Engineer

Container mit Podman und Quadlet betrieben

Eine Containerebene mit Podman und Quadlet unter systemd statt Docker bereitgestellt, da Dockers standardmäßige Portfreigaben im Bridge-Netz UFW-Regeln umgehen können; für Bereitstellungen einen unprivilegierten Nutzer mit einem festen Befehl statt root eingerichtet.

September 2026

Container unter systemd statt oberhalb der Firewall

Situation. Die Plattform benötigte eine Laufzeit für Anwendungscontainer. Der naheliegende Branchenstandard war für diesen Host in einem konkreten Punkt falsch: Er schreibt die Paketfilterregeln des Kernels um und veröffentlicht Containerports vor den Firewallregeln der Härtungsrolle. Ein Container wird dadurch unabhängig von der festgelegten Firewall unbemerkt aus dem Internet erreichbar.

Aufgabe. Die Containerebene durfte die Firewall nicht umgehen, keinen zweiten Prozessmanager neben dem bereits vertrauten hinzufügen und für ein Release keine root-Anmeldung verlangen.

Massnahmen. Ein Containerwerkzeug ohne Daemon steuert Units, die der betriebssystemeigene Prozessmanager erzeugt. Es gibt keine zweite Aufsicht: Container sind Dienste, starten wie Dienste und werden ebenso deklarativ beschrieben wie der Rest. Sie nutzen Hostnetzwerk ohne veröffentlichte Ports. Das beseitigt die Firewallumgehung, statt sie nur abzumildern. Units laufen auf Systemebene statt rootless. Die Abwägung ist dokumentiert: einfache, übliche Automatisierung gegen die stärkere Isolation des rootless-Betriebs. Ebenso ist festgehalten, wohin die Lösung wechseln sollte, wenn Container-Ausbrüche wichtiger werden als einfache Automatisierung. Bereitstellung und Provisionierung wurden getrennt. root richtet den Bereitstellungsweg einmal ein. Danach führt ein unprivilegierter Nutzer für

erneute Bereitstellungen genau ein festes Skript über eine eng begrenzte Regel ohne erlaubte Argumente aus: Image bauen, Dienst neu starten. Keine root-Shell und keine beliebigen Befehle.

Ergebnis. Container laufen unter der bereits vertrauten Prozessaufsicht hinter der bereits deklarierten Firewall. Routinemäßige Releases nutzen einen einzelnen, klar begrenzten Befehl ohne Rootshell. Die Entscheidung gegen den Standard ist mit Begründung dokumentiert. Das zählt mehr als die Wahl selbst, weil jeder gelesene Artikel der nächsten Person den Standard empfehlen wird.

Diese Erfahrung für Ihr Projekt nutzen

Nutzen Sie „Container mit Podman und Quadlet betrieben“ als Ausgangspunkt für eine ähnliche Herausforderung in Ihrer Organisation. Die Leistungen hinter dieser Arbeit stehen auch für Ihr Projekt zur Verfügung. Server werden nach dem tatsächlichen Bedarf dimensioniert und in die Cloud oder aus ihr heraus verlagert — die monatlichen Kosten stehen vorher fest.

Unsere Leistungen entdecken Kontakt aufnehmen →

Hinter das Ergebnis schauen

Lesen Sie die Situation, die Entscheidungen und das Ergebnis dieses Beispiels. Wir können besprechen, welche Teile sich auf Ihre Rahmenbedingungen übertragen lassen und welche einen anderen Ansatz erfordern. Container mit Podman und Quadlet betrieben — Container unter systemd statt oberhalb der Firewall

Unsere Leistungen entdecken Kontakt aufnehmen →

Sollen Container ohne Löcher in der Firewall laufen?

Besprechen Sie Ihr Projekt mit der Ingenieurin, die für die Umsetzung verantwortlich ist. Wir vereinbaren Umfang, Preisgrundlage und Übergabe schriftlich, bevor die Arbeit beginnt.

Rollenkontext: Ingenieurin für Infrastrukturautomatisierung. Die Arbeit baut auf DevOps, Infrastruktur, Container (Docker/Kubernetes), Automatisierung und CI/CD, Linux und Server und Sicherheit. Und wenn Sie schon hier sind: Wir sind auch ziemlich gut in Cloud-Infrastruktur und Cloud-Migration, DevOps- und CI/CD-Automatisierung, Containerisierung und Orchestrierung und Sicherheits- und Zugriffsverwaltung.

Kontakt aufnehmen Unsere Leistungen entdecken

Ein Teil einer **längeren Arbeitsbilanz** — vollständig auf dieser Website zu finden.

Jeder Eintrag folgt demselben Aufbau: die Situation, die Aufgabe, unser Vorgehen und die Veränderungen.

Alle Arbeiten ansehen

Die benötigte Verbesserung definieren

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

Preise ansehen Kontakt aufnehmen →

Sollen Container ohne Löcher in der Firewall laufen?

Fragen Sie nach den Entscheidungen hinter „Container mit Podman und Quadlet betrieben“. Sie sprechen mit den Menschen, die die Arbeit erklären und Ihr eigenes Projekt einschätzen können.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

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

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://engineer.company/de/portfolio/ran-containers-on-podman-and-quadlet/