

Kerrie Meyler
Byron Holt
Greg Ramsey

with Jason Sandys, Cameron Fuller,
and Anthony Puca

Plan
and Install
**Configuration
Manager**
2007 **R2**

System Center Configuration Manager 2007

UNLEASHED

SAMS

System Center Configuration Manager 2007 Unleashed

Copyright © 2010 by Sams Publishing

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and authors assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-672-33023-0

ISBN-10: 0-672-33023-7

Library of Congress Cataloging-in-Publication Data:

Meyler, Kerrie.

System center configuration manager 2007 unleashed / Kerrie Meyler, Byron Holt, Greg Ramsey ; with Jason Sandys, Cameron Fuller, and Anthony Puca.
p. cm.

Includes bibliographical references.

ISBN-13: 978-0-672-33023-0

ISBN-10: 0-672-33023-7

1. Computer networks--Management--Computer programs. 2. Software configuration management--Computer programs. 3. Microsoft System center configuration manager--Computer programs. I. Holt, Byron. II. Ramsey, Greg. III. Title.

TK5105.5.M488 2009

005.36--dc22

2009020058

Printed in the United States of America

First Printing July 2009

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Sams Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the programs accompanying it.

Bulk Sales

Sams Publishing offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales

1-800-382-3419

corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales

international@pearsoned.com

Editor-in-Chief

Karen Gettman

Executive Editor

Neil Rowe

Development Editor

Mark Renfrow

Technical Editor

Steve Rachui

Managing Editor

Kristy Hart

Project Editors

Lori Lyons

Anne Goebel

Copy Editor

Bart Reed

Indexer

Publishing Works,
Inc.

Proofreader

Williams Woods

Publishing Services

Publishing

Coordinator

Cindy Teeters

Cover Designer

Gary Adair

Composition

Jake McFarland

Foreword

To all of our customers...

Wow—it's been almost 15 years now since the announcement was made for this new product from Microsoft: Microsoft Systems Management Server (SMS) 1.0. The original charter was to “provide easier and more cost-effective management of desktop hardware and software throughout large-scale computing systems, easing what has been one of the most expensive and time-consuming aspects of client-server computing, and enabling customers to run their businesses more effectively.” Sound applicable today? That charter still applies, even though the characteristics and importance for those features have taken on different meanings over the past 15 years, and we are so proud of what we think System Center Configuration Manager (SCCM) 2007 and SCCM 2007 R2 add to this long history. Quite frankly, this is the most significant release of SMS/SCCM ever, and the value we believe it will bring to you, our customers, is tremendous. Fifteen years ago, deploying Windows wasn't as hard—you just put in six floppy diskettes! Sarbanes-Oxley and HIPAA were just part of the “golden rule”—not governmental and corporate obligations. And software distribution was “good enough” if it did just slightly better than you could do if you went from machine to machine manually. Now...you bet your business success on the ability to get software to the right systems at the right time. The core disciplines have remained the same, but the world has evolved to place further demands on those cores. That is what SCCM 2007 is all about: continuing to solidify and extend that core discipline of change and configuration management to today's business problems, with the reliability you've come to expect.

But the greatest thing in those 14+ years is not the 1's and 0's we've shipped to the market—it's the relationships we've made with you, the tens of thousands of SCCM administrators around the world. We are very aware that a large degree of the SMS/SCCM success over the years is attributable to you, your passion and commitment to the problem of systems management and our product. What we've built, you've tweaked. What we've omitted, you've filled in. What we've gotten wrong, you've worked around—and let us know how to do it right next time. It's this relationship in working with you, in building our software and solving your needs, that makes us most proud to come to work every day.

What we've all learned in the software industry is that software is never perfect. We obviously continue to strive for perfection when it comes to quality and security, but we know with as large and diverse a group of customers that we have, there will be no way we get every feature you need, or every feature done in the way you need it. However, our “luxury” is that we have the *best* people on the planet using our product on a daily basis. You—our SCCM administrators—share the same passion in solving your problems and helping your fellow administrators, that we do in building the product. This book is just another testament to that dedication and spirit. We want to thank the authors (SCCM administrators, like you) for their ongoing support of our product and this community. And we look forward to continuing this relationship for years (and releases) to come!

With greatest admiration,
The System Center Configuration Manager Product Group

Introduction

With the release of System Center Configuration Manager 2007, Microsoft continues to enhance its premier systems management software product, used to manage large groups of Windows-based computer systems. Configuration Manager (ConfigMgr) 2007, formerly known as SMS or Systems Management Server, is a wide and diverse product. It enables you to deploy, assess, and update servers, clients, and devices across physical, virtual, distributed, and mobile environments, as well as manage clients that connect only over the Internet (IBCM). Configuration Manager provides software distribution, patch management, operating system deployment, hardware and software inventory, asset management, and desired configuration management. Perhaps it is not surprising that writing this book has been just about as wide and diverse a project as the software itself. *System Center Configuration Manager 2007 Unleashed* provides in-depth technical information about the capabilities and features of ConfigMgr 2007, including information on other products and technologies on which Configuration Manager features and components depend. Our purpose is to go beyond just describing the product and its features, however, and provide insight and examples of how ConfigMgr can be used to help solve real-world problems. The book begins by describing a methodology and framework for solutions-based deployments, and then maps the numerous ConfigMgr feature areas to the architecture, design, and implementation requirements for that topic. Information is current as of Configuration Manager 2007 Release 2 (R2).

Regarding the domain name used in the examples in this book—the official abbreviation of Configuration Manager is “ConfigMgr,” which is the abbreviation we use for the product throughout the book. However, because we were unsuccessful in registering a domain name that had ConfigMgr or some permutation of it, the domain name is SCCMUnleashed.com, because SCCM is another commonly used abbreviation.

Part I: Configuration Management Overview and Concepts

System Center Configuration Manager 2007 Unleashed begins with an introduction to configuration management, including initiatives and methodologies such as Dynamic Systems Initiative (DSI), the IT Infrastructure Library (ITIL), Microsoft Operations Framework (MOF), and Microsoft Solutions Framework (MSF). Although some consider this to be more of an alphabet soup of frameworks than constructive information, these strategies and approaches give a structure to managing one's environment—from system configuration and inventory management to proactive management and infrastructure optimization. Moreover, implementing Configuration Manager is a project, and as such should include a structured approach with its own deployment. Chapter 1, "Configuration Management Basics," starts with the big picture and brings it down to the pain points that system administrators deal with on a daily basis, showing how Microsoft's System Center suite plans to address these challenges.

Chapter 2, "Configuration Manager 2007 Overview," shows how Configuration Manager has evolved from its first days in 1994 as SMS 1.0, and introduces key concepts and feature dependencies. In Chapter 3, "Looking Inside Configuration Manager," we peel back the layers of the onion to discuss the design concepts behind ConfigMgr 2007, the major ConfigMgr components, its relationship with Windows Management Instrumentation (WMI), and the ConfigMgr database.

Part II: Planning, Design, and Installation

Before installing any software, one needs to spend time planning and designing its architecture. ConfigMgr 2007 is no exception. Chapter 4, "Configuration Manager Solution Design," begins this discussion with envisioning the solution and tying into the MSF process phases. In Chapter 5, "Network Design," Chapter 6, "Architecture Design Planning," and Chapter 7, "Testing and Stabilizing," we step through the network and architectural concepts to consider when planning and prototyping a Configuration Manager architecture and deployment. Finally, it is time to implement that design, and Chapter 8, "Installing Configuration Manager 2007," and Chapter 9, "Migrating to Configuration Manager 2007," walk you through the process of installing a new environment or upgrading an SMS 2003 infrastructure to ConfigMgr 2007.

Part III: Configuration Manager Operations

The third part of the book deals with Configuration Manager operations. This is where the bulk of time is spent using ConfigMgr 2007. Our discussion of operations starts with using the console, discussed in Chapter 10, "The Configuration Manager Console." Chapter 11, "Related Technologies and References," introduces some of the related technologies used with the product. Using ConfigMgr requires an installed client on managed systems, as covered in depth in Chapter 12, "Client Management." Day-to-day operations include software packaging and distribution (Chapter 13, "Creating Packages," and Chapter 14,

“Distributing Packages”) and activities such as patch management (Chapter 15, “Patch Management”), desired configuration management (Chapter 16, named appropriately enough, “Desired Configuration Management”), running queries (Chapter 17, “Configuration Manager Queries”), reporting (Chapter 18, “Reporting”), and operating system deployments (Chapter 19, “Operating System Deployment”).

Part IV: Administering Configuration Manager 2007

The last part of the book discusses Configuration Manager administration. This includes security requirements (Chapter 20, “Security and Delegation in Configuration Manager 2007”) as well as backups and maintenance (Chapter 21, “Backup, Recovery, and Maintenance”).

Part V: Appendixes

This book contains two appendixes:

- ▶ Appendix A, “Configuration Manager Log Files,” describes the usage of the myriad log files used by Configuration Manager 2007 that are helpful when trying to troubleshoot assorted issues. It also discusses how to enable those log files not enabled by default, and setting debug and verbose logging levels.
- ▶ Appendix B, “Reference URLs,” includes references and descriptions for many URLs helpful for ConfigMgr administrators, also included as live links under the Downloads tab at the InformIT website at <http://www.informit.com/store/product.aspx?isbn=0672330237>.

Disclaimers and Fine Print

We do have several disclaimers. Although several chapters include information on using Configuration Manager 2007 for meeting various regulatory compliances, this book does not provide legal advice. It only provides factual and technical information related to regulatory compliance. Do not rely exclusively on this book for advice about how to address your regulatory requirements. For specific questions, consult your legal counsel or auditor.

In addition, the information we provide is probably outdated the moment the book goes to print. Microsoft is continually publishing Knowledge Base (KB) and TechNet articles, Service Pack 2 is in development, and as we continue to work with the product, we will always find yet another wrinkle in it. The authors and contributors of *System Center Configuration Manager 2007 Unleashed* have made every attempt to present information that is accurate and current, as we know it. Updates and corrections will be provided as errata on the InformIT website.

Who Should Read This Book

This book is targeted toward the systems professional who wants to be proactive in managing his or her Windows computing environment. This audience is cross-industry, ranging from a single system administrator in a smaller organization, to larger businesses where multiple individuals are responsible for managing servers, clients, and Windows devices. By providing insight into Configuration Manager's many capabilities, discussing tools to help with a successful implementation, and sharing real-world experiences, this book strives to enable a more widespread understanding and use of System Center Configuration Manager.

CHAPTER 1

Configuration Management Basics

System Center Configuration Manager (ConfigMgr) 2007 represents a significant maturation in Microsoft's systems management platform. Configuration Manager is an enterprise management tool that provides a total solution for Windows client and server management, including the ability to catalog hardware and software, deliver new software packages and updates, and deploy Windows operating systems with ease. In an increasingly compliance-driven world, Configuration Manager delivers the functionality to detect "shift and drift" in system configuration. ConfigMgr 2007 consolidates information about Windows clients and servers, hardware, and software into a single console for centralized management and control.

Configuration Manager gives you the resources you need to get and stay in control of your Windows environment and helps with managing, configuring, tuning, and securing Windows Server and Windows-based applications. For example, Configuration Manager includes the following features:

- ▶ **Enterprisewide control and visibility**—Whether employing Wake On LAN to power up and apply updates, validating system configuration baselines, or automating client and server operating system deployment, Configuration Manager provides unprecedented control and visibility of your computing resources.
- ▶ **Automation of deployment and update management tasks**—ConfigMgr greatly reduces the administrative effort involved in deployment of client and server operating systems, software applications, and

IN THIS CHAPTER

- ▶ Ten Reasons to Use Configuration Manager
- ▶ The Evolution of Systems Management
- ▶ Systems Management Defined
- ▶ Microsoft's Strategy for Service Management
- ▶ Bridging the Systems Management Gap
- ▶ Overview of Microsoft System Center
- ▶ The Value Proposition of Configuration Manager 2007

software updates. The scheduling features in software and update deployment ensure minimal interruption to the business. The ConfigMgr summary screens and reporting features provide a convenient view of deployment progress.

- **Increased security**—Configuration Manager 2007 provides secure management of clients over Internet connections, as well as the capability to validate Virtual Private Network-connected client configurations and remediate deviations from corporate standards. In conjunction with mutual authentication between client and server (available in Configuration Manager native mode only), Configuration Manager 2007 delivers significant advances in security over previous releases.

This chapter serves as an introduction to System Center Configuration Manager 2007. To avoid constantly repeating that very long name, we utilize the Microsoft-approved abbreviation of the product name, Configuration Manager, or simply ConfigMgr. ConfigMgr 2007, the fourth edition of Microsoft's systems management platform, includes numerous additions in functionality as well as security and scalability improvements over its predecessors.

This chapter discusses the Microsoft approach to Information Technology (IT) operations and systems management. This discussion includes an explanation and comparison of the Microsoft Operations Framework (MOF), which incorporates and expands on the concepts contained in the Information Technology Infrastructure Library (ITIL) standard. It also examines Microsoft's Infrastructure Optimization Model (IO Model), used in the assessment of the maturity of organizations' IT operations. The IO Model is a component of Microsoft's Dynamic Systems Initiative (DSI), which aims at increasing the dynamic capabilities of organizations' IT operations.

These discussions have special relevance in that the objective of all Microsoft System Center products is in the optimization, automation, and process agility and maturity in IT operations.

Ten Reasons to Use Configuration Manager

Why should you use Configuration Manager 2007 in the first place? How does this make your daily life as a systems administrator easier? Although this book covers the features and benefits of Configuration Manager in detail, it definitely helps to have some quick ideas to illustrate why ConfigMgr is worth a look!

Here's a list of 10 scenarios that illustrate why you might want to use Configuration Manager:

1. The bulk of your department's budget goes toward paying for teams of contractors to perform OS and software upgrades, rather than paying talented people like you the big bucks to implement the platforms and processes to automate and centralize management of company systems.
2. You realize systems management would be much easier if you had visibility and control of all your systems from a single management console.

3. The laptops used by the sales team have not been updated in 2 years because they *never* come to the home office.
4. You don't have enough internal manpower to apply updates to your systems manually every month.
5. Within days of updating system configurations to meet corporate security requirements, you find several have already mysteriously "drifted" out of compliance.
6. When you try to install Vista for the accounting department, you discover Vista cannot run on half the computers, because they only have 256MB of RAM. (It would have been nice to know that when submitting your budget requests!)
7. Demonstrating that your organization is compliant with regulations such as Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), or *<insert your own favorite compliance acronym here>* has become your new full-time job.
8. You spent your last vacation on a trip from desktop to desktop installing Office 2007.
9. Your production environment is so diverse and distributed that you can no longer keep track of which software versions should be installed to which system.
10. By the time you update your system standards documentation, everything has changed and you have to start all over again!

While trying to bring some humor to the discussion, these topics represent very real problems for many systems administrators. If you are one of those people, then you owe it to yourself to explore how Configuration Manager can be leveraged to solve many of these common issues. These pain points are common to almost all users of Microsoft technologies to some degree, and Configuration Manager holds solutions for all of them.

However, perhaps the most important reason for using Configuration Manager is the peace of mind it brings you as an administrator, knowing that you have complete visibility and control of your IT systems. The stability and productivity this can bring to your organization is a great benefit as well.

The Evolution of Systems Management

The landscape in systems and configuration management has evolved significantly since the first release of Microsoft Systems Management Server, and is experiencing great advancements still today. The proliferation of compliance-driven controls and virtualization (server, desktop, and application) has added significant complexity and exciting new functionality to the management picture.

Configuration Manager 2007 is a software solution that delivers end-to-end management functionality for systems administrators, providing configuration management, patch management, software and operating system distribution, remote control, asset management, hardware and software inventory, and a robust reporting framework to make sense of the various available data for internal systems tracking and regulatory reporting requirements.

These capabilities are significant because today's IT systems are prone to a number of problems from the perspective of systems management, including the following:

- ▶ Configuration “shift and drift”
- ▶ Security and control
- ▶ Timeliness of asset data
- ▶ Automation and enforcement
- ▶ Proliferation of virtualization
- ▶ Process consistency

This list should not be surprising—these types of problems manifest themselves to varying degrees in IT shops of all sizes. In fact, Forrester Research estimates that 82% of larger IT organizations are pursuing service management, and 67% are planning to increase Windows management. The next sections look at these issues from a systems management perspective.

Hurdles in the Distributed Enterprise

You may encounter a number of challenges when implementing systems management in a distributed enterprise. These include the following:

- ▶ **Increasing threats**—According to the SANS Institute, the threat landscape is increasingly dynamic, making efficient and proactive update management more important than ever (see <http://www.sans.org/top20/>).
- ▶ **Regulatory compliance**—Sarbanes-Oxley, HIPAA and many other regulations have forced organizations to adopt and implement fairly sophisticated controls to demonstrate compliance.
- ▶ **OS and software provisioning**—Rolling out the operating system (OS) and software on new workstations and servers, especially in branch offices, can be both time consuming and a logistical challenge.
- ▶ **Methodology**—With the bar for effective IT operations higher than ever, organizations are forced to adapt a more mature implementation of IT operational processes to deliver the necessary services to the organization's business units more efficiently.

With increasing operational requirements unaccompanied by linear growth in IT staffing levels, organizations must find ways to streamline administration through tools and automation.

The Automation Challenge

As functionality in client and server systems has increased, so too has complexity. Both desktop and server deployment can be very time consuming when performed manually. With the number and variety of security threats increasing every year, timely application of security updates is of paramount importance. Regulatory compliance issues add a new

burden, requiring IT to demonstrate that system configurations meet regulatory requirements.

These problems have a common element—all beg for some measure of automation to ensure IT can meet expectations in these areas at the expected level of accuracy and efficiency. To get IT operational requirements in hand, organizations need to implement tools and processes that make OS and software deployment, update management, and configuration monitoring more efficient and effective.

Configuration “Shift and Drift”

Even in those IT organizations with well-defined and documented change management, procedures fall short of perfection. Unplanned and unwanted changes frequently find their way into the environment, sometimes as an unintended side effect of an approved, scheduled change.

You may be familiar with an old philosophical saying: *If a tree falls in a forest and no one is around to hear it, does it make a sound?*

Here’s the configuration management equivalent: *If a change is made on a system and no one knows, does identifying it make a difference?*

The answer to this question is absolutely “yes.” Every change to a system has some potential to affect the functionality or security of the system, or that system’s adherence to corporate or regulatory standards.

For example, adding a feature to a web application component may affect the application binaries, potentially overwriting files or settings replaced by a critical security patch. Or, perhaps the engineer implementing the change sees a setting he or she thinks is misconfigured and decides to just “fix” it while working on the system. In an e-commerce scenario with sensitive customer data involved, this could have potentially devastating consequences.

At the end of the day, your selected systems management platform must bring a strong element of baseline configuration monitoring to ensure configuration standards are implemented and maintained with the required consistency.

Lack of Security and Control

Managing systems becomes much more challenging when moving outside the realm of the traditional LAN (local area network)-connected desktop or server computer. Traveling users who rarely connect to the trusted network (other than to periodically change their password) can really make this seem an impossible task.

Just keeping these systems up to date on security patches can easily become a full-time job. Maintaining patch levels and system configurations to corporate standards when your roaming users only connect via the Internet can make this activity exceedingly painful. In reality, remote sales and support staff make this an everyday problem. To add to the quandary, these users are frequently among those installing unapproved applications from

unknown sources, subsequently putting the organization at greater risk when they finally do connect to the network.

Point-of-sale (POS) devices running embedded operating systems pose challenges of their own, with specialized operating systems that can be difficult to administer—and for many systems management solutions, they are completely unmanageable. Frequently these systems perform critical functions within the business (such as cash register, automated teller machine, and so on), making the need for visibility and control from configuration and security perspectives an absolute necessity.

Mobile devices have moved from a role of high-dollar phone to a mini-computer used for everything: Internet access, Global Positioning System (GPS) navigation, and storage for all manner of potentially sensitive business data. From the Chief Information Officer's perspective, ensuring that these devices are securely maintained (and appropriately password protected) is somewhat like gravity. It's more than a good idea—it's the law!

But seriously, as computing continues to evolve, and more devices release users from the strictures of office life, the problem only gets larger.

Timeliness of Asset Data

Maintaining a current picture of what is deployed and in use in your environment is a constant challenge due to the ever-increasing pace of change. However, failing to maintain an accurate snapshot of current conditions comes at a cost. In many organizations, this is a manual process involving Excel spreadsheets and custom scripting, and asset data is often obsolete by the time a single pass at the infrastructure is complete.

Without this data, organizations can over-purchase (or worse yet, under-purchase) software licensing. Having accurate asset information can help you get a better handle on your licensing costs. Likewise, without current configuration data, areas including Incident and Problem Management may suffer because troubleshooting incidents will be more error prone and time consuming.

Lack of Automation and Enforcement

With the perpetually increasing and evolving technology needs of the business, the need to automate resource provisioning, standardize, and enforce standard configurations becomes increasingly important.

Resource provisioning of new workstations or servers can be a very labor-intensive exercise. Installing a client OS and required applications may take a day or longer if performed manually. Ad-hoc scripting to automate these tasks can be a complex endeavor. Once deployed, ensuring the client and server configuration is consistent can seem an insurmountable task. With customer privacy and regulatory compliance at stake, consequences can be severe if this challenge is not met head on.

Proliferation of Virtualization

There's an old saying: *If you fail to plan, you plan to fail*. In no area of IT operations is this truer than when considering virtualization technologies.

When dealing with systems management, you have to consider many different functions, such as software and patch deployment, resource provisioning, and configuration management. Managing server and application configuration in an increasingly “virtual” world, where boundaries between systems and applications are not always clear, will require considering new elements of management not present in a purely physical environment.

Virtualization as a concept is very exciting to IT operations. Whether talking about virtualization of servers or applications, the potential for dramatic increases in process automation and efficiency and reduction in deployment costs is very real. New servers and applications can be provisioned in a matter of minutes. With this newfound agility comes a potential downside, which is the reality that virtualization can increase the velocity of change in your environment. The tools used to manage and track changes to a server often fail to address new dynamics that come when virtualization is introduced into a computing environment.

Many organizations make the mistake of taking on new tools and technologies in an ad-hoc fashion, without first reviewing them in the context of the process controls used to manage the introduction of change into the environment. These big gains in efficiency can lead to a completely new problem—inconsistencies in processes not designed to address the new dynamics that come with the virtual territory.

Lack of Process Consistency

Many IT organizations still “fly by the seat of their pants” when it comes to identifying and resolving problems. Using standard procedures and a methodology can help minimize risk and solve issues faster.

A *methodology* is a framework of processes and procedures used by those who work in a particular discipline. You can look at a methodology as a structured process defining the who, what, where, when, and why of one's operations, and the procedures to use when defining problems, solutions, and courses of action.

When employing a standard set of processes, it is important to ensure the framework you adopt adheres to accepted industry standards or best practices as well as takes into account the requirements of the business—ensuring continuity between expectations and the services delivered by the IT organization. Consistently using a repeatable and measurable set of practices allows an organization to quantify more accurately its progress to facilitate the adjustment of processes as necessary for improving future results. The most effective IT organizations build an element of self-examination into their service management strategy to ensure processes can be incrementally improved or modified to meet the changing needs of the business.

With IT's continually increased role in running successful business operations, having a structured and standard way to define IT operations aligned to the needs of the business is critical when meeting the expectations of business stakeholders. This alignment results in improved business relationships in which business units engage IT as a partner in developing and delivering innovations to drive business results.

The Bottom Line

Systems management can be intimidating when you consider the fact that the problems described to this point could happen even in an ostensibly “managed” environment. However, these examples just serve to illustrate that the very processes used to manage change in our environments must themselves be reviewed periodically and updated to accommodate changes in tools and technologies employed from the desktop to the datacenter.

Likewise, meeting the expectations of both the business and compliance regulation can seem an impossible task. At the end of the day, as technology evolves, so must IT's thinking, management tools, and processes. This makes it necessary to embrace continual improvement in those methodologies used to reduce risk while increasing agility in managing systems, keeping pace with the increasing velocity of change.

Systems Management Defined

Systems management is a journey, not a destination. That is to say, it is not something achieved at a point in time. Systems management encompasses all points in the IT service triangle, as displayed in Figure 1.1, including a set of processes and the tools and people that implement them. Although the role of each varies at different points within the IT service life cycle, the end goals do not change. How effectively these components are utilized determines the ultimate degree of success, which manifests itself in the outputs of productive employees producing and delivering quality products and services.

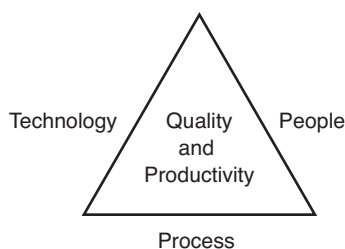


FIGURE 1.1 The IT service triangle includes people, process, and technology.

At a process level, systems management touches nearly *every* area of your IT operations. It can continually manage a computing resource, such as a client workstation, from the initial provisioning of the OS and hardware to end-of-life, when user settings are migrated

to a new machine. The hardware and software inventory data collected by your systems management solution can play a key role in incident and problem management, by providing information that facilitates faster troubleshooting.

As IT operations grow in size, scope, complexity, and business impact, the common denominator at all phases is efficiency and automation, based on repeatable processes that conform to industry best practices. Achieving this necessitates capturing subject matter expertise and business context into a repeatable, partially or fully automated process. At the beginning of the service life cycle is the service provisioning, which from a systems management perspective means OS and software deployment. Automation at this phase can save hours or days of manual deployment effort in each iteration.

After resources are in production, the focus expands to include managing and maintaining systems, via ongoing activities IT uses to manage the health and configuration of systems. These activities may touch areas such as configuration management, by monitoring for unwanted changes in standard system and application configuration baselines.

As the service life cycle continues, systems management can affect release management in the form of software upgrades. Activities include software-metering activities, such as reclaiming unused licenses for reuse elsewhere. If you are able to automate these processes to a great degree, you achieve higher reliability and security, greater availability, better asset allocation, and a more predictable IT environment. These translate into business agility, more efficient, less expensive operations, with a greater ability to respond quickly to changing conditions.

Reducing costs and increasing productivity in IT Service Management are important because efficiency in operations frees up money for innovation and product improvements. Information security is also imperative because the price tag of compromised systems and data recovery from security exposures can be large, and those costs continue to rise each year.

Microsoft's Strategy for Service Management

Microsoft utilizes a multifaceted approach to IT Service Management. This strategy includes advancements in the following areas:

- ▶ Adoption of a model-based management strategy (a component of the Dynamic Systems Initiative, discussed in the next section, "Microsoft's Dynamic Systems Initiative") to implement synthetic transaction technology. Configuration Manager 2007 delivers Service Modeling Language-based models in its Desired Configuration Management (DCM) feature, allowing administrators to define intended configurations.
- ▶ Using an Infrastructure Optimization (IO) Model as a framework for aligning IT with business needs and as a standard for expressing an organization's maturity in service management. The "Optimizing Your Infrastructure" section of this chapter discusses the IO Model further. The IO Model describes your IT infrastructure in terms of cost, security risk, and operational agility.

- ▶ Supporting a standard Web Services specification for system management. WS-Management is a specification of a SOAP-based protocol, based on Web Services, used to manage servers, devices, and applications (SOAP stands for *Simple Object Access Protocol*). The intent is to provide a universal language that all types of devices can use to share data about themselves, which in turn makes them more easily managed. Support for WS-Management is included with Windows Vista and Windows Server 2008, and will ultimately be leveraged by multiple System Center components (beginning with Operations Manager 2007).
- ▶ Integrating infrastructure and management into OS and server products, by exposing services and interfaces that management applications can utilize.
- ▶ Building complete management solutions on this infrastructure, either through making them available in the operating system or by using management products such as Configuration Manager, Operations Manager, and other components of the System Center family.
- ▶ Continuing to drive down the complexity of Windows management by providing core management infrastructure and capabilities in the Windows platform itself, thus allowing business and management application developers to improve their infrastructures and capabilities. Microsoft believes that improving the manageability of solutions built on Windows Server System will be a key driver in shaping the future of Windows management.

Microsoft's Dynamic Systems Initiative

A large percentage of IT departments' budgets and resources typically focuses on mundane maintenance tasks such as applying software patches or monitoring the health of a network, without leaving the staff with the time or energy to focus on more exhilarating (and more productive) strategic initiatives.

The Dynamic Systems Initiative, or DSI, is a Microsoft and industry strategy intended to enhance the Windows platform, delivering a coordinated set of solutions that simplifies and automates how businesses design, deploy, and operate their distributed systems. Using DSI helps IT and developers create operationally aware platforms. By designing systems that are more manageable and automating operations, organizations can reduce costs and proactively address their priorities.

DSI is about building software that enables knowledge of an IT system to be created, modified, transferred, and operated on throughout the life cycle of that system. It is a commitment from Microsoft and its partners to help IT teams capture and use knowledge to design systems that are more manageable and to automate operations, which in turn reduce costs and give organizations additional time to focus proactively on what is most important. By innovating across applications, development tools, the platform, and management solutions, DSI will result in

- ▶ Increased productivity and reduced costs across all aspects of IT;
- ▶ Increased responsiveness to changing business needs;

- ▶ Reduced time and effort required to develop, deploy, and manage applications.

Microsoft is positioning DSI as the connector of the entire system and service life cycles.

Microsoft Product Integration

DSI focuses on automating datacenter operational jobs and reducing associated labor through self-managing systems. Here are several examples where Microsoft products and tools integrate with DSI:

- ▶ Configuration Manager employs model-based configuration baseline templates in its Desired Configuration Management feature to automate identification of undesired shifts in system configurations.
- ▶ Visual Studio is a model-based development tool that leverages SML, enabling operations managers and application architects to collaborate early in the development phase and ensure applications are modeled with operational requirements in mind.
- ▶ Windows Server Update Services (WSUS) enables greater and more efficient administrative control through modeling technology that enables downstream systems to construct accurate models representing their current state, available updates, and installed software.

NOTE

SDM and SML—What's the Difference?

Microsoft originally used the System Definition Model (SDM) as its standard schema with DSI. SDM was a proprietary specification put forward by Microsoft. The company later decided to implement SML, which is an industrywide published specification used in heterogeneous environments. Using SML helps DSI adoption by incorporating a standard that Microsoft's partners can understand and apply across mixed platforms. Service Modeling Language is discussed later in the section "The Role of Service Modeling Language in IT Operations."

DSI focuses on automating datacenter operations and reducing total cost of ownership (TCO) through self-managing systems. Can logic be implemented in management software so that the management software can identify system or application issues in real time and then dynamically take actions to mitigate the problem? Consider the scenario where, without operator intervention, a management system moves a virtual machine running a line-of-business application because the existing host is experiencing an extended spike in resource utilization. This is actually a reality today, delivered in the quick migration feature of Virtual Machine Manager 2008; DSI aims to extend this type of self-healing and self-management to other areas of operations.

In support of DSI, Microsoft has invested heavily in three major areas:

- ▶ **Systems designed for systems management**—Microsoft is delivering development and authoring tools—such as Visual Studio—that enable businesses to capture

the knowledge of everyone from business users and project managers to the architects, developers, testers, and operations staff using models. By capturing and embedding this knowledge into the infrastructure, organizations can reduce support complexity and cost.

- ▶ **An operationally aware platform**—The core Windows operating system and its related technologies are critical when solving everyday operational and service challenges. This requires designing the operating system services for manageability. Additionally, the operating system and server products must provide rich instrumentation and hardware resource virtualization support.
- ▶ **Virtualized applications and server infrastructure**—Virtualization of servers and applications improves the agility of the organization by simplifying the effort involved in modifying, adding, or removing the resources a service utilizes in performing work.

NOTE

The Microsoft Suite for IT Operations

End-to-end automation could include update management, availability and performance monitoring, change and configuration management, and rich reporting services. Microsoft's System Center is a family of system management products and solutions that focuses on providing you with the knowledge and tools to manage your IT infrastructure. The objective of the System Center family is to create an integrated suite of systems management tools and technologies, thus helping to ease operations, reduce troubleshooting time, and improve planning capabilities.

The Importance of DSI

There are three architectural elements behind the DSI initiative:

- ▶ That developers have tools (such as Visual Studio) to design applications in a way that makes them easier for administrators to manage after those applications are in production
- ▶ That Microsoft products can be secured and updated in a uniform way
- ▶ That Microsoft server applications are optimized for management, to take advantage of Operations Manager 2007

DSI represents a departure from the traditional approach to systems management. DSI focuses on designing for operations from the application development stage, rather than a more customary operations perspective that concentrates on automating task-based processes. This strategy highlights the fact that Microsoft's Dynamic Systems Initiative is about building software that enables knowledge of an IT system to be created, modified, transferred, and used throughout the life cycle of a system. DSI's core principles of knowledge, models, and the life cycle are key in addressing the challenges of complexity and manageability faced by IT organizations. By capturing knowledge and incorporating health models, DSI can facilitate easier troubleshooting and maintenance, and thus lower TCO.

The Role of Service Modeling Language in IT Operations

A key underlying component of DSI is the XML-based specification called the Service Modeling Language (SML). SML is a standard developed by several leading information technology companies that defines a consistent way for infrastructure and application architects to define how applications, infrastructure, and services are modeled in a consistent way.

SML facilitates modeling systems from a development, deployment, and support perspective with modular, reusable building blocks that eliminate the need to reinvent the wheel when describing and defining a new service. The end result is systems that are easier to develop, implement, manage, and maintain, resulting in reduced TCO to the organization. SML is a core technology that will continue to play a prominent role in future products developed to support the ongoing objectives of DSI.

NOTE

SML Resources on the Web

For more information on Service Modeling Language, view the latest draft of the SML standard at <http://www.w3.org/TR/sml/>. For additional technical information on SML from Microsoft, see <http://technet.microsoft.com/en-us/library/bb725986.aspx>.

IT Infrastructure Library (ITIL) and Microsoft Operations Framework (MOF)

ITIL is widely accepted as an international standard of best practices for operations management, and Microsoft has used ITIL v3 as the basis for Microsoft Operations Framework (MOF) v4, the current version of its own operations framework. Warning: Fasten your seatbelt, because this is where the fun really begins!

What Is ITIL?

As part of Microsoft's management approach, the company relied on an international standards-setting body as its basis for developing an operational framework. The British Office of Government Commerce (OGC) provides best-practices advice and guidance on using Information Technology in service management and operations. The OGC also publishes the IT Infrastructure Library, known as *ITIL*.

ITIL provides a cohesive set of best practices for IT Service Management (ITSM). These best practices include a series of books giving direction and guidance on provisioning quality IT services and facilities needed to support Information Technology. The documents are maintained by the OGC and supported by publications, qualifications, and an international users group.

Started in the 1980s, ITIL is under constant development by a consortium of industry IT leaders. The ITIL covers a number of areas and is primarily focused on ITSM; its IT Infrastructure Library is considered to be the most consistent and comprehensive documentation of best practices for IT Service Management worldwide.

ITSM is a business-driven, customer-centric approach to managing Information Technology. It specifically addresses the strategic business value generated by IT and the need to deliver high-quality IT services to one's business organization. ITSM itself has two main components:

- ▶ Service support
- ▶ Service delivery

A New Version of ITIL

ITIL has recently undergone a refresh, and the core books for version 3 (ITIL v3) were published on June 30, 2007. The major difference between v3 and its v2 predecessor is that v3 has adopted an integrated service life cycle approach to IT Service Management, as opposed to organizing itself around the concepts of IT service delivery and support.

ITIL v2 was a more targeted product, explicitly designed to bridge the gap between technology and business, with a strong process focus on effective service support and delivery. The v3 documents recognize the new service management challenges brought about by advancements in technology, such as virtualization and outsourcing, as well as emerging challenges for service providers.

The framework has been repositioned from its previous emphasis on the process life cycle and alignment of IT to an emphasis on “the business” (that is, managing the life cycle of the services provided by IT and the importance of creating business value rather than just the execution of processes). As an example, it is a publicly stated aim of the refresh to include more references to return on investment (ROI).

There are five core volumes of ITIL v3:

- ▶ **Service Strategy**—This volume identifies market opportunities for which services could be developed to meet a requirement on the part of internal or external customers. Key areas here are Service Portfolio Management and Financial Management.
- ▶ **Service Design**—This volume focuses on the activities that take place to develop the strategy into a design document that addresses all aspects of the proposed service and the processes intended to support it. Key areas of this volume are Availability Management, Capacity Management, Continuity Management, and Security Management.
- ▶ **Service Transition**—This volume centers on implementing the output of service design activities and creating a production service (or modifying an existing service). There is some overlap between Service Transition and Service Operation, the next volume. Key areas of the Service Transition volume are Change Management, Release Management, Configuration Management, and Service Knowledge Management.
- ▶ **Service Operation**—This volume involves the activities required to operate the services and maintain their functionality as defined in Service Level Agreements (SLAs) with one's customers. Key areas here are Incident Management, Problem Management, and Request Fulfillment.

- **Continual Service Improvement**—This volume focuses on the ability to deliver continual improvement to the quality of the services that the IT organization delivers to the business. Key areas include Service Reporting, Service Measurement, and Service Level Management.

ITIL v3 really is a repackaging of what was in v2, with an additional layer of abstraction.

Philosophically speaking, ITSM focuses on the customer's perspective of IT's contribution to the business, which is analogous to the objectives of other frameworks in terms of their consideration of alignment of IT service support and delivery with business goals in mind.

Although ITIL describes the what, when, and why of IT operations, it stops short of describing how a specific activity should be carried out. A driving force behind its development was the recognition that organizations are increasingly dependent on IT for satisfying their corporate objectives relating to both internal and external customers, which increases the requirement for high-quality IT services. Many large IT organizations realize that the road to a customer-centric service organization runs along an ITIL framework.

ITIL also specifies keeping measurements or metrics to assess performance over time. Measurements can include a variety of statistics, such as the number and severity of service outages, along with the amount of time it takes to restore service. These metrics can be used to quantify to management how well IT is performing. This information can be particularly useful for justifying resources during the next budget process!

What Is MOF?

ITIL is generally accepted as the “best practices” for the industry. Being technology-agnostic, it is a foundation that can be adopted and adapted to meet the specific needs of various IT organizations. Although Microsoft chose to adopt ITIL as a standard for its own IT operations for its *descriptive* guidance, Microsoft designed MOF to provide *prescriptive* guidance for effective design, implementation, and support of Microsoft technologies.

MOF is a set of publications providing both descriptive (what to do, when and why) and prescriptive (how to do) guidance on IT Service Management. The key focus in developing MOF was providing a framework specifically geared toward managing Microsoft technologies. Microsoft created the first version of the MOF in 1999. The latest iteration of MOF (version 4) is designed to further

- Update MOF to include the full end-to-end IT service life cycle;
- Let IT governance serve as the foundation of the life cycle;
- Provide useful, easily consumable best practice-based guidance;
- Simplify and consolidate service management functions (SMFs), emphasizing workflows, decisions, outcomes, and roles.

MOF is designed to complement Microsoft's previously existing Microsoft Solutions Framework (MSF), which provides guidance for application development solutions.

Together, the combined frameworks provide guidance throughout the IT life cycle, as shown in Figure 1.2.

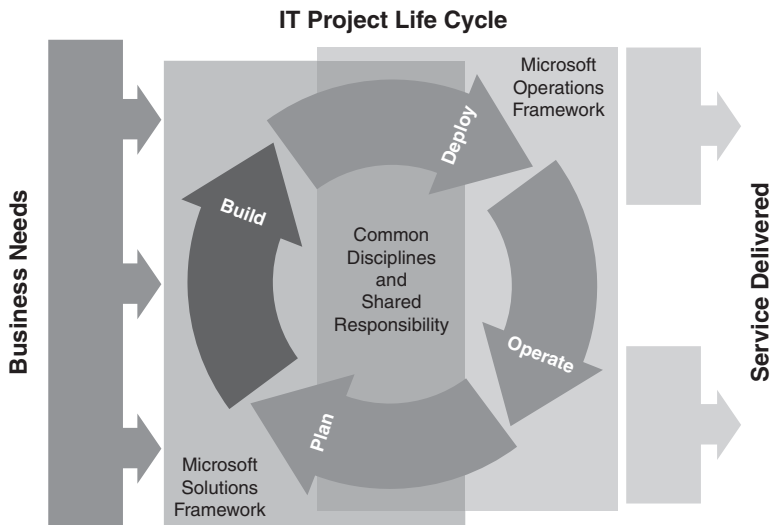


FIGURE 1.2 The IT life cycle and Microsoft frameworks

TIP

Using MSF for ConfigMgr Deployment

Microsoft uses MOF to describe IT operations and uses Configuration Manager as a tool to put that framework into practice. However, Configuration Manager 2007 is also an application and, as such, is best deployed using a disciplined approach. Although MSF is geared toward application development, it can be adapted to support infrastructure solution design and deployment, as discussed in Chapter 4, "Configuration Manager Solution Design."

At its core, the MOF is a collection of best practices, principles, and models. It provides direction to achieve reliability, availability, supportability, and manageability of mission-critical production systems, focusing on solutions and services using Microsoft products and technologies. MOF extends ITIL by including guidance and best practices derived from the experience of Microsoft's internal operations groups, partners, and customers worldwide. MOF aligns with and builds on the IT Service Management practices documented within ITIL, thus enhancing the supportability built on Microsoft's products and technologies.

MOF uses a process model that describes Microsoft's approach to IT operations and the service management life cycle. The model organizes the core ITIL processes of service

support and service delivery, and it includes additional MOF processes in the four quadrants of the MOF process model, as illustrated in Figure 1.3.

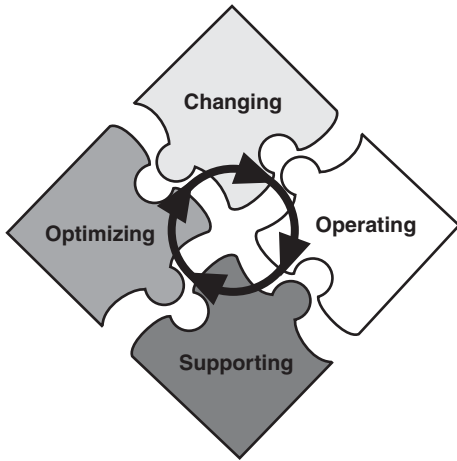


FIGURE 1.3 The MOF process model

It is important to note that the activities pictured in the quadrants illustrated in Figure 1.3 are not necessarily sequential. These activities can occur simultaneously within an IT organization. Each quadrant has a specific focus and tasks, and within each quadrant are policies, procedures, standards, and best practices that support specific operations management-focused tasks.

Configuration Manager 2007 can be employed to support operations management tasks in different quadrants of the MOF Process Model. Let's look briefly at each of these quadrants and see how one can use ConfigMgr to support MOF:

- **Changing**—This quadrant represents instances where new service solutions, technologies, systems, applications, hardware, and processes have been introduced.

The software and OS deployment features of ConfigMgr can be used to automate many activities in the Changing quadrant.

- **Operating**—This quadrant concentrates on performing day-to-day tasks efficiently and effectively.

ConfigMgr includes many operational tasks that you can initiate from the Configuration Manager console, or that can be automated completely. These are available through various product components, such as update management and software deployment features. The Network Access Protection feature can be utilized to verify clients connecting to the network meet certain corporate criteria, such as antivirus software signatures, before being granted full access to resources.

- **Supporting**—This quadrant represents the resolution of incidents, problems, and inquiries, preferably in a timely manner.

Using the Desired Configuration Management feature of ConfigMgr in conjunction with software deployment, widespread shifts in system configurations can be identified and reversed with a minimum of effort.

- **Optimizing**—This quadrant focuses on minimizing costs while optimizing performance, capacity, and availability in the delivery of IT services.

ConfigMgr reporting delivers in a number of functional areas of IT operations. For example, out of the box reports provide instant insight into hardware readiness for operating system deployment to help minimize the hands-on aspects of hardware assessment in upgrade planning. In conjunction with the software metering and asset intelligence features of Configuration Manager, reports can provide insight into unused software licenses that can be reclaimed for use elsewhere.

Service Level Agreements and Operating Level Agreements (OLAs) are tools many organizations use in defining accepted levels of operation and ability. Configuration Manager includes the ability to schedule software and update deployment, as well as to define maintenance windows in support of SLAs and OLAs.

Additional information regarding the MOF Process Model is available at <http://go.microsoft.com/fwlink/?LinkId=50015>.

MOF Does Not Replace ITIL

Microsoft believes that ITIL is the leading body of knowledge of best practices; for that reason, it uses ITIL as the foundation for MOF. Rather than replacing ITIL, MOF complements it and is similar to ITIL in several ways:

- MOF (with MSF) spans the entire IT life cycle.
- Both MOF and ITIL are based on best practices for IT management, drawing on the expertise of practitioners worldwide.
- The MOF body of knowledge is applicable across the business community—from small businesses to large enterprises. MOF also is not limited only to those using the Microsoft platform in a homogenous environment.
- As is the case with ITIL, MOF has expanded to be more than just a documentation set. In fact, MOF is now intertwined with another System Center component, Operations Manager 2007!

Additionally, Microsoft and its partners provide a variety of resources to support MOF principles and guidance, including self-assessments, IT management tools that incorporate MOF terminology and features, training programs and certification, and consulting services.

Service Management Mastery: ISO 20000

You can think of ITIL and ITSM as providing a framework for IT to rethink the ways in which it contributes to and aligns with the business. ISO 20000, which is the first international standard for IT Service Management, institutionalizes these processes. ISO 20000 helps companies to align IT services and business strategy, to create a formal framework

for continual service improvement, and provides benchmarks for comparison to best practices.

Published in December 2005, ISO 20000 was developed to reflect the best-practice guidance contained within ITIL. The standard also supports other IT Service Management frameworks and approaches, including MOF, Capability Maturity Model Integration (CMMi) and Six Sigma. ISO 20000 consists of two major areas:

- ▶ Part 1 promotes adopting an integrated process approach to deliver managed services effectively that meets business and customer requirements.
- ▶ Part 2 is a “code of practice” describing the best practices for service management within the scope of ISO 20000-1.

These two areas—what to do and how to do it—have similarities to the approach taken by the other standards, including MOF.

ISO 20000 goes beyond ITIL, MOF, Six Sigma, and other frameworks in providing organizational or corporate certification for organizations that effectively adopt and implement the ISO 20000 code of practice.

TIP

About CMMi and Six Sigma

CMMi is a process-improvement approach that provides organizations with the essential elements of effective processes. It can be used to guide process improvement—across a project, a division, or an entire organization—thus helping to integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes.

Six Sigma is a business management strategy, originally developed by Motorola, which seeks to identify and remove the causes of defects and errors in manufacturing and business processes.

Optimizing Your Infrastructure

According to Microsoft, analysts estimate that over 70% of the typical IT budget is spent on infrastructure—managing servers, operating systems, storage, and networking. Add to that the challenge of refreshing and managing desktop and mobile devices, and there's not much left over for anything else. Microsoft describes an Infrastructure Optimization Model that categorizes the state of one's IT infrastructure, describing the impacts on cost, security risks, and the ability to respond to changes. Using the model shown in Figure 1.4, you can identify where your organization is, and where you want to be:

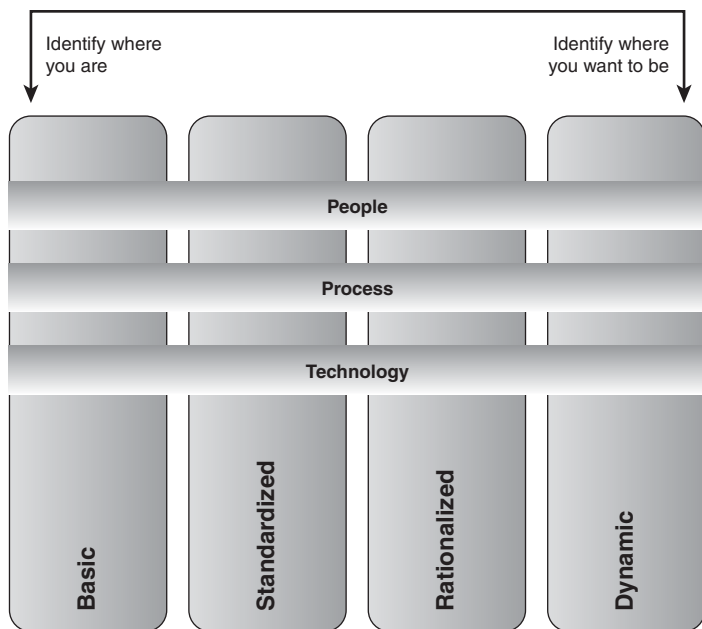


FIGURE 1.4 The Infrastructure Optimization Model

- ▶ **Basic**—Reactionary, with much time spent fighting fires
- ▶ **Standardized**—Gaining control
- ▶ **Rationalized**—Enabling the business
- ▶ **Dynamic**—Being a strategic asset

Although most organizations are somewhere between the basic and standardized levels in this model, typically one would prefer to be a strategic asset rather than fighting fires. Once you know where you are in the model, you can use best practices from ITIL and guidance from MOF to develop a plan to progress to a higher level. The IO Model describes the technologies and steps organizations can take to move forward, whereas the MOF explains the people and processes required to improve that infrastructure. Similar to ITSM, the IO Model is a combination of people, processes, and technology.

More information about Infrastructure Optimization is available at <http://www.microsoft.com/technet/infrastructure>.

About the IO Model

Not all IT shops will want or need to be dynamic. Some will choose, for all the right business reasons, to be less than dynamic! The IO Model includes a three-part goal:

- ▶ Communicate that there are levels.
- ▶ Target the desired levels.

- Provide reference on how to get to the desired levels.

Realize that infrastructure optimization can be by application or by function, rather than a single ranking for the entire IT department.

Items that factor into an IT organization's adoption of the IO model include cost, ability, and whether the organization fits into the business model as a cost center versus being an asset, along with a commitment to move from being reactive to proactive.

1

From Fighting Fires to Gaining Control

At the Basic level, your infrastructure is hard to control and expensive to manage. Processes are manual, IT policies and standards are either nonexistent or not enforced, and you don't have the tools and resources (or time and energy) to determine the overall health of your applications and IT services. Not only are your desktop and server management costs out of control, but you are in reactive mode when it comes to security threats. In addition, you tend to use manual rather than automated methods for applying software deployments and patches. To try to put a bit of humor into this, you could say that computer management has you all tied up, like the system administrator shown in Figure 1.5.

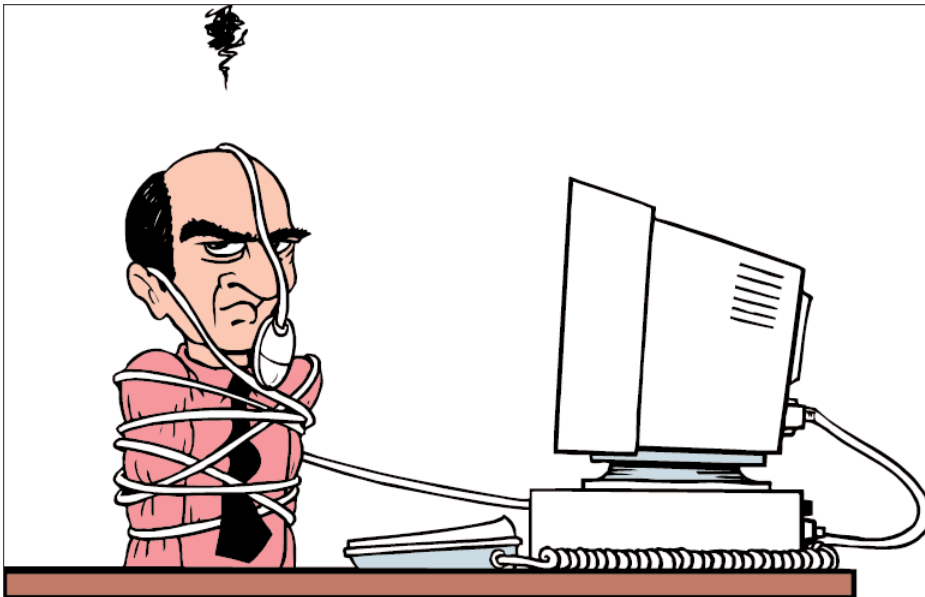


FIGURE 1.5 The Basic level can leave you feeling tied up in knots.

Does this sound familiar? If you can gain control of your environment, you may be more effective at work! Here are some steps to consider:

- Develop standards, policies, and controls.

- ▶ Alleviate security risks by developing a security approach throughout your IT organization.
- ▶ Adopt best practices, such as those found in ITIL, and operational guidance found in MOF.
- ▶ Build IT to become a strategic asset.

If you can achieve operational nirvana, this will go a long way toward your job satisfaction and IT becoming a constructive part of your business.

From Gaining Control to Enabling the Business

A Standardized infrastructure introduces control by using standards and policies to manage desktops and servers. These standards control how you introduce machines into your network. As an example, using Directory Services will manage resources, security policies, and access to resources. Shops in a Standardized state realize the value of basic standards and some policies, but still tend to be reactive. Although you now have a managed IT infrastructure and are inventorying your hardware and software assets and starting to manage licenses, your patches, software deployments, and desktop services are not yet automated. Security-wise, the perimeter is now under control, although internal security may still be a bit loose.

To move from a Standardized state to the Rationalized level, you will need to gain more control over your infrastructure and implement proactive policies and procedures. You might also begin to look at implementing service management. At this stage, IT can also move more toward becoming a business asset and ally, rather than a burden.

From Enabling the Business to Becoming a Strategic Asset

At the Rationalized level, you have achieved firm control of desktop and service management costs. Processes and policies are in place and beginning to play a large role in supporting and expanding the business. Security is now proactive, and you are responding to threats and challenges in a rapid and controlled manner.

Using technologies such as lite-touch and zero-touch operating system deployment helps you to minimize costs, deployment time, and technical challenges for system rollouts. Because your inventory is now under control, you have minimized the number of images to manage, and desktop management is now largely automated. You also are purchasing only the software licenses and new computers the business requires, giving you a handle on costs. Security is now proactive with policies and control in place for desktops, servers, firewalls, and extranets.

Mission Accomplished: IT as a Strategic Asset

At the Dynamic level, your infrastructure is helping run the business efficiently and stay ahead of competitors. Your costs are now fully controlled. You have also achieved integration between users and data, desktops and servers, and the different departments and functions throughout your organization.

Your Information Technology processes are automated and often incorporated into the technology itself, allowing IT to be aligned and managed according to business needs.

New technology investments are able to yield specific, rapid, and measurable business benefits. Measurement is good—it helps you justify the next round of investments!

Using self-provisioning software and quarantine-like systems to ensure patch management and compliance with security policies allows you to automate your processes, which in turn improves reliability, lowers costs, and increases your service levels.

According to IDC research, very few organizations achieve the Dynamic level of the Infrastructure Optimization Model—due to the lack of availability of a single toolset from a single vendor to meet all requirements. Through execution on its vision in DSI, Microsoft aims to change this. To read more on this study, visit http://download.microsoft.com/download/a/4/4/a4474b0c-57d8-41a2-afe6-32037fa93ea6/IDC_windesktop_IO_whitepaper.pdf.

Relating the IO Model to Desktop Management

The June 2008 issue of *Redmond Magazine* includes an article by Greg Shields titled “5 Rules for Managing User Desktops.” Greg makes the following points:

- ▶ If you leave any component of desktop management to the user, you are no longer managing that machine—abdicating responsibility means you are effectively rescinding proactive control over that environment you are supposed to control and manage.
- ▶ Never interrupt the user’s workflow—only distribute software and patches when users are logged out of their workstations.
- ▶ Never ask for the user’s opinion when it comes to desktop management—giving users choices is often giving them enough rope to hang themselves.
- ▶ Computing equipment belongs to the business, not IT and not the user.
- ▶ Moving desktop management from reactive to proactive can initially involve quite a bit of work—jumping from firefighting to measured and calculated change requires a systems management toolset to help with automating tasks, and you will need the knowledge and experience to implement broad changes with minimal impact.

You can read Greg’s article in full at <http://redmondmag.com/columns/article.asp?editorialsid=2635>.

Bridging the Systems Management Gap

System Center Configuration Manager 2007 is Microsoft’s software platform for addressing systems management issues. It is a key component in Microsoft’s management strategy and System Center that can be utilized to bridge many of the gaps in service support and delivery. Configuration Manager 2007 was designed around four key themes:

- ▶ **Security**—ConfigMgr delivers numerous security enhancements over its predecessor, such as the mutual authentication of native mode and Network Access Protection (NAP), which in conjunction with the NAP feature available with Windows 2008 protects assets connecting to the network by enforcing compliance with system health requirements such as antivirus version.

- ▶ **Simplicity**—ConfigMgr delivers a simplified user interface with fewer top-level icons, organized in a way that makes resources easier to locate. Investments in simplicity have been made throughout the user interface (UI) in several features, such as the simplified wizard-based UI and common rule templates in DCM 2.0. Such improvements are also evident in the areas of software deployment and metering, as well as OS deployment. Improvements in branch office support also serve to not only simplify management of the branch office, but also reduce ConfigMgr infrastructure costs in these scenarios.
- ▶ **Manageability**—Some of the most important improvements in ConfigMgr come in the form of manageability improvements in common “fringe” scenarios where bandwidth or connectivity are in short supply. Offline OS and driver packages can now be created to support OS deployment in scenarios with no or low-bandwidth connectivity. Native Wake On LAN support makes patching workstation after hours a more hands-off scenario. Internet-Based Client Management (ICBM) is now a reality, providing management for remote clients not connected to the corporate network. Finally, the update management feature of ConfigMgr supports scans the WSUS Server as opposed to distributing a local copy of the catalog to each client.
- ▶ **Operating system deployment**—Systems Management Server (SMS) 2003’s OS deployment feature (OSD) has been integrated into the product, and Microsoft investments in this area have made the feature truly enterprise-ready. For instance, OSD now supports both client and server OS deployment from the same interface, eliminating the need for a separate tool for server deployment.

The driver catalog feature available with OS deployment eliminates the need for a separate OS image for each driver set. Likewise, the task sequencer accommodates configuration of software deployment in conjunction with OS deployment through a wizard more easily than ever before.

Additionally, OEM and offline scenarios are now fully supported through OS deployment using removable media.

Central Control in the Distributed Enterprise

While centralized management and visibility are benefits of the platform, ConfigMgr 2007 employs a distributed architecture that delivers an agent-based solution. This brings numerous advantages:

- ▶ Once client policy is passed to the ConfigMgr client by the management point, data collection is managed locally on each managed computer, which distributes the load of collecting and handling information. This type of distributed management offers a clear scalability advantage, in that the load on the ConfigMgr server roles is greatly reduced. From the perspective of network load, because all the script execution,

Windows Management Instrumentation (WMI) calls, and such are local to the client, network traffic is reduced as well.

Data is then passed from the ConfigMgr client back to the management point and is ultimately inserted into the site database, and can then be viewed through the ConfigMgr console.

- ▶ A distributed model also enables fault tolerance and flexibility in the event of interruptions in network connectivity. If the network is unavailable, the local client agents still collect information. This model also reduces the impact of data collection on the network by forwarding only information that needs forwarding.
- ▶ With a distributed server topology that allows clients to connect to the ConfigMgr server in their local site, clients can access resources no matter where they may roam. This model can reduce response time and improve compliance in a large enterprise, where a traveling client might otherwise attempt to pull software across a slow wide area network (WAN) link, or even require manual intervention to receive needed software applications or updates.

The functionality implemented at the ConfigMgr client is determined by the client agents that are enabled for that client. There are 10 client agents, each of which delivers a subset of ConfigMgr functionality. The client agents, displayed in Figure 1.6, include the following:

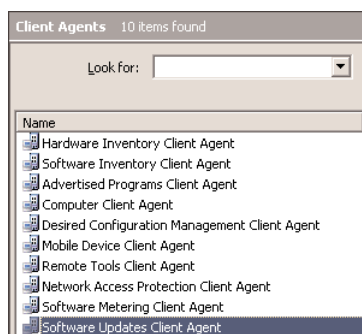


FIGURE 1.6 Client agents available in the ConfigMgr Setup Wizard

- ▶ Hardware Inventory
- ▶ Software Inventory
- ▶ Advertised Programs
- ▶ Computer

- ▶ Desired Configuration Management
- ▶ Mobile Device
- ▶ Remote Tools
- ▶ Network Access Protection
- ▶ Software Metering
- ▶ Software Updates

Data is forwarded from the client to the ConfigMgr site server, which inserts data into the ConfigMgr database. From here, data is available for use in a variety of reporting and filtering capacities, allowing granular customization in terms of how data is presented to administrators in the Configuration Manager console.

Automation and Control

In an environment with hundreds or even thousands of client and server systems, automating common software provisioning activities becomes a critical component to business agility. Productivity suffers when resources cannot be deployed in a timely manner with a consistent and predictable configuration. Once resources are deployed, ensuring systems are maintained with a consistent and secure configuration can be not only of operational importance, but of legal importance as well. ConfigMgr has several features to address the layers of process automation required to provision and maintain systems in a distributed enterprise. The following sections peel back the layers to explore common issues in each phase and examine how ConfigMgr 2007 addresses them.

Software Deployment

One process frequently automated in large IT environments is software deployment. Software deployment can be a time-consuming process, and automating the installation or upgrade of applications such as the Microsoft Office suite can be a huge timesaver. What is perhaps most impressive about the software deployment capabilities of ConfigMgr is the flexibility and control the administrator has in determining what software to deploy, to whom it is deployed, and how it is presented. The software deployment capabilities of ConfigMgr include a range of options, such as the ability to advertise a software package for installation at the user's option and to assign and deploy by a target deadline. The feature handles software upgrades as easily as new deployments, making that Office 2007 upgrade much less laborious.

Let's take software deployment a step further. Have you ever asked yourself, "Who is actually using application X among the users for whom it is installed?" Well, by using the software metering functionality in ConfigMgr, it is possible to report on instances of a particular application that have not been used in a certain period of time. This allows administrators to reclaim unused licenses for reuse elsewhere, saving the organization money on software licensing.

In ConfigMgr 2007 Release 2 (R2), software deployment takes another leap forward with adding support for deployment of virtual applications (using Microsoft Application

Virtualization version 4.5) to ConfigMgr clients from the ConfigMgr distribution points. You can read a detailed accounting of software deployment in ConfigMgr in Chapter 14, “Distributing Packages.”

Operating System Deployment

If manually deploying applications is painful from a time perspective, operating system deployment would be excruciating. You can move a step beyond software deployment to operating system deployment in ConfigMgr, which allows configuring of the automated deployment for both the client and server OS using the same interface in the Configuration Manager console.

One of the most common areas of complexity in OS deployment is device drivers. In the past, drivers have forced administrators to maintain multiple OS images, each image containing the drivers for a particular system manufacturer and model. OS deployment in ConfigMgr 2007 introduces a new feature called *driver catalogs*. Using driver catalogs lets you maintain a single OS image. Here's how it works: A scan of driver catalogs is performed at runtime to identify and extract the appropriate drivers for a target system. This allows the teams responsible for desktop and server deployment to maintain a single golden OS image along with multiple driver catalogs for the various hardware manufacturers and systems models. There are some limitations here, which are discussed in Chapter 19, “Operating System Deployment.”

Task sequences take automation of OS and software deployment yet one step further, allowing administrators, through a relatively simple wizard interface, to define a sequence of actions, incorporating both OS and software deployment activities into an ordered sequence of events. This enables nearly full automation of the resource-provisioning process.

While on the topic, the value of task sequences in advertisements is often overlooked. Task sequences can be deployed as advertisements, allowing administrators to control the order of software distribution and reboot handling, and as diagnostic actions to analyze and respond to those systems with configurations out of compliance with corporate standards.

A detailed walkthrough of operating system deployment in ConfigMgr is included in Chapter 19.

Compliance and Enforcement

Once you automate the provisioning process, what can be done to ensure system configurations remain consistent with corporate standards throughout the environment? With the proliferation of legislated regulatory requirements, ensuring configurations meet a certain standard is critical. The fines levied against an organization for noncompliance and breaching these requirements when sensitive client data is involved can be quite costly. This is an area that cannot be addressed by simple hardware and software inventory, making visibility in this area historically quite challenging. This is where the new Desired Configuration Management feature of ConfigMgr comes into play.

DCM allows administrators to define a list of desired settings (called *configuration items*) into a group of desired settings for a particular set of target systems. This is known as a

configuration baseline. To facilitate faster adoption, Microsoft provides predefined configuration baselines (templates, so to speak) called *configuration packs*, available as free downloads from Microsoft's website at <http://technet.microsoft.com/en-us/configmgr/cc462788.aspx>. Microsoft provides configuration packs as a starting point to help organizations evaluate Microsoft server applications against Microsoft best practices or regulatory compliance requirements, such as Sarbanes-Oxley or HIPAA.

With DCM reports (available by default), administrators can identify systems that have “drifted” out of compliance and take corrective action. Although there is no automated enforcement functionality in this version of DCM, noncompliant systems can be dynamically grouped in a collection and then targeted for software deployment, providing some measure of automation in bringing systems back into compliance.

You can read more about Desired Configuration Management in ConfigMgr in Chapter 16, “Desired Configuration Management.”

Securing Systems

The update management and network access protection features in ConfigMgr provide a platform for securing clients more effectively than ever before. The following sections discuss these capabilities.

Update Management

Microsoft overhauled the entire patch management process for ConfigMgr 2007, and the product uses WSUS 3.0 as its base technology for patch distribution to clients. However, ConfigMgr extends native WSUS capabilities, grouping clients based on user-defined criteria (in collections) and updates, as well as scheduling update packages of desired patches, providing more control than with WSUS alone. Using the maintenance window feature of ConfigMgr, you can define a window of time during which a particular group of clients should receive updates, thus ensuring the application of updates does not interrupt normal business. Microsoft recommends a four-phase patch management process to ensure your environment is appropriately secured (see Figure 1.7). You can read more about update management in ConfigMgr in Chapter 15, “Patch Management.”

Internet Client Management

Many organizations have client machines, such as those belonging to sales staff working remotely, that rarely access the corporate network and make timely application of updates to the OS and applications very challenging. Using the Internet-Based Client Management feature in ConfigMgr in conjunction with an Internet-based management point, you can still deliver updates to clients that never attach to the corporate network. This ensures that clients outside the intranet on the local area network maintain patch levels similar to clients inside the network.

However, when Internet-based clients do attach to the trusted network, updates can resume seamlessly on the intranet. This intelligent roaming capability works in both directions, allowing clients to move seamlessly between Internet and intranet connectivity.

You can read more on IBCM in ConfigMgr in Chapter 6, “Architecture Design Planning.”

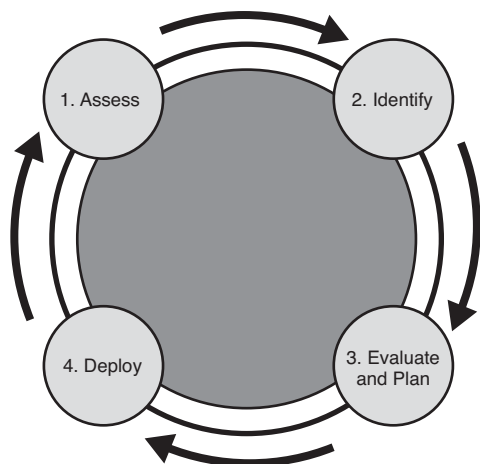


FIGURE 1.7 Microsoft's recommended four-phase update management process

Securing Remote Access Clients

As the saying goes, “one rotten apple can spoil the barrel.” To that effect, clients connecting to the corporate network with computers that are not appropriately patched or perhaps not running antivirus software are always a concern. When integrated with the Network Access Protection functionality delivered in Windows Server 2008, the NAP feature in ConfigMgr can help IT administrators dynamically control the access of clients that do not meet corporate standards for patch levels, in addition to antivirus and other standard configurations.

NAP allows network administrators to define granular levels of network access based on who a client is, the groups to which the client belongs, and the degree to which that client is compliant with corporate governance policy. Here's how it works: If a client is not compliant, NAP provides a policy mechanism to compare client settings to corporate standard settings, and then automatically restricts the noncompliant client to a quarantine network where resources can be used to bring the client back into compliance, thus dynamically increasing its level of network access as the required configuration criteria are met.

Chapter 15 provides additional information about Network Access Protection.

Visibility

You cannot use information you cannot see. The ability to view the state and status of both the resources and processes in your environment is a critical component of IT operations because it helps to understand where attention is needed. One of the most powerful aspects of the Configuration Manager console (a Microsoft Management Console [MMC] 3.0 application) in ConfigMgr 2007 is the visibility it brings to all status of software, OS and update deployment, and inventory and configuration compliance of client agents deployed in the environment.

Home Pages

The *home pages* capability provides at-a-glance status of software deployment progress, application of patches, and so on. Each of the root nodes in the Configuration Manager console provides a home page displaying the status of activity related to that particular feature. For example, the Software Updates home page, shown in Figure 1.8, displays the progress of patch distribution.

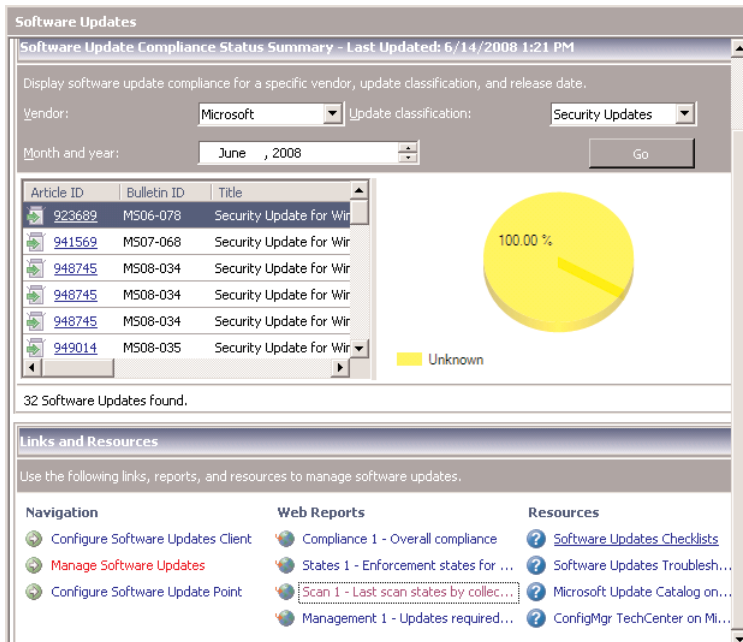


FIGURE 1.8 Software Updates home page

Search Folders

If you like having your surroundings organized, you will love search folders. Search folders provide a way to organize collections of similar objects in your ConfigMgr environment, such as packages, advertisements, boot images, OS installation packages, task sequences, driver packages, software metering, reports, configuration baselines, and configuration items. You can create custom search folders based on your own criteria. This makes it really easy to keep track of the resources deployed in your environment in a way that is meaningful to you.

Queries

Queries are a convenient way to facilitate ad-hoc retrieval of data stored in the ConfigMgr SQL Server database. Queries can be constructed using a wizard interface, which allows

selection of criteria through the UI, thus minimizing the need for knowledge of the WMI Query Language (WQL) in which these queries are written. However, if you are familiar with WQL or Transact SQL (T-SQL), you can easily access the query directly to make changes to the query syntax and criterion.

For example, you could create a query that retrieves a list of all computers with hard drives containing less than 2GB of free space. This sort of logic could be used in determining client readiness for an upgrade to a new version of Microsoft Office.

Reporting in Configuration Manager

The default set of reports in ConfigMgr is huge. The product comes with more than 300 reports in 20 categories, out of the box (see Figure 1.9). The Reporting area also provides a filtering feature to display only the reports that match your criteria, making the reports you care about easier to locate. Reports are categorized by feature, with reporting categories including Asset Management, Desired Configuration Management, Hardware, Network Access Protection, Software Updates, and several others. Each category is then organized further into subcategories. For example, the Software Updates category includes approximately 40 reports in six subcategories:

- ▶ Compliance
- ▶ Deployment Management
- ▶ Deployment States
- ▶ Scan
- ▶ Troubleshooting
- ▶ Distribution Status for SMS 2003 Clients

Authoring new reports is quite easy, as is repurposing existing reports. You can actually clone an existing report, allowing you to make the desired changes to suit your particular situation without affecting the original report. You can even import and export reports between sites, allowing ConfigMgr administrators to easily share their customizations with other administrators of other sites.

You can view reports either through the Configuration Manager console or through the Configuration Manager Report Viewer.

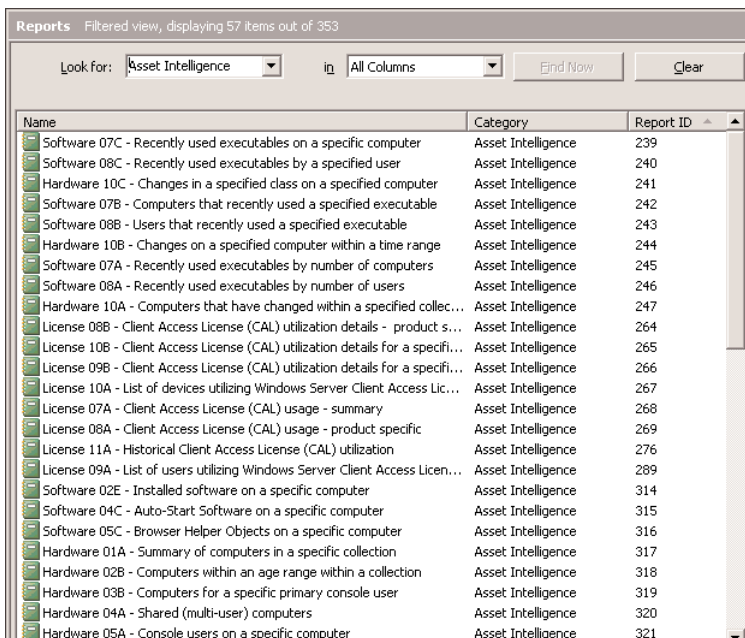
NOTE

ConfigMgr Reporting and SRS

ConfigMgr reporting is fully integrated into the ConfigMgr console, and incorporates the Report Viewer that was present in SMS 2003. Reports are accessed using the ConfigMgr user interface and rendered in Internet Explorer.

However, in ConfigMgr 2007 R2, administrators have the option of moving from the existing reporting environment to SQL Reporting Services as the reporting engine. This requires converting existing reports, but once this is completed, the reports function as they did before and can continue to be administered through the ConfigMgr console. The conversion process is discussed in Chapter 18, “Reporting.”

The Dashboard feature provides additional flexibility in that it allows administrators to group multiple default or custom reports into a single view. This can be used for a number of common scenarios, such as grouping reports that display a certain type of information (for example, hardware and software inventory). This is also very handy for grouping process-related reports, such as the current evaluation and installation state of software and updates. You could further filter your data by site, using a dashboard-per-site strategy to display the status of these processes at individual ConfigMgr sites, each in its own dashboard. All reports are accessible and searchable through the Reports home page, displayed in Figure 1.9.



Name	Category	Report ID
Software 07C - Recently used executables on a specific computer	Asset Intelligence	239
Software 08C - Recently used executables by a specified user	Asset Intelligence	240
Hardware 10C - Changes in a specified class on a specified computer	Asset Intelligence	241
Software 07B - Computers that recently used a specified executable	Asset Intelligence	242
Software 08B - Users that recently used a specified executable	Asset Intelligence	243
Hardware 10B - Changes on a specified computer within a time range	Asset Intelligence	244
Software 07A - Recently used executables by number of computers	Asset Intelligence	245
Software 08A - Recently used executables by number of users	Asset Intelligence	246
Hardware 10A - Computers that have changed within a specified collec...	Asset Intelligence	247
License 08B - Client Access License (CAL) utilization details - product s...	Asset Intelligence	264
License 10B - Client Access License (CAL) utilization details for a specifi...	Asset Intelligence	265
License 09B - Client Access License (CAL) utilization details for a specifi...	Asset Intelligence	266
License 10A - List of devices utilizing Windows Server Client Access Lic...	Asset Intelligence	267
License 07A - Client Access License (CAL) usage - summary	Asset Intelligence	268
License 08A - Client Access License (CAL) usage - product specific	Asset Intelligence	269
License 11A - Historical Client Access License (CAL) utilization	Asset Intelligence	276
License 09A - List of users utilizing Windows Server Client Access Licen...	Asset Intelligence	289
Software 02E - Installed software on a specific computer	Asset Intelligence	314
Software 04C - Auto-Start Software on a specific computer	Asset Intelligence	315
Software 05C - Browser Helper Objects on a specific computer	Asset Intelligence	316
Hardware 01A - Summary of computers in a specific collection	Asset Intelligence	317
Hardware 02B - Computers within an age range within a collection	Asset Intelligence	318
Hardware 03B - Computers for a specific primary console user	Asset Intelligence	319
Hardware 04A - Shared (multi-user) computers	Asset Intelligence	320
Hardware 05A - Console users on a specific computer	Asset Intelligence	321

FIGURE 1.9 The ConfigMgr Reports home page

You can read more about the reporting capabilities in Configuration Manager 2007 in detail in Chapter 18.

Benefits

Configuration Manager is quite flexible in that it also allows deployment in an incremental fashion. You can begin by managing a specific group of servers or a department. Once

you are comfortable with the management platform and understand its features and how those work, you can then deploy to the rest of your organization.

With ConfigMgr as the core component of your systems management toolset handling your systems management objectives, you can take comfort in knowing the tools are available to meet the high expectations of business stakeholders. It plays the role of a trusted partner, helping your IT organization improve service delivery and build a better relationship with the business, while working smarter, not harder.

Overview of Microsoft System Center

Beginning with SMS 2003, Configuration Manager has been a component of Microsoft's System Center strategy. System Center is the brand name for Microsoft's product suite focused on IT service delivery, support, and management. As time passes (and Microsoft's management strategy progresses), expect new products and components added over time. System Center is not a single product; the name represents a suite of products designed to address all major aspects of IT service support and delivery.

As part of a multiyear strategy, System Center is being released in "waves." The first wave included SMS 2003, MOM 2005, and System Center Data Protection Manager 2006. In 2006, additions included System Center Reporting Manager 2006 and System Center Capacity Planner 2006. The second wave includes Operations Manager 2007, Configuration Manager 2007, System Center Essentials 2007, System Center Service Manager, Virtual Machine Manager, and new releases of Data Protection Manager and System Center Capacity Planner. Presentations at popular Microsoft conferences in 2008 included discussions of a third wave, expected to begin around 2010-2011.

Microsoft System Center products share the following DSI-based characteristics:

- ▶ Ease of use and deployment
- ▶ Based on industry and customer knowledge
- ▶ Scalability (from the mid-market to the large enterprise)

Reporting in System Center

The data gathered by Configuration Manager 2007 is collected in a self-maintaining SQL Server database and comes with numerous reports viewable using the Configuration Manager console. ConfigMgr delivers more than 300 reports out of the box for categories including asset intelligence, agent health and status, hardware and software inventory, and several others. Using the native functionality in SQL Reporting Services (SRS) in ConfigMgr 2007 R2, reports can also be exported to a variety of formats, including a Report Server file share, web archive format, Excel, and PDF. You can configure ConfigMgr to schedule and email reports, enabling users to open these reports without accessing the Configuration Manager console.

Together with the reporting available in Operations Manager 2007, administrators will find a very complete picture of present system configuration and health, as well as a detailed history of changes in these characteristics over time.

Ultimately, the integrated reporting feature for System Center is moving under the to-be-released System Center Service Manager product and then will no longer be a separate product.

Operations Management

Microsoft rearchitected MOM 2005 to create System Center Operations Manager 2007, its operations management solution for service-oriented monitoring. Currently in its third release, the product is completely rewritten. The design pillars in Operations Manager (OpsMgr) include a focus on end-to-end service monitoring, best-of-breed manager of Windows, reliability and security, and operational efficiency. Features in OpsMgr 2007 include the following:

- ▶ **Active Directory Integration**—Management group information and agent configuration settings can be written to Active Directory, where they can be read by the OpsMgr agent at startup.
- ▶ **SNMP-enabled device management**—OpsMgr can be employed to discover and perform up/down monitoring on any SNMP-enabled server or network device.
- ▶ **Audit Collection Services (ACS)**—ACS provides centralized collection and storage of Windows Security Event Log events for use by auditors in assessment and reporting of an organization's compliance with internal or external regulatory policies.
- ▶ **Reporting enhancements**—Reporting has been retooled to support reporting targeted to common business requirements such as availability reporting. Data is automatically aggregated to facilitate faster reporting and longer data retention.
- ▶ **Command shell**—Based on PowerShell, the OpsMgr Shell provides rich command-line functionality for performing bulk administration and other tasks not available through the Operations console UI.
- ▶ **Console enhancements**—The console interfaces of MOM 2005 have been consolidated into a single Operations console to support all operational and administrative activities. The new console has an Outlook-like look and feel to minimize the need for training users how to navigate the interface. (A separate console is provided for in-depth management pack authoring.)
- ▶ **Network-Aware Service Management (NASM) and cross-platform monitoring**—In Operations Manager 2007 R2, Microsoft delivers network-aware service management using technology acquired from EMC Smarts, along with native cross-platform monitoring for a number of common Linux and Unix platforms.

System Center Essentials

System Center Essentials 2007 (Essentials for short) is a System Center application, targeted to the medium-sized business, that combines the monitoring features of OpsMgr with the inventory and software distribution functionality found in ConfigMgr into a single, easy-to-use interface. The monitoring function utilizes the form of the OpsMgr 2007 engine that utilizes OpsMgr 2007 management packs, and Essentials brings additional network device discovery and monitoring out of the box. The platform goes beyond service-oriented monitoring to provide systems management functionality, software distribution, update management, as well as hardware and software inventory, all performed using the native Automatic Updates client and WSUS 3.0. Using Essentials, you can centrally manage Windows-based servers and PCs, as well as network devices, by performing the following tasks:

- ▶ Discovering and monitoring the health of computers and network devices and viewing summary reports of computer health
- ▶ Centrally distributing software updates, tracking installation progress, and troubleshooting problems using the update management feature
- ▶ Centrally deploying software, tracking progress, and troubleshooting problems with the software deployment feature
- ▶ Collecting and examining computer hardware and software inventory using the inventory feature

Although Essentials 2007 provides many of the same monitoring features as OpsMgr (and ConfigMgr to some degree), the product lacks the granularity of control and extensibility required to support distributed environments, as well as enterprise scalability. The flip side of this reduced functionality is that Essentials greatly simplifies many functions compared to its OpsMgr and ConfigMgr 2007 counterparts. Customization and connectivity options for Essentials are limited, however. An Essentials deployment supports only a single management server; all managed devices must be in the same Active Directory forest. Reporting functionality is included, but only accommodates about a 40-day retention period.

Essentials 2007 also limits the number of managed objects per deployment to 30 Windows server-based computers and 500 Windows non-server-based computers. There is no limit to the number of network devices.

Service Manager: A Complete Service Desk Solution

Using System Center Service Manager (not yet released) will implement a single point of contact for all service requests, knowledge, and workflow. The Service Manager (previously code-named “Service Desk”) incorporates processes such as incident, problem, change, and

asset management, along with workflow for automation of IT processes. From an MOF perspective, Service Manager will be an anchor for the MOF Supporting quadrant. Figure 1.10 illustrates the mapping between the quadrants of the MOF Process Model and System Center Components.

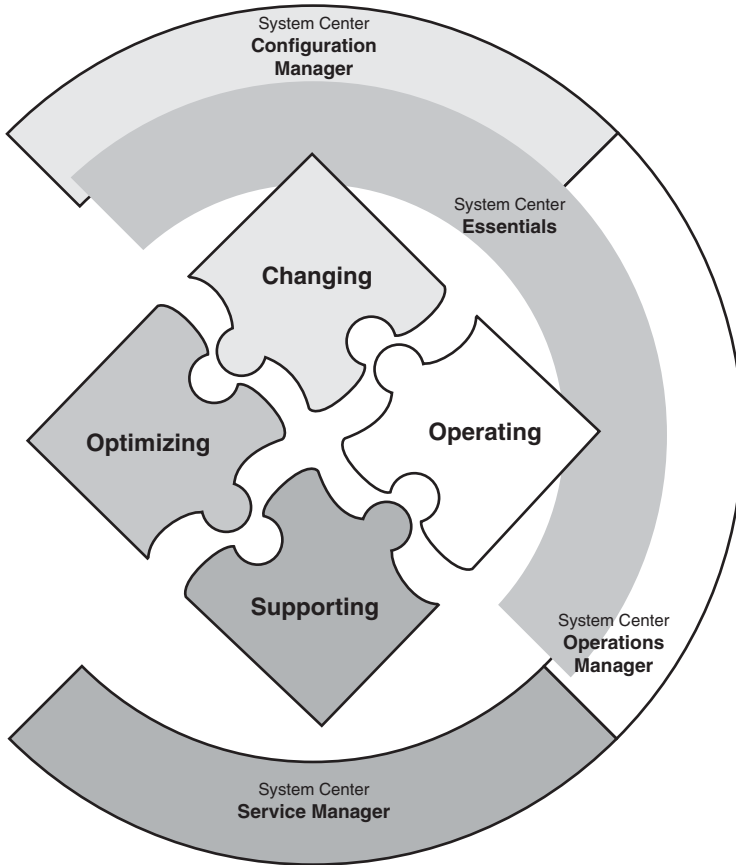


FIGURE 1.10 MOF quadrants and related System Center applications

Service Manager is Microsoft's new help desk product and fills a gap in Operations Manager—What do you do when OpsMgr detects a condition that requires human intervention and tracking for resolution? Until Service Manager, the answer was to create a ticket or incident in one's help desk application, which generally required a third-party product connector to facilitate data exchange between OpsMgr and the ticketing system. Now, within the System Center framework, OpsMgr can hand off incident management to

Service Manager. Similarly, you can use Service Manager in conjunction with ConfigMgr for software distribution. Design goals of Service Manager include the following:

- ▶ Incorporating Self-Service Portal technologies to help organizations reduce support costs, including providing the administrator with a view into the overall performance of the IT environment using reports and dashboards.
- ▶ Ready-to-use process-automated workflows based on processes defined in the Microsoft Operations Framework, using DSI models.
- ▶ A Service Manager Solution Pack framework, similar to the Operations Manager management packs, to enable customers and partners to develop additional custom functionality for the Service Manager.
- ▶ A Configuration Management Database (CMDB) based on SML and XML schema. Microsoft is positioning the CMDB as the foundation of its asset and change management capability, which parallels the CMDB function as defined in ITIL.

Supported scenarios include the following Service Management Functions (SMFs) and capabilities from the MOF Operating and Supporting quadrants:

- ▶ **Incident management**—Creating incident records based on information in management tools
- ▶ **Problem management**—Identifying problems by searching common incidents
- ▶ **Asset management**—Tracking movement and ownership of hardware assets
- ▶ **Change management**—Reviewing and approving change requests
- ▶ **Self-Service Portal**—Resolving an issue without calling the help desk

The console interface of Service Manager in style mirrors that of OpsMgr and Essentials, which have an appearance similar to Outlook. It uses the OpsMgr agent, and the console will have the ability to run OpsMgr tasks. Service Manager brings the “designed for operations” moniker full circle by providing a means to feed production and user data back into the development process using Visual Studio through incident and problem tracking.

Protecting Data

System Center’s Data Protection Manager (DPM) 2007 is a disk-based backup solution for continuous data protection supporting servers running Windows 2003 Service Pack 1 and above. DPM provides byte-level backup as changes occur, utilizing Microsoft’s Virtual Disk Service and Shadow Copy technologies.

Microsoft describes DPM 2007 as a “best of breed” product, adding support for tape media. The Enterprise Edition offers native protection for Windows applications such as Microsoft SQL Server, Exchange, SharePoint Portal Server, plus bare-metal restore capability. This means that in addition to selecting file shares, you can back up SQL Server databases and

Exchange Server storage groups. Via online snapshots, disk-based recovery can maintain backup points to a 15-minute window.

To support the burgeoning presence of virtual machines, DPM supports host-based backups of virtual machines using a single agent on the host. To support branch office and low-bandwidth scenarios, DPM advances de-duplication technology and block-level filter technology that only moves changed data during full backups.

Capacity Planning

System Center Capacity Planner is designed to provide tools and guidance to determine an optimal architecture for successful deployments, while also incorporating hardware and architecture “what-if” analyses for future planning. The Capacity Planner assists with planning deployments of Operations Manager, Exchange Server, and Microsoft Office SharePoint 2007.

In conjunction with the second “wave” of System Center, the newest version of Capacity Planner includes a model for OpsMgr 2007, which supports modeling the following areas:

- ▶ All core server and database components
- ▶ Gateway servers
- ▶ Backup servers for the Operations database, Root Management Server (RMS), and data warehouse
- ▶ 64-bit hardware support
- ▶ Database sizing recommendations
- ▶ Support for background loads
- ▶ Trusted and untrusted agents
- ▶ An enhanced predeployment wizard

The OpsMgr model for Capacity Planner only supports those OpsMgr 2007 installations running SP 1 and above.

The Capacity Planner creates models with information on topology, hardware, software, and usage profiles. It also allows you to run iterative simulations on the models for performance information. Capacity Planner ties into the DSI strategy by identifying when systems deviate from a defined performance model, providing guidance to correct those variations.

Virtual Machine Management

System Center Virtual Machine Manager (VMM) 2008 is Microsoft’s management platform for heterogeneous virtualization infrastructures, providing centralized management of virtual machines across several popular platforms, specifically Virtual Server 2005 R2, Windows Server 2008 Hyper-V, and VMware ESX 3.x. VMM enables increased utilization of physical servers, centralized management of a virtual infrastructure, delegation of

administration in distributed environments, and rapid provisioning of new virtual machines by system administrators and users via a Self-Service Portal.

VMM also delivers advanced functionality for enterprise environments, such as guidance in placement of Microsoft and VMware virtual guests (called intelligent placement), reliable physical-to-virtual (P2V) conversion, as well as virtual-to-virtual (V2V) transfer of VMware hosts. Integration with OpsMgr 2007 provides VMM access to historical performance data in the System Center data warehouse to augment intelligent placement decisions.

The Value Proposition of Configuration Manager 2007

The value of Configuration Manager lies in these areas:

- ▶ Increasing the agility of the IT organization in service delivery to the business
- ▶ Improving the organization's ability to monitor and manage change across client systems and server infrastructure
- ▶ Reducing the cost to deliver services as well as reducing the cost of maintenance throughout the life of the service

As a tool for managing system provisioning, configuration, and security, Configuration Manager is designed as a best-of-breed systems management solution for the Windows Server platform, providing enterprise scale for distributed environments. By incorporating rich OS and software deployment functionality, along with configuration compliance monitoring, it brings simplicity and automation to previously complex tasks.

As an enterprise-grade solution, ConfigMgr provides redundancy and high availability with an open architecture—a requirement for computing enterprises that include critical infrastructure. Configuration Manager is extensible, so it can integrate with other Microsoft technologies, such as SoftGrid Application Virtualization, as well as third-party infrastructure partner solutions.

The goal for the IT manager considering ConfigMgr is to lower the cost of deploying, maintaining, and managing Windows solutions. This can include a variety of areas within IT operations, such as providing systems configuration insight to reduce time-to-resolution problem and incident management, and numerous functions within the configuration management realm, such as monitoring system configuration baselines or deployment of software updates. Its broad functionality makes Configuration Manager 2007 a key component of DSI.

Out of the box, Configuration Manager 2007 reduces manual configuration effort through integration with Active Directory, and it ensures secure communications through mutual authentication (native mode only) and encryption. Comprehensive configuration compliance and update management functionality serve to ensure that the configurations of clients connected to your network are secure and up to date.

Many of the enterprise management platforms provide an infrastructure that has the potential to do great things, and they are sold based on that promise. Frequently though, the complexity of configuration renders these products permanent shelfware that will never be implemented, resulting in wasted IT dollars and missed opportunities.

ConfigMgr introduces a shift in the complexity paradigm with a platform that can be configured by IT pros without the need for extensive professional services engagements. This instant return on investment provides a huge win when the process improvements can be introduced with only hours of effort, with little or no IT effort.

Summary

The purpose of this chapter was to introduce the challenges of systems management and to discuss what Configuration Manager 2007 brings to the table to meet those challenges. You learned that systems management is a process that touches many areas within ITIL and MOF, such as change and configuration management, asset management, security management, and, indirectly, release management. You also learned about the functionality delivered in ConfigMgr that you can leverage to meet these challenges more easily and effectively.

The chapter discussed ITIL v3, which is an internationally accepted framework of best practices for IT Service Management. ITIL describes what should be accomplished in IT operations, although not actually how to accomplish it and how the processes are related and affect one another. To provide additional guidance for its own IT and other customers, Microsoft chose ITIL as the foundation for its own operations framework, the Microsoft Operations Framework. The objective of MOF was to provide both descriptive (what to do and why) as well as prescriptive guidance (how to do it) for IT service management as they relate to Microsoft products.

Microsoft's management approach, which incorporates the processes and software tools of MOF and DSI, is a strategy or blueprint intended to build automation and knowledge into datacenter operations. Microsoft's investment in DSI includes building systems designed for operations, developing an operationally aware platform, and establishing a commitment to intelligent management software.

Configuration Manager is a tool for managing Windows systems in a way that increases the quality of service IT delivers while reducing the operational cost of service delivery. Together with OpsMgr and the other members of the System Center family of products, ConfigMgr is a critical component in Microsoft's approach to system management that can increase your organization's agility in delivering on its service commitments to the business.

Systems management is a key component in an effective service management strategy. Throughout this book, you will see this functionality described and demonstrated, as the authors hope to illustrate the full value of Configuration Manager as a platform for improving the automation, security, and efficiency of service support and delivery in your IT organization.

The next chapter includes an overview of ConfigMgr terminology and discusses key concepts, feature dependencies, and what's new in Configuration Manager 2007.

Index

Numbers

"5 Rules for Managing User Desktops," 29

64-bit environments website, 1104

64-bit Windows

redirection, 783

reports, configuring, 836

A

access

administrative. *See* administration

Service Manager, 429

SQL database, 150

accessibility, reports, 200

accountability, security, 985

accounts

Client Push Installation, 1021

local, managing, 994

Local Service, 92

machine, 1020

Network Service, 92

Package Access, 1023

security, 982, 1019-1020

CSR, 1026

database connections, 1021

health state references, 1025-1026

infrastructure support, 1020-1021

OOB Management, 1023-1024

OSD, 1022-1023

Proxy Account for Internet-Based
Clients, 1026

software updates, 1025

Site System Installation, 1020

site-to-site communications, 1021

system, 92

website, 1020

ACPI HALs, 914**ACS (Audit Collection Services), 993****ACT (Application Compatibility Toolkit), 330, 873****actions (Service Manager), 500-501****Actions pane, 65, 468****activating SUPs, 559****Active Directory**

- discovery, 67, 564
- forests, 321, 344
- group discovery, 566
- integration, 91-92
- overview, 90-91
- POC environment, 342-345
 - cloning DCs, 343
 - new AD forests, 344
 - peel-off method, 343
- resources, 92
- schema, editing, 95
- schema extensions, 93-95
 - benefits, 102-103
 - ConfigMgr updates, 95
 - configuring sites to publish to Active Directory, 100-102
 - finishing tasks, 98
 - System Management containers, 98-99
 - tools, 93-94
 - verifying, 98
 - viewing, 96
- search computer property attributes, 562
- security, 1004
- Security Group Discovery, 562
- sites as boundaries, 277
- SMS 2003 integration, 50-51
- System Discovery, 562-566
- System Group Discovery, 561-562, 566
- trusted root keys, 1018
- User Discovery, 562-566

Active Directory Users and Computers (ADUC), 990**Active Management Technology (AMT), 535-537, 1024****ActiveSync website, 316****adding**

- branch distribution points, 674
 - BITS, enabling, 675
 - properties, 675
 - system role, selecting, 676
- distribution points to Wildflower site server, 667
 - account settings, 668
 - communication settings, 670
 - completing, 671
 - distribution point selection, 669
 - enabling, 669-671
 - FQDN settings, 668
 - group memberships, 671
 - security settings, 668
- drivers
 - boot images, 925
 - systems, 968
- programs, Forefront package, 623-625
- PXE service points, 919-920
- reports to spreadsheets, 852
- state migration points, 921

Add/Remove Snap-in dialog box, 491**addresses**

- IP network identification, 275
- MAC, 925
- overview, 69
- secondary sites, 426
- sender
 - bandwidth, 254
 - configuring, 253-256, 417-421
 - creating, 418
 - destinations, 253
 - priorities, scheduling, 418
 - properties, 420
 - rate limits, 419
 - schedules, 254
 - sites, throttling, 419

Admin User Interface, 1087

administration

- controls, 986
- rights, 608
- security, 982, 987-989, 1029-1030
 - audit messages, 1003
 - copying Local System account rights to ConfigMgr administrative group, 997
 - job roles, managing, 988
 - local Administrators groups, 994-996
 - namespace, 996-997
 - operating system, 989-991
 - outsourcing, 989
 - permission characteristics, 1000-1003
 - permissions, 996-999
 - remote, 1003
 - risk management, 987-989
 - user rights, editing, 997

AdminUI.log, 1087

Adobe Reader virtual application

- data source settings, 633
- distributing, 692
 - advertisement schedule, 696
 - advertisement selection, 696
 - advertisement, creating, 695-696, 700
- App-V 4.5 client installation, 693-694
- application testing, 694
- assignments, 698
- availability, 699
- distribution points, 696
- package selection, 695
- program selection, 696
- status, 698
- test collections, creating, 694
- general settings, 633
- package source, 632
- security settings, 633
- summary, 633

Adsgdis.log, 1084

ADSIEdit MMC snap-in, 562

- installing, 98
- object attributes, viewing, 884
- System Management AD container, creating, 99

Adsysisdis.log, 1084

Adsysisgrp.log, 1084

ADUC (Active Directory Users and Computers), 990

Adusrdis.log, 1084

Advanced Client (SMS 2003), 51-52

advanced queries, 823

- hardware scans within last 30 days, 823
- Query Builder, 821
- systems discovered since midnight, 823
- WQL, 822

Advanced tab (Site Properties dialog box), 382-385

Advertised Programs Client Agent, 549-550, 677-678

advertisements

- administrative rights, running, 608
- allow virtual application packages, 630
- configuring, 688
- content, locating/retrieving, 287
- creating, 678-680
 - creating with Distribute Software to Collection Wizard, 680
 - distribution points, 680
 - names, 682
 - package selection, 680
 - program assignment, 683-684
 - program selection, 680
 - scheduling advertisements, 682
 - subcollection options, 682
- distribution points, 690-691
- interaction settings, 691-692
- mandatory, 68
- monitoring, 684-685
- names, 682
- OpsMgr, 686-688

- overview, 68
- packages, 595
- programs, assigning, 683-684
- reports, 858
- scheduling, 682, 689-690
- security, 692
- software distribution, 745
- static collections, 646
- status, troubleshooting, 972
- task sequences, 329
- virtual applications
 - advertisement selection, 696
 - assignments, 698
 - availability, 699
 - creating, 695-696, 700
 - distribution points, 696
 - package selection, 695
 - program selection, 696
 - scheduling, 696
 - status, 698

agents

- client, 216
 - Advertised Programs Client Agent, 677-678
 - advertised programs, 549-550
 - computer clients, 550, 553
 - configuring, 541-542
 - DCM, 553
 - hardware inventory, 542-544
 - mobile devices, 553
 - NAP, 556, 755-756
 - remote tools, 554-555
 - scheduling, 543
 - SMS_Def.mof file, 545-546
 - software inventory, 546-549
 - software metering, 557-559
 - software updates, 559-560, 719-721

clients

- DCM, 767-768
- selecting, 368

- ConfigMgr, uninstalling, 597
- Hardware Inventory Client, 62
- mobile device client agent settings, 317
- policy, 131
- SHAs, 757-758
- Software Inventory Client, 62-64

Aikbmgr.log, 1084

alerts (DCM), 802

All messages for a specific message ID report, 862-863

All Packages report, 858

All resources in a specific collection report, 858

allow virtual application package advertisement, 630

AMT (Active Management Technology), 535-537, 1024

Amtopmgr.log, 1097

Amtproxymgr.log, 1097

AMTSPSetup.log, 1097

antivirus

- scanning, 305
- software, 1013

App-V 4.5 (Application Virtualization), 628-630

- activating, 630
- allow virtual application package advertisement, 630
- client installation, 693-694
- client packaging, 694
- client verification, 694
- references, 631
- resources, 700, 1107
- virtual applications, sequencing, 631

AppCompat (Application Compatibility Toolkit), 330, 873

AppDeploy website, 626

application compatibility reports, 873-874

Application Compatibility Toolkit (ACT), 330, 873

Application Virtualization. See App-V 4.5

applications. See also software

- adding, Forefront package, 623-625
- Adobe Reader virtual package, 696

- assigning advertisements, 683-684
- configuration items, 769
- distribution testing, 694
- OpsMgr installation, configuring, 605
 - advanced options, 610-611
 - configuring, 602-605
 - environment, 608-609
 - general settings, 605
 - installation program, configuring, 613
 - installation source management, 611
 - MOM maintenance modes, 611
 - requirements, 605-607
- packages, 593-594
- virtual
 - activating, 629-630
 - Adobe Reader, distributing, 693-700
 - allow virtual application package advertisement, 630
 - creating, 632-633
 - deploying, 700
 - importing, 630
 - prepackaged, 636
 - sequenced applications packaging preparations, 632
 - sequencing with App-V, 631

Apply Data Image task, 956

Apply Driver Package task, 958

Apply Network Settings task, 959

Apply Operating System Image task, 955-956

Apply Windows Settings task, 959

architecture

- clients, 179, 216-217
- components, 139-140
- DSI, 18
- envisioning implementation, 178
- servers, 201
 - database servers, 201-202
 - disk performance, 204-207
 - envisioning phase, 179

- performance monitoring, 207

- system performance, 203

SUP, 309-312

- points storage, 311

- synchronization, 310

arrays (disks), 205

asset data timeliness, 12

Asset Intelligence, 53

- catalog synchronization with System Center Online, 871

- overview, 83

- reports, 83, 868

- CAL, monitoring, 870

- classes, enabling, 870

- configuring, 870-872

- license information, importing, 872

- Synchronization Point site role, configuring, 871

- viewing, 872-873

- resources, 1107

- SMS 2003, compared, 868

- synchronization points, configuring, 395

- website, 873

Assign Configuration Baseline Wizard, 774

assigning

- clients to fallback status points, 198

- permissions, 996

- programs, advertisements, 683-684

- virtual applications, 698

associations (WMI classes), 115

asymmetrical encryption, 509-511

attaching child sites to parents, 421-422

attacks

- network-based, 1015

- surface reduction, 1007, 1012

attributes

- classes, 813

- objects, viewing, 884

- queries, 813, 819

- resource views, 154

Audit Collection Services (ACS), 993**audit logs**

- managing, 993
- security, 991-993

audit messages, 1003**auditing**

- directory services objects, 990
- objects, 995
- WMI namespaces, 111

Auditing Entry dialog box, 990**authentication**

- data source, 837-839
- named pipes, 229

Auto Apply Drivers task, 530, 958**auto-enrollment, PKI certificate deployment, 519****AutoIT tool, 627****auto-remediation (DCM), 804****automation, 32**

- challenges, 10
- compliance/enforcement, 33-34
- deployment, 7
- image creation and capture, 931
 - packages, adding, 932-933
 - results, 934
 - task sequences, 932-934
- operating system deployment, 33
- package deployment, 589
- sites
 - assignment, 306
 - system installations, 390-393
- software
 - deployment, 32-33
 - removal, 590
- systems management, 12
- update management tasks, 7

availability

- roles, 200
- security, 984

Available Certificates dialog box, enabling, 388**B****Back Up Group Policy Object dialog box, 345****Background Intelligent Transfer Service. See BITS****Backup ConfigMgr Site Server task, 1037**

- default configuration, 1038
- enabling, 1038
- file structure, 1040
- folders created, 1039

backups

- Backup ConfigMgr Site Server task, 1037
 - default configuration, 1038
 - enabling, 1038
 - file structure, 1040
 - folders created, 1039
- daily, 1040
- database, 1063
- log files, 1086
- POC testing, 348
- restoring, 1041
 - functional crashes, 1041-1045
 - new environment migrations, 1048-1049
 - server operating system crashes, 1041
 - site resets, 1045-1047
 - validating functionality, 1048
- sites, 436
- troubleshooting, 1040
- weekly, 1040

bandwidth

- BITS maximum, 266-267
- pulse mode, 256
- sender addresses, 254
- site boundaries, 262-263
- throttling, 252

baselines, DCM configuration, 772-777

- administrative part, editing, 796
- assigning to collections, 774
- configuration packs, 775-776
- console authoring. *See* console authoring, configuration baselines

- context menu, 774
- creating, 772-773
- editing, 773
- exporting, 796
- external authoring, 797-800
- importing, 776-777
- Microsoft tools, 795-796
- properties, 773
- reports, 775
- rules, 772
- third-party tools, 796
- troubleshooting, 806-807

Basic level (Infrastructure Optimization Model), 27-28

BDD (Business Desktop Deployment Toolkit), 905

benchmarking, 207

best practice configuration packs, 776

binary delta replication, 670

BITS (Background Intelligent Transfer Service), 263, 552

- benefits, 265
- customizing
 - ConfigMgr console, 267-268
 - conflicts, 269
 - group policy options, 266-267
- defined, 70
- distribution points, 69, 269
- enabling, 675
- features, 264
- GetBestInterface function, 269
- IDG counter data error, 266
- infrastructure impact, minimizing, 77
- maximum network bandwidth
 - ConfigMgr console, 267
 - group policies, 266
- overview, 263
- throttling, 552
- versions supported, 265-266

blog resources, 1107-1109

boot critical drivers, 915

boot images, 529-530

- distribution points, 924
- drivers, adding, 925
- PXE booting, 922
- removable media, 922-924

bootable task sequence media, 923

boundaries (sites), 277

- AD sites as, 277
- configuring, 415
- controlling, 277
- defining as slow/fast, 262-263
- planning, 210-211, 306
- protected, 277, 417
- side-by-side migrations, 460
- SMS 2003 migrations, 458
- updating, 289

branch distribution points, 674-676

- adding, 674
 - BITS, enabling, 675
 - properties, 675
 - system role, selecting, 676
- characteristics, 80
- configuring, 80, 399
- creating, 675
- distribution points, compared, 400
- enabling, 671
- infrastructure impact, minimizing, 78
- site systems, 59
- website, 401

broadcasts, subnet directed, 331, 382

Browse list, network discovery retrieval, 276

build-and-capture task sequences, 532-533

Business Desktop Deployment Toolkit (BDD), 905

bypassing maintenance windows, 746

C

caches

- client, 683
- SoH, 557

CALs (Core Client Access Licenses), 181, 870

Capability Maturity Model Integration (CMMI), 25

Capacity Planner, 44, 305

capacity planning, 207-210

- NLB, 208
- state migration points, 209-210

Capture Network Settings task, 958

Capture Operating System Image task, 957

capture task sequence media, 923

Capture User State task, 953

Capture Windows Settings task, 959

capturing

- images, 531-533
 - media, 531-532
 - new build-and-capture task sequences, 532-533
- user state, 940, 953

CAs (Certificate Authorities), 324

CAS.log, 1083, 1095

catalog synchronization, Software Updates, 722

categories

- reports, 842-844
- tasks, 947
 - Disk, 951-952
 - Drivers, 957-958
 - General, 948-951
 - Images, 955-957
 - Settings, 958-959
 - User State, 952-954

CCM_InstalledComponent class, 130

CCM_SoftwareDistribution class, 132

Ccm.log, 1084

Ccmcca.log, 1092

CcmExec.log, 1083

Ccmperf.log, 1092

CCMSSetup.log, 1089

Center for Internet Security (CIS), 1004

central sites, 57, 293

centralized hierarchies, 188

centralized management, distributed enterprises, 30-32

Certificate Authorities (CAs), 324

CertificateMaintenance.log file, 1083

Certificate Revocation Lists (CRLs), 517, 976

Certificate Services, installing, 514-515

certificates

- Certificate Services, installing, 514-515
- CRLs, 517, 976
- native mode, enabling, 388
- PKI, 324-325
 - CAs, 324
 - certificate types, 324
 - deploying, 517-519
 - deploying for native mode, 515-516
 - mixed mode sites, 326
 - native mode sites, 325, 390
 - overview, 324
 - requirements, 513-515
 - templates, 516-517
 - validation, 517
 - website, 508
- types, 324

change control, task sequences, 962-963

change verification, DCM, 766

Change.log, 1096

checkpoint restarting, 52

child primary sites

- attaching to parent site, 421-422
- installing, 422

choosing. See selecting

Ciagent.log, 1092-1095

Ciamgr.log, 1094

Cidm.log, 1084

CIM (Common Information Model), 113

- resources, 1105
- WMI object model, 113-116

CIMV2 namespace

- classes, 125
- root classes, 116
- viewing, 116
- Win32_LogicalShareSecuritySetting class, 116, 119-124

ciphers, 509**CIS (Center for Internet Security), 1004****CIs (configuration items), 339****classes**

- Asset Intelligence reports, 870
- attribute, 813
- CCM_InstalledComponent, 130
- CCM_SoftwareDistribution, 132
- common, 114
- extended, 114
- hardware/software inventory, 825
- inheritance, 114
- InventoryDataItem, 126
- permissions, 996
- querying discovery data, 824-825
- root, 116
- SMS_Client WMI, 129
- SMS_Collection, 136-138
- SMS_SCI_SiteDefinition, 156
- SMS_Site, 134
- SoftwareDistributionClientConfig, 132
- system, 114
- Win32_LogicalShareSecuritySetting, 116
 - class associations, 121
 - class qualifiers, 123-124
 - help entries, 119
 - methods, 119
- WMI
 - attributes, 114
 - namespaces, 115

- qualifiers, 115

- viewing, 134

classic reports

- configuring, 835-836
- copying to SRS, 839, 842
- creating, 894-896
- security, 1027
- viewing from console, 478-479

classifications, software update points, 715**Client.msi.log, 1089****Client Push Installation, 570**

- accounts, 1021
- Properties dialog box, 572
 - Accounts tab, 571
 - Client tab, 572
 - General tab, 570
- Wizard, 570-574

Client Status Reporting Host System role, 301**client status reporting. See CSR****ClientIDManagerStartup.log file, 1083****ClientLocation.log file, 1083****clients**

- advertisements, 68
- agents, 31, 216
 - advertised programs, 549-550, 677-678
 - computer clients, 550-553
 - configuring, 541-542
 - DCM, 553, 767-768
 - hardware inventory, 542-544
 - mobile devices, 553
 - NAP, 556, 755-756
 - remote tools, 554-555
 - scheduling, 543
 - selecting, 368
 - SMS_Def.mof file, 545-546
 - software inventory, 546-549
 - software metering, 557-559
 - software updates, 559-560, 719-721
- App-V 4.5, 693-694

- approval, 585
- architecture, 179, 216-217
- caches, 683
- CALs, 181
- communication
 - assigned sites, 247-248
 - client to server security, 1016-1018
 - customizing, 234
 - headers, 235
 - HTTP native mode, 248
 - initial communication, 246-247
 - NAP traffic, 235
 - native mode sites, 389
 - packets, 234
 - ports, 235, 244-245
 - protocols, 235, 248-251
- Configuration Manager, 60
- DCM requirements, 767
- deployment, 567
 - Client Push Installation, 570-574
 - command-line properties, 567-569
 - imaging, 574
 - manual, 569-570
 - SUP, 574
- discovery, 560
 - AD discovery, 561-564
 - data, deleting, 1062
 - Heartbeat Discovery, 564
 - include groups, 561
 - method selection, 566
 - network, 564-566
 - recursive, 561
- fallback status point assignments, 198
- Forefront package, 620
 - configuring, 621-623
 - creating with New Package Wizard, 621
 - programs, adding, 623-625
- Hardware Inventory Client, 62
- installing
 - resources, 1106
 - testing, 347
- Internet-based, 85, 318
 - disconnected/sometimes-connected users, 272
 - features, 319
 - Internet-Based client solution, 319
 - requirements, 319
 - resources, 1107
 - security, 34, 321-323
 - server deployment, 320-321
 - VPNs, 318-319
- inventories, testing, 347
- large load simulation, 349
- local policies, 131
- logs, 1082-1084, 1093
- Machine Policy Retrieval and Evaluations Cycles, 349
- management point connectivity
 - configuring, 540-541
 - connectivity, testing, 281-282
- mobile devices
 - agent settings, 317
 - logs, 1088-1089
 - software installations, 315-317
- multiple sites, 541
- network installation issues, 283-284
- offline, 284
- patches, 576
- PKI certificate deployment, 518
- push installation, 246
- remote access, 35
- roaming, 211-213, 666
- server locator point specifications, 397
- side-by-side migrations, 460-461
- SMS 2003 upgrading, 455-457
- Software Inventory, 62-64

- software updates
 - enabling, 719
 - logs, 1095-1096
- status reports, 865
 - accounts, 1026
 - client management, 865-867
 - ConfigMgr R2, 867-868
- support, 86
- topology network discovery, 564
- troubleshooting, 576
 - common issues, 576
 - conflicting hardware IDs, 579
 - functionality tests, 582
 - online assistance, 577
 - Toolkit, 579-581
 - uninstalling/reinstalling, 581
- uninstalling, 575
- update scans, 763
- upgrading, 575
- WOL support, 382
- XP Embedded, 314
- Clispy tool, 581**
- cloning DCs, 343**
- CMDB (Configuration Management Database), 338-339**
- CMMI (Capability Maturity Model Integration), 25**
- COBIT (Control Objectives for Information and Related Technology), 987**
- codes**
 - sites, 293
 - storing, 139
- Collection Settings dialog box, 745**
- collections, 594**
 - based on query results, creating, 827-828
 - building with queries, 641
 - creating, 641
 - criteria, 660
 - DCM configuration baselines, 774
 - dynamic, 594, 649
 - converting to static, 649
 - creating, 649-655
 - limiting based on other collections, 655-656
 - membership rules, 650
 - names, 650
 - operating system versions, 653
 - query editing, 651
 - Vista/XP criteria, 651-654
 - evaluation intervals, 195
 - exclusion, 661-665
 - Forefront Client Deployment collection without Validated Systems collection example, 662-665
 - restricting collections query, 662
 - selecting collection for exclusion, 661
 - files, 63, 547
 - flexibility, 665
 - membership rules, 858
 - multiple, 664
 - overview, 66-67
 - predefined, 641
 - queries, compared, 639-641
 - right-clicking, 666
 - static, 594, 642
 - advertisements, 646
 - creating, 642-648
 - dynamic additions, 648-649
 - membership rules, 643-646
 - naming, 643
 - security, 648
 - subcollections, 67, 657
 - advertisement options, 682
 - dependent, 657-659
 - linking, 657-660
 - test, creating, 694
 - updates, scheduling, 646, 658-659
 - viewing, 150-151
 - WMI behind, exploring, 136-138

Collevel.log, 1084**columns**

- console, sorting, 469
- reports, customizing, 878-880

combining

- DCM configuration items, 772
- log files, 162

command-line

- client deployment properties, 567-569
- console options, 504-505
- LDIFDE utility switches, 93

commands

- DOS, 948
- NSlookup, 280
- ping, 279
- SQL, 1064

common classes, 114**Common Information Model. See CIM****communication**

- clients
 - assigned sites, 247-248
 - customizing, 234
 - headers, 235
 - HTTP native mode, 248
 - initial communication, 246-247
 - Internet clients, 321
 - NAP traffic, 235
 - native mode sites, 389
 - packets, 234
 - ports, 235, 244-245
 - protocols, 235, 248-251

components, 149**intrasite, 228-229**

- basic network services, 234
- delta replication, 233
- differential replication, 234
- HTTP/HTTPS, 232
- RPC, 229
- SMB, 231-232
- SQL Server, 229

mobile devices with site systems, 314-315**network issues, 289-290****resources, 1107****security, 982, 1015-1016****client to server, 1016-1018****server to server, 1018-1019****site-to-site, 1018-1019****site-to-site, 251****accounts, 1021****data compression, 261****data priorities, 257****sender addresses, configuring, 253-256****senders, configuring, 251-252****site planning, 261****status message replication,
tuning, 257-261****compatibility reports, 873-874****compliance****automation/control, 33-34****DCM****configuration items, 770****troubleshooting, 807****features, 90****NAP, 758****scanning****forced/unforced, 724****Software Updates, 722-723****state, 723****status reporting, 775****Compmn.log, 1084****components****architecture, 139-140****Discovery Data Manager, 140****Executive Service, 140****in-memory queues, 140****inboxes, 140****interaction example, 147-148****intersite communications, 149****Inventory Data Loader, 140****listing of, 140**

- Management Point File Dispatcher, 140
- replicating data to another site, 149
- servers, 58, 390
- Service Manager, 429
 - logging, 431
 - managing, 431
 - querying, 430
- Site Component Manager, 140
- Site Control Manager, 147
- Site Hierarchy Manager, 147
- Software Inventory Processor, 140
- State System, 140
- compression, source files, 601**
- Compsumm.log, 1084**
- computer associations, 925-926**
 - New Computer Association dialog box, 926
 - recovery, 926
 - unknown computer support, 928
 - computers, importing, 928-929
 - MDT, 930
 - unknown system resources, 930
- Computer Client agent, 550, 553**
- computer details report, 853-854**
- computer information for specific computer report, 848-852**
 - general information, 848
 - properties, 850-852
 - SQL statement, 848
- Computer Management node, 473**
- Computer Management tool, 994**
- computers matching specific criteria report, 855**
- computers with specific product name/version report, 855**
- conditions, task sequences, 944-946**
- confidentiality, 984**
- ConfigMgr, 8**
 - agent, uninstalling, 597
 - features, 7-8
 - functionality, 8-9
 - history, 47
 - 2007, 53
 - SMS 1.1, 47
 - SMS 1.2, 48
 - SMS 2.0, 48-50
 - SMS 2003, 50-53
 - timeline of versions, 47
 - installing, 364
 - client agent selection, 368
 - completing, 373
 - custom/simple settings, 365
 - database servers, 368
 - licensing, 365
 - log files, reviewing, 373
 - management points, 370
 - monitoring with SMS Trace, 363
 - port selection, 370
 - prerequisites, 360-363, 370-371
 - previous installations, 364
 - product keys, 366
 - resources, 1106
 - SCCM installation splash screen, 364
 - settings summary, 371
 - setup options, 364
 - silent, 374
 - site modes, 368
 - site settings, 366
 - site type selection, 366
 - SMS provider settings, 370
 - splash screen, 364
 - Windows Server 2008, 380
 - workstations, 365
 - manageability, 30
 - MOF support, 23-24
 - MSF deployment of, 22
 - new features
 - Asset Intelligence, 83
 - branch distribution points, 80
 - client support, 86

- device management, 83-84
- fallback status points, 82
- IBCM, 85
- OSD, 83
- PXE service points, 82
- site systems, 82
- SQL support, 85-86
- SUP, 80
- OSD, 30
- R2 release, 55
 - CSR, 867-868
 - installing, 378-379
- SDK download, 139
- security enhancements, 29
- Service Packs, 55-56, 374-378
- simplicity, 30
- Site Repair Wizard
 - completing, 1045
 - configuring, 1041
 - hierarchy, 1043
 - package recovery, 1043
 - restore process, 1041
 - site configuration, 1041
 - starting, 1041
- SMS 2003, compared, 53-55
- Toolkit, 158, 797
- value, 45-46
- website, 1103
- configuration baselines, 34**
- configuration drifts, 766**
- configuration items (CIs), 339**
- Configuration Management Database (CMDB), 338-339**
- Configuration.mof file, 126**
- configuration packs (CPs), 34, 775-776**
- configurations (DCM)**
 - administrative part, editing, 796
 - baselines, 772-777
 - assigning to collections, 774
 - configuration packs, 775-776
 - context menu, 774
 - creating, 772-773
 - editing, 773
 - exporting, 796
 - importing, 776-777
 - properties, 773
 - reports, 775
 - rules, 772
- client agents, 767-768
- console authoring, 777
 - administrative part, 796
 - configuration item object properties, 783
 - configuration item properties, 777-780, 783
 - configuration item settings properties, 783
 - configuration item validation criteria, 790-795
 - content part, 796
 - creating configuration items, 777
 - exporting baselines, 796
 - Microsoft tools, 795-796
 - third-party tools, 796
- content part, editing, 796
- external authoring, 797-800
 - CP Studio, 798-800
 - DCM Digest, 797
 - SML, 797
- items, 769-770, 772
 - applicability, 780
 - combining, 772
 - creating, 777
 - detection methods, 778-780
 - evaluation criteria property types, 770
 - hierarchies, 771
 - identifications, 778
 - non-compliance security-levels, 770
 - object properties, 783
 - objects, 780
 - organizing, 771
 - properties, 777-780, 783

- settings, 780
- settings properties, 783
- types, 769
- validation criteria, 790-795
- Windows versions, 780

- Microsoft tools, 795-796

- third-party tools, 796

- troubleshooting, 806-807

Configure Distribution Wizard, 405

Configure Validation dialog box, 790-792

configuring

- advertisements, 688
- Asset Intelligence reports, 870-872
- Asset Intelligence synchronization points, 395
- branch distribution points, 80, 399
- client agents, 541-542
 - advertised programs, 549-550
 - computer clients, 550, 553
 - DCM, 553
 - hardware inventory, 542-544
 - mobile devices, 553
 - NAP, 556
 - remote tools, 554-555
 - SMS_Def.mof file, 545-546
 - software inventory, 546, 549
 - software metering, 557-559
 - software updates, 559-560, 719-721
- Client Push Installation Wizard, 572
- ConfigMgr Site Repair Wizard, 1041
- DCM. See configurations (DCM)
- fallback status points, 393
- Forefront package, 621-623
- hardware, site servers, 302-304
- management points, 540-541
- Mobile Device Client Agent settings, 317
- multicasting, 916-918
- multiple sites, 417
 - child primary sites, installing, 422
 - parent site attachment, 421-422
 - secondary sites, installing, 422-423

- secondary sites, troubleshooting, 424-426
- sender addresses, 417-421
- transferring settings between sites, 426-427

- NAP policies, 521-522

networks

- discovery, 272
- troubleshooting, 278-279

- OOB service points, 395

- OpsMgr installation program, 605, 613

- advanced options, 610-611
- environment, 608-609
- general settings, 605
- installation source management, 611
- MOM maintenance modes, 611
- package, 602-605
- requirements, 605-607

- protected distribution points, 673

- PXE service points, 393-394, 920

- reporting points, 394-395

reports

- classic, 835-836
- SRS, 837-839

- senders, 251-252

- addresses, 253-256
- standard, 252

- server locator points, 397

- SHV points, 399

sites

- boundaries, 415
- modes, 385-387
- properties, 380-385
- publishing to Active Directory, 100-102
- server databases, 845

- Software Updates, 398, 712

SQL replication

- pre-replication setup tasks, 404-405
- setup tasks, 405-410

- state migration points, 398

- status filter rules, 257-258

System Management container
permissions, 99

Windows Server 2008, 326, 362

WOL, 753-754

conflicts

BITS settings, 269

hardware IDs, troubleshooting, 579

records, 383

Connect to Network Folder task, 950

connections

clients to management points, testing,
281-282

database accounts, 1021

intermittent network, 271-272

networks, troubleshooting, 279

site databases, 491

consistency

GUIDs, 440

packages, 589

console

Actions pane, 65, 468

authoring. *See* console authoring

BITS

benefits, 268

customizing, 267

columns, sorting, 469

customizing, 491-496

drag and drop feature, 469

home pages, 469-473

installing

completing, 490

Customer Experience Improvement Program
Configuration, 483

destination folders, 486

installation prerequisite check, 486

installation status, 486

licensing, 483

options, 483

Setup Wizard, 483-490

site server selection, 486

summary, 486

unattended, 490

keystrokes, 477

navigating, 468-469

new features, 469

nodes, 66, 473-474

platforms supported, 64-65

prerequisites, 483

queries, viewing, 810

Registry information, 491

report links, 844

reports, 478-480

result pane, 468

Rights node, 999

search bar, 469

search folders, 469-471

security, 497

DCOM permissions, 497-498

WMI permissions, 498-499

site databases, 491-492

SMS 2003 migrations, 458

snap-ins, 467, 491

supported platforms, 482

tree, 468

troubleshooting

command-line options, 504-505

common issues, 502

large queries, 503

verbose logging, 501-502

Update Repository node, 728-731

console authoring

baselines

administrative part, 796

exporting, 796

Microsoft tools, 795-796

third-party tools, 796

configuration baselines, 777

administrative part, 796

content part, 796

creating, 777

- Microsoft tools, 795-796
- object properties, 783
- properties, 777-783
- settings properties, 783
- third-party tools, 796
- validation criteria, 790-795
- Content Transfer Management component (WMI), 132**
- ContentTransferManager.log file, 1083**
- continual service improvement (ITIL v3), 21**
- Control Objectives for Information and related Technology (COBIT), 987**
- controls, 32, 986**
 - administrative, 986
 - compliance/enforcement, 33-34
 - ConfigMgr, 7
 - operating system deployment, 33
 - physical, 986
 - site boundaries, 277
 - software deployment, 32-33
 - systems management, 11
 - technical, 986
- Convert Disk to Dynamic task, 952**
- Copy Package Wizard, 428**
- Copy Reports Wizard, 840**
- copying**
 - classic reports to SRS, 839-842
 - Local System account rights to ConfigMgr
 - administrative group, 997
 - packages, 428
 - site databases, 375
- Core Client Access Licenses (CALs), 181, 870**
- costs, licensing, 181-182**
- counters**
 - database servers, 201
 - system performance, 203
- courier senders, 252, 417**
- Course 6451A syllabus website, 183**
- CP Studio, 798-800**
- CPs (configuration packs), 775-776**
- Create Configuration Baseline Wizard, 772**
- Create Direct Membership Rule Wizard, static collections, 643-646**
 - limits, 644
 - resources
 - searching, 643
 - selecting, 646
 - updates, scheduling, 646
- Create Package from Definition Wizard**
 - client upgrade packages, 457
 - OpsMgr package, 597
 - OpsMgr agent, 599
 - package definitions, 599
 - source files, 599-601
 - summary, 602
 - welcome screen, 598
- Create Report Wizard, 896**
- CreateTSMedia.log, 1089**
- criteria**
 - collections, 660
 - queries, 816-819
 - status filter rules, 1070
- Criteria Builder (CP Studio), 798**
- Criterion Properties dialog box, 651-653**
 - collections, 660
 - queries, 816-817, 820
- CRLs (Certificate Revocation Lists), 517, 976**
- cryptography, 508-511**
 - asymmetrical encryption, 509-511
 - PKI. See PKI
 - symmetrical encryption, 509
- Cscfsvc.log, 1084**
- CSR (client status reporting), 865**
 - accounts, 1026
 - client management, 865-867
 - ConfigMgr R2, 867-868
- current environment, assessing, 177**
- Custom Schedule dialog box, 658-659**
- Customer Experience Improvement Program Configuration page (Setup Wizard), 483**

customizing. See also editing**BITS**

bandwidth maximum, 266-267

ConfigMgr console, 267-268

conflicts, 269

group policy options, 266-267

client communication, 234

assigned sites, 247-248

headers, 235

initial communication, 246-247

NAP traffic, 235

packets, 234

ports, 235, 244-245

protocols, 235, 248-251

configurations (DCM), 777

administrative part, 796

configuration item object properties, 783

configuration item properties,
777-783

configuration item settings properties, 783

configuration item validation criteria,
790-795

content part, 796

creating configuration items, 777

exporting baselines, 796

external authoring, 797-800

Microsoft tools, 795-796

third-party tools, 796

console, 491-496

site database connections, 491

site databases, 492

snap-ins, 491

database maintenance tasks, 1064

hierarchies, 435

reports, 876

appearance, 878-879

column order, 878

columns, 880

data selection, 879

discovery data, 884-886

external data sources, 889-893

inventory data, 887-889

links, 878

rows, 880-883

websites, 893

SMS_Def.mof file, 545-546

solutions, 357

status filter rules, 1067

task sequences, 960-963

user rights, 997

WinPE, 529

D**Dabney branch distribution point, 675****daily backups, 1040****DASH (Desktop and Mobile Architecture for
System Hardware), 333****dashboards (reports), 38, 875-876****data**

access properties, 615-616

client discovery, deleting, 1062

compression, 261

DDRs

Active Directory example, 1059

creating, 562

data preservation for troubleshooting,
1059

generating, 349

retention, 1055-1060

SMS 2.0 processing, 49

obsolete records, 1060-1062

client discovery data, deleting, 1062

creating, 1060

tasks, 1061

priorities, 257

sources

authentication, SRS reporting, 837-839

external, 889-893

OpsMgr package properties, 613-615

status, 1069-1070

types, 792

data discovery records. See DDRs

Data Protection Manager (DPM), 43

Database Connection Wizard, 491-492

Database Monitor, site configuration files, 162

databases

backing up, 1063

CMDB, 338-339

data deletion, 883

maintenance, 1062-1065

custom task, 1064

Monitor Keys task, 1063

Rebuild Indexes task, 1063

SQL maintenance commands, 1064

multiple, 369

names, 149

placement, 188

relational, 844

SELECT statement, 845-847

tables, 845

views, 845

servers, 201-202, 393

sites

connection accounts, 1021

copying, 375

security, 1015

server, configuring, 845

upgrade tests, 375-376

sizes, 206

SMS, migrating, 462

SQL access, 150

SQL views

collections, 150-151

DiscoveryArchitectures table data, 153

inventory architecture groups, 154

Resource IDs, 153

resource view attributes, 154

schema, 152-153

site properties, 151-152

upgrading, 445-447, 362

views, 150

DataDiff() function, 822

Dataldr.log, 1084

DataService.log file, 1083

DateAdd() function, 822

day-to-day security operations, 983

administration, 1029-1030

inventory, 1033-1034

mobile devices, 1034-1035

OSD, 1032

Remote tools, 1032-1033

software distribution, 1030-1032

DCM (Desired Configuration Management), 33, 71

alerts, 802

change verification, 766

clients

agent properties, 553

requirements, 767

configurations

baselines, 772-777

console authoring. *See* console authoring

drifts, 766

external authoring, 797-800

items, 769-772

Digest, configuration items/baselines, 797

enabling, 767-768

evaluating

criteria, 769

cycles, 807

home page, 72

on-demand results, 802

overview, 71

regulatory compliance, 766

remediation, 803-804

reporting, 801-802

reports, 860-861

scenarios, 801

security, 982

SMS 2003 feature pack conversion, 765

- state messages, 801
- time to resolution, 766
- troubleshooting, 805-807
 - compliance, 807
 - configurations, 806-807
 - log files, 805

Dcmagent.log, 1093

DCOM (Distributed Component Object Model), 497-498

DCs (Distributed Components), cloning, 343

Ddm.log, 1084

DDRs (data discovery records), 349

- Active Directory example, 1059
- creating, 562
- data preservation for troubleshooting, 1059
- generating, 349
- retention, 1055-1060
- SMS 2.0 processing, 49

debug logging, 805, 1080

default views, 889

Delete Aged Status Messages task, 1070

Delete Obsolete Client Discovery Data task, 1062

Delete site maintenance task, 1061

deleting

- client discovery data, 1062
- database data, 883
- status messages, 1070

deliverables (POC), 350

delivery services, testing, 348

delta replication, 233-234, 670

delta site control file logs, 164, 167

denial of service (DoS) attacks, 1016

dependencies

- features, 86-87
- network discovery, 276
- OOB Management, 332
- subcollections, 657-659
- website, 1104

deployment, 225-226

- automation, 7
- client, 567
 - Client Push Installation, 570-574
 - command-line properties, 567-569
 - imaging, 574
 - manual, 569-570
 - SUP, 574
- ConfigMgr, 22
- images, 909-910, 937-939
 - goals, 912-913
 - operating system images, 938
 - software distribution packages, 938
 - task sequence, 937-939
- mandatory, enforcing, 720
- operating systems, 30-33, 860
- packages, 589
 - distribution points, 742
 - linking, 740
 - software updates, 738-740
 - source folders, 740
- PKI certificates, 517-519
 - auto-enrollment, 519
 - clients, 518
 - native mode, 515-516
 - references, 519
 - site servers, 518
 - site systems, 518
- servers, 320-323
- simplifying, 91
- sites
 - system roles, 299-300
 - Virtual Machines, 304
- software
 - automation/control, 32-33
 - website, 626
- storage drivers, 915
- updates, 736
 - best practices, 743-744
 - creating, 736-737

- deadlines, 737-738
- hiding, 720
- implementing, 740-742
- maintenance windows, 744-747
- reevaluating, 721
- templates, 733-735
- virtual applications website, 700
- WDS, 533-534

Deployment Template Wizard, 734

designing sites, 213-214

- 25,000 client environments, 215
- 50,000–100,000 client environments, 215
- greater than 100,000 client environments, 216
- smaller environments, 214

Desired Configuration Management. See DCM

Desktop and Mobile Architecture for System Hardware (DASH), 333

desktop management, 29

despool.log file, 424, 1084

destination volumes, formatting, 934

detection methods, configuration items, 778-780

development phase, 186

- capacity planning, 207-210
- client architecture, 216-217
- ConfigMgr roles, 193-194
 - availability, 200
- distribution points, 195-196
- fallback status points, 197
- management points, 197
- reporting points, 199
- server locator points, 197
- SHV, 196
- site servers, 194-195
- software update points, 198-199

hierarchies

- centralized, 188
- flat, 188
- tiered, 186

MOF, 21

multilanguage scenarios, 218-219

- ICP files, 219
- ICP scenarios, 220-221
- ICP versioning, 219-220
- languages supported, 218

network infrastructure, 189-191

roaming, 211-213

scalability numbers, 187

schema extensions, 191

secondary site servers, 192

server architecture, 201

- database servers, 201-202
- disk performance, 204-207
- performance monitoring, 207
- system performance, 203

site boundaries, 210-211

site design, 213-214

- 25,000 client environments, 215
- 50,000–100,000 client environments, 215
- greater than 100,000 client environments, 216
- smaller environments, 214
- site security modes, 193

device drivers, 969

device management points, 59

devices

managing, 312-313

- benefits, 313
- client agent settings, 317
- client software installations, 315, 317
- mobile devices supported, 83-84, 312
- reports, 861
- site system communication, 314-315
- Windows CE operating systems, 313
- XP Embedded clients, 314

mobile

- client agents, 317, 553
- client software installations, 315-317
- logs, 1087-1089
- resources, 1107

- security, 1034-1035
- site system communication, 314-315
- supported, 312
- Windows CE operating system, 313
- Windows Mobile, 313

DHCP (Dynamic Host Configuration Protocol), 275

dialog boxes. *See specific dialog boxes*

digital signing, 511

direct membership rules, 651

directory services objects, auditing, 990

Disable BitLocker task, 952

Disable Publishing and Distribution Wizard, 413

disabling

- publishing, 414
- SQL replication, 413-414
- Windows Updates GPOs, 721

disconnected users, 271-272

discovery

- Active Directory, 67
- client data, deleting, 1062
- clients, 560
 - AD discovery methods, 561-563
 - Heartbeat Discovery, 564
 - include groups, 561
 - method selection, 566
 - network, 564-566
 - recursive, 561
- custom reports, 884-886
- data queries, 824-825
- data reports, 848
 - computer details, 853-854
 - computer information for a specific computer, 848-852
 - computers matching specific criteria, 855
 - computers with specific product names/versions, 855
 - low free disk space, 855
 - network, 856
 - users, 856
- listing of, 1056

network, 272-273

- Browse list, 276
- configuring, 272
- dependencies, 276
- device information, accessing, 276
- IP addresses, identifying, 275
- network topology, 274-275
- resources, 273
- subnet masks, 276
- subnets, 273
- overview, 67
- systems discovered since midnight query, 823

Discovery Data Manager, 140

DiscoveryArchitectures table data, viewing, 153

Discovery.log, 1093

Disk tasks, 951-952

disks

- arrays, 205
- characteristics, 204
- I/O, 204
- life cycle, 204
- optimization, 205
- performance, 204-207
 - arrays, 205
 - characteristics, 204
 - database sizes, 206
 - distribution points, 206
 - drive life cycle, 204
 - I/O bottlenecks, 204
 - optimization, 205
 - OSD functionality, 206
 - storage, 205
- storage, 205

Distmgr.log, 1084, 1094

Distribute Software to Collection Wizard

- advertisements, creating, 680
- distribution points, 680
- names, 682
- package selection, 680
- program assignment, 683-684

- program selection, 680
- scheduling advertisements, 682
- subcollection options, 682
- limitations, 679

Distributed Component Object Model (DCOM), 497-498

Distributed Components (DCs), cloning, 343

distributed enterprises

- centralized management, 30-32
- challenges, 10

Distributed Management Task Force (DMTF), 104

distributing

- Adobe Reader virtual application, 693
 - advertisements, creating, 695-696, 700
- App-V 4.5 client, 693-694
- application testing, 694
- assignments, 698
- availability, 699
- distribution points, 696
- package selection, 695
- program selection, 696
- status, 698
- test collections, creating, 694

software

- advertisements, 745
- network issues, 286-287
- packages, 938
- pulling software, 76-77
- pushing software, 77
- reports, 857-859
- security, 1030-1032
- troubleshooting, 702
- updates, 725

Distribution Database page (Configure Distribution Wizard), 405

Distribution Manager, status messages, 286

distribution points

- Adobe Reader virtual package, 696
- advertisements, 680, 690-691
- Application Virtualization roles, 301

- BITS, enabling, 69, 269
- branch, 59, 674-676
 - adding, 674
 - BITS, enabling, 675
 - characteristics, 80
 - compared to regular distribution points, 400
 - configuring, 80
 - creating, 675
 - enabling, 671
 - infrastructure impact, minimizing, 78
 - properties, 675
 - system role, selecting, 676

- client roaming, 666
- copying packages, 428
- data storage, 672
- deployment packages, 742
- disk performance, 206
- infrastructure impact, minimizing, 78
- mobile device communication, 315
- NAS support, 302
- OSD, 916-918
- overview, 69
- packages, 594-595
- placement, site planning, 301
- protected, 277, 672-674
- role, 195-196
- SAN support, 302
- secondary site servers, 58
- server shares, 667
- as servers, 667
- site systems, 59, 390
- standard, 667-671
- types, 666
- website, 401
- Windows PE boot images, 924

DLLs (dynamic link libraries), 139

DmCertEnroll.log, 1088

DMCertResp.htm file, 1088

DmClientHealth.log, 1087

DmClientRegistration.log, 1088

DmClientSetup.log, 1088

DmClientXfer.log, 1088

DmCommonInstaller.log, 1088

DmInstaller.log, 1089

DmInvExtension.log, 1089

DmpDatastore.log, 1088

DmpDiscovery.log, 1088

DmpFileCollection.log, 1088

DmpHardware.log, 1088

Dmplsapi.log, 1088

DmpMSI.log, 1088

DmpSetup.log, 1088

DmpSoftware.log, 1088

DmpStatus.log, 1088

DmSvc.log, 1089

DMTF (Distributed Management Task Force), 104

DNS (Domain Naming Service), 342

incorrect referrals, 280

management point publication, 385

POC environment, 342

security, 1026-1027

documenting hierarchies, 298

DoS (denial of service) attacks, 1016

DOS commands, 948

Download Updates Wizard, 739-740

downloading updates, 762-763

DPM (Data Protection Manager), 43

drag and drop (console), 469

DriverCatalog.log, 1089

drivers

adding, boot images, 925

boot critical, 915

images, 530-531

mass storage, 958

OSD, 966-969

adding to catalog, 967

adding to systems, 968

device, 969

images, 969-970

importing, 967

layering, 970

managing, 970

storing, 967

troubleshooting, 968

website, 971

SATA, 915

tasks, 957-958

Windows XP 964

DSI (Dynamic Systems Initiative), 16-17

architectural elements, 18

importance, 18

Microsoft product integration, 17-18

SML, 19

dynamic collections, 594, 649

converting to static, 649

creating, 649-655

membership rules, 650

names, 650

operating system versions, 653

query editing, 651

Vista/XP criteria, 651-654

limiting based on other collections, 655-656

Dynamic Host Configuration Protocol (DHCP), 275

Dynamic level (Infrastructure Optimization Model), 28

dynamic link libraries (DLLs), 139

Dynamic Systems Initiative. See DSI

E

eavesdropping attacks, 1015

editing. See also customizing

Active Directory schema, 95

images, offline, 910-912

LDF files, 94

queries, dynamic collections, 651

site control file, 147

site properties, 147-148

user rights, 997

Emerald. See SMS, 2003

Enable BitLocker task, 952

enabling

- Asset Intelligence report classes, 870
- Backup ConfigMgr Site Server task, 1038
- BITS distribution points, 269, 675
- branch distribution points, 671
- DCM, 767-768
- hardware inventory, 542
- logging, 1080
 - debug/verbose, 1080
 - NAL, 1081
 - reporting point servers, 1081-1082
 - SQL, 1081
- multicasting, 916-918
- native mode, 387-390
- Software Updates, 710-712, 719
- standard distribution points, 669
- verbose logging, 501-502

encryption, 1016

- asymmetrical, 509-511
- defined, 509
- key lengths, 513
- symmetrical, 509

Enterprise Server MLs, 180

environments

- migrating to new, 1048-1049
- OpsMgr installation program, running, 608-609
- POC, 338-339
 - AD, 342-345
 - connected to production networks, 346-347
 - DNS, 342
 - lab, 340-342
 - PKI, 342
 - WINS, 342
- testing, 341

envisioning phase

- architecture, 178
- client architecture, 179
- current environment assessment, 177
- licensing, 179-182
 - CALs, 181
 - costs, 181-182
 - Standard/Enterprise Server MLs, 180
- network infrastructure, 177-178
- server architecture, 179
- training, 182
 - technical, 183
 - users, 182

error codes (OSD), 973

Error Lookup tool, 581

Essentials (System Center), 41

evaluation criteria, 769-770

evaluation cycles (DCM), 807

evaluation intervals (collections), 195

evaluation software, 346

EventLogForwarder.log, 1093

evolution of systems management

- asset data, 12
- automation, 10-12
- change identification, 11
- distributed enterprise challenges, 10
- problems, 10
- process consistency, 13-14
- security/control, 11
- virtualization, 13

exclusion collections, 661-665

- Forefront Client Deployment collection without Validated Systems collection example, 662-665
- restricting collections query, 662
- selecting collection for exclusion, 661

Execmgr.log file, 1083

Executive Service, 140

exit criteria (POC), 350-351

exporting

- configuration baselines, 796
- object definitions to MOF files, 138, 355
- queries
 - between sites, 827
 - results to text files, 826

ExtADSch.exe utility, 93

extensions

- classes, 114
- files, identifying with PowerShell, 327
- schema, 191

external authoring, configuration items/baselines, 797-800

- CP Studio, 798-800
- DCM Digest, 797
- SML, 797

external data sources, report inclusion, 889-893

F

fallback status points, 59, 82

- clients
 - assignments, 198
 - installations, 584
- configuring, 393
- installing, 82
- Microsoft documentation, 198
- mobile device communication, 315
- role, 197
- security, 82

fast networks, site boundaries, 262-263

feature dependences, 86-87

feature packs (SMS 2003 migrations), 436

features, 7-8

Federal Information Security Management Act and Agency Privacy Management, 308

file level imaging, 528

FileBITS.log file, 1083

files

- Admin User Interface log, 1087
- backup log, 1086
- client log, 1083, 1093
- collecting, 63, 547
- Configuration.mof, 126
- delay site control, 164-167
- despool.log, 424
- extensions, identifying with PowerShell, 327
- hardware inventory, 462-463
- help, 1105
- ICP, 219
- installation, 598
- LDF, editing, 94
- log, 688
- malware signature, 312
- management point log, 1086-1087
- MIF, 1033
- mobile device log
 - clients, 1088-1089
 - management, 1087-1088
- MOF, object definition exports, 138, 355
- mpmsi.log, 541
- NAP log, 1092-1093
- OOB Management log, 1097-1098
- OSD
 - log, 1089-1091
 - multicasting log, 1091-1092
- package definition, 355
 - benefits, 620
 - OpsMgr package, 613-620
 - website, 1106
- server logs, 1084-1086
- SHV log, 1092
- sites
 - configuration, dropping, 162
 - control, 147
 - settings, transferring, 351-352
- SMS_Def.mof, 126, 545-546

- smsprov.log, 158
- smsts.log, 972
- software update log
 - clients, 1095-1096
 - site servers, 1094-1095
- source, 601
- WIMs
 - benefits, 906
 - mounting, 911
 - Vista, Windows Server 2008 DVDs, 938
- Windows Update Agent log, 1097
- WOL log, 1094
- WSUS log, 1096

Filter tool, client troubleshooting, 580

filters

- status filter rules
 - criteria, 1070
 - predefined, 1071-1072
- status message, 863, 1065
 - customizing, 1067
 - priorities, 1067
 - summarizer data, 1069

finding GUIDs, 779

firewall requirements, 319

flat hierarchies, 188

flexibility, collections, 665

folders

- backup, 1039
- inboxes, 140
- search, 36

ForeFront

- advertisements
 - distribution points, 680
 - names, 682
 - package selection, 680
 - program assignment, 683-684
 - program selection, 680
 - scheduling, 682
 - subcollection options, 682

- Client Deployment collection exclusion example, 662-665
- client package, 620
 - configuring, 621-623
 - creating with New Package Wizard, 621
 - programs, adding, 623-625

forests (AD)

- Internet clients, 321
- POC environment, 344

Format and Partition Disks task, 951

formatting destination volumes, 934

free utilities websites, 1111-1112

fresh SoH, 557

Fsinvprovider.log file, 1083

Fsp.Isapi.log, 1088

functional crash recovery, 1041-1045

functional specification, 183

functional testing, 347-348

functionality

- ConfigMgr, 8-9
- SoftGrid, 628

G

general configuration items, 769

general properties (OpsMgr package), 613

general resource websites, 1099-1103

General tab

- Site Properties dialog box, 380
- WMI Control, 109

General tasks, 948-951

- Connect to Network Folder, 950
- Install Software, 949
- Install Software Updates, 950
- Join Domain or Workgroup, 950
- Restart Computer, 951
- Run Command Line, 948
- Set Task Sequence Variable, 951

GetBestInterface function, 269

GetDate() function, 822

Gilbert, Jeff, 546

global roaming, AD schema extensions, 102

Globally Unique Identifiers (GUIDs), 440, 779

goals

image deployment, 912-913

POC, 337

security, 984

Golden Master Creation Wizard (CP Studio), 798

GPMC (Group Policy Management Console), 344

GPOs (group policy objects), 721

BITS

benefits, 267

conflicts, 269

customizing, 266-267

management website, 267

post-deployment tasks, 971

software distribution, 590-592

Software Updates, 721

transferring to POC environment, 344

Windows Updates, disabling, 721

groups

inventory architecture, viewing, 154

local Administrators, 994-996

Schema Admins, 94

SMS Admins, 497

task sequences, 946-947

GUIDs (Globally Unique Identifiers)

consistency, 440

finding, 779

H

HALs (Hardware Accessibility Lists), 913-914

hardening servers, 1007

hardware

HALs, 913-914

HCLs, 301

IDs, conflicting, 965

inventory, 62

classes, 825

files, migrating, 462-463

resources, 1106

WMI, 126-129

OSD, 913-915

resource websites, 1103

scans, querying, 823

security, 1007

sizing/configuring, 302-304

Hardware Inventory Client agent, 62, 542-544

hash values, 511

HCLs (Hardware Compatibility Lists), 301

headers, client communication, 235

health policies, 757

health state reference accounts, 1025-1026

Heartbeat Discovery, 564-566

help files, 1105

Hermes, 47

hiding update deployments, 720

hierarchies

attaching to sites, 376

centralized, 188

DCM configuration items, 771

flat, 188

reports, 834

security, 982, 1004-1006

sites, 293

codes, 293

designing, 293-295

documenting, 298

overview, 60

parent/child relationships, 296

primary versus secondary, 295-296

restoration, 1043

three-tiered example, 294, 297

two-tiered example, 296-297

SMS 2003 migrations to ConfigMgr, 435

tiered, 186

update lists, 733

Hierarchy Manager, 164
historical data reports, 861
history of ConfigMgr, 47
 2007, 53
 SMS 1.1, 47
 SMS 1.2, 48
 SMS 2.0, 48-50
 SMS 2003, 50-53
 timeline of versions, 47

Hman.log, 1084

Hobbs, Cliff, 304

home pages
 console, 469-473
 visibility, 36

hotfixes (ICP), 220

HTTP (Hypertext Transfer Protocol)
 intrasite communication, 232
 native mode client communication, 248
 ports, inventorying, 545

HTTPS (secure HTTP), 232

Hyper-V, 304

I

I/O (input/output), disk performance, 204

IBCM (Internet-Based Client Management), 85, 318

 disconnected/sometimes-connected users, 272
 features, 319
 Internet-Based client solution, 319
 requirements, 319
 resources, 1107
 security, 34, 321-323
 server deployment, 320-321
 VPNs, 318-319

ICP (International Client Pack), 218

 download website, 218
 files, 219
 hotfixes, 220

 ICP files, 219

 languages included, 218

 Microsoft documentation, 219

 scenarios, 220-221

 versions, 219-220

identification properties, configuration items, 778

IDG BITS counter data error, 266

IDMIF files, 1033

IDS (intrusion detection systems), 190

IIS, configuring, 389

Image Capture Wizard, 923

Image Deployment task sequence, 939

images, 524-525

 automated creation and capture, 931

 packages, adding, 932-933

 results, 934

 task sequences, 932-934

 boot, 529-530

 distribution points, 924

 drivers, adding, 925

 PXE booting, 922

 removable media, 922-924

 capturing, 531-533

 client deployment, 574

 defined, 910

 deploying, 937-939

 operating system images, 938

 software distribution packages, 938

 task sequence, 937-939

 drivers, 530-531, 969-970

 file level, 528

 ImageX, 527-528

 offline image editing, 910-912

 OSD, 906-907

 manual creation and capture, 935-937

 New PC scenario, 525

 offline editing, 910-912

 OSD, 909-913

 Refresh PC scenario, 525

 Replace PC scenario, 526

- sector-based, 528

- thick/thin, 910

- WIM, 527

Images tasks, 955-957

- Apply Data Image, 956

- Apply Operating System Image, 955-956

- Capture Operating System Image, 957

- Install Deployment Tools, 956

- Prepare ConfigMgr for Client, 956

- Prepare Windows for Capture, 956

- Setup Windows and ConfigMgr, 956

ImageX, 527-528

- offline image editing, 910-912

- OSD, 906-907

implementing

- MSF planning, 186

- WOL, 754

Import Computer Information Wizard, 928-929

Import Configuration Data Wizard, 776

Import New Driver Wizard, 967

importing

- configuration baselines, 776-777

- drivers, 967

- licensing, 872

- queries between sites, 827

- virtual application packages, 630

in-memory queues, components, 140

in-place migration scenario (OSD), 908

in-place upgrades, 435

- database upgrades, 445-447

- feature packs, 436

- post-upgrade considerations, 457-458

- prerequisite checker, running, 437-442

- GUID consistency, 440

- options screen, 437

- output, 438

- schannel hotfix rule, 442

- WSUS SDK on site server rule, 438

- prerequisites, 436-437

- primary site upgrades, 447-453

- action status, monitoring, 450

- completing, 452

- ITMU upgrade, 450

- licensing, 448

- options, 448

- updated prerequisites, 449

- WSUS installation, 451

- secondary site upgrades, 453-455

- completing, 454

- installation source files, 454

- site selection, 454

- SMS 2003 client upgrades, 455-457

- SQL Server upgrades, 442-445

- performing, 444-445

- Upgrade Advisor, running, 442-443

- WSUS, 458-459

Inboxast.log, 1084

inboxes, 140

Inboxmgr.log, 1085

Inboxmon.log, 1085

include groups client discovery, 561

incorrect referrals, 280

infrastructure

- minimizing impact, 77-80

- BITS, 77

- branch distribution points, 78

- distribution points, 78

- Download and Execute, 78

- inventory, 79

- senders, 78

- testing, 79

- network

- developing, 189-191

- envisioning phase, 177-178

- optimizing, 25

- Basic level, 27-28

- Dynamic level, 28

- Infrastructure Optimization Model, 26-27

- Rationalized level, 28

- Standardized state, 28

planning, 292

public key. *See* PKI

security

accounts. *See* accounts, security

communications, 1015-1019

hierarchy, 1004-1006

name resolution, 1026-1027

reports, 1027-1029

site systems, 1007-1015

WMI, 106-108

Infrastructure Optimization (IO) Model, 15, 26-28, 983

inheritance, classes, 114

input/output (I/O), disk performance, 204

Install Deployment Tools task, 956

Install Packages task, 931

Install Software task, 949

Install Software Updates task, 950

installation files, storing, 598

installing

ADSIEdit, 98

App-V 4.5 client, 693-694

Certificate Services, 514-515

child primary sites, 422

client software, mobile devices, 315-317

clients

push installation, 246

resources, 1106

testing, 347

troubleshooting, 283-284

ConfigMgr, 364

client agent selection, 368

completing, 373

custom/simple settings, 365

database servers, 368

licensing, 365

log files, reviewing, 373

management points, 370

monitoring, SMS Trace, 363

port selection, 370

prerequisites, 360-363, 370-371

previous installations, 364

product keys, 366

resources, 1106

SCCM installation splash screen, 364

settings summary, 371

setup options, 364

silent, 374

site modes, 368

site settings, 366

site type selection, 366

SMS provider settings, 370

Windows Server 2008, 380

workstations, 365

ConfigMgr R2, 378-379

console

completing, 490

Customer Experience Improvement
Program Configuration, 483

destination folders, 486

installation prerequisite check, 486

installation status, 486

licensing, 483

options, 483

Setup Wizard, 483-490

site server selection, 486

summary, 486

unattended, 490

fallback status points, 82

secondary sites, 422-423

Security Configuration Wizard, 1008

service packs, 374-376

hierarchy attachments, 376

performing, 376-378

site database upgrade tests, 375-376

site systems, 390-401

automatically, 390-393

component servers, 390

database servers, 393

distribution points, 390

- management points, 391
- roles, adding, 393-400
- site servers, 391
- testing, 347
- troubleshooting, 282-283, 429
- verifying, 429

WDS, 918

WSUS, 711

instance permissions, 996

integrity, security, 984

Intel

- AMT, 535-537

- vPro, 534-537

intelligent placement, 45

intermittent network connections, 271-272

International Client Pack (ICP), 218-220

Internet clients

- managing, 319

- planning, 318

- IBCM, 319

- security, 323

- server deployment, 320-321

- VPNs, 318-319

- security, 34

- Active Directory forests, 321

- dedicated sites, 321

- internal/perimeter network site span, 322

- site-to-site communication, 321

- troubleshooting, 577

Internet Explorer, viewing reports, 481-482

Internet Protocol Security (IPSec), 1019

Internet Security and Acceleration (ISA) Server, 193

Internet-Based Client Management. See IBCM

intersite communications, 149

intersite replication, viewing, 168-172

intrasite communication, 228-229

- delta replication, 233-234

- differential replication, 234

- HTTP/HTTPS, 232

- RPC, 229

- SMB, 231-232

- SQL Server, 229

intrusion detection systems (IDS), 190

intrusion prevention systems (IPS), 190

inventories

- architecture groups, viewing, 154

- clients, testing, 347

- custom reports, 887-889

- data queries, 825-826

- data reports, 848

- computer details, 853-854

- computer information for a specific computer, 848-852

- computers matching specific criteria, 855

- computers with specific product names/versions, 855

- low free disk space, 855

- network, 856

- users, 856

- hardware, 62

- classes, 825

- files, migrating, 462-463

- resources, 1106

- WMI, 126-129

- infrastructure impact, minimizing, 79

- MIF files, 1033

- overview, 61

- security, 546, 1033-1034

- sitewide settings, 62

- SMS 2.0, 49

- software, 62-64, 546-549

- file collection, 547

- filenames, 546

- names, 548

Inventory Data Loader, 140

InventoryAgent.log file, 1083

InventoryDataItem class, 126

Inventory Tool for Microsoft Updates (ITMU), 450, 708-709

Invproc.log, 1085

IO (Infrastructure Optimization) Model, 15, 26-28, 983

IP addresses, network identification, 275

IPS (intrusion prevention systems), 190

IPSec (Internet Protocol security), 1019

ISA (Internet Security and Acceleration) Server, 193

ISO 20000, 24-25

IT Infrastructure Library. See ITIL

IT projects, life cycle, 337

IT Service Management. See ITSM

IT service triangle, 14-15

items (DCM configuration)

- administrative part, editing, 796
- applicability, 780
- console authoring, 777, 796
- content part, editing, 796
- creating, 777
- detection methods, 778-780
- identifications, 778
- external authoring, 797-800
- Microsoft tools, 795-796
- objects, 780-783
- properties, 777-783
- settings, 780-783
- third-party tools, 796
- troubleshooting, 806-807
- validation criteria, 790-795
- Windows versions, 780

ITIL (IT Infrastructure Library), 19

- customer-centric service organizations, 21
- measurements, 21
- MOF, compared, 24
- overview, 19
- version 3, 20-21

ITMU (Inventory Tool for Microsoft Updates), 450-453, 708-709

ITSM (IT Service Management), 17-19

- DSI, 16-17
- architectural elements, 18
- importance, 18

- Microsoft product integration, 17-18
- SML, 19

infrastructure optimization, 25

- Basic level, 27-28
- Dynamic level, 28
- Infrastructure Optimization Model, 26-27
- Rationalized level, 28
- Standardized state, 28

ISO 20000, 24-25

ITIL, 19

- customer-centric service organizations, 21
- measurements, 21
- MOF, compared, 24
- overview, 19
- version 3, 20-21

MOF

- ConfigMgr support, 23-24
- development, 21
- ITIL, 22-24
- MSF combination, 22
- overview, 21-24
- process model, 23-24
- version 4, 21

J-K

Job Activity Monitor, 410

Join Domain or Workgroup task, 950

joining sites

- delta site control file log entries, 164-167
- Hierarchy Manager, 164
- new parent site replication log entries, 167-168
- Process Monitor, 163
- status messages, 159-161

key exchanges, 385, 424-425

keystrokes (console), 477

L

lab environments (POC), 340-342

languages (ICP), 218

latency between sites, 256

Launch and Activation Permissions dialog box, 498

layout, reports, 878-879

LDF file, editing, 94

LDIFDE utility, 93-94

licensing

Asset Intelligence, importing, 872

ConfigMgr installation, 365

console installation, 483

costs, 181-182

enforcement, 49

evaluation software, 346

Microsoft Volume Licensing website, 182

POC, 346

primary site upgrades, 448

requirements, 179-182

CALs, 181

Standard/Enterprise Server MLs, 180

resources, 1105

life cycle

disk drives, 204

IT projects, 337

management, simplifying, 91

links

reports, customizing, 878

subcollections, 657-660

living documents, 184

local accounts, managing, 994

local Administrators groups, 994-996

local client policies (WMI), 131

Local Service accounts, 92

Local System account rights, 997

LocationServices.log, 1083, 1092-1095

locking screens, 908

logs, 156, 688

Admin User Interface, 1087

audit, 991-993

backup, 1086

client, 1082-1084, 1093

locating/retrieving advertised content, 287

network issues, 284

combining, 162

ConfigMgr installation, reviewing, 373

Database Monitor dropping site configuration files, 162

DCM, troubleshooting, 805

debug, 805, 1080

enabling, 1080

intersite replication, 168-172

management point, 1086-1087

mobile devices

clients, 1088-1089

management, 1087-1088

NAL, 1081

NAP, 1092-1093

OOB Management, 1097-1098

OSD, 972, 1089-1092

PatchDownloader.log file, 763

reporting point server, 1081-1082

resources, 1079

server, 1084-1086

Service Manager components, 431

setup, 1082

SHV, 1092

site joins

delta site control file, 164-167

Hierarchy Manager, 164

new parent site replication, 167-168

smsprov.log, 158

smsts.log file, 972

software updates

clients, 1095-1096

site servers, 1094-1095

SQL, 158, 1081
 toggling on/off, 1080
 verbose, 501-502, 805, 1080
 viewing, 156
 Windows Update Agent, 1097
 WOL, 1094
 WSUS, 1096

low free disk space report, 855

M

MAC (Media Access Control) addresses, 925

machine accounts, 1020

Machine Policy Retrieval and Evaluation Cycles, 349

magic packets, 330

maintenance

databases, 1062-1065
 custom task, 1064
 Monitor Keys task, 1063
 Rebuild Indexes task, 1063
 SQL maintenance commands, 1064
 DDR retention, 1055-1060
 monitoring with OpsMgr, 1073
 obsolete records, 1060-1062
 OpsMgr, 735
 services, 1074
 status data, 1070
 tasks, 1049-1050
 windows
 software distribution advertisements, 745
 update deployments, 744-747

Maintenance Windows Available to a Particular Client report, 858

malware signature files, 312

man in the middle (MITM) attacks, 1015

manageability, 30

Managed Object Format (MOF), 355

management licenses (MLs), 180

management packs, 208, 1073

management points

client connectivity, testing, 281-282
 ConfigMgr installation, 370
 configuring, 540-541
 File Dispatcher, 140
 logs, 1086-1087
 offloading, 414-415
 publishing to DNS, 385
 role, 197
 site systems, 58, 391

managing

desktop, 29
 devices, 312-313
 benefits, 313
 client agent settings, 317
 client software installations, 315-317
 mobile devices supported, 312
 reports, 861
 site system communication, 314-315
 Windows CE operating systems, 313
 XP Embedded clients, 314
 drivers, 970
 Internet clients. See IBCM
 local accounts, 994
 malware signature files, 312
 mobile devices, 83-84
 patches, 307, 981
 IT process integration, 309
 ITMU, 708-709
 native mode sites, 749-751
 notifications, 707
 offline VMs, 742
 planning, 706-708
 political support, 707
 regulatory compliance, 308
 scheduling, 707
 scope, 706
 SCUP 733

SMS 2003, 747-749

Software Updates. *See* Software Updates

support, 307

testing, 706

third-party support, 706

Windows Update Agent, 708

WOL, 751

WSUS, 709

permissions, 997-999

power, 330

risks, 985-989

security logs, 993

updates, 34

WMI

remotely, 109

WMI Control. *See* WMI, Control

mandatory advertisements, 68

mandatory deployments, enforcing, 720

manual client deployment, 569-570

manual image creation and capture, 935-937

mass storage drivers, 958

master project schedule, 183

masters, 524, 931

McsExec.log, 1091

McsISAPI.log, 1091

McsMSI.log, 1091

McsPerf.log, 1092

McsPrv.log, 1091

McsSetup.log, 1091

MDMP (Mobile Device Management Point), 314

MDOP (Microsoft Desktop Optimization Pack), 628, 693

MDT (Microsoft Deployment Toolkit), 905, 930

Mean Time Between Failure (MTBF), 204

MEBx accounts, 1023

Media Access Control (MAC) addresses, 925

media image captures, 531-532

membership rules

collections, 858

direct, 651

dynamic collections, 650

query, 651

static collections, 643-646

memory, Windows Server support, 303

messages

audit, 1003

ID 4404, 425

ID 4405, 425

state, 801

status, 1065

data maintenance, 1070

DCM troubleshooting, 806-807

deleting, 1070

filter rules, 1065-1067, 1070-1072

filters, 863

queries, 828-830

replication, 1065-1066

reports, 862-865

summarizer data, 1069

metering software

overview, 67

reports, 862

methodologies, 13

methods

client discovery, 566-567

Win32_LogicalShareSecuritySetting, 119

WMI classes, 114

Microsoft

Application Virtualization for Terminal Services, 628

Center Pack Catalog website, 71

Certificate Services dialog box, 514

DCM configuration tools, 795-796

Deployment Toolkit (MDT), 905, 930

Desktop Optimization Pack (MDOP), 628, 693

DHCP FAQ website, 275

fallback status point documentation, 198

Official Curriculum (MOC), 183

official scenarios, 909

Operations Framework. *See* MOF

- Operations Manager (MOM), 611, 832
- product integration with DSI, 17-18
- Software Assurance program, 871
- Software License Terms dialog box, 448
- Solution Framework. *See* MSF
- Sysinternals website, 795
- System Center
 - Capacity Planner, 44
 - DPM, 43
 - Essentials, 41
 - operations management, 40
 - overview, 39
 - reporting, 39
 - Service Manager, 41-43
 - VMM, 44
- Volume Licensing Software (MVLS), 182, 872
- Microsoft IT Service Management strategy, 15-16**
 - DSI, 16-17
 - architectural elements, 18
 - importance, 18
 - Microsoft product integration, 17-18
 - SML, 19
 - infrastructure optimization, 25
 - Basic level, 27-28
 - Dynamic level, 28
 - Infrastructure Optimization Model, 26-27
 - Rationalized level, 28
 - Standardized state, 28
 - ISO 20000, 24-25
 - ITIL, 19
 - customer centric service organizations, 21
 - measurements, 21
 - MOF, compared, 24
 - overview, 19
 - version 3, 20-21
 - MOF
 - ConfigMgr support, 23-24
 - development, 21
 - ITIL, 22-24
 - MSF combination, 22
 - overview, 21-24
 - process model, 23-24
 - version 4, 21
- MIF files, inventory, 1033**
- Mifprovider.log file, 1083**
- migrating**
 - ConfigMgr environments to new environments, 1048-1049
 - side-by-side, 1106
 - user state, 940-941
 - virtual machines to Hyper-V article, 304
- migrating from SMS 2003**
 - hardware inventory files, 462-463
 - hierarchy customizing, 435
 - in-place upgrades, 435
 - database upgrade, 445-447
 - feature packs, 436
 - post-upgrade considerations, 457-458
 - prerequisite checker, running, 437-442
 - prerequisites, 436-437
 - primary site upgrade, 447-453
 - secondary site upgrade, 453-455
 - SMS 2003 client upgrades, 455-457
 - SQL Server upgrades, 442-445
 - WSUS, 458-459
 - interoperability, 463
 - planning, 433-435
 - side-by-side, 434, 459
 - clients, 460-461
 - database objects, 462
 - flowchart, 459
 - site boundaries, 460
 - troubleshooting, 463-464
- misdirection attacks, 1015**
- MITM (man in the middle) attacks, 1015**
- mixed mode**
 - configuration, 385-387
 - PKI, 326
 - reverting from native mode, 386

MLs (management licenses), 180

Mobile Device Center website, 316

**Mobile Device Client Agent Properties
dialog box, 553**

mobile devices

- client agents, 317, 553
- client software installations, 315-317
- logs
 - clients, 1088-1089
 - management, 1087-1088
- managing, 83-84, 314
- resources, 1107
- security, 1034-1035
- site system communication, 314-315
- supported, 312
- Windows CE operating system, 313
- Windows Mobile, 313

MOC (Microsoft Official Curriculum), 183

modes

- MOM maintenance, 611
- sites, 385-390
 - mixed, 385-387
 - native, 387-390
 - security, 193

MOF (Microsoft Operations Framework), 19

- ConfigMgr support, 23-24
- development, 21
- files
 - hardware inventory, migrating, 462
 - object definition exports, 138
- ITIL, 22-24
- MSF combination, 22
- object definition exports, 355
- overview, 21-24
- process model, 23-24
- version 4, 21

MOF (Managed Object Format), 355

MOM (Microsoft Operations Manager)

- OpsMgr installation program, 611
- reports, 832

Monitor Keys task, 1063

monitoring

- advertisements, 684-685
- CAL, 870
- ConfigMgr, 363, 1073
- Job Activity Monitor, 410
- networks, 356
- packages, 684-685
- performance, 207
- Software Updates, 761-762

mounting WIMs, 911

MP_ClientID.log, 1086

MP_ClientIDManager.log, 1089

MP_ClientREG.log, 1086

MP_Ddr.log, 1086

MP_DriverManager.log, 1086

MP_DriverMGR.log, 1089

MP_GetAuth.log, 1086

MP_GetPolicy.log, 1086

MP_GetSdmPackage.log, 1093

MP_Hinv.log, 1086

MP_Location.log, 1087-1089

MP_Policy.log, 1087

MP_RegistrationManager.log, 1087

MP_Relay.log, 1087

MP_Retry.log, 1087

MP_Sinv.log, 1087

MP_Status.log, 1087

Mpcontrol.log, 1085

Mpfdm.log, 1085

mpmsi.log file, 541, 1085

MPs (Management Packs), 208, 1073

MPSetup.log, 1085

MscMgr.log, 1091

MSF (Microsoft Solution Framework), 22, 175-176

- ConfigMgr deployment, 22
- deployment phase, 225-226
- development phase, 186
 - capacity planning, 207-210
 - centralized hierarchies, 188

- client architecture, 216-217
- ConfigMgr roles, 193-200
- flat hierarchies, 188
- ICP scenarios, 220-221
- ICP versioning, 219-220
- multilanguage scenarios, 218-219
- network infrastructure, 189-191
- roaming, 211-213
- scalability numbers, 187
- schema extensions, 191
- secondary site servers, 192
- server architecture, 201-207
- site boundaries, 210-211
- site design, 213-214
- site security modes, 193
- tiered hierarchies, 186

- envisioning phase, 176
 - architecture, 178
 - client architecture, 179
 - current environment assessment, 177
 - licensing, 179-182
 - network infrastructure, 177-178
 - server architecture, 179
 - training, 182-183
- MOF combination, 22
- piloting phase, 223-224
- planning phase, 183-186
 - implementation, 186
 - pilots, 185-186
 - POC, 184-185
- testing phase, 221-223
- website, 176

MTBF (Mean Time Between Failure), 204

Mtrmgr.log file, 1083

multicasting, 916-918

- configuring, 916-918
- disadvantages, 916
- properties, 917

Multilanguage scenarios, 218-219

- ICP, 219-220
- languages supported, 218

multiple collections, 664

multiple maintenance windows, 746

multiple PXE providers, 918

multisite configurations, 417

- child primary sites, installing, 422
- parent site attachment, 421-422
- secondary sites
 - installing, 422-423
 - troubleshooting, 424-426
- sender addresses, 417-421
- transferring settings between sites, 426-427

MVLS (Microsoft Volume Licensing Software), 182, 872

N

NAL (Network Abstraction Layer), 1081

named pipes, authentication, 229

names

- advertisements, 682
- dependent subcollections, 659
- dynamic collections, 650
- resolution
 - incorrect referrals, 280
 - security, 1026-1027
 - troubleshooting, 279-280
- static collections, 643

namespaces

- access, 996-997
- CIMV2
 - classes, 125
 - root classes, 116
 - viewing, 116
- Win32_LogicalShareSecuritySetting class, 116-124
- Root\CCM, 125-130
- SMS provider, 134

WMI

- classes, 115
- auditing, 111

NAP (Network Access Protection), 72, 519-520, 981

- AD schema extensions, 103
- clients
 - agent, 556, 755-756
 - communication, 235
- compliance, 758
- evaluating, 522-523
- logs, 1092-1093
- NPS, 520-521
- operating systems supported, 520
- overview, 72-73
- policies, configuring, 521-522
- ports, 235, 1107
- remediation, 522, 760
- reports, 861
- requirements, 755
- SoH, 522-524, 756-757

NAS (Network Attached Storage), 302**native mode, 193**

- clients, HTTP communication, 248
- configuration, 387
- enabling, 387-390
- OSD, 974-975
- PKI deployment, 325, 515-516
- reverting to mixed mode, 386
- Software Updates, 749-751

navigating, console, 468-469**.NET Framework, 807****NetDiag.exe utility, 279****Netdisc.log, 1085****Network Abstraction Layer (NAL), 1081****Network Access Protection. See NAP****Network Attached Storage (NAS), 302****network load balance (NLB), 208****Network Policy Server (NPS), 520-521, 755****networks**

- attacks, 1015
- discovery, 272-273, 564-566
 - Browse list, 276
 - configuring, 272
 - dependencies, 276
 - device information, accessing, 276
 - IP addresses, identifying, 275
 - network topology, 274-275
 - resources, 273
 - subnets, 273, 276
- infrastructure
 - developing, 189-191
 - envisioning phase, 177-178
- intermittent connections, 271-272
- intrasite communications, 228-229
 - basic network services, 234
 - delta replication, 233
 - differential replication, 234
 - HTTP/HTTPS, 232
 - RPC, 229
 - SMB, 231-232
 - SQL Server, 229
- issues
 - client installation, 283-284
 - communication, 289-290
 - site system installation, 282-283
 - software distribution, 286-287
 - SPNs, 284-285
- monitoring tools, 356
- reports, 856
- service accounts, 92
- troubleshooting
 - blocked/unresponsive ports, 280-281
 - configurations, 278-279
 - connectivity, 279
 - name resolution, 279-280
 - timeouts, 282

New Advertisement Wizard, 329, 679, 960

New Collection Wizard

- dynamic collections
 - membership rules, 650
 - names, 650
 - operating system versions, 653
 - query editing, 651
 - Vista/XP criteria, 651-654

- static collections
 - advertisements, 646
 - membership rules, 643-646
 - names, 643
 - security, 648

New Computer Association dialog box, 926**New Dashboard Wizard, 875-876****New Deployment Template wizard, 735****New Package Wizard, 621****New PC imaging scenario, 525****New Policies Wizard, 758****New Program Wizard, 623-625****New Publication Wizard, 406****New Query Wizard, 814-817**

- completing, 817
- criteria, 816-817
- General page, 814
- query statements, 815
- result properties, 816

New Report Wizard

- classic reports, 896
- Drill Through Sequence for a Specific Report, 896
- General page, 894
- Prompt Properties page, 894

New Site Role Wizard

- distribution point server role
 - account settings, 668
 - communication settings, 670
 - distribution point selection, 669
 - enabling, 669-671
 - FQDN settings, 668

group memberships, 671

security settings, 668

summary, 671

management points, 540

PXE service points, 919

state migration points, 921

SUP roles, 713-716

New Site System Server Share Wizard, 401**New Site System Server Wizard**

management point configuration, 415

PXE service points, 919

SUP role to site systems, adding, 713-716

New Site System Wizard, 401**New Software Metering Rule Wizard, 558-559****New Standard Sender Address Wizard**

priorities, scheduling, 418

rate limits, 419

New Status Filter Rule Wizard, 1067**New Subscription Wizard, 409-410**

Parameters page, 900

Schedule page, 898

Subscription Delivery page, 898

new system scenario (OSD), 908**New Task Sequence Wizard, 933****New Virtual Application Package Wizard, 632-633****New WQL Query Settings Properties dialog box, 793****NLB (network load balance), 208****nodes**

console, 66, 473-474, 810

Rights, 999

NOIDMIF files, 1033**noncompliance events, 792****NPS (Network Policy Server), 520-521, 755****NSlookup command, 280****Ntsvrdis.log, 1085****null values (queries), 819**

O

object model (WMI), 113-116**objects**

- attributes, viewing, 884
- auditing, 995
- configuration item properties, 783
- configuration items, 780
- definitions, exporting to MOF files, 138
- directory services, auditing, 990
- permissions, 1000-1003
- replicating, 407
- transferring, 355
- types, 812-813

Objreplmgr.log, 1094**obsolete records, 1060-1062**

- client discovery data, deleting, 1062
- creating, 1060
- tasks, 1061

Offermgr.log, 1085**Offersum.log, 1085****Office of Government Commerce (OGC), 19****offline clients, 284****offline image editing, 910-912****offloading**

- management points, 414-415
- site roles, 403

OGC (Office of Government Commerce), 19**OLAs (Operating Level Agreements), 24****on-demand results (DCM), 802****OoB (Out of Band), 105****Management**

- accounts, 1023-1024
- client installations, 584
- dependencies, 332
- logs, 1097-1098
- planning, 331-332
- scenarios, 584

support, 331

website, 584, 1104

service points, configuring, 395

Oobconsole.log, 1098**Oobmgmt.log, 1098****Opal, 48-50****Operating Level Agreements (OLAs), 24**

operating system deployment. See OSD

operating system environments (OSEs), 180-181

operating systems

- configuration items, 769
- deployment reports, 860

Operations Manager. See OpsMgr**operations reports, 857**

- DCM, 860-861
- device management, 861
- NAP, 861
- operating system deployment, 860
- software
 - distribution, 857-859
 - metering, 862
 - updates, 859-860
- status messages, 862-863
 - All messages for a specific message ID, 862-863
 - computer status, 862
 - details, viewing, 863-865
 - site function, 862
- WOL, 862

operators

- configuration item validation, 790
- queries, 820

OpsMgr (Operations Manager), 40

- advertisement, 686-688
- ConfigMgr monitoring, 1073
- installation program, configuring, 605
 - advanced options, 610-611
 - environment, 608-609
 - general settings, 605
 - installation source management, 611

- MOM maintenance modes, 611
- requirements, 605-607
- maintenance mode, 735
- package
 - creating with Create Package from Definition Wizard, 597-602
 - data access properties, 615-616
 - data source properties, 613-615
 - distribution properties, 617-618
 - general properties, 613
 - installation program, configuring, 613
 - package definition files, 613-620
 - programs, configuring, 602-605
 - reporting properties, 618
 - security properties, 619
- website, 1073
- optimizing**
 - disks, 205
 - infrastructure, 25
 - Basic level, 27-28
 - Dynamic level, 28
 - Infrastructure Optimization Model, 26-27
 - Rationalized level, 28
 - Standardized state, 28
 - queries, 902
- Organizational Units (OUs), 990**
- organizing configuration items, 771**
- OSD (operating system deployment), 30**
 - accounts, 1022-1023
 - automated image creation and capture, 931
 - packages, adding, 932-933
 - results, 934
 - task sequences, 932-934
 - automation/control, 33
 - boot images
 - distribution points, 924
 - drivers, adding, 925
 - PXE booting, 922
 - removable media, 922-924
 - computer associations, 925-926
 - New Computer Association dialog box, 926
 - recovery, 926
 - unknown computer support, 928-930
 - disk performance, 206
 - distribution points, 916-918
 - drivers, 966-969
 - adding to catalog, 967
 - adding to systems, 968
 - device, 969
 - images, 969-970
 - importing, 967
 - layering, 970
 - managing, 970
 - storing, 967
 - troubleshooting, 968
 - website, 971
 - error codes, 973
 - hardware, 913-915
 - hardware IDs, 965
 - image deployment, 937-939
 - operating system images, 938
 - software distribution packages, 938
 - task sequence, 937-939
 - imaging, 909-913
 - Install Packages, 931
 - logs, 972, 1089-1091
 - manual image creation and capture, 935-937
 - multicasting, 391, 1091-1092
 - native mode, 974-975
 - overview, 83
 - package availability, 964
 - planning, 328-330
 - post-deployment tasks, 971
 - PXE
 - deployment, 964
 - service points, 918-920
 - scenarios, 908-909
 - security, operational, 1032

SMS 2003 Feature Pack, 976

state migration points, 921

task sequences, 942-943

 change control, 962-963

 conditions, 944-946

 customizing, 960-963

 Disk tasks, 951-952

 Drivers tasks, 957-958

 General tasks, 948-951

 grouping, 946-947

 Images tasks, 955-957

 Settings tasks, 958-959

 targeting, 960-962

 task categories, 947

 testing, 965

 User State tasks, 952-954

 variables, 943-944

testing, 966

tools, 904

 BDD, 905

 ImageX, 906-907

 MDT, 905

 SIM, 907

 Sysprep, 904-905

 USMT, 905

 WAIK, 906

 Windows PE, 907

troubleshooting, 972

 advertisement status, 972

 command-line support, 974

 home page, 972

 smsts.log file, 972

 status reports, 973

Überbug, 965

user data, 940-941

Windows XP drivers, 964

OSDAppChooser, 960

OSEs (operating system environments), 180-181

OUTs (Organizational Units), 990

Out of Band. See OOB

P

Package Access accounts, 1023

package definition files, 355

 benefits, 620

 OpsMgr package, 613-620

 data access properties, 615-616

 data source properties, 613-615

 distribution properties, 617-618

 general properties, 613

 reporting properties, 618

 security properties, 619

 resources, 1106

packages, 588-593

 advertisements, 595

 App-V 4.5 client, 694

 automated deployment, 589

 benefits, 588

 collections, 591-594

 ConfigMgr compared to GPO-based
 distribution, 590-592

 consistency, 589

 copying, 428

 creating, 596-597

 deployment

 linking, 740

 software updates, 738-740

 source folders, 740

 distribution

 distribution points, 594-595, 742

 example, 595

 Forefront, 620

 configuring, 621-623

 creating with New Package Wizard, 621

 programs, adding, 623-625

 ITMU, 709

 loader tool, 429

 monitoring, 684-685

OpsMgr

- creating with Create Package from Definition Wizard, 597-602
- data access properties, 615-616
- data source properties, 613-615
- distribution properties, 617-618
- general properties, 613
- installation program, configuring, 613
- package definition files, 613-620
- programs, configuring, 602-605
- reporting properties, 618
- security properties, 619

overview, 68

Preload Package tool, 429

programs, 593-594

repackaging, 626-627

reusability, 590

scripted installations, 627

SoftGrid, 627

- App-V 4.5, 628

- example, 627

- functionality, 628

- SMS integration, 629

targeted deployment, 589

testing, 637-638

troubleshooting, 636-638

uninstalling software, 590

update, 709

virtual applications

- activating, 629-630

- allow virtual application package advertisement, 630

- creating, 632-633

- data source settings, 633

- general settings, 633

- importing, 630

- package source, 632

- prepackaged, 636

- security settings, 633

- sequenced applications packaging preparations, 632

- sequencing with App-V, 631

- summary, 633

packets, 234, 331

PAE (Physical Address Extension), 303

parent sites

- child relationships in site hierarchies, 296

- child site attachments, 421-422

patch management

- NAP, 754

- Client agent, 755-756

- client compliance, 758

- remediation, 760

- requirements, 755

- SoH, 756-757

- native mode sites, 749-751

- notifications, 707

- offline VMs, 742

- planning, 706-708

- political support, 707

- scheduling, 707

- scope, 706

- SCUP, 733

- SMS 2003, 747-749

- software

- ITMU, 708-709

- Software Updates, 709

- Windows Update Agent, 708

- WSUS, 709

- Software Updates

- catalog synchronization, 722

- client agents, configuring, 719-721

- compliance scanning, 722-724

- deployment packages, 738-740

- deployment templates, 733-735

- distribution, 725

- GPO settings, 721

- management flow, 740

- pilot group of workstations example, 727-728

- process, 722-727

- requirements, 710-712
- software update points, creating, 712-717
- synchronization, 718
- update deployments, 736-738
- update deployments best practices, 743-744
- update deployments implementation, 740-742
- update deployments maintenance windows, 744-747

- update lists, 731-733

- Update Repository, 728-731

- updates, choosing, 725

- testing, 706

- third-party support, 706

- troubleshooting

- client scans, 763

- downloads, 762-763

- monitoring, 761-762

- WSUS, 762

- WOL, 751

- configuring, 753-754

- implementing, 754

- requirements, 751-752

- subnet-directed, 752

- unicast, 752

PatchDownloader.log file, 763, 1094-1095

patches

- clients, 576

- managing, 307, 981

- IT process integration, 309

- regulatory compliance, 308

- support, 307

- software, 49

peel-off method, 343

pending status, secondary sites, 425

performance

- benchmarking, 207

- disks, 204-207

- arrays, 205

- characteristics, 204

- database sizes, 206

- distribution points, 206

- drive life cycle, 204

- I/O bottlenecks, 204

- optimization, 205

- OSD functionality, 206

- storage, 205

- monitoring, 207

- system, 203

perimeter networks, 320

permissions

- assigning, 996

- characteristics, 1000-1003

- class, 996

- DCOM, 497-498

- instance, 996

- managing, 997-999

- namespaces, 996-997

- System Management container, 99

- WMI, 498-499

Physical Address Extension (PAE), 303

physical controls, 986

pilot group of workstations software update

example, 727-728

piloting phase, 223-224

pilots

- planning, 185-186

- POC, 355-356

ping command, 279

pipes, named, 229

PKI (Public Key Infrastructure), 323-325, 342

- certificates

- CAs, 324

- deploying, 515-519

- native mode sites, 390

- requirements, 513-515

- templates, 516-517

- types, 324

- validation, 517

- certificates website, 508, 1104

- cryptography, 508-511
- encryption key length, 513
- mixed mode sites, 326
- native mode sites, 325
- overview, 324
- POC environment, 342
- requirements, 508
- SSL, 511-512

placement

- distribution points, 301
- reporting point role, 195
- servers, 269-271, 1006
- site databases, 188

plain text, 509

planning, 183-184

- certificate requirements, 324-326
- device management, 312-313
 - benefits, 313
 - client agent settings, 317
 - client software installations, 315-317
 - mobile devices supported, 312
 - site system communication, 314-315
 - Windows CE operating systems, 313
 - XP Embedded clients, 314
- hierarchies, sites, 293-298
- implementation, 186
- infrastructure, 292
- Internet-Based clients, 318
 - IBCM, 319
 - security, 321-323
 - server deployment, 320-321
 - VPNs, 318-319
- OOB Management, 331-332
 - dependencies, 332
 - support, 331
- OSD, 328-330
- patch management, 706-708
 - ITMU, 708-709
 - native mode sites, 749-751
 - notifications, 707

- offline VMs, 742
- political support, 707
- scheduling, 707
- scope, 706
- SCUP, 733
- SMS 2003, 747-749
- Software Updates. *See* Software Updates
- testing, 706
- third-party support, 706
- Windows Update Agent, 708
- WOL, 751-754
- WSUS, 709
- pilots, 185-186
- POC, 184-185
- resources, 1106
- simplifying, 91
- sites
 - antivirus scanning, 305
 - boundaries, 306
 - distribution point placement, 301
 - hardware sizing/configuring, 302-304
 - new site system roles, 301
 - security, 306
 - site system requirements, 300-302
 - site system roles, deploying, 299-300
 - site-to-site communication, 261
 - very large sites, 305
- SMS 2003 migrations to ConfigMgr, 433-435
- Software Updates, 307-309
 - architecture, 309-312
 - patch management, 307-309
 - points storage, 311
 - WSUSutil utility, 312
- testing, 221-223
- Windows Server 2008, 326-327
- WOL, 330-331
 - limitations, 331
 - requirements, 330
 - subnet-directed broadcasts, 331
 - unicast packets, 331

platforms

- console support, 482
- console supported, 64-65

POC (proof of concept), 184

- deliverables, 350
- documents, 337
- environment setup, 338-339
 - AD, 342-345
 - connected to production networks, 346-347
 - DNS, 342
 - lab, 340-342
 - PKI, 342
 - WINS, 342
- exit criteria, 350-351
- functional testing, 347-348
- goals, 337
- licensing, 346
- object transfers, 355
- pilot phase, 355-356
- planning, 184-185
- requirements, 337
- results, 357
- site settings transfers, 351-352
- stress testing, 348-350

policies

- agents, 131
- group, 267
 - BITS, 266-267
 - management website, 267
 - post-deployment tasks, 971
- health, 757
- NAP, configuring, 521-522

Policy Spy, 581**PolicyAgent.log file, 1083, 1095****PolicyAgentProvider.log file, 1083****PolicyEvaluator.log file, 1083, 1095****polycypv.log, 1085****political support, patch management, 707****polling intervals, 551****Port Detail dialog box, 245****PortQry command-line utility, 281****PortQryUI utility, 281****ports**

- client communication
 - customizing, 235
 - listing of, 235
 - specifying, 244-245
- HTTP inventorying, 545
- NAP, 235, 1107
- numbers, 235
- properties, 382
- selecting, 370
- troubleshooting, 280-281

Ports tab (Site Properties dialog box), 382**POST (Power-On Self-Test), 536****post-deployment tasks, 971****post-replication setup tasks (SQL replication), 410-413****power management, 330****PowerShell, file extension identification, 327****Pre-Boot Execution Environment. See PXE****predefined collections, 641****predefined reports, 842-844****Preload Package tool, 429****prepackaged virtual applications, 636****Prepare ConfigMgr for Client task, 956****Prepare Windows for Capture task, 956****preplanning worksheets website, 292****prerequisite checker, 363**

- resources, 1106
- SMS 2003 migrations, 437-442
 - GUID consistency, 440
 - options screen, 437
 - output, 438
 - schannel hotfix rule, 442
 - WSUS SDK on site server rule, 438

prerequisites. See also requirements

- ConfigMgr installation, 360
 - component downloads, 370
 - paths, 371
 - prerequisite checker, 363
 - SQL Server, 362
 - verification, 371
 - Windows components, 361-362
 - WSUS, 363

- console, 483

- SMS 2003 migrations, 436-437

- SRS subscriptions, 898

primary sites, 56-57

- child, 421-422

- ConfigMgr installation, 364
 - client agent selection, 368
 - completing, 373
 - custom/simple settings, 365
 - database servers, 368
 - licensing, 365
 - log files, reviewing, 373
 - management points, 370
 - port selection, 370
 - prerequisite components, 370-371
 - prerequisite verification, 371
 - previous installations, 364
 - product keys, 366
 - SCCM splash screen, 364
 - settings summary, 371
 - setup options, 364
 - silent, 374
 - site modes, 368
 - site settings, 366
 - site type selection, 366
 - SMS provider settings, 370
 - workstations, 365

- hierarchy, 295-296

- upgrades, 447, 450-453

- action status, monitoring, 450
 - completing, 452

- ITMU upgrade, 450

- licensing, 448

- options, 448

- updated prerequisites, 449

- WSUS installation, 451

priorities

- sender addresses, 418

- status filter rules, 259, 1067

privacy issues, 539**Process Monitor (ProcMon), 163, 795****processes**

- consistency, 13-14

- MOF process model, 23-24

programs. See applications; software**prompted values (queries), 819****proof of concept. See POC****protecting**

- distribution points, 672-674

- boundaries, 277

- configuring, 673

- site boundaries, 277, 417

protocols. See specific protocols**providers (WMI), 106****Proxy Account for Internet-Based Clients accounts, 1026****public forum resources, 1110-1111****Public Key Infrastructure. See PKI****published configuration data website, 71****Publishers page (Configure Distribution Wizard), 405****publishing, 403-406**

- Active Directory, 100-102

- disabling, 414

- management points to DNS, 385

- properties, 385

- Web, security, 193

pulling software, 76-77**pulse mode (bandwidth), 256****push installation (clients), 246****pushing software, 77**

PXE (Pre-Boot Execution Environment)

- booting, 922
- deployment, controlling, 964
- service points, 59, 82
 - configuring, 393-394, 919
 - OSD, 918-920
 - resources, 919
 - troubleshooting, 920

Pxecontrol.log, 1089

PXEMsi.log, 1089

PXESetup.log, 1090

Q

QST (Quiet System Technology), 537

qualifiers

- Win32_LogicalShareSecuritySetting, 123-124
- WMI classes, 115

queries

- advanced, 821
 - hardware scans within last 30 days, 823
 - Query Builder, 821
 - systems discovered since midnight, 823
 - WQL, 822
- attributes, 813, 819
- collections
 - building, 641
 - compared, 639-641
 - restrictions, 662
- creating, 811
- creating with New Query Wizard, 814-817
 - completing, 817
 - criteria, 816-817
 - general options, 814
 - query statements, 815
 - result properties, 816
- criterion, 819
- discovery data, 824-825
- editing, 651

- functions, 640
- inventory data, 825-826
- list of values, 819-820
- membership rules, 651
- null values, 819
- object types, 812-813
- operators, 820
- optimizing, 902
- prompted values, 819
- reports, compared, 818
- results
 - collections based on, creating, 827-828
 - exporting to text files, 826
 - importing/exporting between sites, 827
 - properties, 816
 - viewing, 810
- Service Manager components, 430
- simple values, 819
- statements, creating, 815
- status message, 828-830
- subselected values, 819
- values, 821
- viewing, 810
- visibility, 36
- WMIC, 779
- WQL, 811, 823

Queries node, 810

Query Builder, 821

Query Rule Properties dialog box, 643

Query Statement Properties dialog box, 815

queues, in-memory, 140

Quiet System Technology (QST), 537

R

RAID types article website, 304

RAS sender addresses, 417

RAS Sender Phone Book Account, 1021

rate limits, sender addresses, 419

Rationalized level (Infrastructure Optimization Model), 28

RDBMS (relational database management system), 845

RebootCoordinator.log, 1095

Rebuild Indexes task, 1063

records

conflicting, 383

DDRs

Active Directory example, 1059

creating, 562

data preservation for
troubleshooting, 1059

generating, 349

retention, 1055-1060

SMS 2.0 processing, 49

obsolete, 1060-1062

client discovery data, deleting, 1062

creating, 1060

tasks, 1061

ResourceIds, 384

recovering

POC testing, 348

previously captured user data, 926

recursive client discovery, 561

reducing TCO

infrastructure impact, minimizing, 77-80

remote management, 76

software distribution, 76-77

standardization, 75

reference PCs, 524, 931

references

App-V 4.5, 631

PKI certificate deployment, 519

systems, 909

Refresh PC imaging scenario, 525

Registry

console information, 491

Service Manager component
management, 431

Registry Monitor (RegMon), 795

regulatory compliance

configuration packs, 776

DCM, 766

software updates, 308

relational database management system (RDBMS), 845

relational databases, 844

SELECT statement, 845-847

joins, 846-847

Where clause, 846

tables, 845

views, 845

Release State Store task, 954

Remctrl.log file, 1083

remediation

DCM, 803-804

defined, 520

NAP, 522, 760

remote access clients, security, 35

Remote Activation permissions, 497

remote administrative access, 1003

remote helpdesk functions, 331

remote management, 76

Remote Procedure Call (RPC), 229

Remote tools

Client agent, 554-555

security, 1032-1033

removable media boot images, 922-924

repackaging software, 626-627

RepairWizard.log, 1087

Replace PC imaging scenario, 526

replication

binary delta, 670

delta, 670

intersite, viewing, 168-172

objects, 407

SQL, 403

disabling, 413-414

distributer replication, 405

management points, offloading, 414-415

- post-replication setup tasks, 410-413
- pre-replication setup tasks, 404-405
- publishers, 403, 406
- setup tasks, 405-410
- subscribers, 403, 409-410
- status messages, 1065-1066
 - status filter rules, 257-259
- stopping, 258
- tuning, 257-261

Replmgr.log, 1085, 1094

Report Builder website, 898

Report Options dialog box, 844

Reporting Services Point role, 301, 395, 837-839

reports

- accessibility, 200
- application compatibility, 873-874
- areas covered, 831
- Asset Intelligence, 83, 868
 - CAL monitoring, 870
 - catalog synchronization with System Center Online, 871
 - classes, enabling, 870
 - configuring, 870-872
 - license information, importing, 872
 - Synchronization Point site role, configuring, 871
 - viewing, 872-873

classic

- configuring, 835-836
- copying to SRS, 839, 842
- creating, 894-896
- security, 1027
- viewing from console, 478-479

compliance status, 775

computer details links, 854-855

configuring

- classic, 835-836
- SRS, 837-839

console links, 844

CSR, 865

- client management, 865-867

- ConfigMgr R2, 867-868

custom data

- discovery, 884-886
- external data sources, 889-893
- inventory, 887-889

customizing, 876

- appearance, 878-879
- column order, 878
- columns, 880
- data selection, 879
- rows, 880-883
- websites, 893

dashboards, 875-876

DCM, 801-802, 860-861

DCM configuration baselines, 775

device management, 861

hierarchy, 834

historical data, 861

home page, 38

inventory/discovery data, 848

- computer details, 853-854
- computer information for specific computers, 848-852
- computers matching specific criteria, 855
- computers with specific product names/versions, 855
- low free disk space, 855
- network, 856
- users, 856

Microsoft System Center, 39

MOM, 832

NAP, 861

operating system deployment, 860

operations, 857-859

OpsMgr package properties, 618

overview, 73-74

- points, 59
 - configuring, 394
 - logging, 1081-1082
 - placement, 195
 - requirements, 199
 - role, 199
 - predefined, 842-844
 - queries
 - compared, 818
 - optimizing, 902
 - relational databases, 844
 - SELECT statement, 845-847
 - tables, 845
 - views, 845
 - resources, 1106
 - security, 1027-1029
 - best practices, 1028
 - classic, 1027
 - SRS, 1027-1028
 - sites, 856-857
 - software distribution, 857
 - advertisements, 858
 - All Packages, 858
 - All resources in a specific collection, 858
 - Maintenance Windows Available to a Particular Client, 858
 - software metering, 862
 - software updates, 859-860
 - spreadsheets, adding, 852
 - SQL Reporting Services, 38, 832-834
 - SRS
 - classic reports, copying, 839, 842
 - configuring, 837-839
 - creating, 896-898
 - data source authentication, 837-839
 - security, 1027-1028
 - subscriptions, creating, 898-900
 - viewing from console, 480
 - status messages, 862-863
 - All messages for a specific message ID, 862-863
 - computer status, 862
 - details, viewing, 863-865
 - OSD, troubleshooting, 973
 - site function, 862
 - troubleshooting, 900-902
 - viewing
 - console, 478-480
 - Internet Explorer, 481-482
 - visibility, 37-39
 - WOL, 862
- Reports home page, 38**
- Request State Store task, 952**
- requirements. See also prerequisites**
- capacity, 207-210
 - NLB, 208
 - state migration points, 209-210
 - certificates, 324-326
 - DCM clients, 767
 - firewalls, 319
 - IBCM, 319
 - licensing, 179-182
 - CALs, 181
 - costs, 181-182
 - Standard/Enterprise Server MLs, 180
 - NAP, 522, 755
 - OpsMgr installation program, 605-607
 - PKI, 508, 513-515
 - POC, 337
 - reporting points, 199
 - roles, 201
 - site systems, 300-302
 - Software Updates, 710-712
 - SQL Server, 362
 - SRS subscriptions, 898
 - training, 182-183

- Windows components, 361-362
- WOL, 330, 751-752
- WSUS, 363
- Resource Explorer (Windows XP Professional client), 542**
- Resource IDs, viewing, 153**
- resource views, attributes, 154**
- ResourceExplorer.log, 1087**
- ResourceIDs, new records, 384**
- Restart Computer task, 951**
- Restore User State task, 954**
- restoring backups, 1041**
 - functional crashes, 1041-1045
 - new environment migrations, 1048-1049
 - server operating system crashes, 1041
 - site resets, 1045-1047
 - validating functionality, 1048
- result pane (console), 468**
- Result Properties dialog box, 816**
- results**
 - POC, 357
 - queries
 - collections based on, creating, 827-828
 - exporting to text files, 826
 - importing/exporting between sites, 827
 - properties, 816
 - viewing, 810
- Right Click tools, 478**
- right-clicking collections, 666**
- rights**
 - machine accounts, 1020
 - users, customizing, 997
- Rights node, 999**
- risk management, 985-980**
- risks, 985**
- roaming, 211-213, 666**
- roles, 193-194**
 - availability, 200
 - distribution points, 195-196
 - fallback status points, 197
 - management points, 197
 - NPS, 755
 - reporting points, 195, 199
 - Reporting Services Point, 837-839
 - requirements, 201
 - security, 1005
 - server locator points, 197
 - SHV, 196
 - sites
 - Asset Intelligence synchronization points, 395
 - branch distribution points, 399
 - deploying, 299-300
 - fallback status points, 393
 - new, 301
 - OOB service points, 395
 - offloading, 403
 - PXE service points, 393-394
 - reporting points, 394
 - reporting services points, 395
 - resource, 1103
 - server locator points, 397
 - servers, 194-195
 - SHV points, 399
 - state migration points, 398
 - SUPs, 398
 - Windows Server 2008 configuration, 326
 - software update points, 198-199, 713-716
 - Synchronization Point, 871
- root classes, CIMV2 namespace, 116**
- Root\CCM namespace, 125, 129-130**
- rows (reports), customizing, 880-883**
- RPC (Remote Procedure Call), 229**
- Rsetup.log, 1085**
- rules**
 - DCM configuration baselines, 772
 - status filter, 1065
 - criteria, 1070
 - customizing, 1067

- predefined, 1071-1072
- priorities, 1067
- status filters
 - configuring, 257-258
 - creating, 258
 - priorities, 259

Run Command Line task, 948, 960

runtimes, maintenance windows, 746

S

SA (Software Assurance), 871

SAN (Storage Area Network), 302

Sarbanes-Oxley Act, 308

SATA (Serial Advanced Technology Attachment), 204, 915

scalability, 57

- enhancements, 91
- numbers, 187

scanning

- clients for updates, 763
- compliance
 - compliance state, 723
 - forced/unforced, 724
 - Software Updates, 722-723
- schedules, 719

ScanAgent.log, 1095

ScanWrapper.log, 1095

SCCM Installation Prerequisite Check Options screen, 437

SCCM Setup Wizard. See Setup Wizard

scenarios requiring ConfigMgr, 8-9

schannel hotfix rule, 442

Sched.log, 1085

Scheduler (WMI), 132

Scheduler.log file, 1083

scheduling

- advertisements, 682, 689-690
- client agents, 543

collection updates, 646

maintenance windows, 745

patch management, 707

scans, 719

sender addresses, 254, 418

software, 707

updates, 658-659

schema

editing, 95

extensions, 93-95, 191

benefits, 102-103

ConfigMgr updates, 95

configuring sites to publish to Active Directory, 100-102

finishing tasks, 98

System Management container, 98-99

tools, 93-94

verifying, 98

viewing, 96

Schema Admins group, 94

scope, patch management, 706

screens, locking, 908

scripting

installations, 627

large client load simulations, 349

SCSI (Small Computer System Interface), 204

SCUP (System Center Updates Publisher), 311, 733

SDK resources, 1105

SDM (System Definition Model), 17

SDMAgent.log, 1092-1093, 1096

Sdmdiscagent.log, 1093

search bar (console), 469

Search Folder Criteria dialog box, 729

search folders

console, 469-471

Update Repository, 729-730

visibility, 36

secondary sites

- Creation Wizard, 423
- hierarchy, 295-296
- installing, 422-423
- pending status, 425
- servers, 57-58
 - developing, 192
 - distribution points, 58
- troubleshooting, 424-426
 - addresses, 426
 - secondary site pending status, 425
 - secure key exchanges, 424-425
- upgrades, 453-455

sector-based imaging, 528

secure HTTP (HTTPS), 232

Secure Sockets Layer (SSL), 511-512

security

- accountability, 985
- accounts, 982, 1019-1020
 - CSR, 1026
- database connections, 1021
- health state references, 1025-1026
- infrastructure support, 1020-1021
- OOB Management, 1023-1024
- OSD, 1022-1023
- Proxy Account for Internet-Based Clients, 1026
- software updates, 1025
- Active Directory trusted root keys, 1018
- administrative access, 982, 987-989
 - audit messages, 1003
 - copying Local System account rights to ConfigMgr administrative group, 997
 - job roles, managing, 988
 - local Administrators groups, 994-996
 - namespace, 996-997
 - operating system level, 989-991
 - outsourcing, 989
 - permission characteristics, 1000-1003
 - permissions, 996-999

remote, 1003

risk management, 987-989

user rights, editing, 997

Adobe Reader virtual application, 633

advertisements, 692

audit logs, 991-993

availability, 984

best practices, 987

certificates

native mode, enabling, 388

PKI, 324-236

communications, 982, 1015-1016

client to server, 1016-1018

server to server, 1018-1019

site-to-site, 1018-1019

confidentiality, 984

Configuration Wizard

Action page, 1009

Administrative and Other Options
page, 1010

Audit Policy page, 1012

Confirm Service Changes page, 1010

installing, 1008

Open Ports and Approve Applications
page, 1011

Registry settings page, 1012

Select Server page, 1009

site system security roles, applying,
1008-1012

templates, 1008

websites, 1012

console, 497

DCOM permissions, 497-498

WMI permissions, 498-499

controls, 986

cryptography, 508-511

day-to-day operations, 983

DCM, 770, 982

digital signing, 511

encryption, 1016

- enhancements, 29
- fallback status points, 82
- features, 8, 90
- goals, 984
- hardware, 1007
- hierarchy, 982, 1004-1006
- IDS/IPS, 190
- integrity, 984
- Internet clients
 - Active Directory forests, 321
 - dedicated sites, 321-323
 - internal/perimeter network site span, 322
 - management, 34
 - site-to-site communication, 321
- inventory, 546
- IO Model, 983
- IPSec, 1019
- key exchanges, 385, 424-425
- local accounts, 994
- name resolution, 1026-1027
- NAP, 72, 519-520, 981
 - AD schema extensions, 103
 - client agent properties, 556, 755-756
 - client communication, 235
 - compliance, 758
 - evaluating, 522-523
 - logs, 1092-1093
 - NPS, 520-521
 - operating systems supported, 520
 - overview, 72-73
 - policies, configuring, 521-522
 - ports, 235, 1107
 - remediation requirements, 522
 - reports, 861
 - SoH, 522-524, 756-757
- network attacks, 1015
- operations
 - administration, 1029-1030
 - inventory, 1033-1034
 - mobile devices, 1034-1035
 - OSD, 1032
 - Remote tools, 1032-1033
 - software distribution, 1030-1032
- OpsMgr package, 619
- overview, 74-75
- patch management, 981
- PKI certificates, 390
- policies, testing, 1012
- privacy issues, 539
- programs, 983
- remote access clients, 35
- reports, 1027-1029
 - best practices, 1028
 - classic, 1027
 - SRS, 1027-1028
- resources, 1105
- risk management, 985-986
- server deployment to Internet-Based clients, 320
- sites, 1007
 - attack surface reduction, 1007, 1012
 - boundary protection, 417
 - databases, 1015
 - hardware, 1007
 - modes, developing, 193
 - planning, 306
 - policies, applying, 1008-1012
 - server hardening, 1007
 - software, 1007, 1013-1015
- software metering, 559
- SQL Server, 1004
- SSL, 511-512
- standard distribution points, 669
- static collections, 648
- systems management, 11
- updates, managing, 34
- web browsing, 1029
- web publishing, 193

websites, 1007

WMI, managing, 109

Security rights node, 473

Security tab (WMI Control), 109

Select Distributer page (Configure Distribution Wizard), 405

SELECT statements, 845-847

selecting

client agents, 368

collections for exclusion, 661

discovery methods, 566

ports, 370

site security, 1005

software updates for deployment, 725

Sender.log, 1085

senders

addresses

bandwidth, 254

configuring, 253-256, 417-421

creating, 418

destinations, 253

priorities, scheduling, 418

properties, 420

rate limits, 419

schedules, 254

configuring, 251-252

courier, 252

defined, 251

infrastructure impact, minimizing, 78

overview, 69

standard, 251-252

sequences (tasks), 329

sequencing virtual applications with App-V 4.5, 631

Serial Advanced Technology Attachment (SATA), 204, 915

Server Message Block (SMB) protocol, 231-232

Server Virtualization Validation Program (SVVP), 304

servers

architecture, 201

database servers, 201-202

disk performance, 204-207

envisioning phase, 179

performance monitoring, 207

system performance, 203

communications

client to server security, 1016-1018

server to server security, 1018-1019

components, 58, 390

database, 201-202

counters, 201

site system installations, 393

deploying, 320-323

distribution points as, 667

hardening, 1007

ISA, 193

locator points, 59

client specification, 397

configuring, 397

role, 197

log files, 1084-1086

NPS, 520-521

operating system crash recovery, 1041

placement, 269-271, 1006

reporting points, 1081-1082

secondary sites, developing, 192

share distribution points, 667

site, 58-60

antivirus scanning, 305

database, 58

defined, 56

hardware sizing/configuring, 302-304

PKI certificate deployment, 518

primary, 56-57

role, 194-195

secondary, 57-58

site installations, 391

- very large sites, 305
- software update, 1094-1095
- SQL Server
 - auditing services website, 1004
 - Books Online, 1004
 - query optimization, 902
 - security, 1004
 - Surface Area Configuration tool, 1013
 - upgrading, 442-445
- Systems Management Server. *See* SMS
- Windows, 303
- Windows Server 2003, 514-515
- Windows Server 2008
 - Certificate Services installation, 515
 - configuration, 362
 - planning, 326-327
 - reports, configuring, 836
 - site system role configuration, 326
- WMI for server operations, 134
 - exporting object definitions to MOF files, 138
 - SMS provider namespace views, 134
 - WMI behind collections, exploring, 136-138
- Service Management Functions (SMFs), 43**
- Service Manager, 41-43**
 - accessing, 429
 - actions, 500-501
 - components, 429-431
 - logging properties, 431
 - querying components, 430
 - starting, 500
- Service Modeling Language (SML), 17-19, 797**
- service operation (ITIL v3), 20**
- service packs**
 - ConfigMgr Service Pack 1, 55
 - ConfigMgr Service Pack 2, 55-56
 - installing, 374-376
 - hierarchy attachments, 376
 - performing, 376-378
 - site database upgrade tests, 375-376
 - SMS 2.0, 50
 - SMS 2003, 52-53
- Service Principal Names (SPNs), 284-285, 1015**
- services**
 - delivery, testing, 348
 - ITIL v3, 20
 - maintenance, 1074
 - WMI, invoking, 104
- ServiceWindowManager.log, 1096**
- Set Task Sequence Variable task, 951**
- Settings tasks, 958-959**
- Setup Actions Status Monitoring dialog box, 450**
- setup logs, 1082**
- Setup Prerequisite Checks website, 440**
- Setup Windows and ConfigMgr task, 956**
- Setup Wizard**
 - Client Agent Selection page, 368
 - completing, 373
 - console installation, 483-490
 - completing, 490
 - Customer Experience Improvement Program Configuration page, 483
 - destination folders, 486
 - installation prerequisite check, 486
 - installation status, 486
 - licensing, 483
 - options, 483
 - site server selection, 486
 - summary, 486
 - Database Server page, 369
 - Installation Prerequisite Check page, 371
 - Installation Settings page, 365
 - Management Point page, 370
 - primary site upgrades
 - action status, monitoring, 450
 - completing, 452
 - licensing, 448
 - options, 448

- updated prerequisites, 449
- welcome screen, 448
- Port Settings page, 370
- Settings Summary page, 371
- Setup Action Status Monitoring page, 371
- Site Settings page, 366
- Site Type page, 366
- SMS Provider Settings page, 370
- splash screen, 364
- Updated Prerequisite Components page, 371
- Setupact.log, 1090**
- Setupapi.log, 1090**
- Setuperr.log, 1090**
- shares, site system servers, 401
- SHAs (System Health agents), 757-758**
- Shields, Greg, 29**
- SHV (System Health Validator), 1092**
 - logs, 1092
 - points, configuring, 60, 399
 - role, 196
- side-by-side migrations, 434**
 - OSD, 909
 - resources, 1106
 - SMS 2003 to ConfigMgr, 459
 - clients, 460-461
 - database objects, 462
 - flowchart, 459
 - site boundaries, 460
- silent installation of ConfigMgr, 374**
- SIM (Subscriber Identity Module), 907**
- Simple Network Management Protocol (SNMP), 274-275**
- Simple Object Access Protocol (SOAP), 16**
- simple values (queries), 819**
- simplicity, 30**
- Sinvproc.log, 1085**
- Site Address account, 1021**

Site Mode tab (Site Properties dialog box), 385-390

- mixed mode, 385-387
- native mode, 387-390

Site Properties dialog box, 380

- Advanced tab, 382-385
- General tab, 380
- parent site attachment, 421
- Ports tab, 382
- Site Mode tab, 385-390
 - mixed mode, 385-387
 - native mode, 387-390
- Wake On LAN tab, 380-382

Site Replication Service. See SRS

Site Role Wizard, 393-400

- Asset Intelligence synchronization points, 395
- branch distribution points, 399
- fallback status points, 393
- OOB service points, 395
- PXE service points, 393-394
- reporting points, 394
- reporting services points, 395
- server locator points, 397
- SHV points, 399
- state migration points, 398
- SUPs, 398

Site System Installation accounts, 1020

site-to-site communications

- accounts, 1021
- Internet clients, 321
- security, 1018-1019

Sitecomp.log, 1085

Sitectl.log, 1085

sites

- addresses
 - overview, 69
 - throttling, 419
- automatic assignment, 306

- backing up, 436, 1037-1038
 - daily, 1040
 - enabling, 1038
 - file structure, 1040
 - folders created, 1039
 - new environment migrations, 1048-1049
 - restoring, 1041-1047
 - validating functionality, 1048
 - weekly, 1040
- bandwidth throttling, 252
- boundaries, 277
 - AD sites as, 277
 - configuring, 415
 - controlling, 277
 - defining as slow/fast, 262-263
 - planning, 210-211, 306
 - protecting, 277, 417
 - side-by-side migrations, 460
 - SMS 2003 migrations, 458
 - updating, 289
- central, 293
- child primary, 421-422
- client assigned, 247-248
- codes, 293
- communication, 251
 - components, 149
 - data compression, 261
 - data priorities, 257
 - sender addresses, configuring, 253-256
 - senders, configuring, 251-252
 - site planning, 261
 - status message replication, tuning, 257-261
- Component Manager, 140
- configuration files, dropping, 162
- control file, 147
- Control Manager, 147
- creating, New Site System Wizard, 401
- databases
 - backing up, 1063
 - connection accounts, 1021
 - copying, 375
 - data deletion, 883
 - maintenance, 1062-1065
 - multiple, 369
 - security, 1015
 - servers, 58
 - upgrade tests, 375-376
 - upgrading to SQL Server 2008, 362
- dedicated Internet clients, 321-323
- defined, 58-60
- deploying, Virtual Machines, 304
- designing, 213-214
 - 25,000 client environments, 215
 - 50,000–100,000 client environments, 215
 - greater than 100,000 client environments, 216
 - smaller environments, 214
- distribution point placement, 301
- hierarchies, 60, 293
 - codes, 293
 - designing, 293-295
 - documenting, 298
 - Hierarchy Manager, 147
 - parent/child relationships, 296
 - primary versus secondary, 295-296
 - three-tiered example, 294-297
 - two-tiered example, 296-297
- importing/exporting queries between, 827
- installing, 390-401
 - automatically, 390-393
 - component servers, 390
 - database servers, 393
 - distribution points, 390
 - management points, 391
 - roles, adding, 393-400

- site servers, 391
- troubleshooting, 429
- verifying, 429
- intersite replication, 168-172
- joining
 - delta site control file log entries, 164, 167
 - Hierarchy Manager logs, 164
 - Hierarchy Manager status message, 164
 - new parent site replication log entries, 167-168
 - Process Monitor, 163
 - status messages, 159-161
- latency, 256
- maintenance
 - DDR retention, 1055-1060
 - obsolete records, 1060-1062
 - tasks, 1049-1050
- Management node, 473
- mixed mode, PKI, 326
- mobile device communication, 314-315
- modes, 385-390
 - mixed, 385-387
 - native, 387-390
- multisite configuration, 417
 - child primary sites, installing, 422
 - parent site attachment, 421-422
 - secondary sites, installing, 422-423
 - secondary sites, troubleshooting, 424-426
 - sender addresses, 417-421
- native mode, PKI, 325
- network installation issues, 282-283
- new, 82
- PKI certificate deployment, 518
- planning
 - antivirus scanning, 305
 - boundaries, 306
 - distribution point placement, 301
 - hardware sizing/configuring, 302-304
 - new roles, 301
 - requirements, 300-302
 - roles, deploying, 299-300
 - security, 306
 - site-to-site communication, 261
 - very large sites, 305
- primary. *See* primary sites
- properties, 380
 - advanced, 382-385
 - conflicting records, 383
 - editing, 147-148
 - general, 380
 - ports, 382
 - publishing, 385
 - secure key exchanges, 385
 - site modes, 385-390
 - SQL view, 151-152
 - WOL, 380-382
- protecting, 277
- publishing to Active Directory, configuring, 100-102
- replicating data between, 149
- reports, 856-857
- requirements, 300-302
- resets, 1045-1047
- roles
 - deploying, 299-300
 - new, 301
 - offloading, 403
 - security, 1005
 - Windows Server 2008 configuration, 326
 - website, 1103
- secondary
 - hierarchy, 295-296
 - installing, 422-423
 - pending status, 425
 - troubleshooting, 424-426
 - upgrading, 453-455
- security
 - attack surface reduction, 1007, 1012
 - databases, 1015
 - hardware, 1007

- modes, developing, 193
 - planning, 306
 - policies, applying, 1008-1012
 - selecting, 1005
 - server hardening, 1007
 - software, 1007, 1013-1015
- servers
 - databases, configuring, 845
 - defined, 56
 - PKI certificate deployment, 518
 - primary, 56-57
 - role, 194-195
 - secondary, 57-58
 - shares, 401
 - site system installations, 391
- settings, transferring, 351-352
- SQL replication, 403
 - disabling, 413-414
 - distributers, configuring, 405
 - management points, offloading, 414-415
 - post-replication setup tasks, 410-413
 - pre-replication setup tasks, 404-405
 - publishers, 406
 - setup tasks, 405-410
 - subscribers, 409-410
- SUP role, adding, 713-716
- system installations, testing, 347
- upgrading, 374
- Sitestat.log, 1085**
- sitewide settings, 62**
- Six Sigma, 25**
- size
 - client caches, 683
 - databases, 206
 - site servers, 302-304
- slow networks, site boundaries, 262-263**
- Small Computer System Interface (SCSI), 204**
- SMB (Server Message Block) protocol, 231-232**
- SMFs (Service Management Functions), 43**
- SML (Service Modeling Language), 19**
 - configuration items/baselines, editing, 797
 - IT Service Management, 19
 - resources, 19
 - SDM, compared, 17
 - website, 797
- Smplsapi.log, 1090**
- Smpmgr.log, 1090**
- SmpMSI.log, 1090**
- SMS (Systems Management Server), 47**
 - 1.1, 47
 - 1.2, 48
 - 2.0
 - DDR processing, 49
 - inventory, 49
 - license enforcement, 49
 - overview, 48
 - service packs, 50
 - software metering, 49
 - software updates/patches, 49
 - 2003, 50
 - Active Directory integration, 50-51
 - Advanced Client, 51-52
 - Asset Intelligence, compared, 868
 - changes, 50
 - clients, upgrading, 455-457
 - ConfigMgr 2007, compared, 53-55
 - DCM feature pack conversion, 765
 - OSD Feature Pack, 976
 - R2 (Release 2), 53
 - service packs, 52-53
 - Site Boundaries dialog box, 460
 - software updates, 747-749
 - Admins group, Remote Activation permissions, 497
 - database objects, 462
 - Map, hierarchy documentation, 298
 - Object Generator, 349-350
 - provider namespace, WMI views, 134

- providers, 58
- Right Click tools, 478
- SoftGrid integration, 629
- SQL Monitor, SMS 2003 migrations, 458
- Trace, ConfigMgr installation, monitoring, 363

SMS 2003 migrations

- hardware inventory files, 462-463
- hierarchy customizations, 435
- in-place upgrades, 435
 - database upgrade, 445-447
 - feature packs, 436
 - post-upgrade considerations, 457-458
 - prerequisite checker, running, 437, 440-442
 - prerequisites, 436-437
 - primary site upgrade, 447, 450-453
 - secondary site upgrade, 453-455
 - SMS 203 client upgrades, 455-457
 - SQL Server upgrades, 442-445
 - WSUS, 458-459
- interoperability, 463
- planning, 433-435
- side-by-side, 434, 459
 - clients, 460-461
 - database objects, 462
 - flowchart, 459
 - site boundaries, 460
- troubleshooting, 463-464
- v4. See ConfigMgr

SMS_Client WMI class, 129**SMS_Collection class, 136-138****SMS_Def.mof file, 126, 545-546****SMS_SCI_SiteDefinition class, 156****SMS_Site class, 134****SMS Site – Client Information report, 865****SMS Site – Discovery and Inventory report, 866****SMSAdminUI.log, 1087****Smsbkup.log, 1086****Smscliui.log file, 1083, 1096****SmsClrHost.log, 1093****Smsdbmon.log, 1086, 1094****Smsexec.log, 1086****Smsprov.log, 158, 1086-1090****Smspxe.log, 1090****SMSReportingInstall.log, 1086****SMSSha.log, 1092****SmsSHV.log, 1092****SmsSHVADCacheClient.log, 1093****SmsSHVCacheStore.log, 1093****SmsSHVQuarValidator.log, 1093****SmsSHVRegistrySettings.log, 1093****SMSSHVSetup.log, 1093****SMSSMPSetup.log, 1090****Smssqlbkup.log, 1086****Smsts.log, 1090****smsts.log file, 972****Smswriter.log, 1086****SmsWusHandler file, 1096****snap-ins, 467**

- adding, 491

- ADSIEdit MMC, 562

sniffer-based attacks, 1015**SNMP (Simple Network Management Protocol), 274-275****SOAP (Simple Object Access Protocol), 16****SoftGrid, 627**

- App-V 4.5, 628

- example, 627

- functionality, 628

- SMS integration, 629

Softricity, 627**software. See also applications; tools**

- client, mobile device installations, 315-317

- deployment
 - automation/control, 32-33
 - website, 626

- distribution, 76

- advertisements, 745

- network issues, 286-287

- packages, creating, 938

- pulling software, 76-77
- pushing software, 77
- security, 1030-1032
- troubleshooting, 702
- evaluation, 346
- inventory, 62-64, 825
 - client agent, 62-64, 546
 - file collection, 547
 - filenames, 546
 - names, 548
 - Processor, 140
- metering, 67, 557-559
 - privacy, 559
 - SMS 2.0, 49
- MVLS, 872
- packages. *See* packages
- post-deployment tasks, 971
- repackaging, 626-627
- reports
 - compatibility, 873-874
 - distribution, 857-859
 - metering, 862
 - updates, 859-860
- resource websites, 1103
- security, 1007
 - antivirus, 1013
 - virus scanning exclusions, 1013-1015
- third-party software
 - DCM configurations, 796
 - hardware configuration packs, 776
 - patch management, 706
 - websites, 1113
- uninstalling, 588
- updates. *See* Software Updates
- Software Assurance (SA), 871**
- Software Update Points. *See* SUPs**
- Software Updates, 709**
 - accounts, 1025
 - architecture, 309-312
 - client agent, 559-560, 719-721
 - configuration items, 769
 - configuring with NLB article, 712
 - deployments, 736
 - best practices, 743-744
 - creating, 736-737
 - deadlines, 737-738
 - implementing, 740-742
 - maintenance windows, 744-747
 - packages, 738-740
 - templates, 733-735
 - home page, 36
 - GPO settings, 721
 - ITMU, 708-709
 - logs
 - clients, 1095-1096
 - site servers, 1094-1095
 - malware signature files, 312
 - management flow, 740
 - monitoring, 761-762
 - NAP, 754
 - Client agent, 755-756
 - client compliance, 758
 - remediation, 760
 - requirements, 755
 - SoH, 756-757
 - native mode sites, 749-751
 - notifications, 707
 - offline VMs, 742
 - patch management, 307-309
 - pilot group of workstations example, 727-728
 - planning, 307-309, 706-708
 - political support, 707
 - process, 722-727
 - catalog synchronization, 722
 - compliance scanning, 722-724
 - distribution, 725
 - updates, choosing, 725
 - regulatory compliance data, 308
 - requirements, 710-712
 - risks of delaying, 307

- scheduling, 707
- scope, 706
- SCUP, 733
- SMS 2.0, 49
- SMS 2003, 747-749
- synchronization, 718
- testing, 706
- third-party support, 311-312, 706-709
- troubleshooting
 - client scans, 763
 - downloads, 762-763
 - monitoring, 761-762
 - WSUS, 762
- update lists, 731-733
 - hierarchies, 733
 - updates, adding, 732
 - viewing, 731
- Update Repository, 728-731
- virtual applications, 636
- WOL, 751
 - configuring, 753-754
 - implementing, 754
 - requirements, 751-752
 - subnet-directed, 752
 - unicast, 752

SoftwareDistribution.log, 1096

SoftwareDistributionClientConfig class, 132

SoH (Statement of Health), 756

- caching versus fresh, 557
- NAP, 522-524, 756-757

sometimes-connected users, 271-272

source files, compression, 601

source folders, packages, 740

SPNs (Service Principal Names), 284-285, 1015

spoofing attacks, 1015

SQL Server

- auditing services website, 1004
- Books Online, 1004
- ConfigMgr database access, 150

- database maintenance commands, 1064

- intrasite communication, 229

- logging, 158, 1081

- Management Studio views, 150

- collections, 150-151

- DiscoveryArchitectures table data, 153

- inventory architecture groups, 154

- Resource IDs, 153

- resource view attributes, 154

- schema, 152-153

- site properties, 151-152

- Profiler website, 158

- queries, 902

- relational databases, 844-847

- replication, 403

- disabling, 374-378, 413-414

- management points, offloading, 414-415

- post-replication setup tasks, 410-413

- pre-replication setup tasks, 404-405

- publishers/subscribers, 403

- setup tasks, 405-410

- Reporting Services, 38, 832-834

- requirements, 362

- security, 1004

- statements, 848

- support, 85-86

- Surface Area Configuration tool, 1013

- Surface Area Configuration Wizard, 404

- upgrading, 442-445

- performing, 444-445

- Upgrade Advisor, running, 442-443

- WQL conversions, 823

SRS (Site Replication Service)

- subscriptions, creating, 898-900

- reporting

- classic reports, copying, 839, 842

- configuring, 837-839

- creating, 896-898

- data source authentication, 837-839

- security, 1027-1028
- User Properties dialog box, 1028
- viewing from console, 480

Srvacct.log, 1086

SSL (Secure Sockets Layer), 511-512

stand-alone task sequence media, 923

standard distribution points, adding to Wildflower site server, 667

- account settings, 668
- communication settings, 670
- completing, 671
- distribution point selection, 669
- enabling, 669
- enabling as branch distribution point, 671
- FQDN settings, 668
- group memberships, 671
- security settings, 668

standard senders, 251-252, 417

Standard Server MLs, 180

standardization, 75

Standardized state (Infrastructure Optimization Model), 28

Start to Finish Guide to MOF Editing, 546

state

- DCM messages, 801
- migration points, 59
 - capacity planning, 209-210
 - configuring, 398
 - OSD, 921
 - properties, 210
- System components, 140

Statement of Health (SoH), 522-524, 557, 756-757

StateMessage.log, 1096

Statesys.log, 1086

static collections, 594, 642

- creating, 642-644, 648
 - advertisements, 646
 - membership rules, 643-646

- names, 643

- security, 648

- dynamic additions, 648-649

Statmgr.log, 1086

status filters, 257-259, 863

status messages, 156, 1065

- client network issues, 284
- data maintenance, 1070
- DCM troubleshooting, 806-807
- deleting, 1070
- Distribution Manager issues, 286
- filter rules, 1065
 - criteria, 1070
 - customizing, 1067
 - predefined, 1071-1072
 - priorities, 1067

- filters, 863

- Hierarchy Manager, 164

- queries, 828-830

- replication, 1065-1066

- status filter rules, 257-259

- stopping, 258

- tuning, 257-261

- reports, 862-863

- All messages for a specific message ID, 862-863

- computer status, 862

- details, viewing, 863-865

- site function, 862

- site joins, 159-161

- summarizer data, 1069

status reports, 973

StatusAgent.log file, 1083

storage

- code, 139
- disks, 205
- distribution point data, 672
- drivers, 915, 967
- installation files, 598
- software update points, 311

Storage Area Network (SAN), 302

stress testing, 348-350

string replacements, 944

subcollections, 67, 657

advertisement options, 682

dependent, 657-659

names, 659

linked, 657-660

subnet-directed broadcasts, 331, 382, 1031

subnet-directed WOL, 752

subnet masks, network discovery, 276

Subscriber Identity Module (SIM), 907

subscribers, 403, 409-410

subscriptions (SRS), 898-900

subselected values (queries), 819

support

BITS versions, 265-266

clients, 86

console platforms, 64-65

distribution/software update points, 302

memory, 303

mobile devices, 312

OOB Management, 331

patch management, 307-308

SQL, 85-86

third-party software, 706

SUPs (Software Update Points), 59, 80, 198

activating, 559

client deployment, 574

Component Properties dialog box, 716

configuring, 398

Connection accounts, 1025

creating, 712-716

active SUPs, 714

classification selection, 715

product selection, 715

proxy server information, 714

synchronization schedule, 715

synchronization source, 714

WSUS components, 717

NAS support, 302

network load balanced, 208

Proxy Server accounts, 1025

resource websites, 1104

role, 198-199

SAN support, 302

storage, 311

SUPSetup file, 1095

Surface Area Configuration tool, 1013

SVVP (Server Virtualization Validation Program), 304

Swmproc log file, 1086

SWMTRReportGen.log file, 1084

symmetrical encryption, 509

synchronization

catalog, 722

Software Updates, 718

Synchronization Manager (WSUS), 718

Synchronization Point site role, 871

Sysprep, 904-905

System Center

Alliance members website, 358

resources, 1109-1110

Visio Pro add-ins, 893

System Center Updates Publisher (SCUP), 311, 733

System Definition Model (SDM), 17

System Health agents (SHAs), 757-758

System Health Validator (SHV), 60, 196, 399, 1092

System Resource class, 824

System Status node, 473

systems

accounts, 92

boards, 535

classes, 114

management, 9

AD containers, 98-99

asset data, 12

automation, 10-12

- change identification, 11
- defined, 14
- distributed enterprise challenges, 10
- IT service triangle, 14-15
- Microsoft IT Service Management strategy. *See* ITSM
- problems, 10
- process consistency, 13-14
- security/control, 11
- virtualization, 13
- performance, 203
- validating, 661

Systems Management Server. *See* SMS

T

tables, relational databases, 845

targeted deployment, packages, 589

tasks

- Backup ConfigMgr Site Server, 1037
 - default configuration, 1038
 - enabling, 1038
 - file structure, 1040
 - folders created, 1039
- categories, 947
- database maintenance, 1063-1064
- Delete Aged Status Messages, 1070
- Delete Obsolete Client Discovery Data, 1062
- Delete site maintenance, 1061
- Disk, 951-952
- Drivers, 957-958
- General, 948-951
 - Connect to Network Folder, 950
 - Install Software, 949
 - Install Software Updates, 950
 - Join Domain or Workgroup, 950
 - Restart Computer, 951
 - Run Command Line, 948
 - Set Task Sequence Variable, 951

- Images, 955-957
 - Apply Data Image, 956
 - Apply Operating System Image, 955-956
 - Capture Operating System Image, 957
 - Install Deployment Tools, 956
 - Prepare ConfigMgr for Client, 956
 - Prepare Windows for Capture, 956
 - Setup Windows and ConfigMgr, 956

post-deployment, 971

sequences, 942

- accounts, 1022-1023
- action/built-in variables, 943
- advertising, 329
- change control, 962-963
- conditions, 944-946
- creating, 933-934
- customizing, 960-963
- error codes, 973
- grouping, 946-947
- image deployment, 937-939
- Media Wizard, 936
- OSD, 943
- overview, 70
- preparations, 932
- resources, 1107
- targeting, 960-962
- testing, 965
- variables, 943-944

Settings, 958-959

site maintenance, 1049-1050

site resets, 1045

update management, automation, 7

User State, 952-954

- Capture User State, 953
- Release State Store, 954
- Request State Store, 952
- Restore User State, 954

TaskSequenceProvider.log, 1091

TCO (total cost of ownership), reducing, 17

- infrastructure impact, minimizing, 77-80
- remote management, 76
- software distribution, 76-77
- standardization, 75

TCP (Transmission Control Protocol), 229

technical controls, 986

technical training, 183

templates

- PKI certificates, 516-517
- Security Configuration Wizard, 1008
- update deployment, 733-735

testing, 221-223

- application distribution, 694
- clients
 - functionality, 582
 - management point connectivity, 281-282
- collections, 694
- environments, virtualization, 341
- infrastructure impact, minimizing, 79
- OSD, 966
- packages, 637-638
- patches, 706
- planning, 221-223
- POC
 - deliverables, 350
 - environment, 338-347
 - exit criteria, 350-351
 - functional, 347-348
 - goals, 337
 - object transfers, 355
 - pilot phase, 355-356
 - results, 357
 - site settings transfers, 351-352
 - stress, 348-350
- security policies, 1012
- site database upgrade tests, 375-376
- solutions, customizing, 357
- task sequences, 965

thick/thin images, 910

third-party software

- DCM configurations, 796
- hardware configuration packs, 776
- patch management, 706
- websites, 1113

threats, 985

three-tiered hierarchy example, 294-297

thresholds, Delete Obsolete Client Discovery Data task, 1062

throttling

- BITS, 552
- site addresses, 419

tiered hierarchies, 186

time to resolution (DCM management), 766

timeouts, troubleshooting, 282

TLS (Transport Layer Security), 511

Tondt, Jeff, 298

Toolkit (ConfigMgr), 158, 579-581, 763, 797

tools. See specific tools

Tools node, 473

top-level objects. See nodes

topology, network discovery, 564

total cost of ownership (TCO), 17, 75-80

TPM (Trusted Platform Module), 537

Trace Logging (WMI), 113

Trace32, client troubleshooting, 579

training

- requirements, 182-183
- resources, 1104

Transact-SQL website, 847

Transfer Site Settings Wizard, 426-427

- Export or Transfer Settings Site screen, 352
- Gather Settings screen, 351
- Select Site Settings screen, 352
- Select Source Site screen, 352
- Summary screen, 352
- website, 1106
- Welcome screen, 351

transferring

- GPOs to POC environment, 344
- objects, 355
- site settings, 351-352, 426-427

Transmission Control Protocol (TCP), 229**Transport Layer Security (TLS), 511****triggers, 159****troubleshooting**

- backups, 1040
- clients, 576
 - common issues, 576
 - conflicting hardware IDs, 579
 - functionality tests, 582
 - online assistance, 577
 - Toolkit, 579-581
 - uninstalling/reinstalling, 581
- console
 - command-line options, 504-505
 - common issues, 502
 - large queries, 503
 - verbose logging, 501-502
- DCM, 805-807
 - compliance, 807
 - configurations, 806-807
 - log files, 805
- drivers, 968
- network issues
 - blocked/unresponsive ports, 280-281
 - client installations, 283-284
 - communication, 289-290
 - configurations, 278-279
 - connectivity, 279
 - name resolution, 279-280
 - site system installations, 282-283
 - software distribution, 286-287
 - SPNs, 284-285
 - timeouts, 282
- OSD, 972
 - advertisement status, 972
 - command-line support, 974

home page, 972

SMSTS.log file, 972

status reports, 973

packages, 636-638

PXE service points, 920

reports, 900-902

resources, 1106

secondary sites, 424-426

addresses, 426

pending status, 425

secure key exchanges, 424-425

site installations, 429

SMS 2003 migrations, 463-464

software distribution, 702

Software Updates

client scans, 763

downloads, 762-763

monitoring, 761-762

WSUS, 762

WDS, 920

WSUS website disappearance, 719

Trusted Platform Module (TPM), 537**trusted root keys, 1018****tuning status message replication, 257-261**

status filter rules, 257-259

stopping, 258

two-tiered hierarchy example, 296-297**U****Überbug, 965****UDP (User Datagram Protocol), 229****unattended console installations, 490****unattended setups, resources, 1106****unicast WOL, 331, 752****uninstalling**

clients, 575

ConfigMgr agent, 597

software, 588-590

United States Computer Emergency Response Team (US-CERT), 1007

unknown computer support, 928

- computers, importing, 928-929
- MDT, 930

unknown system resources, 930

unprovisioned computers, 930

Update List Wizard, 727-732

update lists, 731-733

- hierarchies, 733
- updates, adding, 732
- viewing, 731

Update Repository, 728-731

Updated Prerequisite Components dialog box, 449

updates

- boot images, 529
- collections, scheduling, 646, 658-659
- management tasks, automation, 7
- managing, 34
- packages, 709
- site boundaries, 289
- software. *See* Software Updates
- WinPE, 530

UpdatesDeployment.log, 1096

UpdatesHandler.log, 1096

UpdatesStore.log, 1096

Upgrade Advisor

- Analysis Wizard, 443
- SQL upgrades, 442-443

Upgrade Secondary Site Wizard, 454

upgrades

- clients, 575
- ConfigMgr R2, 378-379
- databases, 362, 445-447
- in-place, 435
 - database upgrades, 445-447
 - feature packs, 436
 - post-upgrade considerations, 457-458

prerequisite checker, running, 437-442

prerequisites, 436-437

primary upgrades, 447-453

secondary upgrades, 453-455

SMS 2003 clients, 455-457

SQL Server upgrades, 442-445

WSUS, 458-459

primary sites, 447-453

action status, monitoring, 450

completing, 452

ITMU upgrade, 450

licensing, 448

options, 448

updated prerequisites, 449

WSUS installation, 451

secondary sites, 453-455

site backups, 436

SMS 2003, 455-457, 976

SQL replication, disabling, 374

SQL Server, 442-445

performing, 444-445

Upgrade Advisor, running, 442-443

US-CERT (United States Computer Emergency Response Team), 1007

User Datagram Protocol (UDP), 229

User Group Resource, 824

User Resource class, 824

users

disconnected, 271-272

previously captured data, recovering, 926

reports, 856

rights, customizing, 997

sometimes-connected, 271-272

state

capturing, 940

migration, 940-941

tasks, 952-954

volume, calculating, 207

training, implementation, 182

USMT (User State Migration Tool), 905

- tools, 905
- versions, 938
- XML integration, 905

USMT Log loadstate.log file, 1091**USMT Log scanstate.log file, 1091**

utilities. *See* applications; software

Utility Spotlight TechNet article, 743**V****v_Collection view, 150-151****v_GroupMap view, 154****v_ResourceAttributeMap view, 154****v_ResourceMap view, 153****v_R_System view, 153****v_SchemaViews view, 152-153****v_site view, 151-152****validating**

- configuration items, 790-795
 - data types, 792
 - example, 792-794
 - operators, 790
- PKI certificates, 517
- site functionality after restores, 1048
- systems, 661-665

values (queries), 819-821**variables (task sequences), 943-944****verbose logging, 501-502, 805, 1080****verifying**

- App-V 4.5 client, 694
- DCM changes, 766
- schema changes, 98
- site installations, 429

viewing

- Asset Intelligence reports, 872-873
- CIMV2 namespace, 116
- collections, 150-151
- default views, 889

DiscoveryArchitectures table data, 153

- intersite replication, 168-172
- inventory architecture groups, 154
- logs, 156
- object attributes, 884
- queries, 810
- relational databases, 845
- reports
 - console, 478-480
 - customizing, 878-879
 - Internet Explorer, 481-482

Resource IDs, 153

- resource view attributes, 154
- schema changes, 96
- site properties, 151-152
- SQL, 150-154
- update lists, 731
- WMI classes/properties, 134

virtual applications. *See also* SoftGrid

- activating, 629-630
- Adobe Reader, distributing, 693-700
- allow virtual application package advertisement, 630
- creating, 632-633
- deploying, 700
- importing, 630
- prepackaged, 636
- sequenced applications packaging preparations, 632
- sequencing with App-V, 631

Virtual Machine Manager (VMM), 44, 743**Virtual Machines**

- offline maintenance, 742
- reference computers, 931
- site deployment, 304

Virtual Private Networks (VPNs), 318-319**virtualization**

- systems management, 13
- testing environments, 341

viruses, scanning, 305

visibility

- ConfigMgr, 7
- home pages, 36
- overview, 35
- queries, 36
- reports, 37-39
- search folders, 36

Visio Pro, System Center add-ins, 893

Visual Studio, DSI integration, 17

VMM (Virtual Machine Manager), 44, 743

VPNs (Virtual Private Networks), 318-319

vPro, 534-537

vulnerabilities, 985

W-X-Y-Z

WAIK (Windows Automated Installation Kit), 527, 906

Wake On LAN tab (Site Properties dialog box), 380-382

Wake On LAN. See WOL

WBEM (Web-Based Enterprise Management), 104

WCM.log, 1095

WDS (Windows Deployment Integration), 533-534

- benefits, 533
- installing, 918
- troubleshooting, 920

web browsing, security, 1029

web publishing, security, 193

websites. See specific websites

weekly backups, 1040

Where clause (SELECT statements), 846

Wildflower site server, distribution points, adding, 667

- account settings, 668
- communication settings, 670
- completing, 671
- distribution point selection, 669
- enabling, 669-671

FQDN settings, 668

group memberships, 671

security settings, 668

WIM (Windows Imaging Format), 527

benefits, 906

mounting, 911

Vista, Windows Server 2008 DVDs, 938

Win32_LogicalShareSecuritySetting class, 116

class associations, 121

class qualifiers, 123-124

help entries, 119

methods, 119

Windows

64-bit redirection, 783

Automated Installation Kit (WAIK), 527, 906

CE operating systems, 313

components, required, 361-362

Deployment Integration (WDS), 533-534

benefits, 533

installing, 918

troubleshooting, 920

Embedded CE website, 313

Imaging Format (WIM), 527

benefits, 906

mounting, 911

Vista, Windows Server 2008 DVDs, 938

Internet Naming Service (WINS), 342

POC environment, 342

security, 1026-1027

Management Instrumentation. *See* WMI

Mobile, 313

Pre-Install Environment (WinPE)

boot images, 922-925

customizing, 529

images, 529-530

OSD, 907

updates, 530

- Server
 - 2003, Certificate Services installation, 514-515
 - memory support, 303
 - Update Services. *See* WSUS
- Server 2008
 - Certificate Services installation, 515
 - ConfigMgr installations, 380
 - configuration website, 362
 - planning, 326-327
 - reports, configuring, 836
 - site system role configuration, 326
 - WIM files, 938
- Update Agent (WUA), 708, 1097
- Updates GPOs, disabling, 721
- versions, configuration items, 780
- Vista
 - dynamic collections, 651-654
 - WIM files, 938
- XP
 - drivers, 964
 - dynamic collections, 651-654
 - Embedded operating systems, 314
- WinPE (Windows Pre-Install Environment)**
 - boot images, 922-925
 - customizing, 529
 - images, 529-530
 - OSD, 907
 - updates, 530
- WINS (Windows Internet Naming Service), 342**
 - POC environment, 342
 - security, 1026-1027
- Wizard Actions page (Configure Distribution Wizard), 405**
- wizards. *See specific wizards***
- WMI (Windows Management Instrumentation), 104, 497**
 - CCM_SoftwareDistribution class, 132
 - CIMV2 namespace
 - classes, 125
 - root classes, 116
 - viewing, 116
 - Win32_LogicalShareSecuritySetting class, 116-124
 - classes
 - attributes, 114
 - namespaces, 115
 - qualifiers, 115
 - viewing, 134
 - ConfigMgr server operations, 134
 - exporting object definitions to MOF files, 138
 - SMS provider namespace views, 134
 - WMI behind collections, exploring, 136-138
 - Console (WMIC), 779
 - Content Transfer Management component, 132
 - Control
 - General tab, 109
 - namespace auditing, 111
 - running, 108
 - Security tab, 109
 - Trace Logging, enabling, 113
 - Diagnosis Utility (WMIDiag), 113
 - hardware inventory, 126-129
 - infrastructure, 106-108
 - local client policies, 131
 - namespace auditing, 111
 - object model, 113-116
 - OOB, 105
 - permissions, 498-499
 - policy agents, 131
 - properties, 134
 - providers, 106
 - Query Builder, 799
 - query language. *See* WQL
 - remote management, 109
 - resources, 1105-1106
 - Root\CCM namespace, 125, 129-130
 - Scheduler, 132

1190 WMI (Windows Management Instrumentation)

- Security dialog box, 110
- services, invoking, 104
- SMS_Collection class, 136-138
- SMS provider namespace views, 134
- SMS_Site class, 134
- Software DistributionClientConfig class, 132
- WS-Management, 105

WMIC (WMI Console), 779

WOL (Wake On LAN), 68

- client support, 382
- configuring, 753-754
- implementing, 754
- limitations, 331
- logs, 1094
- magic packets, 330
- mandatory advertisements, 68
- planning, 330-331
- properties, 380-382
- reports, 862
- requirements, 330, 751-752
- Software Updates, 751
- subnet-directed, 331, 752
- unicast, 331, 752

WolCmgr.log, 1094

Wolmgr.log, 1094

workstations, ConfigMgr installation, 365

WQL (WMI Query Language), 105, 811

- advanced queries, 822
- converting to SQL, 823
- resources, 1107

WS-Management, 16, 105

WSUS (Windows Server Update Services), 17

- DSI integration, 17
- installing, 711
- logs, 1096
- migrating to ConfigMgr, 458-459
- primary site upgrades, 451
- requirements, 363

- software updates, 311, 709
 - components, 717
 - troubleshooting, 762
- SP 1, 199
- Synchronization Manager, 718
- website, 363
- website disappearance, 719

WSUSCtrl.log, 1095

WSUSUtil utility, 312

WSUSyncXML.log, 1096

Wsyncmgr.log, 1095

WUA (Windows Update Agent), 708, 1097

WUAHandler.log, 1096

XML, USMT integration, 905

zero-day exploits, 760