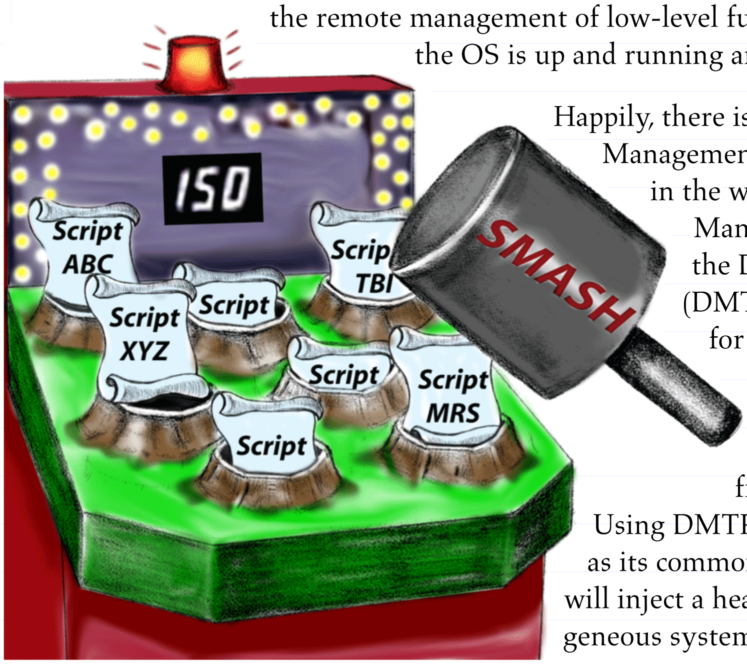
SMASH Those Non-Standard Scripts

an Analyst Notebook by Thomas Deane, 21 September 2005

Diversity is a good thing when it means more choices and more legitimately differentiated options. But when it comes to managing systems from different vendors, diversity is not only bad, it's downright ugly. Diversity here means performing management functions with a bevy of customized scripts that are specific (often in gratuitous ways) to each individual flavor of hardware. The low-level functions that remotely twiddle system hardware, such as to power it on or to set it up, are among the worst offenders. In these heterogeneous system environments, low-level remote management becomes a real pain in the—well, you know….

It should be no surprise, therefore, that IT shops are screaming for computer makers to standardize the remote management of low-level functions, both for environments where the OS is up and running and for those where it is not.



Happily, there is good news to report—SMASH (System Management Architecture for Server Hardware) is in the works. Created by the Systems Management Working Group (SMWG) of the Distributed Management Task Force (DMTF)[1], SMASH is a new set of standards for remote low-level system hardware management that will allow SMASH-enabled systems from any vendor to be controlled, monitored and configured from any SMASH-enabled system tool. Using DMTF's Common Information Model (CIM)[2] as its common repository of information, SMASH will inject a healthy dose of standardization into heterogeneous systems management.

Recently, the specifications for two SMASH components—the Command Line Protocol (CLP) and Server Management Managed Element Addressing—were published. The SMASH CLP describes a way to manage heterogeneous systems via a common command line language. SM Managed Element Addressing provides end users with friendlier, shorthand methods for naming and addressing CIM database object names.

Specifications for other SMASH components—CLP-to-CIM Mapping, CLP Discovery, and Profiles —have yet to be released. CLP-to-CIM Mapping describes the mapping of CLP commands to CIM elements. CLP Discovery describes the process whereby the managing system becomes aware of what servers and other datacenter components are available to be managed. Profiles provide a way of mapping similar components in various systems to a defined set of SMASH objects,thereby providing consistency between different implementations.

[1] Founded in 1992, the Distributed Management Task Force (DMTF) is an industry consortium that develops, supports, and maintains standards for the management of computer systems.

[2] See http://www.dmtf.org/standards/cim/

The SMASH CLP architecture describes a command line protocol used to manage systems and defines three components—Client, Manageability Access Point (MAP), and Managed System—and the way in which these components can interact. The architecture describes how CLP implementations should behave, including the management of different servers regardless of hardware or OS state. It provides a way—a *common* way—to manage different systems regardless of whether they are up and running (in-band) or powered off (out-of-band). Hurrah! Avocent, Dell, Hitachi, HP, IBM, Intel, The Open Group , Peppercon, RLX Technologies, the Storage Networking Industry Association (SNIA), and Sun Microsystems have all stated that they will support SMASH CLP.

SMASH guards and restricts access to its functionality. This is a good thing considering that it provides total remote control of system hardware. The SMASH architecture provides the mechanisms for secure network access, such as passwords, encryption, and digital authentication. NICs contained in SMASH-based products should, therefore, provide these security features. Secure network access is one respect in which SMASH is different from the Intelligent Platform Management Interface (IPMI),[3] a lightweight specification developed by HP, Dell, Intel, and NEC defining a set of common low-level OS-agnostic standards used to monitor system health and manage the system. IPMI implementations generally use low-cost, limited-functionality hardware which does not allow—or has limited support for—secure access.

Historically, DMTF and IPMI manageability efforts have been sometimes at cross-purposes. However, the two organizations—which have many of the same members—are shifting toward a more complementary relationship with IPMI handling "inside the box" interfaces (such as those for power and cooling systems) and providing the infrastructure for more advanced DMTF services.

Because SMASH CLP is a new and still-evolving standard, only a handful of products based on it are shipping. However, HP is one vendor that is delivering early implementations—beginning earlier this year with some of its Integrated Lights-Out (iLO) controllers.[4] These reprogrammed iLOs provide complete SMASH CLP support for all iLO configuration and control functionality. In principle, SMASH could eventually replace each vendor's proprietary scripting languages and tools. In particular, HP plans for the existing proprietary tools—including SmartStart[5]—to co-exist with SMASH until customers are willing to make the migration fully.

HP is rallying the push for SMASH standardization because it correctly realizes that today's value-add comes from higher level tools, such as its Systems Insight Manager (SIM),[6] rather than the low-level control foundations. In the future, SMASH will interface directly with HP SIM using the next generation of Structured Protocol interfaces, for which SIM plug-ins are targeted early next year. Vendors like HP are on the bandwagon to promote, nurse, and use these low-level standards because it helps them up-sell to their more profitable services and tools. The chef concentrates on his cooking,not on making frying pans.

[3] See http://en.wikipedia.org/wiki/Intelligent_Platform_Management_Interface

[4] iLO with SMASH CLD functionality on ProLiant 100 Series Servers became available on August 15, 2005. The same functionality will arrive in iLO for HP Integrity, scheduled for Q106.

[5] HP's SmartStart is a software tool for setting up HP Servers, taking them all the way from bare-metal to up-and-running with an installed operating system.

[6] See Illuminata report "HP Systems Insight Manager: One Console to Rule Them All" (April 2005)