



SYSLOG Analyzer is a core component of Cirries's Data Analysis in Real-Time (DART) solution. SYSLOG Analyzer captures all network SYSLOG records from network elements and stores them with indexing for flexible future searching and retrieval. It includes rules-based policies to flag network exceptions and execute a workflow to initiate resolution for critical issues in the network.

COLLECTS SYSLOGS FROM ALL ELEMENTS

DART SYSLOG Analyzer is built on a high-availability, scalable architecture providing a comprehensive, unified perspective on the network by collecting all SYSLOG records from all elements for integrated, centralized log analysis. Its capabilities include:

- Alert rules
- Troubleshooting
- Trends

ALERT RULES

By collecting SYSLOG records from all network elements and establishing a rules-based policy that the network operator defines, DART makes it possible to report alarms for network-wide exceptions that could not be reported by a single element.

TROUBLESHOOTING

DART's centralized SYSLOG collection helps identify and correct problems across multiple network types more quickly and easily to maximize network performance. The DART dashboard provides a dynamic chart of the Top 10 SYSLOG message generators, which assists with the rapid identification of an issue in the network and the cause of the issue.

TREND ANALYSIS

DART collects SYSLOG records from every network element, stores them for multiple months/years, and provides flexible reporting capability so that network operators can analyze years of network data trends to plan more effectively.

STORAGE

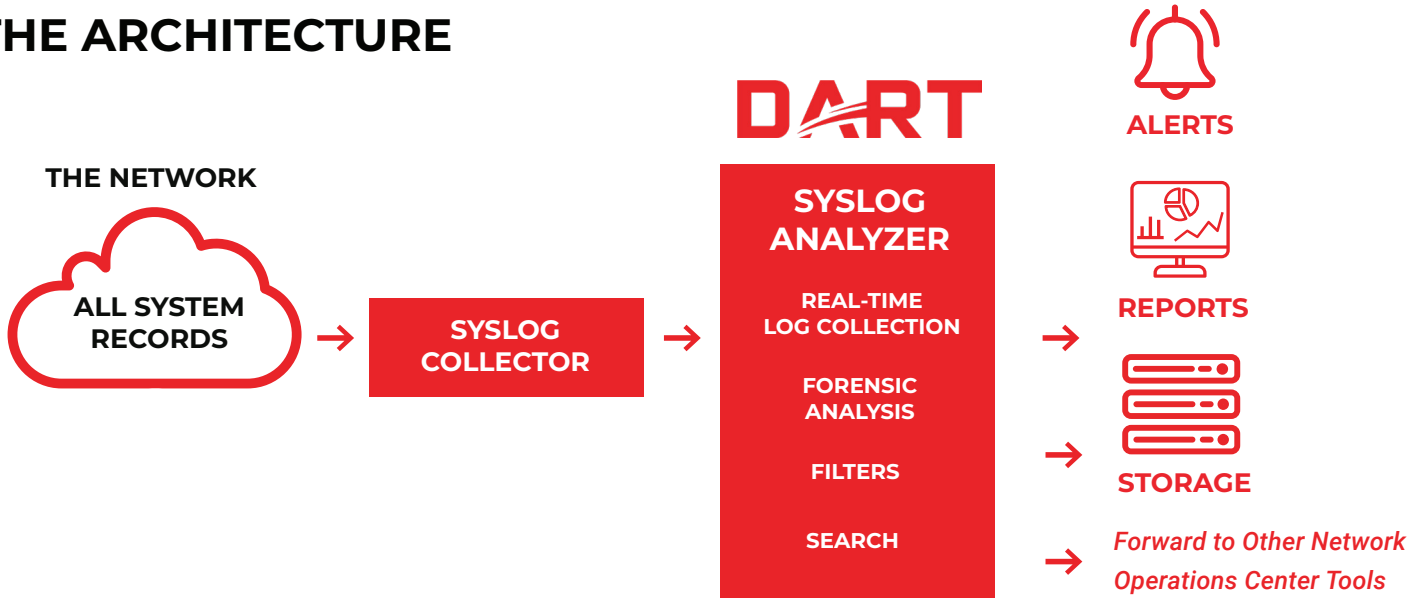
Every SYSLOG record is stored in raw and in an indexed format. Raw allows for compression for greater storage efficiency and indexed allows for rapid search capability.

BENEFITS

- Allows tight integration with other Network Operations Center (NOC) tools via REST API/ SNMP. Forwarding only the SYSLOG records which are critical for action
- Solutions up to 200K records per second
- Physical or virtual deployments
- Centralized monitoring, management, and analysis of each network element with an intuitive web console for real time view and rapid action.



THE ARCHITECTURE



DISCOVERS SYSTEM ANOMALIES

Recognizes anomalies and other spurious activity in the real-time SYSLOG stream using alert rules, then visualizes the incident to allow you to troubleshoot network performance issues.

ALERTS DASHBOARD

Customizable dashboard allows creation of policies and thresholds that generates alerts for defined conditions in the network.

WHY CIRRIES SYSLOG ANALYZER?

SYSLOG Analyzer provides -proactive problem detection, rapid resolution, and extremely granular traffic collection. This capability allows service providers and enterprises to optimize network performance, network planning, and routing policy planning. This solution minimizes the total cost of the network operations while maximizing network performance, capacity and reliability.

ABOUT CIRRIES

Cirries unleashes the full value and potential of any kind of network for full visibility in real-time with our high performance, extremely adaptable platform. For over fourteen years Cirries has provided data solutions to customers worldwide enabling increased network efficiency. The company is based in Richardson, Texas with offices in Bolivia, Mexico, and India.