Engineer Plataformas

Menor exposición en cada unidad systemd

Reduje la exposición de aislamiento systemd en todas las unidades que instala la plataforma — un servicio de monitorización por ausencia de señal pasó de 9,6 UNSAFE a 1,5 y una forja git expuesta a Internet de 8,3 EXPOSED a 1,5 — y añadí una comprobación del analizador durante la convergencia tras encontrar una directiva mal escrita que se ignoraba silenciosamente en tres plantillas de unidades.

septiembre 2026

cada unidad aislada y una errata antes ignorada

Situación. Este repositorio instalaba trece archivos de unidad que se ejecutaban en el host de producción con los privilegios predeterminados del supervisor, que son la mayoría. Una puntuación de endurecimiento situó el servicio del interruptor de hombre muerto en 9,6 y lo calificó de inseguro; la forja git expuesta a Internet obtuvo un 8,3 y la calificación de expuesta. Ambos números eran correctos y ninguno había provocado ninguna actuación, porque una puntuación sin un umbral asociado es un número que la gente aprende a saltarse.

Tarea. Cada unidad necesitaba un entorno de aislamiento proporcional a lo que hace realmente, y esos entornos necesitaban una comprobación, porque el modo de fallo de un aislamiento incorrecto consiste en que la unidad arranca y luego se rompe en un punto que el analizador no puede ver.

Acción. Se incorporaron restricciones de privilegios a cada plantilla de unidad — un techo de privilegios fijado en los propios de la unidad, un filtro de llamadas al sistema, familias de direcciones restringidas y memoria que puede ser escribible o ejecutable, pero nunca ambas cosas. Los resultados medidos: el interruptor de hombre muerto pasó de 9,6 a 1,5, la forja de 8,3 a 1,5 y las dos unidades de copia de seguridad de 9,6 a 2,3 y 2,5. Al escribirlas apareció algo mejor que las puntuaciones. Una directiva llevaba mal escrita en tres plantillas de unidad desde que existían esos roles — un nombre de aspecto plausible que no

existe, al que el supervisor responde registrando que no reconoce la clave y arrancando la unidad de todos modos. Buscar una directiva con grep demuestra que se escribió; solo el analizador demuestra que surtió efecto. Por eso, un rol de verificación pasa ahora cada unidad por el verificador del propio supervisor durante la convergencia, y todos los roles que instalan una unidad lo incluyen. Lo que aún no puede ver queda dicho claramente en los mismos documentos: todas las directivas capaces de romper estas unidades las rompen en tiempo de ejecución, no durante el análisis, y una puntuación no puede decir si un script sigue llegando a su última línea.

Resultado. Cada unidad se ejecuta con los privilegios que necesita y sin los que no necesita, los números se miden en lugar de afirmarse y la clase de defecto en la que una errata se convierte en un control ausente de forma silenciosa hace fallar ahora una ejecución. Los límites de la medición están registrados junto a ella, que es la parte que evita que la siguiente persona que la lea confíe demasiado en una banda verde.

Aplique esta experiencia a su proyecto

Utilice «Menor exposición en cada unidad systemd» como punto de partida para un reto similar en su organización. Los servicios que respaldan este trabajo están disponibles para su proyecto. Toda la configuración escrita en archivos para poder recrearla con exactitud y evitar que exista solo en la memoria de una persona.

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. Menor exposición en cada unidad systemd — cada unidad aislada y una errata antes ignorada

Explore nuestros servicios Póngase en contacto →

¿Tienen sus servicios más acceso del que necesitan?

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 fiabilidad de sistemas. Se apoya en Infraestructura, Contenedores (Docker/Kubernetes), Automatización y CI/CD, Linux y servidores, Seguridad y Pruebas y control de calidad. Y ya que está aquí, también se nos da bien Infraestructura como código, Contenedores y orquestación, Administración de sistemas 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 →

¿Tienen sus servicios más acceso del que necesitan?

Pregunte por las decisiones detrás de «Menor exposición en cada unidad systemd». 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/cut-systemd-sandbox-exposure-on-every-unit/