

## Applying Updates for Dell PowerEdge Servers Using Microsoft Systems Management Server 2003 **Part 1**

Managing hardware updates has become a key feature of Microsoft® Systems Management Server (SMS) 2003 with the introduction of the SMS 2003 Inventory Tool for Dell Update. When designing and implementing a methodology to manage software updates, administrators can also plan for and select appropriate hardware updates, thereby consolidating both functions into a single process that can help keep environments stable and reliable.

### Related Categories:

*Change management*

*Dell OpenManage*

*Dell PowerEdge servers*

*Dell Update Packages*

*Microsoft Systems Management Server (SMS)*

*Storage management*

Visit [www.dell.com/powersolutions](http://www.dell.com/powersolutions) for the complete category index.

**T**he Microsoft Systems Management Server (SMS) 2003 Inventory Tool for Dell Update (ITDU) helps administrators update Dell™ PowerEdge™ servers with the latest system BIOS; system firmware, also known as Embedded Server Management (ESM) firmware; remote access controller firmware; RAID controller firmware; and device drivers. This tool utilizes the existing software update management feature of SMS 2003 Service Pack 1 (SP1) and later to help automate the update process for Dell systems, minimizing the resources required to transport Dell Update Packages across a network. Once the SMS 2003 ITDU software is installed, the SMS console interface seamlessly provides access to its set of Dell update capabilities (see Figure 1).

This article provides best-practices guidelines for those who manage, review, or approve hardware updates for Dell servers or oversee Dell server-based data centers and test environments. The update process described in this article is based on a high-level, four-stage patch management process model. The four phases are as follows:

- **Assess:** Administrators determine what systems are in the production environment, what security threats and vulnerabilities might affect those systems, and whether the organization is prepared to respond to updates.
- **Identify:** Administrators discover updates in a reliable way, determine whether the updates are relevant to the environment, and determine whether an update represents a standard response or an emergency change.
- **Evaluate and Plan:** Administrators decide whether to deploy the update, determine what is needed to deploy it, and test the update in a production-like environment to help confirm that it does not compromise critical systems and applications.
- **Deploy:** Administrators roll out the approved update to the production environment to meet the requirements of any deployment service-level agreements (SLAs).

This article discusses the Assess phase and the Identify phase; for the Evaluate and Plan phase and the Deploy phase, see “Applying Updates for Dell PowerEdge Servers Using Microsoft Systems Management Server 2003: Part 2” at [www.dell.com/downloads/global/power/ps3q06-20060249-Microsoft-SOE.pdf](http://www.dell.com/downloads/global/power/ps3q06-20060249-Microsoft-SOE.pdf).

## Prerequisites for using the SMS 2003 Inventory Tool for Dell Update

Before using the SMS 2003 ITDU tools for patch management, administrators should have basic network and system administrative skills, including the ability to manage software and hardware update life cycles. In addition, they should be familiar with Microsoft SMS 2003 and SMS 2003 SP1; SMS 2003 software update scanning tools, consisting of the Security Update Inventory Tool and the Office Inventory Tool for Updates; the latest version of Microsoft Baseline Security Analyzer (MBSA); and Dell server hardware components and models.

The SMS 2003 ITDU is designed to scan and update supported servers<sup>1</sup> that meet all of the following criteria:

- Managed by SMS 2003 SP1 or later
- Running a supported OS: Microsoft Windows® 2000 Server SP3 or later; Microsoft Windows 2000 Advanced Server SP3 or later; or Microsoft Windows Server® 2003 Standard Edition or Enterprise Edition
- Using one of the supported OS languages within a supported SMS configuration

The SMS 2003 ITDU must be installed on an SMS 2003 SP1 site server, and it should be installed and configured from the most central SMS 2003 SP1 site in the hierarchy, allowing central administration and configuration of hardware updates.

The SMS 2003 ITDU uses components from a Dell Partner Development Kit (PDK), and support for these components does not follow the standard Microsoft enterprise product support life cycle. Microsoft intends to issue periodic updates to the SMS 2003 ITDU; only the most current version will be supported. Dell intends to issue periodic updates to the PDK, and the SMS 2003 ITDU includes a feature to automatically download compatible PDK versions; if

this feature is not used, administrators must manually download the PDK at regular intervals. Only the current and two previous versions of the PDK support the SMS 2003 ITDU.

## Key challenges for the hardware update process

Administrators should be aware of several key challenges in applying hardware updates to Dell server environments. For example, some Dell server models require multiple updates to be applied at the same time and in the correct sequence. Some servers may also not have a working SMS agent installed, meaning SMS may not be able to inventory or manage them. In addition, custom configurations may cause unexpected results during update deployment.

## Assess phase

During the Assess phase, administrators establish baselines for the existing IT environment to prepare the environment for patching. This ongoing process helps determine which Dell server models and hardware components exist in the environment.

Activities carried out during the Assess phase include discovering and inventorying Dell servers, assessing Dell hardware configurations, assessing Dell hardware dependencies, and establishing a baseline for Dell server hardware.

## Discovering and inventorying Dell servers

Administrators can use the SMS 2003 systems discovery mechanism to discover computers in the IT environment. They must then inventory the systems to identify Dell servers according to

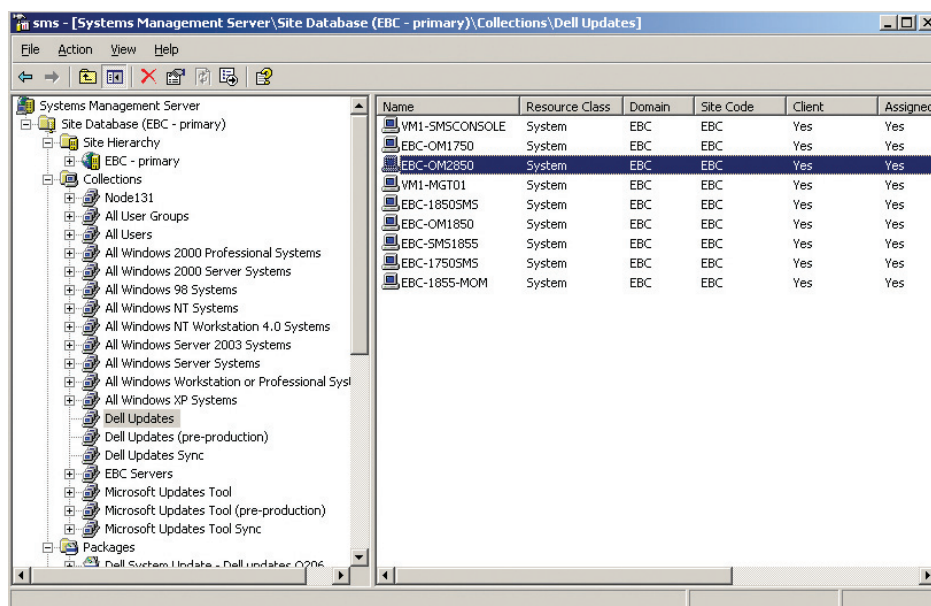


Figure 1. Access to Dell updates following installation of the SMS 2003 Inventory Tool for Dell Update within an SMS site

<sup>1</sup> For a list of Dell server models supported by the SMS 2003 ITDU, see the readme file at [ftp.dell.com/cmsdk/PDK\\_readme.doc](http://ftp.dell.com/cmsdk/PDK_readme.doc).

the server model types and versions, OS types and versions, server roles, applications and versions, application dependencies, network connectivity, and applicable and installed hardware updates.<sup>2</sup>

The SMS 2003 ITDU assists with the Assess phase using the following:

- **Scan component:** Enables administrators to scan Dell servers for installed and missing updates, in the same way MBSA determines compliance for Microsoft security updates
- **Synchronization Host component:** Downloads the Dell Update Catalog from within SMS directly from the Dell FTP site on a recurring schedule
- **Dell-specific reports:** Show installed and missing Dell system and component updates

### Assessing Dell hardware configurations

The next step in the Assess phase requires understanding how Dell servers have been configured, specifically whether a server is attached to an external storage device, such as a storage area network (SAN) or network attached storage (NAS) device. Depending on how an external device is configured with the server, a reboot may need to be suppressed until a local administrator is physically available on-site.

The SMS 2003 ITDU cannot determine the types of devices attached to a Dell server. Nevertheless, administrators should understand how external devices interact with the server and how the server manages and configures devices. They can use the SMS 2003 SP1 hardware inventory feature to inventory a server for applications or tools that are loaded when a disk controller or external device connectivity is set up.

Some items that should be considered when assessing Dell hardware configurations include the following:

- Attached devices and their configurations, including SAN, NAS, and SCSI
- Dell servers configured in an active/active or active/passive cluster
- Potential compatibility issues with Dell management tools such as the Dell OpenManage™ suite and Dell OpenManage Array Manager, which require specific hardware versions to be intact on Dell servers
- Customized BIOS settings, including BIOS passwords, boot sequence, and so on
- Multiple operating systems on a single Dell server
- Boot configuration order, including drives and directories
- SLAs associated with the specific server and the services it is providing

- Approved maintenance windows for applying updates and taking the server out of service

Although stand-alone servers may not need as much attention as servers with attached devices, administrators should use the SMS 2003 SP1 hardware and software inventory features to assess stand-alone configurations.

### Assessing Dell hardware dependencies

Updating hardware components on Dell server models using the SMS 2003 ITDU requires an assessment of the following:

- OS version and service pack
- Server manufacturer and model
- Hardware component versions, including drivers for devices such as the Dell PowerEdge Expandable RAID Controller (PERC); firmware for devices such as the PERC, Cost Effective RAID Controller (CERC), Dell Remote Access Controller II (DRAC II), DRAC III, and so on; ESM firmware; and BIOS
- Dell OpenManage version, including Server Administrator and Array Manager
- SMS site maintenance tasks, particularly the Delete Aged Inventory History and Delete Inactive/Obsolete Client Discovery Data tasks
- Patch age date, located in `X:\Program Files\Dell Update Inventory Tool\PkgSource\Scan.ini`, where `X` represents the drive where the SMS 2003 ITDU was originally installed

**Validity of assessment results.** The SMS 2003 ITDU scans for applicable and installed hardware updates for supported Dell server models. Hardware component details reported to the SMS 2003 site database depend on the hardware component manufacturer's ability to publish this information to Windows Management Instrumentation (WMI) and on whether the vendor's hardware configuration software has been installed to pick up those additional hardware attributes in WMI. It is not always possible to capture all details, such as the asset tag, serial number (service tag), or system ID.

*Note:* Administrators should consider the time interval of Dell hardware updates, because hardware updates may not occur as frequently as OS and application updates. If hardware inventory does not run during a 20-day period, hardware updates are aged out of the `WIN32_PatchStat_Extended` WMI class. To help avoid this problem, administrators should modify the value of the `PatchAge` setting in the `Scan.ini` file to coincide with the hardware upgrade interval. If this setting is left at the default setting of 20, updates

<sup>2</sup> For more information about SMS 2003 systems discovery and inventory features, see the *Systems Management Server 2003 Operations Guide* at [www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/default.mspx](http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/default.mspx) and *Systems Management Server 2003 Concepts, Planning, and Deployment Guide* at [www.microsoft.com/technet/prodtechnol/sms/sms2003/cpdg/default.mspx](http://www.microsoft.com/technet/prodtechnol/sms/sms2003/cpdg/default.mspx).

may not report back properly within the SMS Administrator console, especially if the SMS site maintenance tasks are configured to occur frequently. After this file has been updated, administrators should refresh the distribution points to reflect the change and have the clients perform a scan with the updated file.

**Dell OpenManage dependencies.** The Dell OpenManage suite, including Server Administrator and Array Manager, can be dependent on a particular hardware component version. Administrators may need to upgrade the suite in conjunction with a hardware update—for example, BIOS, firmware, and driver updates are typically dependent on the latest Dell OpenManage version. If the updates are applied and do not correlate with the Dell OpenManage version, the suite may not operate correctly.

Once the SMS 2003 ITDU software has been installed in the site, the SMS console can indicate whether a server is running the required minimum version of Dell OpenManage (4.2 or later). Administrators also have several other ways to assess the Server Administrator and Array Manager components of Dell OpenManage 4.2 or later. First, they can create a query to collect the version information using the SMS hardware class Add/Remove Programs (assuming the application has published its information into Add/Remove Programs, which by default it does not do). Second, they can modify the `Sms_def.mof` file<sup>3</sup> and create a new hardware inventory class based on a registry provider for Server Administrator and Array Manager. Finally, they can use the SMS software inventory feature to capture the file versions.

### Establishing a baseline for Dell server hardware

Establishing a baseline for each Dell server model is an important step prior to deploying a hardware update. With the help of the SMS 2003 ITDU, administrators can establish a baseline for Dell servers to a particular system update version, which helps simplify the update process by reducing what needs to be tracked and deployed. The specific update version depends on the environment's current needs, which can include the need to improve performance, increase server stability, or resolve known problems.

Prior to establishing a baseline, administrators should understand the current Dell support model for hardware update versions, which requires that an update be no more than six versions older than the most current update.

The steps to begin establishing a baseline are as follows:

1. Install the SMS 2003 ITDU software tools on the primary site.
2. Create an SMS 2003 collection organized by "All Dell Servers," then create subcollections by each model or hardware component. Optionally, administrators can also customize the newly created SMS collections.
3. Configure and deploy the SMS 2003 ITDU program and advertisement to occur on a schedule according to the organization's needs.
4. Verify the health of the Scan component package installation process using SMS reports and the SMS Advertisement Status Message Viewer. For more information about recommended reports for each patch management phase, see the second part of this article at [www.dell.com/downloads/global/power/ps3q06-20060249-Microsoft-SOE.pdf](http://www.dell.com/downloads/global/power/ps3q06-20060249-Microsoft-SOE.pdf).

To determine the existing servers in an environment, administrators can use SMS 2003 SP1 to run a discovery method, such as Active Directory System Discovery, and organize the results. After the hardware inventory runs, the results are propagated back to the SMS site database, and the Extended Software Updates hardware class is populated with a list of all Dell hardware updates that are both installed and applicable for each Dell server. The Scan Package Version hardware class indicates the name of the PDK scan package (Dell component update) and the last time the package was updated.

When establishing a baseline, administrators should also consider the following:

- **Monitoring failed deployments:** Administrators can use the SMS "Software update health" report to track failed SMS 2003 ITDU deployments across the update life cycle. The report provides a list of failures for catalog synchronization, scanning, and the patch installation agent.
- **Updating PDK files:** The PDK files used by the Scan component must always be the latest version because they are used to scan the server for hardware updates that appear in the `Catalog.cab` Dell Version Control Catalog file. If the latest PDK files are not available when the scan takes place, the server may not report applicable updates.

After establishing a baseline, administrators should determine which servers fall below the compliance level for particular server models. This level depends primarily on the conditions necessitating the hardware update. Administrators can use the powerful built-in SMS 2003 compliance reporting functions for Dell system updates to view which servers meet or fail the compliance level for the Dell system update along with the associated component updates (see Figure 2). *Note:* If a component update version is not present on a Dell server, it will not meet the particular system update version compliance level and thus will not be considered in compliance.

<sup>3</sup>For more information about modifying this file, visit [www.microsoft.com/downloads/details.aspx?FamilyID=8dfa57f6-291d-4ece-8b07-50bb3ebee2ab](http://www.microsoft.com/downloads/details.aspx?FamilyID=8dfa57f6-291d-4ece-8b07-50bb3ebee2ab).

Dell-UpdateID	Dell-ProductID	Title	Product Name	Information	Applicable	Installed
DELL-R84979	DELL-3-14A	System Bundle (Windows) PE1750 v13	PowerEdge 1750	http://support.dell.com	0	1
DELL-R84981	DELL-3-14A	System Bundle (Windows) PE1750 v14	PowerEdge 1750	http://support.dell.com	0	1
DELL-R87523	DELL-3-14A	System Bundle (Windows) PE1750 v18	PowerEdge 1750	http://support.dell.com	1	0
DELL-R84983	DELL-3-14A	System Bundle (Windows) PE1750 v19	PowerEdge 1750	http://support.dell.com	1	0

Figure 2. SMS 2003 compliance report for Dell system updates showing available update packages for a specific Dell server model

## Identify phase

The Identify phase begins when a hardware update is released. Administrators may want to update Dell servers for a number of reasons, including the following:

- Correcting a security concern
- Correcting a system problem based on a Dell Support recommendation
- Updating a hardware driver or firmware component to a minimum level required by an application, such as Server Administrator
- Gaining access to a new feature or improved performance in a hardware component, such as a RAID controller
- Updating all hardware components (such as BIOS, ESM, or PERC drivers or firmware) for a particular server model as part of periodic maintenance

Activities carried out during the Identify phase include identifying patch types, assigning update severity levels, discovering update sources, identifying relevant updates, and obtaining and verifying updates.

## Identifying patch types

The SMS 2003 ITDU introduces different terminology for the tool's critical components: Dell component updates, Dell system updates, Bundle Applicator, and Dell Update Packages.

**Dell component updates.** A Dell component update is a single hardware update, such as a BIOS, firmware, or driver update, packaged in the update package format with standardized command-line and graphical user interfaces for installation. Administrators can select component updates when running the Distribute Software Updates Wizard (DSUW), as shown in Figure 3.

Administrators should keep in mind that when they have more than one component update configured in a single package, they cannot control the installation order. Best practices recommend deploying only one component update version in a package at a time, which helps provide consistency in deployments.

**Dell system updates.** A Dell system update is a collection of Dell component updates configured in a single SMS package that has been tested by Dell to bring a specific Dell server model to a known and supported state. All component updates are automatically configured appropriately for deployment.

For example, a system update for a Dell PowerEdge 2600 server might include five PERC component updates and one BIOS component update. Even though the system update includes multiple PERC component updates, only the relevant and required component updates are installed on a server (for example, if a server has a PERC 4, Dual Channel integrated, only that PERC component update is installed). This automatic configuration is a key feature of SMS 2003, because it helps eliminate guesswork and associated operational complexity—administrators do not need to target patches to the appropriate servers.

*Note:* When configuring a system update in an SMS package, administrators cannot choose the component updates to include in the system update. If certain component updates cannot be deployed to a particular environment, the recommended procedure is to deploy a single component update in an SMS package.

**Bundle Applicator.** Bundle Applicator (BundleApp.exe) is a subcomponent of the PDK that installs Dell system updates. Using the Catalog.xml Dell Version Control Catalog to obtain the list of included component updates in a system update, Bundle Applicator applies all required component updates in a logical sequence.

Occasionally, a component update included in a system update may require a reboot before the next component update is installed—for example, a BIOS update may require an immediate restart. In this case, Bundle Applicator applies all component updates up to and including the component update that requires the reboot, after which SMS initiates the reboot. After the reboot, the SMS software

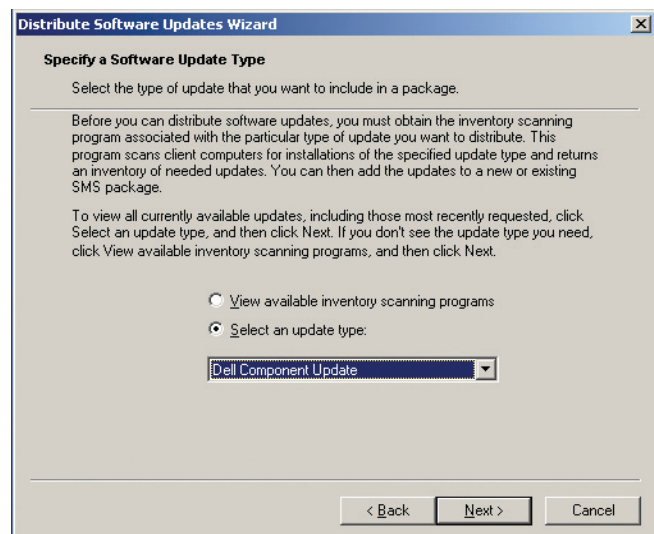


Figure 3. Dell Component Update selection in the Distribute Software Updates Wizard

update management feature reruns the advertisement that initiated the system update. This advertisement restarts Bundle Applicator, and Bundle Applicator applies the next component update.

**Dell Update Packages.** A Dell Update Package is an intelligent installer technology for any updatable element on a Dell server, such as the BIOS, a device driver, or a peripheral's firmware, that can be wrapped. All component updates use this installer technology as well.

*Note:* Administrators should not normally change the default settings in the DSUW, because these settings have been tested in a supported configuration by both Dell and Microsoft.

The standard Dell Update Package provides several benefits for administrators. First, it allows for a consistent method to update any Dell server system software component in the supported matrix. The package also verifies all prerequisites before the update is applied. In addition, administrators do not need to create additional media, such as a floppy disk, just to perform the update. Administrators can apply an update even if Dell OpenManage software has not been installed, and they can deploy packages remotely using SMS software distribution. Furthermore, administrators can perform an update without shutting down the system (although reboots are still required for some, such as BIOS updates).

### Assigning update severity levels

Dell assigns hardware updates a severity value between 1 and 3. Level 3 severity denotes *optional* updates that contain changes affecting only certain configurations (for example, an update to Server Administrator). Level 2 severity denotes *urgent* updates that can help improve system reliability or availability (for example, a BIOS update that adds functionality or resolves a noncritical issue). Level 1 severity denotes *recommended* updates that can help keep system software current and compatible with other system modules such as firmware, BIOS, drivers, and software (for example, a BIOS update that resolves a bug that could result in loss of data, or an update to Server Administrator that addresses a security vulnerability).

### Discovering update sources

Dell hardware updates are typically released quarterly. Updates can be discovered through the Dell File Watch e-mail notification service, SMS 2003 Dell update reports, SMS 2003 ITDU Scan component, or SMS 2003 ITDU Synchronization Host component.

**Dell File Watch e-mail notification service.** To help stay current on hardware updates, administrators can subscribe to the Dell File Watch e-mail notification service (available at [support.dell.com/support/notifications/filewatch.aspx](http://support.dell.com/support/notifications/filewatch.aspx)). After registering, administrators receive e-mail notifications when Dell releases hardware updates.

**SMS 2003 Dell update reports.** Many SMS reports can be used to determine applicable Dell hardware updates. For example, administrators can run a report to identify all Dell PowerEdge 6450 servers that fall below the recommended Dell system update baseline.

**SMS 2003 ITDU Scan component.** The Scan component (ITDUScan.exe) performs ongoing automated scans of servers for installed and missing Dell system and component updates. The Scan component runs Inventory Collector (Invcol.exe) first to extend the WMI class, which then populates the Win32\_Extended\_Patch\_State WMI class with all installed and applicable hardware updates using the Catalog.xml Dell Version Control Catalog. The Dell Version Control Catalog is an important PDK component that identifies applicable and installed updates. An update for a network interface card driver, for example, would not be reported because this hardware component is currently not supported by the Dell Version Control Catalog (Dell anticipates that the content and coverage of this catalog will improve with each release).

The Scan component uses the configuration settings in such files as Scan.ini and Scanconfig.xml to scan Catalog.xml and either hold the hardware update status in WMI for a period of time set by the SMS hardware inventory site or expedite the results to the SMS site server after the scan has completed. Because updates do not report back to the SMS site database until the next SMS site hardware inventory has run, the Scan component package provides an additional program to run with the expedited switch to start the hardware inventory cycle immediately after the scan has completed. In a large SMS environment, administrators must test and carefully evaluate the impact of running a hardware inventory before selecting the expedited program, because it can cause performance degradation on the SMS site server.

The Dell Scan component is downloaded to the `X:\windows\system32\vpccache\PackageID` directory (where *X* represents the drive where the SMS 2003 ITDU was originally installed and *PackageID* is the package ID) on all Dell servers targeted to receive the SMS 2003 ITDU advertisement.

**SMS 2003 ITDU Synchronization Host component.** The Synchronization Host component (ITDUSync.exe) periodically downloads the PDK component files from the Dell Web site on a schedule set by the administrator. These PDK files are then sent to the SMS distribution points and used by Dell servers to conduct scans of missing and applicable updates.

Administrators should keep two considerations in mind regarding how the synchronization host obtains its updates and the importance the synchronization host plays in the hardware update life cycle. First, after the setup process completes, the synchronization host advertisement triggers the Synchronization Host component to run on a computer specified during the setup process. The Synchronization Host component obtains the Internet location or the path of a network shared folder from the ITDUDownload.ini file. If, after setup, administrators have changed the original method of obtaining updates, they must edit each of the Source fields in the ITDUDownload.ini file.

If administrators have full Web access from the site server, then downloading the latest PDK files by using the synchronization host should not be a problem. However, if they have decided to run the synchronization host on a system isolated from the production servers, either in a separate domain or behind a demilitarized zone, they must make additional configurations explained in the SMS 2003 ITDU administrator's guide.<sup>4</sup>

The second consideration is that, if the synchronization host fails for a reason that is not detected before a new hardware update scan is conducted, the latest PDK components may not be used by the Dell servers to conduct scans of installed and applicable updates, which can result in misleading and incorrect data being sent to the SMS site database. Regularly monitoring the synchronization host status is critical, particularly after the release of a new Dell Version Control Catalog. By examining the ITDUSync.log on the SMS site server or running an SMS report such as "Software update health," administrators can stay current on the synchronization host's health.

**Update life cycle.** Dell typically updates the PDK files quarterly, with the possibility of mid-quarter releases for updates to existing releases and hot fixes. Administrators should run the synchronization host daily to catch any updates or hot fixes relating to the SMS 2003 ITDU released before the new quarter begins. Anything that changes on the Dell update Web site is also typically changed in the Dell Version Control Catalog—that is, if the release ID is updated, the Catalog.xml Dell Version Control Catalog is also updated.

**Dell update Web site.** Once administrators are notified of a hardware update, they may need to visit the support.dell.com Web site to obtain more information about what the update fixes, enhances, or stabilizes. At this site, they should use the Advanced Search option so that all drivers appear for the Dell server they wish to update.

Every Dell release includes a release title explaining the Dell server model affected, a release date indicating when the update was officially released for use in a production environment, and a category naming the particular hardware component applicable for the update. Dell also provides a criticality rating for the update along with the included fixes or enhancements.

### Identifying relevant updates

Identifying relevant hardware updates means screening out those that do not apply to the server models in a particular environment or addressing the issues identified in those that do apply. For example, suppose an environment includes a Dell PowerEdge 2550 server running Microsoft Exchange Server that has experienced slow disk I/O for


the past two months. Although this slow I/O has not affected SLAs, it has caused concern because the server has fallen below the past year's baseline. After the Scan component has run on the Dell servers, the tool identifies an applicable RAID controller driver designed to fix a known issue similar to the performance degradation being experienced. After reviewing the information through the DSUW, the administrator determines that the update is indeed relevant for this environment.

After using the Scan component to identify updates, administrators can use the Software Updates node in the SMS Administrator console to determine whether the updates are requested by a Dell server, which is an effective way to identify relevant updates.

### Obtaining and verifying updates

Administrators have several ways to obtain Dell Update Package and PDK files. This topic is discussed in more detail in the SMS 2003 ITDU administrator's guide, which is included in the software installer download.

### Integrated update management

The four-stage patch management process described in this article helps administrators assess, identify, evaluate and plan, and deploy updates in IT environments. To continue reading about the remaining two phases of the process—the Evaluate and Plan phase and the Deploy phase—see Part 2 of this article at [www.dell.com/downloads/global/power/ps3q06-20060249-Microsoft-SOE.pdf](http://www.dell.com/downloads/global/power/ps3q06-20060249-Microsoft-SOE.pdf). Using this process with the Systems Management Server 2003 Inventory Tool for Dell Update provides a powerful way for administrators to integrate both software and hardware updates into a simplified process that can help keep servers running reliably and efficiently. 

*Edited with permission from Microsoft Corporation. Copyright © 2005 Microsoft Corporation. All rights reserved.*

#### FOR MORE INFORMATION

"Applying Updates for Dell PowerEdge Servers Using Microsoft Systems Management Server 2003: Part 2." *Dell Power Solutions*, August 2006. [www.dell.com/downloads/global/power/ps3q06-20060249-Microsoft-SOE.pdf](http://www.dell.com/downloads/global/power/ps3q06-20060249-Microsoft-SOE.pdf)

#### SMS 2003 Inventory Tool for Dell Update Version 3 installer download:

[www.microsoft.com/smsserver/downloads/2003/tools/dellupdates.msp](http://www.microsoft.com/smsserver/downloads/2003/tools/dellupdates.msp)

<sup>4</sup> Administrators should also review the "Task 4: Deploy the Software Update Inventory Tools" section in the *Systems Management Server 2003 Operations Guide* (available at [www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops\\_bv3p.msp](http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_bv3p.msp)), which provides additional guidance on configuring the synchronization host in an unattended mode with an account that has pass-through authentication through the firewall.