MANAGING OPERATING SYSTEMS AND APPLICATIONS WITH THE DELL MANAGEMENT CONSOLE

By Jordan Gardner

The Dell™ Management Console Powered by Altiris™ from Symantec™, based on the modular Symantec Management Platform architecture, is designed to provide comprehensive, simplified systems management in enterprise IT environments. By taking advantage of the extensibility and scalability of the Symantec framework, administrators can use this console to support robust one-to-many OS and application management policies.

Related Categories:
Altiris
Dell Management Console
Dell OpenManage
Symantec
Systems management
Visit DELL.COM/PowerSolutions
for the complete category index.

In enterprise IT environments, efficient management processes can be critical to success. Effective management tools must provide broad support for different devices and technologies while still delivering powerful capabilities.

To help meet these needs, Dell has partnered with Symantec to develop its new management solution: the Dell Management Console.[1] Based on the modular Symantec Management Platform architecture, this tool enables administrators not only to increase their control over Dell hardware, but also to take inventory, distribute software packages and OS patches, push images or scripted installations, perform IT Infrastructure Library (ITIL)–compliant asset management, schedule and perform backup and recovery operations, and more.[2] Over 20 plug-in solutions are available to help manage a variety of devices and technologies, with more expected to be released from Symantec, Dell, and their partners in the future. Taking advantage of this flexible, extensible framework enables administrators to implement robust one-to-many OS and application management through a single simplified management solution.

SYMANTEC MANAGEMENT PLATFORM ARCHITECTURE

The Symantec Management Platform architecture is a key component of the Dell Management Console, providing a modular framework for comprehensive systems management (see Figure 1). This framework provides administrators with a single console to manage multiple aspects of their environments, from network switches to the applications installed on handheld devices. Rather than requiring multiple point solutions functioning independently to perform their specific tasks, this architecture enables supported plug-ins to integrate and use data from one another. For example, if a disk drive were failing, alert information would be sent to the Dell Management Console through the monitoring solution, which could then automatically trigger a backup using the backup solution, after which detailed warranty information about the server could be sent to the administrator

[1] The Dell Management Console had not yet been released to ship at press time (February 20, 2009); features and capabilities in production version are subject to change.

[2] For more information on ITIL, see “Implementing Best Practices: The Dell Management Console and ITIL,” by John Stahmann, in *Dell Power Solutions*, March 2009, DELL.COM/Downloads/Global/Power/ps1q09-20080450-Stahmann.pdf. For more information on migrating to this new management platform, see “Migrating to the New Dell Management Console,” by Manoj Poonia and Ed Casmer, in *Dell Power Solutions*, March 2009, DELL.COM/Downloads/Global/Power/ps1q09-20080448-Gonzalez.pdf.

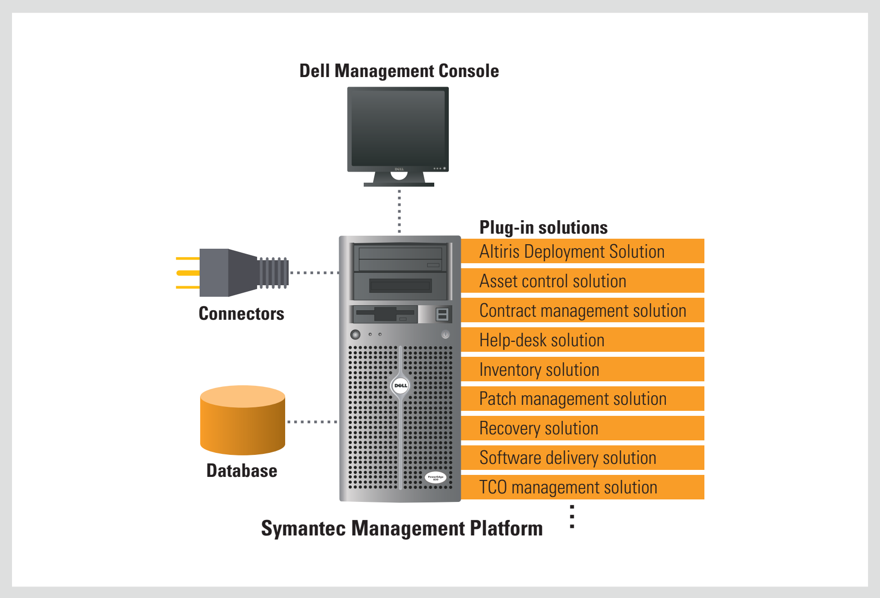


***Figure 1.** Symantec Management Platform architecture*

using the data from the asset management solution. The Symantec Management Platform architecture allows this process to happen seamlessly by leveraging the same database and user interface across all of the plug-in solutions. Administrators could also install the Dell Management Console, inventory solutions, and handheld management solutions on the same back-end server framework to provide a single management console for server, desktop, and mobile device management. The role and scope security engine can also work across multiple installed solutions.

The Symantec Management Platform is available as a complimentary download and can be installed independently of other supported components. Once installed, it serves as the engine that manages communication with remote agents and the Microsoft® SQL Server® or SQL Server Express database. Administrators can install the database on the same server as the platform or on a remote server. The Symantec Management Platform provides features common to each of the modular solutions, including the Web browser–based console for uniform navigation between solutions, common agent, reporting engine, event and alert engine, task and automation engine, and notification functionality. (For more information, see the "Symantec Management Platform communication architecture" sidebar in this article.)

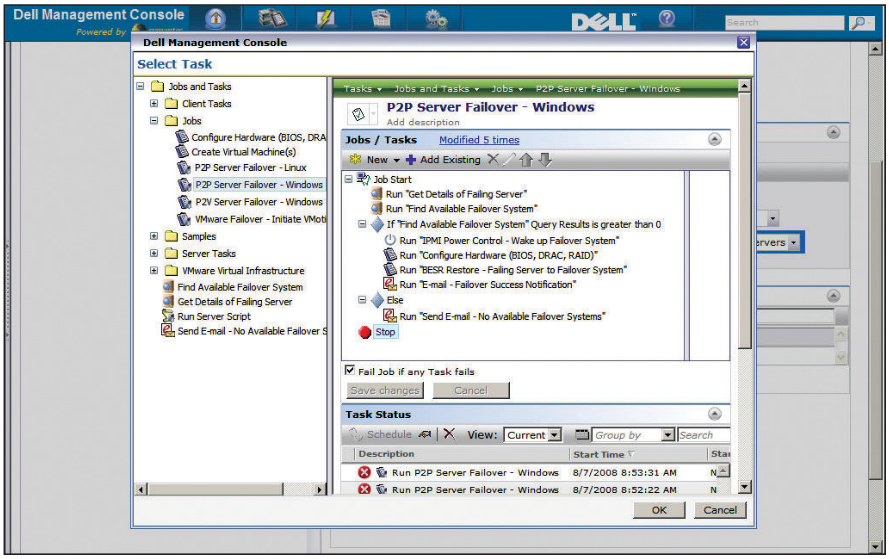
OS MANAGEMENT

The modular Symantec Management Platform architecture enables administrators to use the Dell Management Console to manage not only Dell hardware, but also many aspects of operating systems—including deployment, migration, and hardware refreshes; security; and monitoring and availability. Using other plug-in solutions can also further enhance OS management capabilities.

Deployment, migration, and hardware refreshes

Server deployment can be challenging and time-consuming even for experienced administrators. Dell and Symantec have worked together to integrate the hardware component configuration capabilities of the Dell OpenManage™ Deployment Toolkit with the powerful automation capabilities of the Altiris Deployment Solution™ plug-in, creating Altiris Deployment Solution for Dell Servers (see Figure 2). This solution can plug into existing Dell Management Console implementations and help significantly reduce server deployment times—potentially from hours to minutes.

Altiris Deployment Solution is designed not only for servers, but also for desktops, handheld devices, and thin clients. It can use hardware inventory information captured by the Dell Management Console to assist in a migration assessment or hardware refresh assessment, helping identify systems that are capable of migration or that should be retired. Other key processes involved



Jobs and Tasks
- Client Tasks
- Jobs
  - Configure Hardware (BIOS, DRA
  - Create Virtual Machine(s)
  - P2P Server Failover - Linux
  - P2P Server Failover - Windows
  - P2V Server Failover - Windows
  - VMware Failover - Initiate VMoti
- Samples
- Server Tasks
- VMware Virtual Infrastructure
- Find Available Failover System
- Get Details of Failing Server
- Run Server Script
- Send E-mail - No Available Failover S

P2P Server Failover - Windows

```
Job Start
  Run "Get Details of Failing Server"
  Run "Find Available Failover System"
  If "Find Available Failover System" Query Results is greater than 0
    Run "IPMI Power Control - Wake up Failover System"
    Run "Configure Hardware (BIOS, DRAC, RAID)"
    Run "BESR Restore - Failing Server to Failover System"
    Run "E-mail - Failover Success Notification"
  Else
    Run "Send E-mail - No Available Failover Systems"
  Stop
```

☑ Fail Job if any Task fails

Description	Start Time	Sta
Run P2P Server Failover - Windows	8/7/2008 8:53:31 AM	N
Run P2P Server Failover - Windows	8/7/2008 8:52:22 AM	N

***Figure 2.** Automated server failover job using Altiris Deployment Solution for Dell Servers and Symantec Backup Exec System Recovery in the Dell Management Console*

in a migration can then be automated, including configuration capture, imaging, application deployment, and configuration restore operations.

The monitoring capabilities of the Dell Management Console enable data to be continually gathered and summarized to help administrators keep servers up and running 24 hours a day. Reports, dashboards, and the event console view provide an enterprise-wide status of monitored systems. In addition to dashboard views, alerts received that match a set of predefined criteria can trigger a series of automated actions. Administrators can be automatically notified through e-mail, or trigger a set of remediation tasks when a given alert is received that matches the automated action criteria.

The Altiris Monitor Solution™ plug-in contains a set of predefined rules and metrics for monitoring OS performance and availability. It includes predefined monitor packs for Microsoft Windows®, Linux®, and VMware® ESX servers that administrators can easily import into the Dell Management Console to help ensure optimal system uptime and performance.

Security

The Dell Management Console incorporates comprehensive endpoint security through its integration with Symantec Endpoint Protection, which combines multiple endpoint security technologies, including antivirus, anti-spyware, personal firewall, intrusion prevention, device control, and network access control. Through the Dell Management Console, administrators can manage installations and client settings of the Endpoint Protection agent, perform quick scans, and report and fix outdated virus definitions.

In addition to Endpoint Protection, Symantec plans to continue to integrate powerful security, compliance, and backup solutions into the Symantec Management Platform, including Symantec Backup Exec™ and Data Loss Prevention software.

SYMANTEC MANAGEMENT PLATFORM COMMUNICATION ARCHITECTURE

Communication between the management agent and the management server (where the Symantec Management Platform is installed) fundamentally consists of XML files that are compressed and transferred through HTTP (on port 80) or HTTP over Secure Sockets Layer (HTTPS) (on port 443). Each management agent requests a policy update from the management server on an interval defined by the administrator; the default setting is once every hour.

During this update, the agent sends a request to the Symantec Management Platform to request new policies that apply to the system running the agent. If administrators have made any policy additions or modifications, the agent downloads a new policy configuration XML file specifying the work to be performed by the agent and its solution plug-in. For example, the agent might download and parse this XML configuration file to determine that it should now run a software inventory scan every 12 hours and a hardware inventory scan once a week, deny access to unauthorized software programs (such as games or instant messaging clients) during the working hours of 8 A.M. to 5 P.M., and download and execute the most recent Microsoft patches or Dell BIOS updates from the management server immediately. The process of downloading the configuration policy typically generates a little less than 2 KB of round-trip traffic per agent.

POLICIES, TASKS, AND FILTERS

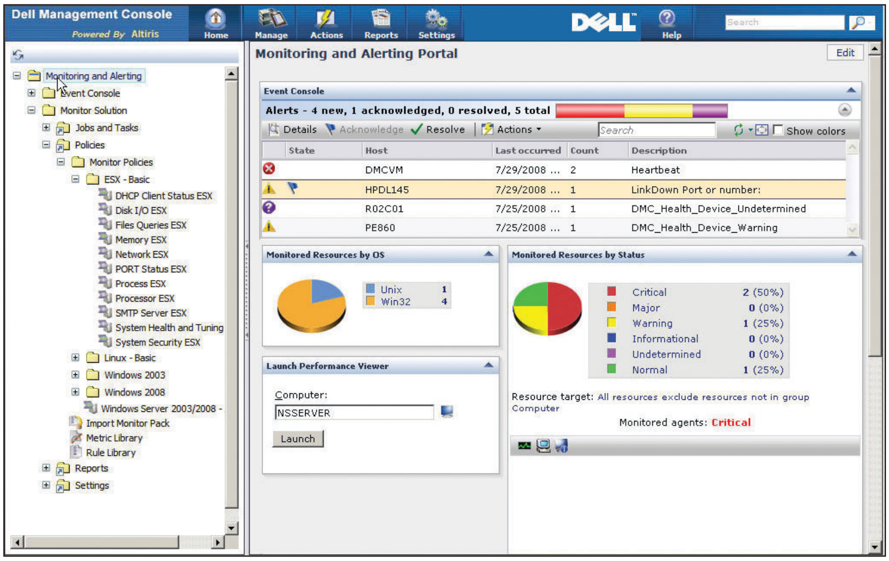
The Symantec Management Platform uses filters to associate policies and tasks with systems. Filters are simply groupings of systems defined by a rule or query. A given system may belong to no filters, one filter, or multiple filters. There are two different types of filters:

- **Static filters:** A system's membership in a static filter changes only when an administrator explicitly adds it to or removes it from the filter.
- **Dynamic filters:** A system's membership in a dynamic filter changes based on the system properties; as those properties change, the system automatically moves into or out of the filter. It can be helpful to think of dynamic filters as being based on a SQL `WHERE` clause. For example, administrators might create a dynamic filter that consists of all systems running the Microsoft Windows Server® 2008 OS with 8 GB of RAM and joined to a specific domain. If either of those two properties changes for a particular system, the system is automatically removed from the filter, thereby disassociating it from policies assigned to that filter.

Dynamic filters provide a powerful mechanism for automating systems management. For example, administrators could create an ongoing policy to deliver a specific Dell BIOS update to systems that may require it. If a new system with the management agent is added to the network several months later, it would automatically join the predefined filters for which it qualifies. Policies assigned to those filters then become effective for the new system, which not only automatically receives the BIOS update it needs, but also executes other tasks assigned to the policies that govern the system.

Monitoring and availability

The Dell Management Console includes robust agent and agentless monitoring of resources, helping ensure server availability and helping reduce costs associated with server downtime through comprehensive, Web browser–based performance and event monitoring (see Figure 3). Administrators can use real-time monitoring to assess current operational states, view historical data to identify trends and isolate recurring issues, and manage problem tasks with integrated alert management.



Alerts - 4 new, 1 acknowledged, 0 resolved, 5 total

State	Host	Last occurred	Count	Description
	DMCVM	7/29/2008 ...	2	Heartbeat
	HPDL145	7/29/2008 ...	1	LinkDown Port or number:
	R02C01	7/25/2008 ...	1	DMC_Health_Device_Undetermined
	PE860	7/25/2008 ...	1	DMC_Health_Device_Warning

Unix	1
Win32	4

Critical	2 (50%)
Major	0 (0%)
Warning	1 (25%)
Informational	0 (0%)
Undetermined	0 (0%)
Normal	1 (25%)

Computer: NSSERVER

Resource target: All resources exclude resources not in group Computer

Monitored agents: Critical

Figure 3. *Robust, comprehensive performance and event monitoring in the Dell Management Console*

APPLICATION MANAGEMENT

The Dell Management Console supports robust application management through plug-in components, enabling administrators to inventory, meter, and report software usage and to package, deliver, and monitor end-user applications.

Inventory, metering, and reporting

The Altiris Client Management Suite™ and Server Management Suite™ plug-ins can capture detailed information about servers, desktops, and laptops and determine how many copies of an application are installed on these systems. The suite's software metering technology can determine which software applications are actually being used and how often, helping administrators eliminate or reallocate unused licenses, prepare for audits, and plan for future software purchases. Matching usage information to purchased license counts stored in the configuration management database (CMDB) can also help administrators accurately gauge future software needs and purchase accordingly, helping reduce the costs and risks associated with over- and underbuying.

Packaging, delivery, and monitoring

The Altiris Client Management Suite and Server Management Suite plug-ins enable powerful application packaging, delivery, and monitoring capabilities, including secure, bandwidth-sensitive distribution of applications and updates throughout an organization. These solutions can support software distribution over local area networks (LANs) or wide area networks (WANs) to servers, desktops, and laptops from the central console, and offer features such as multicasting, Intel® Active Management Technology, and Wake-on-LAN.

Administrators can target specific groups of systems, users, or departments by creating authorized filters to receive the software. Administrators can also apply software uninstall policies to help avoid the malicious installation of unauthorized software, permit or deny the execution of a given application, and send custom denial messages or restrict application usage to certain hours of the day.

Administrators can also import application monitor packs to proactively monitor the performance of critical applications such as Microsoft Exchange and SQL Server. These packs include predefined rules and system performance metrics designed to accurately report current application status, helping administrators to maximize the performance and availability of critical applications.

COMPREHENSIVE, SIMPLIFIED SYSTEMS MANAGEMENT

The Dell Management Console is designed to provide a comprehensive, simplified tool for one-to-many systems management in enterprise IT environments. By taking advantage of the modular Symantec Management Platform architecture, administrators can use this console not only to manage Dell-specific functions and hardware, but also to implement robust automation, control, and extensibility through a single management interface.

Jordan Gardner is a technical strategist on the Dell Alliance team at Symantec. He has a bachelor's degree in Computer Science from Brigham Young University.

MORE ONLINE
DELL.COM/PowerSolutions

QUICK LINKS

Dell systems management:
DELL.COM/OpenManage

Symantec and Dell:
www.symantec.com/dell