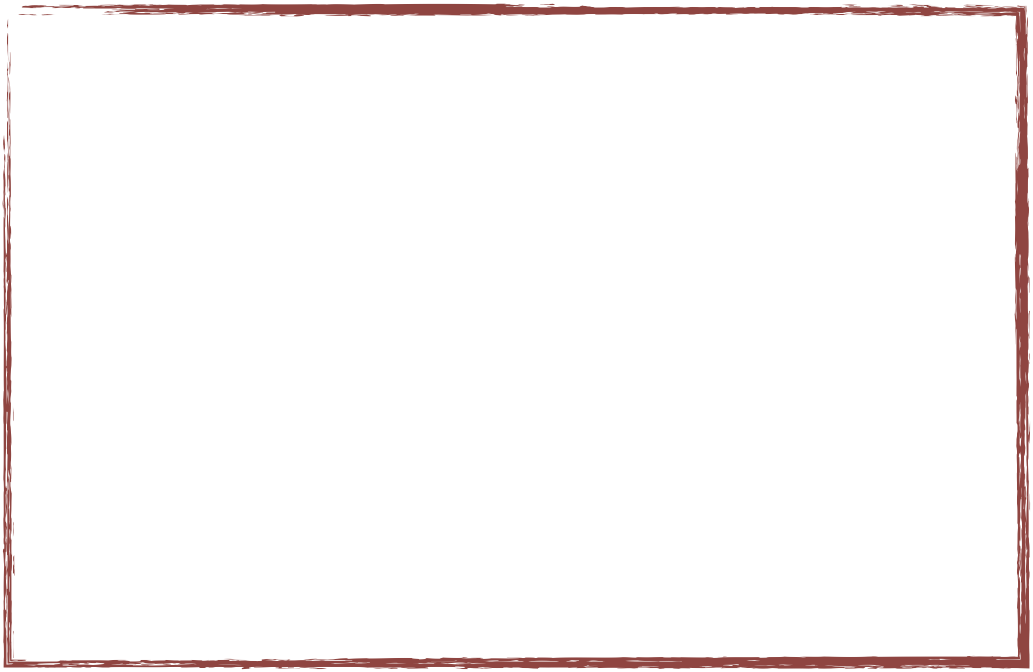


**Computer Science and Engineering Department**



**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

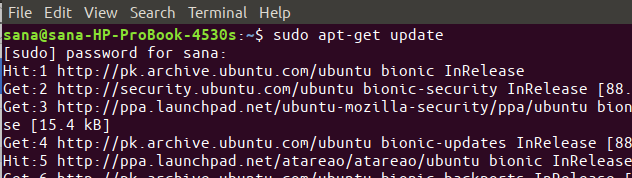
**1.** **Syncing Times**

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:

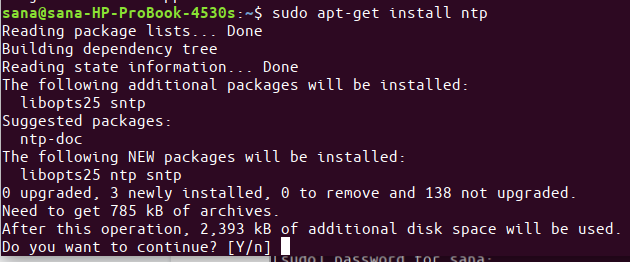
$ sudo apt-get update



**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:

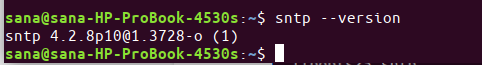
$ sudo apt-get install ntp



**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



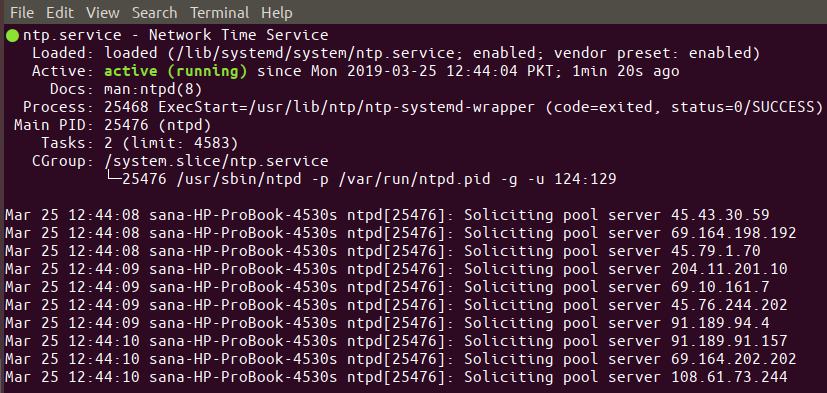
**1.4 Restart the NTP server**

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



**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:

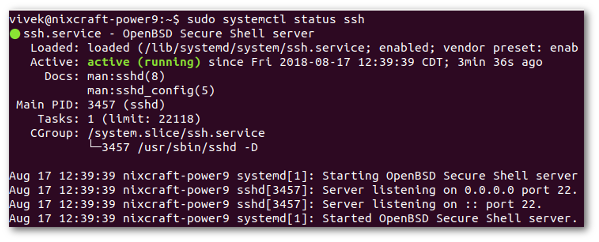
$ sudo apt-get update

**2.2 Install OpenSSh-Server**

$ sudo apt install openssh-server

**2.3 Verify That SSH Service Running**

$ sudo systemctl status ssh



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

$ sudo systemctl enable ssh

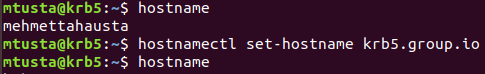
$ sudo systemctl start ssh

**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

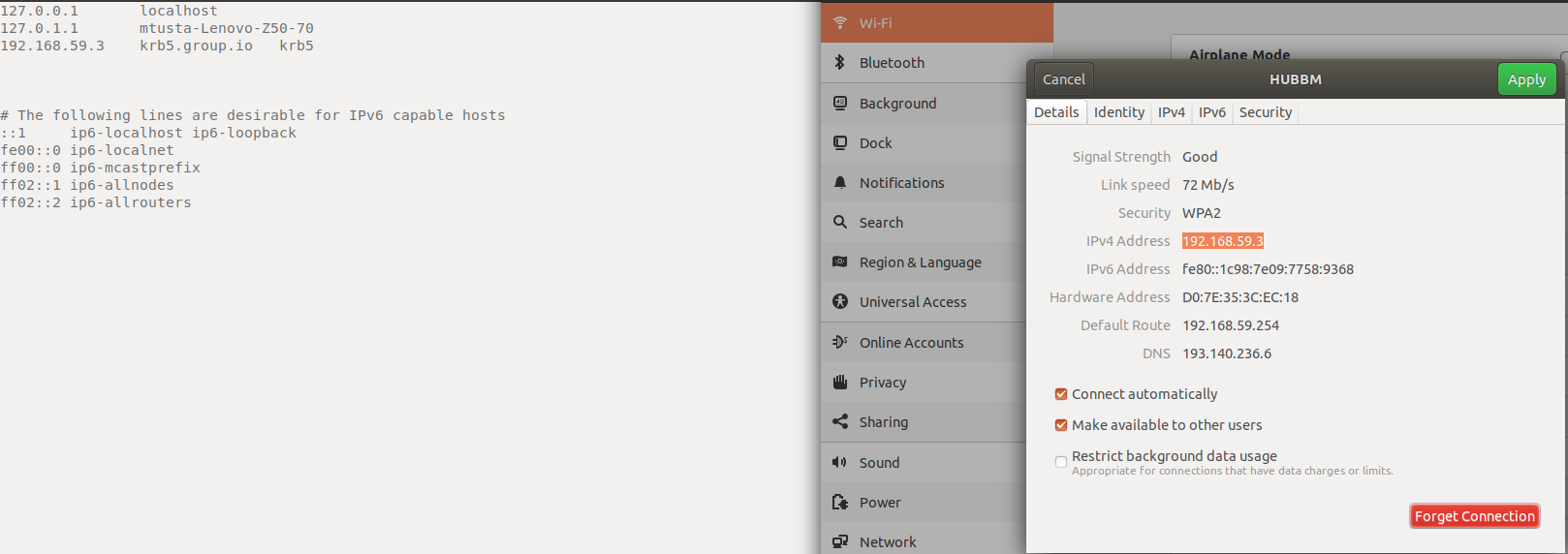


After that, edit the '/etc/hosts' file.

sudo gedit /etc/hosts



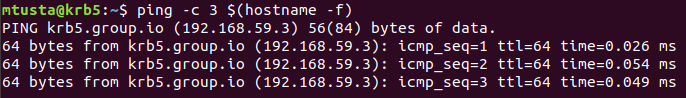
Add the IP address and FQDN with your own and paste into it.



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)



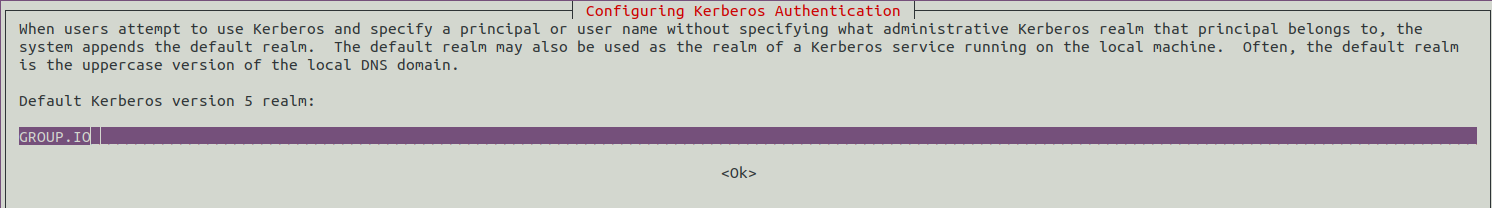
**3.2 Install KDC Kerberos Server**

Install Kerberos server using the following apt command.

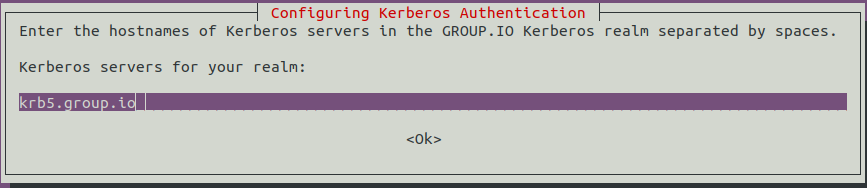
sudo apt install krb5-kdc krb5-admin-server krb5-config -y

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

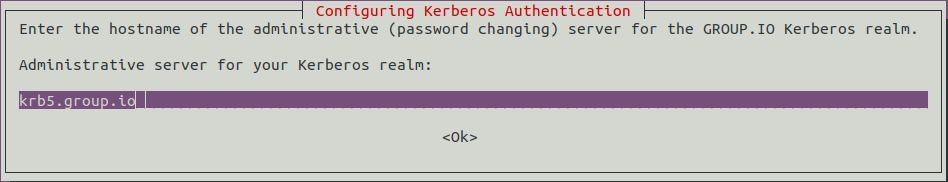
By default, the Kerberos will use the Kerberos server domain name as a REALM, **'GROUP.IO'**.



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



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

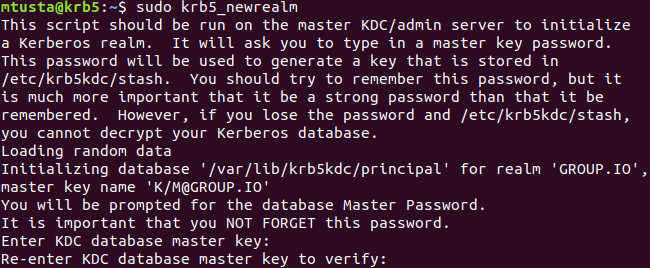


**3.3 Configure KDC Kerberos Server**

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.



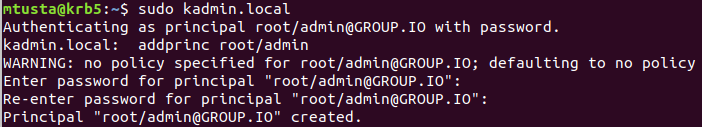
After that, we need to create the admin user (admin principal) for the KDC Kerberos server, add the Kerberos server hostname to the database, and then create the keytab for the Kerberos server.

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



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

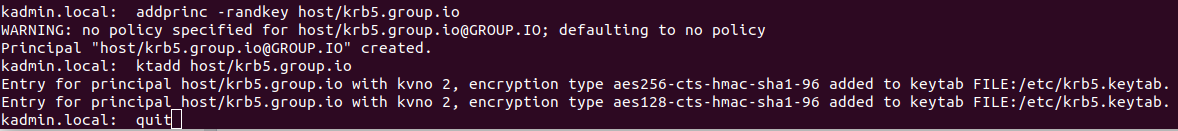
Add the KDC Kerberos server to the database and create the keytab file for the KDC host.

addprinc -randkey host/krb5.group.io

ktadd host/krb5.group.io

Then close the 'kadmin.local' utility.

quit

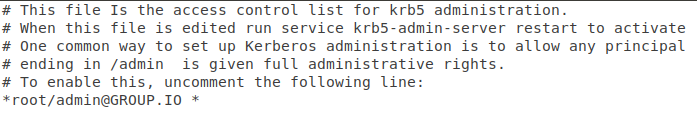


Next, we need to add the 'root' admin principle to the access control list by editing the '/etc/krb5kdc/kadm5.acl' file.

sudo gedit /etc/krb5kdc/kadm5.acl

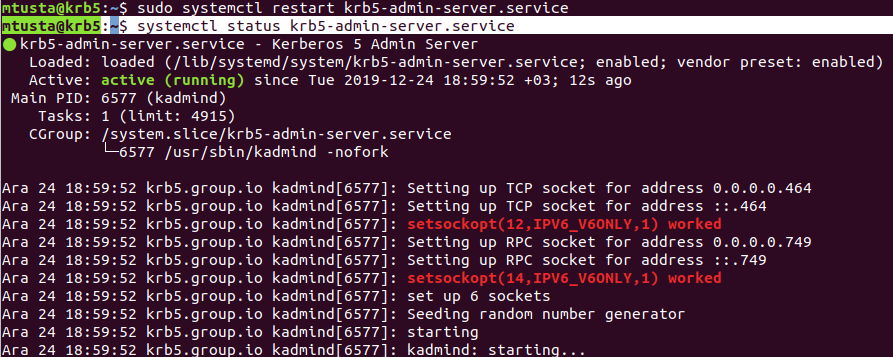


Change the following configuration.



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

sudo systemctl restart krb5-admin-server.service



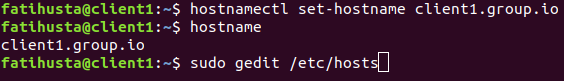
**3.4 Install and Configure Kerberos Client**

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

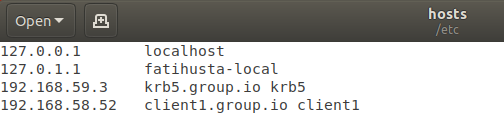
Hostname set-hostname client1.group.io

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

sudo gedit /etc/hosts



Paste both KDC Kerberos server and the client as below.



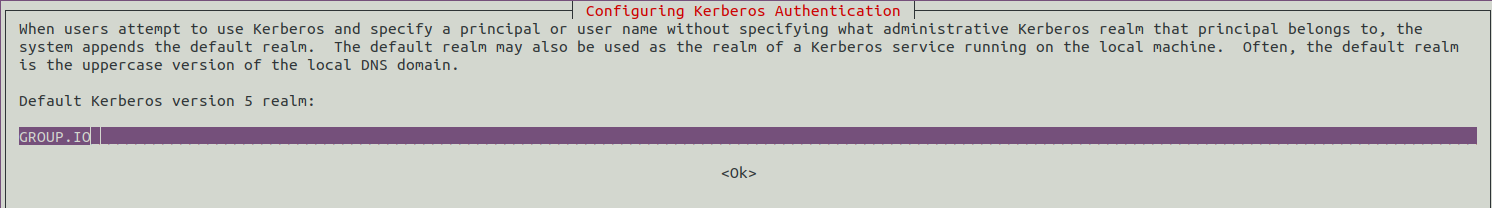
Save and close.

Install Kerberos client packages by running the following apt command.

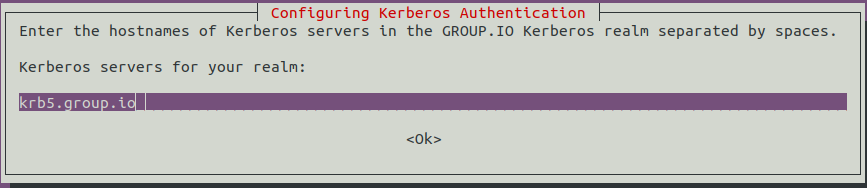
sudo apt install -y krb5-user libpam-krb5 libpam-ccreds auth-client-config

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

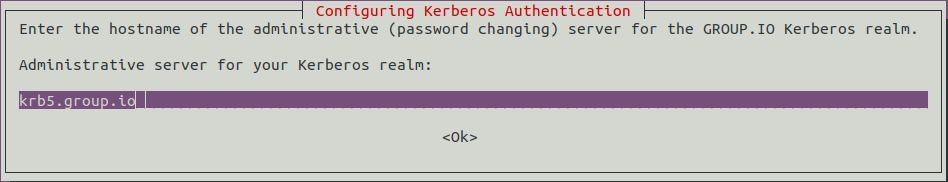
By default, Kerberos will use the Kerberos server domain name as a REALM, **'GROUP.IO'**.



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'.

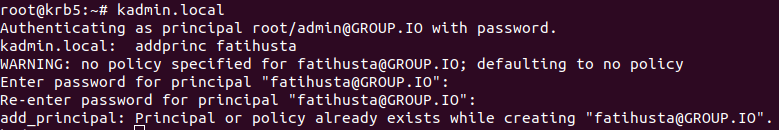
useradd -m -s /bin/bash fatihusta



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

kadmin.local

addprinc fatihusta



Close the Kerberos Administration interface and edit the ssh configuration '/etc/ssh/sshd\_config'.

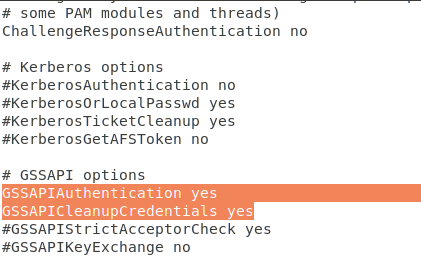
sudo gedit /etc/ssh/sshd\_config



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

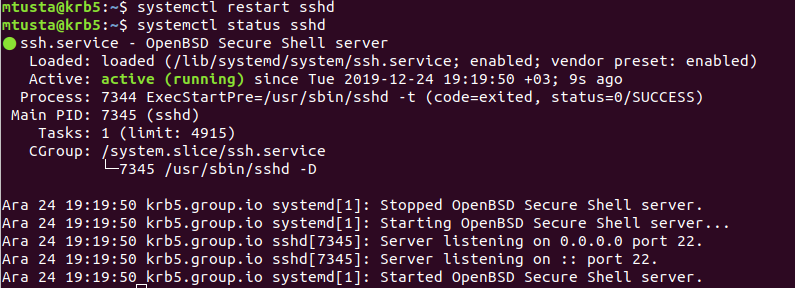
GSSAPIAuthentication yes

GSSAPICleanupCredentials yes



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

systemctl restart sshd



- 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



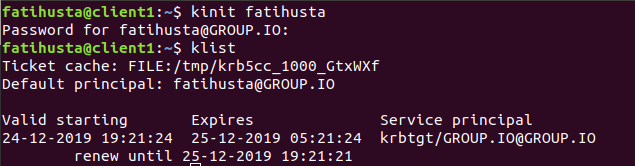


After that, initialize the Kerberos user principal 'fatihusta'.

kinit fatihusta

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

klist



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.group.io' server through SSH with Kerberos authentication.

