Exploring Windows Server 2003 Cluster Management

The Microsoft® Windows® Server 2003 operating system includes flexible, customizable, and powerful management tools. This article describes ways to automate cluster administration and improve cluster management.

By Ananda Sankaran

The Microsoft® Windows® Server 2003 operating system provides powerful management capabilities that IT organizations can use to administer server clusters based on Microsoft Cluster Service (MSCS). By leveraging the tools and other utilities included with the Windows Server 2003 operating system and Resource Kit, administrators can formulate flexible management schemes customized for specific cluster administrator tasks. These tools are simple, but very powerful.

An enhanced command-line infrastructure is one key benefit of the Windows Server 2003 family. Windows Management Instrumentation (WMI), a component of the Windows operating system, provides a consistent means of accessing systems management information. The WMI Command-line (WMIC) utility allows administrators to perform WMI-related management tasks from the command line or through scripts and other management applications. Such capabilities give Windows Server 2003 the power and flexibility often associated with UNIX®-based systems—at a low total cost of ownership (TCO).

Generating SNMP traps for cluster-specific events

Simple Network Management Protocol (SNMP) traps are a standard mechanism for managed systems and devices to communicate system-specific events over the network to a management application. The management application can then take a suitable action, such as alerting an administrator, sending an e-mail, or paging a responsible party.

Administrators can configure the cluster-specific events logged into the Windows event log to generate SNMP traps, which are then forwarded to a management application. The evntwin command within Windows Server 2003 starts the Event to Trap Translator, a
graphical user interface— (GUI—) based utility that helps to translate Windows events to traps (see Figure 1). A command-line interface (CLI) version of this tool, called evntcmd, also exists. These utilities are installed as part of the SNMP service installation on Windows Server 2003. For more information, see Windows Server 2003 online help, available from the operating system GUI.

Administrators should use evntwin on all the cluster nodes to identify and register cluster events for translation into SNMP traps. Using evntwin on all the nodes is important because the cluster virtual server may reside on any node, which means that cluster events may be logged on different nodes at different times. Also, if cluster event replication is enabled (the default), every cluster event is logged into every node’s event log—so all nodes generate SNMP traps for the same event. To prevent multiple SNMP traps from being generated, administrators should disable event replication.

Dell™ OpenManage™ IT Assistant, a management application with a rich feature set, can be configured to receive SNMP traps from the cluster. Administrators must also configure the SNMP service on each cluster node to send traps to the IT Assistant server station. To correctly interpret SNMP traps, IT Assistant requires further configuration; for more information, visit http://support.dell.com and download the Dell OpenManage IT Assistant User’s Guide. Once configured, IT Assistant can send e-mail, pages, and alerts based on the SNMP traps sent to it.

**Using WMI to manage clusters**

WMI is an operating system component that manipulates and stores information about managed objects (see Figure 2). A managed object is a logical or physical system component—such as a hard drive, network router, database system, or cluster—that creates a data representation of an object. Management applications and scripts can use WMI to query and set management information on enterprise hardware and software components, providing a means to automate cluster administration tasks.

WMI derives from the Web-Based Enterprise Management (WBEM) initiative, a set of management and Internet standard technologies developed to unify the management of enterprise computing environments. The core component of the WBEM standard is a specification known as the Common Information Model (CIM).

CIM provides a uniform and consistent data description mechanism for any data provided by the managed objects. WMI includes a CIM object manager and a CIM object repository for manipulating and storing this data. A management application or script can obtain information regarding a managed object from the WMI infrastructure. For more information on WMI, see the Windows Server 2003 online help available from the operating system GUI or visit the Microsoft Developers Network (MSDN) at http://msdn.microsoft.com.

**Exploring useful scripting resources**

Windows Server 2003 contains a standard set of WMI classes and providers for handling managed objects of the Windows operating system. The Scripting API (application programming interface) for WMI facilitates developing quick, simple scripts for accessing these classes (see Figure 3). For example, administrators can write a
script to manage a cluster using the server cluster WMI provider and classes.

Scripts written using Windows Script Host (WSH) or Microsoft Visual Basic® Scripting Edition (VBScript) can perform operations on file system objects, manipulate network printers, or change environment variables. Other useful scripting tools include wbemtest.exe, for checking the list of WMI classes on a system, and scriptomatic.exe, for developing WMI scripts. Scriptomatic.exe automatically recognizes WMI classes on a system and helps to include them in a script. Administrators also can use the wmic.exe utility to directly query WMI managed objects on a system. Both wmic.exe and wbemtest.exe are shipped with Windows Server 2003; for scriptomatic.exe, visit Microsoft Technet at http://www.microsoft.com/technet.

Writing an audit-logging or alert e-mailing script
Audit logs help to track all changes and problems associated with clustered components. These logs simplify discovering how changes occurred, understanding the changes, and monitoring or preventing the recurrence of those changes. By using server cluster WMI provider classes, administrators can create scripts triggering specific cluster events to write information to an audit log in real time. Administrators can determine the log format and the information to be written. Also, the same technique can be used for sending real-time e-mail alerts when crucial cluster events are generated. For examples, please see “Sample VBScript scripts for cluster management” in the online version of this article (http://www.dell.com/powersolutions).

Using the ClusterRecovery utility to recover a quorum disk
Cluster applications store data on shared disks accessible by all nodes in the cluster. The cluster configuration database itself and cluster checkpoint files are stored in a special shared disk called the quorum disk (see Figure 4). Administrators can recover the application data on shared disks by using standard data backup software, but recovering data on the quorum disk requires a different procedure.

The cluster checkpoint files (.cpt files) store the cluster resource configuration data in the registry of the cluster node owning the resource. The cluster service continually updates the checkpoint file from the corresponding registry data. During failover, these files are used to update the registry of an available node, so they must be consistent with registry data for proper operation of the cluster and applications.

A quorum disk recovered from standard backup may not contain the latest resource registry state in the checkpoint files, so the data in the registry could be overwritten by the recovered quorum data, leading to inconsistent resource states. After a failure, the checkpoint files should be re-created from the latest registry settings on the nodes, not from the quorum. However, the cluster database information and other data on the quorum can be recovered using standard backup procedures.

The ClusterRecovery utility in the Windows Server 2003 Resource Kit helps recover resource checkpoint files on the quorum and failed shared disks from the latest registry data that exists on the nodes (see Figure 5). Administrators also can use...
this utility for re-creating a checkpoint file for a single resource, not just the whole cluster.

Following a disk failure in a cluster, administrators typically replace the failed physical disk and restore data files recovered from backup onto the new physical disk. However, before performing a restore on the new physical disk, administrators must create a logical cluster disk resource within MSCS that represents the new disk.

Using ClusterRecovery, administrators can include the new resource as the old failed resource and then delete the old resource representation of the failed disk. The utility automatically transfers the properties of the failed resource to the new resource. Any dependencies on the old resource are changed to point to the new resource. The new disk now has the same resource representation in the cluster that the failed disk did, and administrators can restore application data to the new disk from backup.

**Taking advantage of native Windows Server 2003 tools**

High-availability computer clusters running on standards-based hardware such as Dell PowerEdge™ servers using the Windows Server 2003 operating system offer many advantages to IT organizations, including cost-effective reliability, availability, and high performance. Managed these systems can be complex, but Windows Server 2003 provides several tools for simplifying cluster management. Using these tools, administrators can track and log system events, write scripts to generate alerts, and recover cluster disks safely. By taking advantage of native support in the Windows Server 2003 operating system, administrators can automate cluster administration tasks and gain more control over the clusters they manage.

Ananda Sankaran (ananda_sankaran@dell.com) is a software engineer in the HighAvailability Cluster Development Group at Dell. His current interests related to high-availability clustering include cluster management, databases, and storage area networks (SANs). Ananda has a master’s degree in Computer Science from Texas A&M University.