Engineer

Logging

å skrive ned det som skjer, mens det skjer

Hva det er

Logging, også kalt hendelseslogging, er at et program fører en løpende beretning om sin egen oppførsel, med én oppføring per hendelse: en forespørsel som ble besvart, et passord som ble avvist, et nytt forsøk, et krasj. Hver oppføring, en logglinje eller loggpost, har minst et tidspunkt og en melding, slik at noen senere kan rekonstruere hva som skjedde, og i hvilken rekkefølge. OpenTelemetry-prosjektet definerer en logg som en tekstpost med tidsstempel, strukturert eller ustrukturert, med valgfrie metadata, og bemerker at av alle telemetrisignalene er det loggene som bærer på mest arv fra fortiden.

Den arven har en standard. Syslog, den gamle protokollen for å sende hendelsesmeldinger videre til en innsamler, ble standardisert som RFC 5424 i mars 2009. Den gjør den eldre RFC 3164 foreldet og gir hver melding én av åtte alvorlighetsgrader, fra 0 for Emergency til 7 for Debug. De fleste loggbiblioteker har en kortere stige bygd på den samme ideen: debug, info, warning, error. Loggdatamodellen i OpenTelemetry legger alle sammen på ett tall fra 1 til 24, fordelt på seks bånd fra TRACE til FATAL.

En ustrukturert linje er fritekst: lett for et menneske å lese, og noe en maskin bare kan plukke fra hverandre med et regulært uttrykk skrevet for akkurat den ordlyden. En strukturert linje følger et fast skjema, så hver oppføring har de samme navngitte feltene, med de samme typene og den samme betydningen. OpenTelemetry foretrekker strukturerte logger i produksjon og legger til en advarsel som er lett å overse: en linje kodet som JSON er ikke strukturert bare fordi den lar seg tolke; det som gjør den strukturert, er et stabilt skjema. Her er en strukturert oppføring vist over flere linjer, men på disken er den én enkelt linje:

```
{
    "time": "2026-09-14T03:12:07.412Z",
    "severity": "WARN",
    "service": "checkout",
    "event": "payment.retry",
    "attempt": 3,
    "trace_id": "4bf92f3577b34da6a3ce929d0e0e4736"
}
```

Metrikker og sporinger, traces på engelsk, er signalene som vanligvis samles inn ved siden av loggen. Metrikker er tall som måles over tid, billige å ta vare på og gode til å si hvor ofte noe skjer. En sporing følger én forespørsel gjennom hver tjeneste den berører. En logg tar vare på detaljene i enkelthendelser, og det gjør den til det noen leser etter et driftsvarsel for å finne ut hvorfor. OpenTelemetry knytter logger til sporinger ved å feste ID-ene til den aktive sporingen og det aktive spennet, span, på hver loggpost.

Bruk begrepet i en beslutning

Bruk «Hva er logging?» i en konkret beslutning. Vi kan knytte begrepet til systemet dere bygger eller kjøper. Overvåking og varsler som sier fra mens en feil fortsatt er liten, og tallene som viser hvor ofte den holder seg liten.

Se tjenestene våre Ta kontakt →

Undersøk antakelsene bak ordet

Bruk forklaringen og det tilknyttede arbeidet til å formulere spørsmål for prosjektet. Vi kan undersøke antakelsene sammen før et verktøy velges. Bygde selskapets første observerbarhetsdashbord — selskapets første innsyn i egne systemer

Bygde selskapets første observerbarhetsdashbord Ta kontakt →

Hvorfor det er viktig

En logg er den eneste beretningen om fortiden de fleste systemer etterlater seg. En metrikk kan si at feilene økte klokken 03.12; loggen sier hvilken forespørsel det gjaldt, fra hvilken tjeneste, med hvilken verdi, og hva programmet gjorde etterpå. Når noe går i stykker om natten og har hentet seg inn igjen til morgenen, er loggen vitnet som fortsatt er der.

Den beretningen har en pris, og den betales på tre måter. Hver linje koster diskplass, lese- og skriveoperasjoner og prosessortid, og enda mer hvis den sendes videre til et sentralt lager, der en innkjøpt loggtjeneste som regel tar betalt etter hvor mye som tas inn. Hver linje er også data om noen: tilgangsloggen til en webserver inneholder adressene og nettleserne til alle som har vært innom. Og hver linje må voktes. OWASP Logging Cheat Sheet ber om at

hver hendelse registrerer når, hvor, hvem og hva, og at selve loggene beskyttes mot manipulering og mot uautorisert tilgang, endring og sletting, fordi de kan inneholde personopplysninger og andre sensitive opplysninger.

For en hel organisasjon blir dette et spørsmål om mer enn ett program. NIST Special Publication 800-92, Guide to Computer Security Log Management, skrevet av Karen Kent og Murugiah Souppaya og utgitt i september 2006, behandler loggforvaltning som infrastruktur og prosesser som drives på tvers av hele virksomheten, ikke som en innstilling i ett enkelt program.

Logger gjør også mest nytte ved siden av tall. Veiledningen for instrumentering fra Prometheus-prosjektet foreslår en teller for hver linje med loggekode, slik at du, når en interessant melding dukker opp, kan se hvor ofte den har kommet, og hvor lenge det har pågått. Den foreslår også å sammenligne summene av linjer på nivåene info, warning og error fra én utgivelse til den neste.

Slik ser det ut i praksis

Nettstedets egen tilgangslogg er beskrevet linje for linje på personvernsiden. Hver forespørsel registrerer siden og tidspunktet, svarstatusen, nettleserens beskrivelse av seg selv, navnet på nettstedet den besøkende kom fra, og en tilslørt nettverksadresse: siste del erstattes med nuller i det øyeblikket linjen skrives, før noe når disken. En linje lever i omtrent tretti dager. Serverprogramvaren lukker hver fil én gang i døgnet, eller tidligere ved omtrent 10 MB, og sletter en lukket fil tjueåtte dager senere, og hver natt leser en kontroll gjennom alle filene og feiler hvis en linje er eldre enn tretti dager. Det har gått galt to ganger, og personvernsiden forteller om begge. I september 2026 fylte de stille adressene 10 MB så sakte at filene deres aldri hadde blitt lukket, og de inneholdt fortsatt hver linje siden loggingen ble slått på, så det ble lagt til en daglig jobb som skulle lukke dem. Den 26. oktober 2026 skrev sju av de tretten adressene som fører logg, fortsatt til filer jobben hadde merket som lukket, og én hadde en lukket fil som var førtisju dager gammel. Jobben er fjernet, og nå lukker og sletter serverprogramvaren filene selv.

En fullstendig testkjøring av en macOS-applikasjon registrerte 610 996 core-logglinjer. En bølge av core-logghendelser ble beholdt i en ubegrenset hovedstrøm og kopiert til abonnentstrømmer der konsumentene ikke brukte dem. Hendelsesdokumentasjonen omtaler separat diagnoserapporter som viste 111 GB komprimerte sider på en maskin med 36 GB, og en stikkprøvemåling av minnebruken som viste en vekst på omtrent 41 MB per sekund under en løkke

med gjentatte tilkoblingsforsøk. Avgrensede buffere, abonnementer filtrert etter hendelsestype og et frekvensbudsjett for loggingen rettet opp denne hendelsesbehandlingen. I den dokumenterte sammenligningen av fullstendige testkjøringer sank antallet core-logglinjer til 1 411. Dette er ikke en ytelsesmåling i produksjon eller en målt verdi for minnebruk etter rettingen. Budsjettet forkaster informasjon med vilje: gjentatte diagnosehendelser kan forkastes, og berørt tilstand kan oppdateres i stedet for å beholde et ubegrenset antall hendelser. Separate tidsavbrudd ved avslutning krevde en egen retting.

På en produksjonsvert avdekket en herdingsrunde over tretten systemd-enheter ett direktiv som hadde vært feilstavet i tre enhetsmaler så lenge de rollene hadde eksistert. Tjenestestyreren svarer på en nøkkel den ikke kjenner igjen, ved å logge det og starte enheten likevel, så det eneste sporet av feilen var en advarsel i en logg. Den kom for dagen mens enhetene ble skrevet om. Nå går hver enhet gjennom tjenestestyrerens eget verifiseringsverktøy ved hver konvergering, så den samme skrivefeilen får en kjøring til å feile.

Hvor det går galt

Loggen vokser raskest når systemet allerede svikter. En løkke som logger hvert nytt forsøk, skriver en håndfull linjer på en god dag og tusenvis i sekundet på en dårlig, og tar disk, minne og prosessortid fra et system som ikke har noe å avse. OWASP ber team verifisere at loggingen ikke kan brukes til å tømme systemets ressurser, for eksempel ved å fylle disken. Gi hver kodesti som kjører tett, et budsjett, slå sammen gjentatte meldinger til én linje med et antall, og hold en teller ved siden av meldingen, så frekvensen overlever når linjer blir kastet.

Hemmeligheter og personopplysninger blir skrevet ned. En forespørsel som logges i sin helhet, bærer med seg alt som var i den. OWASP har en liste over det som som regel bør fjernes, maskeres, hashes eller krypteres før det når en logg, og den omfatter sesjons-ID-er, tilgangstokener, passord, tilkoblingsstrenger til databaser, krypteringsnøkler og betalingskortdata. Gjør det i det øyeblikket linjen skrives, slik tilgangsloggen ovenfor gjør med adressene, fordi linjen kan ligge i en sikkerhetskopi eller et arkiv før noen rekker å rydde.

Inndata utenfra skriver en falsk linje. En verdi fra en bruker som inneholder et vognretur- eller linjeskifttegn, og som skrives rett inn i en tekstlogg uten at tegnene kodes om, kan starte en ny linje som ser nøyaktig ut som en linje applikasjonen selv har skrevet. OWASP kaller dette logginjeksjon og ber om at

slike tegn renses, og at data kodes for det formatet de skrives i. En strukturert logger som skriver hver verdi som en JSON-streng med spesialtegnene kodet om, gjør dette uten at noen må huske det.

En logg som blir stille, ser ut som et friskt system. En full disk, en rotert fil som programmet aldri åpnet på nytt, eller en innsamler som gikk ned, ser like ut utenfra: linjene slutter å komme. OWASP ber om en måte å oppdage at loggingen har stoppet på. Tell linjer per minutt for hver kilde, og la et driftsvarsel gå når et antall faller til null, slik at et hull i loggen blir en alarm i seg selv.

Les mer

- Logs — OpenTelemetry om hva en logg er, hvorfor strukturerte logger foretrekkes, og hvordan logger knyttes til sporinger.
- Logs Data Model — feltene i en loggpost, de to tidsstemplene og alvorlighetsskalaen fra 1 til 24.
- RFC 5424: The Syslog Protocol — meldingsformatet i syslog og de åtte alvorlighetsgradene.
- NIST SP 800-92 — Guide to Computer Security Log Management, veiledningen om loggforvaltning i en hel virksomhet.
- Logging Cheat Sheet — OWASP om hvilke hendelser som bør registreres, hvilke data som skal holdes utenfor, og hvordan resultatet beskyttes.
- Instrumentation — Prometheus-prosjektets praksis for å instrumentere kode, logging medregnet.

Ordliste

Velg ut fra deres faktiske rammer

Ta med utrullingsløpet, driftsrisikoene og dem som har vakt. Vi kan avgrense en endring med kontroller, en vei tilbake og tydelig ansvar.

Se hva det koster Ta kontakt →

Gjør begrepene praktiske

Spør hvordan «Hva er logging?» gjelder i organisasjonen deres. Et konkret eksempel fra dagens system er nok til å starte samtalen.

Se tjenestene våre

welcome@engineer.company +45 50 10 61 84 København, Danmark

Ta med deg denne siden

Visittkort

Laget med kjærlighet av D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Opphavsrett © 2025 – nå · Engineer ApS · Alle rettigheter forbeholdt.

Skrevet ut fra https://engineer.company/nb/glossary/logging/