Rocky Enterprise Linux 9.2 Manual Pages on command 'cockpit_session_selinux.8cockpit'

$ man cockpit_session_selinux.8cockpit

cockpit_session_selinux(SELinux Policy cockpit_sessicockpit_session_selinux(8)

NAME

cockpit_session_selinux - Security Enhanced Linux Policy for the cock?

pit_session processes

DESCRIPTION

Security-Enhanced Linux secures the cockpit_session processes via flex?

ible mandatory access control.

The cockpit_session processes execute with the cockpit_session_t

SELinux type. You can check if you have these processes running by exe?

cuting the ps command with the -Z qualifier.

For example:

ps -eZ | grep cockpit_session_t

ENTRYPOINTS

The cockpit_session_t SELinux type can be entered via the cockpit_ses?

sion_exec_t file type.

The default entrypoint paths for the cockpit_session_t domain are the

following:

/usr/libexec/cockpit-ssh, /usr/libexec/cockpit-session

PROCESS TYPES

SELinux defines process types (domains) for each process running on the system

You can see the context of a process using the -Z option to ps

Policy governs the access confined processes have to files. SELinux cockpit_session policy is very flexible allowing users to setup their cockpit_session processes in as secure a method as possible.

The following process types are defined for cockpit_session:

cockpit_session_t

Note: semanage permissive -a cockpit_session_t can be used to make the process type cockpit_session_t permissive. SELinux does not deny access to permissive process types, but the AVC (SELinux denials) messages are still generated.

BOOLEANS

SELinux policy is customizable based on least access required. cock? pit_session policy is extremely flexible and has several booleans that allow you to manipulate the policy and run cockpit_session with the tightest access possible.

If you want to allow all domains to execute in fips_mode, you must turn on the fips_mode boolean. Enabled by default.

setsebool -P fips_mode 1

If you want to allow confined applications to run with kerberos, you must turn on the kerberos_enabled boolean. Enabled by default.

setsebool -P kerberos_enabled 1

If you want to allow system to run with NIS, you must turn on the nis_enabled boolean. Disabled by default.

setsebool -P nis_enabled 1

If you want to enable polyinstantiated directory support, you must turn on the polyinstantiation_enabled boolean. Disabled by default.

setsebool -P polyinstantiation_enabled 1

MANAGED FILES

The SELinux process type cockpit_session_t can manage files labeled with the following file types. The paths listed are the default paths

for these file types. Note the processes UID still need to have DAC permissions.

auth_cache_t

/var/cache/coolkey(/.*)?

auth_home_t

/root/.yubico(/.*)?

/root/.config/Yubico(/.*)?

/root/.google_authenticator

/root/.google_authenticator~

/home/[^/]+/.yubico(/.*)?

/home/[^/]+/.config/Yubico(/.*)?

/home/[^/]+/.google_authenticator

/home/[^/]+/.google_authenticator~

faillog_t

/var/log/btmp.*

/var/log/faillog.*

/var/log/tallylog.*

/var/run/faillock(/.*)?

initrc_var_run_t

/var/run/utmp

/var/run/random-seed

/var/run/runlevel.dir

/var/run/setmixer_flag

lastlog_t

/var/log/lastlog.*

pam_var_run_t

/var/(db|adm)/sudo(/.*)?

/var/lib/sudo(/.*)?

/var/run/sudo(/.*)?

/var/run/pam_ssh(/.*)?

/var/run/sepermit(/.*)?

/var/run/pam_mount(/.*)?

/var/run/pam_timestamp(/.*)?

security_t

/selinux

shadow_t

/etc/shadow.*

/etc/gshadow.*

/etc/nshadow.*

/var/db/shadow.*

/etc/security/opasswd

/etc/security/opasswd.old

var_auth_t

/var/ace(/.*)?

/var/rsa(/.*)?

/var/lib/abl(/.*)?

/var/lib/rsa(/.*)?

/var/lib/pam_ssh(/.*)?

/var/lib/pam_shield(/.*)?

/var/opt/quest/vas/vasd(/.*)?

/var/lib/google-authenticator(/.*)?

wtmp_t

/var/log/wtmp.*

FILE CONTEXTS

SELinux requires files to have an extended attribute to define the file type.

You can see the context of a file using the -Z option to ls

Policy governs the access confined processes have to these files.

SELinux cockpit_session policy is very flexible allowing users to setup their cockpit_session processes in as secure a method as possible.

The following file types are defined for cockpit_session:

cockpit_session_exec_t

- Set files with the cockpit_session_exec_t type, if you want to tran? sition an executable to the cockpit_session_t domain.

Paths:

/usr/libexec/cockpit-ssh, /usr/libexec/cockpit-session

Note: File context can be temporarily modified with the chcon command. If you want to permanently change the file context you need to use the semanage fcontext command. This will modify the SELinux labeling data? base. You will need to use restorecon to apply the labels.

COMMANDS

semanage fcontext can also be used to manipulate default file context mappings.

semanage permissive can also be used to manipulate whether or not a process type is permissive.

semanage module can also be used to enable/disable/install/remove pol? icy modules.

semanage boolean can also be used to manipulate the booleans

system-config-selinux is a GUI tool available to customize SELinux pol? icy settings.

AUTHOR

This manual page was auto-generated using sepolicy manpage .

SEE ALSO

selinux(8), cockpit_session(8), semanage(8), restorecon(8), chcon(1), sepolicy(8), setsebool(8)

cockpit_session 21-04-16 cockpit_session_selinux(8)