Policy language:

<https://selinuxproject.org/page/PolicyLanguage>

sepolgen walkthrough: <https://unix.stackexchange.com/questions/309122/how-to-create-a-custom-selinux-label>

sample security policy:

<https://github.com/TresysTechnology/refpolicy/tree/master/policy/modules/services>

Creating a policy with sepolicy generate:

<https://mgrepl.wordpress.com/2015/05/20/how-to-create-a-new-initial-policy-using-sepolicy-generate-tool/>

Permission sets:

<https://selinuxproject.org/page/ObjectClassesPerms#Common_Permission_Sets>

Remove policy:

sudo semodule -r <policy\_name>

Add rpm-build:

sudo yum install rpm-build

Compile policy:

sudo sh <policy\_name>.sh

Change file security contexts:

chcon

Modifying security context for certain users:

<https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security-enhanced_linux/sect-security-enhanced_linux-confining_users-confining_existing_linux_users_semanage_login>

Better:

<https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security-enhanced_linux/sect-security-enhanced_linux-confining_users-confining_new_linux_users_useradd>

File security contexts

<https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/SELinux_Guide/rhlcommon-section-0019.html>

<https://wiki.gentoo.org/wiki/SELinux/Tutorials/Controlling_file_contexts_yourself>

<https://docs.fedoraproject.org/en-US/Fedora/11/html/Security-Enhanced_Linux/sect-Security-Enhanced_Linux-SELinux_Contexts_Labeling_Files-Persistent_Changes_semanage_fcontext.html>

<https://linux.die.net/man/1/chcon>

Note: for some reason, I had to manually change the context of my data files

MANY SELINUX CHANGES DON’T APPLY UNLESS ‘sudo setenforce 0’ is run

TODO: try data separation by allowing existing users to associate with new types (system\_u associating with student\_r)

Security context components: <https://fedoraproject.org/wiki/Security_context>

Assigning security contexts to processes: <https://wiki.gentoo.org/wiki/SELinux/Tutorials/How_does_a_process_get_into_a_certain_context>

**HOW I LEARNED TO DEBUG**

1. After creating the policy, I compiled it with the shell file
2. If it compiled, I ran the executable, if what I expected to happen happened (and I wasn’t done), I modified the .te file and went back to step 1. If something went wrong, I went to step 3
3. First, I made sure the executable was running in the context I expected it to. I checked this by running the executable from another shell and running **ps -uZ**. Note that this only worked because I made my executable wait for program input before terminating. If the executable terminates immediately, you can’t do this.
4. If you think your .te file has the rules it needs, run the following:  
   **date  
   <executable>  
   sudo ausearch -i -ts <time printed out by date> | grep <executable name>**
5. If something shows up, check out this link: <https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sec-understanding_audit_log_files>, figure out the problem, modify the .te file, and go back to step 1.
6. If nothing shows up, selinux might be hiding the error messages. Run **sudo semodule -DB** to rebuild the policy to show every error message. Return to step 4, but after you do your debugging, go to step 7.
7. If you’ve run **sudo semodule -DB**, you need to rebuild the policy properly with **sudo semodule -B**