

목차

sshd[xxxx]: Did not receive identification string from a.b.c.d	3
---	----------

sshd[xxxx]: Did not receive identification string from a.b.c.d

sshd[1234]: Did not receive identification string from 127.0.0.1

해당 메시지는 sshd 서비스에 접근하여 login/password 입력 행위등이 없이 접속만 하고 바로 연결을 끊었을 경우 발생하는 경우 나타내는 메시지이며, sshd port scan 이 이루어 졌을때도 나타납니다.

해당 로그가 지속적으로 찍힐 경우 아래와 같은 경우를 의심 및 확인 해 봐야 한다.

- 서버에 네트워크 모니터링 서비스가 실행되고 있을 경우
- 지속적인 포트 스캔 해킹 시도

간단하게 해당 로그가 찍히는것을 방지 하기 위한 방법으로는 아래와 같이 설정 하면 된다.

1. sshd 포트를 변경하는 것이다.

```
# vim /etc/ssh/sshd_config  
port 22 -> port 5022
```

2. vsftpd 포트 변경

```
# vim /etc/vsftpd/vsftpd.conf  
port 21 -> 50021
```

3. iptables 를 이용하여 공격 IP 차단

```
#iptables -A INPUT -s 127.0.0.1 -j REJECT ( or DROP )
```

4. rsyslog 를 이용하여 시스템에서 메시지 필터링

```
# vim /etc/rsyslog.conf  
##### RULES #####  
: meg, contains, "Did not receive identification string from 127.0.0.1" ~
```

redhat solution url <https://access.redhat.com/solutions/98293>

From:
<https://atl.kr/dokuwiki/> - **AllThatLinux!**

Permanent link:
https://atl.kr/dokuwiki/doku.php/did_not_receive_identification_string_from



Last update: **2016/02/04 07:29**