### Syslog 수신 진단

웹 관리 콘솔에서 수집기를 설정해도 전달 서버를 경유하여 Syslog가 정상적으로 수집되지 않는 경우에는 아래와 같이 진단합니다. 아래 예시에서는 IP 주소 172.20.100.100에서 패킷을 전송한다고 가정합니다.

#### 전달 서버 트레이스

리눅스 셸에서 아래 명령어로 로그프레소 셸에 진입합니다.

$ ssh -p7022 root@localhost

Syslog 서버 설정 목록을 조회합니다.

logpresso> syslog.serversSyslog Servers----------------[logpresso] 0.0.0.0:514 (udp), charset=UTF-8 (override: 0), capacity=20000, rx\_buf\_size=0, receiver\_cpu\_id=-1, queue\_count=1, buffer\_file\_path=./, buffer\_file\_size=10737418240, start from=2024-12-11 13:22:13, received=7

아래와 같이 클라이언트 IP 주소별 수신 통계를 조회할 수 있습니다.

logpresso> syslog.stats logpressoSyslog Statistics-------------------x.x.x.x => 1 (first seen 2025-01-20 10:58:44, last seen 2025-01-20 10:58:44)

아래와 같이 실시간으로 수신되는 Syslog 패킷 내용을 추적할 수 있습니다. Ctrl+C 키 조합으로 중단합니다.

logpresso> syslog.trace logpressopress ctrl-c to stop------------------------

#### Syslog 패킷 확인

tcpdump 명령어를 이용하여 패킷이 로그프레소 전달 서버에 도달하는지 검증합니다.

# tcpdump -i any host 172.20.100.100 port 514 -A

#### 포트 개방 확인

전달 서버에 Syslog 패킷이 도달하고 있는 것이 확인되었다면 포트가 열려있는지 확인합니다.

# netstat -na | grep :514udp 0 0 0.0.0.0:514 0.0.0.0:\*

위와 같이 포트가 열려있지 않다면 설치 단계에서 [JVM 권한 부여 단계](https://docs.logpresso.com/ko/sonar/4.0/forwarder/ko/sonar/4.0/forwarder/deploy-forwarder)를 누락하여 포트 개방에 실패했거나, 포트 설정이 변경되었을 수 있습니다.

아래 명령어를 실행하여 cap\_net\_raw가 출력되는지 확인합니다.

# getcap /opt/logpresso/java/jdk-11.0.14.1-jemalloc/bin/java

권한이 부여되어 있지 않다면 setcap 단계를 다시 수행하고 데몬을 재시작합니다.

#### 호스트 방화벽 정책 확인

Syslog 패킷이 수신되고 514 포트가 열려있는데 로그가 수신되지 않는다면 호스트 방화벽 정책을 다시 확인합니다.

# firewall-cmd --list-ports

#### rp\_filter 설정 확인

방화벽 정책, 포트 개방 상태가 모두 정상인데 로그프레소 셸에서 syslog.trace 명령으로 수신을 확인할 수 없는 경우에는 Reverse Path Filtering 문제일 수 있습니다.

리눅스 커널의 [Reverse Path Filtering](https://tldp.org/HOWTO/Adv-Routing-HOWTO/lartc.kernel.rpf.html) 기능은 패킷의 출처를 확인하여 스푸핑된 패킷을 차단하는 기능입니다. 기본값은 1로 설정되어 있으며 유효하지 않은 경로에서 들어오는 패킷을 버립니다.

즉, 전달 서버에 여러 개의 네트워크 인터페이스 카드가 구성된 경우에 발생할 수 있는 문제이며, 아래와 같이 설정을 변경한 후 패킷이 정상적으로 수신되는지 다시 확인합니다.

**기존 설정 확인**

예를 들어 eth2 인터페이스라면 아래와 같이 명령어를 입력합니다.

# cat /proc/sys/net/ipv4/conf/eth2/rp\_filter1

/etc/sysctl.conf 파일 끝에 아래 설정을 추가합니다.

net.ipv4.conf.eth2.rp\_filter = 2

관리자 권한으로 아래 명령어를 실행하여 커널 설정을 변경합니다.

# sysctl -p

**rp\_filter 설정 값**

* 0 (비활성화): Reverse Path Filtering을 수행하지 않음
* 1 (기본값, 엄격): 패킷의 출발지 IP 주소를 기준으로 해당 인터페이스의 경로를 확인하고, 일치하지 않으면 패킷을 드롭
* 2 (느슨함): 동일한 출발지 IP 주소를 가진 패킷이 어느 인터페이스를 통해서든 유효한 경로를 가지면 허용