High Volume and Real Time

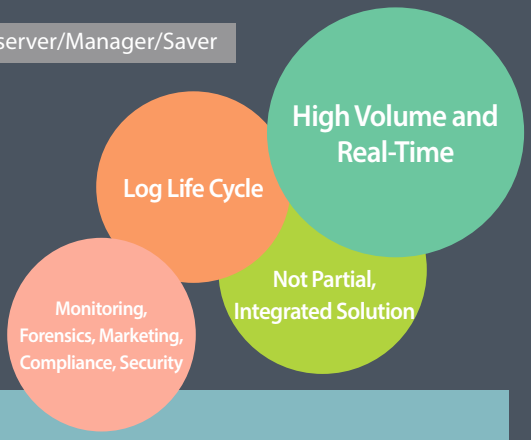
Log Analysis and Management System for Full Log Life Cycle

LogCops

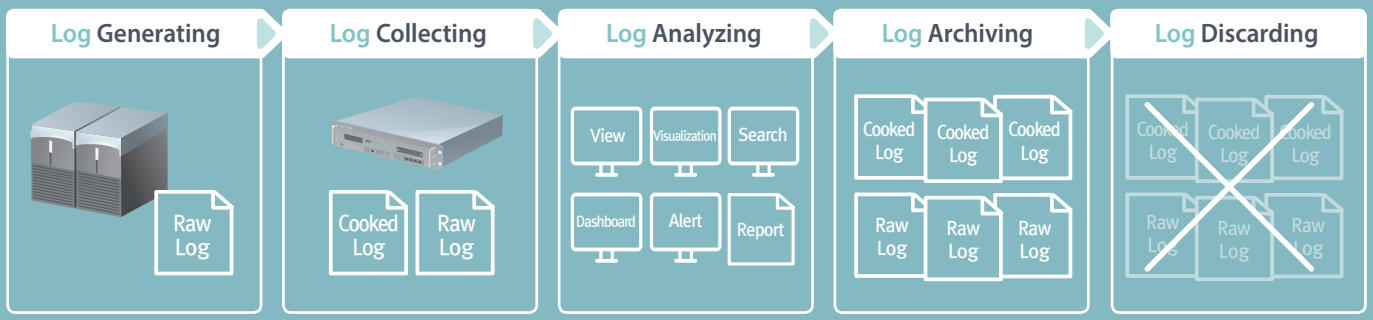
Collector/Agserver/Manager/Saver

Full log life cycle from creating, collecting, analyzing, archiving to discarding should be manageable and real-time log view, search and analysis should be available. However, Web, Firewall/VPN, IDS/IPS and Application logs which stacks multi-terabytes a day are impossible with current software based system.

LogCops system is the log analysis and management system for high volume and real-time log collection, view, search, analysis, archive and discard.



Log Life Cycle



LogCops System Characteristics

- Real-time processing of all VIEW, SEARCH, REPORT, VISUALIZATION, DASHBOARD and ALERT
- Various log collecting methods including AGENT, SYSLOG, SNMP, FTP type and extracting from DBMS
- High performance of log collection : 10,000/20,000/50,000 messages per second
- High performance of log search : response instantly or within minutes from multi-terabytes
- Advanced settings for VIEW, SEARCH, REPORT, VISUALIZATION, DASHBOARD and ALERT
- Various and powerful JOIN function including INNER, LEFT, RIGHT and CROSS
- Various and powerful filtering with regular expression (including POSIX standard) for log fields
- Default compressed archiving of raw logs by ratio 12:1 and optional encrypted archiving
- User based strict authentication and authorization by user, device, log, GUI function
- Export data analyzed or reported to HTML, MS Word / Excel, PDF or Text file
- Various combined selection of summing or individual processing from same, different, single or multi log
- Optional and systemized log archiving for retention period, repository and number of copy (primary and secondary)
- Various reports using user-defined settings
- User-defined scenario-based search system
- Combined selection and filtering of same or different log
- Various virtual fields for IP or specific log fields
- Optional archiving at WORM storage
- Search within the search result infinitely
- Intuitive and easy web service GUI
- Centralized log management
- Various and powerful alert functions
- Various dashboard configurations by user-defined settings
- Extended pivot search using the multiple unique fields for log fields
- Extended group-by search using the multiple unique fields for log fields

LogCops Screen Shots

- Various system configuration screen of real-time view, real-time search, real-time analysis etc and easy, intuitive, user-friendly web service GUI supports

LogCops Introduction to LogCops System

High Volume and Real-Time Log Analysis and Management System for Full Log Life Cycle

01 **Integrated System Supporting Full Log Life Cycle**

Integrated total system not partly solution which support partial log life cycle but integrated total system which manage full log life cycle.

02 **High Volume Real-Time Log Processor**

Collecting various servers, networks or security equipments' various log in real-time and analyzing real-time generated logs.

03 **Variously applied Multi-Purpose Solution**

Multi-purpose solution for system healthy monitoring, forensics, regulatory compliance, marketing and information security.

LogCops System Effectiveness

- Saving log data securely and in real-time
- Centralized log management system with efficient disk management
- Responsibility tracking for security accident
- Stored logs as legal evidences
- Security policy establishment based on log term scope log analysis
- Extended and reinforced log policy support

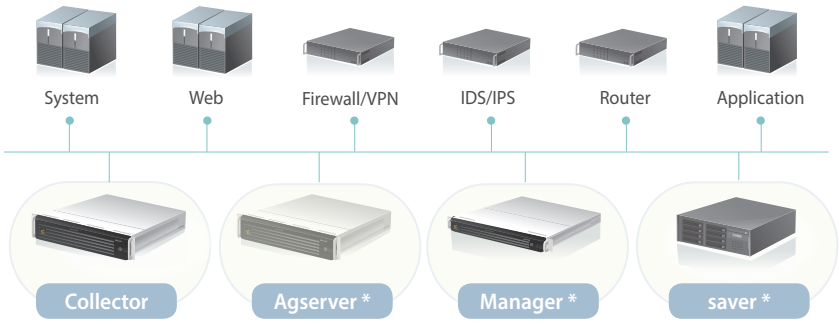
Regulations and Compliance

U.S.A

- FISMA Federal Information Security Management Act of 2002
- GLBA Gramm-Leach-Bliley Act
- HIPPA Health Insurance Portability and Accountability Act of 1996
- SOX Sarbanes-Oxley Act of 2002
- PCI DSS Payment Card Data Security Standard

LogCops System Configuration

Product	Environment	Misc.
Collector	Back-end collector with memory queue, linux, HW appliance	Collector Agserver Manager
Agserver	Front-end collector, linux, HW appliance	Option
Manager	Manager with web server, linux, HW appliance	Option
Saver	NAS/SAN/Shared file system, linux, HW appliance	Option



LogCops Recommended Specification

Model	LCA-7010	LCA-7020	LCA-7050	LCA-AGS	LCA-MGR
Appearance	Collector	Collector	Collector	Agserver	Manager
CPU	Intel Xeon 4-Core 2.5 GHz	Intel Xeon 4-Core 2.5 GHz x 2	Intel Xeon 6-Core 2.6 GHz x 2	Intel Xeon 4-Core 2.5 GHz	Intel Xeon 4-Core 2.5 GHz
Memory	16GB	32GB	64GB	16GB	8GB
Disk	4 TB (1 TB x 4)	8 TB (2 TB x 4)	16 TB (2 TB x 8)	4 TB (1 TB x 4)	2 TB (1 TB x 2)
Power	650W x 2 High efficiency Redundant Power Supply	650W x 2 High efficiency Redundant Power Supply	720W x 2 High efficiency Redundant Power Supply	650W x 2 High efficiency Redundant Power Supply	600W AC Power Supply
Chassis	1U	1U	2U	1U	1U
Ethernet	Dual-port Gigabit Ethernet	Dual-port Gigabit Ethernet	Dual-port Gigabit Ethernet	Dual-port Gigabit Ethernet	Dual-port Gigabit Ethernet

Above specification can be changed without any notification.

NileSOFT
Kolon Digital Tower Billant 10th Fl. #1004, 30, Digital-ro 32-gil, Guro-gu, Seoul, 08390, South Korea
TEL. +82-2-783-0961 FAX. +82-2-783-0963 e-mail. nileman@nilesoft.co.kr
www.nilesoft.co.kr/eng