IDG.net

NetworkWorld Reprint

The leader in network knowledge ■ www.nwfusion.com March 18, 2002 ■ Volume 19, Number 11

Buyer's GUIDE Review: Network management software suites

Despite its price, Lucent's VitalSuite is the tool of choice for solving network performance and connectivity problems.

Tightly focused network management suites

By Barry Nance, Network World Test Alliance

Managing network connectivity and performance on a large network with a few diverse, nonintegrated tools is an expensive use of a network administrator's or network engineer's time. On the other hand, for many networks, installing and administering a large-scale integrated tool such as UniCenter TNG or OpenView likewise can be unproductive. A small cadre of network administrators or engineers can grow into an entire department of network people trying to keep up with such a complex tool.

The answer for networks in which UniCenter or OpenView isn't justified is a midtier network-management suite. Midtier suites focus on network connectivity and performance. They forego any attempt to manage users, groups, user rights and the distribution of files to particular locations. A narrower focus means configuring and using a midtier network-management tool takes less time and effort than configuring and using a large-scale, full-featured tool. If all you want from a network software tool is to detect or avoid connectivity and performance problems, a midtier network-management suite is the right choice.

Vendors of midtier network-management products have designed their tools to help you quickly diagnose connectivity problems; accurately locate bottlenecks and congestion points; comprehensively understand your network's utilization; proactively spot trends; and faithfully plan for your network's future capacity needs. Four vendors submitted network management tools to our lab for evaluation. For networks consisting of roughly 1,000 to 50,000 computers and devices, our testing concentrated on software products capable of monitoring, diagnosing, measuring, managing, reporting and correcting a network's ills.

We tested Lucent's VitalSuite 8.1, Chevin's Tevista 2.0, Concord Communications' eHealth suite 5.0 and Tavve Software's eNMS 2.0 installed on a Sun computer.

Lucent's VitalSuite proved to be a superior but somewhat pricey tool for monitoring and managing networks as well as an excellent aid to capacity planning. Its high accuracy and support for a range of network devices and configurations earned VitalSuite the World Class Award for best midtier network-management product.

Vital statistics

Starting at $53,000, VitalSuite is a tightly integrated collection of software modules for monitoring network activity, ensuring service-level agreement (SLA) compliance, tracking network performance, and watching over applications and their transactions. VitalSuite accurately and easily pinpointed the deliberately caused connectivity problems and performance slowdowns in all our tests. We liked the product's responsive and intuitive user interface. It's surprisingly easy to use in light of its complexity. VitalSuite's flexible architecture impressed us with its ability to handle a variety of business application environments. VitalSuite is so finely

Copyright 2002 by Network World, Inc., Southborough, MA 01772 — Posted from Network World • An IDG Company
#311724 Managed by Reprint Management Services. (717) 399-1900 www.reprintbuyer.com

scalable you can choose to install, for example, the reporting server module on a separate computer.

The VitalSuite package consists of VitalNet, VitalAnalysis, VitalHelp, VitalAgent, AutoMon and Transact Toolkit. VitalNet gathers information from SNMP-aware devices and from desktop machines on which you've installed the VitalAgent client software, then relays the information to VitalAnalysis and VitalHelp. VitalAnalysis monitors applications and maintains an historical analysis of system and application performance and trends. For capacity planning and other purposes, it stores a year's worth of data in the included Microsoft SQL Server database. Lucent bundles both SQL Server 7.0 and SQL Server 2000 with VitalSuite, and you choose which one you want to use.

VitalHelp assesses the health of TCP/IP-based applications. When it determines the cause of a problem, VitalHelp posts alerts to a network administrator. VitalSuite's AutoMon is a script-driven synthetic transaction engine, and the Transact Toolkit lets programmers define unique business application transactions for VitalSuite to monitor.

VitalSuite's key report, Heat Chart, made troubleshooting application bottlenecks a breeze with its at-a-glance identification of problems and their causes. Each Heat Chart displays a color-coded matrix of application performance factors and computing components, termed resource classes. Each Heat Chart cell corresponds to a resource class and a performance metric. Heat Chart cells change color to indicate the health of the underlying computing resources that comprise each of the corresponding resource classes.

VitalSuite reports application performance data in three views: Business, Applications and Reports. Customizing the Business view as either My Vital or My Business is a user's preference, with each view a different way of looking at performance metrics from application and network statistics. The My Vital personal Web page is highly configurable and uses password protection to restrict access to and configuration of the page. The Applications view groups tab-indexed information into categories such as domains, groups, clients and servers. Each tab index displays network-related application performance criteria, including lost packets; round-trip delays; availability; response time throughput; and client, network and server delay times.

The Reports view is a high-level menu of available reports, categorized by job description. These descriptions include management, application monitoring, network monitoring and capacity planning. To show network and application performance trends, VitalSuite's planning report uses a simple trending arrow, pointing up or down, along with the current average, one-month, three-month, six-month and one-year utilizations. It offers only a relatively small number of preconfigured reports but setting up new reports is easy. Moreover, linking the reports to show increasing levels of detail takes just a few mouse clicks and makes the reports highly effective and useful.

Lucent's suite of tools runs on Windows NT or Windows 2000. Installation is painless and the documentation is superb.

Physical exam

A four-part suite of network monitoring components, Concord's eHealth consists of Network Health, Live Health, System Health and Application Health modules. By actively polling SNMP-manageable devices, Live Health determines their status and condition, and displays in real time its detection of faults, potential outages and response-time delays. Network Health monitors the performance and availability of WAN interfaces, routers, switches, Frame Relay circuits and remote-access equipment. System Health monitors servers and selects clients to alert administrators to application performance problems, server crashes and disk space shortages. Application

Net Results

4.5 RATING
VitalSuite 8.1

Company: Lucent Technologies, (888) 467-8324, www.vitalsuite.com **Price:** Starts at $53,000. **Pros:** Full-featured midtier network monitoring and management tool; intuitive user interface; highly scalable. **Cons:** Expensive.

4.2 RATING
eHealth suite 5.0

Company: Concord Communications, (800) 851-8725, www.concord.com **Price:** Starts at $15,000. **Pros:** Superior reporting; highly configurable. **Cons:** User interface not quite as intuitive as VitalSuite's.

3.2 RATING
eNMS 2.0

Company: Tavve Software, (888) 950-2131, www.tavve.com **Price:** $16,000 for 50 nodes. **Pros:** Good topology mapping aid; reports are an excellent basis for service-level agreement monitoring, vendor assessments and capacity planning. **Cons:** Requires that you have Network Node Manager or NetView.

2.7 RATING
Tevista 2.0

Company: Chevin, (866) 838-4782, www.chevin.com **Price:** Starts at $14,999 for 25 agents (1 agent per network segment). **Pros:** Frugal bandwidth utilization; offers packet decoding. **Cons:** Limited documentation; requires Microsoft Excel expertise to produce useful trend or capacity planning reports; threshold parameters are too simplistic.

What's the score?	VitalSuite 8.1 (WORLD CLASS WINNER)	eHealth suite 5.0	eNMS 2.0	Tevista 2.0
Management 20%	4	4	3	3
Reporting 20%	5	5	4	2
Ease of use 20%	5	4	3	3
Notification 10%	4	4	3	3
Corrective action 10%	4	4	3	2
Installation 10%	4	4	3	4
Documentation 10%	5	4	3	2
TOTAL SCORE	4.5	4.2	3.2	2.7

Individual category scores are based on a scale of 1 to 5. **Percentages** are the weight given each category in determining the total score. **Scoring Key: 5:** Exceptional showing in this category. Defines the standard of excellence. **4:** Very good showing. Although there may be room for improvement, this product was much better than the average. **3:** Average showing in this category. Product was neither especially good nor exceptionally bad. **2:** Below average. Lacked some features or lower performance than other products or than expected. **1:** Consistently subpar, or lacking features being reviewed.

Health is a transaction-oriented collection of tools for determining the cause of poor application-response times. The Application Assessment component of Application Health watches over software such as Microsoft Exchange, Microsoft Internet Information Server, Microsoft SQL Server, Oracle and the Apache Web server.

EHealth can present its collected performance metrics and device status data via a browser-based interface, a server-based console and Adobe Acrobat-based reports. EHealth also can send device status and condition data to network management products such as OpenView. It graphically depicts the network as a "fishbone" — a spine whose ribs represent the different network segments.

EHealth is complex software. In addition to its sophisticated network monitoring and reporting elements, eHealth comes with its own Web server for rendering management data and reports as Web pages, Open Ingres database engine for storing network device data and Tarentella's (formerly Santa Cruz Operation) XVision PC X server, which eHealth's server console uses to display screen data.

EHealth's discovery process is quick and accurate. By default, eHealth discovers network nodes daily at midnight, but we could use the server console to run the discovery process interactively or schedule discovery to occur on specific days and at specific times.

At 5-minute intervals (or less often, if you wish), the SNMP polling process probes the condition and status of network devices. EHealth understands a plethora of Management Information Bases (MIB), and it correctly recognized Lucent routers, Hitachi switches and all the other devices in our lab. Concord supplies MIB definitions for more than 500 SNMP-aware devices. EHealth uses these MIBs for determining device performance and availability. It stores the collected network device information for six weeks in the Open Ingres database. Via Open Database Connectivity, eHealth also worked well with the Oracle, Sybase and Microsoft relational databases in our tests.

In its first few days, eHealth builds a baseline that characterizes a network's normal behavior. It excels thereafter at highlighting out-of-the-ordinary events, such as excessively high or low traffic through a router or switch port, based on a set of multifaceted and highly configurable rules. We found eHealth's default rules adequate for our network. These adjustable rules help eHealth identify exceptions such as a WAN port that has varying activity levels from its historical day-of-week and time-of-day historical usage patterns. Once eHealth displays an exception, a network administrator can choose to monitor the problem device in what Concord calls fast mode. EHealth polls the device up to twice per minute to help an administrator track the situation. EHealth offers real-time monitoring of server parameters such as CPU utilization, memory usage, memory paging/swapping and log file entries.

Via its SystemEdge component, eHealth can e-mail or page someone when a problem occurs, and it offers links to third-party help-desk programs. It can also automatically restart failed processes.

Concord's expertise in producing network status reports is quite apparent in eHealth. For instance, its reports show device information by time period, relationship to the organizational structure and type of behavior or exception. We could also see devices that had experienced problems, by type of problem, as well as those associated with a particular application. EHealth's reports are excellent for capacity planning, keeping an eye on Web site responsiveness, guarding against network hacking attempts and tracking hardware and software assets. EHealth can display its reports through its quick and responsive Web interface, or it can generate Adobe Acrobat PDF files for viewing or printing.

EHealth runs on HP-UX, Solaris, Windows 2000 and NT. Installation is straightforward,

How we did it

In our evaluation of these network management aids, we looked primarily for the ability to monitor and manage the health and availability of our servers and network devices. The ability to take corrective action to resolve a problem automatically was a plus. We tested the sending of alerts by pager, Web page and single or multiple recipient e-mail to notify us of network problems. We expected a product to produce reports that helped us establish baselines, show available and unavailable devices, log device availability histories, identify trends and spot future problems.

We noted whether a product checks for TCP/IP port device availability and monitors TCP/IP services such as SMTP, HTTP and telnet. We also noted whether a product uses SNMP to retrieve details about a device. We studied these products to see if they collected Windows NT/2000 auditing information, filtered Unix log activity and monitored Unix system activity and Win 2000/NT services and events. Network device inventory was important, and we also wanted these products to monitor and reveal server or client CPU usage, disk space and memory consumption.

The test bed network consisted of six Fast Ethernet subnet domains connected by Cisco routers and a Covad synchronous DSL internet link. Our client platforms included Windows 98/Millennium Edition/NT/2000; Red Hat Linux 6.2; Macintosh System 8; and OS/2 Warp 4.0. Relational databases on the network were Oracle 8i, Sybase Adaptive Server 11.5 and Microsoft SQL Server 2000. Win 2000/NT and NetWare 5.1 shared files, while Internet Information Server, Netscape and Apache software served up Web pages. The network's transport layer protocols were TCP/IP, IPX/SPX, AppleTalk and SNA.

We ran Lucent's VitalSuite, Concord's eHealth and Chevin's Tevista network management products on a four-way Compaq ProLiant ML570 computer with 900-MHz Pentium III CPUs, 2G bytes of RAM, eight 18G-byte SCSI RAID drives and two NC3134 10/100 network adapters. For these three products, the operating system platform was Windows NT Server 4.0 with Service Pack 6. Tavve preloaded its eNMS software on a Solaris 8.0-based Sun Blade 100 Workstation with a 500-MHz UltraSPARC-IIe CPU, 2G bytes of RAM and a 15G-byte Integrated Drive Electronics disk drive. Tavve also installed Hewlett-Packard Network Node Manager 6.2 on the Sun machine. An Agilent Advisor protocol analyzer generated packets as well as decoded and displayed network traffic. The generated traffic let us cause performance slowdowns for the products to analyze, and we simulated connectivity problems by unplugging Ethernet cables at the switch.

and the documentation is comprehensive and clear.

Complements on your network

When Tavve's network experts, who had gained considerable experience as OpenView and Tivoli NetView consultants, saw room for improvement in HP Network Node Manager and NetView, they created a number of complementary software tools instead of asking HP and Tivoli for NNM and NetView enhancements. Tavve now offers the tools in a suite it calls eNMS, a collection of software modules for fault management, root-cause analysis, event correlation, network topology map-building and customization, performance reporting, troubleshooting and distributed network management. The individual modules are EventWatch, PreView, eProbe and QuickView. Tavve did not send us an eProbe, saying it was simply a remote copy of eNMS. The company bills eProbe as a hardware and software device that contains an instance of EventWatch and PreView for distributing network management chores across remote network segments and firewall-protected sites.

Yet another complementary product from Tavve, Amerigo, helps NNM users build and publish detailed topology maps that show extra information beyond what NNM captures.

The core module, EventWatch, processes NNM or NetView data to correlate events, perform root-cause analysis of connectivity problems for Layer 2 and Layer 3 devices, and notification to network administrators and network engineers via paging, e-mail, pop-up alert windows, trouble tickets and entries in log files. Our tests showed EventWatch's root-cause analysis to be a welcome addition to NNM's handling of outages and link failures. In particular, EventWatch's switch port monitoring feature accurately apprised us of connectivity problems within just a minute or two by identifying the culprit switch (but not the port) when we caused a variety of switch errors. Using Tavve's patent-pending correlation engine and device database, EventWatch filtered out transient and duplicate alerts to tell us exactly where in the network each problem occurred. EventWatch reduced NNM analysis time as we pored over NNM's displays to locate specific network errors. It's a worthwhile tool for use with mission-critical servers, routers, switches and other important network resources. However, its $125 per node price is a little steep for pervasively and indiscriminately using the product to monitor every nook and cranny of a network.

EventWatch's browser-based interface is often verbose, displaying sentences and paragraphs when simple menu items would do. However, once we grew familiar with Tavve's terminology, the Web pages provided direct access to the tool's configuration options and reports. The browser-based interface sported an operational status indicator for monitoring EventWatch, but did not offer continuously updated real-time displays to show the dynamic resolution (or worsening) of a network problem.

In contrast, PreView offers real-time information, but only on demand, not on a continuous basis. Its browser-based reports, graphs, charts and commentary on the status of the network are highly configurable. We were able to quickly and easily segment the information into groups of devices or individual devices and then categorize it by device type, vendor, geographical location and business unit. Like EventWatch, PreView uses NNM or NetView data. The reports identify the top-10 talkers, bandwidth utilization, CPU usage, bottlenecks, network errors and trends. From at-a-glance summaries, we drilled down through the PreView data to see information on the performance of individual devices and WAN links. The reports are an excellent basis for SLA monitoring, vendor assessments and capacity planning.

Amerigo is a handy add-on for NNM. We used it to enhance NNM's network topology maps with detailed information, such as device types, vendors, agents and locations, on our network's devices. After creating our customized maps, Amerigo automatically detected network configuration changes and updated the corresponding NNM topology maps. It made NNM's maps much more useful. We especially liked the ability to show logical connections between user-defined submaps. Amerigo propagated the connectivity indicators throughout the various map levels to help us always know the context of any submap we viewed. It offers an intuitive native user interface (we tested the Solaris version) but no Web-based interface. However, Amerigo integrates with EventWatch to display network outages. When EventWatch detects a problem, it forwards the location of the connectivity event to Amerigo, which highlights that location on an Amerigo map.

The eNMS suite runs on Unix and Windows, but Tavve says the Windows version doesn't have all the bells and whistles of the Unix version. As we watched, the Tavve systems engineer installed the product on the Sun computer without much difficulty. The documentation was clear and detailed.

A panoramic vista

Through a well-designed, intelligent extension to Remote Monitoring that Chevin calls HSRMON, Tevista's network monitoring suite uses network bandwidth especially frugally as it tracks connectivity and performance. In a highly unobtrusive fashion, HSRMON even worked well over a 28.8K-byte modem link in our lab.

Tevista consists of Enterprise Manager, which displays icons representing the locations or segments of your network; Network Asset Manager, which collects and shows detail about the devices on the network; and Visibility Agents, which are Chevin software modules you distribute across your network.

We set up a variety of locations in Enterprise Manager, with each becoming a labeled icon in the main Tevista window. Double-clicking an Enterprise Manager icon opens a Network Asset Manager window for that location. For each location, based on a range of IP addresses we specified, Network Asset Manager discovered SNMP devices as well as the visibility agents we had installed. We told Network Asset Manager to identify whether a device offered Telnet, FTP, HTML (Web server) or SMTP access. Network Asset Manager uses SNMP, ping (TCP/IP Internet Control Messaging Protocol packets) and, for visibility agents, Chevin's proprietary HSRMON to poll the network.

We installed a visibility agent on each network segment. Through Network Asset Manager, we configured each visibility agent's time periods and intervals for gathering statistics and set thresholds for which events should trigger alerts. Tevista's list of thresholds we could choose from included such simple conditions as short packets, long packets, broadcasts, multicasts, LAN over- or underutilization and new nodes.

Unlike the more sophisticated VitalSuite, eHealth and

eNMS, Tevista's alarm conditions don't let you specify that it should produce warnings only when network utilization exceeds more than specific criteria. For instance, 5 minutes of greater than 80% utilization during any hour between 8 a.m. and noon. When it detects an alarm condition, Tevista can play a sound (.wav) file or run a computer program. Chevin supplies a program you can use to send e-mail messages when an alarm condition occurs.

The visibility agents gathered statistics, discovered devices on that network segment, aided (via HSRMON) in Network Asset Manager's troubleshooting of connectivity problems and even decoded packets for Network Asset Manager to display.

Tevista does not prepare a wealth of sophisticated reports. For a particular visibility agent, it offers lists of network adapter card error counts, network segment statistics (overall usage, packets per second, percentage error rate and average packet size), devices and top-10 protocols. It can also prepare pie charts showing busiest nodes, busiest protocols, NetWare protocol usage, TCP/IP usage, network usage by group and network usage by type (router and terminal).

If you have Microsoft Excel or Word for Windows available on the Tevista machine, you can export Tevista data via Object Linking and Embedding to Excel or Word for Windows (the manual contains a brief, general description of OLE). Chevin supplies Excel and Word macros, but you must be a spreadsheet maven to properly design and produce reports that show Tevista network events over time, event histories and utilization trends. On an offline basis, once Tevista has collected statistics into its data files, you can choose to have Tevista run a Java applet that creates an HTML-formatted report containing statistics from that data file.

In contrast to the Media Access Control and IP address-based license key approaches of VitalSuite, eHealth and eNMS, Tevista uses a dongle (parallel or Universal Serial Bus port connector). Tevista runs on Win 2000, NT 4.0, Windows 98 and Windows 95. Installation is quick. The manual falls short of providing the explanations you'll need to truly understand how to use the product, and the index in particular is skimpy.

Conclusion

High-end network management companies, such as Tivoli, CA and BMC, have something to worry about. Competitors offering midtier network management products have added significant enhancements, such as highly useful real-time displays and sophisticated capacity planning reports, to those products. These midtier tools lack some of the features of the high-end products, such as the ability to automatically distribute software files or data files, and the ability to manage user identifications and groups across a large network. Nonetheless, the current crop of second-echelon network management tools impressed us greatly.

For networks of virtually any size, we highly recommend Lucent's VitalSuite. It's the right tool for the job.

Nance, a software developer and consultant for 29 years, is the author of Introduction to Networking*, 4th Edition and* Client/Server LAN Programming. *He can be reached at barryn@erols.com.*

Global Test Alliance

Nance is a member of the Network World Global Test Alliance, a cooperative of the premier reviewers in the network industry, each bringing to bear years of practical experience on every review. For more Test Alliance information, including what it takes to become a member, go to ww.nwfusion.com/alliance.

Other members: John Bass, Centennial Networking Labs, North Carolina State University. Travis Berkley, University of Kansas. Bob Currier, Duke University. Jeffrey Fritz, West Virginia University. James Gaskin, Gaskin Computing Services. Thomas Henderson, ExtremeLabs, Inc. Miercom, Inc., Network Consultancy and Product Test Center. David Newman, NetworkTest, Inc. Christine Perey, Perey Research & Consulting. Barry Nance, Independent Consultant. Thomas Powell, PINT. Joel Snyder, Opus One.

Lucent Technologies
Bell Labs Innovations



To learn more, contact your Lucent Technologies Representative, Authorized Reseller, or Sales Agent. Or, visit our web site at http://www.lucent.com/vital or contact one of the following Response Centers:

Asia-Pacific
Tel: +65-248-5441

Europe, Middle East, Africa
Tel: +32-7022-2052 or: +800-11-22-3333

Latin America
Tel: 1-305-569-3600

North America
Tel: 1-888-426-2252