XpoLog Search

Overview

Data is constantly entering your system's IT infrastructure from various sources. This data is of all types – performance data and statistics, traps and alerts, log files, configurations, scripts and messages, and arrives from various sources – your logs, folders, applications, network devices, database tables, and servers.

XpoLog indexes in real time all data entering your system's IT infrastructure from various sources, and structures and normalizes this data – both raw and rich, into a single database of a structured format.

XpoLog provides a search engine – XpoSearch, which enables you to conduct a search through this immense amount of data for anything that you like. Using the XpoSearch interface, you can search all the logs in XpoLog Center (applications, servers, network devices, database tables, and more).

Search Types

XpoSearch provides two main types of searches:

- **Simple search** – initial search, using simple search syntax, which results in a list of matching events
- **Complex search** – an advanced search, using complex search syntax, which results in a summary table of matching events, or transactions

Search Stages

A search can be run in three stages:

- **Initial search**
- **Refined search**
- **Complex search**

Initial Search

In the initial search, the user enters a search query of simple criteria, and the search runs on all the event data. In this simple search, the user can search the event data for a simple term or more than one term, run a Boolean search, a search with wildcards, or a column-based search.

Running the search query returns a list of all matching events from all relevant logs (latest on top). In addition, XpoSearch returns a graphical view of the distribution of the matching events over time and per data source.

Refined Search

The resulting events of a simple search can be minimized by refining the search results using either or both of the following methods:

- **Filtered Search** – filtering the resulting events according to the source of the event – logs, files, applications, or servers
- **Analytics-based Search** – adding one of the event data fields discovered during the simple search to the search criteria of the simple search

Complex Search

Complex search queries are used to perform advanced complex operations and reporting on the log events resulting from a simple search. Running a complex search query results in a summary table, and can also be visualized as gadgets in XpoLog Dashboards.