

SELinux: Referentiel des classes d'objet et des Permissions

Table of Contents

- [SELinux: Referentiel des classes d'objet et des Permissions](#)
- [Common Permission Sets](#)
 - [common database](#)
 - [common file](#)
 - [common ipc](#)
 - [common socket](#)
 - [common x_device](#)
- [Kernel Object Classes](#)
 - [appletalk_socket](#)
 - [association IPSEC](#)
 - [blk_file](#)
- [capability](#)
 - [capability2](#)
 - [chr_file](#)
 - [dccp_socket](#)
 - [dir](#)
 - [fd](#)
 - [fifo_file](#)
 - [file](#)
 - [filesystem](#)
 - [ipc](#)
 - [kernel_service](#)
 - [key](#)
 - [key_socket](#)
 - [lnk_file](#)
 - [memprotect](#)
 - [msg](#)
 - [msgq](#)
 - [netif](#)
 - [netlink_socket](#)
 - [netlink_audit_socket](#)
 - [netlink_dnrt_socket](#)
 - [netlink_firewall_socket](#)
 - [netlink_ip6fw_socket](#)
 - [netlink_kobject_uevent_socket](#)
 - [netlink_nflog_socket](#)
 - [netlink_route_socket](#)

- netlink_selinux_socket
- netlink_tcpdiag_socket
- netlink_xfrm_socket
- node
- packet
- packet_socket
- peer
- process
- rawip_socket
- security
- sem
- shm
- sock_file
- socket
- system
- tcp_socket
- tun_socket
- udp_socket
- unix_dgram_socket
- unix_stream_socket
- Database Object Classes
 - db_blob
 - db_column
 - db_database
 - db_procedure
 - db_table
 - db_tuple
- DBus Object Classes
 - dbus
- MLS Context Translation Object Classes
 - context
- NSCD Object Classes
 - nscd
- Password Object Classes
 - passwd
- X Server Object Classes
 - x_application_data
 - x_client
 - x_colormap
 - x_cursor
 - x_device
 - x_drawable
 - x_event
 - x_extension
 - x_font

- x_gc
- x_keyboard
 - x_pointer
 - x_property
 - x_resource
 - x_screen
 - x_selection
 - x_server
 - x_synthetic_event

Ce document contient une liste des genres d'objet (object classes) et des permissions que l'on peut accorder : avec les réserves suivantes:

- Les descriptions des autorisations servent uniquement à donner une idée générale des objectifs des autorisations; une permission peut entraîner de nombreuses opérations.
- Le développement de SELinux étant en cours, ce document peut être incomplet ou inexact.

Common Permission Sets

common database

Permission	Description
create	Crée un nouvel objet de base de données.
drop	Supprime un objet de base de données.
getattr	Obtenir les attributs d'un objet de base de données.
setattr	Définissez les attributs d'un objet de base de données.
relabelfrom	Modifier le contexte de sécurité en fonction du type existant.
relabelto	Modifier le contexte de sécurité en fonction du nouveau type.

common file

Permission	Description
getattr	Obtenir les attributs de fichier pour le fichier, tels que le mode d'accès. (par exemple, stat, certains ioctl. ...)
relabelto	Ré-étiqueter dans un nouveau contexte de sécurité.
unlink	Supprimer le lien physique (supprimer).
ioctl	Demande d'appel du système de contrôle IO non traitées par d'autres autorisations.
execute	Exécuter
append	Écrire dans un fichier ouvert avec O \ _APPEND.
read	Lire le contenu du fichier.
setattr	Modifier les attributs de fichier pour un fichier tel que le mode d'accès. (par exemple, chmod, certains ioctls, ...)
swapon	Permet au fichier d'être utilisé pour la pagination / échange d'espace.
write	Ecrire dans un fichier.

Permission	Description
lock	Définit et désactive les verrous de fichiers.
create	Créer un nouveau fichier.
rename	Renomme un fichier.
mounton	Utiliser comme point de montage; utile uniquement pour les répertoires et les fichiers sous Linux.
quotaon	Utiliser comme un fichier de quota.
relabelfrom	Ré-étiquetez de l'ancien contexte de sécurité.
liink	Créer un autre lien dur au fichier

common ipc

Permission	Description
write	Écrire.
destroy	Détruire.
unix_write	Accès en écriture générique.
getattr	Obtenir des attributs, par exemple Opération IPC_STAT *ctl.
create	Créer.
read	Lire
setattr	Modifier les attributs, par exemple IPC_SET.
unix_read	Accès en lecture générique.
associate	Associer une clé

common socket

Permission	Description
append	Ecrire pour ouvrir fd marqué avec O \ _APPEND.
relabelfrom	Modifier le contexte de sécurité en fonction du type existant.
create	Créer un nouveau socket.
read	Lire de la prise.
sendto	Envoyer à la prise.
connecter	Lancer la connexion.
recvfrom	Vérification NetLabel héritée; obsolète par les pairs recv
envoyer \ _msg	Legacy Check; n'est plus présent.
bind	Lie un nom à la prise.
lock	Applique le verrouillage de fichier sur un socket.
ioctl	Demandes d'appel du système de contrôle IO non traitées par d'autres autorisations.
getattr	Obtenir les attributs de socket, par exemple fstat.
write	Ecrire à socket.
setopt	Définir les options de socket.
getopt	Obtenir les options de socket.
listen	Écoutez les connexions.
setattr	Changer les attributs du socket.
shutdown	Ferme la connexion.
relabelto	Modifie le contexte de sécurité en fonction du nouveau type.
recv_msg	Obsolète.

Permission	Description
accept	Accepter une connexion.
name_bind	Associer avec un port ou un fichier; pour les sockets AF_INET, contrôle la relation entre une socket et son numéro de port; pour AF_UNIX sockets, contrôle la relation entre une socket et son fichier

common x_device

Permission	Description
getattr	
setattr	
use	
read	
write	
getfocus	
setfocus	
bell	
force_cursor	
freeze	
grab	
manage	
list_property	
get_property	
set_property	
add	
remove	

Kernel Object Classes

appletalk_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock

Permission	Description
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind

association IPSEC

Permission	Description
sendto	Envoyer à une association IPSEC.
recvfrom	Recevoir d'une association IPSEC.
setcontext	Définit le contexte d'une association IPSEC lors de la création.
polmatch	Faire correspondre une entrée de stratégie IPSEC

blk_file

Hérite de: common file

Permission	Description
getattr	file:getattr
relabelto	file:relabelto
unlink	file:unlink
ioctl	file:ioctl
execute	file:execute
append	file:append
read	file:read
setattr	file:setattr
swapon	file:swapon
write	file:write
lock	file:lock
create	file:create
rename	file:rename
mouton	file:mouton
quotaon	file:quotaon
relabelfrom	file:relabelfrom
link	file:link
open	Open a block device file.

capability

Permission	Description
chown	Ignorer les restrictions sur la modification de la propriété de fichier et de la propriété de groupe.
dac_override	Ignorez toutes les restrictions d'accès DAC. Vérifié avant <code>dac \ _read \ _search</code> , donc candidat non auditable.
dac_read\ _search	Ignorez les restrictions d'accès en lecture / recherche du CAD.
fowner	Remplace toutes les exigences du propriétaire de fichier (par exemple, pour <code>chmod</code> , <code>setxattr</code>) sauf là où <code>fsetid</code> s'applique.
fsetid	Remplace les exigences de propriétaire de fichier et de groupe lors de la définition de bits <code>setuid</code> ou <code>setgid</code> sur un fichier. Peut être vérifié comme un effet secondaire sur les opérations <code>chmod</code> et <code>write</code> ; candidat audité.
kill	Remplace la restriction selon laquelle l'ID utilisateur réel ou effectif d'un processus envoyant un signal doit correspondre à l'ID utilisateur réel ou effectif du processus recevant le signal.
setgid	Autorise <code>setgid (2)</code> ou <code>setgroups (2)</code> ou des gids forgés sur des informations d'identification transmises via un socket.
setuid	Autoriser <code>set * uid (2)</code> . Autorise la transmission d'identifiants forgés sur les informations d'identification transmises via un socket.
setpcap	Ajouter une capacité de jeu de bornes à un jeu pouvant être hérité, supprimer la capacité de jeu de limites, modifier des bits sécurisés.
linux_immutable	Accordez le privilège de modifier les attributs de fichier <code>S \ _IMMUTABLE</code> et <code>S \ _APPEND</code> sur les systèmes de fichiers pris en charge.
net_bind \ _service	Autoriser la liaison à faible port. Port <1024 pour TCP / UDP. VCI <32 pour ATM.
net_diffusion	Accordez la diffusion sur le réseau et l'écoute des multidiffusions entrantes.
net_admin	Permet toutes les configurations et modifications de mise en réseau. Voir <code>linux / capacity.h</code> pour plus de détails.
net_raw	Permet d'ouvrir des sockets brutes et des sockets packet.
ipc_lock	Autorise le verrouillage des segments de mémoire partagée et <code>mlock / mlockall</code> .
ipc_owner	Ignorer les contrôles de propriété IPC.
sys_module	Autorise la modification non restreinte du noyau, y compris, sans toutefois s'y limiter, le chargement et la suppression de modules du noyau. Permet la modification du masque de capacité de limite de noyaux. Voir <code>sysctl</code> .
sys_rawio	Accordez la permission d'utiliser <code>ioperm (2)</code> et <code>iopl (2)</code> , ainsi que la possibilité d'envoyer des messages à des périphériques USB via <code>/ proc / bus / usb</code> .
sys_chroot	Autoriser l'utilisation de l'appel <code>chroot (2)</code> .
sys_ptrace	Autoriser une trace de tout processus.
sys_pacct	Autoriser la modification de la comptabilité pour n'importe quel processus.
sys_admin	Trop nombreux pour être énumérés ici (voir <code>/usr/include/linux/capability.h</code>)
sys_boot	Accorder la possibilité de redémarrer le système.
sys_nice	Donne le privilège de changer la priorité de tout processus. Permet de modifier l'algorithme de planification utilisé par n'importe quel processus.
sys_resource	Trop nombreux pour être énumérés ici (voir <code>/usr/include/linux/capability.h</code> pour plus de détails.)
sys_time	Accorde la permission de définir l'heure système et le verrouillage en temps réel.
sys_tty\ _config	Accordez la permission de configurer les périphériques tty. Autorise l'appel <code>vhangup (2)</code> sur un terminal.
mknod	Donne la permission de créer des noeuds de périphérique de caractère et de bloc.

Permission	Description
lease	Donne la capacité de prendre des baux sur un fichier. Pour plus de détails sur les baux, voir fcntl (2).
audit_write	Générez des messages d'audit à partir de l'espace utilisateur.
audit_control	Contrôlez la configuration / les règles d'audit du noyau. Définir l'identifiant de connexion.
setfcap	Définir les capacités du fichier.

capability2

Permission	Description
mac_override	Ignorer les restrictions MAC - Ignoré par SELinux
mac_admin	Modifier la configuration MAC - Pour SELinux, obtenir / définir des valeurs de contexte de sécurité brutes inconnues de la stratégie actuelle.
syslog	Configurer le sous-système syslog du noyau
wake_alarm	Déclencher quelque chose qui va réveiller le système
block_suspend	Empêcher le système suspend

chr_file

Hérite de: common file

Permission	Description
getattr	file:getattr
relabelto	file:relabelto
unlink	file:unlink
ioctl	file:ioctl
execute	file:execute
append	file:append
read	file:read
setattr	file:setattr
swapon	file:swapon
write	file:write
lock	file:lock
create	file:create
rename	file:rename
mouton	file:mouton
quotaon	file:quotaon
relabelfrom	file:relabelfrom
link	file:link
execute_no_trans	Exécuter un fichier dans le domaine des appelants.
entrypoint	Peut être exécuté en tant que point d'entrée du nouveau domaine dans une transition.
execmod	Rendre exécutable un mappage de fichier qui a été modifié par copie sur écriture. (Relocalisation de texte)
open	Ouvre un fichier de périphérique de caractère.

dccp_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind
connectto	Connect to server socket.
newconn	Create new socket for connection.
acceptfrom	Accept connection from client socket.
node_bind	Ability to bind to a node.
name_connect	Connect to a specific port number.

dir

Hérite de: common file

Permission	Description
getattr	file:getattr
relabelto	file:relabelto
unlink	N/A
ioctl	file:ioctl
execute	N/A
append	N/A
read	file:read

Permission	Description
setattr	file:setattr
swapon	N/A
write	Accès en écriture général; nécessaire pour ajouter ou supprimer
lock	file:lock
create	file:create
rename	file:rename
mouton	file:mouton
quotaon	N/A
relabelfrom	file:relabelfrom
link	N/A
search	Search access
rmdir	Supprimer un répertoire.
remove_name	Supprimer un fichier du répertoire.
reparent	Renommer un répertoire parent différent (.. change).
add_name	Ajouter un fichier dans le répertoire.
open	Ouvrir un répertoire.

fd

Permission	Description
use	Autorisation d'utiliser un descripteur de fichier hérité

fifo_file

Hérite de: common file

Permission	Description
getattr	file:getattr
relabelto	file:relabelto
unlink	file:unlink
ioctl	file:ioctl
execute	file:execute
append	file:append
read	file:read
setattr	file:setattr
swapon	file:swapon
write	file:write
lock	file:lock
create	file:create
rename	file:rename
mouton	file:mouton
quotaon	file:quotaon
relabelfrom	file:relabelfrom
link	file:link
open	Open a FIFO.

file

Hérite de: common file

Permission	Description
getattr	file:getattr
relabelto	file:relabelto
unlink	file:unlink
ioctl	file:ioctl
execute	file:execute
append	file:append
read	file:read
setattr	file:setattr
swapon	file:swapon
write	file:write
lock	file:lock
create	file:create
rename	file:rename
mouton	file:mouton
quotaon	file:quotaon
relabelfrom	file:relabelfrom
link	file:link
execute_no_trans	Exécuter un fichier dans le domaine des appelants.
entrypoint	Peut être exécuté comme point d'entrée du nouveau domaine dans une transition
execmod	Rendre exécutable un mappage de fichier qui a été modifié par copie sur écriture. (Relocalisation de texte)
open	Ouvrir un fichier.

filesystem

Permission	Description
mount	Montez le système de fichiers.
remount	Changer les indicateurs de montage du système de fichiers.
unmount	Démonter le système de fichiers.
getattr	Obtenir les attributs de fichier, tels que le mode d'accès. (par exemple, stat, certains ioctls. ...)
relabelfrom	Modifier le contexte de sécurité en fonction du type existant.
relabelto	Modifiez le contexte de sécurité en fonction du nouveau type.
transition	Transition vers un nouveau SID (changer le contexte de sécurité).
associate	Associer un fichier au système de fichiers.
quotamod	Modifier les informations de quota.
quotaget	Obtenir des informations sur les quotas

ipc

Hérite de: common ipc

Permission	Description
write	ipc:write
destroy	ipc:destroy
unix_write	ipc:unix_write
getattr	ipc:getattr
create	ipc:create
read	ipc:read
setattr	ipc:setattr
unix_read	ipc:unix_read
associate	ipc:associate

kernel_service

Permission	Description
use_as_override	Accorder à un processus le droit de désigner un autre ID de sécurité de processus à utiliser par le noyau en tant que substitution pour la sécurité subjective SELinux lors de l'accès à des éléments pour le compte d'un autre processus.
create_files_as	Accorder à un processus le droit de nommer une étiquette de création de fichier à utiliser par un service du noyau.

key

Permission	Description
view	
read	
write	
search	
link	
setattr	
create	

key_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind

Permission	Description
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind

Ink_file

Hérite de: common file

Permission	Description
getattr	file:getattr
relabelto	file:relabelto
unlink	file:unlink
ioctl	file:ioctl
execute	file:execute
append	file:append
read	file:read
setattr	file:setattr
swapon	file:swapon
write	file:write
lock	file:lock
create	file:create
rename	file:rename
mouton	file:mouton
quotaon	file:quotaon
relabelfrom	file:relabelfrom
link	file:link

memprotect

Permission	Description
mmap_zero	Mmap la première page de mémoire.

msg

Permission	Description
receive	Supprimer un message d'une file d'attente.
send	Ajouter un message à une file d'attente.

msgq

Hérite de: common ipc

Permission	Description
write	ipc:write
destroy	ipc:destroy
unix_write	ipc:unix_write
getattr	ipc:getattr
create	ipc:create
read	ipc:read
setattr	ipc:setattr
unix_read	ipc:unix_read
associate	ipc:associate
enqueue	Le message peut être ajouté à une file d'attente.

netif

Permission	Description
tcp_rcv	Receive TCP packet.
tcp_send	Send TCP packet.
udp_rcv	Receive UDP packet.
udp_send	Send UDP packet.
rawip_rcv	Receive raw IP packet.
rawip_send	Send raw IP packet.
dccp_rcv	Receive DCCP packet.
dccp_send	Send DCCP packet.
ingress	network_peer_controls
egress	network_peer_controls

netlink_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read

Permission	Description
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind

netlink_audit_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept

Permission	Description
name_bind	socket:name_bind
nlmsg_read	Lecture de l'état du sous-système d'audit (par exemple, AUDIT_GET).
nlmsg_write	Ecrire l'état du sous-système d'audit (par exemple, AUDIT_SET).
nlmsg_relay	Envoyer des messages d'audit d'espace utilisateur au système d'audit du noyau.
nlmsg_readpriv	Lire l'état du sous-système d'audit sensible à la sécurité.
nlmsg_tty_audit	Audit de contrôle TTY

netlink_dnrt_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind

netlink_firewall_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read

Permission	Description
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind
nlmsg_read	Read firewall configuration state.
nlmsg_write	Write firewall configuration state.

netlink_ip6fw_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto

Permission	Description
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind
nlmsg_read	Read netlink message.
nlmsg_write	Write netlink message.

netlink_kobject_uevent_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind

netlink_nflog_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto

Permission	Description
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind

netlink_route_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind

Permission	Description
nlmsg_read	Read route configuration state.
nlmsg_write	Write route configuration state.

netlink_selinux_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind

netlink_tcpdiag_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg

Permission	Description
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind
nlmsg_read	Read tcp diagnostics.
nlmsg_write	Unused.

netlink_xfrm_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind
nlmsg_read	Read xfrm configuration state.

Permission	Description
nlmsg_write	Write xfrm configuration state.

node

Permission	Description
tcp_rcv	Recevoir un paquet TCP.
tcp_send	Envoyer un paquet TCP.
udp_rcv	Recevoir un paquet UDP.
udp_send	Envoyer un paquet UDP.
rawip_rcv	Recevoir un paquet IP brut.
rawip_send	Envoyer un paquet IP brut.
enforce_dest	Assurez-vous que le nœud de destination peut appliquer des restrictions au socket de destination.
dccp_rcv	Recevoir un paquet DCCP.
dccp_send	Envoyer un paquet DCCP.
recvfrom	network_peer_controls
sendto	network_peer_controls

packet

Permission	Description
send	Envoyer un paquet.
receive	Recevoir un paquet.
relabelto	
flow_in	Deprecated
flow_out	Deprecated
forward_in	
forward_out	

packet_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl

Permission	Description
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind

peer

Permission	Description
recv	Recevoir d'un homologue de réseau étiqueté

process

Permission	Description
fork	Fork en deux processus.
transition	Transition vers un nouveau contexte sur exec().
sigchld	Envoyer le signal SIGCHLD.
sigkill	Envoyer un signal SIGKILL.
sigstop	Envoyer un signal SIGSTOP
signull	Vérifier l'existence d'un autre processus sans envoyer de signal
signal	Envoyez un signal autre que SIGKILL, SIGSTOP ou SIGCHLD.
ptrace	Joindre à un autre processus de traçage.
getsched	Obtenir la priorité d'un processus.
setsched	Définir la priorité d'un processus.
getsession	Obtenir l'identifiant de session d'un autre processus.
getpgid	Obtenir l'ID de processus de groupe d'un processus.
setpgid	Définir l'ID de processus de groupe d'un processus.
getcap	Obtenez des capacités Linux.
setcap	Définir les capacités de Linux.
partager	Autoriser le partage d'état avec un processus cloné ou créé
getattr	Obtenir les attributs d'un fichier.
setexec	Remplace le contexte par défaut pour le prochain exec().
setfscreate	Remplacez le contexte par défaut pour la création de fichier.
setrlimit	Changer les limites du processus.
noatsecure	Désactiver le nettoyage de l'environnement en mode sécurisé (AT_SECURE).
Siginh	Hériter du signal de l'appelant.
rlimitinh	Hériter des limites de ressources de l'appelant.
dyntransition	Transition dynamique vers un nouveau contexte.
setcurrent	Définir le contexte de processus actuel.

Permission	Description
execmem	Rendre exécutable un mappage anonyme ou un mappage de fichier privé accessible en écriture.
execstack	Rendre la pile de processus principale exécutable.
execheap	Rendre le tas exécutable.
setkeycreate	Remplacer le contexte par défaut pour la création de clé.
setsockcreate	Remplacer le contexte par défaut pour la création de socket.

rawip_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind
node_bind	Possibilité de se lier à un nœud.

security

Permission	Description
compute_user	Obtenir les informations sur l'utilisateur dans selinuxfs.
compute_relabel	Obtenir les informations de ré-étiquetage dans selinuxfs.
compute_create	Obtenir des informations de création dans selinuxfs.
compute_av	Calcule un vecteur d'accès à partir d'une source / cible / classe.
compute_membre	Détermine le contexte à utiliser lors de la sélection d'un membre d'un objet polyinstancié.

Permission	Description
setenforce	Changer l'état d'application de SELinux.
check_context	Ecrire le contexte dans selinuxfs.
load_policy	Charger la politique de sécurité.
setbool	Définir une valeur booléenne.
setseparam	Définir les paramètres de réglage du cache du vecteur d'accès au noyau.
setcheckreqprot	Défini si SELinux vérifie le mode de protection d'origine ou le mode de protection modifié (read-implique-exec) pour mmap / mprotect.

sem

Hérite de: common ipc

Permission	Description
write	ipc:write
destroy	ipc:destroy
unix_write	ipc:unix_write
getattr	ipc:getattr
create	ipc:create
read	ipc:read
setattr	ipc:setattr
unix_read	ipc:unix_read
associate	ipc:associate

shm

Hérite de: common ipc

Permission	Description
write	ipc:write
destroy	ipc:destroy
unix_write	ipc:unix_write
getattr	ipc:getattr
create	ipc:create
read	ipc:read
setattr	ipc:setattr
unix_read	ipc:unix_read
associate	ipc:associate
lock	(Un)lock page(s) in memory.

sock_file

Hérite de: common file

Permission	Description
getattr	file:getattr
relabelto	file:relabelto
unlink	file:unlink
ioctl	file:ioctl
execute	file:execute
append	file:append
read	file:read
setattr	file:setattr
swapon	file:swapon
write	file:write
lock	file:lock
create	file:create
rename	file:rename
mounton	file:mounton
quotaon	file:quotaon
relabelfrom	file:relabelfrom
link	file:link
open	Open a named socket file.

socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept

Permission	Description
name_bind	socket:name_bind

system

Permission	Description
ipc_info	Obtenir des informations pour un socket ipc.
syslog_mod	Effectuer une opération syslog autre que la journalisation syslog_read ou de la console.
syslog_read	Effectue une lecture syslog.
syslog_console	Effectuer la console syslog.

tcp_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind
connectto	Connect to server socket.
newconn	Create new socket for connection.
acceptfrom	Accept connection from client socket.
node_bind	Ability to bind to a node.
name_connect	Connect to a specific port number.

tun_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind

udp_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr

Permission	Description
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind
node_bind	Possibilité de se lier à un nœud.

unix_dgram_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind

unix_stream_socket

Hérite de: common socket

Permission	Description
append	socket:append
relabelfrom	socket:relabelfrom
create	socket:create
read	socket:read
sendto	socket:sendto
connect	socket:connect
recvfrom	socket:recvfrom
send_msg	socket:send_msg
bind	socket:bind
lock	socket:lock
ioctl	socket:ioctl
getattr	socket:getattr
write	socket:write
setopt	socket:setopt
getopt	socket:getopt
listen	socket:listen
setattr	socket:setattr
shutdown	socket:shutdown
relabelto	socket:relabelto
recv_msg	socket:recv_msg
accept	socket:accept
name_bind	socket:name_bind
connectto	Connectez-vous à la prise du serveur.
newconn	Créer un nouveau socket pour la connexion.
acceptfrom	Accepter la connexion du socket client.

Database Object Classes

db_blob

Hérite de: common database

Permission	Description
read	Read a blob.
write	Write a blob.
import	Import a blob.
export	Export a blob.

db_column

Hérite de: common database

Permission	Description
use	Deprecated
select	
update	
insert	

db_database

Hérite de: common database

Permission	Description
access	
install_module	
load_module	
get_param	Deprecated
set_param	Deprecated

db_procedure

Hérite de: common database

Permission	Description
execute	Execute a stored procedure.
entrypoint	
install	

db_table

Hérite de: common database

Permission	Description
use	Deprecated
select	
update	
insert	
delete	
lock	

db_tuple

Permission	Description
relabelfrom	
relabelto	
use	Deprecated
select	

Permission	Description
update	
insert	
delete	

DBus Object Classes

dbus

Permission	Description
acquire_svc	
send_msg	Envoyer un message sur le bus.

MLS Context Translation Object Classes

context

Permission	Description
translate	Traduire une étiquette MLS brute.
contains	Calculer un sous-ensemble MLS.

NSCD Object Classes

nscd

Permission	Description
getpwd	
getgrp	
gethost	
getstat	
admin	
shmempwd	
shmemgrp	
shmemhost	
getserv	
shmemserv	

Password Object Classes

passwd

Permission	Description
passwd	Mettre à jour le mot de passe de l'utilisateur.
chfn	Changer les informations de doigt. Par exemple, nom réel, salle de travail, téléphone et téléphone à la maison.
chsh	Changer le shell de connexion.
rootok	Autoriser la mise à jour si l'utilisateur est root et que le processus dispose de l'autorisation rootok PAM.
crontab	crontab sur un autre utilisateur.

X Server Object Classes

x_application_data

Permission	Description
paste	
paste_after_confirm	
copy	

x_client

Permission	Description
destroy	Ferme un client.
getattr	Obtenir les attributs d'un client X
setattr	Définir les attributs d'un client X
manage	

x_colormap

Permission	Description
create	Créer une nouvelle palette de couleurs.
destroy	Libérer une palette de couleurs.
read	Lire les cellules de couleur de la palette de couleurs.
write	
getattr	Obtenir la gamme de couleurs d'un écran.
add_color	
remove_color	
install	Copier une palette de couleurs virtuelle dans le matériel d'affichage.
uninstall	Supprimer une palette de couleurs virtuelle du matériel d'affichage.
use	

x_cursor

Permission	Description
create	Créer un objet curseur arbitraire.
destroy	Supprimer un objet curseur.
read	
write	
getattr	Obtenir les attributs du curseur.
setattr	Définir les attributs du curseur.
use	Associer un objet curseur à une fenêtre.

x_device

Hérite de: common x_device

Permission	Description
getattr	x_device: getattr
setattr	x_device: setattr
use	x_device: use
read	x_device: read
write	x_device: write
getfocus	x_device: getfocus
setfocus	x_device: setfocus
bell	x_device: bell
force_cursor	x_device: force_cursor
freeze	x_device: freeze
grab	x_device: grab
manage	x_device: manage
list_property	x_device: list_property
get_property	x_device: get_property
set_property	x_device: set_property
add	x_device: add
remove	x_device: remove

x_drawable

Permission	Description
create	Créer un objet Drawable.
destroy	Détruire un Drawable.
read	
write	
blend	
getattr	Obtenir les attributs d'un objet Drawable
setattr	Définir les attributs d'un objet Drawable
list_child	
add_child	
remove_child	
list_property	

Permission	Description
get_property	
set_property	
manage	
override	
show	
hide	
send	
receive	

x_event

Permission	Description
send	
receive	

x_extension

Permission	Description
query	
use	

x_font

Permission	Description
create	Charger une police.
destroy	Libérer (déréférencer) une police.
getattr	
add_glyph	
remove_glyph	
use	Utiliser une police pour dessiner.

x_gc

Permission	Description
create	Créer un objet Contextes graphiques.
destroy	Libérer (déréférencer) un objet Graphics Contexts.
getattr	Obtient les attributs de l'objet Contextes graphiques.
setattr	Définissez les attributs de l'objet Contextes graphiques.
use	

x_keyboard

Hérite de: common x_device

Permission	Description
getattr	x_device: getattr
setattr	x_device: setattr
use	x_device: use
read	x_device: read
write	x_device: write
getfocus	x_device: getfocus
setfocus	x_device: setfocus
bell	x_device: bell
force_cursor	x_device: force_cursor
freeze	x_device: freeze
grab	x_device: grab
manage	x_device: manage
list_property	x_device: list_property
get_property	x_device: get_property
set_property	x_device: set_property
add	x_device: add
remove	x_device: remove

x_pointer

Hérite de: common x_device

Permission	Description
getattr	x_device: getattr
setattr	x_device: setattr
use	x_device: use
read	x_device: read
write	x_device: write
getfocus	x_device: getfocus
setfocus	x_device: setfocus
bell	x_device: bell
force_cursor	x_device: force_cursor
freeze	x_device: freeze
grab	x_device: grab
manage	x_device: manage
list_property	x_device: list_property
get_property	x_device: get_property
set_property	x_device: set_property
add	x_device: add
remove	x_device: remove

x_property

Permission	Description
create	Créer un objet de propriété.

Permission	Description
destroy	Libérer (déréférencer) un objet de propriété.
read	Lire une propriété.
write	Ecrire une propriété.
append	Ajouter une propriété.
getattr	Obtenir les attributs d'une propriété.
setattr	Définir les attributs d'une propriété.

x_resource

Permission	Description
read	
write	

x_screen

Permission	Description
getattr	
setattr	
hide_cursor	
show_cursor	
saver_getattr	
saver_setattr	
saver_hide	
saver_show	

x_selection

Permission	Description
read	
write	
getattr	
setattr	

x_server

Permission	Description
getattr	
setattr	
record	
debug	
grab	
manage	

x_synthetic_event

Permission	Description
send	
receive	
Navigation menu	

From:

<http://www.ouarte.garden/> - **dwndoc**

Permanent link:

<http://www.ouarte.garden/doku.php?id=securite:selinux-policy-classes>

Last update: **2025/02/19 10:59**

