Microsoft® Systems Management Server 2003

Scalable Management for Windows®-based Systems

Reviewer's Guide

Microsoft Corp.
October 2003

Abstract

Designed especially for technology reviewers, this guide offers a number of evaluation materials for the latest version of Microsoft® Systems Management Server 2003. The content describes the goals of the Systems Management Server 2003 product and the new features and architecture that meet those goals. The document concludes with detailed step-by-step instructions for evaluating the key features of Systems Management Server 2003.

Contents

Introduction

For many years, IT administrators have been successfully using Microsoft® Systems Management Server to manage Windows®-based desktops and servers within their organizations. As the number of Windows PCs deployed within these organizations has grown dramatically, Systems Management Server has helped IT administrators contain the cost of managing such heavily distributed systems, keeping the overall cost of ownership low while allowing the number of deployed PCs and applications to grow.

However, the environment in which Windows-based PCs are deployed is constantly changing as new technologies are adopted and as PCs are used in increasingly complex configurations. The next release of Systems Management Server, Systems Management Server 2003, is designed to track and support these changing trends in PC usage and provide support for emerging usage scenarios and technologies.

The cornerstone features of Systems Management Server — software deployment, inventory tracking and remote troubleshooting — are extended in this release, but in addition, support has been added for the increasing number of mobile users in organizations today. This support simplifies management of Windows-based PCs and users who commonly roam to different physical locations, reducing the IT cost of managing such users and machines and providing seamless one-to-many solutions for desktop, laptop and server users.

With the increased need to maintain the security of all deployed software in an enterprise, Systems Management Server 2003 also adds support for Security Patch Management of deployed Windows systems. This new feature allows administrators to easily monitor the patch state of all systems within their enterprise through a set of powerful web reports. These reports are used to identify any vulnerability in the network, at which point the system can then be used to download and deploy the latest patches from www.microsoft.com to those machines which require them.

Since many organizations are deploying Windows 2000 Server's Active Directory® service within their networks, Systems Management Server 2003 is able to take advantage of this technology, further simplifying the process of managing clients and users. Many Active Directory features map directly to Systems Management Server targeting concepts, allowing IT administrators to target software and inventory tasks using Active Directory constructs and containers.

This guide starts with an overview of the management solutions provided by Microsoft Corp. today, before introducing the new solutions provided by Systems Management Server 2003. The document then enumerates the new features of Systems Management Server 2003 that enable these solutions. After a brief review of the architecture of Systems Management Server 2003, the guide offers a series of step-by-step procedures to walk through the operation of the new product features.

Microsoft and Management

Microsoft is committed to delivering a combination of technologies and products to make Windows-based systems the most manageable environment available. The complete management solution for Windows is based on a combination of the management services and technologies built into the Windows operating system as well as stand-alone management products available from Microsoft. In addition to these technologies and products, Microsoft has also developed a set of operational procedures, or best practices, outlined in the Microsoft Operations Framework.

Products such as Systems Management Server 2003, Microsoft Operations Manager 2000 and Microsoft Application Center 2000 are designed from the ground up to work with the Windows operating system and provide solutions to the IT administrators tasked with managing large numbers of desktops and servers deployed by their organizations today.

The management technologies built into the Windows operating system, such as Windows Management Instrumentation, Windows Installer, Active Directory and Windows Update, enable these management products to offer exceptionally powerful solutions, but with greatly simplified and therefore more reliable implementations.

Two of the most common categories of systems management that enterprises rely upon today are change and configuration management and operations management. Change and configuration management involves the installation and configuration of computer software and hardware throughout the life cycle of the computer systems involved. Operations management provides the real-time event and performance monitoring of servers and their applications, enabling administrators to maximize the uptime of services and minimize the impact of downtime on end users and business operations. These two disciplines provide complementary management services: operations management alerts managers to the need for change and configuration management.

Microsoft offers solutions in both of these areas: Systems Management Server for change and configuration management, and Microsoft Operations Manager for operations management. Application Center 2000 embraces both change and configuration tasks, as well as operations management functions, specifically in the role of managing dense clusters of Web-based content servers.

The remainder of this guide examines the new solutions offered by Systems Management Server 2003 to address the change and configuration needs of the Windows-based enterprise.

What's New in Systems Management Server 2003

The new features added in Systems Management Server 2003 provide solutions for a number of key issues faced by IT administrators managing Windows-based PC environments today. The release addresses the following key problem areas:

- How to manage computers and users that roam around the network, often connecting over poor bandwidth links or from different geographic locations on a regular basis
- How to track the deployment and usage of software assets in the organization, and use this to plan licensing and software acquisition across the company
- How to monitor the patch state of all deployed Windows PCs and applications in the enterprise, and to remove vulnerabilities proactively in a closed loop process with real-time patch deployment status
- How to offer managers and users access to the rich management data aggregated by Systems Management Server, including live configuration and operations reports
- How to scale management solutions to the ever-growing population of Windows-based PCs and devices in the environment, which now include more than 200,000 managed end points
- How to manage Windows PCs securely, but with a minimum of administrative overhead, while fending off the seemingly ever-increasing number of external security threats

These specific problems are directly addressed by features in the Systems Management Server 2003 release, as described below.

Better management of mobile systems and users

Research by industry analysts and others has shown a significant increase in the number of laptops being deployed within organizations in recent years. This deployment reflects an increase in the mobility of the workforce, many members of which are no longer tied to a specific physical location or office in today's dynamic work environment.

Providing management solutions to such a mobile workforce is one of the most complex and demanding problems within the systems management space. To provide management services to mobile users and machines in a way that is consistent with traditional static users adds a new level of complexity for the IT administrator.

The Systems Management Server 2003 product specifically addresses this problem by adding a completely new client agent, the Advanced Client, designed from the ground up to support these scenarios. This new client agent supports the full management feature set — software distribution, asset management and remote troubleshooting — without requiring a fixed set of local servers or services. Furthermore, such agents integrate seamlessly within the existing Systems Management Server framework, allowing administrators to manage roaming users alongside static users without needing to differentiate between them.

The new Advanced Client also uses a Windows technology called Background Intelligent Transfer Services (BITS) to provide connectivity for all management operations over intermittent, low-bandwidth or poor-quality network links, such as Remote Access Service dialup and remote Virtual

Private Network. This HTTP-based protocol was developed to support the Windows Update infrastructure, and the code base currently handles more than 60 million update downloads a month from http://windowsupdate.microsoft.com/.

To ease migration for existing Systems Management Server 2.0 users, a Legacy Client is also provided in Systems Management Server 2003. The Legacy Client supports all client platforms from Windows 98 upwards, and is a direct upgrade of the client used in Systems Management Server 2.0. The Legacy and Advanced clients offer the same features and services to an administrator, though their behavior and implementation differ. Users upgrading from Systems Management Server 2.0 will likely follow an upgrade path initially to the Legacy Client before then moving all managed clients to the Advanced Client (operating system permitting).

Better management of software assets

As the range of products and services deployed in most organizations increases year by year, it is becoming increasingly important for IT administrators to manage the full life cycle of all such applications. The simplest but most direct financial savings can often be made by tracking true software usage against current license levels, ensuring that annual license costs are in step with usage. By monitoring not only what applications are installed on each machine but which are actively used, administrators can build a much more accurate picture of license needs within the organization. In addition, by understanding which applications are broadly used, test scenarios and upgrade projects can more accurately reflect the true deployment environment, reducing the cost of making changes across the enterprise.

Systems Management Server 2003 provides solutions in this space by allowing administrators to track application installations, and to correlate this with actual application usage. Systems Management Server 2003 achieves this with a complete rewrite of the previous Systems Management Server 2.0 software metering that improves scale dramatically for the largest of organizations and focuses on the key need for understanding what applications are being used, how often, and how many users are using the same applications concurrently. Administrators can then better measure the actual application licenses required for their enterprise, and can also identify redundant application installations, removing their disk footprint from client machines.

Significant indirect savings are also possible by maximizing the uptime and availability of deployed applications. Enterprise application stability is best maintained by ensuring that all deployed applications and services are running the most recent updates and service releases available. By constantly tracking deployed applications and services in the network and providing tools to compare these with a list of available patches, service packs and upgrades, Systems Management Server allows administrators to circumvent outages by proactively replacing deployed code with known issues.

Such actions increase overall productivity by minimizing downtime for users and customers alike, and also keep the entire business environment secure by ensuring that all known weaknesses are eradicated as soon as patches are available.

Better management of software security patch status

Corporations today need tools and processes that allow them to determine which Windows systems and applications on their network are in need of critical patches, and then quickly test and deploy

these patches throughout the enterprise. The consequences of failing to implement a comprehensive patch management strategy can be severe, directly impacting the bottom line of the company or organization. Systems Management Server provides an enterprise proven solution for managing patch deployment, allowing enterprises to proactively maintain the integrity of their Windows environment. The solution is applied in two phases – Vulnerability Assessment and Streamlined Patch Deployment – which together provide the control which administrators need to effectively and reliably target, test, deploy and track patches across the enterprise.

Systems Management Server 2003 leverages standard Microsoft security tools like the Microsoft Baseline Security Inventory Analyzer and Office Update Inventory tool to inventory systems for applicable patches and vulnerabilities and centrally stores this information which is used to provide comprehensive web reports tracking vulnerabilities and patch deployment, as well as how and when these have been addressed.

Rather than manually creating a software patch deployment, administrators use the Patch Distribution Wizard, which steps them through the whole process. The wizard can also automatically download the latest patches from the Microsoft website using Windows Update technology, reducing operational costs for repackaging and allowing the enterprise to remain current with all the latest patches and hotfixes from Microsoft.

Better access to configuration and deployment data

Systems Management Server maintains a central database containing a wide range of valuable information about the systems and users being managed. With inventory extensions in Systems Management Server 2003 to add application data from Add/Remove Programs as well as application install state from the Windows Installer service, an even richer set of configuration data is maintained at each Systems Management Server site.

Administrators are commonly required to provide reports describing the progress of ongoing deployment and upgrade projects, as well as maintaining reports about the overall network configuration state. The time taken to generate and update such reports takes valuable time away from actually managing the projects themselves. Systems Management Server 2003 now offers a secure Web interface to the management database, including a large number of preconfigured reports covering the configuration of all machines on the network, the software deployment and usage status, and details of individual machine configurations. This new Web interface improves upon the Web-based reporting Systems Management Server administrators came to rely upon in Systems Management Server 2.0, allowing administrators to offer secure live reports to their managers, each of whom can use a Web browser to view the current state of the managed systems in their organization. The set of Web reports is fully extensible, allowing administrators to create custom views for specific ongoing projects.

Better scalability and manageability of Systems Management Server operations

In recent years, the number of Windows-based PCs deployed in a typical organization has increased significantly. As the deployed PC base increases, the importance of providing centralized management of the platform becomes increasingly critical. The number of clients being managed by

typical Systems Management Server deployments therefore has also been increasing, with many customers now managing well over 200,000 client machines.

The Systems Management Server product architecture is inherently scalable and has been successfully deployed in many such environments. However, as the number of end nodes grows and the amount of data being processed increases, two factors become critical:

- System processing load increases, increasing the delay between configuration change and administrator notification

The deployed management infrastructure increases in size, requiring more administrative effort to manage the management system itself

Systems Management Server 2003 addresses both of these issues, by increasing the throughput of the Systems Management Server infrastructure and by simplifying the administrative model. The performance of core Systems Management Server services has been improved significantly to ensure that high client data throughput can be supported with minimal transit delay through the system. For smaller or static environments, this improvement results in lower hardware requirements for the same level of system functionality.

The administrative experience for Systems Management Server administrators has been simplified by removing high-overhead operations and services, and also by implementing a new optional security model that allows a Systems Management Server to be operated with few, or no, Windows domain accounts. These two new features dramatically simplify the role of all Systems Management Server administrators, while also providing an inherently more secure Systems Management Server environment.

Systems Management Server 2003 Features at a Glance

Feature	New	Description
Mobile support and bandwidth management		
Bandwidth-aware clients	●	The new Advanced Client uses the Background Intelligent Transfer Service (BITS) technology to automatically detect the capacity of the client network connection and adjust transfer rates efficiently. The download rate is dynamically tuned to drop Systems Management Server traffic into the background as other services start using the shared link. This is supported on Microsoft Windows 2000 and Windows XP-based clients only. Software can now be distributed to machines over slow connections without interrupting core user business functions.
Checkpoint/ restart	●	Upon reconnection, any partial downloads to clients will continue where they left off; there is no need to restart transmissions because of a disconnected session. Checkpoint/restart works at a byte level, requiring only the download of those bytes in a package that haven't already been transferred. This feature is particularly useful to dial-up users on slow connections, but also works well on a local area network (LAN).
Download and execute	●	After a new software package has been successfully downloaded to a client, it remains in cache on the client system until the prescheduled install time, at which time it is executed. Administrators also may elect to have clients execute packages directly from a Systems Management Server 2003 distribution point.
Flexible site boundaries	●	Mobile users may be connected on high-speed, stable networks, but from a variety of geographic locations. As these users roam around the enterprise, flexible site boundaries ensure that they always receive software packages and updates from the nearest appropriate installation source, and are not required to install software across the enterprise WAN.
Software distribution		
Rich distribution targeting		Software distribution and other management tasks can be finely targeted to machines and users using a wide variety of properties including network and hardware configuration, Active Directory organizational unit, or group membership and software installation status. Software can be deployed based on business organization, not just the properties of the network infrastructure.
Dynamic distribution targeting		If a new user joins a user group, software is automatically sent to the user according to predefined administrative settings for that group. Likewise, new computers that match predefined targeting policies (such as IP subnet, Active Directory organizational unit or installed video card) automatically receive specified packages or driver updates. When a new computer or user is added to an organization, it can automatically receive the software it requires without any administrative intervention.

Feature	New	Description
Delta distribution between site servers and distribution points	●	When alterations are made to previously deployed software package sources, only the source changes are propagated between Systems Management Server 2003 site servers and distribution points, rather than the entire application image. Only the specific files that are new or changed are transferred, minimizing the impact that Systems Management Server 2003 has on expensive network bandwidth.
Courier Sender		Courier Sender allows software to be sent between Systems Management Server sites by CD-ROM or other media, rather than across the network. This is particularly useful in situations where the available network bandwidth is low or too expensive to use for the delivery of large packages.
Software program removal		In addition to distributing software to systems, Systems Management Server can be used to remove deployed software. Administrators can issue instructions to remove applications from particular computers, users or groups.
Security Patch Management		
Scanning of security patch state	●	Systems Management Server 2003 leverages the Microsoft Baseline Security Inventory Analyzer and Office Update Inventory tool to scan all managed systems for missing security patches. The results of these individual scans are then rolled up into the central database for reporting and targeting purposes. As missing patches are deployed, this data may be optionally updated in real time.
Patch web reports	●	Powerful web reports allow administrators to view the vulnerability of the networked systems and the progress of patch deployments from any web browser. Drill-through to underlying system details and links to specific patch documentation provide all data needed to plan patch remediation steps.
Patch deployment wizard	●	A simple console wizard is provided to assist administrators in deploying required patches to managed devices. The wizard handles all aspects of the process specific to Systems Management Server, allowing operators to focus on the security patch download, installation and policy. This allows its use by security administrators, who may be unfamiliar with Systems Management Server.
Patch installation agent	●	An intelligent patch installation agent is used at each targeted system to manage the entire patch installation process, handling the chaining of multiple patches, handling of any required re-boot and any required interaction with end users.
Security		
Advanced Security Mode	●	Built-in computer and local system accounts can be used for all server functions (such as database access), dramatically simplifying the management of accounts and passwords within Systems Management Server and making the enterprise more secure by not creating extra high-rights accounts.
Security delegation		Administrators can be assigned specific privileges, granting access to a subset of the Systems Management Server feature set. This allows different IT operators to handle different aspects of system support, such as help desk and package creation, without granting everyone full rights to the Systems Management Server system.

Feature	New	Description
Inventory		
WMI-based hardware inventory		Systems Management Server 2003 has been designed to use WMI, which is built into the Windows operating system, to collect inventory data. Because WMI is based on the Common Information Model standard, Systems Management Server 2003 has access to data from many sources, including the Win32® API, the Simple Network Management Protocol (SNMP) and the Desktop Management Interface (DMI), providing administrators with a rich collection of inventory and configuration data.
Discovery-based software inventory		Every configured file type is searched for version and developer information rather than relying on unreliable file-to-product mapping databases. This provides a dynamic, efficient mechanism for gathering global software inventory data.
Support for WMI 1.5 and later	●	Enhancements to Windows Management Instrumentation (WMI) are included in version 1.5 of that technology, which is installed and used by Systems Management Server 2003. These enhancements allow improved client-side performance during inventory scans and a richer set of inventory data, including BIOS and chassis enclosure data.
Granular file inventory search options	●	Now IT administrators can configure Systems Management Server 2003 to get all of the asset discovery they need, but *only* what they need. This is done with wild cards, environment variables and file properties that can now be used to scope software inventory searches more effectively (such as “search for *.exe or *.dll files under the %Program Files% folder root”). Other options allow for compressed and encrypted files to be skipped, reducing the client CPU load during scans.
Add/Remove Programs support	●	Installed software that is registered in Add/Remove Programs is now inventoried and reported as part of normal inventory scans. Administrators can now reconcile the files on their systems with the way the vendor describes the application upon installation for more accurate asset tracking of software.
Active Directory Integration		
Active Directory discovery	●	Systems Management Server 2003 can automatically discover the Active Directory properties of both users and systems, including organizational unit container and group level membership. Software packages can then be targeted based on these Active Directory attributes. This directory-enabled management allows enterprises with an investment in Active Directory to use Systems Management Server 2003 to manage their enterprise according to how their business is organized and therefore provide greater service to their users. **NOTE:** While Systems Management Server 2003 can use Active Directory where it is available, it does not require it. Organizations that have not yet deployed Active Directory can still benefit from Systems Management Server 2003.

Feature	New	Description
Active Directory-based site boundaries	●	Site boundaries can now be based on Active Directory site names, rather than simply on IP subnets. Active Directory-based site boundaries allow real IP subnets to be logically split or combined (sub-netted or super-netted). In enterprises with an investment in Active Directory, this dramatically simplifies the enterprise infrastructure and operational costs.
Software packaging		
Creating packages using the Windows Installer Service	●	The new Systems Management Server Installer packaging tool enables administrators to convert existing Systems Management Server Installer executables into Windows Installer-compatible packages. It also allows administrators to create brand-new packages in Windows Installer format. Generating packages in Windows Installer format allows administrators to take advantage of the self-repair, just-in-time install and enhanced software deployment tracking abilities of the Windows Installer technology.
Creating packages from Windows Installer files	●	Systems Management Server 2003 can automatically generate packages for distribution from any standard Windows Installer file. Windows Installer configuration files contain all the information needed to generate a Systems Management Server package, which in turn can support self-repair and just-in-time installation.
Add/Remove Programs Wizard integration	●	Applications advertised by Systems Management Server can be published in the Windows 2000 and Windows XP Add/Remove Programs Control Panel applet. Now users have a single place to go to understand all software they can install on their system.
Elevated rights Windows Installer applications	●	Because Systems Management Server 2003 supports the Windows Installer service, it is able to switch user account contexts during a package installation. This enables installation of software packages that require administrative access during some parts of the installation and user access during user-specific portions of the installation (such as short-cut creation). This allows user accounts to be “locked down” to the minimum rights required to do their daily business tasks, dramatically reducing the cost of ownership associated with managing Windows computers.
No logon points	●	Systems Management Server services and files no longer need to reside on domain controllers. Instead, computers can be manually assigned to Systems Management Server sites or targeted via Active Directory. Systems Management Servers may also be used to automatically discover and assign computers to sites. This reduces the overall infrastructure, making the return on investment that much quicker with Systems Management Server 2003.
Reporting		
Web-enabled reporting service	●	A comprehensive set of Systems Management Server 2003 reports can be viewed using Internet Explorer. More than 120 pre-built reports are included, covering hardware and software inventory as well as computer status and software deployment progress. The Web reporting function is also fully extensible, allowing administrators to easily generate their own custom reports.

Feature	New	Description
Software Metering		
Usage monitoring	●	Summary and detail reports can be generated describing which applications were used by which users, for how long and on which managed systems. Usage can be tracked by user or computer, and reports created comparing concurrent usage data to current license ownership (compliance reports). This is useful for reconciling purchased software with used software for smarter purchasing decisions in the future, as well as prioritizing testing of new applications or operating systems so only the most frequently used applications are tested.
Terminal Server monitoring	●	The new Systems Management Server 2003software metering implementation also monitors application usage across Windows Terminal Services sessions. Now administrators will know who is running Terminal Server applications, when and for how long.
Scalable	●	The new software metering service can scale to large client deployments, supporting very large sites with thousands of client systems. For greater efficiency, WMI is used to monitor running applications.
Offline metering	●	Software usage is tracked even when computers are disconnected from the corporate network. Usage reports are collected each time a client synchronizes with the network, or on a configurable schedule. This feature is particularly useful for mobile users who are not always connected to the corporate network.
Troubleshooting		
Windows XP Remote Assistance support	●	The high-performance Windows XP Remote Assistance feature is now an option for remotely troubleshooting clients directly from the Systems Management Server Administrator Console when a user is present at the remote machine. By integrating with the manageability features already in Windows XP, customers get a better managed desktop at a reduced cost.
Online Help and improved documentation	●	Electronic help files and documentation are now built into the Systems Management Server 2003 Administrative console. The articles include links to the Microsoft Web site, ensuring the information presented is as up-to-date as possible.
Built-in backup	●	A complete Systems Management Server backup and recovery system is included with every Systems Management Server 2003 site installation. This automation further ensures that Systems Management Server 2003 customers can rely on Systems Management Server as a mission-critical component of their IT infrastructure.
Network topology tracing tool		A basic graphical display of network systems and devices relating to a specific Systems Management Server site can be automatically generated. This diagram shows routes between the servers used by the Systems Management Server services.

Feature	New	Description
Status tools		The status data provides real-time information about the current state of Systems Management Server processes, both on servers and clients. Various aspects of Systems Management Server system performance can be monitored, including the detailed progress of software package distributions. The status system can also be configured to execute custom commands when specific status messages are detected, allowing paging of operators in the event of critical outage conditions.
Other features		
Large environment support		Systems Management Server 2.0 has already proven itself capable of managing organizations with more than 200,000 managed systems. Systems Management Server 2003 has been tuned and tested to exceed even this level of scalability.
MMC interface		The Systems Management Server 2003 user interface is a Microsoft Management Console snap-in.

Systems Management Server 2003 Feature Review

Systems Management Server 2003 provides centralized change and configuration management for organizations managing Windows-based PC deployments of any size. From one or more centralized administrator consoles, Systems Management Server 2003 can provide support for these functions:

Inventory: asset management and configuration tracking

Provisioning: software and configuration change deployment

Metering: monitoring software usage

Troubleshooting: remote help desk support

Reporting: access to detailed system and service reports

Support is provided without requiring the interaction of end users or the dispatching of IT staff to remote locations. This allows the centralized administration of large numbers of Windows-based PCs with a minimum level of IT staffing.

The following sections describe each of the key features added in Systems Management Server 2003 in detail, describing how they help solve the problems in the scenarios presented earlier.

Inventory

Both software and hardware on all managed computers can be exhaustively inventoried by Systems Management Server. A wide variety of reports can be run against the resulting data, allowing organizations to plan upgrades, track computer and software assets, or check software license compliance.

For example, before deploying a new software package, administrators may want to build a report showing how many of the PCs being targeted have enough memory and disk space to support the application. This allows noncompliant systems to be upgraded before the deployment begins, ensuring a higher overall project success rate.

Extensive use is made of the information offered by Windows Management Instrumentation (WMI), which has been built into the Windows operating system since Windows 98. Systems Management Server 2003 uses the latest version of WMI, version 1.5, to offer the richest set of system data possible including BIOS, motherboard and enclosure data. Administrators can customize which of the more than 700 classes of system data should be recorded during an inventory scan, allowing them to select the appropriate balance between performance and inventory depth for their organization.

Instead of relying on a manual process to map discovered files to known applications, Systems Management Server 2003 scans the resource headers of all executable or binary files to build a complete picture of all software installed on each managed client. Such an approach is inherently scalable, automatically identifying new applications as they ship (instead of waiting for a database of known software to be updated).

New options in Systems Management Server 2003 give administrators more control over which files should be scanned, allowing each organization to balance software inventory scope against client processor load during a scan:

- Wild cards can be used to limit the inventory search to specific files or file roots, minimizing the data retrieved and the impact on the managed device.
- Software inventory can scan specific directories and drives, using environment variables to build the scope across different machines to optimize the data-gathering process.
- Inventory can indicate relevant critical software patches that are required but not yet deployed to specific machines by comparing install state to a critical update database.
- Inventory can report software registered in Add/Remove Programs or installed by the Windows Installer service. This is a good checkpoint against the file-based inventory for accurate descriptions of installed applications, not just the files present on a machine.

The Systems Management Server 2003 inventory engine is also extensible by administrators who wish to expand on the native WMI data set. Scripts or executables can be written to add additional information from the Windows registry, configuration files or application interfaces into an inventory scan. Asset information relating to non-Windows items such as computer leases, scanners, photocopiers, fax machines or human resources data can also be stored as part of the Systems Management Server 2003 inventory data set.

Software distribution

A key strength of the Systems Management Server feature set has always been its rugged but flexible software deployment support for Windows-based desktops, laptops and servers. From a central console, administrators can package, replicate, target, advertise and track software packages as they are deployed to target machines across the network. Packages can be deployed with or without end-user intervention, and without any IT staff visiting the target systems.

Whether it's a new operating system such as Windows XP Professional, an entire application suite such as Microsoft Office, daily line-of-business applications from third-party vendors or written in-house, or a critical Windows system update, Systems Management Server 2003 uses simple interfaces, wizards and tight integration with operating system services to significantly reduce the work required to keep software up to date.

For example, administrators can use Systems Management Server to deploy a new service pack to all the Windows NT-based servers throughout the company. The source files required to install the Service Pack can first be replicated to Systems Management Server sites around the world, possibly using the network WAN links during off-peak hours. The actual installation of the package can then be scheduled to occur during the off hours for each office around the world. Each machine would install the service pack using the nearest copy of the source files on the network, minimizing the resulting network traffic.

The distributed architecture, with local Systems Management Servers at strategic locations and a variety of bandwidth management features, allows software to be easily deployed in extremely large environments without overloading the network, interrupting key business traffic or inconveniencing users. Status reports further assist large deployments by allowing administrators to pinpoint any installation problems as soon as they occur, allowing remedial action to be taken quickly to avert any similar failures.

Packaging

Before software is actually distributed with Systems Management Server, administrators must create logical packages, which contain the files to be deployed, configuration settings for the target systems and any scripted actions to be taken during installation.

Systems Management Server 2003 offers a number of options for packaging applications for deployment. The simplest option is to use applications already packaged using Windows Installer technology. Thousands of third-party software applications already take advantage of Windows Installer technologies and can be used directly by Systems Management Server 2003. In addition, Systems Management Server administrators can modify the Windows Installer definition files either directly or using one of a variety of third-party tools to customize the application installation options.

Some of the key benefits of using Windows Installer packages for deployment are as follows:

- **Self-repairing.** Applications are automatically repaired if installed files are damaged or deleted.
- **Just-in-time installation.** Administrators commonly wish to deliver only the core components of an application initially, with any additional features being faulted into place on first invocation by the user. In this way, the administrator can minimize the initial network impact and minimize the client disk footprint on each target machine.
- **Rollback/restart.** Occasionally an installation can fail before completion, possibly due to some change in the machine state during install. In case of such a failure, the Windows Installer service cleanly reverses all installation steps already completed, undoing the partial install and returning the target system to a known working state.

These features are supported natively by the Windows Installer service. However, when combined with Systems Management Server 2003, Windows Installer capabilities can provide additional installation features, including these:

- **Add/Remove Programs integration.** Advertised software can be registered in Add/Remove Programs, proving a simple, clean interface to users wishing to install optional packages.
- **Elevated rights installations.** Individual applications can be installed using multiple security account contexts during the install. Steps requiring local administrative privileges (such as installing drivers) may be executed with elevated rights, while user-related steps such as creating shortcuts and making profile changes would be executed in the target user security context.
- **Automatic package creation.** Because the Windows Installer format is rich with information about how the software installs, Systems Management Server 2003 can simply import all of that information to create the package logic described above. Now, by simply pointing Systems Management Server 2003 at a Windows Installer file, an administrator can deploy it with Systems Management Server 2003.

If an application is not available in Windows Installer package format, several alternative options exist, including these:

- **Repackage to MSI file.** The Systems Management Server Installer tool may be used to monitor a non-Windows Installer installation on a reference machine and generate a corresponding Windows Installer package that will produce the same end result.

- **Repackage to Systems Management Server Installer file.** A similar procedure to the above can be used, but a native Systems Management Server Installer executable (setup.exe) package can be generated to reproduce the original installation, but with enhanced Systems Management Server status reporting enabled.
- **Build custom installation script.** The Systems Management Server Installer tool may be used to script an installation from scratch using its native scripting support. This option also offers rich Systems Management Server status integration.
- **Use the legacy installation system.** Systems Management Server 2003 can be used to transport the original package to all locations and then launch the required command line (such as “setup.exe /s /u”) on each target machine.

Targeting

A broad range of options are available to select exactly which users or computers should be targeted with a software package in Systems Management Server 2003. Administrators can combine any of the following attributes to build a definition of the machines and users to be targeted:

- Explicit user, machine or group names
- Hardware inventory data
- Software inventory and usage data

For example, Systems Management Server 2003 could be used to distribute a new company spreadsheet template to all members of the finance organization who have Microsoft Excel 2000 or above installed on their computers and sufficient free disk space and memory to support loading the new template.

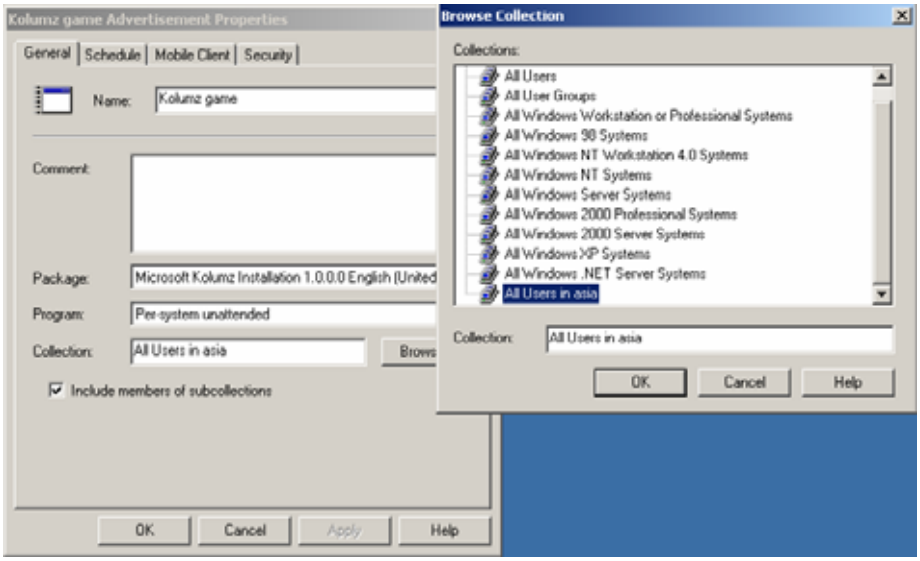


Figure 1. Software distributions targeted at groups

Security Patch Management

Systems Management Server 2003 is designed to allow administrators to quickly and effectively apply and implement critical software updates to the systems they manage. It provides key

capabilities for detecting which computers are missing critical updates, providing network-wide reports of such vulnerabilities and facilitates the deployment of these critical updates.

The Patch Management Process

The process of managing software security patch status can be broken down into three distinct phases: Vulnerability Assessment, Deployment Planning and Patch Deployment. Systems Management Server 2003 provides solutions for all three phases, tightly integrated to form a simple overall solution.

Vulnerability Assessment starts when the administrator, in a one-time event, downloads and installs the Security Update Inventory Tool and the Microsoft Office Inventory Tool from the Microsoft Download Center Web site. These files are also provided on the Systems Management Server 2003 CD. The inventory tool installer programs automatically create the necessary packages, collections, and advertisements to execute the software update scan tools on all managed clients at regular intervals. The installer program also configures Systems Management Server to automatically download any newer versions of these scanners as they become available.

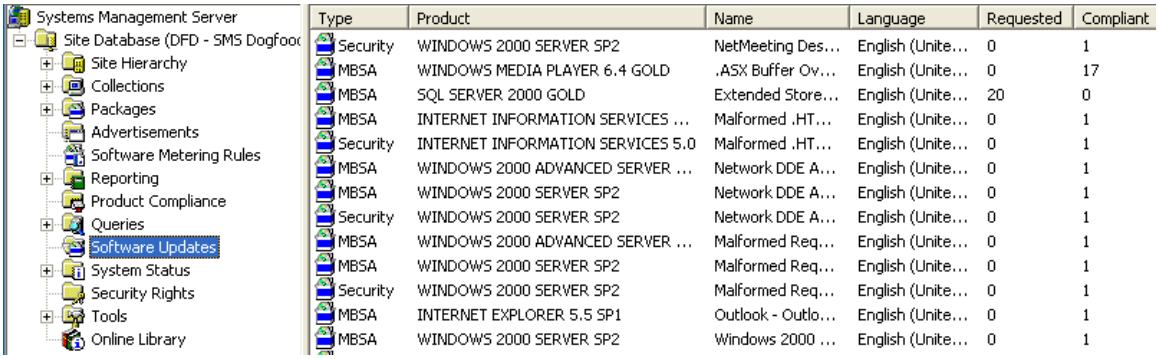
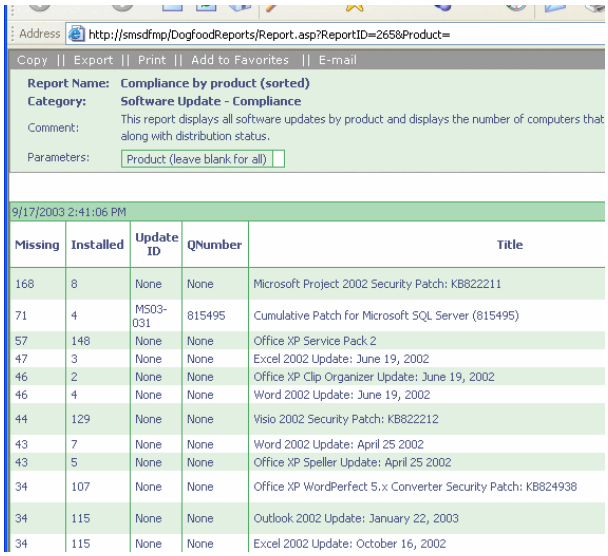


Figure 2. Software update patch compliance of all systems

As the scan tools execute on each client, they analyze the current state of installed and applicable software updates and the results are converted to inventory data which is propagated to the site server. The propagation may be initiated on completion of the scan to provide immediate results, or may be batched up in the next scheduled hardware inventory scan to minimize bandwidth utilization.



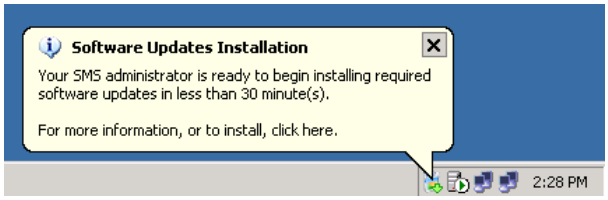
Patch Deployment Planning starts when the administrator reviews the web reports presented by Systems Management Server. These reports allow the administrator to asses the overall vulnerability of the network, and plan which patches are the top priority for distribution, based either on the severity of the patch scenario or the number or type of the vulnerable machines.

Having selected the patch or patches to be

deployed in the next phase, the administrator now starts Patch Deployment phase by launching the Distribute Software Updates Wizard from the administrative console. The Wizard displays summary information based on the software update data collected during the Vulnerability Assessment phase.

The Distribute Software Updates Wizard walks the administrator through the process of downloading the required patch binary files for the planned software updates from the Microsoft Download Center Web site. The wizard also automatically creates or updates the necessary packages, programs, and advertisements for distributing the software updates to all targeted clients. The specifics of Systems Management Server internal operations are not exposed in this wizard, allowing it to be used by non-SMS trained personnel such as Security administrators.

When a patch or set of patches arrives at a managed client for installation, a Software Update Installation Agent is launched on that client to setup the software updates. The agent is supplied with a list of the one or more patches to be installed and it starts by verifying which of the patches are actually required on the local machine. The required patch list is then built into a chain and each patch binary is executed in sequence. The agent minimizes the number of re-boots required, by suppressing individual re-boots and managing any re-boot requirement at the end of the chain.



The Software Update Installation Agent implements administrator set “policy” relating to each patch deployment. A variety of patch installation options can be set by the administrator from within the Distribute Software Updates Wizard. Some examples of the options include: agent behavior when no user is preset, whether or not to “force” system re-boots on workstations or servers and provision of detailed information from the administrator to the end user may be configured. These functions are implemented during installation by the installation agent.

A particular patch installation may be configured to be re-executed on a regular basis, possibly weekly, to ensure that patches are not “lost” when a user winds back their system using System Restore or some other back process. This ensures that not only are the targeted systems secured, but that they remain secure without further action by the administrator.

Active Directory integration

The integration of Active Directory support with Systems Management Server 2003 makes it possible for administrators to target software deployments based on membership of organizational units, user groups, machine groups and even non-security objects such as Microsoft Exchange 2000 distribution lists.

This Active Directory support is accomplished by discovering the directory object memberships for all users and machines attached to the directory and adding these memberships as attributes to the inventory data held in the Systems Management Server 2003 database. Administrators may then build target sets using these Active Directory attributes in the same way that they would use hardware or software inventory attributes.

Administrators can customize the Active Directory discovery process, selecting different schedules and scoping the parts of the Active Directory hierarchy that should be searched. This granularity of control ensures that the overall directory performance is not significantly affected by the process.

Systems Management Server 2003 can also use Active Directory to advertise the location of specific Systems Management Server services and servers to clients around the network. By using Active Directory as a location service, Systems Management Server 2003 simplifies client-side operations and minimizes the network traffic generated during client service discovery.

In addition, Systems Management Server 2003 site boundaries may now be logically mapped to Active Directory site definitions. Since Active directory site definitions allow administrators to use subnet wildcards to define site boundaries, this allows broad ranges of IP addresses to be easily integrated into Systems Management Server site boundary sets.

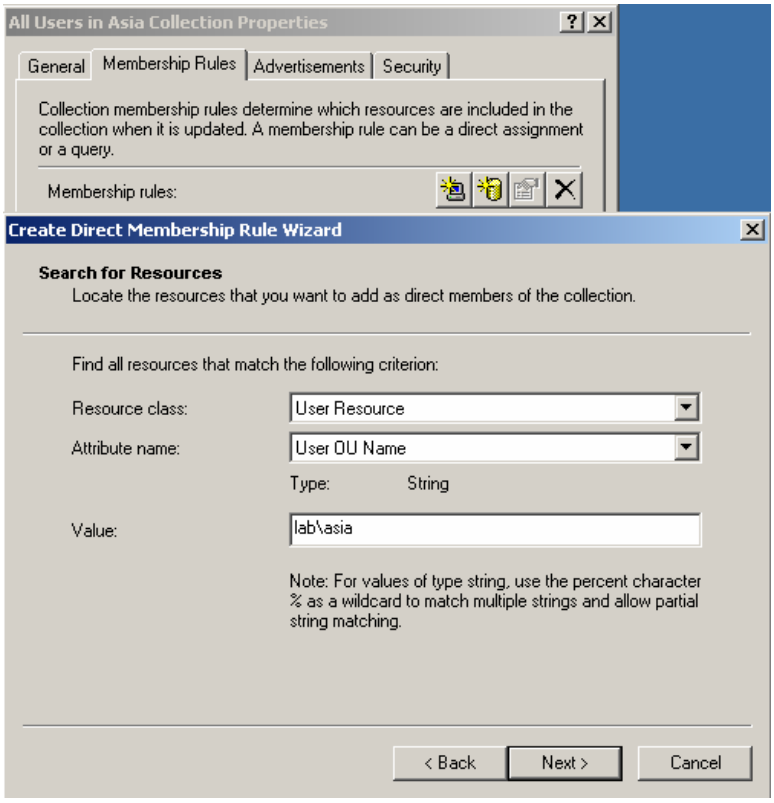


Figure 2. Systems Management Server collections (or groups) can be based on Active Directory organizational units.

Bandwidth management

Bandwidth management options have always been a key feature of previous versions of Systems Management Server. Along with the site-to-site WAN bandwidth features previously supported, users can now take advantage of new network traffic control capabilities between clients and servers. These new bandwidth management capabilities are particularly powerful when used by mobile users connecting over slow dial-up connections, although there is also benefit in fixed LAN environments.

For example, a traveling employee might dial into the corporate network using a 56Kbps dial-up modem and discover that a new update to the corporate sales database is available and must be

downloaded and installed immediately. The new database package may be 10 MB, but during the download the user can continue to use the RAS link for other purposes, such as sending or receiving e-mail or browsing the Web. As each application uses the RAS link, the software download is forced into the background, reducing its bandwidth usage.

If the user terminates the dial-up session before the download is complete, the process is resumed the next time a connection is established with the corporate network. Eventually, the entire database software will be downloaded to the local machine, possibly over multiple dial-up sessions spanning several days. Once the download is complete, Systems Management Server will launch the associated installation command for the sales database software.

Mobile bandwidth management

Advanced Client bandwidth management capabilities are significantly enhanced by the use of the Background Intelligent Transfer Service (BITS), which is built into Windows XP and can be added to Windows 2000-based machines. BITS file transfers are based on the industry-standard HTTP protocol and provide a checkpoint-restartable mechanism to download or upload files between a server and client. The technology is based on the framework used by the Windows Update service, which currently services more than 60 million download requests a month. The key capabilities added to the Systems Management Server 2003 Advanced client by BITS are as follows:

- **Checkpoint/restart.** Interrupted file downloads to clients continue from where they left off once a connection is re-established.
- **Background transfers.** Systems Management Server 2003 client-server traffic is forced into the background of other application traffic, and bandwidth usage is dynamically adjusted during all transfers.
- **Download and execute model.** Many customers want to download the source package for the software onto the local computer. This allows checkpoint/restart to verify that all pieces are in place before installation, and lets users take advantage of the power of the Windows Installer service for self-healing and just-in-time feature installation. Systems Management Server 2003 allows the administrator to make packages function in this way to provide users with the right software no matter where they are located.

Administrators should note that all traffic in both directions between the Advanced Client and a Systems Management Server is bandwidth controlled. This ensures that inventory data, software usage data and status messages also do not impede traffic during transmission to the Systems Management Servers.

Bandwidth management between Systems Management Server site servers

Communications have also been improved between site servers in Systems Management Server 2003. Specifically, throttling and scheduling of all traffic between Systems Management Server sites ensures that only a specified portion of bandwidth is used at specific times of day. This feature was supported in earlier versions of Systems Management Server, but Systems Management Server 2003 now extends this with a new feature called Delta Package Replication, which only replicates changes to software packages between sites without retransmitting the complete image of an updated package.

As in previous releases, Systems Management Server 2003 supports a tiered architecture with multiple Systems Management Server sites spanning remote geographic locations. This tiered, hierarchical approach allows fan-out software distributions, the routing of packages across WAN links to minimize repeat transmissions between sites.

Reporting

Systems Management Server 2003 includes a Web-based reporting service with more than 120 pre-built reports and the option to extend these with custom reports under administrator control. The supplied standard reports cover a variety of inventory, software usage activity and Systems Management Server operations options.

A dashboard feature is also supported, allowing IT staff to insert the most useful or powerful reports into a single “heads-up display” of Systems Management Server 2003 operations.

Systems Management Server 2003 Web reports also enable a user to drill into underlying reports by clicking on a line in a single report of interest. Each underlying report may offer greater detail to the administrator, until finally the complete inventory information for a single machine or user may be displayed.

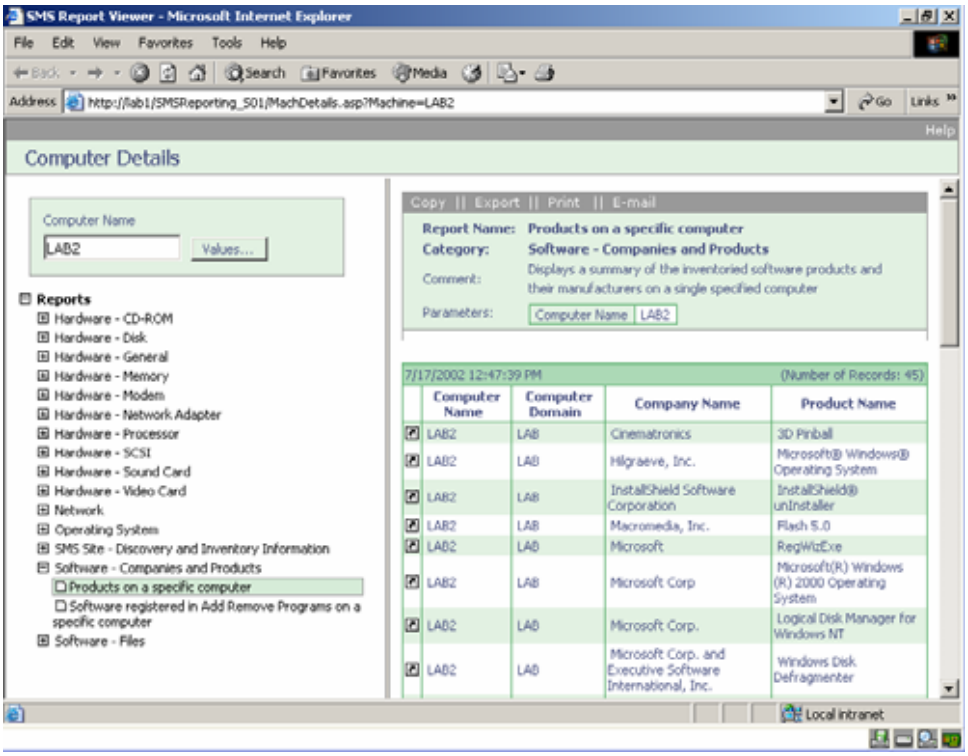


Figure 3. Computer inventories viewed from a Web browser

A menu displays all the pre-built reports ranging from Windows XP upgrade readiness to those machines requiring one or more critical updates.

Software Metering

Administrators can configure Systems Management Server 2003 to track software application

usage by users across all managed machines on and off the network. Through the Systems Management Server Administrator Console, administrators create metering rules to monitor and control the activity of any arbitrary executable file they wish to track. Managed computers then record software usage even while disconnected from the corporate network, uploading usage reports either on a schedule or the next time a connection is available to the Systems Management Server site.

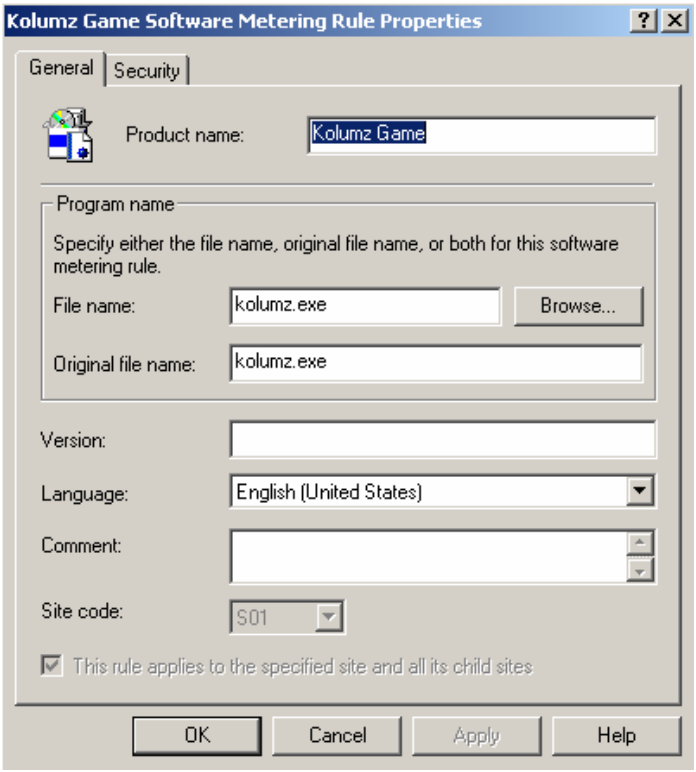


Figure 4. Application usage can be tracked.

The software usage data from all machines in the network is stored in the site database and correlated with the software inventory data. To prevent the software usage data from bloating the SQL database, the data is summarized over time, rolling individual usage records into summary application records. This process is fully configurable by the Systems Management Server site administrator.

The Software Metering subsystem has been fully rebuilt in Systems Management Server 2003, improving its performance and integrating the metering user interface with the Systems Management Server Administrative console and reporting system.

Troubleshooting

Administrators and help desk personnel alike can use the tools and features of Systems Management Server 2003 to remotely troubleshoot problems on managed systems. In addition to the diagnostic tools, the Web-based reporting service can also prove invaluable in providing access to current system configuration data and recent changes.

In addition, the software distribution capabilities of Systems Management Server make it possible for administrators to uninstall and reinstall applications without requiring end-user input.

The troubleshooting tools include the following:

- **Resource Explorer.** This tool allows administrators to query the inventory database for the current configuration state of managed systems, even if the computer is offline. Recent changes to the machine configuration can also be examined.
- **Remote control.** Native Systems Management Server remote control is included as an option on both Systems Management Server client agents, allowing administrators to easily connect to the screen, keyboard and mouse of a remote Systems Management Server client. Systems Management Server 2003 also supports connection to remote Windows XP-based machines using the Remote Assistance feature of that platform. For down-level managed clients, however, the Systems Management Server remote control client can be used. Access to both these remote control features is controlled via user security privileges to ensure that only authorized operators have access to remote machines.
- **Remote chat.** Administrators can initiate a text chat with any user through the Remote Tools application.
- **File transfer.** Files can be managed directly on remote systems using the Systems Management Server Remote Tools applet. Files can be copied to and from specific locations on the remote system. In addition, administrators can delete or move files. Normal operating system user security privileges apply.
- **Remote execute.** Commands can be issued from the Systems Management Server Remote Tools applet to be executed on remote systems.
- **Network Monitor.** Network Monitor can capture, decode and display packets from the network adapter of local and remote managed systems.
- **Network Trace.** The Network Trace tool creates a simple diagram of the network topology immediately surrounding any designated managed Systems Management Server site server selected in the Systems Management Server Administrator Console. Network Trace simplifies debugging by showing the devices dependencies.

Higher scalability and performance

The distributed, hierarchical design of Systems Management Server allows it to manage even the largest of distributed Windows-based environments. Systems Management Server has been in use at numerous organizations with hundreds of thousands of managed nodes.

Every managed environment is managed using a hierarchy of Systems Management Server sites, each of which in turn consists of one or more servers running Systems Management Server software. Content, such as software packages, is replicated down the hierarchy between site servers using the various bandwidth management features described earlier. Global scalability (the management of remote geographically distributed sites) is achieved by placing Systems Management Server sites strategically wherever managed clients are located. Local scalability is achieved by adding servers to share the load of large client bases within a single site location.

Easy installation and operation

One of the key benefits of Systems Management Server 2003 is the relatively short period of time it takes to plan, deploy and start using it. No extensive customization is required before IT departments can begin to see real value from the deployment.

Much of this fast return on investment is due to the high level of integration between Systems Management Server 2003 and the operating systems it manages. Because Systems Management Server was built from the ground up to manage Windows-based systems, it takes advantage of many of the built-in capabilities of the operating system such as Microsoft Management Console and Internet Information Server.

Of course, some planning is always needed to deploy any management system, and the larger and more complex the IT environment, the longer the planning phase required. However, the time required to plan and deploy Systems Management Server in a typical environment is significantly less than for other products in this space.

Simplified deployment

Graphical installation wizards walk the administrator through the process of installing Systems Management Server and automatically detecting if the required services and prerequisites are present (such as the appropriate service pack or an SQL Server™ 2000 database). For example, if Active Directory is available, Systems Management Server will detect it and offer to configure the location services it requires.

Easy to use

Systems Management Server 2003 makes full use of the Microsoft Management Console, presenting administrative functions in a consistent format with other Windows management tools. Administrators can drill through the tree-like interface to access high-level or low-level options. Access to each UI node is controlled via security credentials, allowing custom consoles to be created for different administrative roles.

Wizards are also used to simplify certain key processes such as the creation and distribution of software packages. The Web reporting service also simplifies access to the rich data offered by the Systems Management Server database.

Scriptability

All of the functions and tasks of Systems Management Server 2003 offered through the Administrative user interface can also be executed via scripting. This makes it possible to build a library of scripts to automate common business and administrative processes, such as the weekly distribution of an updated company price list to all sales staff.

Security

Systems Management Server 2003 has many enhancements to increase the overall system security while also simplifying the administrative tasks involved in keeping managed systems and software protected.

Protects against misuse

By making full use of the built-in user security subsystem of the Windows operating systems, Systems Management Server provides extensive protection against misuse. Administrative privileges can be delegated granularly, ensuring that IT staff have only those permissions they need to perform their assigned tasks.

In addition, Systems Management Server 2003 can be operated in an optional Advanced Security mode. In this mode, all Systems Management Server services run under the Network System security context, using the host machine accounts to access other resources on the network. This eliminates the need to maintain multiple account passwords on each site, ensuring compliance with local security policies. Active Directory must be available at all network locations for the advanced security mode to be enabled.

The previous Systems Management Server security model, with multiple firewall-protected accounts used for all server-side activity, is still supported as an option if Active Directory is not available.

Systems Management Server 2003 support for Microsoft Operations Manager 2000

Systems Management Server 2003 complements other Microsoft management products such as Microsoft Operations Manager (MOM) 2000. While the strengths of Systems Management Server lie in software distribution, asset management, software metering and troubleshooting, it is not an appropriate solution for real-time performance and event monitoring. MOM 2000 is designed for this role, optimized to monitor servers running Windows and Microsoft .NET Services. MOM 2000 alerts administrators to problems as they occur, advising operations staff of the detected problem and likely steps to resolution.

MOM 2000 has built-in knowledge of the Systems Management Server product, which allows it to automatically detect Systems Management Server site servers and monitor Systems Management Server-specific activities. Systems Management Server administrators will find that MOM 2000 provides a powerful tool monitoring the Systems Management Server infrastructure and detecting issues as they arise and before they become critical.

Support for industry standards and third-party tools

By using industry-standard protocols and technologies, Systems Management Server 2003 fits well into any environment and can be easily extended to work with other products.

Some of the standards Systems Management Server uses are as follows:

- **Common Information Model.** Microsoft has fully integrated the Distributed Management Task Force Inc.'s Common Information Model, also known as Web-Based Enterprise Management (WBEM), into the Windows operating system. Systems Management Server 2003 makes extensive use of Windows Management Instrumentation (WMI), Microsoft's implementation of the Common Information Model, for collecting inventory information from managed clients. In addition, Systems Management Server offers up its own information through WMI, enabling customers and third-party ISVs to interface with and extend Systems Management Server without the need for complex API coding.

- **XML.** The new Systems Management Server 2003 Advanced Client uses XML to encode the files it transfers to and from the Systems Management Server site servers. Similarly, all policy information passed to the Advanced Client by the Systems Management Server site is encoded in XML.
- **HTTP.** The Advanced Client communicates with the Systems Management Server site services using the standard HTTP protocol, making it easy to manage clients across a firewall.
- **HTML.** The Web reporting feature of Systems Management Server 2003 is handled entirely through a Web service. All reports are rendered in HTML, making them easily accessed from Internet Explorer.

Many third parties have built add-ons to the Systems Management Server product or integrated other solutions with it. Users can check the list of partner products at http://www.microsoft.com/smserver/partners/.

Systems Management Server 2003 Architecture

Systems Management Server 2003 uses a distributed, hierarchical architecture that allows the product to scale beyond the largest customer environments found today. This architecture has proven itself over the years, as previous versions of Systems Management Server have been used to successfully manage environments with hundreds of thousands of Windows-based PC systems.

The design of Systems Management Server deployments varies from the simplest single-server configuration to the most complex multi-server, multi-site solutions, as required to support the specific customer network configuration and hardware. By default, the installation process creates a single Systems Management Server to handle all systems management tasks, with little user interaction required during the setup process. However most typical Systems Management Server deployments require planning and analysis before installation, to ensure that the optimal site design is implemented for a particular customer environment.

Site hierarchy model

In large environments, IT departments can organize Systems Management Server into multiple sites, allowing the architecture to reflect existing business structures with different groups and areas of responsibility.

The primary building block of Systems Management Server 2003 is the site server. Every Systems Management Server environment requires at least one site server, but administrators can configure as many site servers as are required. This allows the site servers to be strategically located to conserve bandwidth, spread workloads and offer redundancy. At least one site server must be designated as a primary server, with an SQL Server database for storage of configuration and operations data. Additional sites may be primary or secondary site servers, with secondary site servers requiring no SQL Server database and no local administration support.

By default, Systems Management Server 2003 installs all its services on a single system. However, this configuration is suitable only for locations with relatively small numbers of managed clients. In larger deployments, administrators will add additional servers to the site, spreading the processing load and providing redundancy in case of a server failure. The different roles that a server may perform within a Systems Management Server site are as follows:

- **Primary site server.** This site sever manages the information store in the SQL Server database. All secondary site servers that report up to this site derive their configuration and policy from the settings held here.
- **Secondary site server.** This site server acts as a low-maintenance remote proxy for managed systems. Primary site servers send instructions to the secondary site servers for the clients managed by such secondary sites. The secondary sites forward information such as deployment status, client inventory data and status back to their parent primary site. As with primary site servers, secondary site servers have bandwidth management capabilities that allow them to efficiently use low-bandwidth links.
- **Management Point.** This role provides the site server interface for Advanced Clients. All client policy is passed via the Management Point to the Advanced Clients. These policies govern

everything from software metering rules to which inventory classes should be collected and at what frequency. Management Points transfer information between Advanced Clients and the Site Servers, translating from XML encoding the native Systems Management Server formats. Any primary or secondary site server can be a Management Point. Management Points only work for nodes running the Advanced Client. Systems Management Server 2003 supports multiple Management Points per site, and allows Windows Network Load Balancing to be used to balance client load across all such servers, providing a highly scalable client management infrastructure.

- **Client Access Point.** Computers using the Legacy Client communicate with their site server via Client Access Points, which perform a similar function to Management Points, but using standard file copying protocols for communication.
- **Distribution point.** Any Windows server can act as a distribution point, as this role simply offers distribution packages either on a Windows share or via the BITS protocol described earlier. Providing multiple distribution points within a site allows for redundancy and improved performance, as the clients' load during a large deployment is spread across all available distribution points.

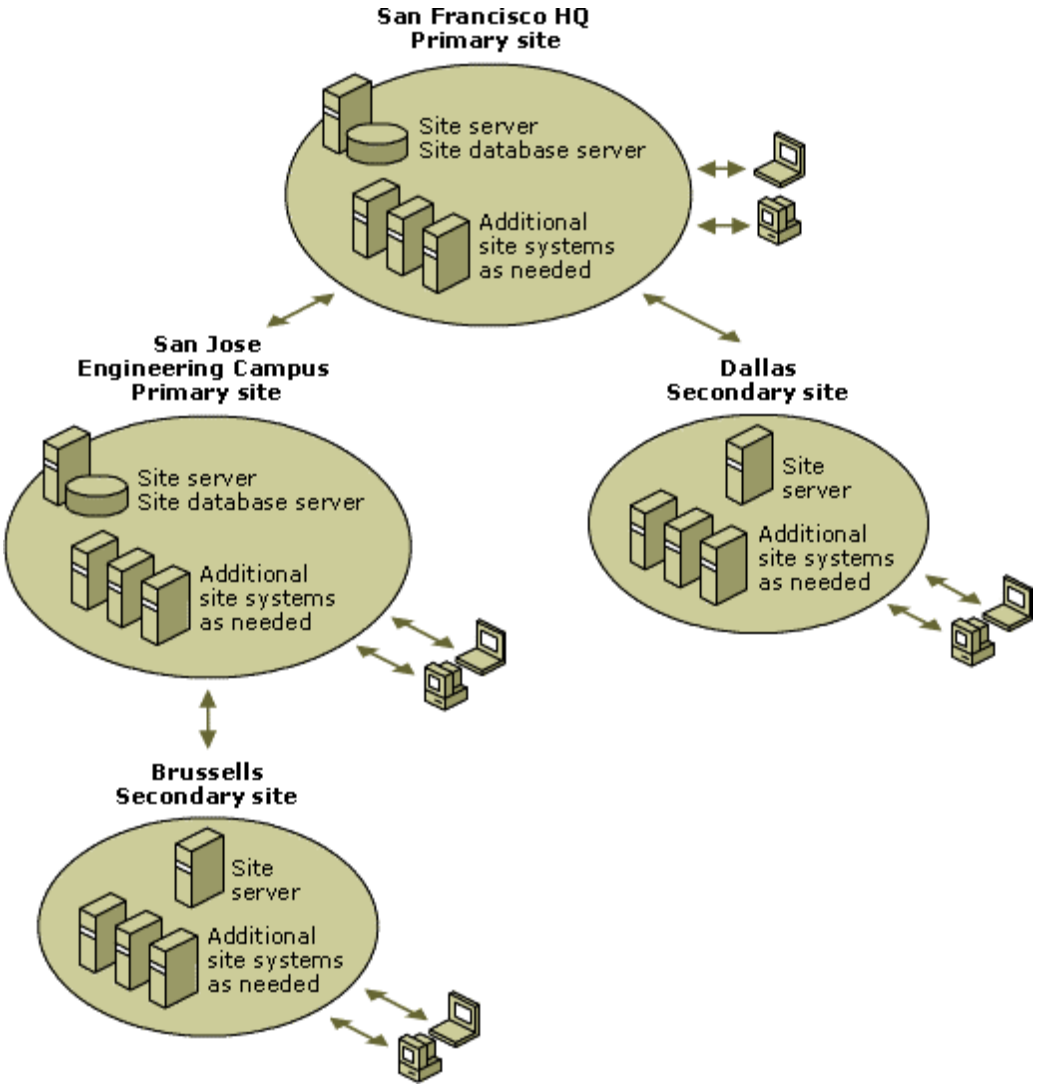


Figure 5. Systems Management Server supports a flexible hierarchical design.

Test-Driving Systems Management Server 2003

This section of the guide provides a series of exercises designed to give you a thorough introduction to the features of Systems Management Server 2003.

To work through the Test-drive you will need a copy of the SMS 2003 product CD and a copy of SQL Server 2000 SP3a product or above. If you choose to work through the Test-drive", you will also need a base system which meets the requirements detailed below. During the Test-drive you will carry out the entire system and feature configuration yourself.

Full Test-drive System requirements

To ensure that the step-by-step instructions work correctly when building your own Systems Management Server 2003 evaluation system from the ground up, the following basic requirements must be met by the system hosting the installation:

- ☑ The host server is running Microsoft Windows 2000 Server or Windows Server 2003 Standard Edition, configured as an Active Directory domain controller of its own forest. In the text below, the domain being managed is "review.sms.net"
- ☑ In the text descriptions the server domain controller is called ***LAB2***, although any name may be used. The Test-drive assumes an Administrator account named *sms-tour* has been created on this domain. You should create an account of this name with all Administrative rights for the purposes of the Test-drive.
- ☑ Microsoft Internet Explorer 6 or later must be installed on the Windows Server.
- ☑ Microsoft Internet Information Services must be installed on the Windows 2000 Server (available as a standard option under Add/Remove Windows Components).
- ☑ If Windows Server 2003 is being used as the host OS, then the Background Intelligent Transfer Service Extensions must be installed and enabled on the Internet Information Services application (available as an option under Add/Remove Windows Components – Application Server – Internet Information Services).
- ☑ If Windows Server 2003 is being used as the host OS, then the WebDAV Web Service Extensions must be enabled on the Internet Information Services Manager (accessible from the Administrative Tools menu).
- ☑ If Windows 2000 Server is being used as the host OS, then Service Pack 4 must be installed.
- ☑ Microsoft SQL Server 2000 must be installed on the host machine, with Service Pack 3 or greater applied.
- ☑ The Active Directory must be called lab.com, and the simple directory name should be set to lab.
- ☑ There must be one client computer running Microsoft Windows XP Professional. This computer must be a member of the lab.com Active Directory and should be called LAB2.
- ☑ A Microsoft SQL Server 2000 CD must be available for the installation of Systems Management Server 2003.

NOTE: Most of the above requirements are for the purposes of enabling the walk-through scenarios below, and are not requirements of the Systems Management Server 2003 product itself.

1. Installing Systems Management Server 2003

If you are building your own evaluation system rather than using a prepared Virtual PC image, please verify that the prerequisites outlined above under “Full Test-drive System Requirements” have been completed before starting this section.

NOTE: If you are using the preconfigured Virtual PC image, you do not need to complete these steps (though you may wish to review them for reference).

A. Enabling Active Directory schema extensions (Windows 2000 only)

The steps in this section are only required if the host server is running Windows 2000 Server. If you are installing Systems Management Server 2003 on a Windows Server 2003 host, you may jump to step **B.** below.

Before Systems Management Server 2003 can integrate with Active Directory on a Windows 2000 server appropriate security privileges must be set to allow the directory schema to be extended by the administrator. We start by loading the configuration tool which allows this change to be made.

1. Insert the Windows 2000 Server CD into the host machine named ***lab2***.
2. Run the AdminPak.msi program in the \I386 directory on the Windows Server CD.
3. In the **Windows 2000 Administration Tools Setup Wizard** window, click on **Next**.
4. In the **Setup Options** window, select **Install all of the Administrative Tools**, and then click on **Next**.
5. Click on **Finish**.
6. On the taskbar, click on the **Start** button, and then click on **Run**.
7. Type **mmc.exe**, and then click on **OK**. The **Console1** window appears displaying a blank snap-in.
8. On the **Console** menu, click on **Add/Remove Snap-in**. The **Add/Remove Snap-in** dialog box appears.
9. Click on **Add**. The **Add Standalone Snap-in** dialog box appears, displaying all available snap-ins.
10. Under **Snap-in**, select **Active Directory Schema**, and then click **Add**.
11. Click on **Close**. The **Add/Remove Snap-in** dialog box appears, displaying the Active Directory Schema snap-in that was added.
12. Click on **OK**. The **Console1** window appears, displaying the Active Directory Schema snap-in.
13. In the console tree, right-click on **Active Directory Schema**, and then select **Operations Master**. The **Change Schema Master** dialog box appears.
14. Click on **The Schema may be modified on this Domain Controller**, and then click on **OK**. The **Console1** window appears, displaying the Active Directory Schema snap-in.

15. On the **Console** menu, click on **Exit**. A Microsoft Management Console message box appears prompting you to save the changes to Console1.

16. Click on **No**, opting not to save the console settings.

You have now configured the computer so that the Active Directory schema can be extended on this Windows 2000 server. .

B. Installing Systems Management Server 2003

In this section, you will install Systems Management Server 2003 onto the host system, using the installed copy of SQL Server 2000 and with default settings enabled.

1. Load the Systems Management Server 2003 installation CD onto the Windows 2000 Server domain controller called ***lab2***. The **Systems Management Server 2003 Setup** dialog box appears.

2. Click on the **SMS 2003** link. The **Welcome to the Microsoft Systems Management Server Setup Wizard** dialog box appears.

3. Click on **Next**. The **Systems Management Server Setup Wizard System Configuration** dialog box appears, indicating Setup did not find any existing Systems Management Server installation on the computer.

4. Click on **Next**. The **Systems Management Server Setup Wizard Setup Options** dialog box displays options for installation.

5. Click on **Install an SMS primary site** option, and then click on **Next**. The **Systems Management Server Setup Wizard Installation Options** window appears.

6. Select **Express Setup**, and then click on **Next**. The **Systems Management Server Setup Wizard License Agreement** dialog box appears. Read the licensing information.

7. Click on **I Agree**, and then click on **Next**. The **Systems Management Server Setup Wizard Product Registration** dialog box requests registration information.

8. In the **Name box**, type your name.

9. In the **Organization** box, type your company name.

10. In the **CD Key** box, type the evaluation key **111-1234567**, and then click on **Next**. The **Systems Management Server Setup Wizard Systems Management Server Site Information** dialog box appears, prompting you for site information.

11. In the **Site code** box, type **S01**.

12. In the **Site name** box, type **labsite**. The **Site domain** box should already have the domain *review* listed by default. If not, the Active Directory domain may not have been properly set up.

13. Click on **Next**. The **Systems Management Server Setup Wizard Systems Management Server Active Directory Schema** dialog box appears, providing information regarding extending the Active Directory schema to implement server locator or Management Points.

14. Click on **Extend the Active Directory schema**, and then click on **Next**. The **Systems**

Management Server Setup Wizard Systems Management Server Security Information dialog box appears prompting you for Systems Management Server Service account information and the level of Systems Management Server security mode to implement.

15. Select **Advanced security**, and then click on **Next**. The **Systems Management Server Setup Wizard Systems Management Server Primary Site Client Load** dialog box appears, prompting you for the number of clients expected in this Systems Management Server site. This is to provide automatic configuration of the Systems Management Server database.
16. Click on **Next** to accept the default of 100. The **Systems Management Server Setup Wizard Concurrent Systems Management Server Administrator Console** dialog box appears.
17. Keep the default setting of 5 Systems Management Server Administrator Consoles, and then click on **Next**. The **Systems Management Server Setup Wizard Completing Systems Management Server setup** dialog box appears.
18. Click on **Finish**.
19. When the **Systems Management Server Setup Wizard** window appears saying the installation is complete, click on **OK**.

2. Installing and Assigning the Advanced Client

For the purposes of simplified testing in the reviewers guide, a single machine – the Systems Management Server itself – will be managed. The agent installation will be triggered manually on the Windows Server host machine for this test-drive, however in real-world deployments, administrators could trigger installation via user logon scripts, application of Group Policy, by "pushing" the agent remotely over the network or by including it as a standard component in new computer builds.

The following steps will cause the new Advanced Client agent to be downloaded and installed onto the server.

A. Installing the Advanced Client agent

Note: In these tests, you will be using the new Systems Management Server Advanced Client, which supports new features such as checkpoint/restart and download and execute. A Legacy Client is still provided with Systems Management Server 2003 both for legacy system support (the Advanced Client only runs on Windows 2000 and later) and to provide a staged transitional step during system upgrades.

1. From the server named ***LAB2***, log on as a local administrator (usually the **Administrator** ID should suffice).

Note: Administrative privileges are required to install the Systems Management Server agent using this manual process. This is a requirement of the test-drive scenario only – in normal deployment end users are not required to have such access to trigger agent installation.

2. Open the **Run** command window (**Start→Run…**), and enter the command line ***\\lab2\smsclient\i386*** and click on **OK**.
3. After a few seconds, a new Windows Explorer window will open showing the files in this server folder.
4. Double-click the file named ***ccmsetup.exe***. This application will silently download the ***client.msi*** file to the local machine and then execute it to install all required client management components.

NOTE: The new Systems Management Server 2003 Advanced Client will now be installed silently in the background, requiring no user intervention. This process will take 10-15 minutes, and includes a re-startable download phase to assist with client install over intermittent RAS links.

You should allow 10-15 minutes to elapse before proceeding to step **E.** where you will confirm the installation. If you wish to monitor the installation progress, you may wish to view the ***ccmsetup*** log file located at ***<WINDIR>\System32\CCMSETUP\ccmsetup.log***.

E. Assigning the Advanced Client to a site

1. From the Server named ***LAB2***, click on the **Start** button on the taskbar, and then click on **Control Panel**.
2. Be sure that **Classic View** is selected in Control Panel by clicking on **Switch to Classic View**. A **Systems Management** icon will be visible once the client setup has completed.

3. Open the **Systems Management** icon in Control Panel.
4. In the **Systems Management Properties** window, click on the **Advanced** tab. Notice that the Systems Management Server site code can be changed as well as the location and space allocated for local caching. Local caching is a new option in Systems Management Server 2003 that allows software packages to be downloaded before installation.

Note that the **Currently assigned to site code** box is empty. In this instance the advanced client has not yet been assigned to a specific Systems Management Server site for management. Normally such assignment would happen automatically during installation, but this has been suppressed for the purposes of this walkthrough.

5. We will now trigger the client to look in the directory for the nearest site, and assign itself to that site for management. Under the **SMS Site** section, press the **Discover** button.
6. A message box titles **SMS Site Discovery** is displayed, indicating that discovery was successful. The client found itself to be within the boundaries of an SMS site advertised in Active Directory.
7. Click **OK** to dismiss the message box. Note that the **Currently assigned to site code** box now indicates this client is assigned to site **S01**. Press the **Apply** button to commit this information.
8. Click the **Actions** tab on the dialog to display a list of agent tasks which can be manually initiated by the user at this time. Two items are currently displayed: **Machine Policy Retrieval & Evaluation Cycle** and **User Policy Retrieval & Evaluation Cycle.** Click the **Machine Policy Retrieval & Evaluation Cycle** item and then press the **Initiate Action** button to trigger that action.
9. This will cause the agent to immediately query the currently assigned site (**S01**) for the management policy and settings to be applied to this machine. Such a policy check happens on a recurring basis – in this case we have simply forced the policy check to be initiated at once.
10. Close the **Systems Management Properties** window by pressing **OK**.

3. Linking Systems Management Server to Active Directory

To demonstrate Active Directory links, you will need to create some directory objects and containers with which Systems Management Server can interact.

A. Creating a user account in Active Directory

To carry out the Systems Management Server 2003 test-drive, you need to create an Active Directory account and organizational unit.

1. From the Systems Management Server 2003 primary site server named ***LAB2***, run the Active Directory Users and Computers administration tool by clicking on the **Start** button, clicking on **Programs**, clicking on **Administrative Tools** and clicking on **Active Directory Users and Computers**.
2. From the **Active Directory Users and Computers** management console, right-click on **review.sms.net** in the left pane, click on **New** and click on **Organizational Unit**.
3. In the **New Object – Organizational Unit** window, type **asia** in the **Name** box, and then click on **OK**. The organizational unit "***asia***" appears in the left pane directory tree.
4. Right-click on the organizational unit "***asia***" in the right pane, click on **New**, and then click on **User**.
5. In the **New Object – User** window, type **Albert** in the **First name** box, type **Smith** in the **Last name** box, type **albert** in the **User logon name** box and then click on **Next**.
6. In the next **New Object – User** window, type a suitable password in the **Password** boxes, select **Password never expires** and then click on **Next**.
7. In the next **New Object – User** window, click on **Finish**.
8. In the left pane of the **Active Directory Users and Computers** management console, click on the "***asia***" organizational unit. Notice that the user Albert Smith is now a member of the "***asia***" organizational unit.
9. Close the **Active Directory Users and Computers** management console.

B. Linking with Active Directory

To prevent accidental performance problems with large directories, Systems Management Server 2003 requires that administrators choose which directory trees, and containers are to be synchronized with SMS. Since we are using a test network with a small directory for this walk-through, we will enable linking with the entire domain.

1. From the Systems Management Server 2003 primary site server, open the management console by clicking on the **Start** button, clicking on **Programs**, clicking on **Systems Management Server** and clicking on **Systems Management Server Administrator Console**.
2. In the console tree, expand **Site Database**, expand **Site Hierarchy**, expand the **S01 - labsite**, expand **Site Settings** and then select **Discovery Methods**. The list of discovery

methods for the local site appears in the details pane. Notice the three discovery methods related to Active Directory environments.

3. In the details pane, right-click on **Active Directory System Discovery**, and then select **Properties**. The **Active Directory System Discovery Properties** dialog box appears.
4. Select **New** (the icon in the shape of a star). The **Browse for Active Directory** dialog box appears, allowing you to specify the use of a local domain, local forest or remote forest for discovery.
5. Verify that **Local domain** is selected, and then click on **OK**. The **Select New Container** dialog box appears, allowing you to specify the container to use for discovery.
6. Select the local domain named **review**, and then click on **OK**. The **Active Directory System Discovery Properties** dialog box appears. Notice the distinguished name for the container to search. Also notice that by default a recursive search will be performed on that container.
7. Click the **Polling Schedule** tab, select **Run discovery as soon as possible**, and then click on **OK**. The Systems Management Server Administrator Console is now in the foreground.
8. In the details pane, right-click on **Active Directory User Discovery**, and then select **Properties**. The **Active Directory User Discovery Properties** dialog box appears.
9. Select **New** (the icon in the shape of a star). The **Browse for Active Directory** dialog box appears, allowing you to specify the use of a local domain, local forest or remote forest for discovery.
10. Verify that **Local domain** is selected, and then click on **OK**. The **Select New Container** dialog box appears, allowing you to specify the container to use for discovery.
11. Select the local domain named **review**, and then click on **OK**. The **Active Directory User Discovery Properties** dialog box appears. Notice the distinguished name for the container to search. Also notice that a recursive search will be performed on that container.
12. Click on the **Polling Schedule** tab, select **Run discovery as soon as possible**, and then click on **OK**.

C. Verifying Active Directory system and user discovery

Note: It may take a few minutes for Active Directory discovery to complete. If the users or systems do not show up under collections as expected, wait a few minutes and then repeat the steps below.

1. In the Systems Management Server console tree, expand **Site Database**, and then select **Collections**. The list of collections appears in the details pane.
2. In the console tree, expand **Collections**, and then click on **All Systems**. The members of the All Systems collection appear in the details pane. The local site server (***LAB2***) appears.
3. Right-click on **All Systems**, click on **All Tasks** and then click on **Update Collection Membership**. The **All Systems** message box appears, prompting you to update subcollection membership.
4. Click on **OK**. The collection is updated. Notice the hourglass icon next to the All Systems

collection. This indicates that the collection must be refreshed to display the updated membership information.

5. Click on the **Refresh** icon on the **console** menu. The collection membership is updated and the current membership of the All Systems collection appears.
6. In the console tree, click on **All Users**. The members of the All Users collection appear in the details pane. Notice that no members are listed.
7. Right-click on **All Users**, click on **All Tasks** and then click on **Update Collection Membership**. The **All Users** message box appears prompting you to update subcollection membership.
8. Click on **OK**. The collection is updated. Notice the hourglass icon next to the All Users collection. This indicates the collection must be refreshed to display updated membership information.
9. Click on the **Refresh** icon on the **console** menu. The collection membership is updated and the current membership of the All Users collection appears. The user ***Albert Smith*** appears in the right pane.

D. Creating an organizational unit based collection

1. In the Systems Management Server console tree, expand **Site Database** and then select **Collections**. The list of collections appears in the details pane.
2. Right-click on **Collections**, click on **New** and then click on **Collection**. The **Collection Properties** window appears.
3. In the **Name** box, type “All Users for asia.”
4. Click on the **Membership Rules** tab.
5. Click on the **Direct Membership** icon (the computer with a star on the screen). The **Create Direct Membership Rule Wizard** appears.
6. Click on **Next**. The **Create Direct Membership Rule Wizard Search for Resources** window appears.
7. In the **Resource class** box, select **User Resource**; in the **Attribute name** box, select **User OU Name**; and in the **Value** box, type “lab\asia.”
8. Click on **Next**. The **Create Direct Membership Rule Wizard Collection Limiting** window appears.
9. Leave the **Search in this collection** box blank, and then click on **Next**. The **Create Direct Membership Rule Wizard Select Resources** window appears. The user LAB\albert appears in the list.
10. Click on **Select All** and then click on **Next**. The **Create Direct Membership Rule Wizard Completing the Create Direct Membership Rule Wizard** window appears.
11. Click on **Finish**. The Membership wizard disappears and the **Collection Properties** window reappears.

12. Click on **OK**. A new collection called **All Users in asia** appears in the console tree.
13. In the console tree, select the **All Users in asia** collection. Notice that the user ***Albert Smith*** appears in the details pane.

3. Exploring the Administrator console

This section walks through several key features within the Systems Management Server 2003 Administrator console, which is implemented within the Microsoft Management Console subsystem.

A. Managing collections

Managed computers may be assigned to one or more containers called collections. Membership of collections may be static, or based on rules defined as queries against object properties. Systems Management Server 2003 automatically creates a number of predefined collections, but administrators may create new collections as required.

1. If the Systems Management Server Administrator Console is not already open, from the Systems Management Server 2003 primary site server, open the management console by clicking on the **Start** button, clicking on **Programs**, clicking on **Systems Management Server** and then clicking on **Systems Management Server Administrator Console**.
2. In the console tree, expand **Site Database** and then expand **Collections**. Notice that there are already many predefined collections (or groupings) of computers, users and groups.
3. In the console tree, right-click on **Collections**. Notice that new collections can be created under **New**. Do not select any options.
4. In the console tree, select the **All Systems** collection.
5. In the details pane, right-click on the managed machine **LAB2**.
6. Select **All Tasks**. Notice the many options for managing the individual PC that appear.

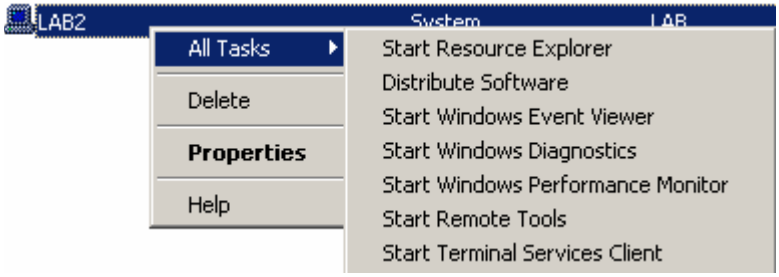


Figure 6. Management tasks for specific computers

Note: The Remote Tools and Terminal Services Client options will not be visible in this test-drive, as the server cannot connect to itself remotely. These options would be displayed for any other managed system. A Remote Assistance option will also appear if the Administrator console is run from a Windows XP or Windows Server 2003-based system and the client is Windows XP or above . In most environments, it makes sense to run Systems Management Server 2003 administrative tools from a computer running Windows XP Professional to allow the use of Remote Assistance and provide more options for remote assistance.

7. The other options under the **All Tasks** menu allow you to view the event log, monitor performance and view detailed system information. A software distribution wizard can also be selected to easily deploy applications.

4. Deploying a software package

You will use a wizard to deploy a sample Windows Installer-ready software package and verify that self-repairing works. For this walk-through, the ***orca.msi*** utility from the Windows Installer Resource Kit is used. This example tool displays the contents of Windows Installer setup (.MSI) files. Any software with an .MSI extension can be used for this test. Systems Management Server 2003 can also distribute any other kind of software package, but extra features and capabilities are possible when working with Windows Installer.

A. Using the software distribution wizard

Targeting and distributing software requires several steps by an administrator. The SMS Console provides a simple to use wizard which combines all these steps into a single serial process, simplifying the overall experience.

NOTE: For this exercise you will need a copy of the ***orca.msi*** file or some other MSI installation package file. If you are following the Virtual Test-drive using the Virtual PC image, you will find a copy of this file in the ***C:\Misc\Orca*** folder of the machine ***LAB2***. If you are following the Full Test-drive you will find a copy of the file on the supplied DVD-R media. Create a directory on the SMS server called ***C:\Misc\orca***, and then copy the ***orca.msi*** file to it.

1. If the Systems Management Server Administrator Console is not already open, open the Administrator console from the Systems Management Server 2003 primary site by clicking on the **Start** button, clicking on **Programs**, clicking on **Systems Management Server** and then clicking on **Systems Management Server Administrator Console**.
2. In the console tree, expand **Site Database**, expand **Collections** and then select **All Users in asia**.
3. Verify that the user name Albert Smith appears in the details pane.
4. In the console tree, right-click on **All Users in asia**, click on **All Tasks**, and then click **on Distribute Software**. The **Distribute Software to Collection Wizard** appears.
5. Click on **Next**. The **Distribute Software to Collection Wizard Package** window appears.
6. Verify that **Create a new package from a definition** is selected, and then click on **Next**. By using a definition file, you can distribute software that has been previously prepared by the Systems Management Server snapshot tool, Windows Installer definition files (with an .msi extension) or some other formats. It is preferable to use Windows Installer packages because they will be able to take advantage of self-repairing and other Windows Installer capabilities.
7. In the **Distribute Software to Collection Wizard Package Definition** window, click on **Browse**. A directory browsing window now appears.

8. In the ***C:\Misc\orca*** directory, select **orca.msi** and then click on **Open**. You are returned to the **Distribute Software to Collection Wizard Package Definition** window.
9. Click on **Next**.
10. In the **Distribute Software to Collection Wizard Source Files** window, select **Always obtain files from a source directory** and then click on **Next**.
11. In the **Distribute Software to Collection Wizard Source Directory** window, select **Local drive on site server**, and then enter the correct directory location for orca.msi (such as C:\orca) for the path.
12. Click on **Next**.
13. In the **Distribute Software to Collection Wizard Distribution Points** window, select ***LAB2***. Systems Management Server 2003 can easily use multiple distribution points, allowing for a scalable distributed hierarchy.
14. Click on **Next**.
15. In the **Distribute Software to Collection Wizard Select a Program to Advertise** window, select **Per-user unattended**.
16. Click on **Next**.
17. In the **Distribute Software to Collection Wizard Advertisement Name** window, type "orca utility" in the **Name** box. The name entered for the Advertisement is what the user will see in the list of available programs.
18. Click on **Next**.
19. In the **Distribute Software to Collection Wizard Advertise to Subcollections** window, select **Advertise the program to members of subcollections as well**, and then click on **Next**.
20. In the **Distribute Software to Collection Wizard Advertisement Schedule** window, ensure that the date and time are set to the day and time you are running this test.
21. Select **No. This advertisement never expires**, and then click on **Next**.
22. In the **Distribute Software to Collection Wizard Assign Program** window, select **No. Do not assign the program**. Click **on Next.**
23. In the **Distribute Software to Collection Wizard** window, click on **Finish**.

B. Specifying download and execute mode

In this procedure, we will enable the download and execute option so that the Orca software package will take advantage of the new mobile support, thereby ensuring that the package is copied locally onto remote systems before it is installed.

1. In the console tree, expand **Site Database** and then select **Advertisements**. The advertisement for the orca utility appears in the details pane on the right.
2. In the details pane, right-click on the advertisement called **orca utility**, and then select **Properties**. The **orca utility Advertisement Properties** window appears.

3. Click on the **Advanced Client** tab.
4. Under **When a local distribution point is available**, select **Download before running**.

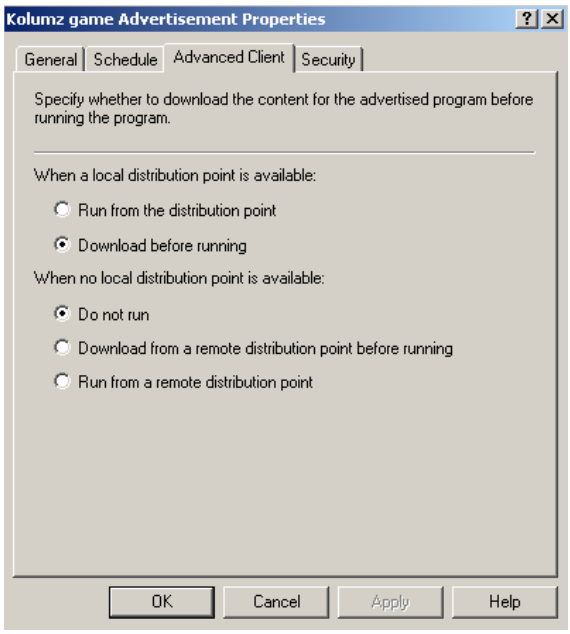


Figure 7. Mobile users can benefit from having software downloaded to their local machines before installation.

5. Click on **OK**.

C. Self-healing and elevated installs

Many additional options can be set for distributing software packages. The following procedures set the install option to allow self-healing of a Windows Installer package and ensure that the software is installed using administrative privileges.

1. In the console tree, expand **Site Database**, and then select **Packages**. The package for the orca utility appears in the details pane on the right.
2. Expand **Packages** in the console tree.
3. Expand the **Microsoft Orca** item listed under **Packages**.
4. Select **Programs** under the **Microsoft orca** item in the console tree.
5. Right-click on **Per-user unattended** in the details pane. Select **Properties**. The **Per-user unattended Program Properties** window appears.
6. In the General Tab, replace the **"/i"** parameter with **"/j"** in the **Command line** field.

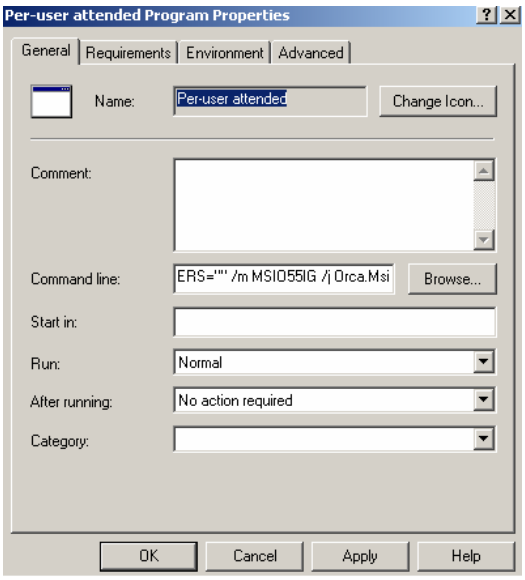


Figure 8. The /j parameter enables allows self-healing in Windows Installer.

7. Click on the **Environment** tab and ensure the **Run with administrative rights** option is chosen.
8. Click on **OK**.

D. Forcing immediate software distribution to users

To avoid waiting for distributions to occur at a scheduled time, you can speed things up from the client PC.

Note: Make sure to wait at least 2 minutes after completing the previous software distribution exercise in section B. This is to ensure that Systems Management Server has completed creation of all the necessary policy files for the clients.

---

1. From the machine named ***LAB2***, log on with the user ID **albert** using the **review** domain.
2. In Control Panel, double-click on the **Systems Management** icon. Make sure Control Panel is set to Classic View so that the Systems Management icon is visible.
3. In the **Systems Management Properties** window, click on the **Actions** tab.
4. Select **User Policy Retrieval & Evaluation Cycle** and then click on **Initiate Action**. The **User Policy Retrieval & Evaluation Cycle** window appears.
5. Click on **OK**. The **Systems Management Properties** window returns.
6. Click on **OK**.

Note: It may take several minutes for the software advertisement to transfer. Systems Management Server is designed to work in large environments with scheduling; many processes do not occur instantaneously.

E. Installing the software on a client computer

In this section, you will install the software package that was distributed by the Systems Management Server administrator to a managed client.

1. From the managed machine named ***LAB2***, make sure you are logged on as the user ***albert*** in the ***review*** domain. After a short delay, a message will appear in the bottom right-hand corner of the screen saying that new software is available. Keep in mind that new packages might not show up for several minutes. Client policy polling intervals are set to minimize the network impact of management traffic, and so batch delays are to be expected.
2. In Control Panel, double-click on the **Add or Remove Programs** icon.
3. In the left pane, click on **Add New Programs**. The **Microsoft Orca** utility appears as an available program.
4. Select **Microsoft Orca** and then click on **Add**. The **Program Download Required** window appears.
5. Select **Run program automatically when download completes**, and then click on the **Download** button. If you were to try this from an additional client assigned to the server, you could try the checkpoint/restart capability of Systems Management Server 2003 by disconnecting the client from the network while it was in the middle of downloading the package. As soon as you reconnected the client to the network, the download would continue where it left off.

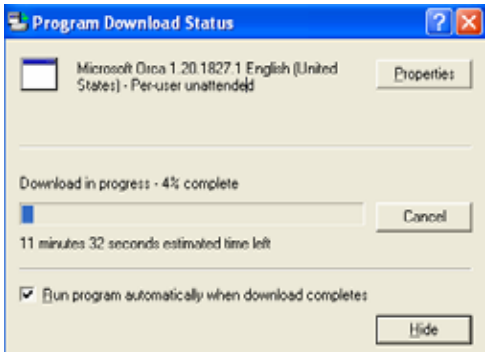


Figure 9. Status of software downloads

6. An icon for **Orca** should now appear under **Start -> All Programs**. Select the icon and begin the program. Orca will run.
7. Verify that Orca has been properly registered in the operating system by going to Control Panel and double-clicking on the **Add or Remove Programs** icon. Orca should show up as one of the existing applications in **Change or Remove Programs**.

Note: Systems Management Server 2003 also supports mandatory software distributions. This scenario demonstrates a user-initiated installation for simplicity.

Bonus: The Orca software package was created using Windows Installer and takes advantage of self-repairing. This can be verified by going to the *C:\Program Files\Orca* directory on the managed client PC and deleting *orca.exe*. When the program is executed from the Start menu, it will automatically replace the deleted file and execute properly. You will need to log on with local administration privileges on the client PC to delete the files.

---

5. Software Metering

A. Configuring Software Metering

To monitor software usage in your organization it is first necessary to define which software you wish to track and how the usage information should be summarized. This test-drive is designed to allow the tracking of usage patterns to learn how many users use an application and at what times. For the purposes of this example, we are going to change the scheduled time for data collection and rules propagation so that the process will be accelerated. Typically in large Systems Management Server 2003 environments, the defaults are set to collect this data over days and weeks rather than minutes and hours.

1. In the console tree, expand **Site Database** and then select **Software Metering Rules**.
2. In the console tree, right-click on **Software Metering Rules**, click on **New** and then click on **Software Metering Rule**. The **Software Metering Rule Properties** window appears.
3. Click on the **General** tab, type “orca utility” in the **Product name** box and then type “orca.exe” in the **File name** and **Original file name** boxes. Type ***** into the version field.
4. Click on **OK**.
5. Under **Site Database**, expand **Site Hierarchy**, expand **S01 - labsite** and then expand **Site Settings**.
6. Select **Client Agents** in the console tree. Right-click on **Software Metering Client Agent** in the right pane and select **Properties**. The **Software Metering Client Agent Properties** window appears.
7. Click on the **Schedule** tab.
8. Click on the Data collection **Schedule** button. The **Schedule** window appears.
9. Change the interval to recur every 15 minutes.
10. Click on **OK**.
11. The **Software Metering Client Agent Properties** window appears.
12. Click on the Metering rules download **Schedule** button.
13. The **Schedule** window appears.
14. Change the interval to recur every 15 minutes.
15. Click on **OK**. The **Software Metering Client Agent Properties** window appears.
16. Click on **OK**.
17. Log on to the client PC called LAB2 using the user ID **albert** in the LAB domain. To speed up the metering process, you can manually tell the client to immediately retrieve the latest metering policies. Normally the managed nodes wait for scheduled times to check for policy updates.
18. In Control Panel, double-click on the **Systems Management** icon.

19. Click on the **Actions** tab.
20. Select **Machine Policy Retrieval & Evaluation Cycle**, and then click on **Initiate Action**. The **Machine Policy Retrieval & Evaluation Cycle** window appears.
21. Click on **OK**.
22. Run the Orca program from the **Start -> All Programs menu**. Running Orca allows us to record some activity for metering reports.

Note: Instructions on viewing the Software Metering report are listed in the Web reporting section. It may be necessary to wait for 15 minutes or more before usage data will start to appear in the web reports. This is normal – the system is optimized to provide daily usage data and patterns while minimizing client and network loading.

---

6. Web reporting

A. Configuring a reporting point

Systems Management Server is highly modular, allowing many of its key services to be duplicated across multiple different servers, providing redundancy and scalability of service. To enable reporting, at least one IIS server on the network must be configured as a reporting point for the site.

1. In the console tree, expand **Site Database**, expand **Site Hierarchy**, expand **S01 - labsite** and then expand **Site Settings**. The list of configurable site options appears in the details pane.
2. In the console tree, click on **Site Systems**. The list of site systems appears in the details pane. Notice that the site server \\LAB2 appears as the only site system.
3. In the details pane, right-click on **\\LAB2**, and then select **Properties**. The **\\LAB2 Site System Properties** dialog box appears.
4. Click on the **Reporting Point** tab. The **\\LAB2 Site System Properties** dialog box appears displaying the options for establishing a reporting point.
5. Click on **Use this site system as a reporting point**, and then verify that **SMSReporting_S01** is listed In the **Report folder** box and that the web reports URL is listed as ***http://LAB2/SMSReporting_S01***.

Note: It may take a few minutes for the reporting point to be configured.

B. Running an inventory Web report

1. In the console tree, expand **Site Database** and then expand **Reporting**. The available Systems Management Server Reporting tool functions appear in the console tree.
2. In the console tree, click on **Reports**. The list of available pre-configured reports appears in the details pane. Notice that more than 140 reports are available, although an SMS Administrator may add new reports or modify existing ones at any time.
3. In the details pane, right-click on **Discovery Information for a Specific Computer**, click on **All Tasks**, click on **Run** and then click on **Lab2**. Internet Explorer starts and displays the Systems Management Server Report results. Notice that this machine has been discovered by three different discovery mechanisms.
4. Click on the arrow to the left of one of the rows in the report. The **Systems Management Server Report** window appears with the results of the **Hardware – General** report. Notice that basic properties from hardware inventory are displayed.
5. Click on the arrow to the left of the LAB2 computer row. The **Computer Details Report** window appears with the results, which is a list of hardware reports for the Systems Management Server client computer.
6. Under **Reports**, expand **Software – Companies and Products**, and then click on **Products on a specific computer**. The **Systems Management Server Report** window shows all the

software products found on this machine and the names of the companies which developed them.

7. Close both the **Systems Management Server Report** windows. The **Systems Management Server Report** windows close and the Systems Management Server Administrator Console appears.

C. Running a Software Metering Web report

The software metering reports show what software is being used, by whom and how frequently. However, the reporting system is designed to work in a large distributed environment, and does not provide real-time information. As seen in earlier procedures, we can configure data collection to occur more frequently, but even with the fastest settings, it could take 15 or 20 minutes for data to appear in these reports.

Note: It will take a whole day for the data to be processed even after the data collection settings have been modified. These reports must be run at least one day from the time metering is first configured in the earlier procedures.

---

1. Under **Reporting** in the console tree, select **Reports**.
2. Right-click on the **Install base for all metered software programs** report. Select **All Tasks -> Run -> LAB2**. The Systems Management Server Report window appears, showing the software that has been configured for metering and the number of machines on which it has been installed.
3. Click on the arrow to the left of one of the rule names. The drill-through report lists all machines which show the product as installed.

D. Creating a dashboard

Web-based dashboards can be created to allow administrators to get a quick overview of the data they need, tailored to their specific role.

1. In the console tree, expand **Reporting** and then click on **Dashboards**. The list of dashboards appears. Notice that there are no dashboards available.
2. Right-click on **Dashboards**, click on **New**, and then click on **Dashboard**. The **Dashboards Properties** dialog box appears, allowing the creation of a new dashboard.
3. In the **Name** box, type “Site Status.”
4. In the **Comment** box, type “Monitor the state of this SMS site.”
5. Click on the **Reports** tab. The **Dashboards Properties** dialog box appears, allowing the configuration of report properties for the new dashboard.
6. In the **Rows** box, type “2.”
7. In the **Columns** box, type “1,” and then click on **Set**.
8. Under **Dashboard reports**, select **row 1 column 1** and then click on **Properties** (the icon of a hand pointing to a sheet of paper). The **Select Report** dialog box appears, allowing the selection of the report for this row.
9. Under **Reports**, select **Sites by hierarchy with time of last site status update** and then

click on **OK**. The **Dashboards Properties** dialog box appears, displaying the assigned report for the new dashboard.

10. Under **Dashboard reports**, select **row 2 column 1** and then click on **Properties**. The **Select Report** dialog box appears, allowing the selection of the report for this row.
11. Under **Reports**, select **Count clients assigned and installed for each site** and then click on **OK**.
    The **Dashboards Properties** dialog box appears, displaying the assigned reports for the new dashboard.
12. Click on **OK**. The list of dashboards appears in the details pane. Notice the Managed Clients dashboard is now listed. If the Managed Clients dashboard does not appear, refresh the list of dashboards.
13. In the details pane, right-click on **Site Status**, click on **All Tasks**, click on **Run** and then click on **LAB2**. The **Dashboard Site Status** window appears in Internet Explorer, displaying the results of both the discovered systems and the count of operating systems reports in a single view.
14. Click on **Close**. The **Systems Management Server Administrator Console** window appears.

7. Security Patch Management

Systems Management Server 2003 leverages all of the above features to enable administrators to monitor and maintain the security patch state of all deployed Windows applications and operating systems. We will start by setting up the Security and Microsoft Office Inventory Tools which scan the patch state of all managed clients. We will then go on to deploy a patch using the Deploy Software Updates Wizard.

A. Installing the latest Update Inventory Scanners

The latest versions of the Microsoft Security and Office Update Inventory Tools are always available from the link at ***http://www.microsoft.com/smserver/downloads***, but once installed on an SMS 2003 site, the scanners will update themselves automatically on a configurable schedule.

For this Test-drive we will install versions of the Inventory Tools provided in the Test-drive DVD for Systems Management Server 2003. Note that this section has already been completed on the Virtual Test-drive image.

1. Locate the installation files on the SMS 2003 test-drive DVD, under the ***SUPatchInv*** folder.
2. Execute the ***SecurityPatch_ENU.exe*** file first, which will launch the Security Update Inventory Tool Installation Wizard.
3. Proceed through the wizard by accepting the **End User License Agreement** and the default **Destination Path,** taking you to the **Scan Tool Download** page. At this point an Internet connection from the Site Server is required, to enable a download of the most recent Security Patch database.
4. With the Internet connection enabled, press the **Download** button and wait for a message box indicating the download was completed successfully. Press **Next** to reach the **Ready to Install** page and press **Next** again to start the installation.
5. In the **Distribution Settings** page, leave all items checked and enter ***Security Scan*** in the **Package Name** field, then press **Next.**
6. On the **Database Updates** page, leave the **Obtain updates using** field set to ***LAB2*** so that the site server itself will be used to download updates to the patch database on a schedule. Press **Next** to reach the **Test Computer** page.
7. Type ***LAB2*** in the **Test Computer** field to use the server as the pilot machine for patch testing. Press **Next** to reach the **Ready to Install** page and press **Next** again to start the creation of SMS objects enabling the scanning process.
8. Once the **Installation Completed** page is presented press **Finish** to close it. The Security scanner is now installed and ready to execute on all managed systems.
9. Execute the ***OfficePatch_ENU.exe*** file first, which will launch the Microsoft Office Update Inventory Tool Installation Wizard.
10. Proceed through the wizard by accepting the **End User License Agreement** and the default **Destination Path,** taking you to the **Office Update Tool Download** page. At this point an

Internet connection from the Site Server is required, to enable a download of the most recent Office Patch database.

11. With the Internet connection enabled, press the **Download** button and wait for a message box indicating the download was completed successfully. Press **Next** to reach the **Ready to Install** page and press **Next** again to start the installation.
12. In the **Distribution Settings** page, leave all items checked and change the **Package Name** field to ***Office Scan***, then press **Next.**
13. On the **Database Updates** page, leave the **Obtain updates using** field set to ***LAB2*** so that the site server itself will be used to update the patch database on a schedule. Press **Next** to reach the **Test Computer** page.
14. Type ***LAB2*** in the **Test Computer** field to use the server as the pilot machine for patch testing. Press **Next** to reach the **Ready to Install** page and press **Next** again to start the creation of SMS objects enabling the scanning process.
15. Once the **Installation Completed** page is presented press **Finish** to close it. Both scan agents are now deployed. We will force the ***LAB2*** machine to execute these scans at once, to generate results for our review.
7. In Control Panel, double-click on the **Systems Management** icon.
8. In the **Systems Management Properties** window, click on the **Actions** tab.
9. Select **Machine Policy Retrieval & Evaluation Cycle** and then click on **Initiate Action**. The **Machine Policy Retrieval & Evaluation Cycle** window appears.
10. Click on **OK**. The **Systems Management Properties** window returns.
11. Click on **OK to close the applet**.

Note: It may take several minutes for the software advertisement to arrive, execute and then transfer results to the site via the inventory agent. Allow sufficient time to elapse before proceeding to the next section. A message balloon will appear on the system tray when the Scan Tools are about to run. Allow time after this for the data to replicate.

B. Review results of the Patch Scan Inventory tools

1. From the server ***LAB2***, in the Admin Console select the **Software Updates** node. The results pane shows a list of the patches recorded as being required on the network, across all scanned machines. The numbers in the **Requested** column indicate the number of machines requiring but missing each patch. The numbers in the **Compliant** column show the number of machines requiring each patch, and with it installed correctly. The goal of the administrator becomes to reduce the **Requested** count to zero for a fully compliant network.
2. You may review the same data in a number of Web reports under the **Software Update – Compliance** heading. With this information in hand, an administrator can now plan the deployment of remedial patches to the network. We will carry out these steps in the next section.

C. Deploying a security patch to a client

1. On the server ***LAB2***, in the Admin Console right-click the **Software Updates** node and select the **All Tasks** and then the **Distribute Software Updates** options. The **Welcome to the Distribute Software Updates Wizard** page appears.
2. Click **Next** to reach the **Specify a Software Update Type** page. We will distribute a patch from the Security database, so set the **Select an update type** combo box to **Security** and then press **Next.**
3. In the **Create or Modify SMS Packages** page select **New** and then press **Next.**
4. In the **Identify the SMS Package** page enter a name such as **Review Patch** in the **Package Name** field and press **Next**.
5. Leave the entries unchanged on the **Customize the Organization** page. Note that an administrator could import an RTF file here, the contents of which would be displayed to end users during installation. Such a document could explain the reason for installing certain patches. Press **Next**.
6. On the **Select an Inventory Scanning Program** page leave all settings unchanged, identifying the Security Update scanner as being appropriate for finding the vulnerable machines. Press **Next.**
7. On the **Add and Remove Updates** page, a list of patches detected as missing on the network is displayed, together with the number of machines vulnerable as a result from each. An administrator can press the **Information** button here to view full details of a selected patch.
8. Select a patch from the list by checking the box on the left and then press **Next.**
9. At the **Specify a Source Directory for Files** page, the administrator may elect to pull the patch source files directly from Microsoft via the Internet, or use cached (and presumably pre-tested) binaries stored locally. At this stage in the test drive you have two options – you may download and deploy a real patch live from the Internet, or you can use a patch "emulator" to simulate a patch deployment without affecting the machine patch state.
10. **To deploy a live patch from the Internet**: Leave the selection set to **Download any available update source files for me automatically** and then press **Next.** There will be a pause as the wizard downloads the requested patch files over the Internet. A progress bar is displayed during this download. Once completed the **Software Update Status** page is displayed. If multiple patches were selected for deployment, they will each have been downloaded and would now be listed here. Skip the next step.
11. **To deploy a patch simulator to emulate deployment:** Change the selection to **I will download the source files myself** and then press **Next**.
12. The installation parameters for each selected patch must be set at this page before the wizard will continue. To configure the command line parameters for each patch, select it in the list and then press **Properties** to display the **Patch Properties**. Repeat step 13 or 14 below for each patch in the list.

13. **If you are deploying a live patch (step 10 above):** At this point the only information missing from the properties are the command line parameters. If you are deploying a live Windows patch, you should probably enter the string **/q /z** in the **Parameters** field. For full details of all relevant patch command line options press the **Syntax** button to view a web page detailing the available switches. Now press **OK** and go to step 15.

14. **If you are deploying the patch simulator (step 11 above):** Press the **Import…** button and browse to the location of the **SyntheticPatch.exe** file provided on the Virtual Test-drive DVD. Press **Open** and then **Yes** on the message box that follows. In the **Parameters** field enter the string **/s /reboot**. This will cause the patch simulator to run silently (no UI) and return an exit code indicating a reboot is required. Now press **OK**.

15. In the **Software Update Status** page, the **Ready** column now indicates **Yes** and so we may proceed with the distribution. Press **Next** to move to the **Update Distribution Points** page.

16. Select the checkbox marked **LAB2** to offer the package from this server and then press **Next** to move to the **Configure Installation Agent Settings** page.

17. On this page the administrator can set the install-time behavior of the patch or patches on all client machines. We will change one setting by selecting the **Collect client inventory immediately** option at the top of the page. This will force each client to send updated patch state to the server once installation is complete. Leave all other settings at their defaults and press **Next** to move to the next page.

18. More install-time policy settings are offered here, including the option to present the user with a UI detailing the patches about to be deployed. We will accept all the defaults which enables the install to run silently, without presenting a UI. Press **Next** to move to another page of install-time settings. Here again we will take the defaults and press **Next** to move to the **Advertise Updates** page.

19. This page enables the advertising of the patch to clients. Check the **Advertise** box to enable this and enter **All Systems** in the **Collection** field. We will leave the advert set to recur every 7 days, to ensure patched machines do not regress due to a later roll-back via System Restore, backup recovery or a new or reformatted machine joining the network. Press **Next** to move to the final page of the wizard.

20. Press **Finish** to initiate deployment of the patch to all machines.

21. Shortly afterwards, you will see the balloon message indicating that the patch is about to be installed. Five minutes later the client side installation will begin, with the special Patch Management UI being presented to the end user.

Related Links

The latest information about Systems Management Server can be found at http://www.microsoft.com/sms/ .

More information on all of Microsoft's management products can be found at http://www.microsoft.com/management/ .