**Use boolean settings to modify system SELinux settings.**

**Presentation**

**SELinux** uses booleans to makes its policy more flexible.

The basic policy is pretty strict but suits most requirements. But if you’ve got special needs, you can easily adjust it thanks to the **SELinux** booleans.

**Standard Management**

Get the list of **SELinux** booleans on a particular topic (here **ftp**):

# getsebool -a | grep **ftp**

allow\_ftpd\_anon\_write --> off

allow\_ftpd\_full\_access --> on

allow\_ftpd\_use\_cifs --> off

allow\_ftpd\_use\_nfs --> off

ftp\_home\_dir --> on

ftpd\_connect\_db --> off

ftpd\_use\_fusefs --> off

ftpd\_use\_passive\_mode --> off

httpd\_enable\_ftp\_server --> off

tftp\_anon\_write --> off

tftp\_use\_cifs --> off

tftp\_use\_nfs --> off

To set a specific **SELinux** boolean according to your need (here **ftp\_home\_dir**), type:

# setsebool -P **ftp\_home\_dir** on

or

# yum install -y **setroubleshoot-server**

# semanage boolean -m --on **ftp\_home\_dir**

Note1: You can use **on** or **1**, **off** or **0** with the **setsebool** command.  
Note2: The **-P** option means **P**ermanent. If you don’t use it, the boolean will restore its previous permanent or default configuration after the next reboot.  
Note3: The **semanage boolean** command only assigns permanent configurations.

To get a more detailed list of **SELinux** booleans, type:

# yum install -y **setroubleshoot-server**

# semanage boolean -l

SELinux boolean                State  Default Description

ftp\_home\_dir                   (off  ,  off)  Allow ftp to read and write files in the user home directories

smartmon\_3ware                 (off  ,  off)  Enable additional permissions needed to support devices on 3ware controllers.

xdm\_sysadm\_login               (off  ,  off)  Allow xdm logins as sysadm

xen\_use\_nfs                    (off  ,  off)  Allow xen to manage nfs files

mozilla\_read\_content           (off  ,  off)  Control mozilla content access

ssh\_chroot\_rw\_homedirs         (off  ,  off)  Allow ssh with chroot env to read and write files in the user home directories

postgresql\_can\_rsync           (off  ,  off)  Allow postgresql to use ssh and rsync for point-in-time recovery

allow\_console\_login            (on   ,   on)  Allow direct login to the console device. Required for System 390

spamassassin\_can\_network       (off  ,  off)  Allow user spamassassin clients to use the network.

authlogin\_shadow               (off  ,  off)  Allow users login programs to access /etc/shadow.

httpd\_can\_network\_relay        (off  ,  off)  Allow httpd to act as a relay

openvpn\_enable\_homedirs        (on   ,   on)  Allow openvpn to read home directories

...

**Important note**: The **State** column respectively shows the **current** boolean configuration and the **Default** column the **permanent** boolean configuration.

To get the list of all the **SELinux** booleans with a current value different from the **default** one (**-C** option for local **C**ustomization), type:

# semanage boolean -l -C

SELinux boolean State Default Description

ftp\_home\_dir (on , on) Allow ftp to read and write files in the user home directories

httpd\_can\_sendmail (on , on) Allow http daemon to send mail

allow\_postfix\_local\_write\_mail\_spool (on , on) Allow postfix\_local domain full write access to mail\_spool directories

allow\_ftpd\_full\_access (on , on) Allow ftp servers to login to local users and read/write all files on the system, governed by DAC.

To display the list of **SELinux** booleans related to **NFS**, type:

# semanage boolean -l | egrep "nfs|SELinux"

SELinux boolean State Default Description

xen\_use\_nfs (off , off) Allow xen to use nfs

virt\_use\_nfs (off , off) Allow virt to use nfs

mpd\_use\_nfs (off , off) Allow mpd to use nfs

nfsd\_anon\_write (off , off) Allow nfsd to anon write

ksmtuned\_use\_nfs (off , off) Allow ksmtuned to use nfs

git\_system\_use\_nfs (off , off) Allow git to system use nfs

virt\_sandbox\_use\_nfs (off , off) Allow virt to sandbox use nfs

logrotate\_use\_nfs (off , off) Allow logrotate to use nfs

git\_cgi\_use\_nfs (off , off) Allow git to cgi use nfs

cobbler\_use\_nfs (on , off) Allow cobbler to use nfs

httpd\_use\_nfs (off , off) Allow httpd to use nfs

sge\_use\_nfs (off , off) Allow sge to use nfs

ftpd\_use\_nfs (off , off) Allow ftpd to use nfs

sanlock\_use\_nfs (off , off) Allow sanlock to use nfs

samba\_share\_nfs (off , off) Allow samba to share nfs

openshift\_use\_nfs (off , off) Allow openshift to use nfs

polipo\_use\_nfs (off , off) Allow polipo to use nfs

use\_nfs\_home\_dirs (off , off) Allow use to nfs home dirs

nfs\_export\_all\_rw (on , on) Allow nfs to export all rw

nfs\_export\_all\_ro (on , on) Allow nfs to export all ro