Engineer プラットフォーム

PodmanとQuadletでコンテナを運用

Dockerの既定のブリッジネットワークでのポート公開がUFWルールを迂回する場合があるため、systemd配下のPodman・Quadletでコンテナ基盤を構築。デプロイにはrootではなく、固定コマンド1つを使う非特権ユーザーを用いた。

9月 2026

ファイアウォールより前ではなくsystemd配下のコンテナ

状況. アプリ用コンテナの実行基盤が必要だった。業界標準の選択肢は、このホストでは不適切だった。カーネルのパケットフィルターを書き換え、堅牢化ロールのルールより前にポートを公開するため、ファイアウォールへ何を指示してもコンテナが静かに公開されるためだった。

課題. ファイアウォールを迂回せず、信頼済みの管理機構に加えて別の監督プロセスを置かず、rootにならずにリリースできる基盤が必要だった。

行動. デーモンを持たないコンテナエンジンと、OSの監督機構が生成するユニットを採用した。別の管理器はなく、コンテナも同じ宣言形式の通常サービスとして起動する。ポート公開なしのhost networkとし、迂回を軽減するのでなく問題自体をなくした。rootlessでなくsystem ユニットで動かす点は、強い分離と引き換えに自動化を簡単で標準的に保つ選択として記録し、脱出リスクが簡便さより重要になった場合の移行先も示した。構築とデプロイを分け、rootが一度経路を整えた後は、引数なしの固定スクリプト1つだけを許す限定ルールで非特権ユーザーが再導入する。イメージを作りサービスを再起動するだけで、root Shellも任意コマンドも与えない。

結果. 既存の信頼済み管理機構の下、宣言済みファイアウォールの背後で動き、通常のリリースはrootシェルを使わず、実行範囲を限定したコマンド1つで行う。次の人は読む記事すべてから標準を勧められるため、標準に逆らう選択以上に、その理由を記したことが重要だった。

この経験をお客様のプロジェクトに

「PodmanとQuadletでコンテナを運用」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。 実際の使用量に合わせてサーバーを構成し、月額費用を事前に把握したうえで、クラウドへの移行もクラウドからの移転も進めます。

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。 PodmanとQuadletでコンテナを運用 — ファイアウォールより前ではなくsystemd配下のコンテナ

サービスを見る お問い合わせ →

ファイアウォールに穴を開けずコンテナを動かせますか？

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：インフラ自動化エンジニア。 関連する分野： DevOps, インフラ, コンテナ（Docker/Kubernetes）, 自動化・CI/CD, Linux・サーバーおよび セキュリティ. こちらのサービスも得意としています クラウドインフラ・移行, DevOps・CI/CD自動化, コンテナ化・オーケストレーションおよび 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 →

ファイアウォールに穴を開けずコンテナを動かせますか？

「PodmanとQuadletでコンテナを運用」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://platform.engineer.company/ja/portfolio/ran-containers-on-podman-and-quadlet/