

Helgen

Ingeniería que produce, mantenimiento que protege

Consulta de Logs en Grafana

Observabilidad del backend `htracker` — Grafana Loki (capa gratuita)

Helgen Drogheda

Fleet RTK GPS — Hutchison Ports (ICAVE · TIMSA · EIT · LCT)

Documento	Manual de Operación
Versión	1.0
Fecha	22 de junio de 2026
Autor	Dr. Leopoldo Rodríguez Salazar — Helgen Technologies
Sistema	<code>htracker</code> (retranslator + monitor), servidor <code>HelgenServer</code>
Fuente	<code>04-Source-Code/htracker/log-shipping/</code>
Clasificación	Confidencial — Uso interno

Índice general

1	Propósito	1
2	Arquitectura del envío de logs	1
3	Acceso a Grafana	2
3.1	Grafana en la nube (nada que instalar)	2
3.2	Grafana local (si prefieres correr la interfaz tú mismo)	2
4	Cómo consultar los logs (LogQL)	2
5	Qué se registra	2
6	Retención, límites y seguridad de disco	3
7	Verbosidad (nivel de log)	3
8	Salud del envío y diagnóstico	3
9	Puesta en marcha / reinstalación	3
10	Referencia rápida de consultas	4

1 Propósito

El servidor del backend tiene **muy poco disco**, por lo que el gateway **no** guarda logs localmente. En su lugar, los registros se **envían fuera del servidor** a **Grafana Loki** (capa gratuita) y se consultan desde **Grafana**. Este manual explica cómo *entrar* a Grafana y *consultar* los logs de la flota – no requiere acceso al servidor para leer.

En una frase

Los logs del backend viven en **Grafana Loki**. Para verlos: abre Grafana → **Explore** → fuente de datos **Loki** → escribe `{job="htracker"}`.

2 Arquitectura del envío de logs

El gateway escribe a la salida estándar; `systemd` la captura en `journald` (un búfer en anillo **limitado a 200 MB**, que nunca llena el disco); un agente ligero (**Vector**, o **Grafana Alloy**) lee el journal y lo empuja por HTTPS a Loki.



Por qué así: el gateway nunca escribe un archivo que crece; `journald` es un búfer pequeño y limitado (sobrevive cortes breves de Loki); el agente empuja con un búfer acotado que *descarta lo más nuevo* si Loki no responde – de modo que la ruta de logs **jamás** bloquea ni tumba al gateway.

¿Vector o Alloy? — verifícalo una vez

El `setup-logging.sh` instala **Vector** por defecto (etiqueta `job="htracker"`). Si en su lugar se usó el *onboarding de Linux* de Grafana Cloud, el agente es **Alloy** y los logs aparecen por unidad de `systemd` (`{unit="htracker.service"}`). Si una consulta no devuelve nada, usa el **Label browser** de Grafana para

ver qué etiquetas existen.

3 Acceso a Grafana

3.1 Grafana en la nube (nada que instalar)

1. Entra a tu **stack de Grafana Cloud** (URL del tipo `https://<stack>.grafana.net`).
2. Menú lateral → **Explore**.
3. Arriba, selecciona la fuente de datos **Loki**.
4. Escribe la consulta (sección 4) y presiona **Run query**. Ajusta el rango de tiempo arriba a la derecha.

3.2 Grafana local (si prefieres correr la interfaz tú mismo)

Los datos siguen en Grafana Cloud; sólo el visor es local.

```
docker run -d --name grafana -p 3000:3000 grafana/grafana-oss
# http://localhost:3000 (admin/admin)
# Connections -> Data sources -> Loki:
# URL: <LOKI_URL> Auth: Basic user: <LOKI_USER> password: <LOKI_TOKEN>
```

Credenciales

LOKI_URL, LOKI_USER y LOKI_TOKEN están en `/etc/vector/htracker.env` del servidor y en la consola de Grafana Cloud (*Connections* → *Hosted logs*). **Son secretos** – viven en `.env.vector` (ignorado por git); nunca se suben al repo.

4 Cómo consultar los logs (LogQL)

En **Explore** con la fuente **Loki**. Loki indexa **etiquetas**, no el texto; todo lo demás se filtra con `|=` (contiene) en el momento de la consulta.

```
{job="htracker"} # todo el backend
{job="htracker", level="error"} # sólo errores
{job="htracker", unit="htracker.service"} # sólo el gateway (retranslator)
{job="htracker"} |= "Anti-Salto" # rechazos del filtro anti-salto
{job="htracker"} |= "victimas_backend" # el resumen 1/min (victimas de backend)
{job="htracker"} |= "ADDR-CHANGE" # cambios de direccion SIM/NAT
```

Si el envío es por **Alloy** (no Vector), usa la unidad de systemd:

```
{unit="htracker.service"}
{unit="htracker.service"} |= "victimas_backend"
```

5 Qué se registra

Etiquetas (labels)	<code>job=htracker, host, unit (htracker.service / -web / -notifier), level (info/warn/error/debug)</code>
Nivel por defecto	INFO: sólo eventos + una línea de resumen cada 60 s ([SUMMARY] / <code>victimas_backend</code>). El detalle por paquete es DEBUG y no se envía.
Eventos clave	anti-salto (Anti-Salto), cambios de dirección SIM/NAT (ADDR-CHANGE), víctimas de backend (unidad en línea en htracker pero ausente en Wialon).

6 Retención, límites y seguridad de disco

- **Loki (capa gratuita):** 50 GB/mes, **retención de 14 días**, Grafana incluido. Tras el recorte de verbosidad se usa una fracción mínima.
- **journald (servidor):** SystemMaxUse=200M, retención 3 días (/etc/systemd/journald.conf.d/htracker.conf). Aunque Loki esté caído días, el disco **no** se llena.
- **Búfer de Vector:** en memoria, descarta lo más nuevo si Loki no responde.

7 Verbosidad (nivel de log)

- GW_LOG_LEVEL (por defecto INFO). Para depurar una unidad en vivo, ponlo en DEBUG *temporalmente*.
- GW_LOG_SUMMARY_S (por defecto 60) – cadencia del resumen.

No dejes DEBUG encendido

DEBUG registra cada paquete e inunda la tubería (y consume la cuota de Loki). Úsalo unos minutos y regresa a INFO.

8 Salud del envío y diagnóstico

En el servidor (ssh HelgenServer):

```
systemctl status vector          # esta activo el agente?
journalctl -u vector -f          # esta enviando? errores de Loki?
```

No aparecen logs en Grafana: (1) confirma vector activo; (2) revisa credenciales/endpoint en /etc/vector/htracker.env; (3) verifica el rango de tiempo en Grafana; (4) revisa el **Label browser** (¿job o unit?, Vector vs Alloy).

9 Puesta en marcha / reinstalación

Sólo si hay que reinstalar el envío (normalmente ya está activo). En el servidor, desde /home/itadmin/htracker/log-shipping:

```
cp .env.vector.example .env.vector
nano .env.vector          # pega LOKI_URL / LOKI_USER / LOKI_TOKEN
./setup-logging.sh        # limita journald, --no-filelog, instala Vector, arranca
# ./setup-logging.sh --journald-only # si Grafana Alloy ya envía el journal
```

deploy.sh ya sincroniza la carpeta log-shipping/ al servidor. Detalle completo: 04-Source-Code/htracker/log-shipping/README

10 Referencia rápida de consultas

Consulta	Qué muestra
<code>{job="htracker"}</code>	Todo el backend
<code>{job="htracker", level="error"}</code>	Sólo errores
<code>{job="htracker", unit="htracker.service"}</code>	Sólo el gateway (retranslator)
<code>{job="htracker"} = "victimas_backend"</code>	Resumen 1/min – víctimas de backend
<code>{job="htracker"} = "Anti-Salto"</code>	Rechazos del filtro anti-salto
<code>{job="htracker"} = "ADDR-CHANGE"</code>	Cambios de dirección SIM/NAT