Cheatsheet SELinux

RPM Packages	Purpose
setroubleshoot	RPM for setroubleshootd and sealert
policycoreutils-gui	RPM for system-config-selinux
setools	RPM for seaudit and apol
policycoreutils-python	RPM containing policy create scripts

Commands	Purpose
/etc/sysconfig/selinux	Config file
/etc/selinux	Policy locations
setroubleshootd	Service to translate AVC denial messages in audit.log
/var/log/audit/audit.log	Log of all SELinux messages
/var/log/messages	Log of all denials if setroubleshootd is running
sealert -a audit.log -H > file.html	Creates HTML webpage out of audit.log
setenforce	Sets mode of SELinux in real time
sestatus	Tool to show you the status of SELinux
seinfo -c	Prints list of object classes
seinfo -t	Prints list of object types
seinfo -u	Prints list of SELinux users
seinfo -n	Prints list of network contexts
seinfo -p	Prints list of network port contexts
seinfo -b	Prints list of booleans
getsebool -a	Get list of booleans and current setting
setsebool <boolean> <on | off>	Sets boolean, use -P to survive reboot (persistent)
restorecon <file>	Restores files to default SELinux security context
chcon -t <context_t> <file>	Sets context of <file> to <context_t>
ls -Z <file>	List Security Context of Object
ps -AZ	List Security Context of Subjects
id -Z	List Security Context of User
system-config-selinux	Redhat Gui Policy Management tool
semanage	Command line Policy Management tool
checkpolicy	Compiles policy into binary for the kernel
audit2allow	Creates policy modules
semodule -i <policy module>	Inserts plicy module created by audit2allow
`grep http audit.log | audit2allow –m local && semodule –i local.pp`	