로그 한 줄에 담기는 정보 정리 (메모장/텍스트용)

1) 핵심 개념 - 로그 한 줄에는 보통 "언제(시간) / 어디서(호스트) / 누가(계정·프로세스) / 무엇을(요청·행위) / 결과(상태·에러) / 부가정보(지연시간·바이트·포트·프로토콜 등)"가 함께 들어감 - 목표: 한 줄에서 '필드(컬럼)'를 뽑아내고, 기준별로 집계(TOP)해서 이상징후를 빨리 찾는 것

---

2) Access 로그(웹서버: Nginx/Apache)

(예시: combined 계열) 203.0.113.10 - - [09/Feb/2026:12:34:56 +0900] "GET /login HTTP/1.1" 200 1234 "https://example.com" "Mozilla/5.0" 0.043

(필드 의미) - 203.0.113.10 : 클라이언트 IP - [..] : 요청 시간 - "GET /login HTTP/1.1" : HTTP 메서드 / URI / 프로토콜 - 200 : 상태코드(성공/리다이렉트/클라에러/서버에러) - 1234 : 응답 바이트 수 - Referer : 유입 경로 - User-Agent : 브라우저/봇 식별 - 0.043 : 처리시간(초) (포맷 설정에 따라 없을 수도 있음)

(바로 해볼 집계 아이디어) - 상태코드 TOP - URI TOP - 느린 요청(예: 1초 이상) 필터링

---

3) MySQL 로그(종류별로 포맷이 다름)

3-1) Error log (서버 에러/시작/경고/크래시) (예시) 2026-02-09T03:12:01.123456Z 0 [ERROR] [MY-010123] [Server] Can't open file: ...

(포인트) - 시간 / 스레드ID / 레벨(ERROR/WARNING/Note) / 에러코드 / 메시지

3-2) Slow query log (느린 쿼리) (예시)

Time: 2026-02-09T12:30:11.123456Z

User@Host: app[app] @ 203.0.113.10 [] Id: 12345

Query_time: 2.341 Lock_time: 0.001 Rows_sent: 10 Rows_examined: 200000

SELECT ...;

(포인트) - 누가(User) / 어디서(Host·IP) / 얼마나 느렸는지(Query_time) / 얼마나 읽었는지(Rows_examined) - 성능/인덱스/쿼리 튜닝 감 잡는 데 가장 실전적

3-3) General log / Audit log - 접속/쿼리 이벤트가 남음 - 운영에서는 성능 부담 때문에 꺼져 있는 경우가 많고, 보안/감사 목적이면 Audit 로그를 쓰기도 함

---

4) Firewall 로그(리눅스 iptables/ufw 또는 장비 로그)

(예시) Feb 9 12:34:56 host kernel: [UFW BLOCK] IN=eth0 OUT= MAC=... SRC=203.0.113.10 DST=192.168.0.10 LEN=60 TOS=0x00 TTL=51 PROTO=TCP SPT=54321 DPT=22 SYN

(필드 의미) - IN=eth0 / OUT= : 인/아웃 인터페이스 - SRC= / DST= : 출발지/목적지 IP - PROTO=TCP : 프로토콜(TCP/UDP/ICMP 등) - SPT= / DPT= : 출발지 포트 / 목적지 포트 - SYN : TCP 플래그(연결 시도)

(포인트) - 방화벽 로그는 IP만이 아니라 "PROTO + PORT"가 핵심인 경우가 많음 - 어떤 서비스(22/3389/3306 등)를 두드렸는지로 공격/스캔 성격이 보이는 경우가 많음

(집계 아이디어) - 목적지 포트(DPT) TOP - 출발지 IP(SRC) TOP

---

5) Error 로그(범위가 넓음: 시스템/앱 공통)

5-1) Linux auth.log(SSH 로그인 실패 등) (예시) Feb 9 12:35:01 host sshd[1234]: Failed password for invalid user admin from 203.0.113.10 port 54321 ssh2

(포인트) - 어떤 서비스(sshd)에서 - 어떤 계정 시도(invalid user admin) - 어디서(IP) - 어떤 포트(port) - 결과(Failed)

(집계 아이디어) - Failed password IP TOP - 특정 IP가 임계치(예: 10회) 넘으면 ALERT

5-2) 애플리케이션 로그(Spring/PHP 등) - 흔한 구성: timestamp / level / traceId(MDC) / 클래스 / 메시지 / 스택트레이스 - 운영 포인트: 요청 단위 추적(traceId), 에러 스택, 응답시간

---

6) 실습을 “로그 한 줄 구조 이해”로 확장하는 3단계 미션

미션 A) access.log 샘플 만들기 - 상태코드 TOP - URI TOP - 느린 요청 필터

미션 B) firewall.log 샘플 만들기 - DPT TOP 5 - SRC TOP 5

미션 C) auth.log 샘플 만들기 - Failed login IP TOP - 10회 이상이면 [ALERT]로 리포트에 표시

---

7) 기억 포인트(한 줄 요약) - Access 로그: "IP + 시간 + 메서드/URI + 상태코드 + (UA/리퍼러/지연시간)" - Firewall 로그: "SRC/DST + PROTO(TCP/UDP) + SPT/DPT + (SYN 등 플래그)" - MySQL Slow 로그: "User/Host + Query_time + Rows_examined" - Auth 로그: "로그인 실패(계정) + IP + 포트 + 결과"

원하면, 지금 쓰는 분석 스크립트 스타일(리포트 생성 방식)로 access/firewall/auth까지 한 번에 TOP 집계하는 형태로 확장 설계도 같이 정리해줄 수 있음.