ipsec_selinux(8) - Linux man page

Name

ipsec_selinux - Security Enhanced Linux Policy for the ipsec processes

Description

Security-Enhanced Linux secures the ipsec processes via flexible mandatory access control.

The ipsec processes execute with the ipsec_t SELinux type. You can check if you have these processes running by executing the **ps** command with the **-Z** qualifier.

For example:

ps -eZ | grep ipsec_t

Entrypoints

The ipsec_t SELinux type can be entered via the "ipsec_exec_t" file type. The default entrypoint paths for the ipsec_t domain are the following:"

/usr/**lib**(64)?/ipsec/spi, /usr/**lib**(64)?/ipsec/pluto, /usr/**lib**(64)?/ipsec/eroute, /usr/**lib**(64)?/ipsec/klipsdebug, /usr/local/**lib**(64)?/ipsec/spi, /usr/local/**lib**(64)?/ipsec/pluto, /usr/local/**lib**(64)?/ipsec/eroute, /usr/local/**lib**(64)?/ipsec/klipsdebug, /usr/libexec/ipsec/spi, /usr/libexec/ipsec/pluto, /usr/libexec/ipsec/eroute, /usr/libexec/ipsec/klipsdebug

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

The following process types are defined for ipsec:

ipsec_t, ipsec_mgmt_t

Note: **semanage permissive -a ipsec_t**

can be used to make the process type ipsec_t permissive. Permissive process types are not denied access by SELinux. AVC messages will still be generated.

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

The following file types are defined for ipsec:

ipsec_conf_file_t

- Set files with the ipsec_conf_file_t type, if you want to treat the files as ipsec conf content.

ipsec_exec_t

- Set files with the ipsec_exec_t type, if you want to transition an executable to the ipsec_t domain.

ipsec_initrc_exec_t

- Set files with the ipsec_initrc_exec_t type, if you want to transition an executable to the ipsec_initrc_t domain.

ipsec_key_file_t

- Set files with the ipsec_key_file_t type, if you want to treat the files as ipsec key content.

ipsec_log_t

- Set files with the ipsec_log_t type, if you want to treat the data as ipsec log data, usually stored under the /var/log directory.

ipsec_mgmt_exec_t

- Set files with the ipsec_mgmt_exec_t type, if you want to transition an executable to the ipsec_mgmt_t domain.

ipsec_mgmt_lock_t

- Set files with the ipsec_mgmt_lock_t type, if you want to treat the files as ipsec mgmt lock data, stored under the /var/lock directory

ipsec_mgmt_var_run_t

- Set files with the ipsec_mgmt_var_run_t type, if you want to store the ipsec mgmt files under the /run directory.

ipsec_tmp_t

- Set files with the ipsec_tmp_t type, if you want to store ipsec temporary files in the /tmp directories.

ipsec_var_run_t

- Set files with the ipsec_var_run_t type, if you want to store the ipsec files under the /run directory.

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 database. You will need to use **restorecon** to apply the labels.

Port Types

SELinux defines port types to represent TCP and UDP ports.

You can see the types associated with a port by using the following command:

semanage port -l

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

The following port types are defined for ipsec:

ipsecnat_port_t
Default Defined Ports:
    tcp 4500 udp 4500

Managed Files

The SELinux process type ipsec_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.

initrc_tmp_t

ipsec_key_file_t

/etc/ipsec.d(/.*)?

/etc/racoon/certs(/.*)?

/etc/ipsec.secrets

/etc/racoon/psk.txt

ipsec_tmp_t

ipsec_var_run_t

/var/racoon(/.*)?

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

/var/run/racoon.pid

mnt_t

/mnt(/[^/]*)

/mnt(/[^/]*)?

/rhev(/[^/]*)?

/media(/[^/]*)

/media(/[^/]*)?

/etc/rhgb(/.*)?

/media/.hal-.*

/net

/afs

/misc

/rhev

net_conf_t

/etc/ntpd?.conf.*

/etc/yp.conf.*

/etc/denyhosts.*

/etc/hosts.deny.*

/etc/resolv.conf.*

/etc/ntp/step-tickers.*

/etc/sysconfig/networking(/.*)?

/etc/sysconfig/network-scripts(/.*)?

/etc/sysconfig/network-scripts/.*resolv.conf

/etc/hosts

/etc/ethers

root_t

/

/initrd

security_t

tmp_t

/tmp

/usr/tmp

/var/tmp

/var/tmp/vi.recover

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 port can also be used to manipulate the port definitions

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

Author

This manual page was auto-generated using **sepolicy manpage** by mgrepl.

See Also

selinux(8), **ipsec**(8), **semanage**(8), **restorecon**(8), **chcon**(1), **sepolicy**(8) , **ipsec_mgmt_selinux**(8)