

Chapter 12: Kerberos Command Descriptions

In this chapter we list the native Kerberos commands, and provide a brief description and option list with descriptions adapted from the man pages. Programs that Kerberos provides for ticket and password management include **kinit**, **klist**, **kpasswd** and **kdestroy**.

12.1 kinit

kinit obtains and caches a ticket (a ticket-granting ticket, by default) for the default principal or for a specified principal.

12.1.1 Syntax

```
% kinit [-l <lifetime>] [-s <start_time>] [-v] [-p] [-f] [-F] \  
[-k [-t <keytab_file>]] [-r <renewable_life>] [-R] [-a] \  
[-A] [-c <cache_name>] [-S <service_name>] [<principal>]
```

12.1.2 Option Descriptions

-l <lifetime> requests a ticket with the lifetime **<lifetime>**. The value for **<lifetime>** must be a number followed immediately by a delimiter indicating the unit of time, as follows:

<n>s (seconds)

<n>m (minutes)

<n>h (hours)

<n>d (days)

For example: **kinit -l 90m**. You cannot mix units; e.g., a value of “**-l 1h30m**” will result in an error.

If the **-l** option is not specified, the default ticket lifetime (26 hours, at Fermilab) is used. This option is only useful for specifying a ticket lifetime shorter than the default; to extend the lifetime beyond this limit you must renew the ticket; see **-r** and **-R**.

-s <start_time>

requests a postdated ticket, which can be validated (by action of the user) any time after **<start_time>**. Its lifetime starts when it gets validated. Format for the date and time can be any of the following:

yyyymmddhhmmss

yyyy.mm.dd.hh.mm.ss

yymmddhhmmss

yy.mm.dd.hh.mm.ss

yymmddhhmm

hhmmss

hhmm

hh:mm:ss

hh:mm

Postdated tickets are issued with the “invalid” flag set, and need to be validated before use; see **-v**.

-v requests that the post-dated ticket in the cache (with the “invalid” flag set) be passed to the KDC for validation. If the start time has passed, the cache is replaced with the validated ticket.

-p requests proxiable tickets

-f requests forwardable tickets

-F requests nonforwardable tickets

-r <renewable_life>

requests renewable tickets, with a maximum lifetime of **<renewable_life>**. If given a value longer than the preconfigured seven day limit, it will be set to seven days. **<renewable_life>** uses the same format as the **<lifetime>** associated with the **-l** option, with the same delimiters.

-R requests renewal of the renewable ticket. Renewal must take place before the ticket's lifetime expires. An expired ticket cannot be renewed, even if the ticket is still within its renewable life.

-k [-t <keytab_file>]

requests a host ticket, obtained from a key in the local host's keytab file. The name and location of the keytab file should be specified with the **-t <keytab_file>** option; otherwise the default name and location will be used (the default `/etc/krb5.keytab` is not useful here (except to *root*); users cannot read it). Keytab files are generally used for service principals. They are also used for **cron** jobs (see section 10.3.1 *Specific-User Processes (cron Jobs)*).

-c <cache_name>

uses **<cache_name>** as the credentials (ticket) cache name and location; if this option is not used, the default cache name and location are used.

The default credentials cache may vary by system. If the `KRB5CCNAME` environment variable is set, its value is used to name the default ticket cache. At Fermilab, this variable is typically set to

FILE:/tmp/krb5cc_<some_string>. Any existing contents of the cache are destroyed by **kinit**.

-S <service_name>

specifies a particular service name to use when getting initial tickets. If this option is not used, you get a ticket-granting-ticket by default.



-a

run **aklog** after obtaining tickets

-A

do not run **aklog** after obtaining tickets

12.1.3 Examples

Default

Typically you can run the **kinit** command without options. This gets you a 26-hour ticket with the flags `FIA` set by default (Forwardable, Initial, Preauthenticated; flags are viewable using **klist -f**, see section 12.2 *klist*), plus an AFS token if AFS is running on the machine.

Get Ticket with Specified Lifetime

Request a ticket valid for three hours using the `-l` option:

```
% kinit -l 3h
```

Get Renewable Ticket

Using the `-r` option, request a renewable ticket with a maximum renewable lifetime of four days (this sets the `R` flag on the ticket for `Renewable`, and sets the AFS token lifetime to four days):

```
% kinit -r 4d
```

Then, before the lifetime of 26 hours has passed, and before four days expire (you can renew a ticket multiple times within its renewable lifetime, but not after it has expired), renew the ticket using the `-R` option:

```
% kinit -R
```

The ticket will remain active an additional 26 hours or until its original four days expires, whichever comes first.

Get Postdated Ticket

Next, request a postdated ticket (using the `-s` option), with a lifetime of six hours (the lifetime starts at validation time):

```
% kinit -s 12:25 -l 6h
```

Until it gets validated, the invalid ticket has the flags `FdiIA` set by default, where `d` is `PostDated` and `i` is `Invalid`. Validate it after the start time has passed (using the `-v` option):

```
% kinit -v
```

Get Ticket based on Key

The following command requests a TGT for the principal `project/group/host.fnal.gov`, for the duration 30 minutes, with authentication done on the basis of a key previously stored in the keytab file `/usr/tmp/project.keytab` (this command would normally be included in a **cron** job file, not run interactively; see section 10.3.1 *Specific-User Processes (cron Jobs)*):

```
% kinit -l 30m -k -t /usr/tmp/project.keytab \  
project/group/host.fnal.gov
```

If you have an automatic process running as `root`, it is simplest to consider that the host on which the job runs is the party responsible for the accesses it initiates, and have it use the `/etc/krb5.keytab` to obtain credentials as `host/<hostname>.<domain>`:

```
% kinit -l 30m -k host/<hostname>.<domain>
```


12.2 klist

klist lists the Kerberos principal and Kerberos tickets held in a credentials cache (the default), or lists the keys held in a keytab file.

12.2.1 Syntax

```
% klist [-e] [[-c] [-f] [-s] [<cache_name>]] \
        [-k [-t] [-K] [<keytab_name>]]
```

12.2.2 Option/Argument Descriptions

- e** displays the encryption types of the session key and the ticket for each credential in the credential cache, or each key in the keytab file.
- c** lists tickets held in a credentials cache (as opposed to keys in a keytab file). Invalid with **-k**. This is the default if neither **-c** nor **-k** is specified.
- f** shows the flags present in the credentials, using the following abbreviations:
 - A** preAuthenticated
 - F** Forwardable
 - f** forwarded
 - P** Proxiabile
 - p** proxy
 - D** postDateable
 - d** postdated
 - R** Renewable
 - I** Initial
 - i** invalidInvalid with **-k**.
- s** causes **klist** to run silently (produce no output), while still setting the exit status according to whether it finds the credentials cache. The exit status is “0” if **klist** finds a credentials cache, and “1” if it does not. Invalid with **-k**.

- <cache_name>** specifies the credentials cache. If **<cache_name>** is not specified, **klist** will display the credentials in the default credentials cache (unless instructed to operate on a keytab file). If the KRB5CCNAME environment variable is set, its value is used to name the default ticket cache. At Fermilab, this variable is typically set to **FILE:/tmp/krb5cc_<some_string>**. Invalid with **-k**.
- k** lists keys held in a keytab file (as opposed to tickets in a credentials cache). Keytab files are generally used for service principals. Invalid with **-c**.
- t** displays the time entry timestamps for each keytab entry in the keytab file. Invalid with **-c**.
- K** displays the value of the encryption key in each keytab entry in the keytab file. Invalid with **-c**.
- <keytab_name>** specifies the keytab file. If **<keytab_name>** is not specified, **klist** will display the keys in the default keytab file (unless instructed to operate on a credentials cache). Invalid with **-c**.

12.2.3 Examples

Most frequently this command is issued with the **-f** option to indicate the flags set on each ticket:

```
% klist -f
Ticket cache: /tmp/krb5cc_ttyp0
Default principal: aheavey@FNAL.GOV

Valid starting    Expires          Service principal
02/11/00         12:45:33        02/12/00         01:45:33
krbtgt/FNAL.GOV@FNAL.GOV
    Flags: FIA
02/11/00 12:45:33  02/12/00 01:45:33  afs/fnal.gov@FNAL.GOV
    Flags: FA
```

To list the keys in a keytab file (for example a keytab file created for use with a **cron** job, see section 10.3.1 *Specific-User Processes (cron Jobs)*), use the **-k** and **-t <filename>** options:

```
% klist -k -t /usr/tmp/user1.keytab
Keytab name: FILE:/usr/tmp/user1.keytab
KVNO Timestamp          Principal
```


9 02/15/00 10:34:28 user1/cron@FNAL.GOV

12.3 kpasswd

The **kpasswd** command is used to change a Kerberos principal's password. You can change a principal's password from any account on a machine in the realm. **kpasswd** prompts for the current Kerberos password, and if supplied correctly, the user is then prompted twice for the new password, and the password is changed. **kpasswd** works even if the old password has expired. In the FNAL.GOV realm, a policy is in effect that specifies the length and minimum number of character classes required in the new password. The password must be at least ten characters long and contain at least two character classes. For *root*, the password must contain at least 13 characters of at least three classes. The character classes are: lower case, upper case, numbers, punctuation, and all other characters.

12.3.1 Syntax

```
% kpasswd [<principal>]
```

12.3.2 Argument Description

<principal>	Change the password for the Kerberos principal <principal> . If not given, the principal is derived from the identity of the user invoking the kpasswd command.
--------------------------	---

12.4 kdestroy

The **kdestroy** utility destroys the user's active Kerberos credentials (tickets) by writing zeros to the specified credentials cache that contains them, and then deleting the cache. If the credentials cache is not specified, the default credentials cache specified by `$KRB5CCNAME` is destroyed.

12.4.1 Syntax

```
% kdestroy [-q] [-c cache_name]
```

12.4.2 Option Descriptions

-q Runs quietly. Normally **kdestroy** beeps if it fails to destroy the user's tickets. The **-q** flag suppresses this behavior.

-c <cache_name>

Uses **<cache_name>** as the credentials (ticket) cache name and location; if this option is not used, the default cache name and location are used. If the `$KRB5CCNAME` environment variable is set, its value is used to name the default cache. At Fermilab, this variable is typically set to **FILE:/tmp/krb5cc_<some_string>**.