

Monolith for Systems Monitoring



Monolith – Delivering Next Generation Monitoring for Operations

The Challenge

Systems monitoring is a key component of an organization's enterprise technology monitoring and management strategy and a key enabler in the delivery of business services. Until now, monitoring solutions have fallen short of the task, with restrictive approaches and limited monitoring capabilities. Prior to Monolith, a large financial institution was using multiple open source monitoring software for linux servers, Microsoft MOM for Windows, HP OVO for HP's unix servers, and Oracle OEM for Solaris servers running Oracle databases.

This siloed and incompatible monitoring approach, however, fails to represent the comprehensive nature of the services and applications delivered by IT today. It is also time consuming, inefficient and expensive. More importantly, this approach prevented the financial institution from developing a consolidated monitoring dashboard that their NOC could leverage to monitor their mission critical applications and services.

When managing large number of diverse systems, it is imperative that a systems monitoring application enable an IT organization to do more with less. While monitoring needs may vary across the various systems types, there are a great many commonalities and tasks that can be standardized. Organizations also seek to be more proactive in monitoring and measuring service levels across the entire application and service hierarchy. To meet this goal, organizations must deploy a systems monitoring solution that provides a consolidated view delivering real time IT dashboards, service level management, consolidation of faults, a centralized metric warehouse and a topology/hierarchy component structure for managing the interrelationships between assets. Common systems monitoring functions required by organizations today include:

- **Monitoring System Availability** – This functionality monitors the overall condition of the system. Is the system up? Can system administrators talk to it, ping it, run a command against it? Are the specific services running on the system responding and performing? Detecting system availability ranges from whether the system is up to determining whether its sub-systems are performing properly.
- **Monitoring System Resource Utilization** – Applications require certain system resources for them to run correctly. This can include a specific amount of CPU or I/O bandwidth, the number of sockets, threads, or message segments allocated to the application. Most operating systems have a limited set of these resources, so monitoring resource use is important.
- **Monitoring System Performance** – Monitoring the performance of the system is a proactive method of eliminating problems before they impact service delivery, and organizations should watch specifically for CPU, memory and disk I/O bottlenecks. A good monitoring solution should help identify baselines of normal behavior, provide forward looking trending for capacity planning, and support threshold definitions for proactive notification of issues.
- **Monitoring System Logs** – Monitoring of system logs or events is a critical aspect of overall systems monitoring. Systems will communicate if experiencing issues or problems, but a facility must exist to receive and process these messages. Each of the areas described above all tie into the monitoring of system logs. Because of the high number of things that can go wrong on a system there is a plethora of alarm messages that need to be processed. A good systems monitoring solution should be scalable, easy to filter, perform de-duplication and correlation.

The Solution – Unified and Comprehensive Systems Monitoring

In today's complex environments, companies need a comprehensive and unified monitoring solution that offers multiple methods for systems monitoring that goes beyond CPU, disk and memory. It should put no platform limitations on your organizations monitoring abilities as well as provide auto deployment, roll up, consolidation, dashboarding and integrated alerts.

Competing tools are built on aged and proprietary architecture which monitor only a sub set of environments, face scalability and platform limitations and then force you to align to their model. Most of all, the competing tools are difficult and expensive to maintain.

Monolith Software's solution for systems monitoring is built on simpler standards and protocols which allow organizations to reduce administration and maintenance costs while delivering improved and broader monitoring capabilities. Monolith Software recognizes the need for organizations to have an end to end solution for systems monitoring and our comprehensive capabilities meet this need to an exacting level. Monolith views systems monitoring in three distinct ways:

Metric Management for
Systems

Systems Dashboarding &
Service Level Management

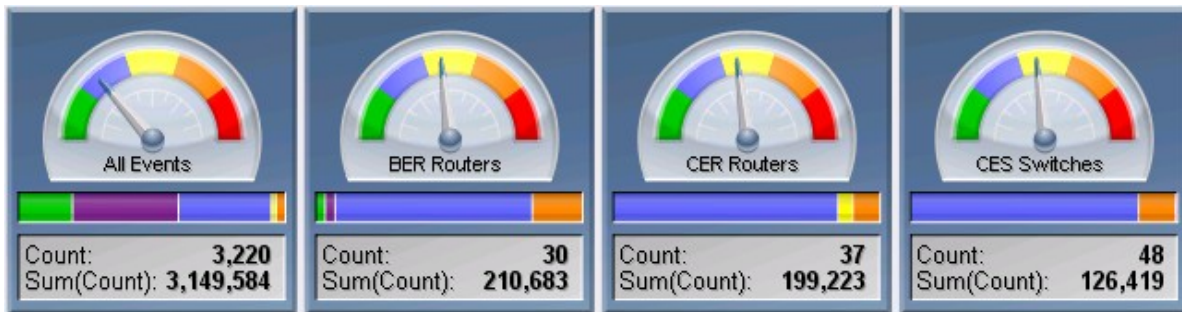
Event Management for
Systems

Monolith for Systems Monitoring

Event Management for Systems

Monolith offers an industry leading solution for event collection and aggregation via its Event Manager, a highly scalable event processing, filtering, correlation and presentation system. Event Manager easily receives events from any system in any format (trap, syslog, NT event log, TLI, ASCII message) and allows these disparate event types to come together within a single event management system, reducing the multiple panes of glass effect so often seen in operations centers. Monolith's out of the box de-duplication feature summarizes 'like' events within a single row in the event list rather than repeatedly listing them as is done in HP OpenView NNM, and reduces event load within the system by an order of magnitude. Monolith's completely customizable rules engine enables event processing which allows administrator to utilize standard, pure pearl syntax - a powerful language common to system administrators -- to flexibly control the logic of how various event flows are handled.

- **Event Filtering** – Monolith provides easy to use and highly granular filtering of events (system messages). Rather than viewing all events in one big event bucket, users can easily create event filters that meet the needs of a specific user or group. Monolith provides many different filtering options to users - event filters, quick filter, load filter and forensic search.



- **Broker Technology** – Monolith is built to support easy, yet secure, communications between various components. The platform's powerful broker technology provides a centralized administration interface for the complete Monolith system. All components - aggregators, collectors, connectors - can be controlled from this central interface as well as scheduling, start, stop and run features. Communication occurs over two user definable ports making the system firewall and DMZ friendly.
- **Event Correlation** – Monolith's systems management solution offers robust event correlation capabilities including basic de-duplication, rules based correlation, time & count based correlation, X & Y correlation, compound event or disparate event correlation, state based correlation and topology based hierarchy correlation. The key behind Monolith's correlation engine is its extensive flexibility, allowing the platform to meet the various and differing correlation needs of organizations.

Device	Event Type	Event Text	Count	First Occurred	Last Occurred
testing-odin	DeviceUpDown	ICMP Ping Failure : Device Availability	1	2009-02-24 11:44:59	2009-02-24 11:44:59
testing-hydra	DeviceUpDown	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) (99.0 / 90)	1	2009-02-24 11:44:59	2009-02-24 11:44:59
leto	CPUHigh	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
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) (95.0 / 90)	1	2009-02-24 11:44:59	2009-02-24 11:44:59
leto	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

- **Northbound Event Feeds and Notification** – Most organizations own multiple systems to monitor their complex environment. Monolith can either function as a primary event console or it can forward events northbound to other systems via trap, syslog or email. Additionally Monolith has an integrated escalation and notification engine to not only alert the correct personnel when an incident occurs, but also to track mean-time-to-resolution and mean-time-to-repair metrics for incidents.

Features

- Delivers standard system monitoring capabilities (CPU, disk, memory) with advanced features for discovery, availability (process, service and port checks), performance utilization, and fault data (traps, Syslogs, NT event logs)
- Flexible monitoring approach - broad support for agent-based, agentless or third party agents including MS MOM, Zabbix, Hyperic, Net-SNMP, Microsoft/Informant, Nagios/NetSaint
- Flexible Top-N reporting allows for display of top offenders by device group or metric type, by location (i.e. Data Center), by application or by customer
- Easily discover and add new devices / systems

Benefits

- Enhanced predictive, diagnostic and resolution capabilities covering the entire systems environment surrounding a critical application or business service
- Supports a broad range of monitoring approaches for maximum flexibility and customer adaptability
- Meet 99.999 percent availability and uptime tolerances and SLAs for applications and business services
- Improve customer service by preventing system environment and resulting application failures before they occur
- Pinpoint and categorize top offenders with high degrees of accuracy
- Easy to use and quick to deploy
- Reduced administrative burden

Metric Management for Systems

Monolith offers customers the highest degree of flexibility available to meet the varying needs of organizations today. One of the key functions of systems monitoring is the collection and aggregation of performance related information and metrics from the servers themselves. Monolith offers clients a number of ways to collect and aggregate metrics.

- **Agentless** — Monolith's Metric Manager can utilize an agentless approach using SNMP or WMI polling of performance information from the server itself. Much information can be polled including CPU utilization, memory utilization, disk space utilization, process monitoring, and thread counts.
- **Agent-based** — Monolith offers its own host agent for monitoring information on the server, providing significant flexibility for systems administrators. Administrators can run local queries on the host itself, and the agent packages up this information and pushes it through Monolith's broker communication path back to the desired Monolith module - Metric Manager for metrics and Event Manager for system messages.
- **Third Party Systems** — Minimizing configuration points and interfaces and making key information available to SLM calculations and real-time dashboards is a benefit to any organization. Monolith allows organizations to easily integrate third party information into the Monolith system through its Metric Manager collection engine. Highly flexible collectors allow organizations to take in third party metric data. For instance, an organization using SNMP to collect Linux system performance metrics and a Monolith MOM/SCOM collector can take in Windows server performance metrics to provide a consistent graphing interface, a single thresh-holding engine, and consolidated Top-N reporting.

A key enabler of Monolith's collection layers is the system's simple and flexible facility to integrate/poll metric data into the Monolith platform. If an organization prefers agent-based monitoring, has firewall restrictions that prevent it from using an agent less monitoring solution, or has an existing investment in third-party monitoring tools, Monolith's flexible platform design can accommodate that need and supports all available monitoring methods. This allows organizations to select an agent approach that works best for the environment, and for its customers. And Monolith integrates with most third-party agents including Microsoft Operations Manager, Zabbix, Hyperic, Net-SNMP, Microsoft/Informant, and Nagios/NetSaint.

Additional benefits behind Monolith's Metric Manager solution for systems management include:

- **Automatic Discovery and Configuration** — With ever-changing and rapidly expanding systems environments, most service providers find the administration of their monitoring platform a significant challenge. Most monitoring solutions require that an administrator manually add and delete devices from coverage, and many organizations dedicate a full-time headcount simply to the administration task. Monolith Software's automatic discovery and configuration of devices allows our systems monitoring solution to search the environment, detect new devices, and instantly begin monitoring their health and performance. Not only does this improve the quality of an organization's monitoring coverage - it also dramatically cuts the administration burden. Many of our clients have been able to cut administration time by two-thirds, and have reallocated that valuable headcount to other revenue-generating tasks.
- **Top-N Reporting** — Forewarned is forearmed in preventing future failures. Whether an organization is seeking detailed information on potential trouble spots in a system environment, or experiencing a critical system failure and needing to troubleshoot, Monolith Software's Top-N reporting capability allows IT operations groups to quickly and precisely zero in on top offenders. Monolith can help predict and prevent potential failures, as well as find and fix problems when they occur. Monolith's flexible TopN reports provide system administrators with the ability to view a defined number of offenders based on device category, application or business service, by data center or other geographic location, or by metric class.
- **Device Overview** — Group Availability is presented dynamically within Metric Manager. Organizations can easily create their own device groups (e.g. Windows Servers, Linux Servers) that not only present Top-N overviews per group as described above, but that also provide dynamic availability metrics for each group with full drill down support to determine the problematic hosts or devices. This is particularly useful for providing at-a-glance group availability statistics in large scale environments.

Advantages of a Single Code Base for Holistic Monitoring

The usefulness of any monitoring system is limited by the ability of your personnel to tweak it to the environment. Packages requiring high complexity for making changes such as complex API's, Java Script based extension, proprietary scripting languages like prolog or Netcool rules make the system either wildly expensive by requiring outside consultants to make changes or quickly stagnant.

The enterprise systems management market is ripe for new competitors, such as Monolith, that utilize Web 2.0 style, integrated architectures and that utilize an open platform and scripting language versus trying to forsee each and every need that organizations may have. The goal is to enable the users of the systems monitoring software; not to limit changes to only those that the software vendor can provide.

Monolith delivers the benefits of the Big Four, but at 20% the cost, without millions of lines of Java code, without an army of consultants, and without a different interface for each module.

"Scripting languages beat Java in the area of monitoring hands down and if a monitoring product can be extended via a scripting language this should be considered to be a strategic advantage -- an advantage that is worth fighting for."

Dr. Nikolai Bezroukov, Softpanorama

Monolith for Systems Monitoring

Dashboarding and Service Level Management

Monolith offers excellent capabilities in availability, performance and event management of systems which very few companies can match. When organizations also consider the need to deliver real-time IT or systems dashboards and service level management they will find that Monolith's capabilities are unmatched in the industry today. Systems managers at large organizations are being tasked with delivering real-time dashboards and service level management metrics for their vast array of systems. Until now, this capability has been unavailable in the marketplace.

- **Real-Time Dashboards** — Monolith's real-time dashboards are a crucial component of our systems management solution is our real-time dashboards. The value of systems management is typically directly correlated with the size of the environment to be managed, and systems managers and administrators have long desired the ability to create specific and real-time dashboards that reflect the performance of their server environments. Monolith offers the industry's most advanced real-time dashboard solution available today, presenting any mixture of availability, fault, performance or metric information in a true real-time dashboard view allowing IT Operations groups unprecedented views and insight into the management of critical systems and their performance in the business.
- **Service Level Management** — Monolith's Service Level Manager presents a true breakthrough in SLA and complex service hierarchy management. Managers historically have either forgone providing SLA metrics for complex service trees or have performed complex and time consuming manual calculations to derive SLA values. Monolith completely automates the service level management process allowing IT professionals to define and track in real-time the performance of any service structure.

Dashboard Gallery

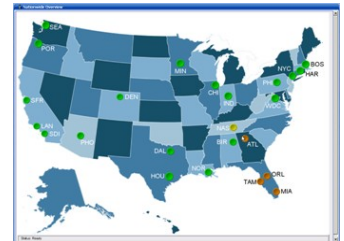
Button



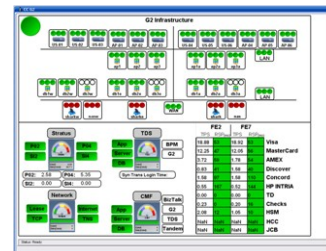
Server Group



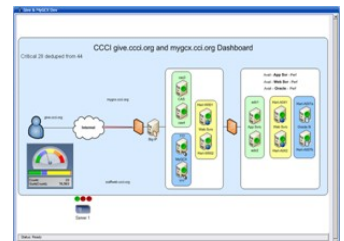
Geographic



Application #1

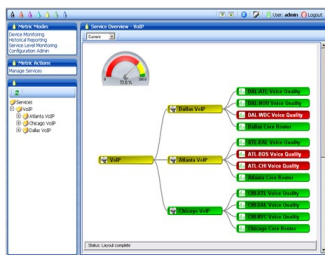


Application #2



SLM Gallery

Service Overview



Service History



SLM Gauge



About Monolith Software

Monolith Software is the industry's first, and only, unified IT infrastructure management software. Monolith offers a comprehensive, fully integrated solution that provides one consistent rules engine for data acquisition, one unified data warehouse allowing unprecedented access to decision-enabling data, and one, consolidated multi-tenant interface for expanding access to deeper business intelligence. Accessible through real-time dashboarding, this unique, unified approach streamlines and enhances fault, availability, performance, correlation, discovery and topology mapping. The result is a simplified process for SLA management and capturing network KPIs. Comprehensive granular visibility, never before available by using disparate legacy tools, increases operational efficiency and allows for enhanced customer intimacy.