간단하면서도 막강한 파일 무결성 체크 프로그램 Fcheck

오늘과 내일 넷센터 홍석범(antihong@tt.co.kr)

리눅스에는 기본적으로 약 30,400 여개가 넘는 파일들이 설치된다고 한다.
리눅스 관리자는 이 많은 파일들에 대해 일일이 각 파일들의 무결성을 체크할 수 없는데, 이를 틈타 악의적인 목적을 가지고 시스템에 중요한 파일을 변조하거나 관리자의 허락 없이 임의의 파일을 설치할 수 있다. 이를 체크하고 감시하기 위해 "파일 무결성 체크 프로그램"의 필요성이 제기되는데, 여기에서는 간단한 설정만으로 강력한 기능을 제공하는 Fcheck 라는 파일 무결성 체크 프로그램을 소개하고자 한다.

일반적으로 파일 무결성 체크 프로그램으로는 Tripwire 가 알려져 있지만, 많은 기능을 제공하는 만큼 설정이 너무 복잡하여 리눅스 초보자나 간단한 설정으로 관리하고자 하는 리눅스 관리자에게는 Fcheck 라는 프로그램을 권장한다.
Fcheck 는 간단한 설정으로 특정 디렉토리나 파일 또는 전체 파일 시스템에 대해 파일의 추가, 변경, 삭제여부를 체크하여 그 결과를 알려준다.

다운로드 및 설치

먼저 Fcheck 홈페이지인 http://www.geocities.com/fcheck2000/ 에 접속하여
최신 버전의 Fcheck 를 다운로드 한다. 필자가 글을 쓸 때 당시의 최신버전은 2.07.59 이며 위 사이트에서 FCheck_2.07.59.tar.gz 파일을 다운로드후 압축을 해제한다.
참고로 이 프로그램은 프리웨어로 자유롭게 이용이 가능하다.

```
[root@www local]# tar zxvfp FCheck_2.07.59.tar.gz
fcheck/
fcheck/license
fcheck/fcheck
fcheck/fcheck.cfg
fcheck/README
fcheck/install
.
```

/usr/local 디렉토리에서 압축을 풀면 fcheck 라는 디렉토리가 생기면서 관련 파일들이 설치된다. 생성된 fcheck 디렉토리로 이동 후 fcheck 라는 실행파일과 fcheck..cfg 라는 설정파일 이렇게 두개 파일만 수정해 주면 된다.

Fcheck 파일 수정하기.

위 파일을 열면

$config="/usr/local/admtools/conf/fcheck.cfg";

라는 부분이 있는데, 이는 fcheck 의 설정파일인 fcheck.cfg 파일의 위치를 지정해 주는 것으로 현재의 디렉토리를 적절히 지정해 주면 된다.

필자의 경우처럼 /usr/local/fcheck 디렉토리에 설치하였다면

$config="/usr/local/fcheck/fcheck.cfg"; 처럼 변경한다.

Fcheck 파일에 대한 설정은 이곳으로 끝이다.

Fcheck.cfg 파일 수정하기.

이제 Fcheck.cfg 의 설정을 내 환경에 맞도록 변경해 보자.

 # Directory

이 부분은 파일의 무결성을 체크하고자 하는 디렉토리를 정의한다.

주로 시스템 관련 파일이 존재하면서 파일의 속성이 자주 변경되지 않는 디렉토리를 지정한다. 필자의 경우에는

Directory=/etc/

Directory=/bin/

Directory=/usr/bin/

Directory=/sbin/

Directory=/usr/sbin/

Directory=/lib/

와 같이 설정하였다.

 # Exclusion

이 부분은 위의 “Directory” 부분에서 지정한 무결성 여부를 체크할 디렉토리내에서 자주 변경되는 디렉토리나 파일이 있어 체크를 제외할 파일이나 디렉토리등을 지정하면 된다.

(물론 제외할 디렉토리나 파일이 없으면 설정하지 않으면 된다.)

필자는 아래와 같이 /etc/passwd 와 /etc/shadow 파일 그리고 /lib/modules/ 디렉토리를 추가하였다.

Exclusion = /etc/passwd

Exclusion = /etc/shadow

Exclusion = /lib/modules/

 # DataBase

fcheck 는 무결성 상태의 파일 시스템에 대한 각종 정보를 DB 형태로 기억하고 있다가 일정시간마다 DB 에 기록된 정보와 현재의 파일 시스템을 비교하여 파일의 추가/변경/삭제가 있을 경우 이를 알려주게 되는데, DataBase 는 이때 기억되는 각종 파일 시스템에 대한 정보를 기억하고 있을 DB 의 경로 및 파일명을 지정하여 주는 것이다.

필자는

DataBase = /usr/local/fcheck/data/data.dbf

와 같이 설정하였다.

이를 위해 /usr/local/fcheck 디렉토리밑에 mkdir data 로 data 디렉토리를 생성한다.

이와 같이 설정한 후 DB 생성 명령어(fcheck –ac)를 입력하면 data 라는 해당 디렉토리에 data..dbf 라는 파일이 생성된다.

 # TimeZone

TimeZone 은 시스템의 각종 시간등에 대한 정보를 위해 필요하다.

한국의 TIMEZONE 은 GMT+9 인데, GMT+9 를 입력하면 시간의 차이가 생기며 오히려 GMT-9 로 설정해 주어야 정상적으로 작동한다. 이는 프로그램의 버그인듯 하다.

따라서 아래와 같이 설정해 준다.

TimeZone =GMT-9

 # File

이 부분은 설정할 필요가 없는 부분이므로 아래와 같이 주석처리하면 된다.

#File = /usr/local/admtools/logs/sol.dbf

이로서 설정이 끝났다.

이외 다른 설정도 몇가지 있지만 그대로 두어도 무방하다.

현재의 상태에서

[root@www fcheck]# ./fcheck –ac 를 입력하면 현재의 파일 시스템을 체크하여

파일 시스템에 대한 정보를 아래와 같이 생성한다.

[root@www fcheck]# ls -la data/

-rw------- 1 root root 156519 Apr 10 11:33 data.dbf

이제 정상적으로 체크가 되는지 확인해 보자.

아래와 같이

[root@www fcheck]# touch /usr/bin/test 로 파일을 생성한 후 fcheck –a 를 실행해보았다.

ADDITION: [www.tt.co.kr] /usr/bin/[

Inode	Permissons	Size	Created On
273211	-rw-r--r--	0	Apr 10 12:21 2001

ADDITION: [www.tt.co.kr] /usr/bin/test

Inode	Permissons	Size	Created On
273211	-rw-r--r--	0	Apr 10 12:21 2001

위와 같이 /usr/bin/test 가 생성되었음을 알려준다.
각자 파일의 생성이나 변경, 삭제를 한 후 테스트를 해 보기 바란다.

무결성 체크 자동으로 하기.

관리하는 리눅스 시스템이 많다면 일일이 각 시스템에 로긴후 모두 체크하기란 여간 귀찮은 일이 아닐 수 없다. 따라서 이를 자동으로 체크하여 만약 파일 시스템의 변동이 있을 경우 관리자에게 변동 내용을 메일로 통보해주면 편리할 것이다. 아쉽게도 Fcheck 는 기본적으로 이러한 기능은 제공되지 않는데, 이를 위해 약간의 추가설정을 하면 된다.
이를 위해 /etc/cron.daily/ 에 fcheck.cgi 라는 파일을 생성하여 아래와 같이 추가한 후 실행할 수 있도록 권한을 700 으로 설정해 주기만 하면 된다.

```
#!/usr/bin/perl

$TASK = `/usr/local/fcheck/fcheck -a|grep Inode`;   ##자신의 경로에 맞게 설정한다.
$HOSTNAME = `/bin/hostname`;
$TO_MAIL          = 'antihong@tt.co.kr';     ## 통보를 받을 e-mail 주소를 입력한다.
$SUBJECT          = "$HOSTNAME File 변조 확인"; ## 메일로 통보받을 제목을 지정한다.
$MAIL_PROGRAM    = "/usr/sbin/sendmail";
if ($TASK){
   $TASK_CONFIRM = `/usr/local/fcheck/fcheck -a`;   ## 자신의 경로에 맞게 설정한다.
&task_confirm;
}
sub task_confirm{
open(MAIL, "|$MAIL_PROGRAM -t");
      print MAIL "To: $TO_MAIL \n";
```

```
        print MAIL "Subject: $SUBJECT \n\n";
        print MAIL "Host: $HOSTNAME \n";
        print MAIL "$TASK_CONFIRM \n";
close(MAIL);
  }
```

위와 같이 설정후에는 매일 자동으로 파일 시스템의 무결성을 체크하여 변경이 있을 경우에는 변경된 내용을 관리자에게 메일로 통보해준다.
만약 통보된 변화가 정상적인 것이라면 관리자는 “fcheck –ac” 명령을 이용하여 데이터 베이스를 새로운 정보로 업데이트 하면 된다.