

# Event Enrichment & Correlation



Monolith – Delivering Next Generation Monitoring for Operations

## The Challenge

Technology infrastructures today are a continuously changing and evolving collection of devices, operating systems, servers, applications, routers, and switches. As the hub for modern business, these infrastructures must continually operate, providing optimal performance 24x7, 365 days a year in order to meet service provider and corporate guarantees of 99.999 percent uptime and availability.

Monitoring is an essential task within a complex technology environment. Monitoring efforts track the health and performance of the infrastructure as a whole, its individual elements, and their many interconnections. This is necessary in order to provide alerts to administrators and other network operations center (NOC) staff that failures have occurred in the performance chain.

The challenge for NOC staff however, lies in creating meaning from the torrent of alarms and other event information that are by-products of the monitoring effort. The reality facing NOC staff today is that event feeds are simply too large. This makes it impossible for IT managers and NOC staff to separate the wheat from the chaff. This becomes even more challenging over time because, as the technology infrastructure grows and becomes more complex, so grows the volume and heterogeneous mix of events. The effort of sifting through this event noise to zero in on the root cause of failure and identifying the business impact negatively affects team productivity and causes unnecessary downtime by lengthening mean time to recovery (MTTR) from a critical incident.

## Key Technology Benefits

- Increase productivity & accuracy of operations
- Eliminate unnecessary downtime by speeding Mean Time to Recovery (MTTR)
- Protect revenue and customer satisfaction levels
- Quickly assess impact of network failure on multiple fronts – dark fiber, customers, circuits, business services and service level agreements to enable more rapid and efficient communication in the event of a problem
- Pinpoint suspicious network behavior fast
- Boost NOC staff productivity and efficiency
- Focus attention on root cause events versus

Device	Event Type	Event Text	Count	First Occurred	Last Occurred
ibse	DeviceUpDown	Device Down	567	2008-05-21 10:30:00	2008-05-23 09:40:00
pdn	DeviceUpDown	Device Down	567	2008-05-21 10:30:00	2008-05-23 09:40:00
apollo	DeviceUpDown	Device Down	567	2008-05-21 10:30:00	2008-05-23 09:40:00

## The Solution

What is needed is a comprehensive platform that delivers advanced event enrichment & correlation. Event enrichment & correlation are key enablers of improved NOC performance. Together they deliver operational efficiency, automate and streamline work flow, utilize artificial intelligence to deliver a greater degree of accuracy around problem diagnosis, and reduce mean-time-to-response/repair (MTTR). The ultimate measure and impact of effective event enrichment and correlation is protection against loss of revenue and an increase in productivity and customer satisfaction.

A number of solutions exist in the market today professing to deliver correlation capabilities. The challenge is that these are point tools that address a subset of the needs required by leading edge operations groups. The challenges include:

- Significant financial investment
- Poorly integrated into the larger monitoring structure
- Point technology focused versus comprehensive in nature
- Difficult to implement, administer & maintain
- Lacking enrichment due to inability to leverage data from existing systems

If we can agree that the goal of the NOC / IT Operations is to reduce downtime while minimizing cost, then it is clear that the current method of performing manual correlation to attempt to tie together data points to identify root cause analysis is inadequate. Monolith Software addresses this challenge by delivering a major advancement in the arena of event enrichment & correlation.

# Monolith for Event Enrichment & Correlation

## Enrichment & Correlation Functions

### Collection Layer

- Listen / collect events
- Process Events
- Normalize events
- Enrichment — flat file, d/b, socket, SNMP, command line
- Rules-based correlation — priority scoring

### Database Layer

- Real-time event storage (RDBMS)
- Stored Procedures / Mechanizations — generic clear, expire, reapers
- De-duplication

### Post Collection Processing

- Connectors — generic, ticketing, PRCA
- Agents — time of day correlation; time of day existence or absence of events
- State-based auto-diagnostics, analysis, remediation
- Heartbeating — time/interval event existence or absence
- Stacked events — i.e. clustered servers
- Disparate events — correlation of disparate events to generate meta event
- Event thresholding — X in Y correlation
- PRCA (Probable Root Cause Analysis) — utilizes Monolith's HSE (Hierarchy Storage Engine) to provide automatic correlation of any hierarchy definition

## Event Enrichment & Correlation Introduction

Event enrichment & correlation has historically been highly sought after, yet difficult to achieve for most organizations. This subset of the overall technology monitoring and management realm has clearly proven to be the most difficult for software companies to deliver upon and becomes increasingly difficult due to the many different types and methods of correlation arising to meet ever expanding customer needs. The following sections will delineate the different methods and explain Monolith's ability to deliver in each area.

## Collection Layer Enrichment & Correlation Capabilities

Correlation can only occur if event aggregation is possible. This occurs at what we define as the collection layer. Monolith makes this possible via our vast array of aggregators. Aggregators allow us to receive any event no matter what underlying event type or format (e.g. trap, syslog, email, flat file, TL1). At the collection layer Monolith leverages its aggregator based rules logic to listen, collect, process, enrich and normalize events. Because this occurs pre-insertion to the database, the speed and granularity by which organizations can perform filtering, enrichment and priority-scoring is extensive and completely customizable. It is important to note that Monolith's aggregators can not only perform enrichment via hash files in the rules logic itself, but can also jump outside the rules engine to perform correlation or custom direct access lookups to enrich event data on the fly.

## Database Layer Enrichment & Correlation Capabilities

Monolith Software leverages the power of the database to maximize and automate on the fly as well as pre and post processing enrichment and correlation within your network environment. Real time event storage using Monolith's real-time RMDBS event manager provides a higher level of performance than competitive marketplace solutions that rely on memory-based storage and database locking every five minutes. NOC staff can store and mechanize database procedures for **generic clear, expire and reapers** in addition to custom mechanization to match defined business rules. Monolith also helps to reduce duplication of event data based on an automated monitoring of event re-occurrence in the database. The placement of a **counter** in the event engine gives NOC staff the ability to suppress repeat notifications and eliminate unnecessary crowding of information on the event screen.

## Post Collection Processing for Enrichment & Correlation

Monolith offers a wide variety of post-processing correlation capabilities via its **Watcher** and **CAPE** (Custom Action Policy Engine) components. **Watcher** allows organizations easily built custom correlation policies to meet a wide variety of correlation needs including: **event stacking** to extrapolate network behavior based on the similar/duplicate or related events (i.e. in a clustered server scenario);

### Event Stacking

Source	Source Port	Destination	Destination Port	Event Text	Last Occurred	Count
64.55.2.232	80	172.16.10.1	9101	Successful Attack through Firewall Detected by IDS	2006-10-08 08:30:45	1
64.55.2.232	80	172.16.10.1	9101	Firewall Accept Message	2006-10-08 08:30:45	1
64.55.2.232	80	172.16.10.1	9101	IDS Attack	2006-10-08 08:30:45	1

correlation of **disparate events**, seemingly unrelated events that happen together actually indicate a specific meaning or implication to the business;

### Disparate Events

Device	Event Type	Event Text	Count	First Occurred	Last Occurred
EMAIL	EmailSvcDown	Email Service Down	1	2006-10-08 08:30:45	2006-10-08 08:30:45
nodeb	DeviceUpDown	Device Down	1	2006-10-08 08:30:45	2006-10-08 08:30:45
nodea	DeviceUpDown	Device Down	1	2006-10-08 08:30:45	2006-10-08 08:30:45

**event thresholding** (classic X in Y) monitors for event occurrences over a specific timeframe, which may identify suspicious behavior or intermittent problems like flapping interfaces; and **heartbeating** monitors the existence or absence of events over a specified time or interval.

### Heartbeating

Device	Event Type	Event Text	Count	First Occurred	Last Occurred
sourcea	Watcher - No Events	No Events for 15 minutes from SourceA	1	2006-10-08 08:30:45	2006-10-08 08:30:45

# Monolith for Event Enrichment & Correlation

## Post Collection Processing for Enrichment & Correlation (continued)

State based auto diagnostics, analysis and remediation allow NOC teams to improve the productivity of their operations and reduce response times through automated policy actions that are triggered by the occurrence of specific events versus relying on the manual process to be initiated by human operators. Monolith Software allows business rules and states to be flexibly defined within the database to align correlation efforts to standard operating procedures and automate response to a variety of events.

Monolith's **CAPE** (Custom Action Policy Engine) provides an excellent example of conducting post-collection processing for enrichment and correlation outside of the database environment. Network staff can mix and match **connectors** (generic, ticketing, probable root cause analysis) and **agents** (time of day correlation, time of day existence or absence of events) and use any internal or external datasets to create their own custom correlation models.

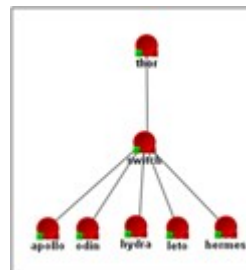
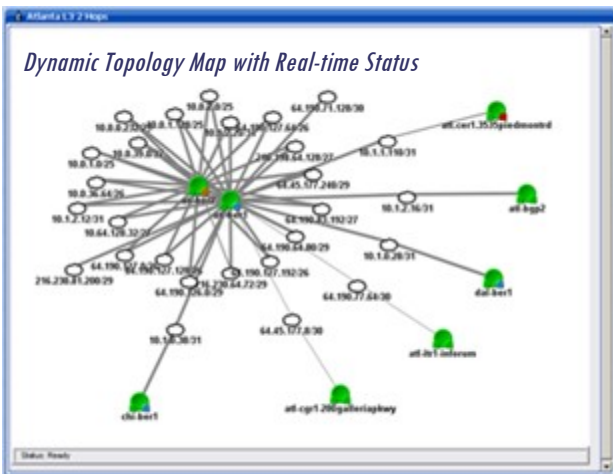
The below screen shot shows the result of a CAPE policy for 'High CPU' events. The policy works as follows:

*event is received by Event Manager → triggers a CAPE policy for "High CPU" events → initiates the CAPE action (in this case, a query to identify the process consuming the most memory on the server) → enriches the event summary in Event Manager with the offending process name*

Device	Event Type	Event Text	Count	First Occurred	Last Occurred
testing-prod	DeviceDown	ICMP Ping Failure - Device Availability	1	2009-02-24 11:44:59	2009-02-24 11:44:59
testing-hydra	DeviceDown	ICMP Ping Failure - Device Availability	1	2009-02-24 11:44:59	2009-02-24 11:44:59
testing-hydra	MemHigh	Memory Used Util Greater Than 90% : Device Utilization : Crossed Utilization Threshold (Rate=3) (99....	1	2009-02-24 11:44:59	2009-02-24 11:44:59
lito	CPUHigh	CPU Util Greater Than 90% : Device Value : Crossed Value Threshold (Rate=3) (100.0 / 90)- CAPE High...	1	2009-02-24 11:44:59	2009-02-24 11:44:59
hermes	MemHigh	CPU Util Greater Than 90% : Device Value : Crossed Value Threshold (Rate=3) (100.0 / 90)- CAPE HighestProc=[services.exe]	1	2009-02-24 11:44:59	2009-02-24 11:44:59
odin	MemHigh	Memory Used Util Greater Than 90% : Device Utilization : Crossed Utilization Threshold (Rate=3) (95....	1	2009-02-24 11:44:59	2009-02-24 11:44:59
lito	CPUHigh	CPU Util Greater Than 75% : Device Value : Crossed Value Threshold (Rate=3) (100.0 / 75)	1	2009-02-24 11:44:59	2009-02-24 11:44:59

A final post-processing event enrichment & correlation function can be found via Monolith's **PRCA** (Probable Root Cause Analysis) capabilities. Monolith's PRCA engine allows organizations to perform advanced correlation of incidents in order to more rapidly isolate the root cause issue and eliminate the associated noise. PRCA benefits:

- Downstream suppression of events
- Auto-correlation of parent/child relationships
- IP-based topology correlation
- Support for customer specific custom correlation models
- Dramatic reduction in troubleshooting time and effort



Tree shows dependency model; event list below shows parent events in red and symptomatic events in purple

Device	Event Type	Event Text	Count	First Occurred	Last Occurred
lito	DeviceDown	Device Down	567	2008-05-21 10:30:00	2008-05-21 09:40:00
odin	DeviceDown	Device Down	567	2008-05-21 10:30:00	2008-05-21 09:40:00
apollo	DeviceDown	Device Down	567	2008-05-21 10:30:00	2008-05-21 09:40:00

**About Monolith Software** – Monolith Software is the leading provider of operationally focused technology management software for network operations centers (NOCs) delivering the only fully integrated platform for managing fault, availability and performance on the market today. Service providers and IT organizations seeking to increase operational efficiency and drive down costs while maintaining 99.999 percent uptime and availability turn to Monolith Software's next generation management and monitoring solution for real time insight into the health, performance and availability of mission critical systems and applications.