Table Of Contents

Table Of Contents 1
How Do I Enable SELinux under Redhat / Fedora and CentOS Linux Systems? 2
Understanding SELinux Configuration 2
Prepare File System For The Reboot 2
Restore Default Security Contexts 2
Relabel Complete Filesystem 2
Make Sure SELinux is Properly Enabled 3
How Do I Print Full List Of Allowed Network Ports? 3
How Do I Allow Lighttpd / Apache / Nginx At Port 8181? 3
How Do I Find Out Unprotected Services? 3
How Do I See SELinux Labels? 3
Troubleshooting SELinux Policy Errors 3
Recommended readings: 4

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

CentOS / Redhat: Turn On SELinux Protection

Posted by Vivek Gite <vivek@nixcraft.com>


[1]

SELinux enforces the idea that programs should be limited in what files they can access and what actions they can take. However, by default it is turned off under RHEL / CentOS 5.x server? How do I turn it on?

SELinux is a kernel security extension, which can be used to guard against misconfigured or compromised programs. It comes with Mandatory Access Control (MAC) system that improves the traditional UNIX/Linux DAC (Discretionary Access Control) model.

How Do I Enable SELinux under Redhat / Fedora and CentOS Linux Systems?

Edit /etc/selinux/config file, run:


[2]

```
# vi /etc/selinux/config
```

Update the configuration file as follows:

```
SELINUX=enforcing
SELINUXTYPE=targeted
```

Understanding SELinux Configuration

- **SELINUX=enforcing** : Enforcing is the default mode which will enable and enforce the SELinux security policy on the Linux. It will also deny unauthorized access and log actions in a log file.
- **SELINUXTYPE=targeted** : Only targeted network daemons (such as DNS, Apache and others) are protected.

Save and close the file. Make sure SELinux is not disabled using Grub boot loader. Search /boot/grub/grub.conf file using grep and make sure the following line DO NOT appears:

```
# egrep -i 'selinux=0|enforcing=0' /boot/grub/grub.conf
```

If you found lines with **selinux=0** or **enforcing=0**, remove them and save the changes.

Prepare File System For The Reboot

The chcon command can be used to change SELinux security context of a file. However, it is recommended that you relabel complete filesystem.

Restore Default Security Contexts

Type the following command to restore default security contexts for /home:

```
# restorecon -Rv -n /home
```

You can run this on root (/) file system too.

Relabel Complete Filesystem

Do not skip this step and reboot the system. Type the following commands:

```
# touch /.autorelabel
```

```
# reboot
```

It will take some time to relabel complete filesystem. If you get any errors or common services mysqld or sshd failed, try the following solution (go to a single user mode):

```
# init 1
# genhomedircon
# touch /.autorelabel
# reboot
```

Make Sure SELinux is Properly Enabled

Type the following command:

```
# sestatus
```

Sample outputs:

```
SELinux status:                 enabled
SELinuxfs mount:                /selinux
Current mode:                   enforcing
Mode from config file:          enforcing
Policy version:                 21
Policy from config file:        targeted
```

How Do I Print Full List Of Allowed Network Ports?

Type the following commands

```
# semanage port -l
# semanage port -l | less
#### look for port 80 ####
# semanage port -l | grep -w 80
```

How Do I Allow Lighttpd / Apache / Nginx At Port 8181?

By default SELinux will block access to many ports including 8181. You need to allow access to a port # 8181 so that it can bind and listen for incoming requests on non privileged ports. You need to use the semanage command as follows:

```
# semanage port -a -t http_port_t -p tcp 8181
```

How Do I Find Out Unprotected Services?

Type the following command:

```
# ps -eZ | egrep "initrc" | egrep -vw "ps|tr|egrep|awk|bash" | tr ':' ' ' | awk '{ print
$NF }'
```

You should not see any output on fully configured SELinux systems.

How Do I See SELinux Labels?

Type the following command:

```
# ls -lZ /path/to/file
# ls -lZd /path/to/dir
# ls -lZd /etc
# ls -lZ /dev/ | grep deviceName
# ls -lZ /etc/resolv.conf
```

Sample outputs:

```
-rw-r--r--  root root system_u:object_r:net_conf_t      /etc/resolv.conf
```

Troubleshooting SELinux Policy Errors

SELinux is pretty complicated kernel software. It takes time to fix error. Use the following tools to find and debug SELinux policy problems (refer to your local man pages):

- ps -Z -p PID
- ls -Z fileName
- ausearch
- restorecon
- semodule
- audit2allow
- Log files: /var/log/audit/audit.log and /var/log/setroubleshoot/setroubleshootd.log

Recommended readings:

- Introduction to the Red Hat SELinux Guide [3]