



*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 'cockpit\_session\_selinux.8cockpit' command**

**`$ 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. cockpit\_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 transition 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 policy modules.

semanage boolean can also be used to manipulate the booleans

system-config-selinux is a GUI tool available to customize SELinux policy settings.

#### AUTHOR

This manual page was auto-generated using sepolity manpage .

#### SEE ALSO

selinux(8), cockpit\_session(8), semanage(8), restorecon(8), chcon(1),

sepolity(8), setsebool(8)

cockpit\_session            21-04-16       cockpit\_session\_selinux(8)