What is SELinux trying to tell me?

The 4 key causes of SELinux errors.
SELinux Problem Solutions

1. SELinux == Labeling
2. SELinux Needs to Know
3. SELinux Policy/Apps can have bugs.
4. You could be COMPROMISED!!!!
SELinux == Labeling

- Every process and object on the machine has a label associated with it
- If your files are not labeled correctly access might be denied.
  - If you use alternative paths for confined domains SELinux needs to KNOW.
    - # semanage fcontext -a -t httpd_sys_content_t '/srv/myweb(/.*)?'
    - # restorecon -R /srv/myweb
**SELinux == Labeling**

![SELinux Administration screen with file labeling configuration](image-url)
SELinux == Labeling

- Fedora 11 introduces equivalency labeling
  - `semanage fcontext -a -e /srv/myweb /var/www`
    - Tells SELinux to label all files directories under /srv/myweb the same as /var/www
    - `/srv/myweb/cgi-bin/mycgi.cgi` will get labeled `httpd_sys_script_t`
  - `semanage fcontext -a -e /export/home /home`
    - Label all files under /export/home as if they were under /home
    - `/export/home/dwalsh/.ssh` will get labeled `ssh_home_t`
SELinux needs to KNOW

→ How did you configure your apache server?
   Tell SELinux!!

→ If you want httpd to send email
   → # setsebool -P httpd_can_sendmail 1

→ Vsftp setup for users to login
   → # setsebool -P ftp_home_dir 1

→ Http is setup to listen on port 8585
   → # semanage port -a -t http_port_t -p tcp 8585
SELinux needs to KNOW...
SELinux needs to KNOW
SELinux Policy/Apps Can Have bugs

- SELinux Policy might have a bug
  - Unusual Code Paths
  - Configurations
  - Redirection of stdout
- Apps have bugs
  - Leaked File Descriptors
  - Executable Memory
  - Badly built libraries
- Report the bugs in Bugzilla so we can fix them
SELinux Policy/Apps Can Have bugs!!!

- You can tell SELinux to just allow
  - Selinux is blocking postgresql
    - Labeling is correct? No appropriate boolean?
    - Use audit2allow to build a policy module
      - `grep postgresql /var/log/audit/audit.log | audit2allow -M mypostgresql`
      - `# semodule -i mypostgresql.pp`
  - Examine mypostgresql.te
    - Make sure you are not allowing too much?
    - Ask for help?
      - `#fedora`
      - Fedora-selinux mail list
      - `dwalsh@redhat.com`
You could be COMPROMISED!!!

- Current tools do not do a good job of differentiating
  - If you have a confined domain that tries to:
    - Load a kernel module
    - Turn off SELinux enforcing mode
    - Write to etc_t? shadow_t
    - Modify iptables rules
    - Sendmail?????
    - others
  - You might be compromised