리눅스에서 로그인 실패 시도 모니터링하기

Sandra Henry-Stocker | Network World 2020.12.02

리눅스 서버에서 로그인 시도 실패가 반복적으로 나타나면, 누군가 계정 침입을 시도하는 것일 수도 있고, 단순히 비밀번호를 잊었거나 잘못 입력하는 상황을 의미할 수도 있다. 이 기사에서는 로그인 실패 시도를 점검하고 시스템 설정에서 계정이 잠기는 조건을 확인해서 문제에 대처하는 방법을 살펴본다.

가장 먼저 알아야 할 것은 로그인 실패를 확인하는 방법이다. 아래 명령은 우분투 및 관련 시스템에 사용되는 /var/log/auth.log 파일에서 로그인 실패를 찾는다. 누군가 틀린 비밀번호를 사용해 로그인을 시도할 경우 로그인 실패는 아래 라인과 같이 표시된다.

```
$ sudo grep "Failed password" /var/log/auth.log | head -3
Nov 17 15:08:39 localhost sshd[621893]: Failed password for nemo from 192.168.0.7 port 8132 ssh2
Nov 17 15:09:13 localhost sshd[621893]: Failed password for nemo from 192.168.0.7 port 8132 ssh2
```

다음과 같은 명령으로 로그인 실패 인스턴스를 계정별로 요약 표시할 수 있다.

```
$ sudo grep "Failed password" /var/log/auth.log | grep -v COMMAND | awk '{print $9}' | sort | uniq -c
     22 nemo
      1 shs
      2 times:
```

이 명령은 로그인 실패를 사용자 이름별로(grep 출력의 9번째 열) 요약한다. “Failed passwords” 문구가 포함된 조회(예를 들어 누군가 위에 실행된 명령을 실행하는 경우)를 건너뛰기 위해 “COMMAND”라는 단어가 포함된 라인은 확인하지 않고 넘어간다. “times:” 문자열

은 보고된 횟수보다 더 많은 반복적 시도가 있었음을 나타낸다. 이 정보의 출처는 비밀번호가 단시간 내에 연속적으로 여러 차례 잘못 입력되는 경우 로그 파일에 추가될 수 있는 “message repeated 5 times:"라는 문구가 포함된 라인이다.

확인해야 할 또 다른 요소는 로그인 실패 시도가 이뤄진 장소다. 이 경우 다음 예제와 같이 필드를 9번째에서 11번째로 바꾼다.

```
$ sudo grep "Failed password" /var/log/auth.log | grep -v COMMAND | awk '{print $11}' | sort | uniq -c
     23 192.168.0.7
```

예를 들어 한 시스템에서 여러 사용자의 로그인 실패가 나타난다면 특별히 의심스러운 상황으로 볼 수 있다.

RHEL, 센트OS(CentOS) 및 관련 시스템의 경우 **/var/log/secure** 파일에서 로그인 실패와 관련된 메시지를 볼 수 있다. 위와 기본적으로 동일한 쿼리를 사용해서 횟수를 확인할 수 있다. 다음과 같이 파일 이름만 바꾸면 된다.

```
$ sudo grep "Failed password" /var/log/secure | awk '{print $9}' | sort | uniq -c
      6 nemo
```

/etc/pam.d/password-auth 및 **/etc/pam.d/system-auth** 파일의 설정을 확인한다. 이와 같은 라인을 추가하면 설정이 적용된다.

faillog 확인

faillog 명령도 살펴볼 수 있지만, 이 명령이 확인하는 /var/log/faillog 파일은 요즘 그다지 사용되지 않는 것 같다. faillog -a 명령을 사용해서 아래와 같이 시간 열에 12/31/69가 나열된 결과를 얻는다면 이 파일은 사용되지 않는 것이 확실하다.

```
$ faillog -a
```

```
Login        Failures Maximum Latest                      On

root            0        0   12/31/69 19:00:00 -0500
daemon          0        0   12/31/69 19:00:00 -0500
bin             0        0   12/31/69 19:00:00 -0500
sys             0        0   12/31/69 19:00:00 -0500
```

여기 표시된 날짜와 시간은 유닉스의 시작일(01/01/70)을 가리킨다(로컬 시간대에 따라 보정될 수 있음). 아래의 명령을 실행하면 파일이 비어 있지는 않지만 실질적인 데이터를 포함하고 있지도 않음을 확인할 수 있다.

```
$ ls -l /var/log/faillog
-rw-r--r-- 1 root root 32576 Nov 12 12:12 /var/log/faillog
$ od -bc /var/log/faillog
0000000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
000 000
          \0  \0  \0  \0  \0  \0  \0  \0  \0  \0  \0  \0  \0  \0  \0  \0
\0
*
0077500
```

faillog 파일이 실제로 사용된다면 1969년이 아닌 최근 활동이 나타날 것이다.

대응 방법

로그인 실패가 발생하는 이유는 많다. 사용자 한 명이 caps-lock 키가 켜진 줄 모르고 로그인을 시도했을 수도 있고, 최근 비밀번호를 변경했지만 그 사실을 잊고 예전 비밀번호를 입력했을 수도 있고, 다른 시스템용 비밀번호를 착각해 입력했을 수도 있다. 쿼리를 실행할 때마다 어느 한 계정이 자주 눈에 나타난다면 조사를 해보는 것이 좋다. 그러나 간헐적인 로그인 시도 실패는 흔히 발생하는 일이다.

설정 확인

로그인 실패 처리에 있어 시스템이 어떻게 설정되어 있는지 보려면 **/etc/pam.d/common-auth** 파일을 확인한다. 이 파일은 리눅스 플러그형 인증 모듈(PAM)이 있는 시스템에 사용된다. 이 파일에서 계정을 임시로 잠그기 전까지 허용할 로그인 시도 실패 횟수와 계정을 잠그는 기간을 제어하는 설정은 두 가지다.

이와 같은 라인의 경우 PAM은 6번의 로그인 시도 실패 후 계정을 잠그고, 잠금 기간은 5분(300초)이다.

```
auth  required  pam_tally2.so deny=6 unlock_time=300
```

정리

이따금 나타나는 로그인 실패는 흔한 일이다. 그러나 시스템이 어떻게 구성되어 있는지 잘 파악하고 쿼리를 실행해서 이런 활동 유형이 얼마만큼 발생하는지 파악하는 것이 좋다. 쿼리를 **cron** 작업으로 실행하고 그 결과를 자기 자신에게 이메일로 보내는 방법을 추천한다. editor@itworld.co.kr