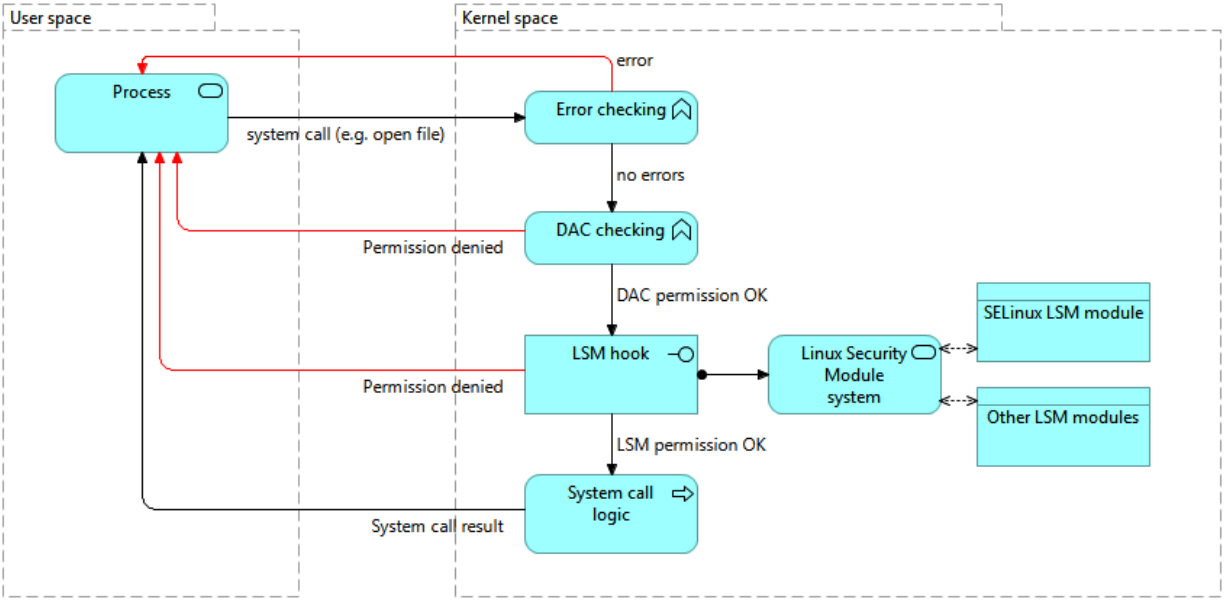
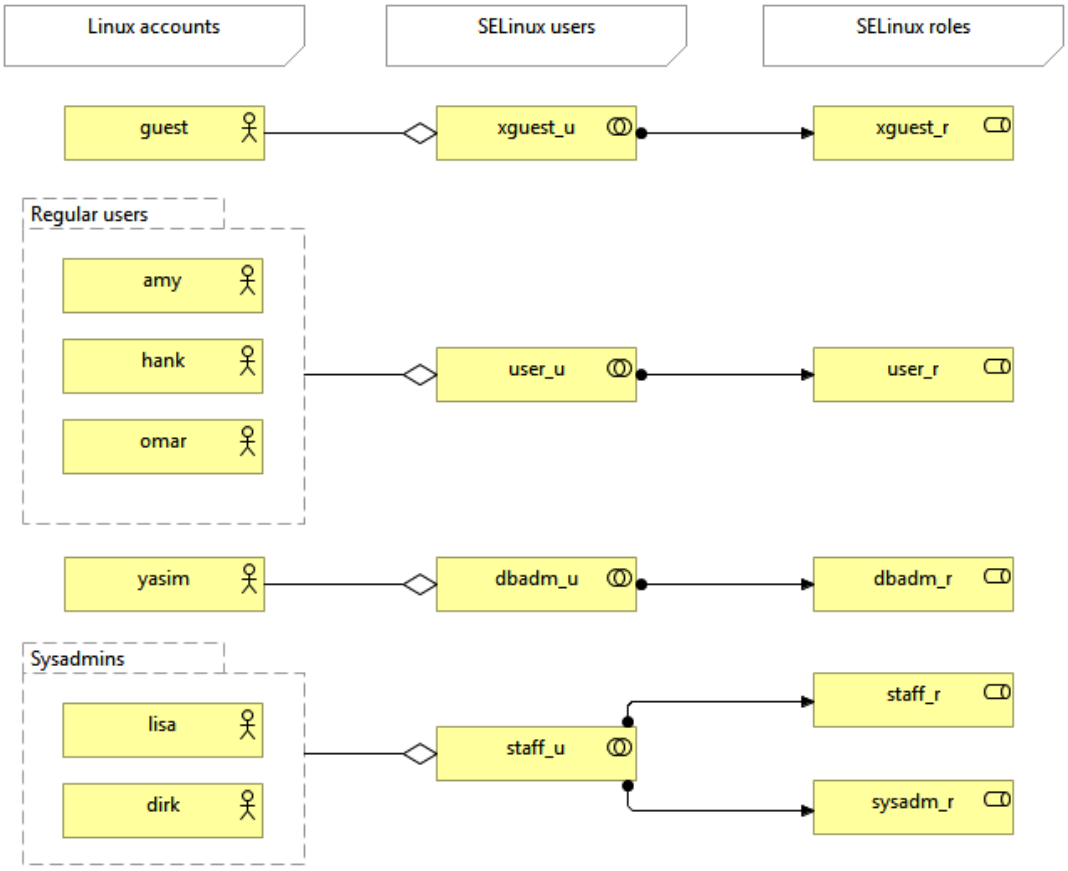
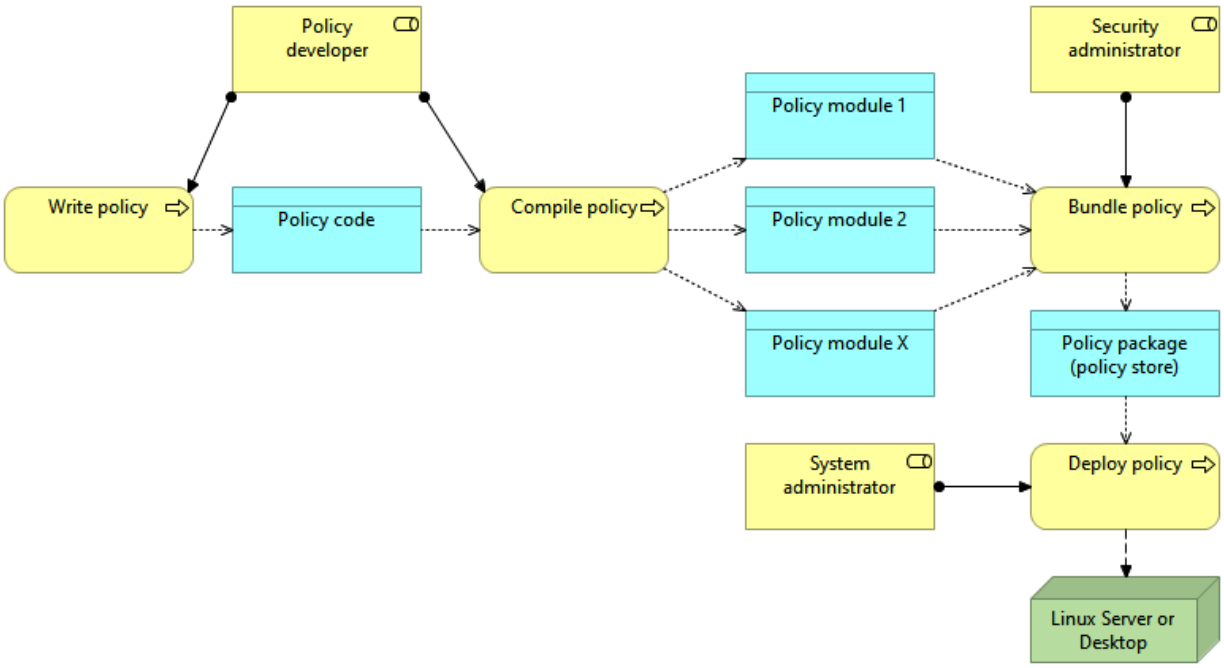
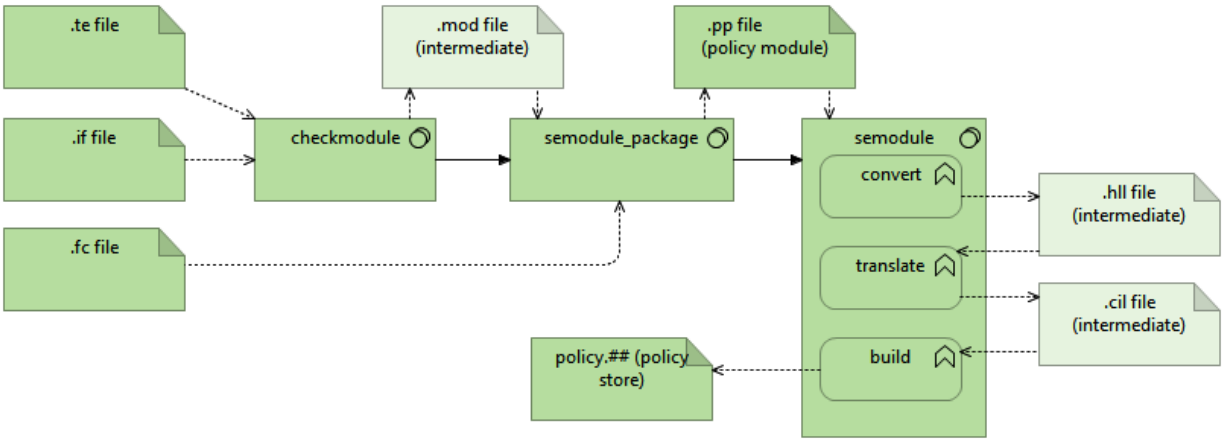
# Chapter 1: Fundamental SELinux Concepts

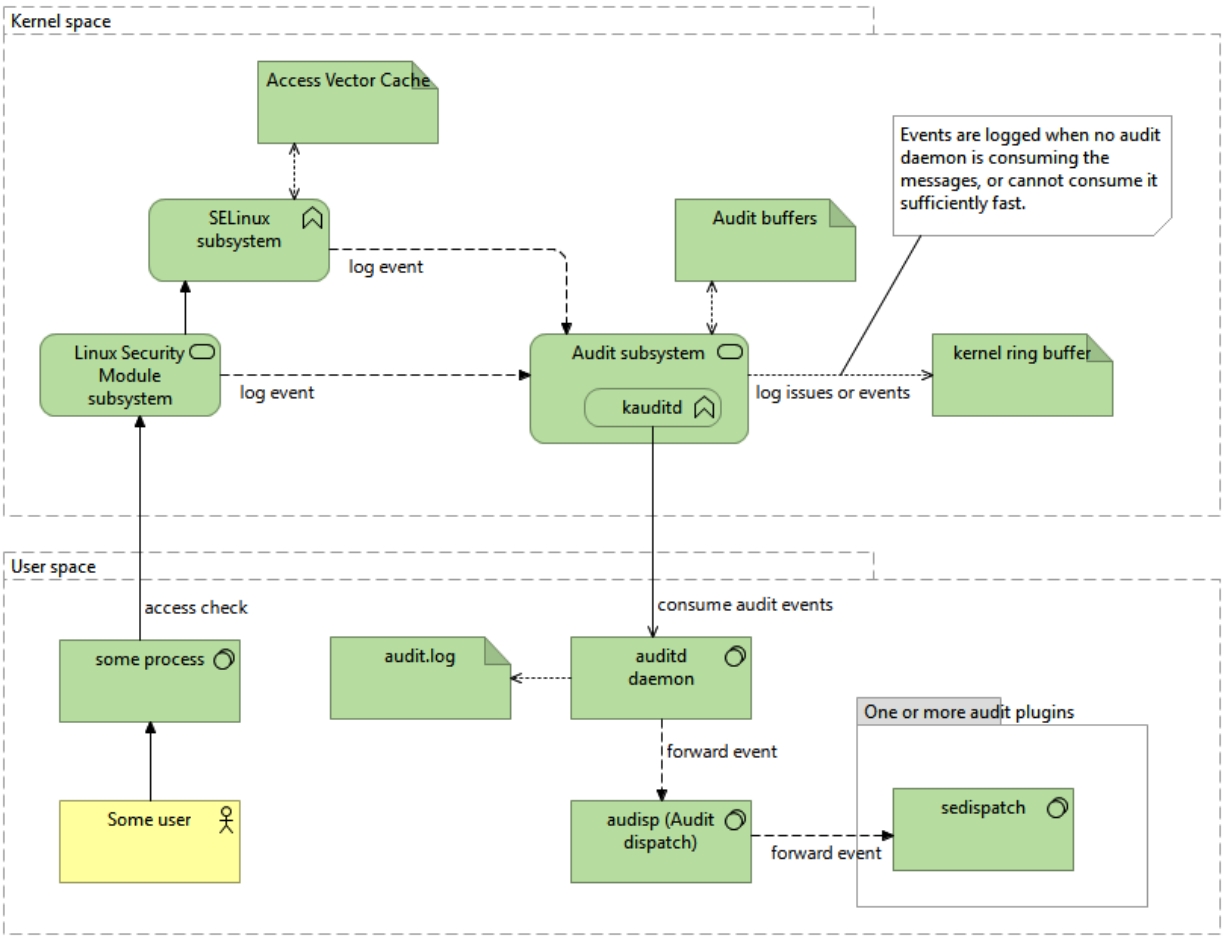


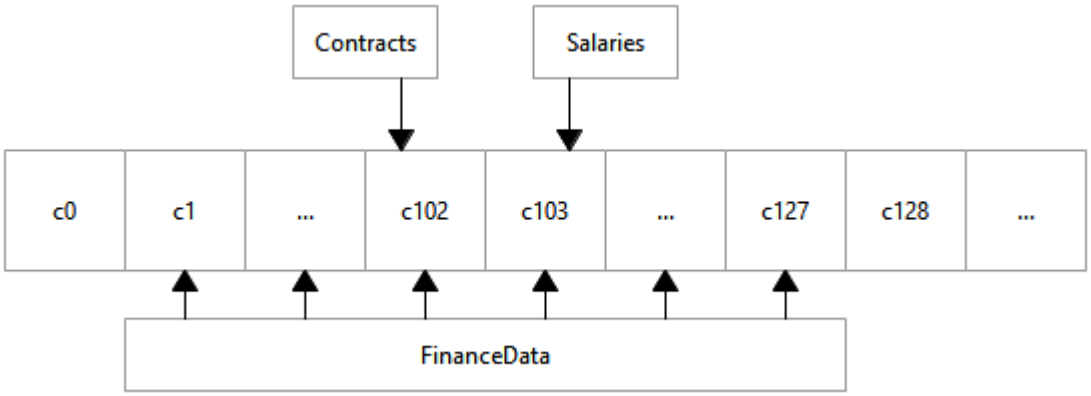

Policy developer
Security administrator
Policy module 1
Write policy
Policy code
Compile policy
Policy module 2
Bundle policy
Policy module X
Policy package (policy store)
System administrator
Deploy policy
Linux Server or Desktop


.te file
.mod file (intermediate)
.pp file (policy module)
.if file
checkmodule
semodule_package
semodule
convert
.hll file (intermediate)
.fc file
translate
.cil file (intermediate)
build
policy.## (policy store)

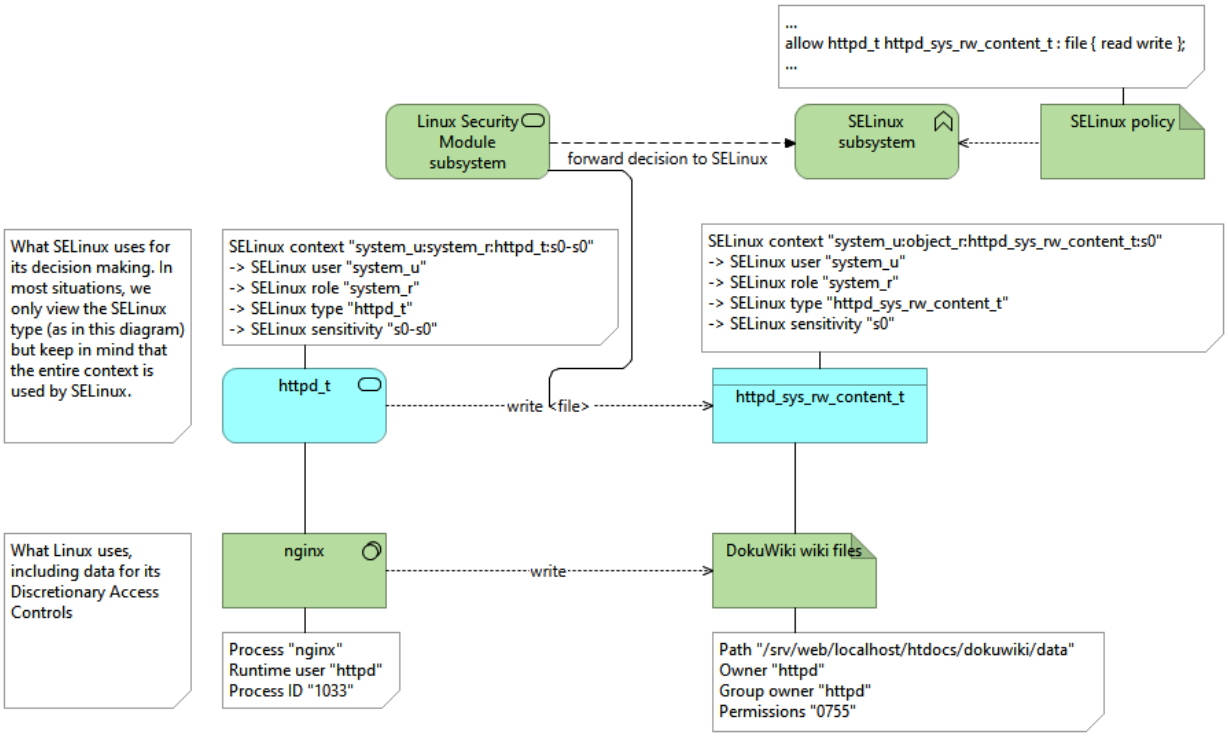
# Chapter 2: Understanding SELinux Decisions and Logging

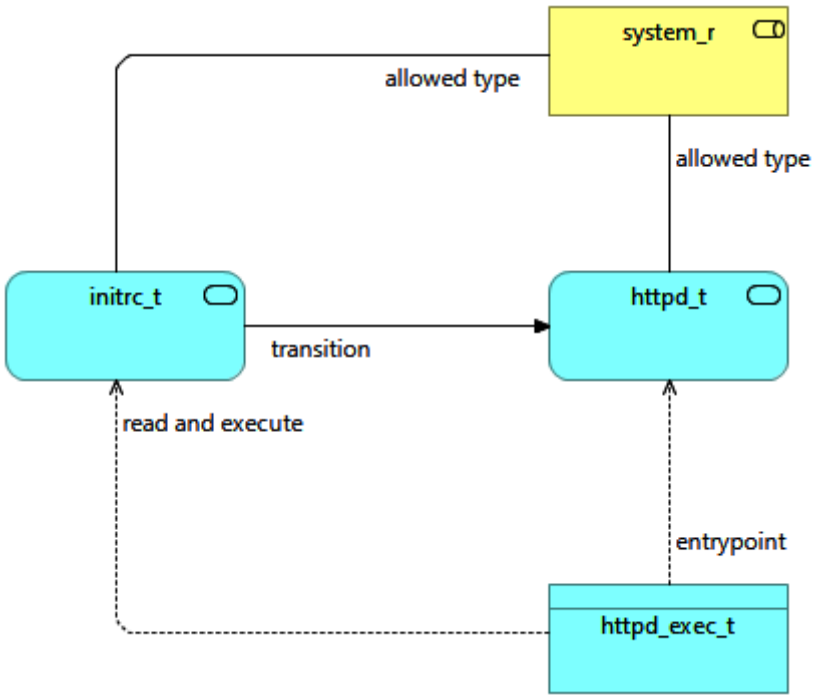


# Chapter 3: Managing User Logins

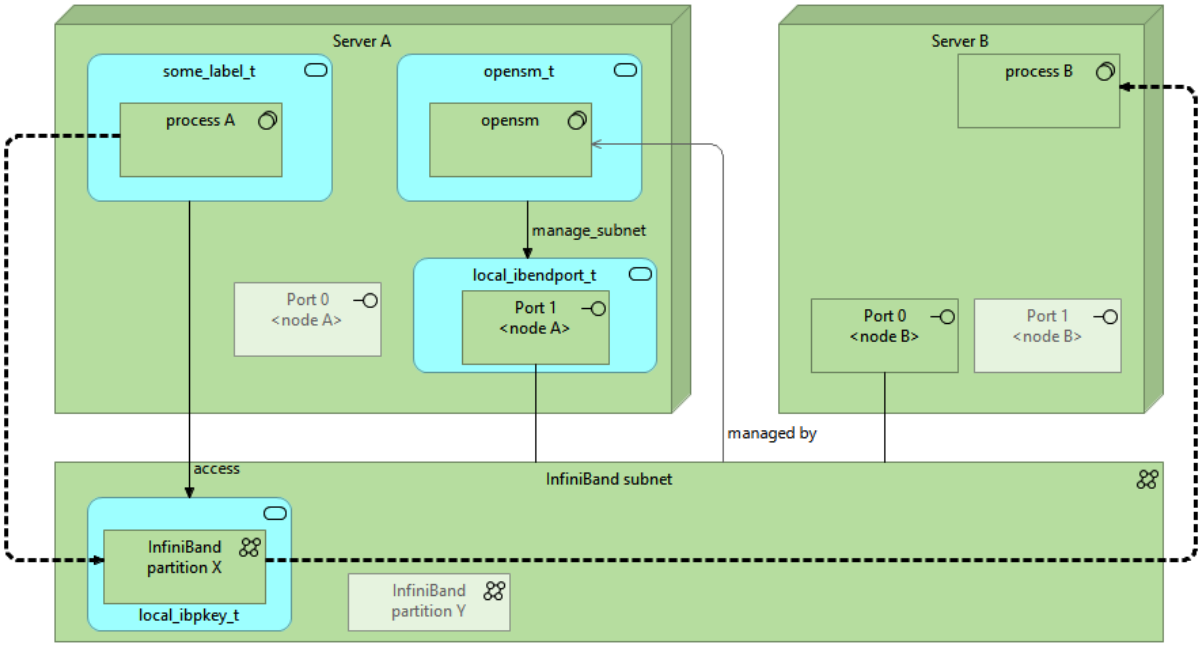


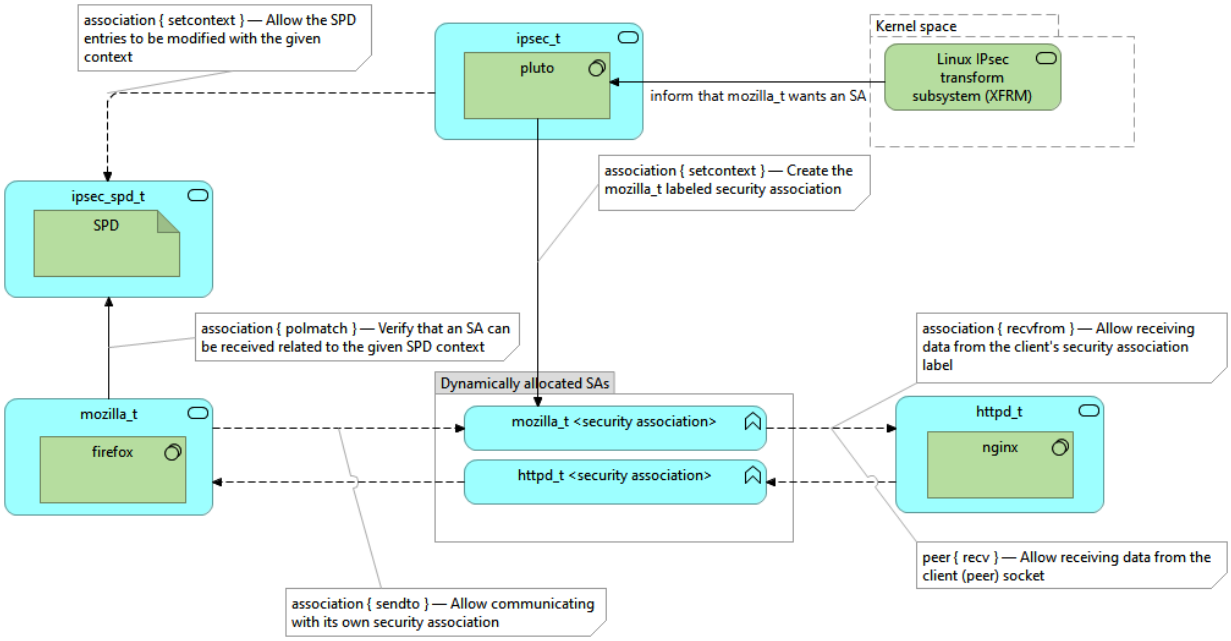
# Chapter 4: Using File Contexts and Process Domains

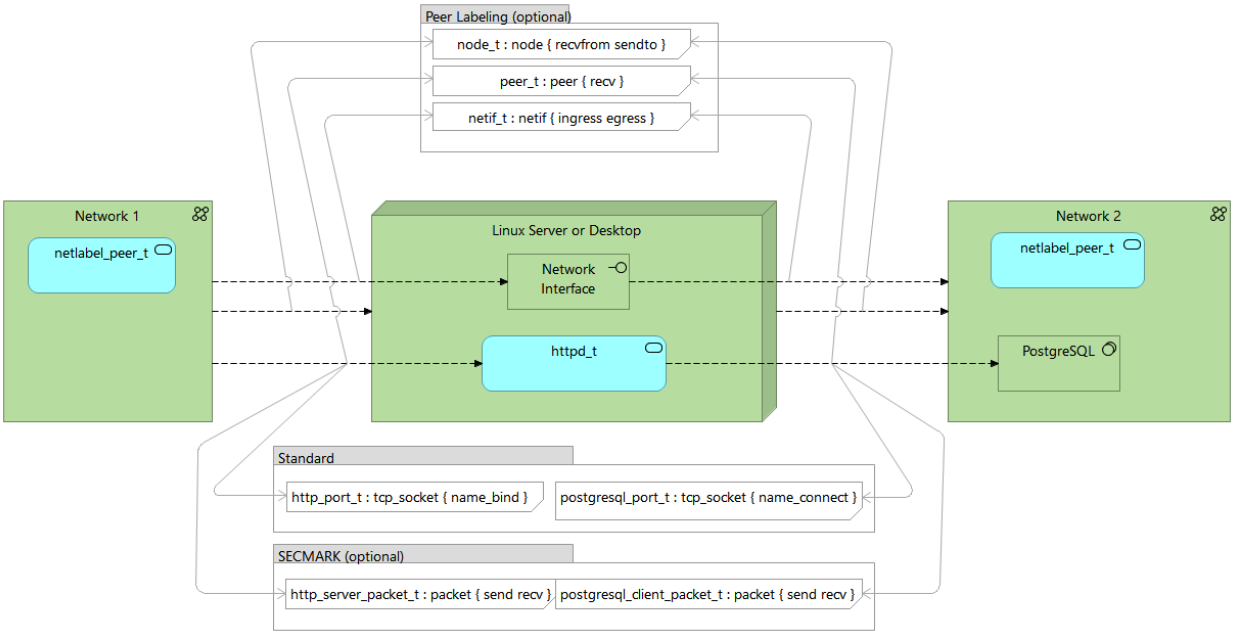


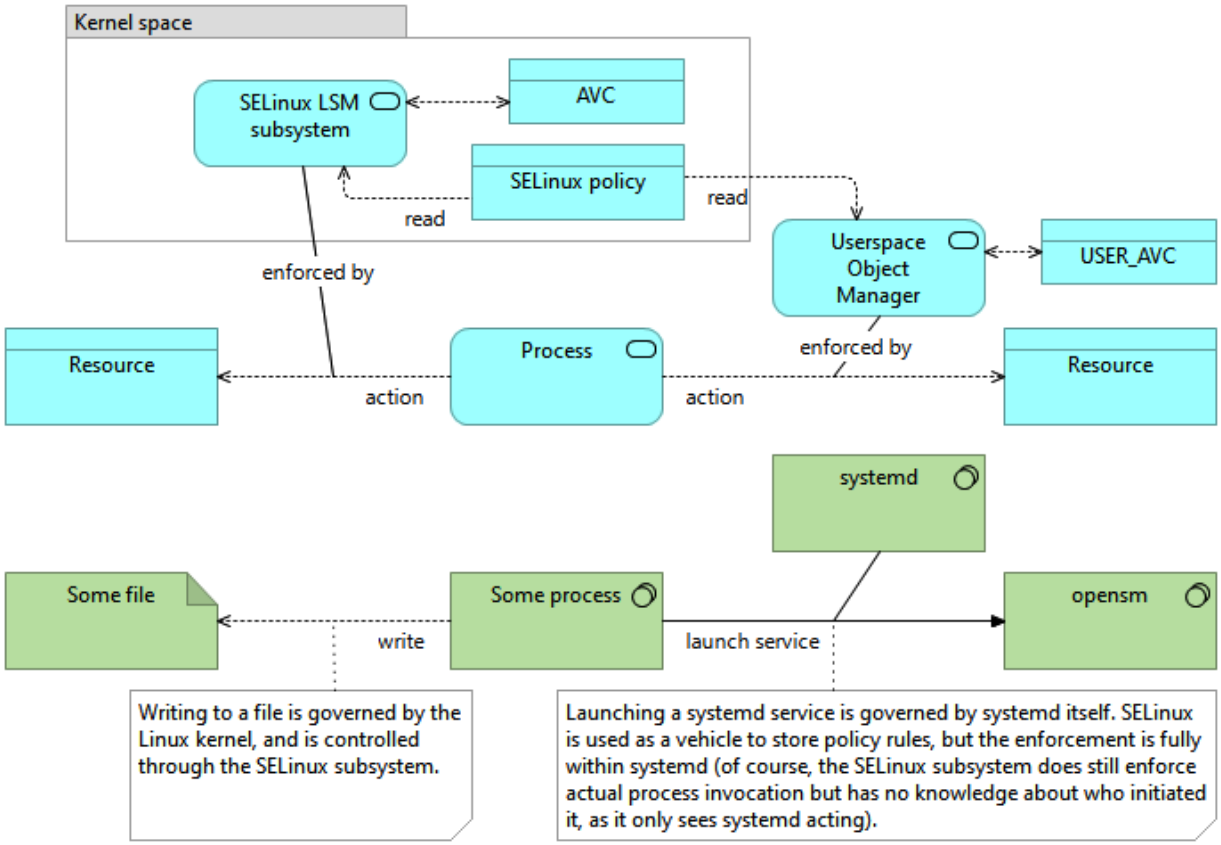
# Chapter 5: Controlling Network Communications



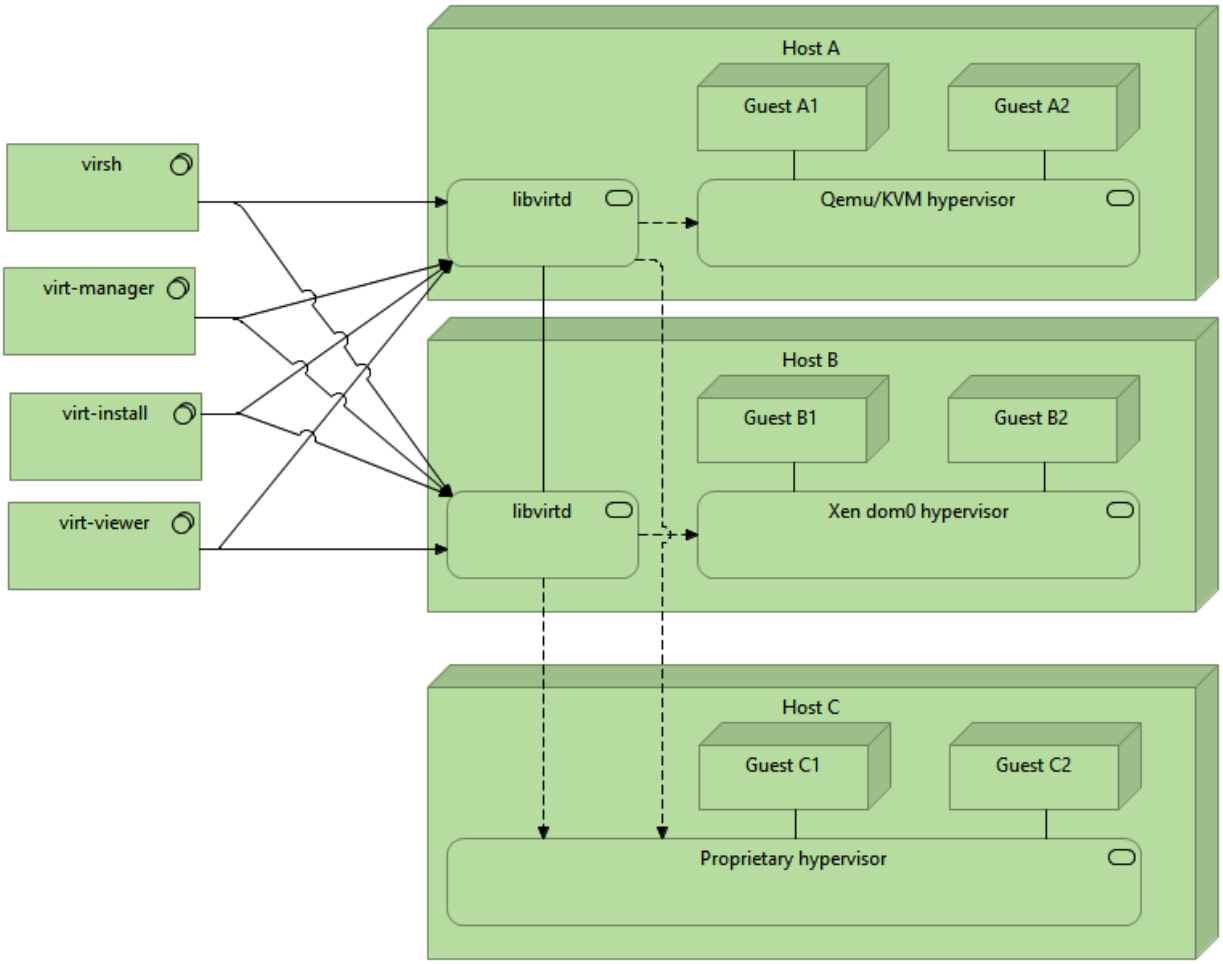




Peer Labeling (optional)
node_t : node { recvfrom sendto }
peer_t : peer { recv }
netif_t : netif { ingress egress }
Network 1
netlabel_peer_t
Linux Server or Desktop
Network Interface
httpd_t
Network 2
netlabel_peer_t
PostgreSQL
Standard
http_port_t : tcp_socket { name_bind }
postgresql_port_t : tcp_socket { name_connect }
SECMARK (optional)
http_server_packet_t : packet { send recv }
postgresql_client_packet_t : packet { send recv }

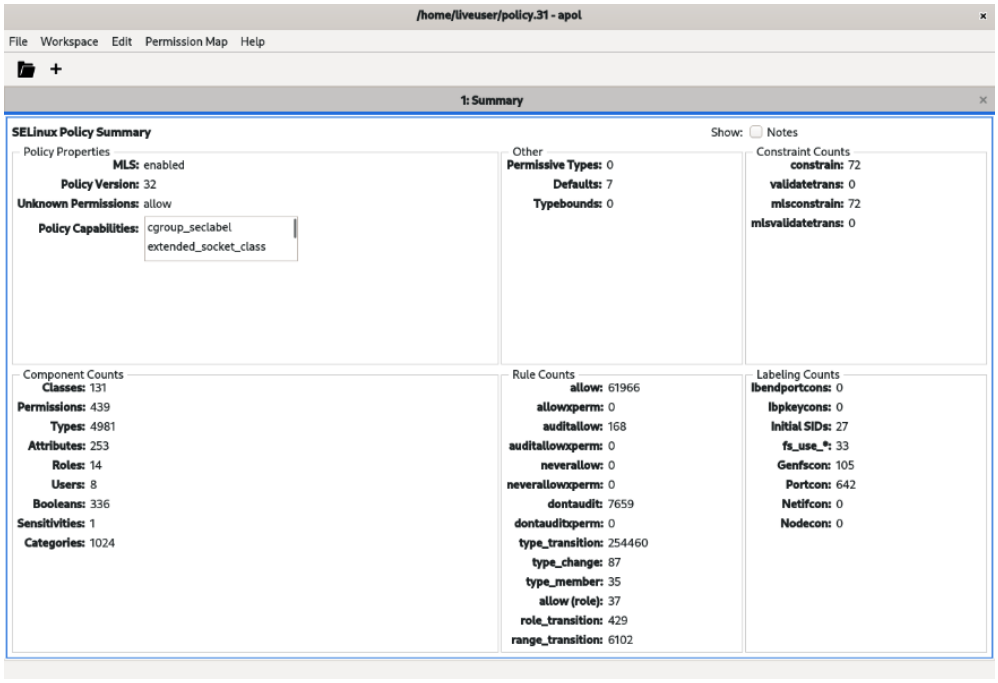
# Chapter 7: Configuring Application-Specific SELinux Controls

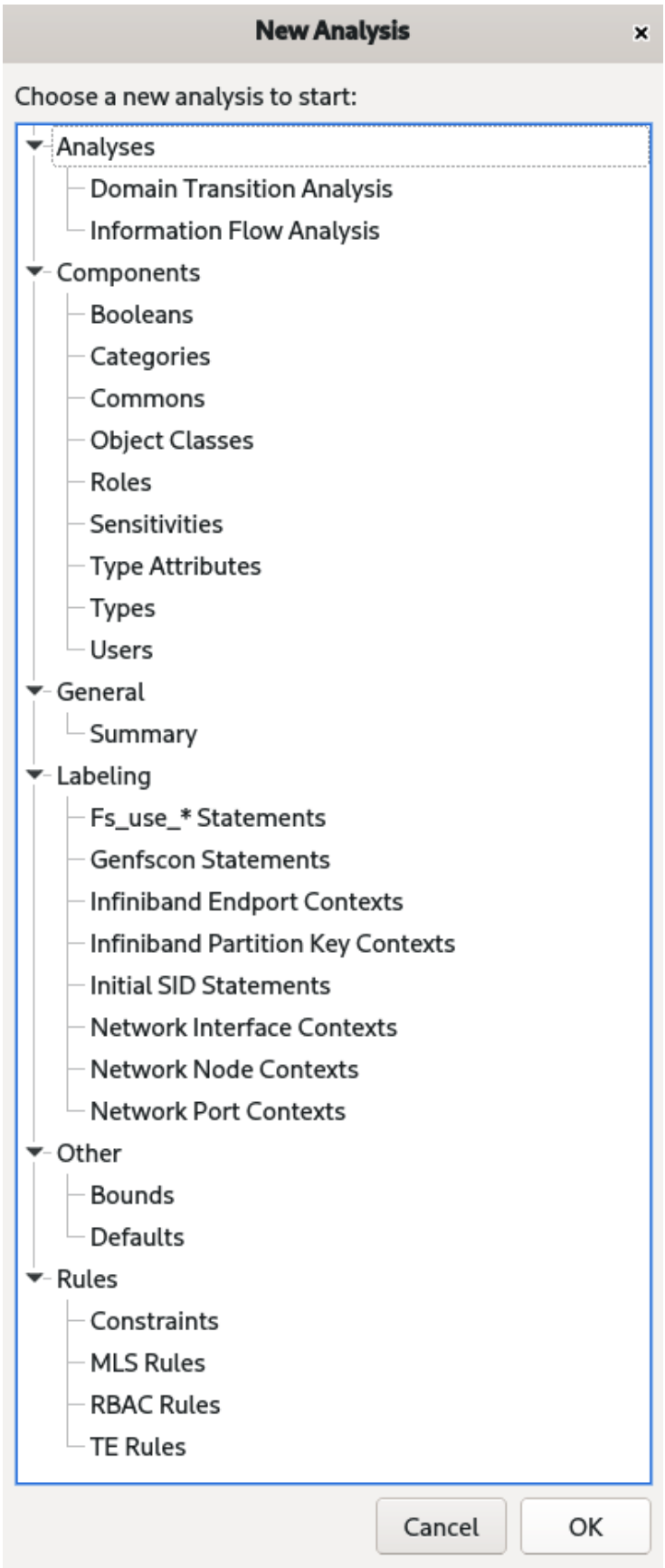


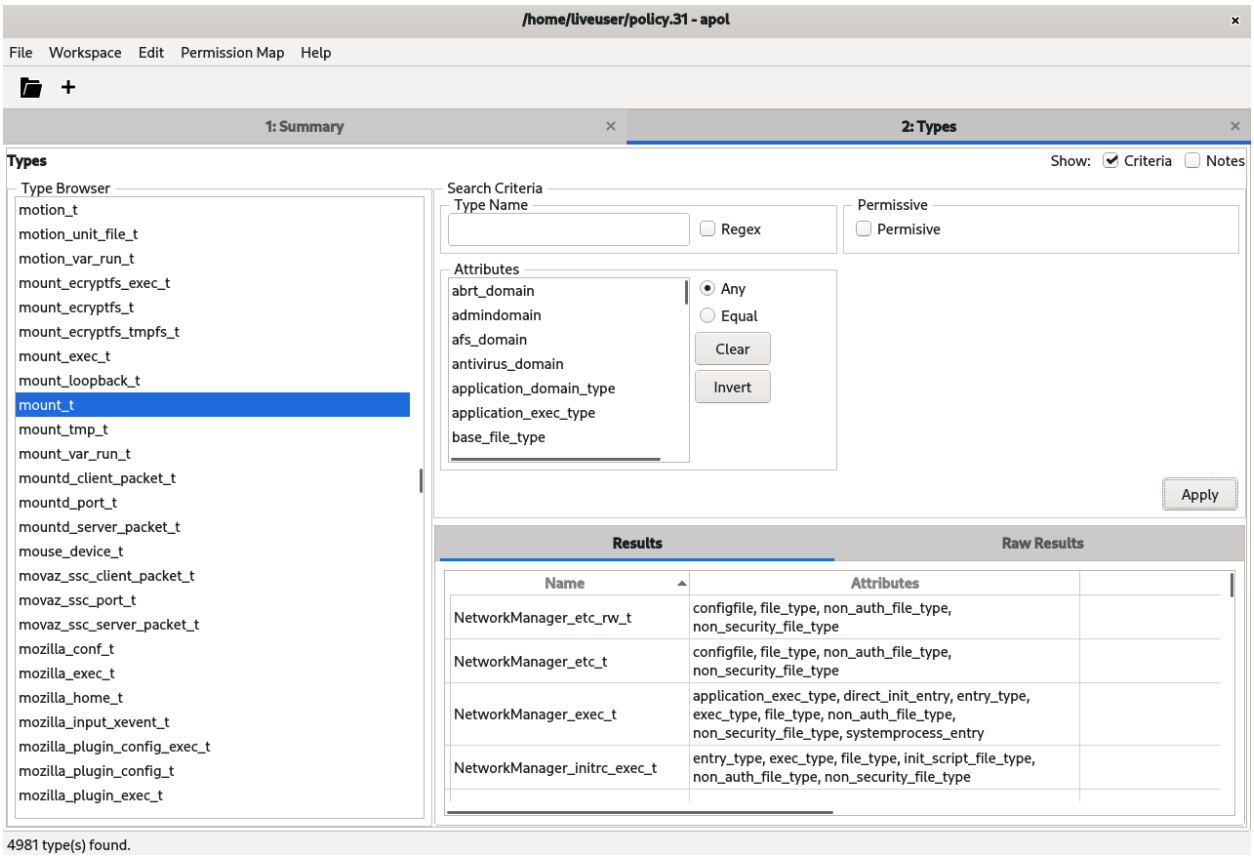
# Chapter 9: Secure Virtualization

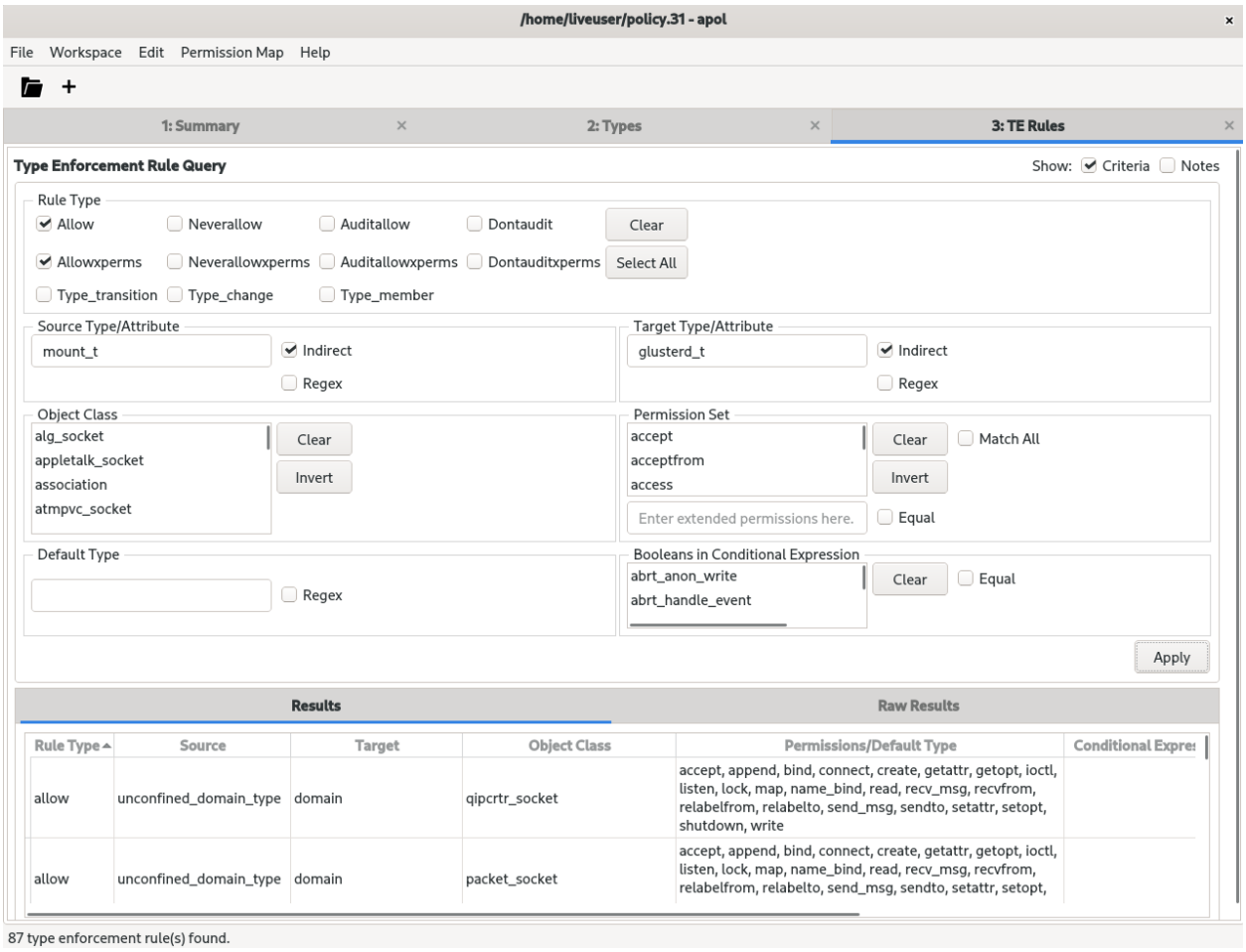


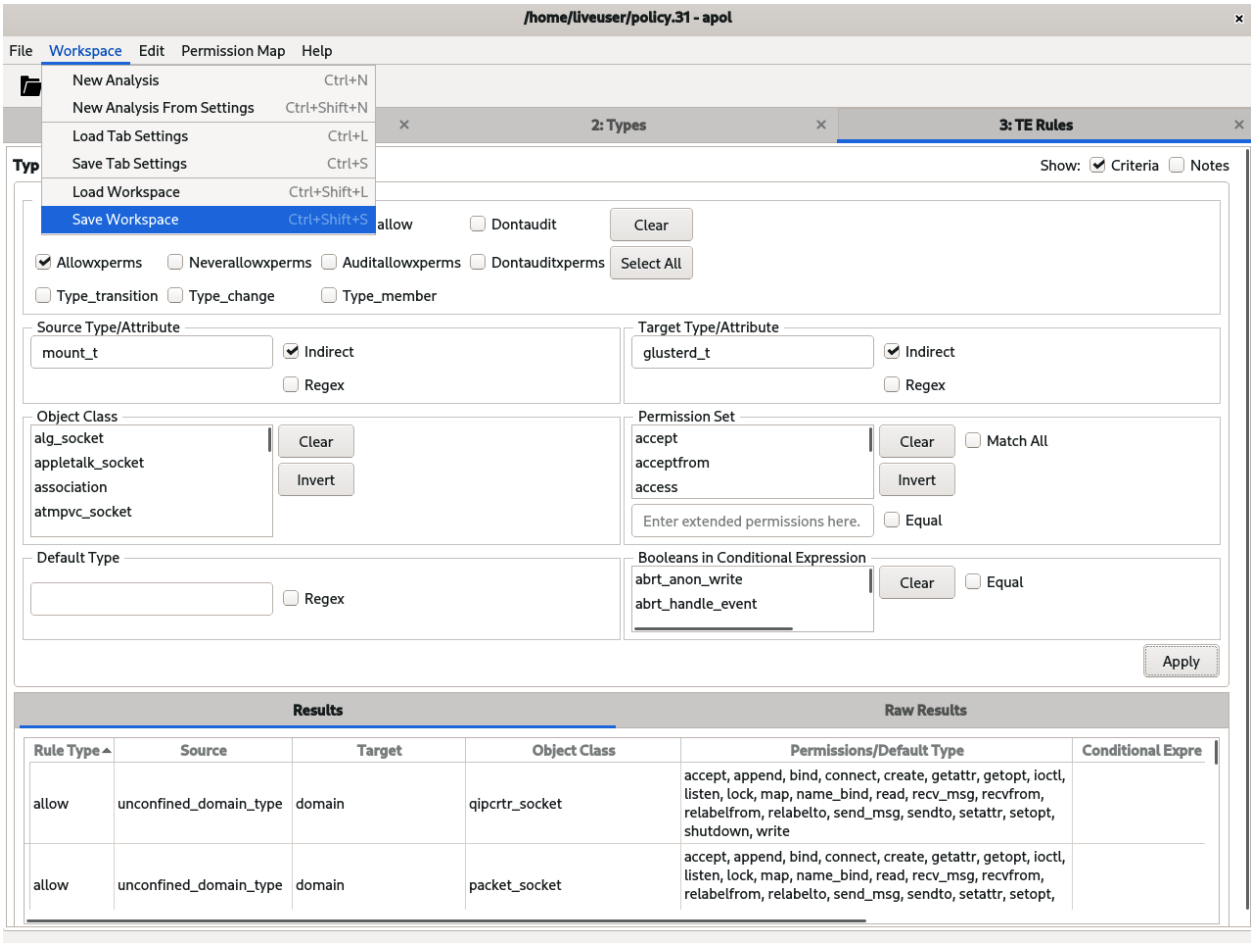
# Chapter 13: Analyzing Policy Behavior

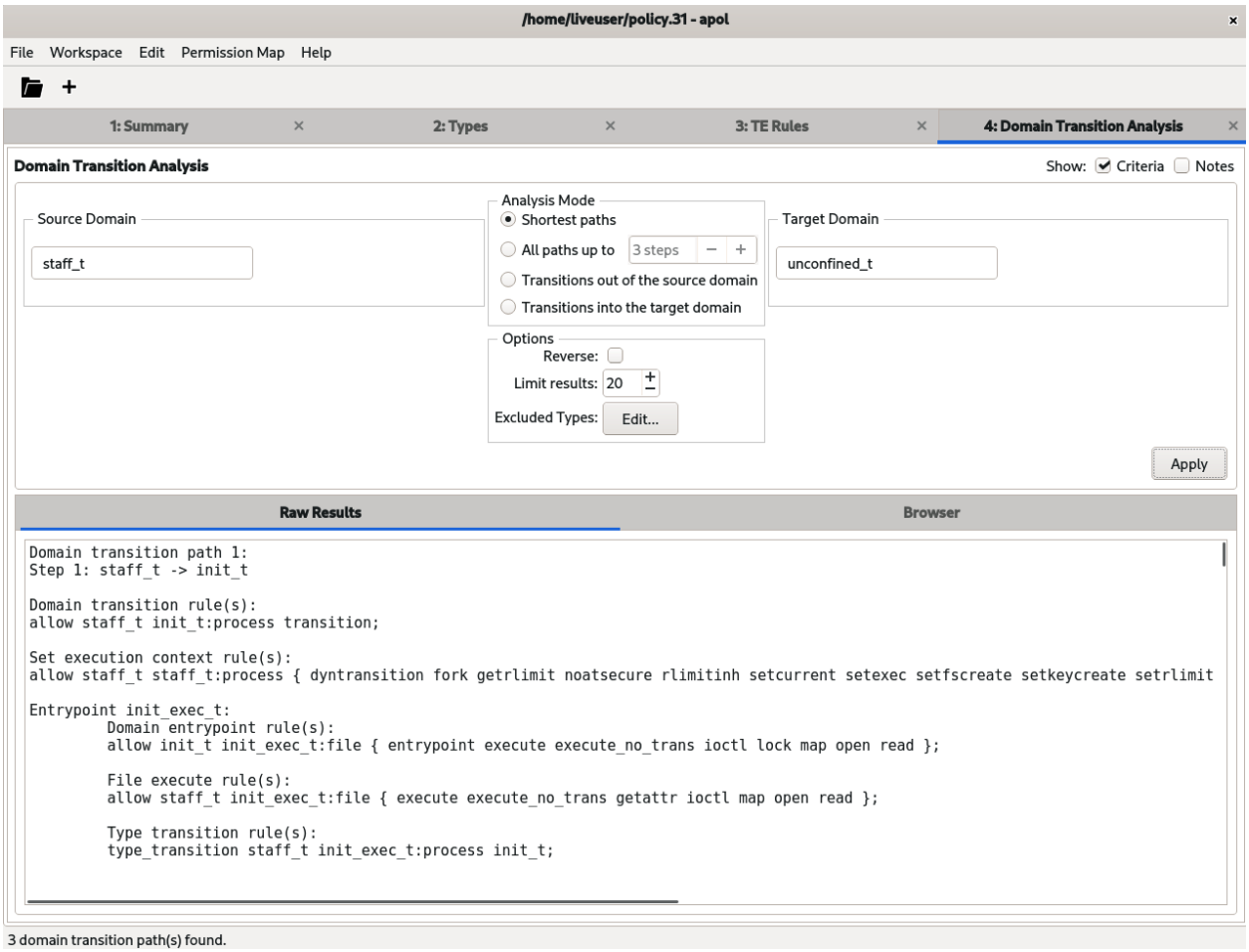


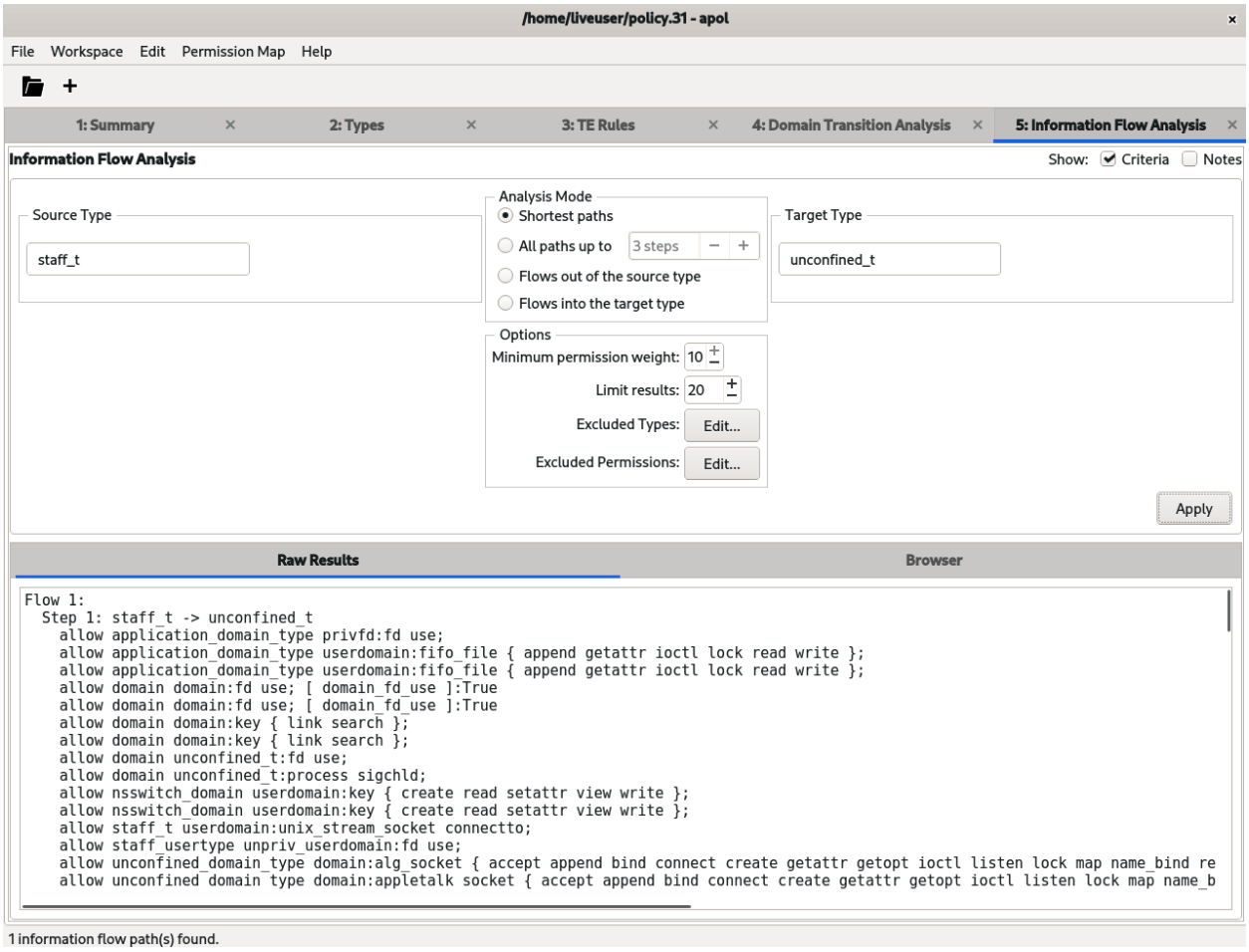

New Analysis
Choose a new analysis to start:
Analyses
Domain Transition Analysis
Information Flow Analysis
Components
Booleans
Categories
Commons
Object Classes
Roles
Sensitivities
Type Attributes
Types
Users
General
Summary
Labeling
Fs_use_* Statements
Genfscon Statements
Infiniband Endport Contexts
Infiniband Partition Key Contexts
Initial SID Statements
Network Interface Contexts
Network Node Contexts
Network Port Contexts
Other
Bounds
Defaults
Rules
Constraints
MLS Rules
RBAC Rules
TE Rules
Cancel
OK

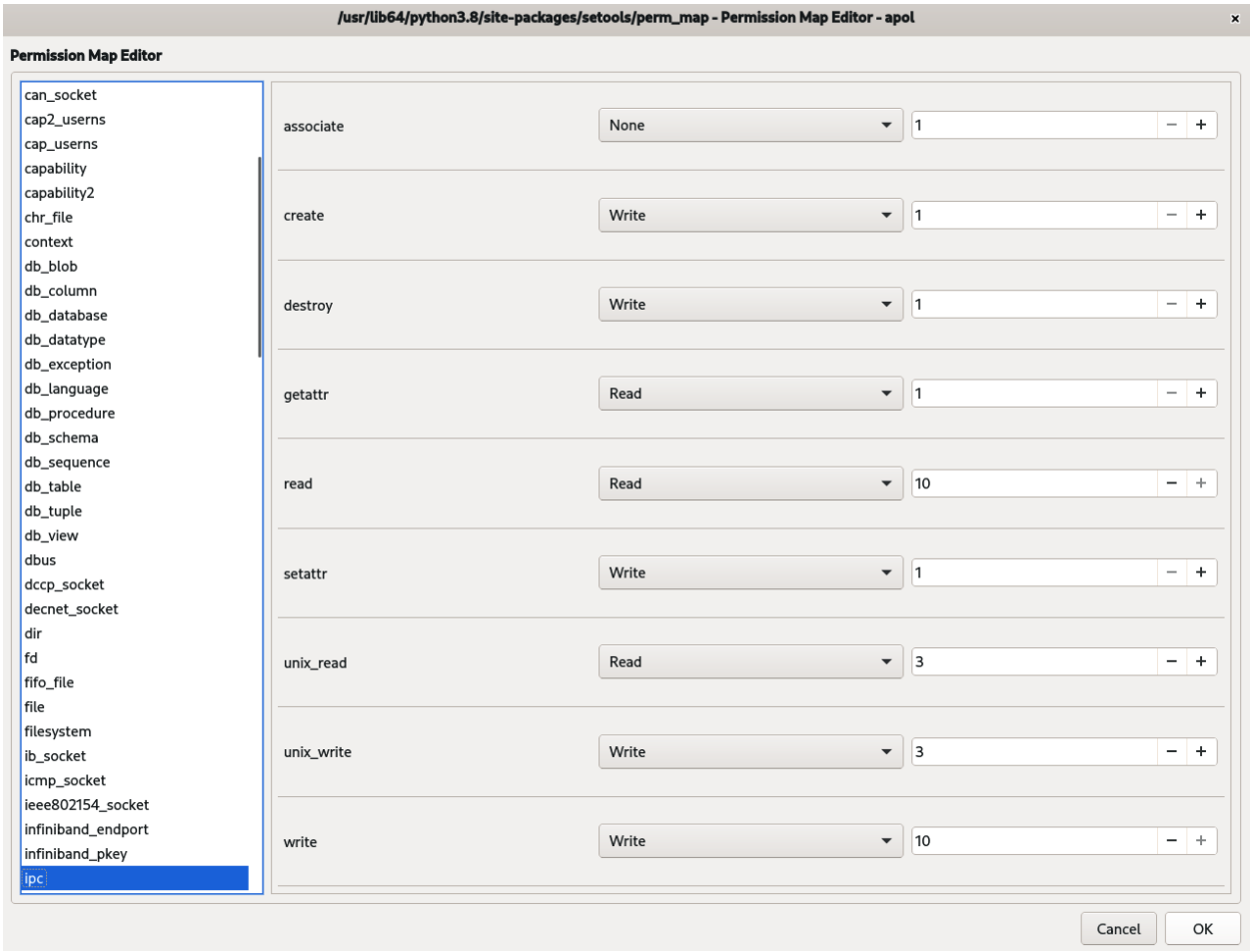

/home/liveuser/policy.31 - apol
File
Workspace
Edit
Permission Map
Help
1: Summary
2: Types
Types
Show:
Criteria
Notes
Type Browser
motion_t
motion_unit_file_t
motion_var_run_t
mount_ecryptfs_exec_t
mount_ecryptfs_t
mount_ecryptfs_tmpfs_t
mount_exec_t
mount_loopback_t
mount_t
mount_tmp_t
mount_var_run_t
mountd_client_packet_t
mountd_port_t
mountd_server_packet_t
mouse_device_t
movaz_ssc_client_packet_t
movaz_ssc_port_t
movaz_ssc_server_packet_t
mozilla_conf_t
mozilla_exec_t
mozilla_home_t
mozilla_input_xevent_t
mozilla_plugin_config_exec_t
mozilla_plugin_config_t
mozilla_plugin_exec_t
Search Criteria
Type Name
Regex
Permissive
Permisive
Attributes
abrt_domain
admindomain
afs_domain
antivirus_domain
application_domain_type
application_exec_type
base_file_type
Any
Equal
Clear
Invert
Apply
Results
Raw Results
Name
Attributes
NetworkManager_etc_rw_t
configfile, file_type, non_auth_file_type, non_security_file_type
NetworkManager_etc_t
configfile, file_type, non_auth_file_type, non_security_file_type
NetworkManager_exec_t
application_exec_type, direct_init_entry, entry_type, exec_type, file_type, non_auth_file_type, non_security_file_type, systemprocess_entry
NetworkManager_initrc_exec_t
entry_type, exec_type, file_type, init_script_file_type, non_auth_file_type, non_security_file_type
4981 type(s) found.


/home/liveuser/policy.31 - apol
File Workspace Edit Permission Map Help
1: Summary
2: Types
3: TE Rules
Type Enforcement Rule Query
Show: Criteria Notes
Rule Type
Allow Neverallow Auditallow Dontaudit Clear
Allowxperms Neverallowxperms Auditallowxperms Dontauditxperms Select All
Type_transition Type_change Type_member
Source Type/Attribute
mount_t
Indirect
Regex
Target Type/Attribute
glusterd_t
Indirect
Regex
Object Class
alg_socket
appletalk_socket
association
atmpvc_socket
Clear
Invert
Permission Set
accept
acceptfrom
access
Clear
Invert
Match All
Enter extended permissions here.
Equal
Default Type
Regex
Booleans in Conditional Expression
abrt_anon_write
abrt_handle_event
Clear
Equal
Apply
Results
Raw Results
Rule Type
Source
Target
Object Class
Permissions/Default Type
Conditional Expres
allow
unconfined_domain_type
domain
qipcrtr_socket
accept, append, bind, connect, create, getattr, getopt, ioctl, listen, lock, map, name_bind, read, recv_msg, recvfrom, relabelfrom, relabelto, send_msg, sendto, setattr, setopt, shutdown, write
allow
unconfined_domain_type
domain
packet_socket
accept, append, bind, connect, create, getattr, getopt, ioctl, listen, lock, map, name_bind, read, recv_msg, recvfrom, relabelfrom, relabelto, send_msg, sendto, setattr, setopt,
87 type enforcement rule(s) found.


/home/liveuser/policy.31 - apol
File
Workspace
Edit
Permission Map
Help
New Analysis Ctrl+N
New Analysis From Settings Ctrl+Shift+N
Load Tab Settings Ctrl+L
Save Tab Settings Ctrl+S
Load Workspace Ctrl+Shift+L
Save Workspace Ctrl+Shift+S
2: Types
3: TE Rules
Show: Criteria Notes
allow
Dontaudit
Clear
Allowxperms
Neverallowxperms
Auditallowxperms
Dontauditxperms
Select All
Type_transition
Type_change
Type_member
Source Type/Attribute
mount_t
Indirect
Regex
Target Type/Attribute
glusterd_t
Indirect
Regex
Object Class
alg_socket
appletalk_socket
association
atmpvc_socket
Clear
Invert
Permission Set
accept
acceptfrom
access
Clear
Invert
Match All
Enter extended permissions here.
Equal
Default Type
Regex
Booleans in Conditional Expression
abrt_anon_write
abrt_handle_event
Clear
Equal
Apply
Results
Raw Results
Rule Type
Source
Target
Object Class
Permissions/Default Type
Conditional Expre
allow
unconfined_domain_type
domain
qipcrtr_socket
accept, append, bind, connect, create, getattr, getopt, ioctl, listen, lock, map, name_bind, read, recv_msg, recvfrom, relabelfrom, relabelto, send_msg, sendto, setattr, setopt, shutdown, write
allow
unconfined_domain_type
domain
packet_socket
accept, append, bind, connect, create, getattr, getopt, ioctl, listen, lock, map, name_bind, read, recv_msg, recvfrom, relabelfrom, relabelto, send_msg, sendto, setattr, setopt,


/home/liveuser/policy.31 - apol
File
Workspace
Edit
Permission Map
Help
1: Summary
2: Types
3: TE Rules
4: Domain Transition Analysis
Domain Transition Analysis
Show:
Criteria
Notes
Source Domain
staff_t
Analysis Mode
Shortest paths
All paths up to
3 steps
Transitions out of the source domain
Transitions into the target domain
Target Domain
unconfined_t
Options
Reverse:
Limit results:
20
Excluded Types:
Edit...
Apply
Raw Results
Browser
Domain transition path 1:
Step 1: staff_t -> init_t
Domain transition rule(s):
allow staff_t init_t:process transition;
Set execution context rule(s):
allow staff_t staff_t:process { dyntransition fork getrlimit noatsecure rlimitinh setcurrent setexec setfscreate setkeycreate setrlimit
Entrypoint init_exec_t:
Domain entrypoint rule(s):
allow init_t init_exec_t:file { entrypoint execute execute_no_trans ioctl lock map open read };
File execute rule(s):
allow staff_t init_exec_t:file { execute execute_no_trans getattr ioctl map open read };
Type transition rule(s):
type_transition staff_t init_exec_t:process init_t;
3 domain transition path(s) found.


/home/liveuser/policy.31 - apol
File
Workspace
Edit
Permission Map
Help
1: Summary
2: Types
3: TE Rules
4: Domain Transition Analysis
5: Information Flow Analysis
Information Flow Analysis
Show:
Criteria
Notes
Source Type
staff_t
Analysis Mode
Shortest paths
All paths up to
3 steps
Flows out of the source type
Flows into the target type
Target Type
unconfined_t
Options
Minimum permission weight:
10
Limit results:
20
Excluded Types:
Edit...
Excluded Permissions:
Edit...
Apply
Raw Results
Browser
Flow 1:
Step 1: staff_t -> unconfined_t
allow application_domain_type privfd:fd use;
allow application_domain_type userdomain:fifo_file { append getattr ioctl lock read write };
allow application_domain_type userdomain:fifo_file { append getattr ioctl lock read write };
allow domain domain:fd use; [ domain_fd_use ]:True
allow domain domain:fd use; [ domain_fd_use ]:True
allow domain domain:key { link search };
allow domain domain:key { link search };
allow domain unconfined_t:fd use;
allow domain unconfined_t:process sigchld;
allow nsswitch_domain userdomain:key { create read setattr view write };
allow nsswitch_domain userdomain:key { create read setattr view write };
allow staff_t userdomain:unix_stream_socket connectto;
allow staff_usertype unpriv_userdomain:fd use;
allow unconfined_domain_type domain:alg_socket { accept append bind connect create getattr getopt ioctl listen lock map name_bind re
allow unconfined_domain_type domain:appletalk socket { accept append bind connect create getattr getopt ioctl listen lock map name_b
1 information flow path(s) found.


/usr/lib64/python3.8/site-packages/setools/perm_map - Permission Map Editor - apol
Permission Map Editor
can_socket
cap2_userns
cap_userns
capability
capability2
chr_file
context
db_blob
db_column
db_database
db_datatype
db_exception
db_language
db_procedure
db_schema
db_sequence
db_table
db_tuple
db_view
dbus
dccp_socket
decnet_socket
dir
fd
fifo_file
file
filesystem
ib_socket
icmp_socket
ieee802154_socket
infiniband_endport
infiniband_pkey
ipc
associate
None
1
create
Write
1
destroy
Write
1
getattr
Read
1
read
Read
10
setattr
Write
1
unix_read
Read
3
unix_write
Write
3
write
Write
10
Cancel
OK

# Chapter 15: Using the Reference Policy