



IRIS Log Analyzer

Large-scale log data management and analysis in real time

- ▶ Integrated analysis of structured and unstructured data
- ▶ Anomaly detection through analysis of log data event pattern

IRIS Log Analyzer

Distributed processing is inevitable to process the large scale log data, generated in the large systems like data centers.

IRIS Log Analyzer is a large scale distributed processing system to collect and analyze various types of logs generated in large scale ICT systems. It is a scale-out type log analyzer, which can be expanded up to tens or hundreds of nodes.

It is optimized for real-time indexing and SQL type analysis can be conducted over the indexed log data.

Features of IRIS Log Analyzer

Large scale log data processing in real time

Distributed architecture guarantees the processing high volume data in real time, through efficient resource management and data distribution.

Prompt log data analysis and tracing

Data collected in the system can be searched rapidly and various data analysis and tracing functions are provided. By doing so, the time required to handle errors and solve problems can be reduced, providing higher level services.

Scale out at the function level

Distributed platform is applied at the function level, so flexible expansion per each function is possible upon large-scale system establishment. All process made in the system can be checked immediately.

Perfect combination of log analysis and SQL analysis

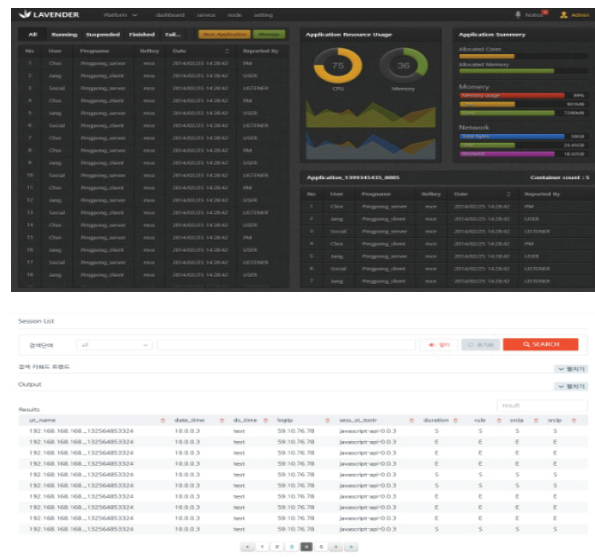
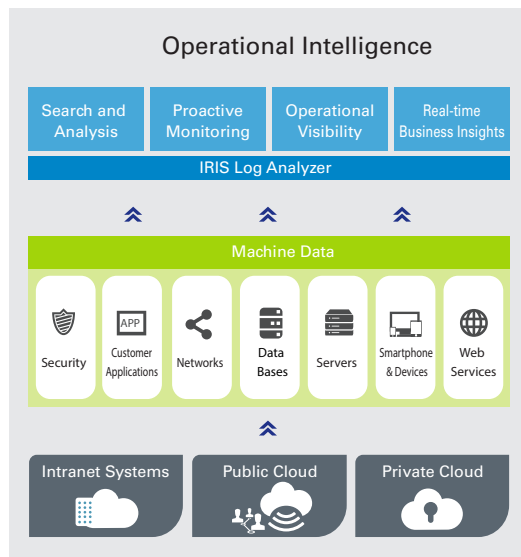
Logs can be easily searched, analyzed and managed by using SQL, which is widely used in existing IT system analysis.

Accommodating open source Hadoop system

It collects all types of data generated from existing IT environment and provides environment where various analysis functions can be performed by connecting with open source Hadoop system.

IRIS Log Analyzer perfect harmonization

All functions and characteristics are harmonized perfectly based on experience and know-how accumulated for many years.



IRIS Log Analyzer

The extreme capacity and performance presented by IRIS Log Analyzer come from our passion to pursue extremity

Major Functions and Characteristics	
Major Functions	Description
Support for structured and unstructured data analysis	Structured and unstructured data analysis can be conducted in an integrated manner by supporting traditional DMBS SQL and full-text indexing.
Real-time full-text indexing	With full-text indexing engine, it supports high speed indexing of data, collected in distributed cluster in real time and it supports limitless scale-out expansion.
Real-time data analysis and alarm	Association analysis on data processed in real time is conducted to generate alarms to report to the users.
Accepting data from all sources	Flexible data model is supported to enable processing of various types of data and maintain logs as original state and unstructured data processing is supported through full-text indexing.
Clustering that guarantees stability	Index sharding/partitioning technology is used to process high volume data based on distributed cluster. Data is stored in a multiplexing way to secure stability of data.

IRIS Log Analyzer supreme player of big data

The best performance can be achieved when the best hardware and the best software meet with the best experience.

Log collection/indexing function

Log Collection Agent

Log collection agent is installed in Linux/Unix server and collects and sends log installed in the servers.

Flexible Parser




This function is to define log pattern and extract meaningful field to accept all types of logs.

Real-time Indexing

Indexing is performed for log data in small block files (1GB) to process high volume data and indexing is performed based on memory. Therefore, the extreme scale log stream from a data center can be processed,

Full-Text Indexing

Full-text indexing function is provided to make searching for all keywords in log text randomly possible. Full-text indexing increases the freedom of search maximizing the utilization of log.

Expansion of log analyzer performance	
Various data analysis through expansion function (bundle functions)	
 Get Data	The easiest way to obtain data
 Get Insight	User-defined alarm report and dashboard
 Get Started	Applied in various fields

Log Analysis Functions

Support for advanced analysis function
Advanced analysis functions are provided over collected log data.

- Support for mining includes clustering and classification.
- Anomaly detection through time series analysis

Support for log data event pattern analysis

The function of automatic pattern detection of individual log is provided.

Based on statistical log analysis, event pattern is recognized, statistics on event pattern become available and anomaly is detected.

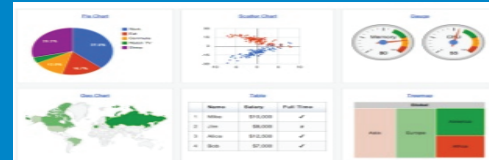
Support for visualization in composite charts

Intuitive analysis on the overall data is supported with scenario-based composite visualization over collected data.

Technology recognized by patent

Method and system to provide independent operating environment for each process in distributed platform (under patent application)

Visualization of composite charts



Composite charts based on scenario

Detection of anomaly

Anomaly detection, error alarm

Automatic pattern recognition

Pattern specific statistics

Data mining and machine learning

Clustering and classification

Distributed index storage

Detection of anomaly



IRIS Log Analyzer Software Architecture

Experience a new level of analysis of integrated distribution and virtualization.

Excellent Usability and Convenience

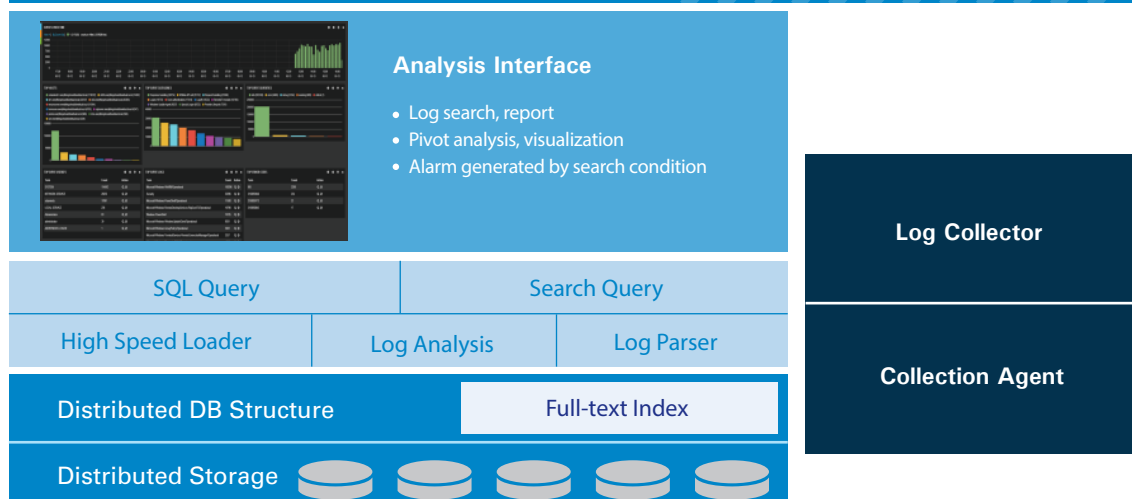
Support for dual log management interface

- Support for search type query interface
- Support for SQL type interface

Support for integrated interface of report and alarm

- Integration of search function and report function

Software Architecture of IRIS Log Analyzer



High-speed indexing for large volume log

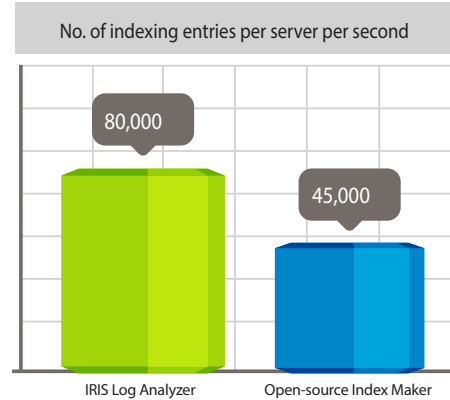
High-speed indexing engine is supported to collect and index large scale integrated network log

Stability through cluster support

Realization of non-stop system through multi-node clustering, with fail proof replication

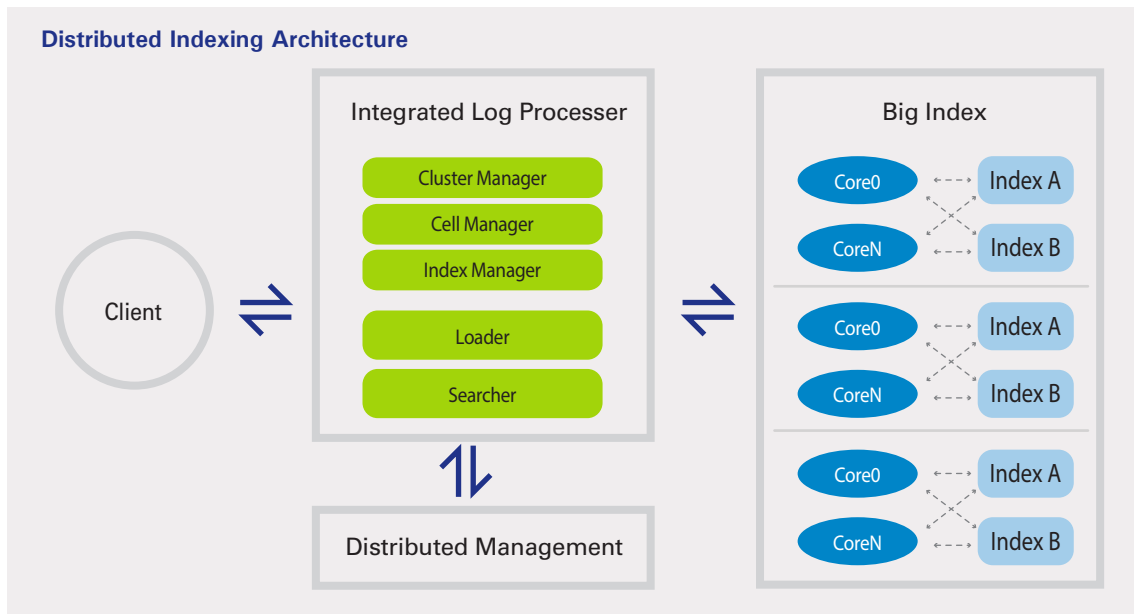
Generation of big index

Generation of huge index structure is guaranteed with sharded /partitioned index structure that supports PB scale Full-text indexing.



Major Characteristics

- Real-Time Full-text Indexing
- Index Sharding / Partitioning
- Index Duplication
- High Availability
- Support for standard API (JDBC, Restful API)
- Support for various schema



Why IRIS Log Analyzer ?



Collection, processing and indexing of log generated from various IT systems and infrastructures are conducted in real time.



Cause analysis and taking action can be done rapidly by searching over large-scale data in real time.



Major information can be monitored at a glance by organizing dashboard as user wants.



The convenience of management and search performance, guaranteed by combining SQL DB type query and full-text type indexing.



Various external interfaces are supported (JDBC, SQL, search query, Hadoop, Hive/Tajo, R)



About Mobigen

Mobigen provides telecom service carriers and enterprises proven big data solutions and service assurance solutions for wired, wireless and IP service networks.

For more information, please visit www.mobigen.com or contact global@mobigen.com