로그생명주기 전 과정을 지원하는

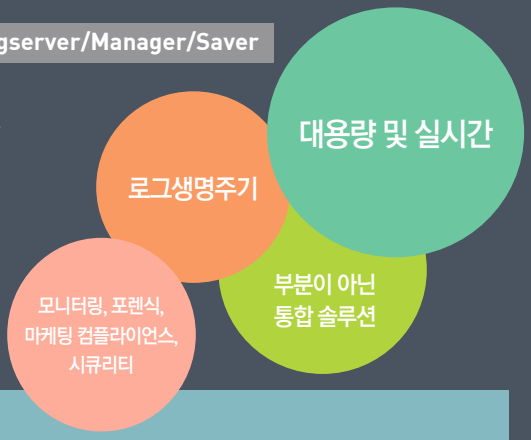
대용량 실시간 로그분석시스템

LogCops

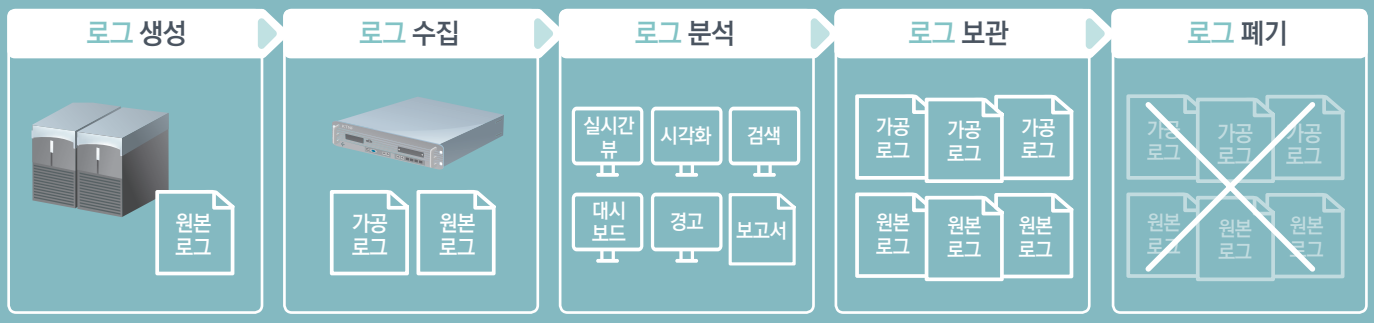
Collector/Agserver/Manager/Saver

로그생명주기인 로그 생성, 수집, 분석, 보관 및 폐기에 이르는 전 과정을 관리하고, 실시간으로 로그를 수집하며, 실시간으로 로그를 감시 및 검색하며, 각종 로그분석을 실시간으로 처리할 수 있어야 합니다. 그러나 장비 별로 하루에 수 GB에서 수십 GB를 생성하는 웹, 방화벽/VPN, IDS/IPS 혹은 특정 응용프로그램 로그 등은 로그 량이 방대하여 기존의 소프트웨어 기반의 로그분석시스템으로는 원천적으로 실시간 처리가 불가능합니다.

LogCops 시스템은 대용량으로 발생하는 로그를 실시간으로 수집, 검색, 분석, 보관 및 폐기 하기 위한 하드웨어 기반 로그분석 전용시스템입니다.



로그 생명 주기



LogCops 상세 특징

- 실시간으로 모든 뷰, 검색, 보고서, 시각화, 대시보드, 경고를 처리
- AGENT, SYSLOG, SNMP, FTP, DB추출 등 다양한 수집방식 지원
- 10,000/20,000/50,000 mps: 최고의 로그수집 성능
- 수집TB 로그를 대상으로 즉시 혹은 수초 이내 검색하는 최고의 검색 성능
- 사용자 시나리오 기반 검색 시스템 지원
- 강력하고 다양한 JOIN (INNER, LEFT, RIGHT, CROSS, 등) 기능 제공
- 강력하고 다양한 정규식(POSIX 표준 포함) 검색 기능 지원
- 검색한 결과에서 재 검색하는 무제한 결과 내 검색 기능
- 다수개의 유일(Unique)필드를 이용한 Group By 검색 기능
- 다수개의 유일(Unique)필드를 이용한 Pivot 검색 기능
- 동종 혹은 이종 로그간의 연관 검색 기능
- IP 및 LOGID에 대해 다양한 가상필드 확장 기능
- 사용자기반 설정을 이용하여 다양한 분석 보고서 생성
- 뷰, 검색, 보고서, 시각화, 대시보드, 경고에 대한 다양한 설정이 가능한 고급선택 기능
- EXCEL, WORD, HTML, TEXT 등 다양한 파일형태로 보고서 생성 및 이출(Export) 가능
- 동종 및 이종로그, 단일 및 다중로그를 합산 혹은 분리 처리할 수 있는 기능
- 로그의 보관기한, 장소 및 복제(1차 및 2차)의 선택적 및 체계적 설정 기능
- WORM장비에 선택적 보관
- 원본로그를 압축율 12:1로 압축화(기본) 보관 및 암호화(선택) 보관
- 간편하고 직관적인 웹 서비스 GUI
- 중앙 집중식 로그관리
- 사용자별, 장비별, 로그별, 기능별 엄격한 권한분리
- 사용자 정의기반의 다양한 대시보드 구성 기능
- 다양하고 강력한 경고처리 기능

LogCops 실행화면

- 실시간 뷰, 실시간 검색, 실시간 분석 등 다양한 시스템 구성화면 및 사용자 중심의 간편하고 직관적인 웹서비스 GUI 지원

LogCops 시스템 소개 대용량 실시간 로그분석 및 관리 시스템

01 대용량 실시간 처리 로그 어플라이언스
(Log Appliance : High Volume Real-Time Log Processor)

각종 서버, 네트워크 혹은 정보보호 장비에서 대용량으로 발생하는 로그를 실시간 (Real-Time) 으로 수집하고, 수집된 로그를 실시간 (Real-Time) 으로 검색 및 분석할 수 있는 어플라이언스 (Appliance) 입니다.

02 로그생명주기를 지원하는 통합 시스템
(Integrated System Supporting Full Log Life Cycle)

로그가 생성된 후 수집, 가공, 검색, 분석, 보관 및 폐기에 이르는 로그생명주기(Log life Cycle)의 일부분을 지원하는 부분 솔루션 (Partical-Solution)이 아니라 전과정을 자동화하여 관리 할 수 있는 통합 시스템 (Intergrated Systerm) 입니다.

03 사용자 행위 감사로그 기록 및 재생
(User Behavior Audit Log Management System)

서버 자산에 접근한 모든 사용자 행위를 녹화(Recording) 및 재연 (Replay) 기능을 제공하며 별도의 관련 솔루션 도입을 대체 할 수 있습니다.

04 다양한 활용방안을 제공하는 다목적 솔루션
(Variously applied Multi-Purpose Solution)

실시간 시스템 감사 모니터링, 포렌식(Forensics), 로그관련 각종 법규 및 지침준수, 마케팅 및 정보보호 등 다양한 활용 방안에 부합할 수 있는 다목적 솔루션 (Multi-Purpose Solution) 입니다.

LogCops 시스템 효율성

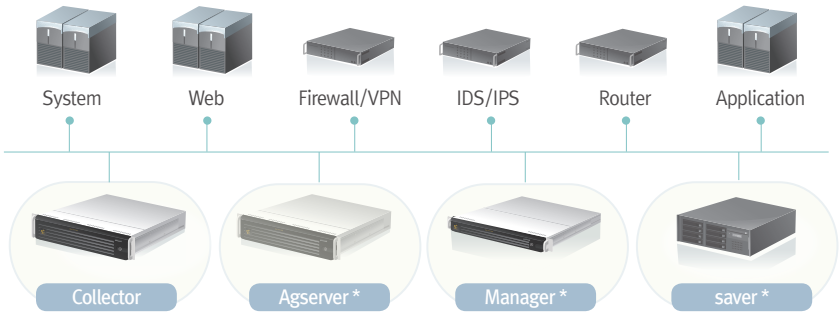
- 로그데이터를 실시간으로 안전하게 저장
- 중앙 집중화 된 로그관리로 효율적인 디스크 관리
- 보안사고 발생시 책임추적 가능
- 저장된 로그파일의 법정 증거자료로 활용가능
- 장기적인 로그분석으로 강력한 보안대응체제 구축
- 강화된 로그관련 법규 준수

로그관련 국내 법규, 지침, 규정 및 인증

미국	FISMA	Federal Information Security Management Act of 2002
	GLBA	Gramm-Leach-Bliley Act
	HIPPA	Health Insurance Portability and Accounta bility Act of 1996
	SOX	Sarbanes-Oxley Act of 2002
	PCI DSS	Payment Card Data Security Standard
한국	정보통신 기반 보호법 13조 1항(침해사고의 통지)	
	정보통신 서비스 정보보호지침 제 3조 5항 (복구 대책)	
	주요정보통신 기반시설 보호지침 제 4조(침해사고 예방조치)	
	전자 금융 대책 안 로그백업 및 보관기간	

LogCops 시스템 구성

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 시스템 규격 및 성능

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
Etherent	Dual-port Gigabit Ethernet	Dual-port Gigabit Ethernet	Dual-port Gigabit Ethernet	Dual-port Gigabit Ethernet	Dual-port Gigabit Ethernet

*상기 규격은 확정된 사항이 아니므로 예고 없이 변경될 가능성이 있습니다.

NileSOFT
서울시 구로구 구로동 디지털로 32길 30, 코오롱디지털타워 빌란트1차 1004호
TEL. 02-783-0961 FAX. 02-783-0963 e-mail. nileman@nilesoft.co.kr
www.nilesoft.co.kr
정보보호의 대중화! 나일소프트가 함께 하겠습니다