**Engineer**

# Infraestructura

49 logros

## Conecte las partes de su sistema

Los trabajos reunidos en «Infraestructura» muestran una parte de un sistema en funcionamiento. Podemos ayudar a conectar esa parte con el resto de su operación. Monitorización y alertas que avisan cuando un fallo aún es pequeño, y cifras que muestran con qué frecuencia se mantiene así.

**Explore nuestros servicios** Póngase en contacto →

## Encuentre un reto comparable

Siga un ejemplo que se parezca a su situación. Su reseña describe las decisiones detrás del resultado, más allá de la etiqueta tecnológica. Primer panel de observabilidad de la empresa — la primera visión de la empresa sobre sus propios sistemas

**Primer panel de observabilidad de la empresa** Póngase en contacto →

### Un plan de infraestructura para 14 departamentos

Diseñé un marco integral de infraestructura para un instituto de investigación que abarcaba 14 departamentos, con módulos flexibles, flujos de datos unificados y estrategias de soporte estructuradas para facilitar su adopción a largo plazo.

### Primer panel de observabilidad de la empresa

Desarrollé y puse en marcha el primer panel de observabilidad de la empresa, con información del rendimiento del sistema en tiempo real y visualizaciones de datos en el televisor grande de la oficina.

### 10 servidores PostgreSQL y MS SQL en Ubuntu

Diseñé, desplegué y mantuve 10 servidores PostgreSQL y MS SQL en VPS con Ubuntu Linux, para mantener un rendimiento y una fiabilidad adecuados.

### 1.000 reglas RBAC para servidores Linux

Reforcé la seguridad de los datos mediante 1.000 reglas RBAC para desarrolladores, instancias de aplicaciones, PostgreSQL, MS SQL y otros servidores Linux, evitando accesos no autorizados y documentando la configuración mediante automatización con Ansible.

### 100 copias críticas automatizadas con Barman

Automaticé 100 copias de seguridad de datos críticos con Barman, Google Cloud, Bash y Python, preservando la integridad de los datos entre bases de datos.

### 20 aplicaciones Docker en Google Cloud y AWS

Desplegué y mantuve 20 aplicaciones en contenedores Docker, resolví incidencias con Podman y Kubernetes y administré aplicaciones basadas en R en Google Cloud y AWS.

### Administración de 30 VPS Ubuntu Linux

Administré 30 instancias VPS con Ubuntu Linux, implementé estrategias de recuperación ante desastres y mantuve configuraciones de red adecuadas.

### Gestión de accesos con M365 y SSO

Prevení brechas de seguridad al dirigir iniciativas de gestión de accesos con M365, 1Password, Red Hat SSO y OKTA SSO.

### Menor riesgo con Grafana y Prometheus

Reduje los riesgos operativos mediante un panel de monitorización con Grafana y Prometheus, mejorando la fiabilidad del sistema.

### Gestión de 8 conexiones VPN WireGuard e IPsec

Administré y resolví incidencias en 8 conexiones VPN de WireGuard e IPsec, manteniendo comunicaciones seguras entre Google Cloud y sistemas Linux.

### Procesos renovados: 8.000 horas ahorradas

Reorganicé los procesos internos y ahorré 8.000 horas mediante mejoras en la arquitectura del software, los sistemas y la planificación.

### Administración de infraestructura de red

Administré la infraestructura de red de más de 1.000 servidores, atendiendo al despliegue, la seguridad y la resolución de incidencias de los sistemas.

### SSL/TLS automático para 100 aplicaciones Docker

Automaticé la creación de certificados SSL/TLS para 100 aplicaciones Docker, manteniendo conexiones seguras entre servidores Ubuntu Linux.

### Configuración y despliegue de 1.000 routers Wi-Fi

Configuré y desplegué 1.000 routers Wi-Fi, mejorando el acceso a la red y su rendimiento para los clientes.

### Administración de 100 servidores Bare Bone

Administré 100 servidores Bare Bone, redes físicas y sistemas de telefonía IP, proporcionando una infraestructura sólida para el crecimiento de la empresa.

### 40 sitios web con Apache y Nginx

Administré 40 sitios web en servidores de alojamiento Ubuntu Linux con Apache y Nginx, manteniendo una disponibilidad y un rendimiento elevados.

### Un producto cartográfico de principio a fin

Diseñé la arquitectura, desarrollé y mantuve infraestructura, procesamiento de datos y una aplicación de mapas durante 2 años, cubriendo tanto entregas de software como mantenimiento operativo.

### Infraestructura simplificada fuera de AWS

Reorganicé la infraestructura de un cliente internacional, eliminando servicios sin uso, ajustando la capacidad y trasladando cargas fuera de AWS. La fundadora informa de una reducción del gasto en la nube por un factor de 10, sin pérdida de productividad.

### Infraestructura Azure como código

Aprovisioné infraestructura Azure como código con Bicep — Container Apps, PostgreSQL Flexible Server, Front Door/WAF y redes — en los entornos de desarrollo, preproducción y producción.

### Despliegues completos de la plataforma en Azure

Asumí los despliegues completos de la plataforma en Azure y gestioné las versiones en desarrollo, preproducción y producción.

### Copias y recuperación ante desastres como código

Configuré la retención de las copias de seguridad de la base de datos como infraestructura como código, audité la capacidad de recuperación y documenté el procedimiento de restauración, dejando explícitas las carencias pendientes para evitar descubrirlas durante un incidente.

### Soporte 24/7 para unos 1.000 servidores IPTV/OTT

Presté soporte de infraestructura 24/7 a una plataforma de distribución IPTV/OTT, administrando unos 1.000 servidores y sistemas de los clientes para usuarios de China, Estados Unidos y Alemania.

### Transmisión IPTV ininterrumpida

Mantuve la entrega ininterrumpida de señales IPTV entre proveedores y clientes, monitorizando y manteniendo la red de distribución y la telefonía IP las 24 horas.

### Infraestructura aún en servicio años después

Planifiqué e implementé nuevas funciones de infraestructura para sistemas internos y externos, con soluciones que siguieron funcionando años después con cambios mínimos.

### Infraestructura principal creada desde cero

Como una de las primeras incorporaciones, diseñé y construí desde cero toda la infraestructura principal y los procesos de soporte de una startup SaaS de energía verde, sentando las bases para un crecimiento rápido.

### Gestor de contraseñas para toda la empresa

Integré un sistema de gestión de contraseñas para toda la empresa, reforzando la seguridad y simplificando el control de accesos.

### Monitorización de errores y trazas propias

Desarrollé internamente la monitorización de errores y las trazas OpenTelemetry, en lugar de adquirirlas — saneamiento de cargas, detección de picos y regresiones, resolución de símbolos y una señal de actividad sintética —, con 11 vistas para operaciones.

### Infraestructura definida en un repositorio

Desarrollé la infraestructura de la empresa mediante 19 playbooks de Ansible y 34 roles en 12.065 líneas de YAML, haciendo converger un servidor activo hacia un estado declarado con todas las ejecuciones idempotentes.

### Servicios públicos en un servidor pequeño

Alojé los servicios públicos de la empresa en un host de 512 MB y un solo núcleo — una forja git, un servidor web para siete dominios, Tor, dos servidores de protocolos alternativos y bloqueo de intrusiones — tomando los 464 MB de memoria utilizable como restricción de diseño; la automatización de copias de seguridad es una implementación aparte.

### Tres cerraduras en la puerta, ninguna cerrada

Detecté y corregí tres protecciones contra fuerza bruta SSH que nunca habían funcionado: una jail de bloqueo que vigilaba el puerto 22 mientras el demonio escuchaba en el 1986, un límite de tasa oculto bajo una regla más amplia y una acción de bloqueo cuyo binario nunca se encontraba, por lo que no se había aplicado ningún bloqueo.

## SSH reforzado con 24 directivas verificadas

Reforcé SSH con 24 directivas verificadas mediante validación en tres etapas — archivo candidato, configuración ensamblada y lectura de la configuración por el propio demonio —, después de que esta última detectara que el servidor en ejecución anulaba silenciosamente dos de las veinticuatro.

## Bloqueo de intrusiones probado en cada ejecución

Verifiqué de extremo a extremo el bloqueo de intrusiones en cada ejecución de refuerzo, bloqueando una dirección reservada para pruebas, comprobando la regla resultante del núcleo y retirando el bloqueo en un bloque de limpieza garantizado, para que una jail averiada haga fallar la ejecución en vez de presentarse como operativa.

## Reglas de cortafuegos verificadas por posición

Verifiqué las reglas del cortafuegos por su posición, además de por su existencia, leyendo la lista numerada de reglas y la cadena activa del filtro de paquetes, porque una regla presente puede no recibir nunca un paquete.

## Automatización de copias con un método explícito de restauración

Implementé automatización de copias con restic, retención, comprobaciones de integridad y un flujo mensual de prueba de restauración; documenté la activación del almacenamiento y la verificación de restauración real como pasos operativos separados.

## Monitorización por ausencia de señal

Desarrollé una monitorización por ausencia de señal que solo avisa de actividad mientras la memoria y el disco están en buen estado, de modo que un servidor degradado genera una alerta al quedar en silencio; además detecté seis variables llamadas «free» cuando el control medía correctamente «available», valores separados por un orden de magnitud en una máquina de 464 MB.

## Modo de comprobación Ansible fiel a la realidad

Hice que el modo de comprobación reflejara la realidad en toda la plataforma tras detectar seis sondeos que decidían a partir de un valor que el servidor nunca había proporcionado, porque el módulo command de Ansible informa de éxito con --check aunque omita la orden por completo.

## Comprobación de secretos en un segundo

Añadí una comprobación previa que ejecuta en aproximadamente un segundo el mismo código de convergencia sobre secretos locales del operador, después de que una ejecución de producción parcialmente aplicada fallara en su novena tarea con los ajustes de intercambio ya escritos en el servidor activo.

## Zona DNS de 20 registros como código

Concilié declarativamente una zona DNS de 20 registros con la API de Cloudflare mediante puntos de entrada separados para auditoría y exportación BIND, y desactivé el proxy CDN por motivos de privacidad después de implementarlo.

## 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.

## 7 roles de informes de solo lectura

Desarrollé siete roles de informes de solo lectura que representan un servidor activo en Markdown — inventario técnico, acceso, git, métricas, tráfico, seguridad e inventario de proveedores — bajo la regla de no imprimir ninguna cifra que la ejecución no haya medido.

## Su código en su propio servidor

Desplegué la forja git propia de la empresa con Soft Serve, privada por defecto, sin panel web y con el puerto SSH limitado a loopback detrás de un servidor de salto, e hice de su página de entrada un artefacto de compilación del sitio principal en lugar de una copia mantenida a mano.

## 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.

## Segundo servidor aprovisionado desde código

Automaticé el aprovisionamiento de un segundo servidor en un segundo proveedor de nube y creé el cortafuegos antes que la máquina para que naciera protegida, con los cortafuegos de ambos proveedores configurados directamente mediante sus API REST para evitar una colección de terceros.

## Regla de alcance tras una fuga de credenciales

Incorporé al repositorio una regla de alcance tras una reorganización que había introducido el inventario, los permisos de cortafuegos y textos de otra empresa, y mantuve los residuos en cuarentena bajo el detector de secretos, sin excluirlos.

## Secretos operativos separados por servidor

Separé los cuatro secretos operativos de cada servidor tras constatar que dos servidores que comparten una señal de actividad alertan menos que dos señales independientes, y que una contraseña compartida de copias de seguridad puede exponer las copias de ambos servidores, incluso en repositorios separados, si alguien la obtiene y puede leer los datos cifrados y los archivos de claves de ambos repositorios.

## Espejos del sitio en Gemini y Gopher

Construí salidas Gemini y Gopher a partir de la misma fuente del sitio web; el logro registra 777 documentos en cada formato en aquella etapa, con cero bytes de HTML modificados al añadir los formatos.

## Ensayo del hook CI: 2 defectos detectados

Ensayé el hook CI del servidor de la forja y encontré dos defectos imposibles de alcanzar leyendo el archivo: una alternativa que introducía un argumento irresoluble en la entrada del hook y una variable de entorno de git que acompañaba al control hasta el checkout y hacía fallar 19 pruebas.

## 13 direcciones medidas sin rastreo

Medí trece direcciones únicamente a partir del registro de accesos del servidor web — sin cookies, rastreadores ni servicios de terceros —, enmascarando la red del cliente al escribir cada línea e incorporando el resultado a un archivo permanente de 21 recuentos diarios y 20 facetas mensuales.

## Espejo onion de Tor con una dirección legible

Publiqué el sitio como espejo onion de Tor en una dirección legible que comienza por engineer, con la clave generada fuera del servidor para que nunca llegara a este repositorio ni a un portátil, y lo mantuve como la única de las cuatro puertas de entrada que nunca se contabiliza.

Centre el esfuerzo de ingeniería

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 →

# Sitúe el tema en su contexto

Cuéntenos cómo aparece «Infraestructura» en su propio sistema. Podemos ayudarle a elegir el servicio relevante y definir el trabajo en torno a él.

**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://engineer.company/es/categories/infrastructure/