Unleashing the Power of iLO, IPMI and Other Service Processors

A GUIDE TO SECURE, CONSOLIDATED REMOTE SERVER MANAGEMENT

PREFACE

In today's Internet-driven economy, the enduring business imperatives – to cut cost and improve service levels and availability – are as crucial as ever. In this marketplace, the success and competitiveness of many enterprises are increasingly dependent on the performance of their *IT infrastructures.** An organization's IT infrastructure needs to be continually up and running, enabling continual service availability.

To support these high availability needs, many businesses have adopted multiple remote management technologies in data centers and remote/branch office locations. Remote management tools enable remote access to an IT asset's management or console port (typically through a serial or Ethernet console port, a power/reset circuit, or a *keyboard, video, mouse* [KVM] port) through separate connections, independent of the IT asset state or its connection to the production network. Therefore, remote management tools provide remote monitoring and control of IT assets even when the managed devices lose connection to the production network.

In addition to serial or KVM connections, an Ethernet-based *service processor* can also be used for remote server management. Service processors are dedicated processors that run independently from the server's main processor and operating system. Service processors enable remote access to power control, sensor readings and, in some cases, server configuration, monitoring and control – even when a server is down. Enterprises of all sizes have deployed servers with service processor technology as part of their IT infrastructures. However, this technology is frequently underutilized, as many

*Italicized terms are defined in the Glossary beginning on page 23.

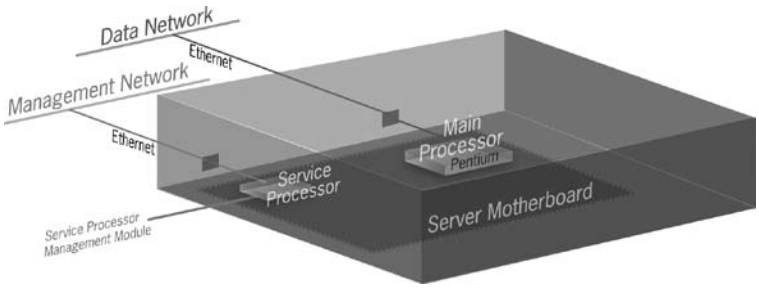
TABLE OF CONTENTS

enterprises are unaware of the potential power of service processors. Some are simply encumbered by compatibility issues caused by numerous proprietary and open source technologies, while others are hampered by enterprise security concerns.

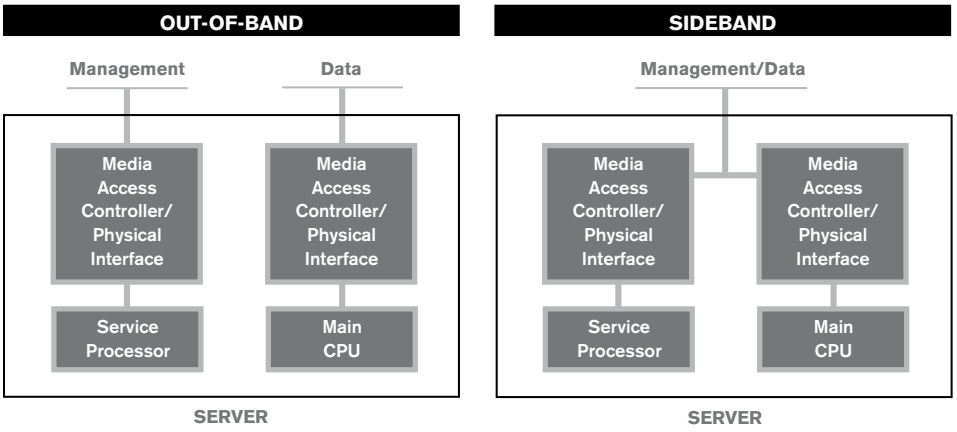
This white paper discusses the leading service processor technologies in use today and introduces the Avocent® MergePoint™ 5200 series of service processor managers, remote management tools that enable secure, consolidated remote management of servers. The white paper further illustrates how these tools provide increased service availability, essential support for multiple vendors and legacy operating systems, greater security and scalability without adding another layer of complexity.

CHAPTER 1: WHAT IS A SERVICE PROCESSOR?

A *service processor* is a separate, dedicated internal processor located on the motherboard of a server, a *PCI* card, or on the chassis of a blade server or telecommunications platform. It operates independently from the server's *CPU* and operating system (OS), even if the CPU or OS is locked up or otherwise inaccessible.



Service processors are accessible through either a dedicated Ethernet interface (out-of-band) or a shared data Ethernet interface (sideband). The figure below illustrates those options. Notice that in the sideband case, although there is only one Ethernet jack in use at the back of the server, there are still two Ethernet hardware sets inside the server, which means those interfaces can have separate *IP* addresses.



Service Processor Features

The feature set of service processors varies depending on the service processor type. This will become clear in the next section, in which each leading service processor technology is discussed in more detail. Nevertheless, there are some features that are common to all service processors.

All service processors provide remote power control (on/off/cycle/status) and enable remote console access via *Serial over LAN* (SoL). Depending on the service processor type, however, they can also provide more advanced functionality, such as server health monitoring (fans speed and status, temperature, voltages), graceful (OS-level) shutdown capabilities, remote KVM and Virtual Media capabilities. The service processor feature set is discussed in more detail in the following pages.

- **Remote power control –** Servers can be remotely powered off, on, or cycled through service processors. This is one of the most useful features of service processors, and it is used to restore servers that are locked up, power down overheated servers, or any other function that requires lower level interaction with the server.

- **Graceful shutdown support –** Certain service processors support a remote power control command that sends a signal to the server OS to shut down gracefully before power cycling or powering off the server. This prevents the possible effects of a "brute force" power cycle or shutdown, such as data corruption in the server hard drives and other undesirable outcomes.

- **Remote SoL console access –** The server console can be accessed through the Ethernet interface of its service processor by using a standard telnet or SSH client, the same way it would be available through a regular serial port. If the server supports *BIOS* redirection to the serial port (which is usually the case with servers equipped with service processors), a user can have full access to the server console, from the time it is booted up and goes through the BIOS, all the way to the OS login prompt. This is very useful for remote troubleshooting.

- **Health monitoring –** Service processors communicate with the appropriate sensor hardware in the server (e.g., fan speed monitors, voltage meters and temperature readers) to access and monitor vital server statistics so that server problems can be detected quickly. The health information can be stored on the server, sent to a remote storage device or communicated directly to the user workstation.

- **Remote ID LED control –** Service processors allow the administrator to turn on or off the server's ID LED, which can be used to identify a specific server in a rack of multiple similar servers. This is especially useful when maintenance is needed on a server and the local technician with physical access to the server does not have access to server information. In that case, the administrator can turn on the ID LED to visually designate for the local technician which server needs maintenance.

- **Local and server-based authentication –** In order to access the service processor features, a user needs to login to it first. That user database is usually stored locally in the service processor. Some service processors can also communicate with central authentication server mechanisms, such as LDAP and Active Directory.

- **Data encryption –** The communication between the service processor and the user may be encrypted should the service processor support communication protocols that allow for encryption, such as Secure Shell (SSH) or Secure Socket Layer (SSL). Most recent service processors support some level of data encryption.

- **System event log (SEL) –** Service processors can store information about events related to the server hardware, such as chassis opening and closing, hard drive functional alarms, RAM test errors, and so on. Those event logs can then be verified by the server administrators directly, or be used as the source for automated alerts.

- **Platform Event Traps (PETs) –** Service processors can be programmed with information about critical thresholds for server environmental variables, such as the maximum operating temperature, minimum CPU fan speed, etc. Based on those thresholds, it can then send out alerts (traps) to a management system, usually in SNMP format, so that the server administrator can take immediate action to remediate the issue at hand.

- **Data logging –** Some service processors provide the ability to log the data flowing through the server's serial console, regardless of whether there is a user directly connected to that session at that time. This enables administrators to review the history of events that happened to the server before a certain issue occurred, which provides a very useful audit trail for change tracking and troubleshooting.

- **Virtual KVM –** This is similar to the SoL feature, but instead of exposing the server's text-based, serial console to the user, Virtual KVM provides access to the server's *graphical user interface* (GUI). This is especially important for operating systems that rely heavily on their GUIs, such as Windows.

- **Virtual Media –** Certain service processors allow the server to access storage media such as CD-ROMs, floppy disks and even DVD-ROMs anywhere on the network – just as if they were directly attached to that server. This allows users to quickly move and copy data between their user workstations to the server (and vice versa), which is useful for emergency OS and application patch installations, as well as diagnostic testing and BIOS upgrades. Virtual Media along with Virtual KVM enables a true lights-out management experience using the interfaces and tools that users are already accustomed to in their daily routine.

Leading Service Processor Technologies

Today's leading service processor technologies include:

- *Intelligent Platform Management Interface* (IPMI)
- HP® *Integrated Lights-Out* (iLO)
- IBM® *Remote Supervisor Adapter* (RSA)
- Dell® *Remote Assistant Card* (DRAC)
- Sun® *Advanced Lights Out Management* (ALOM)
- Sun *Integrated Lights Out Management* (ILOM)

Each is discussed in more detail below. See page 23 for a comparison chart of service processor features.

IPMI

Originally proposed in 1998, IPMI is an *open standard* service processor technology, originally driven by Intel (its main proponent), Dell, HP and NEC. Since then, IPMI has been adopted by more than 150 other companies, including IBM, Sun and every major server platform vendor. The goal of IPMI is to provide a single service processor protocol for servers manufactured by different vendors.

The first version of IPMI supported serial interfaces only and required the use of *console servers*. A subsequent version (1.5) provided IPMI over a *local area network* (LAN) interface. Currently, IPMI version 2.0 provides serial console redirection over LAN, improved *command line interface* (CLI), encryption capabilities and additional support for modular systems like blade servers. These new features enhance management security by supporting well-known and trusted security mechanisms, making IPMI easier to implement within current enterprise security frameworks.

IPMI features include:

- Remote power control, including graceful shutdown support
- SoL console access
- Server health monitoring (fans, temperature, voltages, etc.)
- SEL functionality
- PETs

IPMI's user interface is a text-based CLI, although there are software programs available to present IPMI information through a GUI.

HP iLO

iLO is HP's proprietary service processor technology. iLO is a dedicated *ASIC* on the motherboard of the server that is accessible through a dedicated Ethernet port on the server. Like other service processors, iLO remains active and available, even when the CPU or OS is halted or when the server's power is turned off.

iLO is available in two levels: basic and advanced. Since 2003, almost every HP server – including blade servers – ships with basic iLO included as a standard feature. Basic iLO provides the following features:

- SoL console access (text mode only)
- Remote power control
- Remote ID LED control
- Local user accounts
- Security (SSL, SSH2, user access logging, integrated management log, iLO event log)
- Remote firmware update
- Alert administration (SNMP traps)

Although basic iLO provides a very comprehensive feature set, it can be upgraded to advanced iLO through the purchase and installation of an iLO Advanced Pack, which enables additional functionality in the service processor, such as:

- Virtual KVM
- Virtual Media (floppy, CD)
- *LDAP* and Active Directory integration
- Multifactor (smartcard) authentication
- Terminal Services (RDP) integration

Besides these functionalities, there are other features provided by iLO to make its deployment easier. iLO supports both static IP address configuration and dynamic IP address assignment via *DHCP*. Unlike IPMI, where the only user interface available is text-based, iLO has two user interfaces – a Web-based interface and a CLI available through telnet or SSH sessions. By accessing this Web interface through a standard Web browser, the user is able to perform any service processor function available at that iLO level. Later versions of iLO (v1.60 or greater) in more recent servers (G4 or later, except for blades) also allow for the user to select the Ethernet connection it uses to be either dedicated (default) or shared with the main server Ethernet interface. The

latter allows iLO to be deployed without the need for an additional Ethernet cable and switch port. In those cases, iLO also supports VLANs for logical segregation of the management network traffic.

More recently, HP has released the next generation of iLO, called iLO2, which comes embedded in the most recent models of HP servers. iLO2 also has basic and advanced levels, and the advantages of iLO2 when compared to iLO are as follows:

- Basic iLO2:
  - Virtual KVM text console (allows access to BIOS and POST messages)
  - Power consumption information
  - Embedded system health (fans, temperature, power supply, etc.)

- Advanced iLO2:
  - Java-free virtual KVM
  - Virtual Media (DVD-ROM)

iLO2 is also compatible with IPMI 2.0, for easier integration with existing IPMI-based environments.

IBM RSA

IBM's Remote Supervisor Adapter II or RSA II is a service processor that exists on a PCI card that manages the *Baseboard Management Controller* (BMC) located on the motherboard of a server. A version of the RSA II, called SlimLine, is an internal card that includes the BMC and uses a dedicated Ethernet connector on the server for communication. The IBM BladeCenter's management module uses a modified version of the RSA firmware with an integrated KVM switch to provide access to individual blade servers.

RSA II provides many remote server management options, including:

- Alert and notification management
- Event logging
- Storage of the last screen before a server failure
- Remote power control
- Server health monitoring

All these features are available from the RSA II command line interface. Additionally, RSA II offers a Web-based interface that provides access to all these features plus Virtual Media and Virtual KVM support.

Dell DRAC

DRAC is Dell's proprietary service processor technology. DRAC provides administrators with access to servers and control of the server hardware and OS from client workstations through a Web browser. A telnet connection to DRAC provides access to only a few of the DRAC features when compared to what is available through DRAC's Web user interface. However, it does enable text-based console access. In addition, DRAC logs the probable causes of system crashes and saves current error displays. By communicating with the system's embedded system management hardware, DRAC can report warnings or errors related to voltages, temperatures and fan speeds.

Currently there are five versions of DRAC:

- DRAC II – The initial version of DRAC, provided as a full-length PCI card, required Dell OpenManage IT Assistant software to be installed on the client management workstation. DRAC II can be used with Dell PowerEdge™ EMS2-based systems (i.e., x3xx, x4xx, x5xx servers).
- DRAC III – A half-length PCI card that provides enhancements in Virtual KVM, Virtual Media, and allows access for up to 16 users per card. DRAC III can be used with Dell PowerEdge ESM3-based systems (i.e., 1650, 4600, 6600, and 6650 servers).
- DRAC 4 – Available as either a daughter card (DRAC 4/I) or a half-length PCI card (DRAC 4/P) depending on the system, DRAC 4 can be configured to send e-mail alerts for warnings or errors related to voltages, temperatures and fan speeds. It can also log event data and the most recent crash screen (for systems running the Windows operating system only) to help diagnose the probable cause of a system crash. DRAC 4 can be used with the 8th generation Dell PowerEdge servers (i.e., 800, 1800, 1850, 2800, 2850, 6800 and 6850 servers).
- DRAC 5 – The most recent release of DRAC, it contains major enhancements in the feature set, making DRAC 5 comparable with the most advanced service processors in the market. DRAC 5 can be used with the 9th generation Dell PowerEdge servers (i.e., 1900, 1950, 2900 and 2950 servers).
- DRAC/MC – This version of DRAC, used in Dell's PowerEdge 1855/1955 blade systems, has the regular DRAC functionality along with add-on features specific to the blade environment.

DRAC includes software modules that provide a set of OS-specific services. These services communicate with the DRAC hardware to allow in-band configuration as well as console redirection to the out-of-band connection.

Sun ALOM

Sun was one of the first vendors to have service processors in their servers, which they called System Service Processors (SSPs). SSPs were originally accessible through the server's serial port only, yet provided most of the functionality of modern service processors, such as remote power control, serial console access and low-level system debugging capabilities. ALOM, on the other hand, is accessible through both the server's serial port and through a dedicated Ethernet port on the server, and is the service processor technology of choice for Sun's Volume System Products (VSP) servers and Netra servers, replacing Remote System Control (RSC) and Lights Out Management (LOM and LOMlite).

The servers that currently support ALOM as of its latest version (v1.6) and have it preinstalled as a standard component are as follows:

- Sun Fire V125
- Sun Fire V210
- Sun Fire V215
- Sun Fire V240
- Sun Fire V245
- Sun Fire V250
- Sun Fire V440
- Sun Fire V445
- Sun Netra 210
- Sun Netra 240
- Sun Netra 440

New servers in the VSP and Netra families are also expected to have ALOM installed.

The list of ALOM features include:

- SoL console access
- Data logging for the SoL sessions
- Remote power control
- Remote ID LED control
- Hardware environmental monitoring (disks, fans, power, temperature, FRU info, etc.)
- SELs
- Event management and notification through e-mail and syslog
- OS self watchdog with automatic restart capability
- SSH support for secure access

ALOM's user interface is entirely command line based. It does not provide a built-in GUI or access to the server's GUI.

Sun ILOM

ILOM is Sun's latest addition to its portfolio of service processor technologies. ILOM is available on the Sun Fire X4x00 x64 servers (X4100, X4200, X4500 and X4600).

ILOM combines the functionality of ALOM with the following features:

- Virtual KVM
- Virtual Media (floppy, CD)
- LDAP integration

Besides the text-based CLI, ILOM also has a built-in Web-based interface for the user. Only the Web interface allows access to the Virtual KVM and Virtual Media features of ILOM.

Furthermore, ILOM also supports IPMI 2.0 and SNMP versions 1, 2c and 3. With so many supported interfaces and management protocols, ILOM can be easily integrated into most IT management environments, and it definitely represents the ultimate evolution in service processor functionality delivered by Sun.

Service Processor Benefits

Most of the features provided by service processors are not new, as many of these features are available in some shape or form through other remote management solutions,

such as console servers, KVM switches, *intelligent power distribution units* (IPDUs), etc. The obvious question, therefore, is: what new benefits do service processors provide?

All the benefits provided by remote management tools are available through service processors – lower mean time to repair (MTTR), operating cost savings and improved asset productivity. However, the key difference is that with service processors the complete feature set needed to reap those benefits is already included in the server, and is accessible through one single physical interface. Moreover, this physical interface is Ethernet, the most ubiquitous network interface in the IT marketplace. This greatly simplifies the deployment of a remote server management infrastructure, making it easier for IT managers to take advantage of these technologies. Additionally, the fact that service processors are embedded inside the server provides more detailed and thorough visibility of the server's state, allowing for proactive and preventive management, as well as greater control of the overall server infrastructure. Features such as hardware environmental monitoring and platform event traps are a direct result of the internal presence of service processors in the server.

Chapter 2: Challenges of Service Processor Deployment and Adoption

The demand for remote lights-out management has been increasing significantly due to the general dynamics of the IT industry. Data center consolidation and outsourcing often physically separates data centers from the people who manage them. In addition, the temperature, noise levels and other environmental conditions in data centers are very harsh, which makes them undesirable places for humans to work in.

At the same time, service processors are widely deployed in these environments, since the vast majority of servers purchased in the past three years includes some form of embedded service processor. According to estimates from leading server manufacturers Dell, HP, IBM and Sun, approximately 9 million servers with service processors were shipped in 2005. It has been estimated that this figure will grow to 13 million servers in 2006. It should be the perfect marriage between demand and supply, especially considering that the investment in the service processors needed for remote server management has already been made.

However, service processor adoption has been slow. In spite of all the benefits service processors provide, IT managers are still leaving them unplugged or disabled, not taking advantage of an asset that can provide the exact capabilities they are looking for. The same leading server manufacturers estimate that by the end of 2005, only 1.4 million of the available service processors in the market were being utilized, with an estimated total of 2.2 million used by the end of 2006.

Mainstream adoption of service processors has been hampered by a number of factors. Server vendors are reluctant to adhere to a standard service processor interface such as IPMI because of its perceived limitations. In fact, most server vendors include IPMI in their platforms, but hide it behind proprietary service processor firmware extensions and bundled management solutions. These vendor-specific features only support servers from that specific vendor, and do not support products from other vendors.

To add to that issue, many enterprises are completely unaware of the potential power of service processors, and even when they are aware, specific concerns about how to integrate service processors into their existing management framework prevent their adoption. Some are simply encumbered by compatibility concerns, cost issues and the lack of centralized management, while others are hampered by security and functionality concerns.

Main Service Processor Deployment Challenges

Common reservations about implementing service processors are the following:

- Service processors require an extra Ethernet connection and IP address per server, which translates into extra costs. These costs do not come just from the need to have an additional Ethernet switch port available, but also from maintenance of that connection in accordance to the company's policies. This issue only affects service processors that require a dedicated Ethernet port.
- Lack of proper authentication, authorization and accounting (AAA) security support built in to service processors, which prevents integration and compliance with existing security mechanisms and policies. The exception to this rule is HP iLO.
- Specifically for sideband deployments, IPMI comes disabled in the server, due to security concerns. In order to enable IPMI in that server, the IT manager would need to either access the server BIOS or PXE boot the server with a specific OS image that contains the proper BIOS configuration commands. This is a challenging task, especially in large environments with many servers already deployed.
- Lack of a discovery mechanism for service processor capabilities already deployed, which prevents IT managers from taking immediate advantage of service processors already present and available in their IT environment.
- Consolidation tools for multiple servers are either vendor-specific or do not offer enough features, which causes interoperability and scalability issues in service processor adoption.
- Integration of service processor management into the existing management framework is difficult due to the lack of standardization and the limitations of vendor-specific tools. Also service processors do not integrate with existing remote server management tools such as console servers and KVM switches.

Existing Options to Leverage Service Processor Technology

Enterprises are currently using the following methods to take advantage of service processor functionality in their IT environments. In many deployments, an out-of-band network separate from the production network is desirable.

Routers – Many enterprises use routers with *Network Address Translation* (NAT) to reduce the number of public IP addresses for communication between the users and servers. The NAT function gives the service processor a local IP address that can be changed to a public IP address through the router. Routers also provide some additional security features, and are not limited to any one manufacturer's protocol.

Unfortunately, routers cannot log information, reduce the number of Ethernet switch ports or IP addresses, or interpret any information it has received from the service processor. It can only forward the information. Using routers as a service processor management tool would still require extensive management efforts at the user's workstation.

IPMI gateways – IPMI gateways are located between the IPMI-enabled devices and the user applications. The role of the IPMI gateway is to provide secure access to the IPMI interface of servers for both users and for other applications. The IPMI gateway translates the IPMI protocol into a more usable enterprise protocol to allow user access through the public network and expose the power control, sensors access, system event logs and other IPMI functionality.

Although IPMI gateways provide the security needed for IPMI deployment, they do not allow for scalability, provisioning, configuration control and intelligent monitoring of any IPMI messages from the BMC. In addition, IPMI gateways do not support console management, KVM functions or service processor technologies other than IPMI.

IPMI proxy appliances – IPMI proxy appliances provide security and network integration of IPMI-enabled servers. Unlike gateways, they do not terminate IPMI data but forward the information to a user workstation where the user can control and manage the IPMI server. IPMI proxy appliances provide security with authentication and encryption from the users' workstation to the proxy appliance. IPMI proxy appliances also convert IPMI data from a UDP to a TCP data stream for routing to a user console through a firewall.

Although IPMI proxy appliances do provide the security needed for IPMI deployment, they do not support scalability, provisioning, configuration control or intelligent monitoring of IPMI messages from the BMC. Moreover, they are limited to managing only IPMI-based devices and do not provide management capabilities to other service processors.

Software solutions – Software applications provide IT administrators and managers with the flexibility to control multiple levels of management, which include provisioning, monitoring and management of the entire heterogeneous infrastructure through a single Web-based interface. Operated from a single workstation providing centralized control, service processor software applications allow grouping of devices by custom-

er, location or software deployed, so that tasks can be carried out on groups of devices rather than individual devices. Software applications can increase operational efficiency by automating the tasks required to provision, monitor and manage servers.

Some software programs are specific to a manufacturer's servers such as HP Systems Insight Manager, IBM Director and Dell OpenManage. Other third parties have created software programs for managing multiple service processors from various vendors.

Software applications present a number of challenges in deployment, performance and security. For deployment, the software must first be installed and configured on some servers or workstations, potentially adding complexity and cost. Hardware devices must also support whatever security policy is in place, which may require installing additional software, further adding complexity and leading to compliance issues with security policies. While software programs do simplify the provisioning and configuration of servers, they do not provide consolidation of IP addresses, so management may be costly.

Chapter 3: Avocent Solutions for Service Processor Management

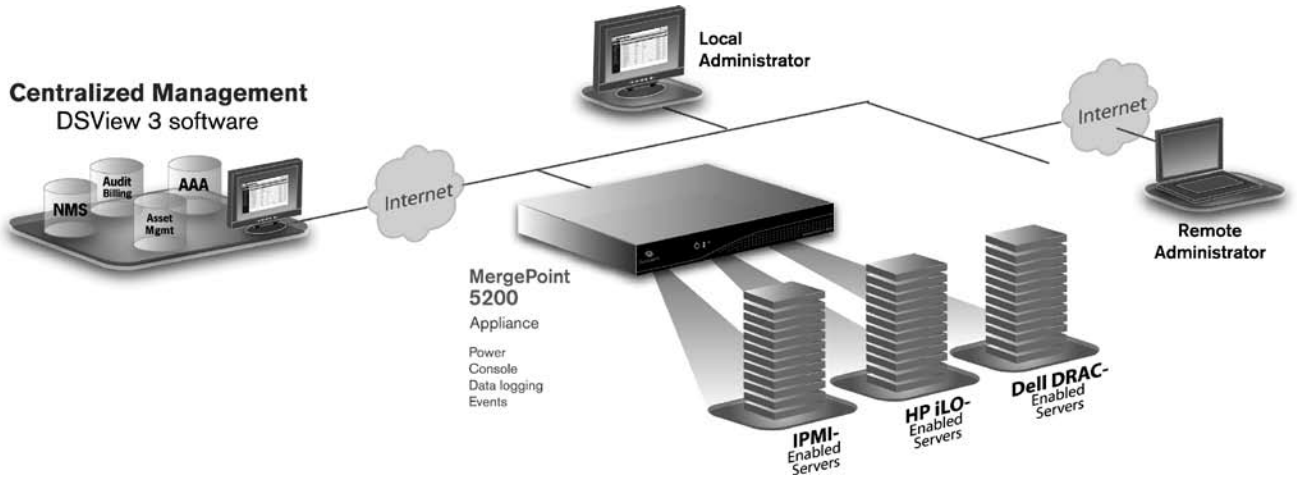
The MergePoint 5200 series of service processor managers is a family of products that enables IT administrators to perform secure, remote management of servers with service processor technologies from anywhere. The different product models are described below.

MergePoint 5200 service processor manager – The MergePoint 5200 appliance streamlines and consolidates management of servers with IPMI (versions 1.5 and 2.0), DRAC and iLO. The MergePoint 5200 appliance provides secure SoL, console access, power control and server hardware monitoring, along with IPMI provisioning and service processor auto discovery. When used in conjunction with DSView® 3 management software, the MergePoint 5200 appliance provides essential server coverage, which complements the overall management infrastructure.

The MergePoint 5200 appliance offers both a feature-rich Web user interface as well as a command line interface that leverages the *Systems Management Architecture for Server Hardware Command Line Protocol* (SMASH CLP), a standards-based user and scripting interface defined by the Distributed Management Task Force (DMTF). This provides a single command line interface to manage servers from multiple manufacturers, simplifying management and streamlining interoperability while providing scripting and automation capabilities.

This appliance not only makes it easier to take advantage of service processor features, but also enhances service processor functionality with add-on features. For example, the SoL feature complements the continuous data logging capabilities, resulting in additional security and auditing. Also, simultaneous power control of multiple servers boosts the already existing power management capabilities of service processors, including graceful shutdown support for IPMI. These features allow the user to completely unleash the power of these embedded server management technologies.

The MergePoint 5200 appliance also eases the deployment and management of these technologies. With easy-to-use IPMI provisioning capabilities and an auto discovery mechanism for server management technologies within the network, the MergePoint 5200 appliance is ideal for enterprise data centers as well as for high performance computing (HPC) and other clustering environments.

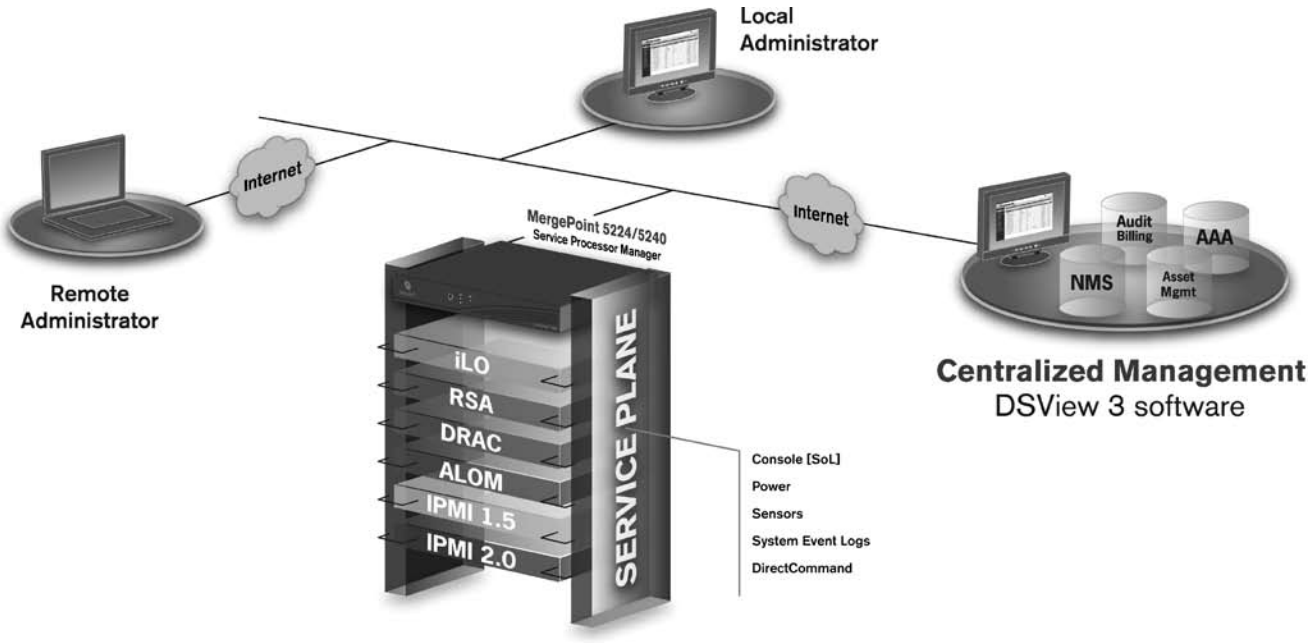


FEATURES	BENEFITS
SERVER MANAGEMENT	
SoL, power control, hardware monitoring and alerts	Complete, full-featured remote server management from a single user interface
SoL with data logging	Better auditing, faster troubleshooting
Group execution of commands	Control the server infrastructure as a whole
Event and alert management	Enables proactive response to server issues
Integrated support for Microsoft® Remote Desktop Protocol (RDP) and Virtual Network Computing (VNC)	Full server management coverage (in-band and out-of-band) from one user interface
SERVICE PROCESSOR MANAGEMENT	
IPMI provisioning	Faster, easier IPMI deployment
Service processor auto discovery	Better use of already deployed server management capabilities
USER INTERFACE	
Single console for multiple service processor types	Consolidated server management regardless of the type of embedded management technologies in use
Embedded Web interface	Intuitive interface provides a shorter learning curve and faster product deployment
Standards-based, consistent, scriptable command line interface (SMASH CLP)	Reduces human error, simplifies training, automation and integration with other management tools
Integration with DSView 3 management software	Provides a single user interface for management of the entire IT infrastructure

MergePoint 5224/5240 service processor managers – The MergePoint 5224/5240 appliances simplify management of servers with service processor technologies by consolidating IP connections, user access and server health information. With multiple Ethernet ports, the MergePoint 5224/5240 appliances connect point-to-point with Ethernet-based iLO, IPMI (versions 1.5 and 2.0), DRAC, RSA and ALOM service processors. By consolidating service processor Ethernet ports, the MergePoint 5224/5240 appliances require only one external IP address for all connected devices, reducing deployment costs associated with service processors. The MergePoint 5224/5240 appliances reduce costs further by consolidating multiple service processor physical interfaces into one Ethernet connection to the production network, significantly reducing the use of production switch ports.

The MergePoint 5224/5240 appliances deliver Secure Rack Management (SRM) by isolating and protecting the connected service processors from the external production network to provide efficient, rack-level management with seamless integration into the management infrastructure. The MergePoint 5224/5240 appliances allow enterprise-class AAA security and encryption, and extend this functionality to all servers. Other standard features include data logging, event detection and notification, SNMP proxy, graphing and alarms for sensors and shared access to management ports.

The MergePoint 5224/5240 service processor managers provide an easy-to-use, consolidated user interface for management of servers from multiple vendors by extracting the native service processor interface for configuration, SoL and power control. Server administrators need only learn one simple interface.



FEATURES	BENEFITS
SERVER MANAGEMENT	
SoL, power control, hardware monitoring and alerts	Complete, full-featured remote server management from a single user interface
SoL with data logging	Better auditing, faster troubleshooting
Physical consolidation of service processors	Ethernet port and IP address savings, superior security
Strong enterprise security features (AAA, granular ACLs, data logging)	Easier compliance with internal security policies, integration with existing security systems
DirectCommand - direct access to SP's native UI	Access to familiar SP UI and all of its features without impact on security
Event and alert management	Enables proactive response to server issues
SERVICE PROCESSOR MANAGEMENT	
Built-in DHCP server for dynamic IP address assignment to service processors	Simpler service processor deployment
USER INTERFACE	
Single console for multiple service processor types	Consolidated server management regardless of the type of embedded management technologies in use
Embedded Web interface	Intuitive interface provides a shorter learning curve and faster product deployment
Consistent, scriptable command line interface	Reduces human error, simplifies training, automation and integration with other management tools
Integration with DSView 3 management software	Provides a single user interface for management of the entire IT infrastructure

Why Choose Service Processor Management Solutions by Avocent?

Avocent is the leading supplier of IPMI embedded firmware solutions for the majority of Tier-1 server vendors in the industry, which attests to Avocent's credibility in the service processor market. Additionally, for years Avocent has been delivering a comprehensive management solution with *KVM over IP*, serial and power management, all consolidated through the DSView 3 management software. The MergePoint 5200 series of service processor managers represents the next generation of management solutions that take advantage of the compelling benefits of service processor technologies.

ABOUT AVOCENT

Avocent (NASDAQ: AVCT) delivers IT operations and infrastructure management solutions for enterprises worldwide, helping customers to reduce costs and simplify complex IT environments via integrated, centralized in-band and out-of-band hardware and software. Through LANDesk, Avocent also is a leading provider of systems, security, and process management solutions. Additional information is available at www.avocent.com.

SUMMARY OF SERVICE PROCESSOR FEATURES

	IPMI	HP iLO	IBM RSA	Dell DRAC	Sun ALOM	Sun ILOM
User Interface	CLI 9 (IPMI specific)	CLI, Web	CLI, Web	CLI, Web	CLI	CLI, Web
Security	Local password	Local, LDAP, Active DIrectory	Local, LDAP	Local, LDAP, Active DIrectory	Local	Local, LDAP
Hardware	Embedded in motherboard	Embedded in motherboard	PCI card	PCI card (II/III), daughter card (4/5)	Embedded in motherboard	Embedded in motherboard
Management Software	Multiple vendors, Open Source tools	HP SIM	IBM Director	Dell OpenManage	None	Sun NI System Manager
Networking	UDP	TCP	TCP	TCP	TCP	TCP/UDP
Logging	Local	Local and Remote	Local	Local	Local and Remote	Local and Remote
Sensors	Yes	iLO only	Yes	Yes	Yes	Yes
Server Console	v2.0	Yes	Yes	Yes	Yes	Yes
Last Screen Saved	No	No	Yes	Yes	No	No
Power	Server line power	Server line power	External supply	External supply	Server line power	Server line power
Virtual KVM	No	Yes (advance pack required)	Yes	Yes	No	Yes
Virtual Media	No	Yes (advance pack required)	Yes	Yes	No	Yes

GLOSSARY

Advanced Lights Out Management - Advanced Lights Out Management (ALOM) is a proprietary service processor technology and protocol developed by Sun Microsystems.

ASIC - Application-specific integrated circuit (ASIC) is a chip custom-designed to perform a specific task.

Baseboard Management Controller - Baseboard Management Controller (BMC), in IPMI terminology, is the separate service processor that sits on the motherboard of a server or the chassis of a blade server or telecommunications platform. The BMC monitors on-board instrumentation (temperature sensors, CPU status, fan speed, voltages), provides remote reset or power-cycle capabilities, and enables remote access to BIOS configuration or operating system console information. The BMC extends the systems' management capabilities and operates independently of the main processor

BIOS - The basic input/output system (BIOS) is the built-in software that determines what a computer can do without accessing programs from a disk. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions.

CPU - The central processing unit (CPU) is the brains of the computer. Sometimes referred to simply as the processor or central processor, the CPU is where most calculations take place. In terms of computing power, the CPU is the most important element of a computer system. On large machines, CPUs require one or more printed circuit boards. On personal computers and small workstations, the CPU is housed in a single chip called a microprocessor.

Command line interface - Command line interface (CLI) is a user interface common to MS-DOS computers. The user sees the command line on the monitor and a prompt that is waiting to accept instructions from the user. The user types in the command, the computer acts on that command and then issues a new prompt for the next instruction from the user. CLI operating systems are becoming less used as GUI operating systems gain in popularity. In a GUI operating system, such as Windows, the user responds to graphic images on the screen instead of typing in commands in response to a prompt.

Console server - A console server provides remote access to the serial management ports included on most servers and other network IT assets (routers, switches, firewalls, etc.).

Dell Remote Assistant Card - Dell Remote Assistant Card (DRAC) is a proprietary service processor technology and protocol from Dell.

DHCP - Dynamic Host Configuration Protocol (DHCP) is a protocol for automatic Transmission Control Protocol/Internet Protocol (TCP/IP) configuration that provides static and dynamic address allocation and management. DHCP enables individual computers on an IP network to extract their configurations from a server (the DHCP server) or servers, in particular, servers that have no exact information about the individual computers until they request the information. The overall purpose of this is to provision a large number of devices in an IP network. The most significant piece of information distributed in this manner is the IP address.

Graphical user interface - Graphical user interface (GUI) is a computer interface that uses graphics to make a program easier to use. Well-designed GUIs can free the user from learning complex command languages.

IT infrastructure - A company's information technology (IT) infrastructure is defined as all the parts found in a data center and its network architecture (hardware – the physical components such as keyboards, monitors, disks, disk drives, printers, boards, chips, etc. and software – the nonphysical components such as computer instructions or data, anything that can be stored electronically). The function of an IT infrastructure is to bring all these networked components together to work effectively.

Integrated Lights-Out - Integrated Lights-Out (iLO) is a proprietary service processor technology and protocol developed by Hewlett-Packard (HP)/Compaq. HP servers that include iLO:

- All blade servers
- Most DL and ML series

HP also offers iLO embedded on the system board to meet the needs of platforms that have a smaller form factor such as the ProLiant DL360 G2.

Intelligent Platform Management Interface - Intelligent Platform Management Interface (IPMI) is a service processor technology and protocol developed by Intel, HP, Dell and other hardware vendors in 1998 and included in many rack-mounted and

blade servers built on Intel's X86 architecture. A technology that uses a separate processor (Baseboard Management Controller or BMC) embedded in the server to enable IT managers to access, monitor and reboot servers.

Intelligent power distribution unit - Intelligent power distribution units (IPDUs) provide the ability to power remote equipment on and off for operational control or recovery from software/hardware failures.

IP - Internet Protocol (IP) is a standard that specifies the format of packets, also called datagrams and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source. IP by itself is something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

Keyboard, video, mouse - Keyboard, video, mouse (KVM) switches that allow users to use the keyboard, monitor and mouse interface at their workstation to access and control multiple servers as if physically present at the asset.

KVM over IP - Keyboard, video, mouse over Internet Protocol (IP) switches enable users to remotely access and use KVM switches in remote locations through the Web. The challenge with KVM technology is that the interface is graphical, and requires a user to be physically present to see and interpret what is transpiring on the server.

LDAP - Lightweight Directory Access Protocol (LDAP) is used as a means to authenticate users. It enables anyone to locate organizations, individuals and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network.

Local area network - Local area network (LAN) is a communications network that connects personal computers, workstations, printers, file servers and other IT devices in a relatively small area, for example, inside a building or within a number of buildings like a college campus.

Network Address Translation - Network Address Translation (NAT) is an Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

Open standard - Technical specifications that are available to the public as opposed to proprietary standards that may be available only through restrictive terms from the organization that owns the specification.

Out-of-band - Any connection that does not depend on the normal production network. Out-of-band connections include a dial-up modem, serial console port over RS-232, or a second IP link.

PCI - Peripheral component interconnect (PCI) is a local bus standard developed by Intel Corporation. Most modern PCs include a PCI bus as do newer versions of MAC computers.

POST - Power-on self test (POST) is a diagnostic test run by a computer's basic input/output system (BIOS) when a computer is initially turned on. The POST determines if the computer's RAM, disk drives, peripheral devices and other hardware components are working properly. If the POST determines the above-mentioned components are working properly, the computer continues to boot.

Remote Supervisor Adapter - Remote Supervisor Adapter (RSA), a proprietary service processor technology and protocol developed by IBM. IBM servers that include RSA II are IBM xSeries e325 and e326 servers, which can use IPMI to manage the BMCs. However, for top-of-the-line xSeries servers, the service processor of choice is RSA II. Most IBM servers can be upgraded to RSA II.

Serial over LAN - Serial over LAN (SoL) is the ability to access the data from a server's serial port console through its service processor Ethernet interface. The service processor allows that by converting the serial data stream from the serial console to network packets, which are then accessible to the user through the user interface of the service processor.

Servers - Computers and devices that allocate resources (memory and/or devices such as printers or disk drives) for a network.

Service processor - A separate internal processor and its communications protocol included on the motherboard of a server, a PCI card, or on the chassis of a blade server or telecommunications platform. It enables administrators to access, monitor and reboot servers whether or not the main processor is operational. Service processors are often referred to as management processors, Baseboard Management Controllers or lights-out managers.

Systems Management Architecture for Server Hardware Command Line Protocol - Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) is a standards-based, command line protocol used to manage servers. SMASH, created by the Distributed Management Task Force (DMTF), provides both user-friendly CLI and a programmatic interface (WS-MAN) for scripting and automation.

REFERENCES

Intelligent Platform Management Interface

http://www.intel.com/design/servers/ipmi/index.htm

HP Integrated Lights-Out (iLO)

http://h18013.www1.hp.com/products/servers/management/ilo/index.html

HP Integrated Lights-Out 2 (iLO2)

http://h18013.www1.hp.com/products/servers/management/ilo2/index.html

Dell Remote Access Controller (DRAC)

http://support.dell.com/support/edocs/software/smdrac3/

Sun Advanced Lights Out Management (ALOM)

http://www.sun.com/servers/alom.html

http://www.sun.com/products-n-solutions/hardware/docs/html/819-2445-11/

Sun Integrated Lights Out Management (ILOM)

https://www.sun.com/products-n-solutions/hardware/docs/html/819-1160-12/

Avocent®
The Power of Being There®

Corporate Headquarters
4991 Corporate Drive, Huntsville, AL 35805
TEL 866.277.1924 FAX 256.430.4030
www.avocent.com

0207-PROCESSOR-WP