

로그 모니터링 프로그램 디자인 및 개발

-정지훈-

목차

1. 개요

2. 스크립트 작성

3. 실행 및 결과

1. 개요

-목표

/var/log/messages에서 warn|error|fail|crit|alert|emerg 같은 단어가 포함되었을 경우 확인후 메일로 전송하는 동작을 수행한다.

-동작원리

배시 셸 스크립트 사용하여 로그파일에 에러가 존재할 경우 root사용자 메일을 통해 확인하고, 직접 메시지를 작성하여 모니터링을 통해 확인하는 작업을 진행한다.

2. 스크립트 작성

방화벽 서비스 등록되어있는지 확인하고, sendmail, mailx, dovecot 패키지 설치한다.

패키지 설치

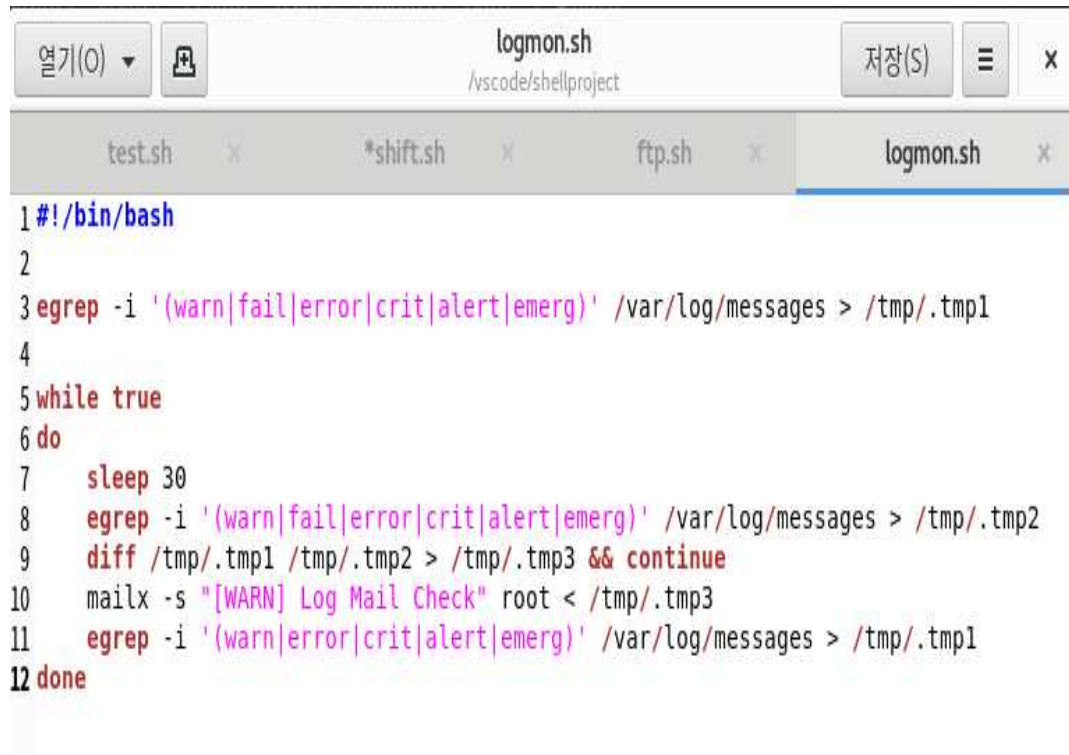
```
# yum -y install sendmail
# yum -y install mailx
# yum -y install dovecot
```

방화벽 서비스 등록

서비스가 등록되어있는지 리스트를 통해 확인한다.

```
[root@main ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: cockpit dhcpv6-client http https imap imaps ntp pop3 pop3s smtp smtps ssh
  ports: 3389/tcp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

-스크립트 작성 내용



The screenshot shows a VS Code editor window with the file 'logmon.sh' open. The window title bar includes '열기(O)', a file icon, 'logmon.sh', the path '/vscode/shellproject', a '저장(S)' button, a menu icon, and a close button 'x'. The editor has four tabs: 'test.sh', '*shift.sh', 'ftp.sh', and 'logmon.sh'. The 'logmon.sh' tab is active and shows the following script content:

```
1 #!/bin/bash
2
3 egrep -i '(warn|fail|error|crit|alert|emerg)' /var/log/messages > /tmp/.tmp1
4
5 while true
6 do
7     sleep 30
8     egrep -i '(warn|fail|error|crit|alert|emerg)' /var/log/messages > /tmp/.tmp2
9     diff /tmp/.tmp1 /tmp/.tmp2 > /tmp/.tmp3 && continue
10    mailx -s "[WARN] Log Mail Check" root < /tmp/.tmp3
11    egrep -i '(warn|error|crit|alert|emerg)' /var/log/messages > /tmp/.tmp1
12 done
```

해당하는 파일의 실행권한 주기

```
# chmod +x logmon.sh
```

3. 실행 및 결과

강제로 에러로그 생성

```
[root@main ~]# logger -p user.error "[ WARN ] log check test"
```

```
[root@main /bin]# mailx root
Subject: 535353
424242
.
EOT
```

관리자에게 보낸 메일을 목록에서 확인할 수 있다.

```
[root@main /bin]# mailx
Heirloom Mail version 12.5 7/5/10. Type ? for help.
"/var/spool/mail/root": 151 messages 2 new 136 unread
U141 root Thu Aug 25 18:38 112/9992 "[WARN] Log Mail Check"
U142 root Thu Aug 25 18:38 115/10198 "[WARN] Log Mail Check"
U143 root Thu Aug 25 18:39 112/9992 "[WARN] Log Mail Check"
U144 root Thu Aug 25 18:39 112/9992 "[WARN] Log Mail Check"
U145 root Thu Aug 25 19:18 112/9992 "[WARN] Log Mail Check"
U146 root Thu Aug 25 19:19 112/9992 "[WARN] Log Mail Check"
U147 root Thu Aug 25 19:19 112/9992 "[WARN] Log Mail Check"
U148 root Thu Aug 25 19:20 112/9992 "[WARN] Log Mail Check"
U149 root Thu Aug 25 19:20 112/9992 "[WARN] Log Mail Check"
>N150 root Thu Aug 25 19:21 111/9982 "[WARN] Log Mail Check"
N151 root Thu Aug 25 19:21 21/796 "535353"
&
```

mailx로 메일이 들어온 것을 확인하고, 정상적으로 오류보고 동작했음을 알 수 있다.