lvm_selinux(8) - Linux man page

Name

lvm_selinux - Security Enhanced Linux Policy for the lvm processes

Description

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

The lvm processes execute with the lvm_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 lvm_t

Entrypoints

The lvm_t SELinux type can be entered via the "mtrr_device_t,unlabeled_t,proc_type,sysctl_type,filesystem_type,file_type,lvm_exec_t" file types. The default entrypoint paths for the lvm_t domain are the following:"

/dev/cpu/mtrr, all files on the system, /lib/lvm-10/.*, /lib/lvm-200/.*, /sbin/lvs, /sbin/vgs, /sbin/pvs, /sbin/lvm, /sbin/vgck, /sbin/pvdata, /sbin/pvmove, /sbin/pvscan, /sbin/lvscan, /sbin/kpartx, /sbin/lvmsar, /sbin/dmraid, /sbin/vgscan, /sbin/vgmerge, /sbin/dmsetup, /sbin/e2fsadm, /sbin/lvmsadc, /sbin/lvmetad, /sbin/vgsplit, /usr/sbin/lvm, /sbin/vgchange, /sbin/vgexport, /sbin/vgcreate, /sbin/vgextend, /sbin/vgimport, /sbin/vgreduce, /sbin/vgremove, /sbin/vgrename, /sbin/pvchange, /sbin/pvcreate, /sbin/pvremove, /sbin/lvreduce, /sbin/lvrename, /sbin/lvresize, /sbin/lvremove, /sbin/lvchange, /sbin/lvextend, /sbin/lvcreate, /sbin/vgdisplay, /sbin/vgmknodes, /sbin/pvdisplay, /sbin/lvdisplay, /sbin/lvmchange, /sbin/vgwrapper, /sbin/multipathd, /sbin/lvm.static, /sbin/cryptsetup, /sbin/vgcfgbackup, /sbin/lvmdiskscan, /sbin/mount.crypt, /sbin/vgcfgrestore, /sbin/lvmiopversion, /sbin/vgscan.static, /sbin/dmsetup.static, /sbin/vgchange.static, /sbin/multipath.static, /lib/udev/udisks-lvm-pv-export

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

The following process types are defined for lvm:

lvm_t

Note: **semanage permissive -a lvm_t**

can be used to make the process type lvm_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 lvm policy is very flexible allowing users to setup their lvm processes in as secure a method as possible.

The following file types are defined for lvm:

lvm_etc_t

- Set files with the lvm_etc_t type, if you want to store lvm files in the /etc directories.

lvm_exec_t

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

lvm_lock_t

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

lvm_metadata_t

- Set files with the lvm_metadata_t type, if you want to treat the files as lvm metadata data.

lvm_tmp_t

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

lvm_var_lib_t

- Set files with the lvm_var_lib_t type, if you want to store the lvm files under the /var/lib directory.

lvm_var_run_t

- Set files with the lvm_var_run_t type, if you want to store the lvm 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.

Managed Files

The SELinux process type lvm_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.

file_type

all files on the system

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.

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), **lvm**(8), **semanage**(8), **restorecon**(8), **chcon**(1), **sepolicy**(8)