**Engineer** Plateforme

# Conteneurs exploités avec Podman et Quadlet

Déployé une couche de conteneurs Podman et Quadlet sous systemd plutôt que Docker, car la publication de ports sur le réseau bridge par défaut de Docker peut contourner les règles UFW, et confié les déploiements à un utilisateur non privilégié autorisé à une seule commande fixe plutôt qu'à root.

septembre 2026

## des conteneurs sous systemd, sans contourner le pare-feu

**Situation.** La plateforme avait besoin d'un endroit où exécuter les conteneurs applicatifs. Le choix évident était la solution standard du secteur, et ce choix était inadapté à cet hôte pour une raison précise : elle réécrit les règles de filtrage des paquets du noyau et publie les ports des conteneurs au-dessus des règles du pare-feu installées par le rôle de durcissement, si bien qu'un conteneur devient silencieusement accessible depuis Internet indépendamment des instructions données au pare-feu.

**Tâche.** Il fallait choisir une couche de conteneurs qui ne contourne pas le pare-feu, n'ajoute pas de second superviseur à côté de celui déjà jugé fiable et n'oblige personne à être root pour livrer une version.

**Action.** La couche repose sur un moteur de conteneurs sans démon qui pilote des unités générées par le superviseur du système d'exploitation lui-même. Il n'y a pas de second gestionnaire de processus : les conteneurs sont des services, démarrent comme des services et sont décrits sous la même forme déclarative que tout le reste. Les conteneurs utilisent le réseau de l'hôte sans aucun port publié, ce qui supprime la question du contournement du pare-feu au lieu de l'atténuer. Les unités s'exécutent au niveau système plutôt qu'en mode rootless, choix consigné comme un compromis — il garde l'automatisation simple et habituelle au prix de l'isolation plus stricte qu'offrirait rootless, et la note indique la direction à prendre si l'évasion de conteneur devient plus importante que la simplicité de l'automatisation. Le déploiement a été séparé du provisionnement : root met en place le chemin de déploiement une fois, puis un

utilisateur sans privilèges redéploie en exécutant un script fixe au moyen d'une règle restreinte qui autorise cette commande et aucun argument. Construire l'image, redémarrer le service. Aucun shell root, aucune commande arbitraire.

**Résultat.** Les conteneurs s'exécutent sous le superviseur déjà jugé fiable, derrière le pare-feu déjà déclaré, et une livraison courante utilise une seule commande au périmètre limité, sans shell root. Le choix contraire à la solution standard du secteur est écrit avec sa raison, ce qui compte plus que le choix lui-même — chaque article lu par la personne suivante lui recommandera la solution standard du secteur.

### Mettez cette expérience au service de votre projet

Prenez « Conteneurs exploités avec Podman et Quadlet » comme point de départ pour un défi similaire dans votre organisation. Les prestations mobilisées pour cette réalisation sont disponibles pour votre projet. Des serveurs dimensionnés selon vos usages réels, migrés vers le cloud ou hors du cloud, avec une estimation préalable de la facture mensuelle.

**Découvrir nos prestations** Contactez-nous →

### Examinez ce qui a conduit au résultat

Découvrez la situation, les décisions et le résultat de cet exemple. Nous pouvons discuter des éléments transposables à vos contraintes et de ceux qui nécessitent une autre démarche. Conteneurs exploités avec Podman et Quadlet — des conteneurs sous systemd, sans contourner le pare-feu

**Découvrir nos prestations** Contactez-nous →

## Des conteneurs à exploiter sans ouvrir de brèches dans le pare-feu ?

Discutez de votre projet avec l'ingénieure responsable de sa réalisation. Nous convenons par écrit du périmètre, de la base tarifaire et de la transmission avant le début des travaux.

Rôle exercé dans ce contexte : Ingénieure automatisation d'infrastructure. Cette réalisation fait appel à DevOps, Infrastructure, Conteneurs (Docker/Kubernetes), Automatisation et CI/CD, Linux et serveurs et Sécurité. Et puisque vous êtes ici, nous sommes aussi plutôt doués en Infrastructure cloud et migration, DevOps et automatisation CI/CD, Conteneurisation et orchestration et Sécurité et gestion des accès.

**Contactez-nous** Découvrir nos prestations

Un élément **d'un parcours plus long** — entièrement présenté sur ce site.

Chaque entrée suit la même structure : la situation, la tâche, ce que nous avons fait et ce qui a changé.

**Voir l'ensemble du parcours**

Définissez l'amélioration nécessaire

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

**Consulter les tarifs** Contactez-nous →

## Des conteneurs à exploiter sans ouvrir de brèches dans le pare-feu ?

Interrogez-nous sur les décisions qui sous-tendent « Conteneurs exploités avec Podman et Quadlet ». Vous parlerez aux personnes capables d'expliquer le travail et d'évaluer votre propre projet.

**Découvrir nos prestations**

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

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

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://platform.engineer.company/fr/portfolio/ran-containers-on-podman-and-quadlet/