인덕대학교

운영체제 보안 3
- 시스템 로그

컴퓨터소프트웨어학과

김병국 교수

학습목표

- 시스템 로그에 대한 분석을 할 수 있다.
- 시스템 로그를 위한 프로그램을 만들 수 있다.

목차

- 로그 개념
- 시스템 로그 서비스

1. 로그 개념

❑ 로그(log)

- 운영체제는 시스템의 상태를 기록(log)
- 서비스(Service) = 데몬(daemon) = 서버(Server)
- 유닉스 운영체제는 “/var/log/” 에 기록

- 대표 파일:
  - syslog : 시스템의 상태를 기록
  - wtmp, btmp, lastlog : 사용자 접속(로그인) 관련 기록

2. 시스템 로그 서비스 (1/4)

❑로그 서비스

- RSyslogD (Reliable System Log Daemon)
- 수집된 이벤트 상태정보를 파일에 기록하는 서버프로그램
  - 네트워크 또는 UNIX 도메인 방식으로 정보를 받음
  - 커널의 상태정보는 /run/system/journal/dev-log에서 읽음
- 설정 파일 : /etc/rsyslog.conf
- 대표적 기록 파일: /var/log/syslog

2. 시스템 로그 서비스 (2/4)

❑ 로그 서비스 동작 및 확인

- 서비스 동작
  - 명령어: service rsyslog restart

- 서비스 동작 확인
  - 명령어: systemctl status rsyslog.service

```
[root@kali: ~]# systemctl status rsyslog.service
● rsyslog.service - System Logging Service
     Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2021-05-17 11:59:22 KST; 6h ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 418 (rsyslogd)
      Tasks: 4 (limit: 4634)
     Memory: 3.1M
        CPU: 74ms
     CGroup: /system.slice/rsyslog.service
             └─418 /usr/sbin/rsyslogd -n -iNONE
```

[rsyslogd 동작 확인]

2. 시스템 로그 서비스 (3/4)

인덕대학교

로그 서비스 설정

- 설정 파일: /etc/rsyslog.conf

대상 파일을 명시
(-)가 붙어 있으면 fsync()를 호출하지 않는다는 의미

- 기본 형태:

Facility{,...} | .Priority | {-}Action

```
###############
#### RULES ####
###############

#
# First some standard log files.  Log by facility.
#
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
daemon.*                        -/var/log/daemon.log
kern.*                          -/var/log/kern.log
lpr.*                           -/var/log/lpr.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log
```

[/etc/rsyslog.conf 내용 中]

범주

```
lity codes */
LOG_KERN        (0<<3)  /* kernel messag
LOG_USER        (1<<3)  /* random user-l
LOG_MAIL        (2<<3)  /* mail system *
LOG_DAEMON      (3<<3)  /* system daemon
LOG_AUTH        (4<<3)  /* security/auth
LOG_SYSLOG      (5<<3)  /* messages gene
LOG_LPR         (6<<3)  /* lin
LOG_NEWS        (7<<3)  /* net
LOG_UUCP        (8<<3)  /* UUC
LOG_CRON        (9<<3)  /* clo
LOG_AUTHPRIV    (10<<3) /*
LOG_FTP         (11<<3) /* ftp
```

```
 * priorities (these are ordered)
 */
#define LOG_EMERG   0   /* system is unusable */
#define LOG_ALERT   1   /* action must be taken immediatel
#define LOG_CRIT    2   /* critical conditions */
#define LOG_ERR     3   /* error conditions */
#define LOG_WARNING 4   /* warning conditions */
#define LOG_NOTICE  5   /* normal but significant condition
#define LOG_INFO    6   /* informational */
#define LOG_DEBUG   7   /* debug-level messages */
```

[/usr/include/sys/syslog.h 中]

```
CODE prioritynames[] =
  {
    { "alert", LOG_ALERT },
    { "crit", LOG_CRIT },
    { "debug", LOG_DEBUG },
    { "emerg", LOG_EMERG },
    { "err", LOG_ERR },
    { "error", LOG_ERR },
    { "info", LOG_INFO },
    { "none", INTERNAL_NOPRI },
    { "notice", LOG_NOTICE },
    { "panic", LOG_EMERG },
    { "warn", LOG_WARNING },
    { "warning", LOG_WARNING },
    { NULL, -1 }
  };
```

2. 시스템 로그 서비스 (4/4)

❑ 로그 서비스 설정

- 설정 파일: /etc/rsyslog.conf
- 로그 발생 명령: logger -p user.debug <발생할 메시지>
- 로그 확인: tail -f /var/log/induk

```
kali@kali:~$ logger -p user.debug Hello World
kali@kali:~$ logger -p user.debug Hello World hahaha
kali@kali:~$ logger -p user.debug asdfasdfs
kali@kali:~$ logger -p user.debug asdf
kali@kali:~$
```

[사용자 로그 발생]

```
[root@kali: /home/kali]# tail -f /var/log/induk.log
May 17 19:15:28 kali kali: hello World
May 17 19:15:51 kali kali: hello World hahaha
May 17 19:16:43 kali kali: adfasdfs
May 17 19:17:09 kali kali: asdf
```

[사용자 로그 확인]

- 실습
  - 사용자 메시지에 대해 별도의 파일에 기록

```
#
# First some standard log files.  Log by facility.
#
auth,authpriv.*                 /var/log/auth.log

mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log

user.*                          /var/log/induk.log

#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files
```

수정 후에는 서비스 재시작 필요

[로그 설정]

3. 시스템 로그 프로그래밍

❑프로그래밍 실습

- 프로그램을 통한 로그화

```c
#include <stdio.h>
#include <syslog.h>
#include <pwd.h>
#include <unistd.h>

int
main(int argc, char* argv[])
{

    for (int i = 0; i < 10; i++)
    {
        syslog(LOG_DEBUG, "[%d] We have a message.", i);
    }

    return 0;
}
```

[파일명: syslog.c]

```c
#include <sys/syslog.h>

int syslog(int type, char *bufp, int len);
```

[syslog() 함수의 프로토타입]

```c
 * priorities (these are ordered)
 */
#define LOG_EMERG 0 /* system is unusable */
#define LOG_ALERT 1 /* action must be taken immediately */
#define LOG_CRIT  2 /* critical conditions */
#define LOG_ERR   3 /* error conditions */
#define LOG_WARNING 4 /* warning conditions */
#define LOG_NOTICE  5 /* normal but significant condition */
#define LOG_INFO  6 /* informational */
#define LOG_DEBUG 7 /* debug-level messages */
```

[참고 헤더(/usr/include/sys/syslog.h)]

4. 기타 로그 서비스

❑로그인 기록

- 사용자의 시스템 접근 시 기록
- /var/log/{wtmp, btmp, lastlog} 파일을 통해 관리됨
- 관련 명령어: last, lastb, lastlog
  - last : 최근 접속자들에 대한 정보를 표시
  - lastb : 접속 실패에 대한 정보를 표시
  - lastlog : 모든 접속시도에 대한 정보를 표시

수고하셨습니다.