kadmin

SYNOPSIS

**kadmin** [**-O**|**-N**] [**-r** *realm*] [**-p** *principal*] [**-q** *query*] [[**-c** *cache\_name*]|[**-k** [**-t** *keytab*]]|**-n**] [**-w** *password*] [**-s** *admin\_server*[:*port*]]

**kadmin.local** [**-r** *realm*] [**-p** *principal*] [**-q** *query*] [**-d** *dbname*] [**-e** *enc*:*salt* ...] [**-m**] [**-x***db\_args*]

DESCRIPTION

kadmin and kadmin.local are command-line interfaces to the Kerberos V5 administration system. They provide nearly identical functionalities; the difference is that kadmin.local directly accesses the KDC database, while kadmin performs operations using [*kadmind*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/admin_commands/kadmind.html#kadmind-8). Except as explicitly noted otherwise, this man page will use “kadmin” to refer to both versions. kadmin provides for the maintenance of Kerberos principals, password policies, and service key tables (keytabs).

The remote kadmin client uses Kerberos to authenticate to kadmind using the service principal kadmin/ADMINHOST (where *ADMINHOST* is the fully-qualified hostname of the admin server) or kadmin/admin. If the credentials cache contains a ticket for one of these principals, and the **-c** credentials\_cache option is specified, that ticket is used to authenticate to kadmind. Otherwise, the **-p** and **-k** options are used to specify the client Kerberos principal name used to authenticate. Once kadmin has determined the principal name, it requests a service ticket from the KDC, and uses that service ticket to authenticate to kadmind.

Since kadmin.local directly accesses the KDC database, it usually must be run directly on the master KDC with sufficient permissions to read the KDC database. If the KDC database uses the LDAP database module, kadmin.local can be run on any host which can access the LDAP server.

OPTIONS

**-r** *realm*

Use *realm* as the default database realm.

**-p** *principal*

Use *principal* to authenticate. Otherwise, kadmin will append /admin to the primary principal name of the default ccache, the value of the **USER** environment variable, or the username as obtained with getpwuid, in order of preference.

**-k**

Use a keytab to decrypt the KDC response instead of prompting for a password. In this case, the default principal will be host/hostname. If there is no keytab specified with the **-t**option, then the default keytab will be used.

**-t** *keytab*

Use *keytab* to decrypt the KDC response. This can only be used with the **-k** option.

**-n**

Requests anonymous processing. Two types of anonymous principals are supported. For fully anonymous Kerberos, configure PKINIT on the KDC and configure **pkinit\_anchors** in the client’s [*krb5.conf*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/krb5_conf.html#krb5-conf-5). Then use the **-n** option with a principal of the form @REALM (an empty principal name followed by the at-sign and a realm name). If permitted by the KDC, an anonymous ticket will be returned. A second form of anonymous tickets is supported; these realm-exposed tickets hide the identity of the client but not the client’s realm. For this mode, use kinit -n with a normal principal name. If supported by the KDC, the principal (but not realm) will be replaced by the anonymous principal. As of release 1.8, the MIT Kerberos KDC only supports fully anonymous operation.

**-c** *credentials\_cache*

Use *credentials\_cache* as the credentials cache. The cache should contain a service ticket for the kadmin/ADMINHOST (where *ADMINHOST* is the fully-qualified hostname of the admin server) or kadmin/admin service; it can be acquired with the [*kinit*](https://web.mit.edu/kerberos/krb5-1.12/doc/user/user_commands/kinit.html#kinit-1) program. If this option is not specified, kadmin requests a new service ticket from the KDC, and stores it in its own temporary ccache.

**-w** *password*

Use *password* instead of prompting for one. Use this option with care, as it may expose the password to other users on the system via the process list.

**-q** *query*

Perform the specified query and then exit. This can be useful for writing scripts.

**-d** *dbname*

Specifies the name of the KDC database. This option does not apply to the LDAP database module.

**-s** *admin\_server*[:*port*]

Specifies the admin server which kadmin should contact.

**-m**

If using kadmin.local, prompt for the database master password instead of reading it from a stash file.

**-e** “*enc*:*salt* ...”

Sets the keysalt list to be used for any new keys created. See [*Keysalt lists*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/kdc_conf.html#keysalt-lists) in [*kdc.conf*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/kdc_conf.html#kdc-conf-5) for a list of possible values.

**-O**

Force use of old AUTH\_GSSAPI authentication flavor.

**-N**

Prevent fallback to AUTH\_GSSAPI authentication flavor.

**-x** *db\_args*

Specifies the database specific arguments. See the next section for supported options.

DATABASE OPTIONS

Database options can be used to override database-specific defaults. Supported options for the DB2 module are:

**-x dbname=**\*filename\*

Specifies the base filename of the DB2 database.

Supported options for the LDAP module are:

**-x host=***ldapuri*

Specifies the LDAP server to connect to by a LDAP URI.

**-x binddn=***bind\_dn*

Specifies the DN used to bind to the LDAP server.

**-x bindpwd=***bind\_password*

Specifies the password for the above mentioned binddn. Using this option may expose the password to other users on the system via the process list; to avoid this, instead stash the password using the **stashsrvpw** command of [*kdb5\_ldap\_util*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/admin_commands/kdb5_ldap_util.html#kdb5-ldap-util-8).

**-x debug=***level*

sets the OpenLDAP client library debug level. *level* is an integer to be interpreted by the library. Debugging messages are printed to standard error. New in release 1.12.

COMMANDS

When using the remote client, available commands may be restricted according to the privileges specified in the [*kadm5.acl*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/kadm5_acl.html#kadm5-acl-5) file on the admin server.

add\_principal

**add\_principal** [*options*] *newprinc*

Creates the principal *newprinc*, prompting twice for a password. If no password policy is specified with the **-policy** option, and the policy named default is assigned to the principal if it exists. However, creating a policy named default will not automatically assign this policy to previously existing principals. This policy assignment can be suppressed with the **-clearpolicy** option.

This command requires the **add** privilege.

Aliases: **addprinc**, **ank**

Options:

**-expire** *expdate*

([*getdate time*](https://web.mit.edu/kerberos/krb5-1.12/doc/basic/date_format.html#getdate) string) The expiration date of the principal.

**-pwexpire** *pwexpdate*

([*getdate time*](https://web.mit.edu/kerberos/krb5-1.12/doc/basic/date_format.html#getdate) string) The password expiration date.

**-maxlife** *maxlife*

([*getdate time*](https://web.mit.edu/kerberos/krb5-1.12/doc/basic/date_format.html#getdate) string) The maximum ticket life for the principal.

**-maxrenewlife** *maxrenewlife*

([*getdate time*](https://web.mit.edu/kerberos/krb5-1.12/doc/basic/date_format.html#getdate) string) The maximum renewable life of tickets for the principal.

**-kvno** *kvno*

The initial key version number.

**-policy** *policy*

The password policy used by this principal. If not specified, the policy default is used if it exists (unless **-clearpolicy** is specified).

**-clearpolicy**

Prevents any policy from being assigned when **-policy** is not specified.

{-|+}**allow\_postdated**

**-allow\_postdated** prohibits this principal from obtaining postdated tickets.**+allow\_postdated** clears this flag.

{-|+}**allow\_forwardable**

**-allow\_forwardable** prohibits this principal from obtaining forwardable tickets.**+allow\_forwardable** clears this flag.

{-|+}**allow\_renewable**

**-allow\_renewable** prohibits this principal from obtaining renewable tickets.**+allow\_renewable** clears this flag.

{-|+}**allow\_proxiable**

**-allow\_proxiable** prohibits this principal from obtaining proxiable tickets.**+allow\_proxiable** clears this flag.

{-|+}**allow\_dup\_skey**

**-allow\_dup\_skey** disables user-to-user authentication for this principal by prohibiting this principal from obtaining a session key for another user. **+allow\_dup\_skey** clears this flag.

{-|+}**requires\_preauth**

**+requires\_preauth** requires this principal to preauthenticate before being allowed to kinit. **-requires\_preauth** clears this flag. When **+requires\_preauth** is set on a service principal, the KDC will only issue service tickets for that service principal if the client’s initial authentication was performed using preauthentication.

{-|+}**requires\_hwauth**

**+requires\_hwauth** requires this principal to preauthenticate using a hardware device before being allowed to kinit. **-requires\_hwauth** clears this flag. When **+requires\_hwauth** is set on a service principal, the KDC will only issue service tickets for that service principal if the client’s initial authentication was performed using a hardware device to preauthenticate.

{-|+}**ok\_as\_delegate**

**+ok\_as\_delegate** sets the **okay as delegate** flag on tickets issued with this principal as the service. Clients may use this flag as a hint that credentials should be delegated when authenticating to the service. **-ok\_as\_delegate** clears this flag.

{-|+}**allow\_svr**

**-allow\_svr** prohibits the issuance of service tickets for this principal. **+allow\_svr** clears this flag.

{-|+}**allow\_tgs\_req**

**-allow\_tgs\_req** specifies that a Ticket-Granting Service (TGS) request for a service ticket for this principal is not permitted. **+allow\_tgs\_req** clears this flag.

{-|+}**allow\_tix**

**-allow\_tix** forbids the issuance of any tickets for this principal. **+allow\_tix** clears this flag.

{-|+}**needchange**

**+needchange** forces a password change on the next initial authentication to this principal. **-needchange** clears this flag.

{-|+}**password\_changing\_service**

**+password\_changing\_service** marks this principal as a password change service principal.

{-|+}**ok\_to\_auth\_as\_delegate**

**+ok\_to\_auth\_as\_delegate** allows this principal to acquire forwardable tickets to itself from arbitrary users, for use with constrained delegation.

{-|+}**no\_auth\_data\_required**

**+no\_auth\_data\_required** prevents PAC or AD-SIGNEDPATH data from being added to service tickets for the principal.

**-randkey**

Sets the key of the principal to a random value.

**-nokey**

Causes the principal to be created with no key. New in release 1.12.

**-pw** *password*

Sets the password of the principal to the specified string and does not prompt for a password. Note: using this option in a shell script may expose the password to other users on the system via the process list.

**-e** *enc*:*salt*,...

Uses the specified keysalt list for setting the keys of the principal. See [*Keysalt lists*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/kdc_conf.html#keysalt-lists) in [*kdc.conf*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/kdc_conf.html#kdc-conf-5) for a list of possible values.

**-x** *db\_princ\_args*

Indicates database-specific options. The options for the LDAP database module are:

**-x dn=***dn*

Specifies the LDAP object that will contain the Kerberos principal being created.

**-x linkdn=***dn*

Specifies the LDAP object to which the newly created Kerberos principal object will point.

**-x containerdn=***container\_dn*

Specifies the container object under which the Kerberos principal is to be created.

**-x tktpolicy=***policy*

Associates a ticket policy to the Kerberos principal.

**Note**

* The **containerdn** and **linkdn** options cannot be specified with the **dn** option.
* If the *dn* or *containerdn* options are not specified while adding the principal, the principals are created under the principal container configured in the realm or the realm container.
* *dn* and *containerdn* should be within the subtrees or principal container configured in the realm.

Example:

kadmin: addprinc jennifer

WARNING: no policy specified for "jennifer@ATHENA.MIT.EDU";

defaulting to no policy.

Enter password for principal jennifer@ATHENA.MIT.EDU:

Re-enter password for principal jennifer@ATHENA.MIT.EDU:

Principal "jennifer@ATHENA.MIT.EDU" created.

kadmin:

modify\_principal

**modify\_principal** [*options*] *principal*

Modifies the specified principal, changing the fields as specified. The options to **add\_principal** also apply to this command, except for the **-randkey**, **-pw**, and **-e** options. In addition, the option **-clearpolicy** will clear the current policy of a principal.

This command requires the *modify* privilege.

Alias: **modprinc**

Options (in addition to the **addprinc** options):

**-unlock**

Unlocks a locked principal (one which has received too many failed authentication attempts without enough time between them according to its password policy) so that it can successfully authenticate.

rename\_principal

**rename\_principal** [**-force**] *old\_principal* *new\_principal*

Renames the specified *old\_principal* to *new\_principal*. This command prompts for confirmation, unless the **-force** option is given.

This command requires the **add** and **delete** privileges.

Alias: **renprinc**

delete\_principal

**delete\_principal** [**-force**] *principal*

Deletes the specified *principal* from the database. This command prompts for deletion, unless the **-force** option is given.

This command requires the **delete** privilege.

Alias: **delprinc**

change\_password

**change\_password** [*options*] *principal*

Changes the password of *principal*. Prompts for a new password if neither **-randkey** or **-pw**is specified.

This command requires the **changepw** privilege, or that the principal running the program is the same as the principal being changed.

Alias: **cpw**

The following options are available:

**-randkey**

Sets the key of the principal to a random value.

**-pw** *password*

Set the password to the specified string. Using this option in a script may expose the password to other users on the system via the process list.

**-e** *enc*:*salt*,...

Uses the specified keysalt list for setting the keys of the principal. See [*Keysalt lists*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/kdc_conf.html#keysalt-lists) in [*kdc.conf*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/kdc_conf.html#kdc-conf-5) for a list of possible values.

**-keepold**

Keeps the existing keys in the database. This flag is usually not necessary except perhaps for krbtgt principals.

Example:

kadmin: cpw systest

Enter password for principal systest@BLEEP.COM:

Re-enter password for principal systest@BLEEP.COM:

Password for systest@BLEEP.COM changed.

kadmin:

purgekeys

**purgekeys** [**-all**|**-keepkvno** *oldest\_kvno\_to\_keep*] *principal*

Purges previously retained old keys (e.g., from **change\_password -keepold**) from *principal*. If **-keepkvno** is specified, then only purges keys with kvnos lower than *oldest\_kvno\_to\_keep*. If **-all** is specified, then all keys are purged. The **-all** option is new in release 1.12.

This command requires the **modify** privilege.

get\_principal

**get\_principal** [**-terse**] *principal*

Gets the attributes of principal. With the **-terse** option, outputs fields as quoted tab-separated strings.

This command requires the **inquire** privilege, or that the principal running the the program to be the same as the one being listed.

Alias: **getprinc**

Examples:

kadmin: getprinc tlyu/admin

Principal: tlyu/admin@BLEEP.COM

Expiration date: [never]

Last password change: Mon Aug 12 14:16:47 EDT 1996

Password expiration date: [none]

Maximum ticket life: 0 days 10:00:00

Maximum renewable life: 7 days 00:00:00

Last modified: Mon Aug 12 14:16:47 EDT 1996 (bjaspan/admin@BLEEP.COM)

Last successful authentication: [never]

Last failed authentication: [never]

Failed password attempts: 0

Number of keys: 2

Key: vno 1, des-cbc-crc, no salt

Key: vno 1, des-cbc-crc, Version 4

Attributes:

Policy: [none]

kadmin: getprinc -terse systest

systest@BLEEP.COM 3 86400 604800 1

785926535 753241234 785900000

tlyu/admin@BLEEP.COM 786100034 0 0

kadmin:

list\_principals

**list\_principals** [*expression*]

Retrieves all or some principal names. *expression* is a shell-style glob expression that can contain the wild-card characters ?, \*, and []. All principal names matching the expression are printed. If no expression is provided, all principal names are printed. If the expression does not contain an @ character, an @ character followed by the local realm is appended to the expression.

This command requires the **list** privilege.

Alias: **listprincs**, **get\_principals**, **get\_princs**

Example:

kadmin: listprincs test\*

test3@SECURE-TEST.OV.COM

test2@SECURE-TEST.OV.COM

test1@SECURE-TEST.OV.COM

testuser@SECURE-TEST.OV.COM

kadmin:

get\_strings

**get\_strings** *principal*

Displays string attributes on *principal*.

This command requires the **inquire** privilege.

Alias: **getstr**

set\_string

**set\_string** *principal* *key* *value*

Sets a string attribute on *principal*. String attributes are used to supply per-principal configuration to the KDC and some KDC plugin modules. The following string attributes are recognized by the KDC:

**session\_enctypes**

Specifies the encryption types supported for session keys when the principal is authenticated to as a server. See [*Encryption types*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/kdc_conf.html#encryption-types) in [*kdc.conf*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/kdc_conf.html#kdc-conf-5) for a list of the accepted values.

This command requires the **modify** privilege.

Alias: **setstr**

del\_string

**del\_string** *principal* *key*

Deletes a string attribute from *principal*.

This command requires the **delete** privilege.

Alias: **delstr**

add\_policy

**add\_policy** [*options*] *policy*

Adds a password policy named *policy* to the database.

This command requires the **add** privilege.

Alias: **addpol**

The following options are available:

**-maxlife** *time*

([*getdate time*](https://web.mit.edu/kerberos/krb5-1.12/doc/basic/date_format.html#getdate) string) Sets the maximum lifetime of a password.

**-minlife** *time*

([*getdate time*](https://web.mit.edu/kerberos/krb5-1.12/doc/basic/date_format.html#getdate) string) Sets the minimum lifetime of a password.

**-minlength** *length*

Sets the minimum length of a password.

**-minclasses** *number*

Sets the minimum number of character classes required in a password. The five character classes are lower case, upper case, numbers, punctuation, and whitespace/unprintable characters.

**-history** *number*

Sets the number of past keys kept for a principal. This option is not supported with the LDAP KDC database module.

**-maxfailure** *maxnumber*

Sets the number of authentication failures before the principal is locked. Authentication failures are only tracked for principals which require preauthentication. The counter of failed attempts resets to 0 after a successful attempt to authenticate. A *maxnumber* value of 0 (the default) disables lockout.

**-failurecountinterval** *failuretime*

([*getdate time*](https://web.mit.edu/kerberos/krb5-1.12/doc/basic/date_format.html#getdate) string) Sets the allowable time between authentication failures. If an authentication failure happens after *failuretime* has elapsed since the previous failure, the number of authentication failures is reset to 1. A *failuretime* value of 0 (the default) means forever.

**-lockoutduration** *lockouttime*

([*getdate time*](https://web.mit.edu/kerberos/krb5-1.12/doc/basic/date_format.html#getdate) string) Sets the duration for which the principal is locked from authenticating if too many authentication failures occur without the specified failure count interval elapsing. A duration of 0 (the default) means the principal remains locked out until it is administratively unlocked with modprinc -unlock.

**-allowedkeysalts**

Specifies the key/salt tuples supported for long-term keys when setting or changing a principal’s password/keys. See [*Keysalt lists*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/kdc_conf.html#keysalt-lists) in [*kdc.conf*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/kdc_conf.html#kdc-conf-5) for a list of the accepted values, but note that key/salt tuples must be separated with commas (‘,’) only. To clear the allowed key/salt policy use a value of ‘-‘.

Example:

kadmin: add\_policy -maxlife "2 days" -minlength 5 guests

kadmin:

modify\_policy

**modify\_policy** [*options*] *policy*

Modifies the password policy named *policy*. Options are as described for **add\_policy**.

This command requires the **modify** privilege.

Alias: **modpol**

delete\_policy

**delete\_policy** [**-force**] *policy*

Deletes the password policy named *policy*. Prompts for confirmation before deletion. The command will fail if the policy is in use by any principals.

This command requires the **delete** privilege.

Alias: **delpol**

Example:

kadmin: del\_policy guests

Are you sure you want to delete the policy "guests"?

(yes/no): yes

kadmin:

get\_policy

**get\_policy** [ **-terse** ] *policy*

Displays the values of the password policy named *policy*. With the **-terse** flag, outputs the fields as quoted strings separated by tabs.

This command requires the **inquire** privilege.

Alias: getpol

Examples:

kadmin: get\_policy admin

Policy: admin

Maximum password life: 180 days 00:00:00

Minimum password life: 00:00:00

Minimum password length: 6

Minimum number of password character classes: 2

Number of old keys kept: 5

Reference count: 17

kadmin: get\_policy -terse admin

admin 15552000 0 6 2 5 17

kadmin:

The “Reference count” is the number of principals using that policy. With the LDAP KDC database module, the reference count field is not meaningful.

list\_policies

**list\_policies** [*expression*]

Retrieves all or some policy names. *expression* is a shell-style glob expression that can contain the wild-card characters ?, \*, and []. All policy names matching the expression are printed. If no expression is provided, all existing policy names are printed.

This command requires the **list** privilege.

Aliases: **listpols**, **get\_policies**, **getpols**.

Examples:

kadmin: listpols

test-pol

dict-only

once-a-min

test-pol-nopw

kadmin: listpols t\*

test-pol

test-pol-nopw

kadmin:

ktadd

**ktadd** [options] *principal*

**ktadd** [options] **-glob** *princ-exp*

Adds a *principal*, or all principals matching *princ-exp*, to a keytab file. Each principal’s keys are randomized in the process. The rules for *princ-exp* are described in the **list\_principals**command.

This command requires the **inquire** and **changepw** privileges. With the **-glob** form, it also requires the **list** privilege.

The options are:

**-k[eytab]** *keytab*

Use *keytab* as the keytab file. Otherwise, the default keytab is used.

**-e** *enc*:*salt*,...

Uses the specified keysalt list for setting the new keys of the principal. See [*Keysalt lists*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/kdc_conf.html#keysalt-lists) in [*kdc.conf*](https://web.mit.edu/kerberos/krb5-1.12/doc/admin/conf_files/kdc_conf.html#kdc-conf-5) for a list of possible values.

**-q**

Display less verbose information.

**-norandkey**

Do not randomize the keys. The keys and their version numbers stay unchanged. This option is only available in kadmin.local, and cannot be specified in combination with the **-e**option.

An entry for each of the principal’s unique encryption types is added, ignoring multiple keys with the same encryption type but different salt types.

Example:

kadmin: ktadd -k /tmp/foo-new-keytab host/foo.mit.edu

Entry for principal host/foo.mit.edu@ATHENA.MIT.EDU with kvno 3,

encryption type aes256-cts-hmac-sha1-96 added to keytab

FILE:/tmp/foo-new-keytab

kadmin:

ktremove

**ktremove** [options] *principal* [*kvno* | *all* | *old*]

Removes entries for the specified *principal* from a keytab. Requires no permissions, since this does not require database access.

If the string “all” is specified, all entries for that principal are removed; if the string “old” is specified, all entries for that principal except those with the highest kvno are removed. Otherwise, the value specified is parsed as an integer, and all entries whose kvno match that integer are removed.

The options are:

**-k[eytab]** *keytab*

Use *keytab* as the keytab file. Otherwise, the default keytab is used.

**-q**

Display less verbose information.

Example:

kadmin: ktremove kadmin/admin all

Entry for principal kadmin/admin with kvno 3 removed from keytab

FILE:/etc/krb5.keytab

kadmin:

lock

Lock database exclusively. Use with extreme caution! This command only works with the DB2 KDC database module.

unlock

Release the exclusive database lock.

list\_requests

Lists available for kadmin requests.

Aliases: **lr**, **?**

quit

Exit program. If the database was locked, the lock is released.

Aliases: **exit**, **q**