



High Availability

Flexibility

Consolidation

Performance

Automation

Reduce TCO



## Overview

로그분석 프로그램의 목적은 각 운영체제 및 네트워크 및 보안장비 또한 어플리케이션 의 로그를 분석하여 보안문제를 사전에 예방함과 동시에 사후 추적관리를 하기 위한 것이다.

- 단기 목표
  - 시스템의 주요 로그파일에 대한 기본적인 분석 및 통계 작업을 자동화
- 중기 목표
  - 분석할 수 있는 로그 및 분석 패턴 강화, 로그 변조 유무 확인 및 통합분석의 정교함 강화
- 장기 목표
  - 분석결과를 토대로 하여 보안 관련한 문제를 예측할 수 있는 기능 강화

## Features

- 기능
  - 실시간 로그 통합관리 및 로그이벤트 모니터링
  - 다양한 리포트 및 통계 자료 제공
  - 로그 파일의 자동 보관, 폐기, 압축 기능
  - 장애 로그 이벤트에 대한 단문발송, 이 메일 그리고 스크립트 실행
  - 장애 발생시 로그 분석을 통한 원인규명
  - 문제 지식관리에 의한 사고 미연 대처
  - 통합로그관리에 의한 비용 절감 효과
  - 로그 설정관리를 통한 장애 예측 기능
  - 로그 관리의 편리성
  - 웹 기반의 편리한 접근성
  - 로그 패턴을 활용한 다양한 검색 및 분석 기능

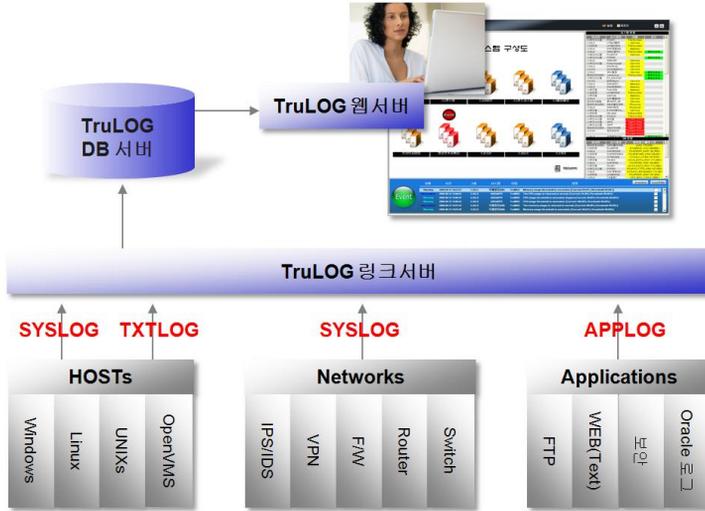
## System Logs



구분	Facility	Severity
<b>SYSLOG</b> For UNIX and Networks	✦ KERN ✦ USER ✦ MAIL ✦ DAEMON ✦ AUTH ✦ SYSLOG ✦ LPR ✦ NEWS ✦ UUCP ✦ CRON	✦ Panic (Emergency) ✦ Alert ✦ Critical ✦ Error ✦ Warning ✦ Notice ✦ Information ✦ Debug
<b>OPCOM</b> For OpenVMS	✦ SYSTEM ✦ LOGIN	✦ Fatal ✦ Critical ✦ Error ✦ Warning ✦ Information
<b>WinLOG</b> For Windows Systems	✦ 시스템 ✦ 응용프로그램 ✦ 보안	✦ Error (오류) ✦ Warning (경고) ✦ Information (정보)



## Configuration



## Specifications

### TruLOG 에이전트 플랫폼

- Host : HP-UX, HP Tru64UNIX, HP OpenVMS, SUN Solaris, IBM AIX  
Linux, Windows
- Network/Security : Switch, Router, Firewall, VPN, IPS/IDS
- Application : FTP, Web, Mail, User Application

**주요기능** : 로그수집

### TruLOG 서버 플랫폼

- Linux Server
- DB : Oracle / MySQL

**주요기능** : TruLOG 링크 서버, DB 서버, 웹 서버



**Total IT  
Management Solution  
Provider in Korea**

**TruITM**

Total IT Management

**ConsoleWorks**

Total Console System

**EnSCHEDULE**

Enterprise Scheduler

**HA\_SYS**

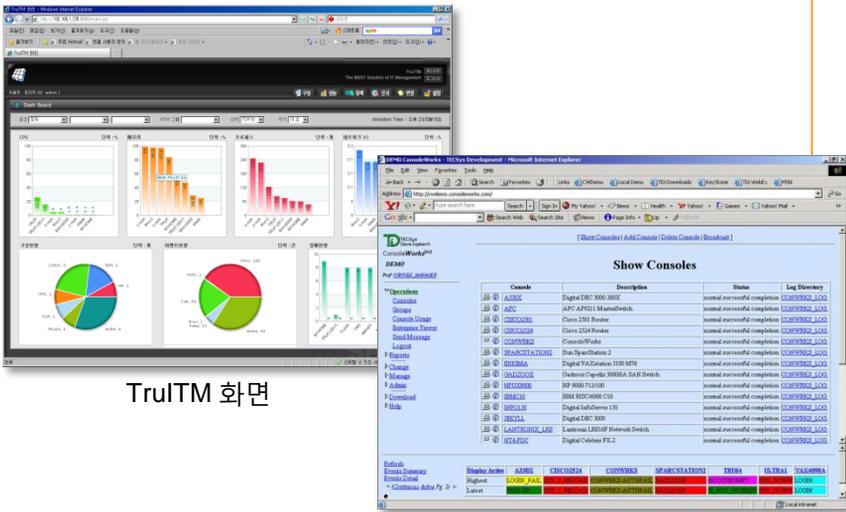
High Availability System

**TruLOG**

Total LOG Management

**TruCON**

Total Console Management



TruITM 화면

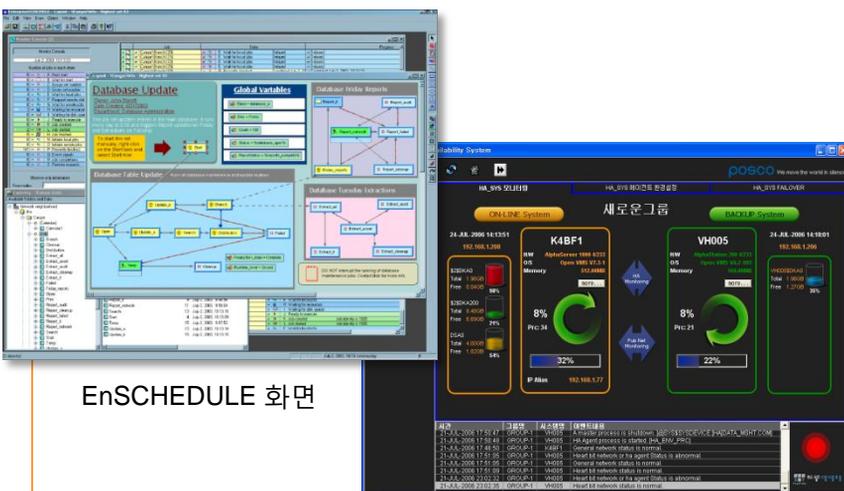
ConsoleWorks 화면

**통합 시스템관리 솔루션의 선두주자**

다양한 기종의 시스템과 그에 따른 서로 다른 운영체제, 그리고 광범위하게 분산되어 있는 시스템과 복잡한 네트워크 환경은 보다 체계적이고 효율적인 시스템 관리가 요구되고 있으며, 또한 급격한 환경 및 기술 변화에는 보다 능동적이고 적극적인 관리 시스템 구축이 요구되고 있습니다.

이에 트루아이티(주)는 시스템 Downtime 및 문제 해결 시간의 최소화, 사전예방 체제 구축, 적용과 사용의 편리성, 선진 기술의 적용 그리고 비용절감 등의 효과를 가져올 수 있도록 다음과 같은 통합 시스템관리 솔루션들을 제공하고 있습니다.

- **TruITM** – ITSM 종합관리 (서버, 네트워크, 데이터베이스관리 포함)
- **ConsoleWorks** – 콘솔시스템 통합관리
- **EnSCHEDULE** – 엔터프라이즈 스케줄 통합관리
- **HA\_SYS** – 고 가용성 시스템
- **TruLOG** – 로그 통합관리
- **TruCON** – 콘솔 통합관리



EnSCHEDULE 화면

HA\_SYS 화면

서울시 양천구 목1동 917-9  
현대41타워 2016호 (우)158-723

Tel : 02-2648-1701  
Fax : 02-2648-1702

<http://www.truit.co.kr>