Engineer

全ユニットのsystemdサンドボックス露出を低減

この基盤が導入するすべてのユニットのsystemdサンドボックスの露出度を低減。デッドマンズスイッチのサービスを9.6 UNSAFEから1.5へ、インターネット公開のgitホスティングを8.3 EXPOSEDから1.5へ改善し、3つのユニットテンプレートで黙って無視されていた設定名の誤記を受け、収束時の構文検査を加えた。

9月 2026

全ユニットのサンドボックス化と無視された誤記

状況. 13個のユニットが、本番で監督プロセスの既定の、ほぼ広範な権限で動いていた。デッドマンズスイッチは堅牢化評点9.6でunsafe、公開gitは8.3でexposedだった。正しい数値でも、閾値がなければ読み飛ばされ、行動につながっていなかった。

課題. 各ユニットの実務に合うサンドボックスと、その検証が必要だった。誤ると起動はしても構文検査に見えない実行箇所で壊れるためだった。

行動. 全テンプレートに、ユニット自身の権限を上限とする制限、システムコールフィルター、アドレス種別の制限、書き込みと実行を同時に許さないメモリーを設定した。実測でスイッチは9.6から1.5、gitは8.3から1.5、バックアップ2 ユニットは9.6から2.3と2.5になった。さらに、3テンプレートに以前から誤記された、もっともらしいが存在しない設定名を発見した。監督プロセスは不明キーをログに記して起動を続けていた。文字列検索は書いたことしか示さず、構文解析こそ適用を示すため、全導入ロールが呼ぶ検証ロールで、収束時に全ユニットを標準の検証器へ通した。ただし、これらを壊す設定は解析時でなく実行時に壊すため、スコアはスクリプトが最終行まで届くかを示さないという限界も記した。

結果. 必要な権限だけで各ユニットが動き、数値は主張でなく実測となった。誤記で制御が静かに欠ける不具合が、実行失敗になった。測定の限界も隣に記録し、次の読み手が緑の表示を過信しないようにした。

この経験をお客様のプロジェクトに

「全ユニットのsystemdサンドボックス露出を低減」を、お客様の組織の似た課題を考える出発点にしてください。この実績を支えたサービスを、お客様のプロジェクトにも提供できます。 構成全体をファイルに記述し、特定の人の記憶だけに頼らず、まったく同じ環境を再現できるようにします。

サービスを見る お問い合わせ →

結果の背景を確かめる

この事例の状況、判断、結果をご覧ください。どの部分がお客様の制約の下でも生かせるか、どこに別の方法が必要かをご相談いただけます。 全ユニットのsystemdサンドボックス露出を低減 — 全ユニットのサンドボックス化と無視された誤記

サービスを見る お問い合わせ →

サービスに必要以上のアクセスを与えていませんか？

納品を担当するエンジニアに、プロジェクトについてご相談ください。着手前に、業務範囲、価格の算定方法、引き継ぎ内容を書面で合意します。

担当した役割：サイト信頼性エンジニア。 関連する分野： インフラ, コンテナ（Docker/Kubernetes）, 自動化・CI/CD, Linux・サーバー, セキュリティ および テスト・品質保証. こちらのサービスも得意としています コードによるインフラ管理, コンテナ化・オーケストレーション, システム管理 および セキュリティ・アクセス管理.

お問い合わせ サービスを見る

より多くの実績の **一つです** — そのすべてをこのサイトで公開しています。

どの項目も、状況、課題、実施内容、変化という同じ構成で記載しています。

すべての実績を見る

必要な改善を定める

デプロイの流れ、運用上のリスク、緊急対応の担当者をお知らせください。検査、復旧手段、明確な責任の所在を伴う変更の範囲を定められます。

料金を見る お問い合わせ →

サービスに必要以上のアクセスを与えていませんか？

「全ユニットのsystemdサンドボックス露出を低減」の判断の背景についてお尋ねください。仕事内容を説明し、お客様のプロジェクトを検討できる担当者が対応します。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く

連絡先カード

心を込めて丁寧に制作： D.

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

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://engineer.company/ja/portfolio/cut-systemd-sandbox-exposure-on-every-unit/