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

Rocky Enterprise Linux 9.2 Manual Pages on command 'sssd_krb5_locator_plugin.8'

$ man sssd_krb5_locator_plugin.8

SSSD_KRB5_LOCATOR_PL(8)   SSSD Manual pages   SSSD_KRB5_LOCATOR_PL(8)

NAME

sssd_krb5_locator_plugin - Kerberos locator plugin

DESCRIPTION

The Kerberos locator plugin sssd_krb5_locator_plugin is used by libkrb5 to find KDCs for a given Kerberos realm. SSSD provides such a plugin to guide all Kerberos clients on a system to a single KDC. In general it should not matter to which KDC a client process is talking to. But there are cases, e.g. after a password change, where not all KDCs are in the same state because the new data has to be replicated first. To avoid unexpected authentication failures and maybe even account lockings it would be good to talk to a single KDC as long as possible.

libkrb5 will search the locator plugin in the libkrb5 sub-directory of the Kerberos plugin directory, see plugin_base_dir in krb5.conf(5) for details. The plugin can only be disabled by removing the plugin file. There is no option in the Kerberos configuration to disable it. But the SSSD_KRB5_LOCATOR_DISABLE environment variable can be used to disable the plugin for individual commands. Alternatively the SSSD option krb5_use_kdcinfo=False can be used to not generate the data needed by the plugin. With this the plugin is still called but will provide no data to the caller so that libkrb5 can fall back to other methods defined in krb5.conf.

The plugin reads the information about the KDCs of a given realm from a file called kdcinfo.REALM. The file should contain one or more DNS names or IP addresses either in dotted-decimal IPv4 notation or the hexadecimal IPv6 notation. An optional port number can be added to the end separated with a colon, the IPv6 address has to be enclosed in squared brackets in this case as usual. Valid entries are:

? kdc.example.com

? kdc.example.com:321

? 1.2.3.4

? 5.6.7.8:99

? 2001:db8:85a3::8a2e:370:7334

? [2001:db8:85a3::8a2e:370:7334]:321

SSSD's krb5 auth-provider which is used by the IPA and AD providers as well adds the address of the current KDC or domain controller SSSD is using to this file.

In environments with read-only and read-write KDCs where clients are expected to use the read-only instances for the general operations and only the read-write KDC for config changes like password changes a kpasswdinfo.REALM is used as well to identify read-write KDCs. If this file exists for the given realm the content will be used by the plugin to reply to requests for a kpasswd or kadmin server or for the MIT Kerberos specific master KDC. If the address contains a port number the default KDC port 88 will be used for the latter.

NOTES

Not all Kerberos implementations support the use of plugins. If sssd_krb5_locator_plugin is not available on your system you have to edit /etc/krb5.conf to reflect your Kerberos setup.

If the environment variable SSSD_KRB5_LOCATOR_DEBUG is set to any value debug messages will be sent to stderr.

If the environment variable SSSD_KRB5_LOCATOR_DISABLE is set to any value the plugin is disabled and will just return KRB5_PLUGIN_NO_HANDLE to the caller.

If the environment variable SSSD_KRB5_LOCATOR_IGNORE_DNS_FAILURES is set to any value plugin will try to resolve all DNS names in kdcinfo file. By default plugin returns KRB5_PLUGIN_NO_HANDLE to the caller immediately on first DNS resolving failure.

SEE ALSO

sssd(8), sssd.conf(5), sssd-ldap(5), sssd-ldap-attributes(5), sssd-krb5(5), sssd-simple(5), sssd-ipa(5), sssd-ad(5), sssd-files(5), sssd-sudo(5), sssd-session-recording(5), sss_cache(8), sss_debuglevel(8), sss_obfuscate(8), sss_seed(8), sssd_krb5_locator_plugin(8), sss_ssh_authorizedkeys(8), sss_ssh_knownhostsproxy(8), sssd-ifp(5), pam_sss(8). sss_rpcidmapd(5) sssd-systemtap(5)

AUTHORS

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

SSSD 07/10/2023 SSSD_KRB5_LOCATOR_PL(8)