

op5 Log Server and a web browser is all you need to be log efficient!



- Are you concerned about attacks on your IT systems?
- Do you spend weekly time on following up logs?
- Do you have a system that assures traceability for internal follow up?
- Does the system handle all logs, from Windows, Unix, Applications and infrastructure?

op5 LOG SERVER

With op5 Log Server you have the opportunity to manage all the enterprise log messages from a central log server, which gives you a good overview. It is easy to use since it is a web based user interface and it saves time and efforts.

Many 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.

Log management is a burden for any system administrator who wants to keep up the good work. Servers, systems or firewalls can generate over 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 on multiple events.

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.

Facility	Severity	Time	Event ID	Ident	Host	Message
local7	err	2006-02-11 11:50:08	2	nt-server1.ncclient	172.27.76.6	2 NSClient CollectData: Call to retrieve counter value for 'Processor_total'/% Processor Time Failed, returning status code 2147483648.
local7	info	2006-02-21 04:44:28	1704	nt-server1.socdi	172.27.76.6	1704

IN CASE OF ATTACK

In case of an attack or a system failure the most accurate source of information will be your logs. Common procedure is to check the logs locally on each affected server or network device. Some devices often saves the logs in RAM which means that they are lost on reboot!

CUSTOMIZE VIEWS

In OP5 Log Server the logs are saved in an event catalogue database and are presented via an easy to use web based interface with color coded log messages. It is easy to handle and it is searchable.

Events can be archived or cleared from the event log as per your business need. You can choose between defined search or you can make the definition yourself. A search is made by description, port, source, event id, time, etc. This enables the system administrator to identify the root problem and what other problems it may have caused.

THE WEB INTERFACE

In the web interface the system administrator can view the log messages and define simple or advanced filters to look into different kinds of messages. All you need, to access all of your log messages is a web browser, you don't need to log on to a separate server.

LOG EFFICIENT

In op5 Log Server there is an option to customize views using multiple windows and rule based filtering. The op5 Log Server monitors and reports your mission critical servers or workstations on events like application, security, dns server, file replication, directory events and any standard log file.

There is also a possibility to define criterias for sending alarms to op5 Monitor. In that way you can define events in the network that you want an alarm on. You can be the efficient analyst your organization requires you to be.

SYSLOG

Syslog is a standard protocol for centralized reporting of system events. Most modern devices use the syslog protocol for reports of debug messages, operating parameters and important events.

Facility	Severity	Time	Event ID	Host	PID	Message
auth	crit	2006-02-21 12:04:20	sshd	rc.op5.se	11319	fatal: Read from socket failed: Connection reset by peer
auth	crit	2006-02-21 11:54:20	sshd	rc.op5.se	10806	fatal: Read from socket failed: Connection reset by peer
daemon	err	2006-02-21 12:03:55	dhcpd	devel.op5.se		from the dynamic address pool for 192.168.1.0/24
daemon	err	2006-02-21 12:03:53	dhcpd	devel.op5.se		Remove host declaration jd or remove 192.168.1.21
daemon	err	2006-02-21 12:03:53	dhcpd	devel.op5.se		Dynamic and static leases present for 192.168.1.21.
daemon	err	2006-02-21 11:59:34	dhcpd	devel.op5.se		if IN A ops-vse131p62.op5.se rrsset doesn't exist add 3600 IN A ops-vse131p62.op5.se 192.168.1.21: connection refused.
daemon	err	2006-02-21 11:59:34	dhcpd	devel.op5.se		from the dynamic address pool for 192.168.1.0/24
daemon	err	2006-02-21 11:58:34	dhcpd	devel.op5.se		Remove host declaration anders or remove 192.168.1.25
daemon	err	2006-02-21 11:58:34	dhcpd	devel.op5.se		Dynamic and static leases present for 192.168.1.25.
mail	warn	2006-02-21 12:00:01	postfix/local	web1.op5.se	3177	warning: biff_notify: Operation not permitted
mail	warn	2006-02-21 11:03:43	postfix/smtpd	linux-server1.op5.se	16053	warning: 216.183.53.159: hostname ppp-53-159.grandriver.com verification failed: Host not found
mail	warn	2006-02-21 11:53:27	postfix/smtpd	linux-server1.op5.se	16048	warning: 201.255.11.56: hostname 201-255-11-56.mrse.com.ar verification failed: Host not found
daemon	notice	2006-02-21 11:59:11	proftpd	linux-server1.op5.se	18184	linux-server1.op5.se (195.24.166.254[195.24.166.254]) - FTP no transfer timeout, disconnected.
daemon	info	2006-02-21 12:04:53	inetd	shares.op5.se	12962	START: Rp pid=1595 from=193.201.96.3
daemon	info	2006-02-21 12:04:17	proftpd	linux-server1.op5.se	19249	linux-server1.op5.se (monitor.op5.se[193.201.96.3]) - FTP session closed.
daemon	info	2006-02-21 12:04:17	proftpd	linux-server1.op5.se	19249	linux-server1.op5.se (monitor.op5.se[193.201.96.3]) - FTP session opened.
daemon	info	2006-02-21 12:04:00	inetd	backup.op5.se	8031	EXIT: Rp pid=4392 duration=0(sec)
daemon	info	2006-02-21 12:04:00	inetd	backup.op5.se	8031	START: Rp pid=4392 from=193.201.96.134

SECURITY AND LOG ROTATION

The need for traceability is growing rapidly. It is the corporate management responsibility that the network and its service are utilized in a legal and professional manner. This means that it is an absolute necessity to be able to backtrack 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.

The op5 Log Server has a three step fully configurable log rotation scheme.

Level one

- All logs go in to a performance optimized SQL database.
- Automatic rotation is set on either time or hard disk space, so when the level is reached, logs are automatically forwarded to level two.

Level two

- Still placed on the local disks of the OP5 Log Server but with higher grades of compression.
- Automatic rotation is set on either time or hard disk space so when the level is reached, logs are automatically forwarded to level three.

Level three

- Logs are now placed on a secondary source of your choice. Could be a SAN or any external disk /space.

Note: all logs are always reachable and searchable from the Web GUI. The difference between the levels is the performance and the time it takes to show the specific logs. The higher the level the longer the time.

OP5 LOG SERVER CAN MANAGE LOGS FROM:

- Windows
- Windows Eventlog
- Windows Application logs (IIS, backup software and so on)
- Unix/Linux
- Firewall
- Network devices
- Switches/Routers (all hardware that can create syslog)

OP5 LOG SERVER MONITORS AND REPORTS ON:

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

op5 Log Server is sold in a simple license model starting at 50 node license. For pricing and other questions please do contact us via info@op5.se.