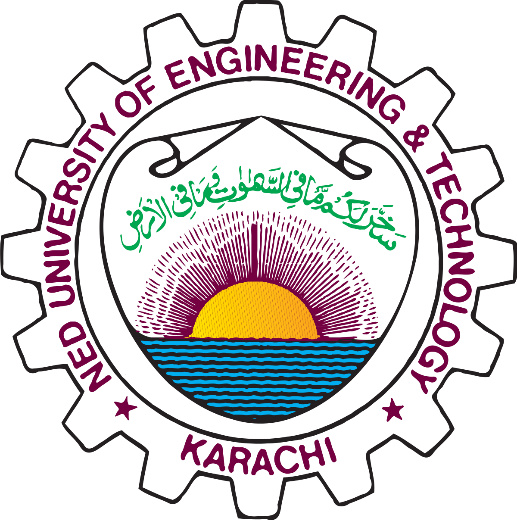
**CT-541 – NETWORK SECURITY**MS-IS 004 2019/20– Evening Fall 2019

**CT-541 NS Assignment-04**

**Kerberos KDC, Server, Client, SSH Connection**



**STUDENT NAME: MUHAMMAD UMAR TARIQ**

**ROLL NUMBER : IS 004 2019/20**

**COURSE INSTRUCTOR: Dr. Mubashir M Khan**

**DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY**

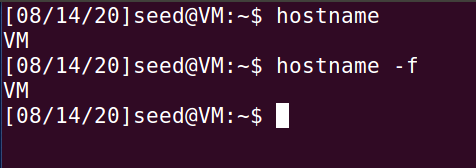
**NED UNIVERSITY, KARACHI CAMPUS**

Kerberos authentication has three components KDC, server and client that will connect using Kerberos authentication.

Each Server has to be assigned a fully qualified domain name.

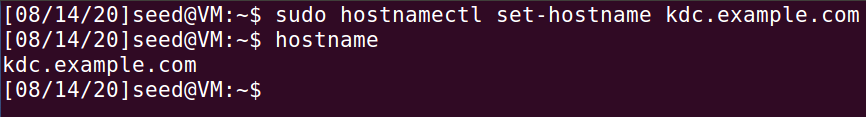
**VM1 is the server in our case, so we change VM1 hostname.**

**VM2 is going to be a Kerberos client that will authenticate from VM1.**

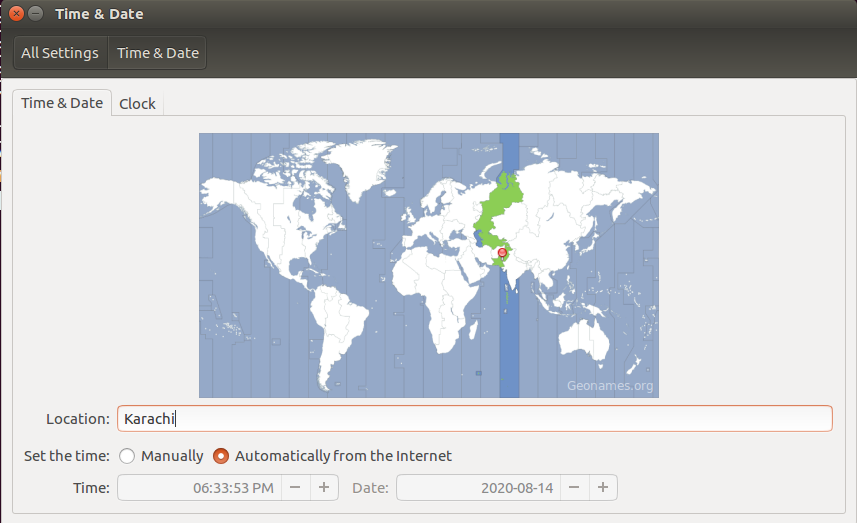


**To change the FQDN:**

**sudo hostnamectl set-hostname kdc.example.com**



**Since we are implementing the default MIT Kerberos system, the time synchronization must be less than equal to 5 minutes between every machine we want to authenticate.So set the time to local time**



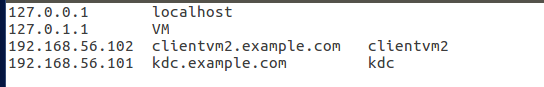
**We also have to add a manual entry for the dns lookups, if we do not have dns server available we can do**

**sudo gedit /etc/hosts**

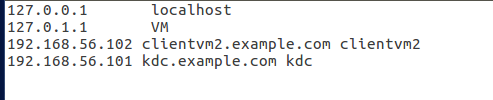
If the server does not already have a FQDN assigned to it and DNS services are not available, name resolution can be implemented by editing the local hosts file (typically this is located in /etc) on each server and client, adding the following line:

127.0.0.1 linuxwork.example.com localhost linuxwork

**Hosts File ON VM1 [KDC SERVER]:**



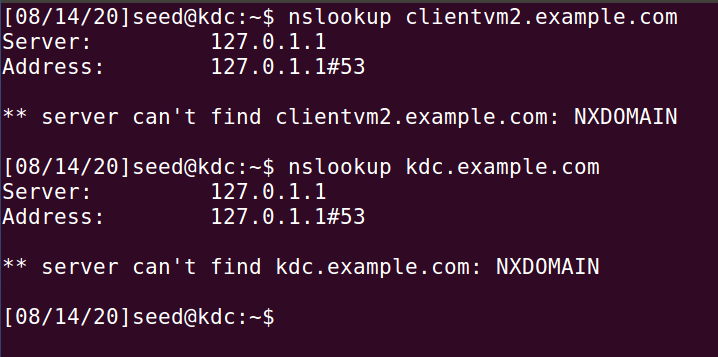
**Hosts File ON VM2 [CLIENT of Kerberos Authentication]:**



Open the file as sudo , and save, and then restart vm after the time settings change and hosts change.

Now we need to perform DNS Lookup to verify that our KDC server has a FQDN assigned to it.

**KDC SERVER And Kerberos Client NSLookup**

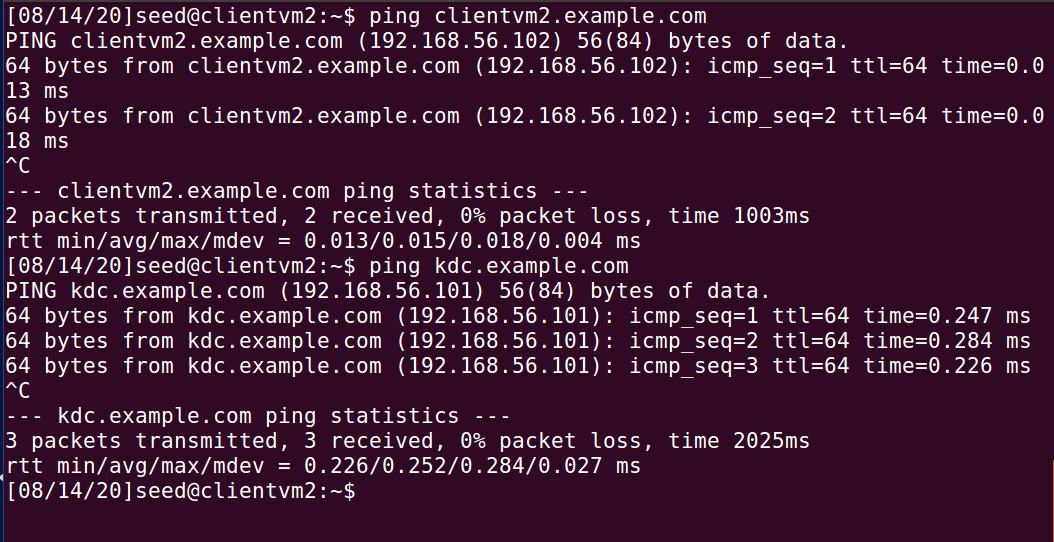


For reverse domain lookups we will set rdns variable to false on Kerberos client machines krb5.conf files.

To verify connectivity, ping each hosts FQDN.

Before pinging, add the Host-Only Mode Private ip addresses to the hosts file of the client.

Both of the client and the KDC server.



On KDC Server VM, run:

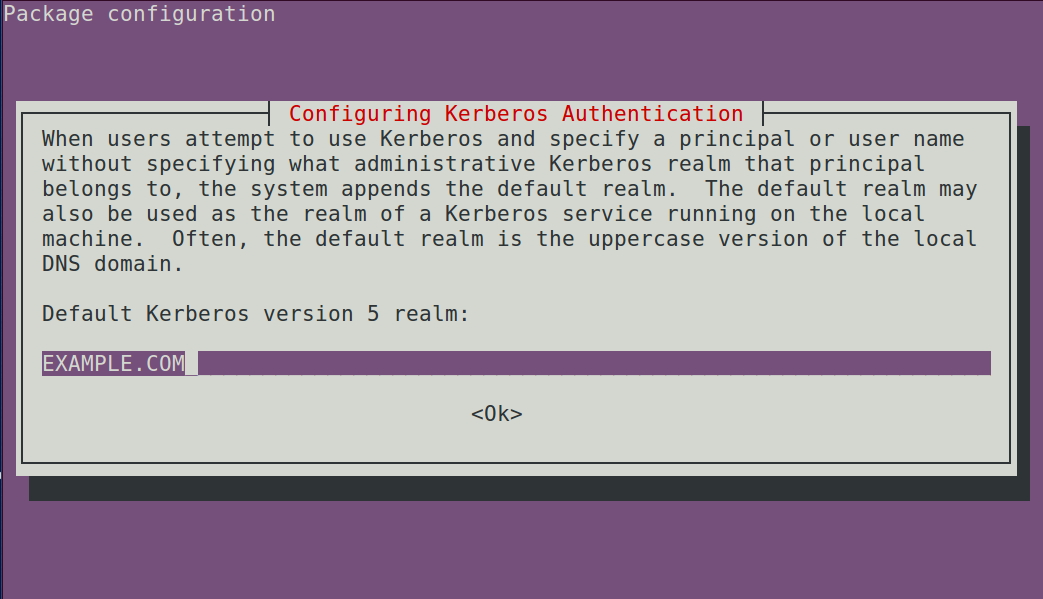
sudo apt-get update

sudo apt-get install aptitude

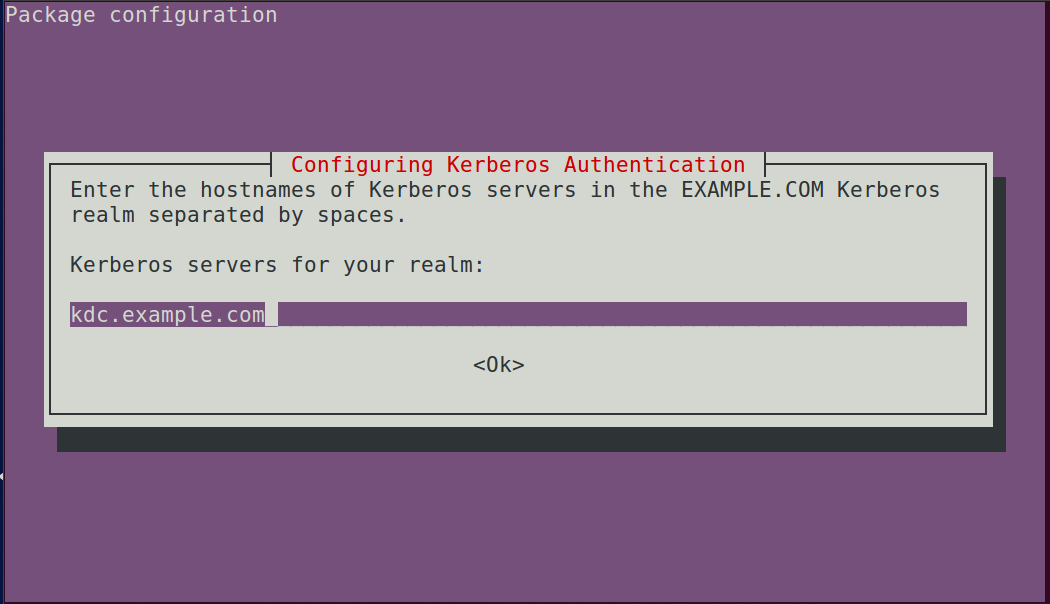
sudo aptitude install krb5-kdc krb5-admin-server

for dependencies issue, first select no and then select Y for downgrading the dependencies.

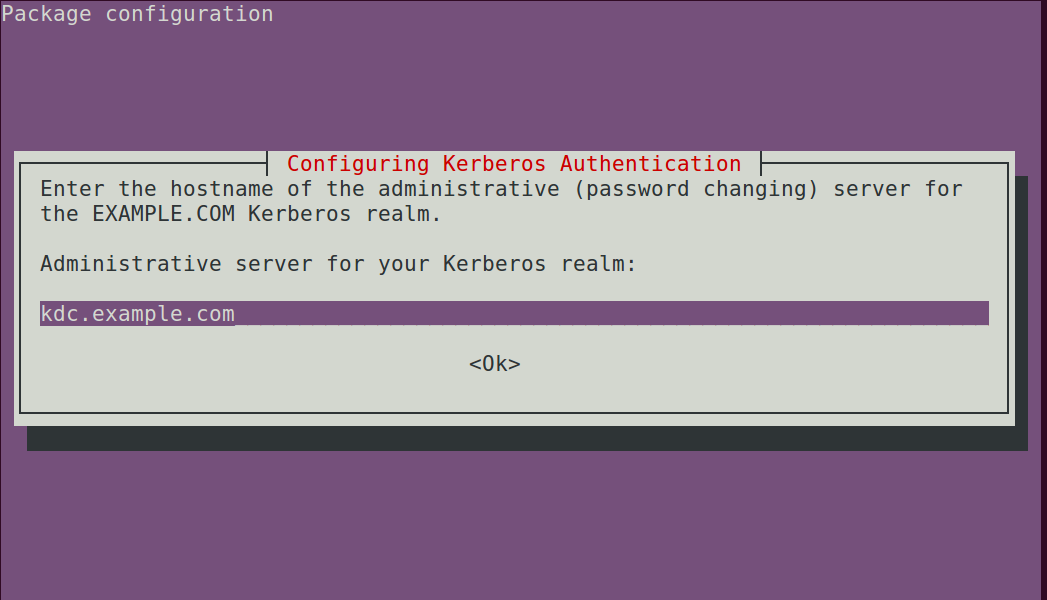
Enter the domain (Realm):

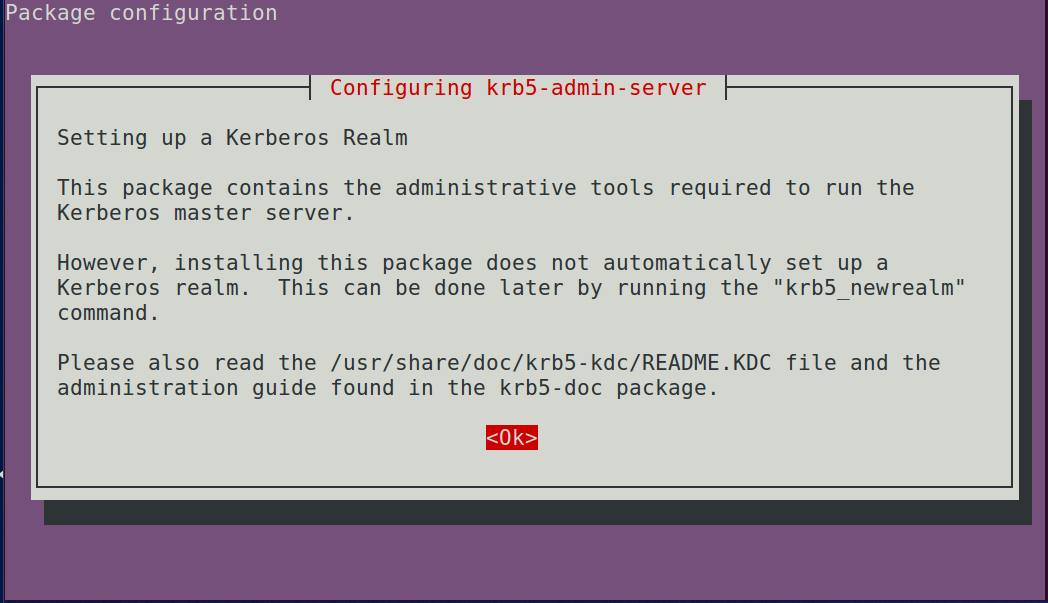


Enter FQDN of KDC:

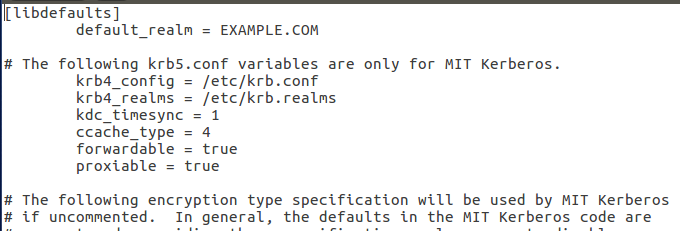


Enter the password changing admin server for Our Realm:

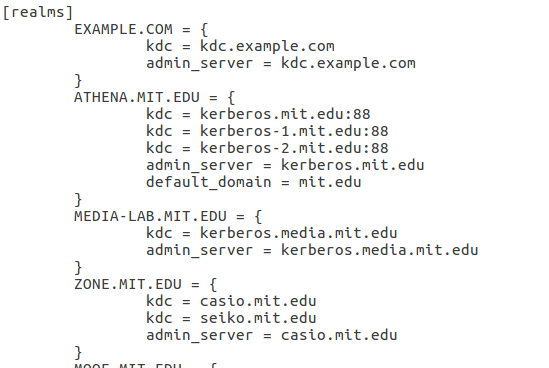




After the package is built check the krb5.conf file and check the FQDN:



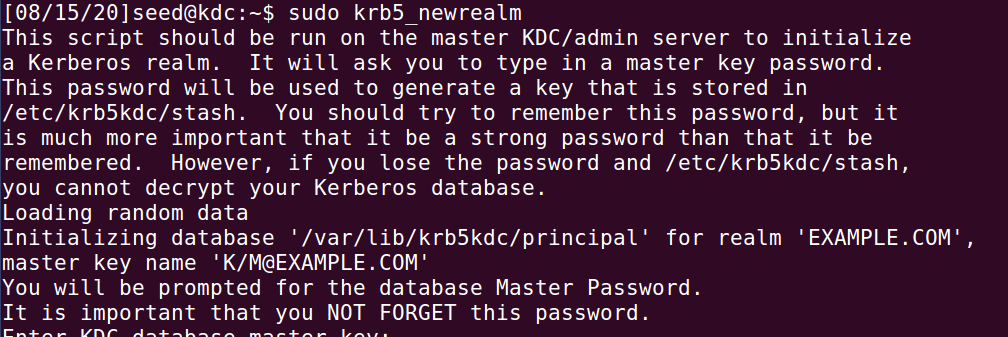
And also check the realm, if this is not properly configured, the clients will not authenticate.

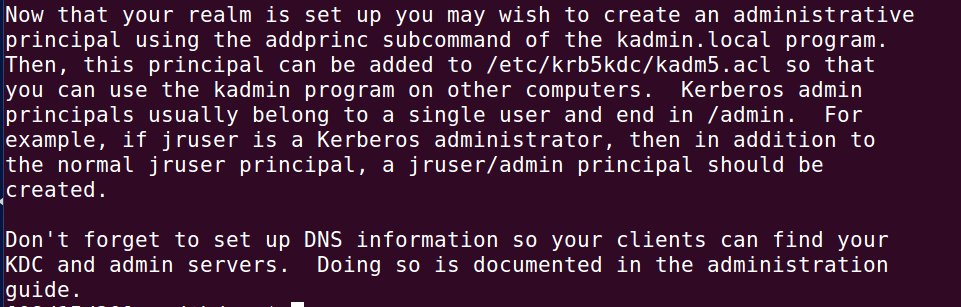


**Now we will create a new KRB5 realm:**

**With the command**:

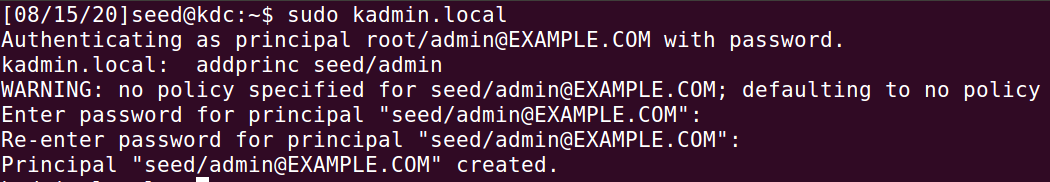
sudo krb5\_newrealm





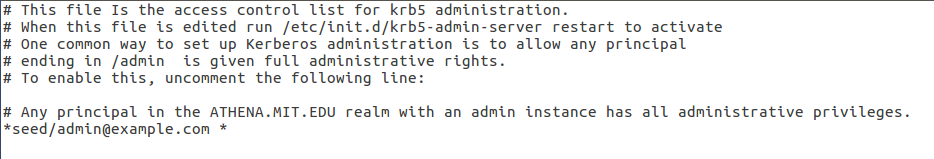
Now we are going to add the principal

sudo kadmin.local



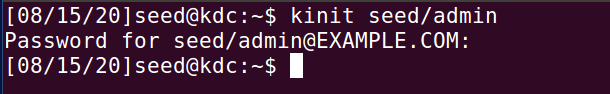
The admin user needs to have proper Access Control List Permissions, so we edit kadm5.acl file

sudo gedit /etc/krb5kdc/kadm5.acl

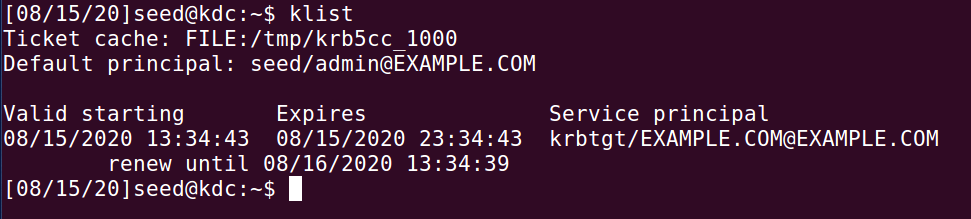


Restart Kerberos server for ACL to take effect.

sudo systemctl restart krb5-admin-server.service

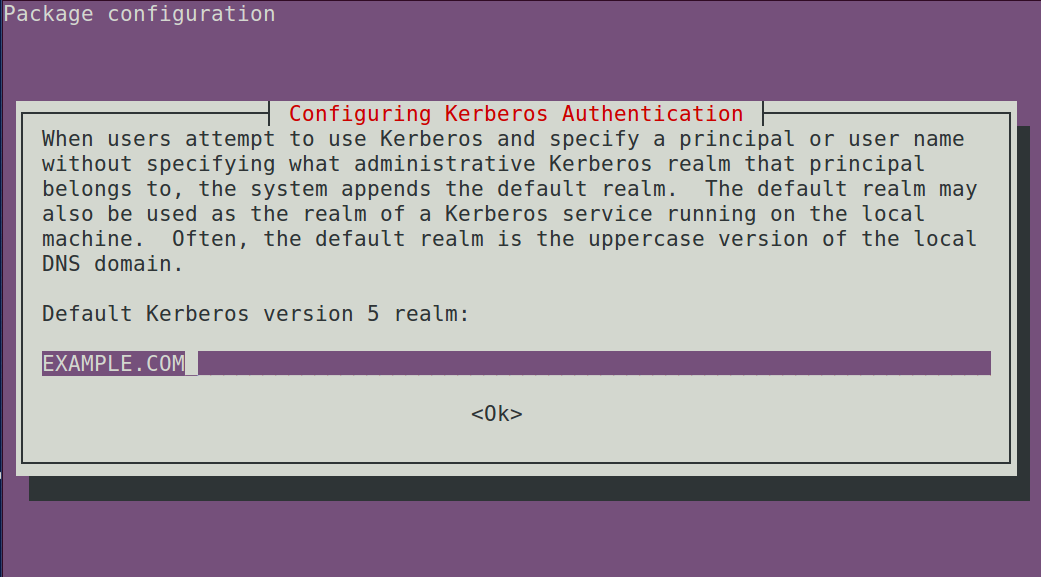


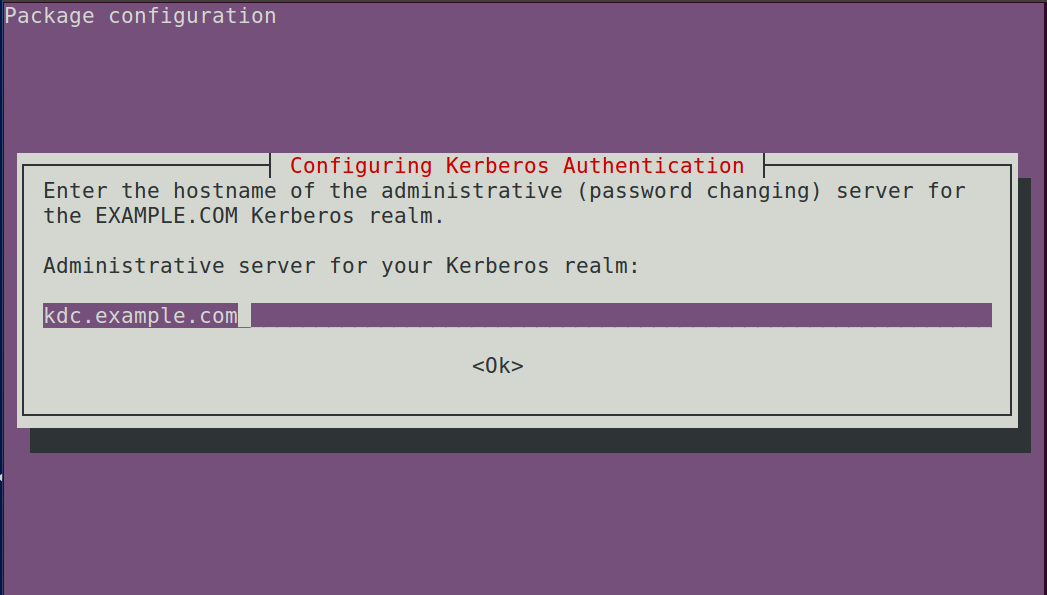
Use klist utility to check the TGT:



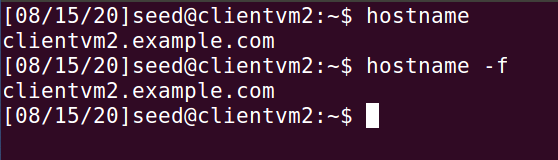
**Kerberos Client Installation and Configuration :**

**sudo aptitude install krb5-user libpam-krb5 libpam-ccreds auth-client-config**

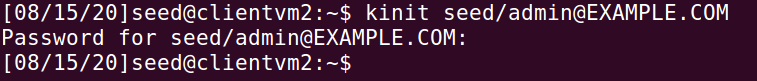


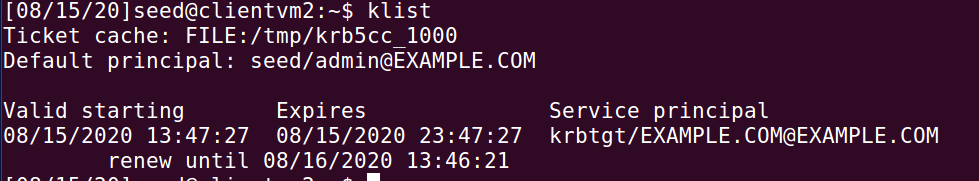


We are on a Kerberos Client now, so we will obtain the service from Kerberos KDC:

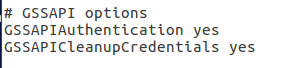


Here we have to write the FQDN i.e domain name in capital, otherwise it will give a credential error. The client should obtain the admin configuration from the access control list settings and then generate a ticket.

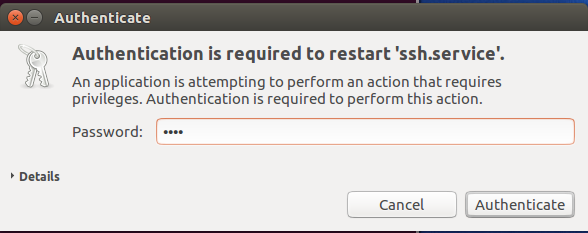




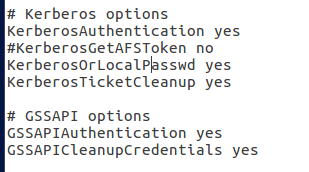
On the SSH server [**KDC] and the Kerberos** client, edit /etc/ssh/sshd\_config



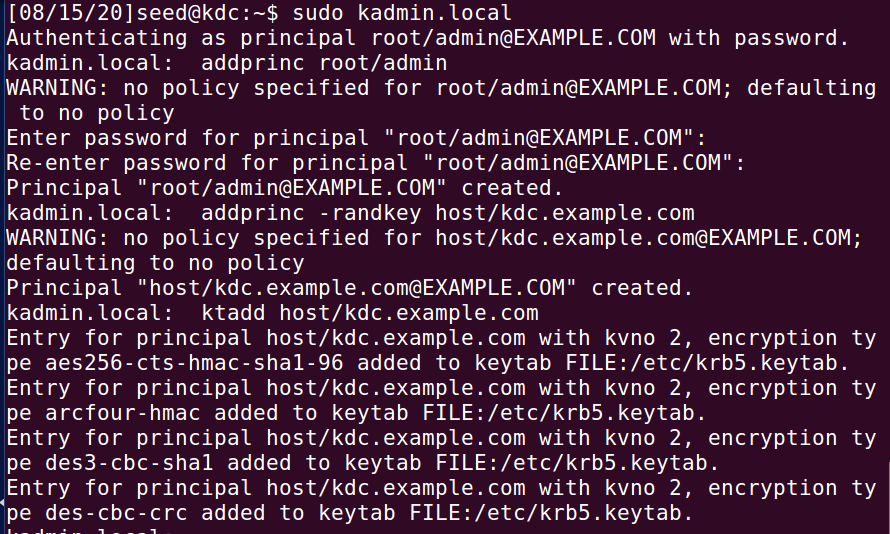
Do service ssh restart on the server and client:

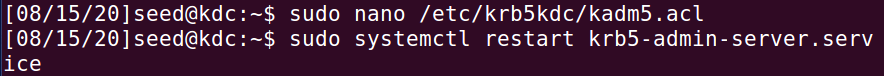


We also have to enable Kerberos Authentication on the server ssh configuration

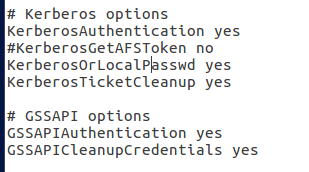


We use the SSH version 1 to connect to our KDC server.



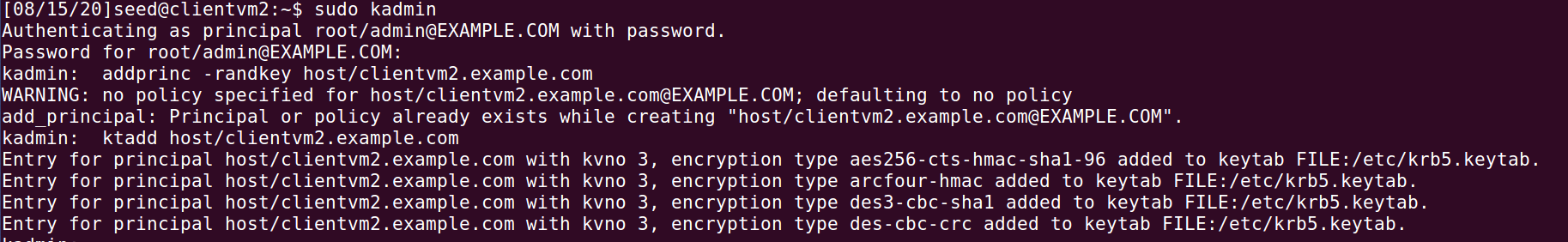


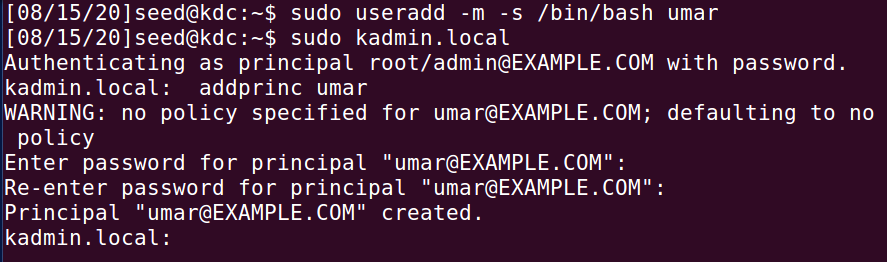
**To make ssh connection we have to add a non-admin user in server and client. And add the principals for them.**

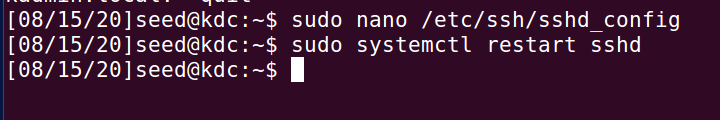


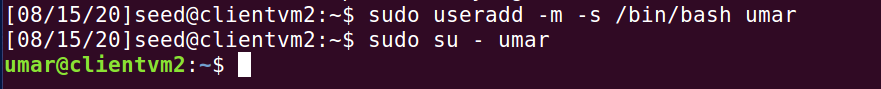
We have to modify these parameters and restart sshd service everytime. So that when we use SSH connection we will not have to enter password everytime.

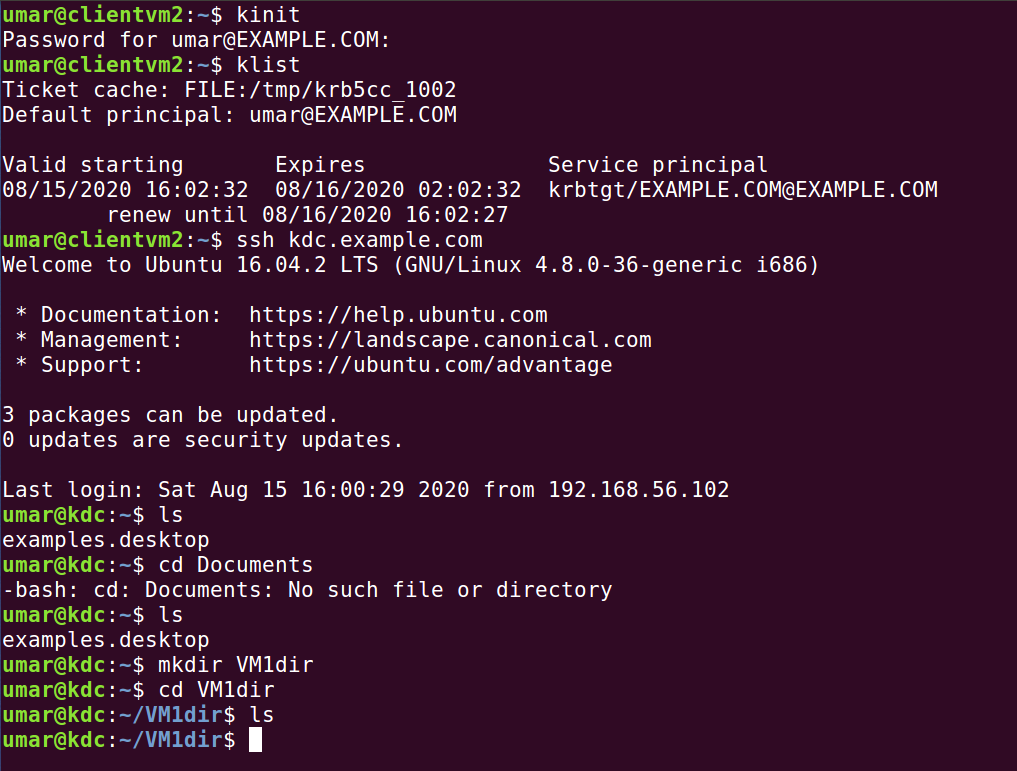
**The default versions use SSH ver. 1 but it is better to use SSH version2.**

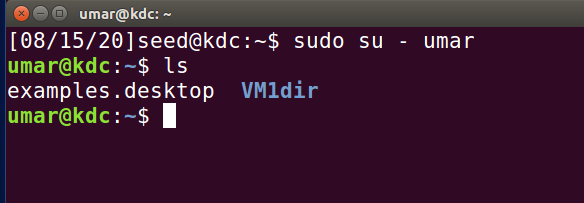


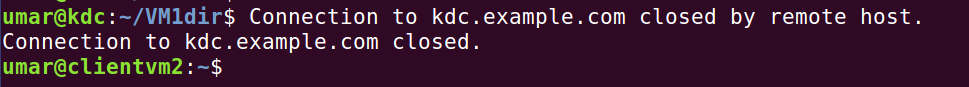












**We made a SSH connection from Kerberos Client, to the principal user we added in the Kerberos Server Virtual Machine.**