

Normalizer and Database Loader

High-Speed Normalization of Syslog Data for Standardized Corporate Reporting

CorreLog Normalizer and Database Loader (NDL) is a flexible syslog data parser that loads user-specified messages into a relational database (RDBMS).

By leveraging CorreLog NDL, business analysts now have a mechanism for getting unstructured, but valuable syslog data into a relational database for formatting into usable business intelligence with Crystal Reports or other package.

A key component of NDL is the high-speed filtering and conversion of raw syslog data to RDBMS. For filtering, NDL parses data from user- and system-defined qualifiers that provide an instruction set for normalizing and loading the data. NDL can parse messages for any system device, with the capability to load the messages at a sustained throughput of more than 1,000 per second.

CorreLog NDL operates with two primary considerations:

1. Where did the data come from (source IP address)?, and
2. What are the unique identifiers that make this message data a candidate (or "Qualifier") for sending to RDBMS?

Ultimately, the primary objective of CorreLog NDL is to provide a high-speed syslog parser that "normalizes" SIEM data for standardized corporate reporting.

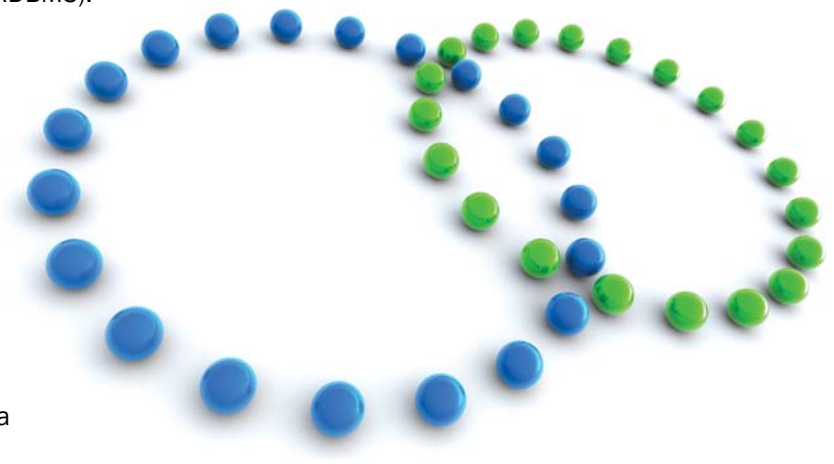
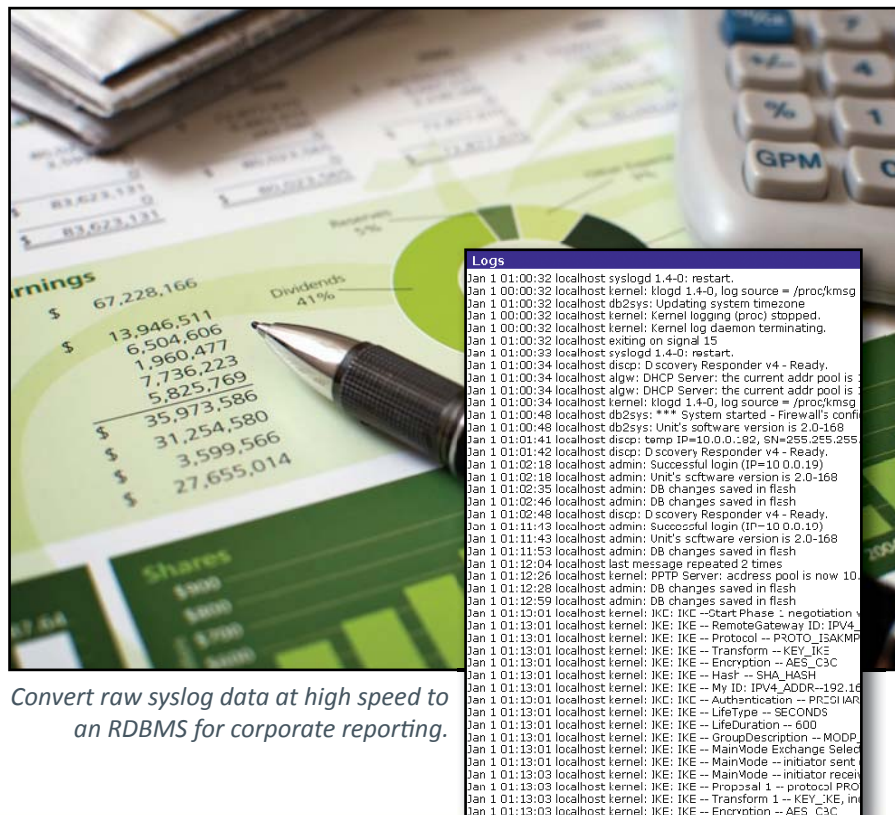
Leveraging IP Address Range

CorreLog NDL utilizes IP address ranges as the initial means by which an incoming message is associated with one or more message formats for possible RDBMS inclusion. NDL links device location to message attributes through a range of IP addresses. The IP range is associated with one or more message formats, and consists of an inclusive lower bound and inclusive upper bound IP source.

Message Formats and Fields

A message format in CorreLog NDL consists of a named collection of fields, and is associated with one or more IP address ranges. The relationship here is that a message format includes one or more fields. A field specifies how data from the message is to be reformatted before insertion into the RDBMS. A field might contain:

- The year, month, date
- The source IP address

Convert raw syslog data at high speed to an RDBMS for corporate reporting.

```

Logs
Jan 1 01:00:32 localhost syslogd 1.4.0: restart.
Jan 1 00:00:32 localhost kernel: klogd 1.4.0, log source = /proc/kmsg
Jan 1 01:00:32 localhost db2sys: Updating system time:one
Jan 1 00:00:32 localhost kernel: kernel logging (proc) stopped.
Jan 1 00:00:32 localhost kernel: Kernel log daemon terminating.
Jan 1 01:00:32 localhost exiting on signal 15
Jan 1 01:00:32 localhost syslogd 1.4.0: restart.
Jan 1 01:00:34 localhost disp: D recovery Responder v4 - Ready.
Jan 1 01:00:34 localhost algw: DHCP Server: the current addr pool is
Jan 1 01:00:34 localhost kernel: klogd 1.4.0, log source = /proc/kmsg
Jan 1 01:00:48 localhost db2sys: *** System started - Firewall's confi
Jan 1 01:00:48 localhost admin: Unit's software version is 2.0-168
Jan 1 01:01:41 localhost disp: temp IP=10.0.0.192, SN=255.255.255
Jan 1 01:01:42 localhost disp: D recovery Responder v4 - Ready.
Jan 1 01:02:18 localhost admin: Successful login (IP=10.0.0.19)
Jan 1 01:02:18 localhost admin: Unit's software version is 2.0-168
Jan 1 01:02:35 localhost admin: DB changes saved in flash
Jan 1 01:02:46 localhost admin: DB changes saved in flash
Jan 1 01:02:48 localhost disp: D recovery Responder v4 - Ready.
Jan 1 01:11:13 localhost admin: Successful login (IP=10.0.0.10)
Jan 1 01:11:43 localhost admin: Unit's software version is 2.0-168
Jan 1 01:12:04 localhost last message repeated 2 times
Jan 1 01:12:28 localhost admin: PPTP Server: address pool is now 10
Jan 1 01:12:29 localhost admin: DB changes saved in flash
Jan 1 01:12:59 localhost admin: DB changes saved in flash
Jan 1 01:13:01 localhost kernel: IKE: IKE --Start Phase : negotiation v
Jan 1 01:13:01 localhost kernel: IKE: IKE -- RemoteGateway ID: IPV4_
Jan 1 01:13:01 localhost kernel: IKE: IKE -- My ID: IPV4_ADDR--192.16
Jan 1 01:13:01 localhost kernel: IKE: IKE -- Authentication -- PR2GIAR
Jan 1 01:13:01 localhost kernel: IKE: IKE -- Transform --KEY_IKE
Jan 1 01:13:01 localhost kernel: IKE: IKE -- Encryption --AES_C3C
Jan 1 01:13:01 localhost kernel: IKE: IKE -- Hasf -- SHA_HASH
Jan 1 01:13:01 localhost kernel: IKE: IKE -- My ID: IPV4_ADDR--192.16
Jan 1 01:13:01 localhost kernel: IKE: IKE -- MainMode Exchange Selc
Jan 1 01:13:01 localhost kernel: IKE: IKE -- LifeType --SECONDS
Jan 1 01:13:01 localhost kernel: IKE: IKE -- LifeDuration -- 600
Jan 1 01:13:01 localhost kernel: IKE: IKE -- GroupDescription --MOODP
Jan 1 01:13:01 localhost kernel: IKE: IKE -- MainMode Exchange Selc
Jan 1 01:13:01 localhost kernel: IKE: IKE -- MainMode -- initiator sent
Jan 1 01:13:03 localhost kernel: IKE: IKE -- MainMode -- initiator recei
Jan 1 01:13:03 localhost kernel: IKE: IKE -- Proposal 1 -- protocol PRO
Jan 1 01:13:03 localhost kernel: IKE: IKE -- Transform 1 -- KEY_IKE, m
Jan 1 01:13:03 localhost kernel: IKE: IKE -- Encryption --AES_C3C

```

Normalizer and Database Loader

- A location/facility
- The degree of message severity
- A range of text string
- Or other qualifier

Message Formats and Fields parameters are identified by customer-specified names. These names are of reasonable length and may contain any character including blanks, accented characters such as ü and ß, and wide characters such as 個 and ١٥. Additionally, the CorreLog NDL allows the user to define output items directly from the UI. An output item specifies a connection to a database into which the data from Syslog messages is to be inserted.

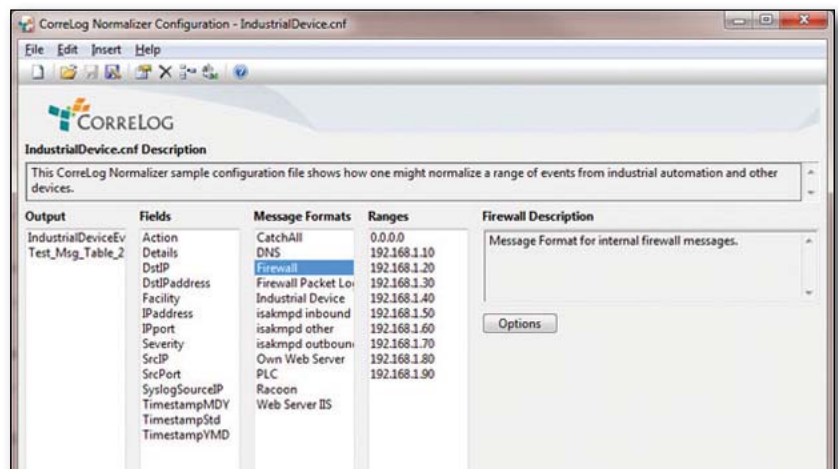
Parsing Data Using Qualifiers

Additionally for further filtering, a message format in CorreLog NDL may contain a “qualifier.” A qualifier specifies what data a syslog message must have a match for to be qualified, and subsequently parsed to the RDBMS. Qualifiers have, as parameters, a parse specification and a value to compare with the parsed data. If the comparison is true, then the qualifier is considered to pass, and the data is loaded into the RDBMS.

When a Syslog message is received within the IP address range, CorreLog NDL checks the qualifier associated with each corresponding message format until it finds one that passes, and then applies that message format’s processing instructions to the syslog message. NDL does not check for qualifiers in all messages, just the messages with an IP address range match. Then it proceeds to further qualify (or rule out) the data for inclusion (or exclusion) to the RDBMS.

Making Raw Message Data Meaningful

CorreLog continues to develop solutions that make raw message data meaningful for better intelligence about the security of enterprise IT environments. With Normalizer and Database Loader, CorreLog provides a better way to sort, arrange, and normalize syslog data for standardized reporting, leveraging existing attributes of syslog data, CorreLog has built a powerfully fast and efficient tool for arranging unstructured data into a relational database. The barriers for automating raw syslog data to a structured table for corporate reporting are now removed with CorreLog NDL.



In

About CorreLog, Inc.

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog is real-time, SIEM software that automatically identifies and responds to network attacks, suspicious behavior and policy violations. CorreLog collects, indexes and correlates user activity and event data to pinpoint security threats, allowing organizations to respond quickly to compliance violations, policy breaches, cyber attacks and insider threats. CorreLog provides auditing and forensic capabilities for organizations concerned with meeting SIEM requirements set forth by PCI DSS, HIPAA, SOX, FISMA, GLBA, NCUA, and others. Maximize the efficiency of existing compliance tools through CorreLog’s investigative prowess and detailed, automated compliance reporting. CorreLog markets its solutions directly and through partners. Visit www.correlog.com for more information.