Engineer Plataformas

Contenedores con Podman y Quadlet

Desplegué una plataforma de contenedores con Podman y Quadlet bajo systemd en lugar de Docker, porque la publicación predeterminada de puertos en redes bridge de Docker puede eludir las reglas UFW, y asigné a los despliegues un usuario sin privilegios con una única orden fija, en vez de root.

septiembre 2026

contenedores bajo systemd sin anteponerse al cortafuegos

Situación. La plataforma necesitaba un lugar donde ejecutar contenedores de aplicaciones. La elección evidente era la opción predeterminada del sector, y esa elección era equivocada para este host de una forma concreta: reescribe las reglas de filtrado de paquetes del kernel y publica los puertos de los contenedores por encima de las reglas del cortafuegos que instala el rol de endurecimiento, de modo que un contenedor pasa silenciosamente a ser accesible desde Internet con independencia de lo que se le haya indicado al cortafuegos.

Tarea. Había que elegir una capa de contenedores que no eludiera el cortafuegos, no añadiera un segundo supervisor junto al que ya era de confianza y no exigiera que una persona fuera root para publicar una versión.

Acción. La capa consiste en un motor de contenedores sin demonio que acciona unidades generadas por el propio supervisor del sistema operativo. No hay un segundo gestor de procesos: los contenedores son servicios, arrancan como arrancan los servicios y se describen en la misma forma declarativa que todo lo demás. Los contenedores utilizan la red del host sin ningún puerto publicado, lo que elimina la cuestión de la elusión del cortafuegos en lugar de mitigarla. Las unidades se ejecutan a nivel del sistema en lugar de sin root, y eso está registrado como una contrapartida — mantiene la automatización sencilla y convencional, a costa del aislamiento más estricto que ofrecería la ejecución sin root, y la nota dice en qué dirección avanzar si una posible fuga de un contenedor llegara a importar más que la sencillez de la automatización. El despliegue se separó del aprovisionamiento: root configura una vez la ruta de despliegue y, a partir de ahí, un usuario sin privilegios vuelve a desplegar ejecutando un único

script fijo mediante una regla de alcance limitado que permite ese comando sin argumentos. Construir la imagen, reiniciar el servicio. Sin shell de root ni comandos arbitrarios.

Resultado. Los contenedores se ejecutan bajo el supervisor que ya era de confianza, detrás del cortafuegos que ya estaba declarado, y una publicación rutinaria usa una única orden de alcance limitado, sin un intérprete de comandos de root. La elección contraria a la opción predeterminada está escrita con su motivo, que importa más que la elección — todos los artículos que lea le dirán a la siguiente persona que use la opción predeterminada.

Aplique esta experiencia a su proyecto

Utilice «Contenedores con Podman y Quadlet» como punto de partida para un reto similar en su organización. Los servicios que respaldan este trabajo están disponibles para su proyecto. Servidores dimensionados para el uso real, trasladados a la nube o fuera de ella, con la factura mensual calculada de antemano.

Explore nuestros servicios Póngase en contacto →

Mire más allá del resultado

Lea la situación, las decisiones y el resultado de este ejemplo. Podemos hablar de qué partes se adaptan a sus restricciones y cuáles necesitan otro enfoque. Contenedores con Podman y Quadlet — contenedores bajo systemd sin anteponerse al cortafuegos

Explore nuestros servicios Póngase en contacto →

¿Ejecuta contenedores sin abrir huecos en su cortafuegos?

Converse sobre su proyecto con la ingeniera responsable de la entrega. Acordamos por escrito el alcance, la base del precio y el traspaso antes de empezar a trabajar.

Contexto de la función: Ingeniera de automatización de infraestructura. Se apoya en DevOps, Infraestructura, Contenedores (Docker/Kubernetes), Automatización y CI/CD, Linux y servidores y Seguridad. Y ya que está aquí, también se nos da bien Infraestructura en la nube y migración, DevOps y automatización CI/CD, Contenedores y orquestación y Seguridad y gestión de accesos.

Póngase en contacto Explore nuestros servicios

Una parte de **una trayectoria más amplia** — y toda ella está en este sitio.

Cada entrada sigue la misma estructura: la situación, la tarea, lo que hicimos y lo que cambió.

Vea la trayectoria completa

Defina la mejora que necesita

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

¿Ejecuta contenedores sin abrir huecos en su cortafuegos?

Pregunte por las decisiones detrás de «Contenedores con Podman y Quadlet». Hablará con las personas que pueden explicar el trabajo y valorar su propio proyecto.

Explore nuestros servicios

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

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

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

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://platform.engineer.company/es/portfolio/ran-containers-on-podman-and-quadlet/