엔터프라이즈 서버관리

14. 로그 분석

SangJun, Im

Department of Computer Science
e_mail : imsangjun@gmail.com

로그 분석 개요

- 주요 대상
  - 시스템 로그
  - 서비스(어플리케이션) 로그
  - 기타 로그

- 시스템 로그
  - secure
  - messages
  - Lastlog 등

- 어플리케이션 로그
  - Web (access_log, error_log 등)
  - Database log

로그 분석

- **분석 솔루션 소개**
  - **GoAccess Features** (https://goaccess.io)
    - 소스코드 컴파일
    - goaccess access.log -c
    - goaccess access.log -o report.html --log-format=common
  - $ wget https://tar.goaccess.io/goaccess-1.7.2.tar.gz
  - $ tar -xzvf goaccess-1.7.2.tar.gz
  - $ cd goaccess-1.7.2/
  - $ ./configure --enable-utf8 --enable-geoip=mmdb
  - $ make
  - # make install
  - #yum install goaccess
  - #goaccess access_log –c
  - #goaccess access_log -o report.html --log-format=COMBINED
  - **logwatch**
    - yum install logwatch
    - logwatch --logfile secure
  - **ksar**
    - https://github.com/vlsi/ksar/releases/download/v5.2.3/ksar-5.2.3-all.jar

yum install ncurses-devel
yum install libmaxminddb-devel

로그 분석 기타

- 분석 솔루션 기타
  - https://www.splunk.com/
  - https://www.elastic.co/kr/logstash

과제

- 소개된 goaccess 를 이용하여 자신의 웹서버의 access_log 를 분석한 결과 제출
  - 자신의 서버에 웹 기반(report.html)으로 제공

END