Kron

Quality Simplified

CARRIER GRADE LOGGER

WHITEPAPER

Secure and High Capacity Logging

Introduction

CG-Logger is an overlay big-data data transfer, processing and distributed infinite-scalable logging platform for your everyday growing data with solid references.

Carrier Grade Logger is an integral element of Kron's appliance based ICT data support products. CG-Logger offers easy and efficient collection of data from distinct, distributed locations. Stored logs can be shared across the enterprise or Telco, empowering a wide range of users with query, analysis and reporting capabilities.

Deploying CG-Logger can enhance an existing Business Intelligence investment or reporting farm with a new dimension in data management, data correlation, analysis, and reporting through the organization. With these benefits operators don't need to overpay to any logging solution for logging requirements like legal recording, tracking, Carrier Grade NAT, flow analysis, CDR analysis, event & alarm logging. The proven return on investment with CG-Logger is in months due to its next generation appliance based high performance architecture.

Appliance based architecture gives chance to deploy CG-Logger collector appliances where data is generated from data center cores to distant offices. CG-Logger transfers data in between collectors to central cabinet appliances in a compressed and secure way.

Highlights

Industrialized Big-Data solution with instant pay-back and ROI effect.

Don't loose time to understand big-data, just benefit it with Kron's appliance based solution.

Customer Benefits

» For a logging system no need to spend millions on other databases designed for other purposes.

» Don't need to have thousands of functions or re-modeling each and every-day

» Mission-critical log capturing and saving without any data loss.

» Flexible architecture for logging capacity or new site expansion.

» Transmit logging packets from remotes site with a reliable protocol

» Monitor logging infrastructure with notification and alarm mechanisms.

» Low administration effort to maintain the entire deployment

» Minimal end user training required to start using the system and gaining benefits

» Distributed architecture brings flexibility in data capture and transfer

Business Scenarios

CG-Logger can be used to support a number of scenarios when deployed in conjunction with different network equipment including routers, firewalls, DPI, NAT devices.

One of the most powerful use cases is Carrier Grade NAT (CGN) need. Due to the lack of IPv4 addresses, operators launches CGN projects but this approach requires to log and correlate each and each user's session and NAT traversal to clarify user identity due to the obligations of legal authorities.

It is not only for obligation but also identifying & authenticating user based on its translated IP address is critical for online application authentication. Most of the operators have online applications (such as online customer operations etc.) which authenticate users via its IP address or MSISDN or similar information that is derived from live logs. This authentication mechanism is broken when the operators introduces projects like CG-NAT unless a correlation solution is deployed to solve this problem.

Other business scenarios well suited with CG-Logger including:

» CG Logger can be used for collecting alarm events/logs coming from network infrastructure and applications

» CG Logger can be used as CDR analyzer, Netflow traffic analyzer for traffic anomaly detections and usage reports.

» As a data store for your DPI solution.

Key Features

» High number of log packet capturing and correlation capacity
» (Up to 2 million log/second per CG-logger appliance)
» Supports Syslog / Netflow and any open logging protocol
» Adaptor based module support for different and new type of log streams
» Distributed architecture with collector and cabinet units.
» Store and forward network level caching
» Sophisticated user credential management
» Enhanced RADIUS/DHCP logging correlation of user data with traffic logs.
» Telco-grade scalability
» No-SQL data store architecture
» Zero packet / data loss infrastructure
» High volume of storage addressing capacity , with no-SQL
» Big-data backend
» Storage area and disk efficiency with compression algorithms and buffering mechanisms.
» Supports low cost storage (from low cost SATA disks to SAN systems)
» Web based user interface for data query
» Federative query support on distributed units
» North-bound interface for data query
» Proven Kron Platform appliance
» AC and DC power options
» Hardened Kron Linux Kernel
» High Availability Support

Case Study-1

Recently one of the tier-1 mobile operators has decided to launch Carrier Grade NAT project. They have millions of sessions to be logged each second and online applications must be authenticated in less than 150 ms., which means during the capturing and correlating user and traffic data, meantime the filtered log data to specific destinations also will be inserted into an SQL database in less than 150 ms.

There are several challenges to be handled to fulfill these requirements. The utmost important challenge is the scalability and fast processing of real-time multi-source data. Kron CG-Logger's parallel-distributed architecture has helped in scalability and on the other hand real-time in-memory correlation function solved difficulties for fast processing that our client is facing.

As the incoming logging data is very critical due to the legal obligations, Kron's high available architecture provides an overall solution without a Single Point of Failure and zero packet or data loss to our tier-1 mobile operator.

Case Study-2

One of our system integrator & solution provider customers was looking for a data store solution for their Deep Packet Inspection system logs. As their existing DPI solution was pre-integrated with a well-known traditional and relational database, in case of large dimensioning figures, they had some performance concerns. These concerns make them also to increase the server processing power, which not surprisingly ended up with multi-million dollar hardware and software costs. Existing database license cost was increasing according to the number of CPU core. As a result of this picture, together with hardware and the licensing costs, it was an unfeasible and affordable project.

Kron CG-Loggers adaptor based architecture of data input modules make it possible to replace any existing data store. After the adaptation of data model and adaptor modules between target DPI product and CG-Logger, data flow from DPI product to CG-Logger is provided. CG-Loggers north-bound interface is utilized for data reports and queries. Due to the NoSQL architecture of CG-Logger and high-performance Kron CG-Logger appliances overall solution made the high cost hardware and licensees unnecessary and our customer could fit into the budgets of their customers.

Technical Specifications

Data Interfaces
Web-based user interface, North-bound interface, CLI interface

Supported Protocols
Syslog, Netflow, Radius, DHCP, any other text or binary logging protocol

Logging Formats
CSV file logging, NoSQL database logging, SQL database logging

Additional Functional Modules
Log Filtering, Real-time Log Correlation, Offline Log Correlation

Supported Kron Appliances
Kron IAP-I, IAP-M, IAP-L, IAP-X

For more details
info@kron.com.tr