SELINUX FOR MERE MORTALS

(Or, “Don't Turn It Off”)

Thomas Cameron, RHCA, RHCDS, RHCVA, RHCSS, RHCX
Managing Solutions Architect, Red Hat
Wednesday, May 4th, 2011

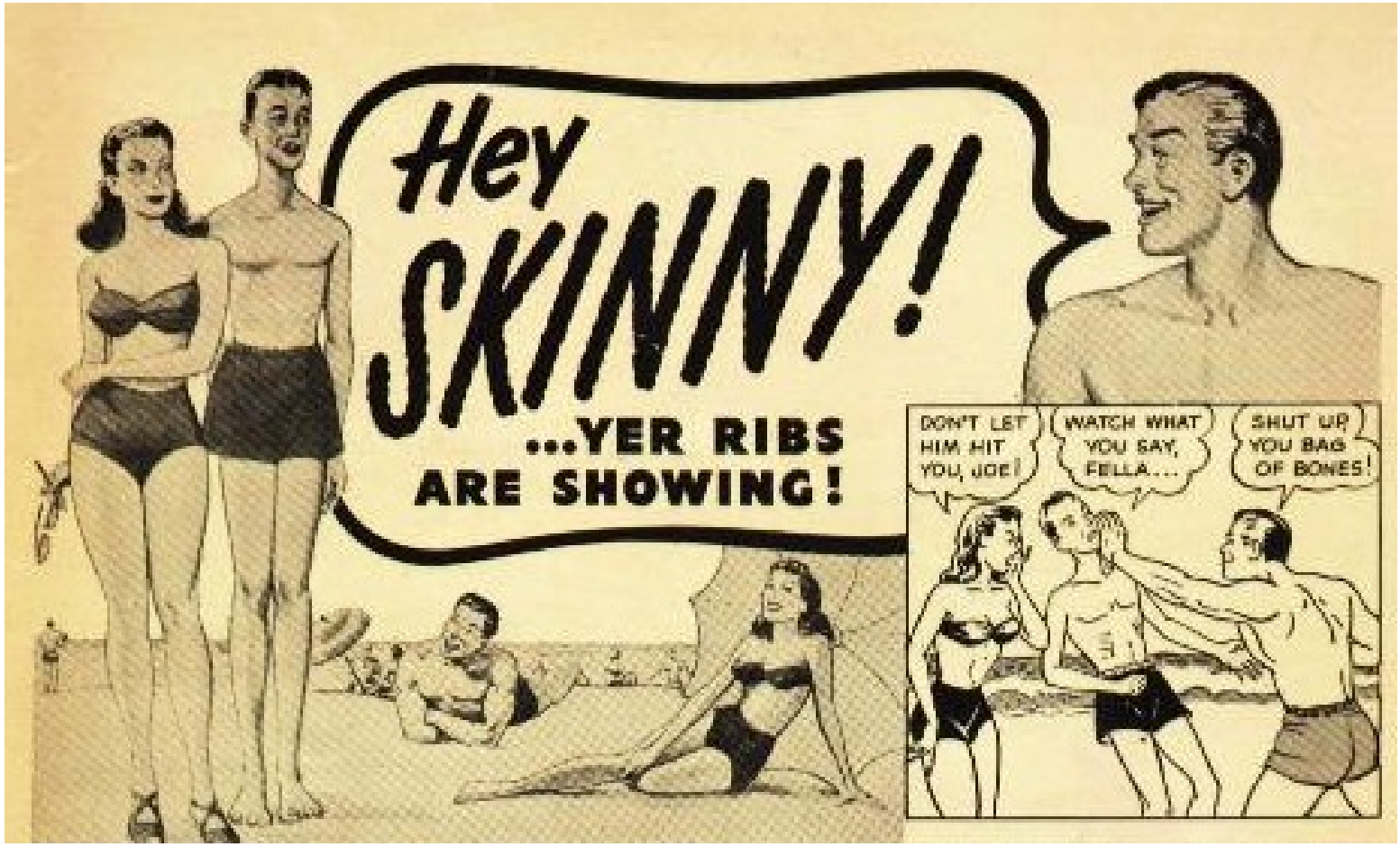
Agenda

- About Us
- What is SELinux?

About Us

- Red Hat leads the way in SELinux development. John Dennis, Ulrich Drepper, Steve Grubb, Eric Paris, Roland McGrath, James Morris and Dan Walsh, all Red Hat staffers, acknowledged by the NSA for their contributions to SELinux at:
- http://www.nsa.gov/research/selinux/contrib.shtml
- Red Hat acknowledged by the NSA as a corporate contributor as well.

What Thomas thought SELinux was



If you feel the same way...

If you feel the same way...

- You're in the right place!

What is SELinux?

- A brief history
  - Created by the United States National Security Agency (NSA) as set of patches to the Linux kernel using Linux Security Modules (LSM)
  - Released by the NSA under the GNU General Public License (GPL) in 2000
  - Adopted by the upstream Linux kernel in 2003

What is SELinux?

- MAC vs. DAC
- Labeling
- Type Enforcement
  - Transitions

MAC vs. DAC

- Typical Unix/Linux: Discretionary Access Control (DAC)
  - User ownership
  - Group ownership
  - Permissions
- If I want, I have the ability (discretion) to `chmod +rwx` my home directory. Nothing will stop me, and in a DAC system, nothing will stop others from getting in.

MAC vs. DAC

- In DAC systems, `root` is omnipotent.

MAC vs. DAC

- SELinux system: Mandatory Access Control (MAC)
- On MAC systems, policy is set centrally and fixed
- Even if you change the DAC settings on your home directory, if a mandatory system policy is in place which prevents another user or process from accessing it, you're generally safe.

MAC vs. DAC

- MAC can be incredibly fine grained. Policies can be set to determine access between:
  - Users
  - Files
  - Directories
  - Memory
  - Sockets
  - tcp/udp ports
  - etc...

Labeling

- Different components of the system - files, directories, running processes, sockets, ports, users and so on – are assigned different labels for their security context.

Labeling

- For example, in the Apache web server, you'll see the following labels:
  - /usr/sbin/httpd has the context system_u:object_r:httpd_exec_t:s0
  - /etc/httpd/ has the context system_u:object_r:httpd_config_t:s0
  - /var/www/html/ has the context system_u:object_r:httpd_sys_content_t:s0
  - /var/log/httpd/ has the context system_u:object_r:httpd_log_t:s0

Labeling

- For example, in the Apache web server, you'll see the following labels:
  - /usr/lib64/httpd/modules/ has the context system_u:object_r:httpd_modules_t:s0
  - /etc/rc.d/init.d/httpd has the context system_u:object_r:httpd_initrc_exec_t:s0
  - ...etc

Labeling

- When httpd is run, it has the label unconfined_u:system_r:httpd_t:s0
- The http ports (80, 443, 488, 8008, 8009, 8443) are labeled http_port_t

Labeling

- These labels are used to enforce policies.

Labeling

- There are other fields in the SELinux context
  - system_u:object_r:httpd_exec_t:s0
  - User (root, unconfined_u, user_u, system_u)
    - Not the same as Linux user! There are usually a very limited number of SELinux users, and typically all regular Linux users will run as the same SELinux user
    - User files and processes will typically be labeled unconfined_u
    - System files and processes will often be labeled system_u
  - SELinux User is not used in targeted policy

```
[tcameron@case ~]$ ssh john@host236
john@host236's password:
Last login: Sun May  1 22:23:47 2011 from localhost
[john@host236 ~]$ id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[john@host236 ~]$
```

```
[tcameron@case ~]$ ssh paul@host236
paul@host236's password:
[paul@host236 ~]$ id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[paul@host236 ~]$
```

```
[tcameron@case ~]$ ssh george@host236
george@host236's password:
[george@host236 ~]$ id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[george@host236 ~]$
```

```
[tcameron@case ~]$ ssh ringo@host236
ringo@host236's password:
[ringo@host236 ~]$ id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[ringo@host236 ~]$
```

root@host236:~

File Edit View Search Terminal Help

```
[tcameron@case ~]$ ssh root@host236
root@host236's password:
Last login: Sun May  1 22:13:46 2011 from case.tc.redhat.com
[root@host236 ~]# id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@host236 ~]#
```

Labeling

- User files will typically be labeled unconfined_u
- System files will often be labeled system_u

root@host236:~

File Edit View Search Terminal Help

```
[root@host236 ~]# ls -Z /home/
drwx------. george  george  unconfined_u:object_r:user_home_dir_t:s0 george
drwx------. john    john    unconfined_u:object_r:user_home_dir_t:s0 john
drwx------. makerpm makerpm unconfined_u:object_r:user_home_dir_t:s0 makerpm
drwx------. paul    paul    unconfined_u:object_r:user_home_dir_t:s0 paul
drwx------. ringo   ringo   unconfined_u:object_r:user_home_dir_t:s0 ringo
[root@host236 ~]#
[root@host236 ~]#
[root@host236 ~]#
[root@host236 ~]# ls -Z /etc/passwd
-rw-r--r--. root root system_u:object_r:etc_t:s0       /etc/passwd
[root@host236 ~]#
[root@host236 ~]#
[root@host236 ~]#
[root@host236 ~]# ls -Z /bin/bash
-rwxr-xr-x. root root system_u:object_r:shell_exec_t:s0 /bin/bash
[root@host236 ~]#
```

Labeling

- User processes will typically be labeled unconfined_u

paul@host236:~

File Edit View Search Terminal Help

```
[paul@host236 ~]$ ps axZ | grep bash
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 25875 pts/1 Ss   0:00 -bash
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 25897 pts/2 Ss+   0:00 -bash
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 25945 pts/0 Ss+   0:00 -bash
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 26183 pts/1 S+   0:00 grep bash
[paul@host236 ~]$
```

Labeling

- System processes will often be labeled system_u

root@host236:~

File Edit View Search Terminal Help

```
[root@host236 ~]# ps axZ | grep [h]ttp
system_u:system_r:httpd_t:s0     1480 ?        Ss     0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1488 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1489 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1490 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1491 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1492 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1493 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1494 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1495 ?        S      0:00 /usr/sbin/httpd
[root@host236 ~]#
```

Labeling

- There are other fields in the SELinux context
  - system_u:object_r:httpd_exec_t:s0
  - Role (unconfined_r, object_r, system_r).
    - Used for role based access control (RBAC), we won't cover that today
    - Used in MLS and strict policy

Labeling

- There are other fields in the SELinux context
  - Role (unconfined_r, object_r, system_r).
    - object_r is typically a file, directory or other entry on the filesystem

root@host236:~

File Edit View Search Terminal Help

```
[root@host236 ~]# ls -dZ /etc/httpd/
drwxr-xr-x. root root system_u:object_r:httpd_config_t:s0 /etc/httpd/
[root@host236 ~]#
[root@host236 ~]#
[root@host236 ~]# ls -Z /usr/sbin/httpd
-rwxr-xr-x. root root system_u:object_r:httpd_exec_t:s0 /usr/sbin/httpd
[root@host236 ~]#
[root@host236 ~]#
[root@host236 ~]#
[root@host236 ~]# ls -Z /home/
drwx------. george  george  unconfined_u:object_r:user_home_dir_t:s0 george
drwx------. john    john    unconfined_u:object_r:user_home_dir_t:s0 john
drwx------. makerpm makerpm unconfined_u:object_r:user_home_dir_t:s0 makerpm
drwx------. paul    paul    unconfined_u:object_r:user_home_dir_t:s0 paul
drwx------. ringo   ringo   unconfined_u:object_r:user_home_dir_t:s0 ringo
[root@host236 ~]#
```

Labeling

- There are other fields in the SELinux context
  - Role (unconfined_r, object_r, system_r).
    - A process in the system_r role is typically a process running which was started at boot time
    - A process in the unconfined_r role is a process running from an unconfined user

root@host236:~

File Edit View Search Terminal Help

```
[root@host236 ~]# ps axZ | grep [h]ttpd
system_u:system_r:httpd_t:s0     1480 ?        Ss     0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1488 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1489 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1490 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1491 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1492 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1493 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1494 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1495 ?        S      0:00 /usr/sbin/httpd
[root@host236 ~]#
[root@host236 ~]#
[root@host236 ~]# ps axZ | grep [b]ash
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 1562 pts/0 Ss   0:00 -bash
[root@host236 ~]#
```

Labeling

- There are other fields in the SELinux context
  - system_u:object_r:httpd_exec_t:s0
  - MLS/MCS component (Single: s0. Range: s0-s15:c0.c1023).
    - Used for finer grained control of security levels
    - Out of scope for today

Type Enforcement

- Type enforcement is just a definition of how types interact.
- Processes running with http_t context should probably be able to access the configuration files labeled with httpd_config_t
- Processes running with http_t context should probably not be able to access files with type shadow_t!

Type Enforcement

- Transition:
  - When root executes a file with the type http_exec_t, it should transition to http_t. You probably don't want network facing services running in root's context.
  - Same is true as the system boots up - /sbin/init starts in its own SELinux context. As it starts other processes, they are transitioned to a their new SELinux context based on transition rules defined in the policy.

Type Enforcement

- Example:
  - root fires up a network listener without a targeted policy
    - In this case, it's just netcat

root@host14:~

File Edit View Search Terminal Help

```
[root@host14 ~]# nc -l 99
```

Type Enforcement

- Example:
  - This “listener” is running unconfined – if a bad guy were to compromise it, that bad guy could own the system

root@host14:~

File Edit View Search Terminal Help

```
[root@host14 ~]# cat ps.out
ps axZ | grep "nc -l"
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 2142 pts/0 S+ 0:00 nc -l 99
[root@host14 ~]#
[root@host14 ~]#
[root@host14 ~]#
[root@host14 ~]# cat netstat.out
netstat -tnlpZ | grep 99
tcp 0 0 0.0.0.0:99  0.0.0.0:*  LISTEN 2142/nc fined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@host14 ~]#
```

Type Enforcement

- Example:
  - root uses system startup script to launch httpd
  - Even though the user context changes, the type does not
  - Since we're dealing with type enforcement, the user context changing is not really important.

root@host14:~

File Edit View Search Terminal Help

```
[root@host14 ~]# ps axZ | grep [h]ttp
system_u:system_r:httpd_t:s0     1572 ?        Ss     0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1579 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1580 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1581 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1582 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1583 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1584 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1585 ?        S      0:00 /usr/sbin/httpd
system_u:system_r:httpd_t:s0     1586 ?        S      0:00 /usr/sbin/httpd
[root@host14 ~]# service httpd stop
Stopping httpd:                                          [  OK  ]
[root@host14 ~]# service httpd start
Starting httpd:                                          [  OK  ]
[root@host14 ~]# ps axZ | grep [h]ttp
unconfined_u:system_r:httpd_t:s0 1956 ?        Ss     0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 1959 ?        S      0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 1960 ?        S      0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 1961 ?        S      0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 1962 ?        S      0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 1963 ?        S      0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 1964 ?        S      0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 1965 ?        S      0:00 /usr/sbin/httpd
unconfined_u:system_r:httpd_t:s0 1966 ?        S      0:00 /usr/sbin/httpd
[root@host14 ~]#
```

Policy

- Policy is just the rule set that defines how these labeled objects interact
- The default policy in RHEL 6 is the targeted policy.
  - Unless covered by a targeted policy, processes run unconfined.
  - Hundreds of apps covered by policy.
- The MLS/MCS policies are far more fine grained
  - If not explicitly allowed, everything is denied.

SELinux Configuration

- You can take a look around /etc/selinux
  - /etc/selinux/config
  - /etc/selinux/targeted/contexts/files
  -

Dealing with labels

- Viewing labels
- Creating labels

Viewing labels

- Many utilities support the -Z argument
- If you've been paying attention, you have already seen some:
  - ls -Z
  - cp -Z
  - ps -Z
  - id -Z

Creating labels

- SELinux aware apps
  - chcon
  - restorecon
  - semanage fcontext
    - See /etc/selinux/targeted/contexts/files/file_contexts
  - RPMs
- Users creating files
  - New files inherit context
  - Moved files maintain context

Creating labels

- Login process sets default context
  - Typically unconfined
- File transitions (defined by policy)
  - If an application foo_t creates a file in a directory labeled bar_t, policy can require a transition so that file is baz_t
  - Example: dhclient_t creates resolv.conf in directory etc_t labeled net_conf_t

Creating labels

- Execution transitions (defined by policy)
  - Process foo_t executes bar_exec_t, policy can require transition to bar_t
  - Example: init_t executes initrc_exec_t which eventually executes all the start/stop scripts via rc

What does it mean if I get an SELinux error?

- When you see an SELinux denial, it means that something is wrong.
- Turning off SELinux is like turning up the radio really loud when your car is making a strange noise!

What does it mean if I get an SELinux error?

- It can mean that the labeling is wrong
  - We'll look at some examples of that

What does it mean if I get an SELinux error?

- The policy needs to be tweaked
  - Booleans and the like

What does it mean if I get an SELinux error?

- There's a bug in the app or the policy
  - We need to know!

What does it mean if I get an SELinux error?

- You've been or are being broken into!
  - Take action!

Tips and tricks

- Make sure you've installed the setroubleshoot and setroubleshoot-server RPMs.
  - Sends messages to /var/log/messages about SELinux errors.
  - Pulls in many of the tools you need to examine alerts and get guidance on how to fix them

```
root@host15:~
File  Edit  View  Search  Terminal  Help
  Installing     : audit-libs-python-2.0.4-1.el6.x86_64                    3/9
  Installing     : libsemanage-python-2.0.43-4.el6.x86_64                  4/9
  Updating       : policycoreutils-2.0.83-19.8.el6_0.x86_64                5/9
  Installing     : policycoreutils-python-2.0.83-19.8.el6_0.x86_64         6/9
  Installing     : setroubleshoot-plugins-2.1.60-1.el6.noarch              7/9
  Installing     : setroubleshoot-server-2.2.94-1.el6.x86_64               8/9
  Cleanup        : policycoreutils-2.0.83-19.1.el6.x86_64                  9/9

Installed:
  setroubleshoot-server.x86_64 0:2.2.94-1.el6

Dependency Installed:
  audit-libs-python.x86_64 0:2.0.4-1.el6
  libsemanage-python.x86_64 0:2.0.43-4.el6
  policycoreutils-python.x86_64 0:2.0.83-19.8.el6_0
  setools-libs.x86_64 0:3.3.7-4.el6
  setools-libs-python.x86_64 0:3.3.7-4.el6
  setroubleshoot-plugins.noarch 0:2.1.60-1.el6

Dependency Updated:
  policycoreutils.x86_64 0:2.0.83-19.8.el6_0

Complete!
[root@host15 ~]#
```

Real World Examples

- We'll look at several examples of real world scenarios where sysadmins make mistakes

Apache vs. SELinux

- Create content and move it

root@host15:~

File Edit View Search Terminal Help

```
[root@host15 ~]# echo "This is my foo" > foo.html
[root@host15 ~]# mv foo.html /var/www/html/
[root@host15 ~]#
```

403 Forbidden - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://host15.tc.redhat.com/foo.html

Most Visited Zimbra Red Hat Application... Red Hat -- Intranet ... American Express B... RHN Satellite - Sign... MySouthwest

403 Forbidden

Forbidden

You don't have permission to access /foo.html on this server.

Apache/2.2.15 (Red Hat) Server at host15.tc.redhat.com Port 80

Done

Move vs copy

root@host15:~

File Edit View Search Terminal Help

```
[root@host15 ~]# ls -Z /var/www/html/
-rw-r--r--. root root unconfined_u:object_r:admin_home_t:s0 foo.html
[root@host15 ~]#
```

Apache vs. SELinux

- We need to change the context

Apache vs. SELinux

- Hardest way - figure out the context and use chcon

root@host15:~

File Edit View Search Terminal Help

```
[root@host15 ~]# ls -Z /var/www/html/
-rw-r--r--. root root unconfined_u:object_r:admin_home_t:s0 foo.html
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]# ls -Z /var/www/
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 error
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 icons
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]# chcon -u unconfined_u -r object_r -t httpd_sys_content_t /var/w
ww/html/foo.html
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]# ls -Z /var/www/html/
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 foo.html
[root@host15 ~]#
```

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://host15.tc.redhat.com/foo.html

Google

Most Visited Zimbra Red Hat Application... Red Hat -- Intranet ... American Express B... RHN Satellite - Sign... MySouthwest

http://host15.tc...at.com/foo.html

This is my foo

Done

Apache vs. SELinux

- Easier way - use chcon --reference

root@host15:~

File Edit View Search Terminal Help

```
[root@host15 ~]# ls -Z /var/www/html/
-rw-r--r--. root root unconfined_u:object_r:admin_home_t:s0 foo.html
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]# ls -Z /var/www/
drwxr-xr-x. root root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 error
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 html
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 icons
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]# chcon --reference /var/www/html /var/www/html/foo.html
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]# ls -Z /var/www/html/
-rw-r--r--. root root system_u:object_r:httpd_sys_content_t:s0 foo.html
[root@host15 ~]#
```

Apache vs. SELinux

- Easiest way - restorecon

root@host15:~

File Edit View Search Terminal Help

```
[root@host15 ~]# mv foo.html /var/www/html/
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]# ls -Z /var/www/html/
-rw-r--r--. root root unconfined_u:object_r:admin_home_t:s0 foo.html
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]# restorecon -vR /var/www/html/
restorecon reset /var/www/html/foo.html context unconfined_u:object_r:admin_home
_t:s0->system_u:object_r:httpd_sys_content_t:s0
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]#
[root@host15 ~]# ls -Z /var/www/html/
-rw-r--r--. root root system_u:object_r:httpd_sys_content_t:s0 foo.html
[root@host15 ~]#
```

Apache vs. SELinux

- Allowing Apache to access Paul's home directory so we can access http://host15.tc.redhat.com/~paul
  - Fix httpd.conf

Booleans

- Booleans turn something on or off
  - getsebool

root@host15:~

File Edit View Search Terminal Help

```
[root@host15 ~]# getsebool -a
abrt_anon_write --> off
allow_console_login --> on
allow_corosync_rw_tmpfs --> off
allow_cvs_read_shadow --> off
allow_daemons_dump_core --> on
allow_daemons_use_tty --> on
allow_domain_fd_use --> on
allow_execheap --> off
allow_execmem --> on
allow_execmod --> on
allow_execstack --> on
allow_ftpd_anon_write --> off
allow_ftpd_full_access --> off
allow_ftpd_use_cifs --> off
allow_ftpd_use_nfs --> off
allow_gssd_read_tmp --> on
allow_guest_exec_content --> off
allow_httpd_anon_write --> off
allow_httpd_mod_auth_ntlm_winbind --> off
allow_httpd_mod_auth_pam --> off
allow_httpd_sys_script_anon_write --> off
allow_java_execstack --> off
allow_kerberos --> on
```

Booleans

- Booleans turn something on or off
  - setsebool

root@host15:~

File Edit View Search Terminal Help

```
[root@host15 ~]# getsebool -a | grep http
allow_httpd_anon_write --> off
allow_httpd_mod_auth_ntlm_winbind --> off
allow_httpd_mod_auth_pam --> off
allow_httpd_sys_script_anon_write --> off
httpd_builtin_scripting --> on
httpd_can_check_spam --> off
httpd_can_network_connect --> off
httpd_can_network_connect_cobbler --> off
httpd_can_network_connect_db --> off
httpd_can_network_relay --> off
httpd_can_sendmail --> off
httpd_dbus_avahi --> on
httpd_enable_cgi --> on
httpd_enable_ftp_server --> off
httpd_enable_homedirs --> on
httpd_execmem --> off
httpd_read_user_content --> off
httpd_setrlimit --> off
httpd_ssi_exec --> off
httpd_tmp_exec --> off
httpd_tty_comm --> on
httpd_unified --> on
httpd_use_cifs --> off
httpd_use_gpg --> off
httpd_use_nfs --> off
[root@host15 ~]#
```

root@host15:~

File Edit View Search Terminal Help

```
[root@host15 ~]# getsebool -a | grep nfs
allow_ftpd_use_nfs --> off
allow_nfsd_anon_write --> off
git_system_use_nfs --> off
httpd_use_nfs --> off
nfs_export_all_ro --> on
nfs_export_all_rw --> on
qemu_use_nfs --> on
samba_share_nfs --> off
use_nfs_home_dirs --> on
virt_use_nfs --> off
xen_use_nfs --> off
[root@host15 ~]#
```

root@host14:~

File Edit View Search Terminal Help

```
# must have permissions of 711, ~userid/public_html must have permissions
# of 755, and documents contained therein must be world-readable.
# Otherwise, the client will only receive a "403 Forbidden" message.
#
# See also: http://httpd.apache.org/docs/misc/FAQ.html#forbidden
#
<IfModule mod_userdir.c>
    #
    # UserDir is disabled by default since it can confirm the presence
    # of a username on the system (depending on home directory
    # permissions).
    #
    #UserDir disabled

    #
    # To enable requests to /~user/ to serve the user's public_html
    # directory, remove the "UserDir disabled" line above, and uncomment
    # the following line instead:
    #
    UserDir public_html

</IfModule>

-- INSERT --
```

Apache vs. SELinux

- Allowing Apache to access Paul's home directory so we can access http://host15.tc.redhat.com/~paul
  - Set permissions to allow httpd to access /home/paul

root@host14:~

File Edit View Search Terminal Help

```
[root@host14 ~]# ls -l /home/
total 24
drwx------. 2 george         george         4096 May  3 23:43 george
drwx------. 2 john           john           4096 May  3 23:43 john
drwx------. 2 paul           paul           4096 May  3 23:43 paul
drwx------. 2 ringo          ringo          4096 May  3 23:43 ringo
drwx------. 4 tcameron       tcameron       4096 May  3 23:34 tcameron
drwx------. 4 thomas.cameron thomas.cameron 4096 May  3 23:34 thomas.cameron
[root@host14 ~]# chmod o+x /home/paul/
[root@host14 ~]# ls -l /home/
total 24
drwx------. 2 george         george         4096 May  3 23:43 george
drwx------. 2 john           john           4096 May  3 23:43 john
drwx-----x. 2 paul           paul           4096 May  3 23:43 paul
drwx------. 2 ringo          ringo          4096 May  3 23:43 ringo
drwx------. 4 tcameron       tcameron       4096 May  3 23:34 tcameron
drwx------. 4 thomas.cameron thomas.cameron 4096 May  3 23:34 thomas.cameron
[root@host14 ~]#
```

Apache vs. SELinux

- Allowing Apache to access Paul's home directory so we can access http://host15.tc.redhat.com/~paul
  - Restart Apache

root@host14:~

File Edit View Search Terminal Help

```
[root@host14 ~]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
[root@host14 ~]#
```

Apache vs. SELinux

- Allowing Apache to access Paul's home directory so we can access http://host15.tc.redhat.com/~paul
  - As Paul, create index.html

paul@host14:~/public_html

File Edit View Search Terminal Help

```
[paul@host14 ~]$ mkdir public_html
[paul@host14 ~]$ cd public_html/
[paul@host14 public_html]$ echo "This is my page" > index.html
[paul@host14 public_html]$
```

Apache vs. SELinux

- Allowing Apache to access Paul's home directory so we can access http://host15.tc.redhat.com/~paul
  - Fire up the browser

403 Forbidden - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://host14.tc.redhat.com/~paul/

Most Visited Zimbra Red Hat Application... Red Hat -- Intranet ... American Express B... RHN Satellite - Sign... MySouthwest

403 Forbidden

Forbidden

You don't have permission to access /~paul/ on this server.

Apache/2.2.15 (Red Hat) Server at host14.tc.redhat.com Port 80

Done

Things to check

- /var/log/httpd/access.log

root@host15:~

File Edit View Search Terminal Help

```
[root@host15 ~]# tail /var/log/httpd/access_log
10.10.10.3 - - [04/May/2011:02:23:32 -0400] "GET /~paul HTTP/1.1" 403 294 "-" "M
ozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.17) Gecko/20110421 Red Hat/3.6
.17-1.el6_0 Firefox/3.6.17"
10.10.10.3 - - [04/May/2011:02:23:33 -0400] "GET /~paul HTTP/1.1" 403 294 "-" "M
ozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.17) Gecko/20110421 Red Hat/3.6
.17-1.el6_0 Firefox/3.6.17"
10.10.10.3 - - [04/May/2011:02:23:33 -0400] "GET /~paul HTTP/1.1" 403 294 "-" "M
ozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.2.17) Gecko/20110421 Red Hat/3.6
.17-1.el6_0 Firefox/3.6.17"
[root@host15 ~]#
```

Things to check

- /var/log/httpd/error.log

root@host15:~

File Edit View Search Terminal Help

```
[root@host15 ~]# cat /var/log/httpd/error_log
[Wed May 04 02:23:21 2011] [notice] SELinux policy enabled; httpd running as con
text unconfined_u:system_r:httpd_t:s0
[Wed May 04 02:23:21 2011] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin
/suexec)
[Wed May 04 02:23:21 2011] [notice] Digest: generating secret for digest authent
ication ...
[Wed May 04 02:23:21 2011] [notice] Digest: done
[Wed May 04 02:23:21 2011] [warn] ./mod_dnssd.c: No services found to register
[Wed May 04 02:23:21 2011] [notice] Apache/2.2.15 (Unix) DAV/2 configured -- res
uming normal operations
[Wed May 04 02:23:32 2011] [error] [client 10.10.10.3] (13)Permission denied: ac
cess to /~paul denied
[Wed May 04 02:23:33 2011] [error] [client 10.10.10.3] (13)Permission denied: ac
cess to /~paul denied
[Wed May 04 02:23:33 2011] [error] [client 10.10.10.3] (13)Permission denied: ac
cess to /~paul denied
[root@host15 ~]#
```

Things to check

- /var/log/messages

root@host14:~

File Edit View Search Terminal Help

```
May  4 00:06:03 host14 setroubleshoot: SELinux is preventing the http daemon fro
m reading users' home directories. For complete SELinux messages. run sealert -l
 3c93734c-4444-4df9-b29a-6ece47b0b2cc
May  4 00:06:03 host14 setroubleshoot: SELinux is preventing the http daemon fro
m reading users' home directories. For complete SELinux messages. run sealert -l
 3c93734c-4444-4df9-b29a-6ece47b0b2cc
```

root@host14:~

File Edit View Search Terminal Help

```
[root@host14 ~]# sealert -l 3c93734c-4444-4df9-b29a-6ece47b0b2cc

Summary:

SELinux is preventing the http daemon from reading users' home directories.

Detailed Description:

SELinux has denied the http daemon access to users' home directories. Someone is
attempting to access your home directories via your http daemon. If you have not
setup httpd to share home directories, this probably signals an intrusion
attempt.

Allowing Access:

If you want the http daemon to share home directories you need to turn on the
httpd_enable_homedirs boolean: "setsebool -P httpd_enable_homedirs=1" You may
need to also label the content that you wish to share. The man page
httpd_selinux will have further information. 'man httpd_selinux'.

Fix Command:

setsebool -P httpd_enable_homedirs=1
```

root@host14:~

File Edit View Search Terminal Help

```
setsebool -P httpd_enable_homedirs=1

Additional Information:

Source Context                system_u:system_r:httpd_t:s0
Target Context                unconfined_u:object_r:home_root_t:s0
Target Objects                /home/paul/public_html/index.html [ file ]
Source                        httpd
Source Path                   /usr/sbin/httpd
Port                          <Unknown>
Host                          host14.tc.redhat.com
Source RPM Packages           httpd-2.2.15-5.el6
Target RPM Packages
Policy RPM                    selinux-policy-3.7.19-54.el6_0.5
Selinux Enabled               True
Policy Type                   targeted
Enforcing Mode                Enforcing
Plugin Name                   httpd_enable_homedirs
Host Name                     host14.tc.redhat.com
Platform                      Linux host14.tc.redhat.com
                              2.6.32-71.24.1.el6.x86_64 #1 SMP Sat Mar 26
                              16:05:19 EDT 2011 x86_64 x86_64
Alert Count                   2
First Seen                    Wed May  4 00:06:01 2011
```

```
root@host14:~
File  Edit  View  Search  Terminal  Help
                                2.6.32-71.24.1.el6.x86_64 #1 SMP Sat Mar 26
                                16:05:19 EDT 2011 x86_64 x86_64
Alert Count                     2
First Seen                      Wed May  4 00:06:01 2011
Last Seen                       Wed May  4 00:06:01 2011
Local ID                        3c93734c-4444-4df9-b29a-6ece47b0b2cc
Line Numbers

Raw Audit Messages

node=host14.tc.redhat.com type=AVC msg=audit(1304485561.334:21462): avc:  denied
  { getattr } for  pid=1586 comm="httpd" path="/home/paul/public_html/index.html
" dev=vda3 ino=285113 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_
u:object_r:home_root_t:s0 tclass=file

node=host14.tc.redhat.com type=SYSCALL msg=audit(1304485561.334:21462): arch=c00
0003e syscall=6 success=no exit=-13 a0=7f0e9a1afee0 a1=7ffffc84b500 a2=7ffffc84b
500 a3=1 items=0 ppid=1575 pid=1586 auid=4294967295 uid=48 gid=48 euid=48 suid=4
8 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="
/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)



[root@host14 ~]#
```

root@host14:~

File Edit View Search Terminal Help

```
                                16:05:19 EDT 2011 x86_64 x86_64
Alert Count                     2
First Seen                      Wed May  4 00:06:01 2011
Last Seen                       Wed May  4 00:06:01 2011
Local ID                        3c93734c-4444-4df9-b29a-6ece47b0b2cc
Line Numbers

Raw Audit Messages

node=host14.tc.redhat.com type=AVC msg=audit(1304485561.334:21462): avc:  denied
  { getattr } for  pid=1586 comm="httpd" path="/home/paul/public_html/index.html
" dev=vda3 ino=285113 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_
u:object_r:home_root_t:s0 tclass=file

node=host14.tc.redhat.com type=SYSCALL msg=audit(1304485561.334:21462): arch=c00
0003e syscall=6 success=no exit=-13 a0=7f0e9a1afee0 a1=7ffffc84b500 a2=7ffffc84b
500 a3=1 items=0 ppid=1575 pid=1586 auid=4294967295 uid=48 gid=48 euid=48 suid=4
8 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="
/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0 key=(null)



[root@host14 ~]# setsebool -P httpd_enable_homedirs=1
[root@host14 ~]#
```

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://host15.tc.redhat.com/~paul/

Google

Most Visited Zimbra Red Hat Application... Red Hat -- Intranet ... American Express B... RHN Satellite - Sign... MySouthwest

http://host15.tc...dhat.com/~paul/

This is my page

Done

How can I see what booleans have been set?

- /etc/selinux/targeted/modules/active/booleans.local

root@host15:~

File Edit View Search Terminal Help

```
[root@host15 ~]# cat /etc/selinux/targeted/modules/active/booleans.local
# This file is auto-generated by libsemanage
# Do not edit directly.

httpd_enable_homedirs=1
[root@host15 ~]#
```

When in doubt...

- Check labels

paul@host15:~

File Edit View Search Terminal Help

```
[paul@host15 ~]$ mkdir public_html
[paul@host15 ~]$ echo "This is my page" > public_html/index.html
[paul@host15 ~]$ ls -Z
drwxrwxr-x. paul paul unconfined_u:object_r:user_home_t:s0 public_html
[paul@host15 ~]$
[paul@host15 ~]$
[paul@host15 ~]$
[paul@host15 ~]$ restorecon -vR /home/paul/
restorecon reset /home/paul/public_html context unconfined_u:object_r:user_home_
t:s0->unconfined_u:object_r:httpd_user_content_t:s0
restorecon reset /home/paul/public_html/index.html context unconfined_u:object_r
:user_home_t:s0->unconfined_u:object_r:httpd_user_content_t:s0
[paul@host15 ~]$
```

Other things to check

- /var/log/audit/audit.log

root@host15:~

File Edit View Search Terminal Help

```
type=AVC msg=audit(1304493885.700:62): avc:  denied  { name_connect } for  pid=1
875 comm="httpd" dest=143 scontext=unconfined_u:system_r:httpd_t:s0 tcontext=sys
tem_u:object_r:pop_port_t:s0 tclass=tcp_socket
type=SYSCALL msg=audit(1304493885.700:62): arch=c000003e syscall=42 success=no e
xit=-13 a0=c a1=7fcd12628b50 a2=10 a3=40 items=0 ppid=1867 pid=1875 auid=0 uid=4
8 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=3 comm
="httpd" exe="/usr/sbin/httpd" subj=unconfined_u:system_r:httpd_t:s0 key=(null)
```

sealert

- Since the log entries aren't terribly intuitive, we can use sealert -a against them
- In this example, setting up SquirrelMail

root@host15:~

File Edit View Search Terminal Help

```
[root@host15 ~]# sealert -a /var/log/audit/audit.log
100% donefound 1 alerts in /var/log/audit/audit.log
--------------------------------------------------------------------------------


Summary:

SELinux is preventing the http daemon from sending mail.

Detailed Description:

SELinux has denied the http daemon from sending mail. An httpd script is trying
to connect to a mail port or execute the sendmail command. If you did not setup
httpd to sendmail, this could signal a intrusion attempt.

Allowing Access:

If you want httpd to send mail you need to turn on the httpd_can_sendmail
boolean: "setsebool -P httpd_can_sendmail=1"

Fix Command:

setsebool -P httpd_can_sendmail=1
```

semanage

- You can use semanage to make changes to policy.
  - File context (semanage fcontext)
  - Network port (semanage port)
  - Network interface (semanage interface)
  - Booleans (semanage boolean)
  - others...
- Note that semanage only changes the policy
  - Use chcon or restorecon to actually label the filesystem

semanage

- semanage is telling us the context is wrong, but the list of options it's giving us is a bit overwhelming

Another example

- Set up httpd to serve content out of someplace weird
  - /foo/bar

root@t510:~

File Edit View Search Terminal Help

```
[root@t510 ~]# mkdir -p /foo/bar
[root@t510 ~]# ls -ld /foo/
drwxr-xr-x. 3 root root 4096 May  4 09:50 /foo/
[root@t510 ~]# ls -ld /foo/bar
drwxr-xr-x. 2 root root 4096 May  4 09:50 /foo/bar
[root@t510 ~]# echo "this is my index" > /foo/bar/index.html
[root@t510 ~]# ls -l /foo/bar
total 4
-rw-r--r--. 1 root root 17 May  4 09:51 index.html
[root@t510 ~]#
```

root@t510:~

File Edit View Search Terminal Help

```
[root@t510 ~]# tail -8 /etc/httpd/conf/httpd.conf

<VirtualHost *:80>
    ServerAdmin webmaster@dummy-host.example.com
    DocumentRoot /foo/bar
    ServerName dummy-host.example.com
    ErrorLog logs/dummy-host.example.com-error_log
    CustomLog logs/dummy-host.example.com-access_log common
</VirtualHost>
[root@t510 ~]#
```

root@t510:~

File Edit View Search Terminal Help

```
[root@t510 ~]# echo "this is dummy-host.example.com" > /foo/bar/index.html
[root@t510 ~]#
```

root@t510:~

File Edit View Search Terminal Help

```
[root@t510 ~]# service httpd start
Starting httpd: Warning: DocumentRoot [/foo/bar] does not exist
                                                           [  OK  ]
[root@t510 ~]#
```

sealert

- For a graphical login, you'll get an setroubleshoot browser alert.
- You can get back to the SELinux Alert Browser any time with sealert -a

Wed May 4, 9:53 AM Thomas Cameron (Work)

New SELinux security alert

AVC denial, click icon to view

Dismiss Show

root@t510:~

File Edit View Search Terminal Help

```
[root@t510 ~]# service httpd start
Starting httpd: Warning: DocumentRoot [/foo/bar] does not exist
                                                           [  OK  ]
[root@t510 ~]#
```

SELinux Security Alerts

SELinux has detected suspicious behavior on your system

Alert **1** of **2** Show all...

SELinux is preventing /usr/sbin/httpd from using potentially mislabeled files foo.

Today on Wed May 4, 2011 at 09:22:54 AM EDT

SELinux has denied the httpd access to potentially mislabeled files foo. This means that SELinux will not allow httpd to use these files. If httpd should be allowed this access to these files you should change the file context to one of the following types, logfile, httpd_nutups_cgi_content_t, sysctl_net_t, httpd_config_t, httpd_cobbler_rw_content_t, calamaris_www_t, httpd_prewikka_script_exec_t, var_spool_t, abrt_var_run_t, httpd_cache_t, httpd_tmpfs_t, httpd_sys_script_exec_t, httpd_munin_rw_content_t, iso9660_t, udev_tbl_t, httpd_tmp_t, smokeping_var_lib_t, httpd_git_script_exec_t, var_lib_t, var_run_t, httpd_cvs_script_exec_t, mysqld_etc_t, setrans_var_run_t, cvs_data_t, configfile, sysctl_crypto_t, dbusd_etc_t, sysctl_t, abrt_t, bin_t, lib_t, mnt_t, root_t, var_lib_t, tmp_t, usr_t, var_t, httpd_squirrelmail_t, httpd_bugzilla_rw_content_t, httpd_nutups_cgi_script_exec_t, var_log_t, samba_var_t, device_t, avahi_var_run_t, etc_t, net_conf_t, proc_t, httpd_cvs_rw_content_t, httpd_git_rw_content_t,

This alert has occurred **4 times** since Wed May 4, 2011 at 09:08:46 AM EDT

Show full error output

Allowing Access

If you want to change the file context of foo so that the httpd daemon can access it, you need to execute it using semanage fcontext -a -t FILE_TYPE 'foo'.

where FILE_TYPE is one of the following: logfile, httpd_nutups_cgi_content_t, sysctl_net_t, httpd_config_t, httpd_cobbler_rw_content_t, calamaris_www_t, httpd_prewikka_script_exec_t, var_spool_t, abrt_var_run_t, httpd_cache_t, httpd_tmpfs_t, httpd_sys_script_exec_t, httpd_munin_rw_content_t, iso9660_t, udev_tbl_t, httpd_tmp_t, smokeping_var_lib_t, httpd_git_script_exec_t, var_lib_t, var_run_t, httpd_cvs_script_exec_t, mysqld_etc_t, setrans_var_run_t, cvs_data_t, configfile, sysctl_crypto_t, dbusd_etc_t, sysctl_t, abrt_t, bin_t, lib_t, mnt_t, root_t, var_lib_t, tmp_t, usr_t, var_t, httpd_squirrelmail_t, httpd_bugzilla_rw_content_t,

Ignore Alert | Delete | Report this Bug... | Copy to Clipboard

Policy Version: 3.7.19-54.el6_0.5

Close | Previous | Next

semanage

- Where would we get a hint as to what the context for /foo should be?

root@t510:~

File Edit View Search Terminal Help

```
[root@t510 ~]# ls -Z /var/www/
drwxr-xr-x. root      root system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x. root      root system_u:object_r:httpd_sys_content_t:s0 error
drwxr-xr-x. root      root system_u:object_r:httpd_sys_content_t:s0 html
drwxr-xr-x. root      root system_u:object_r:httpd_sys_content_t:s0 icons
drwxr-xr-x. root      root system_u:object_r:httpd_sys_content_t:s0 manual
drwxr-xr-x. webalizer root system_u:object_r:httpd_sys_content_t:s0 usage
[root@t510 ~]#
[root@t510 ~]#
[root@t510 ~]#
[root@t510 ~]# semanage fcontext -a -t httpd_sys_content_t "/foo(/.*)?"
[root@t510 ~]#
```

Now fix the label

- Remember we are just updating the definition of the file context under /etc/selinux. That way if the filesystem gets relabeled, the context will be set correctly. Afterwards, we need to actually set the context of the directory with chcon or restorecon

root@t510:~

File Edit View Search Terminal Help

```
[root@t510 ~]# mkdir -p /foo/bar
[root@t510 ~]#
[root@t510 ~]# echo "this is dummy-host.example.com" > /foo/bar/index.html
[root@t510 ~]#
[root@t510 ~]#
[root@t510 ~]# ls -Z /foo/
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 bar
[root@t510 ~]#
[root@t510 ~]#
[root@t510 ~]# semanage fcontext -a -t httpd_sys_content_t "/foo(/.*)?"
[root@t510 ~]#
[root@t510 ~]#
[root@t510 ~]# ls -Z /foo/
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 bar
[root@t510 ~]#
[root@t510 ~]#
[root@t510 ~]# restorecon -vR /foo/
restorecon reset /foo context unconfined_u:object_r:default_t:s0->system_u:objec
t_r:httpd_sys_content_t:s0
restorecon reset /foo/bar context unconfined_u:object_r:default_t:s0->system_u:o
bject_r:httpd_sys_content_t:s0
restorecon reset /foo/bar/index.html context unconfined_u:object_r:default_t:s0-
>system_u:object_r:httpd_sys_content_t:s0
[root@t510 ~]#
```

root@t510:~

File Edit View Search Terminal Help

```
[root@t510 ~]# service httpd start
Starting httpd:                                            [  OK  ]
[root@t510 ~]#
```

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://dummy-host.example.com/

Google

Most Visited Zimbra Red Hat Application... Red Hat -- Intranet ... American Express B... RHN Satellite - Sign...

http://dummy-host.example.com/

this is dummy-host.example.com

Done

semanage hint

- You can see the syntax for that regular expression in /etc/selinux/targeted/contexts/files/file_contexts

tcameron@t510:/etc/selinux/targeted/contexts/files

File Edit View Search Terminal Help

```
/var/www(/.*)?  system_u:object_r:httpd_sys_content_t:s0
/opt/cvs(/.*)?  system_u:object_r:cvs_data_t:s0
/var/cvs(/.*)?  system_u:object_r:cvs_data_t:s0
/etc/dcc(/.*)?  system_u:object_r:dcc_var_t:s0
/var/dcc(/.*)?  system_u:object_r:dcc_var_t:s0
/srv/git(/.*)?  system_u:object_r:git_system_content_t:s0
/etc/gpm(/.*)?  system_u:object_r:gpm_conf_t:s0
/etc/ups(/.*)?  system_u:object_r:nut_conf_t:s0
/etc/nas(/.*)?  system_u:object_r:soundd_etc_t:s0
/etc/tor(/.*)?  system_u:object_r:tor_etc_t:s0
/dev/xvc[0-9]*  -c      system_u:object_r:tty_device_t:s0
/dev/dm-[0-9]+  -b      system_u:object_r:fixed_disk_device_t:s0
/dev/tpm[0-9]*  -c      system_u:object_r:tpm_device_t:s0
/dev/uio[0-9]+  -c      system_u:object_r:userio_device_t:s0
/etc/ppp(/.*)?  --      system_u:object_r:pppd_etc_rw_t:s0
/usr/lib(64)?/amanda    -d      system_u:object_r:amanda_usr_lib_t:s0
/usr/lib(64)?/dpkg/.+   --      system_u:object_r:bin_t:s0
/usr/lib(64)?/sa/sa.*   --      system_u:object_r:sysstat_exec_t:s0
/usr/lib(64)?/sendmail  --      system_u:object_r:sendmail_exec_t:s0
/usr/lib(64)?/rpm/rpmd  --      system_u:object_r:bin_t:s0
/usr/lib(64)?/rpm/rpmq  --      system_u:object_r:bin_t:s0
/usr/lib(64)?/rpm/rpmv  --      system_u:object_r:bin_t:s0
/usr/lib(64)?/rpm/rpmk  --      system_u:object_r:bin_t:s0
:
```

semanage hint

- Also, local changes to policy are stored in /etc/selinux

root@t510:~

File Edit View Search Terminal Help

```
[root@t510 ~]# find /etc/selinux/ | grep local
/etc/selinux/targeted/modules/active/booleans.local
/etc/selinux/targeted/modules/active/file_contexts.local
/etc/selinux/targeted/contexts/files/file_contexts.local
[root@t510 ~]#
```

Creating Basic Policies

audit2why and audit2allow are two utlities to tell you why something was denied and how to allow it

Note that just because audit2allow will create a policy, that does not mean it is the smartest thing to do! Consider security implications before applying policies!

Creating Basic Policies

In the following example, xauth is leaking file descriptors and SELinux is blocking it (well, it would be if it didn't have a permissive type).

Per MITRE, leaking file descriptors is dangerous - “A process does not close sensitive file descriptors before invoking a child process, which allows the child to perform unauthorized I/O operations using those descriptors.”

Creating Basic Policies

You can use audit2why or sealert -b to see why this was blocked:

root@selinux:~

File Edit View Terminal Help

```
type=AVC msg=audit(1276871601.320:11): avc:  denied  { read write } for  pid=165
8 comm="xauth" path="/dev/console" dev=devtmpfs ino=4918 scontext=system_u:uncon
fined_r:xauth_t:s0 tcontext=system_u:object_r:console_device_t:s0 tclass=chr_fil
e

        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow t
his access.

type=AVC msg=audit(1276871601.320:11): avc:  denied  { read write } for  pid=165
8 comm="xauth" path="/dev/console" dev=devtmpfs ino=4918 scontext=system_u:uncon
fined_r:xauth_t:s0 tcontext=system_u:object_r:console_device_t:s0 tclass=chr_fil
e

        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow t
his access.

[root@selinux ~]#
```

SELinux Security Alerts (on selinux.tc.redhat.com)

SELinux has detected suspicious behavior on your system

Alert **1** of **1** Show all...

SELinux is preventing /usr/bin/xauth access to a leaked /dev/console file descriptor.

Today on Fri Jun 18, 2010 at 09:33:21 AM CDT

[xauth has a permissive type (xauth_t). This access was not denied.]

SELinux denied access requested by the xauth command. It looks like this is either a leaked descriptor or xauth output was redirected to a file it is not allowed to access. Leaks usually can be ignored since SELinux is just closing the leak and reporting the error. The application does not use the descriptor, so it will run properly. If this is a redirection, you will not get output in the /dev/console. You should generate a bugzilla on selinux-policy, and it will get routed to the appropriate package. You can safely ignore this avc.

This alert has occurred **14 times** since Thu Jun 17, 2010 at 01:27:12 PM CDT

Show full error output

SELinux denied access requested by the xauth command. It looks like this is either a leaked descriptor or xauth output was redirected to a file it is not allowed to access. Leaks usually can be ignored since SELinux is just closing the leak and reporting the error. The application does not use the descriptor, so it will run properly. If this is a redirection, you will not get output in the /dev/console. You should generate a bugzilla on selinux-policy, and it will get routed to the appropriate package. You can safely ignore this avc.

Allowing Access

You can generate a local policy module to allow this access - see FAQ

Additional Information

Ignore Alert | Delete | Report this Bug... | Copy to Clipboard

Policy Version: 3.7.19-24.el6 | Close

Creating Basic Policies

As indicated in the SE Troubleshoot Browser, you can read the SELinux FAQ at http://bit.ly/8XRSEh for more details about creating policy.

Grab all the xauth entries from /var/log/audit/audit.log and run them against audit2allow and output them to a policy called xauthlocal:

root@selinux:~

File Edit View Terminal Help

```
[root@selinux ~]# grep xauth /var/log/audit/audit.log | audit2allow -M localxaut
h
******************* IMPORTANT ***********************
To make this policy package active, execute:

semodule -i localxauth.pp

[root@selinux ~]# cat localxauth.te

module localxauth 1.0;

require {
        type xauth_t;
        type console_device_t;
        class chr_file { read write };
}

#============= xauth_t ==============
allow xauth_t console_device_t:chr_file { read write };
[root@selinux ~]# semodule -i localxauth.pp
[root@selinux ~]#
```

Creating Basic Policies

Now SELinux will allow the leaked descriptors. This method can be used to allow anything that SELinux is blocking.

BE CAREFUL. UNDERSTAND WHAT YOU'RE DOING BEFORE YOU ALLOW BLOCKED ACCESS!

Creating Basic Policies

- You should ALWAYS report things like this as bugs. Open a ticket, don't rely on Bugzilla - there is no SLA for BZ.

Activating SELinux

SELinux is enabled or disabled in /etc/sysconfig/selinux (which is actually just a link to /etc/selinux/config)

root@selinux:~

File Edit View Terminal Help

```
[root@selinux ~]# cat /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted


[root@selinux ~]#
```

Activating SELinux

To activate SELinux on your machine, there are a couple of ways to do it.

- Set SELINUX=permissive in /etc/sysconfig/selinux
- touch /.autorelabel
- reboot
- Change to enforcing mode

selinux Virtual Machine

File Virtual Machine View Send Key

```
                                                           [  OK  ]
Remounting root filesystem in read-write mode:             [  OK  ]
Mounting local filesystems:                                [  OK  ]
Enabling local filesystem quotas:                          [  OK  ]
                Welcome to Red Hat Enterprise Linux Server
                Press 'I' to enter interactive startup.
Starting udev:                                             [  OK  ]
Setting hostname selinux.tc.redhat.com:                    [  OK  ]
Setting up Logical Volume Management:   2 logical volume(s) in volume group "vg_
dhcp176102" now active
                                                           [  OK  ]
Checking filesystems
/dev/mapper/vg_dhcp176102-lv_root: clean, 95923/429088 files, 894087/1714176 blo
cks
/dev/vda1: clean, 39/128016 files, 54480/512000 blocks
                                                           [  OK  ]
Remounting root filesystem in read-write mode:             [  OK  ]
Mounting local filesystems:                                [  OK  ]
Enabling local filesystem quotas:                          [  OK  ]

*** Warning -- SELinux targeted policy relabel is required.
*** Relabeling could take a very long time, depending on file
*** system size and speed of hard drives.
*****************************************************************************
********_
```

Activating SELinux

Alternatively, you can issue the command "fixfiles relabel" as root

- Reboot after it's done
- Don't do it in runlevel 5 since it deletes everything in /tmp including files the X server needs

selinux Virtual Machine

File Virtual Machine View Send Key

```
Red Hat Enterprise Linux Server release 6.0 Beta (Santiago)
Kernel 2.6.32-36.el6.x86_64 on an x86_64

selinux login: root
Password:
Last login: Thu Jun 17 19:36:46 from dhcp-176-120.dfw.redhat.com
[root@selinux ~]# fixfiles relabel

    Files in the /tmp directory may be labeled incorrectly, this command
    can remove all files in /tmp.  If you choose to remove files from /tmp,
    a reboot will be required after completion.

    Do you wish to clean out the /tmp directory [N]? y
Cleaning out /tmp
_
```

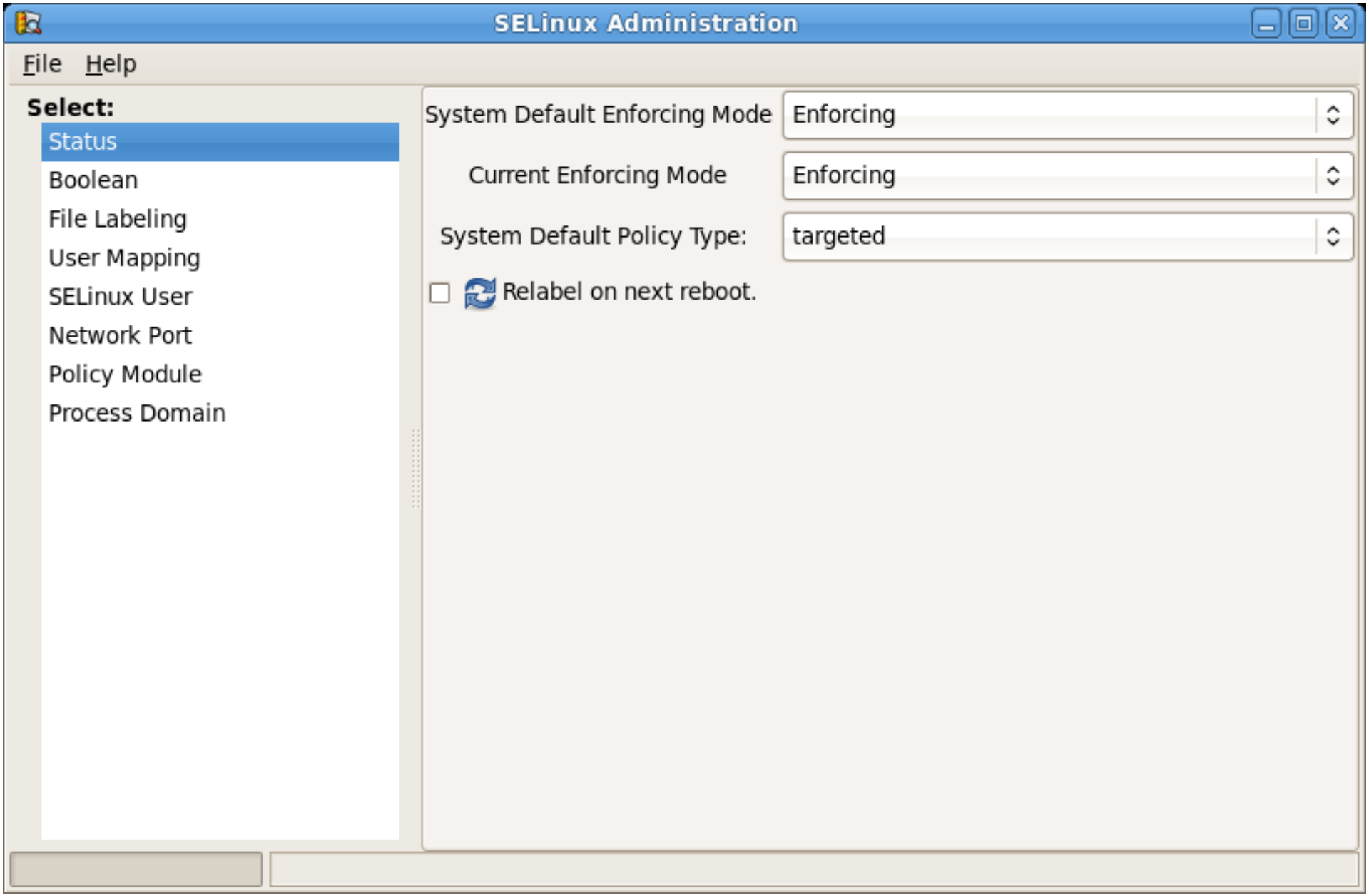
Activating SELinux

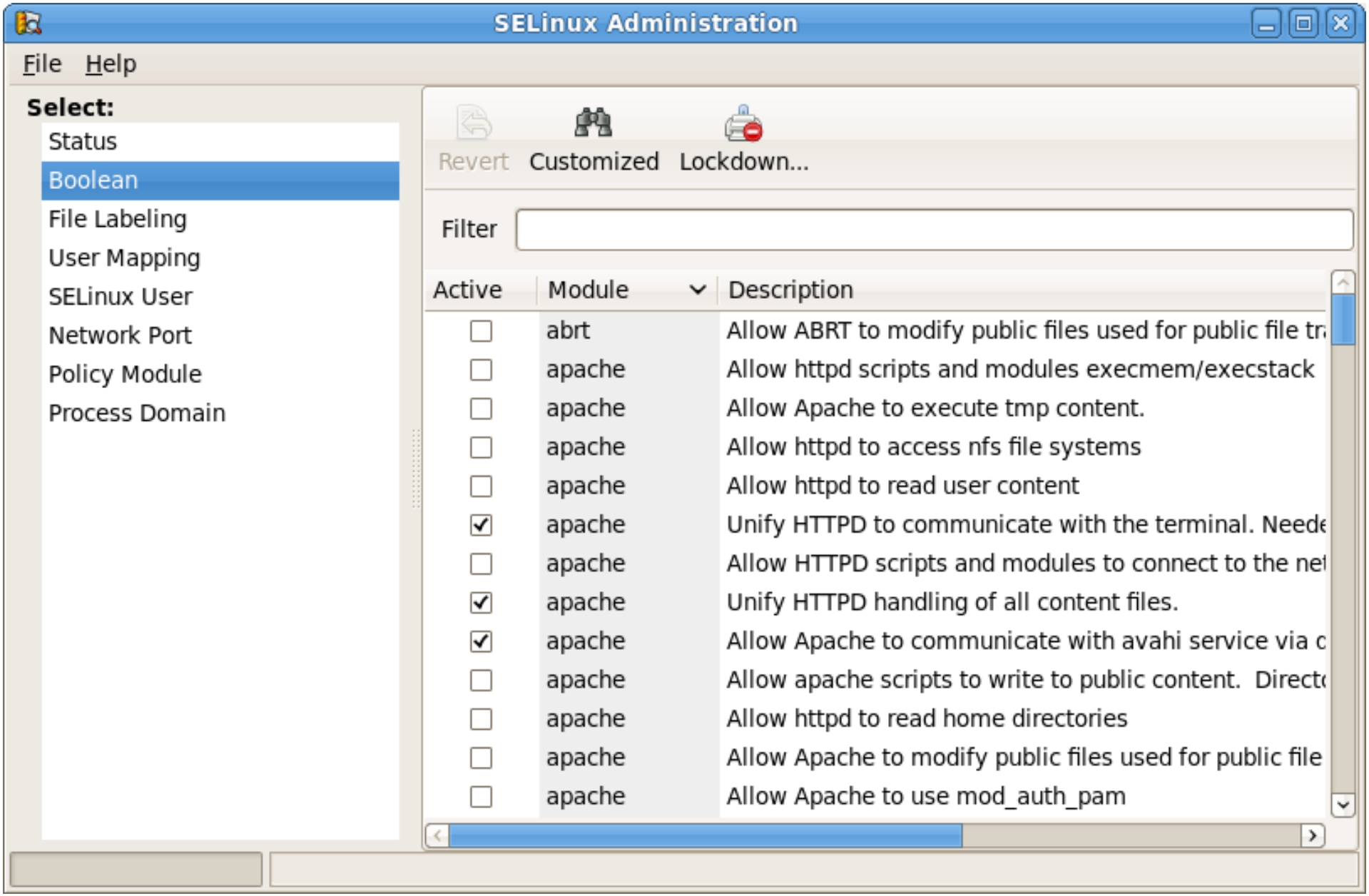
You can also run SELinux in permissive mode, where it will not block anything but it will still log AVC errors.

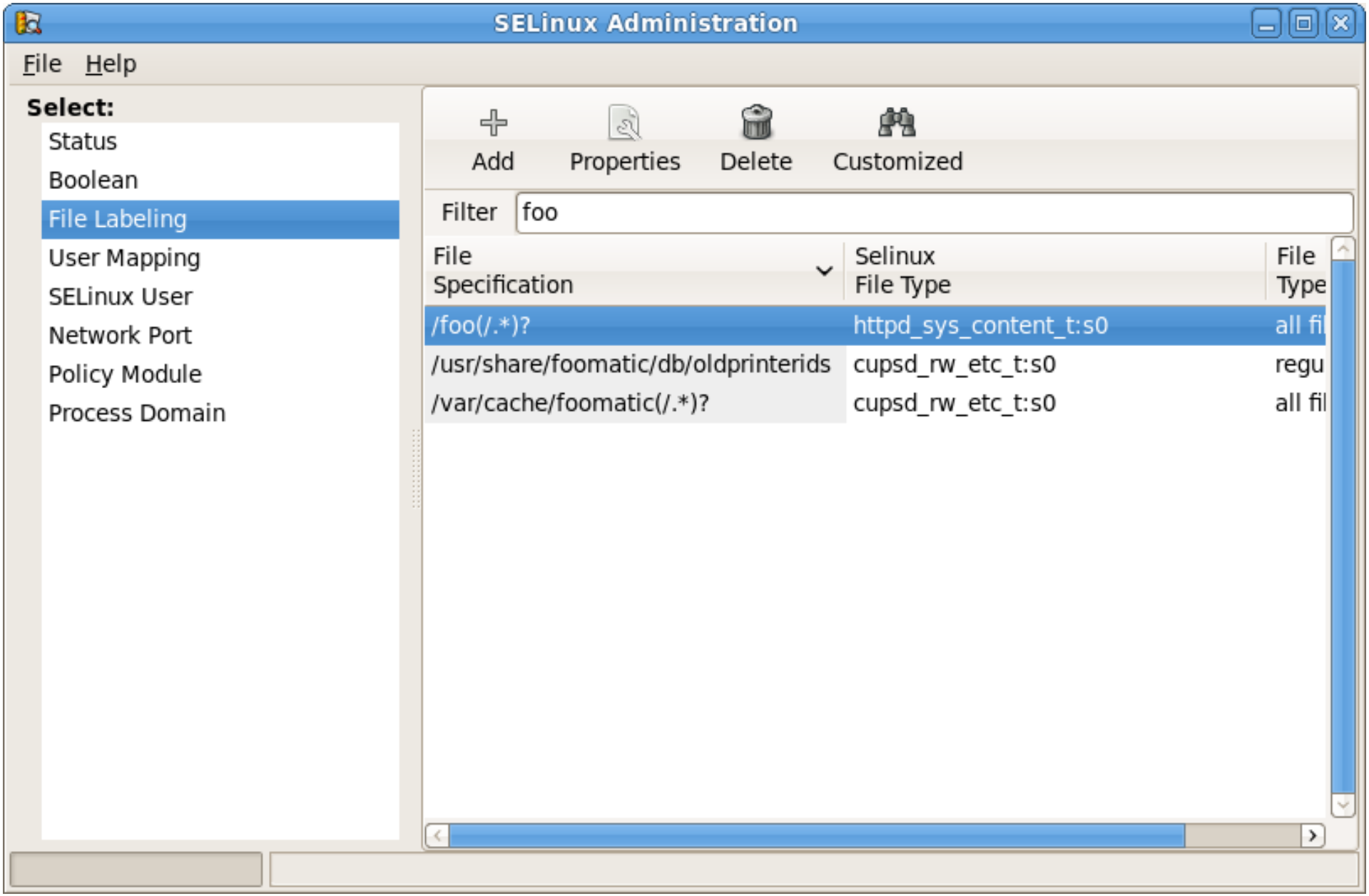
Do this in development environment and set policy or booleans as needed on production machines.

Other tools

- A great graphical interface to SELinux is system-config-selinux
  - System/Administration/SELinux Management


SELinux Administration
File
Help
Select:
Status
Boolean
File Labeling
User Mapping
SELinux User
Network Port
Policy Module
Process Domain
System Default Enforcing Mode
Enforcing
Current Enforcing Mode
Enforcing
System Default Policy Type:
targeted
Relabel on next reboot.


SELinux Administration
File
Help
Select:
Status
Boolean
File Labeling
User Mapping
SELinux User
Network Port
Policy Module
Process Domain
Revert
Customized
Lockdown...
Filter
Active
Module
Description
abrt
Allow ABRT to modify public files used for public file tr
apache
Allow httpd scripts and modules execmem/execstack
apache
Allow Apache to execute tmp content.
apache
Allow httpd to access nfs file systems
apache
Allow httpd to read user content
apache
Unify HTTPD to communicate with the terminal. Neede
apache
Allow HTTPD scripts and modules to connect to the net
apache
Unify HTTPD handling of all content files.
apache
Allow Apache to communicate with avahi service via c
apache
Allow apache scripts to write to public content. Directo
apache
Allow httpd to read home directories
apache
Allow Apache to modify public files used for public file
apache
Allow Apache to use mod_auth_pam


SELinux Administration
File
Help
Select:
Status
Boolean
File Labeling
User Mapping
SELinux User
Network Port
Policy Module
Process Domain
Add
Properties
Delete
Customized
Filter
foo
File Specification
Selinux File Type
File Type
/foo(/.*)?
httpd_sys_content_t:s0
all fil
/usr/share/foomatic/db/oldprinterids
cupsd_rw_etc_t:s0
regu
/var/cache/foomatic(/.*)?
cupsd_rw_etc_t:s0
all fil

Reporting Errors

Please note – if you are getting denials, it means **there is something wrong!**

It's either a configuration issue, which is fairly straight forward, or a problem with code, which **needs to be reported**, or a problem with SELinux policy, which **needs to be reported.**

Please file bug reports! If it's a configuration issue, we'll tell you how to fix it. If it's a code issue, we'll fix it (patches cheerfully accepted).

http://bugzilla.redhat.com/

How Thomas Feels (And Hopefully You Feel) Now

Final Thoughts

Don't turn it off!

SELinux can really save you in the event of a breach.

It's **much** easier to use SELinux today than it was just a few months ago

NSA grade security is available at no extra cost - use it!

Thank You!

- If you liked today's presentation, please let us know!
- Thomas's contact info:
  - thomas@redhat.com
  - choirboy on #rhel on Freenode
  - thomasdcameron on Twitter
  - http://people.redhat.com/tcameron

More Information

- RHEL SELinux Guide:
  - http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/
- Fedora Project SELinux Documentation:
  - http://fedoraproject.org/wiki/SELinux
- fedora-selinux-list (mailing list):
  - https://www.redhat.com/mailman/listinfo
- Red Hat Training - Red Hat Enterprise SELinux Policy Administration:
  - http://red.ht/aoRDyr

More Information

- Dan Walsh's blog:
  - http://danwalsh.livejournal.com/

Questions?

LIKE US ON FACEBOOK

www.facebook.com/redhatinc

FOLLOW US ON TWITTER

www.twitter.com/redhatsummit

TWEET ABOUT IT

#redhat

READ THE BLOG

summitblog.redhat.com

GIVE US FEEDBACK

www.redhat.com/summit/survey

Title Here

- Bullets layer one
  - Bullets layer two
    - Bullets layer three