Syslog 실시간 감시시스템 설계

김도형* · 김귀남*

요 약

기존에는 Syslog 메시지를 확인하기 위해서는 Telnet에나 Console을 통해 대상 System에 로그인을 하여야 했다. 이는 System의 이상유무를 실시간으로 감시할 수 없는 단점이 있다. 이러한 단점을 해결하기 위해 본 논문에서는 Syslog 실시간 감시 시스템을 설계하였다. 제안된 시스템은 로그인 과정 없이 Syslog 메시지를 실시간 감시하여 System의 이상을 실시간으로 탐지함으로써 적시에 문제를 해결할 수 있다. 본 논문에서 제안된 실시간 모니터링 시스템은 Windows 기반으로 구성되었다.

A Design of Syslog Real-time Monitoring System

Do Hyeong Kim* · Kuinam J. Kim*

ABSTRACT

Previously, we need to log-in to the target system to check the system log. This is a problem that can not be monitored in real time. This paper designed a syslog real-time monitoring system to solve this problem. The proposed system be able to detect a problem of system in real time without log-in process and be able to solve problems immediately. The proposed syslog real-time monitoring system in this paper is based on Windows OS.

Key words : Syslog, Syslogd

* 경기대학교 정보보호학과

1. 서 론

시스템관리자에게 가장 중요한 것은 로그파일 관리이다. System 로그를 일일이 점검하고 System에 문제가 있는지 확인하는 일이다. 시스템관리자는 System의 이상여부를 로그서버를 이용해 log를 확인하거나[1], 자동화 스크립트 툴을 이용해 메일 체크를 통해서 한다.

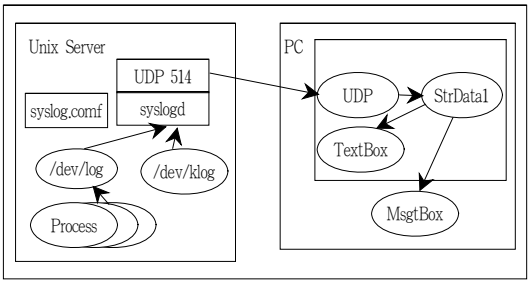
하지만 이러한 방법들은 System의 로그를 실시간으로 확인할 수 없어 조기에 System의 문제를 탐지할 수 없고, 장애 발생 후 사후분석으로만 로그를 활용할 수 밖에 없다.

본 논문에서 제안하는 Syslog 실시간 모니터링 시스템은 GUI(Graphic User Interface)로 구현이 되어 개인 PC에서 수많은 System들의 메시지를 실시간으로 즉시 확인할 수가 있으며, System 메시지를 로그로 남겨서 이전 메시지도 확인할 수 있는 기능을 갖고 있다.

2. Syslog 실시간 모니터링 시스템 설계 및 구현

2.1 Syslog 실시간 모니터링 시스템

본 논문에서 제안하는 시스템은 Syslog 모니터링 시스템으로서 Windows 운영체제 환경에서 여러 System 메시지를 팝업 창을 통해 실시간으로 관리자에게 통보하며, 본 시스템에서 제공하는 Text창을 통해 로그를 기록함으로써 이전의 기록들도 확인 할 수가 있다. 본 시스템은(그림 1)에서와 같이 syslogd Daemon이 UDP 514 Port를 이용해 시스템 메시지를 원격지와 주고받는 기능에 착안한 것이다[5]. 즉, 원격의 System의 syslogd에 의해 UDP 514 Port로 보내주는 메시지를 Windows 운영체제 환경에서 메시지를 받아 유저에게 알려주는 기능이다. 본 시스템은 크게 UDP 514 Port의 생성, System 메시지의 수신, 그리고 마지막으로 수신메시지의 처리부분으로 되어있다[2]. 본 시스템은 Microsoft 사의 Visual Basic 6으로 구현되었다.



(그림 1) Syslog 실시간 모니터링 시스템의 작동 원리

2.2 UDP 514 Port의 생성

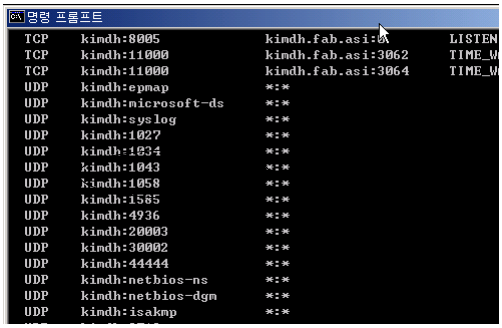
Windows 운영체제 환경에서 원격의 System 메시지를 받기 위해서는 우선 UDP 514 Port가 열려 있어야 된다[7]. Windows 운영체제 환경에서 UDP 514번 Port를 생성하기 위해서는 윈도우 소켓(Winsock)을 이용한다[9]. 프로토콜은 UDP를 사용해야 하며 Port 514 Port를 열어주어야 한다. 프로그램을 실행시키면 Windows OS환경에서 UDP 514번 Port (syslog Port)가 생성된다.

```
Private Sub Form_Load( )

  With sckMonitor

      ◦ LocalPort = 514
      ◦ Bind 514

  End With
End Sub
```

(그림2) UDP 514번 Port의 생성 소스코드

(그림 2)의 소스코드에 의해 메인 프로그램을 실행시키면, 프로그램이 실행된 PC의 Local Port 514번을 바인딩한다. 즉, UDP 514번 Port가 Open 된다[6]. (그림 3)은 프로그램 실행 후 Windows

OS 환경에서 Syslog Port가 할당된 것을 볼 수가 있다. 이는 syslogd이 보내주는 시스템 메시지를 받아들일 준비가 되었다는 것을 의미한다.



(그림 3) Syslog Port의 생성

2.3 메시지의 수신 및 처리

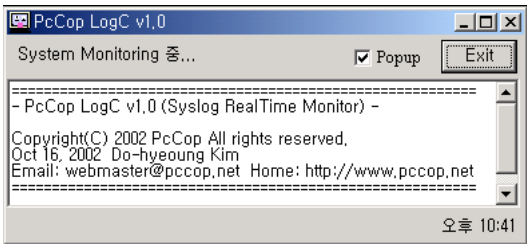
UDP 514번 Port를 생성 후에 System의 syslogd Daemon에서 보내주는 시스템 메시지를 어떻게 받아서 어떻게 처리할 것인가는 다음의 Visual Basic 소스코드를 보면서 설명하겠다.

```
Private Sub sckMonitor_DataArrival(ByVal bytesTotal As Long)

    Dim StrDatal As String
    sckMonitor.GetData,strDatal

    msg = strDatal

    ...〈 중  략 〉.....

End Sub
```

(그림 4) 메시지의 수신 및 처리

우선, UDP 514번 Port를 이용해 메시지 데이터를 받게 되면, 메시지 데이터는 문자일 것이다. 그래서 strData1을 String(문자열)형으로 정의하고, sckMonitor.GetData를 통해 외부의 UNIX Server로부터 날아온 메시지 데이터를 strData1에 저장한다(여기서 sckMonitor는 VB의 윈속컨트롤이다). 그리고, strData1을 표현만 해주면 되는 것이다[6]. 표현하는 방법에는 여러가지가 있을 것이다. 여기에서 소개하는 시스템은 메시지를 팝업 메시지창, Text창으로 표현할 수 있도록 구현하였다.

2.4 Syslog 실시간 모니터링 시스템의 구현



(그림 5) Syslog Real-Time Monitoring System 의 실행화면

본 시스템을 실행을 하면 위 (그림 5)와 같은 창이 나타나면서, 윈속(Winsock)에 의해 UDP 514번 Port가 생성이 된다. 여기서 구현한 시스템은 위와 같은 메인창을 가지고 있으며, 팝업 메시지창의 활성화/비활성화를 선택하는 체크란을 통해(기본적으로 활성화) 파업 메시지 창을 띄울 것인가 말 것인가를 정할 수가 있다. 그리고, Exit 버튼을 이용해 시스템을 종료할 수가 있다. 추가로 Text창이 있어 팝업 메시지창과 동시에 System들의 메시지들을 기록할 수가 있다. Text창에 쓰여지는 메시지 로그는 본 시스템을 종료하지 않는 한 사라지지 않는다. 그리고 Text창을 편집할 수가 있어서, Text창에 기록된 메시지를 Text파일로 저장을 할 수가 있다. 또한 하단의 Status 바를 통해 현재시각을 확인할 수가 있다. 본 시스템의 메인 창은 마우스 조작으로 크기를 마음대로 조절 못하며, 단지 최대화만 할 수 있을 뿐이다.

3. Syslog 실시간 모니터링 시스템의 적용 결과

본 논문에서 구현한 시스템을 HP-UX System 17

대, SUN Solaris System 10대의 환경에서 적용해 보았으며, 시스템을 실행할 PC는 Windows 95, Windows 98, Windows 2000, Windows XP 등의 환경에서 적용해 보았다.

3.1 환경설정

본 시스템을 테스트하기 전 각각의 Unix Server에 대한 설정이 필요하다. 환경설정은 로그서버 구현방식과 동일하다. 한 가지 다른 점이 있다면, 각각의 Unix Server에 로그서버 네임과 로그서버 IP를 설정하는 대신에 Monitoring 시스템이 설치될 PC의 컴퓨터 이름과 IP를 설정해야 한다.

3.1.1 /etc/hosts 파일의 수정

Unix Server의 /etc/hosts 파일에 메시지를 받을 PC의 IP와 컴퓨터 이름을 추가한다[3].

```
#Person
10.145.21.102   kimdh /* windows 2000 */
10.145.21.104   kimsj
10.145.21.191   Mr.Ban /* windows XP */
10.145.21.162   swlee /* windows 98 */
```

(그림 6) /etc/hosts의 설정

kimdh, kimsj라는 PC는 Windows 2000 환경이고, Mr.Ban이라는 PC는 Windows XP 환경, 그리고 swlee 라는 PC는 Windows 98 환경이다.

3.1.2 /etc/syslog.conf 파일의 수정

Unix Server의 /etc/syslog.conf 파일에 메시지를 받을 PC 네임을 추가한다. 어떠한 메시지를 받을 것인지는 시스템의 사용용도에 따라 시스템관리자가 정의해 주면 될 것이다. 여기서는 (그림 7), (그림 8)과 같이 정의하였다.

(그림 7)와 같이 SUN Solaris System에서는 /var/adm/messages에 쌓이는 메시지와 같은 메시지를 PC에서 받을 수 있도록 설정하였다[3]. 내용을 보자면, 모든 Facility에 대해 err Level 이상의 메시지를 받는데, kern Facility는 debug Level 이상의 메시지를 받고, daemon Facility는 notice Level 이상의 메시지를 받고, mail Facility는 crit Level 이상의 메시지를 받도록 설정하였다.

```
#ident "@(#)syslog.conf   1.5   99/02/03 SMI" /* SunOS 5.0 */
#
#Copyright (c) 1991-1999 by Sun Microsystems, Inc.
#All rights reserved.
#
#syslog configuration file.
#
#This file is processed by m4 so be careful to quote (') names
#that match m4 reserved words. Also, within if det's, arguments
#containing commas must be quoted.
#
*.err;kern.notice;auth.notice                   /dev/sysmsg
*.err;kern.debug;daemon.notice;mail.crit        /var/adm/messages
*.err;kern.debug;daemon.notice;mail.crit        @kimdh
*.err;kern.debug;daemon.notice;mail.crit        @kimsj
*.err;kern.debug;daemon.notice;mail.crit        @Mr.Ban
*.err;kern.debug;daemon.notice;mail.crit        @swlee
```

(그림 7) SUN Solaris에서의 /etc/syslog.conf의 설정

```
# @(#) $Revision: 74.1 $
#
#syslogd configuration file.
#
#See syslog d(1M) for information about the format of this file.
#
mail.debug                      /var/adm/syslog/mail.log
*.info;mail.none                /var/adm/syslog/syslog.log
*.info;mail.none                @kimsj
*.info;mail.none                @kimdh
*.info;mail.none                @Mr.Ban
*.info;mail.none                @swlee
*.alert                         /dev/console
*.alert                         root
*.emerg                         *
```

(그림 8) HP-UX에서의 /etc/syslog.conf의 설정

HP-UX System에서는 /var/adm/syslog/syslog.log에 쌓이는 메시지와 같은 메시지를 PC에서 받을 수 있도록 설정하였다[4]. 내용을 보자면, 모든 Facility에 대해 info Level 이상의 메시지를 받는데, mail Facility에 대해서는 메시지를 받지 않도록 설정이 되어있다.

3.1.3 syslogd Daemon restart

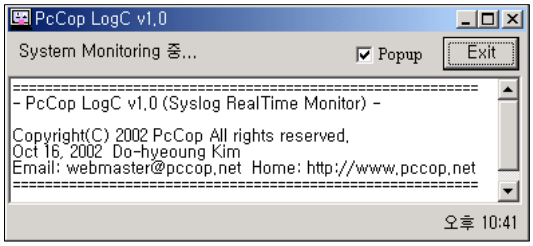
```
# ps -ef | grep syslogd
    root   628     1  0  Sep 20  ?         0:43 /usr/sbin/syslogd -D
# kill -HUP 628
# ps -ef | grep syslogd
    root   628     1  0  Sep 20  ?         0:43 /usr/sbin/syslogd -D
#
```

(그림 9) syslogd Daemon의 Restart

syslogd Daemon을 restart를 할 때에는 '-HUP' 옵션을 주어서 restart를 시킨다. Linux의 경우, syslogd이 어떻게 떠 있는가에 따라 달라지는데 '-r'옵션이 안 붙어 있다면 syslogd Daemon을 완전히 kill시키고 syslogd Daemon을 새로 띄울 때 'r' 옵션을 주도록 한다(Linux의 경우에는 UDP 514번 Port를 사용하기 위해서는 '-r' 옵션을 주어야 한다).

3.2 실 행

여기서 구현한 시스템은 Windows95, Windows 98, Windows 2000, Windows XP의 모든 Windows 환경에서 실행이 가능하며, 메시지를 받는 PC에서 따로 환경을 설정해 줄 것은 없다. 네트워크로 연결된 Windows 운영체제 PC라면 어떠한 PC에도 본 시스템을 실행시켜 사용 할 수가 있다.



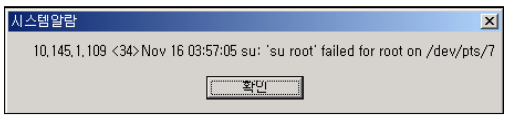
(그림 10) 모니터링 시스템 실행초기 화면

본 시스템을 실행시키면 Popup 체크란에는 default로 체크가 되어 있으며, PC에서 메시지 파업 창을 띄우기 싫으면 체크표시를 없애면 된다. Popup 체크란에 체크표시를 없애면 Text창에만 메시지를 기록한다.

이렇게 실행을 시키면 모든 준비는 끝났다.

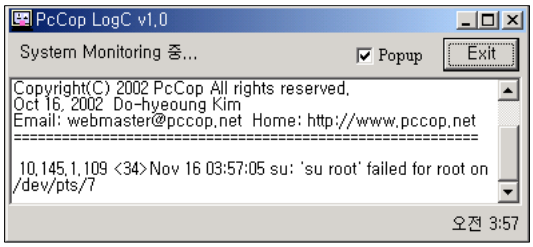
3.3 실행 결과

본 시스템이 실행되면 UNIX Server로부터 실시간으로 메시지를 받을 수가 있다. 팝업 메시지창을 통하여 메시지를 바로 확인할 수가 있으며, 본 시스템의 Text창을 통해 로그로 기록됨으로 이전의 메시지를 확인할 수가 있다(그림 11)~(그림 12).



(그림 11) 팝업메시지의 실행 화면

UNIX Server로부터 메시지를 받으면 (그림 11)과 같이 팝업 메시지창을 팝업창 뜨는 소리와 함께 띄우며 메시지 내용을 보면, 시스템 메시지의 내용을 자세히 알 수가 있다. (그림 11)의 메시지를 보면, 10.145.1.109 Server에서 su 명령을 이용해 root 유저로 접근을 시도하다가 실패했다는 것을 알 수가 있다.



(그림 12) Text창의 로그기록

마찬가지로 메인 프로그램의 Text창을 보게 되면(그림 12) 조금 전 팝업으로 뿌려졌던 메시지가 Text창에 기록되어 있는 것을 확인할 수가 있다. 본 시스템은 HP-UX, SUN Solaris System에서 보내주는 모든 메시지를 실시간으로 팝업 메시지

창으로 뿌려주었으며, 동시에 Text창을 통해서도 정상적으로 메시지를 기록하였다.

위의 모든 일련의 작업들은 실시간으로 이루어진다.

4. 결론 및 향후 과제

본 논문에서 제안한 Syslog 실시간 모니터링 시스템은 syslogd Daemon이 UDP 514번 Port를 이용해 원격으로 메시지를 주고 받는 기능을 응용하여 Windows OS 환경에서 syslogd Daemon이 보내주는 메시지를 실시간으로 받을 수 있다. 제안된 모니터링 시스템은 시스템관리자가 System의 이상을 신속하게 파악해 조치하게 함으로써 System의 지속적인 서비스시간을 높인다. 또한 여러 System들의 로그를 GUI환경에서 편리하게 검토할 수 있게 함으로써 관리자의 시스템 관리가 지속적으로 될 수 있다.

본 논문에서 소개하는 시스템은 로그서버와 마찬가지로 UNIX뿐만 아니라 Syslog 기능이 있는 다른 장비들에게도 응용되어 질 수 있다. 예를 들자면 Syslog 기능이 있는 CISCO라우터, Windows용 syslogd 프로그램 등이 그것이다. 즉, 라우터 시스템의 메시지, Windows 시스템의 메시지들도 받을 수 있다는 것이다[8].

향후 과제로는 메시지의 신뢰성과 분류기능이다. UDP 프로토콜을 이용한 메시지의 전달이기 때문에 중간에 유실되었는지, 누가 가로채지 않았는지에 대해 체크할 수 있는 기능을 고려할 필요가 있다. 그리고 메시지의 기록을 Facility별이나 Level별로 분류해서 기록하고 표현한다면, 좀 더 세분화된 로그 모니터링이 가능해 질 것이다.

참 고 문 헌

[1] Eric Hines, “Complete Reference Guide to Creating a Remote Log Server”, http://www.linuxsecurity.com/feature_stories/remote_logserver-1.html, 2000.

[2] W. Richard Stevens, “UNIX NETWORK PROGRAMMING(Networking APIs : Sockets and XTI)” Prentice-Hall, Inc. 1998.

[3] “SunOS 5.7 Manual Page syslog, syslogd, syslog.conf”, SUN Microsystems, Inc.

[4] “Programming with UNIX System Calls” 50710S C.01, Hewlett-Packard Company. 1997.

[5] 정현철, “UNIX 로그분석을 통한 침입자 추적 및 로그관리”, 한국정보보호진흥원 2001.

[6] 이이표, 김병세, “Microsoft Visual Basic Bible 6.0”, 삼양출판사. 1998.

[7] “syslogd.c”, http://linux.adics.com/bus ybox/S/107.html#BOTTOM.

[8] www.certcc.or.kr.

[9] www.sockets.com.

김 도 형

2001년 한국방송통신대학교 방송정보학과 (문학사)

2003년 경기대학교 정보보호학과 (공학석사)

2007년 경기대학교 정보보호학과 박사수료

1997년~2001년 아남반도체 근무

2001년~현재 동부하이텍 반도체부문 보안담당

김 귀 남

미국 캔자스대학 수학과 (학사)

미국 콜로라도주립대학 (석사)

미국 콜로라도주립대학 (박사)

현재 경기대학교 정보보호학과 교수