SELinux

SELinux is a form of Mandatory Access Control. Well, when we say, many are immediately intimidated so let's start off by saying that SELinux is simply a labeling system.

A label gives you authority. Let's have a look at this basic organogram for Heroes, Inc

Person	Label
Peter Parker	Reception
Bruce Wayne	Plumber
Clarke Kent	CEO

Does Peter Parker have the ability to answer the company telephone?

Well, yes. It's a basic task which most can perform.

Does Peter Parker have the authority to answer the company telephone?

Here we differentiate between ability and authority. Because of the label which Peter Parker has, he has the authority to answer the company telephone. Should the CEO, Clarke Kent walk by and see Peter Parker doing so, he would not bat an eyelid as everything is as it should be.

Now let's introduce Bruce Wayne.

Does Bruce Wayne have the ability to answer the company telephone?

Well, of course. No problem with his ability.

But …

Does Bruce Wayne have the authority to answer the company telephone?

Definitely not because his label doesn't allow for it and with the CEO of the company around enforcing all the rules (in other words, the rules are mandatory), he simply cannot perform that particular action.

Well SELinux is like the CEO of your system, enforcing all the rules associated with labels.

Technically, they're not called labels, they're called contexts but they're really the same thing. Everything in your system has a label … I mean context!

- Users
- Processes
- Files
- Directories
- TCP/IP ports

A context is divided up into 5 components with a colon separating each one.

USER CONTEXT	ROLE CONTEXT	TYPE CONTEXT	SENSITIVITY CONTEXT	CATEGORY CONTEXT

It will take time for you to learn about the 'abilities' associated with the various contexts and more information is always available in man pages.

At this stage we will only focus on the type context. No need to be concerned with the user, role, sensitivity nor category contexts.

Identifying contexts is easy:

USER CONTEXT	ROLE CONTEXT	TYPE CONTEXT	SENSITIVITY CONTEXT	CATEGORY CONTEXT
ends in _u	ends in _r	ends in _t	starts with s	starts with c

The -Z option is generally used to query SELinux elements.

Examples

To see the context of your user account:

```
# id -Z
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

To see the context of a file:

```
# ls -lZ /etc/fstab
-rw-r--r--. root root system_u:object_r:etc_t:s0        /etc/fstab
```

To see the context of a directory:

```
# ls -ldZ /var/
drwxr-xr-x. root root system_u:object_r:var_t:s0     /var/
```

To see the context of TCP ports:

```
# semanage port -l
SELinux Port Type             Proto   Port Number

afs_bos_port_t                udp     7007
afs_client_port_t             udp     7001
afs_fs_port_t         tcp     2040
afs_fs_port_t         udp     7000, 7005
afs_ka_port_t         udp     7004
afs_pt_port_t         udp     7002

---truncated---
```

SELinux may operate in 3 different modes:

- enforcing
- permissive
- disabled

Enforcing mode:

All the rules are applied and may not be broken. While this offers you the best protection, unless you've setup your contexts correctly for other services, things may not work as expected. This is the mode which you eventually want to be at.

Permissive mode:

All the rules are loaded and active but when a rule is broken, SELinux does not block the transaction. Transactions are allowed but any violations are logged so that the administrator may take remedial action. This is the mode you should probably move to immediately.

Disabled mode:

The rules are not loaded, are not active. SELinux effectively doesn't exist on your system. There is no protection, there are no logs of violations. You have nothing. You are probably at this mode currently but should not use it.

Changing your SELinux mode can be done only if you're NOT in disabled mode.

To view your current SELinux mode:

```
# getenforce
Permissive
```

To change from permissive to enforcing:

```
# setenforce enforcing
```

or

```
# setenforce 1
```

To change from enforcing to permissive:

```
# setenforce permissive
```

or

```
# setenforce 0
```

Not that the setenforce command is not persistent as persistency for SELinux is defined in the configuration file /etc/selinux/config

```
# 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 two values:
#         targeted - Targeted processes are protected,
#         mls - Multi Level Security protection.
```

Based on the output above, SELinux will operate in enforcing mode whenever my server boots up.

Should you wish to change from either enforcing or permissive modes to disabled, you can only do so via the configuration file /etc/selinux/config and a reboot is required. When doing the reverse, the same rule applies. This will give the SELinux database the change to reinitialize.

Changing the context of a file or directory can be done using the chcon command but we would prefer to teach you about the semanage command. The reason being that SELinux stores mappings between files & directories and their contexts in a database. This database is only modified when you use the semanage command. The chcon command will modify the mappings for you but when the SELInux database is reinitialized, your mappings will be lost.

```
# mkdir /web_data
# ls -ldZ /web_data
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 /web_data
```

As you can see, the type context is default_t.

To change it from default_t to httpd_sys_content_t you could use either chcon or semanage.

Using chcon is easy:

```
# chcon -t httpd_sys_content_t /web_data
# ls -ldZ /web_data
drwxr-xr-x. root root unconfined_u:object_r:httpd_sys_content_t:s0 /web_data
```

So the syntax is: chcon -t *specify_the_type_context* *specify_file_or_directory*

!!! NOTE !!!

Using the chcon command does not add the context mappings to the SELinux database so while it may survive a reboot, it will not survive a relabel.

Using semanage is a little more complex.

semanage is not usually installed by default as is part of the policycoreutils-python package.

Firstly, we need to add the mapping specifying which context gets allocated to which directory.

```
# semanage fcontext -a -t httpd_sys_content_t /web_data'(/.*)?'
```

Let’s dissect what’s happening here:

semanage	fcontext	-a	-t	httpd_sys_content_t	/web_data’(/.*)?’

1	2	3	4	5	6

1. This is our semanage command
2. The SELinux database consists of different sections, the one which deals with file and directory contexts is called fcontext
3. We're doing an add operation
4. The operation affects the type context
5. We're allocating the context httpd_sys_content_t
6. The mapping applies to the /web_data directory and all children below /web_data as indicated by the regular expression '(/.*)?'

Secondly, we need to restore the mapping as specified in the SELinux database to the directory /web_data.

```
# restorecon -vFR /web_data/
restorecon reset /web_data context unconfined_u:object_r:httpd_sys_content_t:s0-
>system_u:object_r:httpd_sys_content_t:s0
```

SELinux also has a section of the database for booleans. Booleans turn things on or off.

To see all the booleans use the command:

```
# 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

---truncated---
```

That's quite a bit so we will use grep to filter out only those lines containing the pattern ftp.

```
# semanage boolean -l | grep ftp
ftp_home_dir             (off  ,  off)  Allow ftp to read and write files in the user home
directories
tftp_anon_write                  (off  ,  off)  Allow tftp to modify public files used for public file
transfer services.
allow_ftpd_full_access         (off  ,  off)  Allow ftp servers to login to local users and read/
write all files on the system, governed by DAC.
allow_ftpd_use_cifs             (off  ,  off)  Allow ftp servers to use cifs used for public file
transfer services.
allow_ftpd_use_nfs              (off  ,  off)  Allow ftp servers to use nfs used for public file
transfer services.
allow_ftpd_anon_write         (off  ,  off)  Allow ftp servers to upload files,  used for public
file transfer services. Directories must be labeled public_content_rw_t.
ftpd_use_passive_mode        (off  ,  off)  Allow ftp servers to use bind to all unreserved ports
for passive mode
ftpd_connect_db                  (off  ,  off)  Allow ftp servers to use connect to mysql database
httpd_enable_ftp_server       (off  ,  off)  Allow httpd to act as a FTP server by listening on
the ftp port.
```

The 2 values in brackets specify that the boolean is off now and is also persistently set off.

To enable a boolean simple run the setsebool command as follows.

```
# setsebool ftp_home_dir on
```

The above command enabled the boolean but it is not persistent.

```
# semanage boolean -l | grep ftp_home_dir
ftp_home_dir             (on   ,  off)  Allow ftp to read and write files in the user home
directories
```

To enable persistency for a boolean use the setsebool command as follows:

```
# setsebool -P ftp_home_dir on
# semanage boolean -l | grep ftp_home_dir
ftp_home_dir             (on   ,   on)  Allow ftp to read and write files in the user home
directories
```

Managing violations

Violations are typically sent to /var/log/messages but you can enhance your SELinux experience by running the setroubleshoot-server

```
# yum install -y setroubleshoot-server
# setroubleshootd
```

Lab activity

Record the contexts of the following files and directories:

/usr/share/doc/	
/etc/crypttab	
/home/	

What is the current SELinux mode?

Change it to Enforcing and reboot your system. Observe what happens.