Cubbli and Kerberos authentication

University's Cubbli Linuxes use the same authentication mechanism as University's Windows machines. They authenticate and get their user accounts and groups from University's Active Directory (AD) domain, which uses a network protocol called Kerberos (Wikipedia link). Normally all this is configured to happen automatically and you don't need to worry about Kerberos or even know what it is. However, sometimes there are problems related to Kerberos and then the information provided in this page might be useful.

When you use your password to login to a Cubbli from the console, through ssh or just open a locked screen, you get a kerberos ticket, which is a secret random number, which can be used to authenticate against other services in the University's network without typing your password again. This provides the single sign on capabilities at the University.

Cubbli Linuxes use the kerberos ticket to access (at least) the following services at the University's network:

- Network file shares, like home directories and group directories (both SMB and NFS protocols)
- Printing to IT Department's printers, including smartcard printers
- Automatic login to University's web services through https://login.helsinki.fi/ (this is still a work in progress, but should be available later in 2018)
- Logging in remotely to Cubbli hosts through ssh (with Kerberos ticket delegation)

Since the kerberos ticket can be used to access services in the University's network, it should be kept secret and should be available only to you. Kerberos tickets also have a lifetime, after which they cannot be used anymore.

A very common problem when using a kerberos ticket is that the ticket has expired or that there isn't one. This will prevent Cubbli Linux from accessing any service requiring kerberos tickets including but not limited to those listed above. See common problems.

Using Kerberos tickets

You can see your kerberos ticket using the command *klist*. Here is an example output of *klist*, which has been used to access files both in University's file server (Z-drive through SMB) and CS Deparment's file server (/cs/home/ through NFS), to ssh remotely to melkki.cs.helsinki.fi and to print a document to university's smartcard queue:

```
$ klist
Ticket cache: FILE:/tmp/krb5cc_1033431_JVldy8
Default principal: jjaakkol@AD.HELSINKI.FI

Valid starting     Expires            Service principal
13/07/18 12:05:16  13/07/18 22:05:16  krbtgt/AD.HELSINKI.FI@AD.HELSINKI.FI
    renew until 14/07/18 12:05:14
13/07/18 12:06:47  13/07/18 22:05:16  nfs/nas-fs.cs.helsinki.fi@AD.HELSINKI.FI
    renew until 14/07/18 12:05:14
13/07/18 12:07:03  13/07/18 22:05:16  cifs/home3.ad.helsinki.fi@AD.HELSINKI.FI
    renew until 14/07/18 12:05:14
13/07/18 12:07:51  13/07/18 22:05:16  host/melkki.cs.helsinki.fi@AD.HELSINKI.FI
    renew until 14/07/18 12:05:14
13/07/18 12:08:07  13/07/18 22:05:16  cifs/valkokuusi1.ad.helsinki.fi@AD.HELSINKI.FI
```

Tickets have a limited lifetime after which they cannot be used any more. There are two different lifetimes:

- expiration lifetime (default 12h at University) after which the ticket becomes unusable
- longer renewable lifetime (default 24h at the university) during which the ticket can be renewed without providing a password again

Command *krenew* can be used to extend the expiration lifetime of a existing ticket, which still has renewable lifetime left. It also can be used to check if the current ticket is still valid. Here is a example of the command *krenew* when used with the same kerberos ticket as in the previous example:

```
$ krenew
$ klist
Ticket cache: FILE:/tmp/krb5cc_1033431_JVldy8
Default principal: jjaakkol@AD.HELSINKI.FI

Valid starting     Expires            Service principal
13/07/18 12:48:40  13/07/18 22:48:40  krbtgt/AD.HELSINKI.FI@AD.HELSINKI.FI
    renew until 14/07/18 12:05:14
```

When a ticket has become expired and you haven't got a new ticket through other means (opening a screensaver, logging in with your password) you can get a new ticket with command *kinit* using your University AD password:

```
$ kinit
Password for jjaakkol@AD.HELSINKI.FI:
$ klist
Ticket cache: FILE:/tmp/krb5cc_1033431_JVldy8
Default principal: jjaakkol@AD.HELSINKI.FI

Valid starting     Expires            Service principal
13/07/18 12:54:05  13/07/18 22:54:05  krbtgt/AD.HELSINKI.FI@AD.HELSINKI.FI
    renew until 14/07/18 12:54:02
```

Common problems

Expired or missing ticket

Most common problem is that the kerberos ticket has become expired or is missing. When the ticket has expired and you try to access files on a network file share you get the error message 'Key has expired'. This can be fixed by getting a new ticket:

```
jjaakkol@melkinkari:~$ cat hello.txt
cat: hello.txt: Key has expired
jjaakkol@melkinkari:~$ kinit
Password for jjaakkol@AD.HELSINKI.FI:
jjaakkol@melkinkari:~$ cat hello.txt
Hello!
```

Using ssh client from University AD Windows (like putty)

Another common problem happens when a ssh client uses kerberos to login to a ssh server, but does not delegate kerberos tickets to the server. This commonly happens when using Putty ssh client in the University's AD Windows environment, where kerberos authentication is available, but delegation is not. This too can be fixed by getting a new ticket:

```
Last login: Wed Jun 6 11:38:18 2018 from 128.214.138.171
Could not chdir to home directory /home/jjaakkol: Permission denied
realpath: /home/jjaakkol: Permission denied
-bash: /home/jjaakkol/.bash_profile: Permission denied
jjaakkol@tktl-pangolin:/$ kinit
Password for jjaakkol@AD.HELSINKI.FI:
jjaakkol@tktl-pangolin:/$ cd
jjaakkol@tktl-pangolin:~$
```

Classroom host allows login, but home directories are not visible

It is possible to login to a host with cached login credentials, but not get a kerberos ticket because of network problems and then home directories will not be visible. If this happens with a classroom host, you should check that the host is actually connected to the network and then restart it if possible.