Using CIM Tools to Manage Dell PowerEdge Servers on Microsoft Windows

The Common Information Model (CIM) is an evolving industry standard for systems management. It has been adopted by most major computer industry vendors and has become the de facto hardware management standard. This article discusses the current Microsoft and Dell CIM providers and how to use CIM tools to manage Dell™ PowerEdge™ servers in a Microsoft® Windows® environment.

BY RADHAKRISHNA DASARI, LINDA MARTINEZ, PRAMADA SINGIREDDY, AND JIANWEN YIN, PH.D.

The Common Information Model (CIM) provides a standardized conceptual model for describing manageable objects in a systems management environment. CIM makes available a hierarchical set of classes that model the basic characteristics of systems, networks, applications, and user management. Microsoft provides CIM instrumentation for the Microsoft Windows OS through Windows Management Instrumentation (WMI). Dell systems management instrumentation information is enabled in CIM by Dell OpenManage™ software.

Several freely available tools allow administrators to view and modify CIM data—classes, instances, and methods. These tools interact with the CIM Object Manager (CIMOM) to access and modify CIM information. The CIMOM is the core component of CIM-based systems management infrastructure. It is the repository of all CIM data and handles communications between clients (management applications and tools) and CIM providers.

This article discusses the two Windows-based CIM tools used to manage Dell PowerEdge servers:

- **CIM Studio**: WMI graphical user interface (GUI) tool
- **WMI Command-Line (WMIC)**: WMI command-line interface (CLI) tool

This article focuses on how to use these tools to manage Dell servers and provides use-case scenarios.

**Understanding Windows Management Instrumentation**

WMI is the Microsoft implementation of the Web-Based Enterprise Management (WBEM) standard and is based on CIM. It provides an interface to manage devices and applications in a network of Windows-based computing systems. WMI can be used for actions such as viewing and changing properties, executing methods, and receiving
event notifications about computer systems, applications, and the OS. WMI has been built into the Windows OS since the release of Windows 2000.

A WMI provider is a software component that functions as a liaison between the CIMOM and managed objects. Using the WMI application programming interfaces, providers supply the CIMOM with data from managed objects and handle all requests on behalf of management applications.

WMI comes with several built-in providers that support creating, deleting, and querying objects; setting properties; and executing methods. Some of the important providers are the following:

- **Active Directory Provider**: Maps Microsoft Active Directory® objects to WMI
- **Distributed File System (DFS) Provider**: Provides DFS functions for the Microsoft Windows Server® 2003 OS family
- **Event Log Provider**: Provides access to data from the event log service and notification of events
- **Performance Monitoring Provider**: Supplies instances of CIM classes that represent performance information, such as CPU and memory performance
- **Security Provider**: Provides access to security settings that control ownership, auditing, and access rights to NT file system files, directories, and shares
- **Simple Network Management Protocol (SNMP) Provider**: Maps SNMP objects to CIM classes
- **System Registry Provider**: Provides access to data in the system registry
- **Windows Driver Model (WDM) Provider**: Provides access to hardware drivers that conform to WDM

### Examining Dell CIM instrumentation

The Dell CIM instrumentation providers are registered as dccim32 and omprv. Dell-provided classes are enumerated under root\CIMV2\dell and have been defined in the dccim32.mof and invcim.mof files. These classes fall into two categories.

Classes in the first category are Dell-defined and are not related to existing CIM classes. Examples of classes in this category are change-management and log classes. Change-management classes include the following:

- **Dell_CMDevice**: Represents the change-management hardware device
- **Dell_CMApplication**: Represents the BIOS, firmware, or driver
- **Dell_CMInventory**: Provides information about the change-management inventory, such as the system name and system ID
- **Dell_CMDeviceApplication**: Represents the association between the device and application
- **Dell_CMOS**: Provides information about the OS
- **Dell_CMProductInfo**: Provides information about the Dell change-management product

Log classes include the following:

- **Dell_PostLog**: Records the system’s power-on self-test (POST); when the system is turned on, the POST tests various system components, such as RAM, the hard drives, and the keyboard
- **Dell_EsmLog**: Records failure threshold violations collected by the Embedded Server Management (ESM) functionality in the Dell OpenManage Server Administrator application

### Using CIM tools

Administrators can use several CIM tools to execute CIM functionality: CIM Studio, WBEMTest, and WMIC.

**CIM Studio.** This tool has a browser-based interface that is available with the WMI software development kit (SDK). After downloading and installing the WMI SDK, administrators can execute this tool by selecting Start > Programs > WMI Tools > WMI CIM Studio. For more details, see the help file provided with the CIM Studio application.

**WBEMTest.** Also referred to as WMI Tester, WBEMTest is a GUI tool available as part of the OS. To run WBEMTest, administrators should select Start > Run > wbemtest.

---

2. For more information about WBEMTest, visit www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/wbemtest_basics.mspx.
**WMIC.** This tool uses a CLI and scripting interface to manage the CIM-enabled system.²

These tools can be used to perform many CIM tasks, but the following sections address the use of CIM Studio and WMIC to manage a CIM-enabled Dell PowerEdge server. To obtain detailed instructions on all of the CIM functionality supported by each tool, see the help files provided with each application or the Web sites provided in this article.

**CIM Studio**

Administrators can perform the following tasks with the CIM Studio tool: connecting to a specific namespace in the CIMOM, discovering all instances of a managed element, viewing CIM data for a managed element, and viewing an association class.

**Connecting to a specific namespace in the CIMOM.** When CIM Studio launches, the “Connect to namespace” dialog box should appear (see Figure 1). Administrators can enter “root\CIMV2\dell” to connect to the Dell provider namespace, or enter “root\CIMV2” to connect to the Microsoft provider namespace.

If CIM Studio has already been launched, administrators can click the Browse for Namespaces icon to select the namespace (see Figure 2).

**Discovering all instances of a managed element.** Both the Microsoft and Dell providers populate information about several managed elements. To view all instances of a particular managed element, administrators can click the Search for Class icon and enter the full or partial class name to locate the CIM class for the managed element of interest. For example, to look at the CIM data for all of the fans on a system, administrators can enter “fan” as the class name (see Figure 3). They can then highlight the specific CIM class name in the Search Results box—for example, CIM_Fan—and click the OK button. The class should be highlighted in the tree view in the left pane of CIM Studio. To retrieve all instances of the CIM_Fan class, administrators can click the Instances icon.

**Viewing CIM data for a managed element.** To view the CIM data available for a specific managed element, administrators can highlight the instance—after displaying all instances of the managed element—and double-click anywhere in the table row (see Figure 4). All properties data for the specific instance can then be viewed.

---

²For more information about WMIC, visit www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/wmic.mspx.
Setting CIM class properties for a managed element. Many CIM class properties are writable. To determine which CIM class properties are writable, administrators should view the Managed Object Format (MOF) file loaded by the provider. If a property is writable, the property definition contains a write qualifier, as in the following excerpt from an MOF file:

```plaintext
[read, write, MappingStrings (*MIF.DMTF|Voltage Probe|001.12*)]
sint32 LowerThresholdNonCritical;
```

Administrators may want to change the lower noncritical threshold of a sensor. To do this, they can retrieve the instance of the sensor and locate the LowerThresholdNonCritical CIM class property in the Name column. In the Value column, they should use the text box to edit the threshold value, and then click the Save icon to store the new threshold value. To determine whether the new threshold was stored successfully, administrators can view all instances of the managed element, select the specific instance, and view the property data. If the value was not changed, the new threshold may not have been within the valid range, or another error may have occurred.

Viewing an association class. An association class defines a relationship between CIM classes. Dell providers include one association class, Dell_FanSensor. This class associates the fan sensors with each fan device. Microsoft providers implement the Win32_AssociatedProcessorMemory class, which associates the processor cache with the processor.

To view specific associations, administrators should first retrieve all instances of the association class, then select a specific association class, and finally select the Associations tab. Figure 5 shows an instance of the Win32_AssociatedProcessorMemory association class that displays the connection between the processor cache (Win32Cache_Memory) and the processor (Win32_Processor). To view the property values of the cache or processor, administrators can double-click the device in the GUI and select the Properties tab.

To view further associations, administrators can click a device in the Associations tab. For example, double-clicking the Win32_Processor instance shows the computer system and two processor cache instances associated with the processor (see Figure 6).

WMI Command-Line

WMI is a simple CLI for WMI. It is also a powerful tool for managing WMI-enabled servers. WMI can be used as a command-line tool and in the interactive mode as a shell to perform WMI-supported actions. To enter the WMI shell, administrators should type “WMIC”; typing “WMIC /?” provides help information on the basic WMI switches.

Discovering managed elements. Figure 7 shows the result of a WMIC command to retrieve the instances of the Dell_CMDevice classes executed on an eighth-generation Dell PowerEdge server. The text format results are output to the console with the device information on the managed server. The command executed is as follows:

```plaintext
wmic /node:localhost /namespace:\root\CIMV2\Dell path Dell_CMDevice
```

When executing the command on a different server on the network, administrators should use /node:IP address instead of /node:localhost. A username and password are not necessary when the administrator executes the command from a remote system on the same domain. Otherwise, the user credentials need to be provided through the /User and /Password switches. Administrators
can run the WMI command through the network to retrieve the inventory information of all managed servers, and can also write scripts to compare the inventory software and firmware with the latest versions and run automatic updates.

**Viewing CIM data for managed elements.** Advanced command-line options are provided through WMI to retrieve more specific information than is obtainable with basic commands. For example, the following command retrieves the device ID, name, and status information for all the fans on the server that are not healthy:

```plaintext
wmic /node:localhost /namespace:\\root\CIMV2\ Dell path CIM_Fan where (Status = "OK") GET DeviceID,Name,Status
```

Figure 8 shows the result of this command. System administrators can use this function to find any problematic components through scripting.

The `set` switch can be used to set the value of any writable properties. System administrators can use the `set` function to change the values of any writable properties on any node. The `ASSOC` alias can be used to retrieve the association instance of any given class.⁴

Other scripting tools, such as Microsoft Scriptomatic, can be used to generate Microsoft Visual Basic® scripts to retrieve information through WMI.⁵

**Managing Dell PowerEdge servers efficiently through CIM**

Dell PowerEdge servers have been enabled with the CIM standard on various systems management aspects, which can help greatly improve their manageability. By using the CIM Studio GUI tool, administrators can perform one-to-one systems management through the Internet or an intranet securely and efficiently. By using the WMIC CLI tool, administrators can perform efficient one-to-one and one-to-many systems management through scripting. ☞

RadhaKrishna Dasari is a software engineer consultant in the Dell Enterprise Systems Management Software Organization. He currently works on enabling the Distributed Management Task Force (DMTF) CIM standards on Dell servers. He has a bachelor's degree in Computer Science from Osmania University in India and a master's degree in Computer Science from Arizona State University.

Linda Martinez is a software engineer consultant in the Dell Enterprise Systems Management Software Organization. She currently works on enabling the DMTF CIM standards on Dell servers. Linda has a bachelor's degree in Electrical Engineering from The University of Texas at Austin.

Pramada Singireddy is an enterprise system test engineer in the Dell Product Group. She has a bachelor's degree in Computer Science from Osmania University in India and a master's degree in Computer Science from Arizona State University.

Jianwen Yin, Ph.D., is a software engineer senior consultant in the Dell Enterprise Systems Management Software Organization. He currently works on enabling the DMTF CIM standards on Dell servers. Jianwen has a Ph.D. in Computer Science from Texas A&M University.

---

⁴For more information about WMIC aliases, visit www.microsoft.com/resources/documentation/windows/xp/all/products/en-us/wmic.mspx.

⁵For more information about Microsoft scripting tools, visit www.microsoft.com/technet/scriptcenter/default.mspx.