6577]: kadmind: starting...
```

3.4 Install and Configure Kerberos Client

Configure the FQDN on the client machine using the following command.

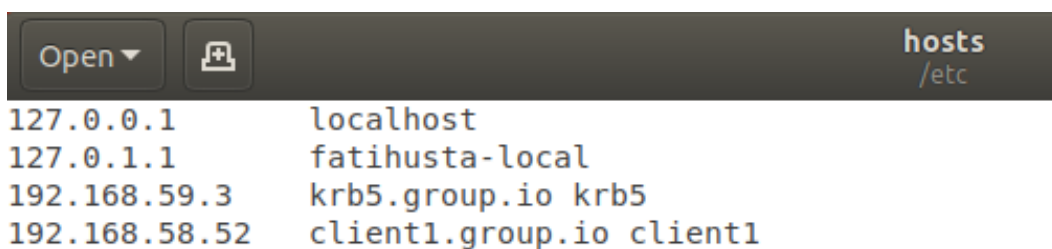
```
Hostname set-hostname client1.group.io
```

After that, edit the '/etc/hosts' file.

```
sudo gedit /etc/hosts
```

```
fatihusta@client1:~$ hostnamectl set-hostname client1.group.io
fatihusta@client1:~$ hostname
client1.group.io
fatihusta@client1:~$ sudo gedit /etc/hosts
```

Paste both KDC Kerberos server and the client as below.



```
127.0.0.1      localhost
127.0.1.1      fatihusta-local
192.168.59.3   krb5.group.io krb5
192.168.58.52  client1.group.io client1
```

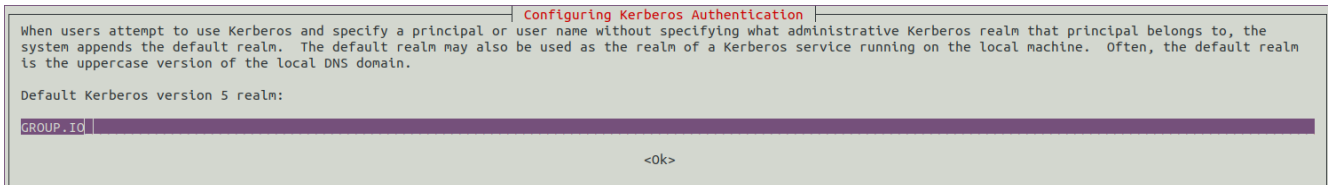
Save and close.

Install Kerberos client packages by running the following apt command.

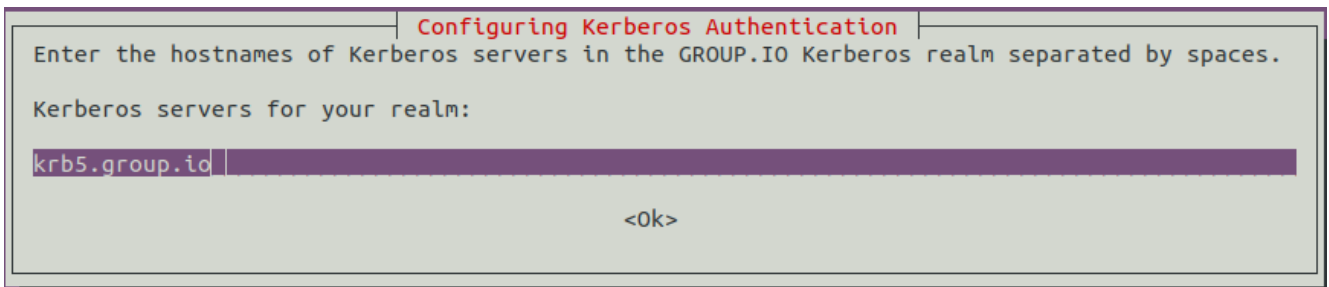
```
sudo apt install -y krb5-user libpam-krb5 libpam-ccreds auth-client-config
```

During the installation, you will be asked about the Kerberos Realm, the Kerberos server of the Realm, and the Admin server.

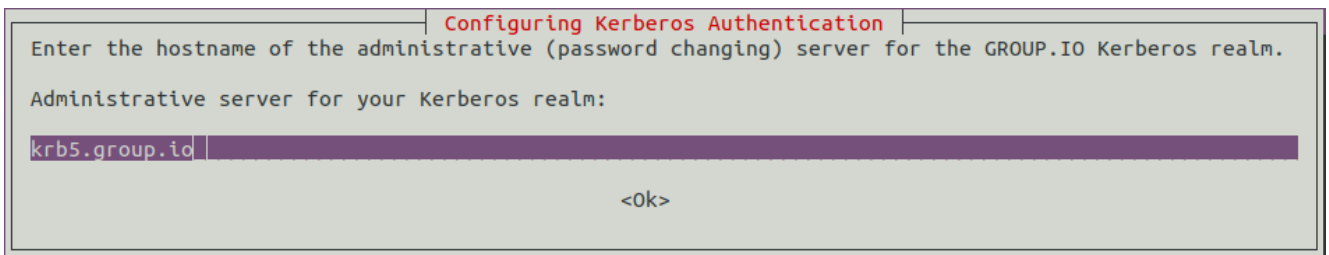
By default, Kerberos will use the Kerberos server domain name as a REALM, '**GROUP.IO**'.



The Kerberos server is '**krb5.group.io**'



And the Admin server same as the Kerberos server '**krb5.group.io**'.



And the installation for Kerberos client is finished.

- Configure Kerberos Client

From the client machine, connect to the KDC Kerberos server using the 'kadmin' command.

```
kadmin
```

And you will be asked for the password of 'root/admin' principle. Type the password and you will be logged in to the KDC Kerberos administration system.

Now add the client FQDN 'client1.group.io' to the Kerberos database and add the keytab file for the client.

```
addprinc -randkey host/client1.group.io
```

```
ktadd host/client1.group.io
```

Then close the kadmin Kerberos Administration interface.

```
quit
```

3.5 Testing

For this testing purpose, we're going to configure the SSH authentication using the Kerberos. The client machine 'client1.group.io' will connect to the server 'krb5.group.io' through SSH with the Kerberos authentication.

- Setup 'krb5.group.io' Server

Create a new system user called 'fatihusta'.

```
useradd -m -s /bin/bash fatihusta
```

```
root@krb5:~# useradd -m -s /bin/bash fatihusta
```

Login to the KDC Kerberos administration and add a new principal user called 'fatihusta'.

```
kadmin.local
```

```
addprinc fatihusta
```

```
root@krb5:~# kadmin.local
Authenticating as principal root/admin@GROUP.IO with password.
kadmin.local: addprinc fatihusta
WARNING: no policy specified for fatihusta@GROUP.IO; defaulting to no policy
Enter password for principal "fatihusta@GROUP.IO":
Re-enter password for principal "fatihusta@GROUP.IO":
add_principal: Principal or policy already exists while creating "fatihusta@GROUP.IO".
```

Close the Kerberos Administration interface and edit the ssh configuration '/etc/ssh/sshd_config'.

```
sudo gedit /etc/ssh/sshd_config
```

```
fatihusta@krb5:~$ sudo gedit /etc/ssh/sshd_config
```

Uncomment the 'GSSAPIAuthentication' and enable it by changing the value to ''.

```
GSSAPIAuthentication yes

GSSAPICleanupCredentials yes
```

```
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
```

Save and close the configuration, then restart the ssh service.

```
systemctl restart sshd
```

```
mtusta@krb5:~$ systemctl restart sshd
mtusta@krb5:~$ systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2019-12-24 19:19:50 +03; 9s ago
     Process: 7344 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 7345 (sshd)
       Tasks: 1 (limit: 4915)
      CGroup: /system.slice/ssh.service
              └─7345 /usr/sbin/sshd -D

Ara 24 19:19:50 krb5.group.io systemd[1]: Stopped OpenBSD Secure Shell server.
Ara 24 19:19:50 krb5.group.io systemd[1]: Starting OpenBSD Secure Shell server...
Ara 24 19:19:50 krb5.group.io sshd[7345]: Server listening on 0.0.0.0 port 22.
Ara 24 19:19:50 krb5.group.io sshd[7345]: Server listening on :: port 22.
Ara 24 19:19:50 krb5.group.io systemd[1]: Started OpenBSD Secure Shell server.
```

- Setup client1.group.io' Machine

Add new system user 'fatihusta' on the client machine and login into it.

```
useradd -m -s /bin/bash fatihusta

su - fatihusta
```

```
fatihusta@client1:~$ useradd -m -s /bin/bash fatihusta
```

```
fatihusta@client1:~$ su - fatihusta
Password:
```

After that, initialize the Kerberos user principal 'fatihusta'.

```
kinit fatihusta
```

Type the password of the user and after that check the available Ticket using the following command.

```
klist
```

```
fatihusta@client1:~$ kinit fatihusta
Password for fatihusta@GROUP.IO:
fatihusta@client1:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000_GtxWXf
Default principal: fatihusta@GROUP.IO

Valid starting      Expires            Service principal
24-12-2019 19:21:24  25-12-2019 05:21:24  krbtgt/GROUP.IO@GROUP.IO
renew until 25-12-2019 19:21:21
```

Now you can connect the 'krb5.group.io' server using the SSH Kerberos authentication.

```
ssh krb5.group.io
```

And you will be connected to the 'krb5.ahmad.io' server through SSH with Kerberos authentication.

```
fatihusta@client1:~$ ssh krb5.group.io
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 5.0.0-37-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.

Your Hardware Enablement Stack (HWE) is supported until April 2023.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```