

SELinux 사용



SELinux 소개

- ❖ object : 일반 파일, 디렉토리, 디바이스
- ❖ subject : 명령을 실행하는 사용자, 프로세스
- ❖ DAC : subject의 권한에 따라 모든 object에 접근 가능
- ❖ MAC : subject와 object에 label 들이 부여되어 규칙이 적용됨
- ❖ 대부분의 시스템은 DAC(Discretionary Access Control) 모델 사용
- ❖ SELinux 를 사용 시 MAC(Mandatory Access Control) 모델 사용
- ❖ DAC 모델이 적용된 후에 MAC 모델이 마지막으로 적용됨
- ❖ subject와 object에 부여되는 label 들을 context 라고 함
- ❖ subject와 object의 context 허용 규칙에 따라 접근을 제한

컨텍스트 system_u:object_r:httpd_sys_content_t:s0

사용자	역할	유형	민감도
system_u	object_r	httpd_sys_content_t	s0

SELinux 소개

❖ Context 확인

사용자 context 확인

```
[root@el7 ~]# id
uid=0(root) gid=0(root) groups=0(root)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

프로세스 context 확인

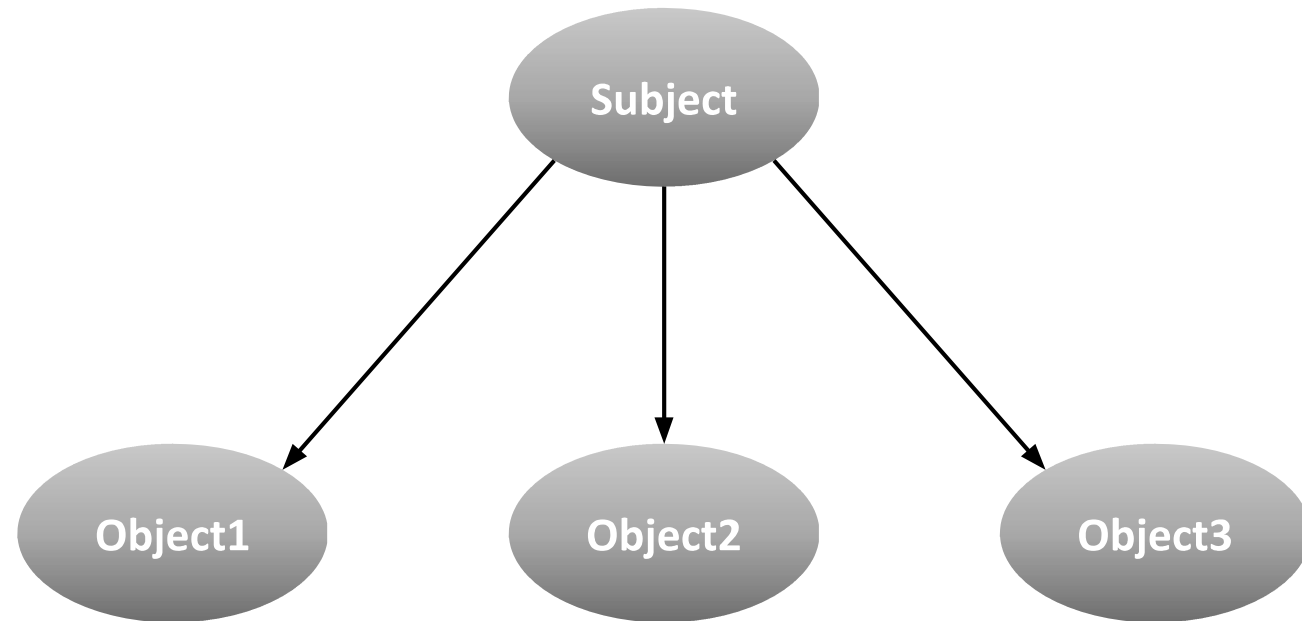
```
[root@el7 ~]# ps xZ | egrep '(LABEL|httpd)'
LABEL                                PID TTY STAT TIME COMMAND
system_u:system_r:httpd_t:s0 1971 ?    Ss   0:01 /usr/sbin/httpd -DFOREGROUND
```

파일 context 확인

```
[root@el7 ~]# ls -dZ /var/www/html/
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0
/var/www/html/
```

SELinux 모드

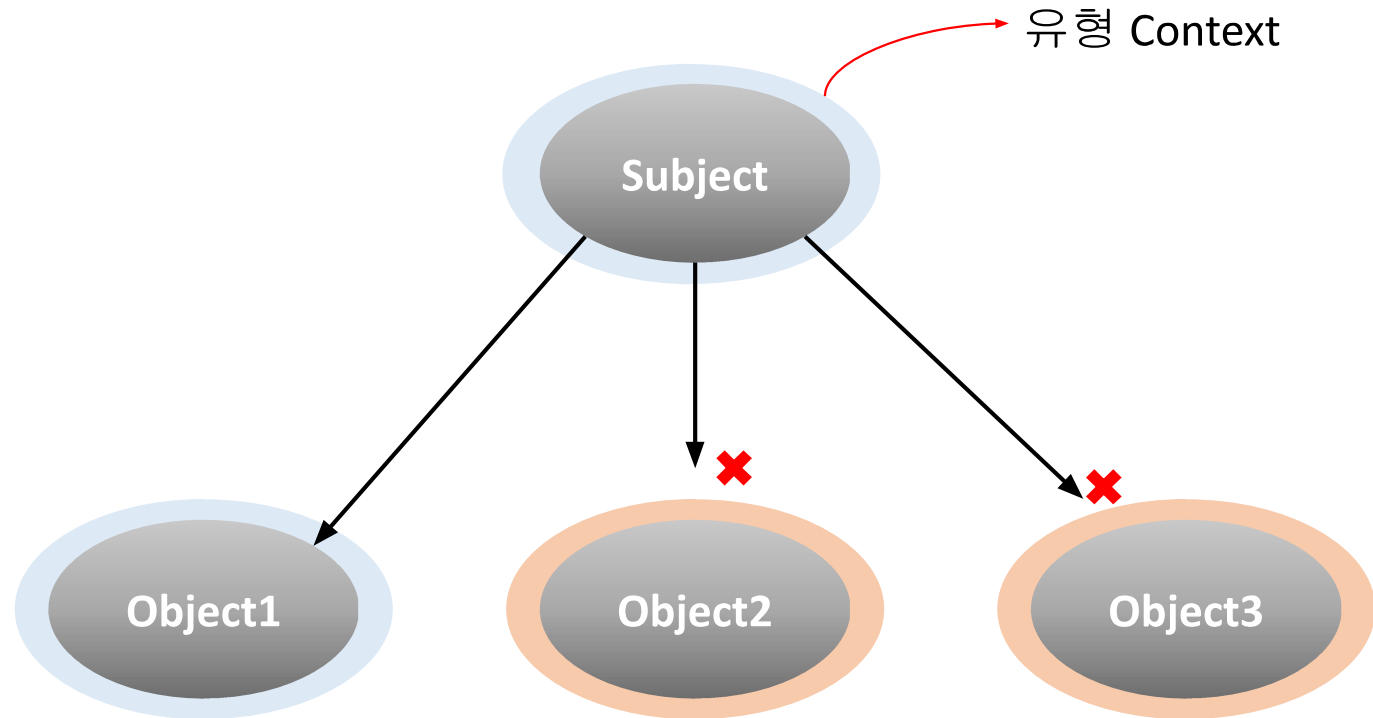
❖ Disabled 모드



- ❖ 시스템에서 완전히 종료된 상태
- ❖ 활성화를 위해서는 시스템을 재부팅 해야 함

SELinux 모드

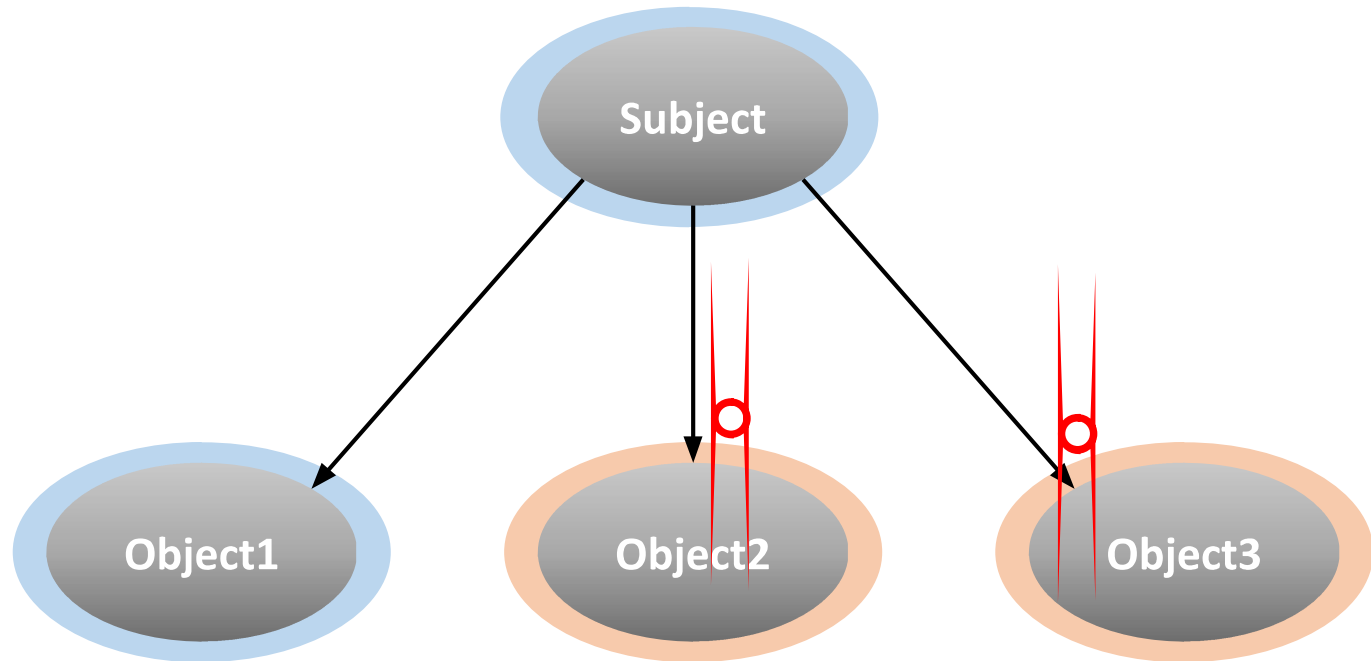
❖ Enforcing 모드



❖ 유형 context 에 따라 subject의 접근이 제한됨

SELinux 모드

❖ Permissive 모드



- ❖ SELinux 를 사용하지 않지만 커널에 저장되어 있는 상태
- ❖ 재부팅을 하지 않아도 SELinux 기능을 켤수있음

SELinux Context

- ❖ SELinux는 유형 context에 의해서 허용 규칙이 적용됨
- ❖ 초기의 context 는 상위 디렉토리의 context 상속 받음
 - ❖ mv 또는 cp -a 명령으로 파일을 복사하거나 이동할 경우 상속받지 않음

초기 context 예제

```
[root@el7 html]# ls -dZ .
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 .
[root@el7 html]# touch index.html
[root@el7 html]# ls -Z index.html
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0
index.html

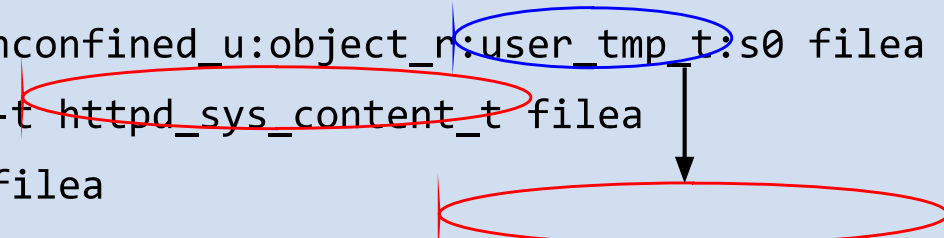
[root@el7 html]# touch /tmp/filea
[root@el7 html]# ls -Z /tmp/filea
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 /tmp/filea
[root@el7 html]# mv /tmp/filea /var/www/html/
[root@el7 html]# ls -Z filea
```

SELinux Context

- ❖ chcon 과 restorecon 명령을 통해 context를 변경
- ❖ chcon은 -t 옵션을 사용해 유형 context 를 명시적으로 지정
- ❖ restorecon은 상위 디렉토리의 유형 context 를 적용

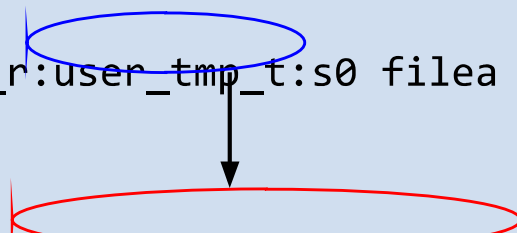
chcon 예제

```
[root@el7 html]# ls -Z filea
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 filea
[root@el7 html]# chcon -t httpd_sys_content_t filea
[root@el7 html]# ls -Z filea
-rw-r--r--. root root unconfined_u:object_r:httpd_sys_content_t:s0 filea
```



restorecon 예제

```
[root@el7 html]# ls -dZ .
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0 .
[root@el7 html]# ls -Z filea
-rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 filea
[root@el7 html]# restorecon filea
[root@el7 html]# ls -Z filea
```



SELinux Context

❖ 디렉토리에 context 지정 및 변경

```
semanage fcontext -a -t CONTEXT 'PATH(/.*)?'
```

```
[root@el7 ~]# ls -dZ /samba/
drwxr-xr-x. root root unconfined_u:object_r:default_t:s0 /samba/
[root@el7 ~]# semanage fcontext -a -t samba_share_t '/samba(/.*)?'
[root@el7 ~]# restorecon -RF /samba/
[root@el7 ~]# ls -dZ /samba/
```

파일에 설정된 context 규칙 확인

```
[root@el7 ~]# semanage fcontext -l
SELinux fcontext      type      Context
/                    directory system_u:object_r:root_t:s0
...(생략)...
```

❖ 노트

❖ (/.*)? 를 포함시키지 않으면 이후에 생성되는 파일은 context가 지정되지 않음

SELinux Bool

- ❖ bool 값을 on, off 함으로써 정책을 제어 할 수 있음
- ❖ 부울 확인 : getsebool [option] BOOL

현재 시스템에 설정된 모든 bool 확인

```
[root@el7 ~]# getsebool -a
abrt_anon_write --> off
abrt_handle_event --> off
...(생략)...
```

특정 bool 확인

```
[root@el7 ~]# getsebool httpd_can_network_connect_db
httpd_can_network_connect_db --> off
```

semanage boolean -l

```
[root@el7 ~]# semanage boolean -l
SELinux boolean  State  Default  Description
ftp_home_dir      (off ,  off)  Determine whether ftpd can read and
write files in user home directories.
...(생략)...
```

SELinux Bool

❖ 부울 설정 : setsebool [option] BOOL [ON | OFF]

런타임 bool 설정

```
[root@el7 ~]# semanage boolean -l | grep httpd_can_network_connect_db
httpd_can_network_connect_db (off, off) Allow HTTPD scripts and
modules to connect to databases over the network.
```

```
[root@el7 ~]# setsebool httpd_can_network_connect_db on
[root@el7 ~]# semanage boolean -l | grep httpd_can_network_connect_db
httpd_can_network_connect_db on, off) Allow HTTPD scripts and
modules to connect to databases over the network.
```

영구 bool 설정

```
[root@el7 ~]# setsebool -P httpd_can_network_connect_db on
[root@el7 ~]# semanage Boolean -l | grep httpd_can_network_connect_db
httpd_can_network_connect_db (on, on) Allow HTTPD scripts and
modules to connect to databases over the network.
```