Engineer

Registro de eventos

Registro de lo que ocurre a medida que sucede

Qué es

El registro de eventos, o logging, consiste en que un programa lleve un historial continuo de su propio comportamiento, con una entrada por evento: una solicitud atendida, una contraseña rechazada, un reintento o un cierre inesperado. Cada entrada, llamada línea o registro de log, contiene al menos una marca de tiempo y un mensaje, de modo que después pueda reconstruirse qué sucedió y en qué orden. El proyecto OpenTelemetry define un log como un registro de texto con marca de tiempo, estructurado o no estructurado, con metadatos opcionales; señala que, de todas las señales de telemetría, los logs son los que tienen un mayor legado.

Ese legado tiene un estándar. Syslog, el veterano protocolo para enviar mensajes de eventos a un recolector, se normalizó en marzo de 2009 mediante RFC 5424, que deja obsoleto el anterior RFC 3164. Asigna a cada mensaje una de ocho severidades, desde 0, Emergency, hasta 7, Debug. La mayoría de las bibliotecas de registro usa una escala más corta con la misma idea: debug, info, warning, error. El modelo de datos de logs de OpenTelemetry asigna a cada severidad un número del 1 al 24, en seis bandas de TRACE a FATAL.

Una línea no estructurada es texto libre: una persona la lee fácilmente, pero una máquina solo puede descomponerla con una expresión regular escrita para esa redacción exacta. Una línea estructurada sigue un esquema fijo: todas las entradas tienen los mismos campos con nombre, tipos y significados. OpenTelemetry prefiere los logs estructurados en producción y añade una advertencia fácil de pasar por alto: que una línea codificada como JSON pueda analizarse no la convierte en estructurada; lo que la hace estructurada es un esquema estable. Aunque aquí se muestra en varias líneas, una entrada estructurada ocupa una sola línea en disco:

```
{
    "time": "2026-09-14T03:12:07.412Z",
    "severity": "WARN",
    "service": "checkout",
    "event": "payment.retry",
    "attempt": 3,
    "trace_id": "4bf92f3577b34da6a3ce929d0e0e4736"
}
```

Las métricas y las trazas son las señales que suelen recopilarse junto a los logs. Las métricas son números muestreados a lo largo del tiempo, baratos de conservar y útiles para indicar con qué frecuencia ocurre algo. Las trazas siguen una solicitud por todos los servicios que atraviesa. Un log conserva el detalle de eventos individuales: por eso se consulta después de una alerta para averiguar la causa. OpenTelemetry vincula los logs con las trazas adjuntando los identificadores de la traza y del tramo activos a cada registro.

Utilice el concepto en una decisión

Aplique «¿Qué es el registro de eventos?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. 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 →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. 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 →

Por qué importa

En la mayoría de los sistemas, el log es el único relato del pasado que queda. Una métrica puede indicar que los errores aumentaron a las 03:12; el log indica qué solicitud fue, de qué servicio, con qué valor y qué hizo el programa después. Si algo falla por la noche y se ha recuperado por la mañana, el log es el testigo que permanece.

Ese relato tiene un precio que se paga de tres maneras. Cada línea consume disco, operaciones de entrada y salida y tiempo de procesador; cuesta más si se envía a un almacén central, donde un servicio alojado suele cobrar por el volumen recibido. Cada línea también contiene datos conservados sobre alguien: el registro de acceso de un servidor web guarda las direcciones y los navegadores de quienes lo consultaron. Y cada línea necesita protección. La hoja de recomendaciones de registro de OWASP pide que cada evento indique cuándo,

dónde, quién y qué, y que los propios logs estén protegidos contra manipulaciones y contra el acceso, la modificación y el borrado no autorizados, porque pueden contener información personal y otros datos sensibles.

A escala organizativa, la publicación especial NIST 800-92, Guide to Computer Security Log Management, de Karen Kent y Murugiah Souppaya, publicada en septiembre de 2006, trata la gestión de logs como infraestructura y procesos de toda la empresa, en lugar de un ajuste de un programa.

Los logs también funcionan mejor junto a los números. La guía de instrumentación de Prometheus propone un contador por cada línea de código que registra eventos, para que, cuando aparezca un mensaje de interés, pueda saberse cuántas veces ha ocurrido y durante cuánto tiempo. También propone comparar los totales de líneas info, warning y error entre versiones.

Cómo se aplica en la práctica

La página de privacidad describe línea por línea el registro de acceso de este sitio. Cada solicitud registra la página y la hora, el estado de la respuesta, la descripción que el navegador da de sí mismo, el nombre del sitio de procedencia y una dirección de red parcialmente ocultada: su último tramo se sustituye por ceros al escribir la línea, antes de que nada llegue al disco. Una línea se conserva unos treinta días. El servidor cierra cada archivo una vez al día, o antes si alcanza unos 10 MB, y elimina el archivo cerrado veintiocho días después; cada noche, una comprobación vuelve a leer todos los archivos y falla si encuentra una línea de más de treinta días. El sistema de conservación falló dos veces, y la página documenta ambos casos. En septiembre de 2026, las direcciones con poco tráfico tardaban tanto en llenar 10 MB que sus archivos nunca se habían cerrado y aún contenían todas las líneas desde el inicio del registro; se añadió una tarea diaria para cerrarlos. El 26 de octubre de 2026, siete de las trece direcciones que mantienen un registro seguían escribiendo en archivos que esa tarea había marcado como cerrados; una conservaba un archivo cerrado de cuarenta y siete días. La tarea se retiró y ahora el propio servidor cierra y elimina los archivos.

Una ejecución completa de pruebas de una aplicación macOS registró 610.996 líneas de log del núcleo de la aplicación. Una ráfaga de eventos del log del núcleo de la aplicación se retenía en un flujo principal sin límite y se copiaba a flujos de suscriptores cuyos consumidores no los usaban. El registro del incidente documenta por separado informes de diagnóstico con 111 GB de páginas comprimidas en una máquina de 36 GB y una muestra del consumo de memoria

que mostraba un crecimiento de unos 41 MB por segundo durante un bucle de reintentos de conexión. Los búferes limitados, las suscripciones filtradas por tipo de evento y un límite de frecuencia de registro abordaron esa ruta de eventos. La comparación documentada de ejecuciones completas de pruebas redujo las líneas del log del núcleo de la aplicación a 1.411. No es una prueba comparativa de producción ni una cifra de memoria medida después de la corrección. El límite descarta información de forma deliberada: pueden descartarse eventos de diagnóstico repetitivos y actualizarse el estado afectado, en lugar de retener eventos sin límite. Otros tiempos de espera durante el cierre necesitaron su propia corrección.

En un servidor de producción, una intervención para reforzar la seguridad de trece unidades systemd encontró una directiva mal escrita en tres plantillas de unidad desde que existían esos roles. Ante una clave que no reconoce, el gestor de servicios registra el hecho y arranca la unidad de todos modos; la única huella del error era una advertencia en un log, y se descubrió al reescribir las unidades. Ahora todas pasan por el verificador del propio gestor de servicios en cada convergencia de la configuración, de modo que esa misma errata hace fallar la ejecución.

Dónde surgen los problemas

El log crece más deprisa cuando el sistema ya está fallando. Un bucle que registra cada reintento escribe unas pocas líneas un día normal y miles por segundo un mal día, quitando disco, memoria y tiempo de procesador a un sistema sin recursos de sobra. OWASP pide comprobar que el registro no pueda usarse para agotar los recursos del sistema, por ejemplo llenando el disco. Asigne un límite a cada ruta de ejecución frecuente, agrupe los mensajes repetidos en una sola línea con un recuento y mantenga un contador junto al mensaje, para conservar la frecuencia aunque se descarten líneas.

Se escriben secretos y datos personales. Registrar una solicitud completa conserva todo lo que contenga. La lista de OWASP de datos que normalmente deben eliminarse, ocultarse, transformarse mediante una función hash o cifrarse antes de llegar al log incluye identificadores de sesión, tokens de acceso, contraseñas, cadenas de conexión a bases de datos, claves de cifrado y datos de tarjetas de pago. Hágalo al escribir la línea, como hace con las direcciones el registro de acceso anterior: cuando alguien vaya a limpiarla, puede estar ya en una copia de seguridad o en un archivo histórico.

Una entrada externa escribe una línea falsa. Un valor proporcionado por el usuario que contenga un retorno de carro o un salto de línea, escrito sin escapar en un log de texto, puede iniciar una línea nueva indistinguible de una escrita por la aplicación. OWASP lo llama inyección en logs y pide sanear esos caracteres y codificar los datos para el formato de destino. Un registrador estructurado que escribe cada valor como una cadena JSON escapada lo hace por construcción.

Se interpreta un log silencioso como un sistema sano. Un disco lleno, un archivo rotado que el programa nunca volvió a abrir o un recolector caído parecen lo mismo desde fuera: dejan de llegar líneas. OWASP pide un mecanismo para detectar que el registro se ha detenido. Cuente las líneas por minuto de cada origen y emita una alerta si el recuento cae a cero, para que un hueco en el log genere su propia alerta.

Lecturas adicionales

- Logs — OpenTelemetry explica qué es un log, por qué se prefieren los logs estructurados y cómo se vinculan con las trazas.
- Modelo de datos de logs — los campos de un registro, sus dos marcas de tiempo y la escala de severidad del 1 al 24.
- RFC 5424: el protocolo Syslog — el formato de los mensajes syslog y sus ocho severidades.
- NIST SP 800-92 — la guía de gestión de registros de seguridad informática.
- Hoja de recomendaciones de registro — OWASP sobre qué eventos registrar, qué datos excluir y cómo proteger el resultado.
- Instrumentación — las prácticas de Prometheus para instrumentar código, incluido el registro de eventos.

Glosario

Elija según sus restricciones reales

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 →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es el registro de eventos?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

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/glossary/logging/