



DMTF Organization Backgrounder

Overview

With more than 4,000 active participants representing 44 countries and nearly 200 organizations, the Distributed Management Task Force, Inc. (DMTF) is the industry organization leading the development, adoption and promotion of interoperable management standards and initiatives. DMTF management technologies are critical to enabling management interoperability among multi-vendor systems, tools, and solutions within the enterprise. By deploying solutions that support DMTF standards, IT managers can choose to deploy a mix of systems and solutions that best meet their users' needs, while reducing management complexity and total cost of ownership. Information about the DMTF technologies and activities can be found at www.dmtf.org.

Organization

Founded in 1992, the DMTF brings the technology industry community and top vendors together in a collaborative, working group approach that involves DMTF members in all aspects of specification development and refinement. Board member companies include Broadcom, Cisco, Dell, EMC, Fujitsu, Hitachi, HP, IBM, Intel, Microsoft, Novell, Sun Microsystems, Symantec and WBEM Solutions.

The DMTF works closely with its Alliance Partners, including Blade Systems Alliance (BladeS), CompTIA, Consortium for Service Innovation, National Institute of Standards and Technology (NIST), Network Applications Consortium (NAC), Open Grid Forum (OGF), Object Management Group (OMG), The Open Group, Organization for the Advancement Of Structured Information Standards (OASIS) Web Services Distributed Management (WSDM) Technical Committee, Printer Working Group (PWG), Service Availability Forum (SA Forum), Storage Networking Industry Association (SNIA), TeleManagement Forum (TM Forum) and the Trusted Computing Group (TCG). These top industry standards bodies are working with and participating in the development of DMTF standards, including CIM – and its semantically rich definitions of management information – as a common approach to address the challenge of providing interoperable distributed management.

The DMTF is led by its Board of Directors, which is responsible for establishing direction and strategies for the organization and the standards it delivers; a Technical Committee, which oversees the Work Groups to develop and document the DMTF's standards; a Marketing Committee, which directs the DMTF's overall industry marketing and communications efforts; and an Interoperability Committee, which supplements the resources of the DMTF so that multi-vendor implementations of DMTF technology can be compatible in the industry. All of the committees collaborate closely with DMTF members, particularly active members of the Work Groups.

Initiatives

Common Diagnostic Model (CDM)

As an extension of the DMTF's CIM, the CDM specification is widely used within the industry to evaluate the health of computer systems in multi-vendor environments. The CDM initiative creates diagnostic instrumentation that can be utilized by platform management applications, and its tight synergy with the other manageability domains in CIM further enables integration of diagnostics into critical management functions.

Desktop and mobile Architecture for System Hardware (DASH)

The DASH Initiative is a forthcoming suite of specifications that takes full advantage of the DMTF's Web Services for Management (WS-Management) specification – delivering standards-based Web services management for desktop and mobile client systems. Through the DASH Initiative, the DMTF will provide the next generation of standards for secure out-of-band and remote management of desktop and mobile systems.

Systems Management Architecture for Server Hardware (SMASH)

The SMASH initiative is a suite of specifications that deliver architectural semantics, industry standard protocols and profiles to unify the management of the data center. The SMASH Server Management (SM) Command Line Protocol (CLP) specification enables simple and intuitive management of heterogeneous servers in the data center independent of machine state, operating system state, server system topology or access method, facilitating local and remote management of server hardware in both Out-of-Service and Out-of-Band management environments. The SMASH initiative also includes the SM Managed Element Addressing Specification, SM CLP-to-CIM Mapping Specification, SM CLP Discovery Specification, SM Profiles, as well as a SM CLP Architecture White Paper.

Standards

Common Information Model (CIM)

CIM allows for the exchange of management information in a platform-independent and technology-neutral way. It is an object-oriented model, describing an organization's computing and networking environments (its hardware, software and services). All managed elements are positioned within this model, clarifying semantics, streamlining integration and reducing costs by enabling end-to-end multi-vendor interoperability in management systems.

Web-Based Enterprise Management (WBEM)

WBEM is a set of management and Internet standard technologies developed to unify the management of distributed computing environments. WBEM provides the ability for the industry to deliver a well-integrated set of standard-based management tools, facilitating the exchange of data across otherwise disparate technologies and platforms.

Alert Standard Format (ASF)

The problem of systems manageability without an operating system has historically been solved with proprietary and relatively expensive solutions. ASF was the first standard to define remote control and alerting interfaces for networked devices, reducing the downtime associated with typical triage and repair required to solve hardware and software failures.

System Management BIOS (SMBIOS)

The SMBIOS Specification addresses how motherboard and personal computer vendors present management information about their products in a standard format, extending the BIOS interface on x86 architecture systems. SMBIOS defines the structure of this system information, allowing its retrieval by management applications that use the Desktop Management Interface (DMI), CIM or direct access, and eliminating the need for error prone operations, such as probing system hardware for presence detection.

For more information, visit the DMTF Web site at <http://www.dmtf.org>. DMTF press releases can be viewed at <http://www.dmtf.org/newsroom>.

###

Press contact:

Lisa Sherwin and Christy Leung
503-619-0425
press@dmtof.org