Engineer

# Strammet inn systemd-sandkassen for hver enhet

Reduserte eksponeringen i systemd-sandkassen for hver enhet plattformen installerer — tjenesten for dødmannsknappen fra 9,6 UNSAFE til 1,5, en internetteksponert git-forge fra 8,3 EXPOSED til 1,5 — og la til en parserkontroll ved konvergering etter å ha funnet et feilstavet direktiv som ble ignorert i det stille i tre enhetsmaler.

september 2026

## hver enhet i sandkasse, og skrivefeilen som ble ignorert

**Situasjon.** Tretten enhetsfiler var installert av dette repoet og kjørte på produksjonsverten med de privilegiene tjenestestyreren gir som standard, og det er de fleste. En herdingsscore satte tjenesten for dødmannsknappen til 9,6 og kalte den usikker; den internetteksponerte git-forgen fikk 8,3 og betegnelsen eksponert. Begge tallene var korrekte, og ingen av dem hadde ført til noe, fordi en score uten en terskel knyttet til seg er et tall folk lærer seg å hoppe over.

**Oppgave.** Hver enhet trengte en sandkasse som sto i forhold til det den faktisk gjør, og sandkassene trengte en sjekk, fordi feilmodusen til en feil sandkasse er at enheten starter og så svikter et sted parseren ikke kan se.

**Handling.** Privilegiebegrensninger gikk inn i alle enhetsmaler — et privilegietak låst til enhetens egne privilegier, et filter for systemkall, begrensede adressefamilier og minne som kan være skrivbart eller kjørbart, men aldri begge deler. De målte resultatene: dødmannsknappen gikk fra 9,6 til 1,5, forgen fra 8,3 til 1,5 og begge sikkerhetskopienhetene fra 9,6 til 2,3 og 2,5. Arbeidet med dem avdekket noe bedre enn scorene. Ett direktiv hadde vært feilstavet i tre enhetsmaler så lenge de rollene hadde eksistert — et navn som ser plausibelt ut, men ikke finnes, og som tjenestestyreren besvarer ved å logge at den ikke kjenner igjen nøkkelen, og så starte enheten likevel. Et søk med grep etter et direktiv beviser at det ble skrevet; bare parseren beviser at det trådte i kraft. Derfor kjører en verifiseringsrolle nå hver enhet gjennom tjenestestyrerens eget verifiseringsverktøy under kjøringen, og rollen inkluderes av hver rolle som

installerer en enhet. Det dette fortsatt ikke fanger, står klart i de samme dokumentene: alle direktiver som kan ødelegge disse enhetene, ødelegger dem ved kjøretid, ikke ved parsing, og en score kan ikke si om et skript fortsatt når frem til sin siste linje.

**Resultat.** Hver enhet kjører med de privilegiene den trenger og ingen andre, tallene er målt og ikke påstått, og den typen feil der en skrivefeil blir et sikkerhetstiltak som i det stille mangler, får nå en kjøring til å feile. Begrensningene ved målingen står dokumentert ved siden av den, og det er den delen som hindrer neste leser i å stole for mye på en score i det grønne området.

### Bruk erfaringen i prosjektet deres

Bruk «Strammet inn systemd-sandkassen for hver enhet» som utgangspunkt for en lignende utfordring i organisasjonen deres. Tjenestene bak arbeidet er tilgjengelige for prosjektet deres. Hele oppsettet skrevet ned som filer, slik at det kan gjenskapes nøyaktig og aldri bare finnes i hodet på én person.

**Se tjenestene våre** Ta kontakt →

### Se bak resultatet

Les om situasjonen, beslutningene og resultatet i eksemplet. Vi kan drøfte hva som passer deres rammer, og hva som krever en annen tilnærming. Strammet inn systemd-sandkassen for hver enhet — hver enhet i sandkasse, og skrivefeilen som ble ignorert

**Se tjenestene våre** Ta kontakt →

## Har tjenestene dine mer tilgang enn de trenger?

Snakk om prosjektet med ingeniøren som har ansvaret for leveransen. Vi avtaler omfang, prisgrunnlag og overlevering skriftlig før arbeidet begynner.

Rolle i oppdraget: Site Reliability Engineer. Det bygger på Infrastruktur, Containere (Docker/Kubernetes), Automatisering og CI/CD, Linux og servere, Sikkerhet og Testing og kvalitetssikring. Og nå som dere er her: vi er ganske gode på Infrastruktur som kode, Containerisering og orkestrering, Systemadministrasjon og Sikkerhet og tilgangsstyring.

**Ta kontakt** Se tjenestene våre

Ett stykke av **en lengre oversikt** — og den ligger i sin helhet her.

Hver oppføring er skrevet på samme måte: situasjonen, oppgaven, hva vi gjorde, og hva som endret seg.

**Se hele oversikten**

Definer forbedringen dere trenger

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 →

## Har tjenestene dine mer tilgang enn de trenger?

Spør om beslutningene bak «Strammet inn systemd-sandkassen for hver enhet». Dere snakker med folk som kan forklare arbeidet og vurdere deres eget prosjekt.

**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/portfolio/cut-systemd-sandbox-exposure-on-every-unit/**