Proactive Monitoring IT Infrastructures

John Telford
JohnTelford.com LLC
13508 NW Springville Road - Portland, Oregon
503.432.8152 - john@johntelford.com - www.johntelford.com

Table of Contents

Proactive Monitoring

Today's IT infrastructures are more dynamic than ever and are increasingly complex, with many different types of technologies, business critical applications, mobile computing, virtualization, expanding networks, cloud technology, etc... It's become complex groups of silos and interconnected technologies.

The growing complexity of IT infrastructures is generating more device event information buried in log files, and making troubleshooting more difficult.

Today's cost-cutting IT organizations are doing more with a smaller workforce, and having less time to fix problems. Upset users usually call the help desk complaining about business services they need to get their jobs done. They know or care little about IT infrastructures, and have little tolerance for downtime and mistakes.

Proactive monitoring collects event and performance data from IT infrastructure devices. It is only as good as the data it collects. The more information collected, the more useful it becomes. The data provides a wealth of information for troubleshooting. Proactive monitoring alerts IT staff to events when they happen, and helps to quickly evaluate and deal with problems before they effect customers, users, and services.

Proactive monitoring is becoming increasingly important. As complexity grows, it is becoming more difficult to put together solutions that meet the monitoring needs of IT organizations today, and can grow with tomorrows IT infrastructures.

Without monitoring, one cannot know the state of IT infrastructures. The British mathematical physicist and engineer Lord Kelvin invented the Kelvin Scale that measures the ultimate extremes of hot and cold. He is quoted saying "**To measure is to know**" and "**If you cannot measure it, you cannot improve it.**" This sums up the importance of proactively monitoring IT infrastructures.

Infrastructure Stack

Information technology is the fastest changing industry ever. Some technologies are obsolete within a year, while others may be relevant for a few more years. Disruptive technologies such as network, storage, and platform virtualization, cloud, and mobility, are rapidly changing the computing landscape.

The evolving IT infrastructure stacks look something like Figure 1. Proactive monitoring is a key layer in the IT infrastructure stack.

Pieces in the stack are changing at their own rate, as new and improved technologies are being offered in the market place by the information technology industry. An example is how traditional networks, storage, and platforms are being virtualized, and are evolving into the software defined data center.

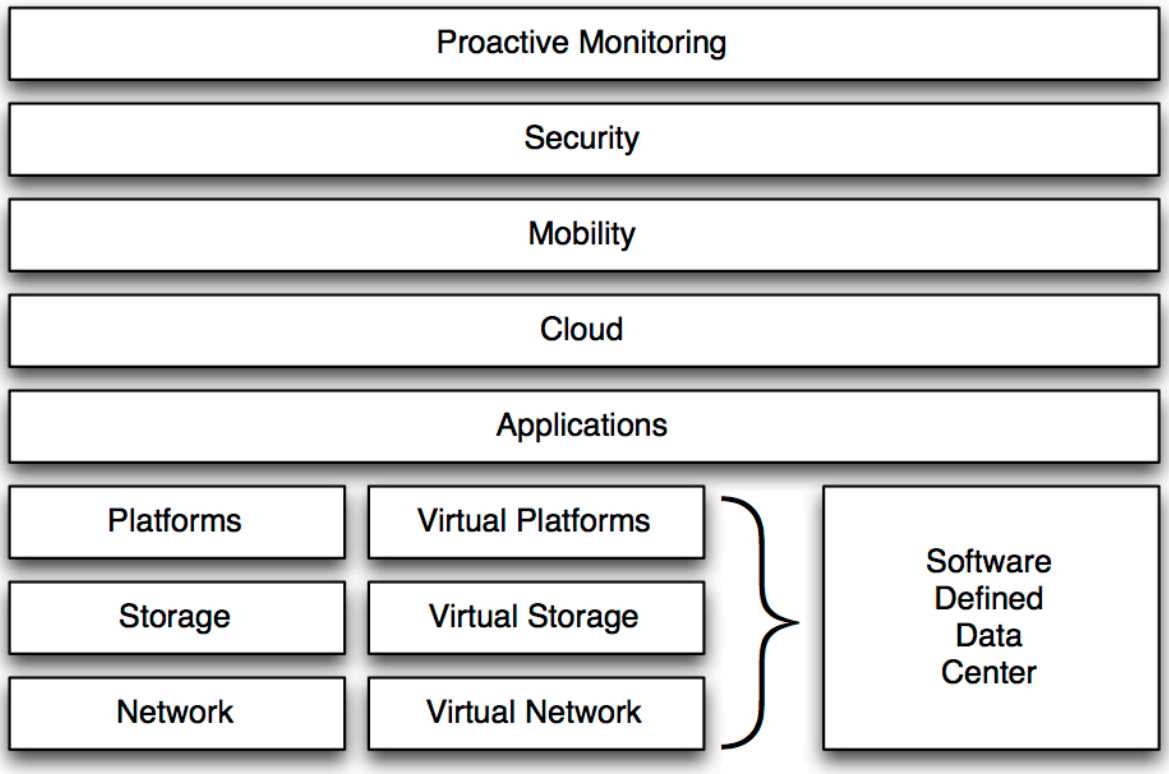

Figure 1 - IT Infrastructure Stack

Proactive monitoring has a formable challenge of keeping up with the ever changing IT infrastructure stacks. It is vital that it does because each change in stack technology could make troubleshooting much more difficult.

Reactive vs Proactive

Reactive.
When something goes wrong, the reactive approach is to go into fire fight mode, and try to get problems under control and back to a normal as quickly as possible, by "winging it" based on knowledge and experience.

The reactive approach does little automated IT infrastructure monitoring for potential risks. The IT staff is usually alerted about problems by irate users contacting the help desk. Troubleshooting begins by talking with others, and then logging on to suspected devices and digging through log files looking for clues. Finding and correlating significant events from different devices log files is difficult and time-consuming.

This manual reactive approach of finding and fixing problems is at odds with today's world of doing more with a smaller workforce, and having less time to fix problems. The more complex the infrastructure grows, the more time it takes to figure out what the problems are and fixing them.

Proactive.
The goal of the proactive monitoring is to deal with issues, problems, and attacks, before they effect customers, users, and services. This is done by monitoring the IT infrastructure and automated alerting IT staff of failures, significant events, and potential risks, when they happen.

Troubleshooting is based on facts from real data about IT infrastructure. Figuring out problems and fixing them by being proactive, is much quicker than reactive fire fighting.

Proactive Monitoring Levels
- Overview -

Proactive monitoring collects event and performance data from IT infrastructure devices. The data provides a wealth of information for troubleshooting. Proactive monitoring alerts IT staff to potential problems, and helps to quickly evaluate and deal with them before they effect users. Users care little about the IT infrastructure. They care about the business services it delivers.

Broadly speaking, there are four levels of proactive monitoring:

- Do It Yourself
- Traditional
- Analytics
- Unified

The capital cost for the different levels of proactive monitoring ranges from nothing for Do It Yourself, to $20K++ for Unified. Each level adds automation features. The more automation there is, the less time is spent finding problems. Unfortunate for troubleshooters, none of the levels fix problems.

Events.
Most IT infrastructure devices detect events, writes them to local log files, and sends them to a syslog server. Logs are the heart and soul of proactive monitoring. The more log sources, the better.

Devices send significant events directly to a SNMP (Simple Network Management Protocol) trap receiver. The trap receiver may be a part of the syslog server. The syslog server is configured to alert IT staff to events of interest.

Network equipment such as routers, switches, and other devices support

sending syslog and SNMP traps to a syslog server or SNMP trap receiver.

Linux and UNIX servers store events in local log files, and support sending them to a syslog server or SNMP trap receiver.

Windows servers store events in local log files. Third party agents installed on Windows servers watch local event logs, transform events into syslog format, and sends them to a syslog server. Windows servers can also send significant events directly to a SNMP trap receiver.

Performance Metrics.
IT infrastructure devices use internal counters to accumulate performance data. It is accessed using SNMP or WMI (Windows Management Instrumentation) protocols to poll performance counters.

Nagios and Paessler PRTG Network Monitor, Windows Perfmon are examples of performance metrics applications.

Proactive Monitoring Levels
- Do It Yourself -

The DIY method is not proactive monitoring. It is a manual process triggered by irate users contacting the help desk.

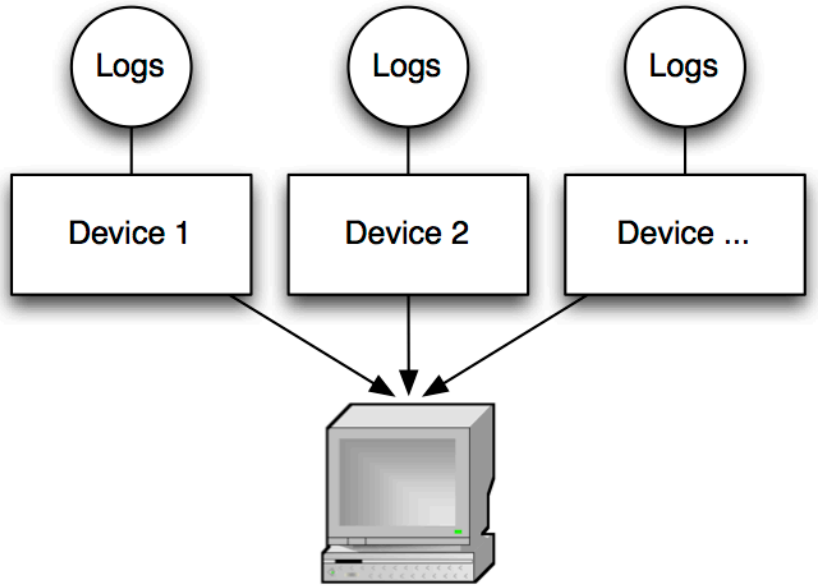

Figure 2 - Do It Yourself

Looking for clues about problems users are reporting is done by manually logging in to suspected devices one by one, and choosing which log files to dig through. Reading logs requires knowledge about systems and applications. Many log messages do not follow standards, and each vendors system may record logs differently. Some log files are human-readable while others consist of arcane message codes.

Manually finding and correlating significant events this way is difficult, time-consuming, and becomes more so as the complexity of the IT infrastructure

grows.

Proactive Monitoring Levels
- Traditional -

Traditional proactive monitoring relies on performance metrics, syslogs and SNMP traps. A syslog server and SNMP trap receiver collect data as shown in Figure 3.

Performance metrics applications use SNMP or WMI protocols to poll IT infrastructure devices performance counters. Events are sent to the syslog server when performance thresholds have been crossed or events of interest are detected. Significant events are sent directly to the SNMP trap receiver.

The syslog server configuration rules send alerts to IT staff when events of interest are detected. The configuration rules also filter and aggregate events of interest to local syslog server log files. The remaining events are discarded.

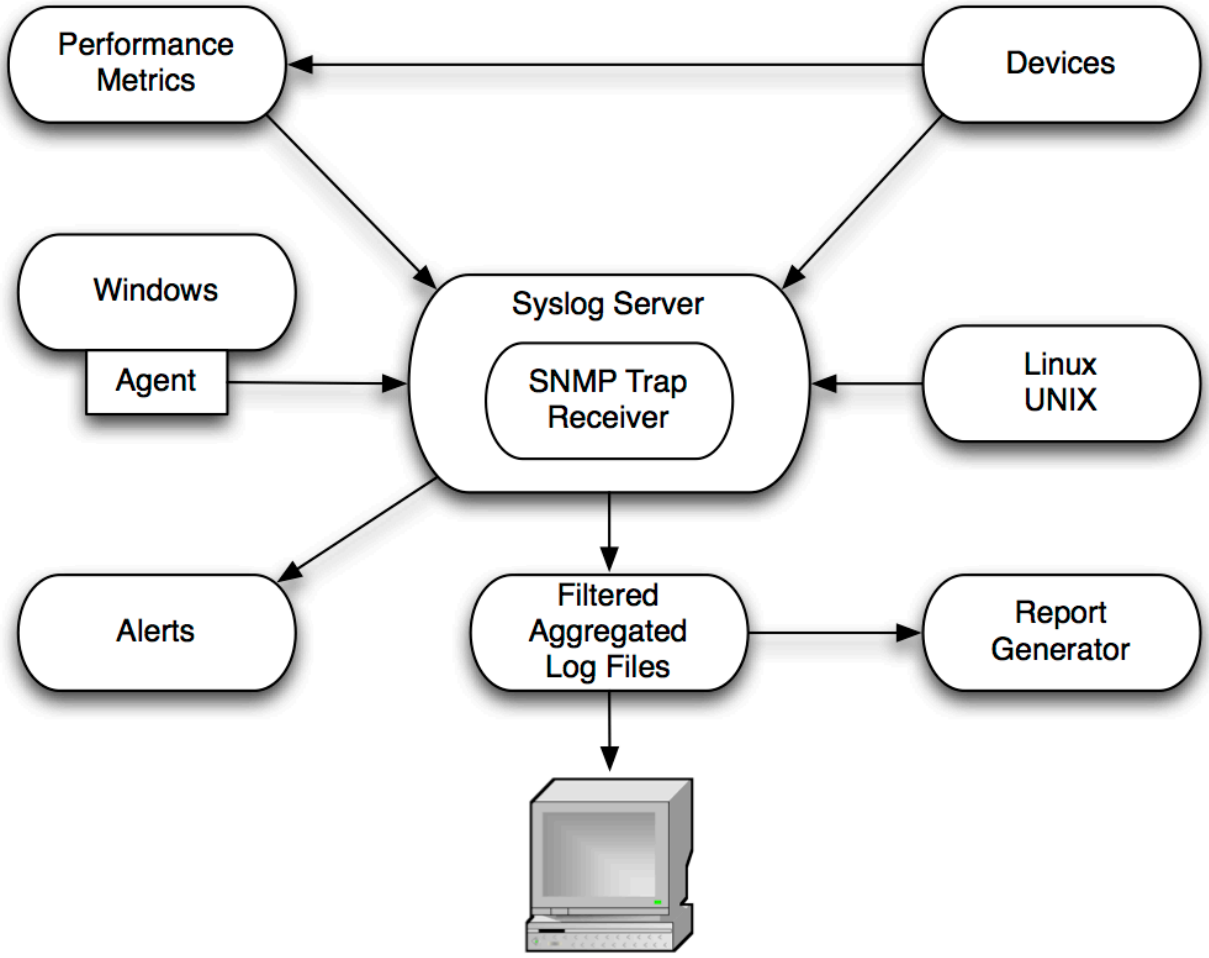

Figure 3 - Traditional Proactive Monitoring

Report generators correlate some of the data, and may give some troubleshooting clues. Digging through local syslog server filtered aggregated log files for more troubleshooting clues is a job for IT staff. Like the manual Do It Yourself method, reading logs requires knowledge about systems and applications. Filtered aggregated log files contain log messages that do not follow standards, and have arcane message codes.

This level of proactive monitoring helps IT staff spend less time determining what problems are. It is a giant step up from Do It Yourself because alerts give clues about problems, and the filtered aggregated log files are available in one place.

The combination of Kiwi syslog server and Sawmill universal log file analysis and reporting applications, is an example of implementing traditional proactive monitoring.

Proactive Monitoring Levels
- Analytics-based -

Analytics are the discovery and communication of significant patterns in data. A simpler and more inclusive architecture is having servers directly connect to an analytics monitoring application via server agents.

Analytics applications like that depicted in Figure 4, provide indexed log file aggregation, analyses, correlation, and search capabilities, enabling IT staff to mine for troubleshooting clues, without logging in to suspected devices and digging through individual log files.

Server agents send configuration files, system log files, application log files, web server log files, and most other log files, to the analytics monitoring application. Syslogs and SNMP traps are also sent directly to the analytics monitoring application.

Agents installed on Windows servers collect Windows system data:

- Windows Event Log data
- Windows Registry data
- Active Directory data
- Performance monitoring data

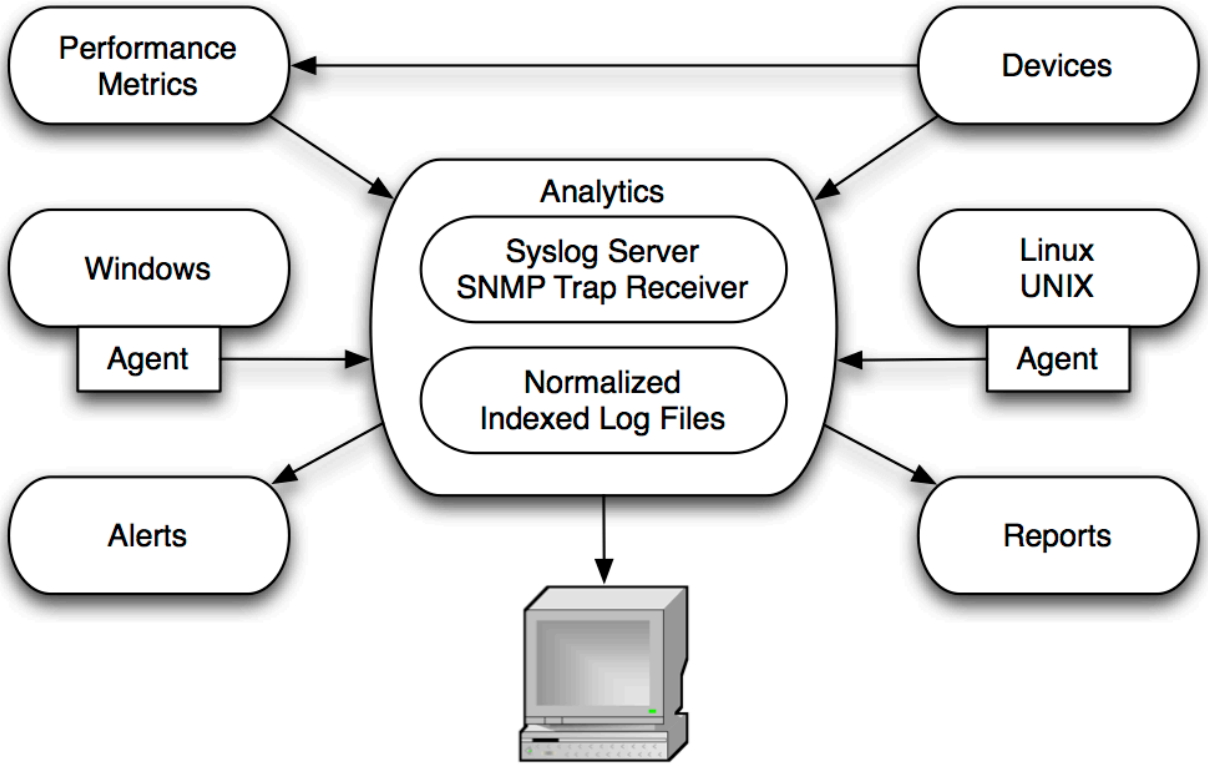

Figure 4 - Analytics-based Proactive Monitoring

Events from devices are stored in normalized indexes. Normalization is breaking down message into common fields. The indexes are optimized to retrieve events in time-series order.

The normalized indexes enables searching for events from multiple devices and correlating them for troubleshooting insights.

Correlation is the process of matching events for sequences and patterns that are apparent to a human. Events from different sources are combined and compared against each other to identify patterns of behavior.

Searches that successfully produce troubleshooting insights can be saved and used again. They can also become apart of the analytics-based proactive monitoring system, and trigger alerts.

This level of proactive monitoring helps IT staff spend even less time determining what problems are.

Splunk is an example of an analytics-based proactive monitoring application.

Proactive Monitoring Levels
- Unified -

Most proactive applications leave it up to IT staff to find problems. Unified proactive monitoring applications finds problems. The job of IT staff is to fix them.

Unified applications like that depicted in Figure 5 provide:

- Near real-time discovery of IT infrastructure devices connected to the network, and finding changes as they happen
- Service dependency mapping and relationships between resources and services, are used in determining the root cause of problems and the impact on services
- Automatic performance, availability, and event monitoring of IT infrastructure networks, servers, storage and applications
- Utilization and health trends across the IT infrastructure
- Aggregates and normalizes configuration, performance and event history
- The IT infrastructure is instrumented without agents

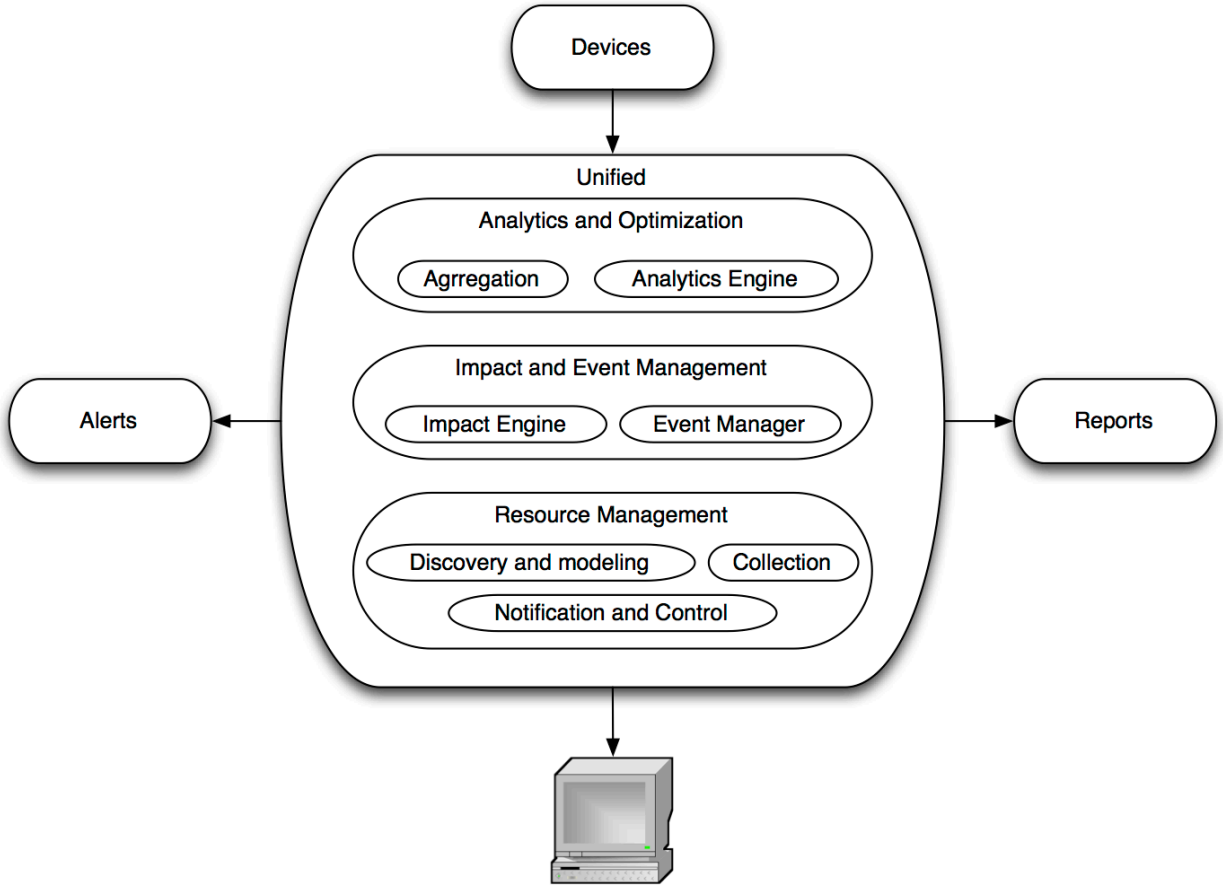

Figure 5 - Unified Proactive Monitoring

The IT staff can spend their time fixing problems instead of finding them, because this level of proactive monitoring finds the problems.

Zenoss is an example of a unified proactive monitoring application.

Bottom Line

Building Solutions.
A combination of Performance Metrics and Traditional, Analytics, or Unified proactive monitoring applications, are assets for troubleshooting problems in growing, dynamic, and ever increasing complex IT infrastructures. They fit well into today's world of doing more with a smaller workforce, having less time to fix problems, and keeping users productive.

Bottom Line.
There is no one-size-fits-all solution for proactive monitoring. IT organizations have different computing infrastructures and monitoring needs.

As IT infrastructure complexity grows, it is becoming more difficult to put together proactive solutions that meet the needs of IT organizations today, and grow with ever changing IT infrastructures tomorrow.

JohnTelford.com LLC works with IT staff:

- Determine todays proactive monitoring requirements
- Architect and build solutions for today and tomorrow
- Train in its use and maintenance

Please see my Résumé and review my experience.

Thanks …John

Monitoring Tools Reference

Below are some tools for creating proactive monitoring systems. The Wikipedia entry Comparison Of Network Monitoring Systems compares many more tools.

Proactive Monitoring Tools.

AlienVault
"Unified Security Management That's Out of This World. Complete. Simple. Affordable. With all of the essential security controls built-in, AlienVault's Unified Security Management™ platform provides complete security visibility, plus a fast & easy way to address compliance & threat management."

Foglight Network Management System
"Visualize, analyze and optimize your entire network infrastructure easily. With Foglight Network Management System (NMS), you can easily discover, map, and monitor network components in disparate locations across the globe. Ensure your network's performance and availability with actionable insights that help detect, diagnose and resolve potential issues anywhere in the stack."

InterSect Alliance - Snare Agents
"The Snare and Epilog agents, from InterSect Alliance, are considered to be the de-facto industry standard for eventlog and audit log collection. "

Kiwi - Syslog Server
"Kiwi Syslog Server is one of the most trusted and affordable syslog servers on the market. Easy to set up and configure, it offers a feature-rich solution for receiving, logging, displaying, alerting, and forwarding syslog, SNMP trap, and Windows event log messages from devices such as routers, switches, Linux and

Unix hosts, Windows servers, and more."

Nagios - The Industry Standard in IT Infrastructure Monitoring
"Achieve instant awareness of IT infrastructure problems, so downtime doesn't adversely affect your business. Nagios offers complete monitoring and alerting for servers, switches, applications, and services."

Paessler PRTG Network Monitor
"PRTG fits into any budget and grows with your needs. Try PRTG now and see how it can make your network more reliable and your job easier. Everything you need is contained in one simple installer, no additional downloads are required."

RRDtool
"RRDtool is the OpenSource industry standard, high performance data logging and graphing system for time series data. RRDtool can be easily integrated in shell scripts, perl, python, ruby, lua or tcl applications."

Sawmill - Universal log file analysis and reporting
"Sawmill: the Only Analytics Solution You'll Need. Throughout your network you need to know what is happening, you need precise and real-time analysis to make the right decisions that affect the growth and security of your business. Whatever you need to track, Sawmill provides the right solution at the right price. Sawmill's easy scalability and universal support helps you make better use of your data, with one application."

Splunk - Operational Intelligence, Log Management
"Splunk Enterprise is a fully featured, powerful platform for collecting, searching, monitoring and analyzing machine data. Splunk Enterprise is easy to deploy and use. It turns machine data into rapid visibility, insight and intelligence."

syslog-ng - Multiplatform Syslog Server and Logging Daemon
"The syslog-ng logging solution allows enterprises to build a powerful, trusted and centralized logging infrastructure for reviewing and auditing log messages"

Tripwire Log Center
"Your organization needs to respond to IT security threats in real time and prove compliance with security standards like PCI, NERC, and the EU Data Privacy Directive. Tripwire Log Center helps you do both by detecting suspicious activity and aggregating the raw log data required for compliance audits and security forensics investigations."

Windows Perfmon
"Performance Monitor can display information as a graph, a bar chart, or numeric values and can update information using a range of time intervals. The categories of information that you can monitor depend on which networking services are installed on your system, but they always include File System, Kernel, and Memory Manager. Other possible categories include Microsoft Network Client, Microsoft Network Server, and protocol categories."

Zabbix
"Zabbix is the ultimate open source availability and performance monitoring solution."

Zenoss
"Zenoss Service Dynamics is a family of integrated products that deliver end-to-end service assurance for real-world, hybrid IT that spans physical, virtual and cloud-based infrastructure."

Emerging Tools.

logstash - Open Source Log Management

"logstash is a tool for managing events and logs. You can use it to collect logs, parse them, and store them for later use (like, for searching). Speaking of searching, logstash comes with a web interface for searching and drilling into all of your logs."

VMware vCenter Log Insight: Log Management & Analytics

"VMware vCenter™ Log Insight™ delivers automated log management through log analytics, aggregation and search, extending VMware's leadership in analytics to log data. With an integrated cloud operations management approach, it provides the operational intelligence and enterprise-wide visibility needed to proactively enable service levels and operational efficiency in dynamic hybrid cloud environments."

Glossary

Proactive

"Action and result oriented behavior, instead of the one that waits for things to happen and then tries to adjust (react) to them. Proactive behavior aims at identification and exploitation of opportunities and in taking preemptory action against potential problems and threats, whereas reactive behavior focuses on fighting a fire or solving a problem after it occurs."

Simple Network Management Protocol (SNMP)

"Simple Network Management Protocol is an Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention."

SNMP Trap

"Asynchronous notification from agent to manager. Includes current sysUpTime value, an OID (Object Identifier) identifying the type of trap and optional variable bindings. Destination addressing for traps is determined in an application-specific manner typically through trap configuration variables in the MIB (Management Information Base)."

Software-defined data center

"Software-defined data center (SDDC) is an architectural approach to IT infrastructure that extends virtualization concepts such as abstraction, pooling, and automation to all of the data center's resources and services to achieve IT as a service. In a software-defined data center, compute, storage, networking, security, and availability services are pooled, aggregated, and delivered as

software, and managed by intelligent, policy-driven software. Software-defined data centers are often regarded as the necessary foundational infrastructure for scalable, efficient cloud computing."

Syslog

"Syslog is a standard for computer data logging. It separates the software that generates messages from the system that stores them and the software that reports and analyzes them."