SECURITY ENHANCED LINUX FOR MERE MORTALS

Or, “Don’t Turn It Off!”

Thomas Cameron, RHCA, RHCSS, RHCDS, RHCVA, RHCX
Digital Transformation Strategist, Red Hat
May 3rd, 2017

AGENDA

Agenda

- About Us
- What is SELinux?
  - Where did it come from?
  - DAC vs. MAC
- So How Does SELinux Work?
  - Labeling and Type Enforcement
- How Do I Deal With Labels?
- Real World Examples

CONTACT INFO

Contact info

- thomas@redhat.com
- @thomasdcameron on Twitter
- https://www.facebook.com/RedHatThomas/
- choirboy on #rhel on Freenode
- http://people.redhat.com/tcameron

ABOUT US

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:
  - https://www.nsa.gov/what-we-do/research/selinux/contributors.shtml
- Red Hat acknowledged by the NSA as a corporate contributor as well.

WHAT IS SELINUX?

Where did it come from?

- 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

HOW I FELT ABOUT SELINUX

What Thomas thought SELinux was

If you feel the same way...

If you feel the same way...

- You're in the right place!

DAC VS. MAC

DAC vs. MAC

- Historically, Linux and Unix systems have used discretionary access control.
  - Ownership (user, group, and other) plus permissions.
  - Users have the ability (discretion) to change permissions on their own files. A user can chmod +rwx his or her home directory, and nothing will stop them. Nothing will prevent other users or processes from accessing the contents of his home directory.

DAC vs. MAC

- Historically, Linux and Unix systems have had discretionary access control.
  - The root user is omnipotent.

DAC vs. MAC

- On a mandatory access control system, there is policy which is administratively set and fixed.
- Even if you change the DAC settings on your home directory, if there is a policy in place which prevents another user or process from accessing it, you're generally safe.

DAC vs. MAC

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

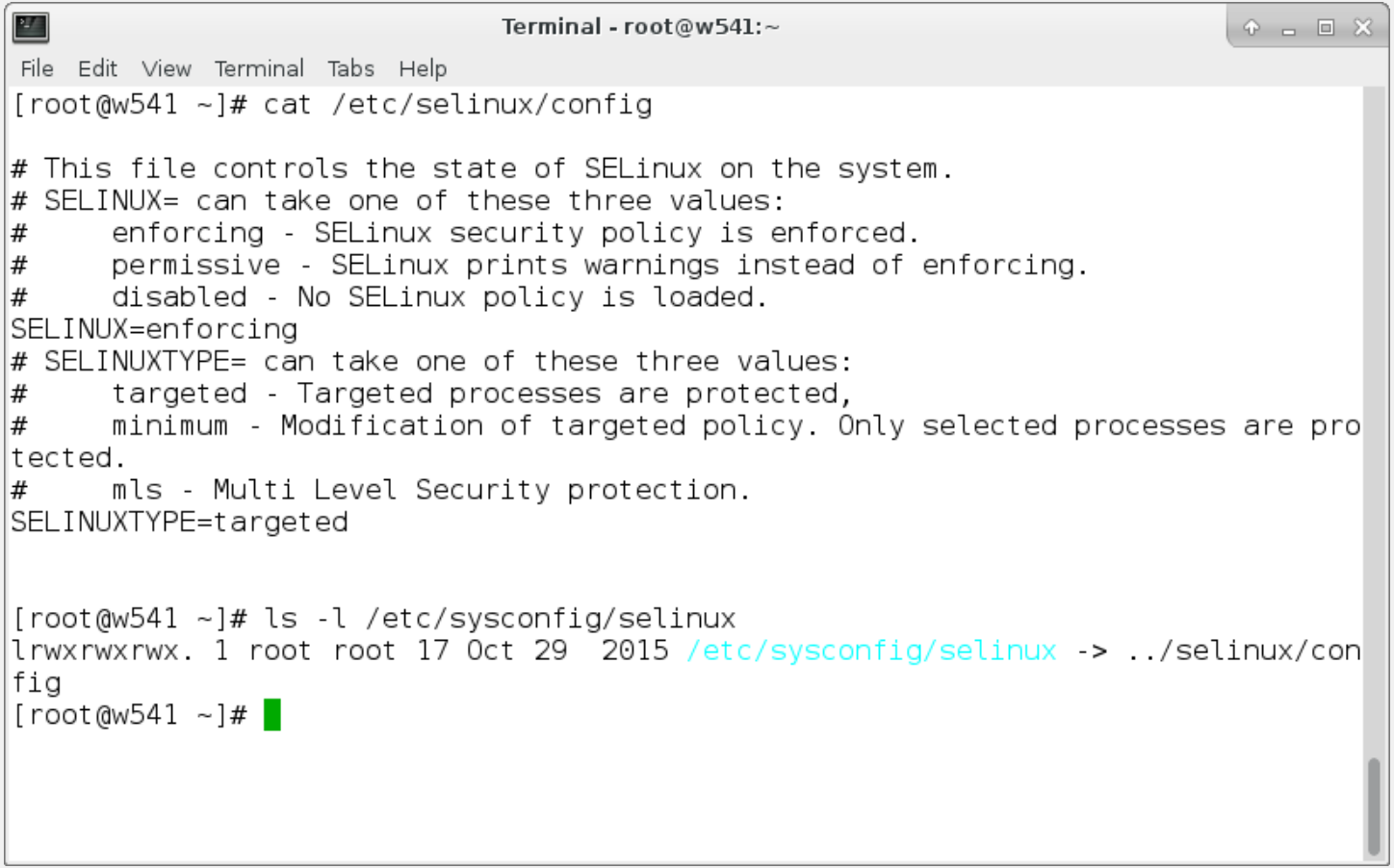
POLICY

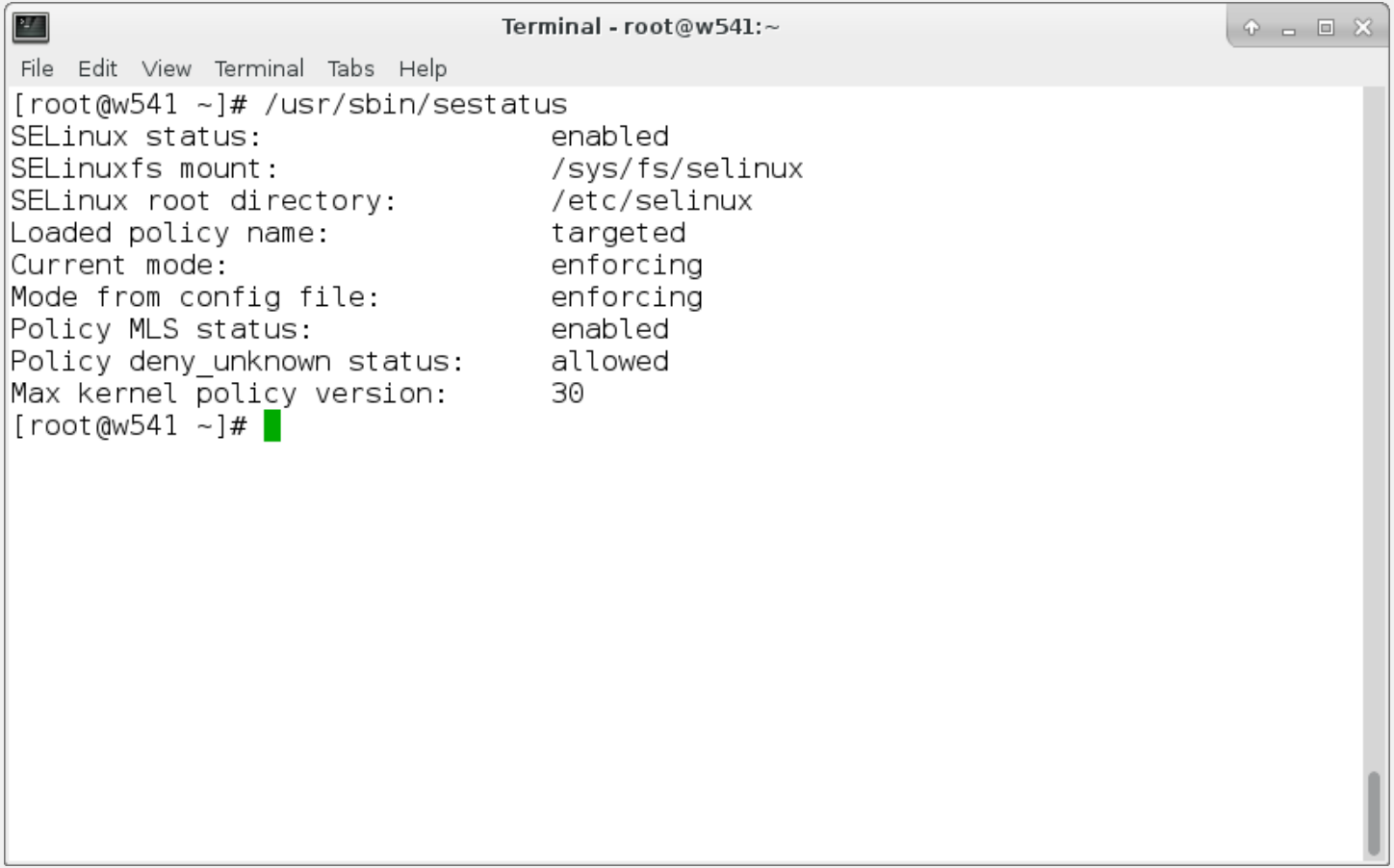
Policy

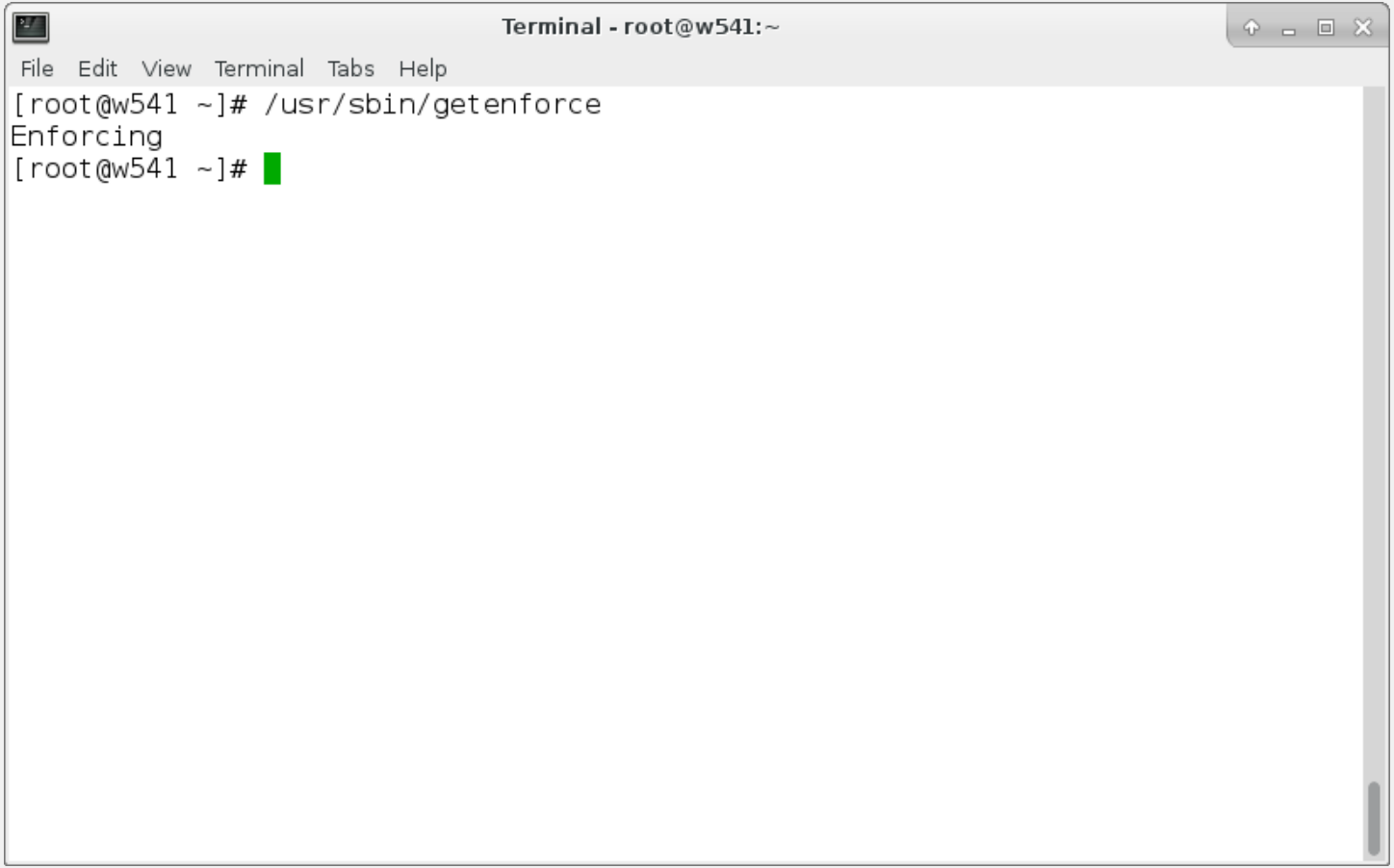
- In Red Hat Enterprise Linux, there are two policies you'll generally see.
  - “targeted” - the default policy
    - Only targeted processes (there are hundreds) are protected by SELinux
    - Everything else is unconfined
  - “mls” - multi-level/multi-category security
    - Out of scope for today's presentation
    - Can be very complex
    - Typically used in TLA government organizations

So How Does SELinux Work?

- You can determine what policy your system is set to use by looking at /etc/selinux/config (which is also symlinked to /etc/sysconfig/selinux)
- You can check via /usr/sbin/sestatus
- You can also check via /usr/sbin/getenforce


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# cat /etc/selinux/config
# 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 three values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are pro
tected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
[root@w541 ~]# ls -l /etc/sysconfig/selinux
lrwxrwxrwx. 1 root root 17 Oct 29 2015 /etc/sysconfig/selinux -> ../selinux/con
fig
[root@w541 ~]#


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# /usr/sbin/sestatus
SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Max kernel policy version: 30
[root@w541 ~]#


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# /usr/sbin/getenforce
Enforcing
[root@w541 ~]#

HOW DOES SELINUX WORK?

So How Does SELinux Work?

- Two of the important concepts to understand with SELinux are:
  - Labeling
  - Type Enforcement

So How Does SELinux Work?

- Labeling
  - Files, processes, ports, etc., are all labeled with an SELinux context.
  - For files and directories, these labels are stored as extended attributes on the filesystem.
  - For processes, ports, etc., the kernel manages these labels.

So How Does SELinux Work?

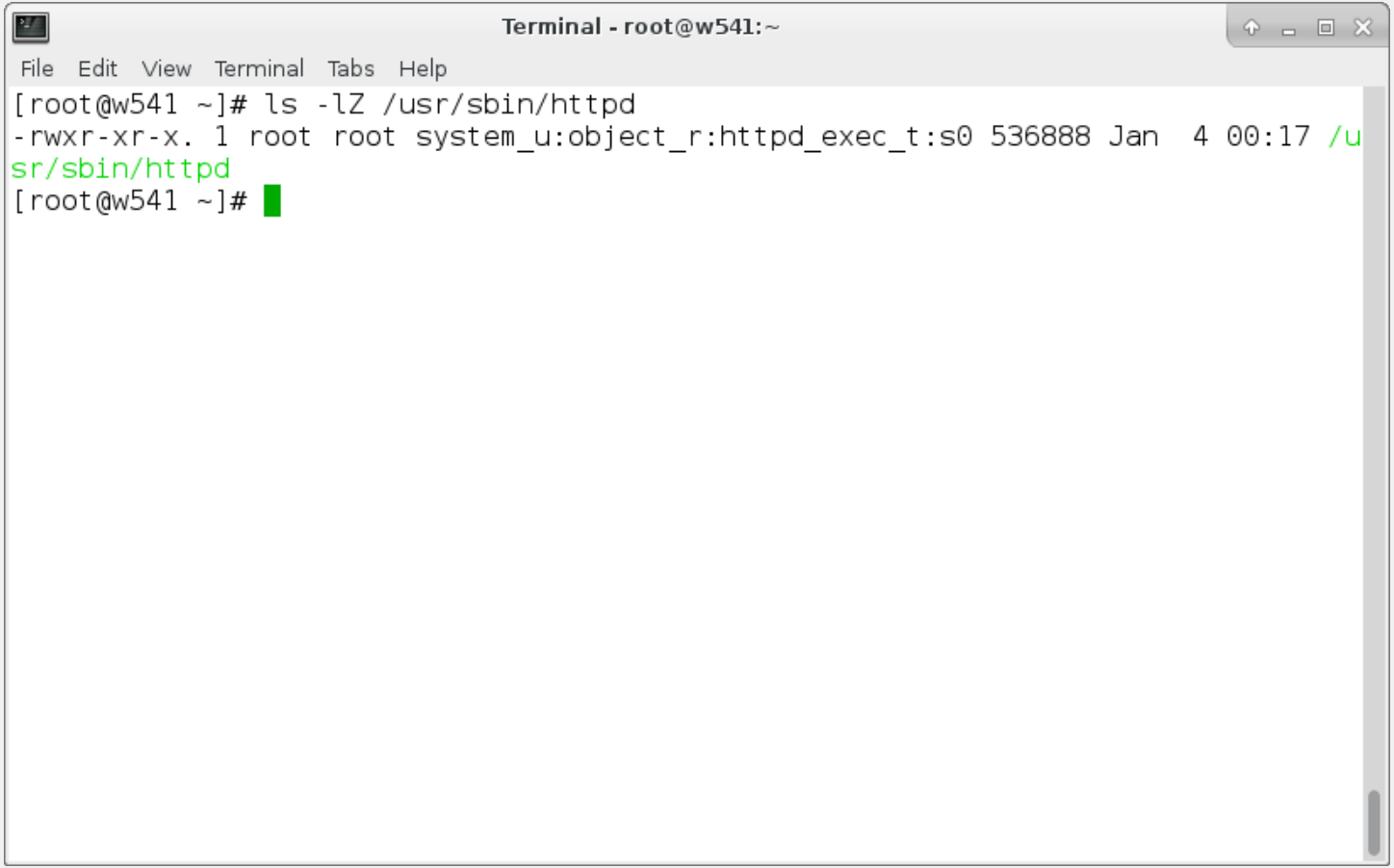
- Labeling
  - Labels are in the format:
    - user:role:type:level(optional)
  - For the purpose of this presentation, we will not deal with the SELinux user, role or level. These are used in more advanced implementations of SELinux (MLS/MCS).
  - What we really care about for today's presentation is the type (remember, labeling and type enforcement).

So How Does SELinux Work?

- We'll look at a fairly complex service, one which provides access from the network, potentially on several ports, and potentially, access to the whole filesystem.
- The Apache web server is not necessarily insecure, it is just very wide ranging in its access.

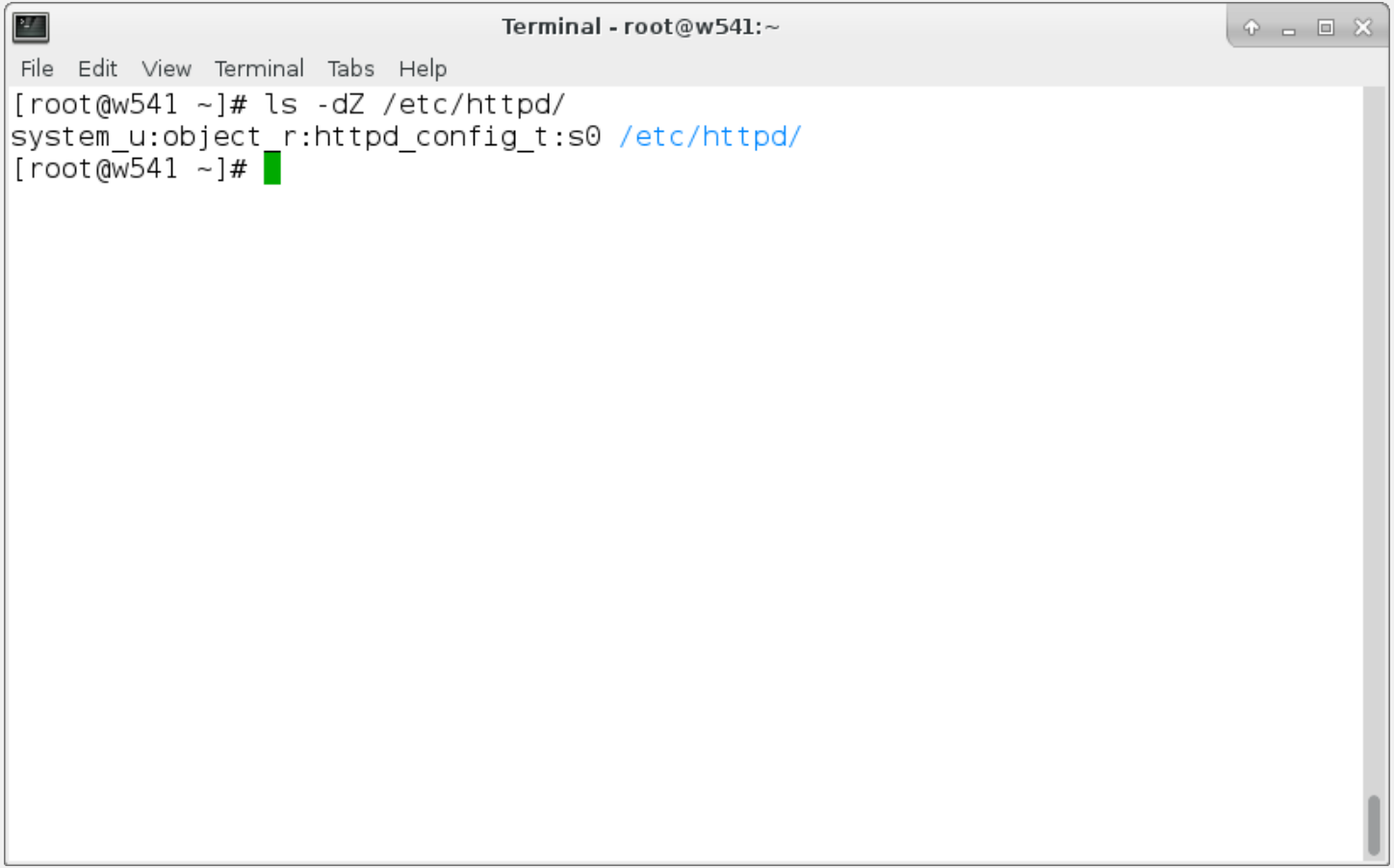
So How Does SELinux Work?

- The Apache web server has a binary executable which launches from /usr/sbin. When you look at that file's SELinux context, you see its type is httpd_exec_t:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# ls -lZ /usr/sbin/httpd
-rwxr-xr-x. 1 root root system_u:object_r:httpd_exec_t:s0 536888 Jan 4 00:17 /u
sr/sbin/httpd
[root@w541 ~]#

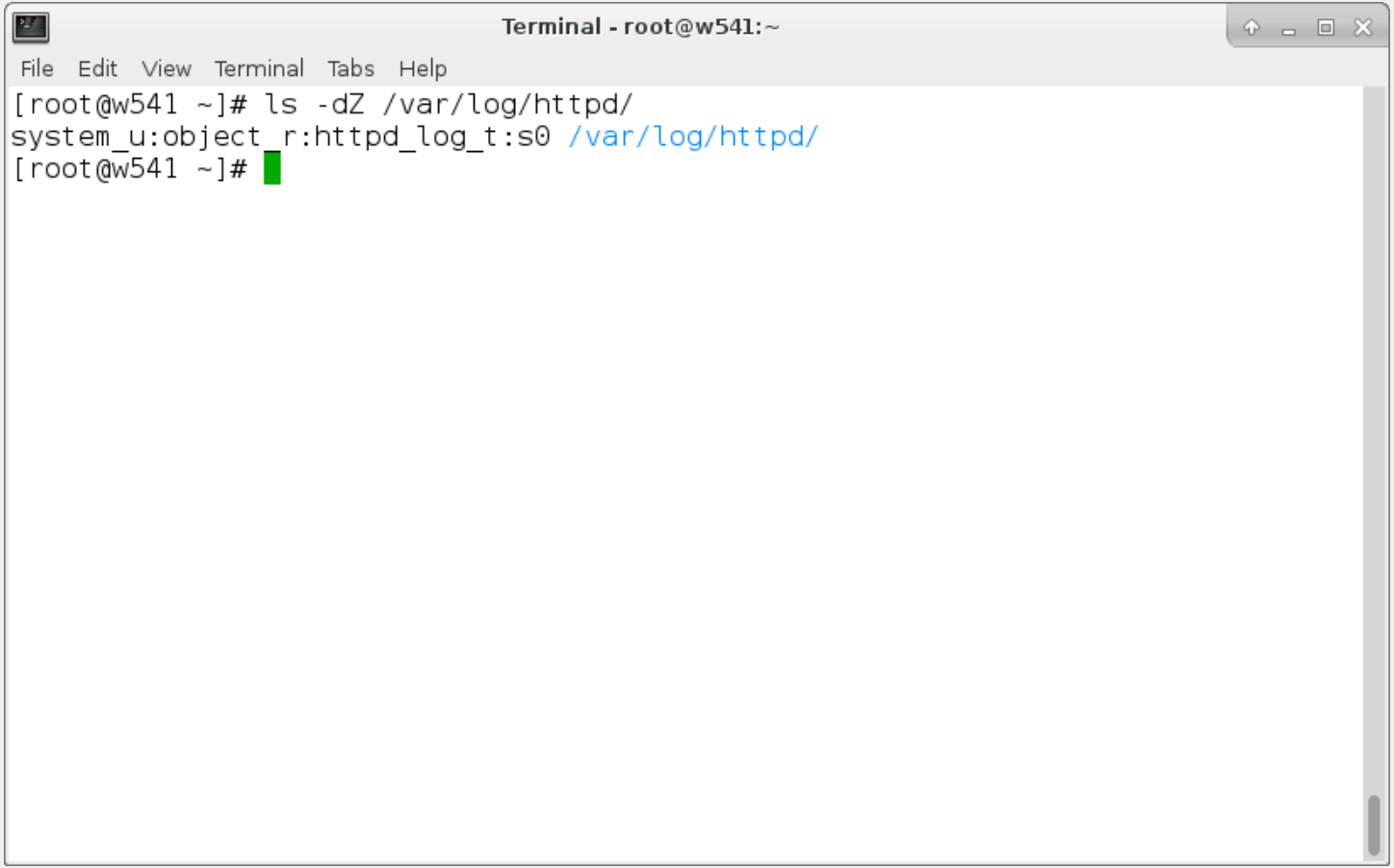
So How Does SELinux Work?

- The web server's configuration directory is labeled httpd_config_t:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# ls -dZ /etc/httpd/
system_u:object_r:httpd_config_t:s0 /etc/httpd/
[root@w541 ~]#

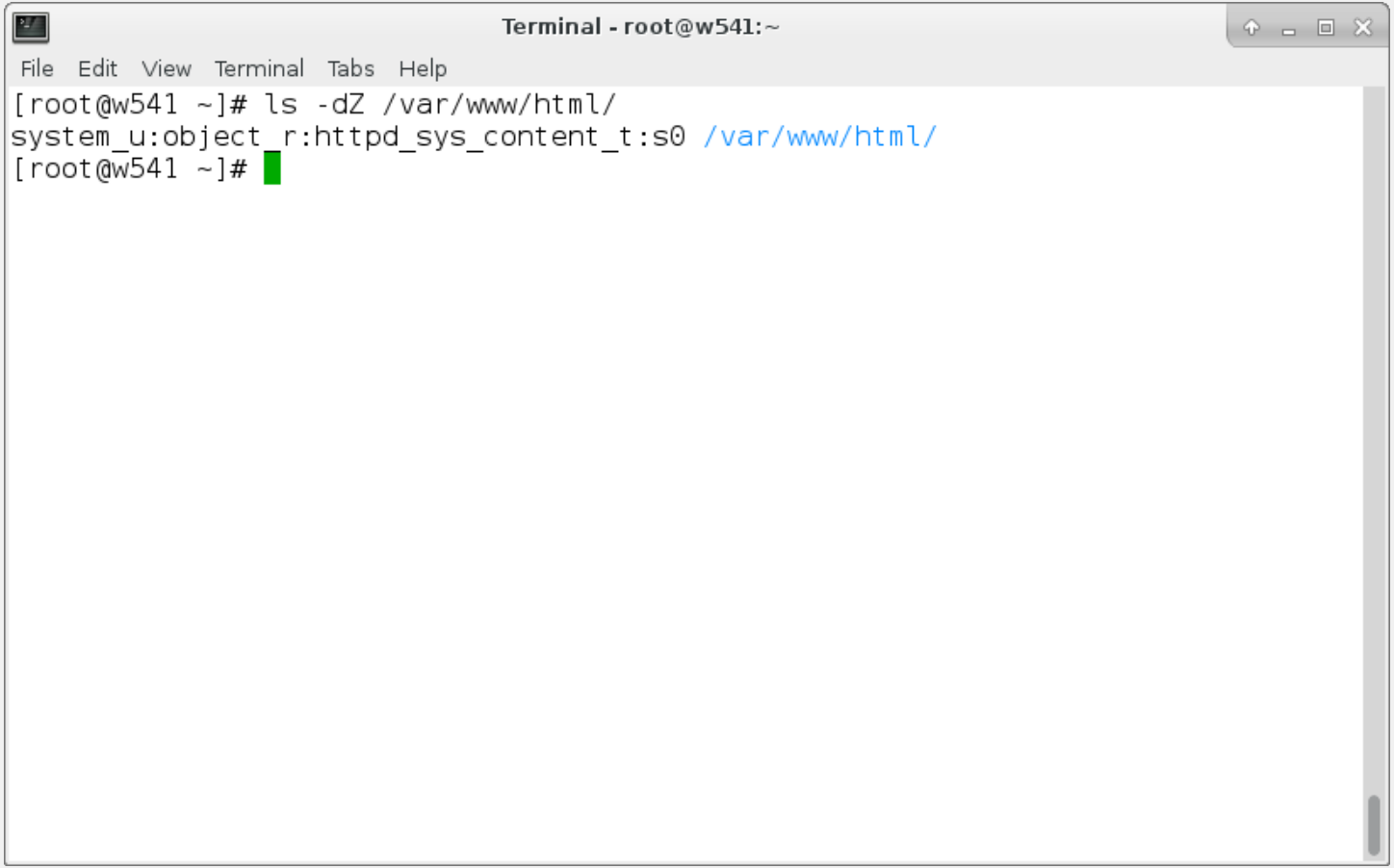
So How Does SELinux Work?

- The web server's logfile directory is labeled httpd_log_t:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# ls -dZ /var/log/httpd/
system_u:object_r:httpd_log_t:s0 /var/log/httpd/
[root@w541 ~]#

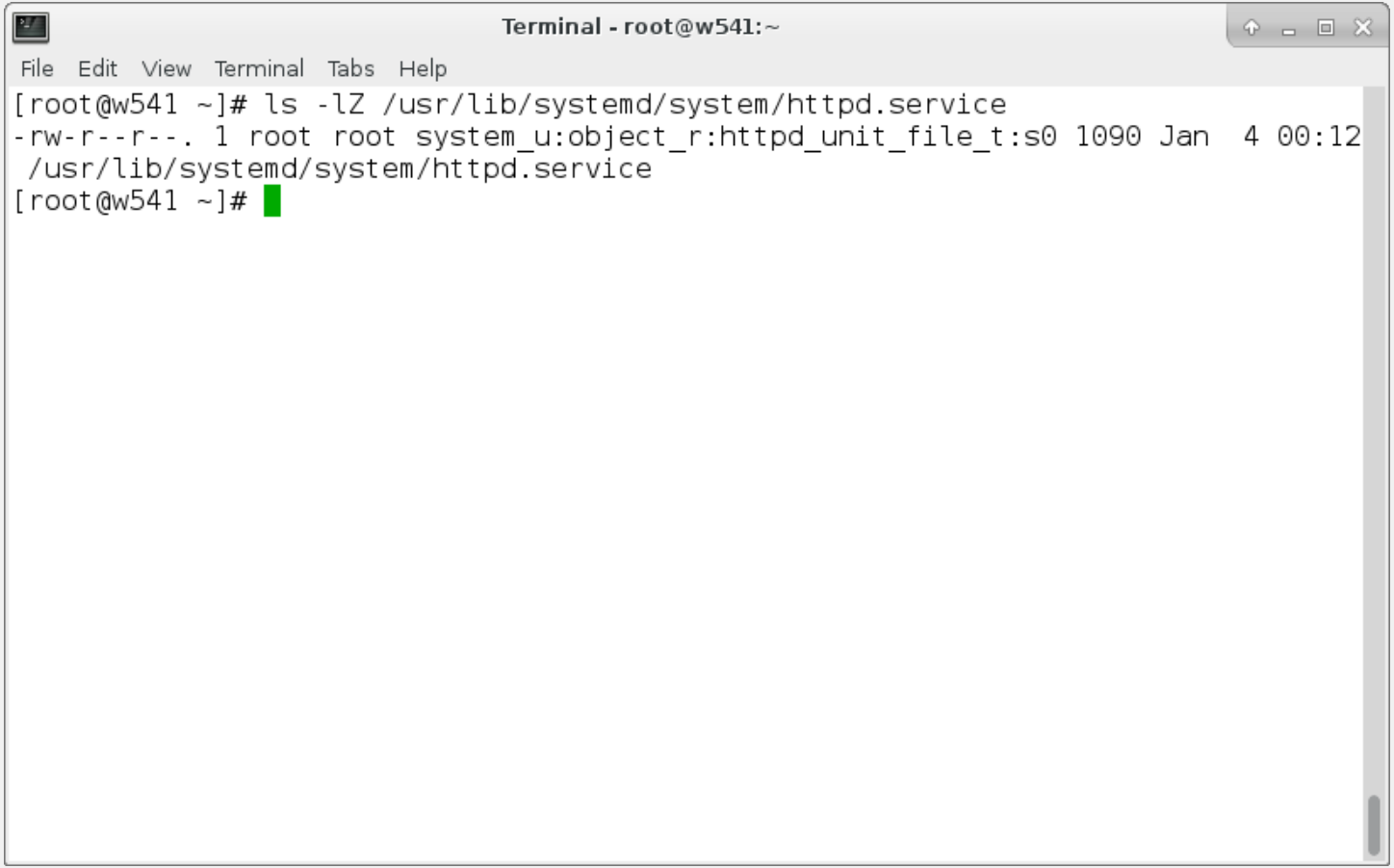
So How Does SELinux Work?

- The web server's content directory is labeled httpd_sys_content_t:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# ls -dZ /var/www/html/
system_u:object_r:httpd_sys_content_t:s0 /var/www/html/
[root@w541 ~]#

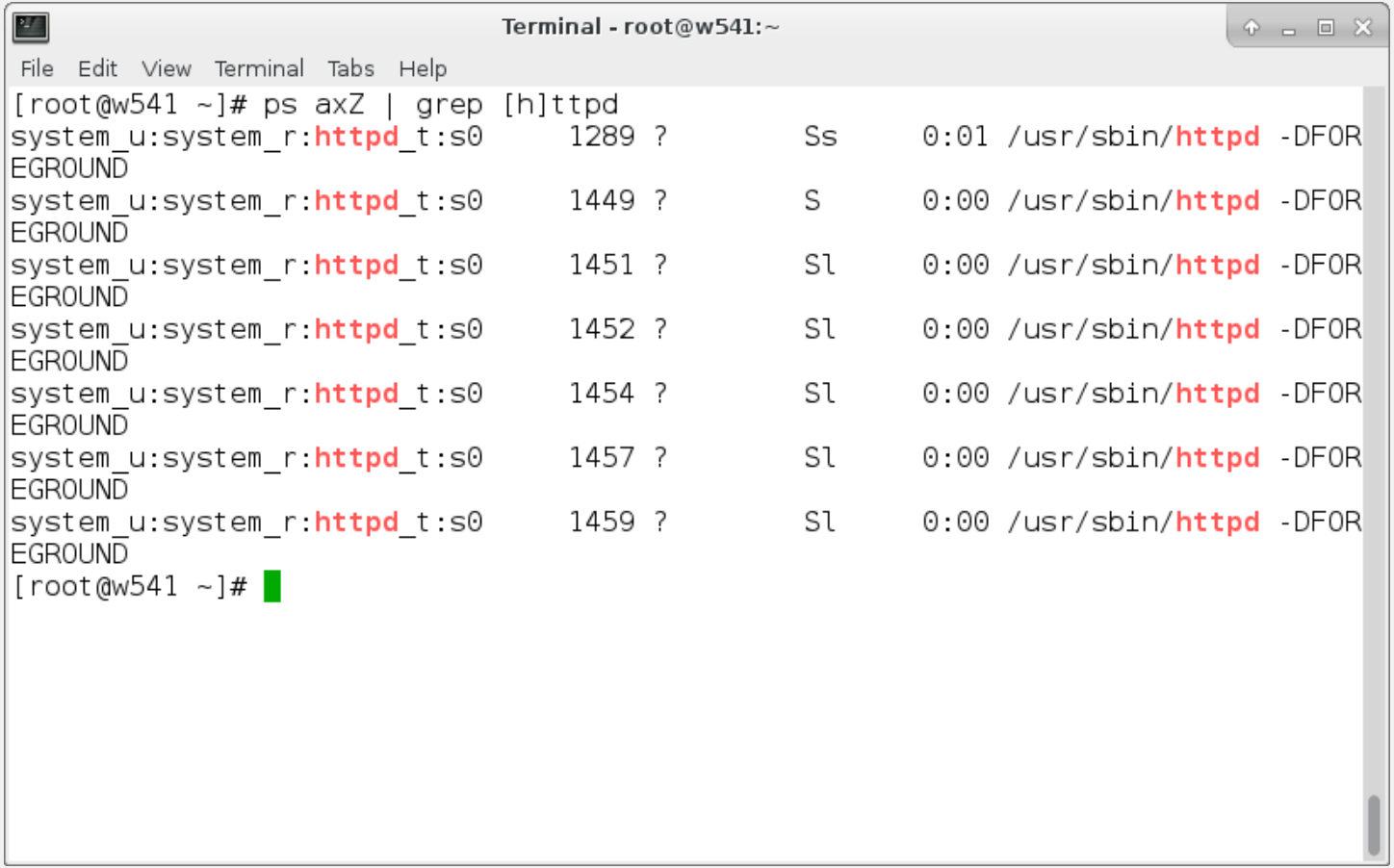
So How Does SELinux Work?

- The web server's startup script is labeled httpd_initrc_exec_t:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# ls -lZ /usr/lib/systemd/system/httpd.service
-rw-r--r--. 1 root root system_u:object_r:httpd_unit_file_t:s0 1090 Jan 4 00:12
/usr/lib/systemd/system/httpd.service
[root@w541 ~]#

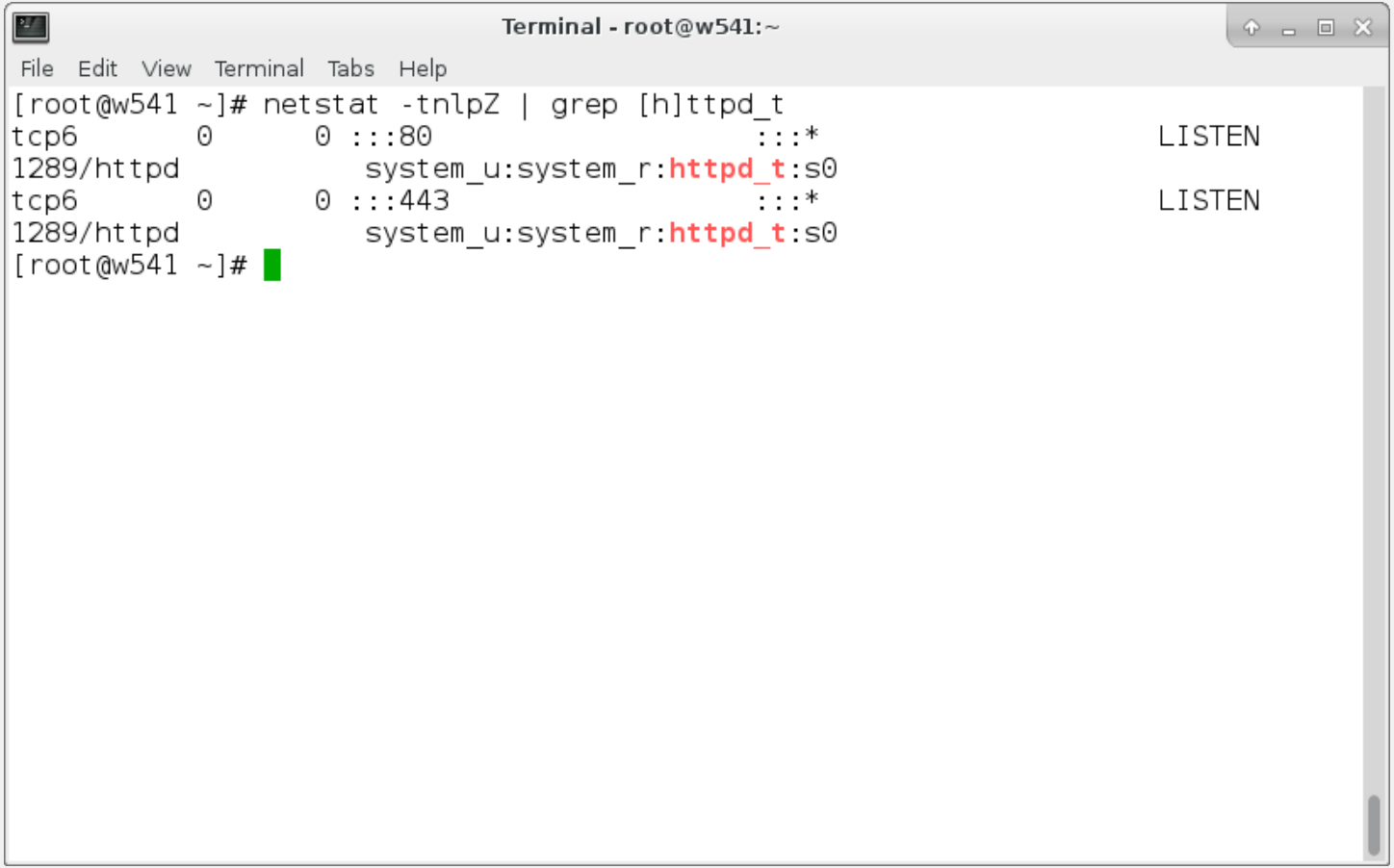
So How Does SELinux Work?

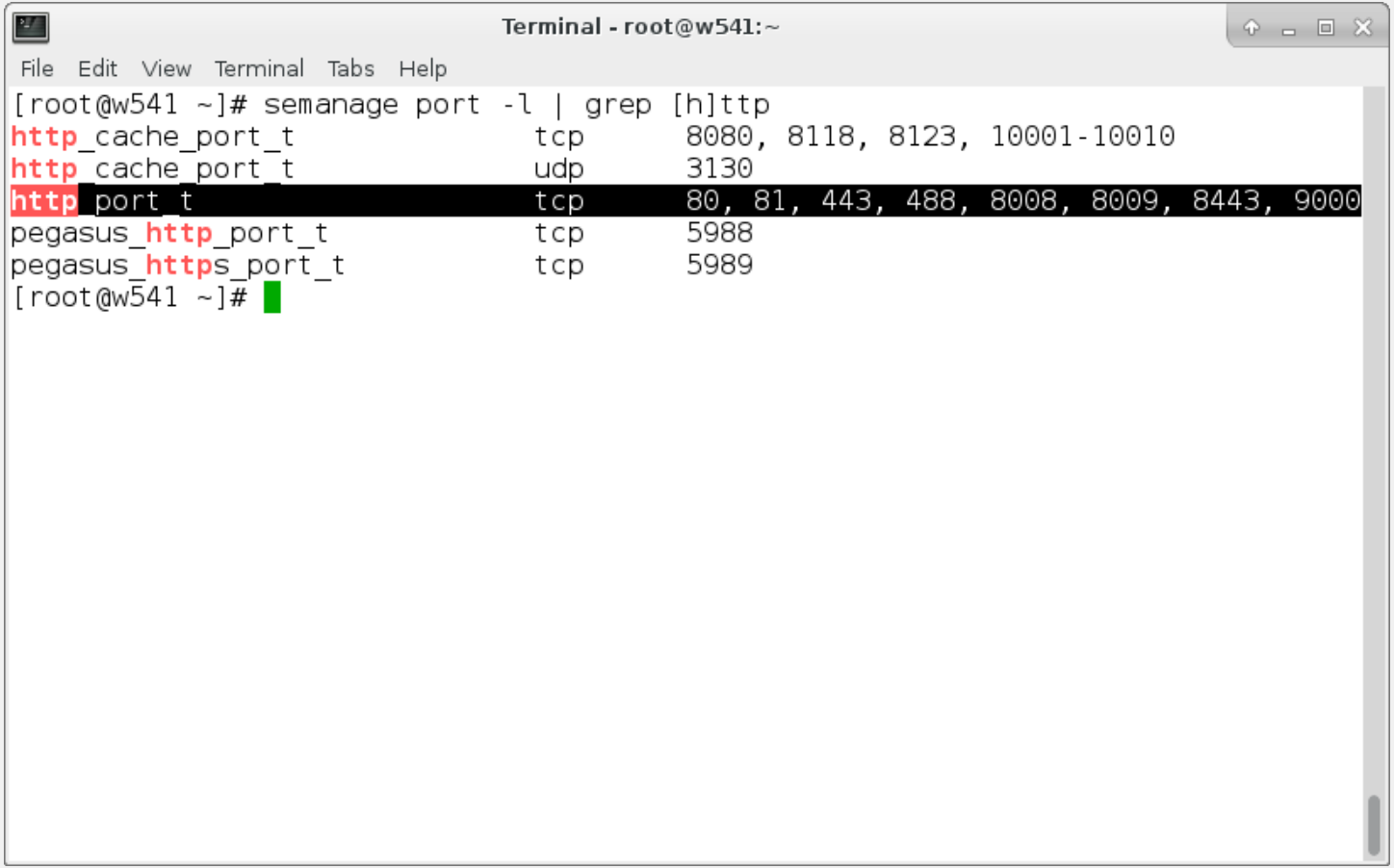
- As the web server runs, it's process is labeled httpd_t:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# ps axZ | grep [h]ttpd
system_u:system_r:httpd_t:s0 1289 ? Ss 0:01 /usr/sbin/httpd -DFOR
EGROUND
system_u:system_r:httpd_t:s0 1449 ? S 0:00 /usr/sbin/httpd -DFOR
EGROUND
system_u:system_r:httpd_t:s0 1451 ? Sl 0:00 /usr/sbin/httpd -DFOR
EGROUND
system_u:system_r:httpd_t:s0 1452 ? Sl 0:00 /usr/sbin/httpd -DFOR
EGROUND
system_u:system_r:httpd_t:s0 1454 ? Sl 0:00 /usr/sbin/httpd -DFOR
EGROUND
system_u:system_r:httpd_t:s0 1457 ? Sl 0:00 /usr/sbin/httpd -DFOR
EGROUND
system_u:system_r:httpd_t:s0 1459 ? Sl 0:00 /usr/sbin/httpd -DFOR
EGROUND
[root@w541 ~]#

So How Does SELinux Work?

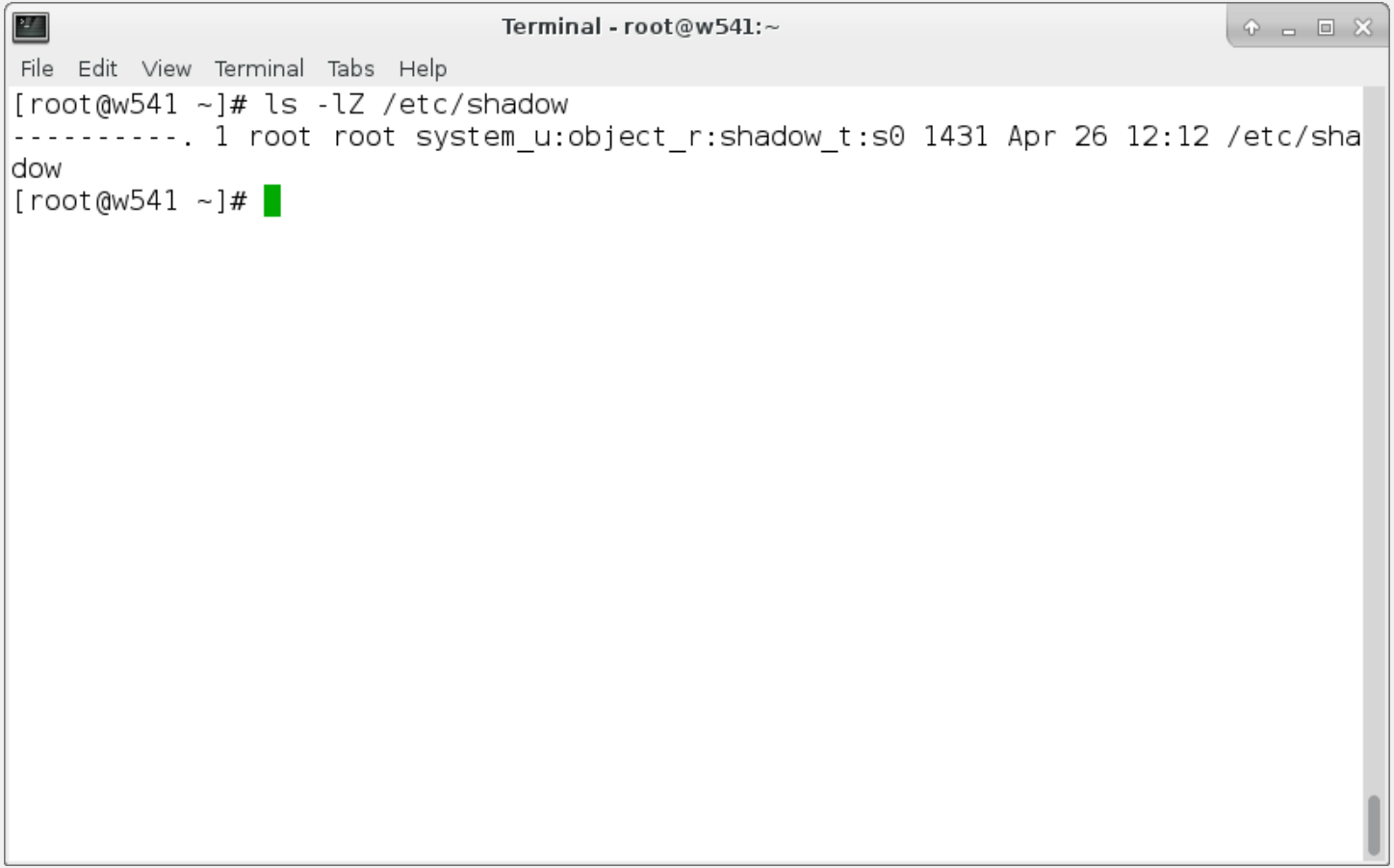
- If you look at the ports upon which the web server listens, you'll see that even they are labeled.


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# netstat -tnlpZ | grep [h]ttpd_t
tcp6 0 0 :::80 :::* LISTEN
1289/httpd system_u:system_r:httpd_t:s0
tcp6 0 0 :::443 :::* LISTEN
1289/httpd system_u:system_r:httpd_t:s0
[root@w541 ~]#


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# semanage port -l | grep [h]ttp
http_cache_port_t tcp 8080, 8118, 8123, 10001-10010
http_cache_port_t udp 3130
http_port_t tcp 80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t tcp 5988
pegasus_https_port_t tcp 5989
[root@w541 ~]#

So How Does SELinux Work?

- Now then... The /etc/shadow file has a type shadow_t:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# ls -lZ /etc/shadow
----------. 1 root root system_u:object_r:shadow_t:s0 1431 Apr 26 12:12 /etc/sha
dow
[root@w541 ~]#

So How Does SELinux Work?

- Type enforcement

So How Does SELinux Work?

- Type enforcement
  - It probably makes sense for a process running in the httpd_t context to interact with a file with the httpd_config_t label.

So How Does SELinux Work?

- Type enforcement
  - Do you think it makes sense for a process running with the httpd_t context label to be able to interact with a file with, say, the shadow_t label?

So How Does SELinux Work?

- Type enforcement
  - Type enforcement is the part of the policy that says, for instance, “a process running with the label httpd_t can have read access to a file labeled httpd_config_t”

HOW DO I DEAL WITH LABELS?

How Do I Deal With Labels?

- You've seen me use the -Z argument to several commands to view context. Many commands accept this argument:
  - ls -Z
  - id -Z
  - ps -Z
  - netstat -Z

How Do I Deal With Labels?

- You can actually use the -Z argument to create and modify files and contexts, as well.
  - cp -Z
  - mkdir -Z

How Do I Deal With Labels?

- You can use SELinux aware tools like chcon or restorecon to change the context of a file (more on this later).
- 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.
- The login process sets the default context (unconfined in the targeted policy)

How Do I Deal With Labels?

- 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 created with the baz_t label.
  - Example: A process, dhclient, running with the dhclient_t label creates a file, resolv.conf, labeled net_conf_t in a directory, /etc, labeled etc_t. Without that transition, /etc/resolv.conf would have inherited the etc_t label.

How Do I Deal With Labels?

- You've also seen me use the semanage command. It can be used to manage SELinux settings for:
  - login
  - user
  - port
  - interface
  - module

How Do I Deal With Labels?

- You've also seen me use the semanage command. It can be used to manage SELinux settings for:
  - node
  - file context
  - boolean
  - permissive state
  - dontaudit

SELINUX ERRORS

What Does It Mean If I Get An SELinux Error?

What Does It Mean If I Get An SELinux Error?

- If you see an SELinux error, it means that something is wrong!

What Does It Mean If I Get An SELinux Error?

- If you see an SELinux error, 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 may mean that labeling is wrong
  - Use the tools to fix the labels. We'll talk more about that later.

What Does It Mean If I Get An SELinux Error?

- It may mean that the policy needs to be tweaked.
  - booleans
  - Policy modules

What Does It Mean If I Get An SELinux Error?

- There could be a bug in the policy
  - We need to know about these! Open a ticket (do not file a Bugzilla report - there are no SLAs around BZ).

What Does It Mean If I Get An SELinux Error?

- You have been, or are being, broken into
  - Man the battle stations!

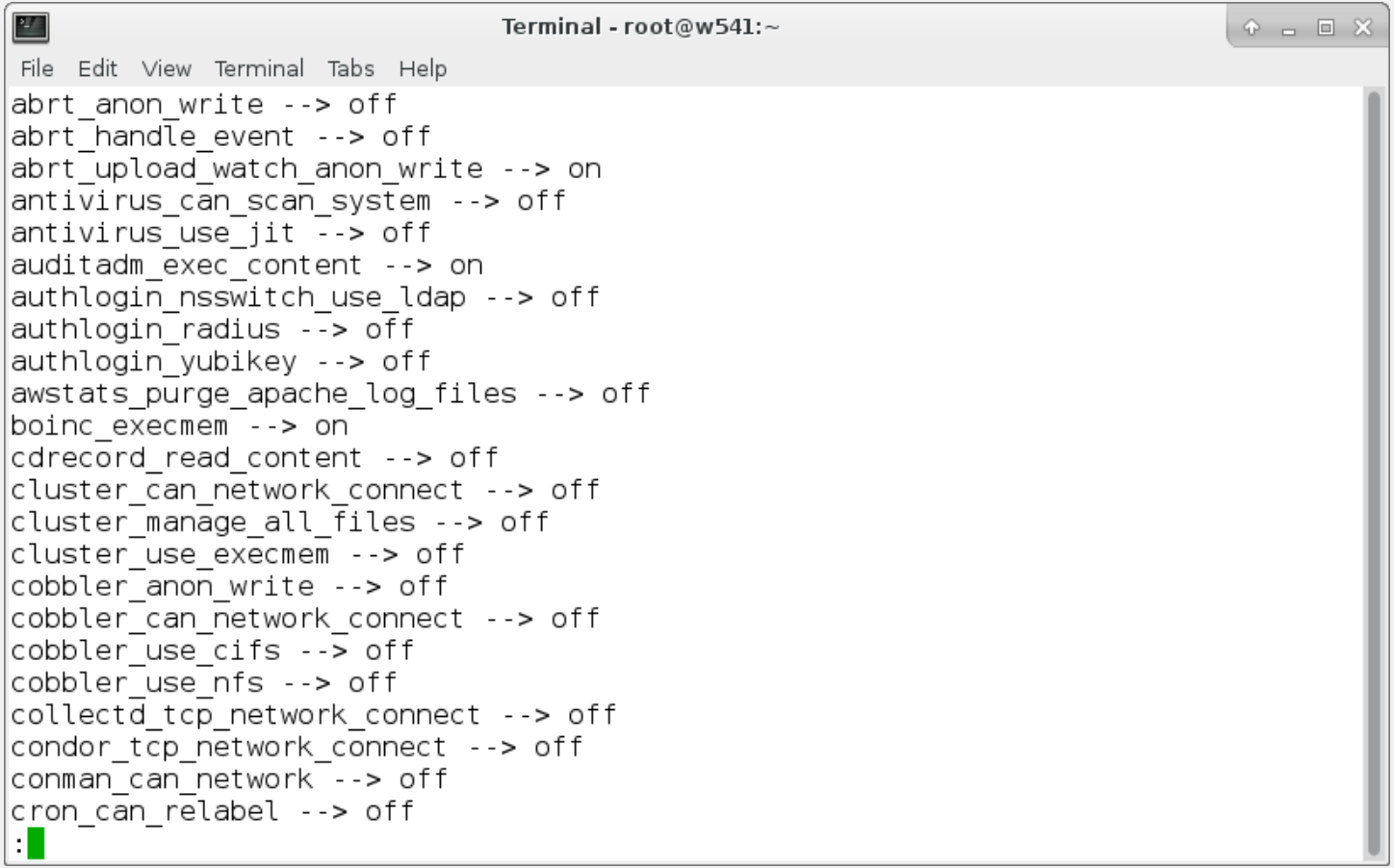
BOOLEANS

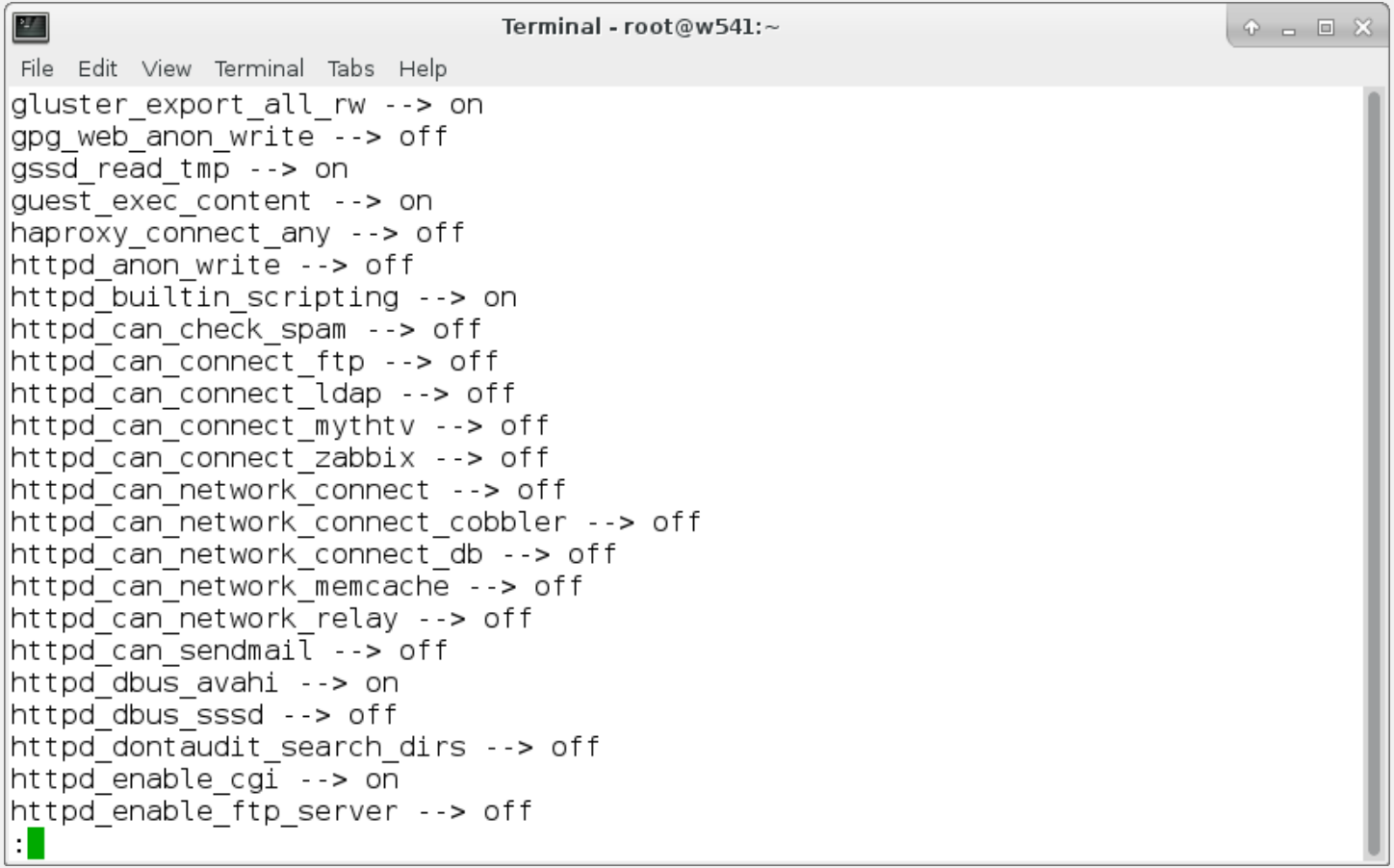
What Are Booleans?

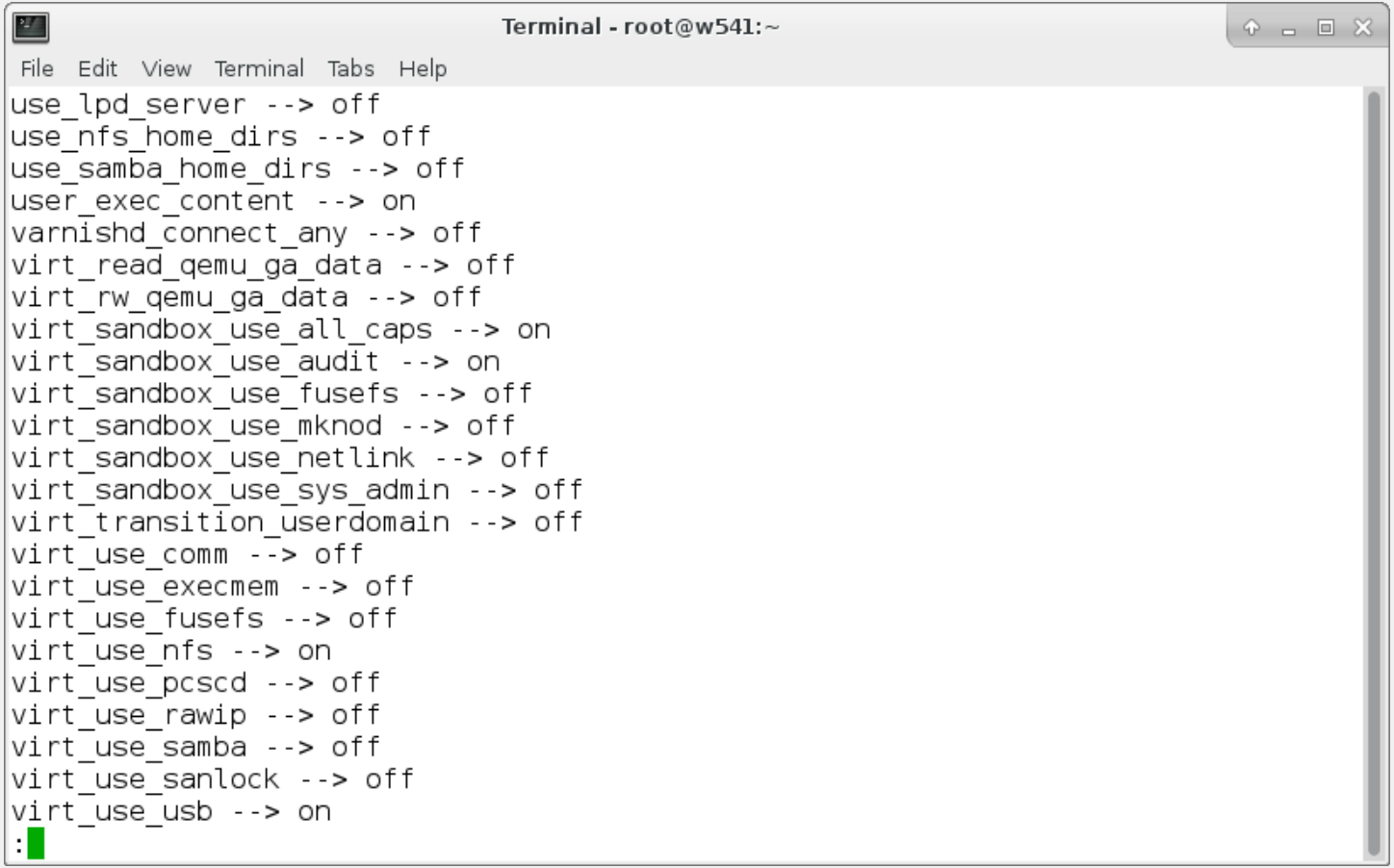
- Booleans are just off/on settings for SELinux.
  - From simple stuff like “do we allow the ftp server access to home directories” to more esoteric stuff like “httpd can use mod_auth_ntlm_winbind.”

What Are Booleans?

- To see all the booleans, run getsebool -a


Terminal - root@w541:~
File Edit View Terminal Tabs Help
abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
antivirus_can_scan_system --> off
antivirus_use_jit --> off
auditadm_exec_content --> on
authlogin_nsswitch_use_ldap --> off
authlogin_radius --> off
authlogin_yubikey --> off
awstats_purge_apache_log_files --> off
boinc_execmem --> on
cdrecord_read_content --> off
cluster_can_network_connect --> off
cluster_manage_all_files --> off
cluster_use_execmem --> off
cobbler_anon_write --> off
cobbler_can_network_connect --> off
cobbler_use_cifs --> off
cobbler_use_nfs --> off
collectd_tcp_network_connect --> off
condor_tcp_network_connect --> off
conman_can_network --> off
cron_can_relabel --> off
:

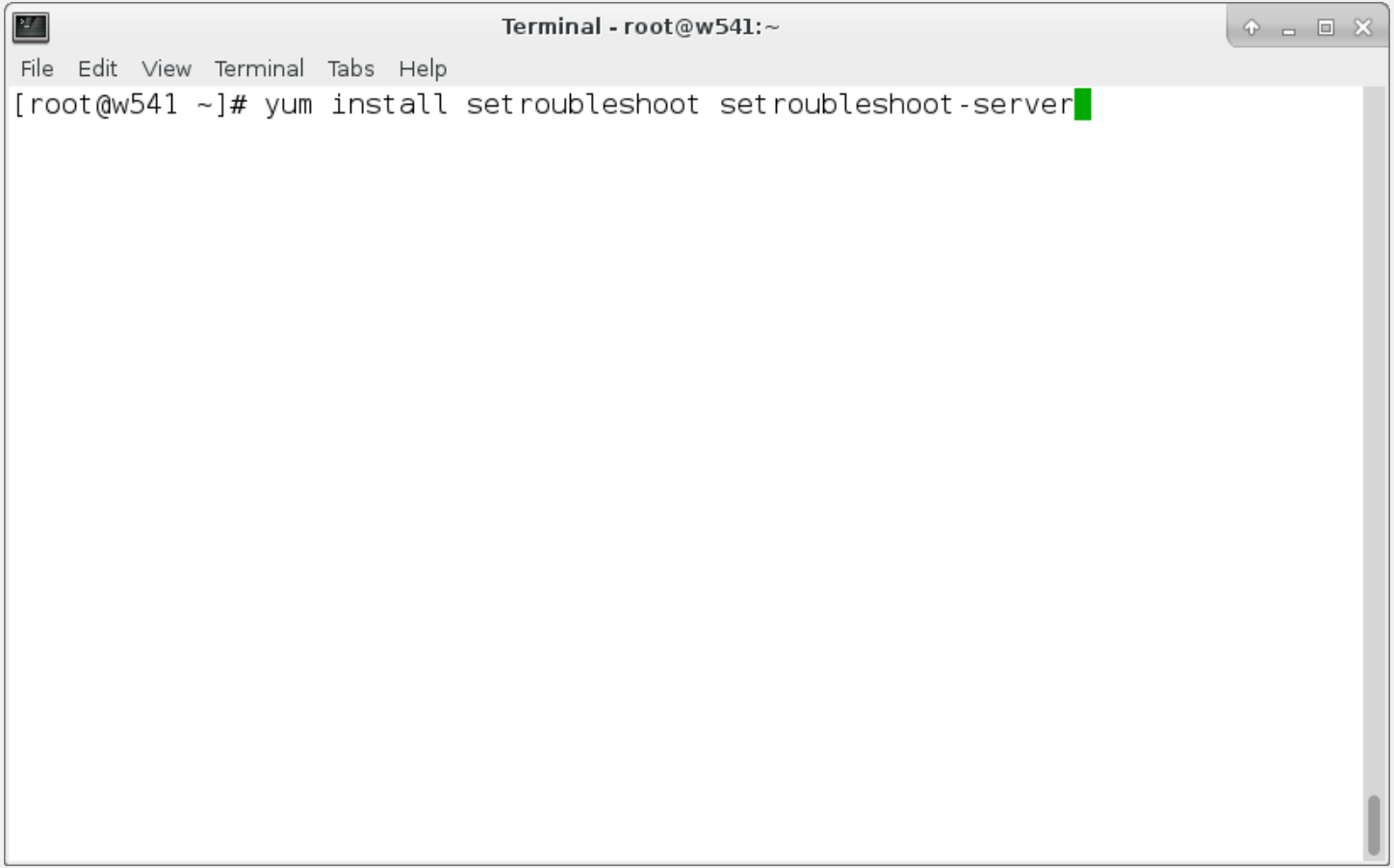

Terminal - root@w541:~
File Edit View Terminal Tabs Help
gluster_export_all_rw --> on
gpg_web_anon_write --> off
gssd_read_tmp --> on
guest_exec_content --> on
haproxy_connect_any --> off
httpd_anon_write --> off
httpd_builtin_scripting --> on
httpd_can_check_spam --> off
httpd_can_connect_ftp --> off
httpd_can_connect_ldap --> off
httpd_can_connect_mythtv --> off
httpd_can_connect_zabbix --> off
httpd_can_network_connect --> off
httpd_can_network_connect_cobbler --> off
httpd_can_network_connect_db --> off
httpd_can_network_memcache --> off
httpd_can_network_relay --> off
httpd_can_sendmail --> off
httpd_dbus_avahi --> on
httpd_dbus_sssd --> off
httpd_dontaudit_search_dirs --> off
httpd_enable_cgi --> on
httpd_enable_ftp_server --> off
:

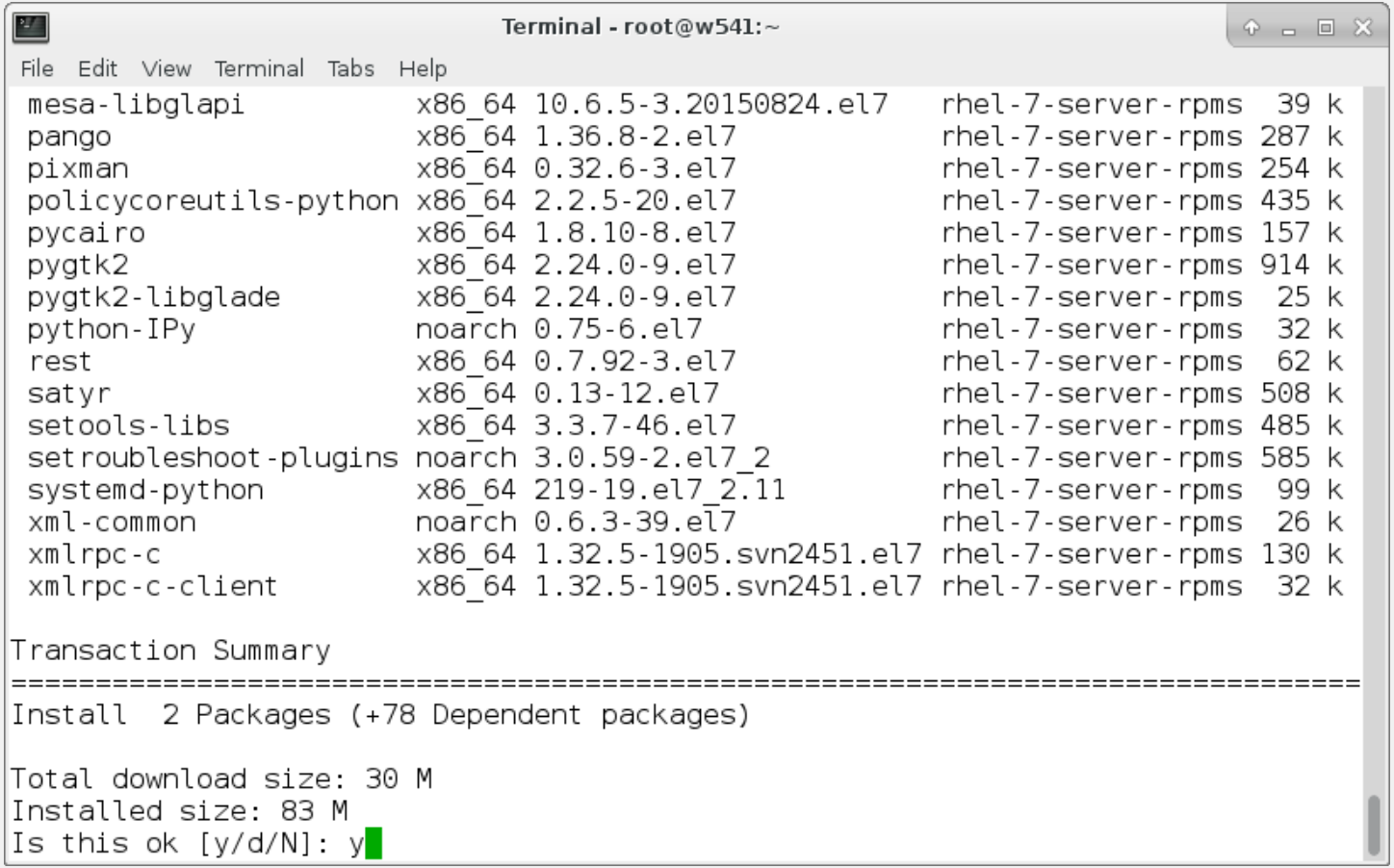

Terminal - root@w541:~
File Edit View Terminal Tabs Help
use_lpd_server --> off
use_nfs_home_dirs --> off
use_samba_home_dirs --> off
user_exec_content --> on
varnishd_connect_any --> off
virt_read_qemu_ga_data --> off
virt_rw_qemu_ga_data --> off
virt_sandbox_use_all_caps --> on
virt_sandbox_use_audit --> on
virt_sandbox_use_fusefs --> off
virt_sandbox_use_mknod --> off
virt_sandbox_use_netlink --> off
virt_sandbox_use_sys_admin --> off
virt_transition_userdomain --> off
virt_use_comm --> off
virt_use_execmem --> off
virt_use_fusefs --> off
virt_use_nfs --> on
virt_use_pcscd --> off
virt_use_rawip --> off
virt_use_samba --> off
virt_use_sanlock --> off
virt_use_usb --> on
:

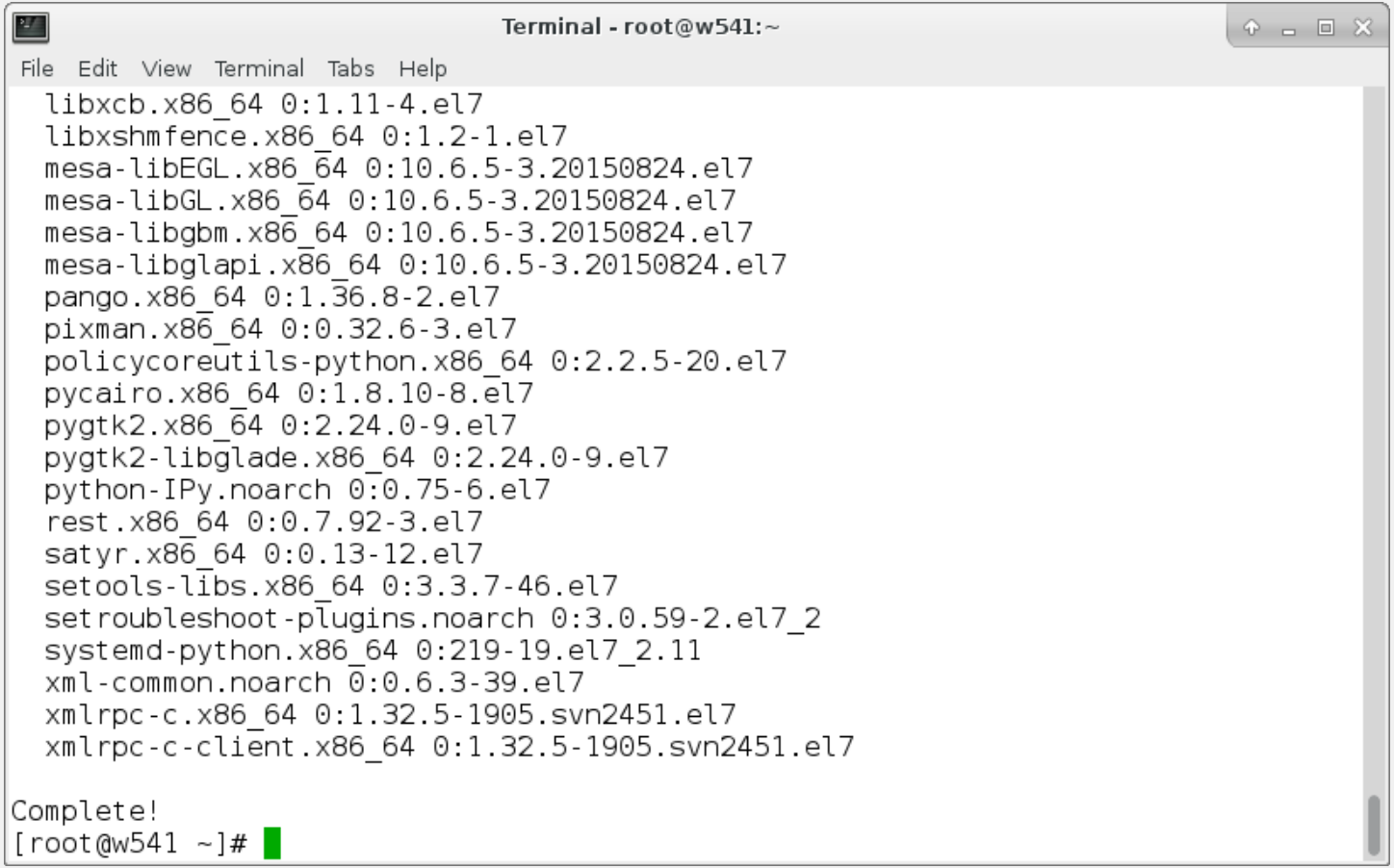
TIPS AND TRICKS

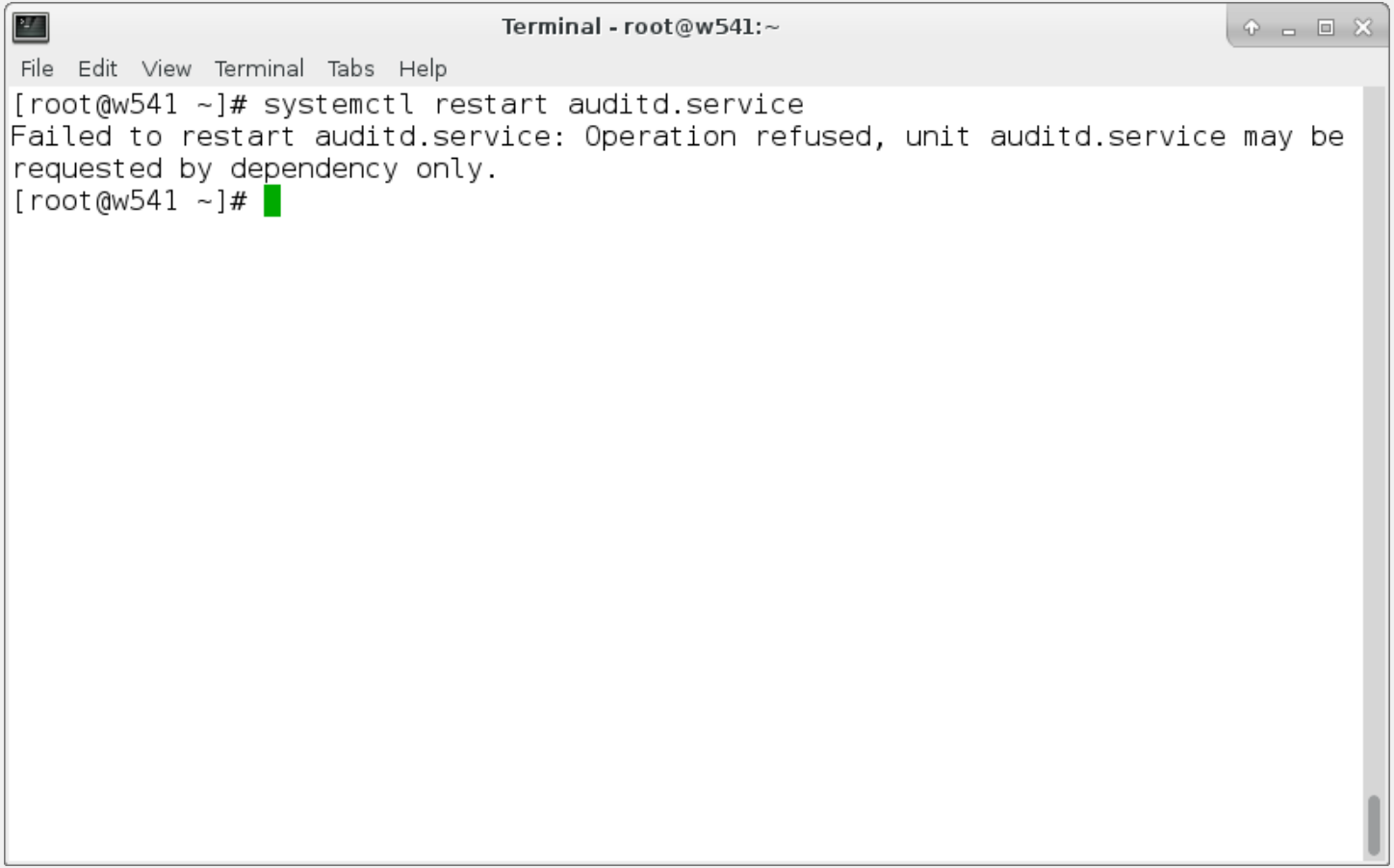
Tips and Tricks

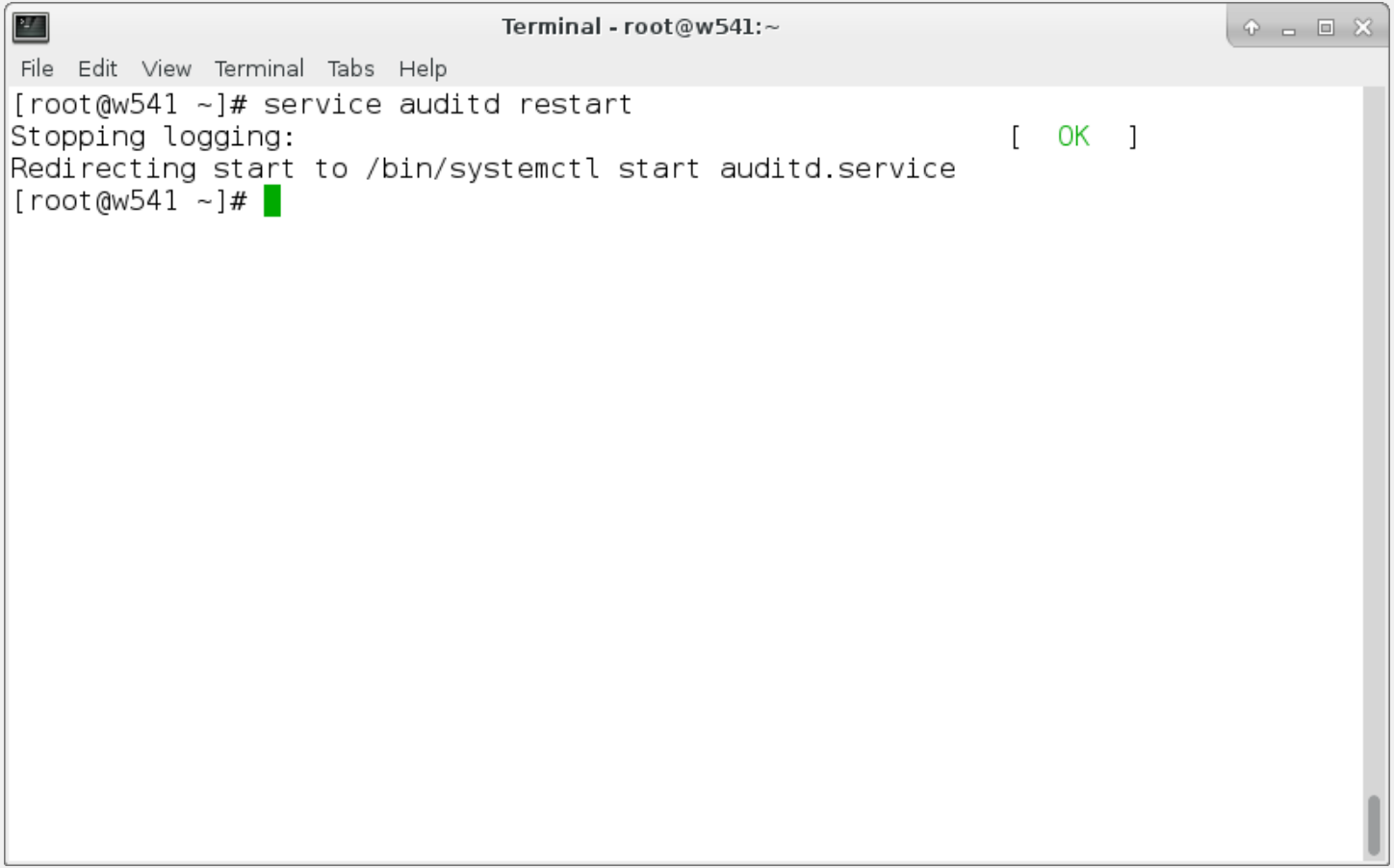
- Install setroubleshoot and setroubleshoot-server on machines you'll be developing policy modules on. They drag in a bunch of tools to help diagnose and fix SELinux issues.
- Reboot or restart auditd after you install.


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# yum install setroubleshoot setroubleshoot-server


Terminal - root@w541:~
File Edit View Terminal Tabs Help
mesa-libglapi x86_64 10.6.5-3.20150824.el7 rhel-7-server-rpms 39 k
pango x86_64 1.36.8-2.el7 rhel-7-server-rpms 287 k
pixman x86_64 0.32.6-3.el7 rhel-7-server-rpms 254 k
policycoreutils-python x86_64 2.2.5-20.el7 rhel-7-server-rpms 435 k
pycairo x86_64 1.8.10-8.el7 rhel-7-server-rpms 157 k
pygtk2 x86_64 2.24.0-9.el7 rhel-7-server-rpms 914 k
pygtk2-libglade x86_64 2.24.0-9.el7 rhel-7-server-rpms 25 k
python-IPy noarch 0.75-6.el7 rhel-7-server-rpms 32 k
rest x86_64 0.7.92-3.el7 rhel-7-server-rpms 62 k
satyr x86_64 0.13-12.el7 rhel-7-server-rpms 508 k
setools-libs x86_64 3.3.7-46.el7 rhel-7-server-rpms 485 k
setroubleshoot-plugins noarch 3.0.59-2.el7_2 rhel-7-server-rpms 585 k
systemd-python x86_64 219-19.el7_2.11 rhel-7-server-rpms 99 k
xml-common noarch 0.6.3-39.el7 rhel-7-server-rpms 26 k
xmlrpc-c x86_64 1.32.5-1905.svn2451.el7 rhel-7-server-rpms 130 k
xmlrpc-c-client x86_64 1.32.5-1905.svn2451.el7 rhel-7-server-rpms 32 k
Transaction Summary
Install 2 Packages (+78 Dependent packages)
Total download size: 30 M
Installed size: 83 M
Is this ok [y/d/N]: y


Terminal - root@w541:~
File Edit View Terminal Tabs Help
libxcb.x86_64 0:1.11-4.el7
libxshmfence.x86_64 0:1.2-1.el7
mesa-libEGL.x86_64 0:10.6.5-3.20150824.el7
mesa-libGL.x86_64 0:10.6.5-3.20150824.el7
mesa-libgbm.x86_64 0:10.6.5-3.20150824.el7
mesa-libglapi.x86_64 0:10.6.5-3.20150824.el7
pango.x86_64 0:1.36.8-2.el7
pixman.x86_64 0:0.32.6-3.el7
policycoreutils-python.x86_64 0:2.2.5-20.el7
pycairo.x86_64 0:1.8.10-8.el7
pygtk2.x86_64 0:2.24.0-9.el7
pygtk2-libglade.x86_64 0:2.24.0-9.el7
python-IPy.noarch 0:0.75-6.el7
rest.x86_64 0:0.7.92-3.el7
satyr.x86_64 0:0.13-12.el7
setools-libs.x86_64 0:3.3.7-46.el7
setroubleshoot-plugins.noarch 0:3.0.59-2.el7_2
systemd-python.x86_64 0:219-19.el7_2.11
xml-common.noarch 0:0.6.3-39.el7
xmlrpc-c.x86_64 0:1.32.5-1905.svn2451.el7
xmlrpc-c-client.x86_64 0:1.32.5-1905.svn2451.el7
Complete!
[root@w541 ~]#


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# systemctl restart auditd.service
Failed to restart auditd.service: Operation refused, unit auditd.service may be requested by dependency only.
[root@w541 ~]#


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# service auditd restart
Stopping logging: [OK]
Redirecting start to /bin/systemctl start auditd.service
[root@w541 ~]#

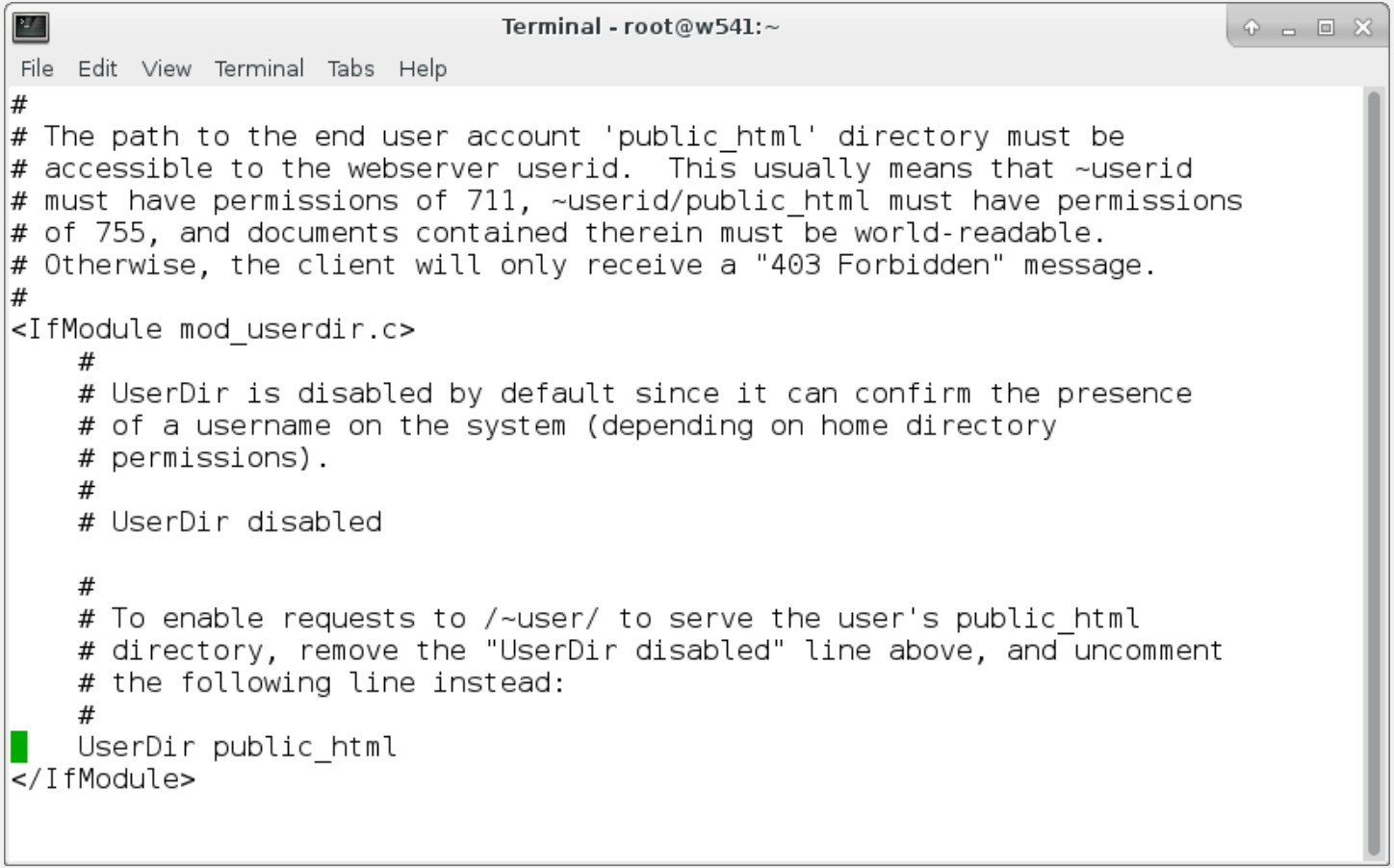
auditd

- This is not a bug. See https://bugzilla.redhat.com/show_bug.cgi?id=1026648 for details.

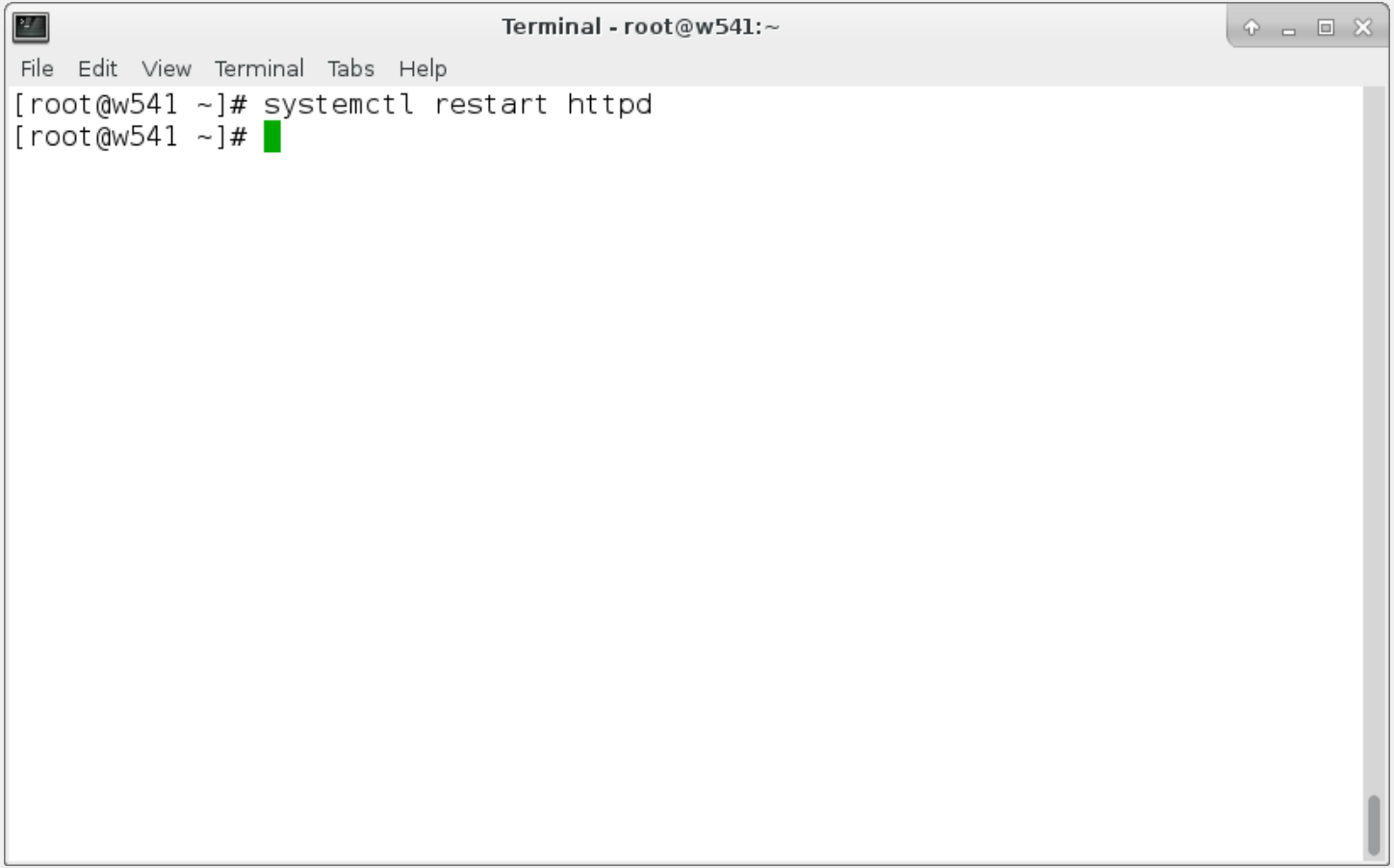
REAL WORLD EXAMPLES

Real World Examples

- A user, fred, wants to have his own web page in /home/fred/public_html on a web server.
  - You enable UserDir in /etc/httpd/conf.d/userdir.conf
  - Restart the web server

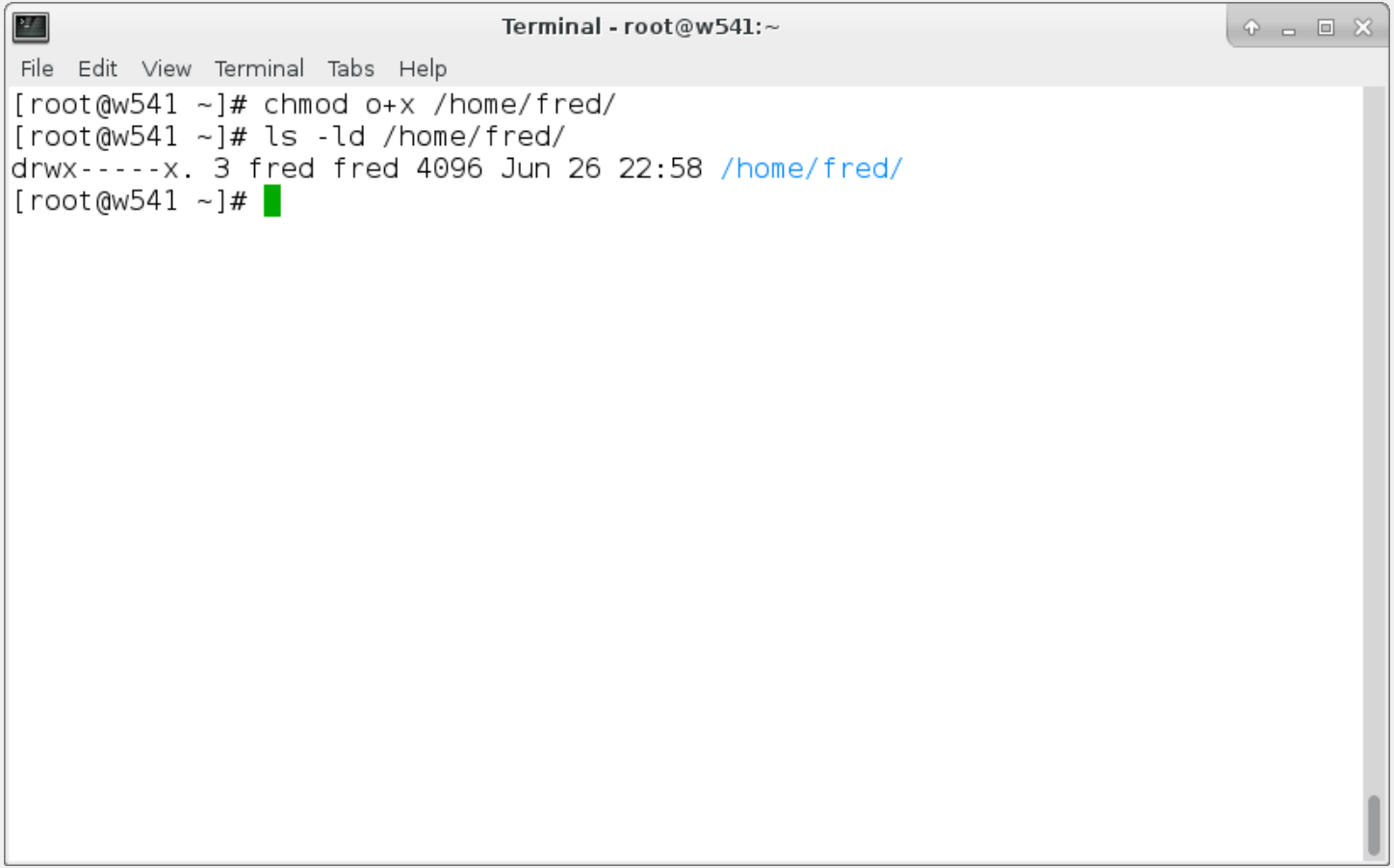

Terminal - root@w541:~
File Edit View Terminal Tabs Help
#
The path to the end user account 'public_html' directory must be
accessible to the webserver userid. This usually means that ~userid
must have permissions of 711, ~userid/public_html must have permissions
of 755, and documents contained therein must be world-readable.
Otherwise, the client will only receive a "403 Forbidden" message.
#
<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>


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# systemctl restart httpd
[root@w541 ~]#

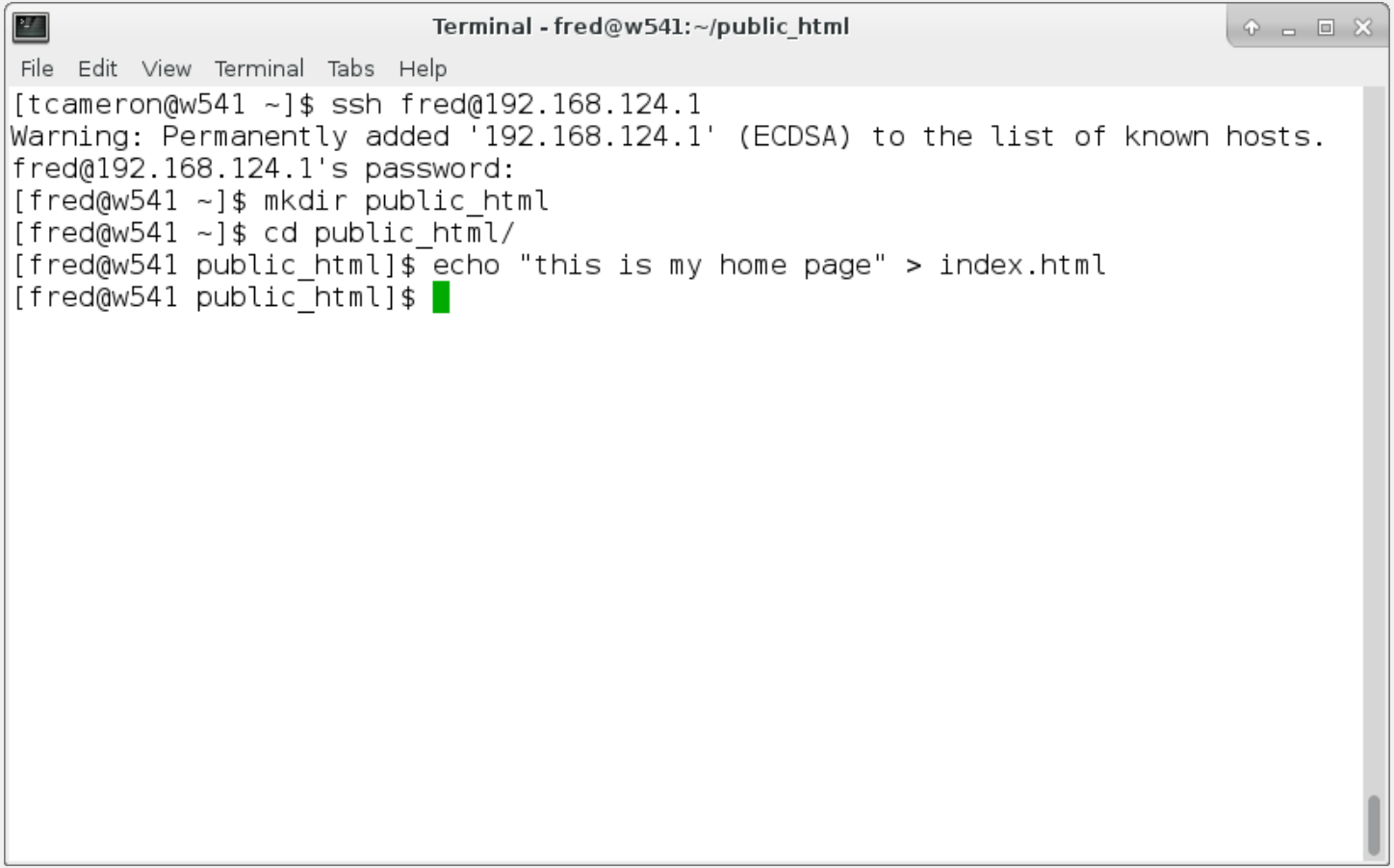
Real World Examples

- A user, fred, wants to start have his own web page in /home/fred/public_html
  - Change permissions so the web server can access his home directory.


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# chmod o+x /home/fred/
[root@w541 ~]# ls -ld /home/fred/
drwx-----x. 3 fred fred 4096 Jun 26 22:58 /home/fred/
[root@w541 ~]#

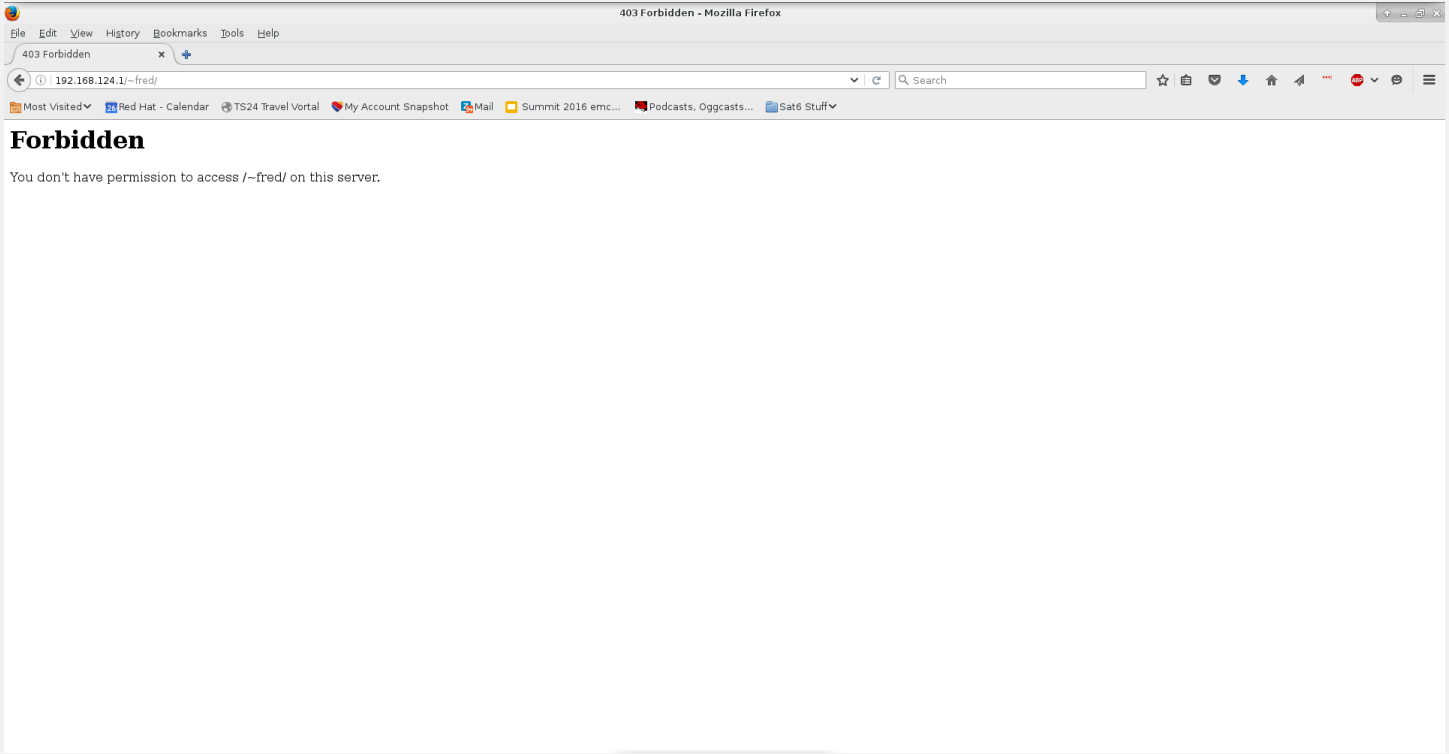
Real World Examples

- A user, fred, wants to start have his own web page in /home/fred/public_html
  - Fred logs in, creates his public_html directory and an index.html file.


Terminal - fred@w541:~/public_html
File Edit View Terminal Tabs Help
[tcameron@w541 ~]$ ssh fred@192.168.124.1
Warning: Permanently added '192.168.124.1' (ECDSA) to the list of known hosts.
fred@192.168.124.1's password:
[fred@w541 ~]$ mkdir public_html
[fred@w541 ~]$ cd public_html/
[fred@w541 public_html]$ echo "this is my home page" > index.html
[fred@w541 public_html]$

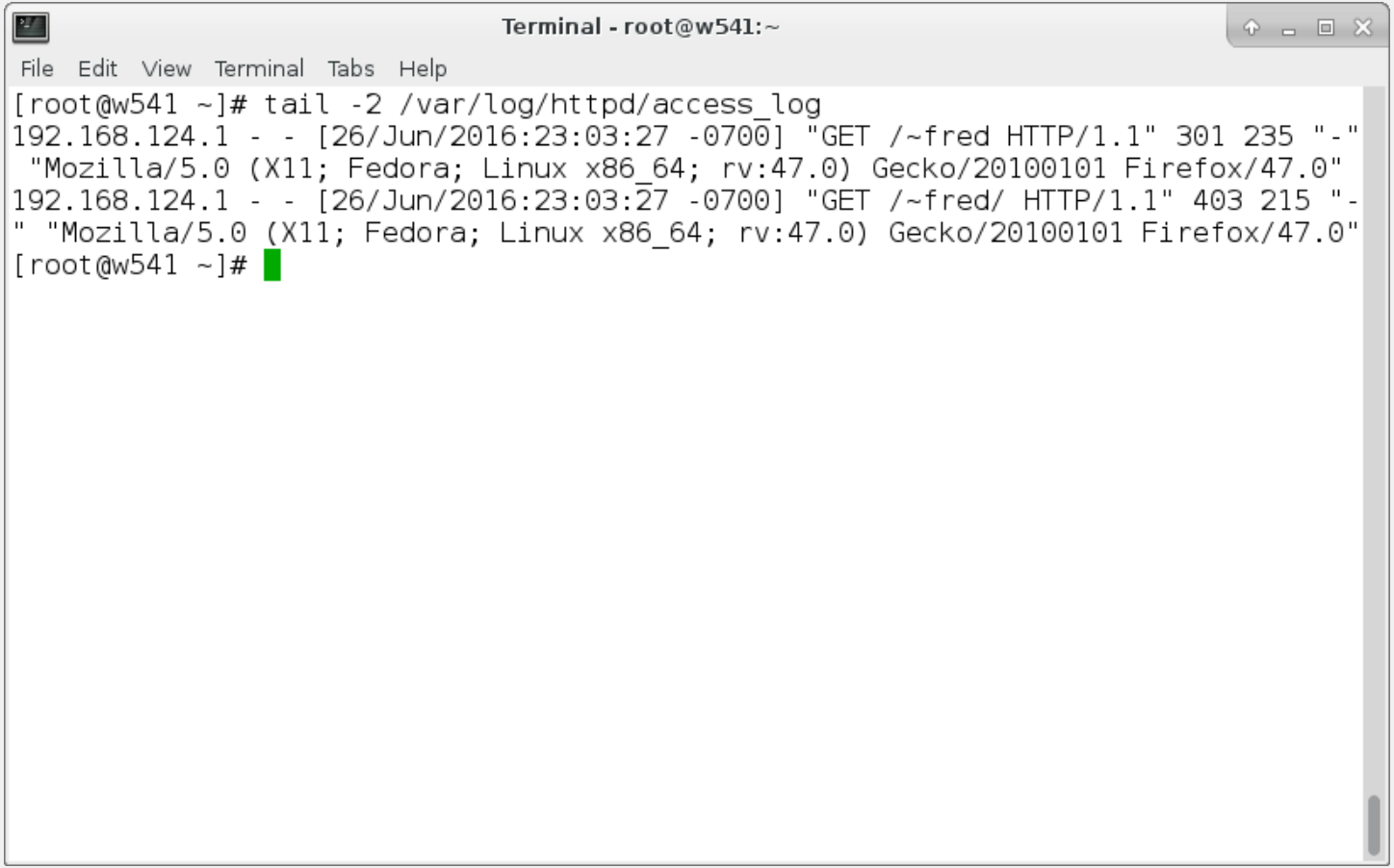
Real World Examples

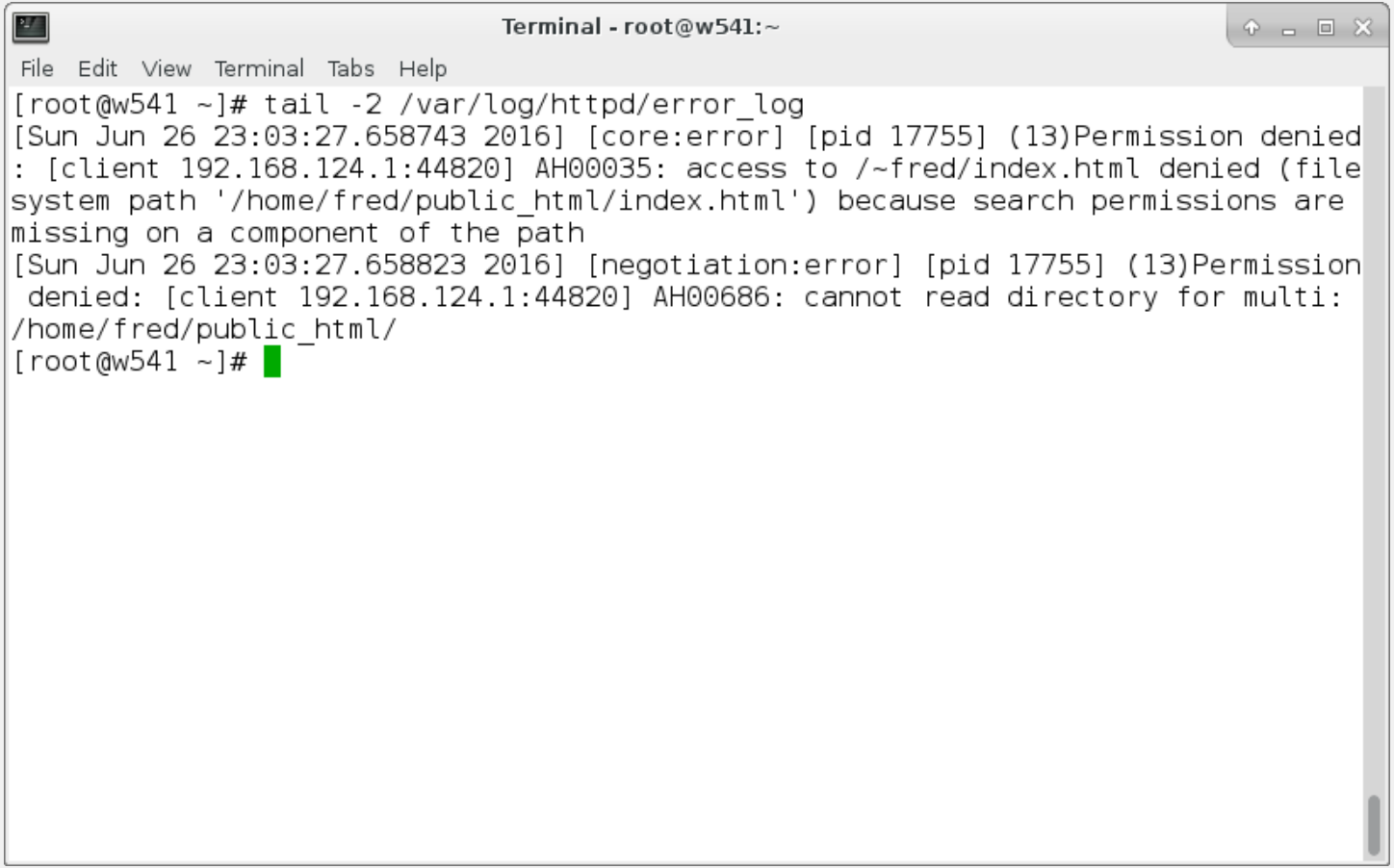
- A user, fred, wants to start have his own web page in /home/fred/public_html
  - We fire up the web browser, and:


403 Forbidden - Mozilla Firefox
File Edit View History Bookmarks Tools Help
403 Forbidden
192.168.124.1/~fred/
Search
Most Visited
Red Hat - Calendar
TS24 Travel Vortal
My Account Snapshot
Mail
Summit 2016 emc...
Podcasts, Oggcasts...
Sat6 Stuff
Forbidden
You don't have permission to access /~fred/ on this server.

Real World Examples

- A user, fred, wants to start have his own web page in /home/fred/public_html
  - So now we check the usual suspects.
    - /var/log/httpd/access_log
    - /var/log/httpd/error_log


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# tail -2 /var/log/httpd/access_log
192.168.124.1 - - [26/Jun/2016:23:03:27 -0700] "GET /~fred HTTP/1.1" 301 235 "-"
"Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:47.0) Gecko/20100101 Firefox/47.0"
192.168.124.1 - - [26/Jun/2016:23:03:27 -0700] "GET /~fred/ HTTP/1.1" 403 215 "-
" "Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:47.0) Gecko/20100101 Firefox/47.0"
[root@w541 ~]#


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# tail -2 /var/log/httpd/error_log
[Sun Jun 26 23:03:27.658743 2016] [core:error] [pid 17755] (13)Permission denied
: [client 192.168.124.1:44820] AH00035: access to /~fred/index.html denied (file
system path '/home/fred/public_html/index.html') because search permissions are
missing on a component of the path
[Sun Jun 26 23:03:27.658823 2016] [negotiation:error] [pid 17755] (13)Permission
 denied: [client 192.168.124.1:44820] AH00686: cannot read directory for multi:
/home/fred/public_html/
[root@w541 ~]#

Real World Examples

- A user, fred, wants to start have his own web page in /home/fred/public_html
  - We already knew that!

Real World Examples

- A user, fred, wants to start have his own web page in /home/fred/public_html
  - So now we look at journalctl


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# journalctl -b -0

Terminal - root@w541:~

File Edit View Terminal Tabs Help

```
Jun 26 23:54:31 w541.tc.redhat.com audit[1489]: AVC avc:  denied  { getattr } for  pid=1489 comm="/usr/sbin/httpd" path="/home/fred/public_html/index.html" dev="dm-0" ino=19803817 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:httpd_user_content_t:s0 tclass=file permissive=0
Jun 26 23:54:31 w541.tc.redhat.com audit[1489]: AVC avc:  denied  { getattr } for  pid=1489 comm="/usr/sbin/httpd" path="/home/fred/public_html/index.html" dev="dm-0" ino=19803817 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:httpd_user_content_t:s0 tclass=file permissive=0
Jun 26 23:54:31 w541.tc.redhat.com audit[1489]: AVC avc:  denied  { read } for  pid=1489 comm="/usr/sbin/httpd" name="public_html" dev="dm-0" ino=19803818 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:httpd_user_content_t:s0 tclass=dir permissive=0
Jun 26 23:54:34 w541.tc.redhat.com dbus[1071]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Jun 26 23:54:34 w541.tc.redhat.com dbus[1071]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Jun 26 23:54:34 w541.tc.redhat.com setroubleshoot[4437]: failed to retrieve rpm info for /home/fred/public_html/index.html
Jun 26 23:54:34 w541.tc.redhat.com setroubleshoot[4437]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /home/fred/public_html/index.html. For complete SELinux messages. run sealert -l c36627c9-7b99-44c9-a78c-a9a737ff119b
Jun 26 23:54:34 w541.tc.redhat.com python3[4437]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /home/fred/public_html/index.html.

                                                  *****  Plugin catchall_boolean (24.7 confidence) suggests   ******************

                                                  If you want to allow httpd to read home directories
                                                  Then you must tell SELinux about this by enabling the 'httpd_enable_homedirs' boolean.
                                                  You can read 'None' man page for more details.
                                                  Do
                                                  setsebool -P httpd_enable_homedirs 1

                                                  *****  Plugin catchall_boolean (24.7 confidence) suggests   ******************

                                                  If you want to allow httpd to read user content
                                                  Then you must tell SELinux about this by enabling the 'httpd_read_user_content' boolean.
                                                  You can read 'None' man page for more details.
                                                  Do
                                                  setsebool -P httpd_read_user_content 1

                                                  *****  Plugin catchall_boolean (24.7 confidence) suggests   ******************

                                                  If you want to unify HTTPD handling of all content files.
                                                  Then you must tell SELinux about this by enabling the 'httpd_unified' boolean.
                                                  You can read 'None' man page for more details.
                                                  Do
                                                  setsebool -P httpd_unified 1

                                                  *****  Plugin public_content (24.7 confidence) suggests   ********************

                                                  If you want to treat index.html as public content
                                                  Then you need to change the label on index.html to public_content_t or public_content_rw_t.
                                                  Do
                                                  # semanage fcontext -a -t public_content_t '/home/fred/public_html/index.html'
                                                  # restorecon -v '/home/fred/public_html/index.html'

                                                  *****  Plugin catchall (3.53 confidence) suggests   **************************

                                                  If you believe that httpd should be allowed getattr access on the index.html file by default.
                                                  Then you should report this as a bug.
```

Real World Examples

- A user, fred, wants to start have his own web page in /home/fred/public_html
  - AH-HAH! Follow the instructions and run “sealert -l c36627c9-7b99-44c9-a78c-a9a737ff119b”
  - It reveals that there are several potential issues/solutions.
    - httpd access to home directories
    - httpd access to user content
    - httpd unified access to all content
    - relabel the content as public

Terminal - root@w541:~

File Edit View Terminal Tabs Help

```
[root@w541 ~]# sealert -l c36627c9-7b99-44c9-a78c-a9a737ff119b
SELinux is preventing /usr/sbin/httpd from getattr access on the file /home/fred/public_html/index.html.

*****  Plugin catchall_boolean (24.7 confidence) suggests   ******************

If you want to allow httpd to read home directories
Then you must tell SELinux about this by enabling the 'httpd_enable_homedirs' boolean.
You can read 'None' man page for more details.
Do
setsebool -P httpd_enable_homedirs 1

*****  Plugin catchall_boolean (24.7 confidence) suggests   ******************

If you want to allow httpd to read user content
Then you must tell SELinux about this by enabling the 'httpd_read_user_content' boolean.
You can read 'None' man page for more details.
Do
setsebool -P httpd_read_user_content 1

*****  Plugin catchall_boolean (24.7 confidence) suggests   ******************

If you want to unify HTTPD handling of all content files.
Then you must tell SELinux about this by enabling the 'httpd_unified' boolean.
You can read 'None' man page for more details.
Do
setsebool -P httpd_unified 1

*****  Plugin public_content (24.7 confidence) suggests   *******************

If you want to treat index.html as public content
Then you need to change the label on index.html to public_content_t or public_content_rw_t.
Do
# semanage fcontext -a -t public_content_t '/home/fred/public_html/index.html'
# restorecon -v '/home/fred/public_html/index.html'

*****  Plugin catchall (3.53 confidence) suggests   **************************

If you believe that httpd should be allowed getattr access on the index.html file by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# ausearch -c '/usr/sbin/httpd' --raw | audit2allow -M my-usrsbinhttpd
# semodule -X 300 -i my-usrsbinhttpd.pp


Additional Information:
Source Context                system_u:system_r:httpd_t:s0
Target Context                unconfined_u:object_r:httpd_user_content_t:s0
```

Real World Examples

- A user, fred, wants to start have his own web page in /home/fred/public_html
  - It also says we can create a policy module to allow this, but in this case, setting a boolean is easier and makes more sense.

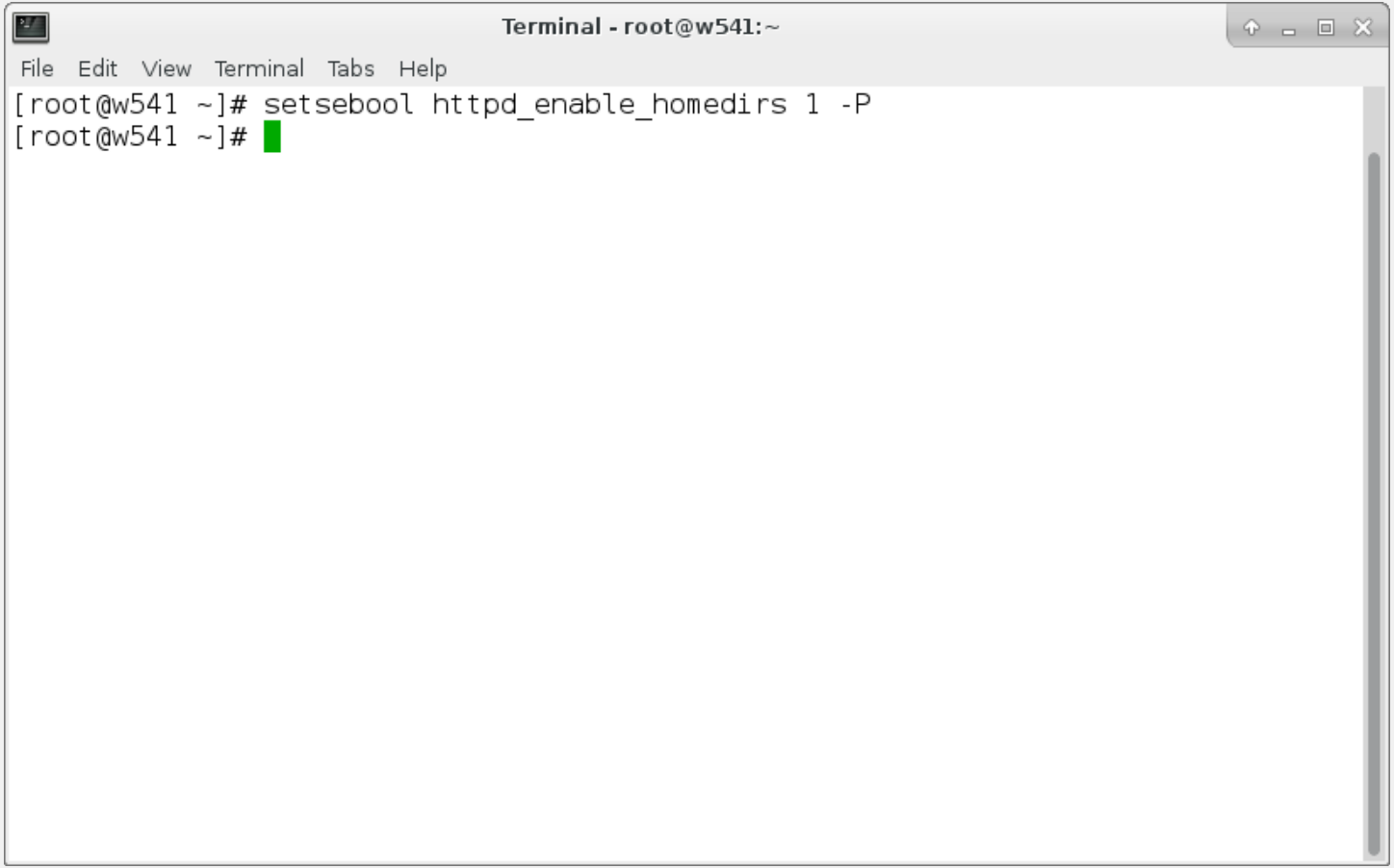
Terminal - root@w541:~

File Edit View Terminal Tabs Help

```
*****  Plugin public_content (24.7 confidence) suggests   ********************

If you want to treat index.html as public content
Then you need to change the label on index.html to public_content_t or public_content_rw_t.
Do
# semanage fcontext -a -t public_content_t '/home/fred/public_html/index.html'
# restorecon -v '/home/fred/public_html/index.html'

*****  Plugin catchall (3.53 confidence) suggests   *************************

If you believe that httpd should be allowed getattr access on the index.html file by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# ausearch -c '/usr/sbin/httpd' --raw | audit2allow -M my-usrsbinhttpd
# semodule -X 300 -i my-usrsbinhttpd.pp


Additional Information:
Source Context                system_u:system_r:httpd_t:s0
Target Context                unconfined_u:object_r:httpd_user_content_t:s0
Target Objects                /home/fred/public_html/index.html [ file ]
Source                        /usr/sbin/httpd
Source Path                   /usr/sbin/httpd
Port                          <Unknown>
Host                          w541.tc.redhat.com
Source RPM Packages           httpd-2.4.18-1.fc23.x86_64
Target RPM Packages
Policy RPM                    selinux-policy-3.13.1-158.15.fc23.noarch
Selinux Enabled               True
Policy Type                   targeted
Enforcing Mode                Enforcing
Host Name                     w541.tc.redhat.com
Platform                      Linux w541.tc.redhat.com 4.5.7-200.fc23.x86_64 #1
                              SMP Wed Jun 8 17:41:50 UTC 2016 x86_64 x86_64
Alert Count                   6
First Seen                    2016-06-26 23:03:27 PDT
Last Seen                     2016-06-26 23:54:31 PDT
Local ID                      c36627c9-7b99-44c9-a78c-a9a737ff119b

Raw Audit Messages
type=AVC msg=audit(1467010471.39:424): avc:  denied  { getattr } for  pid=1489 comm="/usr/sbin/httpd" path="/home/fred/public_html/index.html" dev="dm-0" ino=19803817 scontext=system_u:syste
m_r:httpd_t:s0 tcontext=unconfined_u:object_r:httpd_user_content_t:s0 tclass=file permissive=0


Hash: /usr/sbin/httpd,httpd_t,httpd_user_content_t,file,getattr

[root@w541 ~]#
```

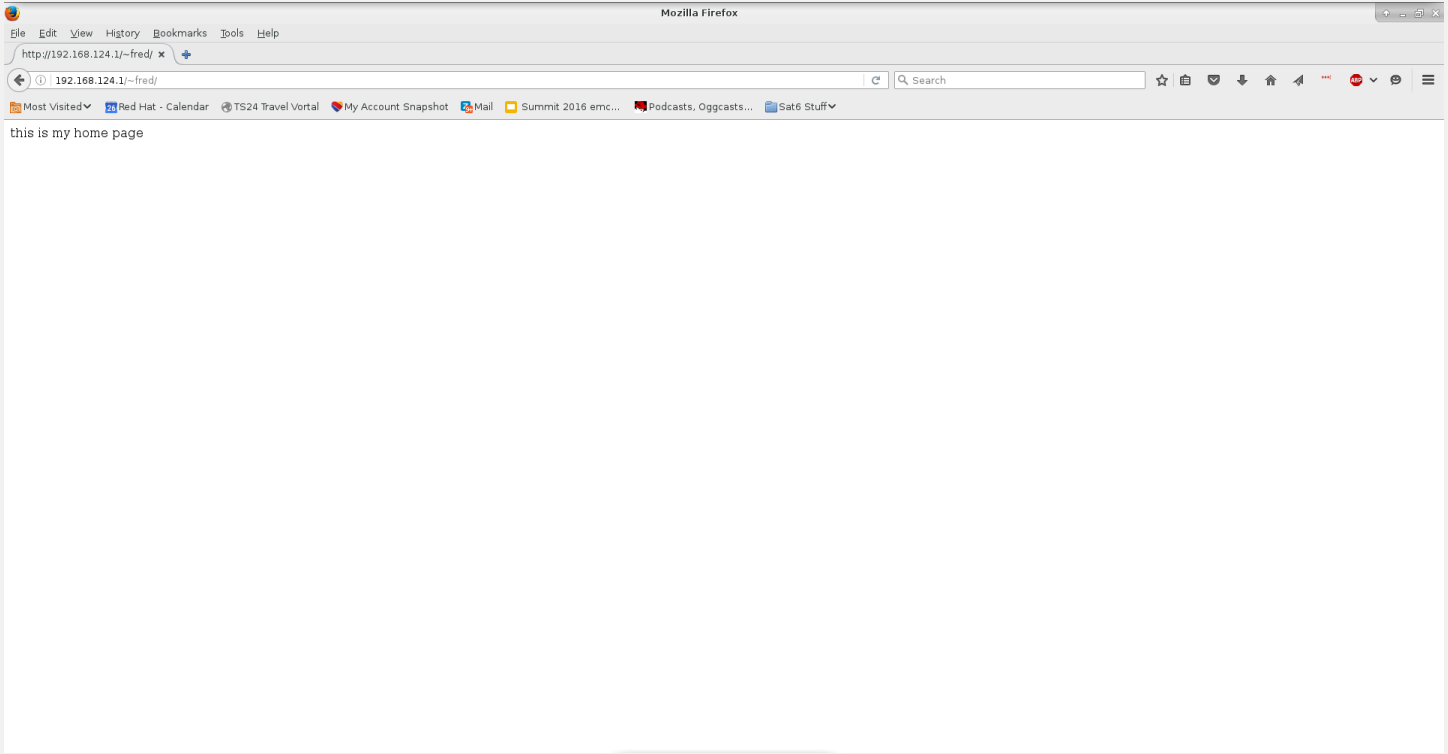
Real World Examples

- A user, fred, wants to start have his own web page in /home/fred/public_html
  - Follow the instructions and set the boolean to allow httpd access to home directories.


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# setsebool httpd_enable_homedirs 1 -P
[root@w541 ~]#

Real World Examples

- A user, fred, wants to start have his own web page in /home/fred/public_html
  - And... Voila!


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.124.1/~fred/
192.168.124.1/~fred/
Search
Most Visited
Red Hat - Calendar
TS24 Travel Vortal
My Account Snapshot
Mail
Summit 2016 emc...
Podcasts, Oggcasts...
Sat6 Stuff
this is my home page

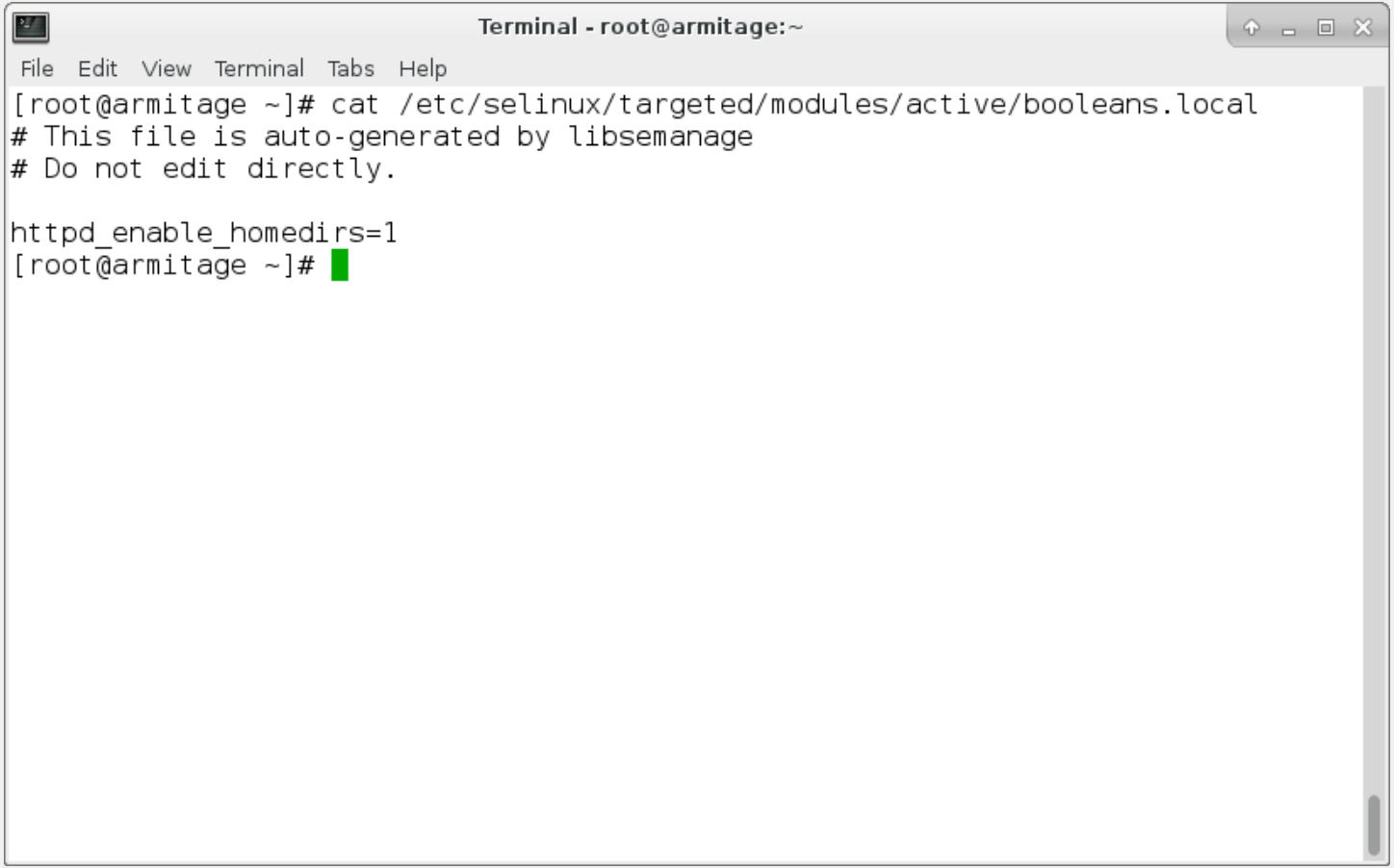
Real World Examples

- And people say this SELinux thing is too hard! Pffft!

HOW CAN I SEE WHAT BOOLEANS HAVE BEEN SET?

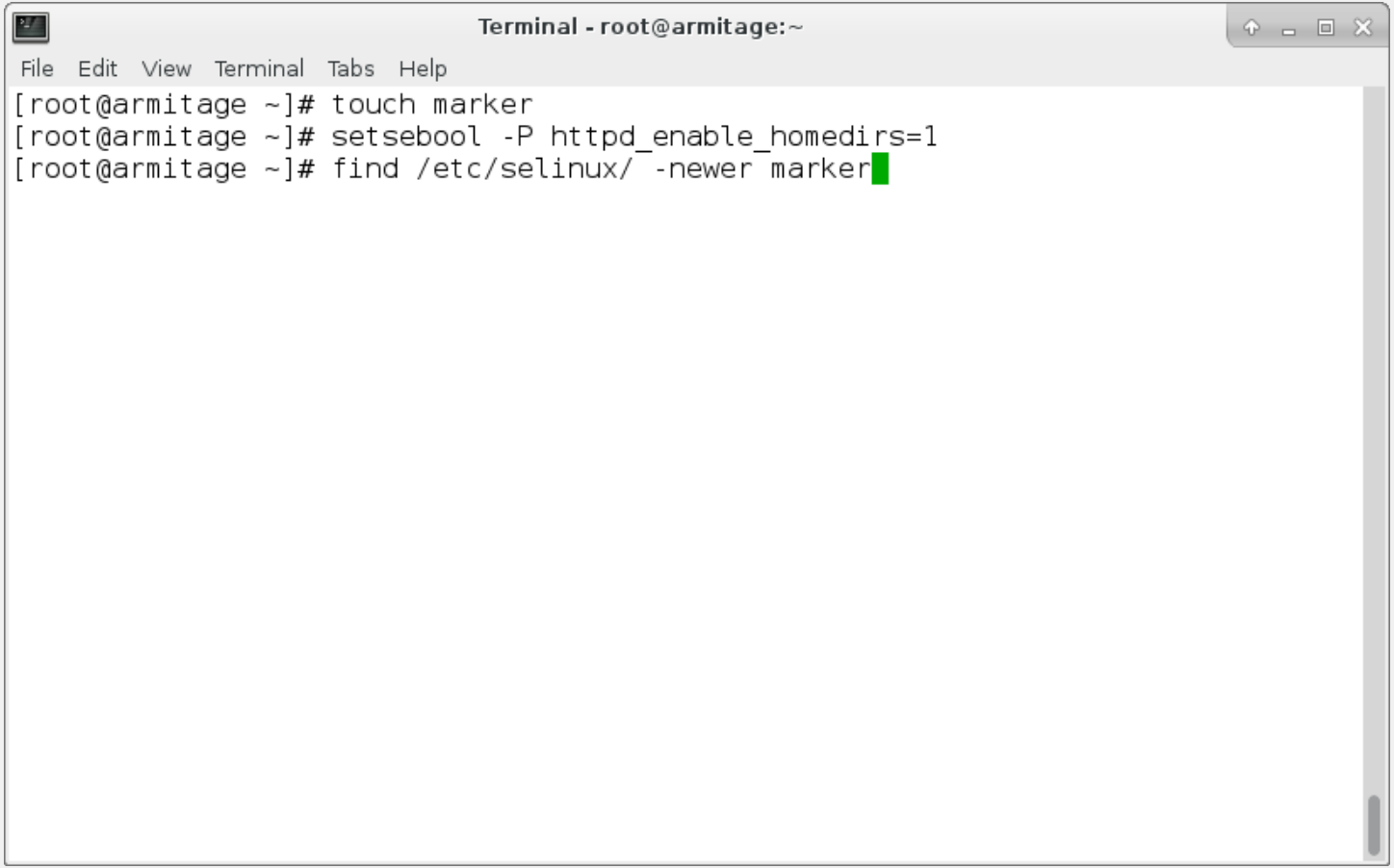
How Can I See What Booleans Have Been Set?

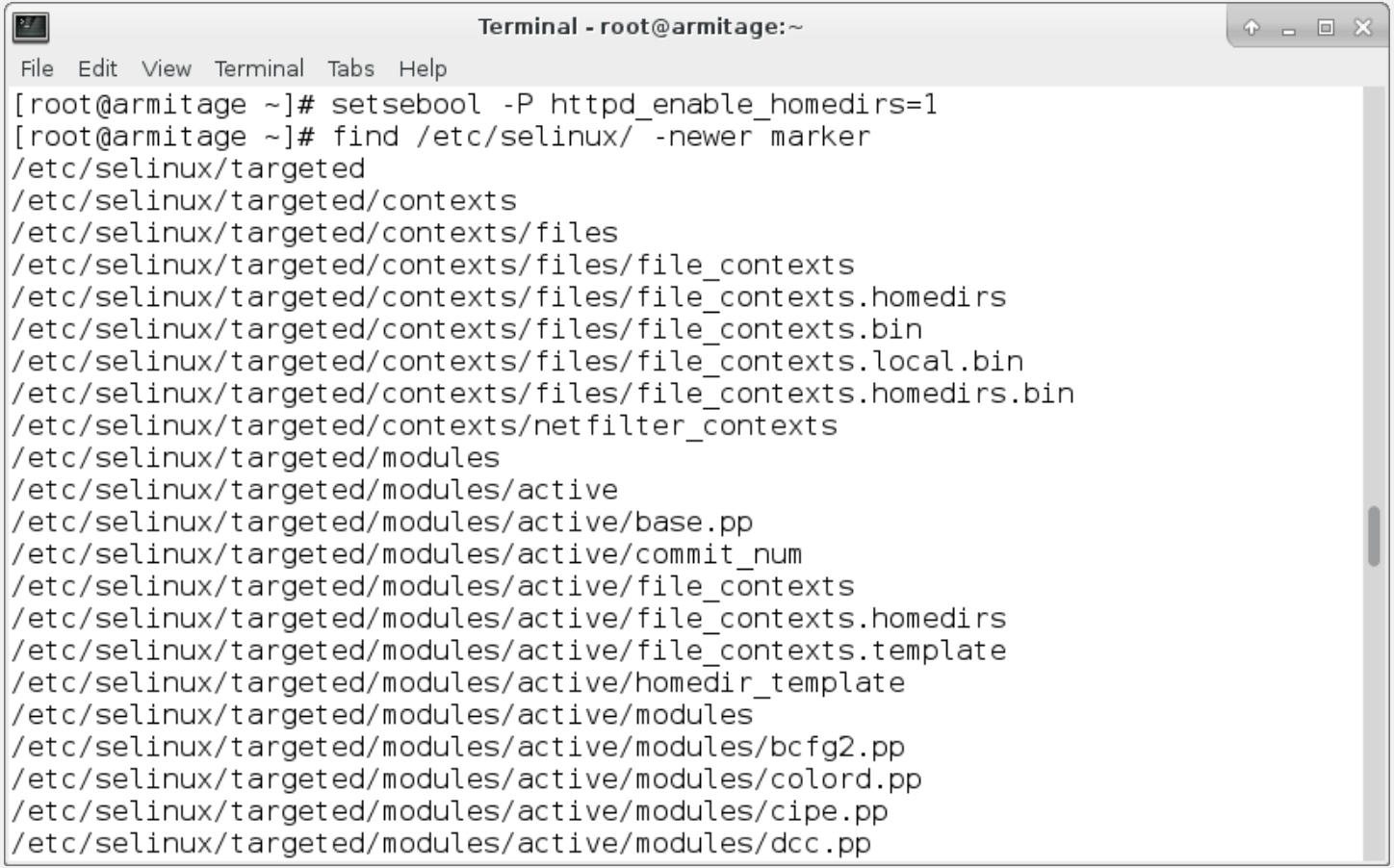
- Look at the booleans.local file under /etc/selinux/targeted/modules/active/

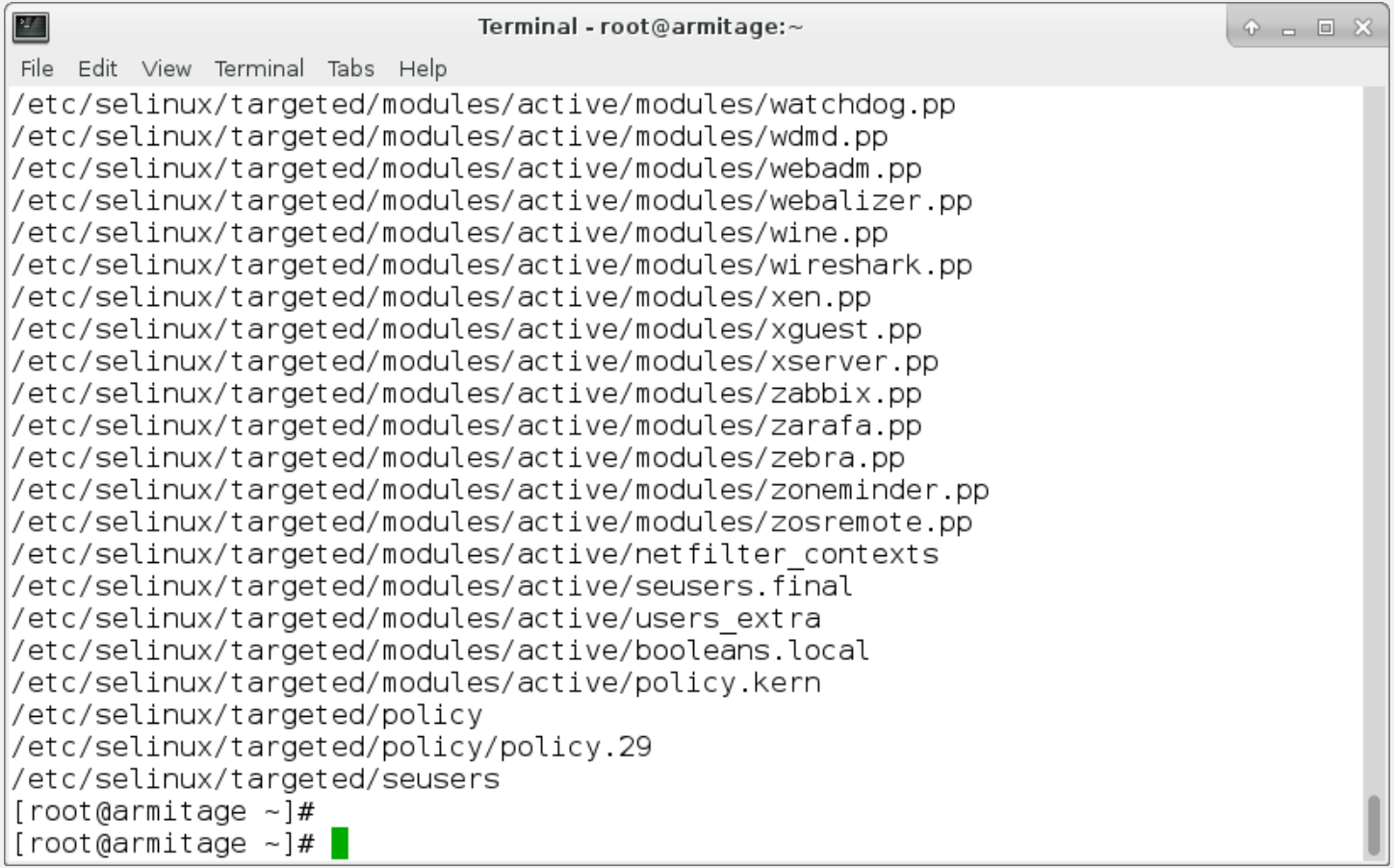

Terminal - root@armitage:~
File Edit View Terminal Tabs Help
[root@armitage ~]# cat /etc/selinux/targeted/modules/active/booleans.local
# This file is auto-generated by libsemanage
# Do not edit directly.
httpd_enable_homedirs=1
[root@armitage ~]#

How Can I See What Booleans Have Been Set?

- Note that when you use setsebool -P (and other commands we'll cover later), the entire /etc/selinux/targeted directory is regenerated. That file doesn't actually do anything - it just tells you what's been set. Believe it when it says “Do not edit directly” - it won't do anything.


Terminal - root@armitage:~
File Edit View Terminal Tabs Help
[root@armitage ~]# touch marker
[root@armitage ~]# setsebool -P httpd_enable_homedirs=1
[root@armitage ~]# find /etc/selinux/ -newer marker


Terminal - root@armitage:~
File Edit View Terminal Tabs Help
[root@armitage ~]# setsebool -P httpd_enable_homedirs=1
[root@armitage ~]# find /etc/selinux/ -newer marker
/etc/selinux/targeted
/etc/selinux/targeted/contexts
/etc/selinux/targeted/contexts/files
/etc/selinux/targeted/contexts/files/file_contexts
/etc/selinux/targeted/contexts/files/file_contexts.homedirs
/etc/selinux/targeted/contexts/files/file_contexts.bin
/etc/selinux/targeted/contexts/files/file_contexts.local.bin
/etc/selinux/targeted/contexts/files/file_contexts.homedirs.bin
/etc/selinux/targeted/contexts/netfilter_contexts
/etc/selinux/targeted/modules
/etc/selinux/targeted/modules/active
/etc/selinux/targeted/modules/active/base.pp
/etc/selinux/targeted/modules/active/commit_num
/etc/selinux/targeted/modules/active/file_contexts
/etc/selinux/targeted/modules/active/file_contexts.homedirs
/etc/selinux/targeted/modules/active/file_contexts.template
/etc/selinux/targeted/modules/active/homedir_template
/etc/selinux/targeted/modules/active/modules
/etc/selinux/targeted/modules/active/modules/bcfg2.pp
/etc/selinux/targeted/modules/active/modules/colord.pp
/etc/selinux/targeted/modules/active/modules/cipe.pp
/etc/selinux/targeted/modules/active/modules/dcc.pp


Terminal - root@armitage:~
File Edit View Terminal Tabs Help
/etc/selinux/targeted/modules/active/modules/watchdog.pp
/etc/selinux/targeted/modules/active/modules/wdmd.pp
/etc/selinux/targeted/modules/active/modules/webadm.pp
/etc/selinux/targeted/modules/active/modules/webalizer.pp
/etc/selinux/targeted/modules/active/modules/wine.pp
/etc/selinux/targeted/modules/active/modules/wireshark.pp
/etc/selinux/targeted/modules/active/modules/xen.pp
/etc/selinux/targeted/modules/active/modules/xguest.pp
/etc/selinux/targeted/modules/active/modules/xserver.pp
/etc/selinux/targeted/modules/active/modules/zabbix.pp
/etc/selinux/targeted/modules/active/modules/zarafa.pp
/etc/selinux/targeted/modules/active/modules/zebra.pp
/etc/selinux/targeted/modules/active/modules/zoneminder.pp
/etc/selinux/targeted/modules/active/modules/zosremote.pp
/etc/selinux/targeted/modules/active/netfilter_contexts
/etc/selinux/targeted/modules/active/seusers.final
/etc/selinux/targeted/modules/active/users_extra
/etc/selinux/targeted/modules/active/booleans.local
/etc/selinux/targeted/modules/active/policy.kern
/etc/selinux/targeted/policy
/etc/selinux/targeted/policy/policy.29
/etc/selinux/targeted/seusers
[root@armitage ~]#
[root@armitage ~]#

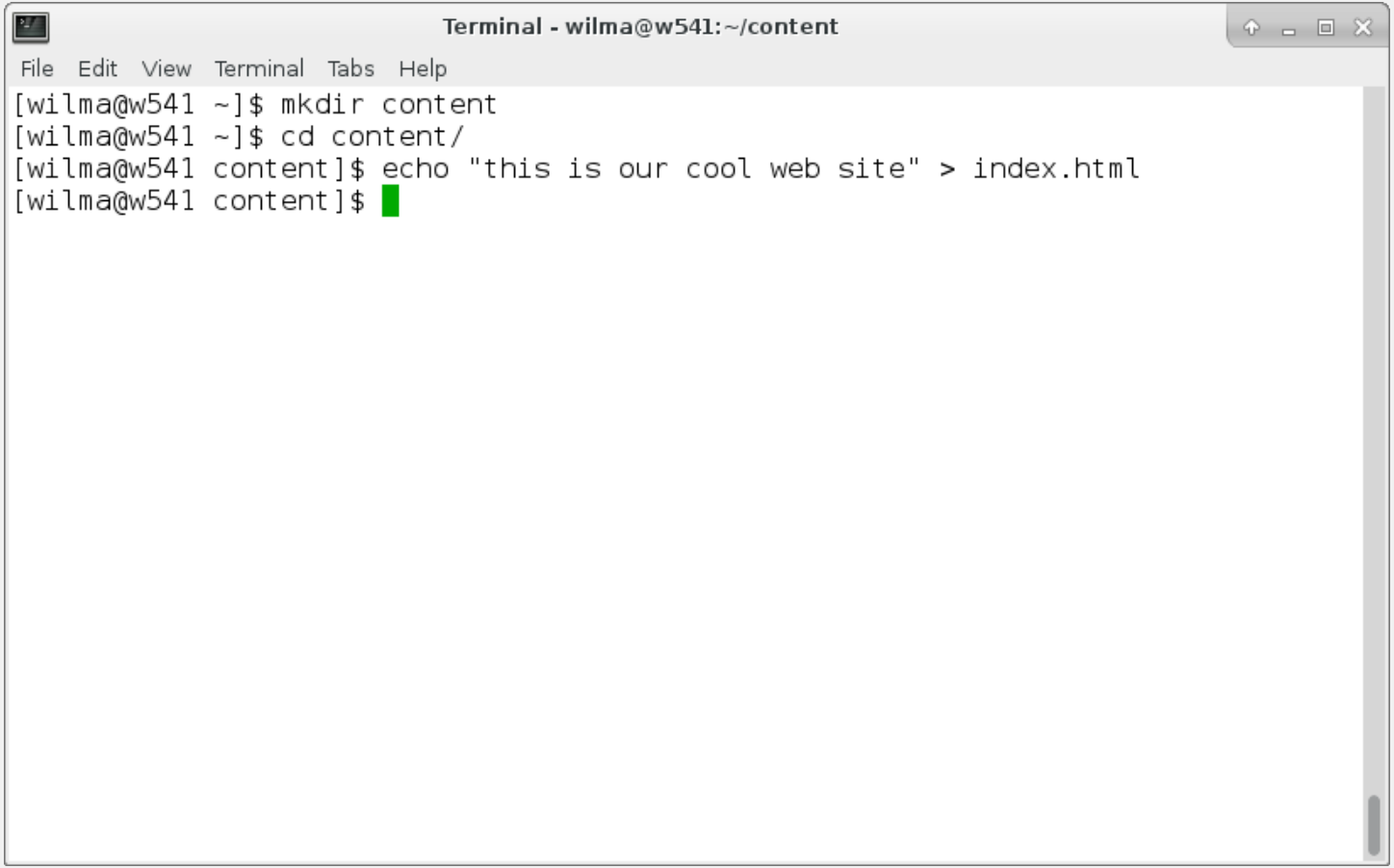
REAL WORLD EXAMPLES

Real World Examples

- This next example assumes an unmodified SELinux environment, so ignore the changes from the last example.

Real World Examples

- A user, Wilma, is a web content author. She has created content in her home directory and asked that you move it to the web site.


Terminal - wilma@w541:~/content
File Edit View Terminal Tabs Help
[wilma@w541 ~]$ mkdir content
[wilma@w541 ~]$ cd content/
[wilma@w541 content]$ echo "this is our cool web site" > index.html
[wilma@w541 content]$

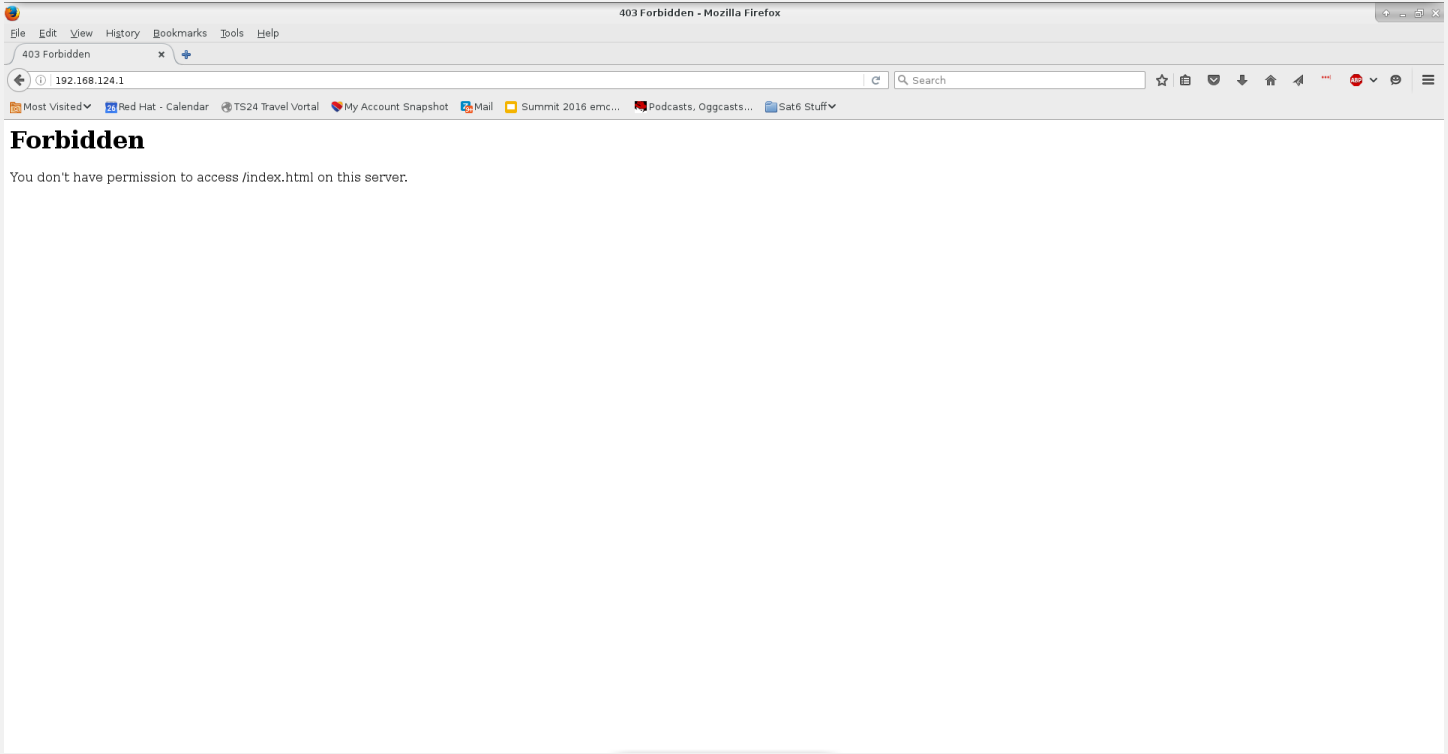
Real World Examples

- So, you move it over.


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# mv /home/wilma/content/* /var/www/html/
[root@w541 ~]#

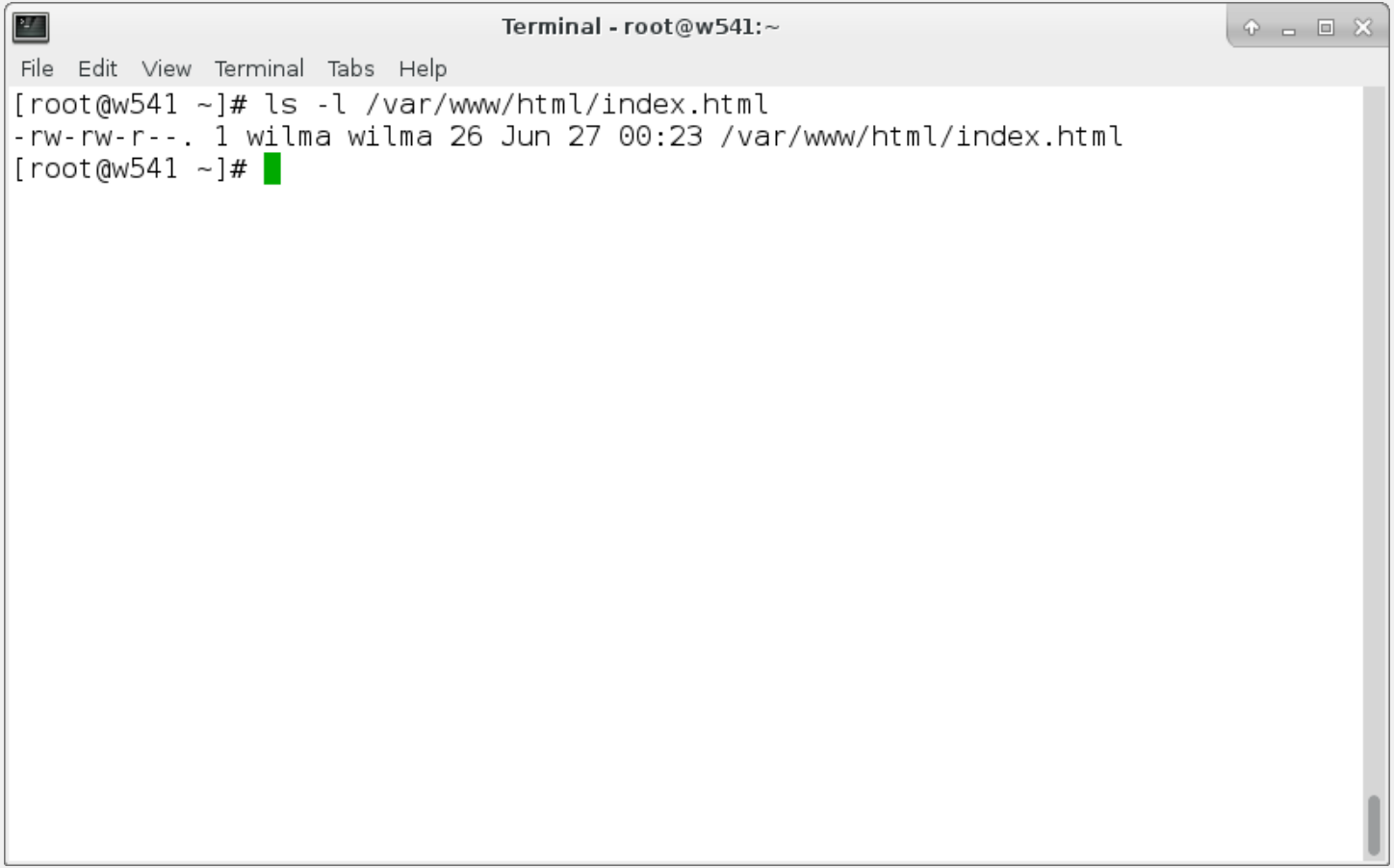
Real World Examples

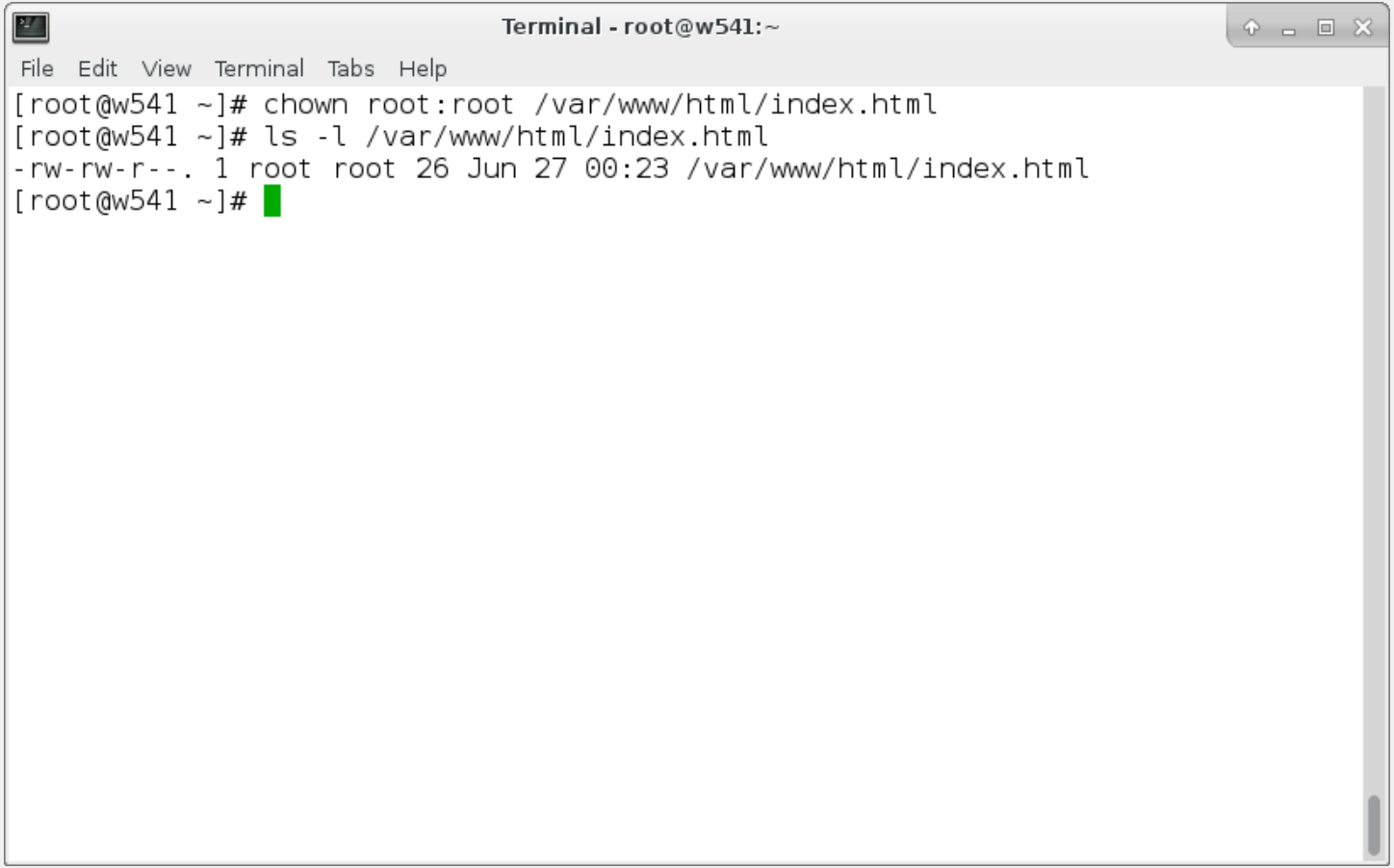
- And when you go to test...


403 Forbidden - Mozilla Firefox
File Edit View History Bookmarks Tools Help
403 Forbidden
192.168.124.1
Search
Most Visited
Red Hat - Calendar
TS24 Travel Vortal
My Account Snapshot
Mail
Summit 2016 emc...
Podcasts, Oggcasts...
Sat6 Stuff
Forbidden
You don't have permission to access /index.html on this server.

Real World Examples

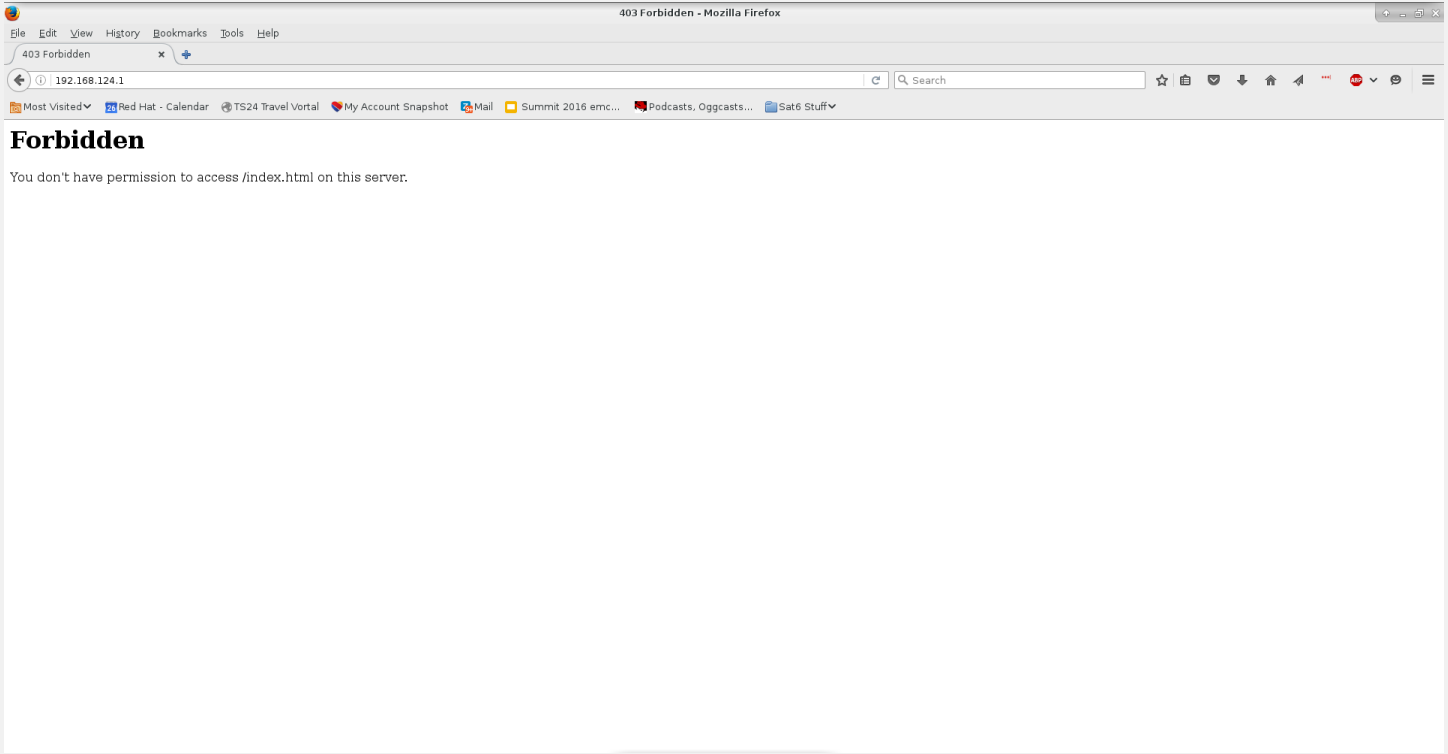
- Ah, it's the wrong owner, right?


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# ls -l /var/www/html/index.html
-rw-rw-r--. 1 wilma wilma 26 Jun 27 00:23 /var/www/html/index.html
[root@w541 ~]#


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# chown root:root /var/www/html/index.html
[root@w541 ~]# ls -l /var/www/html/index.html
-rw-rw-r--. 1 root root 26 Jun 27 00:23 /var/www/html/index.html
[root@w541 ~]#

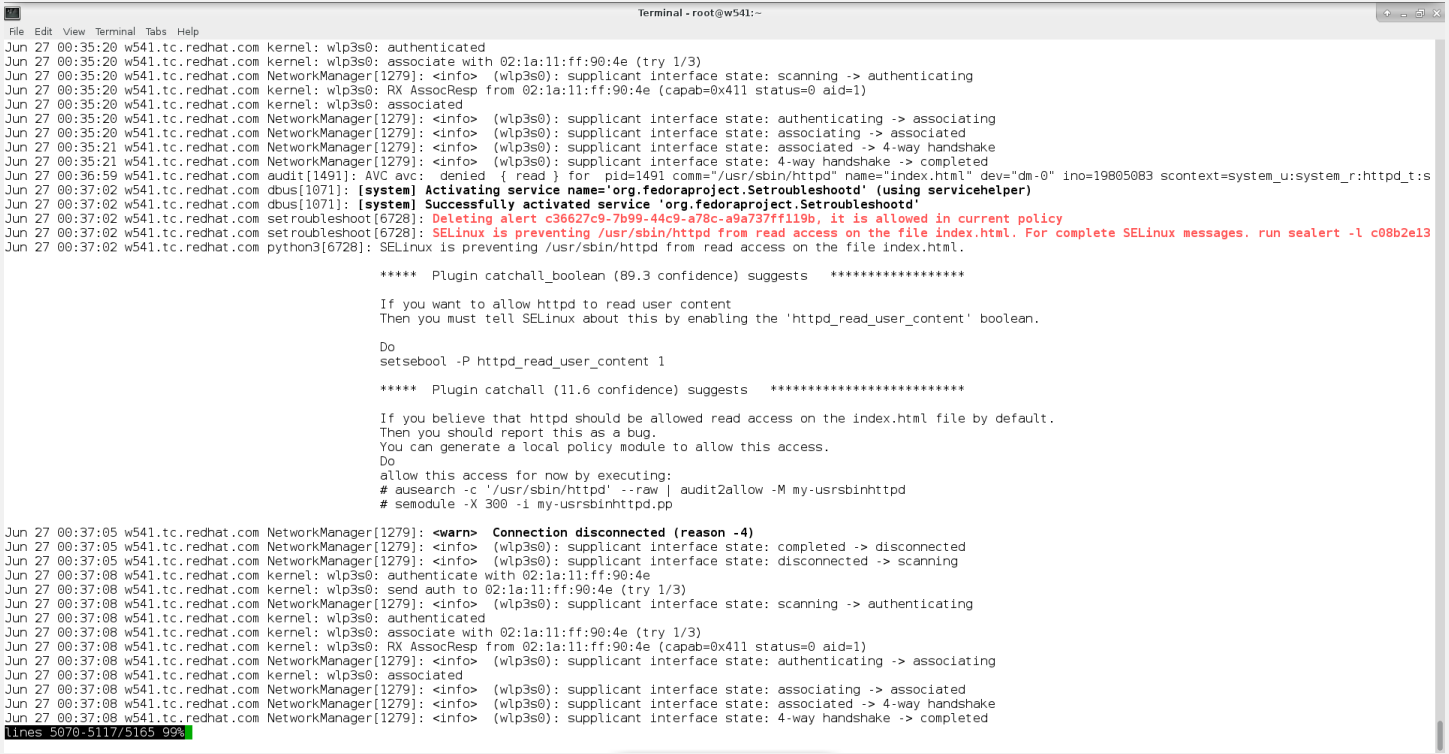
Real World Examples

- But when you test...


403 Forbidden - Mozilla Firefox
File Edit View History Bookmarks Tools Help
403 Forbidden
192.168.124.1
Search
Most Visited
Red Hat - Calendar
TS24 Travel Vortal
My Account Snapshot
Mail
Summit 2016 emc...
Podcasts, Oggcasts...
Sat6 Stuff
Forbidden
You don't have permission to access /index.html on this server.

Real World Examples

- Checking journalctl again tells you to run sealert.


Terminal - root@w541:~
File Edit View Terminal Tabs Help
Jun 27 00:35:20 w541.tc.redhat.com kernel: wlp3s0: authenticated
Jun 27 00:35:20 w541.tc.redhat.com kernel: wlp3s0: associate with 02:1a:11:ff:90:4e (try 1/3)
Jun 27 00:35:20 w541.tc.redhat.com NetworkManager[1279]: <info> (wlp3s0): supplicant interface state: scanning -> authenticating
Jun 27 00:35:20 w541.tc.redhat.com kernel: wlp3s0: RX AssocResp from 02:1a:11:ff:90:4e (capab=0x411 status=0 aid=1)
Jun 27 00:35:20 w541.tc.redhat.com kernel: wlp3s0: associated
Jun 27 00:35:20 w541.tc.redhat.com NetworkManager[1279]: <info> (wlp3s0): supplicant interface state: authenticating -> associating
Jun 27 00:35:20 w541.tc.redhat.com NetworkManager[1279]: <info> (wlp3s0): supplicant interface state: associating -> associated
Jun 27 00:35:21 w541.tc.redhat.com NetworkManager[1279]: <info> (wlp3s0): supplicant interface state: associated -> 4-way handshake
Jun 27 00:35:21 w541.tc.redhat.com NetworkManager[1279]: <info> (wlp3s0): supplicant interface state: 4-way handshake -> completed
Jun 27 00:36:59 w541.tc.redhat.com audit[1491]: AVC avc: denied { read } for pid=1491 comm="/usr/sbin/httpd" name="index.html" dev="dm-0" ino=19805083 scontext=system_u:system_r:httpd_t:s
Jun 27 00:37:02 w541.tc.redhat.com dbus[1071]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Jun 27 00:37:02 w541.tc.redhat.com dbus[1071]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Jun 27 00:37:02 w541.tc.redhat.com setroubleshoot[6728]: Deleting alert c36627c9-7b99-44c9-a78c-a9a737ff119b, it is allowed in current policy
Jun 27 00:37:02 w541.tc.redhat.com setroubleshoot[6728]: SELinux is preventing /usr/sbin/httpd from read access on the file index.html. For complete SELinux messages. run sealert -l c08b2e13
Jun 27 00:37:02 w541.tc.redhat.com python3[6728]: SELinux is preventing /usr/sbin/httpd from read access on the file index.html.
***** Plugin catchall_boolean (89.3 confidence) suggests ******************
If you want to allow httpd to read user content
Then you must tell SELinux about this by enabling the 'httpd_read_user_content' boolean.
Do
setsebool -P httpd_read_user_content 1
***** Plugin catchall (11.6 confidence) suggests ***************************
If you believe that httpd should be allowed read access on the index.html file by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
ausearch -c '/usr/sbin/httpd' --raw | audit2allow -M my-usrsbinhttpd
semodule -X 300 -i my-usrsbinhttpd.pp
Jun 27 00:37:05 w541.tc.redhat.com NetworkManager[1279]: <warn> Connection disconnected (reason -4)
Jun 27 00:37:05 w541.tc.redhat.com NetworkManager[1279]: <info> (wlp3s0): supplicant interface state: completed -> disconnected
Jun 27 00:37:05 w541.tc.redhat.com NetworkManager[1279]: <info> (wlp3s0): supplicant interface state: disconnected -> scanning
Jun 27 00:37:08 w541.tc.redhat.com kernel: wlp3s0: authenticate with 02:1a:11:ff:90:4e
Jun 27 00:37:08 w541.tc.redhat.com kernel: wlp3s0: send auth to 02:1a:11:ff:90:4e (try 1/3)
Jun 27 00:37:08 w541.tc.redhat.com NetworkManager[1279]: <info> (wlp3s0): supplicant interface state: scanning -> authenticating
Jun 27 00:37:08 w541.tc.redhat.com kernel: wlp3s0: authenticated
Jun 27 00:37:08 w541.tc.redhat.com kernel: wlp3s0: associate with 02:1a:11:ff:90:4e (try 1/3)
Jun 27 00:37:08 w541.tc.redhat.com kernel: wlp3s0: RX AssocResp from 02:1a:11:ff:90:4e (capab=0x411 status=0 aid=1)
Jun 27 00:37:08 w541.tc.redhat.com NetworkManager[1279]: <info> (wlp3s0): supplicant interface state: authenticating -> associating
Jun 27 00:37:08 w541.tc.redhat.com kernel: wlp3s0: associated
Jun 27 00:37:08 w541.tc.redhat.com NetworkManager[1279]: <info> (wlp3s0): supplicant interface state: associating -> associated
Jun 27 00:37:08 w541.tc.redhat.com NetworkManager[1279]: <info> (wlp3s0): supplicant interface state: associated -> 4-way handshake
Jun 27 00:37:08 w541.tc.redhat.com NetworkManager[1279]: <info> (wlp3s0): supplicant interface state: 4-way handshake -> completed
lines 5070-5117/5165 99%

Real World Examples

- But this time, sealert is still talking about user content and home directories... We're dealing with content in the system web content directory, /var/www/html.

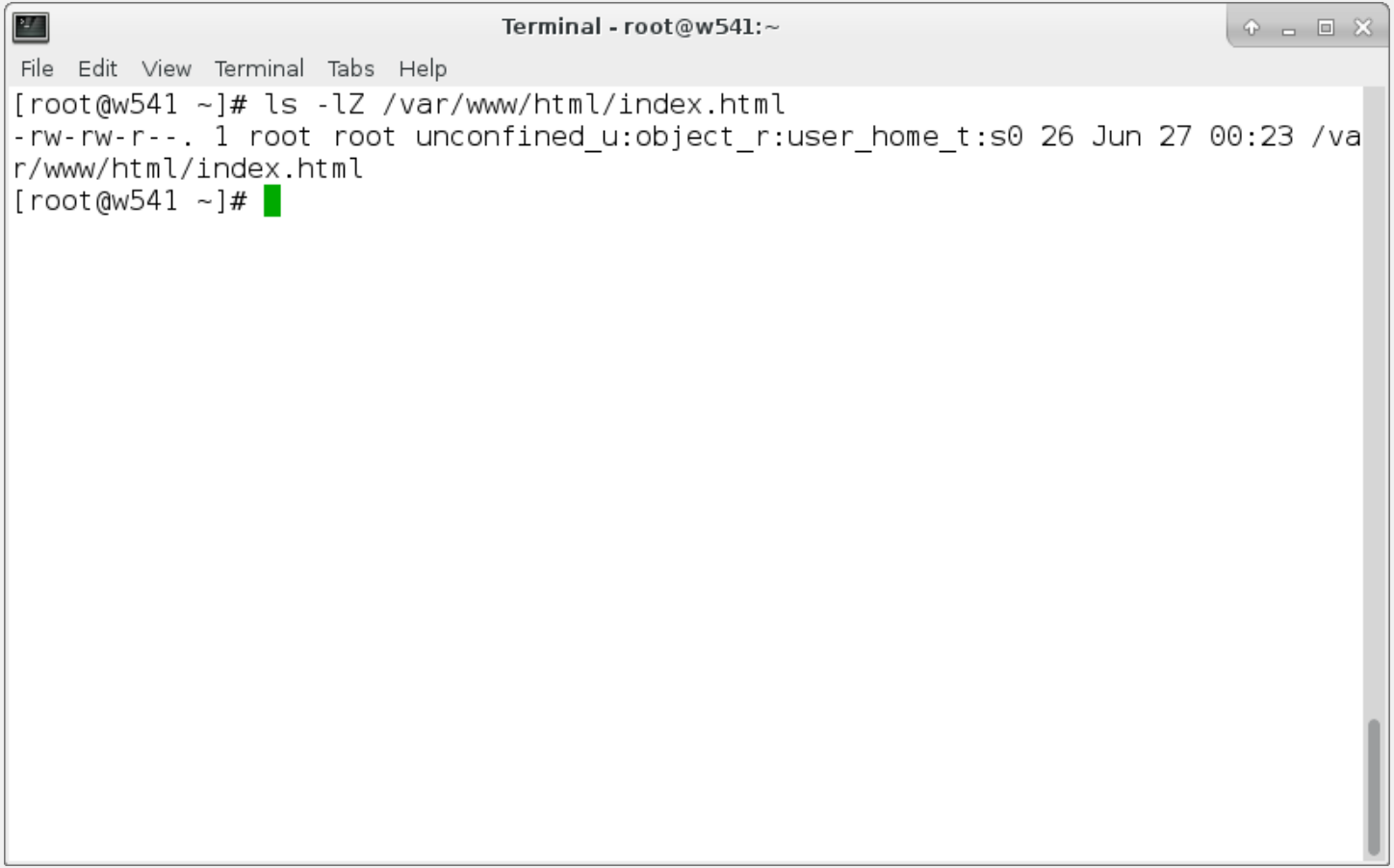
Terminal - root@w541:~

File Edit View Terminal Tabs Help

```
[root@w541 ~]# sealert -l c08b2e13-8637-4564-8916-8288b28f145c
SELinux is preventing /usr/sbin/httpd from read access on the file index.html.

*****  Plugin catchall_boolean (89.3 confidence) suggests   ******************

If you want to allow httpd to read user content
Then you must tell SELinux about this by enabling the 'httpd_read_user_content' boolean.
You can read 'None' man page for more details.
Do
setsebool -P httpd_read_user_content 1

*****  Plugin catchall (11.6 confidence) suggests   **************************

If you believe that httpd should be allowed read access on the index.html file by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
# ausearch -c '/usr/sbin/httpd' --raw | audit2allow -M my-usrsbinhttpd
# semodule -X 300 -i my-usrsbinhttpd.pp


Additional Information:
Source Context                system_u:system_r:httpd_t:s0
Target Context                unconfined_u:object_r:user_home_t:s0
Target Objects                index.html [ file ]
Source                        /usr/sbin/httpd
Source Path                   /usr/sbin/httpd
Port                          <Unknown>
Host                          w541.tc.redhat.com
Source RPM Packages           httpd-2.4.18-1.fc23.x86_64
Target RPM Packages
Policy RPM                    selinux-policy-3.13.1-158.15.fc23.noarch
Selinux Enabled               True
Policy Type                   targeted
Enforcing Mode                Enforcing
Host Name                     w541.tc.redhat.com
Platform                      Linux w541.tc.redhat.com 4.5.7-200.fc23.x86_64 #1
                              SMP Wed Jun 8 17:41:50 UTC 2016 x86_64 x86_64
Alert Count                   1
First Seen                    2016-06-27 00:36:59 PDT
Last Seen                     2016-06-27 00:36:59 PDT
Local ID                      c08b2e13-8637-4564-8916-8288b28f145c

Raw Audit Messages
type=AVC msg=audit(1467013019.225:592): avc:  denied  { read } for  pid=1491 comm="/usr/sbin/httpd" name="index.html" dev="dm-0" ino=19805083 scontext=system_u:system_r:httpd_t:s0 tcontext=u
nconfined_u:object_r:user_home_t:s0 tclass=file permissive=0
```

Real World Examples

- A quick ls -Z reveals the issue.

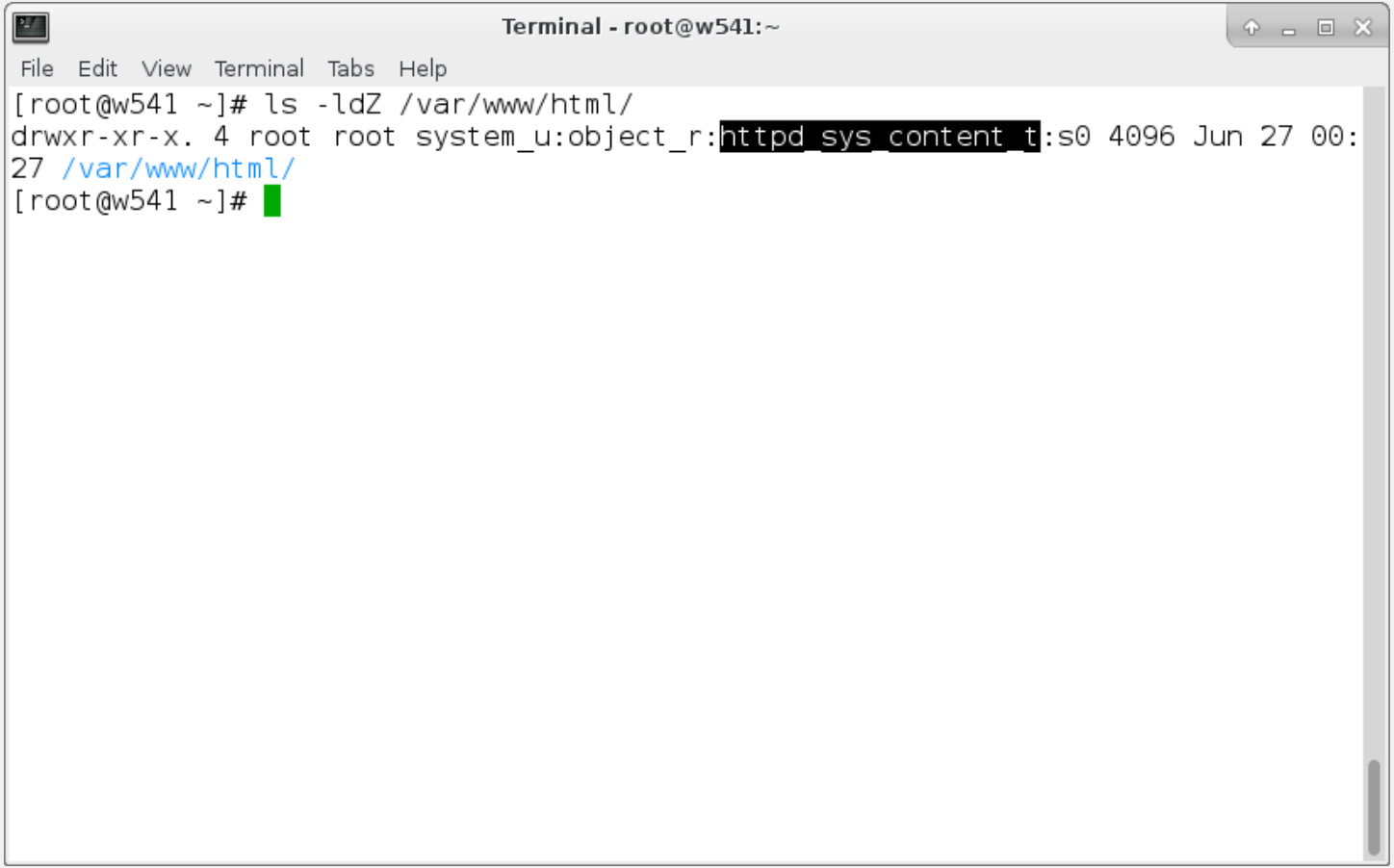

Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# ls -lZ /var/www/html/index.html
-rw-rw-r--. 1 root root unconfined_u:object_r:user_home_t:s0 26 Jun 27 00:23 /var/www/html/index.html
[root@w541 ~]#

Real World Examples

- We moved instead of copied, so the file kept its original context.
- To change the context, we can run one of a couple of commands.

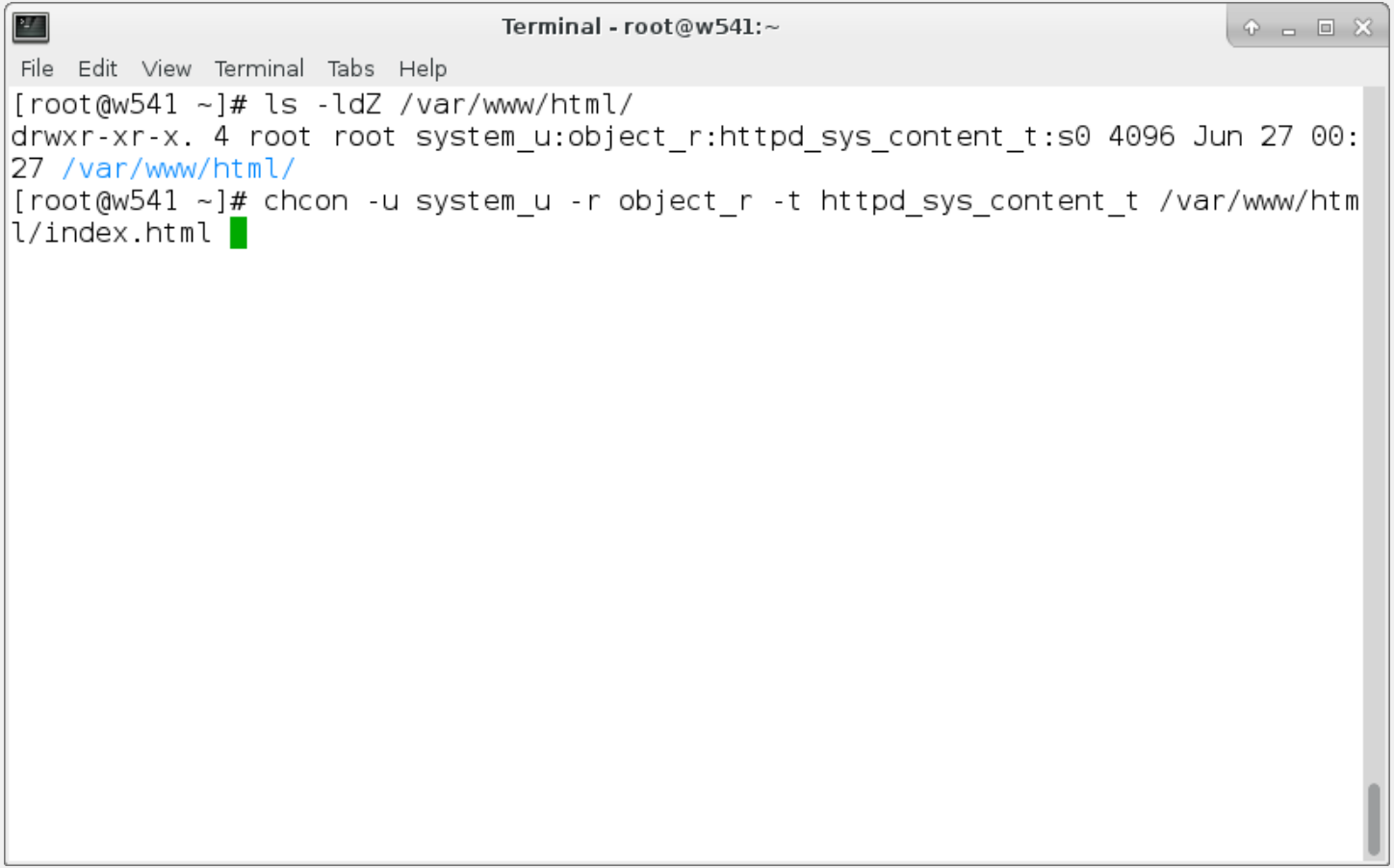
Real World Examples

- First we need to figure out what the label should be. Look at a known good file label.


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# ls -ldZ /var/www/html/
drwxr-xr-x. 4 root root system_u:object_r:httpd_sys_content_t:s0 4096 Jun 27 00:
27 /var/www/html/
[root@w541 ~]#

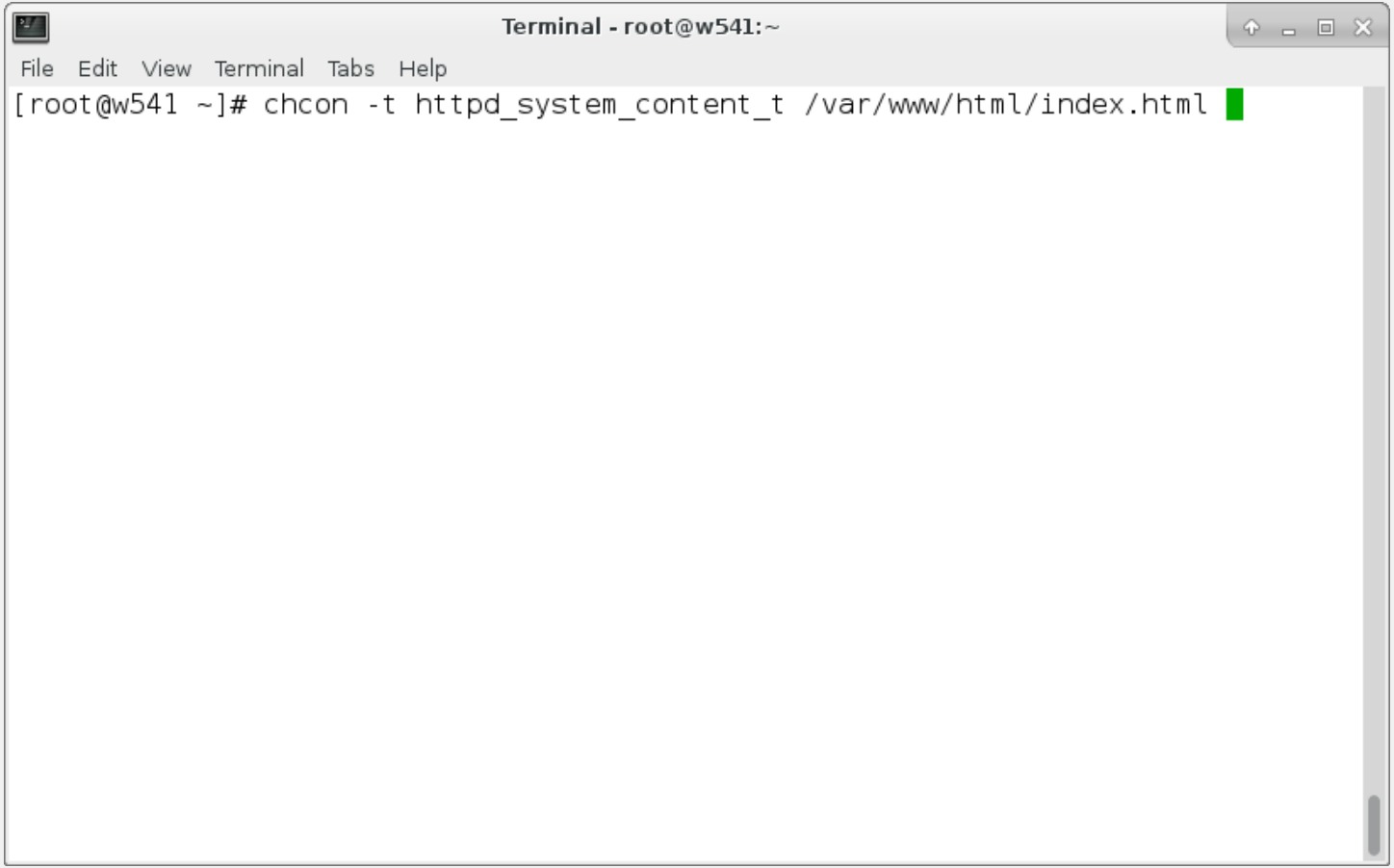
Real World Examples

- Use that information as arguments for the chcon (change context) command
- The long form is:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# ls -ldZ /var/www/html/
drwxr-xr-x. 4 root root system_u:object_r:httpd_sys_content_t:s0 4096 Jun 27 00:
27 /var/www/html/
[root@w541 ~]# chcon -u system_u -r object_r -t httpd_sys_content_t /var/www/htm
l/index.html

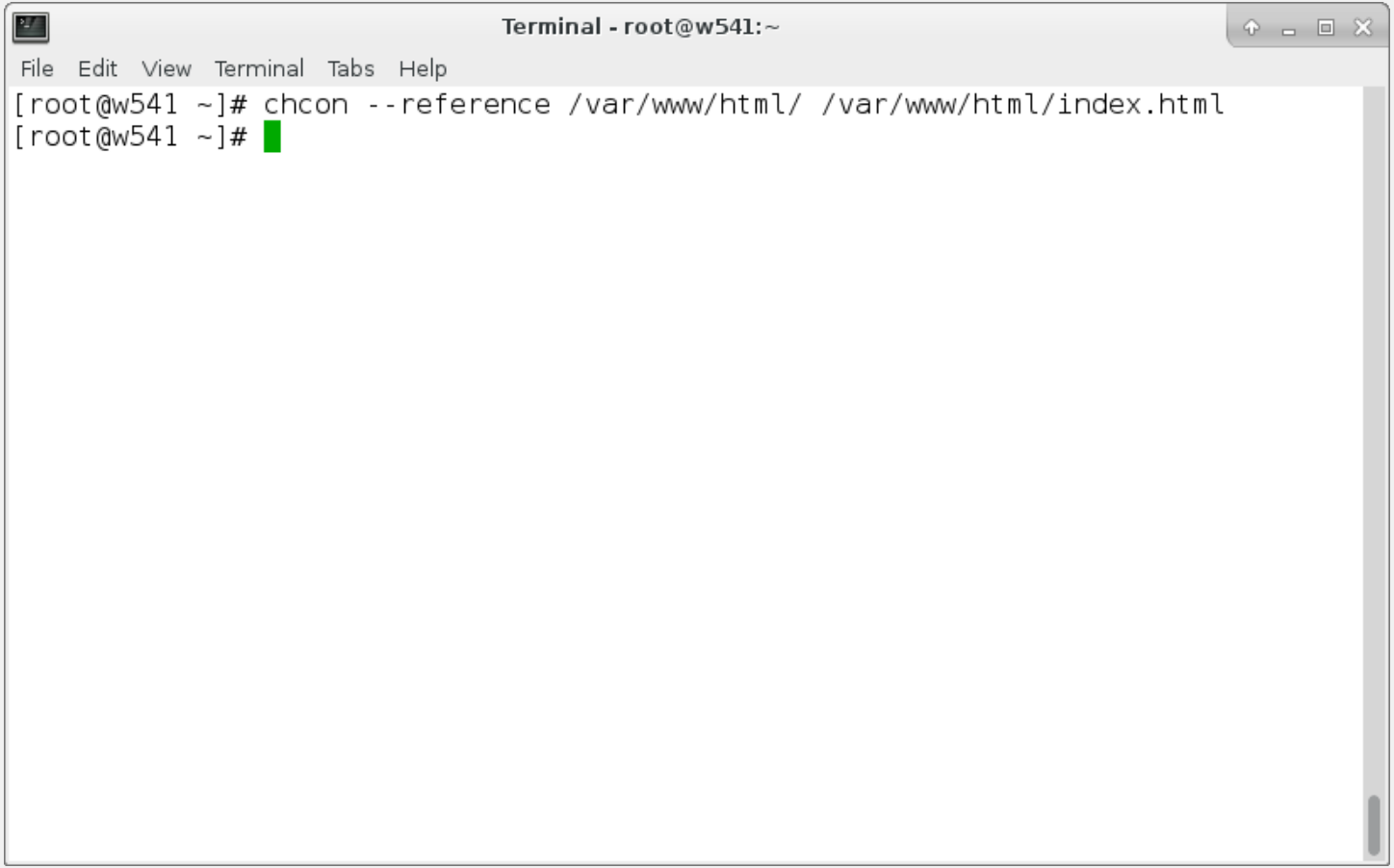
Real World Examples

- Remember that the targeted policy doesn't use the SELinux user or role. The short form is:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# chcon -t httpd_system_content_t /var/www/html/index.html

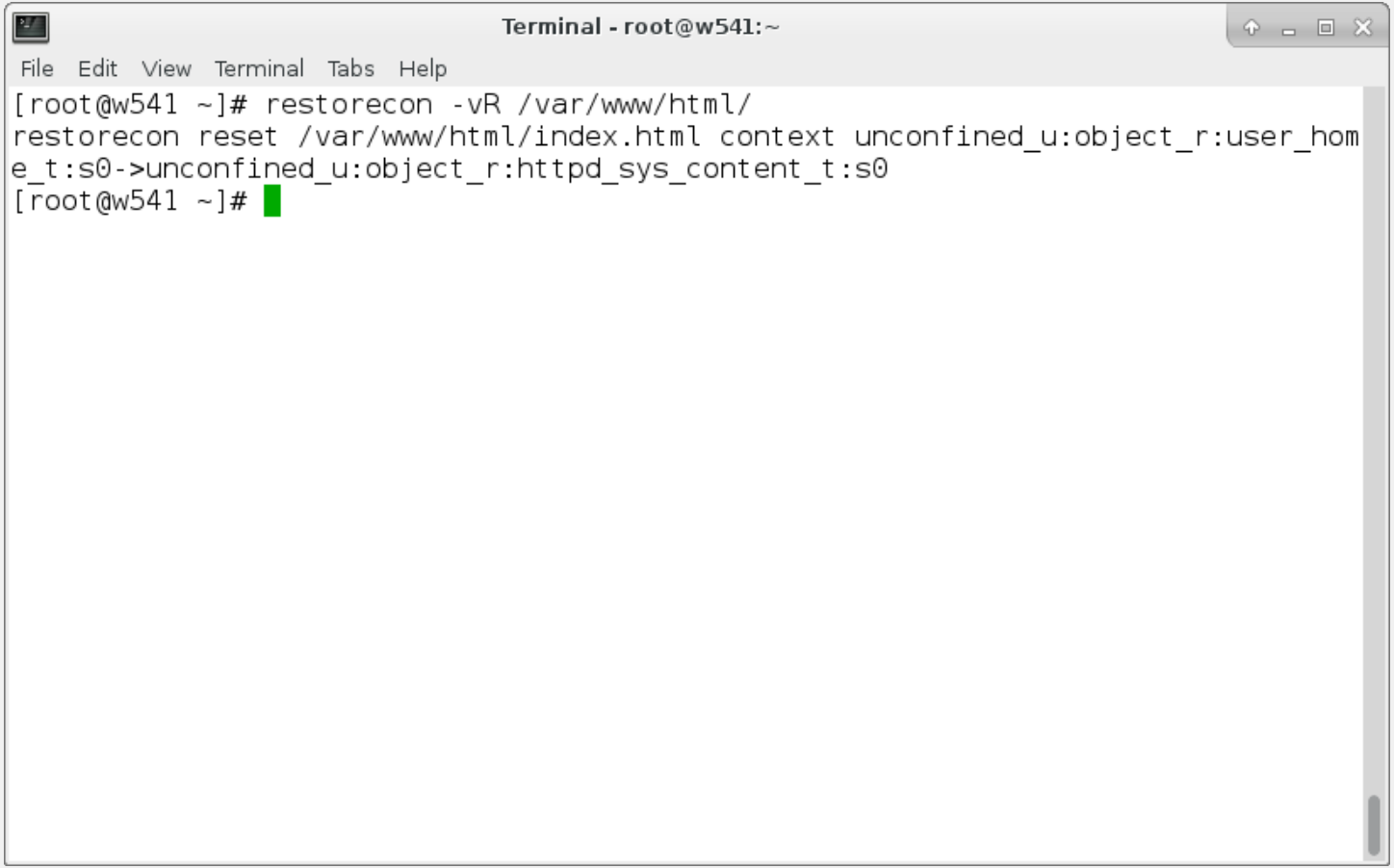
Real World Examples

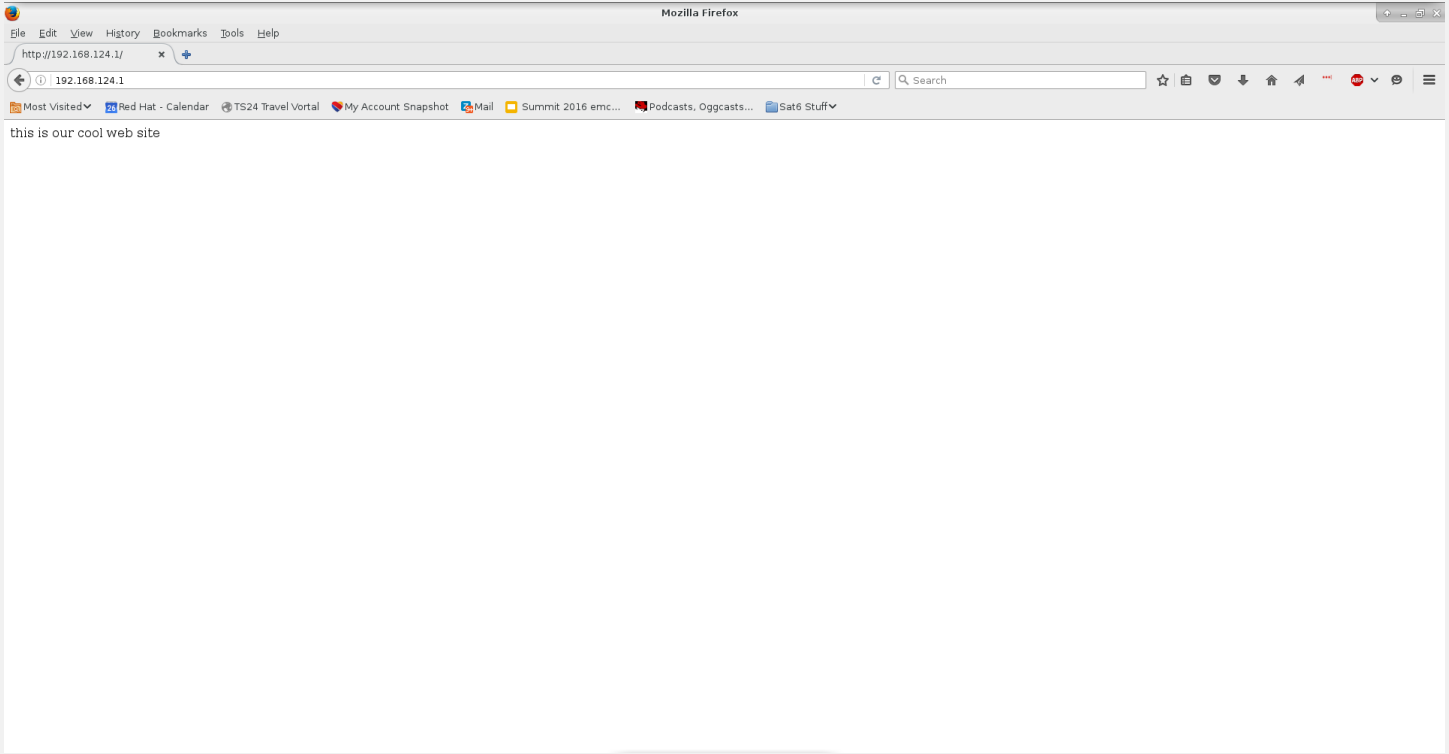
- I'm lazy. If I just want to reference a known good context, the shortest form is:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# chcon --reference /var/www/html/ /var/www/html/index.html
[root@w541 ~]#

Real World Examples

- If you just want to restore a directory and all its files to the default context, the easiest to remember is restorecon:

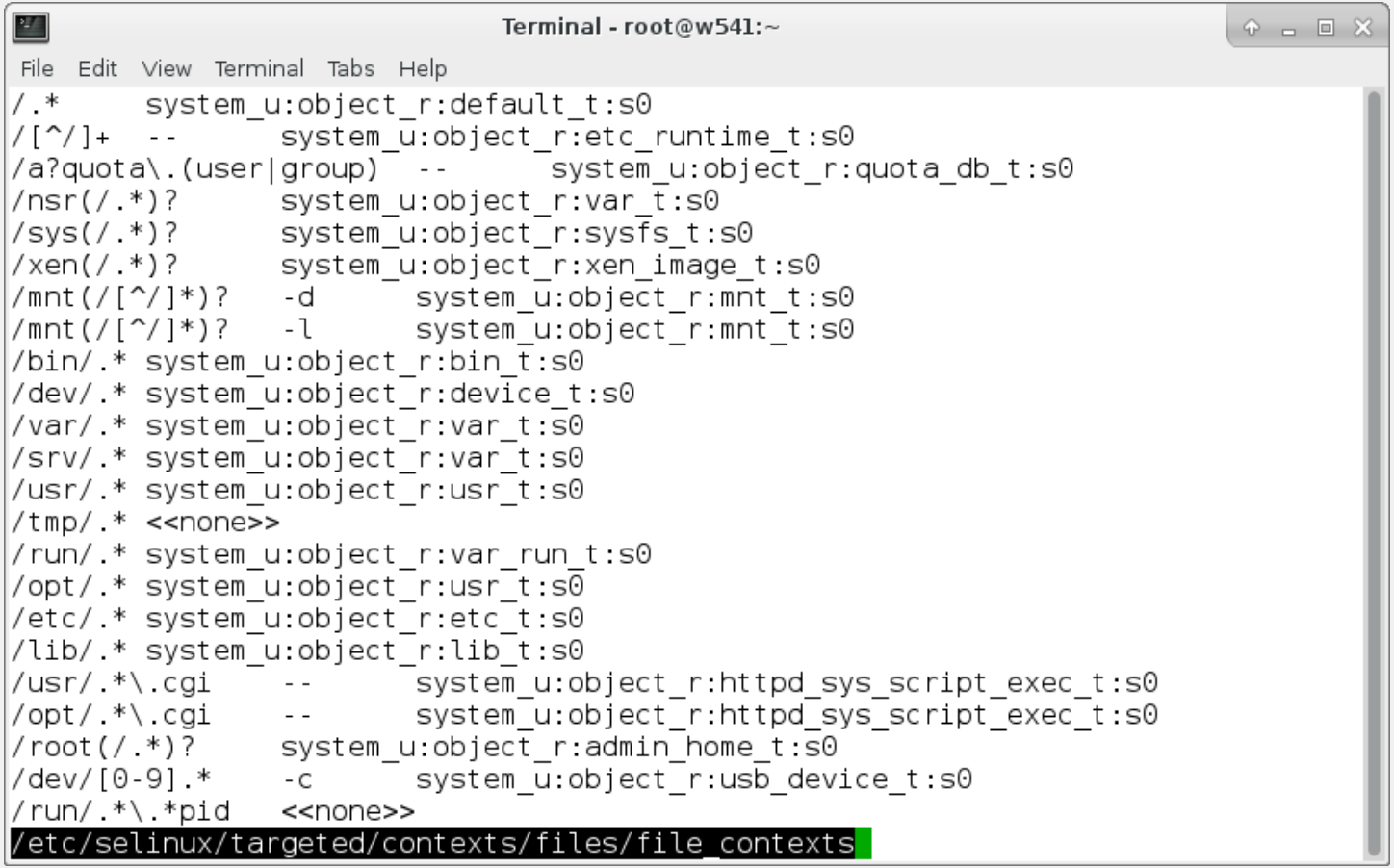

Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# restorecon -vR /var/www/html/
restorecon reset /var/www/html/index.html context unconfined_u:object_r:user_hom
e_t:s0->unconfined_u:object_r:httpd_sys_content_t:s0
[root@w541 ~]#

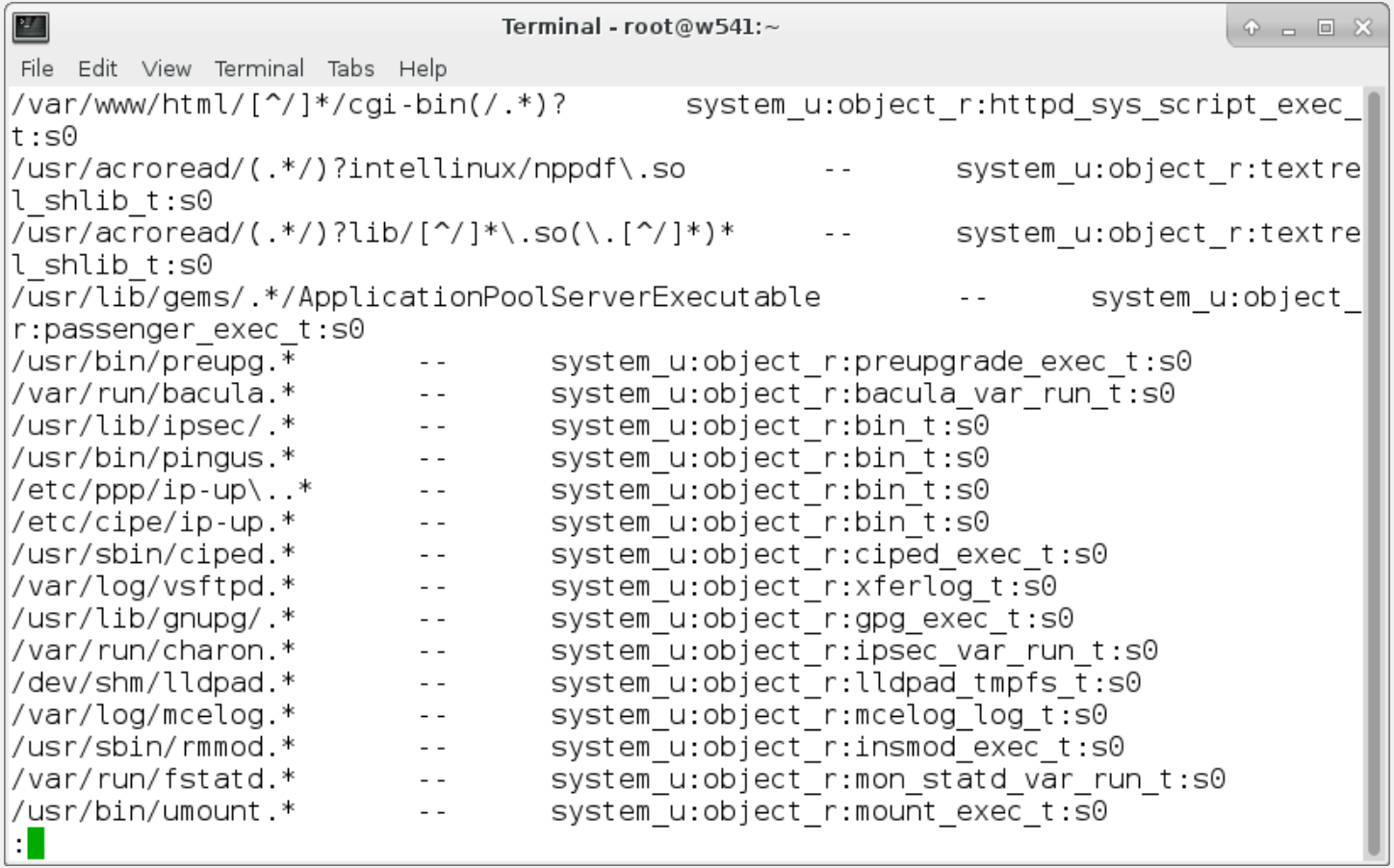

Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.124.1/
192.168.124.1
Search
Most Visited
Red Hat - Calendar
TS24 Travel Vortal
My Account Snapshot
Mail
Summit 2016 emc...
Podcasts, Oggcasts...
Sat6 Stuff
this is our cool web site

CONTEXT INFORMATION

Where Are These Contexts Stored?

- restorecon uses information from /etc/selinux/targeted/contexts/files/file_contexts (and other files in that directory) to determine what a file or directory's context should be.
- There are over 4000 entries in this file. Don't modify this file directly, your changes will be lost!


Terminal - root@w541:~
File Edit View Terminal Tabs Help
/.* system_u:object_r:default_t:s0
/[^/]+ -- system_u:object_r:etc_runtime_t:s0
/a?quota\.(user|group) -- system_u:object_r:quota_db_t:s0
/nsr(/.*)? system_u:object_r:var_t:s0
/sys(/.*)? system_u:object_r:sysfs_t:s0
/xen(/.*)? system_u:object_r:xen_image_t:s0
/mnt(/[^/]*)? -d system_u:object_r:mnt_t:s0
/mnt(/[^/]*)? -l system_u:object_r:mnt_t:s0
/bin/.* system_u:object_r:bin_t:s0
/dev/.* system_u:object_r:device_t:s0
/var/.* system_u:object_r:var_t:s0
/srv/.* system_u:object_r:var_t:s0
/usr/.* system_u:object_r:usr_t:s0
/tmp/.* <<none>>
/run/.* system_u:object_r:var_run_t:s0
/opt/.* system_u:object_r:usr_t:s0
/etc/.* system_u:object_r:etc_t:s0
/lib/.* system_u:object_r:lib_t:s0
/usr/.*\.cgi -- system_u:object_r:httpd_sys_script_exec_t:s0
/opt/.*\.cgi -- system_u:object_r:httpd_sys_script_exec_t:s0
/root(/.*)? system_u:object_r:admin_home_t:s0
/dev/[0-9].* -c system_u:object_r:usb_device_t:s0
/run/.*\.*pid <<none>>
/etc/selinux/targeted/contexts/files/file_contexts


Terminal - root@w541:~
File Edit View Terminal Tabs Help
/var/www/html/[^/]*/cgi-bin(/.*)? system_u:object_r:httpd_sys_script_exec_t:s0
/usr/acroread/(.*/)?intellinux/nppdf\.so -- system_u:object_r:textrel_shlib_t:s0
/usr/acroread/(.*/)?lib/[^/]*\.so(\.[^/]*)* -- system_u:object_r:textrel_shlib_t:s0
/usr/lib/gems/.*/ApplicationPoolServerExecutable -- system_u:object_r:passenger_exec_t:s0
/usr/bin/preupg.* -- system_u:object_r:preupgrade_exec_t:s0
/var/run/bacula.* -- system_u:object_r:bacula_var_run_t:s0
/usr/lib/ipsec/.* -- system_u:object_r:bin_t:s0
/usr/bin/pingus.* -- system_u:object_r:bin_t:s0
/etc/ppp/ip-up\..* -- system_u:object_r:bin_t:s0
/etc/cipe/ip-up.* -- system_u:object_r:bin_t:s0
/usr/sbin/ciped.* -- system_u:object_r:ciped_exec_t:s0
/var/log/vsftpd.* -- system_u:object_r:xferlog_t:s0
/usr/lib/gnupg/.* -- system_u:object_r:gpg_exec_t:s0
/var/run/charon.* -- system_u:object_r:ipsec_var_run_t:s0
/dev/shm/lldpad.* -- system_u:object_r:lldpad_tmpfs_t:s0
/var/log/mcelog.* -- system_u:object_r:mcelog_log_t:s0
/usr/sbin/rmmod.* -- system_u:object_r:insmod_exec_t:s0
/var/run/fstatd.* -- system_u:object_r:mon_statd_var_run_t:s0
/usr/bin/umount.* -- system_u:object_r:mount_exec_t:s0
:

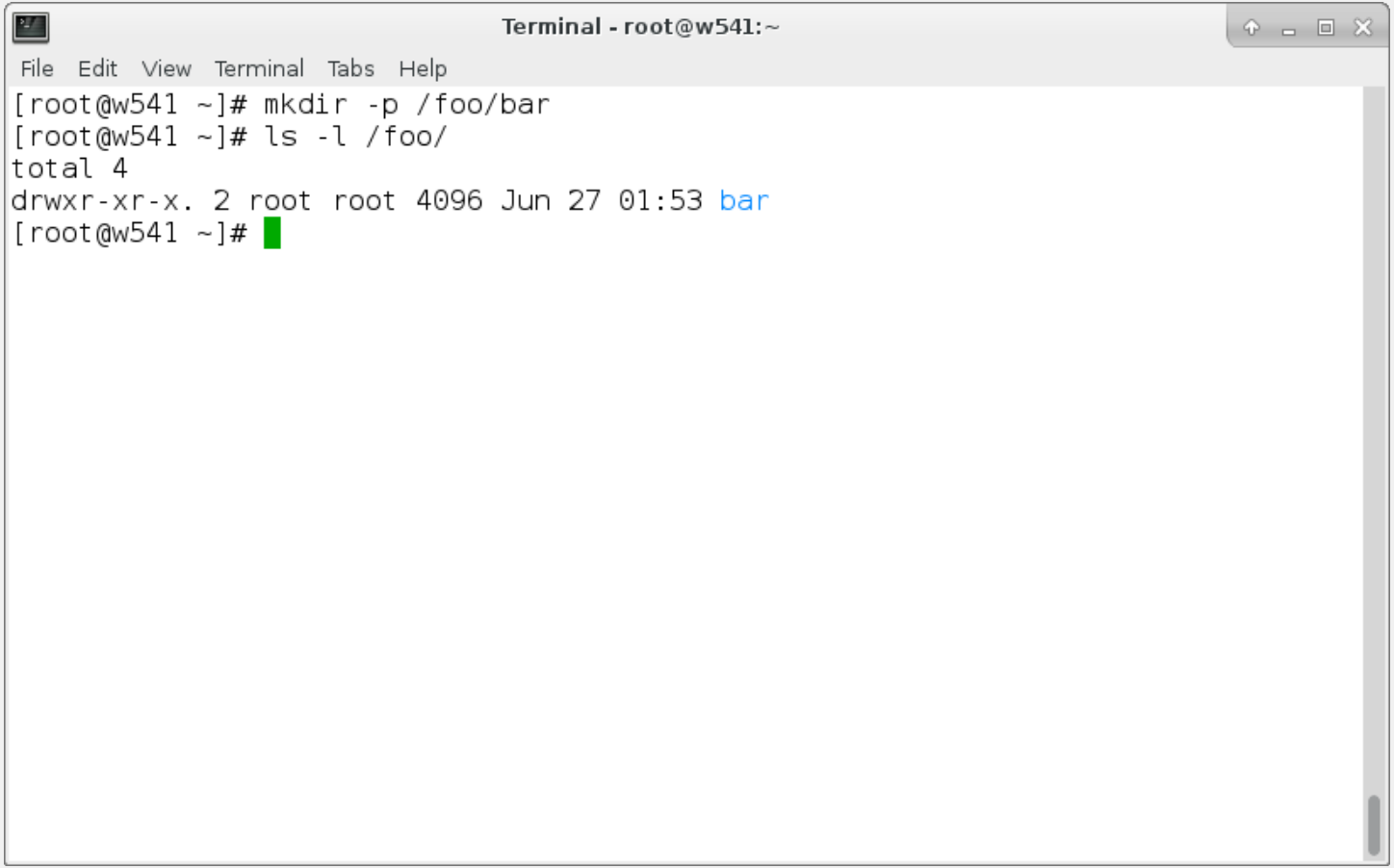
REAL WORLD EXAMPLES

Real World Examples

- Someone tells you to create a web directory somewhere non-standard - /foo/bar - for a virtual web site.

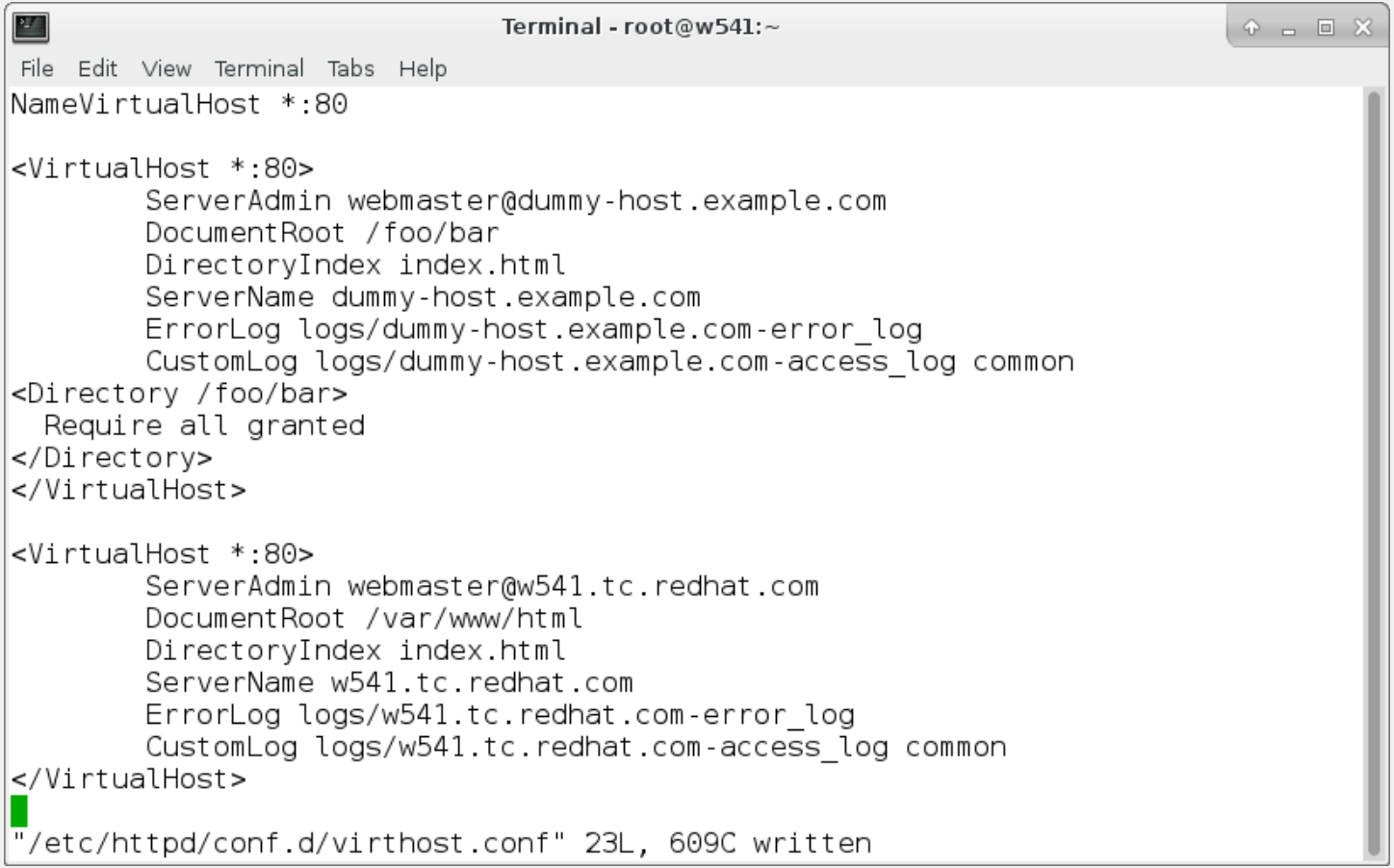
Real World Examples

- You create the directory:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# mkdir -p /foo/bar
[root@w541 ~]# ls -l /foo/
total 4
drwxr-xr-x. 2 root root 4096 Jun 27 01:53 bar
[root@w541 ~]#

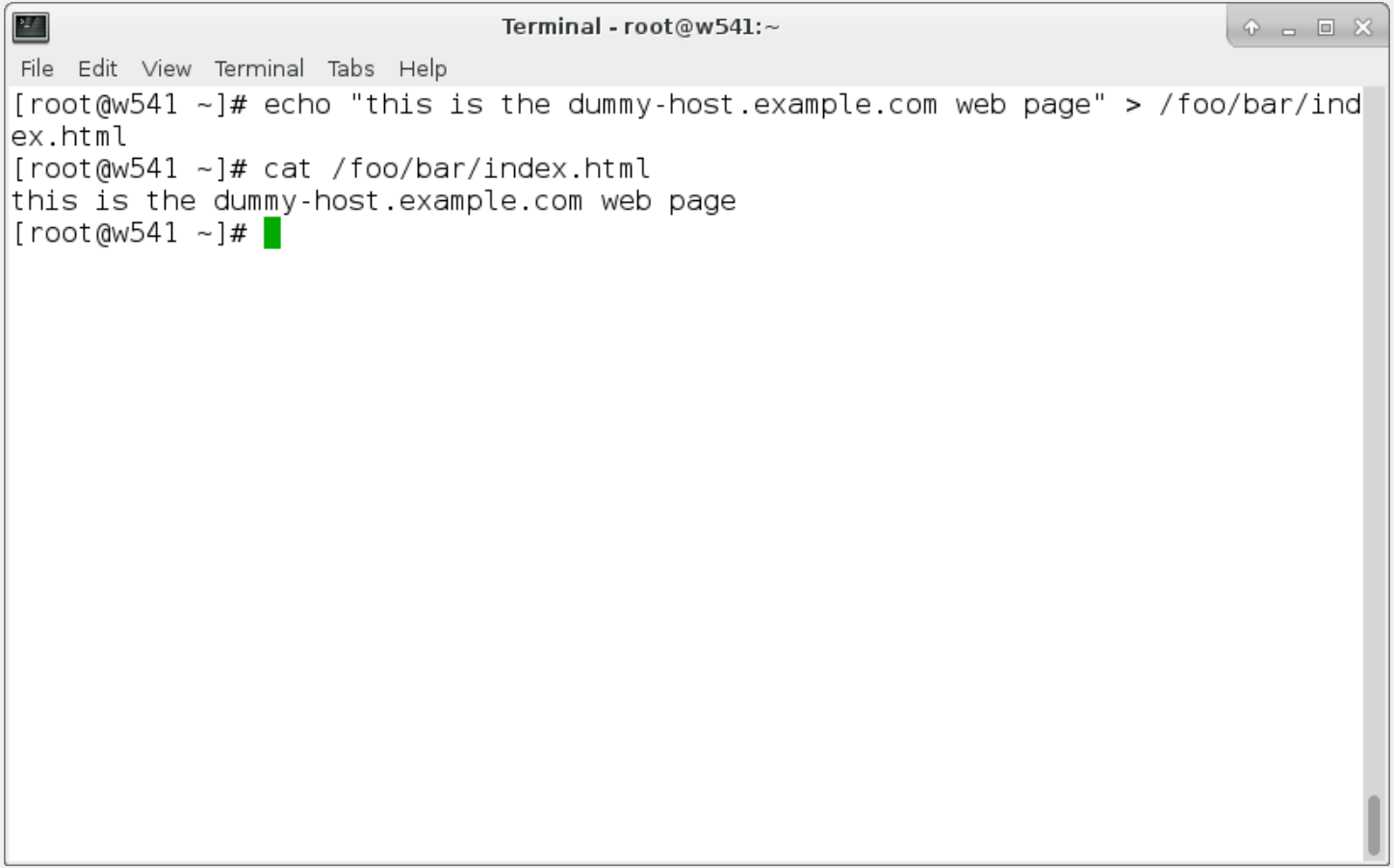
Real World Examples

- You define the virtual web site in httpd.conf:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
NameVirtualHost *:80
<VirtualHost *:80>
ServerAdmin webmaster@dummy-host.example.com
DocumentRoot /foo/bar
DirectoryIndex index.html
ServerName dummy-host.example.com
ErrorLog logs/dummy-host.example.com-error_log
CustomLog logs/dummy-host.example.com-access_log common
<Directory /foo/bar>
Require all granted
</Directory>
</VirtualHost>
<VirtualHost *:80>
ServerAdmin webmaster@w541.tc.redhat.com
DocumentRoot /var/www/html
DirectoryIndex index.html
ServerName w541.tc.redhat.com
ErrorLog logs/w541.tc.redhat.com-error_log
CustomLog logs/w541.tc.redhat.com-access_log common
</VirtualHost>
"/etc/httpd/conf.d/virthost.conf" 23L, 609C written

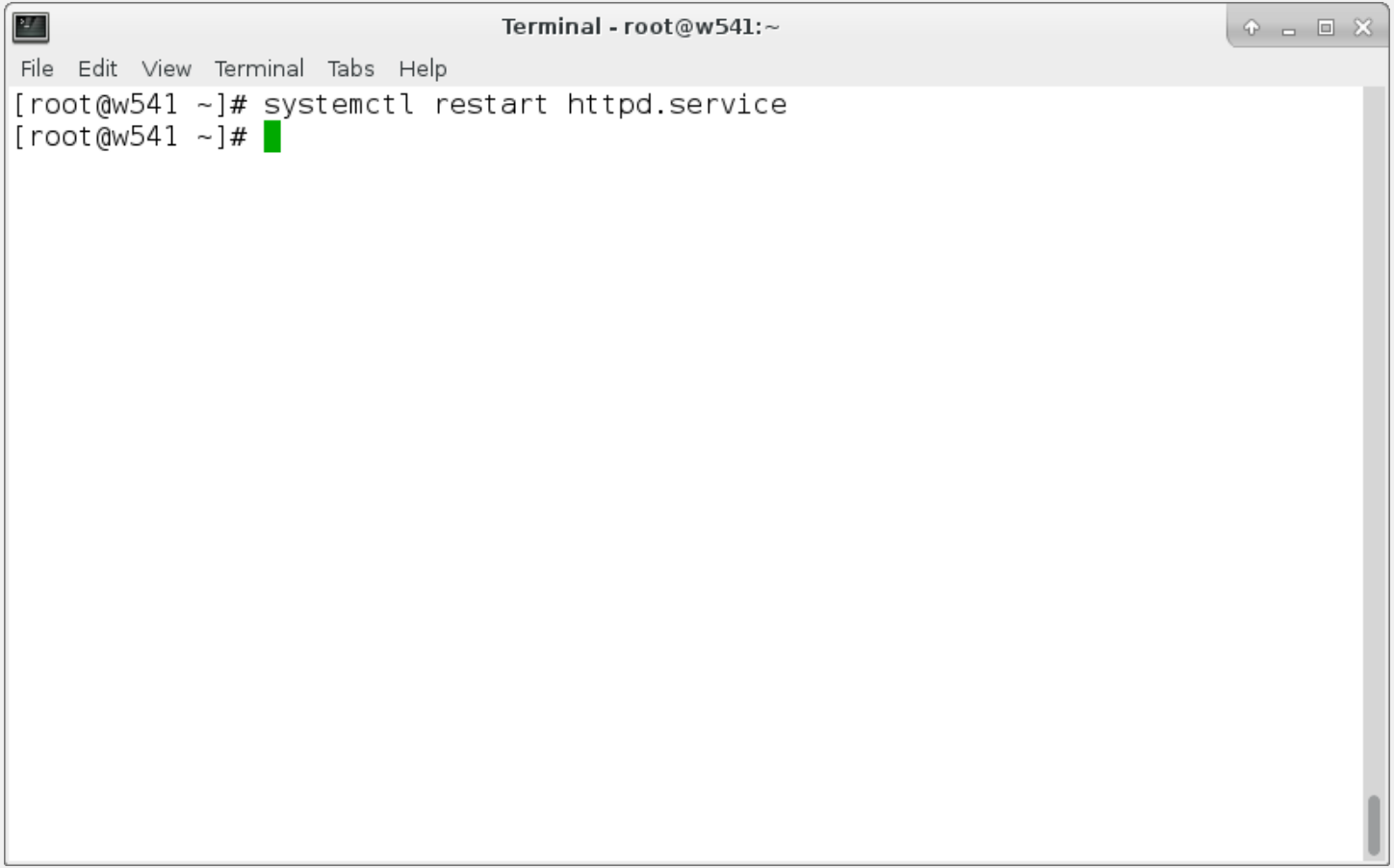
Real World Examples

- You create an index.html file:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# echo "this is the dummy-host.example.com web page" > /foo/bar/ind
ex.html
[root@w541 ~]# cat /foo/bar/index.html
this is the dummy-host.example.com web page
[root@w541 ~]#

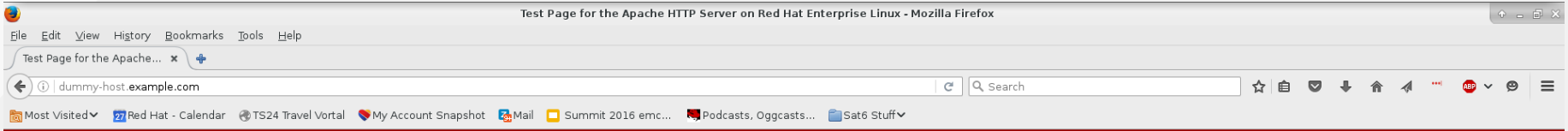
Real World Examples

- Restart the web server:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# systemctl restart httpd.service
[root@w541 ~]#

Real World Examples

- When you test the page...



Red Hat Enterprise Linux **Test Page**

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

For information on Red Hat Enterprise Linux, please visit the Red Hat, Inc. website. The documentation for Red Hat Enterprise Linux is available on the Red Hat, Inc. website.

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the image below on web sites powered by the Apache HTTP Server:

Real World Examples

- What logfile should we check?

Real World Examples

- journalctl

Terminal - root@w541:~

File Edit View Terminal Tabs Help

```
Jun 27 02:47:26 w541.tc.redhat.com audit[4515]: AVC avc:  denied  { getattr } for  pid=4515 comm="/usr/sbin/httpd" path="/foo/bar/index.html" dev="dm-0" ino=25559043 scontext=system_u:system
_r:httpd_t:s0 tcontext=unconfined_u:object_r:default_t:s0 tclass=file permissive=0
Jun 27 02:47:26 w541.tc.redhat.com audit[4515]: AVC avc:  denied  { getattr } for  pid=4515 comm="/usr/sbin/httpd" path="/foo/bar/index.html" dev="dm-0" ino=25559043 scontext=system_u:system
_r:httpd_t:s0 tcontext=unconfined_u:object_r:default_t:s0 tclass=file permissive=0
Jun 27 02:47:29 w541.tc.redhat.com dbus[1071]: [system] Activating service name='org.fedoraproject.Setroubleshootd' (using servicehelper)
Jun 27 02:47:29 w541.tc.redhat.com dbus[1071]: [system] Successfully activated service 'org.fedoraproject.Setroubleshootd'
Jun 27 02:47:29 w541.tc.redhat.com setroubleshoot[4666]: failed to retrieve rpm info for /foo/bar/index.html
Jun 27 02:47:30 w541.tc.redhat.com setroubleshoot[4666]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /foo/bar/index.html. For complete SELinux messages. run sealert
 -l 187c64e6-2bd0-4aa3-9862-249273ab90a7
Jun 27 02:47:30 w541.tc.redhat.com python3[4666]: SELinux is preventing /usr/sbin/httpd from getattr access on the file /foo/bar/index.html.

                                                  *****  Plugin catchall_labels (83.8 confidence) suggests   ******************

                                                  If you want to allow httpd to have getattr access on the index.html file
                                                  Then you need to change the label on /foo/bar/index.html
                                                  Do
                                                  # semanage fcontext -a -t FILE_TYPE '/foo/bar/index.html'
                                                  where FILE_TYPE is one of the following: NetworkManager_exec_t, NetworkManager_log_t, NetworkManager_tmp_t, abrt_dump_oops_exec_t, abrt_etc_
t, abrt_exec_t, abrt_handle_event_exec_t, abrt_helper_exec_t, abrt_retrace_coredump_exec_t, abrt_retrace_spool_t, abrt_retrace_worker_exec_t, abrt_tmp_t, abrt_upload_watch_tmp_t, abrt_var_ca
che_t, abrt_var_log_t, abrt_var_run_t, accountsd_exec_t, acct_data_t, acct_exec_t, admin_crontab_tmp_t, admin_passwd_exec_t, afs_logfile_t, aide_exec_t, aide_log_t, alsa_exec_t, alsa_tmp_t,
amanda_exec_t, amanda_log_t, amanda_recover_exec_t, amanda_tmp_t, amtu_exec_t, anacron_exec_t, anon_inodefs_t, antivirus_exec_t, antivirus_log_t, antivirus_tmp_t, apcupsd_cgi_content_t, apcu
psd_cgi_htaccess_t, apcupsd_cgi_ra_content_t, apcupsd_cgi_rw_content_t, apcupsd_cgi_script_exec_t, apcupsd_log_t, apcupsd_tmp_t, apm_exec_t, apmd_log_t, apmd_tmp_t, arpwatch_tmp_t, asterisk_
log_t, asterisk_tmp_t, audisp_exec_t, auditadm_sudo_tmp_t, auditctl_exec_t, auth_cache_t, authconfig_exec_t, automount_tmp_t, avahi_exec_t, awstats_content_t, awstats_htaccess_t, awstats_ra_
content_t, awstats_rw_content_t, awstats_script_exec_t, awstats_tmp_t, bacula_admin_exec_t, bacula_log_t, bacula_tmp_t, bacula_unconfined_script_exec_t, bin_t, bitlbee_log_t, bitlbee_tmp_t,
blueman_exec_t, blueman_tmp_t, bluetooth_helper_exec_t, bluetooth_helper_tmp_t, bluetooth_helper_tmpfs_t, bluetooth_tmp_t, boinc_log_t, boinc_project_tmp_t, boinc_tmp_t, boot_t, bootloader_e
xec_t, bootloader_tmp_t, brctl_exec_t, bugzilla_content_t, bugzilla_htaccess_t, bugzilla_ra_content_t, bugzilla_rw_content_t, bugzilla_script_exec_t, bugzilla_tmp_t, calamaris_exec_t, calama
ris_log_t, calamaris_www_t, callweaver_log_t, canna_log_t, cardctl_exec_t, cardmgr_dev_t, ccs_tmp_t, ccs_var_lib_t, ccs_var_log_t, cdcc_exec_t, cdcc_tmp_t, cdrecord_exec_t, cert_t, certmaste
r_var_log_t, certmonger_unconfined_exec_t, certwatch_exec_t, cfengine_log_t, cgred_log_t, cgroup_t, checkpc_exec_t, checkpc_log_t, checkpolicy_exec_t, chfn_exec_t, chkpwd_exec_t, chrome_sand
box_exec_t, chrome_sandbox_nacl_exec_t, chrome_sandbox_tmp_t, chronyd_var_log_t, cinder_api_tmp_t, cinder_backup_tmp_t, cinder_log_t, cinder_scheduler_tmp_t, cinder_volume_tmp_t, cloud_init_
tmp_t, cloud_log_t, cluster_conf_t, cluster_tmp_t, cluster_var_lib_t, cluster_var_log_t, cluster_var_run_t, cobbler_etc_t, cobbler_tmp_t, cobbler_var_lib_t, cobbler_var_log_t, cockpit_tmp_t,
 collectd_content_t, collectd_htaccess_t, collectd_ra_content_t, collectd_rw_content_t, collectd_script_exec_t, collectd_script_tmp_t, colord_exec_t, colord_tmp_t, comsat_tmp_t, condor_log_t
, condor_master_tmp_t, condor_schedd_tmp_t, condor_startd_tmp_t, conman_log_t, conman_tmp_t, consolehelper_exec_t, consolekit_exec_t, consolekit_log_t, couchdb_log_t, couchdb_tmp_t, courier_
exec_t, cpu_online_t, cpucontrol_exec_t, cpufreqselector_exec_t, cpuspeed_exec_t, crack_exec_t, crack_tmp_t, cron_log_t, crond_tmp_t, crontab_exec_t, crontab_tmp_t, ctdbd_log_t, ctdbd_tmp_t,
 cups_pdf_tmp_t, cupsd_config_exec_t, cupsd_log_t, cupsd_lpd_tmp_t, cupsd_tmp_t, cvs_content_t, cvs_data_t, cvs_exec_t, cvs_htaccess_t, cvs_ra_content_t, cvs_rw_content_t, cvs_script_exec_t,
 cvs_tmp_t, cyphesis_exec_t, cyphesis_log_t, cyphesis_tmp_t, cyrus_tmp_t, dbadm_sudo_tmp_t, dbskkd_tmp_t, dbusd_etc_t, dbusd_exec_t, dcc_client_exec_t, dcc_client_tmp_t, dcc_dbclean_exec_t,
dcc_dbclean_tmp_t, dccd_tmp_t, dccifd_tmp_t, dccm_tmp_t, ddclient_log_t, ddclient_tmp_t, debuginfo_exec_t, deltacloudd_log_t, deltacloudd_tmp_t, denyhosts_var_log_t, depmod_exec_t, devicekit
_disk_exec_t, devicekit_exec_t, devicekit_power_exec_t, devicekit_tmp_t, devicekit_var_log_t, dhcpc_exec_t, dhcpc_tmp_t, dhcpd_tmp_t, dirsrv_config_t, dirsrv_share_t, dirsrv_snmp_var_log_t,
dirsrv_tmp_t, dirsrv_var_log_t, dirsrv_var_run_t, dirsrvadmin_config_t, dirsrvadmin_content_t, dirsrvadmin_htaccess_t, dirsrvadmin_ra_content_t, dirsrvadmin_rw_content_t, dirsrvadmin_script_
exec_t, dirsrvadmin_tmp_t, dirsrvadmin_unconfined_script_exec_t, disk_munin_plugin_exec_t, disk_munin_plugin_tmp_t, dkim_milter_tmp_t, dlm_controld_var_log_t, dmesg_exec_t, dmidecode_exec_t,
 dnsmasq_var_log_t, dnssec_trigger_tmp_t, docker_log_t, docker_tmp_t, dovecot_auth_tmp_t, dovecot_deliver_tmp_t, dovecot_tmp_t, dovecot_var_log_t, drbd_tmp_t, dspam_content_t, dspam_htaccess
_t, dspam_log_t, dspam_ra_content_t, dspam_rw_content_t, dspam_script_exec_t, etc_runtime_t, etc_t, evtchnd_var_log_t, exim_exec_t, exim_log_t, exim_tmp_t, fail2ban_client_exec_t, fail2ban_l
og_t, fail2ban_tmp_t, fail2ban_var_lib_t, faillog_t, fenced_tmp_t, fenced_var_log_t, fetchmail_exec_t, fetchmail_log_t, file_context_t, fingerd_log_t, firewalld_exec_t, firewalld_tmp_t, fire
walld_var_log_t, firewallgui_exec_t, firewallgui_tmp_t, firstboot_exec_t, foghorn_var_log_t, fonts_cache_t, fonts_t, fprintd_exec_t, freqset_exec_t, fsadm_exec_t, fsadm_log_t, fsadm_tmp_t, f
sdaemon_tmp_t, ftpd_tmp_t, ftpdctl_exec_t, ftpdctl_tmp_t, games_exec_t, games_tmp_t, games_tmpfs_t, gconf_tmp_t, gconfd_exec_t, gconfdefaultsm_exec_t, gear_log_t, geoclue_exec_t, geoclue_tmp
_t, getty_exec_t, getty_log_t, getty_tmp_t, gfs_controld_var_log_t, git_content_t, git_htaccess_t, git_ra_content_t, git_rw_content_t, git_script_exec_t, git_script_tmp_t, git_sys_content_t,
 gitd_exec_t, gitosis_exec_t, gitosis_var_lib_t, gkeyringd_exec_t, gkeyringd_tmp_t, glance_log_t, glance_registry_tmp_t, glance_tmp_t, glusterd_log_t, glusterd_tmp_t, gnomesystemmm_exec_t, g
pg_agent_exec_t, gpg_agent_tmp_t, gpg_exec_t, gpg_helper_exec_t, gpg_pinentry_tmp_t, gpg_pinentry_tmpfs_t, gpm_tmp_t, gpsd_exec_t, groupadd_exec_t, groupd_var_log_t, gssd_tmp_t, haproxy_var_
log_t, hostname_etc_t, hostname_exec_t, hsqldb_tmp_t, httpd_cache_t, httpd_config_t, httpd_exec_t, httpd_helper_exec_t, httpd_keytab_t, httpd_lock_t, httpd_log_t, httpd_modules_t, httpd_pass
wd_exec_t, httpd_php_exec_t, httpd_php_tmp_t, httpd_rotatelogs_exec_t, httpd_squirrelmail_t, httpd_suexec_exec_t, httpd_suexec_tmp_t, httpd_sys_content_t, httpd_sys_htaccess_t, httpd_sys_ra_
```

Real World Examples

- Note that at the end it tells you to restorecon!

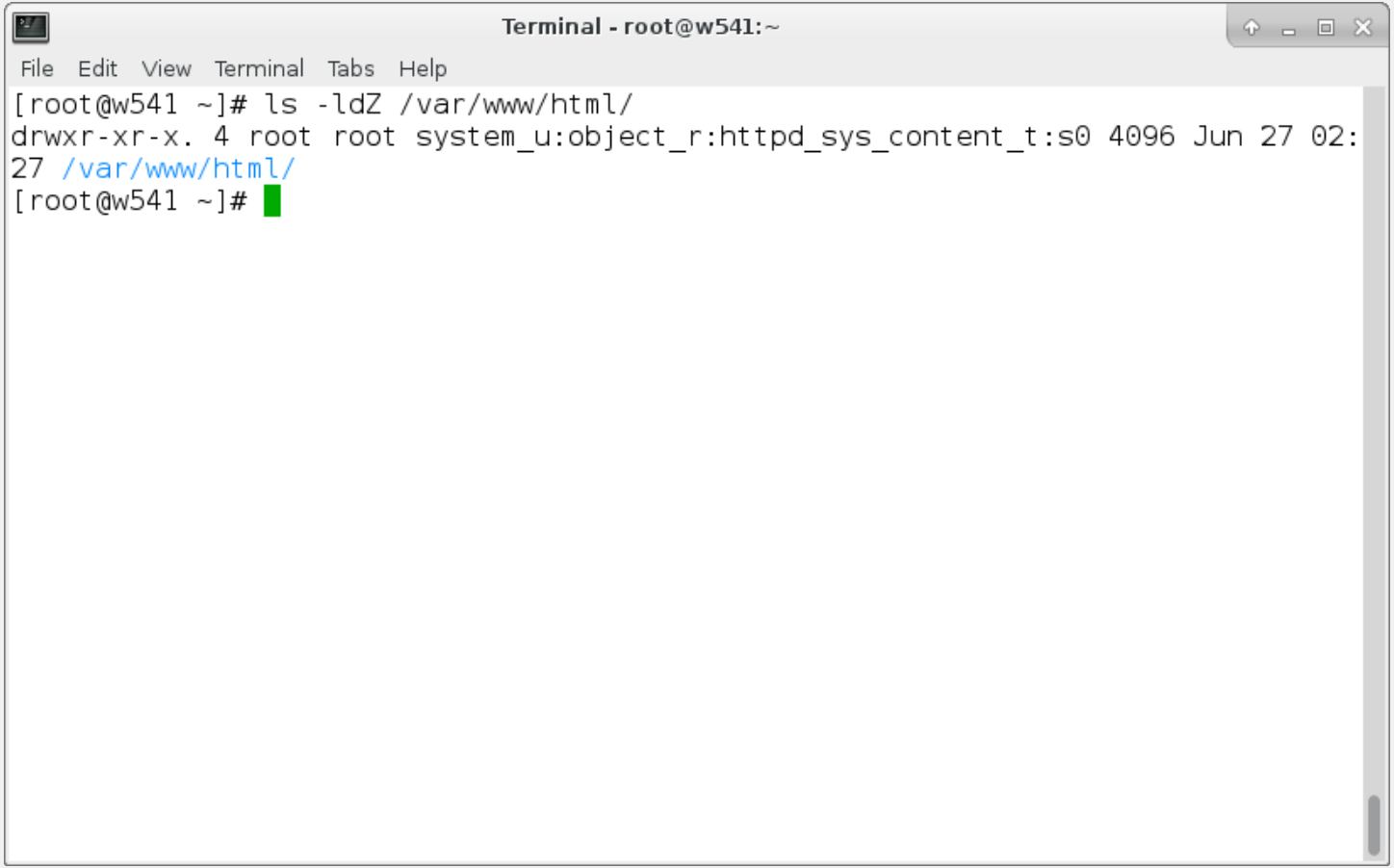
Terminal - root@w541:~

File Edit View Terminal Tabs Help

```
nagios_services_plugin_exec_t, nagios_system_plugin_exec_t, nagios_system_plugin_tmp_t, nagios_tmp_t, nagios_unconfined_plugin_exec_t, nagios_var_lib_t, named_checkconf_exec_t, named_exec_t,
 named_log_t, named_tmp_t, namespace_init_exec_t, ncftool_exec_t, ndc_exec_t, net_conf_t, netlabel_mgmt_exec_t, netutils_exec_t, netutils_tmp_t, neutron_log_t, neutron_tmp_t, newrole_exec_t,
 nova_log_t, nova_tmp_t, nscd_log_t, nsd_log_t, nsd_tmp_t, ntop_tmp_t, ntpd_log_t, ntpd_tmp_t, ntpdate_exec_t, numad_var_log_t, nut_upsd_tmp_t, nut_upsdrvctl_tmp_t, nut_upsmon_tmp_t, nutups_
cgi_content_t, nutups_cgi_htaccess_t, nutups_cgi_ra_content_t, nutups_cgi_rw_content_t, nutups_cgi_script_exec_t, nx_server_tmp_t, obex_exec_t, oddjob_mkhomedir_exec_t, openshift_cgroup_read
_exec_t, openshift_cgroup_read_tmp_t, openshift_content_t, openshift_cron_tmp_t, openshift_htaccess_t, openshift_initrc_tmp_t, openshift_log_t, openshift_net_read_exec_t, openshift_ra_conten
t_t, openshift_rw_content_t, openshift_script_exec_t, openshift_tmp_t, openshift_var_lib_t, opensm_log_t, openvpn_status_t, openvpn_tmp_t, openvpn_var_log_t, openvswitch_log_t, openvswitch_t
mp_t, openwsman_log_t, openwsman_tmp_t, osad_log_t, pads_exec_t, pam_console_exec_t, pam_timestamp_tmp_t, passenger_exec_t, passenger_log_t, passenger_tmp_t, passenger_var_lib_t, passenger_v
ar_run_t, passwd_exec_t, passwd_file_t, pcp_log_t, pcp_tmp_t, pcscd_var_run_t, pdns_control_exec_t, pegasus_openlmi_storage_tmp_t, pegasus_tmp_t, pinentry_exec_t, ping_exec_t, piranha_log_t,
 piranha_web_tmp_t, pkcs_slotd_tmp_t, pki_ra_etc_rw_t, pki_ra_log_t, pki_ra_var_lib_t, pki_ra_var_run_t, pki_tomcat_cert_t, pki_tomcat_log_t, pki_tomcat_tmp_t, pki_tps_etc_rw_t, pki_tps_log_
t, pki_tps_var_lib_t, pki_tps_var_run_t, plymouth_exec_t, plymouthd_var_log_t, podsleuth_exec_t, podsleuth_tmp_t, podsleuth_tmpfs_t, policykit_auth_exec_t, policykit_exec_t, policykit_grant_
exec_t, policykit_resolve_exec_t, policykit_tmp_t, polipo_exec_t, polipo_log_t, portmap_helper_exec_t, portmap_tmp_t, postfix_bounce_tmp_t, postfix_cleanup_tmp_t, postfix_exec_t, postfix_loc
al_tmp_t, postfix_map_exec_t, postfix_map_tmp_t, postfix_pickup_tmp_t, postfix_pipe_tmp_t, postfix_postdrop_exec_t, postfix_postdrop_t, postfix_postqueue_exec_t, postfix_qmgr_tmp_t, postfix_
showq_exec_t, postfix_smtp_tmp_t, postfix_smtpd_tmp_t, postfix_virtual_tmp_t, postgresql_log_t, postgresql_tmp_t, pppd_exec_t, pppd_log_t, pppd_tmp_t, pptp_log_t, prelink_exec_t, prelink_log
_t, prelink_tmp_t, prelude_lml_tmp_t, prelude_log_t, preupgrade_data_t, preupgrade_exec_t, prewikka_content_t, prewikka_htaccess_t, prewikka_ra_content_t, prewikka_rw_content_t, prewikka_scr
ipt_exec_t, privoxy_log_t, proc_t, procmail_exec_t, procmail_log_t, procmail_tmp_t, prosody_log_t, prosody_tmp_t, psad_tmp_t, psad_var_log_t, ptchown_exec_t, public_content_rw_t, public_cont
ent_t, pulseaudio_exec_t, pulseaudio_tmpfs_t, puppet_log_t, puppet_tmp_t, puppet_var_lib_t, puppetca_exec_t, puppetmaster_tmp_t, pwauth_exec_t, pyicqt_log_t, qdiskd_var_log_t, qemu_exec_t, q
mail_tcp_env_exec_t, qpidd_tmp_t, quota_exec_t, rabbitmq_var_log_t, racoon_tmp_t, radiusd_log_t, readahead_exec_t, realmd_exec_t, realmd_tmp_t, redis_log_t, rhev_agentd_log_t, rhev_agentd_tm
p_t, rhsmcertd_exec_t, rhsmcertd_log_t, rhsmcertd_tmp_t, ricci_modcluster_var_log_t, ricci_tmp_t, ricci_var_log_t, rkhunter_var_lib_t, rlogind_tmp_t, rolekit_tmp_t, rpcbind_tmp_t, rpm_exec_t
, rpm_log_t, rpm_script_tmp_t, rpm_tmp_t, rssh_chroot_helper_exec_t, rssh_exec_t, rsync_exec_t, rsync_log_t, rsync_tmp_t, rtas_errd_log_t, rtas_errd_tmp_t, rtkit_daemon_exec_t, run_init_exec
_t, samba_etc_t, samba_log_t, samba_net_exec_t, samba_net_tmp_t, samba_var_t, sambagui_exec_t, sanlock_log_t, sblim_tmp_t, screen_exec_t, secadm_sudo_tmp_t, sectool_tmp_t, sectool_var_log_t,
 sectoolm_exec_t, security_t, selinux_munin_plugin_exec_t, selinux_munin_plugin_tmp_t, semanage_exec_t, semanage_tmp_t, sendmail_exec_t, sendmail_log_t, sendmail_tmp_t, sensord_log_t, servic
es_munin_plugin_exec_t, services_munin_plugin_tmp_t, session_dbusd_tmp_t, setfiles_exec_t, setkey_exec_t, setroubleshoot_fixit_exec_t, setroubleshoot_fixit_tmp_t, setroubleshoot_tmp_t, setro
ubleshoot_var_log_t, setroubleshootd_exec_t, setsebool_exec_t, seunshare_exec_t, sge_job_exec_t, sge_shepherd_exec_t, sge_tmp_t, shell_exec_t, shorewall_log_t, shorewall_tmp_t, showmount_exe
c_t, slapd_cert_t, slapd_log_t, slapd_tmp_t, slpd_log_t, smbcontrol_exec_t, smbd_tmp_t, smokeping_cgi_content_t, smokeping_cgi_htaccess_t, smokeping_cgi_ra_content_t, smokeping_cgi_rw_conten
t_t, smokeping_cgi_script_exec_t, smokeping_var_lib_t, smokeping_var_run_t, smoltclient_exec_t, smoltclient_tmp_t, smsd_log_t, smsd_tmp_t, snapperd_exec_t, snapperd_log_t, snmpd_log_t, snort
_log_t, snort_tmp_t, sosreport_exec_t, sosreport_tmp_t, soundd_tmp_t, spamc_exec_t, spamc_tmp_t, spamd_log_t, spamd_tmp_t, spamd_update_exec_t, speech-dispatcher_exec_t, speech-dispatcher_lo
g_t, speech-dispatcher_tmp_t, squid_content_t, squid_cron_exec_t, squid_htaccess_t, squid_log_t, squid_ra_content_t, squid_rw_content_t, squid_script_exec_t, squid_tmp_t, squirrelmail_spool_
t, src_t, ssh_agent_exec_t, ssh_agent_tmp_t, ssh_exec_t, ssh_keygen_exec_t, ssh_keygen_tmp_t, ssh_keysign_exec_t, ssh_tmpfs_t, sssd_public_t, sssd_selinux_manager_exec_t, sssd_var_lib_t, sss
d_var_log_t, staff_sudo_tmp_t, stapserver_log_t, stapserver_tmp_t, stunnel_tmp_t, su_exec_t, sudo_exec_t, sulogin_exec_t, svc_multilog_exec_t, svc_run_exec_t, svc_start_exec_t, svirt_tmp_t,
 svnserve_tmp_t, swat_tmp_t, swift_tmp_t, sysadm_passwd_tmp_t, sysadm_sudo_tmp_t, sysfs_t, syslogd_tmp_t, sysstat_exec_t, sysstat_log_t, system_conf_t, system_cronjob_tmp_t, system_db_t, syst
em_dbusd_tmp_t, system_dbusd_var_lib_t, system_mail_tmp_t, system_munin_plugin_exec_t, system_munin_plugin_tmp_t, systemd_logind_var_run_t, systemd_passwd_agent_exec_t, systemd_passwd_var_ru
n_t, systemd_systemctl_exec_t, tcpd_tmp_t, telepathy_gabble_exec_t, telepathy_gabble_tmp_t, telepathy_idle_exec_t, telepathy_idle_tmp_t, telepathy_logger_exec_t, telepathy_logger_tmp_t, tele
pathy_mission_control_exec_t, telepathy_mission_control_tmp_t, telepathy_msn_exec_t, telepathy_msn_tmp_t, telepathy_salut_exec_t, telepathy_salut_tmp_t, telepathy_sofiasip_exec_t, telepathy_
sofiasip_tmp_t, telepathy_stream_engine_exec_t, telepathy_stream_engine_tmp_t, telepathy_sunshine_exec_t, telepathy_sunshine_tmp_t, telnetd_tmp_t, tetex_data_t, textrel_shlib_t, tgtd_tmp_t,
 thin_aeolus_configserver_log_t, thin_log_t, thumb_exec_t, thumb_tmp_t, tmp_t, tmpreaper_exec_t, tomcat_log_t, tomcat_tmp_t, tor_var_log_t, traceroute_exec_t, tuned_log_t, tuned_tmp_t, tvtime
_exec_t, tvtime_tmp_t, tvtime_tmpfs_t, udev_tmp_t, udev_var_run_t, ulogd_var_log_t, uml_exec_t, uml_tmp_t, uml_tmpfs_t, unconfined_exec_t, unconfined_munin_plugin_exec_t, unconfined_munin_pl
ugin_tmp_t, update_modules_exec_t, update_modules_tmp_t, updfstab_exec_t, usbmodules_exec_t, usbmuxd_exec_t, user_cron_spool_t, user_fonts_t, user_home_t, user_mail_tmp_t, user_tmp_t, userad
d_exec_t, userhelper_exec_t, usernetctl_exec_t, usr_t, utempter_exec_t, uucpd_log_t, uucpd_tmp_t, uux_exec_t, var_lib_t, var_log_t, var_spool_t, varnishd_tmp_t, varnishlog_log_t, vdagent_log
_t, virsh_exec_t, virt_log_t, virt_qemu_ga_log_t, virt_qemu_ga_tmp_t, virt_qemu_ga_unconfined_exec_t, virt_tmp_t, virtd_lxc_exec_t, vlock_exec_t, vmtools_helper_exec_t, vmtools_tmp_t, vmware
_exec_t, vmware_host_tmp_t, vmware_log_t, vmware_tmp_t, vmware_tmpfs_t, vnstat_exec_t, vpnc_exec_t, vpnc_tmp_t, w3c_validator_content_t, w3c_validator_htaccess_t, w3c_validator_ra_content_t,
 w3c_validator_rw_content_t, w3c_validator_script_exec_t, w3c_validator_tmp_t, watchdog_log_t, watchdog_unconfined_exec_t, webadm_tmp_t, webalizer_content_t, webalizer_exec_t, webalizer_htac
cess_t, webalizer_ra_content_t, webalizer_rw_content_t, webalizer_script_exec_t, webalizer_tmp_t, winbind_log_t, wine_exec_t, wireshark_exec_t, wireshark_tmp_t, wireshark_tmpfs_t, wpa_cli_ex
ec_t, wtmp_t, xauth_exec_t, xauth_tmp_t, xdm_exec_t, xdm_log_t, xdm_unconfined_exec_t, xend_tmp_t, xend_var_log_t, xenstored_tmp_t, xenstored_var_log_t, xferlog_t, xserver_exec_t, xserver_log
g_t, xserver_tmpfs_t, ypbind_tmp_t, ypserv_tmp_t, zabbix_log_t, zabbix_script_exec_t, zabbix_tmp_t, zarafa_deliver_log_t, zarafa_deliver_tmp_t, zarafa_gateway_log_t, zarafa_ical_log_t, zaraf
a_indexer_log_t, zarafa_indexer_tmp_t, zarafa_monitor_log_t, zarafa_server_log_t, zarafa_server_tmp_t, zarafa_spooler_log_t, zarafa_var_lib_t, zebra_log_t, zebra_tmp_t, zoneminder_content_t,
 zoneminder_exec_t, zoneminder_htaccess_t, zoneminder_log_t, zoneminder_ra_content_t, zoneminder_rw_content_t, zoneminder_script_exec_t, zoneminder_var_lib_t, zos_remote_exec_t.
                                        Then execute:
                                        restorecon -v '/foo/bar/index.html'
```

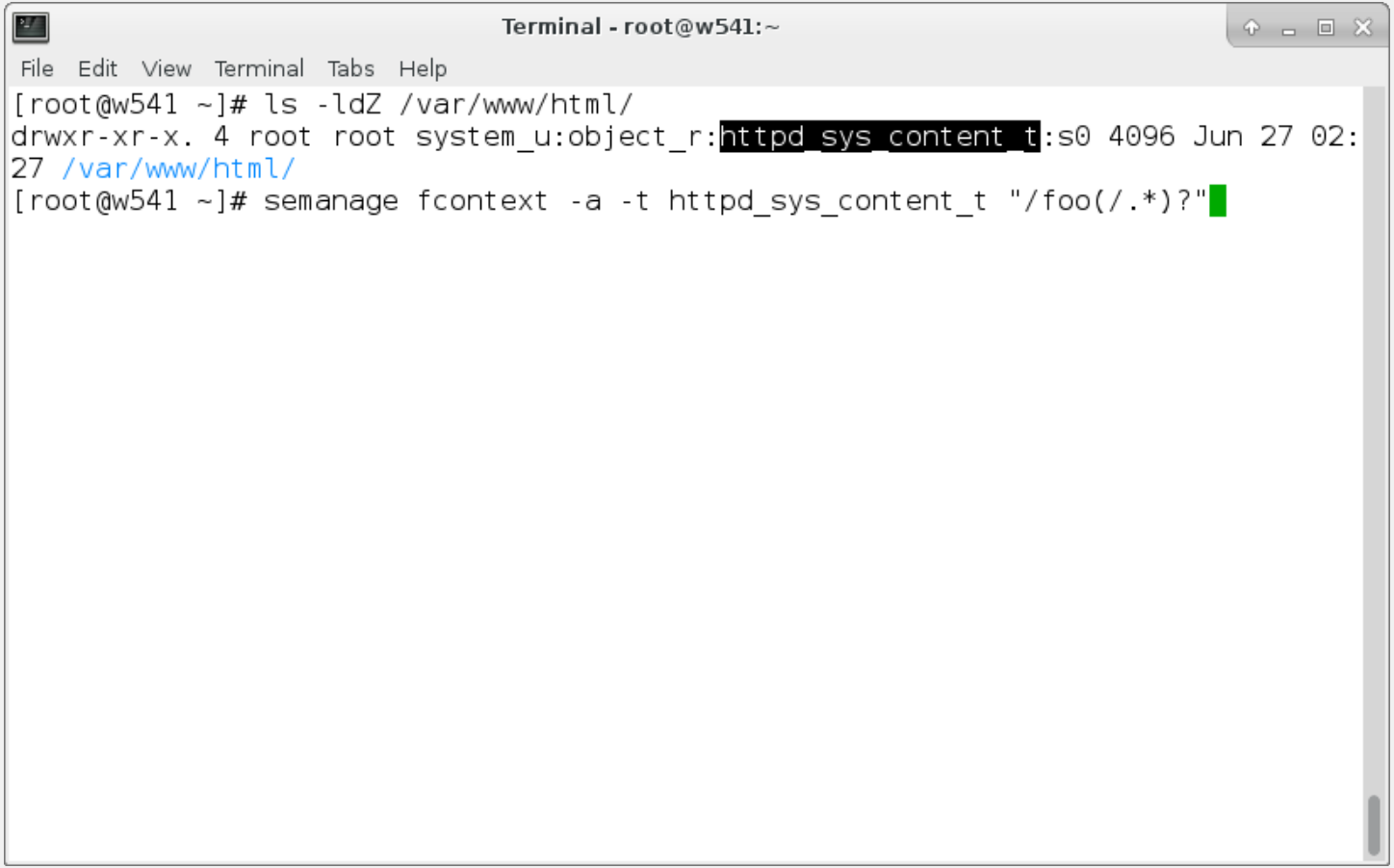
Real World Examples

- What directory should we look at to get the correct context label?


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# ls -ldZ /var/www/html/
drwxr-xr-x. 4 root root system_u:object_r:httpd_sys_content_t:s0 4096 Jun 27 02:
27 /var/www/html/
[root@w541 ~]#

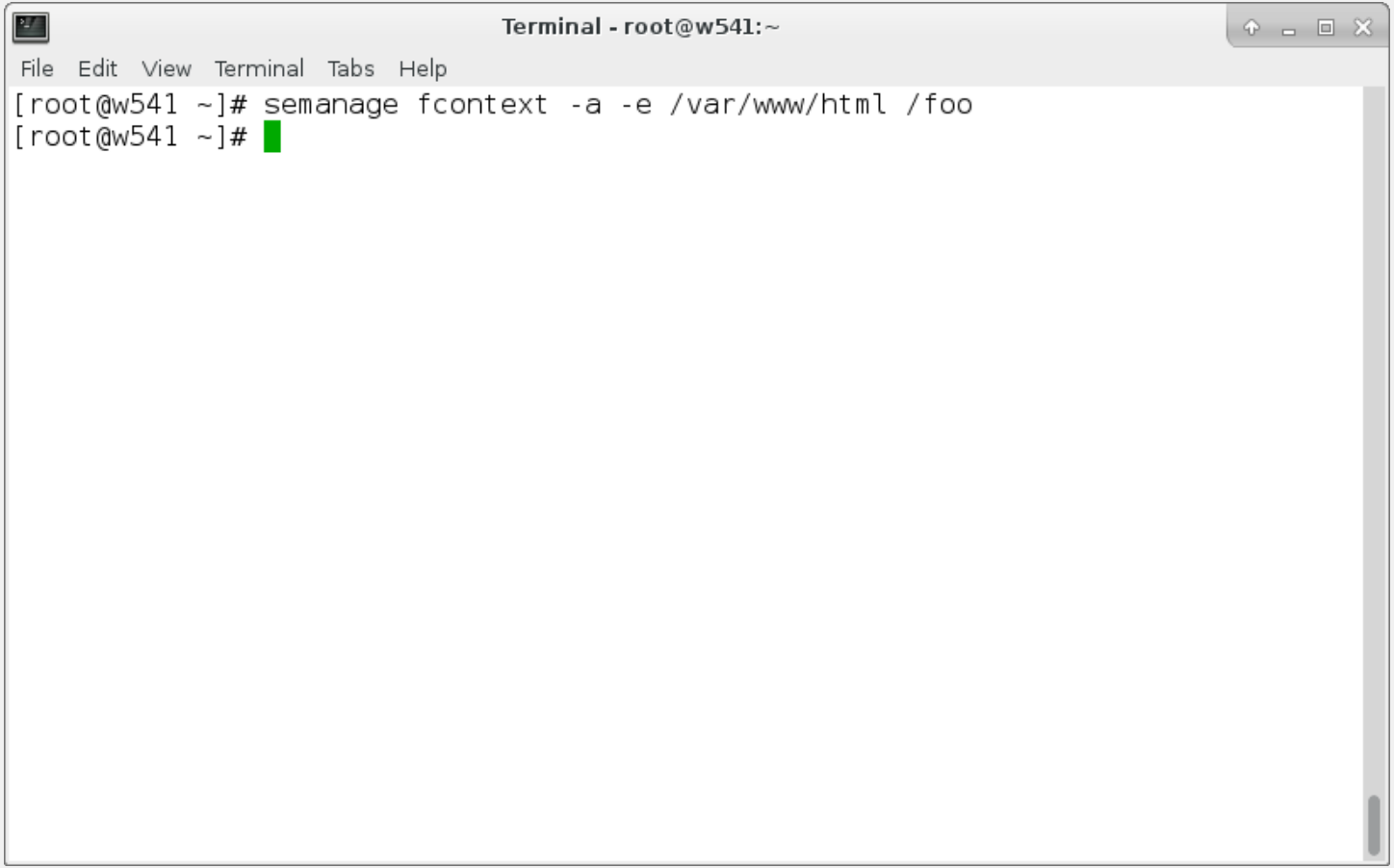
Real World Examples

- We actually want all of the files under /foo to have the right context, so we'll use a regular expression (you can get the syntax from /etc/selinux/targeted/contexts/files/file_contexts):


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# ls -ldZ /var/www/html/
drwxr-xr-x. 4 root root system_u:object_r:httpd_sys_content_t:s0 4096 Jun 27 02:
27 /var/www/html/
[root@w541 ~]# semanage fcontext -a -t httpd_sys_content_t "/foo(/.*)?"

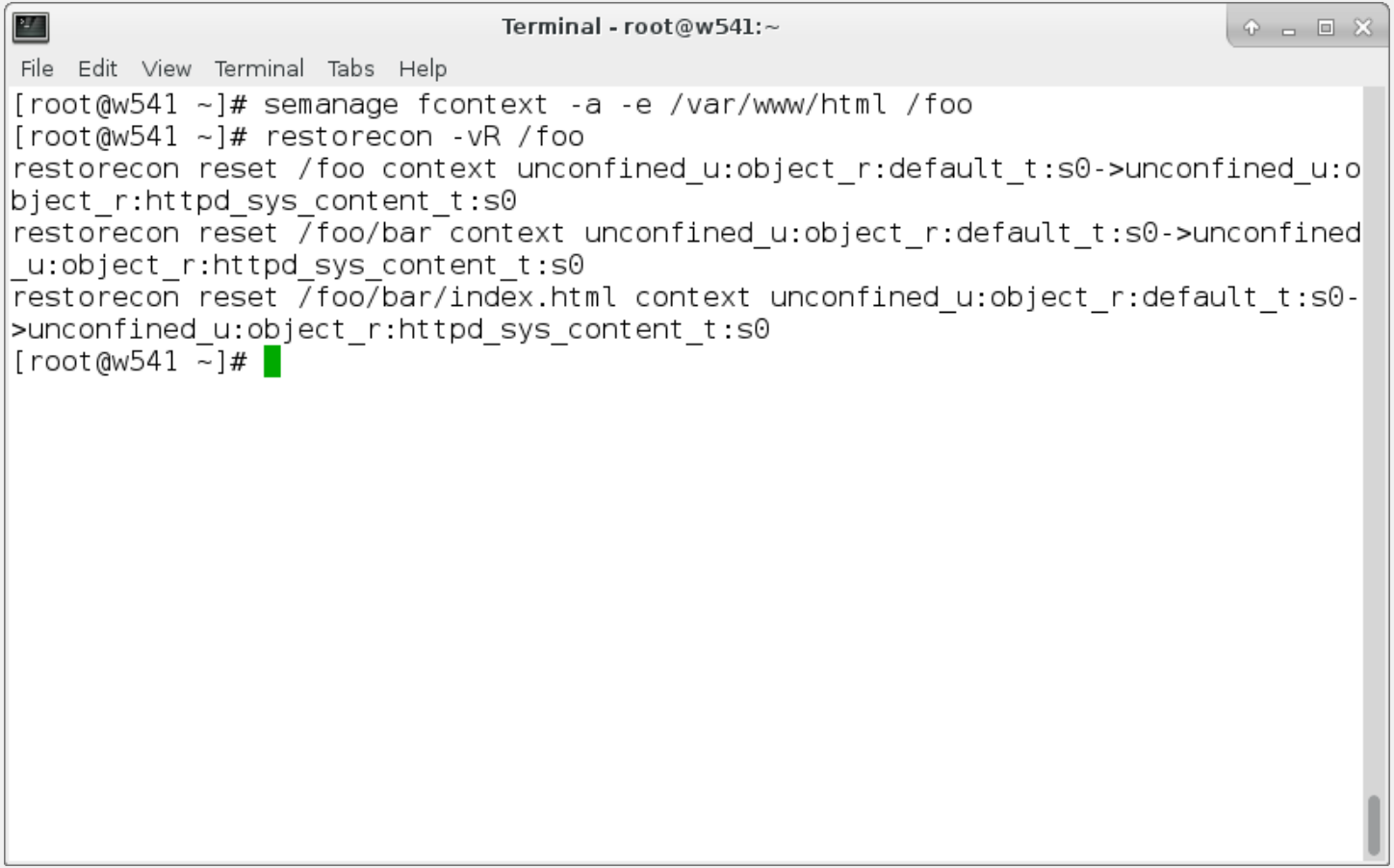
Real World Examples

- Or, if you're like me (lazy), you can use the -e (equals) argument to semanage fcontext:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# semanage fcontext -a -e /var/www/html /foo
[root@w541 ~]#

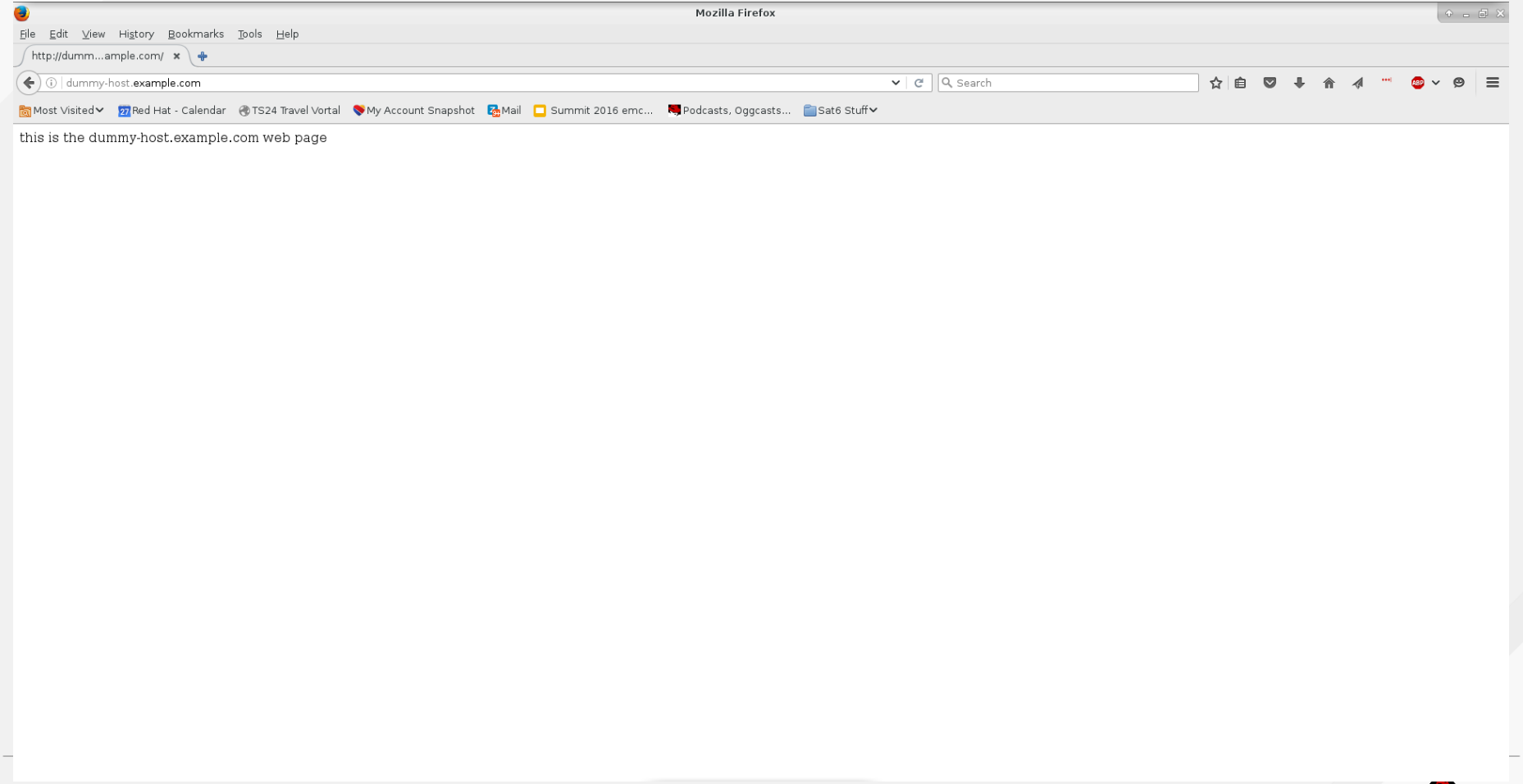
Real World Examples

- Now run restorecon against the directory:


Terminal - root@w541:~
File Edit View Terminal Tabs Help
[root@w541 ~]# semanage fcontext -a -e /var/www/html /foo
[root@w541 ~]# restorecon -vR /foo
restorecon reset /foo context unconfined_u:object_r:default_t:s0->unconfined_u:object_r:httpd_sys_content_t:s0
restorecon reset /foo/bar context unconfined_u:object_r:default_t:s0->unconfined_u:object_r:httpd_sys_content_t:s0
restorecon reset /foo/bar/index.html context unconfined_u:object_r:default_t:s0->unconfined_u:object_r:httpd_sys_content_t:s0
[root@w541 ~]#

Real World Examples

- Test the site:


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://dumm...ample.com/
dummy-host.example.com
Search
Most Visited
Red Hat - Calendar
TS24 Travel Vortal
My Account Snapshot
Mail
Summit 2016 emc...
Podcasts, Oggcasts...
Sat6 Stuff
this is the dummy-host.example.com web page

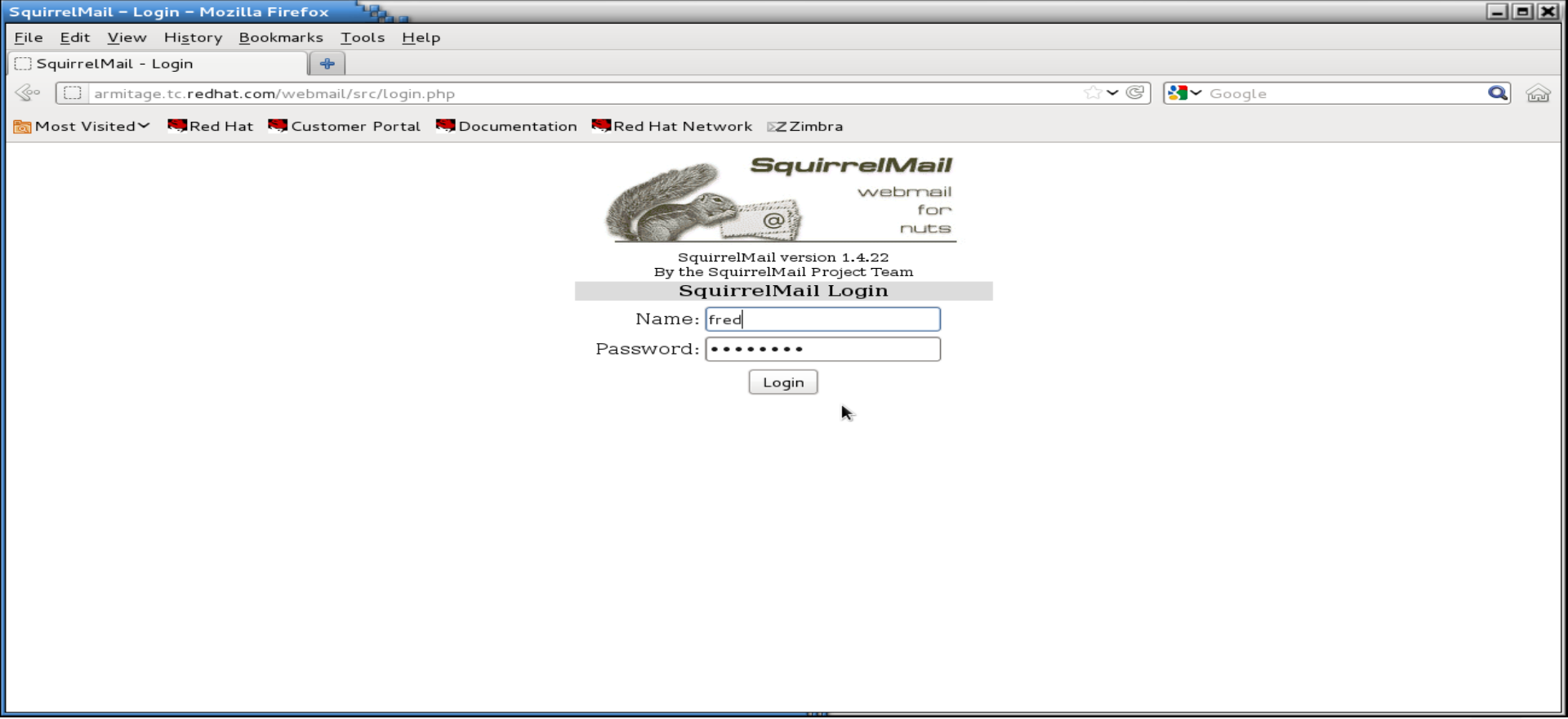
POLICY MODULES

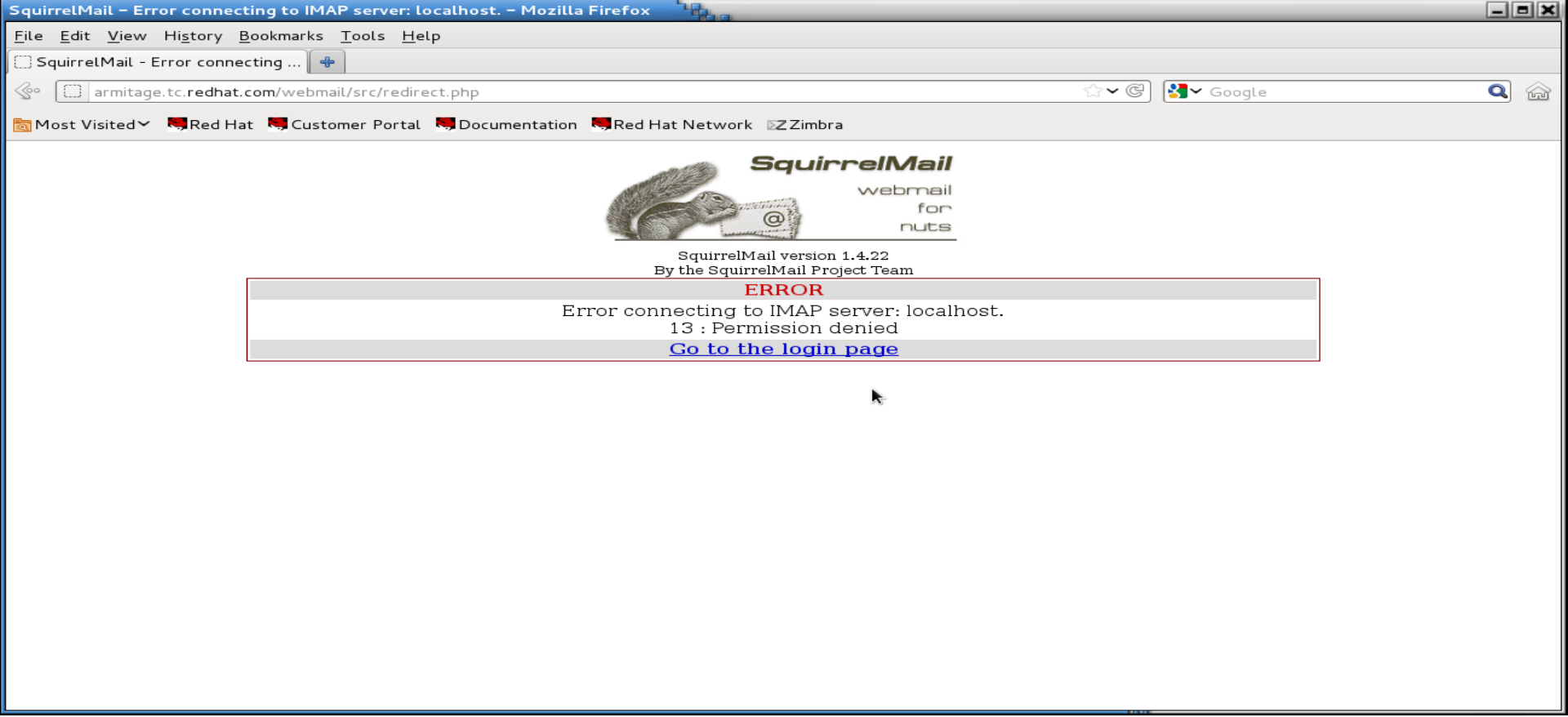
Creating Policy Modules

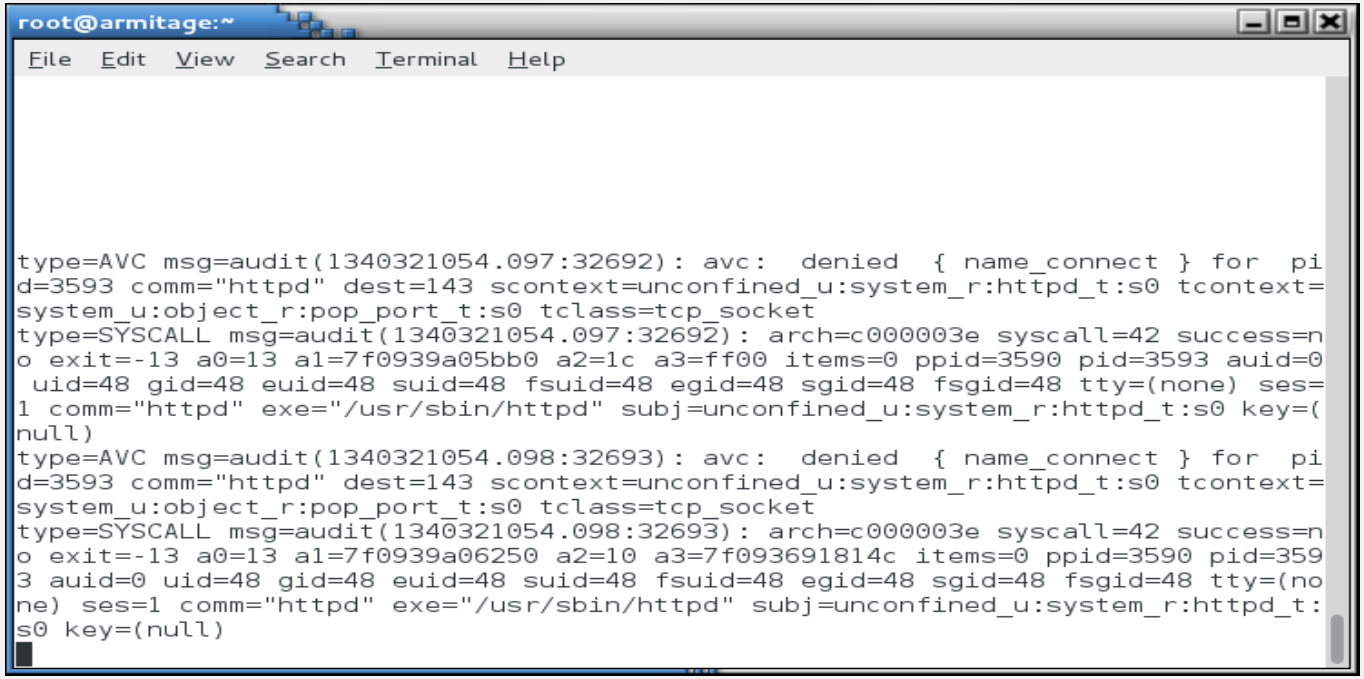
- In the case that a boolean or labeling does not fix your issue, you might have to create a policy module.

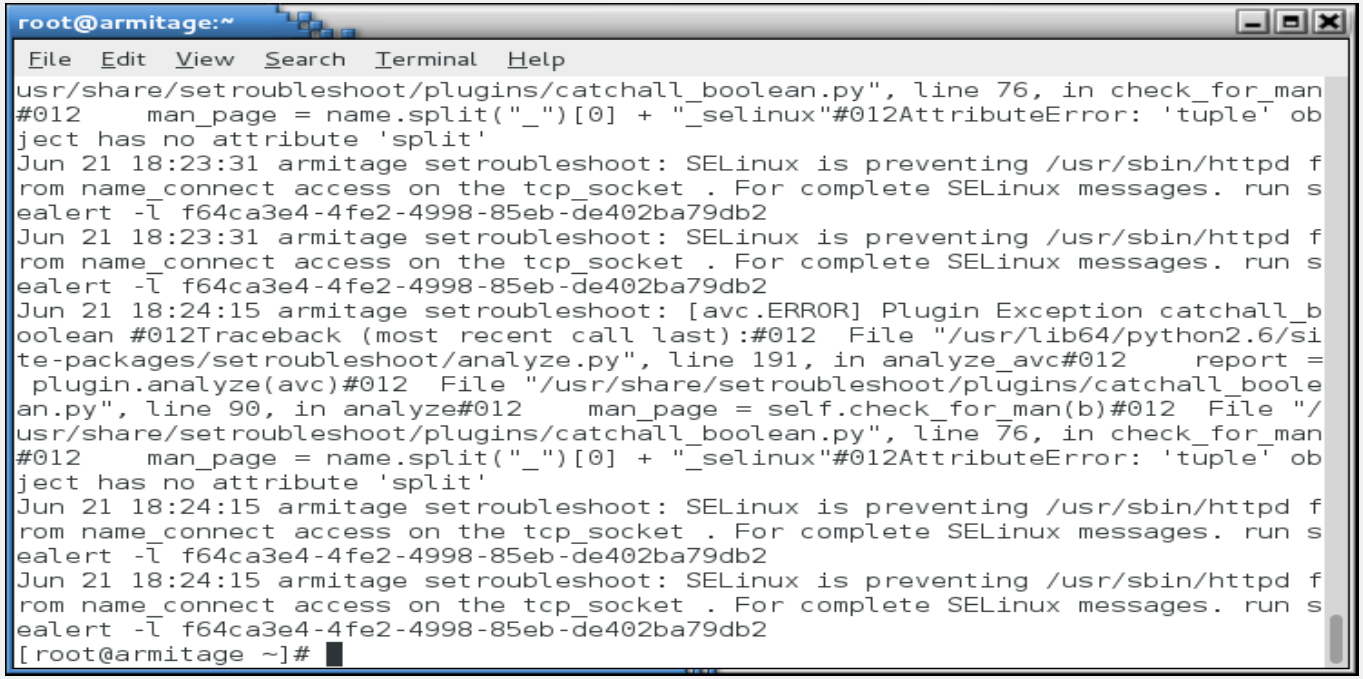
Creating Policy Modules

- In this example, I want to install squirrelmail on a RHEL 6 mail server. Other than using journalctl instead of /var/log/messages, the process is the same.


SquirrelMail – Login – Mozilla Firefox
File Edit View History Bookmarks Tools Help
SquirrelMail - Login
armitage.tc.redhat.com/webmail/src/login.php
Google
Most Visited Red Hat Customer Portal Documentation Red Hat Network Zimbra
SquirrelMail
webmail
for
nuts
SquirrelMail version 1.4.22
By the SquirrelMail Project Team
SquirrelMail Login
Name: fred
Password: ••••••••
Login

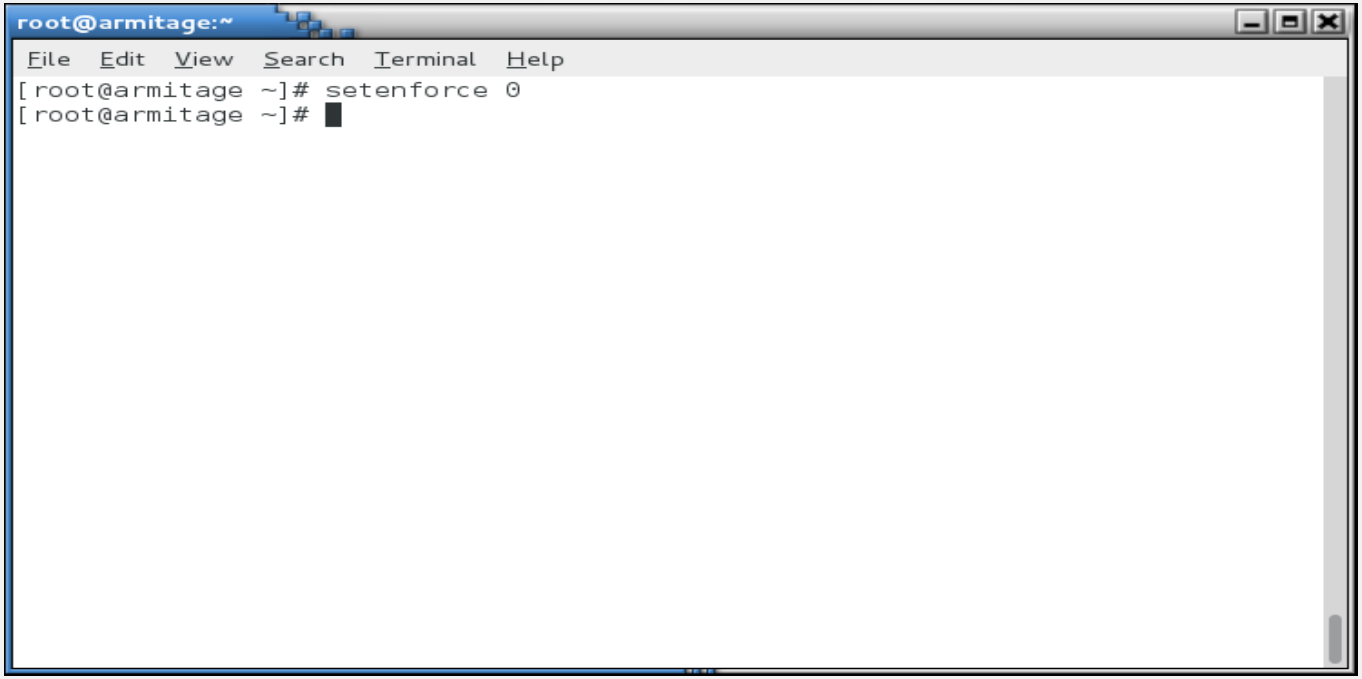

SquirrelMail – Error connecting to IMAP server: localhost. – Mozilla Firefox
File Edit View History Bookmarks Tools Help
SquirrelMail - Error connecting ...
armitage.tc.redhat.com/webmail/src/redirect.php
Google
Most Visited Red Hat Customer Portal Documentation Red Hat Network Zimbra
SquirrelMail
webmail
for
nuts
SquirrelMail version 1.4.22
By the SquirrelMail Project Team
ERROR
Error connecting to IMAP server: localhost.
13 : Permission denied
Go to the login page

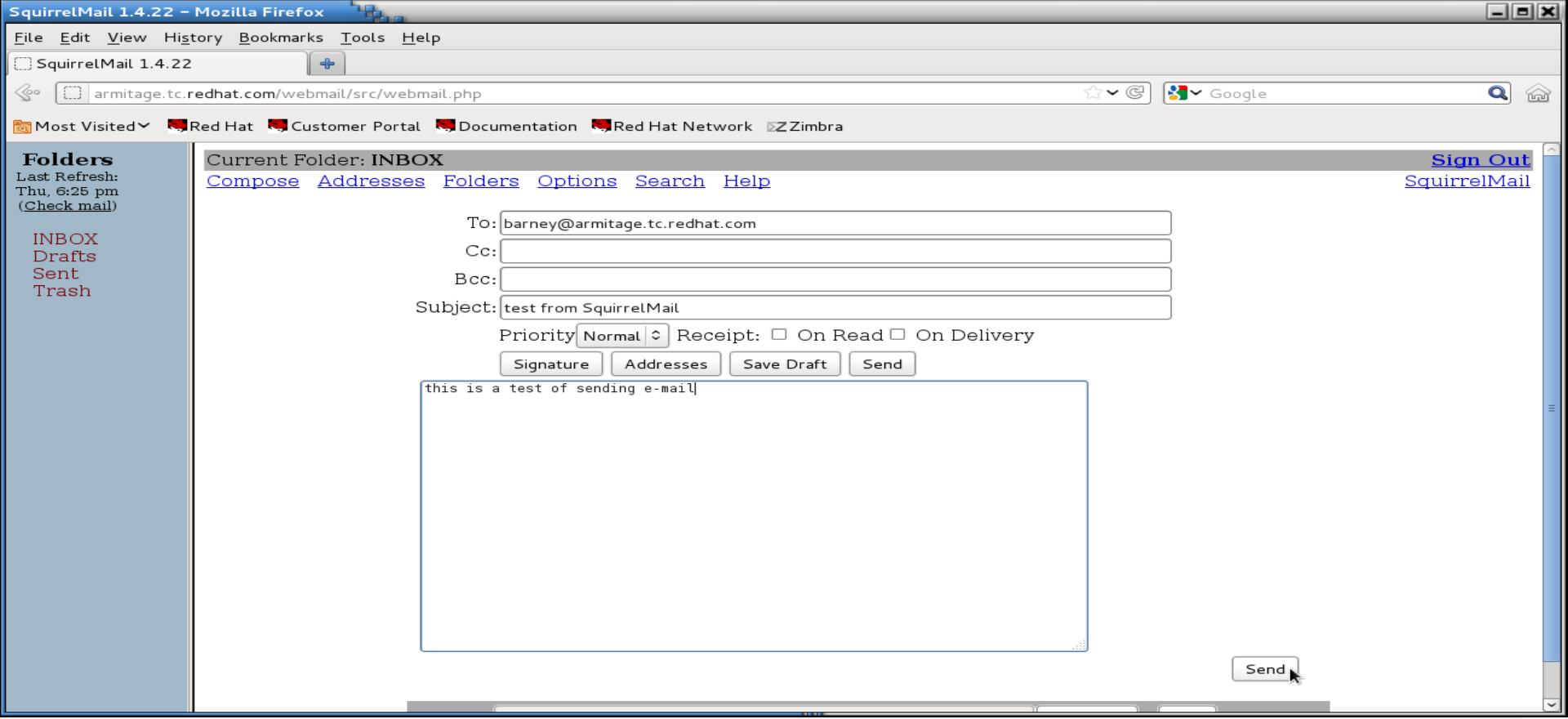

root@armitage:~
File Edit View Search Terminal Help
type=AVC msg=audit(1340321054.097:32692): avc: denied { name_connect } for pi
d=3593 comm="httpd" dest=143 scontext=unconfined_u:system_r:httpd_t:s0 tcontext=
system_u:object_r:pop_port_t:s0 tclass=tcp_socket
type=SYSCALL msg=audit(1340321054.097:32692): arch=c000003e syscall=42 success=n
o exit=-13 a0=13 a1=7f0939a05bb0 a2=1c a3=ff00 items=0 ppid=3590 pid=3593 auid=0
uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=
1 comm="httpd" exe="/usr/sbin/httpd" subj=unconfined_u:system_r:httpd_t:s0 key=(
null)
type=AVC msg=audit(1340321054.098:32693): avc: denied { name_connect } for pi
d=3593 comm="httpd" dest=143 scontext=unconfined_u:system_r:httpd_t:s0 tcontext=
system_u:object_r:pop_port_t:s0 tclass=tcp_socket
type=SYSCALL msg=audit(1340321054.098:32693): arch=c000003e syscall=42 success=n
o exit=-13 a0=13 a1=7f0939a06250 a2=10 a3=7f093691814c items=0 ppid=3590 pid=359
3 auid=0 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(no
ne) ses=1 comm="httpd" exe="/usr/sbin/httpd" subj=unconfined_u:system_r:httpd_t:
s0 key=(null)

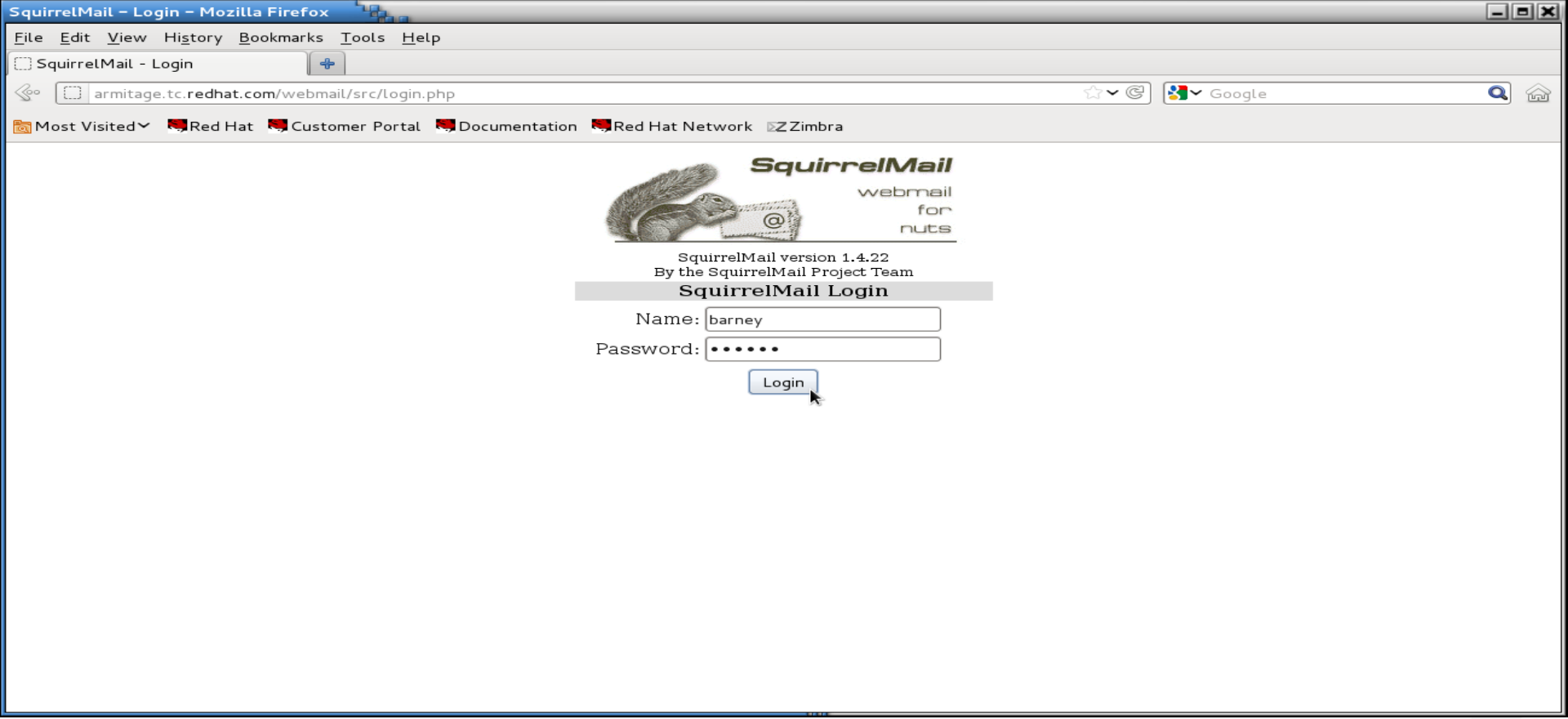

root@armitage:~
File Edit View Search Terminal Help
usr/share/setroubleshoot/plugins/catchall_boolean.py", line 76, in check_for_man
#012 man_page = name.split("_")[0] + "_selinux"#012AttributeError: 'tuple' ob
ject has no attribute 'split'
Jun 21 18:23:31 armitage setroubleshoot: SELinux is preventing /usr/sbin/httpd f
rom name_connect access on the tcp_socket . For complete SELinux messages. run s
ealert -l f64ca3e4-4fe2-4998-85eb-de402ba79db2
Jun 21 18:23:31 armitage setroubleshoot: SELinux is preventing /usr/sbin/httpd f
rom name_connect access on the tcp_socket . For complete SELinux messages. run s
ealert -l f64ca3e4-4fe2-4998-85eb-de402ba79db2
Jun 21 18:24:15 armitage setroubleshoot: [avc.ERROR] Plugin Exception catchall_b
oolean #012Traceback (most recent call last):#012 File "/usr/lib64/python2.6/si
te-packages/setroubleshoot/analyze.py", line 191, in analyze_avc#012 report =
plugin.analyze(avc)#012 File "/usr/share/setroubleshoot/plugins/catchall_boole
an.py", line 90, in analyze#012 man_page = self.check_for_man(b)#012 File "/
usr/share/setroubleshoot/plugins/catchall_boolean.py", line 76, in check_for_man
#012 man_page = name.split("_")[0] + "_selinux"#012AttributeError: 'tuple' ob
ject has no attribute 'split'
Jun 21 18:24:15 armitage setroubleshoot: SELinux is preventing /usr/sbin/httpd f
rom name_connect access on the tcp_socket . For complete SELinux messages. run s
ealert -l f64ca3e4-4fe2-4998-85eb-de402ba79db2
Jun 21 18:24:15 armitage setroubleshoot: SELinux is preventing /usr/sbin/httpd f
rom name_connect access on the tcp_socket . For complete SELinux messages. run s
ealert -l f64ca3e4-4fe2-4998-85eb-de402ba79db2
[root@armitage ~]#

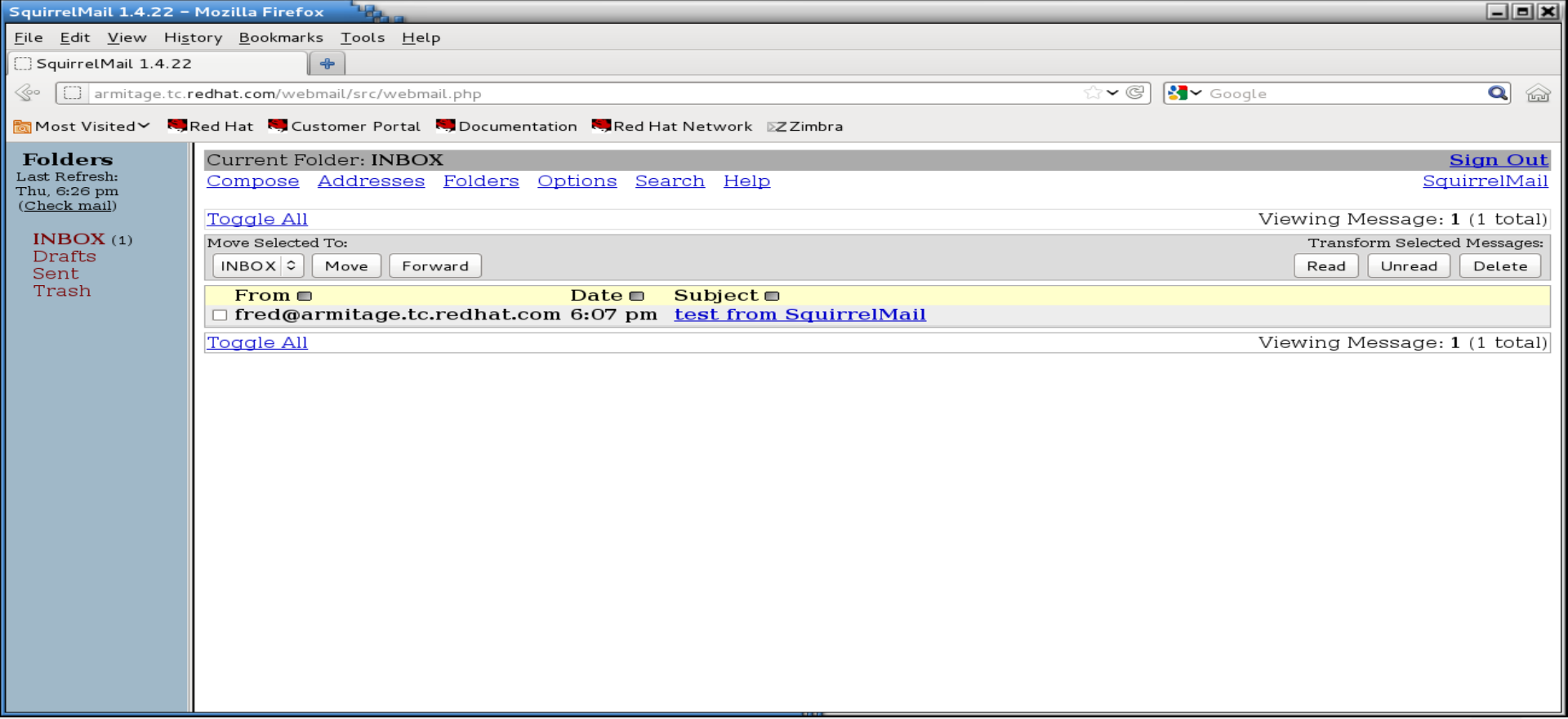
Creating Policy Modules

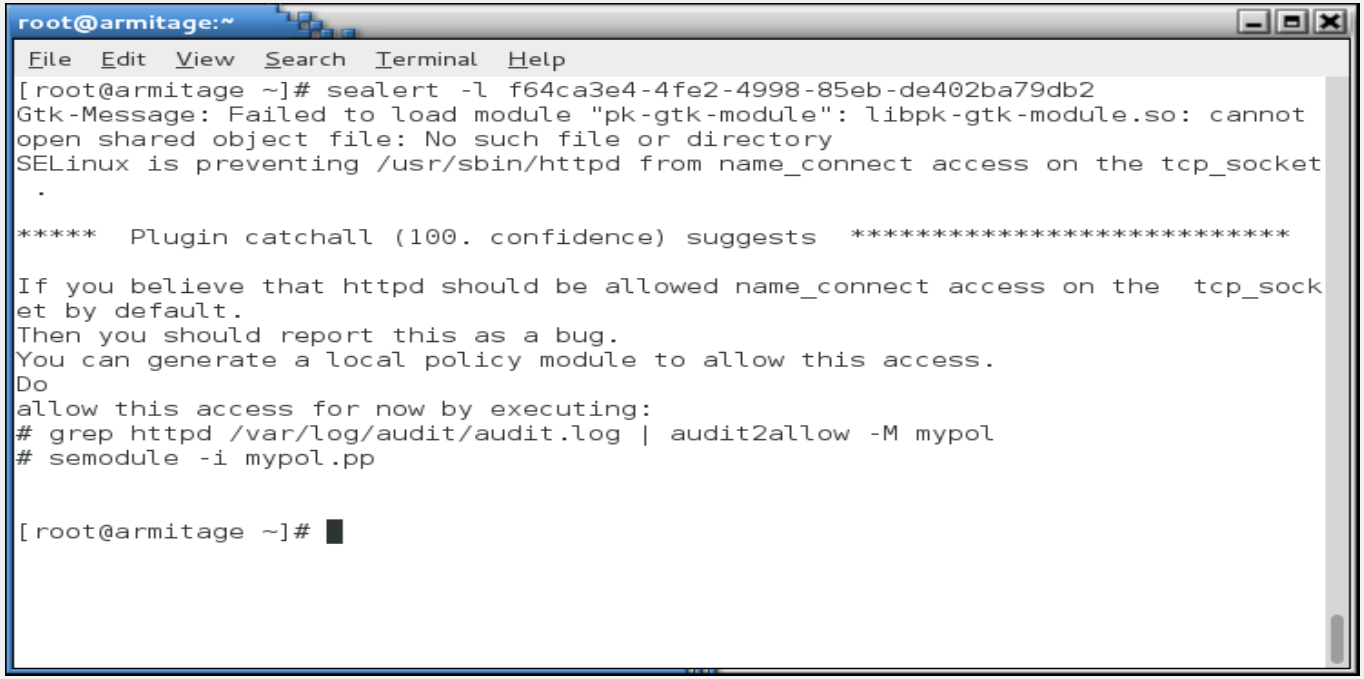
- Now that I know there is an SELinux issue, I set SELinux enforcement to “permissive” and then run the application through all its paces. In this case, sending and receiving mail.
- This will log denials but not act on them. If you don't do this, you'll fix one, trigger a second, fix the second, trigger a third, etc. It's easier to run the app in permissive mode and catch all of them.

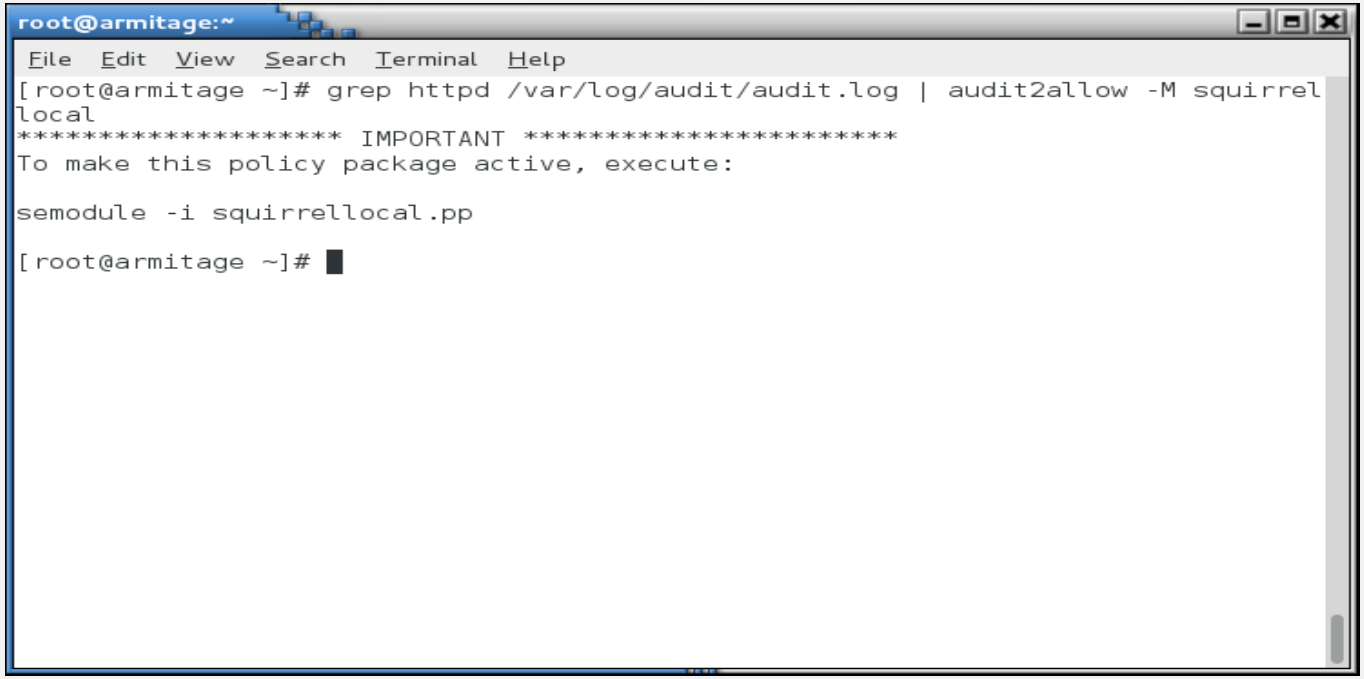

root@armitage:~
File Edit View Search Terminal Help
[root@armitage ~]# setenforce 0
[root@armitage ~]#


SquirrelMail 1.4.22 – Mozilla Firefox
File Edit View History Bookmarks Tools Help
SquirrelMail 1.4.22
armitage.tc.redhat.com/webmail/src/webmail.php
Google
Most Visited Red Hat Customer Portal Documentation Red Hat Network Zimbra
Folders
Last Refresh:
Thu, 6:25 pm
(Check mail)
INBOX
Drafts
Sent
Trash
Current Folder: INBOX
Sign Out
Compose Addresses Folders Options Search Help
SquirrelMail
To: barney@armitage.tc.redhat.com
Cc:
Bcc:
Subject: test from SquirrelMail
Priority Normal Receipt: On Read On Delivery
Signature Addresses Save Draft Send
this is a test of sending e-mail
Send


SquirrelMail – Login – Mozilla Firefox
File Edit View History Bookmarks Tools Help
SquirrelMail - Login
armitage.tc.redhat.com/webmail/src/login.php
Google
Most Visited Red Hat Customer Portal Documentation Red Hat Network Zimbra
SquirrelMail
webmail
for
nuts
SquirrelMail version 1.4.22
By the SquirrelMail Project Team
SquirrelMail Login
Name: barney
Password: ••••••
Login

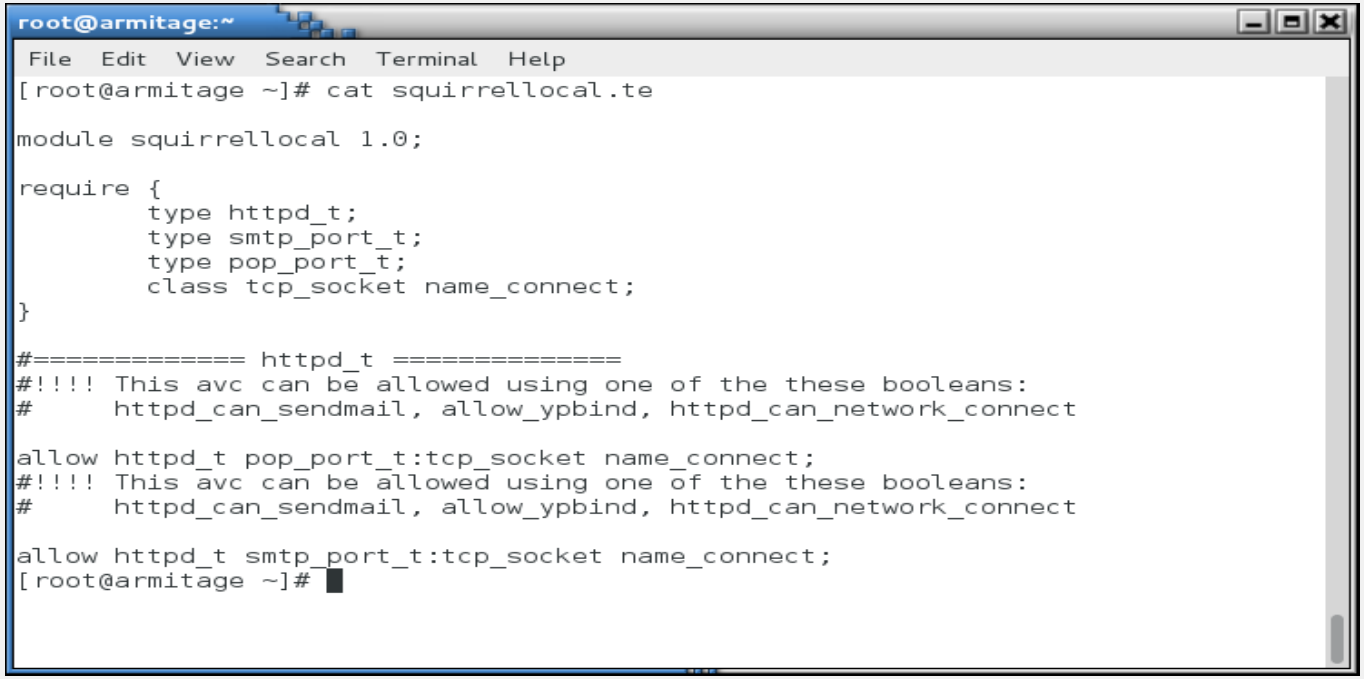

SquirrelMail 1.4.22 – Mozilla Firefox
File Edit View History Bookmarks Tools Help
SquirrelMail 1.4.22
armitage.tc.redhat.com/webmail/src/webmail.php
Google
Most Visited Red Hat Customer Portal Documentation Red Hat Network Zimbra
Folders
Last Refresh:
Thu, 6:26 pm
(Check mail)
INBOX (1)
Drafts
Sent
Trash
Current Folder: INBOX
Sign Out
Compose Addresses Folders Options Search Help
SquirrelMail
Toggle All
Viewing Message: 1 (1 total)
Move Selected To:
INBOX
Move
Forward
Transform Selected Messages:
Read
Unread
Delete
From
Date
Subject
fred@armitage.tc.redhat.com 6:07 pm test from SquirrelMail
Toggle All
Viewing Message: 1 (1 total)

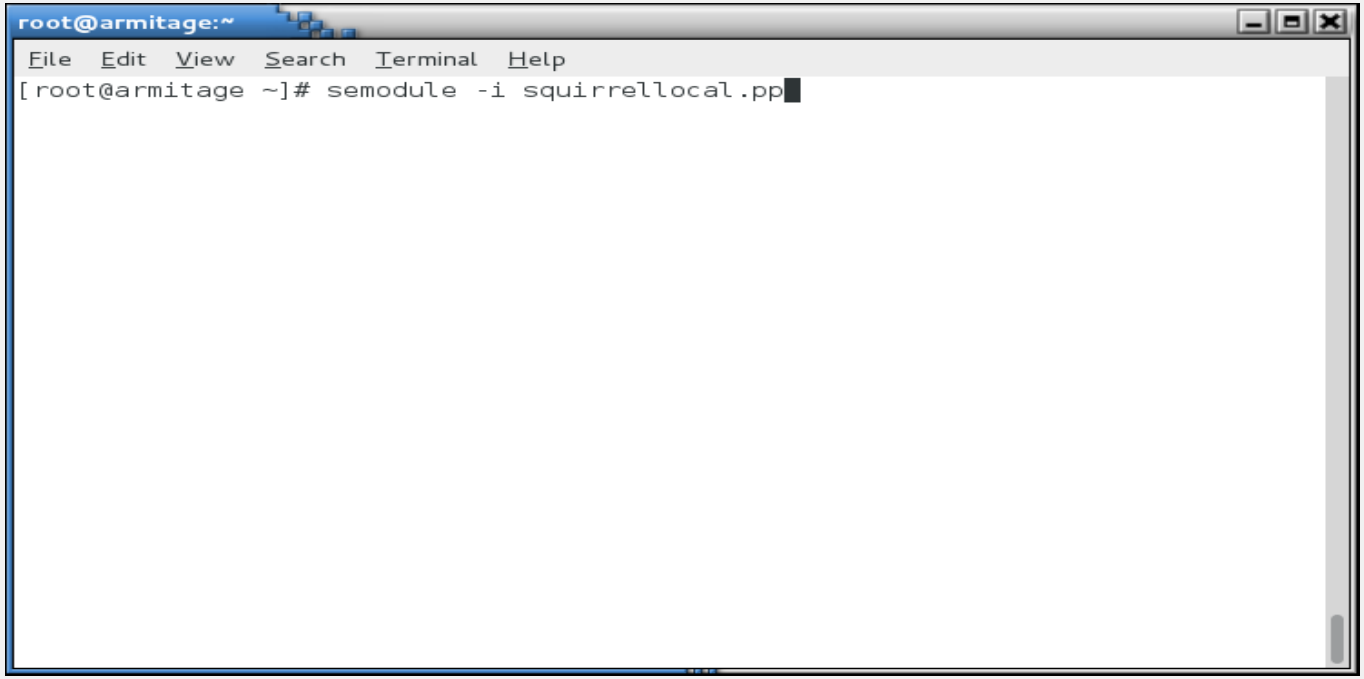

root@armitage:~
File Edit View Search Terminal Help
[root@armitage ~]# sealert -l f64ca3e4-4fe2-4998-85eb-de402ba79db2
Gtk-Message: Failed to load module "pk-gtk-module": libpk-gtk-module.so: cannot
open shared object file: No such file or directory
SELinux is preventing /usr/sbin/httpd from name_connect access on the tcp_socket
.
***** Plugin catchall (100. confidence) suggests **************************
If you believe that httpd should be allowed name_connect access on the tcp_sock
et by default.
Then you should report this as a bug.
You can generate a local policy module to allow this access.
Do
allow this access for now by executing:
grep httpd /var/log/audit/audit.log | audit2allow -M mypol
semodule -i mypol.pp
[root@armitage ~]#

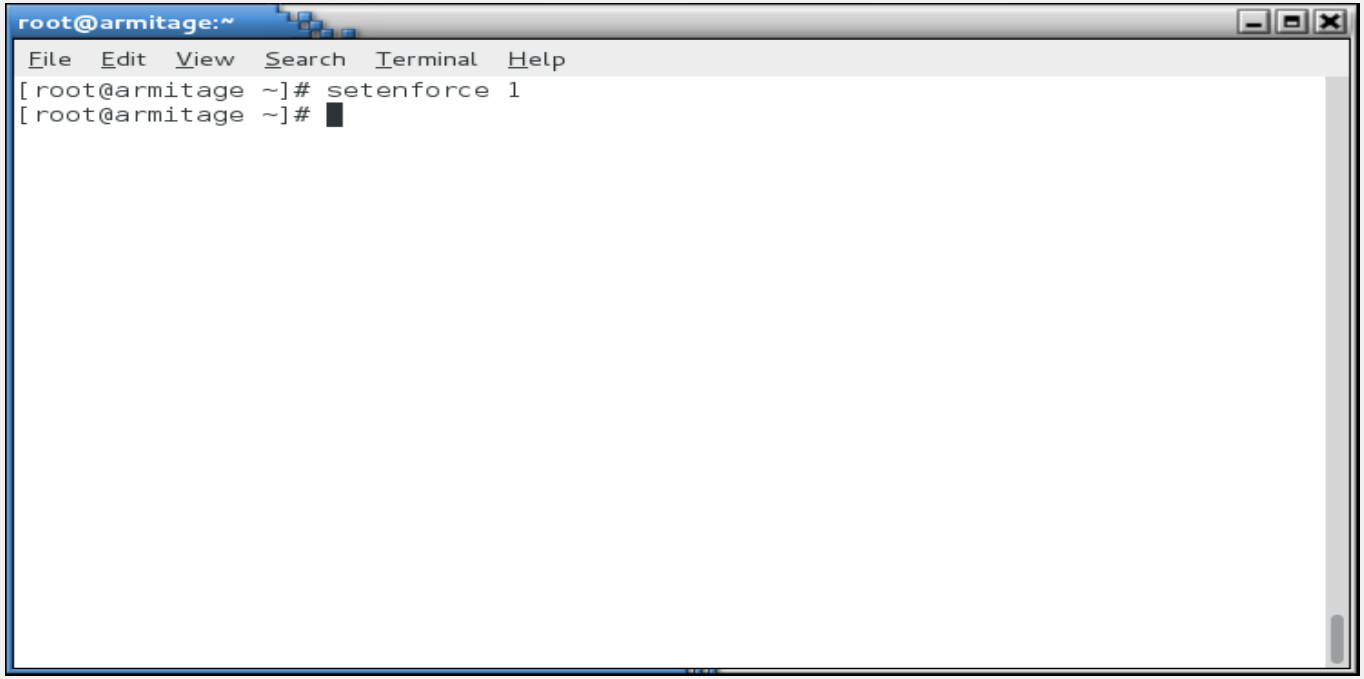

root@armitage:~
File Edit View Search Terminal Help
[root@armitage ~]# grep httpd /var/log/audit/audit.log | audit2allow -M squirrel
local
********************* IMPORTANT ************************
To make this policy package active, execute:
semodule -i squirrellocal.pp
[root@armitage ~]#

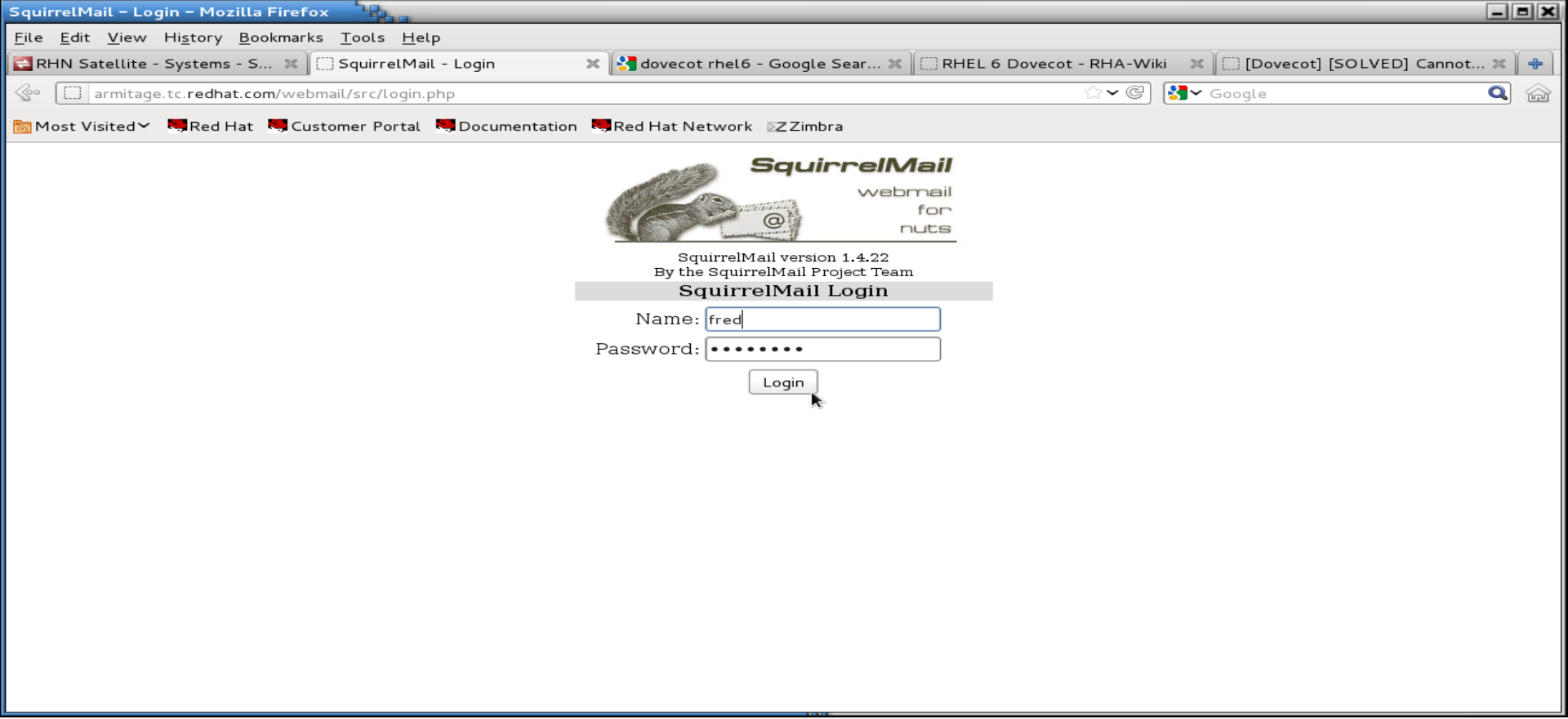
Note

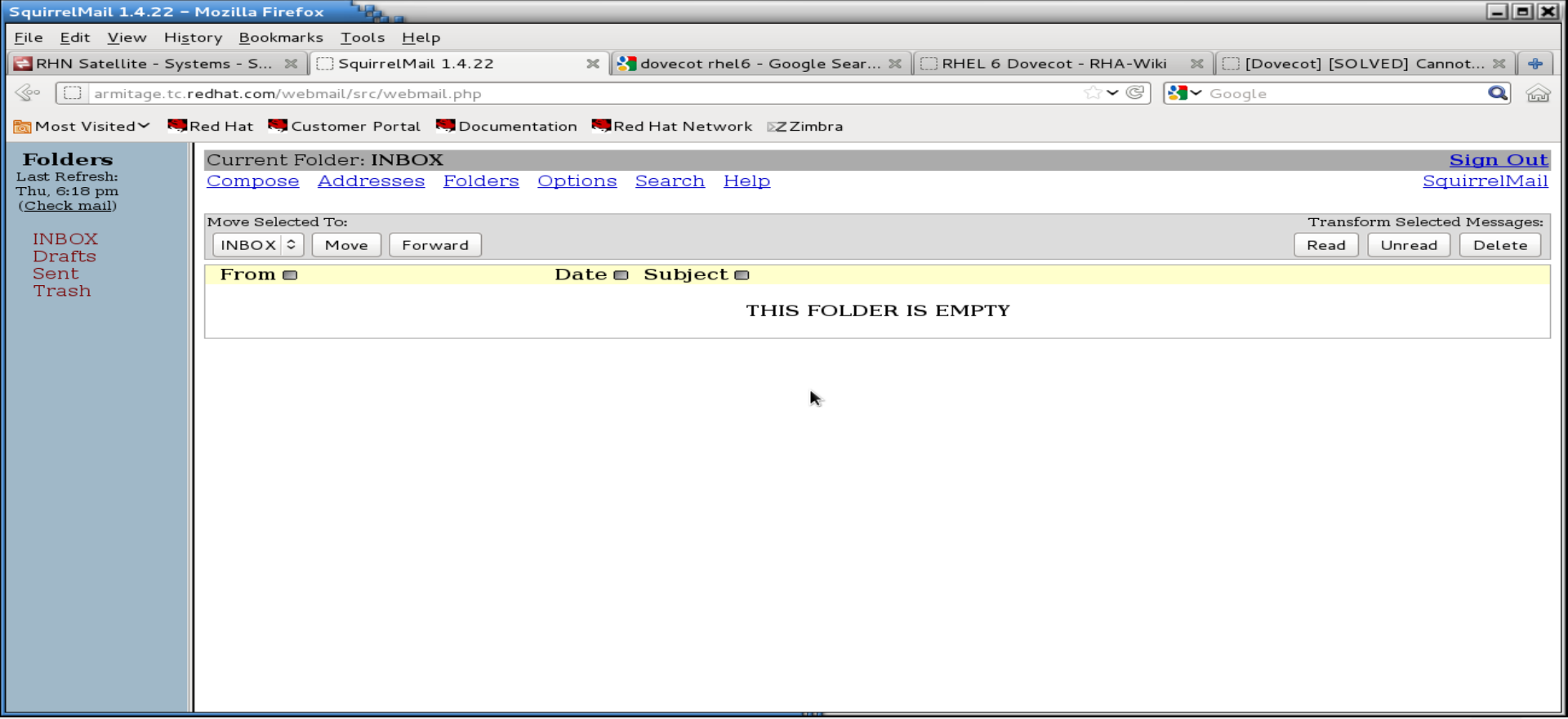
- Actually, this error could be fixed by setting a boolean. I am just creating a policy module so you can see it being done.


root@armitage:~
File Edit View Search Terminal Help
[root@armitage ~]# cat squirrellocal.te
module squirrellocal 1.0;
require {
type httpd_t;
type smtp_port_t;
type pop_port_t;
class tcp_socket name_connect;
}
#============= httpd_t ==============
#!!!! This avc can be allowed using one of the these booleans:
httpd_can_sendmail, allow_ypbind, httpd_can_network_connect
allow httpd_t pop_port_t:tcp_socket name_connect;
#!!!! This avc can be allowed using one of the these booleans:
httpd_can_sendmail, allow_ypbind, httpd_can_network_connect
allow httpd_t smtp_port_t:tcp_socket name_connect;
[root@armitage ~]#


root@armitage:~
File Edit View Search Terminal Help
[root@armitage ~]# semodule -i squirrellocal.pp


root@armitage:~
File Edit View Search Terminal Help
[root@armitage ~]# setenforce 1
[root@armitage ~]#

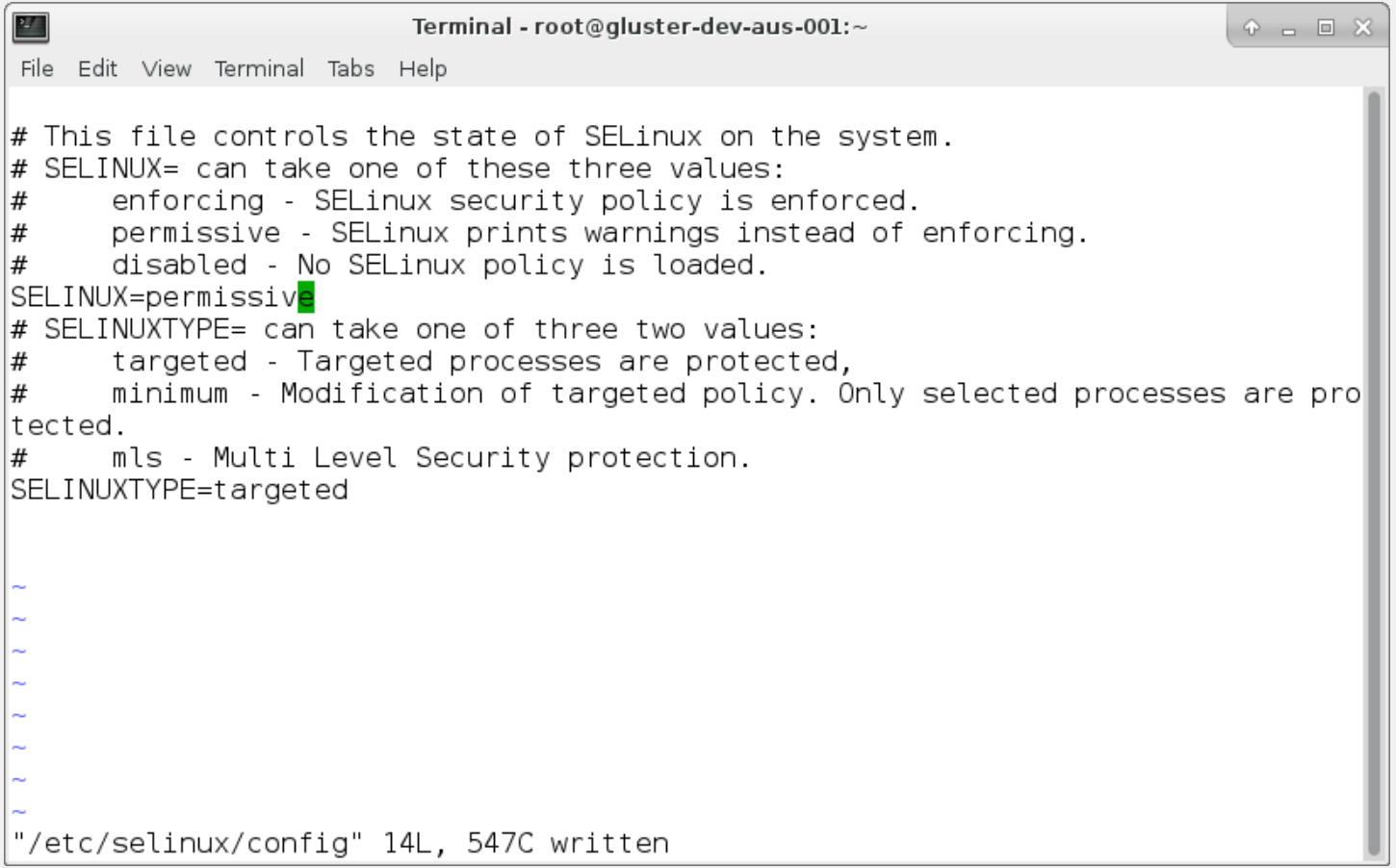

SquirrelMail – Login – Mozilla Firefox
File Edit View History Bookmarks Tools Help
RHN Satellite - Systems - S...
SquirrelMail - Login
dovecot rhel6 - Google Sear...
RHEL 6 Dovecot - RHA-Wiki
[Dovecot] [SOLVED] Cannot...
armitage.tc.redhat.com/webmail/src/login.php
Google
Most Visited
Red Hat
Customer Portal
Documentation
Red Hat Network
Zimbra
SquirrelMail
webmail
for
nuts
SquirrelMail version 1.4.22
By the SquirrelMail Project Team
SquirrelMail Login
Name: fred
Password:
Login


SquirrelMail 1.4.22 – Mozilla Firefox
File Edit View History Bookmarks Tools Help
RHN Satellite - Systems - S...
SquirrelMail 1.4.22
dovecot rhel6 - Google Sear...
RHEL 6 Dovecot - RHA-Wiki
[Dovecot] [SOLVED] Cannot...
armitage.tc.redhat.com/webmail/src/webmail.php
Google
Most Visited
Red Hat
Customer Portal
Documentation
Red Hat Network
Zimbra
Folders
Last Refresh:
Thu, 6:18 pm
(Check mail)
INBOX
Drafts
Sent
Trash
Current Folder: INBOX
Sign Out
Compose Addresses Folders Options Search Help
SquirrelMail
Move Selected To:
INBOX
Move
Forward
Transform Selected Messages:
Read
Unread
Delete
From
Date
Subject
THIS FOLDER IS EMPTY

ENABLING SELINUX

Enabling SELinux

- To enable SELinux on a system, edit /etc/selinux/config and set SELINUX=permissive
- Do not set it to enforcing, as it will more than likely hang at boot time.


Terminal - root@gluster-dev-aus-001:~
File Edit View Terminal Tabs Help
# 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=permissive
# SELINUXTYPE= can take one of three two values:
#   targeted - Targeted processes are protected,
#   minimum - Modification of targeted policy. Only selected processes are pro
tected.
#   mls - Multi Level Security protection.
SELINUXTYPE=targeted
~
~
~
~
~
~
~
~
"/etc/selinux/config" 14L, 547C written

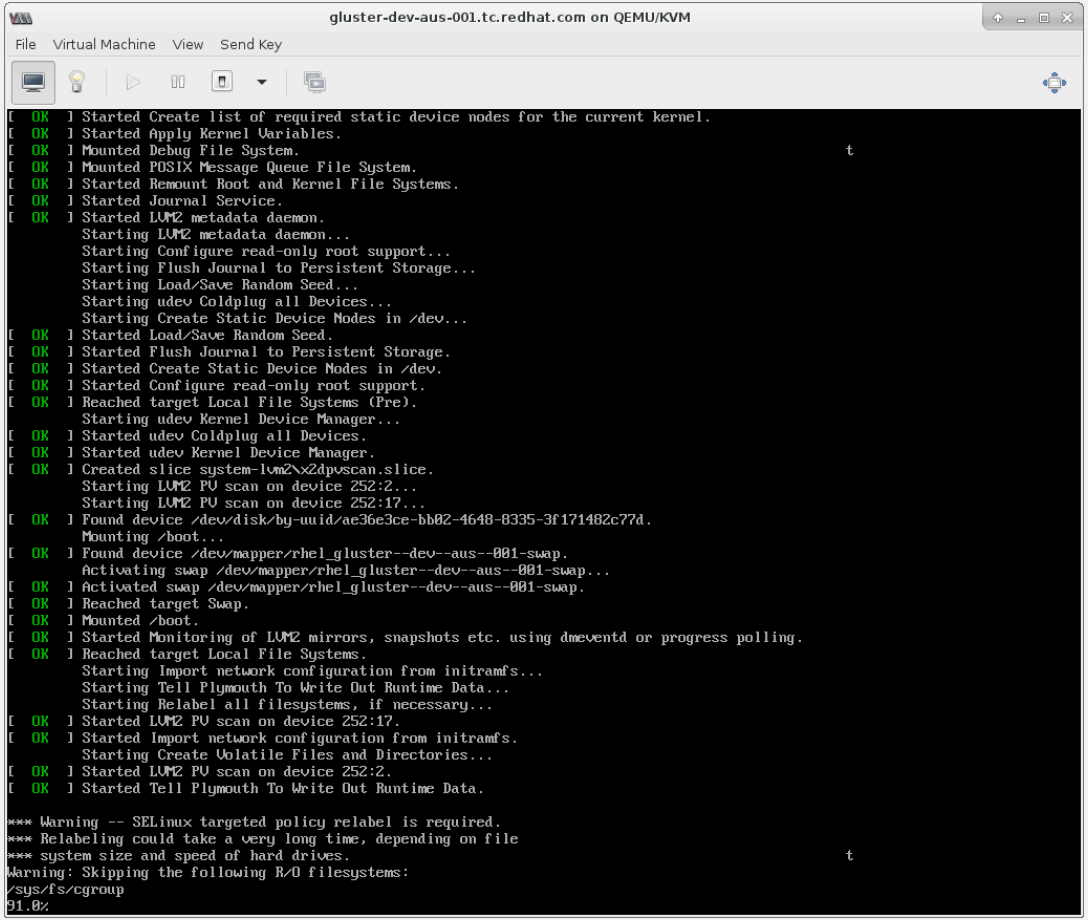
Enabling SELinux

- Then create a file in the root of the filesystem called .autorelabel


Terminal - root@gluster-dev-aus-001:~
File Edit View Terminal Tabs Help
[root@gluster-dev-aus-001 ~]# vi /etc/selinux/config
[root@gluster-dev-aus-001 ~]# touch /.autorelabel
[root@gluster-dev-aus-001 ~]#

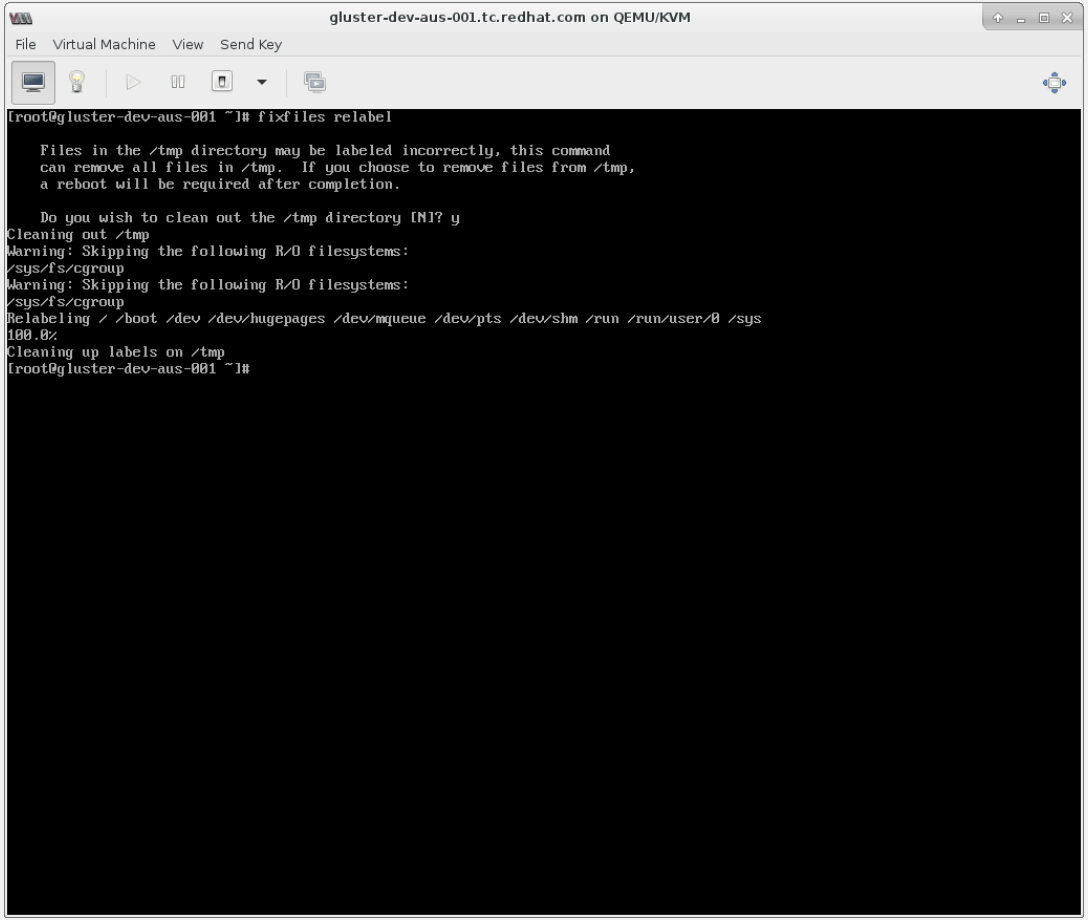
Enabling SELinux

- Reboot, and the system will relabel the filesystem.


gluster-dev-aus-001.tc.redhat.com on QEMU/KVM
File Virtual Machine View Send Key
[OK] Started Create list of required static device nodes for the current kernel.
[OK] Started Apply Kernel Variables.
[OK] Mounted Debug File System.
[OK] Mounted POSIX Message Queue File System.
[OK] Started Remount Root and Kernel File Systems.
[OK] Started Journal Service.
[OK] Started LVM2 metadata daemon.
Starting LVM2 metadata daemon...
Starting Configure read-only root support...
Starting Flush Journal to Persistent Storage...
Starting Load/Save Random Seed...
Starting udev Coldplug all Devices...
Starting Create Static Device Nodes in /dev...
[OK] Started Load/Save Random Seed.
[OK] Started Flush Journal to Persistent Storage.
[OK] Started Create Static Device Nodes in /dev.
[OK] Started Configure read-only root support.
[OK] Reached target Local File Systems (Pre).
Starting udev Kernel Device Manager...
[OK] Started udev Coldplug all Devices.
[OK] Started udev Kernel Device Manager.
[OK] Created slice system-lvm2\x2dpvscan.slice.
Starting LVM2 PV scan on device 252:2...
Starting LVM2 PV scan on device 252:17...
[OK] Found device /dev/disk/by-uuid/ae36e3ce-bb02-4648-8335-3f171482c77d.
Mounting /boot...
[OK] Found device /dev/mapper/rhel_gluster--dev--aus--001-swap.
Activating swap /dev/mapper/rhel_gluster--dev--aus--001-swap...
[OK] Activated swap /dev/mapper/rhel_gluster--dev--aus--001-swap.
[OK] Reached target Swap.
[OK] Mounted /boot.
[OK] Started Monitoring of LVM2 mirrors, snapshots etc. using dmeventd or progress polling.
[OK] Reached target Local File Systems.
Starting Import network configuration from initramfs...
Starting Tell Plymouth To Write Out Runtime Data...
Starting Relabel all filesystems, if necessary...
[OK] Started LVM2 PV scan on device 252:17.
[OK] Started Import network configuration from initramfs.
Starting Create Volatile Files and Directories...
[OK] Started LVM2 PV scan on device 252:2.
[OK] Started Tell Plymouth To Write Out Runtime Data.
*** Warning -- SELinux targeted policy relabel is required.
*** Relabeling could take a very long time, depending on file
*** system size and speed of hard drives.
Warning: Skipping the following R/O filesystems:
/sys/fs/cgroup
91.0%

Enabling SELinux

- You can also run fixfiles relabel.
  - Don't do it in runlevel 5 - it deletes everything in /tmp and your X font server will get real cranky about that.
- Reboot after it's done.


gluster-dev-aus-001.tc.redhat.com on QEMU/KVM
File Virtual Machine View Send Key
[root@gluster-dev-aus-001 ~]# 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
Warning: Skipping the following R/O filesystems:
/sys/fs/cgroup
Warning: Skipping the following R/O filesystems:
/sys/fs/cgroup
Relabeling / /boot /dev /dev/hugepages /dev/mqueue /dev/pts /dev/shm /run /run/user/0 /sys
100.0%
Cleaning up labels on /tmp
[root@gluster-dev-aus-001 ~]#

Enabling SELinux

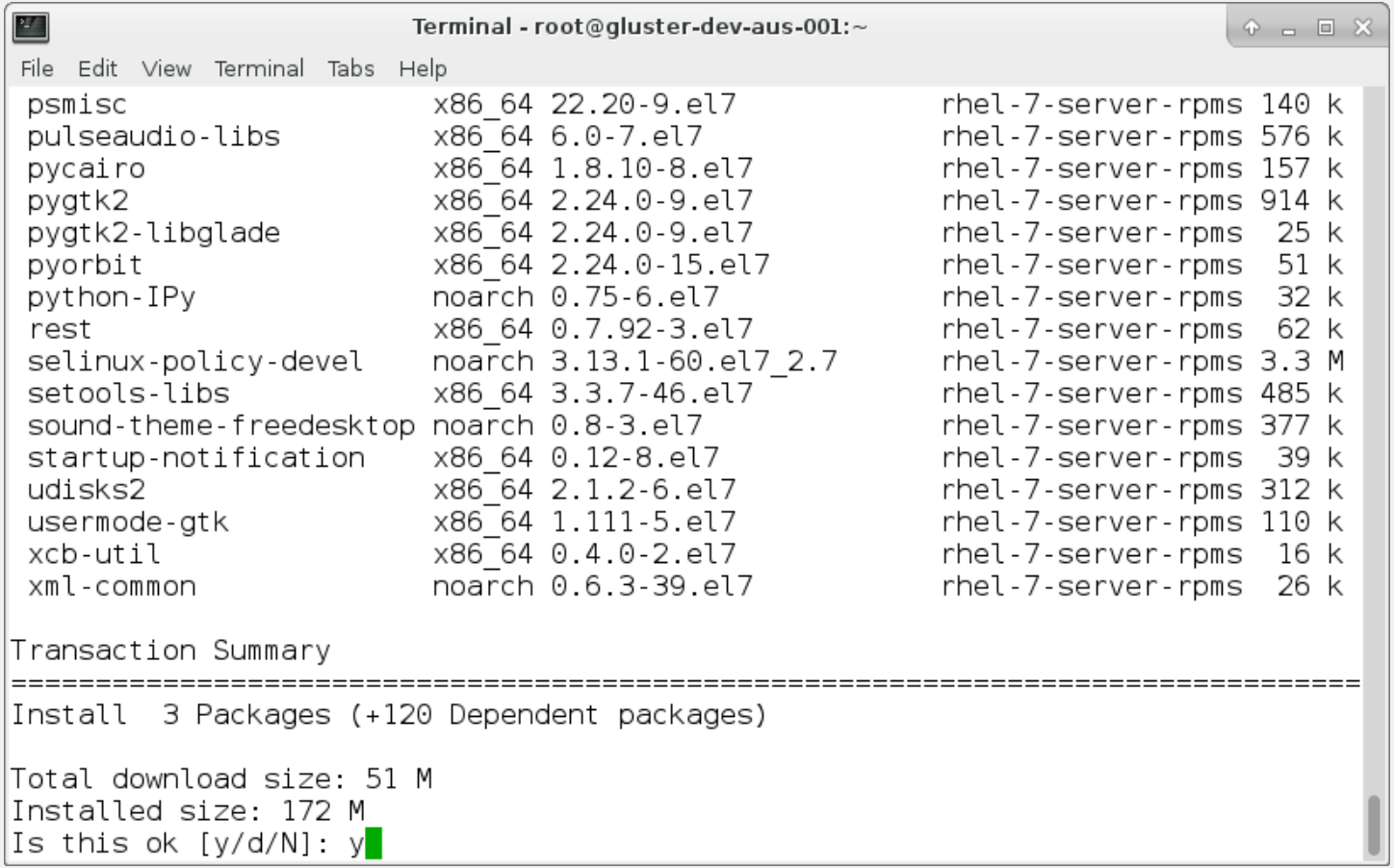
- After everything is relabeled, then set it to enforcing in /etc/selinux/config and reboot or run setenforce 1.

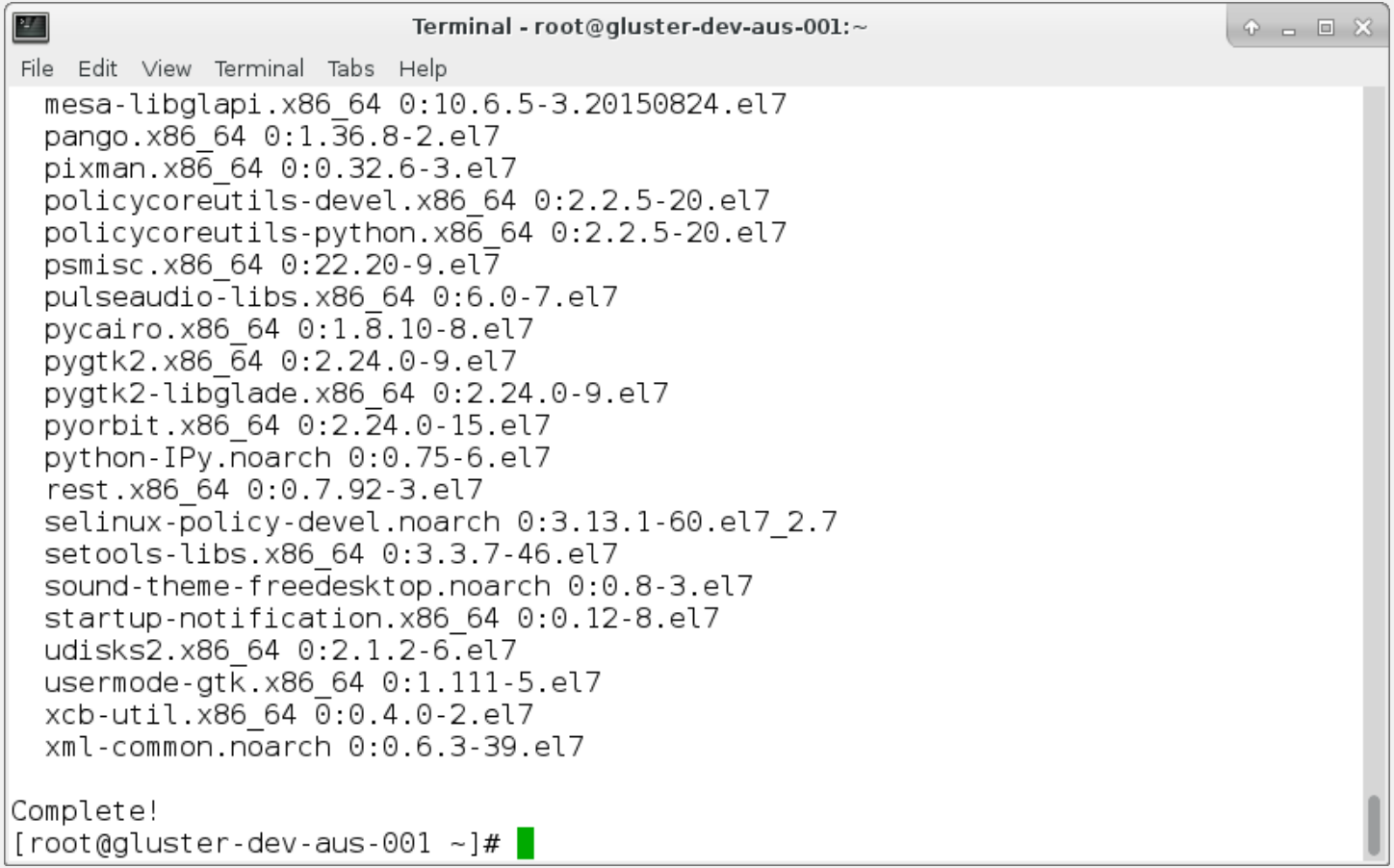
GRAPHICAL TOOLS

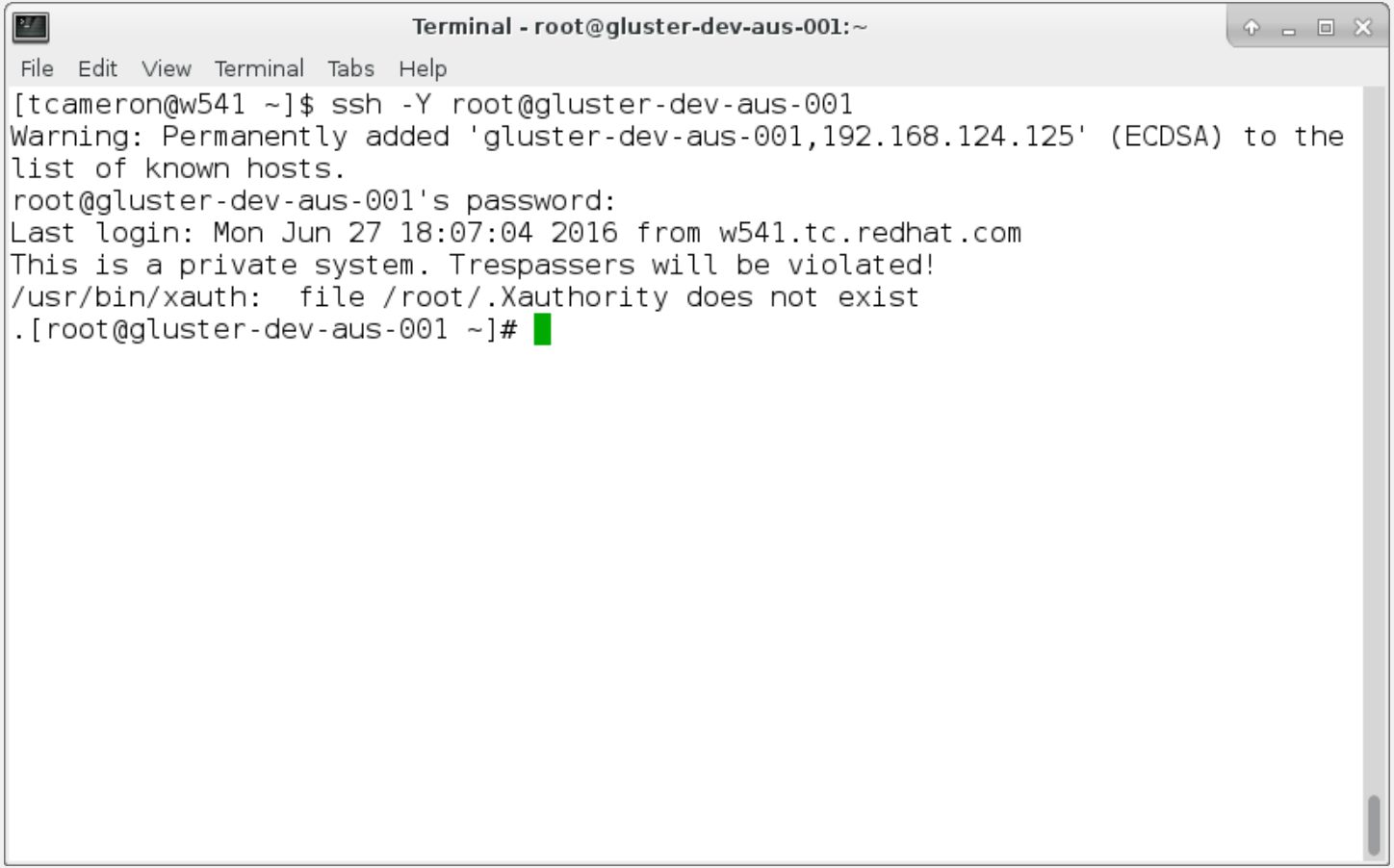
Graphical Tools

- This stuff is so easy, even a Windows admin can do it!
  - Install xorg-x11-xauth, a font (I like bitmap-fixed-fonts, or you can do yum groupinstall fonts), and policycoreutils-gui. and you can ssh -Y into the box and run system-config-selinux


Terminal - root@gluster-dev-aus-001:~
File Edit View Terminal Tabs Help
[root@gluster-dev-aus-001 ~]# yum -y install xorg-x11-xauth policycoreutils-gui
bitmap-fixed-fonts


Terminal - root@gluster-dev-aus-001:~
File Edit View Terminal Tabs Help
psmisc x86_64 22.20-9.el7 rhel-7-server-rpms 140 k
pulseaudio-libs x86_64 6.0-7.el7 rhel-7-server-rpms 576 k
pycairo x86_64 1.8.10-8.el7 rhel-7-server-rpms 157 k
pygtk2 x86_64 2.24.0-9.el7 rhel-7-server-rpms 914 k
pygtk2-libglade x86_64 2.24.0-9.el7 rhel-7-server-rpms 25 k
pyorbit x86_64 2.24.0-15.el7 rhel-7-server-rpms 51 k
python-IPy noarch 0.75-6.el7 rhel-7-server-rpms 32 k
rest x86_64 0.7.92-3.el7 rhel-7-server-rpms 62 k
selinux-policy-devel noarch 3.13.1-60.el7_2.7 rhel-7-server-rpms 3.3 M
setools-libs x86_64 3.3.7-46.el7 rhel-7-server-rpms 485 k
sound-theme-freedesktop noarch 0.8-3.el7 rhel-7-server-rpms 377 k
startup-notification x86_64 0.12-8.el7 rhel-7-server-rpms 39 k
udisks2 x86_64 2.1.2-6.el7 rhel-7-server-rpms 312 k
usermode-gtk x86_64 1.111-5.el7 rhel-7-server-rpms 110 k
xcb-util x86_64 0.4.0-2.el7 rhel-7-server-rpms 16 k
xml-common noarch 0.6.3-39.el7 rhel-7-server-rpms 26 k
Transaction Summary
Install 3 Packages (+120 Dependent packages)
Total download size: 51 M
Installed size: 172 M
Is this ok [y/d/N]: y

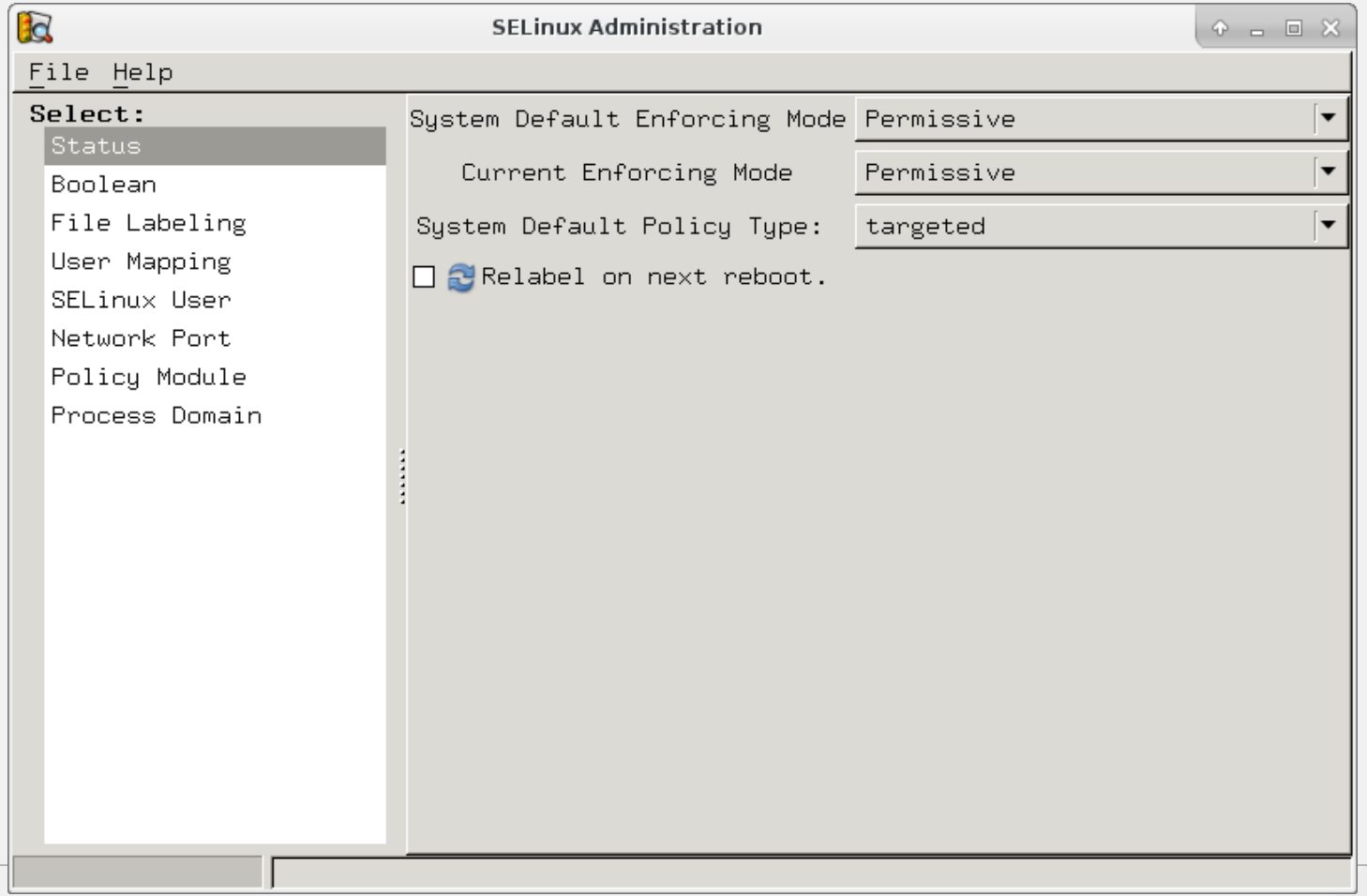

Terminal - root@gluster-dev-aus-001:~
File Edit View Terminal Tabs Help
mesa-libglapi.x86_64 0:10.6.5-3.20150824.el7
pango.x86_64 0:1.36.8-2.el7
pixman.x86_64 0:0.32.6-3.el7
policycoreutils-devel.x86_64 0:2.2.5-20.el7
policycoreutils-python.x86_64 0:2.2.5-20.el7
psmisc.x86_64 0:22.20-9.el7
pulseaudio-libs.x86_64 0:6.0-7.el7
pycairo.x86_64 0:1.8.10-8.el7
pygtk2.x86_64 0:2.24.0-9.el7
pygtk2-libglade.x86_64 0:2.24.0-9.el7
pyorbit.x86_64 0:2.24.0-15.el7
python-IPy.noarch 0:0.75-6.el7
rest.x86_64 0:0.7.92-3.el7
selinux-policy-devel.noarch 0:3.13.1-60.el7_2.7
setools-libs.x86_64 0:3.3.7-46.el7
sound-theme-freedesktop.noarch 0:0.8-3.el7
startup-notification.x86_64 0:0.12-8.el7
udisks2.x86_64 0:2.1.2-6.el7
usermode-gtk.x86_64 0:1.111-5.el7
xcb-util.x86_64 0:0.4.0-2.el7
xml-common.noarch 0:0.6.3-39.el7
Complete!
[root@gluster-dev-aus-001 ~]#

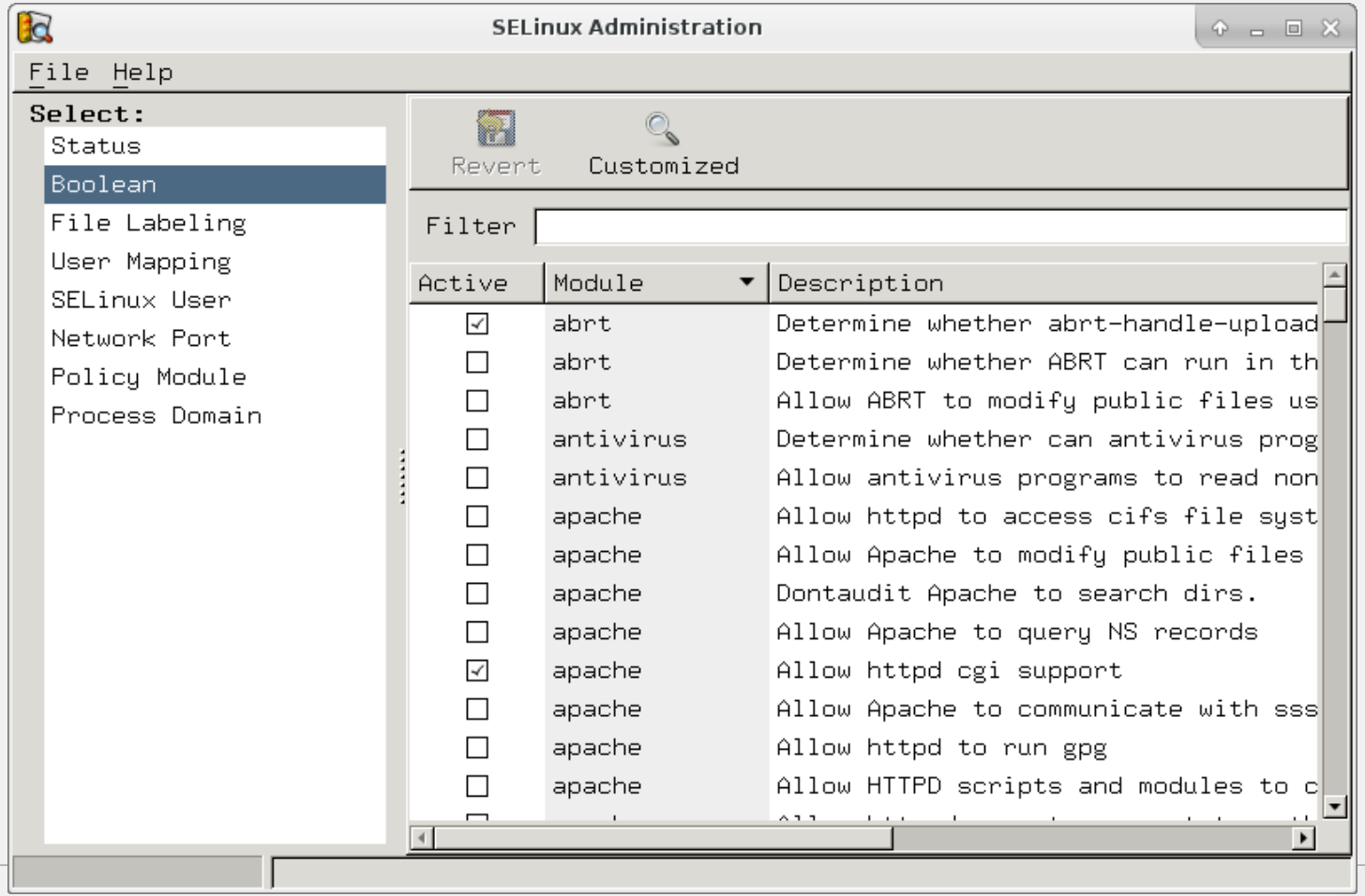

Terminal - root@gluster-dev-aus-001:~
File Edit View Terminal Tabs Help
[tcameron@w541 ~]$ ssh -Y root@gluster-dev-aus-001
Warning: Permanently added 'gluster-dev-aus-001,192.168.124.125' (ECDSA) to the list of known hosts.
root@gluster-dev-aus-001's password:
Last login: Mon Jun 27 18:07:04 2016 from w541.tc.redhat.com
This is a private system. Trespassers will be violated!
/usr/bin/xauth: file /root/.Xauthority does not exist
.[root@gluster-dev-aus-001 ~]#

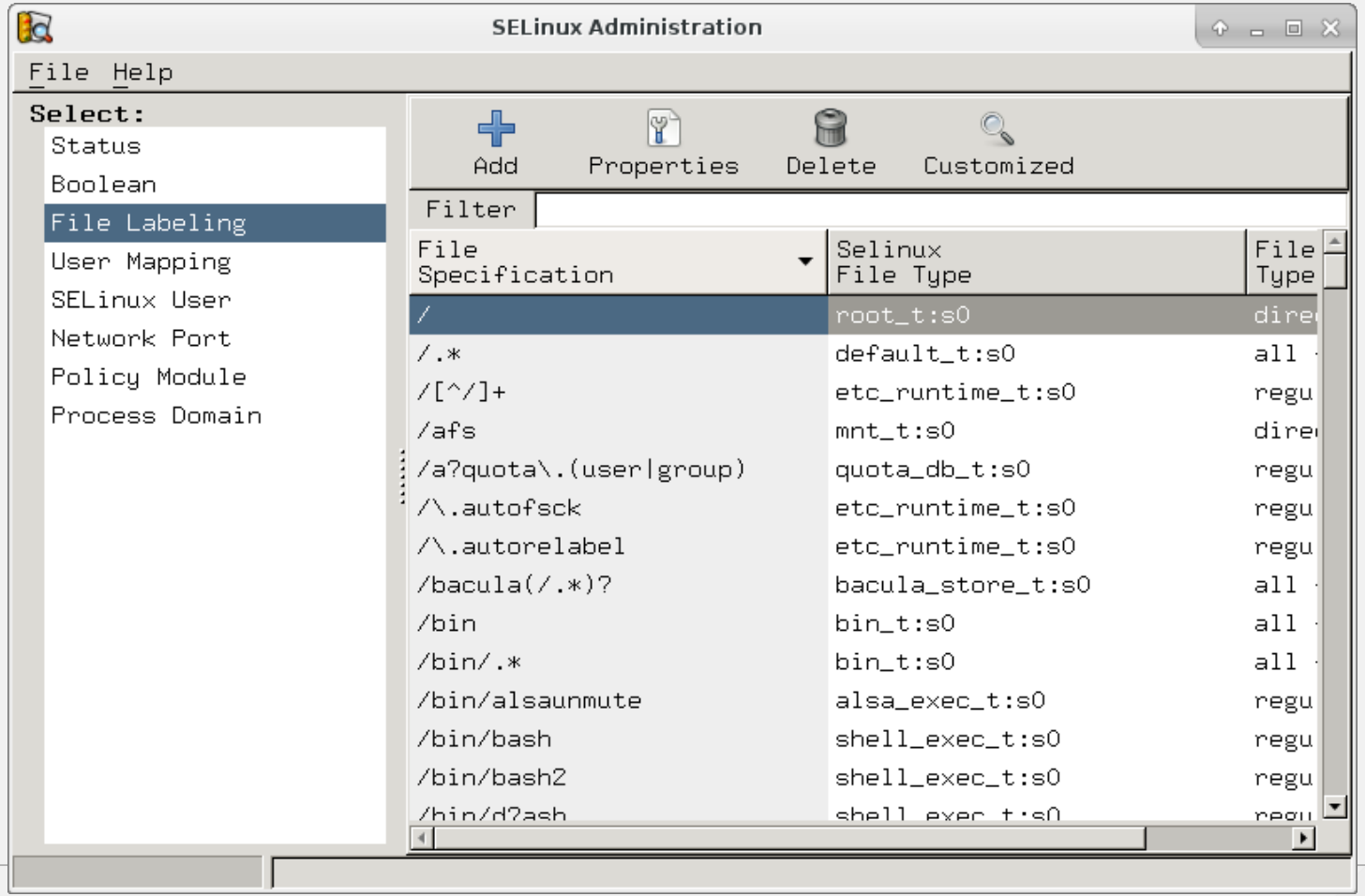
Terminal - root@gluster-dev-aus-001:~

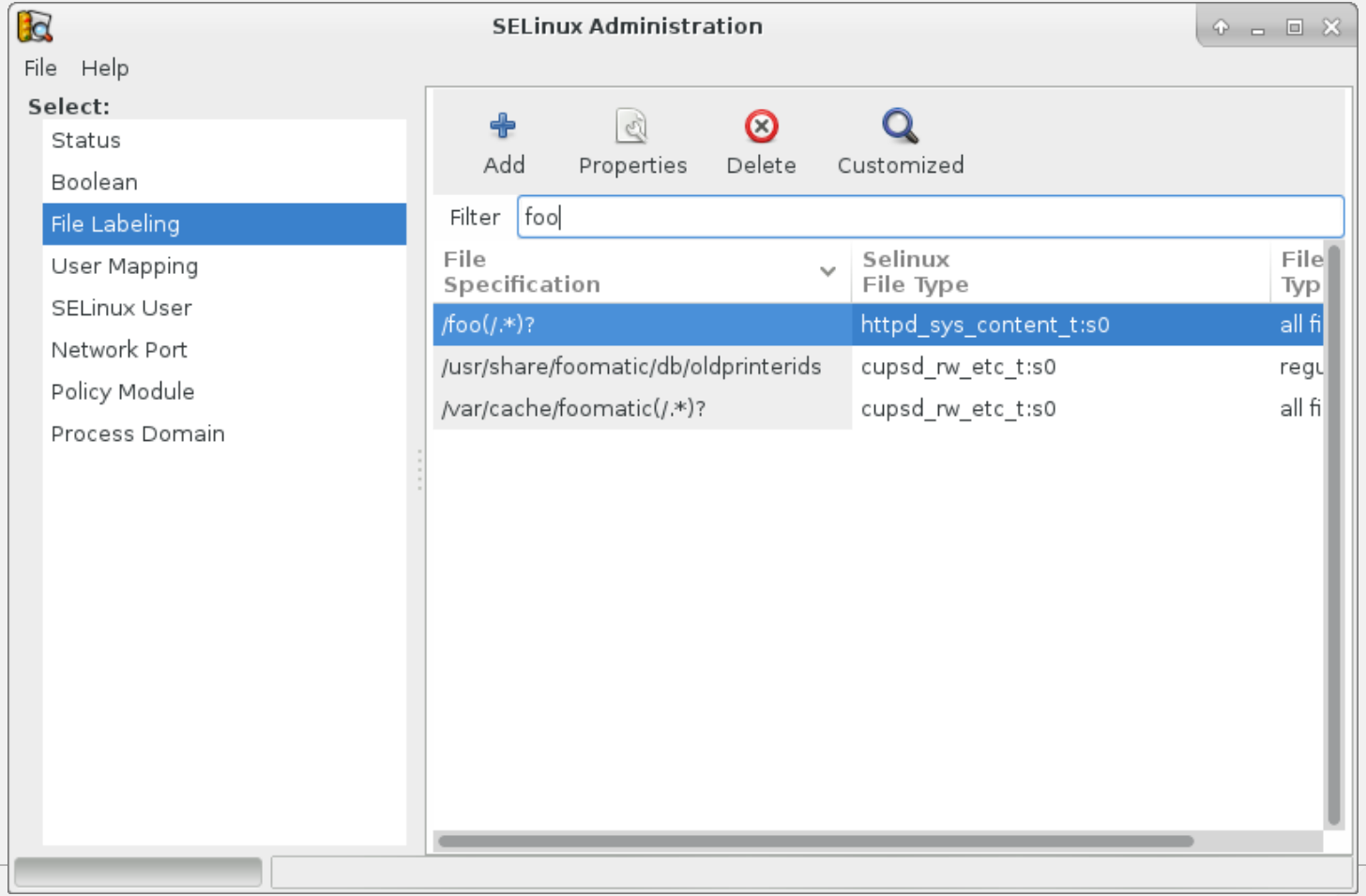
File Edit View Terminal Tabs Help

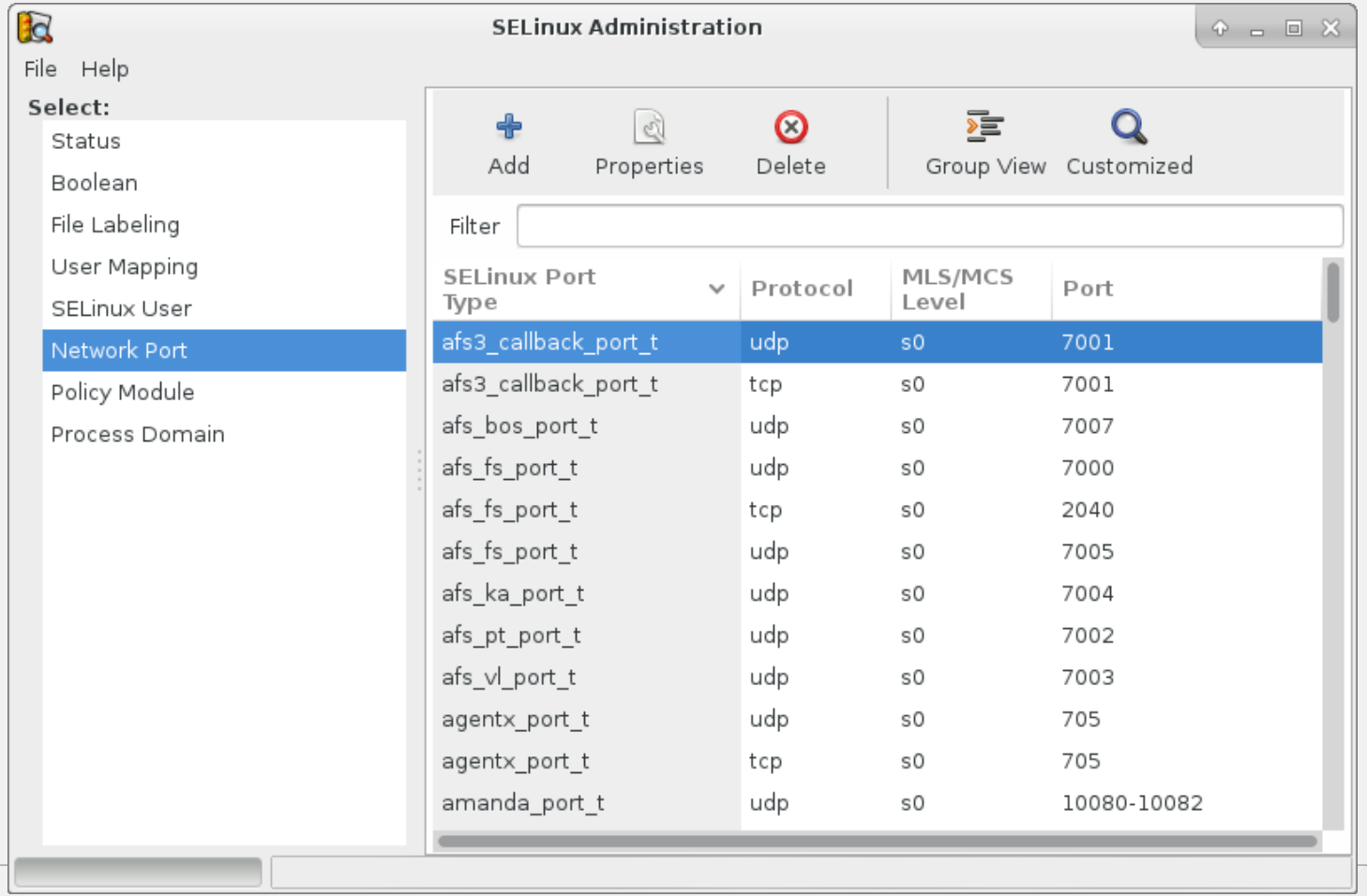
```
Last login: Mon Jun 27 18:07:04 2016 from w541.tc.redhat.com
This is a private system. Trespassers will be violated!
/usr/bin/xauth:  file /root/.Xauthority does not exist
.[root@gluster-dev-aus-001 ~]# system-config-selinux
GConf Error: Client failed to connect to the D-BUS daemon:
/bin/dbus-launch terminated abnormally without any error message
/usr/share/system-config-selinux/system-config-selinux.py:77: Warning: g_object_
get_valist: object class 'GnomeProgram' has no property named 'default-icon'
  xml = gtk.glade.XML ("/usr/share/system-config-selinux/system-config-selinux.g
lade", domain=PROGNAME)
GConf Error: Client failed to connect to the D-BUS daemon:
/bin/dbus-launch terminated abnormally without any error message
GConf Error: Client failed to connect to the D-BUS daemon:
/bin/dbus-launch terminated abnormally without any error message
GConf Error: Client failed to connect to the D-BUS daemon:
/bin/dbus-launch terminated abnormally without any error message
GConf Error: Client failed to connect to the D-BUS daemon:
/bin/dbus-launch terminated abnormally without any error message
GConf Error: Client failed to connect to the D-BUS daemon:
/bin/dbus-launch terminated abnormally without any error message
GConf Error: Client failed to connect to the D-BUS daemon:
/bin/dbus-launch terminated abnormally without any error message
GConf Error: Client failed to connect to the D-BUS daemon:
/bin/dbus-launch terminated abnormally without any error message
```

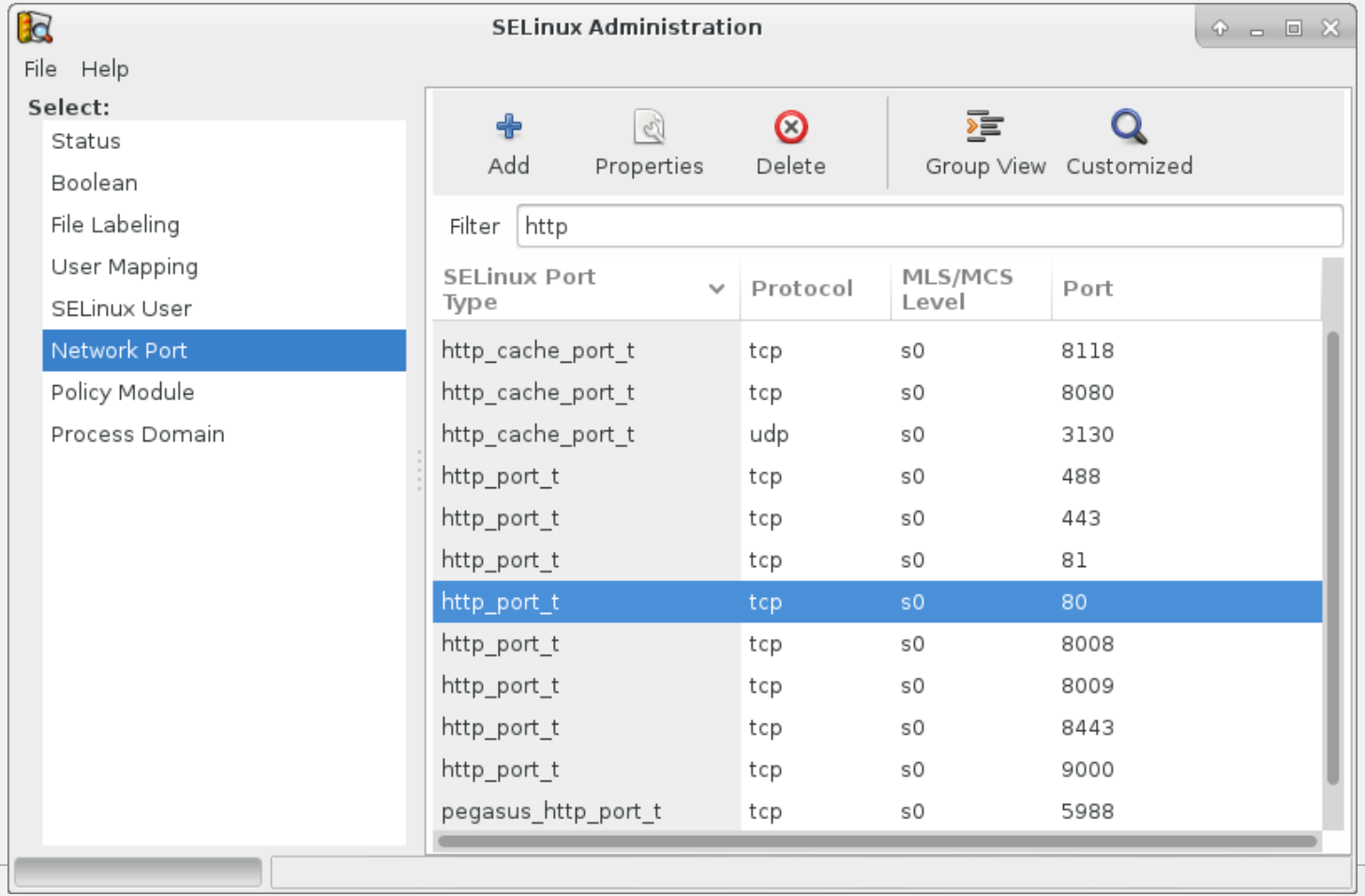

SELinux Administration
File Help
Select:
Status
Boolean
File Labeling
User Mapping
SELinux User
Network Port
Policy Module
Process Domain
System Default Enforcing Mode
Permissive
Current Enforcing Mode
Permissive
System Default Policy Type:
targeted
Relabel on next reboot.

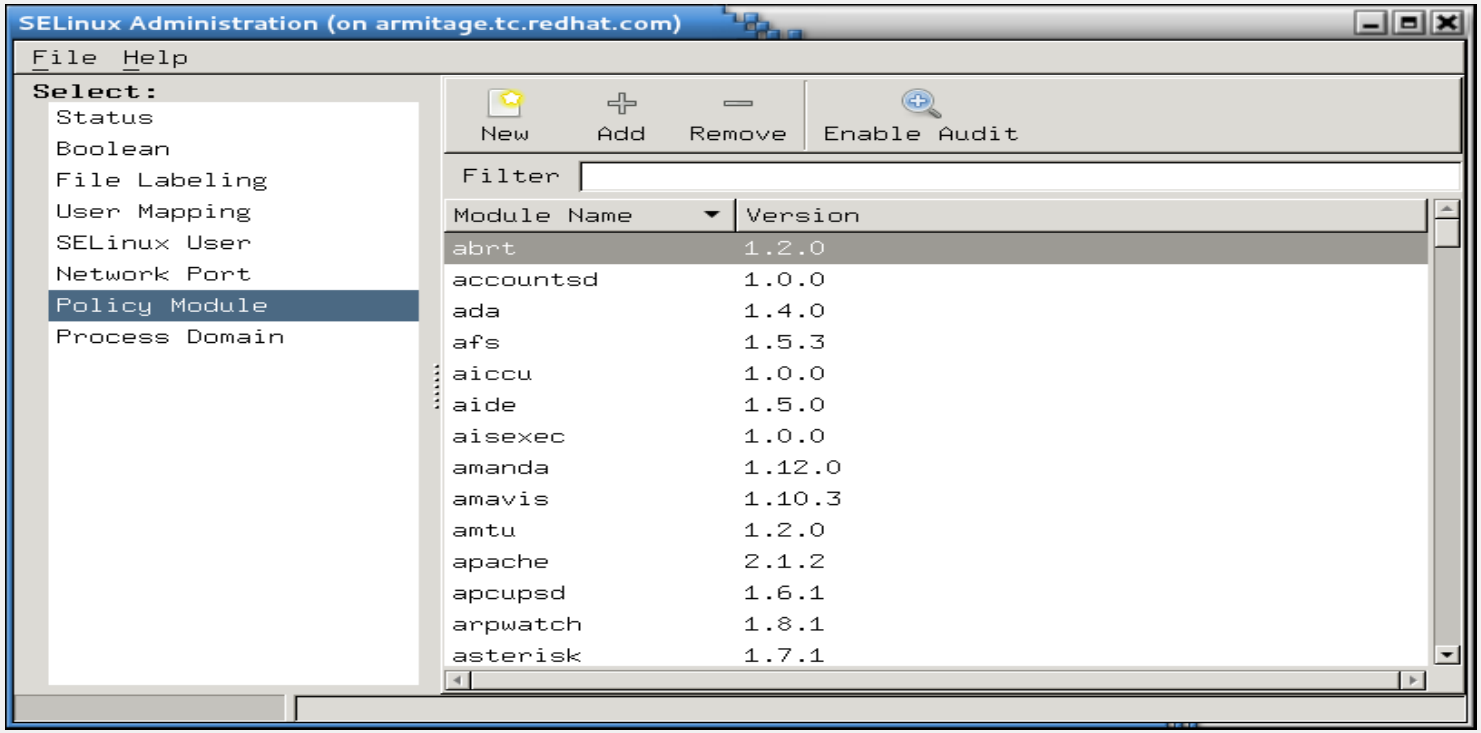

SELinux Administration
File Help
Select:
Status
Boolean
File Labeling
User Mapping
SELinux User
Network Port
Policy Module
Process Domain
Revert
Customized
Filter
Active
Module
Description
abrt
Determine whether abrt-handle-upload
abrt
Determine whether ABRT can run in th
abrt
Allow ABRT to modify public files us
antivirus
Determine whether can antivirus prog
antivirus
Allow antivirus programs to read non
apache
Allow httpd to access cifs file syst
apache
Allow Apache to modify public files
apache
Dontaudit Apache to search dirs.
apache
Allow Apache to query NS records
apache
Allow httpd cgi support
apache
Allow Apache to communicate with sss
apache
Allow httpd to run gpg
apache
Allow HTTPD scripts and modules to c

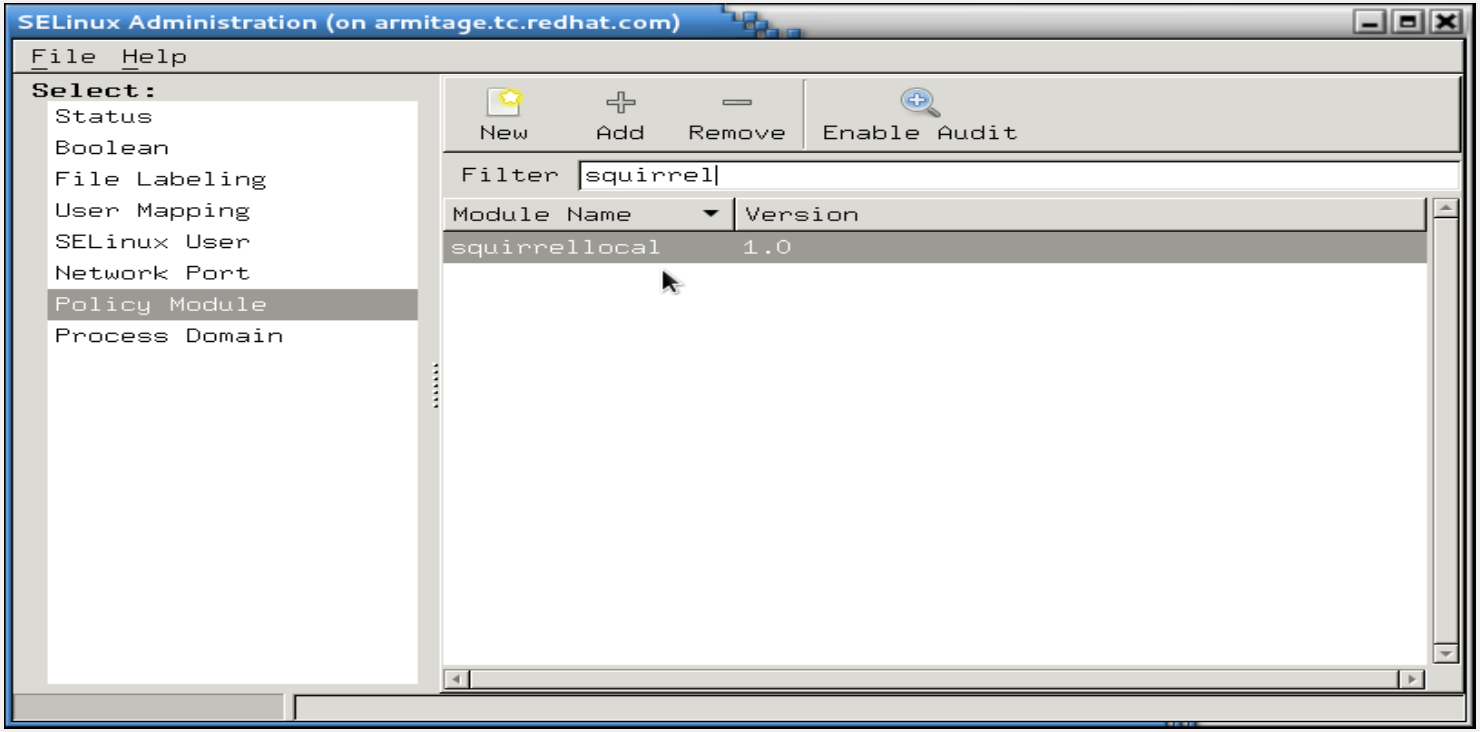

SELinux Administration
File Help
Select:
Status
Boolean
File Labeling
User Mapping
SELinux User
Network Port
Policy Module
Process Domain
Add
Properties
Delete
Customized
Filter
File Specification
Selinux File Type
File Type
/ root_t:s0
/.* default_t:s0
/[^/]+ etc_runtime_t:s0
/afs mnt_t:s0
/a?quota\.(user|group) quota_db_t:s0
/\.autofsck etc_runtime_t:s0
/\.autorelabel etc_runtime_t:s0
/bacula(/.*)? bacula_store_t:s0
/bin bin_t:s0
/bin/.* bin_t:s0
/bin/alsaunmute alsa_exec_t:s0
/bin/bash shell_exec_t:s0
/bin/bash2 shell_exec_t:s0


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 Typ
/foo(/.*)?
httpd_sys_content_t:s0
all fi
/usr/share/foomatic/db/oldprinterids
cupsd_rw_etc_t:s0
regu
/var/cache/foomatic(/.*)?
cupsd_rw_etc_t:s0
all fi


SELinux Administration
File
Help
Select:
Status
Boolean
File Labeling
User Mapping
SELinux User
Network Port
Policy Module
Process Domain
Add
Properties
Delete
Group View
Customized
Filter
SELinux Port Type
Protocol
MLS/MCS Level
Port
afs3_callback_port_t udp s0 7001
afs3_callback_port_t tcp s0 7001
afs_bos_port_t udp s0 7007
afs_fs_port_t udp s0 7000
afs_fs_port_t tcp s0 2040
afs_fs_port_t udp s0 7005
afs_ka_port_t udp s0 7004
afs_pt_port_t udp s0 7002
afs_vl_port_t udp s0 7003
agentx_port_t udp s0 705
agentx_port_t tcp s0 705
amanda_port_t udp s0 10080-10082


SELinux Administration
File
Help
Select:
Status
Boolean
File Labeling
User Mapping
SELinux User
Network Port
Policy Module
Process Domain
Add
Properties
Delete
Group View
Customized
Filter
http
SELinux Port Type
Protocol
MLS/MCS Level
Port
http_cache_port_t tcp s0 8118
http_cache_port_t tcp s0 8080
http_cache_port_t udp s0 3130
http_port_t tcp s0 488
http_port_t tcp s0 443
http_port_t tcp s0 81
http_port_t tcp s0 80
http_port_t tcp s0 8008
http_port_t tcp s0 8009
http_port_t tcp s0 8443
http_port_t tcp s0 9000
pegasus_http_port_t tcp s0 5988


SELinux Administration (on armitage.tc.redhat.com)
File Help
Select:
Status
Boolean
File Labeling
User Mapping
SELinux User
Network Port
Policy Module
Process Domain
New
Add
Remove
Enable Audit
Filter
Module Name
Version
abrt 1.2.0
accountsd 1.0.0
ada 1.4.0
afs 1.5.3
aiccu 1.0.0
aide 1.5.0
aisexec 1.0.0
amanda 1.12.0
amavis 1.10.3
amtu 1.2.0
apache 2.1.2
apcupsd 1.6.1
arpwatch 1.8.1
asterisk 1.7.1


SELinux Administration (on armitage.tc.redhat.com)
File Help
Select:
Status
Boolean
File Labeling
User Mapping
SELinux User
Network Port
Policy Module
Process Domain
New
Add
Remove
Enable Audit
Filter
squirrel
Module Name
Version
squirrellocal
1.0

CONCLUSION

Hopefully you feel like this, 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 years ago
- NSA grade security is available at no extra cost - use it!

Thank You!

- If you liked today's presentation, please rate it!

More Information

- SELinux Guide: https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/7-Beta/html/SELinux_Users_and_Administrators_Guide/index.html
- Fedora Project SELinux Docs: http://fedoraproject.org/wiki/SELinux
- fedora-selinux-list (mailing list):
  - https://www.redhat.com/mailman/listinfo

More Information

- http://access.redhat.com has several videos about SELinux. Dave Egts and Dan Walsh have covered topics from confining users to sandboxing.
- Dan Walsh's blog:
  - http://danwalsh.livejournal.com/

RED HAT SUMMIT

THANK YOU


plus.google.com/+RedHat


facebook.com/redhatinc


linkedin.com/company/red-hat


twitter.com/RedHatNews


youtube.com/user/RedHatVideos

LEARN. NETWORK.
EXPERIENCE
OPEN SOURCE.