NAME

kdc - Kerberos 5 server

SYNOPSIS

kdc [**-c** *file* | **--config-file=***file*] [**-p** | **--no-require-preauth**] [**--max-request=***size*] [**-H** | **--enable-http**]
[**--no-524**] [**--kerberos4**] [**--kerberos4-cross-realm**] [**-r** *string* | **--v4-realm=***string*]
[**-P** *portspec* | **--ports=***portspec*] [**--detach**] [**--disable-des**] [**--addresses=***list of addresses*]

DESCRIPTION

kdc serves requests for tickets. When it starts, it first checks the flags passed, any options that are not specified with a command line flag are taken from a config file, or from a default compiled-in value.

Options supported:

-c *file*, **--config-file=***file*

Specifies the location of the config file, the default is */var/heimdal/kdc.conf*. This is the only value that can't be specified in the config file.

-p, **--no-require-preauth**

Turn off the requirement for pre-autentication in the initial AS-REQ for all principals. The use of pre-authentication makes it more difficult to do offline password attacks. You might want to turn it off if you have clients that don't support pre-authentication. Since the version 4 protocol doesn't support any pre-authentication, serving version 4 clients is just about the same as not requiring pre-athentication. The default is to require pre-authentication. Adding the require-preauth per principal is a more flexible way of handling this.

--max-request=*size*

Gives an upper limit on the size of the requests that the kdc is willing to handle.

-H, **--enable-http**

Makes the kdc listen on port 80 and handle requests encapsulated in HTTP.

--no-524

don't respond to 524 requests

--kerberos4

respond to Kerberos 4 requests

--kerberos4-cross-realm

respond to Kerberos 4 requests from foreign realms. This is a known security hole and should

not be enabled unless you understand the consequences and are willing to live with them.

-r *string*, **--v4-realm=***string*

What realm this server should act as when dealing with version 4 requests. The database can contain any number of realms, but since the version 4 protocol doesn't contain a realm for the server, it must be explicitly specified. The default is whatever is returned by **krb_get_lrealm**(). This option is only available if the KDC has been compiled with version 4 support.

-P *portspec*, **--ports=***portspec*

Specifies the set of ports the KDC should listen on. It is given as a white-space separated list of services or port numbers.

--addresses=*list of addresses*

The list of addresses to listen for requests on. By default, the kdc will listen on all the locally configured addresses. If only a subset is desired, or the automatic detection fails, this option might be used.

--detach

detach from pty and run as a daemon.

--disable-des

disable add des encryption types, makes the kdc not use them.

All activities are logged to one or more destinations, see krb5.conf(5), and krb5_openlog(3). The entity used for logging is **kdc**.

CONFIGURATION FILE

The configuration file has the same syntax as krb5.conf(5), but will be read before */etc/krb5.conf*, so it may override settings found there. Options specific to the KDC only are found in the "[kdc]" section. All the command-line options can preferably be added in the configuration file. The only difference is the pre-authentication flag, which has to be specified as:

require-preauth = no

(in fact you can specify the option as **--require-preauth=no**).

And there are some configuration options which do not have command-line equivalents:

enable-digest = *boolean*

turn on support for digest processing in the KDC. The default is FALSE.

check-ticket-addresses = *boolean*
Check the addresses in the ticket when processing TGS requests. The default is TRUE.

allow-null-ticket-addresses = *boolean*
Permit tickets with no addresses. This option is only relevant when check-ticket-addresses is TRUE.

allow-anonymous = *boolean*
Permit anonymous tickets with no addresses.

max-kdc-datagram-reply-length = *number*
Maximum packet size the UDP rely that the KDC will transmit, instead the KDC sends back a reply telling the client to use TCP instead.

transited-policy = always-check | allow-per-principal | always-honour-request
This controls how KDC requests with the disable-transited-check flag are handled. It can be one of:

always-check
Always check transited encoding, this is the default.

allow-per-principal
Currently this is identical to always-check. In a future release, it will be possible to mark a principal as able to handle unchecked requests.

always-honour-request
Always do what the client asked. In a future release, it will be possible to force a check per principal.

encode_as_rep_as_tgs_rep = *boolean*
Encode AS-Rep as TGS-Rep to be bug-compatible with old DCE code. The Heimdal clients allow both.

kdc_warn_pwexpire = *time*
How long before password/principal expiration the KDC should start sending out warning messages.

The configuration file is only read when the **kdc** is started. If changes made to the configuration file are to take effect, the **kdc** needs to be restarted.

An example of a config file:

```
[kdc]
        require-preauth = no
        v4-realm = FOO.SE
```

BUGS

If the machine running the KDC has new addresses added to it, the KDC will have to be restarted to listen to them. The reason it doesn't just listen to wildcarded (like INADDR_ANY) addresses, is that the replies has to come from the same address they were sent to, and most OS:es doesn't pass this information to the application. If your normal mode of operation require that you add and remove addresses, the best option is probably to listen to a wildcarded TCP socket, and make sure your clients use TCP to connect. For instance, this will listen to IPv4 TCP port 88 only:

```
kdc --addresses=0.0.0.0 --ports="88/tcp"
```

There should be a way to specify protocol, port, and address triplets, not just addresses and protocol, port tuples.

SEE ALSO

kinit(1), krb5.conf(5)