Inyección de Claves SSH en GitHub Actions: Anatomía de un Despliegue rsync

Cuadernillo | Vol. 1

mercedev.es — 2026-05-05 | Fase 11 (CI/CD y Lighthouse)

1. El Desafío (Síntoma)

Durante la configuración del flujo de CI/CD (Continuous Integration / Continuous Deployment - Integración Continua / Despliegue Continuo) en GitHub Actions para el despliegue automático del sitio estático, se presentaron dos fallos críticos que bloquearon la subida de archivos hacia el servidor VPS (Virtual Private Server - Servidor Privado Virtual):

1. **Fallo de variables vacías:** El comando `ssh-keyscan` devolvió un error de sintaxis (`usage: ssh-keyscan...`), indicando que la variable que contenía la IP del servidor no se estaba inyectando en la máquina virtual.
2. **Fallo de autenticación:** Al ejecutar la sincronización de archivos, el servidor rechazó la conexión con un error `Permission denied (publickey)`, a pesar de que la clave había sido configurada.

2. La Maniobra (Lógica)

La resolución de estos incidentes requirió aplicar tres correcciones estrictas sobre la gestión de secretos y la invocación de la herramienta de despliegue:

- **Segregación Estricta de Secretos:** GitHub Actions no procesa archivos combinados ni entiende el formato manual "Clave: Valor" en su interfaz. Se crearon tres secretos independientes (`SERVER_IP` , `SERVER_USER` , `DEPLOY_SSH_KEY`), insertando el valor crudo (raw) en las cajas de texto sin comillas ("") ni etiquetas delimitadoras.
- **Preservación del Formato de la Clave Privada:** La clave privada SSH (Secure Shell) debe conservar escrupulosamente sus saltos de línea y las cabeceras `-----BEGIN OPENSSH PRIVATE KEY-----`. Para evitar la corrupción de formato que a menudo produce la selección de texto en la terminal del sistema, se utilizó un editor de texto gráfico para extraer y copiar la clave inmaculada.

- **Enrutamiento Explícito en rsync:** Se parcheó el flujo de trabajo (`deploy.yml`) para forzar a la herramienta de sincronización a utilizar la clave recién inyectada mediante el parámetro `-e` : `rsync -avz -e "ssh -i ~/.ssh/id_ed25519" --delete public/ ...`

3. El Aprendizaje / Deuda Técnica

En el diseño de Infraestructura como Código (IaC - Infrastructure as Code), la gestión y el paso de secretos hacia herramientas de terceros es el punto de mayor fricción.

Las máquinas virtuales efímeras (runners) no poseen la "inteligencia" de un entorno local preconfigurado; no buscarán claves SSH por defecto si no se les indica explícitamente su ubicación exacta. Convertir variables de entorno en archivos físicos temporales en la nube (`echo "$SSH_PRIVATE_KEY" > ~/.ssh/id_ed25519`) es una técnica válida y segura, pero exige guiar manualmente a herramientas de bajo nivel como `rsync` hacia esa ruta.

Dominar este flujo operativo permite conectar de forma segura cualquier repositorio público con infraestructuras corporativas privadas, manteniendo las claves bajo cifrado de grado militar.