NEURO10

Case Study - N10 for Log Management

Log data records the behaviour of systems, networks and other IT environments. It could provide valuable information about the operations of any organisation, only if it is managed and utilised well.

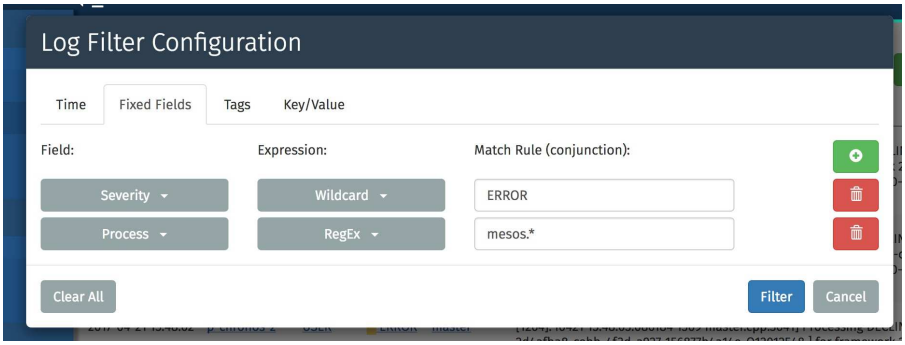
Yet, machines today are producing massive amounts of log data, often up to millions or even billions of records in just an hour. Organisations find it increasingly challenging to manage the *search*, *reporting*, and *monitoring* of their logs, hence underutilising the data to support bigger business objectives.

(1) Advanced *Search* on Logs for Easier Troubleshooting

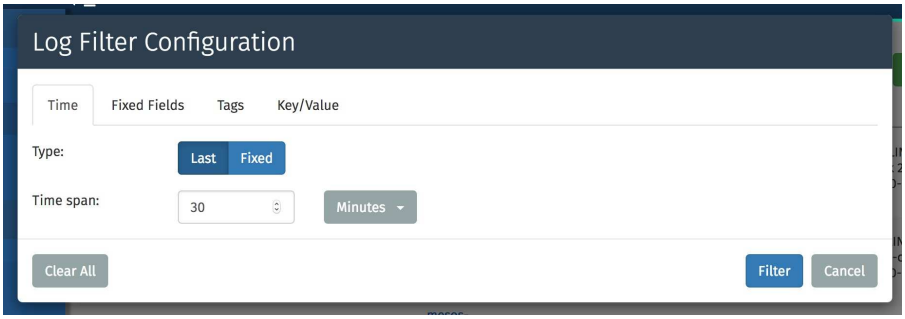
> **Scenario**: The IT team in CompanyX is responsible of maintaining the IT services of the company. One day, their *Mesos* process fails to complete its task.
>
> As *Mesos* runs across a cluster of instances, troubleshooting is tedious. To find the exact process instance that caused the error, the IT team has to enter the virtual machines hosting each instance to search for the error. And the search ability is limited to whatever tools the system offers, such as plain keyword searches with `grep` on Linux-based systems.

Solution: N10 aggregates your logs on a central platform, then indexes the data for better and faster searches. You can do advanced searches by applying filters. The following filters are supported: search by time, fixed fields, key-values or tags.

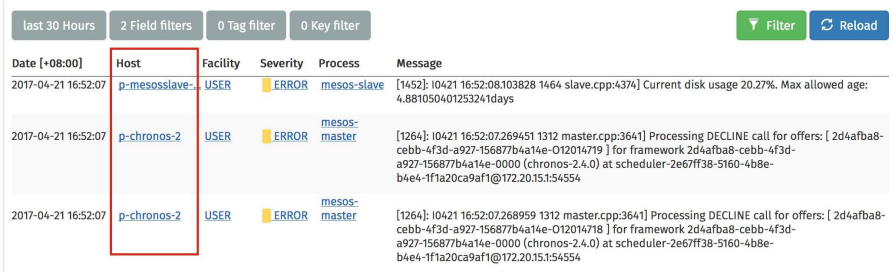
To troubleshoot our *Mesos* process failure, we narrow down our log search to view errors in *Mesos* process. We apply a fixed field filter with two rules - *Severity: ERROR* and *Process: mesos-** -



We also narrow down our search to logs generated in the last 30 minutes with a time filter -



N10 will do the search and present the results in a single table, almost immediately. From this table, we can quickly identify which virtual machine is throwing the error, thus reducing our MTTR -

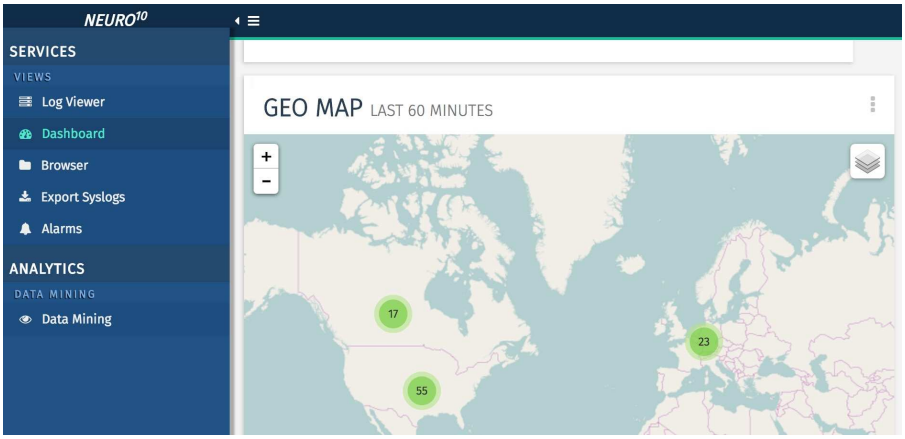


(2) Log *Reporting* in an Instant

> **Scenario**: The IT Director is due for a senior management meeting to discuss the IT strategy of CompanyX. Director needs to understand what the IT needs of the company are, both from a micro- and macro-level.
>
> Log data is machine-generated data that is too raw and unstructured for business users to manipulate and understand easily . Much post-processing of the data is needed to import the relevant information into business user-friendly applications such as Microsoft Excel, which can then be used to generate charts for visualisation of trends.

Solution: N10 does all the work for you so that you can focus on telling the story. Your log data will be processed and visualised in ways that help you gain a comprehensive understanding of your system health across your whole IT infrastructure.

To understand the level of activity of your machines across different regions, view where your logs are coming from on a geographical level -



To understand the level of activity of your processes, view where your logs are coming from on a process level -