Engineer

Loggning

att skriva ned vad som händer, medan det händer

Vad det är

Loggning, eller händelseloggning, är när ett program för en löpande redogörelse för sitt eget beteende, en post per händelse: en besvarad förfrågan, ett nekat lösenord, ett nytt försök, en krasch. Varje post, en loggrad eller loggpost, bär åtminstone en tidpunkt och ett meddelande, så att någon i efterhand kan rekonstruera vad som hände och i vilken ordning. Projektet OpenTelemetry definierar en logg som en tidsstämplad textpost, strukturerad eller ostrukturerad, med valfri metadata, och konstaterar att loggarna, av alla telemetrisignaler, bär på mest arv från äldre system.

Det arvet har en standard. Syslog, det sedan länge etablerade protokollet för att skicka händelsemeddelanden till en insamlare, standardiserades i mars 2009 som RFC 5424, som ersätter det äldre RFC 3164. Protokollet ger varje meddelande en av åtta allvarlighetsgrader, från 0 för Emergency till 7 för Debug. De flesta loggbibliotek har en kortare stege med samma idé: debug, info, warning och error. OpenTelemetrys datamodell för loggar placerar dem alla på ett enda tal från 1 till 24, i sex band från TRACE till FATAL.

En ostrukturerad rad är fri text: lätt för en människa att läsa, men en maskin kan bara plocka isär den med ett reguljärt uttryck som är skrivet för just den formuleringen. En strukturerad rad följer ett schema, så att varje post har samma namngivna fält med samma typer och betydelser. OpenTelemetry föredrar strukturerade loggar i produktion och lägger till en varning som är lätt att missa: en rad som är kodad som JSON är inte strukturerad bara för att den går att tolka, för det som gör den strukturerad är ett stabilt schema. Här visas en strukturerad post över flera rader, men på disken är den en enda rad:

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

Mätvärden och spårningar är de signaler som oftast samlas in bredvid loggen. Mätvärden är tal som samplas över tid, billiga att spara och bra på att säga hur ofta något händer. En spårning följer en enda förfrågan genom varje tjänst som den passerar. Loggen behåller detaljerna i enskilda händelser, och därför är det loggen som någon läser efter ett larm för att ta reda på varför. OpenTelemetry knyter ihop loggar och spårningar genom att fästa id:t för den aktiva spårningen, och för det delsteg i den som pågår (span), vid varje loggpost.

Använd begreppet i ett beslut

Använd ”Vad är loggning?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. Övervakning och larm som säger till medan ett fel fortfarande är litet, och siffrorna som visar hur ofta det förblir så.

Se våra tjänster Hör av er →

Granska antagandena bakom ordet

Använd förklaringen och det länkade arbetet för att formulera frågor till projektet. Vi kan undersöka antagandena tillsammans innan ett verktyg väljs. Byggde företagets första observerbarhetsdashboard — företagets första överblick över de egna systemen

Byggde företagets första observerbarhetsdashboard Hör av er →

Varför det spelar roll

En logg är den enda redogörelse för det förflutna som de flesta system lämnar efter sig. Ett mätvärde kan säga att felen ökade klockan 03.12; loggen säger vilken förfrågan det gällde, från vilken tjänst, med vilket värde och vad programmet gjorde sedan. När något går sönder under natten och har återhämtat sig till morgonen är loggen det vittne som fortfarande finns kvar.

Den redogörelsen har ett pris, och det betalas på tre sätt. Varje rad kostar diskutrymme, in- och utmatning och processortid, och ännu mer om den skickas till ett centralt lager, där en tjänst som drivs av någon annan oftast tar betalt efter den volym som tas emot. Varje rad är också uppgifter som lagras om någon: en webbservers åtkomstlogg innehåller adresserna och webbläsarna hos alla som har anropat den. Och varje rad måste skyddas. OWASP:s Logging Cheat Sheet vill

att varje händelse registrerar när, var, vem och vad, och att själva loggarna skyddas mot manipulation och mot obehörig åtkomst, ändring och radering, eftersom de kan innehålla personuppgifter och andra känsliga uppgifter.

I en hel organisations skala behandlar NIST Special Publication 800-92, Guide to Computer Security Log Management av Karen Kent och Murugiah Souppaya, utgiven i september 2006, logghantering som infrastruktur och processer som drivs i hela verksamheten, snarare än som en inställning i ett enskilt program.

Loggar fungerar också bäst bredvid tal. Prometheus-projektets guide för instrumentering föreslår en räknare för varje rad loggkod, så att det, när ett intressant meddelande dyker upp, går att se hur ofta det har förekommit och hur länge. Guiden föreslår också att summorna av rader på nivåerna info, warning och error jämförs från en utgåva till nästa.

Så ser det ut i praktiken

Webbplatsens egen åtkomstlogg beskrivs rad för rad på integritetssidan. För varje förfrågan sparas sidan och tiden, svarsstatusen, webbläsarens beskrivning av sig själv, namnet på webbplatsen som besökaren kom från och en suddad nätverksadress: den sista delen ersätts med nollor i samma ögonblick som raden skrivs, innan något når disken. En rad finns kvar i ungefär trettio dagar. Serverprogramvaran stänger varje fil en gång om dygnet, eller tidigare vid ungefär 10 MB, och raderar en stängd fil tjugoåtta dagar senare, och varje natt läser en kontroll igenom alla filer och ger fel om någon rad är äldre än trettio dagar. Det har gått fel två gånger, och integritetssidan berättar om båda. I september 2026 fyllde de lugna adresserna 10 MB så långsamt att deras filer aldrig hade stängts och fortfarande innehöll varje rad sedan loggningen slogs på, så ett dagligt jobb lades till för att stänga dem. Den 26 oktober 2026 skrev sju av de tretton adresser som för logg fortfarande i filer som jobbet hade märkt som stängda, och en av dem hade en stängd fil som var fyrtiosju dagar gammal. Jobbet är borttaget, och nu stänger och raderar serverprogramvaran filerna själv.

En fullständig testkörning av en macOS-applikation registrerade 610 996 core-loggrader. En skur av core-logghändelser behölls i en obegränsad huvudström och kopierades till prenumerantströmmar vars konsumenter inte använde dem. Incidentbeskrivningen dokumenterar separat diagnostikrapporter med 111 GB komprimerade sidor på en maskin med 36 GB och ett stickprov av minnesförbrukningen som visade en ökning med ungefär 41 MB per sekund under en återförsöksslinga för anslutningen. Begränsade buffertar,

prenumerationer filtrerade efter händelsetyp och en taktbudget för loggningen åtgärdade den händelsevägen. I den dokumenterade jämförelsen av fullständiga testkörningar minskade antalet core-loggrader till 1 411. Det är inte ett prestandatest i produktion eller en mätning av minnesförbrukningen efter korrigeringen. Budgeten kastar bort information med avsikt: upprepade diagnostiska händelser kan tas bort och berört tillstånd läsas in på nytt i stället för att behålla ett obegränsat antal händelser. Separata tidsgränser vid avstängning krävde en egen korrigering.

På en produktionsvärd hittade en härdning av tretton systemd-enheter ett direktiv som hade varit felstavat i tre enhetsmallar så länge de rollerna hade funnits. Tjänstehanteraren besvarar en nyckel som den inte känner igen genom att logga det och sedan starta enheten ändå, så det enda spåret av misstaget var en varning i en logg, och felet kom i dagen först när enheterna skrevs om. Nu går varje enhet genom tjänstehanterarens egen verifierare vid varje konvergenskörning, så samma stavfel får en körning att fallera.

Var det går fel

Loggen växer snabbast när systemet redan håller på att gå sönder. En loop som loggar varje nytt försök skriver en handfull rader en bra dag och tusentals i sekunden en dålig, och tar diskutrymme, minne och processortid från ett system som inte har något att avvara. OWASP ber team att verifiera att loggningen inte kan användas för att tömma systemets resurser, t.ex. genom att fylla disken. Ge varje het kodväg en budget, slå ihop upprepade meddelanden till en rad med ett antal och håll en räknare bredvid meddelandet, så att takten finns kvar när rader kastas.

Hemligheter och personuppgifter skrivs ned. En förfrågan som loggas i sin helhet bär med sig allt som fanns i den. OWASP:s lista över det som oftast bör tas bort, maskeras, hashas eller krypteras innan det når en logg omfattar sessionsidentifierare, åtkomsttokens, lösenord, anslutningssträngar till databaser, krypteringsnycklar och betalkortsuppgifter. Gör det när raden skrivs, som åtkomstloggen ovan gör med adresserna, för när någon väl städar kan raden redan ligga i en säkerhetskopia eller ett arkiv.

Indata utifrån skriver en falsk rad. Ett värde från en användare som innehåller vagnretur eller radmatning och skrivs in i en textlogg utan att tecknen kodas om kan inleda en ny rad som ser exakt ut som en rad som applikationen själv skrev.

OWASP kallar det logginjektion och ber att sådana tecken saneras och att data kodas för det format som de skrivs i. En strukturerad loggare som skriver varje värde som en korrekt kodad JSON-sträng gör det redan genom sin konstruktion.

En logg som tystnar ser ut som ett friskt system. Utifrån ser en full disk, en roterad fil som programmet aldrig öppnade på nytt och en insamlare som gick ned likadana ut: raderna slutar komma. OWASP ber om ett sätt att upptäcka att loggningen har upphört. Räkna rader per minut för varje källa och larma när ett antal sjunker till noll, så att ett glapp i loggen blir ett eget larm.

Läs mer

- Logs — OpenTelemetry om vad en logg är, varför strukturerade loggar föredras och hur loggar knyts till spårningar.
- Logs Data Model — fälten i en loggpost, dess två tidsstämplar och skalan för allvarlighetsgrad från 1 till 24.
- RFC 5424: The Syslog Protocol — meddelandeformatet för syslog och dess åtta allvarlighetsgrader.
- NIST SP 800-92 — Guide to Computer Security Log Management, vägledningen för logghantering i en hel organisation.
- Logging Cheat Sheet — OWASP om vilka händelser som ska registreras, vilka uppgifter som ska hållas utanför och hur resultatet skyddas.
- Instrumentation — Prometheus-projektets praxis för att instrumentera kod, loggning inräknad.

Ordlista

Välj utifrån era faktiska förutsättningar

Ta med driftsättningsvägen, driftsriskerna och dem som har jour. Vi kan avgränsa en förändring med kontroller, en väg tillbaka och tydligt ansvar.

Se vad det kostar Hör av er →

Gör begreppen praktiska

Fråga hur ”Vad är loggning?” gäller i er organisation. Ett konkret exempel från ert nuvarande system räcker för att börja samtalet.

Se våra tjänster

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

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

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

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/glossary/logging/