

BLX SELinux Policy

```
module BLX_SELinux_Policy 1.0;

require {
    type ssh_port_t;
    type hwdata_t;
    type device_t;
    type sound_device_t;
    type auditd_t;
    type rpm_script_tmp_t;
    type afs3_callback_port_t;
    type init_t;
    type lsmd_t;
    type tmp_t;
    type snmp_port_t;
    type chronyd_t;
    type http_port_t;
    type kubernetes_port_t;
    type modemmanager_t;
    type devicekit_power_t;
    type cupsd_t;
    type etc_t;
    type avahi_t;
    type event_device_t;
    type systemd_logind_t;
    type complex_main_port_t;
    type jboss_management_port_t;
    type iscsid_t;
    type kmsg_device_t;
    type systemd_hwdb_etc_t;
    type udev_t;
    type crond_t;
    type devicekit_disk_t;
    type colord_var_lib_t;
    type autofs_device_t;
    type wireless_device_t;
    type ntop_port_t;
    type udev_var_run_t;
    type systemd_coredump_t;
    type root_t;
    type rtkit_daemon_t;
    type user_home_t;
}
```

```

type afs_pt_port_t;
type accountsd_t;
type xdm_t;
type sshd_t;
type ephemeral_port_t;
type lsmd_var_run_t;
type auditd_log_t;
type zebra_port_t;
type unreserved_port_t;
type rhsmcertd_lock_t;
type rpm_t;
type system_dbusd_tmpfs_t;
type crond_var_run_t;
type unconfined_t;
type syslogd_var_run_t;
type dri_device_t;
type policykit_t;
type syslogd_t;
type tmpfs_t;
type complex_link_port_t;
type firewalld_tmpfs_t;
type kernel_t;
type system_dbusd_t;
type init_var_run_t;
type setroubleshootd_t;
type nsfs_t;
type lvm_t;
type var_log_t;
type mcelog_t;
type NetworkManager_t;
type colord_t;
type firewalld_t;
type setroubleshoot_tmpfs_t;
type var_t;
type unconfined_service_t;
type bin_t;
type unconfined_dbusd_t;
type ifconfig_t;
type sssd_t;
type admin_home_t;
type hugetlbfs_t;
type default_t;
class file { append create execute execute_no_trans
getattr ioctl map open read rename setattr unlink write };
class process { execmem execstack setrlimit };

```

```

class capability { dac_override dac_read_search kill
net_bind_service setgid setuid sys_nice sys_resource };
class tcp_socket { accept getattr listen name_bind
name_connect };
class cap_userns sys_ptrace;
class packet_socket { getattr map };
class fifo_file { getattr open };
class dir { add_name create read remove_name setattr
write };
class sock_file { create getattr setattr unlink write };
class filesystem getattr;
class udp_socket { getattr name_bind };
class chr_file getattr;
class netlink_audit_socket getattr;
class netlink_kobject_uevent_socket getattr;
class unix_dgram_socket getattr;
class unix_stream_socket getattr;
class netlink_route_socket getattr;
class qipctr_socket getattr;
class netlink_netfilter_socket getattr;
class netlink_generic_socket getattr;
class rawip_socket getattr;
}

```

```

#===== ifconfig_t =====
allow ifconfig_t NetworkManager_t:netlink_generic_socket
getattr;
allow ifconfig_t
NetworkManager_t:netlink_kobject_uevent_socket getattr;
allow ifconfig_t NetworkManager_t:netlink_route_socket
getattr;
allow ifconfig_t NetworkManager_t:packet_socket getattr;
allow ifconfig_t NetworkManager_t:rawip_socket getattr;
allow ifconfig_t NetworkManager_t:udp_socket getattr;
allow ifconfig_t NetworkManager_t:unix_dgram_socket
getattr;
allow ifconfig_t NetworkManager_t:unix_stream_socket
getattr;
allow ifconfig_t accountsd_t:unix_stream_socket getattr;
allow ifconfig_t admin_home_t:file { execute execute_no_trans
ioctl open read };
allow ifconfig_t afs3_callback_port_t:tcp_socket { name_bind
name_connect };
allow ifconfig_t afs_pt_port_t:tcp_socket name_bind;
allow ifconfig_t auditd_log_t:file getattr;

```

```

allow ifconfig_t auditd_t:netlink_audit_socket getattr;
allow ifconfig_t auditd_t:unix_dgram_socket getattr;
allow ifconfig_t auditd_t:unix_stream_socket getattr;
allow ifconfig_t autofs_device_t:chr_file getattr;
allow ifconfig_t avahi_t:netlink_route_socket getattr;
allow ifconfig_t avahi_t:udp_socket getattr;
allow ifconfig_t avahi_t:unix_dgram_socket getattr;
allow ifconfig_t avahi_t:unix_stream_socket getattr;
allow ifconfig_t bin_t:dir { add_name remove_name write };
allow ifconfig_t bin_t:file { append create rename setattr unlink
write };
allow ifconfig_t chronyd_t:udp_socket getattr;
allow ifconfig_t chronyd_t:unix_dgram_socket getattr;
allow ifconfig_t colord_t:netlink_kobject_uevent_socket
getattr;
allow ifconfig_t colord_t:unix_dgram_socket getattr;
allow ifconfig_t colord_t:unix_stream_socket getattr;
allow ifconfig_t colord_var_lib_t:file getattr;
allow ifconfig_t complex_link_port_t:tcp_socket
name_connect;
allow ifconfig_t complex_main_port_t:tcp_socket
name_connect;
allow ifconfig_t crond_t:unix_dgram_socket getattr;
allow ifconfig_t crond_var_run_t:file getattr;
allow ifconfig_t cupsd_t:fifo_file getattr;
allow ifconfig_t cupsd_t:tcp_socket getattr;
allow ifconfig_t cupsd_t:unix_dgram_socket getattr;
allow ifconfig_t cupsd_t:unix_stream_socket getattr;
allow ifconfig_t default_t:file { getattr open read };
allow ifconfig_t device_t:filesystem getattr;
allow ifconfig_t
devicekit_disk_t:netlink_kobject_uevent_socket getattr;
allow ifconfig_t devicekit_disk_t:unix_dgram_socket getattr;
allow ifconfig_t devicekit_disk_t:unix_stream_socket getattr;
allow ifconfig_t
devicekit_power_t:netlink_kobject_uevent_socket getattr;
allow ifconfig_t devicekit_power_t:unix_stream_socket getattr;
allow ifconfig_t dri_device_t:chr_file getattr;

#!!!! This avc can be allowed using the boolean 'nis_enabled'
allow ifconfig_t ephemeral_port_t:tcp_socket name_connect;
allow ifconfig_t etc_t:dir { add_name remove_name write };
allow ifconfig_t etc_t:file unlink;
allow ifconfig_t event_device_t:chr_file getattr;
allow ifconfig_t firewalld_t:netlink_netfilter_socket getattr;

```

```
allow ifconfig_t firewalld_t:unix_stream_socket getattr;
allow ifconfig_t firewalld_tmpfs_t:file getattr;
```

```
#!!!! This avc can be allowed using the boolean 'nis_enabled'
allow ifconfig_t http_port_t:tcp_socket name_connect;
allow ifconfig_t http_port_t:tcp_socket name_bind;
allow ifconfig_t hugetlbf_t:filesystem getattr;
allow ifconfig_t hwdata_t:file { getattr open read };
allow ifconfig_t init_t:netlink_audit_socket getattr;
allow ifconfig_t init_t:netlink_kobject_uevent_socket getattr;
allow ifconfig_t init_t:unix_dgram_socket getattr;
allow ifconfig_t init_var_run_t:file { getattr open read };
allow ifconfig_t iscsid_t:unix_stream_socket getattr;
allow ifconfig_t jboss_management_port_t:tcp_socket
name_bind;
allow ifconfig_t kernel_t:unix_dgram_socket getattr;
```

```
#!!!! This avc can be allowed using the boolean
'domain_can_write_kmsg'
allow ifconfig_t kmsg_device_t:chr_file getattr;
allow ifconfig_t kubernetes_port_t:tcp_socket { name_bind
name_connect };
allow ifconfig_t lsmd_t:unix_stream_socket getattr;
allow ifconfig_t lsmd_var_run_t:file getattr;
allow ifconfig_t lvm_t:unix_stream_socket getattr;
allow ifconfig_t mcelog_t:unix_stream_socket getattr;
allow ifconfig_t
modemmanager_t:netlink_kobject_uevent_socket getattr;
allow ifconfig_t modemmanager_t:qipcrt_socket getattr;
allow ifconfig_t modemmanager_t:unix_dgram_socket getattr;
allow ifconfig_t modemmanager_t:unix_stream_socket getattr;
allow ifconfig_t nsfs_t:filesystem getattr;
allow ifconfig_t ntop_port_t:tcp_socket { name_bind
name_connect };
allow ifconfig_t policykit_t:unix_dgram_socket getattr;
allow ifconfig_t policykit_t:unix_stream_socket getattr;
allow ifconfig_t rhsmcertd_lock_t:file getattr;
allow ifconfig_t root_t:dir { add_name remove_name setattr
write };
allow ifconfig_t root_t:file { append create ioctl open unlink
write };
allow ifconfig_t rpm_script_tmp_t:dir setattr;
allow ifconfig_t rpm_t:netlink_route_socket getattr;
allow ifconfig_t rpm_t:unix_dgram_socket getattr;
allow ifconfig_t rpm_t:unix_stream_socket getattr;
```

```
allow ifconfig_t rtkit_daemon_t:unix_dgram_socket getattr;
allow ifconfig_t rtkit_daemon_t:unix_stream_socket getattr;
allow ifconfig_t self:cap_usersns sys_ptrace;
allow ifconfig_t self:capability { dac_override dac_read_search
kill net_bind_service setgid setuid sys_nice sys_resource };
allow ifconfig_t self:packet_socket map;
allow ifconfig_t self:process { execmem execstack setrlimit };
```

```
#!!!! This avc can be allowed using the boolean 'nis_enabled'
allow ifconfig_t self:tcp_socket { accept listen };
allow ifconfig_t setroubleshoot_tmpfs_t:file getattr;
allow ifconfig_t setroubleshootd_t:unix_dgram_socket getattr;
allow ifconfig_t setroubleshootd_t:unix_stream_socket getattr;
allow ifconfig_t snmp_port_t:udp_socket name_bind;
allow ifconfig_t sound_device_t:chr_file getattr;
allow ifconfig_t ssh_port_t:tcp_socket name_bind;
allow ifconfig_t sshd_t:tcp_socket getattr;
allow ifconfig_t sshd_t:unix_dgram_socket getattr;
allow ifconfig_t sssd_t:unix_stream_socket getattr;
allow ifconfig_t syslogd_t:unix_dgram_socket getattr;
allow ifconfig_t syslogd_t:unix_stream_socket getattr;
allow ifconfig_t syslogd_var_run_t:file getattr;
allow ifconfig_t system_dbusd_t:netlink_audit_socket getattr;
allow ifconfig_t system_dbusd_t:unix_dgram_socket getattr;
allow ifconfig_t system_dbusd_t:unix_stream_socket getattr;
allow ifconfig_t system_dbusd_tmpfs_t:file getattr;
allow ifconfig_t systemd_coredump_t:unix_stream_socket
getattr;
allow ifconfig_t systemd_hwdb_etc_t:file getattr;
allow ifconfig_t
systemd_logind_t:netlink_kobject_uevent_socket getattr;
allow ifconfig_t systemd_logind_t:unix_dgram_socket getattr;
allow ifconfig_t systemd_logind_t:unix_stream_socket getattr;
allow ifconfig_t tmp_t:dir { add_name read remove_name write
};
allow ifconfig_t tmp_t:fifo_file open;
allow ifconfig_t tmp_t:file { create execute execute_no_trans
rename unlink };
```

```
#!!!! This avc can be allowed using the boolean
'domain_can_mmap_files'
allow ifconfig_t tmp_t:file map;
allow ifconfig_t tmp_t:sock_file { create getattr setattr unlink
write };
allow ifconfig_t tmpfs_t:file { getattr open read write };
```

```

#!!!! This avc can be allowed using the boolean
'domain_can_mmap_files'
allow ifconfig_t tmpfs_t:file map;
allow ifconfig_t tmpfs_t:filesystem getattr;
allow ifconfig_t udev_t:netlink_kobject_uevent_socket getattr;
allow ifconfig_t udev_t:unix_dgram_socket getattr;
allow ifconfig_t udev_t:unix_stream_socket getattr;
allow ifconfig_t udev_var_run_t:file { getattr open read };
allow ifconfig_t unconfined_dbusd_t:unix_dgram_socket
getattr;
allow ifconfig_t unconfined_dbusd_t:unix_stream_socket
getattr;
allow ifconfig_t
unconfined_service_t:netlink_kobject_uevent_socket getattr;
allow ifconfig_t unconfined_service_t:unix_stream_socket
getattr;
allow ifconfig_t unconfined_t:netlink_kobject_uevent_socket
getattr;
allow ifconfig_t unconfined_t:unix_dgram_socket getattr;

```

```

#!!!! This avc can be allowed using the boolean 'nis_enabled'
allow ifconfig_t unreserved_port_t:tcp_socket { name_bind
name_connect };
allow ifconfig_t var_log_t:dir { add_name remove_name write };
allow ifconfig_t var_log_t:file { create open unlink };

```

```

#!!!! This avc can be allowed using the boolean
'domain_can_mmap_files'
allow ifconfig_t var_log_t:file map;
allow ifconfig_t var_t:dir { add_name create read remove_name
setattr write };
allow ifconfig_t var_t:file { create open rename setattr unlink };
allow ifconfig_t wireless_device_t:chr_file getattr;
allow ifconfig_t xdm_t:netlink_kobject_uevent_socket getattr;
allow ifconfig_t xdm_t:unix_dgram_socket getattr;
allow ifconfig_t zebra_port_t:tcp_socket { name_bind
name_connect };

```

```

#===== init_t =====
allow init_t admin_home_t:file { execute execute_no_trans
ioctl open read };
allow init_t user_home_t:file { append open };

```