Engineer Platform

Split every operational secret per host

Split the four per-host operational secrets after establishing that two hosts sharing one dead-man's switch alert less than two switches, not more, and that a shared backup passphrase can expose both hosts' backups, even in separate repositories, if someone obtains it and can read both repositories' encrypted data and key files.

September 2026

four operational settings, keyed by host

Situation. The platform was built for one host and was about to have two. Several operational secrets had been written as single values on that assumption: one backup repository, one passphrase, one alert switch. Extending them to a second host by sharing them is the path of least resistance and it is wrong in two separate ways, both of which fail quietly.

Task. Each secret had to become a map keyed by host, and the reason had to be written down, because the shared version looks correct and costs nothing until the day it matters.

Action. Two arguments settled it, and both are recorded next to the configuration. A dead-man’s switch shared by two hosts alerts less than two switches, not more: either host still pinging keeps the check green while the other one is dead, so adding a host to a shared switch actively reduces the coverage of the one that was already there. And a backup repository string names a location, not an independent credential boundary. Separate restic repositories can have distinct master keys even when they use the same passphrase. But someone who obtains that passphrase and can read both repositories’ encrypted data and key files can unlock both, so sharing it couples their exposure rather than isolating the hosts. Each value became a map keyed by inventory hostname, resolved per host by a shared task file that both the converge and the preflight run. The existing host was then named in all four

maps with its repository and both switches left empty, which is the truthful state and keeps the two open initiatives honest about owing the operator half of the work rather than the code.

Result. Secrets are per host by construction, and the two failure modes that would have followed from sharing them are written down where the next person edits the file. The empty entries are the part worth keeping: they say the wiring exists and the value does not, which is a different and more useful statement than a missing key.

Bring this experience to your project

Use “Split every operational secret per host” as a starting point for a similar challenge in your organisation. The services behind this work are available for your project. The whole setup written down as files, so it can be recreated exactly and never lives only in one person's head.

Explore our services Get in touch →

Look behind the result

Read the situation, decisions and result in this example. We can discuss which parts transfer to your constraints and which need another approach. Split every operational secret per host — four operational settings, keyed by host

Explore our services Get in touch →

Would one leaked key expose every one of your hosts?

Talk through your project with the engineer responsible for delivery. We agree the scope, price basis and handover in writing before work begins.

Role context: Security Engineer. It draws on Solution Architecture, Infrastructure, Automation & CI/CD, Reliability & Backups, Linux & Servers and Security. And while you are here, we are rather good at Infrastructure as Code, Site Reliability & Monitoring, Backup & Disaster Recovery, Security & Access Management and AI Agent Security.

Get in touch Explore our services

One piece of **a longer record** — and it is all on this site.

Every entry is written the same way: the situation, the task, what we did and what changed.

See the whole record

Define the improvement you need

Bring the deployment path, the operational risks and the people on call. We can scope a change with checks, a recovery route and clear ownership.

See what it costs Get in touch →

Would one leaked key expose every one of your hosts?

Ask about the decisions behind “Split every operational secret per host”. You will speak with the people who can explain the work and assess your own project.

Explore our services

welcome@engineer.company +45 50 10 61 84 Copenhagen, Denmark

Take this page with you

Contact card

Carefully Crafted With Love by D.

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

Copyright © 2025 – present · Engineer ApS · All rights reserved.

Printed from https://platform.engineer.company/portfolio/split-every-operational-secret-per-host/