Consolidating IT Infrastructure Management: Unifying Data Center Hardware and Software Administration

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Emerson Network Power

October 2014

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Consolidating IT Infrastructure Management: Unifying Data Center Hardware and Software Administration

Table of Contents

Consolidating IT Infrastructure Management: Unifying Data Center Hardware and Software Administration

Executive Summary

The effective management of an enterprise IT infrastructure requires an integrated approach for monitoring and administration of hardware, software, and environmental platform elements. Organizations are often challenged to achieve these requirements due to infrastructure complexity, administrative resource constraints, and a lack of visibility into their support stacks. The adoption of service processor technologies provide the system access and detailed information necessary for proactive IT management, but the distributed connections to the platforms in conjunction with a lack of standardization amongst hardware manufacturers greatly reduce the advantages that can be achieved with their use and fail to simplify support processes. The key to truly consolidated IT infrastructure management is the introduction of a centralized interface for access, administration, and data collection of all supported service processor data.

IT Infrastructure Management Challenges

Information Technology (IT) is the lifeblood of any modern day enterprise, and the performance of an enterprise IT infrastructure – including servers, storage, networking and other essential data center components – directly correlates with the success of the business. When key IT systems fail, employee productivity is diminished, quality of service is reduced, reputations are damaged, and profitability is sacrificed. Effective IT management, therefore, is critical to meeting business goals, and IT support organizations are pressured to achieve a high degree of performance assurance. In addition to ensuring high availability of critical systems, IT managers must optimize the efficiency of managed systems while maintaining cost-effectiveness in operational expenses. They are also expected to minimize risk to the business by meeting security and regulatory compliance goals. Although these processes for maintaining the environment are certainly challenging in their own right, to effectively establish control over managed IT infrastructures, organizations must also continually introduce proactive process improvements and strategically plan to meet changing capacity requirements.

Meeting the broad enterprise requirements for IT infrastructure management is often far more demanding than initially conceived. The core of the difficulty is the invariable increase in infrastructure complexity that is introduced over time. Even the most carefully architected environments will eventually drift from an optimal state as updates are introduced and business requirements are expanded. The more complex the system being managed, the more challenging it is to establish control over the environment. Complex infrastructure technologies, such as virtualization and cloud implementations, further increase management difficulties by adding new layers of management requirements.

Complex infrastructure technologies, such as virtualization and cloud implementations, further increase management difficulties by adding new layers of management requirements.

Faced with complex IT requirements, it certainly does not help that most organizations have limited resources for addressing them. Budget constraints reduce the ability to purchase hardware upgrades and expansions, increasing the need to maximize value in existing IT asset investments. Similarly, environmental costs (such as for energy consumption) must be minimized without endangering server or network performance. Limited budgets also have an effect on the availability of IT administrators. This is ironic because it means organizations that are most in need of knowledgeable IT professionals are less likely to be able to afford qualified staff. There is also a direct correlation between the complexity of an IT infrastructure and the support effort and experience required from Full-Time Employees (FTEs) for performing regular

administration and emergency response. Further, support staffs that spend the bulk of their time on mundane tasks and "firefighting" have little opportunity to perform proactive problem prevention and to introduce business-focused improvements.

The first casualty of uncontrolled complexity in data centers is security. According to primary ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) research, risk management is far and away the most significant factor in ensuring data center success. While there are many facets to risk, "security and compliance" was most commonly identified by enterprise IT managers as the primary reason for diminished return on investment in data center management.[1] This is not surprising given the level of compromising legal exposure organizations with unsecured environments must endure as well as how challenging it is for them to achieve compliance objectives. Put simply, the more IT elements there are in a data center to manage (software, hardware, and environmental) the greater the opportunities for security breaches. Complex infrastructures mask vulnerabilities by making it impossible for support staff to monitor risk points through purely manual process. Even after security breaches are identified, infrastructure complexity makes it very difficult for IT professionals to perform detailed forensics to accurately determine who was responsible, what was actually done, and even when it occurred. To successfully mitigate security risks, organizations must fully restrict both physical and remote access to data center resources, allowing access to only authorized personnel that absolutely must perform IT provisioning and maintenance tasks.

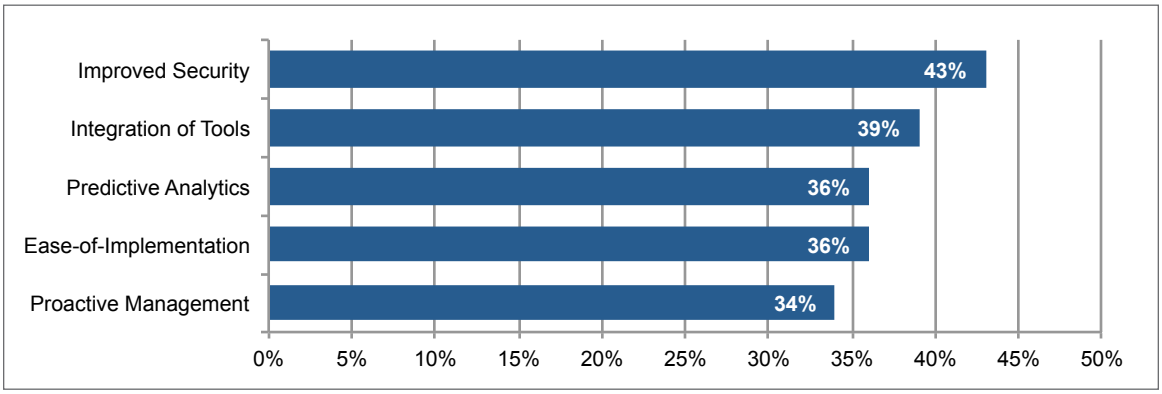

Figure 1: Top 5 data center automation needs as identified by surveyed enterprises

Where IT organizations often fail most tragically in both security and IT management is in enabling full visibility into their support stacks. Again, infrastructure complexity plays a big role in inhibiting success, but it is compounded when organizations rely on separate interfaces, data collection resources, and access points for each managed device. This "swivel chair management" makes it extremely difficult for administrators to correlate events and perform detailed root cause analysis on failure events, trapping organizations into a cycle of continuous reactive "firefighting." Lacking a holistic view of the support stack, organizations are unable to accurately identify the health states of managed devices, proactively identify symptoms of potential failures, and promptly issue escalation processes. Inadequate infrastructure visibility also breaks down communications between multiple IT support and facility management teams as each is focusing on a different set of requirements and conditions rather than attaining an understanding of how performance impacts in one area can directly affect another.

[1] Reference: "Data Center Automation in the Age of Cloud"

Enhancing IT Infrastructure Management with the Use of Service Processors

Unified monitoring, management, and security of hardware across an IT infrastructure require holistic visibility and administrative capabilities that extend beyond the capabilities of traditional server-centric systems management platforms. By leveraging embedded technologies, such as service processors, organizations are able to continuously collect and analyze data across a much broader range of hardware, software, and environmental components than by recording system level data alone. Service processors are physical processors that operate completely independent of the main processor and operating system in order to provide detailed information on the status of the system regardless of its power state. Although service processors can be employed for a variety of purposes, a specific type, Baseboard Management Controllers (BMCs), are used for monitoring the physical state of servers, such as for energy consumption, temperature, and other internal sensor readings.

By leveraging service processor technology, organizations can greatly simplify the monitoring of their infrastructure. Indeed, the very fact that the processors are embedded on the IT platforms themselves negates the need to purchase, deploy, and integrate with third-party sensors and metering devices, reducing the number of components in the management chain. Similarly, service processors are able to monitor conditions directly on the device itself, establishing a single source of truth about the health of the managed system. Since data is collected in real-time, problems are immediately detected and can be promptly remediated before they become business impacting.

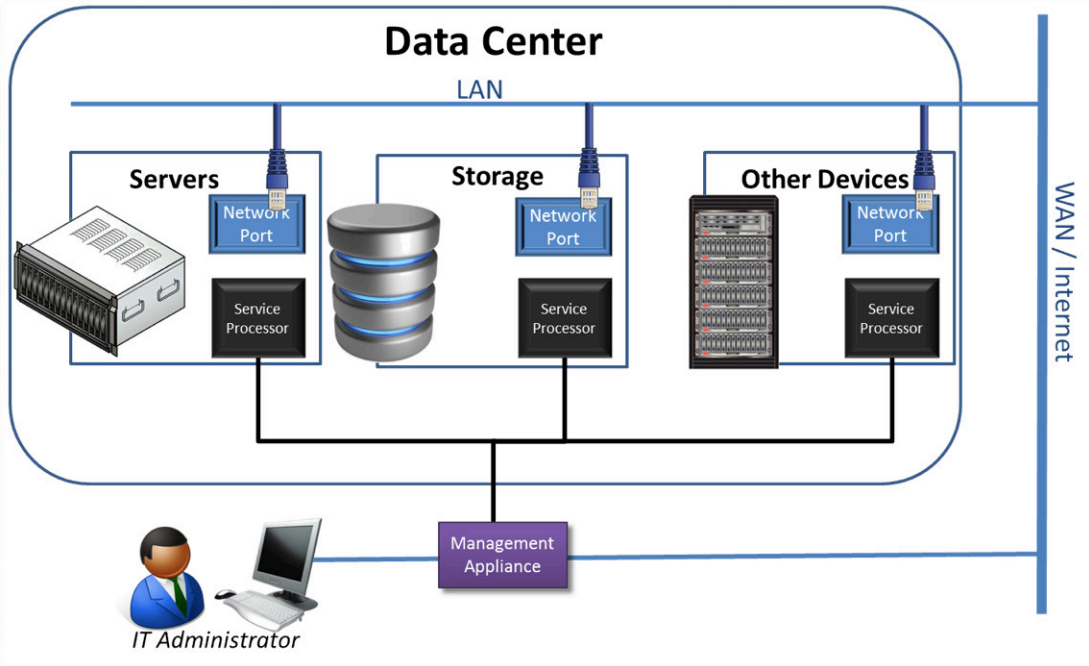

Figure 2: Leveraging service processors for secure and effective IT infrastructure management

The provisioning of new servers, for instance, is also greatly simplified with the assistance of service processors. Because this approach operates independent of a server's operating system, the installation of a new OS, drivers, or other software components can be automated, managed, and continuously tracked even if the deployment requires multiple system restarts. Similarly, major system reconfigurations –

such as kernel rebuilds, disk repartitioning or introducing virtualization – can all be managed remotely through the service processor even when the system needs to be taken off-line.

Perhaps the greatest value service processors offer is in providing critical data to support informed decision making on environment improvements. For instance, knowledge of existing system utilization can assist with capacity planning – ensuring build-outs are right-sized to meet business requirements without wasteful overprovisioning. System usage and performance information can also identify servers that are most appropriate for upgrade, replacement, or out-right retirement, and the data is invaluable in planning for consolidation initiatives and performing impact assessments. Visibility into server conditions additionally provides intelligence for the optimization of system configuration for performance improvements. Comprehensive data collection in conjunction with strategic planning can result in significant cost reductions by facilitating server consolidation and reducing both energy consumption and cooling requirements. The simplified management that is enabled by service processors also reduces required FTE and training costs.

The use of service processors allows all these activities to be performed remotely, minimizing risks due to security breaches and unintentional errors. Since administrators no longer need to be physically present in the data center to perform installations, configurations, repairs and monitoring of infrastructure devices, access to the these can be limited to just personnel that need to install, move, and repair hardware components. Further, since the service processors are remotely accessed, opportunities are created to fully track administrator access and activities, ensuring accountability in any of the tasks performed and allowing any security breaches or configuration error to be immediately logged and reported.

Service processors empower IT management by identifying both immediate impacts and potential problems, and they also provide the detailed information necessary to perform the root cause analysis necessary to prevent systemic failures. These capabilities help transform organizations from reactive to proactive management and lay the groundwork for the implementation of dynamic automation that accelerate process improvements across the infrastructure for even greater performance effectiveness and cost-efficiencies.

Service processors empower IT management by identifying both immediate impacts and potential problems, and they also provide the detailed information necessary to perform the root cause analysis necessary to prevent systemic failures.

Barriers to Success with Service Processors

Despite the clear advantages inherent in the use of service processors, many organizations have been slow in adopting the technology or, at least, using it to its full potential. This is understandable, as a lack of standardization undermines the simplification of the management processes and can actually add a new layer of complexity. Different service processor architectures operate with different command sets and can perform different management activities. Unless an environment is completely homogenous (i.e. managing only identical server or network types) administrators will need to learn and adjust support practices for each unique platform.

The more heterogeneous a server environment, the more complex are the required administrative processes. When administrators must perform different tasks on each managed device, they are unable to standardize processes and configurations, reducing their ability to establish control over the environment. For instance, security enforcement becomes more difficult as no processes are established for authenticating user access, permissions are not easily coordinated to restrict authorization for

performing privileged activities, and no centralized auditing and tracking is enabled to ensure accountability of user activities. In fact, administrators often never even change the default credentials in their service processors or update the service processor firmware to address critical security vulnerabilities just because these activities would be too time consuming to implement on multiple platforms. By extension, this leads to an inability to achieve regulatory compliance objectives, and the process for collecting health and status data becomes convoluted. Not only is the data more difficult to collect, it is invariably in too much of an inconsistent and unstructured format to perform any productive analysis on.

Since each managed device's service processor data is collected and stored locally, there can also be significant challenges with access to the data. In order to access the information, administrators must maintain persistent connectivity with the server. If they are unable to connect to the server for any reason (network failure, power outage, hardware failure, etc.) valuable data necessary for diagnosing the problem may be inaccessible or even lost. Additionally, when data is distributed throughout the support stack, auditing processes become a nightmare as data collection becomes a difficult, time-consuming manual exercise and there is an increased risk of introducing human error into the reporting process. This is further exacerbated when the management of the server, storage or network devices is centralized and the sites are geographically distributed.

The reality of needing to support heterogeneous service processor platforms with distributed administration activities often increases management complexity, eliminating much of the value that is achieved from service processor use. Even if the data is being collected in real-time, it is unlikely administrators will be able to acknowledge and respond to the information in a timely manner. More likely, administers will just ignore information reported by service processors under the pretense that they simply do not have the time to perform the complex processes necessary to collect and correlate the data.

The reality of needing to support heterogeneous service processor platforms with distributed administration activities often increases management complexity, eliminating much of the value that is achieved from service processor use.

Achieving IT Infrastructure Management Success

The "best of both worlds" approach to unifying hardware and software server management is to take advantage of service processor capabilities without increasing support complexity. One way to accomplish this is by consolidating monitoring and management capabilities. Service processors alone only provide the beginning of the management equation – efficiently collecting granular system status data in real time – but a complete solution requires the implementation of a centralized platform for data collecting and the automation of administrative actions. In this way, administrators need only access a single interface to perform management activities on all disparate managed devices. Also, when all health, status, asset and configuration data are stored in a centralized repository, it is more easily and quickly accessible and event correlation is greatly simplified.

A consolidated management approach enables a holistic view of the support stack, facilitating informed decision making for problem identification and environment improvements. This ends the break/fix cycle of reactive "firefighting" by closing the loop on failure events with root cause analysis and enables a proactive process for problem prevention and capacity planning. Consolidated management is an essential step towards enabling dynamic Data Center Infrastructure Management (DCIM) where critical problems are promptly identified and resolved with minimal administrator interaction. This in turn greatly mitigates business risks with improved IT performance, including:

- **Improved agility** – enabling rapid provisioning, changes, and repairs while maintaining cost-effectiveness
- **Improved accuracy** – ensuring information on data center inventory, health status, and configuration is accurate, timely, and complete, and that all compliance requirements are continuously met.
- **Improved access protection** – restricting information and system availability to only authorized personnel with essential business needs for access.
- **Improved availability** – keeping business processes operational by ensuring the continuous and optimal operation of systems, applications, and environmental conditions.

Recognizing the importance of enabling this crucial IT infrastructure management capability, Emerson Network Power has introduced an integrated approach that includes consolidated support for service processors on managed devices across the enterprise. By integrating the Avocent® Universal Management Gateway directly with its DSView 4 management software a secure and consolidated platform is enabled for integrated monitoring, access, and control across the entire IT infrastructure. Supported systems and service processor platforms are automatically discovered, and a single centralized web-accessible interface enables remote access to all physical and virtual assets in the data center. The consolidated server management enabled by Emerson's solution helps enterprises establish control over their IT infrastructure. Access to assets and critical data is restricted to only those with proper authorization, and all activities are logged to ensure administrators are held accountable for their actions on critical systems.

Full data center infrastructure management capabilities are further enabled with Emerson's *Trellis*™ Platform – a self-contained, purpose-built suite of data center management and monitoring resources that integrate directly with the Avocent Universal Management Gateway to help both IT operations and facilities management establish control over their IT and facilities infrastructures. All networked data center assets (including server, storage, network, power, cooling, and environmental control devices) are automatically discovered by the Trellis Inventory Manager and recorded in a centralized data repository. The data center components are continuously monitored at the system level, at the hardware level (i.e. via service processor access in the Avocent® Universal Management Gateway), and at the environmental level to enable a truly holistic view of the infrastructure. From the collected data, Trellis Site Manager tracks, reports, and alerts on the performance of data center elements to enable proactive problem identification and remediation. While traditional static log-based reporting may mask the true root cause of a server failure or performance problem, the holistic views offered by the Trellis platform allow administers to rapidly correlate where the problem initiated, even if the breakdown point is external to the affected server.

Together, Avocent® Universal Management Gateway, Avocent® DSView 4 management software, and the Trellis suite of data center management solutions empower organizations to harness the full potential of service processor data. The integrated platform leverages Emerson's in-depth knowledge of service processor technology to extend support to all existing architectures. Emerson's integrated data center solutions unify the monitoring and management of all data center infrastructure through centralized and real-time data collection coupled with consolidated reporting. These capabilities enable informed decision making for improving performance, reliability, and operational cost-effectiveness.

Together, Avocent® Universal Management Gateway, Avocent® DSView 4 management software, and the Trellis suite of data center management solutions empower organizations to harness the full potential of service processor data.

EMA Perspective

As IT operations engage in a never-ending battle to ensure the performance of managed systems can meet Service Level Agreements (SLAs), it is often easy to forget that the very purpose of IT is to serve the business, rather than the other way around. When organizations are investing excessive time, money, and effort in maintaining IT, productivity and profitability are compromised. Consolidated server and IT infrastructure management is the key to enabling business-focused IT management. It provides holistic views that facilitate proactive infrastructure improvements and greatly simplifies management processes, accelerating administrator proficiency. Both infrastructure and process improvements result in lower operational costs and – by increasing business reliability and agility – position the enterprise to compete better in the marketplace.

Service processors provide the foundation for integrating hardware and software server and IT infrastructure management elements, but are challenging to work with independently due to a lack of standardization. Although IPMI offers the closest to an industry standard, it has not been adopted by leading server manufacturers. The simple truth is that hardware platform vendors want to maintain a competitive edge in the marketplace by offering proprietary service processor formats uniquely designed to support their particular architectures – a trend that does not appear to be changing in the foreseeable future, but does result in an actual increase in management complexity and therefore cost, in heterogeneous environments. Operating alone, service processors distribute administrative processes rather than consolidating them.

To successfully leverage the power of service processors, organizations must unify management and monitoring functions on a single, centralized interface. The Avocent Universal Management Gateway and DSView 4 management software integrate directly with the Emerson *Trellis*™ Platform to achieve IT management success and lay the essential groundwork for achieving dynamic data center infrastructure management where IT performance and efficiency are maximized and proactively maintained.

To successfully leverage the power of service processors, organizations must unify management and monitoring functions on a single, centralized interface.

About Emerson Network Power

Emerson Network Power, a business of Emerson (NYSE: EMR), delivers software, hardware, and services that maximize availability, capacity, and efficiency for data centers, healthcare, and industrial facilities. A trusted industry leader in smart infrastructure technologies, Emerson Network Power provides innovative data center infrastructure management solutions that bridge the gap between IT and facility management and deliver efficiency and uncompromised availability regardless of capacity demands. Emerson Network Power solutions are supported globally by local service technicians. Learn more about Emerson Network Power products and services at www.EmersonNetworkPower.com.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

2971.092314