Access to this document has been brought to you by KnowledgeStorm. You are welcome to distribute this document freely to other colleagues who might find the content valuable.

If you are a registered user of KnowledgeStorm.com:

- This document will open automatically for you.
- You can save this document on any computer.
- You should save this document before emailing to anyone else.
- If you access this document on a different computer, you will need to log in to view the document.

If you are not a registered user of KnowledgeStorm.com:

- This document will not be visible until you register at KnowledgeStorm.com.
- The registration is free, fast, and painless.

Document Summary

Enterprise Remote Management - The Role of Remote Management in Assuring IT Infrastructure Uptime
by Raritan Computer, Inc.

Published on: September 01, 2005
Type of content: Vendor White Paper
Format: Adobe Acrobat (.pdf)
Length: 8 Pages
Price: Free

Overview:
Industry attention has been focused on monitoring the IT infrastructure. But when it comes to actually fixing and validating repairs + IT professionals typically resort to a hodgepodge of expert opinion and software, often with huge chasms of inefficiency. This is ironic, since operational efficiencies in repairing critical devices have become more and more important. This is because more advanced infrastructure monitoring with higher levels of automation will place greater demands on fast and efficient device remediation in order to complete the management process - whether it's availability or performance related. While it's not a new idea, the need for accelerated Mean- Time-To-Repair (MTTR) and enhanced Uptime still remains paramount in most IT organizations, whether mid-tier or enterprise, and in most environments is still not being satisfactorily addressed.

It is perhaps ironic then that fundamental capabilities in actually diagnosing and repairing devices is so often overlooked, given the industry emphasis on cost effectiveness and alignment in supporting business goals. Versatile out-of-band and in-band remote management capabilities have demonstrated as much as a 92% decrease in labor costs for managing devices in distributed environments, and a 66% decrease in the actual time for fixing a problem once it's occurred. Moreover, such capabilities for remote device management help set the stage for longer-term initiatives such as adaptive and on demand management, when realtime device control will become paramount.

Remote management can also contribute to another set of enterprise initiatives which are becoming more and more top-of-mind in enterprise IT: security and compliance. Through flexible, but role-assigned, access control to monitoring and repairing devices supporting key applications, remote management can help ensure that operations is accountable in its support of critical business services.

This report addresses the role and value of remote management, including KVM (keyboard, video, mouse) switches and other "Out of Band" (OOB) capabilities in

Overview Continued:

assuring IT infrastructure control, in context with broader market trends and current market alternatives.

The Role of Remote Management in Assuring IT Infrastructure Uptime

A White Paper Prepared for Raritan Computer, Inc.
July 2005

The Role of Remote Management in Assuring IT Infrastructure Uptime

Table of Contents

ENTERPRISE MANAGEMENT
ASSOCIATES

The Role of Remote Management in Assuring IT Infrastructure Uptime

Executive Introduction

Industry attention has been focused on monitoring the IT infrastructure. But when it comes to actually fixing and validating repairs – IT professionals typically resort to a hodgepodge of expert opinion and software, often with huge chasms of inefficiency. This is ironic, since operational efficiencies in repairing critical devices has become more and more important. This is because more advanced infrastructure monitoring with higher levels of automation will place greater demands on fast and efficient device remediation in order to complete the management process – whether it's availability or performance related. While it's not a new idea, the need for accelerated Mean-Time-To-Repair (MTTR) and enhanced Uptime still remains paramount in most IT organizations, whether mid-tier or enterprise, and in most environments is still not being satisfactorily addressed.

It is perhaps ironic then that fundamental capabilities in actually diagnosing and repairing devices is so often overlooked, given the industry emphasis on cost effectiveness and alignment in supporting business goals. Versatile out-of-band and in-band remote management capabilities have demonstrated as much as a 92% decrease in labor costs for managing devices in distributed environments, and a 66% decrease in the actual time for fixing a problem once it's occurred. Moreover, such capabilities for remote device management help set the stage for longer-term initiatives such as adaptive and on-demand management, when realtime device control will become paramount.

Remote management can also contribute to another set of enterprise initiatives which are becoming more and more top-of-mind in enterprise IT: security and compliance. Through flexible, but role-assigned, access control to monitoring and repairing devices supporting key applications, remote management can help ensure that operations is accountable in its support of critical business services.

This report addresses the role and value of remote management, including KVM (keyboard, video, mouse) switches and other "Out of Band" (OOB) capabilities in assuring IT infrastructure control, in context with broader market trends and current market alternatives.

Managing for Uptime

Like it or not, businesses are becoming more and more dependent upon IT services and the infrastructure that supports them. There are a number of reasons for this, virtually all of them having to do with business competitiveness. Just a few of these include:

- The growing need for global reach to expand existing markets and tap new markets.

- The added efficiencies of automating software applications to capture what has been done manually in the past.

- The accelerating role of Web-based applications for communication, business transactions and information sharing.

- An expanding IT infrastructure that is not only enabling unparalleled geographical reach, but which is supporting complex business-to-business and business-to-consumer relationships, and which in some cases is enabling entirely new kinds of business and consumer services.

- The high cost of downtime to businesses, which in some verticals can be as high as $14 million a minute.

Given these requirements, the importance of uptime for IT services should become obvious. Mean-Time-To-Repair (MTTR) and Mean-Time-Between-Failure (MTBF) are not only established SLA metrics in many environments, they have become almost visceral indicators of success and failure. Reducing MTTR means both happier consumer customers and significant operational savings. Ensuring that fixes are correctly made can also reduce MTBF so that IT can emerge from being a less reactive, fire-fighting organization into one that is more capable of satisfying the business it supports. Needless to say, with hundreds of thousands of devices to sort through across a geographic dispersed organization, there are challenges to reducing downtime, as indicated below. This makes the need for speedy and effective resolution even more critical and more valuable.

Barriers to Reducing MTTR and Expanding MTBF

In spite of this clear requirement to minimize MTTR and maximize MTBF, most IT organizations remain trapped in a kind of circular motion, in which they try unsuccessfully to emerge beyond a purely reactive paradigm. There are many reasons for this – a few of the more salient are listed below.

The Role of Remote Management in
Assuring IT Infrastructure Uptime

- The number and geographic dispersion of infrastructure components is rising, as IT infrastructures expand and become increasingly interdependent across businesses. The dramatic acceleration of infrastructure components has more than offset the fact that the MTBF for most devices shipped today is significantly better than it was in the past.

- As the number of devices and functions per IT professional increases, so does the probability for human error. EMA research indicates that more than 50% of IT infrastructure failures are due to human errors.

- The growing density of the new device infrastructure is also a factor. An increased concentration of functionality in a chassis or networked environment – raises the potential for a failure. Multi-blade server chassis, server clusters and decoupled storage farms are on the rise in data centers. At the same time, a growing volume of wired and wireless transmissions and new applications and network services, such as VoIP and VPNs, are demanding higher density routers.

- Cost still remains a dominant barrier to minimizing MTTR. While IT organizations are more willing to invest in management and control than in the past, they need to be shown clear value before investing. This pressure to "cut corners" can lead to more vulnerable infrastructure with less than adequate support.

- Security threats are more pronounced than ever and from a wider variety of increasingly sophisticated sources. Security problems have become a major factor in slowing MTTR and shortening MTBF.

Marketplace Barriers in Achieving Effective Solution Choices

While the enterprise management marketplace is rich in both choice and range of technologies, and while those choices are growing, the sheer array of choices can become a negative. Figure 1 shows recent data from EMA research on time to resolve problems, from awareness to validation that a proper fix has occurred for n-tier Web-based applications. It should be noted that the average respondent, often an applications architect, used at least nine brand names and even more tool sets, and was still not fully satisfied with functionality. The result is the kind of tool set fragmentation that is indicated in Figure 1.

From Figure 1, it should become clear that, while enterprise systems management vendors are making valuable functional technology and functional advances, the vast array of choices and the complexity of many management deployments, are still leading IT adopters towards fragmented though costly tool set investments.

These percentages reflect brand presence in EMA research targeted at products used to monitor, alert, diagnose, fix and validate correct repairs for critical, distributed Web-based services.
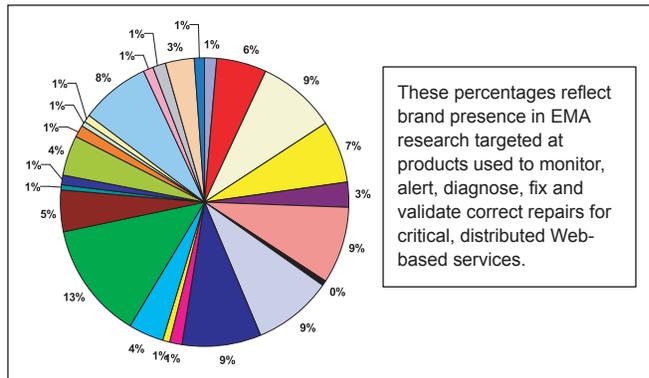
Figure 1: Tool set Fragmentation in Enterprise Management

The result can be tremendous operational overhead with a far from successful management result. Mid-sized businesses are especially poorly served, as their resources for capital and operational investment are considerably less than their larger counterparts. The marketplace is just beginning to provide mid-sized businesses with affordable and pragmatic options for taking charge of the infrastructure and service management needs. Typically, these businesses require tightly integrated functional breadth, as well as deployable solutions with minimal administrative overhead. They also need solutions that can empower a smaller base of skilled professionals to manage what are, in many cases, issues as fully complex as those that larger enterprises face. One of the options that can help mid-tier entrants is remote management, as will be described below.

In-band Tools

The vast majority of solution options for enterprise management are "in-band" products that depend on production-level networks for connectivity. These classic monitoring packages, including platforms such as HP OpenView and CA Unicenter, and a whole host of point solutions, address a range of disciplines and tasks, for example: network and systems management, vulnerability scanning, security, asset management capabilities, traffic analysis and desktop management including solutions from Microsoft and other vendors. All in-band management solutions depend on network connectivity

to gather information for accurate monitoring. Once a connection is severed or the network goes down, then connectivity is lost and most management tools lose touch. In-band solutions also depend upon a healthy OS – which becomes another type of barrier that can force technicians to travel for "at-the-rack" access. In some cases, agents on devices contain diagnostic information that will also be unavailable once connectivity to the device is lost. And while some of these solutions provide automated or active management capabilities, the majority have no real direct device "fix" functionality.
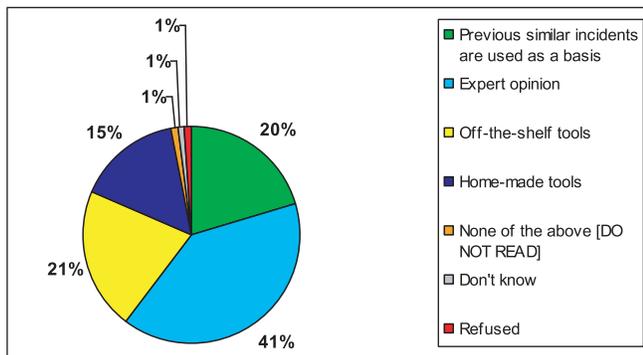

Figure 2: High dependence on expert opinion is an indication of dissatisfaction with existing toolsets

Figure 2, taken from the same EMA research on problem resolution in fixing infrastructure and application issues in n-tiered Web-based application environments, highlights IT dissatisfaction with existing tool sets. The figure shows that far and away the single highest percentage of causes for failure across an application infrastructure is expert opinion at 41%, while off-the-shelf tool sets account for 21% and 15% use home-made tools. Note that the percentage for "expert opinion" goes up 20% to 61% if relying on "previous or similar" incidents is included.

This is not to say that in-band enterprise management solutions are not evolving towards more and more advanced designs. New trends in analytics, federated data stores, portal-based visualization, renewed attention to multi-brand integration, application flow capabilities and more adaptive heuristics are just a few examples of new and promising trends. Enterprises and mid-tier businesses should continue to shop for the right mix of in-band solutions. However, enterprises should plan for strategies that can effectively complement in-band with out-of-band (OOB) tool sets. And mid-tier businesses should look well-integrated options that can unite in-band and out-of-band solutions into a cohesive portfolio.

Remote Management: Simplifying and Enhancing Uptime Control

Historically, the remote management tools market has been self-contained and somewhat isolated, as many IT management workers have focused on the monitoring and diagnosis of IT infrastructure issues – rather than on efficiencies in actually taking corrective action. And while this focus on monitoring has been a constraint for remote management market development, in fact the market for remote management solutions has grown at a double-digit pace over the past several years in large part because of its compelling ROI advantages – with up to 92% savings in labor costs for remote repair. Remote management solutions can also minimize MTTR for critical services, often by as much as 66% or more, so that service quality improves substantially.

Remote Management solutions have classically leveraged "Out-of-Band" (OOB) capabilities, separate networks such as those supporting KVM (keyboard, video, mouse) switches, that provide an alternate, integrated infrastructure for performing remote diagnostics and management. This infrastructure offers a unified approach to managing a wide range of devices, without hampering the production network with added traffic, and without disrupting access when the production network should suffer availability or performance issues.
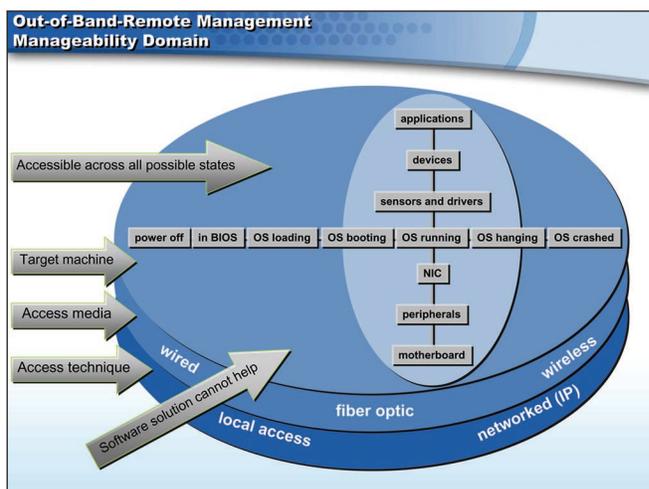

Figure 3: Remote Management – Manageability Domain

Operational advantages in control and efficiencies are becoming increasingly evident for the remote management market through a number of factors. One of those most salient is the proliferation of multi-blade

server deployments that are extending the number of distributed network segments within a single chassis. In other words, server-side systems are becoming virtual networks in themselves, with all the complexity and density created by a federation of networked elements working in tandem. This increase in density makes the remote management of such devices only more compelling; especially, as is often the case, when they are supporting critical business application requirements.

Remote management solutions also bring native advantages in meeting compliance and security requirements. This is because remote management solutions can limit and specify access based on role and security level appropriateness. They can also provide improved security with sophisticated encryption, authentification and authorization by device, location and business process. These capabilities have clear value, given the rise of federal regulations, such as Sarbanes-Oxley and Health Insurance Portability and Accountability Act of 1996, that require IT professionals to track and control material changes within an IT infrastructure more effectively than in the past.

However, not all remote management solutions offer all the same advantages. Here are some of the differentiators to look for in selecting a product:

- *User management advantages.* IT managers should look for solutions that offer single sign-on and centralized, role-based security that can be easily administered centrally according to corporate business and operational policies. These capabilities should include multi-user access, so that multiple professionals can work on a problem together. With that in mind, some remote management solutions offer collaborative tools such as PC Share and SecureChat.

- *Physical and logical views.* Some remote management solutions offer IT professionals both physical and user-defined logical views of devices as they interrelate to a service, organization and customer set. This combination of views can help reduce downtime and operational costs by providing any easy sort – for instance by device type and physical location – when problems occur and technicians need to isolate the problem. This versatility can be enormously valuable in clarifying and prioritizing remote fix activities as they map to business

services and business requirements. They can also help to provide a more consistent context for technical professionals, and technical and customer-facing help-desk professionals to work together more efficiently.

- *Aggregation and consolidation of technologies.* Most remote management solutions offer support for a variety of diagnostic, repair and validation technologies. IT should look for solutions that include both a broad range of technology options, as well as those that integrate these options in a manner that allows IT professionals easy navigation among them. Some of the options to look for include:

  ○ KVM (keyboard, video, mouse) console support – is a mainstay of virtually all remote systems management solutions. It enables access to devices when no in-band connection is available, and/or when the OS is not functioning. KVM has four basic functions. It enables administrators to work with the processor or the system as though they were virtually inside the machine. KVM enables IT to control multi-processor machines or machines with multiple blades. It allows designated IT professionals to stop and start processes, or restart processes that may have failed. KVM also enables administrators to reboot systems and network devices.

  ○ Serial console access – is core to accessing internetworking devices, such as switches, firewalls, load balancers and routers. Virtually every network device has a (RS232 serial) port for management purposes that largely complements any existing in-band management instrumentation/access.

  ○ Support for network and systems devices – should include a wide range of systems devices and system OS support, as well as support for network switches, routers, firewall devices, and even sniffers and other monitoring devices.

  ○ In-band access to complement out-of-band access – is particularly useful for collecting SNMP data from network and systems devices, and log files from systems devices.

  ○ Remote power control is critical for power cycling, when it's necessary to fix device

problems by turning the power on and off. An example might be a system crash where the system is frozen and the keyboard doesn't respond. This is an area where in-band solutions may not work. Control-Alt-Delete isn't useful when the system does not respond.

- *Cost effective packaging and pricing to support small and mid-tier as well as larger enterprises.* Remote management solutions can provide critical value in a wide range of IT environments – even for smaller businesses where there are mission-critical devices that are geographically dispersed. However, not all solutions are priced and packaged to support this range of market requirements.

Perspectives on ROI

The ROI advantages of OOB remote management solutions, in terms of operational efficiencies and minimal MTTR, are substantial and have been mentioned in part throughout this report. Some of the parameters surrounding ROI for remote management are themselves telling. These include:

- Dispatches (dispatching a technician) eliminated per year (which can be in the multiple thousands)

- Hours required per dispatch (which can range from one or two to multiple days)

- Operational advantages through improved collaboration (these are difficult to quantify but real and validated advantages)

- Operational savings gained through headcount consolidation, with the technical skill base more concentrated, while managing remotely

- And, of course, the costs of downtime to business effectiveness – including revenue generation and productivity, morale, and customer/partner loyalty

A brief summary of some critical ROI data points is as follows:

- With the cost of an average trip to fix a failed device in a remote facility currently estimated at $350 an hour, remote management solutions have demonstrated better than a 90% decrease in labor costs.

- Remote management solutions have shown a 66% decrease in MTTR by eliminating travel delays and optimizing in-depth device diagnostics.

- While MTTR costs vary dramatically: For example, a utility estimates downtime costs at $10 to $12 million per day, while for a financial institution the costs are $14 million a minute.

- As IT organizations expand to support business needs, remote management solutions can enable more seamless and cost effective growth. In one environment where remote management solutions were deployed, IT assets increased 33% per year at more than 100 sites, with no increase in IT personnel.

Summary and Conclusion

Remote Management is not new to IT, but its importance is growing as IT transactions and the infrastructure supporting them become increasingly mission-critical to business competitiveness. As business services and IT services continue to blend, this trend will only accelerate.

Remote management provides an effective answer for saving dramatically in operational expense in fixing remote systems and network devices. This capability can save administrators hours and even days of inconvenient and expensive travel time. If a trusted administrator can correct an outage from his or her home, rather than spend a two-hour commute at 4 a.m., both the administrator and the supported business stand to gain. At the same time, remote management helps to ensure the availability of business services and helps to provide business as well as IT infrastructure continuity.

Finally, the designated control that remote management provides is often highly valued where access control to critical infrastructure devices needs to be defined, minimized and governed. In one instance, remote management tools were in place in a location (in the finance industry) where actual physical access to key data centers was all but prohibited.

At the same time, the functional opportunities for remote management are also expanding. EMA has seen the increasing use of remote management for provisioning systems remotely, remote system backup, and remote monitoring for critical devices, among other areas. These are natural extensions to the remote management arsenal, which can best be understood in break-fix operational and uptime-driven cost savings today, but which in the future may become a far more pervasive functional resource for management control of the IT infrastructure.

About Enterprise Management Associates, Inc.

Enterprise Management Associates, Inc. is the fastest-growing analyst firm focused on the management software and services market. EMA brings strategic insights to both vendors and IT professionals seeking to leverage areas of growth across e-business, network, systems, and application management. Enterprise Management Associates' vision and insights draw from its ongoing research and the perspectives of an experienced team with diverse, real-world backgrounds in the IT, service provider, ISV, and publishing communities, and is frequently requested to share their observations at management forums worldwide.

Corporate Headquarters:
Enterprise Management Associates
2585 Central Avenue, Suite 100
Boulder, CO 80301, U.S.A

ENTERPRISE MANAGEMENT
ASSOCIATES

Phone: 303.543.9500
Fax: 303.543.7687
info@enterprisemanagement.com
http://www.emausa.com

946.081505