7. SYSLOG

2016년 지방 1과제

syslog 항목에 대한 풀이집

2016

SUN-srv1로 들어오는 ICMP 패킷을 로그로 기록하기 위해  
syslog-ng 패키지를 사용합니다.

이때, 기록 시 ‘customlog ‘라는 문자열이 붙어 기록되어야 합니다.

로그를 기록하기 위해 IPTABLES를 작성합니다.

<SUN-srv1>

root@SUN-srv1:~# **vi /etc/rc.loca**l



root@SUN-srv1:~# **vi /etc/syslog-ng/syslog-ng.conf**



root@SUN-srv1:~# **systemctl restart syslog-ng**

root@SUN-srv1:~# **tail -f /ZFS/log/ICMP.log**

위와 같이 Follow를 설정한 후

클라이언트에서 SUN-srv1로 핑을 테스트한 후 SUN-srv1에서 확인합니다.



