

Log saver[®]

내부통제 및 감사를 위한
통합로그관리시스템



dsntech
digital solution & technology partner

Digital Solution & Technology Partner

주요 솔루션 요약

고객사의 중요 자산 및 정보를 안전하게 보호하여 본연의 비즈니스에 전념할 수 있도록 "통합로그관리시스템 및 내부정보유출 감사솔루션" 을 제공하는 IT 컴플라이언스 전문업체로서 고객과 더불어 Compliance & Security Community를 추구합니다.



『서버관련 솔루션』



『PC관련 솔루션』

Log saver[®]

통합로그관리

ScriptSafer

Shell Script 해킹 실시간탐지

BLAS

빅데이터 검색/분석

Log saver WORM

위·변조 방지 무결성 스토리지

AUDITSAVER

사용자행위 증거 감사

B2SAUER

PC 블랙박스 / 파일유출 감시

Themis
Universal Authentication

생체 인증 통합 플랫폼

AccountSafer

회계 자금횡령 탐지 및 방지

OFFICESAFER

PC 개인정보보호 유출 통제

RansomSafer

PC 랜섬웨어 방지

위·변조방지 WORM 기술

원본로그는 압축,암호화 되어 보관되며, 무결성 보장을 위한 해시 알고리즘을 적용 합니다. 또한, WORM에 보관중인 원본로그에 대한 위·변조 시도 시 관리자에게 이벤트가 발생 합니다.

주요기능 (위·변조방지 WORM 기술)

WORM 매체

※ WORM : Write Once Read Many



관리 정책

관리 정책
• NFS/CIFS 표준 NAS Interface 지원
• 공인 HASH 알고리즘을 이용한 무결성 검증
• Hidden / Protect / Read-only Folder 설정
• 저장 Data 수정 및 삭제 불가
• Admin 권한으로부터 접근 차단
• 위·변조 방지, 진본성 보장
• KERNEL MODE에서 제어

위·변조 시도 시 관련 로그 생성



분산병렬처리

다수의 금융권의 대용량 기반의 로그처리시스템을 구축 운용하고 있으며, 분산병렬처리 시스템 구성으로 향후 대상장비(서버 및 보안장비, 네트워크장비)의 확장 및 로그용량 증가시에도 손쉬운 확장을 제공합니다.

주요기능 (대용량 기반 분산 병렬 처리 구조)

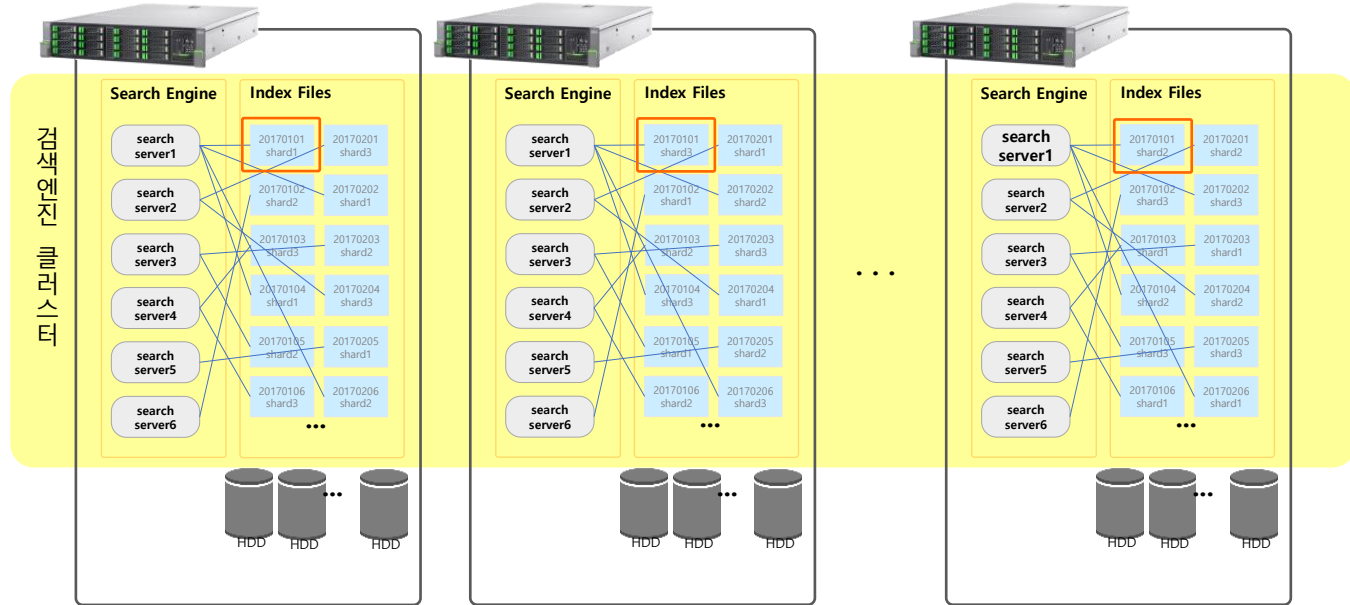
클러스터링 구성

1. 클러스터 구성

- 분석서버 자체의 색인파일 관리 알고리즘
 - 일자별 색인 컬렉션 구조 채용
 - 샤드관리
 - 오래된 색인파일 삭제 절차
 - 검색옵션으로 색인파일 내용 삭제 절차 등
- 실시간 데이터 및 과거데이터 색인
 - 실시간 기반 색인과 과거데이터 배치기반 색인 병행 가능
 - 서버의 부하 정도에 따라 처리 필요

최초 용량산정후 서버 구축.

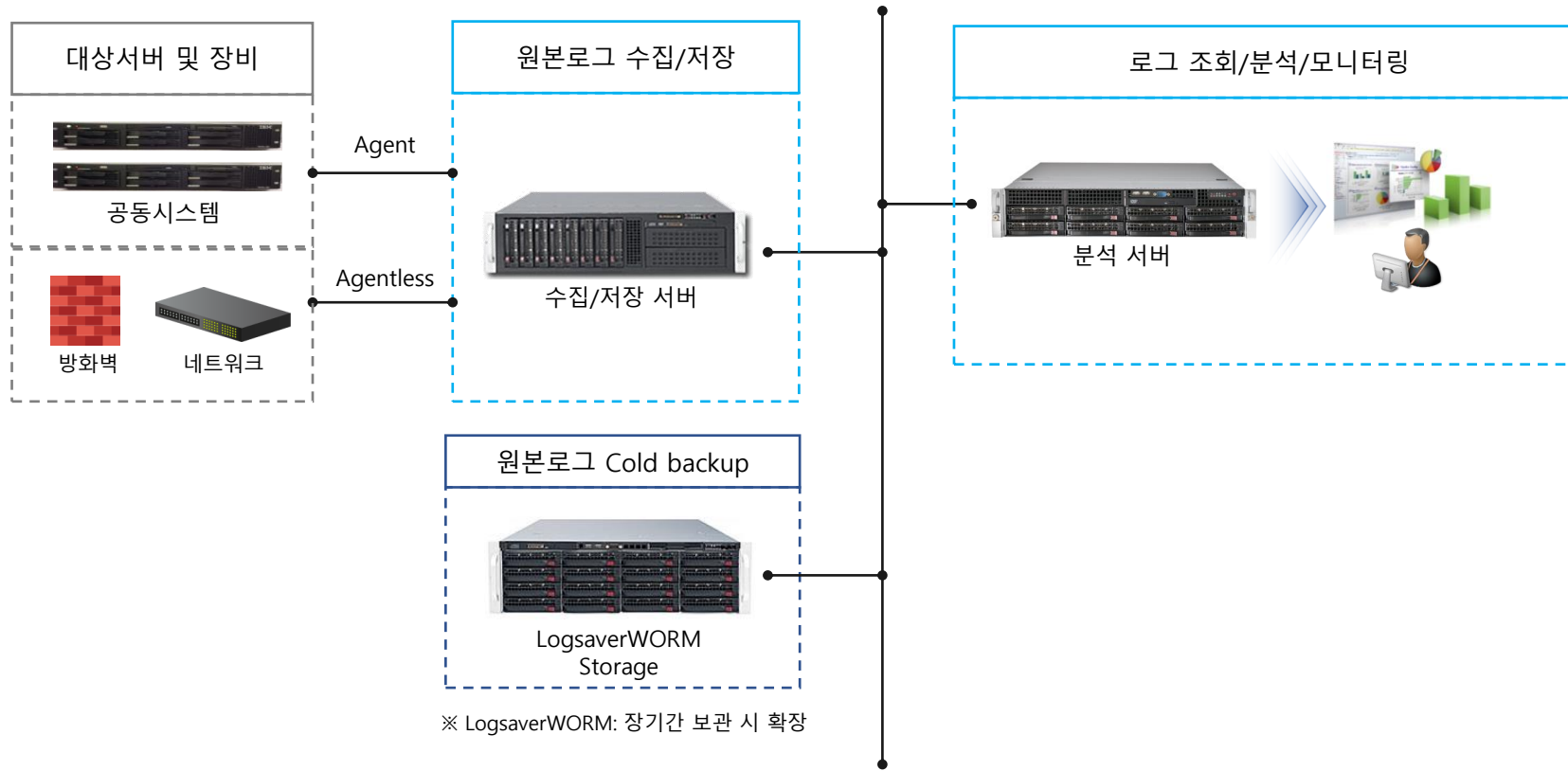
데이터 증가에 따른 서버증설.



로그세이버 구성 개요

통합로그 수집, 저장, 분석, 모니터링을 지원하며, 원본로그 장기 소산백업 보관 시 위·변조 방지 저장을 위한 WORM Storage로 확장 가능합니다.

표준목표 구성도






로그 수집 기술

제안 제품은 설치대상 서버의 다양한 OS를 지원하며 관리서버와 Agent간, 관리서버와 관리콘솔간 네트워크 전송 시에는 암호화 통신을 지원하며 로그수집 시 Agent의 성능은 대상 서버의 CPU 3% 미만의 자원을 활용하여 실시간 또는 비 실시간 로그수집을 지원합니다

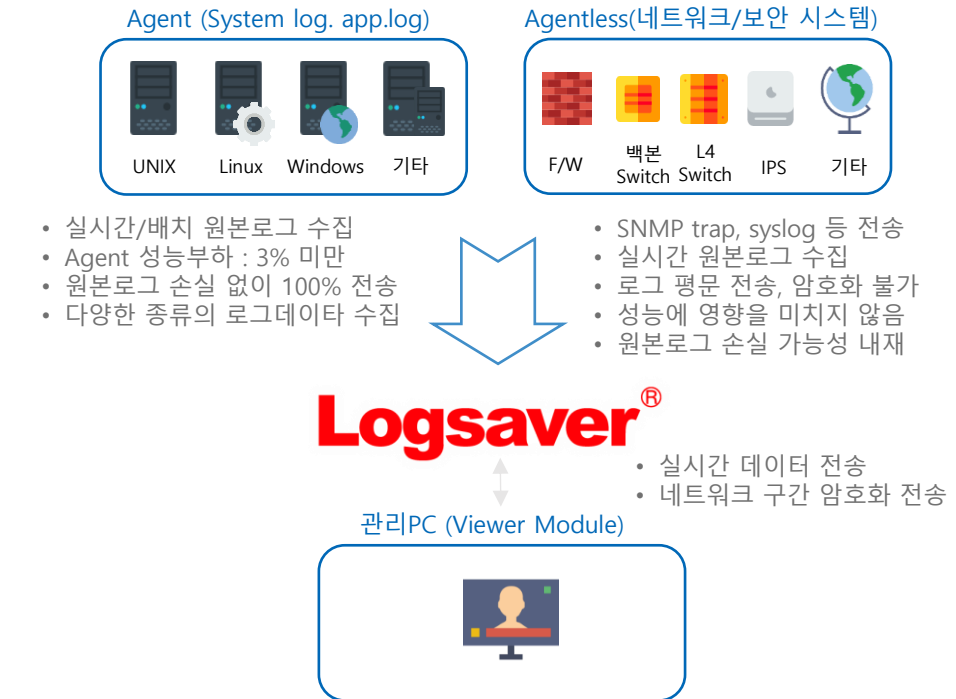
로그수집기술(1/2)

서버 수집 대상 지원 OS

	IBM AIX	5.3 / 6.0 / 6.1 ~ 7.3
	HP-UX	11.23 / 11.31 ~
	Solaris	10 / 11 / Sparc x86
	Linux	2.2 / 2.4 / 2.6 / 3.x~6.x
	FreeBSD	
	Suselinux	10
	Windows (32bit/64bit)	NT4.0 / 2000 / XP / 2003 / 2008 / 2012 / 2016 / 2019 / 2022

* 지속적 버전 업데이트 진행 중

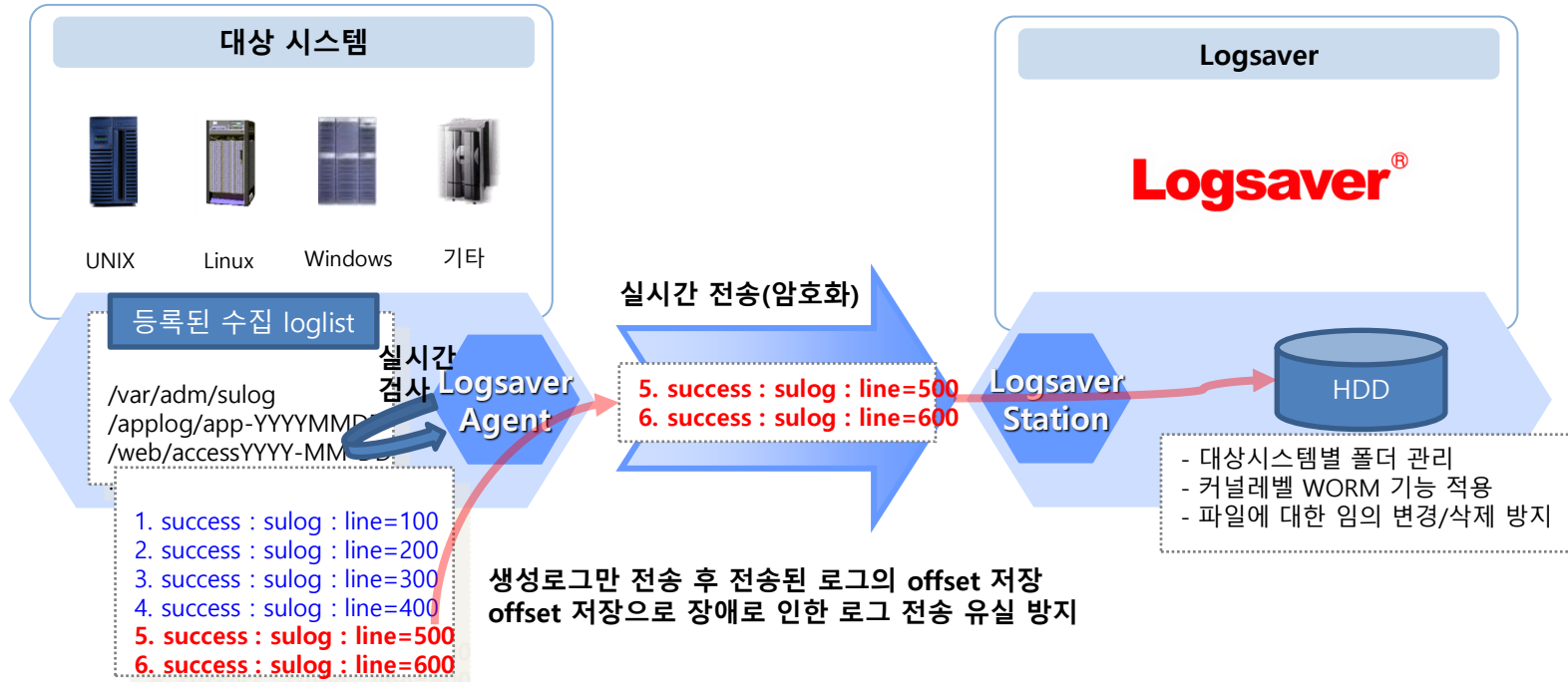
원본 로그 수집 - 실시간/비실시간. 암호화. 성능보장



로그 수집 기술

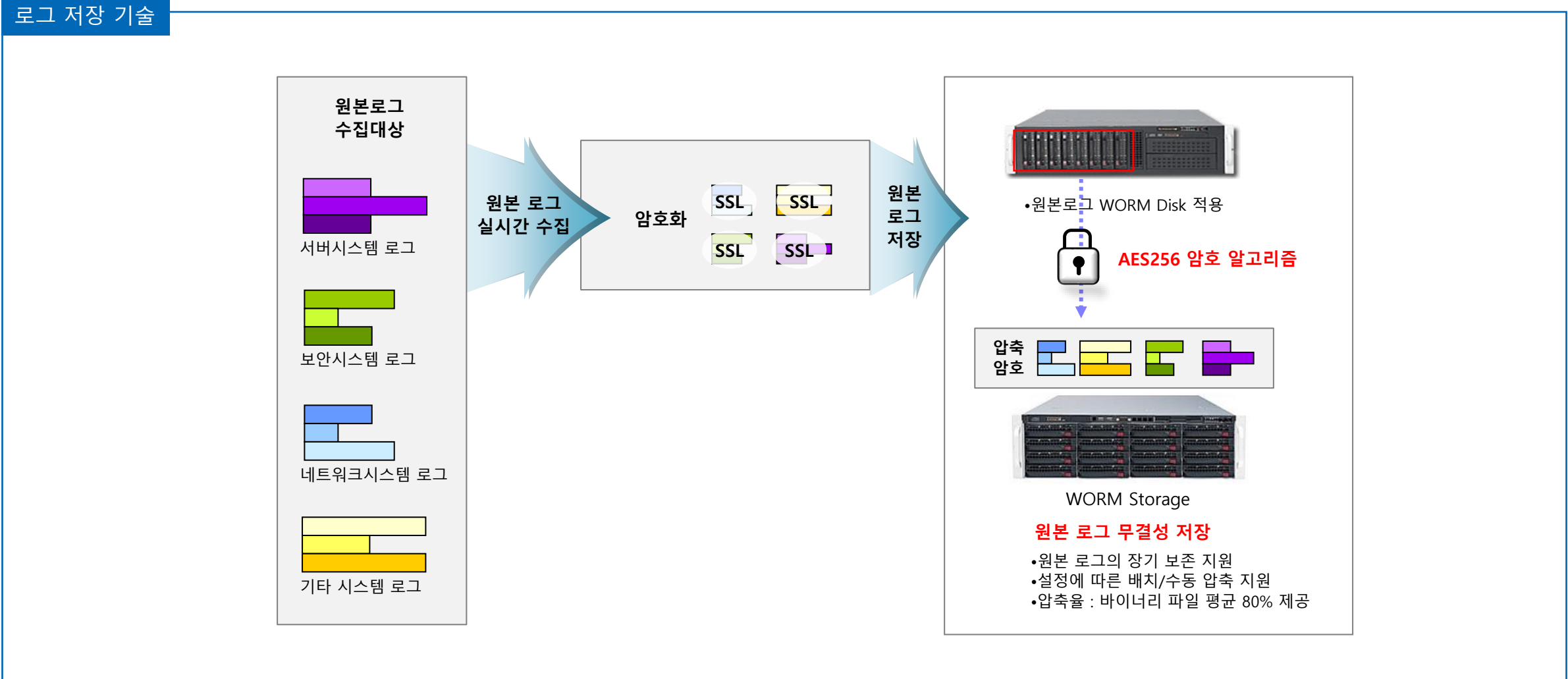
네트워크 및 서버 등의 장애로 인하여 로그 수집이 불가능할 경우 Agent가 전송과 관련한 옵션 값을 기억하였다가 시스템 상태가 정상화되면 처리한 마지막 위치에서 원본로그를 전송하여 미처리 로그에 대한 위험이 없습니다.

로그 수집 기술(2/2) - 정합성



로그 저장 기술

수집한 원본로그를 위·변조가 불가능한 WORM 매체에 실시간으로 원본형태로 저장함으로써 무결성을 보장합니다. 이때 원본로그는 암호화하여 기록하며, 80%이상 압축하여 저장공간활용을 극대화 합니다.



로그 분석기술

로그의 분석은 정규화를 통하여 서로 다른 로그 포맷의 경우에도 공통의 필드 속성값을 부여할 수 있습니다. 모든 정규화 과정은 Web UI 컨피그레이션을 통하여 손쉬운 작성 환경을 제공합니다

로그 검색/분석 기술(1/3)

정규화 항목 구성

No	항목명	데이터형	내용	삭제
1	로그일자	date	2010-06-01 11:07:19	[X]
2	밀리세컨드	short	516	[X]
3	서버 도메인 ID	string	EBZ	[X]
4	서버 INSTANCE ID	string	CA11	[X]
5	거래주적번호	string	20100601110715CV	[X]
6	요청/응답	string	Send	[X]
7	잠번호	string	null	[X]
8	직원번호	string	null	[X]
9	거래 ID	string	SQBL4202A000	[X]
10	거래명	string	결제예정금액	[X]
11	Result Code	string		[X]
12	거래전문 ID	string	SQBL4202A000A	[X]
13	수신기관 ID	string	HOST	[X]

인덱싱 항목 매핑

1. 데이터 파싱 결과를 활용한 손쉬운 항목 구성

- 정규화된 파싱 결과를 활용한 인덱싱 항목 매핑
- 적절한 데이터형 지정을 통한 효율적인 집계 및 분석 기능 제공

2. 항목 별 암호화 설정 구성

- 항목 별 마킹 여부 설정 기능 제공하여 개인의 민감정보 보호
- 항목 별 암호화 여부 설정 기능을 통해 개인의 민감정보 보호

로그 분석기술

실시간으로 정규화 된 로그 데이터를 활용하여 사용자 조건 지정에 의한 실시간 조회 및 분석 뿐만 아니라, 이기종 시스템 로그간 연관 검색 및 상관분석 기능을 제공하여 효율적인 분석을 지원합니다

로그 검색/분석 기술(2/3)

다양한 검색 기능 제공

1. 다양한 검색 방식

- 일반검색 / 순차검색
- 쿼리검색 / 탐지검색

2. 동적으로 구성되는 다양한 검색 조건

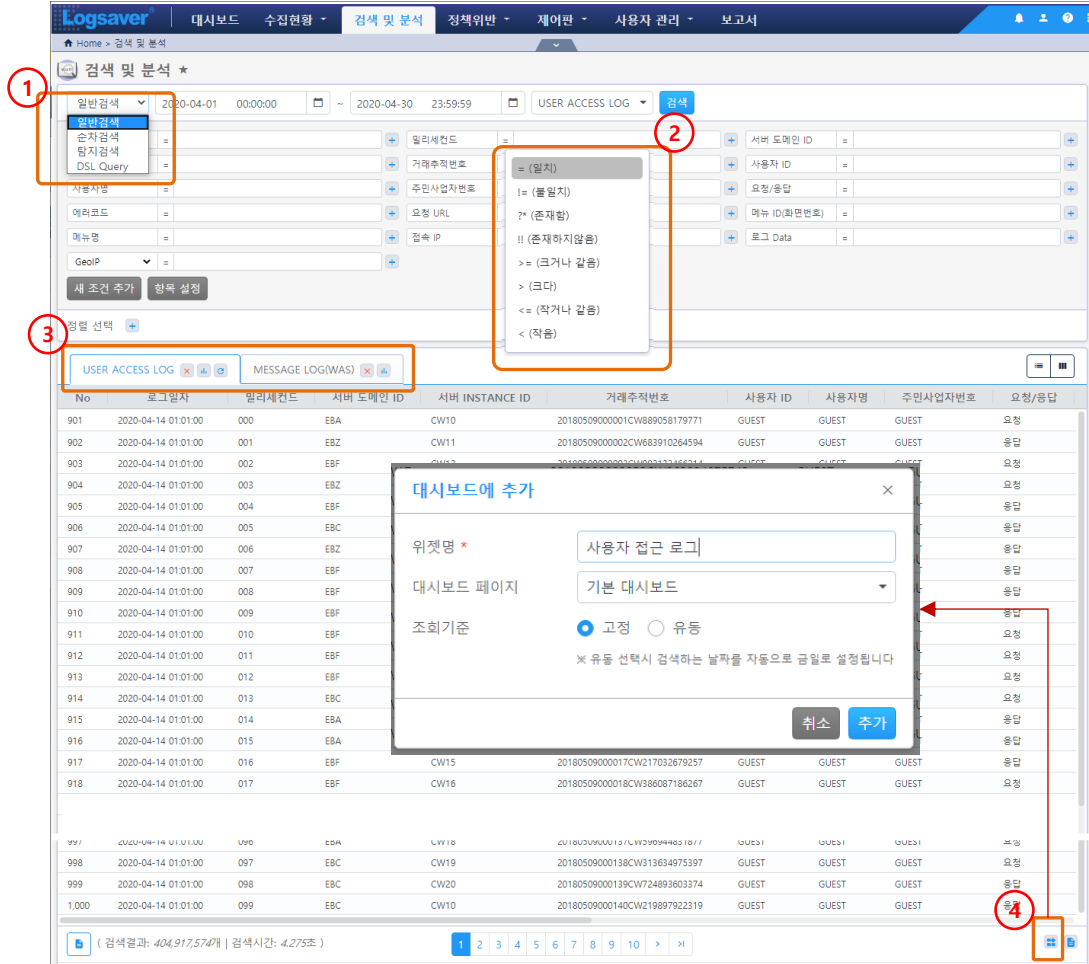
- 각 로그 필드별 조건 지정
- 조건 : =, !=, ?*, !!, <, >, <=, =>
- 필드별 정렬

3. 탭(Tab)으로 구분된 검색 결과

- 탭 선택 시 검색조건 유지
- 이전 탭, 현재 탭 결과 비교 가능

4. 대시보드에 추가

- 검색 결과를 조회 조건과 함께 대시보드에 추가
- 조회기준을 유동으로 설정하여 동일 조건에 대해 현재일 기준으로 검색하는 위젯을 대시보드에 추가



로그 분석기술

실시간으로 정규화 된 로그 데이터를 활용하여 사용자 조건 지정에 의한 실시간 조회 및 분석 뿐만 아니라, 이기종 시스템 로그간 연관 검색 및 상관분석 기능을 제공하여 효율적인 분석을 지원합니다

로그 검색/분석 기술(3/3)

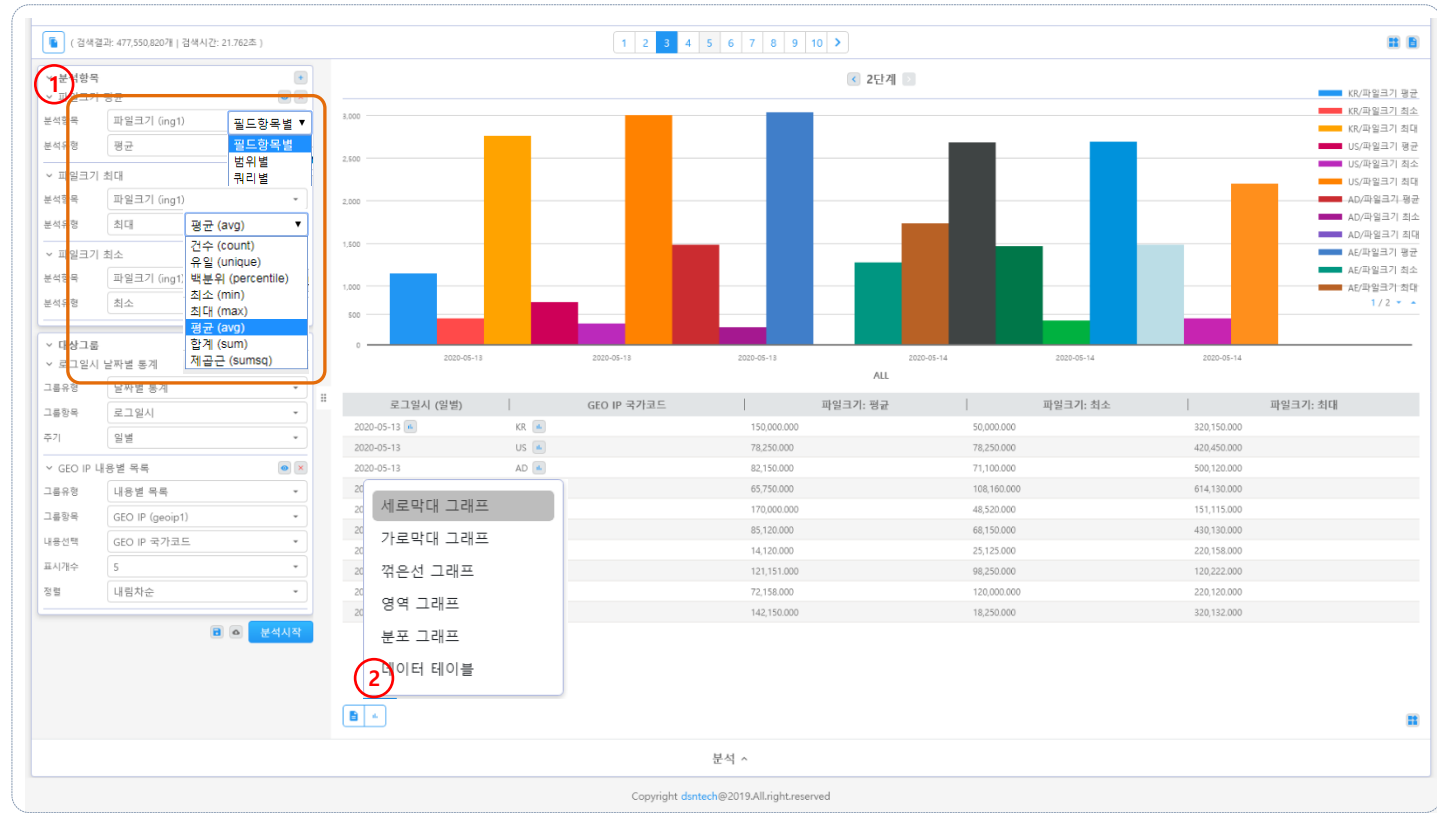
다중 Depth 분석

1. 다중 Depth 분석

- 각 필드에 대하여 분석 Depth를 추가
- 필드항목별, 범위별, 쿼리별 분석
- 다양한 분석 함수 제공
 - ✓ Count, Unique, 백분위
 - ✓ Min, Max
 - ✓ Avg, Sum, Sumsq

2. 다양한 분석 차트 제공

- 파이(PIE)차트(분포 그래프)
- 바(BAR)차트(세로/가로 막대 그래프)
- 영역 차트
- 꺾은선(시계열)차트
- 데이터 테이블



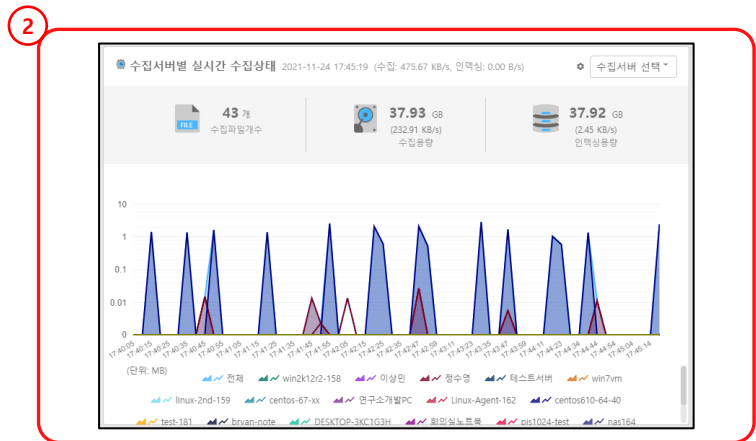
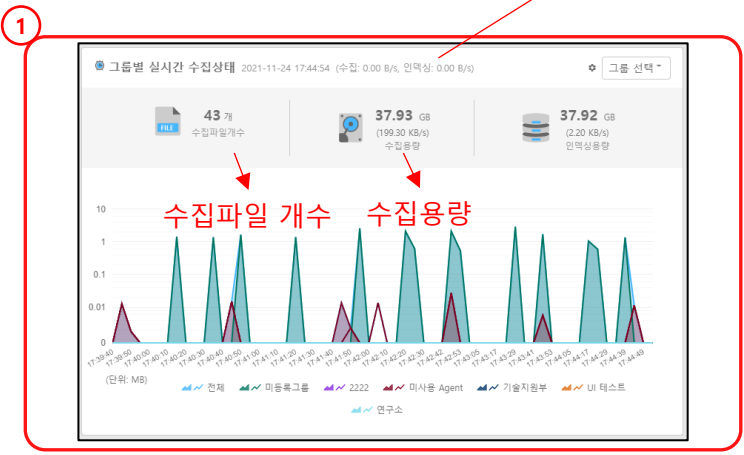
모니터링

수집되는 실시간 로그데이터의 현황(건수, 사이즈) 및 이벤트 처리에 대한 상태 모니터링을 지원합니다.

데이터 처리 현황 모니터링

- 1. 그룹별 데이터 수집 현황**
- 수집 노드의 그룹 별 현황
 - 수집 파일 개수, 인덱싱 용량 등의 정보 제공

- 2. 수집서버 별 데이터 처리 현황**
- 수집 노드 별 데이터 처리 현황
 - 수집 파일 개수, 인덱싱 용량 등의 정보 제공



수집현황

수집서버	호스트명	IP주소	2020-05-24 (일)	2020-05-25 (월)	2020-05-26 (화)	2020-05-27 (수)	2020-05-28 (목)	2020-05-29 (금)	2020-05-30 (토)
win2k12r2-158	WIN-548HT00QR5	192.168.100.158	-	-	-	-	-	-	-
이상민	DESKTOP-TAZJLRN	192.168.100.61	-	-	-	-	-	-	-
황수영	DESKTOP-SSUJBLH	192.168.100.62	-	-	-	-	-	-	-
TEST	test	127.0.0.1	-	-	-	-	-	-	-
159번서버	WIN-CUGID6JC7C	192.168.100.159	-	-	-	-	-	-	-
win2k8-r86	WIN-35AVH0T1VW	192.168.195.132	-	-	-	-	-	-	-
160번서버	WIN-QAPAQVZPC4	192.168.100.160	-	-	-	-	-	-	-
합계	-	-	-	-	-	-	-	-	-

페이지에서 보기

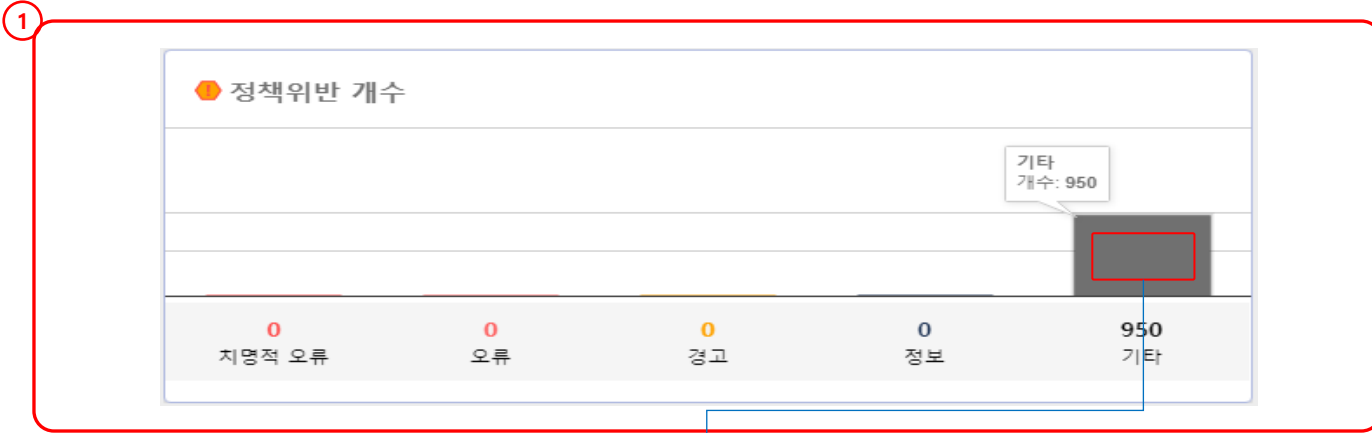
모니터링

모니터링 정책에 대한 현황을 직관적인 방법으로 제공함으로, 모니터링 대시보드 화면에서 이슈사항에 대한 추적/분석이 용이합니다.

이벤트 모니터링

1. 이벤트 발생 현황 그래프

- 이벤트 발생 건수
- 이벤트 경보 분류 별 건수
- 치명적 / 오류 / 경고 / 정보 / 기타 등 카테고리 별 히스토그램



2. 경보 발생 데이터 즉시 조회

- 경보 발생 검색 데이터 표시
- 특정 경보대상 원본로그 가능 (원본인텍싱 시)

No	등급	로그생성일시	위반정책명	로그종류	수집서버명	수집서버 IP	수집서버 호스트명	대상서버 IP	보기	작성	요청
1	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	win2k12r2-158	192.168.100.158	WIN-S4H8T00QQR5	192.168.100.158	→	✎	▶
2	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	win2k12r2-158	192.168.100.158	WIN-S4H8T00QQR5	192.168.100.158	→	✎	▶
3	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	win2k12r2-158	192.168.100.158	WIN-S4H8T00QQR5	192.168.100.158	→	✎	▶
4	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	win2k12r2-158	192.168.100.158	WIN-S4H8T00QQR5	192.168.100.158	→	✎	▶
5	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	win2k12r2-158	192.168.100.158	WIN-S4H8T00QQR5	192.168.100.158	→	✎	▶
6	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	win2k12r2-158	192.168.100.158	WIN-S4H8T00QQR5	192.168.100.158	→	✎	▶
7	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	win2k12r2-158	192.168.100.158	WIN-S4H8T00QQR5	192.168.100.158	→	✎	▶
8	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	win2k12r2-158	192.168.100.158	WIN-S4H8T00QQR5	192.168.100.158	→	✎	▶
9	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	win2k12r2-158	192.168.100.158	WIN-S4H8T00QQR5	192.168.100.158	→	✎	▶

모니터링

거래로그를 FLOW형태로 수집하여 GUID별 그룹화를 제공하며, 거래추적에 대한 입체적인 분석을 지원합니다. 이로써 다양한 채널간 복합한 I/O 흐름에도 직관적인 거래 추적관리 기반을 제공합니다.

추적 모니터링

검색결과 거래추적

거래추적 정보

1. ORI GUID: ITB20220112090334789BBP_MS11000000298

2. 거래추적 다이어그램

3. 거래시간 정보

4. 거래목록

No	로그일시	TR_TIME	CMP_ID	CMP_NM	IO_TP	CMP_TP	BR_NO	CUR_GUID	원본로그
7	2022-01-12 09:03:35	2022.01.12 09:03:35.599	ITB8EEC_SprblJsaAthActing	기업인터넷뱅킹사용자관리환경관리	OUTPUT	SVC	12	ITB20220112090335151888_MS11000000299	>
8	2022-01-12 09:03:35	2022.01.12 09:03:35.603	ITB8EEI_Ebcfclggn	기업뱅킹 인증서 로그인	OUTPUT	SVC	12	ITB20220112090335151888_MS11000000299	>
9	2022-01-12 09:03:35	2022.01.12 09:03:35.635	ITB8EVAL_VaCprlggn	가상계좌 담당자 로그인	OUTPUT	SVC	14	ITB20220112090335631888_MS11000000300	>
10	2022-01-12 09:03:35	2022.01.12 09:03:35.641	ITB000022189	가상계좌 기업사용자로그인처리	INPUT	IMO	14	ITB20220112090335631888_MS11000000300	>
11	2022-01-12 09:03:35	2022.01.12 09:03:35.727	ITB000022189	가상계좌 기업사용자로그인처리	OUTPUT	IMO	15	ITB20220112090335631888_MS11000000300	>
12	2022-01-12 09:03:35	2022.01.12 09:03:35.733	ITB8EVAL_VaCprlggn	가상계좌 담당자 로그인	OUTPUT	SVC	15	ITB20220112090335631888_MS11000000300	>

원본로그

닫기

화면 설명	
1	기본정보 - ORI GUID 정보
2	거래 추적 다이어그램
3	거래시간 정보 SEND : 전송시간 RCV : 수신시간
4	거래 추적 상세 테이블 거래추적 내용 제공, 시간 기준으로 자동 정렬

TIOR – 서버 추적 감사 S/W

서버 감사 추적 소프트웨어 TIOR 는 (Terminal Input Output Recorder)의 약자로 터미널 접속 사용자의 모든 Keystroke 정보를 활용하여 해킹 및 내부자 작업실수로 인한 정보 유출이나 장애발생시 감사 추적 기능을 제공하여 시스템 오남용 방지 및 사후 책임성을 확보합니다.

감사 추적 기술 – Unix, Linux

어플리케이션 선택

유형: 애플리케이션/부식 | 어플리케이션명: TIOR로그 | 선택 기간: 2015-11-08 | 2015-11-11 | 조건등록하기 | 조건 불러오기 | 조건 저장

조건

접속 ID: yeoksam | 접속 IP: | 프로세스명: | 조건 추가

페이지당 출력수: 20 | 건: | 정렬순: 1차 정렬 | 검색

검색

검색 결과: 217 | 소요 시간: 0.016 초 | 역설다운

TIOR로그 검색결과 | TIOR로그 분석결과 | TIOR로그 검색결과 | TIOR로그 분석결과

검색 결과: 217 | 소요 시간: 0.127 초 | reset | column

조건으로 추가 | 필자기

일련번호	con_date(접속 일시)	count
o	con_date(접속 일시) : 20151109112224	45
o	con_date(접속 일시) : 20151109094854	44
o	con_date(접속 일시) : 20151111105905	40
o	con_date(접속 일시) : 20151110144001	32
o	con_date(접속 일시) : 20151111132135	24
o	con_date(접속 일시) : 20151109094317	23
o	con_date(접속 일시) : 20151110095012	6
o	con_date(접속 일시) : 2015111120008	4

con_date(접속 일시)

con_date(접속 일시)	비율
20151109112224	20.74%
20151110144001	14.75%
20151111105905	18.43%
20151111132135	11.06%
20151109094854	20.28%
20151109094317	10.99%
201511095012	2.76%
2015111120008	1.84%

리포트

id	con_date	ip	username	host	port	command
16	2015-11-09 09:49:04	sn1.dnntech.com	yeoksam	20151109094854	192.168.100.55	5816
17	2015-11-09 09:49:09	sn1.dnntech.com	yeoksam	20151109094854	192.168.100.55	5816
18	2015-11-09 09:49:09	sn1.dnntech.com	yeoksam	20151109094854	192.168.100.55	5816
19	2015-11-09 09:49:09	sn1.dnntech.com	yeoksam	20151109094854	192.168.100.55	5816
20	2015-11-09 09:49:09	sn1.dnntech.com	yeoksam	20151109094854	192.168.100.55	5816

1 2 3 4 5 6 7 8 9 10 다음

접속 TTY	추적 TTY	command
pts/0	pts/1	ll
pts/0	pts/1	cd mysql/
pts/0	pts/1	ll
pts/0	pts/1	vi my.cnf
pts/0	pts/1	cd
pts/0	pts/1	cd scripts
pts/0	pts/1	ll
pts/0	pts/1	cd
pts/0	pts/1	ll
pts/0	pts/1	cd patch_make/
pts/0	pts/1	ll
pts/0	pts/1	vi makesh
pts/3	pts/5	ll
pts/3	pts/5	man se
pts/3	pts/5	man sed
pts/3	pts/5	load minimal amounts of data from the input files and flush the output buffers mo...
pts/3	pts/5	output version information and exit
pts/3	pts/5	input is read.
pts/3	pts/5	GNU sed home page: <http://www.gnu.org/software/sed/>. General help using GN...
pts/3	pts/5	field

리포트

사용자 정의 대시보드

통합로그시스템을 관리하는 담당자 및 업무 별 목적에 맞게 사용자정의 대시보드를 제공합니다.

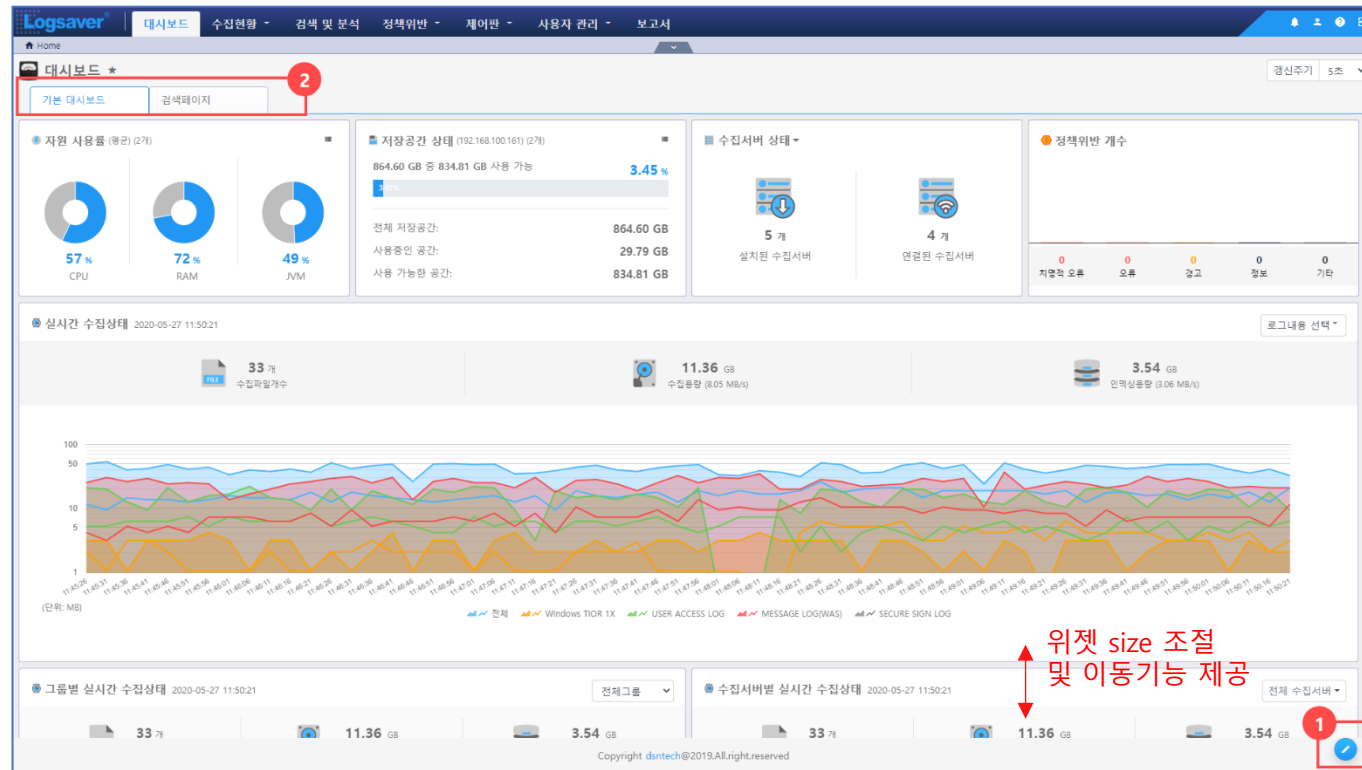
사용자 정의 대시보드

1. 위젯 편집 설정

- 사용자가 원하는 대로 위젯을 수정하고 삭제하는 편의 기능 제공
- 페이지 설정 / 초기화 / 위젯 삭제 / 위젯 이동

2. 사용자 정의 대시보드 전환 탭

- 검색 및 분석 페이지로부터 원하는 결과를 가져와 위젯을 생성하여 실시간 조회용 대시보드 구축 가능



사용자 정의 대시보드

로그분석 추이 및 개별 상태를 확인할 수 있도록 분석결과를 사용자정의 대시보드에 반영하는 기능을 제공합니다.

분석결과 대시보드에 반영

분석결과 실시간 조회

- 분석결과 대시보드에 추가하기 기능을 통해 실로그내용 분석내용 실시간 확인
- data histogram 함수를 사용하여 전일, 전주 분석제공

The screenshot displays a dashboard with three main panels showing log analysis results. A red box highlights the 'Add to Dashboard' dialog box, which is used to configure the dashboard widgets. The dialog box contains the following information:

- 위젯명 ***: 전체 로그인수
- 대시보드 페이지**: 검색결과 모니터링
- 조회기준**: 고정 유동
- ※ 유동 선택시 검색하는 날짜가 최근으로 설정됩니다

The dashboard panels show the following data:

- 사용자별 로그인수** (2021-11-16 00:00:00 - 2021-11-25 23:59:59):

순번	사용자ID	로그일시 전체건수	로그일시 전체건수 비율
1	dsntech_33	232,662	Infinity%
합계		232,662	Infinity%
- 메체별 로그인수** (2000-02-01 00:00:00 - 2021-02-01 23:59:59):

순번	메체명	로그일시 전체건수	로그일시 전체건수 비율
1	YF+HTS	648,396	Infinity%
2	INTERNET	46,314	Infinity%
3	YF+SPEED	46,314	Infinity%
- 대상서버별 로그인수** (2000-02-01 00:00:00 - 2021-02-01 23:59:59):

순번	대상서버명	로그일시 전체건수	로그일시 전체건수 비율
1	centos610-64	648,396	Infinity%
2	KBStar	46,314	Infinity%
3	HOST-1-PC	46,314	Infinity%

개인정보 유출 방지- 개인정보 암호화 및 마스킹

개인정보유출 방지를 위하여 개인정보를 포함하는 필드는 암호화하여 색인하고 마스킹(masking)하여 정보표시를 제한 할 수 있습니다.

개인정보 암호화 및 마스킹 처리

개인정보 암호화 및 마스킹처리

개별 필드 암호화 처리

- 데이터 필드 별 암호화 지정
- 정규화 시점에 암호모듈 적용 (AES-256)
- 인덱싱파일은 암호화된 정보가 저장
- 검색 시 복호화 후 정상 view(암호화 필드는 like 검색 제한)

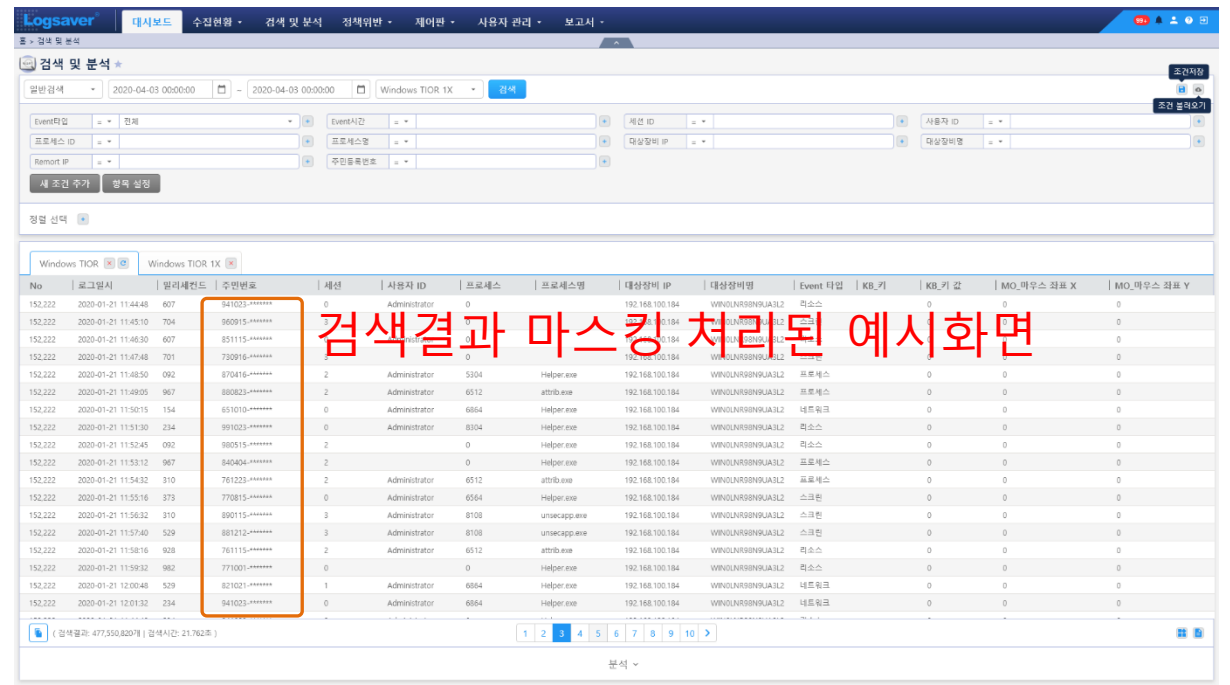


개별 필드 마스킹 처리

- 데이터 필드별 마스킹 지정
- 표시할 자리수 및 마스킹 문자열 지정 가능
- 검색 시 표시된 자리수 만큼 필드값 표시하고, 나머지는 마스킹 문자열로 표시

```
Wd{2}([0]Wd|[1][0-2])([0][1-9][1-2]Wd[3][0-1])[-]*[1-4]Wd{6}
```

정규표현식을 통한 개인정보(주민등록번호) 추출제공



사용자 이력 관리

사용자 및 관리자가 시스템에서 동작한 모든 이력에 대한 전체 정보를 제공함으로 개인정보유출 가능성을 억제할 수 있습니다. 로그접근의 대한 정보를 저장합니다.

사용자별 작업 이력

1. 사용이력 조건 검색

- 기간 및 테이블 항목을 조건으로 검색하여 조회
- 사용행위 / 대상이름 / IP 주소 / URL 등의 조건으로 조회

2. 사용이력 정보 제공

- 사용행위 / 대상이름 / IP 주소 / URL / 사용일시 등의 상세정보 제공

3. 사용이력 다운로드

- 사용이력 검색 결과에 대한 파일 다운로드 제공

No	대상이름	IP주소	행위 (Method)	URL	사용일시
1	수집서버 및 그룹 조회	관리자	192.168.100.68	조회 (get)	server/group 2020-06-02 07:43:07
2	수집서버 및 그룹 조회	관리자	192.168.100.68	조회 (get)	server/group 2020-06-02 07:43:07
3	사용자 로그인	관리자	192.168.100.68	생성 (post)	auth 2020-06-02 07:43:07
4	수집서버 및 그룹 조회	관리자	192.168.100.68	조회 (get)	server/group 2020-06-02 07:43:07
5	수집서버 및 그룹 조회	관리자	192.168.100.68	조회 (get)	server/group 2020-06-02 07:44:37
6	수집서버 및 그룹 조회	관리자	192.168.100.68	조회 (get)	server/group 2020-06-02 07:44:37
7	수집서버 및 그룹 조회	관리자	192.168.100.68	조회 (get)	server/group 2020-06-02 07:44:37
8	대시보드 조회	관리자	192.168.100.68	조회 (get)	dashboard 2020-06-02 07:44:48
9	대시보드 조회	관리자	192.168.100.68	조회 (get)	dashboard 2020-06-02 07:44:48
10	정책 위반내역 조회	관리자	192.168.100.68	조회 (get)	block 2020-06-02 07:44:56
11	정책 위반내역 조회	관리자	192.168.100.68	조회 (get)	block 2020-06-02 07:44:56
12	에이전트 로그 통계	관리자	192.168.100.68	조회 (get)	log/agent_stat 2020-06-02 07:51:25
13	정책 위반내역 조회	관리자	192.168.100.68	조회 (get)	block 2020-06-02 07:51:27
14	대시보드 조회	관리자	192.168.100.68	조회 (get)	dashboard 2020-06-02 07:51:27
15	수집서버 및 그룹 조회	관리자	192.168.100.68	조회 (get)	server/group 2020-06-02 07:51:31
16	대시보드 조회	관리자	192.168.100.68	조회 (get)	dashboard 2020-06-02 07:51:31
17	수집서버 및 그룹 조회	관리자	192.168.100.68	조회 (get)	server/group 2020-06-02 07:51:31
18	수집서버 및 그룹 조회	관리자	192.168.100.68	조회 (get)	server/group 2020-06-02 07:51:31
19	정책 위반내역 조회	관리자	192.168.100.68	조회 (get)	block 2020-06-02 07:51:32
20	대시보드 조회	관리자	192.168.100.68	조회 (get)	log/hour_agent... 2020-06-02 07:53:26
21	대시보드 조회	관리자	192.168.100.68	조회 (get)	dashboard 2020-06-02 07:54:10
22	정책 위반내역 조회	관리자	192.168.100.68	조회 (get)	block 2020-06-02 07:54:11
23	대시보드 조회	관리자	192.168.100.68	조회 (get)	log/hour_agent... 2020-06-02 08:04:28
24	대시보드 조회	관리자	192.168.100.68	조회 (get)	dashboard 2020-06-02 08:05:03
25	정책 위반내역 조회	관리자	192.168.100.68	조회 (get)	block 2020-06-02 08:05:04
26	사용자 로그인	관리자	192.168.100.68	생성 (post)	auth 2020-06-02 08:45:38
27	대시보드 조회	관리자	192.168.100.68	조회 (get)	dashboard 2020-06-02 08:45:38
28	수집서버 및 그룹 조회	관리자	192.168.100.68	조회 (get)	server/group 2020-06-02 08:45:39

개인정보 유출 방지- 소명관리

개인정보 과다 조회 등 특이사항 발견 시 즉시 소명요청을 할 수 있으며, 소명관리 기능을 제공하여 지속적인 관리감독을 할 수 있습니다.

소명 관리 기능

소명 관리

1. 소명 요청 처리 흐름도

- 소명이 필요한 정책 설정
 - ✓ 개인정보 과다 조회 등에 대한 정책 설정
- 이벤트 발생 시 소명당사자에게 소명 요청
 - ✓ 개인정보 과다 조회
 - ✓ 경고 발생
- 소명당사자의 소명응답 / 소명내용 회신에 따라 처리완료
 - ✓ 반려 및 재 요청,
 - ✓ 승인 완료

2. 소명 요청

- E-mail 주소로 소명화면 URL 요청
- 소명 요청 시 해당 이벤트 발생 내역 표시
- URL을 통한 소명응답 화면 접속 후 소명 진행

1

No	등급	정책명	설명	로그종류	작성자	최초 등록일시	마지막 수정일시	적용	수정
1	기타	USER ACCESS LOG GUEST 감지	GUEST 감지	USER ACCESS LOG	이상민,개발용_1	2020-06-12 11:18:52	2020-06-19 14:55:45	<input type="checkbox"/>	<input type="checkbox"/>
2	기타	WinTIOR 1x Test		Windows TIOR 1X	정수영	2020-06-12 11:15:10	2020-06-12 11:16:00	<input type="checkbox"/>	<input type="checkbox"/>
3	기타	USER ACCESS LOG GUEST 감지	GUEST 감지	USER ACCESS LOG		2020-06-12 11:03:35	2020-06-12 13:41:05	<input type="checkbox"/>	<input type="checkbox"/>
4	경고	test		USER ACCESS LOG	관리자	2020-05-06 16:00:23	2020-06-12 11:19:21	<input type="checkbox"/>	<input type="checkbox"/>

2

No	등급	로그생성일시	위반정책명	로그종류	대상서버 IP	대상서버 호스트명	프로세스명 [PID]	위반내용	보기	작성	요청
1	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
17	기타	2020-04-14 01:49:28	USER ACCESS L...	USER ACCESS LOG	192.168.100.158			사용자 ID: GUEST...	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

전체 구축 실적(요약)

제안사가 제안하는 제품은 은행, 증권, 카드, 보험 등의 금융권을 비롯하여, 공공기관, 일반기업체 등 다양한 분야에서 고객을 확보하고 있는 우수한 제품으로써, 국내 시장 점유율 1위 제품입니다.

공공	은행/금융	일반 기업체	국방	해외
대통령비서실 대법원(호적망, 등기망, 가족망) 기획경제부(NAFIS), 해양수산부 기획예산처(디지털회계예산) 안전행정부, 산업통상자원부 고용노동부, 한국산업기술시험원 경찰청(사이버테러대응센터) 조달청, 국세청, 서울지방경찰청 식품의약품안전처, 철도청 충청남도교육청, 한국토지주택공사 한국인터넷진흥원(KISA) 국가정보원, 한국정보화진흥원 한국가스공사, 인천공항공사 국민연금공단, 국민체육진흥공단 인사혁신처, 한국정보인증 한국원자력연구소, 한국마사회 부산항만공사, 광물자원공사 건강보험심사평가원, 김해경전철 한국도로공사, 한국전력공사 수원시청, 한국석유공사 교육부, 국회사무처, 제주시청 한국산업단지공단, 한국환경공단 국가정보자원관리원 경남도청, 성남시청 전국 16개 시도 교육청 (서울, 경기, 인천, 강원, 충북, 충남, 대전, 경북, 경남, 대구, 울산, 부산, 전북, 전남, 광주, 제주) 외 다수	<ul style="list-style-type: none"> • 금융감독원 • 금융정보분석원 • 한국자산관리공사 • 한국예탁결제원 • 한국신용정보원 • 한국금융연수원 • 저축은행중앙회 • 농협중앙회, 농협생명 • 농협NH카드 • 수출입은행 • 산업은행 • 신한은행, 신한금융지주 • 신한생명, 신한카드 • 신한금융투자 • 삼성생명, 삼성화재 • 삼성증권 • 한화생명, 한화손해보험 • 하나카드, 하나멤버스 • SC은행, SC증권 • KTB투자증권 • 미래에셋생명, 미래에셋대우 • SK증권 • KB증권, KB손해보험 • 롯데손해보험, 롯데멤버스 • 메리츠화재 • ING생명보험 • 흥국생명, 흥국화재 • EB카드 외 다수 	<ul style="list-style-type: none"> • KT본부 • KT IT 본부(목동) • KNET(전자문서보관소) • KT(정보보호본부) • 삼성전자(15곳) • 삼성종합기술원 • SK OCMP • SK C&C • 나눔로또위원회 • 메가스터디 • 노틸러스호성 • 롯데면세점 • NC소프트 • 쇼핑엔티 외 다수 <p style="text-align: center;">대학교 및 병원</p> <ul style="list-style-type: none"> • 건국대학교 • 중앙대학교 • 한성대학교 • 서울교육대학교 • 서울여자대학교 • 삼육대학교 • 동남권 원자력 의학원 • 대구 파티마 병원 • 구미 차 병원 • 강동경희대학교 병원 외 다수 	<ul style="list-style-type: none"> • 국방재정 • 국방인사 • 국방인증 • 국군수송사령부 • 합동참모본부 • 방위사업청 • 육군본부 • 해군본부 • 공군본부 • 국방 CPAS • 합참KJCCS(지휘통제체계) • 국방동원 • 국방과학연구소 • 국방기술품질원 • 국군통신사령부 • 국군기무사령부 • 각급 부대 별 납품 외 다수 	<ul style="list-style-type: none"> • 미국 : Princeton University • 일본 : 일본과학기술청, NHK, 삼성JAPAN, 일본 Dreamware, Mitsubishi Research Institute • 독일 : BW Bank, Bohn University • 말레이시아 : Alliance System • 싱가포르 : snttec • 신한은행 해외 지점 (독일, 캐나다, 일본, 베트남)

Log saver®



감사합니다

dsntech
digital solution & technology partner

Digital Solution & Technology Partner