CONCEPTS

SELinux = LABELING system

Every process, file, directory, system object has a LABEL.

Policy rules control access between labeled processes and labeled objects.

The kernel enforces these rules.

Labeling → files, process, ports, etc. (system objects)

Type enforcement → Isolates processes from each other based on types

LABELING

Label format:

user:role:type:level (optional)

user → identity known to the policy authorized for a specific set of roles and a specific MLS/MCS range

role → attribute of RBAC, serves as an intermediary between domains and SELinux users

type → attribute of type enforcement, defines a domain for processes and a type for files

level → attribute of MLS/MCS, pair of levels, written as lowlevel-highlevel if the levels differ, or lowlevel if the levels are identical

TYPE ENFORCEMENT

Targeted:	Processes that are targeted run in a confined domain, and processes that are not targeted run in an unconfined domain
Multi-level security (mls):	Control processes (domains) based on the level of the data they will be using
Multi-category security (mcs):	Protects like processes from each other (like VMs, OpenShift Gears, SELinux sandboxes, containers, etc.)

SELINUX MODES @ BOOT

Kernel parameters:

enforcing=0 → boot in permissive mode

selinux=0 → kernel to not load any part of the SELinux infrastructure

autorelabel=1 → forces the system to relabel

If you need to relabel the entire system:

 # touch /.autorelabel

 # reboot

If the system labeling contains a large amount of errors, you might need to boot in permissive mode for the autorelabel to succeed.

SELINUX STATES

enforcing	SELinux security policy is enforced
permissive	SELinux prints warnings instead of enforcing
disabled	No SELinux policy is loaded

CHECK STATUS:

Configuration file:	Check if SELinux is enabled:	**# getenforce**
/etc/selinux/config	SELinux status tool:	**# sestatus**
	Enable/disable SELinux (temporarily):	**# setenforce [1|0]**

EXAMPLE OF LABELING: APACHE WEB SERVER			CHECK/CREATE/MODIFY SELINUX CONTEXTS/LABELS:
Binary	**/usr/sbin/httpd**	**httpd_exec_t**	Many commands accept the argument -Z to view, create, and modify context: - ls -Z - id -Z - ps -Z - netstat -Z - cp -Z - mkdir -Z Contexts are set when files are created based on their parent directory's context (with a few exceptions). RPMs can set contexts as part of installation.
Configuration directory	**/etc/httpd**	**httpd_config_t**	
Logfile directory	**/var/log/httpd**	**httpd_log_t**	
Content directory	**/var/www/html**	**httpd_sys_content_t**	
Startup script	**/usr/lib/systemd/system/httpd.service**	**httpd_unit_file_d**	
Process running	**/usr/sbin/httpd -DFOREGROUND**	**httpd_t**	
Ports (netstat -tulpnZ)	80/tcp, 443/tcp	**httpd_t**	
Port type (semanage port -l)	80, 81, 443, 488, 8008, 8009, 8443, 9000	**http_port_t**	

TROUBLESHOOTING				
SELinux tools:	**# yum -y install setroubleshoot setroubleshoot-server**		← Reboot or restart auditd after you install	
Logging:	**/var/log/messages**	**/var/log/audit/audit.log**	**/var/lib/setroubleshoot/setroubleshoot_database.xml**	
journalctl	List all logs related to setroubleshoot:	**# journalctl -t setroubleshoot --since=14:20**		
	List all logs related to a particular SELinux label:	**# journalctl _SELINUX_CONTEXT=system_u:system_r:policykit_t:s0**		
ausearch	Look for SELinux errors in the audit log:	**# ausearch -m AVC,USER_AVC,SELINUX_ERR -ts today -i**		
	Search for SELinux AVC messages for a particular service:	**# ausearch -m avc -c httpd -i**		
Edit/modify labels (semanage)	know the label:	**# semanage fcontext -a -t httpd_sys_content_t '/srv/myweb(/.*)?'**		
	know the file with the equivalent labeling:	**# semanage fcontext -a -e /srv/myweb /var/www**		
	Restore the context (for both cases):	**# restorecon -vR /srv/myweb**		
Edit/modify labels (chcon)	know the label:	**# chcon -t httpd_system_content_t /var/www/html/index.html**	Note: If you move instead of copy a file, the file keeps its original context.	
	know the file with the equivalent labeling:	**# chcon --reference /var/www/html/ /var/www/html/index.html**		
	Restore the context (for both cases):	**# restorecon -vR /var/www/html/index.html**		
Add new port to service:	**# semanage port -a -t http_port_t -p tcp 8585**		← SELinux needs to know	
Booleans	Booleans allow parts of SELinux policy to be changed at runtime without any knowledge of SELinux policy writing.			
To see all booleans:	**# getsebool -a**	To see the description of each one:	**# semanage boolean -l**	
To set a boolean execute:	**# setsebool [boolean] [1|0]**	To configure it permanently, add -P:	Example : # setseebol httpd_enable_ftp_server 1 -P	