Red Hat Enterprise Linux Release 9.2 Manual Pages on 'tpm2_policyrestart.1' command

$ man tpm2_policyrestart.1

tpm2_policyrestart(1)   General Commands Manual   tpm2_policyrestart(1)

NAME

tpm2_policyrestart(1) - Restart an existing session with the TPM.

SYNOPSIS

tpm2_policyrestart [OPTIONS]

DESCRIPTION

tpm2_policyrestart(1) - Restarts a session with the TPM back to it?s initial state. This is useful when the TPM gives one a TPM_RC_PCR_CHANGED (0x00000128) error code when using a PCR policy session.

This will be returned if a PCR state affecting policy is altered during the session. One could restart the session and try again, however, the PCR state would still need to satisfy the policy.

OPTIONS

? -S, --session=FILE:

Optional, A session file from tpm2_startauthsession(1)?s -S option. This session is used in lieu of starting a session and using the PCR policy options.

References

COMMON OPTIONS

This collection of options are common to many programs and provide information that many users may expect.

? -h, --help=[man|no-man]: Display the tools manpage. By default, it attempts to invoke the manpager for the tool, however, on failure will output a short tool summary. This is the same behavior if the ?man? option argument is specified, however if explicit ?man? is requested, the tool will provide errors from man on stderr. If the ?no-man? option if specified, or the manpager fails, the short options will be output to stdout.

To successfully use the manpages feature requires the manpages to be installed or on MANPATH, See man(1) for more details.

? -v, --version: Display version information for this tool, supported tctis and exit.

? -V, --verbose: Increase the information that the tool prints to the console during its execution. When using this option the file and line number are printed.

? -Q, --quiet: Silence normal tool output to stdout.

? -Z, --enable-errata: Enable the application of errata fixups. Useful if an errata fixup needs to be applied to commands sent to the TPM. Defining the environment TPM2TOOLS_ENABLE_ERRATA is equivalent. information many users may expect.

TCTI Configuration

The TCTI or ?Transmission Interface? is the communication mechanism with the TPM. TCTIs can be changed for communication with TPMs across different mediums.

To control the TCTI, the tools respect:

1. The command line option -T or --tcti

2. The environment variable: TPM2TOOLS_TCTI.

Note: The command line option always overrides the environment variable.

The current known TCTIs are:

? tabrmd - The resource manager, called tabrmd (https://github.com/tpm2-software/tpm2-abrmd). Note that tabrmd and abrmd as a tcti name are synonymous.

? mssim - Typically used for communicating to the TPM software simulator.

? device - Used when talking directly to a TPM device file.

? none - Do not initalize a connection with the TPM. Some tools allow for off-tpm options and thus support not using a TCTI. Tools that do not support it will error when attempted to be used without a TCTI connection. Does not support ANY options and MUST BE presented as the exact text of ?none?.

The arguments to either the command line option or the environment variable are in the form:

<tcti-name>:<tcti-option-config>

Specifying an empty string for either the <tcti-name> or <tcti-option-config> results in the default being used for that portion respectively.

TCTI Defaults

When a TCTI is not specified, the default TCTI is searched for using dlopen(3) semantics. The tools will search for tabrmd, device and mssim TCTIs IN THAT ORDER and USE THE FIRST ONE FOUND. You can query what TCTI will be chosen as the default by using the -v option to print the version information. The ?default-tcti? key-value pair will indicate which of the aforementioned TCTIs is the default.

Custom TCTIs

Any TCTI that implements the dynamic TCTI interface can be loaded. The tools internally use dlopen(3), and the raw tcti-name value is used for the lookup. Thus, this could be a path to the shared library, or a library name as understood by dlopen(3) semantics.

TCTI OPTIONS

This collection of options are used to configure the various known TCTI modules available:

? device: For the device TCTI, the TPM character device file for use by the device TCTI can be specified. The default is /dev/tpm0.

Example: -T device:/dev/tpm0 or export TPM2TOOLS_TCTI=?device:/dev/tpm0?

? mssim: For the mssim TCTI, the domain name or IP address and port number used by the simulator can be specified. The default are

127.0.0.1 and 2321.

Example: -T mssim:host=localhost,port=2321 or export TPM2TOOLS_TCTI=?mssim:host=localhost,port=2321?

? abrmd: For the abrmd TCTI, the configuration string format is a series of simple key value pairs separated by a `,' character. Each key and value string are separated by a `=' character.

? TCTI abrmd supports two keys:

1. `bus_name' : The name of the tabrmd service on the bus (a string).
2. `bus_type' : The type of the dbus instance (a string) limited to `session' and `system'.

Specify the tabrmd tcti name and a config string of bus_name=com.example.FooBar:

```
\--tcti=tabrmd:bus_name=com.example.FooBar
```

Specify the default (abrmd) tcti and a config string of bus_type=session:

```
\--tcti:bus_type=session
```

NOTE: abrmd and tabrmd are synonymous. the various known TCTI modules.

EXAMPLES

Start a policy session and restart it, unsealing some data.

```
# create a policy and bind it to an object
tpm2_startauthsession -S session.dat
tpm2_policypcr -S session.dat -l "sha1:0,1,2,3" -L policy.dat
tpm2_createprimary -c primary.ctx
tpm2_create -Cprimary.ctx -u key.pub -r key.priv -L policy.dat -i- <<< "secret"
tpm2_load -C primary.ctx -c key.ctx -u key.pub -r key.priv
tpm2_flushcontext session.dat
# satisfy the policy and use the object
tpm2_startauthsession --policy -S session.dat
tpm2_policypcr -S session.dat -l "sha1:0,1,2,3"
# PCR event occurs here causing unseal to fail
tpm2_pcrevent 0 <<< "event data"
```

```
tpm2_unseal -psession:session.dat -c key.ct

ERROR: Esys_Unseal(0x128) - tpm:error(2.0): PCR have changed since checked

# Clear the policy digest to initial state, note access to object no longer allowed by

# policy so policyor would be useful here.

tpm2_policyrestart -S session.dat
```

Returns

Tools can return any of the following codes:

? 0 - Success.

? 1 - General non-specific error.

? 2 - Options handling error.

? 3 - Authentication error.

? 4 - TCTI related error.

? 5 - Non supported scheme. Applicable to tpm2_testparams.

Limitations

It expects a session to be already established via tpm2_startauthses?

sion(1) and requires one of the following:

? direct device access

? extended session support with tpm2-abrmd.

Without it, most resource managers will not save session state between

command invocations.

BUGS

Github Issues (https://github.com/tpm2-software/tpm2-tools/issues)

HELP

See the Mailing List (https://lists.01.org/mailman/listinfo/tpm2)

tpm2-tools tpm2_policyrestart(1)