

op5 LogServer

Log Management made easy



- *Centralized Log Archive enables you to collect and store all your logs into a single centralized log database.*
- *Log Data Integrity, user and group access management to assure integrity.*
- *Log Compression minimizes the storage size required for your log.*
- *Log Rotation enables you to set-up a policy rotating to long term archiving on external media (SAN, Disk etc).*
- *Supported Log Agents. op5 LogServer supports all syslog compatible agents sending (udp/tcp). Agents is also available for Windows and flat text files.*

With op5 LogServer you have the opportunity to manage all the enterprise log messages from a central log server. This gives you excellent overview, effective fault management and enables traceability for compliance with standards such as SOX, PCI, BITS etc.

EASY-TO-USE WEB INTERFACE

All systems can generate some kind of event log. If something happens or goes wrong, the system generates a log. Systems can log in different levels, everything from information logs or debug messages to critical messages.

Through its easy-to-use web interface, complex and distributed log data is instantly available. This greatly saves time and resources for troubleshooting or for creating various traceability reports.

MILLIONS OF LOGS

Log management is a burden for any system administrator who wants to keep up the good work. Servers, systems or fire walls can generate more than one million events every day.

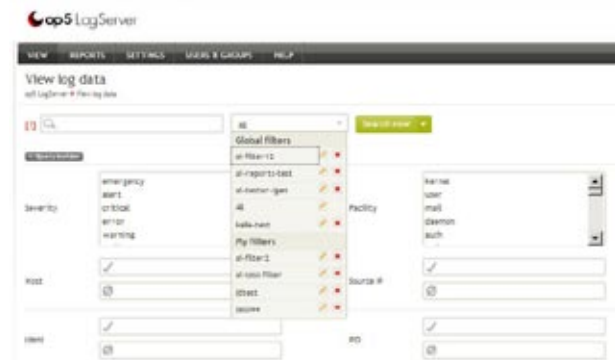
In a medium-sized organization there can be 15-20 millions events per day! It is not unusual to dedicate one day per week to do proper follow-up or analysis of multiple events. This is almost eliminated when using op5 LogServer.

OP5 SMART SEARCH WITH QUERY BUILDER

A challenge when searching logs are to define smart queries. To assist in this task we now introduce a Query Builder as a complement to the Query Language. This makes the search task easy and understandable for anyone.

Logs contain highly detailed data from all layers, but as long as they are hard to find or hard to filter they do no good. Query Builder is an essential part of making log data easy to find and access, and as such a powerful help to find information for problem analysis, SLA breach follow up and security audit.

By collecting and storing all logs in a central structured database important you will achieve:



- Improved security as in case of an attack or a system failure the most accurate source of information will be your logs. With op5 LogServer the logs are stored centrally and can be backed up as any important data.
- Log availability as most infrastructure equipment store logs in RAM memory. In case of a problem of a device a power off is the only way to reboot the device. This will erase any locally stored logs i.e. all logs that could help in problem analysis are now gone.

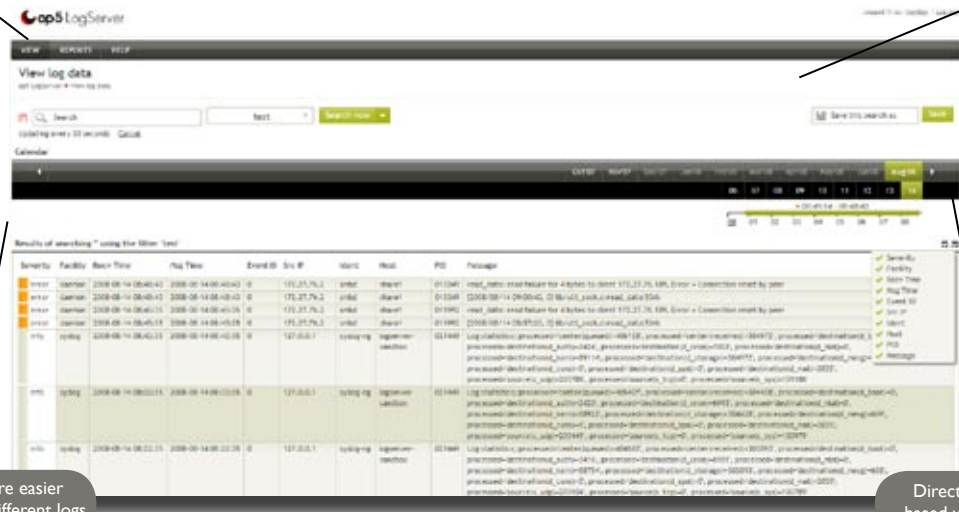
To search each server one by one for unexpected logs is not a sufficient method. The problems with different clocks and just coordinating the log info comparing results between different devices is extremely time-consuming and therefore very inefficient.

Smart free text queries that can be saved as active filters

Simple calendar look up for direct log access

Clear color fore easier identification of different logs

Direct on screen Ajax based view configuration



SUPPORT FOR UDP & TCP LOG TRAFFIC

UDP is the standard way of sending log data. However it lack an important feature with the acknowledgment of send & received. This is why op5 LogServer also supports TCP based log traffic that enables a confirmation on that the logs are sent and received in full.

USER & GROUP MANAGEMENT

Collecting all logs in to a central archive for search and filters is a core and basic function. However it does introduce security and integrity challenges. With op5 LogServer version 3.2 we introduce an easy to administer secure access control to what people can see and do when they access the central Log Database. This enables IT and security staff to distribute access to the log data based on what clearance or function the individual or a group has without the risk of enabling Log access on sensitive data.

SMART FILTERING AND PRO-ACTIVE SCHEDULED REPORTS

The system also supports client and central based filtering which greatly reduces the amount of logs created and stored in the system. This can be automatically processed and formed into weekly or monthly reports that are distributed directly via E-mail to relevant staff.

There is also a possibility to define criteria for sending alarms to op5 Monitor. That way you can define events in the logs that you want an alarm on.

SECURITY, TRACEABILITY AND SCALABILITY

The need for traceability is growing rapidly. It is corporate management's responsibility to ensure that the network and its services are utilized in a legal and professional manner.

This means that it is an absolute necessity to be able to back track any activity on the network and its services. op5 Log Server enables this and stores the information in a secure and structured place for backup and long term storage.

OP5 LOGSERVER CAN MANAGE LOGS FROM:

- Syslog
- Windows
- Windows Event log
- Windows Application logs (IIS, backup software and so on)
- UNIX/Linux
- Firewall
- Network devices, switches/routers (all hardware that can create sys logs)

OP5 LOGSERVER MONITORS AND REPORTS ON

- Application Events
- File Replication Events
- Security Events
- DNS Server Events
- Directory Events
- Any standard log file

BUILT ON SYSLOG-NG

op5 LogServer utilises the market leading syslog-ng as the back end log handler. This enables op5 LogServer to fully support all features in syslog-ng such as smart buffering, Encrypted message transfer (TLS support) etc.

ABOUT OP5

Our business concept is to offer the market the most cost-effective solution for IT support organizations. We utilize the power and effectivity of Open Source as the prime component in our product development.