Engineer

Hardened SSH to 24 validated directives

Hardened SSH to 24 asserted directives with three-stage validation — the candidate file, the assembled config, then the daemon's own read-back — after the read-back caught the running server silently overriding two of the twenty-four.

September 2026

24

SSH directives asserted, then read back from the daemon

Situation. SSH is the only interactive way into the company's host, and its configuration is written by an automation role that had been running clean for months. An access report in September 2026 read the daemon's own resolved settings and found two of them disagreeing with what the role had been writing on every single converge.

Task. The hardening had to become something the daemon confirms rather than something the repository asserts, because the gap between the two had already been open for months without anyone noticing.

Action. The cause was configuration ordering. The operating system ships its own defaults uncommented, above where a drop-in file lands, and for the two settings in question the first occurrence wins. The fix was a filename prefix that sorts ahead of the vendor's, which is a one-character class of change and exactly the sort that stays broken because nobody thinks to look. What was built around it matters more: three stages of validation on every converge. The candidate file is syntax-checked before it is installed, so an invalid config never reaches the host. The assembled configuration is checked after installation. Then the daemon's own resolved output is read back and 24 directives are asserted against it, so a setting that is written but overridden fails the run. Two directives were deliberately left out, both because the daemon no longer implements them and writing them would only look thorough.

Result. The SSH posture is now the daemon's answer rather than the repository's claim, and the difference is not theoretical — it was already two settings wide when the check was written. A converge that cannot see whether a control took effect has not verified it, and grepping for a directive only proves it was written.

Bring this experience to your project

Use "Hardened SSH to 24 validated directives" 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. Hardened SSH to 24 validated directives — 24 SSH directives asserted, then read back from the daemon

Explore our services Get in touch →

Is your remote access as locked down as you think?

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 Infrastructure, Automation & CI/CD, Linux & Servers, Security, Testing & QA and System Administration. And while you are here, we are rather good at Infrastructure as Code, System Administration and Security & Access Management.

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 →

Is your remote access as locked down as you think?

Ask about the decisions behind “Hardened SSH to 24 validated directives”. 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://engineer.company/portfolio/hardened-ssh-to-24-validated-directives/