AINUX

TASTE OF LINUX

WELCOME TO THE WORLD OF LINUX

DAY - 5

CREATED BY : ARYAN M.P

Managing SELinux Security

Security Enhanced Linux (SELinux) is an additional layer of system security. A primary goal of SELinux is to protect user data from system services that have been compromised.

In Linux there are two types of ACCESS CONTROL Mechanism

1. *Discretionary Access control.*
2. *Mandatory Access control.*

1. **Discretionary Access control**: - It's based on user's mind. Means if user wants to give the permission then they can, if not then they block the access by 'chmod' utility.
2. **Mandatory Access control: -** It's based on the predefined policies. It's mainly works on the system processes.

SELinux Context:- SElinux is a set of security rules that determine which process can access which files, directories and ports. Every file, process, directory and port has a special security label called a "SELinux Context".
Note:- You can see the SELinux context of a directory through **"# ll –dZ /etc**"

```
drwxr-xr-x. root  root system_u:object_r:etc_t:s0      etc
    1      | 2   | 3 |  4      |  5    |  6 | 7  |  8
```

Managing SELinux Security

1 - Shows Permission of the file
2 - Shows the file owner
3 - Shows the group owner
4 - Shows ‘system user’
5 - Shows ‘System Role’
6 - Type or Target
7 - Shows security level
8 - Directory or file

SELinux mode of operation

1. Target policy
2. Multi Level Security (MLS)

Note: -

- A file’s SELinux context will be same as its parent folder context.
- By default SELinux does not prevent to access if the SELinux context is same. Other wise it will block the access.
- System created directories SELinux context are predefined. Like /root, /etc, /tmp etc...

Managing SELinux Security

Note: -

- Every process also have it’s own context.

  Now we can see the context of httpd process by ‘**ps –auxZ | grep httpd**’

  “system_u:system_r:httpd_t:s0 root 2768 /usr/sbin/httpd –DFOREGROUND”

  Here we can see the context of httpd process is **‘httpd_t’**. So is can access the directories which has the context started with **‘httpd’. Like ‘/var/www/html’, ‘/etc/httpd’, ‘/var/log/httpd’.** But httpd process not be able to access if the context will be different. Means httpd process not be able to access which context lebel is ‘**admin_home_t**’ or ‘**etc_t**’ etc.
- All these rules are predefined into policies.

SELinux Modes

1. **Enforcing mode :-** In enforcing mode, SELinux actively denies access to the web server attempting to read files with ‘tmp_t’ type context. In enforcing mode, SELinux both logs and protects.
2. **Permissive mode :-** Permissive mode is often used to trouble shoot issues. In permissive mode, SELinux allows all interactions, and it logs those interactions
3. **Disabled mode :-** Disabled, completely disables SELinux. A system reboot is required to disable SELinux entire ly, or to get from disabled mode to enforcing or permissive mode.

CREATED BY : ARYAN M.P

AINUX
TASTE OF LINUX

Managing SELinux Security

To check SELinux status

```
# getenforce
```

To Set SELinux in enforcing mode (Temporarily–means after next restart it takes default)

```
# setenforce  1                [permissive = 0   |   Enforcing = 1]
```

To check SELinux log

1. #cat /var/log /messages | grep httpd | less   [sealert -l 8alert-Number]
2. In Graphical go to ‘**Sundry**’ → ‘SELinux Troubleshooter’

To change the context (Temporarily change the context)

```
#chcon  -R  -t  “context-type”  “Dir-name”
```

Example:-   #chcon -R -t “httpd_sys_content_t” “/webdata”

Note:- Temporarily means, when SELinux restoring the context, then it applies the default context again. Or if you have ‘.autorelabel’ file into your ‘/’ the it also restore context after next reboot.

To restore your SELinux context

Managing SELinux Security

To change the context (Permanently change the context)

```
#semanage  fcontext  -a -t  “context-type”  “Dir-name”
```

Example:-

```
#semanage  fcontext  -a  -t  “httpd_sys_content_t”  “/webdata”
```

Note:-

After executing ‘**semanage**’ command, you can check below mentioned file to check the policy. ‘**/etc/selinux/targeted/contexts/files/file_contexts.local**’. And after that you need to run “**restorecon**” command for automatically labelling.

SELinux Booleans

SELinux Booleans are switches that change the behavior of that SELinux policy. SELinux Booleans are rules that can be enabled or disabled.

To display SELinux Booleans list

```
# getsebool  -a
```

To search particular SELinux Booleans

```
# getsebool  -a | grep “service-name”
```

Example: -

```
# getsebool  -a | grep “ftp”
```

Managing SELinux Security

To display SELinux Booleans list with details

```
# semanage  boolean  -l
```

To search particular SELinux Booleans with details

```
# semanage  boolean  -l | grep “service-name”
```

Example:- #semanage boolean -l | grep “ftp”

To set boolean

```
# setsebool  -P  ‘Boll-name’  1
```

Example:- # setsebool -P ftpd_full_access 1

To Set SELinux in enforcing mode (Permanently)

```
# vim  /etc/sysconfig/selinux
```

Then change the mode “SELINUX=enforcing”

To display SELinux status

```
# sestatus
```

CREATED BY : ARYAN M.P

AINUX

—TASTE OF LINUX—

THANK YOU

CREATED BY : ARYAN M.P