brainlink

YOU RUN YOUR BUSINESS, LEAVE THE IT TO US!

Effective Logging For Unix Systems



Ensuring you can sort and read the logs collected by your Unix system will allow you to gain actionable and understandable intel about the performance of your system.

One of the best features of Unix systems is their flexible and powerful logging system, which will allow you to record nearly any type of event that occurs so you can keep a detailed account of how your systems are performing, as well as manipulate the logs to retrieve the information that you require for a given task.

The key to managing a comprehensive Unix log is to ensure you have an effective taxonomy by which to tag, sort and index your logs. Without a system to sort your logs, there's no right way to review all that information.

An effective way to go about building your taxonomy is to start by organizing by host, and then by log, which looks like this:

TAG	USE	EXAMPLE
Environment	Host Environment	Dev, Stage, QA, Prod
Tier	Host Tier	Web, Application, DB
Service	Host Primary Service	Apache, Ngix, Mysql, Postgress, Application / LOB
Zone	Host Zone	External, DMZ, Internal, Secure, Backup, DR

By tagging at the host level, you ensure that all log inputs from that host or group are correlated when examining events on a group basis, which provides a holistic view of events when searching by groups of hosts.

Furthermore, by tagging log inputs on a per log basis, or by filtering logs to multiple inputs and tagging them will yield a specific way by which to track patterns in events.

When it comes to Unix, the categorization will look like this:

LOG TYPE	USE	TAG
System	OS function(s)	OS
Service	Service Function	Service_Name
Application	Application Specific Logs	Application_name
Event	Event Specific logs	Event_Name or Security

Standard Unix logs, by location and contents, appear as:

LOG	PATH	USE	TYPE
messages	/var/log/message	Catch-all log / centos	OS
syslog	/var/log/syslog	Catch-all log / Debian	OS
auth.log	/var/log/auth.log	Authentication Log	Security
secure	/var/log/secure	Authentication Log / Centos	Security
fail.log	/var/log/fail.log	Authentication Log / Debian	Security
dmesg	/var/log/dmesg	Hardware based events	OS / Performance
kern.log	/var/log/kern.log	Kernal based events	OS / Performance
dmesg	/var/log/dmesg	Hardware based events	OS / Performance
cron	/var/log/cron	Scheduled events	OS
httpd	/var/log/httpd	Basic apache logs / Centos	Web Application
apache2	/var/log/apache2	Basic apache logs / Debian	Web Application
nginx	/var/log/nginx	Basic Nginx logs	Web Application
mysql	/var/log/mysql	Basic mysql logs	DataBase Application
SERVICE	/var/log/SERVICE_NAME	Basic service logs	Service Logs
APPLICATION	/var/log/APPLICATION_NAME	Basic APPLICATION logs	Application Logs

Most commonly, you'll end up using the popular Unix general-purpose logging facility know as syslog. When a given individual program needs to log certain information about an event, it will send that information to syslog. The good news is that syslog is a host-configurable, uniform system logging facility, and uses a centralized system logging process using the subsystem rsyslog.

Beyond that, the way that syslog operates is essentially straightforward. Log entries sent by programs in use are sent to the rsyslog demon, which will then consult the configuration file(s) /etc/rsyslogd.conf or in /etc/rsyslog. Therefore, when a match is found, it will write the log message to the desired log file.

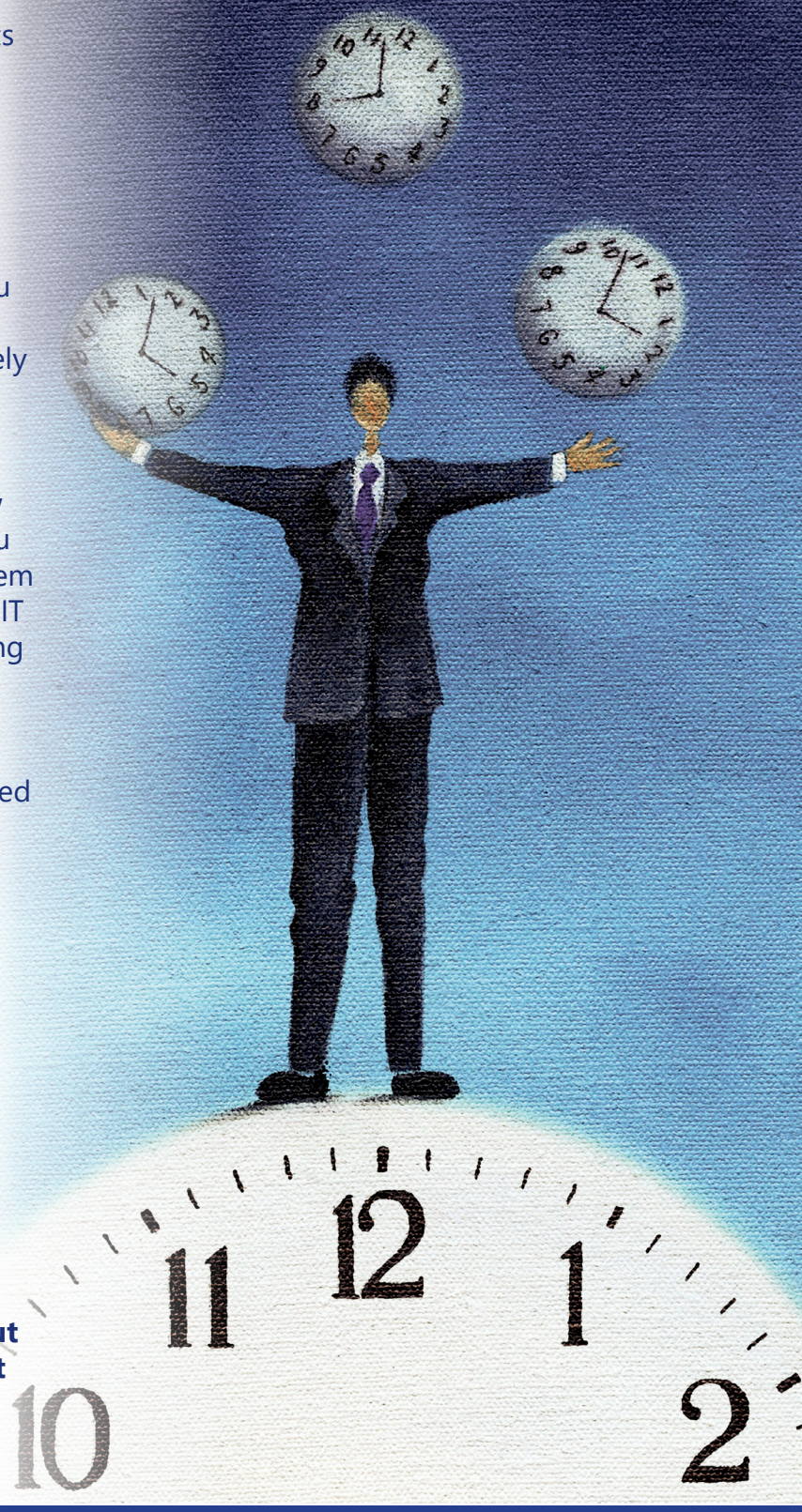
That's not all though - don't forget that you'll need to ensure that you have a set of structured text files residing in a location on disk. You will also have to implement a methodology to aggregate the text files to a central storage and analysis system. Lastly, you need to remember to make sure that the date, time and time zone on all units is correct, and synced to a central authority - it sounds small, but improper configuration can throw off the whole system.

Remember, logging is so important because it's about having the right information. If you aren't equipped with the right information, how will you understand the performance and security of the Unix systems that you and your staff members rely on for work every single day?

The good news is that you don't have to handle this on your own - the Brainlink team knows how important logging is, and we're ready to help you set up a comprehensive and simple logging system at your business. By partnering with our team of IT experts, you can ensure that every event occurring on your systems is logged, sorted and ready for review right when you need it.

Our BrainSENSE logging solution is perfectly suited to integrate with your Unix systems to deliver actionable this data in easy-to-use and read dashboards that are customizable and tailored specifically to your business.





Start harnessing real information about your network for the good of your business by reaching out to us at (347) 460-2238 or raj@brainlink.com for more information about our logging solution, BrainSENSE, and what it will do for your business.