27. SELinux

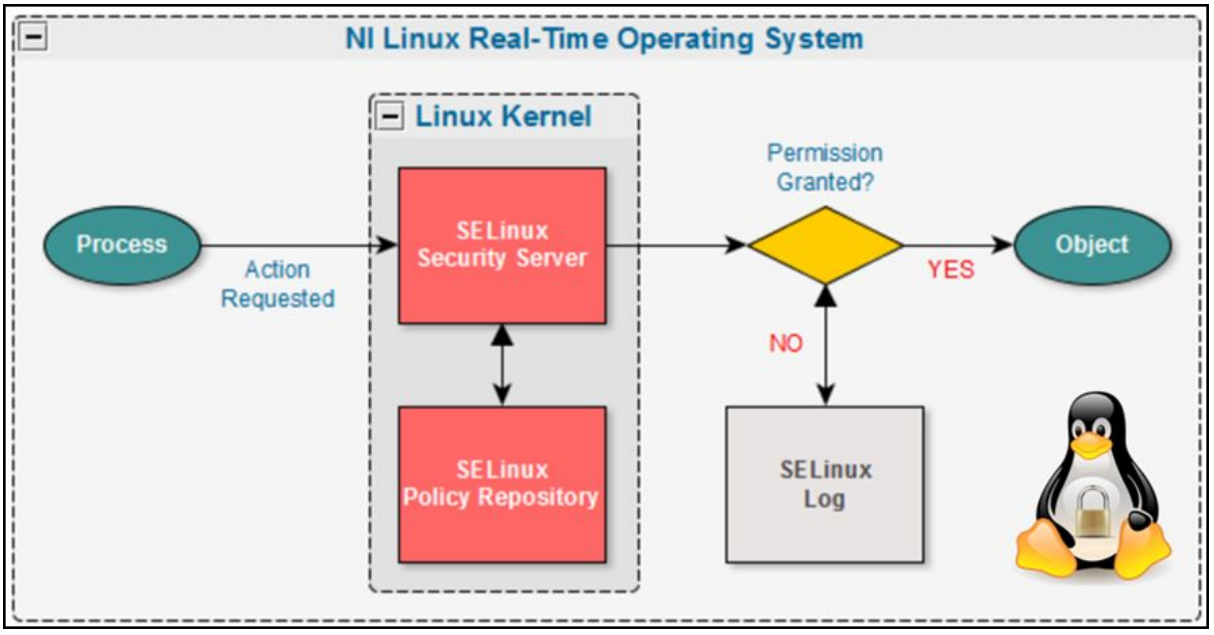
SELinux 개요와 동작

SELinux 개요

- 보안 강화 OS로 널리 알려진 것이 SELinux(Security-Enhanced Linux)이다.
- 미국 국가안전보장국(National Security Agency, NSA)을 중심으로 개발된 오픈 소스 OS이다.
- 관련 정보: http://www.nsa.gov/selinux

SELinux 동작

- SELinux는 실행되는 프로그램이 다룰 수 있는 파일 등의 범위를 제한한다.
- 각 **프로그램(프로세스)**에는 도메인이라는 식별자(레이블)이 주어진다. 예를 들어 웹 서버라면 httpd_t, 메일 서버라면 postfix_master_t, FTP 서버라면 ftpd_t와 같은 식이다.
- **파일**에는 유형이라는 식별자가 주어진다. 즉 웹 서버가 읽을 수 있는 파일에는 httpd_sys_connect_t, 메일 스풀에는 mail_spool_t, FTP 서버가 읽고 쓸 수 있는 파일에는 public_connect_t와 같은 식이다.
- SELinux는 도메인과 유형의 관계를 나타내는 **정책(policy)**을 데이터베이스로 가지고 있다. 예를 들어 '도메인 httpd_t는 유형이 httpd_sys_content_t인 파일을 읽을 수 있음'과 같은 내용을 데이터베이스에 정책으로 저장한다. 어떤 서비스가 특정 파일에 접속하려고 하면 SELinux가 정책을 참고하여 서비스가 파일에 접속할 수 있는지 확인한다.



- 이와 같이 정책으로 허가하지 않은 파일의 접속을 막을 수 있다.
- SELinux 정책은 /etc/selinux 하위 파일에서 확인할 수 있다.

SELinux 활성화/비활성화 전환

SELinux의 3가지 모드

모드	의미
Disabled	SELinux를 비활성화
Permissive	정책으로 허가되지 않은 접속이 있으면 이 정보를 로그 파일에 저장하고 접속을 허가
Enforcing	정책으로 허가되지 않은 접속이 있으면 이 정보를 로그 파일에 저장하고 접속을 거부

SELinux 현재 모드 확인

- **getenforce**

SELinux 모드 변경

- **setenforce** [**Enforcing | Permissive | 1 | 0**]
- 시스템 시작 시 SELinux 모드는 **/etc/selinux/config** 파일에 설정되어 있다.
  SELinux를 비활성화하려면 다음과 같이 수정한다.
  - vi /etc/selinux/config
    - **SELINUX=disabled**

SELinux 정책 설정

설정 가능한 정책과 정책 상태 확인

- **getsebool -a**
  - 모든 정책 목록을 보려면 -a 옵션
  - 각 줄에 정책 이름이 표시되고 활성화와 비활성화를 각각 on과 off로 나타낸다.
- **getsebool 정책이름**
  - 특정 정책의 상태만 표시한다.
- **semanage boolean -l**
  - 각 정책이 어떤 상태인지 간단한 설명과 함께 확인할 수 있다.
  - 만약 명령어가 발견되지 않았다고 메시지가 나타나면 다음 명령으로 설치한다.
    - yum install policycoreutils-python
- **semanage boolean -l | grep 키워드**
  - 특정 키워드를 포함한 정책만 보고 싶을 때는 grep 명령어로 골라낼 수 있다.

정책 설정 변경

- **setsebool -P 정책이름 설정값**

- 예를 들어 httpd_enable_homedirs(홈 디렉터리 내에 저장한 웹 컨텐츠를 웹 서버를 통해 공개하는 정책)를 활성화하려면
    - setsebool -P httpd_enable_homedirs on

SELinux 제어 레벨 확인

SELinux 로그

- SELinux가 작동 중일 때 설정이 적절하지 않으면 프로그램이 SELinx로부터 제한을 받아 제대로 동작하지 않을 수 있다.
- 이럴 때는 SELinux가 /var/log/messages 로그 파일에 프로그램이 받는 제한 내용을 기록한다.
- less /var/log/messages
    - SELinux의 로그는 'SELinux is preventing'과 같이 남겨진다.

SELinux 문제 해결사

- CentOS 7에는 SELinux 제한이 발생했을 때 어떤 조처를 취했는지 확인할 수 있는 SELinux 보안 통지 브라우저가 탑재되어 있다.
- SELinux 로그를 보기 쉬운 형식으로 가공해서 표시해주므로 SELinux로 인해 생긴 제한을 이해하는 데 도움이 된다.
- 프로그램 메뉴에서 잡다 > SELinux 문제 해결사를 선택하여 시작한다.
    - 이전(V) 버튼과 다음(N) 버튼을 누르면 다른 통지 내용을 확인할 수 있다.
    - 해결 방법을 알고 싶을 때는 [문제 해결] 버튼을 누르면 몇 가지 해결 방법이 표시된다.