Engineer

Запустила контейнери на Podman і Quadlet

Розгорнула контейнерну платформу на Podman і Quadlet під systemd, а не на Docker, бо типове публікування портів Docker у мережі bridge може обходити правила UFW, — а для розгортань виділила непривілейованого користувача з однією фіксованою командою замість root.

вересень 2026

контейнери під systemd, а не над фаєрволом

Ситуація. Платформі потрібне було місце для запуску контейнерів застосунків. Очевидним вибором був галузевий стандарт, і для цього хоста він не годився з цілком конкретної причини: він переписує правила пакетного фільтра ядра й публікує порти контейнерів із вищим пріоритетом, ніж правила брандмауера, які встановлює роль посилення захисту, тож контейнер непомітно стає доступним з інтернету, хоч би що було прописано в брандмауері.

Завдання. Треба було обрати контейнерне середовище, яке не обходить брандмауер, не додає другого супервізора поруч із тим, якому вже довіряють, і не вимагає root-доступу, щоб випустити реліз.

Дія. Це середовище — контейнерний рушій без демона, який керує юнітами, згенерованими власним супервізором операційної системи. Другого менеджера процесів немає: контейнери — це служби, вони запускаються так само, як служби, і описані в тій самій декларативній формі, що й усе інше. Контейнери використовують мережу хоста й не публікують жодного порту, тож питання обходу брандмауера не пом’якшено, а знято. Юніти працюють на системному рівні, а не в rootless-режимі, і це записано як компроміс: автоматизація лишається нескладною та звичною ціною суворішої ізоляції, яку дав би rootless-режим, а в примітці сказано, у який бік рухатися, якщо втеча з контейнера колись важитиме більше за простоту автоматизації. Розгортання відокремлено від підготовки хоста: root один раз налаштовує шлях розгортання, а далі непривілейований користувач

перерозгортає застосунок, запускаючи один фіксований скрипт через вузьке правило, яке дозволяє саме цю команду й жодних аргументів. Зібрати образ, перезапустити службу. Жодної root-оболонки, жодних довільних команд.

Результат. Контейнери працюють під супервізором, якому вже довіряли, за брандмауером, який уже було задекларовано, а звичайний реліз виконується однією чітко обмеженою командою без оболонки root. Відмову від стандартного варіанта записано разом із причиною, і це важить більше за сам вибір: наступній людині кожна стаття, яку вона прочитає, радитиме взяти стандартний.

Застосуйте цей досвід у своєму проєкті

Використайте «Запустила контейнери на Podman і Quadlet» як відправну точку для схожого завдання у вашій організації. Послуги, що стоять за цією роботою, доступні й для вашого проєкту. Сервери під те навантаження, яке у вас справді є, перенесені в хмару чи назад, із порахованим наперед місячним рахунком.

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. Запустила контейнери на Podman і Quadlet — контейнери під systemd, а не над фаєрволом

Переглянути наші послуги Зв'язатися з нами →

Запускаєте контейнери, не відкриваючи дір у фаєрволі?

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 автоматизації інфраструктури. Тут задіяні DevOps, Інфраструктура, Контейнери (Docker/Kubernetes), Автоматизація та CI/CD, Linux та сервери та Безпека. І, до речі, ми добре вміємо Хмарна інфраструктура та міграція, DevOps та автоматизація CI/CD, Контейнеризація та оркестрація 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 →

Запускаєте контейнери, не відкриваючи дір у фаєрволі?

Запитайте про рішення в роботі «Запустила контейнери на Podman і Quadlet». 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/ran-containers-on-podman-and-quadlet/