Syslog Analyzer

ABOUT US

OSSera, Inc. is a global provider of Operational Support System (OSS) solutions for IT organizations, service planning, service operations, and network operations. OSSera's multi-threaded symmetrically distributed platform fully leverages modern multi-core server hardware to provide higher flexibility, reliability, and scalability for service and resource management solutions. OSSera's products support the TM Forum's suite of standards especially in the area of Service Management, Fault Management, Performance Management, Data Mediation, and Configuration Management.

info@ossera.com +1-916-290-9300 http://www.ossera.com

Member of the
TeleManagement Forum

Syslogs can provide a clear audit trail of information about user activity and the health of the network infrastructure

Problems and Challenges

Unlike, Fault Management systems which focus on the managed resources and their alert logs. IT organizations also must monitor and analyze Syslogs from Element Management Systems (EMS), servers, and Network Elements.

- **Security Management** - As a hybrid network grows and more vendors are brought into the responsibility of an OSS team. Each EMS must be maintained. Users have different levels of access and security becomes a major concern. EMS security becomes a high risk point of failure to managing critical resources and services.

- **Compliance** - One of the challenges involved with syslog logging, is the need to centrally aggregate and securely maintain the logs. Not protecting the events from being altered can be a major violation of compliance mandates. Syslog log data can be used as authentic evidence in the worst case legal scenario.

- **Effective Root Cause Analysis** - Due to the complexity of today's networks and end-to-end services, sometimes a large percentage of the problems may not be hardware issues but human error. To analyze the Root Cause to problems IT and Operations require visibility to not just faults and performance but also a mechanism for analyzing Syslog files coming from EMS servers.

- **Multi-Protocol** - Syslog data collection is required for not just SNMP but often for non-SNMP managed resources. This may require Telnet or database access. The files are often log files which must be processed and normalized for analysis.

- **Vendor-Neutral** - Syslog data collection needs to be vendor neutral so the Communication Service Provider (CSP) can be agile in selecting the vendor equipment deployed within hybrid networks.

- **Load** - Syslogs can generate several gigabytes of data per day. This information must be processed, stored, and analyzed efficiently. Many systems cannot handle the load requirements.

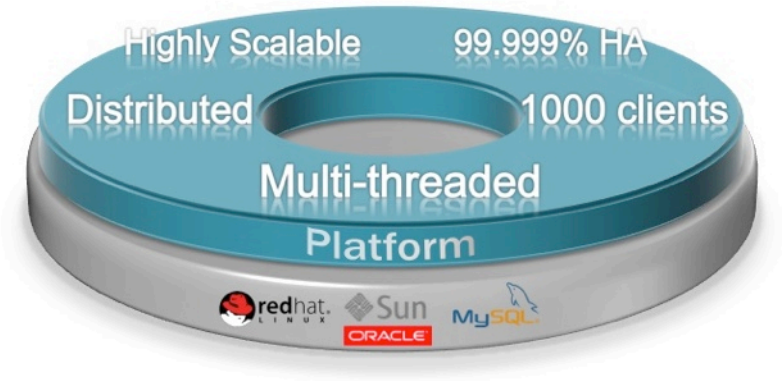
- **Availability** - Syslog data collection must be able to reach 99.999% availability and be completely fault tolerant. Unfortunately if any data is lost the OSS is blind to critical service availability issues.

- **Flexibility** - Syslog has been standardized over the years however some level of flexibility is still required to adapt to deviations. Too often probes, gateways, and adapters are difficult to modify and this is a must with ongoing changes in Syslog access. Therefore IT may be hampered with not being empowered to securely change and modify the adapters themselves. Costly services are required to build or modify an adapter. Syslog messages are sometimes not well defined or normalized. There is usually not a SNMP MIB defining the Syslog data structure. Furthermore messages may include unimportant notifications which must be filtered out.

If used effectively, syslogs can provide a clear audit trail of information about user activity and the health of the network infrastructure.

OSSera

OSSera's Syslog Analyzer is built upon OSSera's OSS Explorer Platform



Our Solution

Good security plans include regular monitoring of the network. Logs that can determine problems must be easy to find, process, analyze, and decipher. Without monitoring and forensic capabilities, network security teams and administrators can't distinguish security threats or operational problems from normal activity.

Some IT personnel within Communication Service Providers are slow on the draw to respond to system downtime issues, network failures and can completely miss vital security related activity. All of these challenges can be solved with log management automation tied to intelligent monitoring and analysis.

OSSera's Syslog Analyzer Application is built upon OSSera's OSS Explorer Platform.

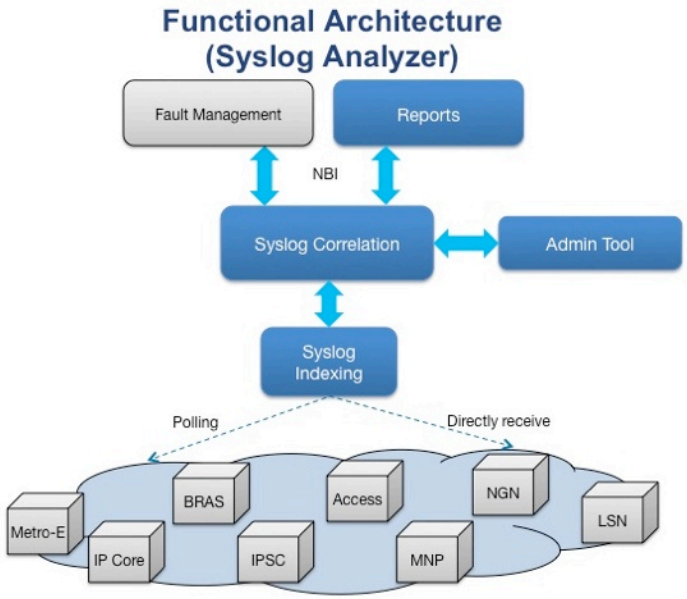
Therefore Syslog Analyzer is unique because of its multi-threaded symmetrically distributed architecture which can support a 99.999% highly available fault-tolerant solution. The platform has been designed from the ground up to be fault-tolerant due to its unique ability to distribute processing across a multi-server/multi-core virtualized environment and shift the load transparently based upon available processors and servers.

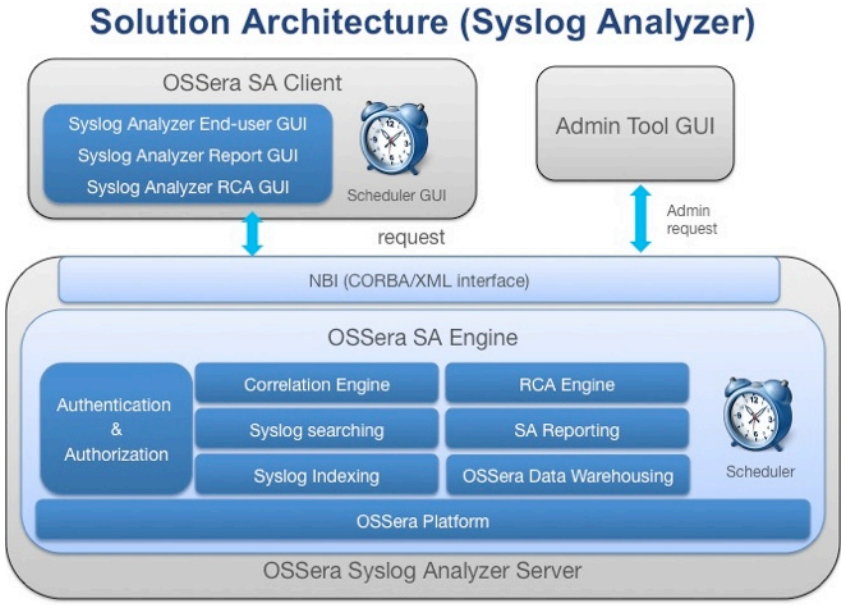
When two or more servers are used, the OSSera platform will distribute and load balance all processing of data, commands, and responses.

Syslog Analyzer is able to handle disaster recovery, event storms, and maintenance upgrades without skipping a beat. Never lose sight to critical logs that are critical for monitoring security, and network infrastructure.

Syslog Analyzer is able to handle log files from south bound feeds. The adapters provide flexibility in handling different syslog formats.

Furthermore any anomalies in the syslog files can be identified and alarms can be forwarded North Bound to other OSS systems like a Fault Management.





Syslog Analyzer Functional Overview

Functional Architecture

OSSera's Syslog Analyzer (SA) Functional architecture includes the following from the bottom up:

- Syslog Collection - leveraging the OSSera adapters to collect and normalize logs.
- Syslog Indexing - messages are indexed appropriately such as by facility and priority level.
- Syslog Correlation - Filtering, suppression, and correlation logic is applied where appropriate.
- Administration Tool - used to modify the above items.
- Reports - are used to run queries and analyze the indexed syslog information.
- North Bound Interface - such as integration to existing Fault Management system.

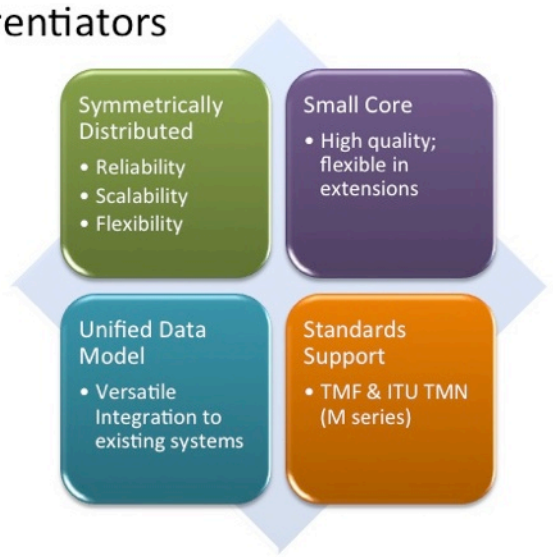
Solution Architecture

The Syslog Analyzer includes various components which are within the OSS Explorer platform. The platform is a flexible platform with:

- Authentication & Authorization - to control access to the SA solution.
- Correlation Engine - to correlate Syslog messages.
- Syslog Searching
- Syslog Indexing
- RCA Engine
- Syslog Analyzer Reporting - real-time, hourly, daily, weekly, monthly, and yearly scheduled reports.
- OSSera Data Warehousing
- North Bound Interface - supporting CORBA and XML
- Administrator Tool to configure the OSSera SA Engine.
- OSSera SA Client: Provides analysis functionality, reporting, and root cause analysis.

OSSera

Visualization, Architecture, Extensibility, and Usability



Technology and Architecture

OSSera's fundamental architecture can support:

Tier 1 Scalability:

- No loss of events or system performance during an "Event Storm"
- Over 1000 concurrent clients
- N-number of redundant servers

99.999% High Availability

OSSera servers can be configured in a symmetrically distributed configuration. The fully distributed and load balanced processes require no primary to secondary back-up configuration where operators lack visibility to critical network/ service monitoring functions. The runtime processes can be configured along with database clustering to meet 99.999% availability requirements. To summarize:

- Servers are policy enabled and managed.
- Each server can be configured with redundant layers of software components.
- All servers are load balanced and share the duty in serving clients.
- In the case of system failure, surviving servers will automatically redistribute the load to provide the highest system availability possible.

OSSera's Unified Services Frameworx architecture supports a complete Linux Redhat and MySQL deployment to lower your Total Cost of Ownership.

Also the software can run on your existing investment in Sun Oracle infrastructure fully leveraging any available hardware processing power.

NOTE: As a member of TMF, OSSera has adopted the TMF specifications on technologies and integration. A technology neutral approach has been followed. The software has been designed to be able to work on different platforms and adapt to technologies that are commonly used by the industry of today. As the technologies evolve, the software can be easily moved on to new technologies.

redhat. LINUX MySQL Sun ORACLE

info@ossera.com +1-916-290-9300 http://www.ossera.com