

ESCUELA INDUSTRIAL SUPERIOR

PEDRO DOMINGO MURILLO

INFORMATICA INDUSTRIAL

gsr – 600

 “logs”

NOMBREs:

 Henrry Condori Chambi

 Gido Nixon Huanca Pacheco

DOCENTE:

 Ing. Hugo Choque

FECHA: 3 / Octubre / 2017

“logs”

**¿Qué son los Logs y por qué deben interesarte?**

En los últimos años, las innovaciones tecnológicas han tenido un fuerte impacto en cualquier ámbito, tanto personal como profesional. A día de hoy, muchas compañías basan gran parte de su actividad empresarial en la tecnología y, en consecuencia, cada vez más estas soluciones se están convirtiendo en herramientas fundamentales para tomar decisiones y detectar problemas de negocio.

**¿Qué es un Log?**

En informática, se usa el término ***log***, **historial de *log*** o **registro** a la grabación secuencial en un [archivo](https://es.wikipedia.org/wiki/Archivo_%28inform%C3%A1tica%29) o en una [base de datos](https://es.wikipedia.org/wiki/Base_de_datos) de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una [red informática](https://es.wikipedia.org/wiki/Red_inform%C3%A1tica), etc.). De esta forma constituye una evidencia del comportamiento del sistema.

Por derivación, el proceso de generación del *log* se le suele llamar guardar, registrar o loguear (un [neologismo](https://es.wikipedia.org/wiki/Neologismo) del inglés *logging*) y al proceso o sistema que realiza la grabación en el *log* se le suele llamar *logger* o registrador.

Generalmente los acontecimientos vienen anotados con:

* El momento exacto o [data](http://dle.rae.es/?id=BsM9P0S) (fecha, hora, minuto, segundo) en el que ocurrió lo que permite analizar paso a paso la actividad.
* Una o más categorizaciones del acontecimiento registrado. Es frecuente usar categorías distintas para distinguir la importancia del acontecimiento estableciendo distintos niveles de registro los cuales suelen ser: depuración, información, advertencia y error.

Tipos

**De aplicaciones**

Los *logs* de aplicaciones graban cronológicamente las operaciones durante el funcionamiento de la aplicación. Su función forma parte de la lógica de la aplicación. Por lo tanto, no debería estar detenida durante el funcionamiento de la misma.

**Del sistemas**

Los archivos de registros de sistema graban cronológicamente los acontecimientos que sobrevienen a nivel de componentes del sistema. Por ejemplo, los sistemas [Unix](https://es.wikipedia.org/wiki/Unix) usan el protocolo [Syslog](https://es.wikipedia.org/wiki/Syslog%22%20%5Co%20%22Syslog) para realizar crear un registro del sistema

Registros

Si la grabación se realiza en un fichero, se llama fichero de registros o archivo de *log* (en inglés *log file*) al [archivo](https://es.wikipedia.org/wiki/Archivo_%28inform%C3%A1tica%29) que contiene las grabaciones. En estos ficheros los eventos vienen por [orden cronológico](https://es.wikipedia.org/wiki/Cronolog%C3%ADa) de tal forma que la generación correcta de estos ficheros es grabar la información concatenando el nuevo contenido al final del contenido del fichero actual.

Típicamente se asigna una línea por acontecimiento, comenzando por el momento exacto o [marca temporal](https://es.wikipedia.org/wiki/Marca_temporal) (fecha, hora, minuto, segundo) en el que tuvo lugar.

¿Cómo se presentan los Logs?

En un escenario habitual, se suelen ejecutar multitud de aplicaciones al mismo tiempo. Su trazabilidad se reduce, en el mejor de los casos, a Logs persistidos en el disco duro de la máquina y, en el peor, a simples trazas de texto por pantalla tipo “print” que desaparecen a los pocos segundos.

Y te estarás preguntado, ¿qué implica esto? Si no se almacenan adecuadamente los Logs, se producen distintos problemas que pueden afectar a la actividad de tu negocio:

* Visibilidad nula de errores para los equipos de desarrollo y/o sistemas. En otras palabras, será difícil detectar problemas y solucionarlos con rapidez.
* Metodología de trabajo no estandarizada, es decir, cada usuario aplicará su propia forma basada en su experiencia.
* Accesos e información descentralizada que causará dificultades para trabajar con estos datos.
* Incremento del tiempo de respuesta ante una incidencia que afectará a niveles de servicio o SLAs (en relación con el nivel de calidad).

¿Cómo lo resolvemos? Afortunadamente, la democratización de la tecnología está permitiendo que cada vez haya más soluciones de código abierto de calidad profesional, como Fluentd. Estas herramientas permiten recolectar de forma eficiente toda la información generada y, en muchos casos, cuentan con opción a soporte de pago.

Explotación de Logs a partir de arquitecturas Big Data

La ingente cantidad de datos que producen las distintas aplicaciones hace que el término Big Datatambién sea aplicable a los Logs. Cada vez más, se tiende a distribuir el trabajo en máquinas más pequeñas pero en mayor número. En consecuencia, es necesario utilizar herramientas que permitan el almacenamiento y procesamiento distribuido de la información. Estamos hablando de arquitecturas Big Data formadas por múltiples sistemas que conforman un clúster de máquinas.

¿Cómo funciona este clúster? Generalmente, los sistemas se reparten las tareas modularmente, es decir, en función de qué son capaces de hacer con esa información. Algunos componentes se encargan de la recolección de datos, así como otros se ocupan de procesar y aplicar operaciones sobre esta información. Por último, varios componentes pueden visualizar y mostrar resultados al usuario final.

¿Qué ventajas tiene la gestión de Logs?

La aplicación de buenas prácticas en la gestión de los Logs aporta distintos beneficios, tanto a nivel de funcionamiento de los sistemas como de objetivos de negocio. Entre otras ventajas, te permitirá:

* Aplicar técnicas de Machine Learning para detectar patrones que te ayuden a tomar decisiones de negocio (por ejemplo, trazas relativas a sistemas de contabilidad).
* Mejorar la gestión y el control de la información facilitando así el acceso y la explotación de estos datos.
* Detectar amenazas de red o virus para poder actuar en consecuencia con rapidez.
* Prevenir fugas de información, así como comportamientos inadecuados que causen errores.

Existen distintas tecnologías libres (Open Source) que nos pueden ayudar a almacenar estos Logs, así como sistemas comerciales que nos permitirán gestionar y visualizar los datos. Con la combinación de ambos elementos, podemos construir sistemas que centralicen y exploten la información para identificar conflictos y tomar mejores decisiones de negocio.