

# z/OS MONITORING, CONTROL & AUTOMATION

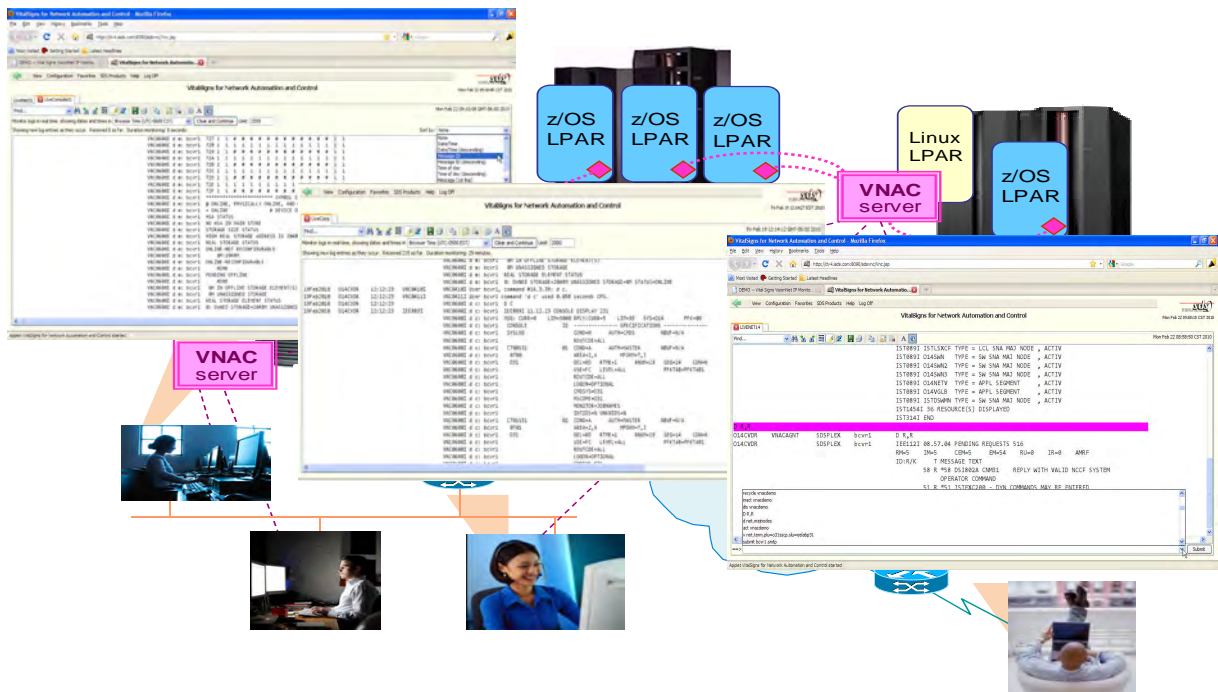
## SANS THE COST OF NETVIEW

### WHEN YOU ONLY WANT TO PAY FOR WHAT YOU USE

#### SOFTWARE DIVERSIFIED SERVICES (SDS)

#### VITALSIGNS FOR NETWORK AUTOMATION & CONTROL (VNAC) FROM SDS

*Focusing on the z/OS monitoring, control and automation functionality most used by NetView® and NetMaster™ customers.*



## TABLE OF CONTENTS

<i>PREAMBLE: AN OVERVIEW OF SDS VITALSIGNS FOR NAC</i> .....	3
MAINFRAME NETWORKING MORPHED, NETVIEW MULTIPLIED .....	4
TYPICAL REMARKS FROM ACTUAL CUSTOMERS AS TO THEIR USE OF NETVIEW FOR z/OS .	6
DETERMINE YOUR CURRENT DEPENDENCE ON NETVIEW FOR z/OS OR NETMASTER .....	6
POTENTIAL FOR REALIZING QUANTIFIABLE COST SAVINGS .....	9
VITALSIGNS FOR NAC'S VERY PRACTICAL AGENT-SERVER ARCHITECTURE .....	10
VITALSIGNS FOR NAC: THE STANDOUT DIFFERENTIATORS .....	12
THE BOTTOM LINE .....	17
SELECTED GLOSSARY.....	19
SOFTWARE DIVERSIFIED SERVICES .....	20

## KEY ACRONYMS

(D)DVIPA	(Distributed) Dynamic Virtual IP Address
EE	Enterprise Extender
FTP	File Transfer Protocol
LPAR	(IBM) Logical Partition
NCCF	Network Communications Control Facility
NPDA	Network Problem Determination Application
OSA	(IBM) Open Systems Adapter
REXX	REstructured eXtended eXecutor
SMF	(IBM) System Management Facility
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SOAP	Originally Simple Object Access Protocol, but as of 2003 a name as opposed to an acronym
SSCP	(SNA) System Services Control Point
VNCA	VTAM Node Control Application
VTAM	(IBM) Virtual Telecommunications Access Method

ALL TRADEMARKS, REGISTERED NAMES AND PRODUCT NAMES USED IN THIS DOCUMENT BELONG TO THEIR RESPECTIVE OWNERS. NETVIEW IS A REGISTERED TRADEMARK OF IBM. NETMASTER IS A REGISTERED TRADEMARK OF COMPUTER ASSOCIATES (CA). IBM IS THE REGISTERED NAME OF IBM CORPORATION.

# **z/OS MONITORING, CONTROL & AUTOMATION**

**SANS THE COST OF NETVIEW**

**WHEN YOU ONLY WANT TO PAY FOR WHAT YOU USE**



## **VitalSigns for Network Automation & Control (VNAC) from SDS**

*When continuing to pay for functionality in NetView for z/OS  
that you never use stops making sense.*

### **PREAMBLE: AN OVERVIEW OF SDS VITALSIGNS FOR NAC**

NetView for z/OS, if you think about it, is really a 'kitchen sink' product, because when it comes to functionality IBM appears to have indiscriminately included within it everything but the kitchen sink. The current release, i.e., the 2009 V5R4, for example, now includes a SOAP-based web services gateway to facilitate interactions with SOA applications. V5R4 also contains a gateway to the Tivoli Service Request Manager (TSRM) to permit the automation of product service requests. Then there is the ever present, built-in, API-level interfaces to PIPEs, LE/370, LU 6.2 and Info Bridge. In addition to all of this specialized, even esoteric, API support, there is also oodles of code in V5R4 for integration with the OMEGAMON XE product suite, Tivoli Enterprise Portal (TEP) and Tivoli Business System Manager.

The SDS VitalSigns for NAC offering, in stark contrast to the everything but the kitchen sink approach, focuses on delivering just the core, most widely used, automation, monitoring and message consolidation capabilities associated with NetView. VitalSigns for NAC is a scalpel. NetView for z/OS is

an oversized chainsaw with external fuel tanks sporting built-in GPS, a MP3 player and a fish finder.

The plethora of disparate, disjointed functionality force-fitted into NetView for z/OS is good and bad, but mainly bad. Whether you use the functionality or not, or whether you like it or not, if you have NetView for z/OS you are paying top dollar—some of it for features you have never even heard of. It is like buying your grandmother a Blackberry for Christmas and signing up for a two year contract for a data service when she doesn't even have an email account and worse still, has no interest in checking her email even if you insist on setting her up with a gmail address. Hence, VitalSigns for NAC.

VitalSigns for NAC sets out to be lean, mean and even keen. With VitalSigns for NAC there is no excess; there is no waste. With VITALSIGNS FOR NAC, you get and *pay for* just the essential system/network automation, system/network monitoring and mainframe message consolidating capabilities you need. Since you are not paying for functionality that you do not use, your costs are going to be considerably less and more reasonable. You will also get a more compact and cohesive, easier-to-master product based on a modern, agent-server architecture that enables you to run the server component away from the mainframe to realize additional cost savings. Up front, tangible cost savings by just paying for the functionality that you need, is the no-nonsense, straightforward value proposition for VitalSigns for NAC.

### **MAINFRAME NETWORKING MORPHED, NETVIEW MULTIPLIED**

Many mainframe customers are invariably surprised, in some cases shocked, when they realize how little of the overall NetView for z/OS functionality that they actually use. To be fair, given that NetView has been a mainframe institution since the late 1980s, many have never bothered to pay that much attention to what is included in any given release of NetView for z/OS. Thus, if you happen to have a slightly older release of NetView for z/OS, say V5R1 (c. 2002), you may be amused (or possibly dismayed) to discover that you still have the capability to manage and monitor Novell NetWare LANs, 14.4Kbps Hayes command-set modems and ATM networks (with ATM, in this instance, not referring to 'automated teller machines').

Mainframe NetView (V1R1) came to be in 1986 when hierarchical, mainframe-centric SNA networks ruled the corporate roost. The SNA SSCP functionality, implemented within mainframe VTAM, activated, controlled, sustained and

managed the network. Mainframe NetView, originally just the bundling together of prior SNA-specific network management products, viz. NCCF, NPDA, and STATMON, was meant to complement and enhance the SSCP functionality.

In the mid-1990s there was talk that Mainframe NetView would be structured and marketed as a base plus optional feature sets product (à la the time-honored model for selling cars). Customers would order and pay for just the features they needed. That never came to be. Then came TCP/IP, the web and the rather rapid demise of SNA networks. The basic rationale for mainframe NetView had changed, and changed dramatically.

NetView persevered, throwing in more and more functionality, SNA, TCP/IP, Sysplex, APIs, gateways and cross-product interfaces, rather than giving customers the option of buying smaller, targeted management solutions. Hence, VitalSigns for NAC.

VitalSigns for NAC, in essence, sets out to provide the core NetView for z/OS or CA's NetMaster functionality, without compromise. Additional

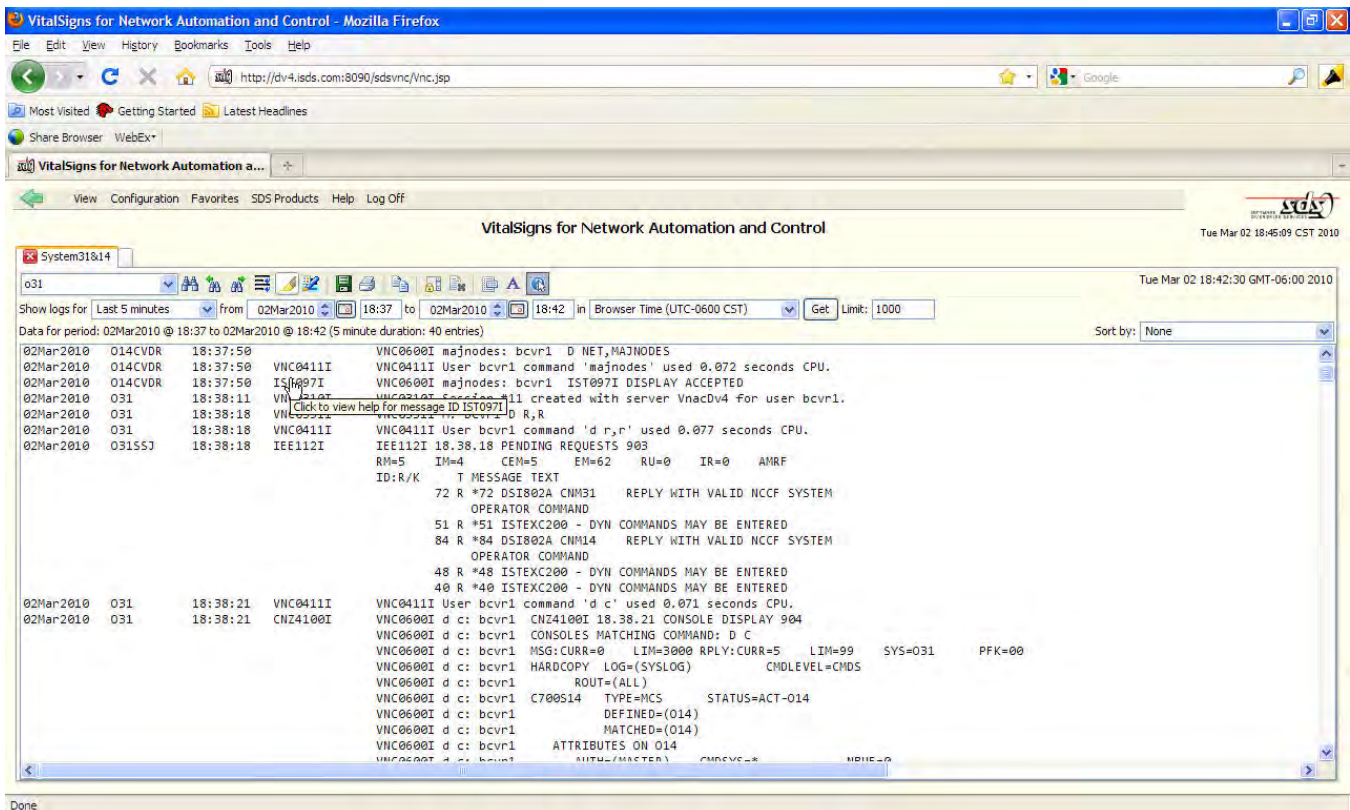


Figure 1: VitalSigns for NAC's consolidated log view feature for simultaneously browsing multiple system logs.

## TYPICAL REMARKS FROM ACTUAL CUSTOMERS AS TO THEIR USE OF NETVIEW FOR z/OS

*"We use NetView mainly for some user written scripts. We do not use NPDA or STATMON. We use logs for problem determination. On average, twenty users use basic ACT, INACT, DIS, RECYCLE commands."*

*"We have limited REXX use. We use Network logs for problem determination."*

*"Our shop uses REXX; uses basic NetView commands; uses NetView for network suppression."*

*"I Use NetView for monitoring of NCP and remaining SNA network."*

*"We Use some REXX scripts and basic commands."*

*"We use NetView for automated scripts with message automation table, for entering basic commands, and for checking log files."*

*"NetView is used here to IPL system. We rely on REXX scripts and STATMON. The shop makes limited use of NPDA."*

*"Our organization makes limited use of NetView."*



**VitalSigns for NAC** could address the NetView-related functions of all such customers

functionality, if needed, per the optional feature set concept, is available via SDS' other highly proven z/OS management offerings such as VitalSigns for IP (VIP), VitalSigns for FTP, and VitalSigns for VTAM. The goal is to rationalize and modernize z/OS management passing on the cost savings thus derived to the customers. Thus, the *potential* to immediately reduce your costs to a fraction of what you are currently paying for NetView for z/OS or NetMaster—provided you, like many NetView customers, only utilize a selected subset of its sprawling functionality.

### **DETERMINE YOUR CURRENT DEPENDENCE ON NETVIEW FOR z/OS OR NETMASTER**

You are reading this white paper because you realize that there may be a better, more cost-effective way for your organization to realize your z/OS management needs than continuing to rely on NetView or NetMaster with their budget-busting price tags. This is then the right time to take careful stock of how and when you use NetView for z/OS or NetMaster. Many organizations rely

on NetView, with REXX-based scripting, for all of their mainframe automation. Some still have a few automation tasks written in BAL. It is unlikely that you are still using any automation that was written in PL/I, in the 80s. If you do, this may be a great time to seriously evaluate, in the spirit of software modernization, whether it makes sense to standardize all of your z/OS automation in REXX.

Like most, you probably do rely, quite heavily, on the NetView command interface for system and network control and management. This command interface, dating back to the 1980s NCCF, like REXX automation, is definitely a core, extensively used, feature of NetView. You need to take a look at the browser-based command interface provided by VitalSigns for NAC. With VitalSigns for NAC you get a seamless, cross-system interface from which you can issue any and all system or network commands. Even better, it has a built-in history function whereby all previously entered commands are remembered,

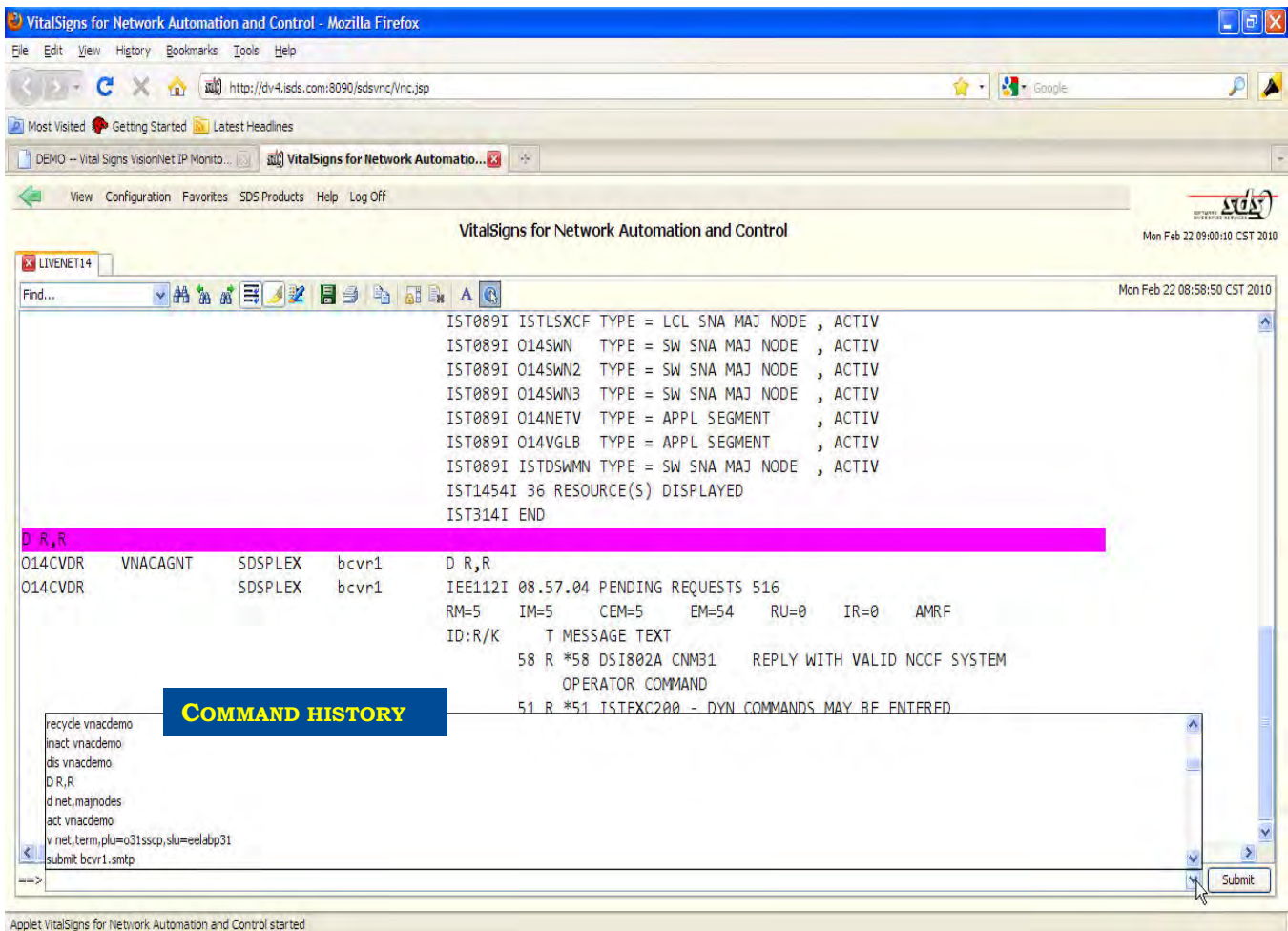


Figure 2: VitalSigns for NAC's value-added command interface with its productivity-enhancing history feature.

sorted by frequency of use. A click on the mouse will activate a drop-down tool bar with this prior command history. You no longer have to type in commands from scratch. You can just click on a previously issued command or quickly update it for your current needs.

NetView is also quite often used for consolidating system/network messages and for browsing through system logs. VitalSigns for NAC, per its goal of supporting the core features of NetView and NetMaster, caters for these functions—*with value-adds*. With VitalSigns for NAC you can carefully customize which messages you want to listen to in terms of job name, message ID or a combination of both. Thus you can effortlessly cut through the incessant chatter and just focus on specific jobs or potential incidents. It is an easy way to enhance productivity, boost operator morale and minimize disruptions.

When it comes to browsing logs, VitalSigns for NAC offers the option of a consolidated log view. The log entries from multiple, specified systems will be merged together, with the entries sorted per their timestamp. This gives you a precise, comprehensive, chronological view of system/network activity—showing how any specific event unfolded. As with VitalSigns for NAC's message filtering, this consolidated log view is guaranteed to expedite problem resolution times, significantly. It has to. Leveraging technology to help z/OS operators is a hallmark of VitalSigns for NAC.

SNA sessions, by and large, are now based on Enterprise Extender (EE) or tn3270(E). SDS' VitalSigns for IP product offers real-time, state-of-the-art monitoring of EE and tn3270(E), including end-to-end tn3270(E) Response Time Monitoring (RTM).

The bottom line here is that the most pervasively used, core (or baseline) NetView for z/OS functionality, in 2010, appears to consist of:

- the **command line** Interface for system/network commands.
- **REXX-based automation**.
- System/network **message concentration** and logging.
- SNA end-to-end **session monitoring**.
- **System log** browsing for problem determination.
- Real-time **monitoring of system/network status**.
- Access of **online help data** for faster problem resolution.

## POTENTIAL FOR REALIZING QUANTIFIABLE COST SAVINGS

If your NetView for z/OS or NetMaster usage falls within the core functionality outlined above, you should, most certainly, contact SDS as soon as you finish reading this white paper to schedule an evaluation of VitalSigns for NAC.

VitalSigns for NAC, per SDS' expressed goals, is likely to provide you with immediate, tangible, software cost savings. In these scenarios you can just replace NetView for z/OS or NetMaster with the significantly less costly VitalSigns for NAC.

The reduction in the software licensing costs though the most significant and obvious, is, however, not the only way you will realize data center savings with VitalSigns for NAC. NetView for z/OS and NetMaster are entirely mainframe-based; they utilize expensive CPU cycles, on z/OS LPARs, for everything they do. Hence, you are using mainframe MIPS even to browse a system log. This will certainly not be the case with VitalSigns for NAC. With VitalSigns for NAC's agent-server architecture you have the option to off-load nearly all of the requisite data consolidation, data analysis and data presentation functions onto less costly Windows or Linux server platforms (keeping in mind that even the cost profile for a Linux LPAR is significantly lower than that for a z/OS LPAR).

In addition, you also need to factor in the productivity and morale-enhancing attributes of VitalSigns for NAC, for example the command interface history or message filtering when browsing consolidated system logs. There will also, inevitably, be some reduction of lost-opportunity costs. With VitalSigns for NAC helping to expedite problem determination and resolution times, troubleshooters can spend their time elsewhere, on other problems. The bottom line here is that if you are looking at ways to optimize your data center spending, you should start by looking at VitalSigns for NAC.

Even if your NetView for z/OS or NetMaster usage extends beyond the core functionality set outlined above, it is possible that SDS could still provide you with attractive cost savings (not to mention some compelling value-added capabilities) with a customized, **VitalSigns for NAC with VitalSigns for IP** combo solution. VitalSigns for IP is a highly proven, state-of-the-art z/OS network manager with extensive real-time capabilities for monitoring, diagnosing and repairing IP, SNA and EE resources.

Just some of the capabilities available with **VitalSigns for IP** include:

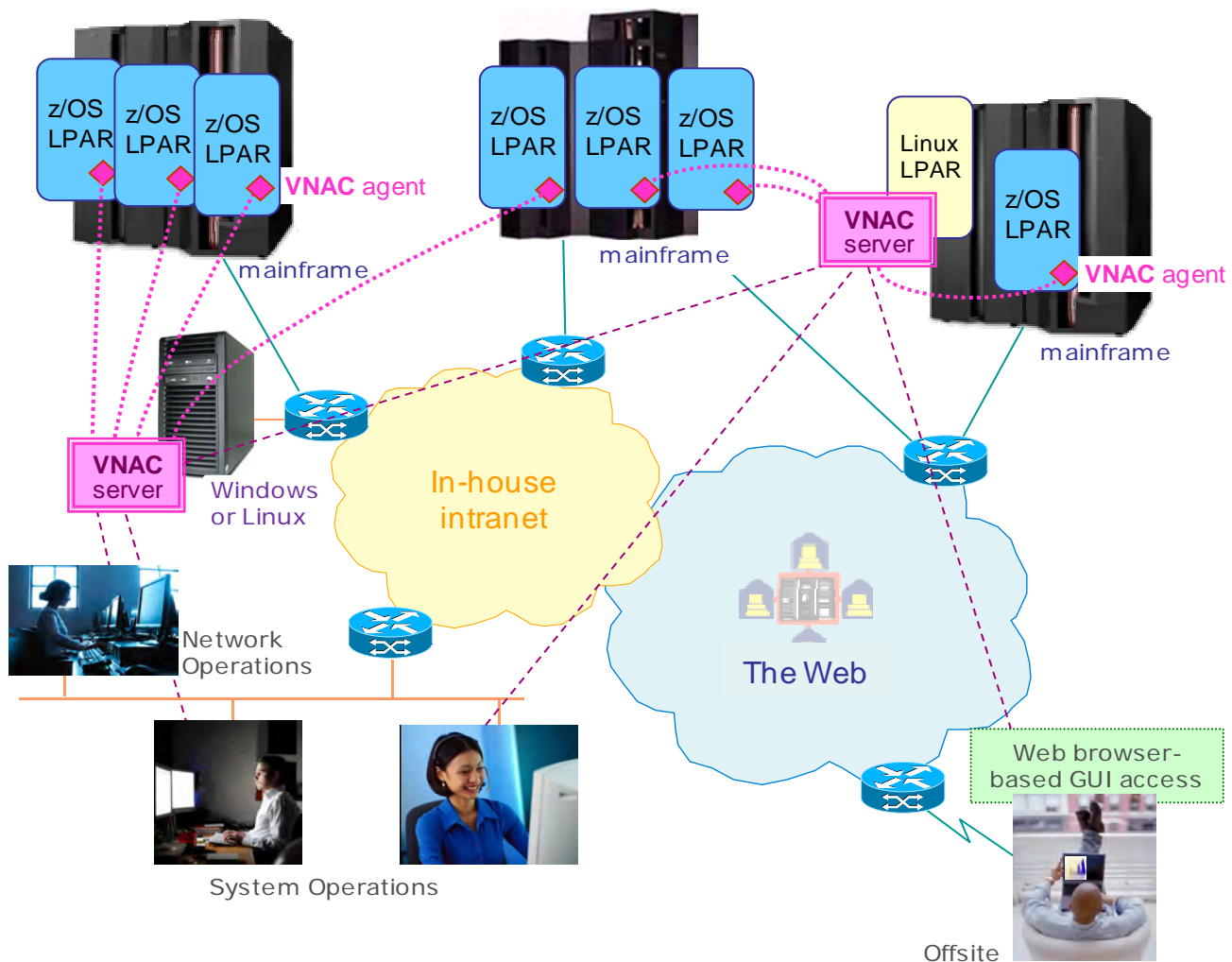
- ❖ FTP, TELNET, OSA, ENTERPRISE EXTENDER, AND SOCKET APPLICATION TRAFFIC
- ❖ TCP/IP CONNECTION MANAGEMENT
- ❖ SYSPLEX DISTRIBUTOR
- ❖ TN3270 RESPONSE TIMES
- ❖ TCP APPLICATIONS RESPONSE TIME MONITOR
- ❖ EE TRACEROUTE
- ❖ REAL-TIME IP PACKET TRACE
- ❖ REAL-TIME ALERTING AND CUSTOMIZABLE THRESHOLDS
- ❖ HEAVY-HITTERS ANALYSIS
- ❖ ONE VIEW FOR MANAGING ALL YOUR TCPIP STACKS
- ❖ EXTENSIVE BATCH REPORTING SYSTEM
- ❖ MONITORING OF REMOTE APPLICATIONS AND REMOTE HOSTS

SDS will provide you with a detailed list of all of the z/OS management and monitoring capabilities that would be available with a VitalSigns for NAC- VitalSigns for IP combo solution—along with a cost-savings analysis. So once you get to the end of this white paper contact SDS and schedule a conference call to discuss how you can stop paying IBM (or CA) for z/OS management functionality you do not need and you do not use.

## **VITALSIGNS FOR NAC'S VERY PRACTICAL AGENT-SERVER ARCHITECTURE**

NetView's monolithic approach is not unique to NetView. Way back, in the early 90s IBM did have a client-server version of NetView with PCs acting as clients to provide the necessary processing for a graphical user interface. IBM, however, developed the PC client software to run only on OS/2—IBM's ill-fated joint venture with Microsoft to develop an IBM equivalent to Windows. OS/2 is history.

VitalSigns for NAC, on the other hand, relies on a tried-and-tested agent-server architecture—the same architecture very successfully used by SDS' VitalSigns for IP since its debut in 2002. With this architecture only the agent components need to run on z/OS LPARs -- as shown in [Figure 3](#). These agent components, written in optimized IBM assembler, are responsible for



**Figure 3:** The low-overhead, flexible, cost-curbing agent-server architecture of VitalSigns for NAC with its ability to provide fault-tolerant, redundant server configurations.

monitoring and collecting the necessary z/OS data, for example system/network messages corresponding to the specified VitalSigns for NAC message-filtering criteria. These agents feed the data they collect, in real-time, to one or more VitalSigns for NAC servers (with the agents making sure that only the data that has changed (i.e., modified data) is sent to the servers so as to minimize agent-server traffic).

Deploying multiple servers guarantees resilience for 'zero downtime' mission-critical operations. The VitalSigns for NAC servers, which are implemented in Java, can be deployed on PCs running Windows, on Linux/Unix servers (including Linux LPARs), or on an MVS LPAR with Unix System Services (USS). Thanks to VitalSigns for NAC's agent-server architecture, LPARs or mainframes that need to be monitored can be easily and quickly added, non-disruptively, to an existing VitalSigns for NAC-managed network, on-the-fly.

VitalSigns for NAC's easy-to-master, very pragmatic and straightforward user interface is web-browser-based. As with the architecture, this browser-based access is another proven methodology, extremely popular with customers, borrowed from VitalSigns for IP. With this browser-based access *authorized* operators can readily access all VitalSigns for NAC services from any network-attached client running a standard web browser, even across the web—as depicted in Figure 3. This universal access is a boon for contemporary data center operations. Now, experienced or expert operators and system programmers could jump in and help out in the event of a system/network incident even if they are not on-site. This can be a great help when running a 24x7 data center operation.

### VITALSIGNS FOR NAC: THE STANDOUT DIFFERENTIATORS

When evaluating VitalSigns for NAC as a viable, cost-competitive replacement for NetView for z/OS or NetMaster you should pay particular attention to the following VitalSigns for NAC features and capabilities. It is these features and capabilities that ensure that VitalSigns for NAC will indeed provide you with the core system/network monitoring and management functions you need.

1. **COMPLETE SYSTEM/NETWORK AUTOMATION SUPPORT:** VitalSigns for NAC includes a flexible but at the same time very capable user-customizable interface. This interface can be precisely configured to listen to any

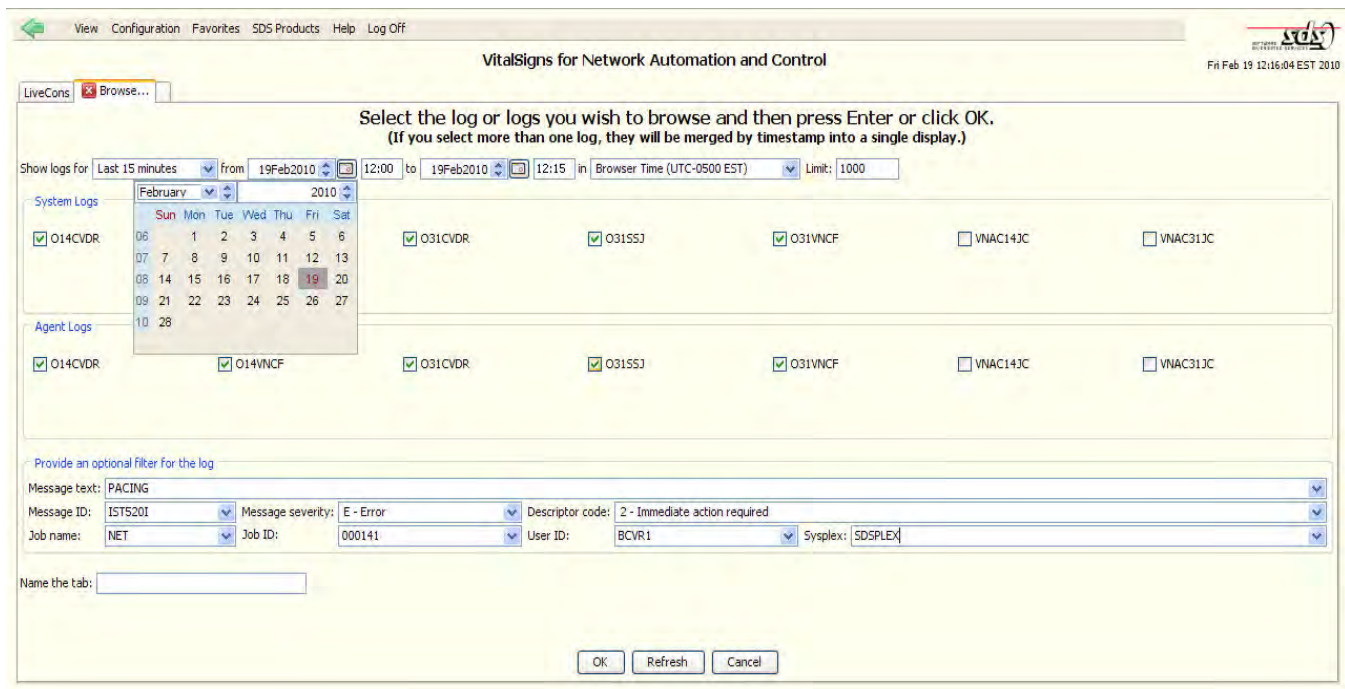


Figure 4: Using VitalSigns for NAC to select the system logs that need to be browsed, by time.

system or network message that meets pre-specified message-filtering criteria. These message-filtering criteria can be specified in terms of job name, message ID or a combination of both—with full support for ‘wildcard’ (i.e., ‘\*’) designations. Job names would typically be of the form: VTAM, CICS, TCPIP, IMS, JES etc., while message IDs, with wildcard designations, would be: DFH\*, IST\*, EZZ\*, HASP\* etc. It is also possible to exclude certain messages. Thus, for example, you could listen for all messages from VTAM with the exception of those with message IDs IST530I, IST889I & IST1096I.

The interface can be further exploited in conjunction with VitalSigns for NAC’s unstinted support for REXX and the various timers offered by VitalSigns for NAC. Using REXX, the interface and the timers, you can easily implement various levels of automation, ranging from simple to highly sophisticated, triggered by specific events or messages. (#4, below)

2. **BROWSING OF CONSOLIDATED SYSTEM LOGS (WITH FILTERING):** With VitalSigns for NAC it is possible to browse individual system logs or consolidated, chronologically ordered entries from *multiple* system logs. Please refer to [Figure 1](#). As with the interface (#1, above) extensive message filtering is available to eliminate chatter and enable operators to easily pick-out the messages of consequence as well as the ability to specify time periods of interest. Message-filtering criteria, again replete with wildcard designations, may be specified in terms of message severity, message ID, message text, job ID, job name or even Sysplex ID. Time periods of interest can be specified, along the lines of ‘the last 15 minutes’, ‘the last hour’ or ‘the last two days.’ It is also possible to define very specific customized searches, for a specific time period, based on multiple filtering criteria.

Consistency and overall integration are fundamental design goals of VitalSigns for NAC. Consequently, you can easily combine messages culled from the interface with messages extracted, per filtering criteria, from one or more system logs. This provides an additional level of system/network message consolidation. Overall, as you have probably already worked out, this carefully designed consolidated system log/selected messages view can really turbo-charge system/network problem determination. With VitalSigns for NAC, operators can easily and quickly determine how a problem came to be by following the exact message trail related to that incident. By eliminating all of the spurious

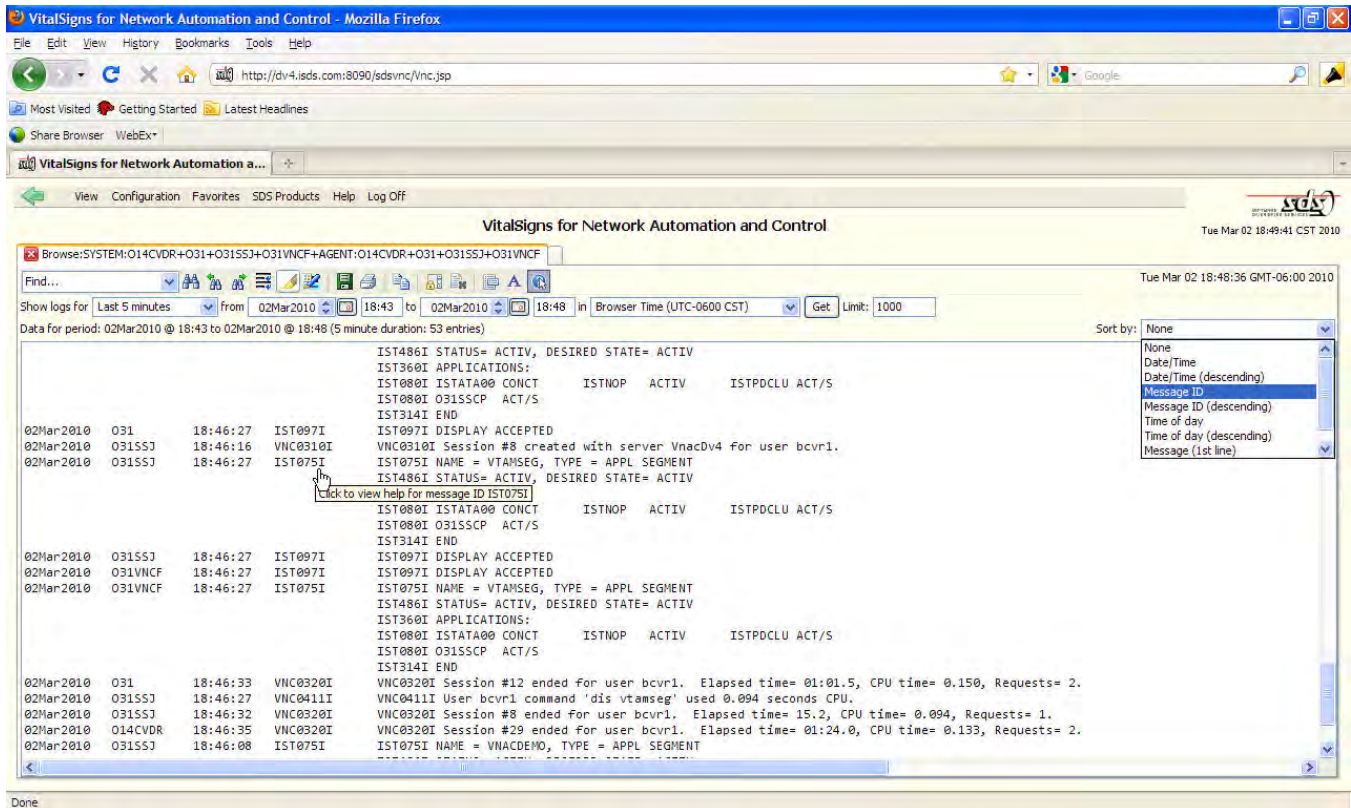


Figure 5: Consolidated system log display from VitalSigns for NAC, in this instance the messages being filtered by message ID. See the 'Sort by' menu on the right-hand edge.

chatter, the precisely filtered, consolidated view permits operators study, unimpeded, the exact circumstances that resulted in an issue. VitalSigns for NAC will thus help reduce lost-opportunity costs, minimize down time and satisfy service level agreements (SLAs).

3. **COMMAND INTERFACE (WITH HELPFUL HISTORY):** VitalSigns for NAC includes a command line interface modeled around the NCCF functionality in NetView for z/OS. Via this command interface, authorized operators can issue all appropriate system/network commands to control, manipulate and manage the mainframe environment and attached networks. As shown in Figure 2 and discussed earlier, the VitalSigns for NAC command interface includes a productivity boosting history function—similar to that provided by web browsers when it *comes to entering web address*. *VitalSigns for NAC remembers the previously entered commands*. These previously entered commands, sorted by their frequency of use, are then available to the operators via a drop-down menu. Now, rather than having to type in a command from fresh, and possibly get it wrong because of a typo caused by 'finger trouble,'

operators can just click and select the command they want from the history list. Operators love the convenience. It makes their lives easier. It allows them to get things done faster.

4. **REXX SCRIPTING SUPPORT (WITHOUT ANY CAVEATS):** VitalSigns for NAC includes unrestricted support for REXX equivalent to the REXX scripting available in NetView for z/OS. Consequently, existing REXX scripts used with NetView for z/OS can be migrated across for use with VitalSigns for NAC.

This REXX scripting is the basis for realizing system/network automation with VitalSigns for NAC. This REXX scripting in combination with VitalSigns for NAC's customizable interface, the filtered, consolidated system log access and the event timers can be used, with relative ease, to implement very sophisticated automation scenarios. To fully appreciate what can be accomplished with VitalSigns for NAC you should talk with the experts at SDS. They will be able to show you examples of existing automation scripts and help inspire you as to what your organization could implement using VitalSigns for NAC.

5. **ACCESS TO z/OS DATASETS OR DATASET MEMBERS:** The VIEW function of VitalSigns for NAC can be used to access and view z/OS datasets or dataset members (albeit subject to administrative control and the pertinent authorization and SAF access control policies). A valuable member-name search capability is included whereby VitalSigns for NAC, when given just the member name, will automatically locate the partitioned dataset containing that member. There is also an option to limit the size of dataset members that can be viewed—in the event there is a concern as to the volume of data that should be viewed via this feature.
6. **ONLINE MESSAGE HELP:** VitalSigns for NAC will provide instant, online message help for any and all system log messages (including VTAM IST) replete with return code explanations, sense code data and feedback parameters. If CICS messages are being monitored through the customizable interface (#1, above), online help will also be available for DFH\* messages.

7. **REAL TIME MONITORING OF SYSTEM/NETWORK LOGS:** In parallel to the browsing of filtered, consolidated system logs (#2, above) VitalSigns for NAC also permits operators to monitor system and network logs in real time. Depending on the tasks and message a VitalSigns for NAC operator wishes to monitor, the VitalSigns for NAC interface can even be defined as a 'TARGETED SYSTEM CONSOLE.'
8. **INSTANT COLLABORATION BETWEEN VITALSIGNS FOR NAC OPERATORS:** VitalSigns for NAC includes a nifty instant messaging (IM) capability. Using this secure IM, authorized VitalSigns for NAC operators can freely interact with each other, 'in-band' so to speak, to exchange status, request information, or coordinate recovery actions. It is a handy feature given today's penchant for texting. With VitalSigns for NAC IM, operators can work 'heads down' during 'crunch' periods without the encumbrance of having to use telephones or intercoms to get in touch with their peers.
9. **MULTI-LEVEL SECURITY:** VitalSigns for NAC offers four different modes of security that can be assigned to the various VitalSigns for NAC operators

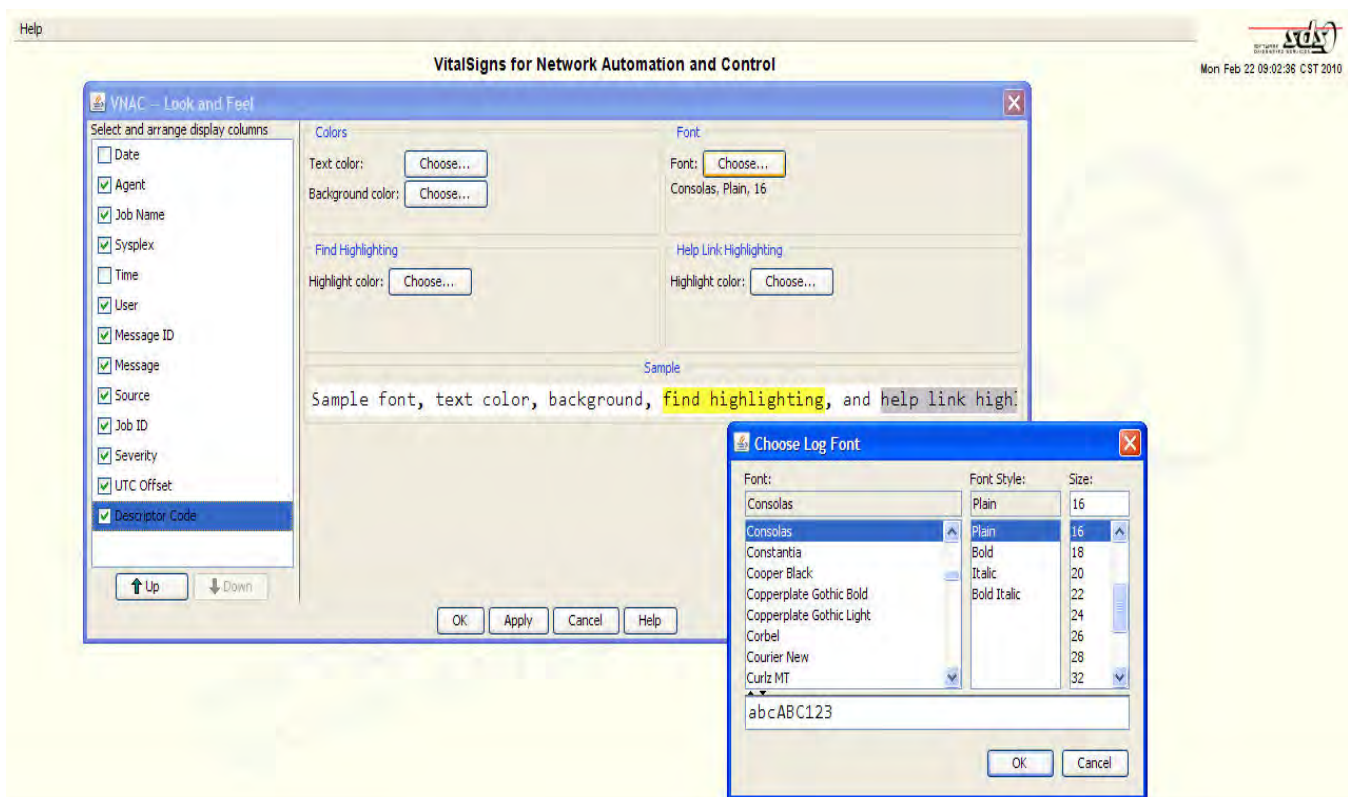


Figure 6: VitalSigns for NAC provides extensive options for customizing the look-&-feel of its user interface.

depending on their function and clearance. Thus, it is possible to ensure that only select operators have access to sensitive data or the capability to issue certain 'system meltdown' commands.

10. **AGENT-SERVER ARCHITECTURE:** As discussed earlier, VitalSigns for NAC's mainframe offload agent-server architecture minimizes the use of expensive mainframe cycles, fosters redundancy, permits the non-disruptive inclusion of new mainframes and facilitates universal access.

### THE BOTTOM LINE

NetView for z/OS is significantly underutilized in many installations around the world. Most customers have no idea, whatsoever, as to the bewildering plethora of functionality packed into each release of NetView. Despite the all the bells and whistles, not to mention a few dinner gongs and claxons, many a customer still continues to use only basic NCCF functionality from the earliest days of NetView.

If you only use the core, baseline functionality of NetView for z/OS or NetMaster, i.e., REXX-based automation, command entry, message consolidation, system log perusal and system message decoding, you definitely need to seriously evaluate why you are paying what you do to IBM (or CA). There is obviously a raft of functionality in NetView and NetMaster that you are not using, but are paying for indirectly. With VitalSigns for NAC, SDS sets out to provide the most widely used essentials for z/OS management, control and automation at a realistic price—sans the fat.

Thus, it is a very simple and straightforward call. If you only use the baseline NetView or NetMaster functionality you definitely could do better in terms overall costs, mainframe CPU utilization, operator productivity, problem resolution times, lost opportunity cost minimization and operator satisfaction by opting for VitalSigns for NAC. Since SDS will also allow you to test-drive VitalSigns for NAC, on your mainframes, for free, you can truly test out VitalSigns for NAC's strengths before you have to make any commitments. It is a no-lose scenario. If the functionality available with VitalSigns for NAC stacks up against your needs, don't vacillate, just try out VitalSigns for NAC. What have you got to lose? You could end up saving a lot of money for your organization.

At this juncture, before wrapping up, let us remind you of VitalSigns for IP. VitalSigns for IP is SDS' proven, state-of-the-art z/OS monitoring, diagnosis, and management solution for IP, SNA, EE, OSA, HiperSockets, FTP,

telnet/tn3270(E), Sysplex Distributors and HTTP applications. VitalSigns for IP includes: tn3270(E) response time monitoring (RTM), IBM's intrusion detection notifications, SNA session history, IP fragmentation analysis (for performance optimization), diagnostic tools, DVIPA monitoring, DNS lookup, SNA LU name correlation, SNMP MIB queries, IBM SMF record access and ping for both ICMP & UDP.

VitalSigns for NAC and VitalSigns for IP can be used together, synergistically, to realize a very pragmatic, targeted, powerful and affordable solution for z/OS monitoring, management, control and automation that in many cases can be far superior, from a value standpoint, than what you are getting from NetView for z/OS or NetMaster. Since there are many variables and considerations that come into play you really have to talk with SDS to determine the potential cost savings with a VitalSigns for NAC and VitalSigns for IP solution. The bottom line is that VitalSigns for NAC, and VitalSigns for IP, set out to be cost-effective by being lean and mean. With VitalSigns for NAC and VitalSigns for IP there is no superfluous functionality -- for example, esoteric SOAP gateways. You just pay for the functionality that you know you are going to use. It is as simple as that.



## SELECTED GLOSSARY

<b>ATM</b>	A once strategic data transmission scheme based on the rapid switching of 53-byte cells. Also used to refer to automated teller machines.
<b>DVIPA/ DDVIPA</b>	Virtual IP addresses used in Sysplex Distributor configurations, while DDVIPA refers to the dynamic allocation of such addresses.
<b>EE</b>	HPR-over-UDP/IP, created by committee and codified in RFC 2353 in 1998, which permits SNA/APPN networking, replete with native COS and routing, across IP networks.
<b>FTP</b>	File Transfer Protocol.
<b>HiperSockets</b>	TCP/IP-based, inter-LPAR communications scheme.
<b>Intrusion Detection System</b>	Intelligent systems that attempt to intercept unauthorized access into computer systems or networks by proactively monitoring suspicious activity based on previously identified policies.
<b>LPAR</b>	An independent, mainframe image (or a mainframe virtual machine) created through software within an IBM mainframe.
<b>LU</b>	SNA's software interface (or 'port') through which end users gain access to the SNA network.
<b>MIB</b>	Management information base, a database of network management objects for a given entity.
<b>NCCF</b>	IBM application to provide a network operations oriented interface to ACF/VTAM and permit network operations automation via scripting.
<b>NPDA</b>	IBM's original management application for centralized problem determination in SNA networks.
<b>OSA</b>	Strategic, high-speed LAN adapter on mainframes.
<b>REXX</b>	High-level, easy-to-master interpretive programming language developed by IBM in the late 1970s. Now the preferred means for mainframe scripting.
<b>SAF</b>	Security Authentication Facility; e.g., RACF, ACF2 or TopSecret.
<b>SMF</b>	IBM's long-standing System Management Facilities (SMF) mechanism for collecting mainframe-related management information via application generated SMF records.
<b>SNMP</b>	Set of TCP/IP-centric network management protocols.
<b>SSCP</b>	SNA's System Services Control Point, in an hierarchical network, typically implemented on a mainframe within VTAM, that is

	responsible for directory services and configuration management. Now superseded by the peer-to-peer oriented functionality of APPN/HPR control points.
STATMON	IBM-speak for status monitoring.
telnet	TCP/IP-based terminal protocol for application access.
tn3270(E)	3270 specific variant of telnet that works on a client-server basis.
tn3270(E)	Widely used, client-server technology that permits TCP/IP clients to access mainframe-resident SNA applications using 3270 data streams.
VitalSigns for FTP	SDS' management and security enhancing product for FTP.
VitalSigns for IP	SDS' highly popular, state-of-the-art z/OS network monitoring product.
VIPA	Virtual IP address, akin to an alias, assigned to a mainframe IP resource (e.g. stack, OSA interface, TCP/IP application), to facilitate fault-tolerance and resource movement by masking the actual IP addresses of resources from external entities.
VitalSigns for VTAM	SDS' economical performance monitor for TCP/IP and SNA networks.
VTAM	IBM's mainframe-based software for implementing an SNA/APPN/HPR node within an LPAR.



## SOFTWARE DIVERSIFIED SERVICES

Software Diversified Services (SDS), ([www.sdsusa.com](http://www.sdsusa.com)) based in Minneapolis, MN, has been providing premium mainframe solutions to the IBM world since 1982. It has licensed in excess of 1,000 mainframe customers worldwide.

SDS' mainframe product repertoire now includes over twenty z/OS, VM and VSE products, with the highly regarded VitalSigns for IP (VIP) being one of these. SDS also markets PC software related to mainframe operations. The products marketed by SDS focus on network management, performance monitoring, report distribution and data compression.

SDS is noted for having the highest quality software, documentation, and technical support in this industry sector. SDS technical support has been rated #1 by the prestigious IBEX Bulletin.