IJDCST @Jan Issue- V-2, I-1, SW-18
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

NimBus for Network Monitoring based on SNMP Service Level Monitoring Gateway Solution

Mrs. Uppalapati Srilakshmi[1]
Dept. Computer Science & Engineering, MLR Institute of Technology & Management, Hyderabad, India.
Email: srilu.uppalapati@gmail.com
Mr. Jampani Satish Babu[2], Mr. Kancherla Balakrishna[3],
Dept. Computer Science & Information Technology, NRI Institute of Technology, Guntur, India.
Email: jampanisatishbabu@gmail.com[2],
babu.kancherla@gmail.com[3].

Abstract— The NimBUS for Network Monitoring solution provides an SNMP Gateway that will transform NimBUS alarm messages to SNMP trap messages that are readable by any SNMP based event manager. Predefined SNMP Gateway solutions are available for HP OpenView Network Node Manager, CA Unicenter-TNG and BMC Patrol Enterprise Manager (PEM). The Syslog Gateway serves as a gateway from the Syslog "world" into the NimBUS environment. Network-devices, such as routers, switches, firewalls and servers report events using SNMP as well as using the well-known Syslog format. The Syslog Gateway will listen to port 514/udp when running in a receive mode and covert messages to NimBUS event formats. This paper analyzes several facts of Network Performance Monitoring, evaluating several motivations as well as examining many commercial and public domain products.

Keywords— network performance monitoring, application monitoring, flow monitoring, packet capture, sniffing, wireless networks, path analysis, bandwidth analysis, network monitoring platforms, Ethereal, Netflow, tcpdump, Wireshark, Ciscoworks

I. Introduction

In today's world of networks, it is not enough simply to have a network; assuring its optimal performance is key. Customers who are turned away or disconnected due to any sort of network failure are likely to change vendors or providers. Consequently, network performance monitoring (NPM) must be done to find these errors quickly, so that they can be corrected as soon as possible.

But, as real-world experience with a network will quickly demonstrate, there is no one single factor that explains all difficulties and failures, nor is there any one level of monitoring that can detect every issue. Attackers from both outside and within may have planted viruses or Trojan Horse programs, which can drain company resources or transmit classified data to unauthorized recipients. Misconfiguration of any aspect of the system can introduce artificial or unnecessary bottlenecks in the network, or may simply cause the existing network capabilities to be used inefficiently. Employees may be using the network for their personal interests, in violation of policy. Further issues include the possibility of hardware or software failures within a server, causing either erroneous output or none at all.

NPM is a multi-faceted task, with several areas that must be considered: application/host-based monitoring, flow monitoring, packet capture (sniffing), path/bandwidth analysis, and wireless network monitoring. Additionally, some commercial products have been created in order to address many issues simultaneously, and are entitled network monitoring platforms (NMPs). The remainder of this paper will address these aspects of NPM, as well as presenting several freeware and commercial products that can be used to serve these goals. The NimBUS service level monitoring solution provides four core functions:

- Real time performance monitoring and reporting of potential problems
- Service level agreement (SLA) definition, monitoring and reporting
- Customizable business service and operations dashboards
- End-to-end response time measurement with end-user service levels

For data collection and automation NimBUS offers a comprehensive suite of infrastructure monitoring robots and probes. NimBUS probes will enable full coverage of heterogeneous IT infrastructures. Monitoring probes include support for networks, databases, servers, middleware, email, applications, web-based services, directory services, and much more. NimBUS open APIs, flexible architecture, and out-of-the-box 3rd party integrations and gateways, ensures that adapting to other management tools and service level monitoring processes is easily achieved.

With NimBUS, all service level monitoring functions are inherent functions; they are written collectively as a single architecture and single code base. The result is easy installation, deployment, configuration,

administration, and most important - usability - with NimBUS there is no requirement for strenuous installation integrations and ongoing administration efforts.

II. Network Monitoring Platforms

Where price is not an issue, commercial products can be used in order to cover most network bases simultaneously. For networks that have especially high value and use, these Network Monitoring Platforms (NMPs) may be the optimal solution. These NMPs are generally commercial programs with higher costs, with four of such being VitalSuite, NimBUS, Ciscoworks and NetCool.

A. Basis of Network Monitoring Platforms

Although the whole is generally thought to be more than the sum of its parts, this maxim will not hold true for network administrators implementing a multifaceted monitoring scheme comprised of several different programs created by different organizations. Packet sniffers cannot be guaranteed to output data in a format readable by the other tools, and while translation utilities exist, these simply add to overall complexity and waste time. Perhaps more critically, programs may be redundant and may unnecessarily consume resources by each attempting to gather the same data. Alternatively, using a large number of monitoring programs may simply add an aggregate CPU overhead such that the network performance monitoring programs themselves may be the ones degrading performance. With NMPs, all aspects of the platform are designed to work together, such that efficiency and performance are increased.

Even if such issues are not considered, integrated NMPs are preferable for their reliability. Established companies such as Lucent and Cisco have created effective, high-quality software, and can be trusted to release products that will not include egregious exploits and will not covertly pass on sensitive company information. The same cannot necessarily be said for free utilities that are maintained by a small group of individuals releasing unfinished builds. Furthermore, these NMPs come with user support and comprehensive documentation; the inexperienced network administrator can be assisted through carefully reading product notes, or directly contacting dedicated support personnel of the vendor. A more accurate adage concerning NPM would be that one gets what one pays for; for NMPs, although costs will be high, quality will be assured.

B. Commercial Network Monitoring Platforms

The first commercial NMP examined is VitalSuite [VitalSuite] by Lucent Technologies. VitalSuite is designed to handle monitoring of up to hundreds of different devices in an automated manner. In fact, up to ten million total objects can be monitored at a time. Dynamic charts and statistics are constantly updated in order to find network congestion and failures before they significantly impact the company. VitalSuite improves data collection through efficient importation of device information; consequently, hardware elements can be identified by more than just a generic title. A variety of configurations are supported, as well as the latest protocols, enhancing flexibility. Additionally, system requirements are not excessively prohibitive; any Windows 2000 or newer operating system is supported, as well as Sun Solaris platforms. One issue, however, is that Lucent's site is undergoing renovation as of the time of this paper, causing some links to be missing their targets, including some relevant VitalSuite documentation. The price for this NMP is also left somewhat unclear; administrators desiring further information on VitalSuite would be advised to contact Lucent directly concerning the product status.

Another commercial NMP is NimBUS [NimBUS] from Nimsoft. Although this is not a well-known company, the product is still excellent, providing detailed monitoring capabilities, even for global networks. NimBUS includes the common scope of abilities for NMPs, including monitoring access periods and response times for devices and applications, performing traffic analysis, gathering SNMP statistics, and providing extensive graphical display possibilities. Extensive documentation is available, although users must register on the Nimsoft website to access these files. Additionally, the price for the software and the system requirements are not clearly stated. While NimBUS advertises its flexibility in its ability to be deployed at multiple points throughout the network, and it is stated that it will work on Windows-based hosts, its compatibility with other operating systems is unclear. However, a trial download of NimBUS is provided, allowing for administrators to determine whether this product will be acceptable for their domain. This is highly encouraged, as for all that is provided on the product website, real-world testing can provided practical responses to previously answered questions about NimBUS.

A well-known NMP is Cisco's Ciscoworks [Ciscoworks]. While one might expect this NMP to be monolithic, it is actually composed of several pieces that can be applied to specific areas. Ciscoworks includes solutions for Wireless LANs, VPNs, and quality of service analysis, with even a specific subsection designed for serving smaller companies. This wide range of products cannot be described within this paper, but the basic LAN Management Solution (LMS) bears brief examination, as it may be the most commonly used

for wired networks. LMS further delineates the LAN into layers, such that devices, flows, hosts and links can all be analyzed effectively by appropriate subsystems. Up to 1500 devices can be monitored simultaneously, providing real-time results concerning performance. LMS is only available for Solaris and Windows systems, and requires high-end hardware; for Windows systems, a 2.8 GHz machine with between 2-8 GB of RAM is required for the main host, with all clients needing 512 MB of memory for LMS applications. Consequently, networks with low-end machines may be unable to use Ciscoworks products such as this or may encounter performance issues. The Ciscoworks family is broad, as well as expensive; it is advised to do significant research into the products supported in addition to contacting Cisco directly to determine which tools would be best for any specific company. A final NMP is NetCool [NetCool] by IBM and Micromuse. Micromuse states their goals from a very business-oriented perspective, attempting to discover where extra resources are needed most and how service-level agreements can be followed as closely as possible. Four main modules are included within NetCool; the first of these is DataLoad, which polls SNMP devices and reads data files. DataChannel collects and analyze data, processing it for display within seconds. DataMart acts as a storage utility for both old and new data as well as network policies. Finally, DataView aids in providing an exceptional user interface, able to deliver reports within seconds. With this modular design, each step of the monitoring process can easily be identified and defined, creating an overall system that is both flexible and comprehensive. Although the recent merger of IBM and Micromuse might seem to inhibit development, IBM's resources have instead allowed for a multimedia demo to be created for NetCool. However, it does appear that NetCool may be in the process of being combined with a similar product titled Tivoli; potential users are advised to check for news updates concerning the service. As no trial version of NetCool is available, contacting IBM concerning the current status of the project and its cost is very much recommended.

The following table provides a brief summary of network monitoring platforms.

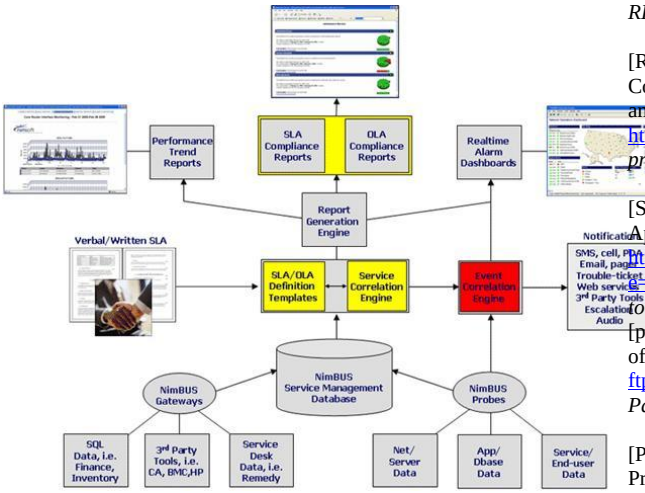
	Cost	Download Size	Platform	Notable Information
VitalSuite	$35,000+ [Nance06]	Minimal	Windows, Solaris	Lucent/Alcatel merger causes product website issues; can poll and monitor up to 10 million devices
NimBUS	$10,000+ [Biggs05], Trial Version Available	Unspecified	Windows	Extensive documentation; some information unavailable; high quality monitoring and display capabilities
Ciscoworks	$9,000 - $20,000 for LMS [Windows Marketplace]	2-8 GB of RAM for server, 512 MB RAM for clients	Windows, Solaris	High-quality, well known product; allows simultaneously monitoring of diverse devices; many products available depending on specific needs
NetCool	$75,000+ [MM_SLM]	Unspecified	Windows, Solaris, Linux	Uses multiple modules to split tasks into definable pieces; very business oriented; can read data and deliver dynamic reports within seconds

Table: Summary of Network Monitoring Platforms

While these commercial NMPs may represent the pinnacle of NPM, they do come at a price. For many networks, the individual public domain NPM tools may suffice, especially where reliability is high. However, when considering which products to obtain, and considering the seemingly high costs of NMPs, network administrators must ask themselves two questions: what will happen to the business if the network fails, and tools are not in place to determine the solution? Similarly, how will it reflect on the administrator when it is discovered that utilities could easily have been installed to detect and control damage? As such failures are generally catastrophic both economically and professionally, this question drives researchers to improve NPM principles and develop new products.

4. AVAILABILITY AND BUSINESS SERVICE MANAGEMENT

- TRUE ENTERPRISE-WIDE AVAILABILITY MANAGEMENT
- QUICK IMPLEMENTING, IMMEDIATE RESULTS
- UNIQUE HORIZONTAL AND VERTICAL SCALABILITY
- QUALITY OF SERVICE MONITORING BASED ON SERVICE LEVEL AGREEMENTS
- APPLICATION RESPONSE TIME MONITORING FROM AN END-USER PERSPECTIVE



The NimBUS advantages for your enterprise

CONCLUSION

This paper analyzes several facts of Network Performance Monitoring, evaluating several motivations as well as examining many commercial and public domain products.

REFERENCES

[Azoff06] Michael Azoff. "Technology Audit: IT Management". Butler Group analytical paper on recent Compuware version. May 2006. http://www.compuware.nl/perskamer/pdf/Compuware-Vantage_9.9.pdf. *Analytical paper discussing Vantage.*

[Biggs05] Margie Biggs. "Web Site Sleuths". FCW.com comparative article on monitoring solutions. March 14, 2005 issue. http://www.fcw.com/article88255. *Article discusses and compares different monitoring utilities.*

[MM_SLM] Unsigned; Enterprise Management Associates. "Micromuse Service Level Management Buyer's Guide - 2nd Edition". Product summary and cost analysis document. 2004. http://www.micromuse.com/downloads/pdf_lit/Micromuse_SLM_Brief_ema_jan2003.pdf. *Detailed guide for potential buyers of NetCool.*

[Nance06] Barry Nance. "Lucent Clear Winner in Network and Application Performance Management Software Test". NetworkWorld Custom Media article comparing various products. September 2006. http://www.networkworldpartners.com/lucent/Bakeoff4.pdf. *Article discusses and compares different application monitoring utilities.*

[RFC2723] Natalie Brownlee. "SRL: A Language for Describing Traffic Flows and Specifying Actions for Flow Groups". Official RFC Document, October 1999. http://www.ietf.org/rfc/rfc2723.txt. *RFC discussing process used in NetraMet.*

[RFC3176] P. Phaal, S. Panchen and N. McKee. "InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks". Official RFC Document, September 2001. http://www.rfc-editor.org/rfc/rfc3176.txt. *RFC discussing processes used in sFlow.*

[Sticky] Unsigned. "Tool info: AppMonitor". Brief description of AppMonitor. October 13, 2005. http://stickyminds.com/sitewide.asp?Function=edetail&ObjectType=TOOL&ObjectId=1688. *Brief examination of the AppMonitor tool including pricing.*

[pathchar] Van Jacobson. "pathchar - a tool to infer characteristics of Internet paths". Official Product Documentation. ftp://ftp.ee.lbl.gov/pathchar/msri-talk.pdf. *Document discussing Path Analysis tool.*

[Pathload] Constantine Dovrolis, Manish Jain. "Pathload". Official Product Website. http://www.cc.gatech.edu/fac/Constantinos.Dovrolis/bw.html. *Website for Bandwidth Analysis tool.*

[Pathrate] Constantine Dovrolis, Ravi Prasad. "Pathrate". Official Product Website. http://www.cc.gatech.edu/fac/Constantinos.Dovrolis/pathrate.html. *Website for Bandwidth Analysis tool.*

[Ribiero03] Vinay J. Ribeiro, Jiri Navratil, Les Cottrell, et al. "pathChirp: Efficient Available Bandwidth Estimation for Network Paths". Passive and Active Measurement Workshop. April 2003. http://moat.nlanr.net/PAM2003/PAM2003papers/3824.pdf. *Document discussing Bandwidth Analysis tool.*

[sFlow] Unsigned. "sFlow.org - Making the Network Visible". Official Commercial Product Website. http://www.sflow.org/index.php. *Company website for Flow Monitoring tool.*

[tcpdump] JWS. "TCPDUMP Public Repository". Official Product Website. http://www.tcpdump.org/. *Website for Packet Capture / Sniffing tool.*

[Vantage] Compuware. "Vantage - Compuware's complete application service management solution". Official Commercial Product Website. http://www.compuware.com/products/vantage. *Company website for Application Monitoring tool.*