Engineer

Logning

at skrive ned, hvad der sker, mens det sker

Hvad det er

Logning, også kaldet hændelseslogning, er et program, der løbende fører regnskab med sin egen opførsel, én post pr. hændelse: en forespørgsel besvaret, en adgangskode afvist, et genforsøg, et nedbrud. Hver post, en loglinje eller logpost, bærer mindst et tidspunkt og en besked, så nogen bagefter kan stykke sammen, hvad der skete, og i hvilken rækkefølge. OpenTelemetry-projektet definerer en log som en tekstpost med tidsstempel, struktureret eller ustruktureret, med valgfrie metadata, og bemærker, at af alle telemetrisignalerne har logge den største arv.

Den arv har en standard. Syslog, den mangeårige protokol til at sende hændelsesbeskeder videre til en opsamler, blev standardiseret i marts 2009 som RFC 5424, der erstatter den ældre RFC 3164, og den giver hver besked én af otte alvorsgrader, fra 0 for Emergency til 7 for Debug. De fleste logbiblioteker har en kortere stige med samme idé: debug, info, warning, error. OpenTelemetrys logdatamodel lægger dem alle ind på ét tal fra 1 til 24, i seks bånd fra TRACE til FATAL.

En ustruktureret linje er fri tekst: let for et menneske at læse, og noget en maskine kun kan skille ad med et regulært udtryk skrevet til netop den ordlyd. En struktureret linje følger et skema, så hver post har de samme navngivne felter med de samme typer og betydninger. OpenTelemetry foretrækker strukturerede logge i produktion og tilføjer en advarsel, der er let at overse: en linje kodet som JSON er ikke struktureret, blot fordi den kan parses; det, der gør den struktureret, er et stabilt skema. Her vist over flere linjer er en struktureret post én linje på disken:

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

Metrikker og traces er de signaler, der normalt samles ind ved siden af. Metrikker er tal målt over tid, billige at gemme og gode til at sige, hvor tit noget sker. Traces følger én forespørgsel gennem hver tjeneste, den berører. En log gemmer detaljen i de enkelte hændelser, og derfor er den det, nogen læser efter en alarm for at finde ud af hvorfor. OpenTelemetry binder logge til traces ved at hæfte id'erne for den aktive trace og det aktive span på hver logpost.

Brug begrebet i en beslutning

Brug »Hvad er logning?« i en konkret beslutning. Vi kan knytte begrebet til det system, I bygger eller køber. Overvågning og alarmer, der siger til, mens fejlen stadig er lille, og tallene, der viser, hvor tit den bliver ved med at være det.

Se vores ydelser Kontakt os →

Undersøg antagelserne bag ordet

Brug forklaringen og det tilknyttede arbejde til at formulere spørgsmål til jeres projekt. Vi kan undersøge antagelserne sammen, før et værktøj vælges. Har bygget det første observerbarhedsdashboard — virksomhedens første overblik over sine egne systemer

Har bygget det første observerbarhedsdashboard Kontakt os →

Hvorfor det betyder noget

En log er den eneste beretning om fortiden, de fleste systemer efterlader sig. En metrik kan sige, at fejlene steg kl. 03.12; loggen siger hvilken forespørgsel, fra hvilken tjeneste, med hvilken værdi, og hvad programmet gjorde bagefter. Når noget går i stykker om natten og er kommet sig om morgenen, er loggen det vidne, der stadig er der.

Den beretning har en pris, som betales på tre måder. Hver linje koster disk, input og output og processortid, og mere endnu, hvis den sendes til et centralt lager, hvor en hostet tjeneste typisk tager betaling efter den mængde, der modtages. Hver linje er også data om nogen: en webservers adgangslog rummer adresser og browsere for alle, der har kaldt den. Og hver linje skal beskyttes. OWASP's Logging Cheat Sheet beder om, at hver hændelse registrerer hvornår, hvor, hvem

og hvad, og at selve loggene beskyttes mod manipulation og mod uautoriseret adgang, ændring og sletning, fordi de kan indeholde personoplysninger og andre følsomme oplysninger.

I en organisations målestok behandler NIST Special Publication 800-92, Guide to Computer Security Log Management af Karen Kent og Murugiah Souppaya, udgivet i september 2006, loghåndtering som infrastruktur og processer på tværs af hele virksomheden frem for en indstilling i ét program.

Logge virker også bedst ved siden af tal. Prometheus-projektets vejledning om instrumentering foreslår en tæller for hver linje logkode, så man, når en interessant besked dukker op, kan se, hvor tit den er sket, og hvor længe, og foreslår at sammenligne antallet af info-, warning- og error-linjer fra én udgivelse til den næste.

Sådan ser det ud i praksis

Sitets egen adgangslog er beskrevet linje for linje på siden om privatliv. Hver forespørgsel registrerer siden og tidspunktet, svarets status, browserens beskrivelse af sig selv, navnet på det site, der henviste, og en sløret netværksadresse: den sidste del erstattes med nuller i det øjeblik, linjen skrives, før noget rører disken. En linje lever i omkring tredive dage. Serverprogrammet lukker hver fil en gang i døgnet, eller tidligere ved omkring 10 MB, og sletter en lukket fil otteogtyve dage senere, og hver nat læser en kontrol alle filer igennem og slår fejl, hvis en linje er ældre end tredive dage. Det er gået galt to gange, og siden om privatliv fortæller om begge. I september 2026 fyldte de stille adresser 10 MB så langsomt, at deres filer aldrig var blevet lukket og stadig rummede hver linje, siden logningen blev slået til, så der blev sat et dagligt job op til at lukke dem. Den 26. oktober 2026 skrev syv af de tretten adresser, der fører log, stadig i filer, som jobbet havde markeret som lukkede, og én havde en lukket fil, der var syvogfyrre dage gammel. Jobbet er fjernet, og nu lukker og sletter serverprogrammet selv filerne.

En fuld testkørsel af en macOS-applikation registrerede 610.996 core-loglinjer. En byge af core-loghændelser blev beholdt i en ubegrænset hovedstrøm og kopieret til abonnentstrømme, hvis forbrugere ikke brugte dem. Hændelsesbeskrivelsen dokumenterer separat diagnoserapporter med 111 GB komprimerede sider på en maskine med 36 GB og en måling af hukommelsesforbruget, som viste en vækst på omkring 41 MB i sekundet under en løkke med gentagne forbindelsesforsøg. Afgrænsede buffere, abonnementer

filtreret efter hændelsestype og et hastighedsbudget for logning håndterede den hændelsesvej. I den registrerede sammenligning af fulde testkørsler faldt antallet af core-loglinjer til 1.411. Det er ikke et benchmark fra produktion eller en måling af hukommelsesforbruget efter rettelsen. Budgettet kasserer information med vilje: gentagne diagnostiske hændelser kan kasseres, og den berørte tilstand genindlæses i stedet for at beholde ubegrænset mange hændelser. Separate timeouts ved nedlukning krævede deres egen rettelse.

På en produktionsvært fandt en hærdning af tretten systemd-units ét direktiv, der var stavet forkert i tre unit-skabeloner, så længe de roller havde eksisteret. Servicemanageren svarer på en nøgle, den ikke genkender, ved at logge det og starte unitten alligevel, så det eneste spor af fejlen var en advarsel i en log; den kom frem, mens unittene blev skrevet om. Nu kører hver unit gennem servicemanagerens egen verifikator under hver konvergering, så den samme stavefejl stopper en kørsel.

Hvor det går galt

Loggen vokser hurtigst, når systemet allerede er ved at gå ned. En løkke, der logger hvert genforsøg, skriver en håndfuld linjer på en god dag og tusinder i sekundet på en dårlig og tager disk, hukommelse og processortid fra et system, der intet har at give af. OWASP beder teams efterprøve, at logning ikke kan bruges til at opbruge systemets ressourcer, for eksempel ved at fylde disken. Giv hver hyppigt benyttet kodesti et budget, slå gentagne beskeder sammen til én linje med et antal, og hold en tæller ved siden af beskeden, så raten overlever, når linjer smides væk.

Hemmeligheder og personoplysninger bliver skrevet ned. En forespørgsel, der logges hel, bærer alt det med, der var i den. OWASP's liste over det, der som regel bør fjernes, maskeres, hashes eller krypteres, før det når en log, omfatter sessions-id'er, adgangstokens, adgangskoder, forbindelsesstrenge til databaser, krypteringsnøgler og betalingskortdata. Gør det, når linjen skrives, som adgangsloggen ovenfor gør med adresser, for når nogen når at rydde op, kan linjen allerede ligge i en sikkerhedskopi eller et arkiv.

Input udefra skriver en falsk linje. En værdi fra en bruger, der indeholder et vognretur- eller linjeskifttegn og skrives uescapet ind i en tekstlog, kan begynde en ny linje, der ligner en, applikationen selv skrev, på en prik. OWASP kalder det

log injection og beder om, at sådanne tegn renses, og at data kodes til det format, de skrives i. En struktureret logger, der skriver hver værdi som en escapet JSON-streng, gør det af sig selv.

En log, der tier, ligner et sundt system. En fuld disk, en roteret fil, programmet aldrig åbnede igen, eller en opsamler, der gik ned, ser ens ud udefra: linjerne holder op med at komme. OWASP beder om en måde at opdage, at logningen er gået i stå. Tæl linjer pr. minut for hver kilde, og slå alarm, når et antal falder til nul, så et hul i loggen bliver en alarm i sig selv.

Læs mere

- Logs — OpenTelemetry om, hvad en log er, hvorfor strukturerede logge foretrækkes, og hvordan logge bindes til traces.
- Logs Data Model — felterne i en logpost, dens to tidsstempler og alvorsskalaen fra 1 til 24.
- RFC 5424: The Syslog Protocol — syslog-beskedformatet og dets otte alvorsgrader.
- NIST SP 800-92 — Guide to Computer Security Log Management.
- Logging Cheat Sheet — OWASP om, hvilke hændelser der skal registreres, hvilke data der skal holdes ude, og hvordan resultatet beskyttes.
- Instrumentation — Prometheus-projektets praksis for at instrumentere kode, logning medregnet.

Ordliste

Vælg ud fra jeres faktiske vilkår

Medbring udrulningsforløbet, driftsrisiciene og dem, der har vagten. Vi kan afgrænse en ændring med kontroller, en vej tilbage og tydeligt ansvar.

Se, hvad det koster Kontakt os →

Gør begreberne praktiske

Spørg, hvordan »Hvad er logning?« gælder i jeres organisation. Et konkret eksempel fra jeres nuværende system er nok til at begynde samtalen.

Se vores ydelser

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

Tag denne side med dig

Visitkort

Lavet med kærlighed af D.

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

Copyright © 2025 – nu · Engineer ApS · Alle rettigheder forbeholdes.

Udskrevet fra https://engineer.company/da/glossary/logging/