Engineer

Посилила ізоляцію systemd для кожного юніта

Знизила оцінку відкритості (exposure) у пісочниці systemd для кожного юніта, який встановлює платформа: служба dead man's switch — з 9,6 UNSAFE до 1,5, відкритий в інтернет git-сервер — з 8,3 EXPOSED до 1,5, — і додала перевірку парсером під час converge, після того як знайшла у трьох шаблонах юнітів директиву з орфографічною помилкою, яку systemd мовчки ігнорував.

вересень 2026

кожен юніт у пісочниці — і друкарська помилка, яку ігнорували

Ситуація. Тринадцять юніт-файлів встановлював цей репозиторій, і на продакшн-хості вони працювали з привілеями, які супервізор надає за замовчуванням, тобто майже з усіма. Оцінка захищеності дала службі dead man’s switch 9,6 і назвала її небезпечною; git-сервер, доступний з інтернету, отримав 8,3 і позначку «відкритий». Обидва числа були точними, і жодне ні до чого не спонукало, бо оцінка без порога — це число, яке люди звикають пропускати.

Завдання. Кожен юніт потребував пісочниці, співмірної з тим, що він насправді робить, а самі пісочниці — перевірки, бо хибна пісочниця відмовляє так: юніт запускається, а потім ламається там, де парсер цього не бачить.

Дія. Обмеження привілеїв додано до кожного шаблону юніта — верхня межа привілеїв на рівні власних привілеїв юніта, фільтр системних викликів, обмежені сімейства адрес і пам’ять, яка може бути записуваною або виконуваною, але ніколи водночас. Виміряні результати: dead man’s switch — з 9,6 до 1,5, git-сервер — з 8,3 до 1,5, обидва юніти резервного копіювання — з 9,6 до 2,3 і 2,5. Під час роботи над ними знайшлося дещо цінніше за оцінки. Одна директива відтоді, як існують ці ролі, була написана з помилкою у трьох шаблонах юнітів — правдоподібна

на вигляд назва, якої не існує; супервізор відповідає на неї записом у журналі, що не розпізнає ключ, і все одно запускає юніт. Пошук директиви через grep доводить лише, що її написали; що вона набула чинності, доводить тільки парсер. Тому тепер окрема роль перевірки під час converge проганяє кожен юніт через вбудований верифікатор супервізора, і її підключає кожна роль, що встановлює юніт. Чого ця перевірка досі не бачить, прямо сказано в тих самих документах: кожна директива, здатна зламати ці юніти, ламає їх під час виконання, а не під час розбору, а оцінка не скаже, чи скрипт досі доходить до останнього рядка.

Результат. Кожен юніт працює з тими привілеями, які йому потрібні, і без зайвих, числа виміряно, а не задекларовано, а клас дефектів, де описка непомітно перетворюється на відсутній засіб контролю, тепер обриває прогін. Межі вимірювання записано поруч із ним, і саме це вбереже наступного читача від надмірної довіри до зеленої зони.

Застосуйте цей досвід у своєму проєкті

Використайте «Посилила ізоляцію systemd для кожного юніта» як відправну точку для схожого завдання у вашій організації. Послуги, що стоять за цією роботою, доступні й для вашого проєкту. Уся конфігурація записана у файлах, тож її можна відтворити точно, і вона не живе лише в чиїйсь голові.

Переглянути наші послуги Зв'язатися з нами →

Дізнайтеся, що привело до результату

Прочитайте про ситуацію, рішення та результат цього прикладу. Ми можемо обговорити, що відповідає вашим умовам, а що потребує іншого підходу. Посилила ізоляцію systemd для кожного юніта — кожен юніт у пісочниці — і друкарська помилка, яку ігнорували

Переглянути наші послуги Зв'язатися з нами →

Ваші служби мають більше доступу, ніж потребують?

Обговоріть свій проєкт з інженером, відповідальним за виконання. Обсяг, основу розрахунку вартості та передачу результатів узгоджуємо письмово до початку робіт.

Роль у цій роботі: Інженер з надійності (SRE). Тут задіяні Інфраструктура, Контейнери (Docker/Kubernetes), Автоматизація та CI/CD, Linux та сервери, Безпека та Тестування та QA. І, до речі, ми добре вміємо Infrastructure as Code, Контейнеризація та оркестрація, Системне адміністрування та Безпека та керування доступом.

Зв'язатися з нами Ознайомтеся з нашими послугами

Одна частина **довшого переліку** — і він увесь на цьому сайті.

Кожен запис написано однаково: ситуація, завдання, що ми зробили і що змінилося.

Переглянути весь перелік

Визначте потрібне покращення

Опишіть шлях розгортання, експлуатаційні ризики та чергову команду. Ми можемо визначити зміну з перевірками, шляхом відновлення та чіткою відповідальністю.

Дивитися, скільки це коштує Зв'язатися з нами →

Ваші служби мають більше доступу, ніж потребують?

Запитайте про рішення в роботі «Посилила ізоляцію systemd для кожного юніта». Ви говоритимете з людьми, які можуть пояснити роботу й оцінити ваш проєкт.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

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

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/portfolio/cut-systemd-sandbox-exposure-on-every-unit/