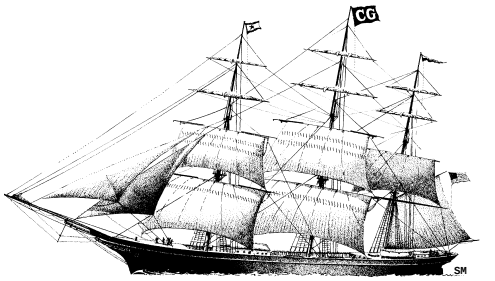
THE CLIPPER GROUP
Navigator™



Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2005033 June 1, 2005

The Benefits of Comprehensive, Extensible Remote Management of Hardware Infrastructure

Analyst: Anne MacFarland

Management Summary

The need to troubleshoot effectively and on the fly has never been more urgent. Many data centers are centralized in concept only, and are responsible for servers at many locations, as well as for the health of the system as a whole. If you are in this situation, and have been dashing (or dispatching people) from pillar to post for some years, it is time to pause and consider what remote management now could do for you. "Bah!" you may say, "that means a different console and a different set of tools for each brand and there is no way that the standards to make that really work are coming any time soon." Well, there is a standard that covers device health, power, and environmentals. It is *IPMI (Intelligent Platform Management Interface)*, introduced by Dell, Intel, HP, and NEC in 1998, and it has been used by KVM switch-based solutions to provide independent remote management of server environments. Late in 2004, NICs were re-designed with a side band to offload transmission of management information from the main processor. This design permits an embedded controller chip to transmit information to a remote console, when a processor ails, hangs, or fails. The embedded capability provides a slightly less "out-of-band" but far-easier-to-deploy alternative to a KVM-based system. OS-dependent instrumentation or resident agents, by contrast, are disabled when the device fails. IPMI chips are in every server shipped by Dell and IBM since September 2004, and also in an expanding list of branded and white-box elements from major and minor vendors. The IPMI capability does have to be turned on, however, for security reasons. This may not have been done when the capability was less prevalent and usable.

Avocent Corporation (Huntsville, Alabama) makes the firmware for the chips that enable IPMI. It also makes KVM switches that allow and administrator to control and diagnose many computers from a single place using IPMI information. Avocent has surveyed data centers and found woeful ignorance and neglect of the capabilities that IPMI affords. IPMI is not some big, seven-figure-pricey hunk of iron accessorized by a direct sales force with a compelling and carefully crafted line of patter about its every virtue. The features of IPMI may be subtle, but their aggregate virtue is huge. Take a look at the bigger picture of your entire hardware infrastructure, besieged by big demands, level-set budgets, and an escalating cost of down-time. Think of the remote equipment for which you are also responsible, and the risks a less-than-locked-down environment poses. IPMI-based management a classic case of the little, pervasive stuff – stuff you may already have - that can make a huge difference. Read on for more details.

IN THIS ISSUE

Four Reasons to Go with Remote Management Via IPMI

Reason #1: Autonomics are great, but an independent source of information, in addition, is even better

If your systems instrumentation is part of the software supported by BIOS or the operating system (such as an agent), when the system crashes, so does your ability to diagnose what is wrong. If the management information is also dependent on the network stack of the operating system, and that has a problem, your ability to diagnose goes down with the networking.

To get adequate documentation of faults and forensics of failure, you must have an *independent* subsystem for management, with an independently supported network access that can relay information for aggregation and analysis. To be more useful, this should not be part of the operating system, which may be a contributing party in the situation. No element should be its one and only doctor.

Reason #2: Independent, detailed metrics let you employ comprehensive analysis, not a litany of scapegoats

The difficulty of fault isolation increases factorially as the number of elements involved increases. In today's data center, the switches, gateways, accelerators, etc., that lie between a process and its data make fault diagnosis a very complex problem**. The need to correlate quickly the different elements involved in a** situation **demands that this be done from one console, using one set of tools, for not just the server and the storage, but for all elements in between.** Obviously, this scope of control requires moving control from the consoles on the elements themselves. Where this console is located is immaterial, as long as it is secure. The remoteness may well be a secure laptop that travels with the administrator.

Who is Avocent?

Avocent was formed in 2000 by the merger of two major KVM (keyboard-video-mouse) switch manufacturers. It has a more than 20-year heritage, and an enduring focus on IT management through hardware elements. It has grown by acquisition to encompass all the elements and capabilities needed by today's data center (embedded, wireless, serial, digital, or analog, and compression, for all of the above).

Avocent's Products

- ***KVM over IP switches*** (digital, serial, analog, and combined analog/digital) let administrators control the functionality and environmental systems of all their data center, remote, wireless, and/or serial devices from one remote console. Features include single sign-on, authentication and role-based access, encryption, LDAP support and GUI features like resizable windows.
- ***DSI 5100, the Avocent IPMI proxy appliance,*** hosts the *DSView 3* software (see below), and tales the UDP transmissions from controller chips, converts them to TCP and sends them to the administrator s console. This avoids the risks of transmitting UDP over IP.
- ***DSView 3*** software is the means by which you manage your infrastructure and use all of the above elements. The database of information on the central management hub server is mirrored to up to 15 spoke servers. Administrators securely log on to one of the servers to manage the elements for which they are responsible, wherever those elements reside.

  The hub and spoke architecture lets administrators coordinate for transparent administrative hand-offs. The symmetry of the system is highly resilient and supports real-time updating. It produces a detailed audit log and can interface with IT management systems. Security is enabled by internal and external authentication, selectable encryption, and exit macros to log out ailing devices on session termination to limit their vulnerability.
- ***Virtual Media*** is software for KVM switches that emulates physical removable storage devices (such as CDs or memory sticks) by which administrators have traditionally installed patches, upgrades, etc. Use of *Virtual Media* reduces the need to enter the data center physically, making administrators more available and the physical environment more secure.

Reason #3: Proper analysis of hardware infrastructure underlies all higher level optimization

The remote and extensible monitoring of hardware underlies application optimization – the activity that matters most to the business. Without it, the ability to diagnose faults higher up the stack in applications is compromised, and the ability to solve a problem so that it does not happen again (and again and again) is seriously impaired. **As enterprises move to linking applications into composites or to improving server utilization via partitions, virtual machines, or grid-style opportunistic provisioning, the ability to monitor a domain from one console becomes truly mission-critical**.

Reason # 4: Leaving your console to do hands-on management of devices increases the risk that you will be unavailable

You cannot physically be in many places at once. For many, the move to an independent, centralized, remote management paradigm often is triggered by the challenge of managing power in the data center. Moving to remote management gets the administrator out from behind the eight-ball of localization. It also puts the data center servers into a "Fewer touches, less trouble" higher-security paradigm.

Avocent System Diagnostics Architectures

Avocent gives its customers two ways to implement independent management systems. With the classic KVM switches, Avocent's array of switches, management hub, and consoles provide a resilient network for assuring that the health of data center hardware is well managed.

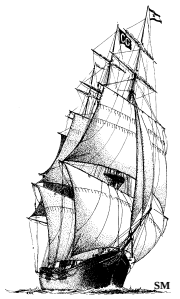
With the controller chip-based architecture, Avocent provides the firmware for the chip, the proxy server, the console, and the middleware to tie them together. There is less hardware to deploy than with traditional KVM switch-based solutions, and the system uses the LAN rather than a separate network.

The Age of Remote Management

It is an inevitable part of the security demanded by modern business life that you are going to have responsibility for things that you cannot touch physically. Kiosk-enabled "everywhere" computing is the latest evidence of technology's move to sealed, do-not-open elements. Take a look under the hood of your car. If you are old enough to remember the days of highly mechanical engine departments, you will notice a change to sealed elements analyzed by remote diagnostics. And, the trend is even more widespread. Ecologists are finding out that robotic motes can document more, while disturbing less, than can human observers blundering about stepping on things. Similarly, for technology elements, the best management is both effective and non-intrusive.

Conclusion

There are many automation tools being produced that promise to make your life as a data center administrator easier. There is a lot of self-managing hardware that will take away a lot of routine decision-making. And, still, there is a need to know what is happening, and how change affects other elements in the system. **Things will still go wrong, and the cheapness of "commodity" hardware does not remove the need to analyze the fault to find the cause to keep it from happening again.** An extensible set of instrumentation that functions independent of the health of the devices in question, is a good base line for the brilliance of your diagnosis. If your technology supports IPMI, turn it on. If it doesn't, consider a KVM switch because, in administration, rogue elements eviscerate your ability to diagnose. Completeness counts!



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

Anne MacFarland **is Director of Infrastructure Architectures and Solutions for The Clipper Group.** Ms. MacFarland specializes in strategic business solutions offered by enterprise systems, software, and storage vendors, in trends in enterprise systems and networks, and in explaining these trends and the underlying technologies in simple business terms. She joined The Clipper Group after a long career in library systems, business archives, consulting, research, and freelance writing. Ms. MacFarland earned a Bachelor of Arts degree from Cornell University, where she was a College Scholar, and a Masters of Library Science from Southern Connecticut State University.

- ***Reach Anne MacFarland via e-mail at Anne.MacFarland@clipper.com or at 781-235-0085 Ext. 128. (Please dial "128" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group** *Captain's Log*, **The Clipper Group Voyager**, and *"clipper.com"* 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.