Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'sssd-kcm.8' command

$ man sssd-kcm.8

SSSD-KCM(8) File Formats and Conventions SSSD-KCM(8)

NAME

sssd-kcm - SSSD Kerberos Cache Manager

DESCRIPTION

This manual page describes the configuration of the SSSD Kerberos Cache Manager (KCM). KCM is a process that stores, tracks and manages Kerberos credential caches. It originates in the Heimdal Kerberos project, although the MIT Kerberos library also provides client side (more details on that below) support for the KCM credential cache.

In a setup where Kerberos caches are managed by KCM, the Kerberos library (typically used through an application, like e.g., kinit(1), is a ?"KCM client"? and the KCM daemon is being referred to as a ?"KCM server"?. The client and server communicate over a UNIX socket.

The KCM server keeps track of each credential caches's owner and performs access check control based on the UID and GID of the KCM client. The root user has access to all credential caches.

The KCM credential cache has several interesting properties:

? since the process runs in userspace, it is subject to UID namespacing, unlike the kernel keyring

? unlike the kernel keyring-based cache, which is shared between all containers, the KCM server is a separate process whose entry point is a UNIX socket

? the SSSD implementation stores the ccaches in a database, typically

located at /var/lib/sss/secrets allowing the ccaches to survive KCM server restarts or machine reboots.

This allows the system to use a collection-aware credential cache, yet share the credential cache between some or no containers by bind-mounting the socket.

The KCM default client idle timeout is 5 minutes, this allows more time for user interaction with command line tools such as kinit.

USING THE KCM CREDENTIAL CACHE

In order to use KCM credential cache, it must be selected as the default credential type in krb5.conf(5), The credentials cache name must be only ?KCM:? without any template expansions. For example:

```
[libdefaults]
    default_ccache_name = KCM:
```

Next, make sure the Kerberos client libraries and the KCM server must agree on the UNIX socket path. By default, both use the same path /var/run/.heim_org.h5l.kcm-socket. To configure the Kerberos library, change its ?kcm_socket? option which is described in the krb5.conf(5) manual page.

Finally, make sure the SSSD KCM server can be contacted. The KCM service is typically socket-activated by systemd(1). Unlike other SSSD services, it cannot be started by adding the ?kcm? string to the ?service? directive.

```
systemctl start sssd-kcm.socket
systemctl enable sssd-kcm.socket
```

Please note your distribution may already configure the units for you.

THE CREDENTIAL CACHE STORAGE

The credential caches are stored in a database, much like SSSD caches user or group entries. The database is typically located at ?/var/lib/sss/secrets?.

OBTAINING DEBUG LOGS

The sssd-kcm service is typically socket-activated systemd(1). To generate debug logs, add the following either to the /etc/sssd/sssd.conf file directly or as a configuration snippet to

/etc/sssd/conf.d/ directory:

```
[kcm]
debug_level = 10
```

Then, restart the sssd-kcm service:

```
systemctl restart sssd-kcm.service
```

Finally, run whatever use-case doesn't work for you. The KCM logs will be generated at /var/log/sssd/sssd_kcm.log. It is recommended to disable the debug logs when you no longer need the debugging to be enabled as the sssd-kcm service can generate quite a large amount of debugging information.

Please note that configuration snippets are, at the moment, only processed if the main configuration file at /etc/sssd/sssd.conf exists at all.

RENEWALS

The sssd-kcm service can be configured to attempt TGT renewal for renewable TGTs stored in the KCM ccache. Renewals are only attempted when half of the ticket lifetime has been reached. KCM Renewals are configured when the following options are set in the [kcm] section:

```
tgt_renewal = true
krb5_renew_interval = 60m
```

SSSD can also inherit krb5 options for renewals from an existing domain.

```
tgt_renewal = true
tgt_renewal_inherit = domain-name
```

The following krb5 options can be configured in the [kcm] section to control renewal behavior, these options are described in detail below

```
krb5_renew_interval
krb5_renewable_lifetime
krb5_lifetime
krb5_validate
krb5_canonicalize
krb5_auth_timeout
```

CONFIGURATION OPTIONS

The KCM service is configured in the ?kcm? section of the sssd.conf file. Please note that because the KCM service is typically socket-activated, it is enough to just restart the ?sssd-kcm? service after changing options in the ?kcm? section of sssd.conf:

systemctl restart sssd-kcm.service

The KCM service is configured in the ?kcm? For a detailed syntax reference, refer to the ?FILE FORMAT? section of the sssd.conf(5) manual page.

The generic SSSD service options such as ?debug_level? or ?fd_limit? are accepted by the kcm service. Please refer to the sssd.conf(5) manual page for a complete list. In addition, there are some KCM-specific options as well.

socket_path (string)

The socket the KCM service will listen on.

Default: /var/run/.heim_org.h5l.kcm-socket

Note: on platforms where systemd is supported, the socket path is overwritten by the one defined in the sssd-kcm.socket unit file.

max_ccaches (integer)

How many credential caches does the KCM database allow for all users.

Default: 0 (unlimited, only the per-UID quota is enforced)

max_uid_ccaches (integer)

How many credential caches does the KCM database allow per UID. This is equivalent to ?with how many principals you can kinit?.

Default: 64

max_ccache_size (integer)

How big can a credential cache be per ccache. Each service ticket accounts into this quota.

Default: 65536

tgt_renewal (bool)

Enables TGT renewals functionality.

Default: False (Automatic renewals disabled)

tgt_renewal_inherit (string)

Domain to inherit krb5_* options from, for use with TGT renewals.

Default: NULL

krb5_auth_timeout (integer)

Timeout in seconds after an online authentication request or change password request is aborted. If possible, the authentication request is continued offline.

Default: 6

krb5_validate (boolean)

Verify with the help of krb5_keytab that the TGT obtained has not been spoofed. The keytab is checked for entries sequentially, and the first entry with a matching realm is used for validation. If no entry matches the realm, the last entry in the keytab is used. This process can be used to validate environments using cross-realm trust by placing the appropriate keytab entry as the last entry or the only entry in the keytab file.

Default: false (IPA and AD provider: true)

Please note that the ticket validation is the first step when checking the PAC (see 'pac_check' in the sssd.conf(5) manual page for details). If ticket validation is disabled the PAC checks will be skipped as well.

krb5_renewable_lifetime (string)

Request a renewable ticket with a total lifetime, given as an integer immediately followed by a time unit:

s for seconds

m for minutes

h for hours

d for days.

If there is no unit given, s is assumed.

NOTE: It is not possible to mix units. To set the renewable lifetime to one and a half hours, use '90m' instead of '1h30m'.

Default: not set, i.e. the TGT is not renewable

krb5_lifetime (string)

Request ticket with a lifetime, given as an integer immediately

followed by a time unit:

s for seconds

m for minutes

h for hours

d for days.

If there is no unit given s is assumed.

NOTE: It is not possible to mix units. To set the lifetime to one and a half hours please use '90m' instead of '1h30m'.

Default: not set, i.e. the default ticket lifetime configured on the KDC.

krb5_renew_interval (string)

The time in seconds between two checks if the TGT should be renewed. TGTs are renewed if about half of their lifetime is exceeded, given as an integer immediately followed by a time unit:

s for seconds

m for minutes

h for hours

d for days.

If there is no unit given, s is assumed.

NOTE: It is not possible to mix units. To set the renewable lifetime to one and a half hours, use '90m' instead of '1h30m'.

If this option is not set or is 0 the automatic renewal is disabled.

Default: not set

krb5_canonicalize (boolean)

Specifies if the host and user principal should be canonicalized.

This feature is available with MIT Kerberos 1.7 and later versions.

Default: false

SEE ALSO

sssd(8), sssd.conf(5),

AUTHORS

The SSSD upstream - https://github.com/SSSD/sssd/