NTP's *System Sentinel* –
The Server Lubricant for Windows

Analyst: Joseph De Natale

Management Summary

Are you attempting to run mission-critical systems on a cranky engine that seems to run in spurts and starts? Are you trying to operate your systems to provide non-stop, reliable service to your users with technology that may sputter and fail at the most crucial times? Need an additive to make your Windows NT applications run smoother? Like that cranky engine, does your system fail at the most inopportune times just when you needed it most? **With Windows-based servers playing a more critical IT role in an enterprise, more tools are needed to improve the reliability of the systems.** An enterprise needs to reduce downtime, improve reliability, and make its systems more secure against virus and hacker attacks to enhance availability of the enterprise's IT infrastructure system. **As more and more enterprises seek more ways to achieve 24x7x365 availability, System Sentinel from NTP may be the lubricant that makes Windows system more responsive to enterprise needs.**

The latest release from NTP Software of System Sentinel provides users with added functions that make the ride easier. Along with the original features, this release adds new capabilities such as fault tolerance and additional templates for applications such as Lotus Notes/Domino and Microsoft Exchange. **These two features make the task of system administrators easier, but more importantly, add to the reliability and availability of mid-to-large Windows servers with the users of these systems being the ultimate beneficiaries.**

NTP Software Sentinel product is built on its EASE framework technology, which makes distributing and managing System Sentinel a straightforward and easy task for administrators. System relationships and configurations are easily changed from the central Administrative Console with a simple drag and drop. When a change is made in configuration settings for one machine, the change is sent to all other machines, guaranteeing that all current information can be accessed from any other server. The Console is the central point for configuring and displaying all of System Sentinel's filters, and monitors all functions, which can be activated by the Console. **Migration from Windows 2000 to Windows NT becomes a straightforward task since applications enabled under EASE will operate without change as they are transferred from one platform to another.** For the details, read on.

New Features

The addition of fault tolerance capabilities to System Sentinel improves the reliability of the total system. In the event that the primary server fails, monitoring data is automatically sent to the next proscribed server in line. The system can be set up so that a cascading number of servers can be assigned the responsibility for collecting system data, allowing continuous monitoring. The system performing temporary backup monitoring function continues to monitor the primary system and returns control to it. NTP's System Sentinel is one of only a few applications that offer a monitoring and failover capability for its own software, a feature that should weigh heavily in evaluating software intended to enhance system reliability. For users concerned with continuous system availability, fault tolerance of the monitoring software gives additional assurance that enterprises will experience fewer outages.

The Event Log monitors gather only specified information for monitoring that passes through user-determined filters. Only those events, which will affect system availability, are presented to the Administrative Console System Sentinel monitors a variety of events including those from Windows NT/2000, Linux and UNIX SYSLOGS, TCP/IP and ASCII logs. Event chaining reduces the amount of information presented to the console by automatically preventing events beyond the failed system component. For example, if a router goes down, there is no need for information on the other side of the failed router.

Additional templates for monitoring Lotus Notes/Domino and Microsoft's Exchange software have been added to System Sentinel, giving users of these applications greater availability. These templates monitor ASCII logs, event filters and performance monitor counters in these applications. These templates are in addition to those already supported in System Sentinel: Citrix MetaFrame, Microsoft IIS, and Microsoft SQL Server and others.

Solid Foundation

The major components of System Sentinel are the Administrative Console that acts as the centralized location for monitoring and configuring the system parameters, and the

---

System Sentinel – Key Features At A Glance

- **Architected under NTP's EASE** distributed management technology, the basis for all NTP products.
- **Enforces quotas on storage use by user.** Individual limits can be incrementally monitored (i.e., by percentage of quota) and notification of reaching threshold can be sent to the user.
- **Employs policy-based storage management and administration** so that the enterprise's business needs are satisfied.
- **Restricts the types of files users can download**, such as MP3 or unlicensed software or other unauthorized software. Prohibition can be designated by specific type of file.
- **Protects the system from virus infection.**
- **Generates reports** on usage for charge back, reporting, or system administrative purposes.

Event Dispatcher Server. The Event Dispatcher Server (EDS), which runs on Windows NT SP4 or Windows 2000, provides the collecting facility from System Sentinel installed agents in the system, and processes the data according to preset parameters. It then transmits the completed information to the Administrative Console for monitoring and action, when the need arises.

The capability for monitoring by System Sentinel extends to Windows NT/2000 event logs, UNIX and Linux SYSLOG's, and TCP/IP servers and devices. In addition, applications such as e-mail, e-business processes, and web servers can be managed with automatic response to anticipated problems, permitting users to approach 24x7 availability.

With System Sentinel, automatic restoration of applications can be accomplished unattended, at any time. When problems occur outside the range of its capabilities, or when an automatic restore

previously defined does not work, System Sentinel will automatically notify or page appropriate personnel. For users this means that they have greater assurance that the system will be available when they come to work the next morning, and that they will be less plagued with extended down times.

System Sentinel can monitor CPU usage, logs, or disk usage on particular systems. When usage grows beyond a specific predetermined limit, several actions are available. Automatic action can take place, manual intervention, or in the event of a failure to remedy the situation, automatic notification to personnel, whose responsibility is to perform remedial action, can be accomplished by a Windows message, e-mail, or by pager.

Performance monitoring of the system or components of the system is simplified by Systems Sentinel's flexibility of setting polling sequences. Event-driven Corrective Action takes place in real time to keep the application or system running. A particular agent called the System Sentinel Service Watcher (SSSW) monitors the state of Windows services. Detection of the service either failing or stopping alerts SSSW attempts to restart it automatically, or will reboot the service either immediately or on a predetermined schedule.

NTP offers more secure systems by minimizing the effects of denial of service attacks. The system monitors access to the site and alerts the administrator if the number of successive accesses exceeds a predetermined limit. Hacker attempts to break into the system is minimized by alerting the administrator if 5 attempts to login fail in 5 seconds. The attempt to inject a virus into the system is limited by System Sentinel by alerts, which permits administrators to stop the spread of the infection to other applications.

Script capability is supported through Microsoft Windows Scripting Host support for users who need or desire to write scripts not available with the system.

Complementary Product

If an enterprise has a large or distributed environment consisting of Windows NT or Windows 2000, IT managers can keep their computing engines running smoother by adding NTP Software's Quota and File

Sentinel to their portfolio of system management products. One of the resources that can affect system performance is the use of disk space. When disks become full, the easy way to overcome that problem is to throw additional hardware at it. But there are financial and technical limits to that. **After setting limits on the use of file space by user and application, NTP's Quota and File Sentinel continually monitor their use.** Users are notified when they are close to their assigned limit. IT prevents them from exceeding it without administrative intervention. Additionally important in maintaining high levels of availability and proper use of computer resources are Quota and File Sentinel's capability to prevent virus penetration into the system. It can also block system downloads of unauthorized or unwanted files such as MP3.

Conclusion

Windows 2000 and NT systems are the legacy wannabes of the IT world. These systems have lacked many of the tools that provide the same tools that we take for granted in legacy systems. The features of RAS, - Reliability, Availability and Scalablity, - are goals that have been desired for some time to make the Windows end server an enterprise worthy system. **NTP's System Sentinel product is the lubricant that tames the cranky Windows engines and makes the ride for the users less fraught with the unknown system failure.**

About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

➢ *The Clipper Group can be reached at (781) 235-0085 and found on the web at www.clipper.com.*

About the Author

Joseph S. De Natale is Director of Enterprise Systems Planning with The Clipper Group. He brings more than forty years of experience in the data processing field with particular emphasis on systems management and application development on large-scale mainframes. Prior to joining The Clipper Group shortly after its founding, Mr. De Natale was an independent consultant, first with Ropes and Gray, Attorneys at Law, where he provided expert opinion on data center management for civil cases. He later joined International Data Corporation (IDC), as a senior consultant and analyst, where he covered banking systems, data center management software, and large systems computers and storage. Formerly, Mr. De Natale spent eleven years at Citicorp Information Resources (CIR) as CIO of the Boston Data Center, where he managed the support of over 200 outsourcing contracts for thrift institutions. Earlier, he was MIS Director for the Lahey Clinic, and prior to that was a Project Manager for Computer Sciences Corporation, where he was involved with NASA and FAA outsourcing and applications contracts. Previously he was Director of AVCO Computer Services for fourteen years. At AVCO, in addition to being responsible for all internal data processing, he initiated the marketing and sales of computer services to commercial clients. Mr. De Natale began his career with Pratt and Whitney Aircraft as a programmer of nuclear physics and business applications. During his career, Mr. De Natale was involved in the evaluation, installation and operation of large-scale mainframe systems and for the development of commercial, scientific and engineering application systems. He has also had successful experience in the marketing and operation of outsourcing contracts. Mr. De Natale earned a Bachelor's and Master's degree in Mathematics from Boston College. During his period at AVCO, he was selected by AVCO to attend the Northeastern University Management Development program, a co-op program covering an MBA curriculum.

➢ *Reach Joe De Natale via e-mail at denatale@clipper.com or at (781) 235-0085 Ext. 24.*

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, and **The Clipper Group** Captain's Log are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and "teraproductivity" are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.