System Center 2012 Configuration Manager UNLEASHED

FREE SAMPLE CHAPTER

SHARE WITH OTHERS
System Center 2012 Configuration Manager UNLEASHED

Kerrie Meyler
Byron Holt
Marcus Oh
Jason Sandys
Greg Ramsey

with Niall Brady
Samuel Erskine
Torsten Meringer
Stefan Schörling
Kenneth van Surksum
Steve Thompson

SAMS
800 East 96th Street, Indianapolis, Indiana 46240 USA
# Contents at a Glance

Foreword .......................................................... xxix  
Introduction .................................................... 1  

**Part I  Configuration Manager Overview and Concepts**  
1 Configuration Management Basics ....................... 7  
2 Configuration Manager Overview ......................... 37  
3 Looking Inside Configuration Manager .................... 79  

**Part II  Planning, Design, and Installation**  
4 Architecture Design Planning .............................. 161  
5 Network Design ................................................ 205  
6 Installing System Center 2012 Configuration Manager ............ 261  
7 Migrating to System Center 2012 Configuration Manager .......... 317  

**Part III  Configuration Manager Operations**  
8 The Configuration Manager Console ....................... 375  
9 Configuration Manager Client Management ................. 419  

**Part IV  Software and Configuration Management**  
10 Managing Compliance ....................................... 491  
11 Packages and Programs ..................................... 533  
12 Creating and Managing Applications ...................... 565  
13 Distributing and Deploying Applications .................. 627  
14 Software Update Management .............................. 669  
15 Mobile Device Management ................................. 751  
16 Endpoint Protection .......................................... 785  
17 Configuration Manager Queries ............................. 833  
18 Reporting ..................................................... 871  
19 Operating System Deployment .............................. 959  

**Part V  Administering System Center Configuration Manager**  
20 Security and Delegation in Configuration Manager ............ 1065  
21 Backup, Recovery, and Maintenance ....................... 1125
Part VI Appendixes

A Configuration Manager Log Files ...................................................... 1179
B Extending Hardware Inventory ........................................................ 1211
C Reference URLs ............................................................................... 1225
D Available Online ............................................................................. 1241
Index ............................................................................................. 1243
Table of Contents

Foreword ................................................................. xxix
Introduction .......................................................... 1

Part I  Configuration Manager Overview and Concepts

1  Configuration Management Basics ................................. 7

Ten Reasons to Use Configuration Manager ......................... 8
The Evolution of Systems Management ................................. 9
- Hurdles in the Distributed Enterprise .............................. 10
- The IT Automation Challenge .................................. 10
- Configuration “Shift and Drift” .................................... 11
- Lack of Security and Control ................................... 11
- Timeliness of Asset Data .......................................... 12
- Lack of Automation and Enforcement ......................... 12
- Proliferation of Virtualization and Cloud Computing ....... 12
- Lack of Process Consistency .................................... 13
- The Bottom Line ..................................................... 13

Systems Management Defined ........................................ 14
Microsoft’s Strategy for Service Management .................... 15
- Microsoft’s Dynamic Systems Initiative .................... 16
IT Infrastructure Library and Microsoft .......................... 19
Operations Framework .............................................. 19
Total Quality Management: TQM .................................. 24
Six Sigma ................................................................... 24
Service Management Mastery: ISO 20000 ......................... 24
Optimizing Your Infrastructure ................................... 25

Overview of Microsoft System Center ............................... 29
- Reporting in System Center ..................................... 30
Operations Management ............................................ 31
- Service Management ............................................ 31
- Protecting Data ................................................... 32
Virtual Machine Management ....................................... 32
Deploy and Manage in the Cloud .................................... 33
Orchestration and Automation ....................................... 33
Cloud-Based Configuration Monitoring .......................... 34
- Endpoint Protection .............................................. 34

The Value Proposition of Configuration Manager ............... 34
Summary .................................................................... 35
2 Configuration Manager Overview

The History of Configuration Manager

- Systems Management Server 1.x .................................................. 38
- Systems Management Server 2.0 .................................................. 38
- Systems Management Server 2003 ............................................... 39
- System Center Configuration Manager 2007 .............................. 41
- System Center 2012 Configuration Manager ............................... 42

Terminology in Configuration Manager

- Site Hierarchy ............................................................................ 43
- Site ........................................................................................... 44
- Site Systems .............................................................................. 46
- Senders ..................................................................................... 48
- Addresses .................................................................................. 49
- Configuration Manager Discovery Types .................................. 49
- Configuration Manager Agent .................................................... 50
- Configuration Manager Console .............................................. 51
- Collections ................................................................................ 52
- Queries ..................................................................................... 52
- Alerts ........................................................................................ 53
- Status System ............................................................................ 53
- Managing Applications ................................................................ 54
- Content Management ................................................................ 57
- Software Update Management .................................................. 59
- Compliance Settings .................................................................. 59
- BITS ......................................................................................... 59
- Software Metering ..................................................................... 60
- Network Access Protection ....................................................... 60
- BranchCache ............................................................................. 61
- Reporting ................................................................................... 61

What’s New in This Version

- 64-Bit Site System Requirements .............................................. 62
- User-Centric Management .......................................................... 62
- Applications and Packages ......................................................... 63
- Hierarchy Changes .................................................................... 63
- New Configuration Manager Console ....................................... 64
- Enhancements to BITS ............................................................... 64
- Application Catalog ................................................................... 64
- Extended Mobile Device Management ....................................... 65
- Management Point Enhancements ............................................. 65
- Boundary Changes .................................................................... 65
- Fallback Site ............................................................................... 66
- Centrally Managed Client Settings ............................................ 66
### Part II Planning, Design, and Installation

#### 4 Architecture Design Planning

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developing the Solution Architecture</td>
<td>161</td>
</tr>
<tr>
<td>Establishing Business Requirements</td>
<td>162</td>
</tr>
<tr>
<td>Assessing Your Environment</td>
<td>163</td>
</tr>
<tr>
<td>Planning for Licensing</td>
<td>165</td>
</tr>
<tr>
<td>Hierarchy Planning</td>
<td>167</td>
</tr>
<tr>
<td>Configuration Manager Sites</td>
<td>167</td>
</tr>
<tr>
<td>Planning Your Hierarchy Structure</td>
<td>169</td>
</tr>
<tr>
<td>Planning Boundaries and Boundary Groups</td>
<td>170</td>
</tr>
<tr>
<td>Choosing Client Discovery and Installation Methods</td>
<td>172</td>
</tr>
<tr>
<td>Defining Your Client Architecture</td>
<td>174</td>
</tr>
<tr>
<td>Planning for User-Centric Management</td>
<td>178</td>
</tr>
<tr>
<td>Planning Content Management</td>
<td>178</td>
</tr>
<tr>
<td>Planning for Infrastructure Dependencies</td>
<td>180</td>
</tr>
<tr>
<td>Active Directory Considerations</td>
<td>180</td>
</tr>
<tr>
<td>Planning Certificate Services</td>
<td>183</td>
</tr>
<tr>
<td>Site Planning</td>
<td>186</td>
</tr>
<tr>
<td>Site Servers and Site Systems Planning</td>
<td>186</td>
</tr>
<tr>
<td>Capacity Planning</td>
<td>188</td>
</tr>
<tr>
<td>Developing the Server Architecture</td>
<td>189</td>
</tr>
<tr>
<td>Planning for Solution Scenarios</td>
<td>190</td>
</tr>
<tr>
<td>Software Update Planning</td>
<td>190</td>
</tr>
<tr>
<td>Planning for Internet-Based Clients</td>
<td>193</td>
</tr>
<tr>
<td>Out of Band Management Planning</td>
<td>195</td>
</tr>
<tr>
<td>Testing and Stabilizing Your Design</td>
<td>197</td>
</tr>
<tr>
<td>The Proof of Concept</td>
<td>198</td>
</tr>
<tr>
<td>The Pilot Deployment</td>
<td>204</td>
</tr>
<tr>
<td>Summary</td>
<td>204</td>
</tr>
</tbody>
</table>

#### 5 Network Design

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding Your Network</td>
<td>206</td>
</tr>
<tr>
<td>Configuration Manager Data Flow</td>
<td>206</td>
</tr>
<tr>
<td>Intrasite Server Communications</td>
<td>208</td>
</tr>
<tr>
<td>Communications with SQL Server</td>
<td>208</td>
</tr>
<tr>
<td>Communications Using RPC</td>
<td>209</td>
</tr>
<tr>
<td>Communications Using SMB</td>
<td>209</td>
</tr>
<tr>
<td>Replication of Deployment Content Refresh Data</td>
<td>213</td>
</tr>
<tr>
<td>Site System Communications Using HTTP and HTTPS</td>
<td>214</td>
</tr>
<tr>
<td>Other Server Communications</td>
<td>214</td>
</tr>
</tbody>
</table>
# Installing System Center 2012 Configuration Manager

- **Configuring Pre-Installation Requirements**
  - Windows Components
  - Supported SQL Server Requirements
  - Validating and Configuring Active Directory Requirements
  - Windows Server Update Services
  - Prerequisite Checker
  - Using the Prerequisite Files Downloader

- **Performing Site Installations**
  - Installing the Central Administration Site
  - Installing Primary Sites
  - Installing Secondary Sites
  - Installation Validation

- **Site Properties**
  - Initial Configuration
  - Installing Optional Site Systems

- **Uninstalling Sites**
  - Uninstalling Primary Sites
  - Uninstalling Secondary Sites
  - Uninstalling a Full Hierarchy

- **Troubleshooting Site Installation**

- **Summary**

## Migrating to System Center 2012 Configuration Manager

- **About Migration**
  - Migration Background and Introduction
  - Migration, Not an Upgrade

- **Planning the Migration**
  - Central Site and Hierarchy Concepts in 2012
  - About Site Mode
  - What Is Migrated
  - What Is Not Migrated
  - Pre-Migration Activities
  - Coexistence Considerations

- **Migrating Your Configuration Manager Infrastructure**
  - Site Servers and Site Roles
  - Security Considerations
  - Boundaries and What’s Changing

- **Performing the Migration**
  - Migrating Features and Objects
  - Migrating by Feature and Dependencies
  - Migration Dependencies Configuration
Contents

Configuring the Active Source Site ............................................. 343
Configuring Child Sites for Data Gathering ................................. 345
Migration Jobs .......................................................................... 347
Shared Distribution Points ......................................................... 366
Migration Clean Up .................................................................. 367
Migrating Reports ..................................................................... 369
  Legacy Reports ...................................................................... 369
  SSRS Reports ...................................................................... 369
  Custom Reports .................................................................... 369
Client Migration and Methods ................................................... 370
  Background and Client Migration Concepts .............................. 370
  Client Migration Strategies for Your Network ............................ 371
Troubleshooting Migration Issues .............................................. 371
Summary ................................................................................ 372

Part III Configuration Manager Operations

8 The Configuration Manager Console ........................................ 375
  Console Highlights ................................................................ 376
  Touring the Console ................................................................ 376
    Configuration Manager Console Panes ................................. 377
    Configuration Manager Console Bars .................................. 378
    Backstage .......................................................................... 378
  ConfigMgr Workspaces .......................................................... 379
    Assets and Compliance Workspace ..................................... 380
    Software Library Workspace .............................................. 380
    Monitoring Workspace ...................................................... 381
    Administration Workspace ................................................. 383
    Console Node Details .......................................................... 384
  Console Deployment ................................................................ 388
    Console Placement ............................................................. 389
    Supported Platforms ......................................................... 389
    ConfigMgr Console Prerequisites ....................................... 390
    Installation Using the ConfigMgr Setup Wizard .................... 391
    Unattended Console Installation ......................................... 394
  Role-Based Administration ...................................................... 395
    Introducing the “Show Me” Behavior .................................. 395
    Behind the Scenes ............................................................... 397
    The Three States of Interaction .......................................... 397
  Connecting to a Site ................................................................. 398
    Recent Connections ............................................................ 398
    Clearing Recent Connections .............................................. 398
  Personalizing the Console ........................................................ 400
The In-Console Alert Experience ......................................................... 401
  Viewing Alerts ........................................................................... 401
  Managing Alerts ...................................................................... 402
  Configuring Alerts .................................................................. 403
  Subscribing to Alerts ............................................................... 404
Configuration Manager Service Manager .................................................. 404
  Initiating the Configuration Manager Service Manager Console ........................................ 406
  Operating the Configuration Manager Service Manager Console ........................................ 407
Security Considerations .......................................................................... 408
  SMS Provider Permissions ...................................................... 409
  DCOM Permissions .................................................................. 409
  WMI Permissions .................................................................... 409
Troubleshooting Console Issues ................................................................. 411
  Console Logging ...................................................................... 411
  Verify Security ....................................................................... 412
  Connectivity Issues ................................................................ 416
  Common Problems with the ConfigMgr Console .......................... 416
Summary ......................................................................................... 417

9 Configuration Manager Client Management .............................................. 419
  Discovery .................................................................................. 419
  Active Directory Forest Discovery ............................................ 420
  Active Directory Group Discovery ............................................ 422
  Active Directory User Discovery .............................................. 424
  Active Directory System Discovery ........................................... 426
  Heartbeat Discovery .................................................................. 427
  Network Discovery ................................................................... 429
  Manually Importing Clients into ConfigMgr ............................. 431
  ConfigMgr Client Requirements ................................................. 432
  Hardware Dependencies ........................................................... 432
  Software Dependencies ............................................................ 433
  Supported Platforms ................................................................. 433
  ConfigMgr Client Installation ...................................................... 435
  Manual Installation .................................................................. 435
  Installing with Logon Scripts .................................................... 441
  Client Push .............................................................................. 442
  Group Policy ............................................................................ 447
  Software Update Point ............................................................... 448
  Client Approval ...................................................................... 449
Part IV Software and Configuration Management

10 Managing Compliance

New and Improved in System Center 2012
- Configuration Manager ...................................... 493

Configuring Compliance Settings ................................ 493

Configuration Items and Baselines ............................ 495
- Configuration Items ........................................... 496
- Configuration Baselines ...................................... 512
- Compliance Evaluation ....................................... 517
- Versioning ....................................................... 519
- Configuration Packs .......................................... 521

Using the Resource Explorer ...................................... 483

Wake On LAN ...................................................... 484

WOL Prerequisites ................................................ 484

Two Types of WOL ............................................... 485

Configuring WOL ................................................ 486

Using WOL ......................................................... 487

Summary .................................................................. 488
### 13 Distributing and Deploying Applications

**Creating and Managing Collections**
- Direct Rule ................................................. 628
- Query Rule ................................................... 630
- Include Rule .................................................. 631
- Exclude Rule .................................................. 634
- About Incremental Updates ............................ 634
- User Collections Versus Device Collections .... 635

**About Distribution Points**
- Installing Distribution Points ........................ 637
- Distribution Point Groups ............................... 640
- Associating Collections with Distribution Point Groups ........ 641
- Sending Content to Distribution Points .......... 642
- Monitoring Distribution Point Status .................. 642
- Updating Content on Distribution Points ........ 645
- Refreshing Content on Distribution Points .......... 646
- Removing Content from Distribution Points ....... 646
- Validating Content .......................................... 647
- Using BranchCache ......................................... 647
- Preferred Distribution Points ....................... 648
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>Software Update Management</td>
<td>669</td>
</tr>
<tr>
<td></td>
<td>What’s New in 2012</td>
<td>670</td>
</tr>
<tr>
<td></td>
<td>Planning Your Update Strategy</td>
<td>670</td>
</tr>
<tr>
<td></td>
<td>Incorporated Tools</td>
<td>672</td>
</tr>
<tr>
<td></td>
<td>The Windows Update Agent</td>
<td>673</td>
</tr>
<tr>
<td></td>
<td>Windows Software Update Services</td>
<td>673</td>
</tr>
<tr>
<td></td>
<td>Preparing for Software Updates with ConfigMgr</td>
<td>674</td>
</tr>
<tr>
<td></td>
<td>Prerequisites for Software Updates</td>
<td>674</td>
</tr>
<tr>
<td></td>
<td>Software Update Points</td>
<td>676</td>
</tr>
<tr>
<td></td>
<td>Client Settings</td>
<td>687</td>
</tr>
<tr>
<td></td>
<td>Group Policy Settings</td>
<td>689</td>
</tr>
<tr>
<td></td>
<td>Software Update Building Blocks</td>
<td>692</td>
</tr>
<tr>
<td></td>
<td>All Software Updates</td>
<td>692</td>
</tr>
<tr>
<td></td>
<td>Software Update Groups</td>
<td>696</td>
</tr>
<tr>
<td></td>
<td>Update Deployments</td>
<td>698</td>
</tr>
<tr>
<td></td>
<td>Update Templates</td>
<td>703</td>
</tr>
<tr>
<td></td>
<td>Deployment Packages</td>
<td>704</td>
</tr>
<tr>
<td></td>
<td>Automatic Deployment Rules</td>
<td>706</td>
</tr>
<tr>
<td></td>
<td>Maintenance Windows</td>
<td>708</td>
</tr>
<tr>
<td></td>
<td>Superseded Updates</td>
<td>711</td>
</tr>
<tr>
<td></td>
<td>The Software Updates Process in Action</td>
<td>711</td>
</tr>
<tr>
<td></td>
<td>Software Update Decisions, Design, and Workflow</td>
<td>714</td>
</tr>
<tr>
<td></td>
<td>Compliance Scanning</td>
<td>716</td>
</tr>
<tr>
<td></td>
<td>End User Experience and Interaction</td>
<td>717</td>
</tr>
<tr>
<td></td>
<td>Notifications</td>
<td>717</td>
</tr>
<tr>
<td></td>
<td>Updates and Software Center</td>
<td>718</td>
</tr>
<tr>
<td></td>
<td>Update Installation</td>
<td>720</td>
</tr>
<tr>
<td></td>
<td>System Restarts and Restart Notifications</td>
<td>721</td>
</tr>
<tr>
<td></td>
<td>Monitoring Software Updates</td>
<td>723</td>
</tr>
<tr>
<td></td>
<td>Individual Update Status</td>
<td>723</td>
</tr>
</tbody>
</table>
Compliance Settings ................................................................. 782
Reporting ................................................................................. 782
Partner Extensibility ................................................................. 783
Summary ......................................................................................... 784

16 Endpoint Protection ................................................................. 785

   Prerequisites for Endpoint Protection .................................................. 787
   Planning and Considerations ............................................................. 788
      Creating Custom Client Settings and Antimalware Policies 788
      Deciding from Where to Update and When 789
      Deploying to a Test Collection First 789
      Categorizing Client Remediation Status ...................................... 790
      Targeting Collections with Custom Antimalware Policy and Client Settings 790
      Installing the Endpoint Protection Role .............................................. 792
      Configuring the SUP for Endpoint Protection ...................................... 797
         Configuring the SUP to Synchronize Definition Updates 797
      Creating Auto Deployment Rules for Definition Updates 799
      Working with Antimalware Policies .................................................... 804
      Understanding the Default Antimalware Policy .................................... 804
      Creating Custom Antimalware Policy ......................................... 807
      Importing and Merging Antimalware Policies .................................. 808
      Configuring Alerts for Endpoint Protection ......................................... 809
      Configuring Email Notification .................................................. 810
      Configuring Alerts for Device Collections ................................... 812
      Configuring Alert Subscriptions ................................................. 813
      Configuring Custom Client Device Settings for Endpoint Protection .... 814
      Deploying Endpoint Protection Custom Client Agent Settings 815
      Monitoring Status in Endpoint Protection ........................................... 816
         Configuring Collections to Appear in Collection View .............. 816
      Security State View for the Selected Collection 816
      Operational State View for Clients and Computers in the Selected Collection 818
      Performing On-Demand Actions for Malware ...................................... 819
      Reporting in Endpoint Protection ....................................................... 820
      Creating and Deploying Windows Firewall Policies 823
      Understanding the Endpoint Protection Client .................................... 824
      Installing the Endpoint Protection Client ............................................ 827
         Understanding Endpoint Protection Client Settings ..................... 827
      Communication Between the Client and the Server 829
Automatic Removal of Antimalware Software ......................................................... 829
Removing the Endpoint Protection Client ................................................................. 830
Delivery of Definition Updates .................................................................................. 830
Summary ..................................................................................................................... 831

17 Configuration Manager Queries ........................................................................ 833
   Introducing the Queries Node .............................................................................. 834
      Organizing the Query List Pane .................................................................... 835
      Viewing Queries and Query Results ............................................................... 837
   Creating Queries ................................................................................................ 838
      WMI Query Language .................................................................................... 838
      Objects, Classes, and Attributes .................................................................... 839
   ConfigMgr Query Builder .................................................................................... 841
   Criterion Types, Operators, and Values ............................................................... 845
      Criterion Types ............................................................................................ 845
      Operators ..................................................................................................... 848
      Values ........................................................................................................... 850
   Writing Advanced Queries .................................................................................. 851
      Limitations of Extended WQL in ConfigMgr ............................................... 852
      Utilizing the Date and Time Functions in WQL Queries ............................... 853
      Examples of Advanced Queries ................................................................... 854
      Converting WQL to SQL .............................................................................. 857
   Relationships, Operations, and Joins ................................................................ 858
      Querying Discovery Data ............................................................................... 860
      Querying Inventory Data ............................................................................... 861
   Using Query Results ............................................................................................ 863
      Exporting Query Results to a Text File ........................................................... 863
      Importing and Exporting Queries Between Sites ............................................ 863
      Creating a Collection Based on Query Results ............................................... 866
   Status Message Queries ...................................................................................... 866
      Viewing Status Messages .............................................................................. 868
      Creating Status Message Queries ................................................................ 868
   Summary .............................................................................................................. 870

18 Reporting ............................................................................................................... 871
   SQL Server Reporting Services Overview ............................................................ 871
   Implementing SSRS ............................................................................................. 872
      SQL Server Version Selection ...................................................................... 872
      Server Placement Options ............................................................................. 872
      SSRS Installation ............................................................................................ 873
      SSRS Configuration ....................................................................................... 876
Chapter 19: Operating System Deployment

19 Operating System Deployment 959

What OSD Does 960
What’s New in OSD 961
Deployment Scenarios 963
Tools Incorporated into OSD 965
Sysprep 965
Windows Automated Installation Kit 966
User State Migration Tool 968
OSD Phases 968
Planning 969
Preparation 969
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creation</td>
<td>970</td>
</tr>
<tr>
<td>Testing</td>
<td>970</td>
</tr>
<tr>
<td>Productionization</td>
<td>970</td>
</tr>
<tr>
<td>OSD Building Blocks</td>
<td>970</td>
</tr>
<tr>
<td>Drivers</td>
<td>971</td>
</tr>
<tr>
<td>Driver Packages</td>
<td>975</td>
</tr>
<tr>
<td>Operating System Images</td>
<td>976</td>
</tr>
<tr>
<td>Operating System Installers</td>
<td>976</td>
</tr>
<tr>
<td>Boot Images</td>
<td>977</td>
</tr>
<tr>
<td>Task Sequences</td>
<td>984</td>
</tr>
<tr>
<td>Site System Roles</td>
<td>1020</td>
</tr>
<tr>
<td>Distribution Points</td>
<td>1020</td>
</tr>
<tr>
<td>State Migration Point</td>
<td>1025</td>
</tr>
<tr>
<td>Driver Management</td>
<td>1030</td>
</tr>
<tr>
<td>Drivers in the Image</td>
<td>1031</td>
</tr>
<tr>
<td>Drivers After the Image</td>
<td>1031</td>
</tr>
<tr>
<td>User State</td>
<td>1032</td>
</tr>
<tr>
<td>USMT</td>
<td>1034</td>
</tr>
<tr>
<td>Computer Associations</td>
<td>1036</td>
</tr>
<tr>
<td>User State Without SMP</td>
<td>1038</td>
</tr>
<tr>
<td>Image Operations</td>
<td>1039</td>
</tr>
<tr>
<td>Image Creation</td>
<td>1039</td>
</tr>
<tr>
<td>Image Upkeep</td>
<td>1044</td>
</tr>
<tr>
<td>Offline Software Updates</td>
<td>1045</td>
</tr>
<tr>
<td>Image Deployment</td>
<td>1047</td>
</tr>
<tr>
<td>User Device Affinity</td>
<td>1049</td>
</tr>
<tr>
<td>Deployment Challenges</td>
<td>1050</td>
</tr>
<tr>
<td>Application Compatibility</td>
<td>1051</td>
</tr>
<tr>
<td>User Data</td>
<td>1052</td>
</tr>
<tr>
<td>Image Maintenance</td>
<td>1052</td>
</tr>
<tr>
<td>Hardware Considerations</td>
<td>1054</td>
</tr>
<tr>
<td>Monitoring Task Sequence Deployments</td>
<td>1057</td>
</tr>
<tr>
<td>Update Deployment Status</td>
<td>1057</td>
</tr>
<tr>
<td>Reporting</td>
<td>1058</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>1058</td>
</tr>
<tr>
<td>Command Line Support</td>
<td>1058</td>
</tr>
<tr>
<td>The Smsts.log File</td>
<td>1060</td>
</tr>
<tr>
<td>Windows Setup Log Files</td>
<td>1061</td>
</tr>
<tr>
<td>Troubleshooting USMT</td>
<td>1061</td>
</tr>
<tr>
<td>Summary</td>
<td>1061</td>
</tr>
</tbody>
</table>
### Part V  Administering System Center Configuration Manager

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>Security and Delegation in Configuration Manager</td>
<td>1065</td>
</tr>
<tr>
<td>21</td>
<td>Backup, Recovery, and Maintenance</td>
<td>1125</td>
</tr>
</tbody>
</table>

#### 20 Security and Delegation in Configuration Manager

- Planning for Security and Delegation ................................................ 1065
- ConfigMgr Security Solutions ........................................................... 1067
- Role-Based Administration ................................................................ 1068
  - Managing Administrative Users .................................................. 1069
  - Security Roles ......................................................................... 1070
  - Security Scopes ....................................................................... 1074
  - Associating Security Scopes and Collections with Individual Roles 1077
  - Administrative Security Reports .............................................. 1078
  - RBA Under the Hood .............................................................. 1079
- Preventing Unauthorized Access to ConfigMgr ................................. 1084
  - Securing Access at the Active Directory Level ............................ 1084
  - Securing Access at the Database Level ....................................... 1085
  - Auditing ConfigMgr Administrative Actions ................................ 1086
- Securing the ConfigMgr Infrastructure .......................................... 1089
  - Building Security into Your Hierarchy ........................................ 1089
  - Securing Site Systems ............................................................. 1090
  - ConfigMgr Cryptographic Controls ............................................. 1096
  - ConfigMgr Network Security ...................................................... 1097
  - ConfigMgr Content Security ...................................................... 1115
  - Securing ConfigMgr Accounts ................................................... 1116
- Summary ....................................................................................... 1123

#### 21 Backup, Recovery, and Maintenance

- Performing Site and SQL Server Backups ...................................... 1125
  - Backing Up ConfigMgr ................................................................ 1126
  - Restoring ConfigMgr Backups ................................................... 1129
  - Site Maintenance Options ....................................................... 1136
  - Using Backup and Restore to Migrate to New Environments .......... 1139
- SQL Replication ........................................................................... 1140
  - Monitoring SQL Replication ..................................................... 1140
  - Replication Link Analyzer ......................................................... 1143
  - Alerts for SQL Replication ....................................................... 1144
- Site Maintenance ........................................................................... 1145
  - Site Maintenance Tasks ............................................................ 1145
  - DDR Retention ......................................................................... 1155
  - Obsolete Records .................................................................... 1162
  - How a Record Can Be Marked Obsolete .................................... 1163
Database Maintenance .......................................................... 1165
Making the Status Message System Work for You .................. 1166
  Maintaining Status Data .................................................. 1167
  Status Filter Rules ....................................................... 1169
  Status Summarizers ..................................................... 1172
Monitoring Configuration Manager with Operations Manager .. 1174
Services and Descriptions .................................................. 1175
Summary ........................................................................... 1176

Part VI Appendixes

A Configuration Manager Log Files ........................................... 1179
  Related Documentation .................................................. 1180
  Viewing Log Files .......................................................... 1180
  Enabling Logging ........................................................... 1181
  Client Logs ..................................................................... 1183
  Server Logs ..................................................................... 1188
  Functionality Logs .......................................................... 1194
  Software and Application Installation Logs ......................... 1207
  Log File Mining .............................................................. 1209

B Extending Hardware Inventory ................................................ 1211
  How to Extend Hardware Inventory ................................... 1212
  Example of Extending Inventory ....................................... 1213
  Creating a Device Collection .......................................... 1223

C Reference URLs ................................................................ 1225
  General Resources .......................................................... 1225
  Microsoft’s Configuration Manager Resources .................... 1229
  Other Configuration Manager Resources ........................... 1234
  Blogs ............................................................................. 1235
  Microsoft System Center .................................................. 1237
  Public Forums .................................................................. 1237
  Utilities .......................................................................... 1238

D Available Online ................................................................. 1241
  SQL Profiler Template ...................................................... 1241
  Top 10 Most Executed Reports Query ................................. 1241
  OSD Starter Scripts ........................................................ 1241
  Live Links ....................................................................... 1242

Index ................................................................................. 1243
This page intentionally left blank
About the Authors

Kerrie Meyler, System Center MVP, is the lead author of numerous System Center books in the Unleashed series, including *System Center Operations Manager 2007 Unleashed* (2008), *System Center Configuration Manager 2007 Unleashed* (2009), *System Center Operations Manager 2007 R2 Unleashed* (2010), *System Center Opalis Integration Server 6.3 Unleashed* (2011), and *System Center Service Manager 2010 Unleashed* (2011). She is an independent consultant and trainer with more than 15 years of Information Technology experience. Kerrie was responsible for evangelizing SMS while a Sr. Technology Specialist at Microsoft, and has presented on System Center technologies at TechEd and MMS.

Byron Holt, CISSP and an IT professional for more than 15 years, has been a lead SMS and Configuration Manager engineer for several Global 5000 corporations and was part of the Active Directory and Enterprise Manageability support teams while working at Microsoft. Byron’s experience includes software development, security architecture, and systems management. He currently works for McAfee managing internal deployment and validation. Byron coauthored *System Center Configuration Manager 2007 Unleashed* (Sams, 2009).

Marcus Oh, System Center MVP, is IT Manager of Directory and Systems Management for a large telecommunications provider, running directory services and management infrastructure for ~30,000 systems. He has been a MVP since 2004 in System Center, specializing in Configuration Manager and Operations Manager. Marcus has written numerous articles for technology websites as well as his own blog. He coauthored *Professional SMS 2003, MOM 2005*, and *WSUS* (Wrox, 2006), and was a contributing author to *System Center Opalis Integration Server 6.3 Unleashed* (Sams, 2011). Marcus is also a coauthor to the upcoming *System Center 2012 Orchestrator Unleashed* (Sams).

Jason Sandys, ConfigMgr MVP, is currently a Technology Evangelist and Principal Consultant at Catapult Systems Inc. and has more than 20 years of experience in a wide range of technologies, environments, and industries with extensive experience implementing and supporting SMS and Configuration Manager beginning with SMS 2.0. Jason is also active in the online support community, was a contributing author to *System Center Configuration Manager 2007 Unleashed* (Sams, 2009), and is a frequent presenter at Microsoft TechEd, MMS, and various user groups.

About the Contributors

**Niall Brady**, ConfigMgr MVP, began working with SMS in 2003 and Forefront Endpoint Protection when it was first integrated with Configuration Manager 2007. Niall is a senior consultant at Enfo Zipper in Sweden and blogs extensively about using and configuring System Center 2012 Configuration Manager according to best practices on windows-noob.com.

**Samuel Erskine**, MCT, MCTS, is a senior IT consultant specializing in Configuration Manager and Service Manager. He holds an ITIL V3 foundation certification. Samuel has worked with the product since SMS 2003 and was an early tester for System Center 2012 Service Manager. With more than 15 years of IT experience, he focuses on providing training and consultancy services in the United Kingdom and other international locations.

**Torsten Meringer**, ConfigMgr MVP, is a self-employed senior consultant in Germany, starting his own business in 1999. His primary focus is to design, migrate, deploy, train, and troubleshoot Microsoft's deployment and management solutions, such as System Center Configuration Manager and Microsoft Deployment Toolkit, in small to large-scale companies of more than 200,000 clients. Torsten manages the German ConfigMgr blog http://www.mssccmfaq.de and holds various MCSA, MCSE, MCTS, and MCITP:EA certifications.

**Stefan Schörling**, ConfigMgr MVP, is a Swedish-based infrastructure consultant focusing on System Center and infrastructure management. With 13 years of experience, Stefan is an expert in system management, security, and IT operations. His primary focus lies in Microsoft technologies and technical security. Stefan has worked and presented at numerous conferences and events worldwide such as TechEd and MMS. Stefan is also the founder of System Center User Group Sweden.

**Kenneth van Surksum**, MCT and Setup & Deployment MVP, works as a trainer and System Center consultant at INOVATIV, a company based in the Netherlands, where he implements and advises customers about System Center and other Microsoft solutions. With more than 10 years of experience with IT, Kenneth has worked with SMS 1.2 and successive versions of the product since 1998, specializing in OS deployment. Kenneth coauthored *Mastering Windows 7 Deployment* (Sybex, 2011) and blogs at http://www.techlog.org.

**Steve Thompson**, ConfigMgr MVP, works for BT Global Services as a senior consultant specializing in all things System Center-related. He was first awarded MVP in Microsoft Access in 1995, was a SQL Server MVP for several years, and then joined the System Center team as a ConfigMgr MVP. Steve has presented at MMS on Configuration Manager, SQL Server, and reporting. You can follow his blog at http://myitforum.com/cs2/blogs/stthompson.
Dedication

To Wally and the ConfigMgr community.

Acknowledgments

Writing a book is an all-encompassing and time-consuming project, and this book certainly meets that description. Configuration Manager is a massive topic, and this book benefitted from the input of many individuals. The authors and contributors would like to offer their sincere appreciation to all those who helped with System Center 2012 Configuration Manager Unleashed. This includes John Joyner and Bob Longo of ClearPointe Technologies along with Joe Stocker and Greg Tate of Catapult Systems for dedicating lab resources, Wally Mead, Sherry Kissinger, Oskar Landman, Frank Rojas, Keith Thornley, Charles Applegrath of SoftMart, Cameron Fuller, Niall Brady, John Marcum, Roger Zander, and Jean-Sébastien Duchêne.

We would also like to thank our spouses and significant others for their patience and understanding during the many hours spent on this book.

Thanks also go to the staff at Pearson, in particular to Neil Rowe, who has worked with us since Microsoft Operations Manager 2005 Unleashed (Sams, 2006).
We Want to Hear from You!

As the reader of this book, you are our most important critic and commentator. We value your opinion and want to know what we’re doing right, what we could do better, what areas you’d like to see us publish in, and any other words of wisdom you’re willing to pass our way.

You can email or write me directly to let me know what you did or didn’t like about this book—as well as what we can do to make our books stronger.

Please note that I cannot help you with technical problems related to the topic of this book, and that due to the high volume of mail I receive, I might not be able to reply to every message.

When you write, please be sure to include this book’s title and author as well as your name and phone or email address. I will carefully review your comments and share them with the authors and editors who worked on the book.

Email: consumer@samspublishing.com

Mail: Sams Publishing
      ATTN: Reader Feedback
      800 East 96th Street
      Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at informit.com/register for convenient access to any updates, downloads, or errata that might be available for this book.
Foreword

You are about to embark on a fantastic journey! System Center 2012 Configuration Manager is an exciting, new version of the Configuration Manager product line. While each release of Configuration Manager, or the predecessor product—Systems Management Server—has been a great improvement over the previous version, we believe that without a doubt this is the most feature-rich and revolutionary version of Configuration Manager that the product group has ever released. From the improved software distribution, focusing on user-centric delivery of applications, to the reduced infrastructure requirements, SQL Server-based replication and improved security, to the enhancements designed to make your lives easier as Configuration Manager administrators, this product is one that we’re extremely confident you’ll enjoy working with and find beneficial in your environments.

After years in development, this product has been thoroughly tested, not only within the Configuration Manager product group, within Microsoft IT, by numerous Technology Adoption Program (TAP) customers testing beta and release candidate releases in production, but also by thousands of open beta customers testing in lab environments. Through all this testing, we are confident that you can have a great experience with Configuration Manager 2012 in your production environments—and see great return on your investment.

To those of you who participated in the open beta, CEP, CEP for Production, OneTAP, and TAP programs: Thank you for your assistance in testing the pre-release versions of Configuration Manager 2012. Your feedback—whether suggestions for enhancements or requests for new features, as well as feedback that reported features not working as they should—certainly helped shape the product that you see today. I want to especially thank our TAP customers because you lived with us through production deployments of the beta 1 and beta 2 releases, which, for some of you, shall we say were somewhat challenging. Thanks for sticking with us and for helping us create a fantastic product, even though some of your experiences were not as smooth as you would have expected. It is through your efforts and dedication that the RTM version of the product is a great one that everyone can take pride in.

To those of you who are new to the Configuration Manager world: Welcome—we are glad to have you join us. To those of you who are migrating from previous releases: Thank you for your desire to venture into this brave new world from a previous version of the product that I am sure is providing great benefit to you. We appreciate your loyalty and trust in us as a product group and believe you can have a great experience with this new, groundbreaking release.
With my personal knowledge of a number of the authors and contributors for this book—and of their professionalism and knowledge—I am confident that this writing will be a great benefit to you for learning and experiencing System Center 2012 Configuration Manager. The best of luck to you all, and again, thanks for your loyalty and trust in us!

Wally Mead, Senior Program Manager
Configuration Manager Product Group
Microsoft Corporation
Introduction

Microsoft’s most recent version of its systems management product can help you empower individuals to use the devices and applications they need while maintaining the corporate compliance and control your organization requires. By adding a layer of abstraction that delivers to the user rather than the device, System Center 2012 Configuration Manager (ConfigMgr) helps you enable users to be productive with a unified infrastructure that delivers and manages user experiences across corporate and consumer devices.

Seeing consumerization as a reality, ConfigMgr’s infrastructure provides the means to deliver and manage user experiences based on identity, connectivity, and type of device. Here are the benefits System Center 2012 Configuration Manager delivers:

▶ **Empowers users to be productive from anywhere on any device**

  ConfigMgr manages a wide range of mobile devices using a single administration console for policies, asset management, and compliance reporting.

  The product provides optimized and personalized application delivery, based on user identity, device type, and network capabilities.

  ConfigMgr allows users to securely self-provision applications on demand using an easy-to-use web catalog.

▶ **Unifies the management infrastructure, integrating client management and protection against mobile, physical, and virtual environments**

  ConfigMgr provides you with a single tool to manage all your client environments.

  This version of ConfigMgr consolidates inventory management, software delivery, antimalware, vulnerability prevention and remediation, and compliance reporting, using a single infrastructure.

  Integration with System Center 2012 Service Manager helps improve user satisfaction with integrated help desk capabilities.

▶ **Simplifies administration**

  The new release of ConfigMgr uses the System Center-standard “Outlook” style user interface.

  System Center 2012 Configuration Manager organizes administrative tasks by role, allows administrators to define an application once for delivery across multiple devices, and provides continuous settings enforcement to automatically identify and remediate noncompliant machines.

  This release includes scalability enhancements, reduces data latency, and consolidates server roles to improve infrastructure efficiency.
In addition, System Center 2012 continues to become more integrated, including a common look and feel between the consoles of the various components, and with data integration between those components both operationally and in a consolidated data warehouse. This integration will continue to grow as System Center evolves and becomes more intertwined with cloud computing.

Part I: Configuration Management Overview and Concepts

System Center 2012 Configuration Manager Unleashed begins with an introduction to configuration management including initiatives and methodology. This includes Dynamic System Initiative (DSI), IT Infrastructure Library (ITIL), and Microsoft Operations Framework (MOF). 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. More important, implementing ConfigMgr is a project, and as such, it 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 System Center plans to address these challenges.

Chapter 2, “Configuration Manager Overview,” shows how ConfigMgr has evolved from its first days in 1994 as Systems Management Server (SMS) 1.0, and introduces key concepts and feature dependencies. In Chapter 3, “Looking Inside Configuration Manager,” the book begins to peel back the layers of the onion to discuss the design concepts behind System Center 2012 Configuration Manager, the major ConfigMgr components, its relationship with Windows Management Instrumentation (WMI), the ConfigMgr database, and more.

Part II: Planning, Design, and Installation

Before installing any software, you need to spend time planning and designing its architecture. ConfigMgr is no exception. Chapter 4, “Architecture Design Planning,” begins this discussion with developing a solutions architecture and assessing your environment, and covers licensing, hierarchy and site planning, planning considerations for specific ConfigMgr services, and implementation considerations. Chapter 5, “Network Design,” steps through the network concepts to consider when planning a ConfigMgr architecture and deployment.

When it is time to implement your design, Chapter 6, “Installing System Center 2012 Configuration Manager,” steps through the installation process; and Chapter 7, “Migrating to System Center 2012 Configuration Manager,” discusses how to move from a Configuration Manager 2007 to 2012 environment.
Part III: Configuration Manager Operations

The third part of this book focuses on ConfigMgr operations in your environment, which is where you will spend the bulk of your time. This includes navigating through the newly designed console discussed in Chapter 8, “The Configuration Manager Console.” Using ConfigMgr requires an installed client on managed systems, as covered in depth in Chapter 9, “Configuration Manager Client Management.”

Part IV: Software and Configuration Management

Compliance settings, discussed in Chapter 10, “Managing Compliance,” provides a set of tools and resources to help assess, track, and remediate the configuration compliance of your client systems.

Configuration Manager’s core capabilities have historically focused around software distribution, and System Center 2012 Configuration Manager adds new capabilities in this area. Software distribution is discussed in Chapter 11, “Packages and Programs,” Chapter 12, “Creating and Managing Applications,” and Chapter 13, “Distributing and Deploying Applications.” Software and configuration management also includes activities such as patch management (Chapter 14, “Software Update Management”), managing mobile devices (Chapter 15, “Mobile Device Management”), endpoint management, previously known as Forefront Endpoint Protection (Chapter 16, “Endpoint Protection”), running queries (Chapter 17, “Configuration Manager Queries”), reporting (Chapter 18, “Reporting”), and operating system deployments (Chapter 19, “Operating System Deployment”). These chapters discuss those key functionalities and their use in System Center 2012 Configuration Manager.

Part V: Administering System Center 2012 Configuration Manager

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

Part VI: Appendixes

By this time, you should have at your disposal all the tools necessary to become a Configuration Manager expert. The last part of the book includes four appendixes:

▶ Appendix A, “Configuration Manager Log Files,” incorporates useful references you can access for further information.
▶ Appendix B, “Extending Hardware Inventory,” takes a deep dive into how to extend hardware inventory.
Appendix C, “Reference URLs,” incorporates useful references you can access for further information about Configuration Manager and System Center, and also includes live links available for download under the Downloads tab at Pearson’s InformIT website, at www.informit.com/title/9780672334375.

Appendix D, “Available Online,” discusses value-added content also available at the InformIT page.

Throughout, this book provides in-depth reference and technical information about System Center 2012 Configuration Manager, as well as information about other products and technologies on which its features and components depend.

**Disclaimers and Fine Print**

There are several disclaimers. The information provided is probably outdated the moment the book goes to print. The authors began working on this book during the early beta releases of System Center 2012 Configuration Manager in an attempt to bring you this information as soon as possible after the release of System Center 2012. This means multiple chapters were written and then rewritten as the Configuration Manager product team continued to fine-tune the product’s development. Screenshots were taken during late release candidate builds, and it is certainly possible Microsoft could slightly tweak the user interface in the production code release.

In addition, the moment Microsoft considers code development on any product complete, it begins working on a service pack or future release; as the authors continue to work with the product, it is likely yet another one or two wrinkles will be discovered! The authors and contributors of *System Center 2012 Configuration Manager Unleashed* have made every attempt to present information that is accurate and current as known at the time. Updates and corrections will be provided as errata on the InformIT website.

Thank you for purchasing *System Center 2012 Configuration Manager Unleashed*. The authors hope it is worth your while (and their effort). Enjoy the ride!
CHAPTER 3

Looking Inside Configuration Manager

This chapter examines the inner workings of System Center 2012 Configuration Manager (ConfigMgr). It describes the design concepts and working principles of ConfigMgr, along with information about how the product utilizes core Windows technologies, specifically Active Directory (AD) and Windows Management Instrumentation (WMI). It also discusses the various components of ConfigMgr, how they communicate with each other, and how they work together to implement product features. The chapter looks inside the site database, which is the heart of ConfigMgr. It shows how to view the inner workings of ConfigMgr through its status messages and logs, as well as through other tools for viewing database and process activity. This chapter focuses on depth rather than breadth. The authors have chosen some of the most important feature sets and data structures to use as examples throughout the chapter, rather than try to provide a comprehensive account of all ConfigMgr functionality.

If you are simply planning to get ConfigMgr up and running, you may find some of the material in this chapter unessential. However, you will find a basic understanding of the product architecture and knowledge of techniques for viewing the inner working of ConfigMgr invaluable for troubleshooting purposes. If you have not decided whether to extend the AD schema, you will want to review the “Schema Extensions” section of the chapter. The “SQL Replication Crash Course” and “Configuration Manager Database Replication” sections may also be helpful for hierarchy and site system planning. Should you want a deeper understanding of what is going on behind the scenes with ConfigMgr; the material in this chapter can help you
grasp the architectural principles of the product and guide you into exploring its inner workings.

**Design Concepts**

System Center 2012 Configuration Manager (ConfigMgr) delivers a variety of configuration management and system support services via a flexible and distributed architecture. The product utilizes standards-based network protocols and object models for its internal working and interaction with client systems. ConfigMgr components store and use data about ConfigMgr infrastructure and activity, the environment, and managed systems in the site database. Sites in a hierarchy replicate data for effective management across the environment.

ConfigMgr 2012 builds on the core functionality of ConfigMgr 2007 and adds an enhanced feature set that includes native 64-bit code, role-based administration, simplified hierarchy design, user-centric management, advanced power management, and client status reporting.

In this latest release of its systems management software, Microsoft emphasizes security and compliance, scalability, and operational simplicity. This chapter focuses on some key architectural principles System Center 2012 Configuration Manager uses to support these goals:

- **Integration with core services:** Rather than reproducing existing functionality, ConfigMgr leverages the rich set of services provided by Windows Server and other Microsoft products. This chapter describes some ways ConfigMgr utilizes Active Directory and WMI. Other chapters present various other integration points. For example, Chapter 14, “Software Update Management,” describes Windows Server Update Services (WSUS) integration, Chapter 18, “Reporting,” discusses the use of SQL Server Reporting Services, and Chapter 19, “Operating System Deployment,” describes Windows Deployment Services integration.

- **Distributed database:** System Center 2012 Configuration Manager has replaced many of the inboxes used in ConfigMgr 2007 and previous versions of Systems Management Server (SMS) with SQL replication. Database replication provides efficient communications and eliminates redundant processing.

- **Flexible distributed component architecture:** System Center 2012 Configuration Manager, like ConfigMgr 2007, implements specific features and functionality as individual threads within the executive service. These threads can run on a single server or across many servers. ConfigMgr 2012 improves on communication between components by replacing many file based exchanges with database updates. This provides high scalability and allows administrators to adapt their deployment to their environment.

ConfigMgr leverages key elements of the Windows platform to implement much of its functionality. The two most important Windows components are AD and WMI. The next sections look in depth at how ConfigMgr uses these technologies.
Active Directory Integration

Active Directory is the central information store used by Windows Server to maintain entity and relationship data for a wide variety of objects in a networked environment. AD provides a set of core services, including authentication, authorization, and directory services. ConfigMgr takes advantage of the AD environment to support many of its features. For information about Active Directory in Windows Server 2008 R2, see http://www.microsoft.com/windowsserver2008/en/us/active-directory.aspx.

ConfigMgr can use AD to publish information about its sites and services, making it easily accessible to Active Directory clients. To take advantage of this capability, you must extend the AD schema to create classes of objects specific to ConfigMgr. Although implementing ConfigMgr does not require extending the schema, it is required for certain ConfigMgr features. Extending the schema also greatly simplifies ConfigMgr deployment and operations. The “Schema Extensions” section discusses extending the AD schema. Chapter 4, “Architecture Design Planning,” discusses the benefits and feature dependencies of the extended schema.

Schema Extensions

All objects in AD are instances of classes defined in the AD schema. The schema provides definitions for common objects such as users, computers, and printers. Each object class has a set of attributes that describes members of the class. As an example, an object of the computer class has a name, operating system, and so forth. Additional information about the AD schema is available at http://msdn.microsoft.com/en-us/library/ms675085.aspx.

The schema is extensible, allowing administrators and applications to define new object classes and modify existing classes. Using the schema extensions provided with Configuration Manager eases administration of your ConfigMgr environment. The ConfigMgr schema extensions are relatively low risk, involving only a specific set of classes not likely to cause conflicts. Nevertheless, you need to test any schema modifications before applying them to your production environment.

NOTE: SCHEMA EXTENSIONS AND CONFIGMGR 2012 UPDATES

There are no changes to the schema extensions from ConfigMgr 2007 to 2012. If you extended the Active Directory schema for ConfigMgr 2007, you do not need to run the System Center 2012 Configuration Manager schema extensions.

After you extend the AD schema and perform the other steps necessary to publish site information to AD, ConfigMgr sites can publish information to AD.

The next sections describe the process for extending the schema and configuring sites to publish to AD, as well as the AD objects and attributes created by the schema extensions.
Tools for Extending the Schema
You can extend the schema in either of two ways:

▶ Running the ExtADSch.exe utility from the ConfigMgr installation media
▶ Using the LDIFDE (Lightweight Data Interchange Format Data Exchange) utility to import the ConfigMgr_ad_schema.ldf LDIF file

To use all the features of ConfigMgr 2012, you must use Active Directory with Windows Server 2003 or later; Windows 2000 domains are supported with reduced functionality; most notably, Active Directory Forest Discovery does not work with Windows 2000 domains. If you are extending the schema on a Windows 2000 domain controller, you must use the LDIF file.

Using ExtADSch  Using ExtADSch.exe is the simplest way to extend the schema and until ConfigMgr 2007 was the only way to extend the schema. ExtADSch.exe creates the log file extadshc.log, located in the root of the system drive (%systemdrive%), which lists all schema modifications it has made and the status of the operation. Following the list of attributes and classes that have been created, the log should contain the entry Successfully extended the Active Directory schema.

Using LDIFDE   LDIFDE is a powerful command-line utility for extracting and updating directory service data on Active Directory servers. LDIFDE provides command-line switches, allowing you to specify a number of options, including some you may want to use when updating the schema for ConfigMgr. Table 3.1 includes the options that you are most likely to use.

<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-i</td>
<td>Turns on Import Mode. Required for updating the schema.</td>
</tr>
<tr>
<td>-f</td>
<td>Filename. (Used to specify the location of the ConfigMgr_ad_schema.ldf file.)</td>
</tr>
<tr>
<td>-j</td>
<td>Log file location.</td>
</tr>
<tr>
<td>-v</td>
<td>Turns on Verbose Mode.</td>
</tr>
<tr>
<td>-k</td>
<td>Ignore Constraint Violation and Object Already Exists errors. (Use with caution. May be useful if the schema is previously extended for ConfigMgr.)</td>
</tr>
</tbody>
</table>

The options vary slightly, depending on the Windows Server version you are running. You can see a complete listing of LDIFDE syntax by entering this command:

```
ldifde /?
```

You can also find detailed information about using LDIFDE at http://technet.microsoft.com/en-us/library/cc731033.aspx. Here is an example of a typical command to update the schema for ConfigMgr:

```
ldifde -i -f ConfigMgr_ad_schema.ldf -v -j SchemaUpdate.log
```
The verbose logging available with LDIFDE includes more detail than the log file generated by ExtADSCh.exe. The ConfigMgr_ad_schema.ldf file allows you to review all intended changes before they are applied. You can also modify the LDF file to customize the schema extensions. As an example, you can remove the sections for creating classes and attributes that already exist as an alternative to using the \( -k \) switch referred to in Table 3.1.

**CAUTION: BE CAREFUL WHEN EDITING THE LDF FILE**

Do not attempt to edit the LDF file unless you have a thorough understanding of LDF, and remember to test all modifications before applying them to your production environment.

**Extending the Schema**

Each AD forest has a single domain controller with the role of schema master. All schema modifications are made on the schema master. To modify the schema, you must log on using an account in the forest root domain that is a member of the Schema Admins group.

**NOTE: ABOUT THE SCHEMA ADMINS GROUP**

The built-in Schema Admins group exists in the root domain of your forest. Normally there should not be any user accounts in the Schema Admins group. Only add accounts to Schema Admins temporarily when you need to modify the schema. Exercising this level of caution will protect the schema from any accidental modifications.

The ConfigMgr schema modifications create four new classes and 14 new attributes used with these classes. Here is what the created classes represent:

- **Management points**: Clients can use this information to find a management point.
- **Roaming boundary ranges**: Clients can use this information to locate ConfigMgr services based on their network location.
- **Server locator points (SLPs)**: ConfigMgr 2007 clients can use this information to find a SLP. This class is created but it is not used in System Center 2012 Configuration Manager. SLP functionality is now integrated into the management point and the SLP no longer exists as a separate site system role.
- **ConfigMgr sites**: Clients can retrieve important information about the site from this AD object.

**REAL WORLD: TIPS AND TECHNIQUES ABOUT CHANGING THE SCHEMA**

Exercise caution when planning any changes to the AD schema, particularly when making modifications to existing classes because this could affect your environment.

When you modify the schema, you should take the schema master offline temporarily while you apply the changes. Regardless of the method used to extend the schema,
review the logs to verify that the schema extensions were successful before bringing the schema master back online. This way, if there is a problem with the schema modifications, you can seize the schema master role on another domain controller and retain your original schema!

Before actually extending the schema for System Center 2012 Configuration Manager, run the \texttt{dcdiag} and \texttt{netdiag} command-line tools, which are part of the Windows Support Tools. These tools validate that all domain controllers (DCs) are replicating and healthy. Because it may be difficult to validate the output of these tools, you can output the results to a text file using the following syntax:

\begin{verbatim}
Ddcdiag >c:\dcdiag.txt
\end{verbatim}

Search the output text file for failures and see if any domain controllers are having problems replicating. If any failures are present, do not update the schema. Upgrading the schema when domain controllers are not healthy or replicating correctly will cause them to be orphaned as AD is revved to a higher version. The machine will then need to be manually and painfully cleaned out of AD.

\section*{Viewing Schema Changes}

If you are new to ConfigMgr and are extending the schema and curious about the details of the new classes, the Schema Management MMC snap-in enables you to view their full schema definitions. Before adding the snap-in to the management console, you must install it by running the following command from the command prompt:

\begin{verbatim}
regsvr32 schmmgmt.dll
\end{verbatim}

\begin{center}
\textbf{TIP: REGSVR32 REQUIRES ADMINISTRATIVE RIGHTS}
\end{center}

On domain controllers running Windows 2008 Server or later, you may need to launch the command prompt using the \texttt{Run as Administrator} option to register the schema management dll.

After installing the snap-in, perform the following steps to add Schema Management to the MMC:

1. Select \texttt{Start}, choose \texttt{Run}, and then enter \texttt{MMC}.
2. Choose Add/Remove snap-in from the File menu of the console.
3. Click the \texttt{Add} button and then choose \texttt{Active Directory Schema}.
4. Choose Close and then click \texttt{OK} to complete the open dialog boxes.

The left pane of the schema management tool displays a tree control with two main nodes—classes and attributes. If you expand out the classes node, you will find the following classes defined by ConfigMgr:
Clicking a class selects it and displays the attributes associated with the class in the right pane. The list of attributes for each class includes many attributes previously defined in AD, in addition to those attributes specifically created for System Center 2012 Configuration Manager. You can right-click a class and choose Properties to display its property page. For example, Figure 3.1 shows the general properties of the mSSMSSite class. For an explanation of these properties, click the Help button on the Properties page.

You can see the 14 ConfigMgr attributes under the Attributes node in the schema management console. The names of each of these attributes start with mS-SMS. You can right-click an attribute and choose Properties to display its property page. Figure 3.2 shows the properties of the mS-SMS-Capabilities attribute.

TIP: VERIFY SCHEMA EXTENSIONS WHEN EXTENDING THE SCHEMA

ExtADSch.log file is created at the root of the system drive on the computer that the extensions were installed from. You should check this log for failures. Seeing Event ID 1137 in the Directory Service event log alone does not confirm the schema was extended properly; several experiences in the field have found failures in the logfile in what seemed to be a successful schema extension.
Additional Tasks

After extending the schema, you must complete several tasks before ConfigMgr can publish the objects it will use to Active Directory:

▶ **Create the System Management container where the ConfigMgr objects will reside in AD:** If you previously extended the schema for ConfigMgr 2007, the System Management container will already exist. Each domain publishing ConfigMgr data must have a System Management container.

▶ **Set permissions on the System Management container:** Setting permissions allows your ConfigMgr site servers to publish site information to the container.

▶ **Configure your sites to publish to AD:** You can specify one or more AD forests to which each site will publish. Publishing to a forest other than the sites server’s local forest requires a cross-forest trust.

The next sections describe these tasks.

**Creating the System Management Container**  You can use the ADSIEdit MMC tool to create the System Management AD container. If you do not already have ADSIEdit installed, you can install the tool yourself.

Add ADSIEdit using Server Manager. Configuring the domain controller server role automatically adds ADSIEdit to the Administrative Tools program group.
To create the System Management container from ADSIEdit, perform the following steps:

1. Right-click the Root ADSI Edit node in the tree pane, select **Connect to**, and then click **OK** to connect to the default name context.

2. Expand the default name context node in the tree pane. Then expand the node showing the distinguished name of your domain (this will begin with DC=<domain>) and right-click **CN=System node**.

3. Select **New** and then choose **Object**.

4. Select **Container** in the Create Object dialog box and click **Next**.

5. Enter the name **System Management** and then click **Next** and **Finish**, completing the wizard.

Figure 3.3 shows ADSIEdit with the tree control expanded to the CN=System node and the Create Object dialog box displayed.

**Setting Permissions on the System Management Container** You can view the System Management container and set permissions on it using the Active Directory Users and Computers (ADUC) utility in the Windows Server Administrative Tools menu group. After launching ADUC, enable the **Advanced Features** option from the View menu. You can then expand out the domain partition and System container to locate System Management.
By default, only certain administrative groups have the rights required to create and modify objects in the System Management container. For security reasons, you should create a new group and add ConfigMgr site servers to it, rather than adding them to the built-in administrative groups. Perform the following steps to grant the required access to the ConfigMgr site server security group:

1. Right-click the System Management container, choose Properties, and then select the Security tab.

2. Click the Add button, and select the group used with your ConfigMgr site servers, as shown in Figure 3.4.

3. Check the box for Full Control, as displayed in Figure 3.5, and choose OK to apply the changes.

FIGURE 3.4 Selecting the Site server security group.

FIGURE 3.5 Assigning permissions to the System Management container.
**Configuring Sites to Publish to Active Directory**  Perform the following steps to configure a ConfigMgr site to publish site information to AD:

1. In the ConfigMgr 2012 console, select the Administration workspace.
2. Expand **Site Configuration** -> **Sites**. In the Sites pane, highlight the desired site, and click **Properties** on the ribbon bar.
3. Select the **Publishing** tab, and then select the check box next to each forest to which the site will publish, as shown in Figure 3.6.

![Figure 3.6](image)

**FIGURE 3.6** Configuring a site to publish to AD.

After extending the schema and taking the other steps necessary to enable your sites to publish to AD, you should see the ConfigMgr objects displayed in the System Management container. Figure 3.7 shows the ConfigMgr objects viewed in Active Directory Users and Computers.
Additional Active Directory Benefits

In an AD environment, all processes run in the security context of a user or a security context supplied by the operating system. System Center 2012 Configuration Manager uses Active Directory to authenticate administrative users and authorize user account for administrative roles. Each system has a computer account that you can add to user groups and grant access to resources. ConfigMgr makes extensive use of system and computer accounts to connect securely to network services and client systems, as well as providing security contexts for its internal operations. Using system accounts greatly simplifies administration. You can use additional AD accounts to supplement the available system accounts. Chapter 20, “Security and Delegation in Configuration Manager,” discusses authentication, access control, and accounts used in ConfigMgr.

Here are other ways ConfigMgr can take advantage of AD:

- Discovering information about your environment; including the existence of potential client systems, users, and groups. Chapter 4 discusses how you can use this information to plan user-centric management. Before implementing AD discovery methods, evaluate your AD data to ensure it is reliable and up to date. Importing obsolete records for users and computers that no longer exist or have changed may cause problems with various ConfigMgr operations. Chapter 9, “Configuration Manager Client Management,” provides details about configuring the discovery process.

- Assigning and installing clients using group policy, also described in Chapter 9.
Using certificates and certificate settings deployed through AD. For example, if you use the System Center Updates Publisher (SCUP) to deploy custom software updates, you can use AD to deploy the required certificates to the trusted store on client computers.

A WMI Primer

If the SQL Server database is the heart of ConfigMgr, WMI is its lifeblood. WMI has been the core management infrastructure for all Windows desktop and server operating systems beginning with Windows 2000. WMI is the Windows implementation of Web-Based Enterprise Management (WBEM). WBEM is a set of standards intended to provide the basis for cross-platform interoperability of technologies to exchange management data and access management interfaces across distributed computing environments.

The Distributed Management Task Force (DMTF) supports WBEM. This group is an industry consortium created to promote standardization and integration of enterprise and Internet management technology. For more information about WBEM in general and the DMTF, see http://www.dmtf.org/standards/wbem. Although much of the architectural material in this chapter is common to all implementations of WBEM, the next sections exclusively focus on WMI and its role in ConfigMgr:

- **WMI architecture**: This includes describing the WMI feature set, reviewing the major components of WMI, and discussing how they interact.
- **WMI object model**: The WMI object model and its implementation are discussed, with several tools you can use to manage WMI and look into its inner workings.
- **ConfigMgr use of WMI**: Configuration Manager’s use of WMI is discussed, with examples of how you can look inside ConfigMgr through its WMI interfaces.

WMI Feature Set and Architecture

WMI makes it much easier to write programs and scripts that interact with local resources on Windows systems. WMI serves as an abstraction layer between management applications and scripts and the physical and logical resources they manage. WMI exposes managed resources through a COM (Component Object Model) API (application programming interface). Programs written in C/C++ can call these resources directly, or you can access them through intermediate layers by applications such as scripts, Windows forms, or web forms. WMI presents a consistent and extensible object model to represent a wide variety of system, network, and other resources. Here are some examples of what you can do with WMI:

- Rename the built in administrator account.
- Compile a list of printers that support color printing.
- Receive an alert each time a new device connects to a USB port.
Using an object model removes much of the complexity that would otherwise be required to access and manipulate these resources. Some examples of resources you can manage through WMI include hardware devices, running processes, the Windows file system and registry, and applications and databases.

Here are several ways you can invoke WMI services:

- Locally on a machine
- Remotely through a DCOM (Distributed COM) connection
- Remotely using a WS-Management (Web Services for Management) connection

WS-Management is a SOAP (Simple Object Access Protocol)-based specification published by the DMTF. SOAP is a standard for invoking objects remotely over an HTTP (Hypertext Transfer Protocol) or HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) connection. The main advantage of SOAP is that it works across many existing network firewalls without requiring additional configuration. You can find a complete description of WS-Management and related specifications at http://www.dmtf.org/standards/wsman.

WMI supports requests from management applications to

- Retrieve or modify individual data items (properties) of managed objects.
- Invoke actions (methods) supported by managed objects.
- Execute queries against the data set of managed objects.
- Register to receive events from managed objects.

ABOUT WMI QUERY LANGUAGE

WMI provides its own query language that allows you to query managed objects as data providers. WMI Query Language (WQL) is essentially a subset of SQL (Structured Query Language) with minor semantic changes. Unlike SQL, WQL does not provide statements for inserting, deleting, or updating data and does not support joins. WQL does have extensions that support WMI events and other features specific to WMI. WQL is the basis for ConfigMgr queries, whereas SQL is used for ConfigMgr reports. Queries and reports are discussed in Chapters 17, “Configuration Manager Queries,” and 18, respectively.

One important advantage of WQL is that a WQL query can return WMI objects as well as specific properties. Because management applications such as the ConfigMgr console interact with WMI objects, WQL queries can return result sets that you can use within the ConfigMgr infrastructure. For example, ConfigMgr collections are based on WQL queries. For more information about WQL, see http://msdn.microsoft.com/en-us/library/aa394606.aspx.

Here is how WMI handles requests from management applications:

1. Management applications submit a request to the WMI infrastructure, which passes the request to the appropriate provider. The next section describes WMI providers.
2. The provider then handles the interaction with the actual system resources and returns the resulting response to WMI.

3. WMI passes the response back to the calling application. The response may be actual data about the resource or the result of a requested operation.

Figure 3.8 shows the basic data flow in WMI.

![Diagram of WMI data flow](image)

**FIGURE 3.8** How WMI accepts a request from a management application and returns a response from a managed resource.

**WMI Providers**

WMI providers are analogous to device drivers in that they know how to interact with a particular resource or set of resources. In fact, many device drivers also act as WMI providers. Microsoft supplies several built-in providers as part of Windows, such as the Event Log provider and File System provider. You will see providers implemented in the following ways:

- As DLLs (Dynamic Link Libraries)
- As Windows processes and services

Just as the WMI infrastructure serves management applications through a COM interface, providers act as COM servers to handle requests from the WMI infrastructure. When a provider loads, it registers its location and the classes, objects, properties, methods, and events it provides with WMI. WMI uses this information to route requests to the proper provider.

**The WMI Infrastructure**

Figure 3.9 displays the main logical components of the WMI infrastructure. The core of the WMI infrastructure is the Common Information Model Object Manager (CIMOM), described in the “Inside the WMI Object Model” section. CIMOM brokers requests between management applications and WMI providers, and communicates with management applications through the COM API, as described earlier in the “WMI Feature Set and Architecture” section. CIMOM also manages the WMI repository, an on-disk database used by WMI to store certain types of data. Beginning with Windows XP, WMI also includes an
XML (eXtensible Markup Language) encoder component, which management applications and scripts can invoke to generate an XML representation of managed objects.

![Diagram of WMI infrastructure components]

**FIGURE 3.9** The major WMI infrastructure components.

Most files used by WMI are stored on the file system by default under the `%windir%\System32\Wbem` folder. The WMI repository is a set of files located by default under `%windir%\System32\Wbem\Repository`. The exact file structure varies slightly depending on the Windows version. WMI uses a customized version of the Jet database engine to access the repository files.

The executable containing the WMI service components is `Winmgmt.exe`. The physical implementation of the WMI infrastructure varies, depending on the version of Windows. In Windows 2000, `Winmgmt` runs as a separate Windows service. In this implementation, WMI providers are loaded into the `Winmgmt` process space, which means that a fault in one provider can crash the entire WMI process. This can cause repository corruption, which is a common cause of WMI problems in earlier Windows implementations. Using a single process space also means that providers share the security context of the `Winmgmt` process, which is generally the highly privileged Local System account. Newer versions of Windows achieve greater process isolation by loading providers into one or more
instances of WMIPrvse.exe. All WMI service components beginning with Windows XP run inside shared service host (SVCHOST) processes. Beginning with Windows Vista, Microsoft introduced several significant enhancements in WMI security and stability, including the ability to specify process isolation levels, security contexts, and resource limits for provider instances. These enhancements are also available as an update for Windows XP and Windows Server 2003 systems at http://support.microsoft.com/kb/933062.

Configuration parameters for the WMI service are stored in the system registry subtree HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM. The keys and values in this section of the registry specify WMI file locations, logging behavior, the list of installed providers, the default namespace for script, and other WMI options. You will rarely need to edit these options directly. As with any modification of the registry, you should use extreme caution as changes to the registry can destabilize your system.

WMI also provides detailed logging of its activities. Prior to Windows Vista, log entries were written in plain text to files in the %windir%\System32\Wbem\logs folder. In Windows Vista, Windows 7, and Windows Server 2008 and newer versions, most of these logs no longer exist, and Windows Event Tracing makes log data available to event data consumers, including the Event Log Service. By default, event tracing for WMI is not enabled. The “Managing WMI” section discusses logging and event tracing options for WMI and describes how to configure tracing for WMI.

Some WMI providers, such as the ConfigMgr provider, also log their activity. The “Viewing Detailed Process Activity” section discusses logging by the ConfigMgr WMI provider.

**Inside the WMI Object Model**

Understanding the WMI object model is essential if you will write programs or scripts that interact with WMI. It is also helpful for ConfigMgr administrators who want a better understanding of ConfigMgr objects such as collections and client settings. The DMTF’s Common Information Model (CIM) is the basis for the WMI object model. CIM defines a core model that provides the basic semantics for representing managed objects and describes several common models representing specific areas of management, such as systems, networks, and applications. Third parties develop extended models, which are platform platform-specific implementations of common classes. You can categorize the class definitions used to represent managed objects as follows:

- Core classes represent general constructs that are applicable to all areas of management. The Managed Element class is the most basic and general class and is at the root of the CIM class hierarchy. Other examples of core classes include
  - Component
  - Collection
  - CIM_StatisticalInformation

Core classes are part of the core model and are the basic building blocks from which other classes are developed.
Common classes represent specific types of managed objects. Common classes are
generalized representations of a category of objects, such as a computer system or an
application. These classes are not tied to a particular implementation or technology.

Extended classes are technology-specific extensions of common classes, such as a
Win32 computer system or ConfigMgr.

WMI classes support inheritance, meaning you can derive a new class from an existing
class. The derived class is often referred to as a child or subclass of the original class. The
child class has a set of attributes available to it from its parent class. Inheritance saves
developers the effort of needing to create definitions for all class attributes from scratch.
Developers of a child class can optionally override the definition of an inherited attribute
with a different definition better suited to that class. A child class can also have additional
attributes not inherited from the parent.

Typically, core and common classes are not used directly to represent managed objects.
Rather, they are used as base classes from which other classes are derived. The “Looking
Inside the CIMV2 Namespace” section of this chapter presents an example of how a class
inherits attributes from its parent class.

A special type of WMI class is the `System` class. WMI uses system classes internally to
support its operations. They represent things such as providers, WMI events, inheritance
metadata about WMI classes, and more.

WMI classes support three types of attributes:

- **Properties** are the characteristics of the managed objects, such as the name of a
computer system or the current value of a performance counter.

- **Methods** are actions that a managed object can perform on your behalf. As an
example, an object representing a Windows service may provide methods to start,
stop, or restart the service.

- **Associations** are actually links to a special type of WMI class, an association class,
which represents a relationship between other objects. The “Looking Inside the
CIMV2 Namespace” section examines the associations that link a file share security
descriptor to the share and to the security principals specified in its access control
lists.

You can also modify WMI classes, properties, and methods by the use of qualifiers. A qual-
ifier on a class may designate it as abstract, meaning the class is used only to derive other
classes and no objects of that class will be created. Two important qualifiers designate data
as static or dynamic:

- **Static data:** Supplied in the class or object definition and stored in the WMI
repository

- **Dynamic data:** Accessed directly through the provider and represents live data on
the system
The CIM specification also includes a language for exchanging management information. The Managed Object Format (MOF) provides a way to describe classes, instances, and other CIM constructs in textual form. In WMI, MOF files are included with providers to register the classes, properties, objects, and events they support with WMI. The information in the MOF files is compiled and stored to the WMI repository. Examples of information in MOF format are included in the next section.

**TIP: ACRONYM USAGE**

Chapter 1, “Configuration Management Basics,” discussed the Microsoft Operations Framework, often referred to as MOF. There is no relationship between the Microsoft Operations Framework and Managed Object Format, although both use the same acronym.

Namespaces organize WMI classes and other elements. A namespace is a container, much like a folder in a file system. Developers can add objects to existing namespaces or create new namespaces. The Root namespace defines a hierarchy organizing the namespaces on a system. The “Managing WMI” section describes the WMI Control tool, which allows you to specify the default namespace for connections to WMI. Generally, the default namespace will be Root\CIMV2. This namespace defines most of the major classes for Windows management, and the next section looks at several classes in that namespace. Because ConfigMgr is all about Windows management, it is not surprising that it uses this namespace extensively. ConfigMgr also defines its own namespaces, discussed in the “Looking Inside Configuration Manager with WMI” section.

If you are familiar with relational databases such as SQL Server, you may find it useful to consider an analogy between WMI and a database system. Table 3.2 presents some corresponding WMI and database concepts.

<table>
<thead>
<tr>
<th>WMI Concept</th>
<th>Database Concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>WMI Infrastructure</td>
<td>Database Engine</td>
</tr>
<tr>
<td>Namespace</td>
<td>Database</td>
</tr>
<tr>
<td>Class</td>
<td>Table</td>
</tr>
<tr>
<td>Instance</td>
<td>Row</td>
</tr>
<tr>
<td>Attribute</td>
<td>Column</td>
</tr>
</tbody>
</table>

This section presented the major concepts of WMI and the CIM model, which are essential to understanding ConfigMgr WMI activity. If you are interested in learning about other aspects of CIM, a good place to start is the tutorial at http://www.wbemsolutions.com/tutorials/CIM/index.html. The full CIM specification can be found at http://www.dmtf.org/standards/cim. Documentation for WMI is available at http://msdn.microsoft.com/en-us/library/aa394582.aspx.
Managing WMI

This section is intended to illustrate the options available for configuring WMI rather than being a “how-to” guide to administering WMI. You will rarely need to modify the WMI settings directly during day-to-day ConfigMgr administration. However, understanding the available options can help you understand the inner workings and functionality of WMI.

The Windows WMI Control is a graphical tool for managing the most important properties of the WMI infrastructure. Only members of the local Administrators group can use the WMI Control. To run this tool, perform the following steps:

1. Launch the Computer Management MMC snap-in. The exact procedure will vary depending on the version of Windows you are running. Generally you can right-click Computer or My Computer, and choose Manage.

2. Expand the Services and Applications node in the tree pane. For server operating systems, expand the Configuration node.

3. Right-click WMI Control and choose Properties.

The WMI Control opens to the General tab. As shown in Figure 3.10, the General properties confirm you have successfully connected to WMI on the local machine, display some basic properties of your system, and specify the installed version of WMI.

![WMI Control General Tab](image.png)

**FIGURE 3.10** The General tab of the WMI Control showing a successful connection to WMI on the local machine.
NOTE: ABOUT MANAGING WMI ON A REMOTE MACHINE

You can use the WMI Control tool to manage WMI on the local machine or on a remote machine. To connect to WMI on a remote machine, you follow the same procedure previously described in this section, with one additional step. Immediately after step 1, right-click the Computer Management node at the top of the tree, and choose **Connect to Another Computer**. Then enter the name or IP address of the computer you want to manage and click **OK**. After connecting to the remote machine, complete steps 2 and 3 in the procedure.

In addition to administrative privilege on the remote machine, you need appropriate DCOM permissions (described later in this section). In addition, DCOM network protocols must not be blocked on the remote machine or on any intermediary devices.

You can manage WMI security from the Security tab of the WMI Control tool. WMI uses standard Windows access control lists (ACLs) to secure each of the WMI namespaces that exist on your machine. A namespace, as described more precisely in the “Inside the WMI Object Model” section of this chapter, is a container that holds other WMI elements. The tree structure in the Security tab shows the WMI namespaces, as displayed in Figure 3.11.

![FIGURE 3.11](image)

FIGURE 3.11 The Security tab of the WMI Control tool, displaying the top-level WMI namespaces.

The namespace is the most granular level in which to apply ACLs in WMI. The process of setting security on WMI namespaces, and the technology behind it, is very similar to the process of setting NTFS (NT File System) security. If you click a namespace to select it and click **Security**, you see a dialog box similar to the one displayed in Figure 3.12.
NOTE: ABOUT THE SMS ADMINS GROUP

ConfigMgr automatically creates a local group named SMS Admins on each computer where you install the SMS Provider, and assigns the appropriate WMI permissions to this group. All administrative users configured as part of role-based administration are automatically added to this group, as is the site server computer account.

The dialog box in Figure 3.12 allows you to add security principals to the discretionary ACL (DACL) of the WMI namespace. The DACL specifies who can access the namespace and the type of access they have. With Windows XP and earlier operating systems, this was the only namespace access control implemented in WMI. Beginning with Windows Vista, enhancements to WMI, mentioned previously in the “WMI Feature Set and Architecture” section, added a system access control list (SACL) for WMI namespaces. The SACL specifies the actions audited for each security principal.

TIP: ABOUT AUDITING

As with other auditing of object access in Windows, auditing access to WMI namespaces requires the effective value of the group policy setting Audit Object Access to be enabled. The Windows Security event log records the events specified in the auditing settings.

![Security for ROOT\ccm.png](image)

FIGURE 3.12 The WMI Security dialog box for the CCM namespace (the root namespace of the ConfigMgr client).

To specify auditing on a WMI namespace, follow these steps:

1. From the Security dialog box, as shown in Figure 3.12, click the Advanced button.
2. In the Advanced Security Settings dialog box, click the Auditing tab.
3. Click the **Add** button and then enter the name of the user, group, or built-in security principal (see Figure 3.13). Click **OK**.

4. Complete the selections in the Auditing Entry dialog box, and click **OK**.

**FIGURE 3.13** Specifying a user, computer, or group for WMI control security.

---

**REAL WORLD: USING AUDITING TO TROUBLESHOOT WMI CONNECTIONS**

You can use auditing as a troubleshooting tool in the following ways:

▶ Auditing for access failures to help determine whether security problems are causing a WMI problem

▶ Auditing for access success to help determine whether there is a successful connection

Be judicious in auditing, as excessive auditing consumes unnecessary system resources and generates noise in the Security event log.

---

Figure 3.14 shows the entries to enable auditing for all access failures by members of the CM12 Servers group.

The remaining tabs of the WMI Control tool allow you to change the default namespace for WMI connections, and provide one of several methods of backing up the WMI repository. Windows system state backups also back up the repository. Prior to Windows Vista, the WMI Control tool also contained a Logging tab that allowed you to specify verbose, normal, or no logging, as well as choose the WMI log location and maximum log size. In newer operating systems, you can enable logging and configure log options in the Windows Event Viewer. To enable WMI Trace Logging in these versions of Windows, perform the following steps:
1. Open Event Viewer.
2. On the View menu, select Show Analytic and Debug Logs.
3. In the tree control, expand Applications and Service Logs -> Microsoft -> Windows -> WMI Activity.
4. Right-click Trace and then select Enable Log from the context menu. Choosing Properties from the same menu allows you to configure logging properties for WMI. You can now view, filter, and manage the WMI log from this node in the Event Viewer tree.

![Image of the WMI Auditing Entry dialog box](http://msdn.microsoft.com/en-us/library/aa394564.aspx)

**FIGURE 3.14** The WMI Auditing Entry dialog box displaying auditing enabled for all access failures by members of the ConfigMgr Site Servers group.


You should be aware that User Account Control, first introduced in Windows Vista, applies to privileged WMI operations. This can affect some scripts and command-line utilities. For a discussion of User Account Control and WMI, see http://msdn.microsoft.com/en-us/library/aa826699.aspx.

Additional command-line tools are available for managing WMI, which you can download from http://msdn.microsoft.com/en-us/library/aa827351.aspx. These tools include a MOF compiler, a command-line tool for performing WMI operations, and more. Another great resource for working with WMI is the WMI Diagnosis Utility (WMIDiag). WMIDiag is a Visual Basic script that tests the WMI functionality on the system and repairs many

**TIP: TROUBLESHOOTING REPOSITORY ISSUES**

SMS 2.0 was one of the first applications to take advantage of WMI. At one time, SMS was often the only WMI management application running on many Windows machines. In those days, it was a common practice among SMS administrators to simply delete the repository when WMI errors were detected, and then restart WMI to re-create the repository. This is no longer a safe practice, as many applications depend on data stored in the repository. Moreover, WMI errors can result from many other problems in your environment and may have nothing to do with WMI. Beginning with Windows Vista and Windows Server 2008, you can run the command `winmgmt /verifyrepository` to check the consistency of the repository. If this command reports that the repository is inconsistent, you can run `winmgmt /salvagerespository` to attempt to rebuild the repository. You can find information about these and other command options at http://blogs.technet.com/b/askperf/archive/2008/07/11/wmi-troubleshooting-the-repository-on-vista-server-2008.aspx. WMIDiag can also help you diagnosis most WMI problems, and in many cases it provides detailed instructions on how to correct those problems.

**Looking Inside the CIMV2 Namespace**

Windows provides a basic tool called WBEMTest that allows you to connect to a WMI namespace and execute WMI operations. However, there are a number of tools from Microsoft and third parties with more intuitive graphical interfaces for displaying and navigating WMI namespaces. This section uses the Microsoft WMI Administrative Tools to look into the `Root\CIMV2` namespace. These tools include the WMI CIM Studio and the WMI Object Browser. To download the latest WMI Administrative Tools, search for WMITools at www.microsoft.com/downloads. After downloading, run the WMITools.exe executable file to install the tools.

You can use CIM Studio to explore the classes in a namespace and view the properties, methods, and associations of each class. Perform the following steps to launch CIM Studio and connect to the CIMV2 namespace:

1. Select **Start -> All Programs -> WMI Tools -> WMI CIM Studio**.

2. CIM Studio opens a web browser and attempts to run an ActiveX control. If your browser blocks the control, select the option **Allow Blocked Content**.

3. Verify that `Root\CIMV2` displays in the **Connect to namespace** dialog box and then click **OK**. Notice that you can also browse to other namespaces on the local computer or a remote computer.

4. Click **OK** to accept the default logon settings.
When you open CIM Studio and connect to a namespace, the Class Explorer in the left pane contains a tree structure that displays the base classes in the selected namespace. Figure 3.15 displays the left pane with some of the root classes of the CIMV2 namespace.

Notice that most of the class names in Figure 3.15 begin with CIM or Win32. Class names starting with CIM indicate that the class is one of the core or common classes defined in the DMTF CIM schema. Classes with names beginning with Win32 are those extended classes that are part of the Win32 schema defined by Microsoft for managing the Win32 environment.

The Win32_LogicalShareSecuritySetting Class

This section uses the Win32_LogicalShareSecuritySetting class to illustrate how you can use CIM Studio to understand a class of managed objects. Figure 3.16 shows the Win32_LogicalShareSecuritySetting class displayed in CIM Studio. This class represents the security settings on a Windows file share. The expand tree shows the root class, CIM_Setting, and the classes derived from each successive subclass.

Looking at the tree structure, you can see that Win32_LogicalShareSecuritySetting is derived from Win32_SecuritySetting, which in turn is derived from CIM_Setting. The Class View in the right pane displays the properties of the Win32_LogicalShareSecuritySetting class. To the left of each property name, you will see one of the following icons:

- ▶ A yellow downward-pointing arrow indicates the property is inherited from the parent class.
▶ A property page indicates the property is defined within the class.
▶ A computer system indicates that the property is a system class. You can also recognize system classes by their names, which always start with a double underscore (_).

FIGURE 3.16 The Win32_LogicalShareSecuritySetting class displayed in CIM Studio.

For example, each WMI class has certain System properties, such as __PATH, __DYNASTY, __SUPERCLASS, and __DERIVATION. Here are some points to keep in mind:

▶ The __PATH property shows the location of the class in the namespace hierarchy. Management applications and scripts use the __PATH property to connect to the class.
▶ __DYNASTY, __SUPERCLASS, and __DERIVATION are all related to class inheritance and represent the root class from which the class is derived its immediate parent, and the entire family tree of the class, respectively.

Clicking the Array button next to __DERIVATION displays the array of parent classes from which the class is derived. The array is essentially the inheritance information already observed by traversing the tree, as shown in Figure 3.17.

The remaining properties of Win32_LogicalShareSecuritySetting are the ones that actually represent characteristics describing instances of Windows file share security settings. You can see that except for the name, all these properties are inherited. An object that has nothing unique about it except its name would not be very interesting, but there is more to the Win32_LogicalShareSecuritySetting class than the class properties. The most interesting attributes of Win32_LogicalShareSecuritySetting are on the remaining tabs of the CIM Studio Class View pane.
Clicking the **Methods** tab displays the two methods (GetSecurityDescriptor and SetSecurityDescriptor) of the **Win32_LogicalShareSecuritySetting** class, as shown in Figure 3.18.

**Getting Additional Information**

These methods let you work with the permissions on the actual file share. Clicking the Help button on the toolbar in the upper-right corner of Class View in Figure 3.18 provides additional information about the class.

**A SAMPLE HELP ENTRY**

The help entry for **Win32_LogicalShareSecuritySetting** returns the following information:

- **Caption**
  A short textual description (one-line string) of the CIM_Setting object.

- **ControlFlags**
  Inheritance-related flags. See SECURITY_DESCRIPTOR_CONTROL

- **Description**
  A textual description of the CIM_Setting object.

- **Name**
  The name of the share

- **SettingID**
  The identifier by which the CIM_Setting object is known.
uint32 GetSecurityDescriptor(
    [out] object:Win32_SecurityDescriptor Descriptor
);

Retrieves a structural representation of the object’s security descriptor. The method returns an integer value that can be interpreted as follows:
0 - Successful completion.
2 - The user does not have access to the requested information.
8 - Unknown failure.
9 - The user does not have adequate privileges.
21 - The specified parameter is invalid.
Other - For integer values other than those listed above, refer to Win32 error code documentation.

Descriptor
<description missing>

uint32 SetSecurityDescriptor(
);

Sets security descriptor to the specified structure. The method returns an integer value that can be interpreted as follows:
0 - Successful completion.
2 - The user does not have access to the requested information.
8 - Unknown failure.
9 - The user does not have adequate privileges.
21 - The specified parameter is invalid.
Other - For integer values other than those listed above, refer to Win32 error code documentation.

Descriptor
<description missing>

FIGURE 3.18 The Win32_LogicalShareSecuritySetting class methods, displayed in CIM Studio, allow management applications to retrieve or modify security on file shares.
Putting It All Together

The Win32_LogicalShareSecuritySetting example in the “A Sample Help Entry” sidebar shows that the GetSecurityDescriptor method returns the current security descriptor of the file share as an object of type Win32_SecurityDescriptor. The SetSecurityDescriptor method accepts a Win32_SecurityDescriptor object as input and replaces the security descriptor on the share with information supplied in the security descriptor object. The example also lists the status codes returned by these methods.

The information on the Class View Associations tab, shown in Figure 3.19, provides the key to understanding the implementation of Win32_LogicalShareSecuritySetting.

The Win32_LogicalShareSecuritySetting Associations tab (refer to Figure 3.19) displays an association with the Win32_Share class as well as associations with the two instances of the Win32_SID class. Class icons marked with a diagonal arrow represent the association classes linking other classes together. If you hover your mouse cursor over the class icons for each of the association classes linking Win32_LogicalShareSecuritySetting to Win32_SID.
class instances, you can see that one is a `Win32_LogicalShareAccess` class instance and the other is a `Win32_LogicalShareAuditing` class instance.

- Instances of the `Win32_LogicalShareAccess` association represent access control entries (ACEs) in the DACL (that is, share permissions).
- The `Win32_LogicalShareAuditing` instances represent ACEs in the SACL (audit settings) on the share. You can double-click any of the classes shown on this tab to navigate to it in Class View.

Because objects of the `Win32_LogicalShareSecuritySetting` class allow you to work with live data on the system, you would expect this to be a dynamic class. You can verify this by returning to the Properties or Methods tab, right-clicking any attribute, and selecting Object Qualifiers. The `Win32_LogicalShareSecuritySetting` object qualifiers are shown in Figure 3.20, including the dynamic qualifier, which is of type boolean with a value of true.

![Figure 3.20](image)

From the Class View, you can also use the Instances button to display all instances of the class, and you can open the properties of an instance by double-clicking it. The “Hardware Inventory Through WMI” section discusses how to use another of the WMI Administrative Tools, the WMI Object Browser, to view class instances. Just above the toolbar are icons that launch the MOF generator and MOF compiler wizards, as shown earlier in Figure 3.16. To launch the MOF compiler, you must check the Class icon next to the class and double-click the Wizard icon. The MOF language defining the `Win32_LogicalShareSecuritySetting` class is as follows:

```mof
#pragma namespace("\\\.\ROOT\\CIMV2")

/****************************************************************************
/* Class: Win32_LogicalShareSecuritySetting
/****************************************************************************
/* * Class: Win32_LogicalShareSecuritySetting */
CHAPTER 3  Looking Inside Configuration Manager

// Derived from: Win32_SecuritySetting
//**************************************************************************
[dynamic: ToInstance, provider("SECRCW32"): ToInstance, Locale(1033): ToInstance,
UUID("{8502C591-5FBB-11D2-AAC1-006008C78BC7}"): ToInstance]
class Win32_LogicalShareSecuritySetting : Win32_SecuritySetting
{
    [key, read: ToSubClass] string Name;
    [Privileges{"SeSecurityPrivilege", "SeRestorePrivilege":[ToSubClass,
    implemented, ValueMap{"0", "2", "8", "9", "21", ",..."}]}
    uint32 GetSecurityDescriptor([OUT] Win32_SecurityDescriptor Descriptor);
    [Privileges{"SeSecurityPrivilege", "SeRestorePrivilege":[ToSubClass,
    implemented, ValueMap{"0", "2", "8", "9", "21", ",..."}]}
    uint32 SetSecurityDescriptor([IN] Win32_SecurityDescriptor Descriptor);
};

The first line of the MOF entry, #pragma namespace ("\\.\\ROOT\\CIMV2"), is a prepro-
cessor command instructing the MOF compiler to load the MOF definitions into the
Root\CIMV2 namespace. A comment block follows, which indicates the class name Class:
Win32_LogicalShareSecuritySetting and the class derivation Derived from: Win32_ SecuritySetting. Next is a bracketed list of object qualifiers:

▶ The dynamic qualifier indicates that the class is dynamic and will be instantiated at runtime.
▶ The provider qualifier specifies that the instance provider is SECRCW32.
▶ The locale qualifier indicates the locale of the class, 1033 (U.S. English).
▶ The UUID qualifier is a Universally Unique Identifier for the class.

Each of these qualifiers propagates to class instances, as indicated by the toinstance keyword. Refer to Figure 3.20 to see a GUI representation of the object qualifiers.

The next section contains the class declaration Win32_LogicalShareSecuritySetting : Win32_SecuritySetting. This declaration derives the Win32_LogicalShareSecuritySetting class from the Win32_SecuritySetting base class. The body of the class declaration declares locally defined class properties and methods. The Name property (the name of the share) is declared to be of type String and designated as a key value, indicating that it uniquely identifies an instance of the class. The GetSecurityDescriptor and SetSecurityDescriptor methods are both of type uint32, indicating that each method return an unsigned 32-bit integer. GetSecurityDescriptor has an output parameter of type Win32_SecurityDescriptor, whereas SetSecurityDescriptor has a corresponding input parameter of the same type. Immediately preceding each of these method definitions, you will see the following method qualifiers specified:

▶ Privileges requests the access privileges required to manipulate Win32 security descriptors.
▶ *Implemented* is a Boolean value indicating the method is implemented in the class.

▶ *Valuemap* specifies the method’s return values. The “A Sample Help Entry” sidebar lists the meaning of each of these values.

In addition to the locally implemented properties and qualifiers, the *Win32_LogicalShareSecuritySetting* class inherits properties and qualifiers defined as part of its parent class, *Win32_SecuritySetting*.

Before continuing, you may want to explore several other classes in the *Root\CIMV2* namespace:

▶ Work your way up the inheritance tree from the *Win32_LogicalShareSecuritySetting* class and see where each of the inherited properties of the class originates. In addition, notice that if you bring up the object qualifiers on the parent classes, you can see these are qualified as abstract classes.

▶ The immediate sibling of the *Win32_LogicalShareSecuritySetting* class is the *Win32_LogicalFileSecuritySetting* class. Notice the differences in the properties and associations for this class. Share security and file security have many characteristics in common but a few important differences. Seeing how they are both derived from the *Win32_SecuritySetting* class demonstrates the power and flexibility of class inheritance.

▶ Expand the *CIM_StatisticalInformation* root class and then the *Win32_Perf* class. The two branches of Win32_Perf show how a variety of performance counters are implemented as managed objects.

This section looked at several of the default classes in the *Root\CIMV2* namespace and discussed how to use CIM Studio to explore a WMI namespace. The “WMI in ConfigMgr” section describes how ConfigMgr uses the classes in *Root\CIMV2* and as well as its own namespaces and classes.

**WMI in ConfigMgr**

ConfigMgr uses WMI extensively for both client and server operations. The ConfigMgr client uses WMI for internal control of its own operations and for gathering hardware inventory. ConfigMgr also uses WMI as an interface to the site database. The next sections discuss how ConfigMgr uses WMI on the client and then describe the use of WMI in ConfigMgr server operations.

**ConfigMgr Client Namespaces**

ConfigMgr 2012 creates and uses several namespaces in addition to adding classes to the *Root\CIMV2* namespace. The primary namespace created by the ConfigMgr client is the *Root\CCM* namespace. Together with several namespaces under *Root\CCM*, this namespace holds the configuration and policies that govern the operation of the ConfigMgr client. The *Root\CIMV2\SMS* namespace contains additional system-wide objects used
by ConfigMgr. The hardware inventory process described in the next section of this chapter uses a policy stored in the `Root\CCM\Policy\Machine\actualconfig` namespace to specify what inventory data to retrieve from managed objects defined in the `Root\CimV2` namespace. The “Additional Client Operations Through WMI” section discusses additional uses of the `Root\CCM` namespace.

**Hardware Inventory Through WMI**

The ConfigMgr client agent gathers hardware inventory data by querying WMI. The Client Agent settings determine which object classes are reported as part of the client inventory. For the majority of hardware inventory policy definitions, enabling or disabling what is reported from the clients to the ConfigMgr infrastructure is done from the console, via Client Agent settings. Modifications can be applied on as site wide basis by editing the Default Client Agent settings. To modify the hardware inventory settings for a subset of the environment (servers for example), create and modify a custom client setting, then assign it to a collection consisting of the appropriate systems. Chapter 9 describes client settings and inventory customization through the ConfigMgr console. Chapter 9 also discusses the changes in client inventory from ConfigMgr 2007. Appendix B, “Extending Hardware Inventory,” provides a detailed discussion of inventory customization.

The `configuration.mof` file defines classes used by the hardware inventory client agent to collect inventory. The CAS or top-level primary site imports the class definitions from the `configuration.mof` file and replicates them throughout the hierarchy. The `configuration.mof` file that ships with ConfigMgr provides a standard set of WMI classes, such as the Win32 classes. In some cases, a custom data class might be required. For example, an application or device driver may act as a WMI provider and create custom classes. You can also create data classes to provide inventory data that is accessible through existing WMI providers, such as data from the client’s system registry. In those cases, the administrator must import a custom `mof` file into the default client agent settings.

To apply inventory settings from a custom `mof` file, navigate to Administration -> Client Settings, and either select the Default Client Settings or create a Custom Client Device Settings object. On the Properties page, choose Hardware Inventory and click Set Classes -> Import.

ConfigMgr clients download client settings as part of their machine policy retrieval cycle. Any changes are compiled and loaded into the WMI repository. The ConfigMgr client stores its machine policy in the `Root\CCM\Policy\Machine\actualconfig` WMI namespace. You can use the WMI Object Browser from the WMI Administrative Tools to examine some to the inventory-related objects in this namespace. To launch the WMI Object Browser and connect to the `Root\CCM\Policy\Machine\actualconfig` namespace, follow these steps:

1. Select Start -> All Programs -> WMI Tools -> WMI Object Browser.

   The WMI Object Browser opens a web browser and attempts to run an ActiveX control.
If your browser blocks the control, select the option **Allow Blocked Content**.

2. Change the entry in the Connect to namespace dialog box to `Root\CCM\Policy\Machine\actualconfig` and then click OK.

3. Click OK to accept the default logon settings.

You can locate objects of a specified class by clicking the **Browse** button (the binocular icon on the toolbar above the left pane). Select **InventoryDataItem** from the available classes, as shown in Figure 3.21. Click OK to display a list of the items that will be inventoried.

![Figure 3.21: Browsing for InventoryDataItem in the WMI Object Browser.](image)

**InventoryDataItem** is the class representing inventory items specified in the machine policy. Figure 3.22 lists several of these instances in the `Root\CCM\Policy\Machine\actualconfig` namespace.

Figure 3.22 has the columns resized to hide the Key (1) column, which displays an object GUID (Globally Unique Identifier), and to display the more interesting information in Key (2) and Key (3).

Selecting the instance that refers to the `Win32_DiskDrive` class in the `Root\CIMV2` namespace and double-clicking this entry displays the instance properties, as shown in Figure 3.23.

The Namespace and ItemClass properties tell the hardware inventory agent it can retrieve inventory data for this class from `Win32_DiskDrive` objects in the `\Root\CIMV2` namespace. The Properties property contains a list of properties to inventory from each instance of `\Root\CIMV2\Win32_DiskDrive`. Here are the properties listed:

- Availability, Caption, Description, DeviceID, Index, InterfaceType, Manufacturer, MediaType, Model, Name, Partitions, PNPDeviceID, SCSIBus, SCSIIOLogicalUnit, SCSPort, SCSITargetException, Size, SystemName
Win32_DiskDrive objects have many other properties besides these. The property list in the machine policy settings instance corresponds to the properties selected in the applicable client settings object. To view these settings in the console, navigate to the Administration workspace and select Default Client Agent Settings -> Properties -> Hardware Inventory -> Set Classes. Classes that are checked will be collected and reported upon. Figure 3.24 shows the client agent hardware inventory settings for Disk Drives (Win32_DiskDrive).

Another InventoryDataItem instance in the Root\CCM\Policy\Machine namespace—Win32Reg_AddRemovePrograms—configures inventory settings for reporting on items of the Win32Reg_AddRemovePrograms class in the \\Root\CIMV2 namespace. Here is the MOF code for Win32Reg_AddRemovePrograms:
The System Registry provider (RegProv) exposes registry data to management applications. The `Win32Reg_AddRemovePrograms` class uses the Registry provider to retrieve the information stored under `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall` in the local registry dynamically. Each key under this location stores information about an item in Add/Remove Programs.
This example shows how the Registry provider exposes registry keys and values through WMI. You can use a mof compiler such as the one in CIM Studio to create classes representing various registry data, which you can then add to the ConfigMgr inventory. You can use similar methods to add data from any provider installed on the ConfigMgr client machines.

Additional Client Operations Through WMI

The ConfigMgr client creates WMI classes to represent its own components and configuration. The root of the ConfigMgr client namespace hierarchy is `Root\CCM`. The `Root\CCM` namespace contains classes representing client properties, such as identity and version information, installation options, and site information. Two of the classes in this namespace expose much of the functionality available through the Configuration Management Control Panel applet:

- The `SMS_Client` WMI class provides methods, displayed in Figure 3.25, that implement client operations such as site assignment, policy retrieval, and client repair.

![WMI CIM Studio](image)

**FIGURE 3.25** The `SMS_Client` class with the Methods tab displayed in CIM Studio.

- The `CCM_InstalledComponent` class defines properties such as name, file, and version information describing each of the installed client components. Figure 3.26 displays a list of the instances of the `CCM_InstalledComponent` class.

You will find managed objects for various client components in namespaces under `Root\CCM`. Figure 3.27 shows an instance of these classes, the `CacheConfig` class. The `CacheConfig` class in the `Root\CCM\SoftMgmtAgent` namespace contains settings for the client download cache, found on the Advanced tab of the Configuration Management Control Panel applet.
The properties of the CacheConfig class instance represent the client download cache settings.

The ConfigMgr client uses the Root\CCM\policy namespace hierarchy to store and process policy settings retrieved from the management point. The client maintains separate namespaces for machine policy and user policy.

During the policy retrieval and evaluation cycle, the policy agent, a component of the client agent, downloads and compiles policy settings and instantiates the requested policy
settings in the Root\CCM\policy\{machine|user\}RequestedConfig namespace, where the value of \{machine|user\} is machine for systemwide policies or user for user specific policies. The Policy Evaluator component then uses the information in RequestedConfig to update the Root\CCM\policy\{machine|user\}ActualConfig namespace. Based on the policy settings in the actual configuration, the Policy Agent Provider component updates various component instances with their appropriate settings. As an example, consider some of the objects used by the client to process policy for a deployment:

- **The policy agent**: The policy agent stores the policy for an assigned deployment as an instance of the CCM_SoftwareDistribution class in the Root\ccm\policy\<machine|user\>ActualConfig namespace, as shown in Figure 3.28.

![FIGURE 3.28 The properties of the CCM_SoftwareDistribution class instance for a ConfigMgr client upgrade deployment.](image)

- **The Scheduler component**: The Scheduler maintains history for the deployment in a CCM_Scheduler_History object in the Root\CCM\scheduler namespace, as displayed in Figure 3.29.

  This namespace can also contain schedule information for other components, including compliance evaluation schedules, software update schedules, and NAP schedules.

- **The Execution history**: The Execution Manager component uses the CCM_ExecutionRequestEx object in the Root\CCM\SoftMgmtAgent namespace, shown in Figure 3.30, to manage execution history for the deployment.
FIGURE 3.30   The CCM_ExecutionRequestEx object is used to manage execution history for the deployment.

FIGURE 3.29   The Scheduler uses the CCM_Scheduler_History object to maintain history for a deployment.

The Software Distribution Client Configuration class: Machine policy also controls the settings of various ConfigMgr client components. The CCM_SoftwareDistributionClientConfig class in the root\ccm\policy\machine\actualconfig namespace, shown in Figure 3.31, contains the Software Distribution client agent settings.
FIGURE 3.31 Some of the properties of the **CCM\_SoftwareDistributionClientConfig** class reflect client agent settings received from the site.

This section looked at some of the more important WMI classes the ConfigMgr client uses for its operations. This is by no means an exhaustive list; in fact, the client uses hundreds of WMI classes. The Configuration Manager server components have an even larger set of WMI classes. The next section presents an overview of how ConfigMgr uses WMI for server operations.

**WMI on ConfigMgr Servers**

The SMS Provider is a WMI provider that exposes many of the most important objects in the ConfigMgr site database as WMI managed objects. This provider is generally installed on either the site server or the site database server, as discussed in Chapter 4. The ConfigMgr console, auxiliary applications such as the Resource Explorer, Service Manager, and various ConfigMgr tools are implemented as WMI management applications. Chapter 8, “The Configuration Manager Console,” discusses the ConfigMgr console. As with other WMI providers, you can also take advantage of the SMS Provider’s objects in custom scripts or other management applications. Some people have even built their own console or web interfaces to replace console operations. The provider also implements the ConfigMgr object security model. Chapter 20 discusses the object security model and explains how to grant users access to the console and rights on various ConfigMgr objects and classes.

The SMS Provider namespace is `Root\SMS\site_<site code>`. You can use standard WMI tools to view ConfigMgr classes and objects.
This section uses ConfigMgr collections to illustrate how to drill down into the underlying WMI using PowerShell. (Chapter 11, “Packages and Programs,” and Chapter 13, “Distributing and Deploying Applications,” discuss collections.) The following PowerShell command connects to the site_CAS namespace on the site server Armada and displays the collection objects:

```
Get-WmiObject -class SMSCollectionView -computer "Armada" -namespace "root\SMS\site_CAS"
```

Here are several selected properties of one collection output by this statement:

- **IsBuiltIn**: True
- **LimitToCollectionID**: SMS00001
- **LimitToCollectionName**: All Systems
- **MemberClassName**: SMS_CM_RES_COLL_SMSDM001
- **Name**: All Mobile Devices
- **OwnedByThisSite**: True

Notice that the **MemberClassName** property shows the WMI class for all members of the collection. This statement displays the complete attribute set of all members of the All Mobile Devices collection:

```
Get-WmiObject -class SMS_CM_RES_COLL_SMSDM001 -namespace root\SMS\site_CAS
```

**TIP: WINDOWS POWERShell SCRIPTOMATIC**


**TIP: FORMATTING POWERSHELL OUTPUT**

Several of the method definitions shown in Figure 3.32 are truncated and displayed with an ellipsis (...). To see the entire definitions you can use the command: `Get-WmiObject -class SMSCollectionView -namespace root\SMS\site_CAS|Get-Member|Format-List`

The **SMSCollectionView** class methods allows you to perform operations such as pushing the ConfigMgr Client to collection members with the Create CCRs method and updating collection membership with the RequestRefresh method. When you perform these operations through the ConfigMgr console, you are actually invoking the methods of the **SMSCollectionView** class. Figure 3.33 displays the **SMSCollectionView** class associations.
FIGURE 3.32 The SMS_Collection class Properties and Methods.

FIGURE 3.33 The SMS_Collection class associations link a collection to its members (class SMS_Resource), and deployments (SMS_Advertisement) assigned to the collection.
The following PowerShell commands create an object representing the Odyssey Computers collection and enumerate all associated objects of type SMS_Resource, writing the results to a text file:

```powershell
$MyCollection = Get-WmiObject -class SMS_Collection -computer "Armada" -namespace "root\SMS\site_CAS" | where {$_.Name -eq "Odyssey Computers"}
$MyCollection.GetRelated() | Where {$_.__SUPERCLASS -eq "SMS_Resource"} | Out-File "OdysseyCollectionComputers.txt"
```

Several blogs referenced in Appendix C, “Reference URLs,” provide additional examples of how you can use PowerShell with ConfigMgr. Microsoft has announced plans to release a PowerShell provider for ConfigMgr by the end of 2012. This provider will extend the usefulness of PowerShell for managing ConfigMgr operations.

The smsprov.mof file contains the MOF language defining the `Root\SMS` namespace and the classes it contains. You can find the smsprov.mof file in the `bin\<platform>` folder under the ConfigMgr installation folder. You can also export MOF definitions for instances of the following ConfigMgr object types directly from the console:

- Device Collections are found in the Assets and Compliance workspace.
- User Collections are found in the Assets and Compliance workspace.
- Queries are found in the Monitoring workspace.

To export objects definitions to MOF files, right-click the workspace node to export multiple object or right-click a single object to export, choose Export, and complete the wizard to choose the instances to export and file location as well as to enter descriptive text. You can use a similar process to import objects from MOF files. You can use this process to copy objects between hierarchies. For example, you might develop and test queries in your lab environment and import them into production.

This section showed how the SMS Provider exposes Configuration Manager server components and database objects as WMI-managed objects. The “Root\CCM Namespace,” “Hardware Inventory Through WMI,” and “Additional Client Operations Through WMI” sections discussed how the ConfigMgr client uses WMI to maintain its configuration and policy and to gather inventory data. The ConfigMgr SDK, which was in prerelease when writing this chapter, is available for download from [http://www.microsoft.com/download/en/details.aspx?id=29559](http://www.microsoft.com/download/en/details.aspx?id=29559) (or search for ConfigMgr SDK at [www.microsoft.com/downloads](http://www.microsoft.com/downloads)). It provides extensive documentation and sample code for using WMI to manage ConfigMgr programmatically, with managed code or scripts.
Components and Communications

ConfigMgr’s code design is based on a componentized architecture, where sets of related tasks are carried out by logically distinct units of executable code, that work together to implement higher-level functionality. Most ConfigMgr code resides in dynamic link libraries (DLLs) in the bin\<processor architecture> folder under the ConfigMgr installation folder. Although most components run as threads of the SMS Executive service, some run as separate services. You can install all the components on the site server, or you can alternatively distribute many components to other servers.

Many of the thread components use folders known as *inboxes* to receive files from other components within the site. Inboxes may consist of a single folder or a folder subtree. Components maintain open file system change notification handles on their inboxes. A component can notify another component that it has work to do by dropping a file in its inbox. The operating system then returns a file change notification event to the component owning the inbox. In ConfigMgr 2012, many components no longer write directly to other components’ inbox folders. Instead, these components apply changes directly to the database. The Database Notification Monitor component detects the change and creates a zero byte file in the appropriate inbox to serve as a wake up call. Some components also use in-memory queues for faster communications with other components on the local machine. Some components also maintain outbox folders in which they place files to be processed by other components. Many components additionally operate a watchdog cycle, in which they wake up at regular intervals to perform specific work. Unlike early SMS versions in which watchdog cycles introduced latency into various operations, time-sensitive processing does not depend on watchdog cycles.

Table 3.3 displays many of the ConfigMgr components with a description of their principal functions, the folders they use to communicate with other components, and the log files they maintain. To view the actual components installed on each server expand the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Components registry key. The actual inboxes installed and their folder locations are found under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\Inbox Source\Inbox Instances. Most components log details of their activities. Appendix A, "Configuration Manager Log Files," discusses logging options and log file locations for specific components. The Component Type column indicates whether the component runs as its own process or as a thread of the Executive service, and if it is monitored by the Site Component Manager. The components installed on a ConfigMgr site system will vary depending on the site roles assigned to the server and the code revision you are running.
TABLE 3.3 Component Names and Descriptions

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Display Name</th>
<th>Description</th>
<th>Directory Used</th>
<th>Log File</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS_SITE_COMPONENT_MANAGER</td>
<td>Site Component Manager (Component not installed by Site Component Manager)</td>
<td>Installs and manages components on site systems</td>
<td>INBOX: sitecomp.box</td>
<td>sitecomp.log</td>
</tr>
</tbody>
</table>

Monitored Service Components

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Display Name</th>
<th>Description</th>
<th>Directory Used</th>
<th>Log File</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS_EXECUTIVE</td>
<td>Executive Service</td>
<td>Host process for thread components</td>
<td></td>
<td>Smsexec.log</td>
</tr>
<tr>
<td>SMS_SITE_SQL_BACKUP</td>
<td>SMS Site SQL Backup Service</td>
<td>Backup process for site database</td>
<td></td>
<td>smssqlbkup.log</td>
</tr>
<tr>
<td>SMS_SITE_VSS_WRITER</td>
<td>SMS Writer Service</td>
<td>Manages volume snapshots for backups</td>
<td></td>
<td>smswriter.log</td>
</tr>
</tbody>
</table>

Monitored Thread Components

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Display Name</th>
<th>Description</th>
<th>Directory Used</th>
<th>Log File</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS_AI_KB_MANAGER</td>
<td>Asset Intelligence Knowledge Base Manager</td>
<td>Maintains Asset Intelligence data in the site database</td>
<td>INBOX: aikbmgr.box</td>
<td>aikbmgr.log</td>
</tr>
<tr>
<td>SMS_ALERT_NOTIFICATION</td>
<td>Alert Notification Manager</td>
<td>Processes instruction files for alerts, sends e-mail, maintains database triggers</td>
<td>INBOX: notictrl.box</td>
<td>NotiCtrl.log</td>
</tr>
<tr>
<td>SMS_AMT_PROXY_COMPONENT</td>
<td>Advanced Management Technology (AMT) Proxy</td>
<td>Handles provisioning, maintenance, and requests for Intel AMT clients</td>
<td>INBOX: amtproxymgr.box</td>
<td>amtproxymgr.log</td>
</tr>
<tr>
<td>SMS_AWEBSVC_CONTROL_MANAGER</td>
<td>Application Catalog Web Service</td>
<td>Maintains Application Catalog web service</td>
<td></td>
<td>awebsctl.log</td>
</tr>
<tr>
<td>SMS_CERTIFICATE_MANAGER</td>
<td>Certificate Manager</td>
<td>Maintains certificates</td>
<td>INBOX: certmgr.box</td>
<td>CertMgr.log</td>
</tr>
<tr>
<td>SMS_CLIENT_CONFIG_MANAGER</td>
<td>Client Configuration Manager</td>
<td>Carries out client push installation and maintains the Client Push Installation account</td>
<td>INBOX: ccr.box</td>
<td>ccm.log</td>
</tr>
<tr>
<td>Component Name</td>
<td>Display Name</td>
<td>Description</td>
<td>Directory Used</td>
<td>Log File</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SMS_CLIENT_HEALTH</td>
<td>Client Health</td>
<td>Processes client health (.POL) files</td>
<td></td>
<td>Chmgr.log</td>
</tr>
<tr>
<td>SMS_COLLECTION_EVALUATOR</td>
<td>Collection Evaluator</td>
<td>Updates collection membership</td>
<td>INBOX: colleval.box; OUTBOX: coll_out.box (used for sending to child sites)</td>
<td>colleval.log</td>
</tr>
<tr>
<td>SMS_COMPONENT_MONITOR</td>
<td>Component Monitor</td>
<td>Maintains registry setting for discovery components</td>
<td></td>
<td>compmon.log</td>
</tr>
<tr>
<td>SMS_COMPONENT_STATUS_SUMMARIZER</td>
<td>Component Status Summarizer</td>
<td>Processes component status summarization rules</td>
<td>INBOX: Compsumm.box</td>
<td>compsumm.log</td>
</tr>
<tr>
<td>SMS_DATABASE_NOTIFICATION_MONITOR</td>
<td>Database Notification Monitor</td>
<td>Watches the database for changes to certain tables and creates files in the</td>
<td>This component writes to many inbox folders</td>
<td>smsdbmon.log</td>
</tr>
<tr>
<td>SMS_DESPOOLER</td>
<td>Despooler</td>
<td>Processes incoming files from parent or child sites</td>
<td>INBOX: despoolr.box</td>
<td>despool.log</td>
</tr>
<tr>
<td>SMS_DISCOVERY_DATA_MANAGER</td>
<td>Discovery Data Manager</td>
<td>Processes discovery data and enters it into the site database</td>
<td>INBOXES: ddm.box; Auth\ddm.box</td>
<td>ddm.log</td>
</tr>
<tr>
<td>SMS_DISTRIBUTION_MANAGER</td>
<td>Distribution Manager</td>
<td>Copies packages to distribution points</td>
<td>INBOX: distmgr.box</td>
<td>distmgr.log</td>
</tr>
<tr>
<td>SMS_ENDPOINT_PROTECTION_MANAGER</td>
<td>Endpoint Protection Manager</td>
<td>Manages endpoint protection configuration</td>
<td>INBOX: epmgr.box</td>
<td>EPMgr.log</td>
</tr>
<tr>
<td>SMS_HIERARCHY_MANAGER</td>
<td>Site Hierarchy Manager</td>
<td>Processes and replicates changes to the site hierarchy</td>
<td>INBOX: hman.box</td>
<td>Hman.log</td>
</tr>
<tr>
<td>SMS_INBOX_MANAGER</td>
<td>Inbox Manager</td>
<td>Maintains inbox files</td>
<td></td>
<td>inboxmgr.log</td>
</tr>
<tr>
<td>Component Name</td>
<td>Display Name</td>
<td>Description</td>
<td>Directory Used</td>
<td>Log File</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>SMS_INBOX_MONITOR</td>
<td>Inbox Monitor</td>
<td>Monitors the file count in various inboxes</td>
<td></td>
<td>inboxmon.log</td>
</tr>
<tr>
<td>SMS_INVENTORY_DATA_LOADER</td>
<td>Inventory Data Loader</td>
<td>Loads hardware inventory data from clients into the site database</td>
<td>INBOXES: dataldr.box; Auth\dataldr.box</td>
<td>dataldr.log</td>
</tr>
<tr>
<td>SMS_INVENTORY_PROCESSOR</td>
<td>Inventory Processor</td>
<td>Converts hardware inventory to a binary format used by the data loader</td>
<td>INBOX: Inventory.box</td>
<td>invproc.log</td>
</tr>
<tr>
<td>SMS_LAN_SENDER</td>
<td>Standard Sender</td>
<td>Initiates intersite communications across TCP/IP networks</td>
<td>INBOX: schedule. box\outboxes\LAN</td>
<td>sender.log</td>
</tr>
<tr>
<td>SMS_MIGRATION_MANAGER</td>
<td>Migration Manager</td>
<td>Schedules migration tasks</td>
<td>INBOX: mmctrl.box</td>
<td>Migmctrl.log</td>
</tr>
<tr>
<td>SMS_MP_CONTROL_MANAGER</td>
<td>Management Point</td>
<td>Manages certificate usage for the management point and monitors management point availability</td>
<td></td>
<td>mpcontrol.log</td>
</tr>
<tr>
<td></td>
<td>Control Manager</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMS_MP_FILE_DISPATCH_MANAGER</td>
<td>Management Point File</td>
<td>Transfers files from management point outboxes to site server inboxes</td>
<td>INBOX: MP\OUTBOXES; OUTBOXES: See note</td>
<td>mpfdm.log</td>
</tr>
<tr>
<td></td>
<td>Dispatcher</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMS_OBJECT_REPLICATION_MANAGER</td>
<td>Object Replication</td>
<td>Creates CIXML representations for the ConfigMgr object for replication to primary child sites</td>
<td>INBOX: objmgr.box</td>
<td>objreplmgr.log</td>
</tr>
<tr>
<td></td>
<td>Manager</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMS_OFFER_MANAGER</td>
<td>Offer Manager</td>
<td>Manages advertisements</td>
<td>INBOX: offermgr.box</td>
<td>offermgr.log</td>
</tr>
<tr>
<td>SMS_OFFER_STATUS_SUMMARIZER</td>
<td>Offer Status Summarizer</td>
<td>Populates advertisement status summary information in the site database</td>
<td>INBOX: OfferSum. box</td>
<td>offersum.log</td>
</tr>
<tr>
<td>Component Name</td>
<td>Display Name</td>
<td>Description</td>
<td>Directory Used</td>
<td>Log File</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>SMS_OUTBOX_MONITOR</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMS_PACKAGE_TRANSFER_MANAGER</td>
<td>Package Transfer Manager</td>
<td>Transfers packages to distribution points</td>
<td>INBOX: PkgTransferMgr.box; OUTBOXES: PkgTransferMgr.box\outboxes</td>
<td>PkgXferMgr.log</td>
</tr>
<tr>
<td>SMS_POLICY_PROVIDER</td>
<td>Policy Provider</td>
<td>Generates policies for ConfigMgr components</td>
<td>INBOX: policypv.box</td>
<td>policypv.log</td>
</tr>
<tr>
<td>SMS_PORTALWEB_CONTROL_MANAGER</td>
<td>Application Catalog Web Portal Manager</td>
<td>Configures web portal service</td>
<td></td>
<td>Portlctl.log</td>
</tr>
<tr>
<td>SMS_REPLICATION_CONFIGURATION_MONITOR</td>
<td>Replication Configuration Monitor</td>
<td>Processes inbound and outbound files for intersite communications</td>
<td>INBOX: rcm.box</td>
<td>Rcmctrl.log</td>
</tr>
<tr>
<td>SMS_REPLICATION_MANAGER</td>
<td>Replication Manager</td>
<td></td>
<td>INBOX: Replmgr.box</td>
<td>replmgr.log</td>
</tr>
<tr>
<td>SMS_RULE_ENGINE</td>
<td>Rule Engine</td>
<td>Processes automatic deployment rules for software updates</td>
<td>INBOX: RuleEngine.box</td>
<td>Ruleengine.log</td>
</tr>
<tr>
<td>SMS_SCHEDULER</td>
<td>Scheduler</td>
<td>Converts replication manager jobs to sender jobs</td>
<td>INBOX: Schedule.box</td>
<td>sched.log</td>
</tr>
<tr>
<td>SMS_SITE_CONTROL_MANAGER</td>
<td>Site Control Manager</td>
<td>Maintains site control data</td>
<td>INBOX: sitectrl.box</td>
<td>sitectrl.log</td>
</tr>
<tr>
<td>SMS_SITE_SYSTEM_STATUS_SUMMARIZER</td>
<td>Site System Status Summarizer</td>
<td>Processes status messages for the local site and applies summarization rules</td>
<td>INBOX: SiteStat.Box\repl</td>
<td>sitestat.log</td>
</tr>
<tr>
<td>SMSSOFTWARE_INVENTORY_PROCESSOR</td>
<td>Software Inventory Processor</td>
<td>Loads software inventory data from clients into the site database</td>
<td>INBOXES: sinv.box; Auth\sinv.box</td>
<td>sinvproc.log</td>
</tr>
<tr>
<td>Component Name</td>
<td>Display Name</td>
<td>Description</td>
<td>Directory Used</td>
<td>Log File</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SMS_SOFTWARE_METERING_PROCESSOR</td>
<td>Software Metering Processor</td>
<td>Processes software metering information from clients and updates metering data in the site database</td>
<td>INBOX: swmproc.box</td>
<td>swmproc.log</td>
</tr>
<tr>
<td>SMS_SRS_REPORTING_POINT</td>
<td>Reporting Services Point</td>
<td>Configures SQL Server Reporting Services</td>
<td></td>
<td>srsrp.log</td>
</tr>
<tr>
<td>SMS_STATE_MIGRATION_POINT</td>
<td>State Migration Point</td>
<td>Maintains user state data</td>
<td>INBOX: Auth\statesys.box</td>
<td>smpmgr.log</td>
</tr>
<tr>
<td>SMS_STATE_SYSTEM</td>
<td>State System</td>
<td>Processes and summarizes state messages</td>
<td>INBOX: Auth\statesys.box</td>
<td>statesys.log</td>
</tr>
<tr>
<td>SMS_STATUS_MANAGER</td>
<td>Status Manager</td>
<td>Processes status messages and writes status information to the site database</td>
<td>INBOX: Statmgr.box; SMS_EXECUTIVE to SMS_STATUS_MANAGER in-memory status message queue</td>
<td>statmgr.log</td>
</tr>
<tr>
<td>SMS_WSUS_CONFIGURATION_MANAGER</td>
<td>WSUS Configuration Manager</td>
<td>Maintains WSUS settings and checks connectivity to upstream server</td>
<td>INBOX: WSUSMgr.box</td>
<td>WCM.log</td>
</tr>
<tr>
<td>SMS_WSUS_CONTROL_MANAGER</td>
<td>WSUS Control Manager</td>
<td>Verifies WSUS component health, configuration, and database connectivity</td>
<td></td>
<td>WSUSCtrl.log</td>
</tr>
<tr>
<td>SMS_WSUS_SYNC_MANAGER</td>
<td>WSUS Synchronization Manager</td>
<td>Synchronizes updates with upstream server</td>
<td>INBOX: wsyncmgr.box</td>
<td>wsyncmgr.log</td>
</tr>
</tbody>
</table>

Unmonitored Service Component
<table>
<thead>
<tr>
<th>Component Name</th>
<th>Display Name</th>
<th>Description</th>
<th>Directory Used</th>
<th>Log File</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS_SITE_BACKUP</td>
<td>Site Backup Agent</td>
<td>Performs the site backup task</td>
<td></td>
<td>Smsbkup.log (in site backup folder)</td>
</tr>
<tr>
<td>Unmonitored Thread Components</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMS_OFFLINE_SERVICING_MANAGER</td>
<td>Offline Servicing for</td>
<td>Manages Software Updates for offline OS images</td>
<td></td>
<td>OfflineServicingMgr.log</td>
</tr>
<tr>
<td></td>
<td>Operating System Images</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMS_NETWORK_DISCOVERY</td>
<td>Network Discovery Agent</td>
<td>Performs network discovery</td>
<td>Drops DDRs in DDR.box</td>
<td>netdisc.log</td>
</tr>
<tr>
<td>SMS_WINNT_SERVER_DISCOVERY_AGENT</td>
<td>Server Discovery Agent</td>
<td>Performs discovery on ConfigMgr site systems</td>
<td>Drops DDRs in DDR.box</td>
<td>ntsvrdis.log</td>
</tr>
</tbody>
</table>
Here is additional information regarding some of the components described in Table 3.3:

▶ The Site Component Manager monitors the Site Control inbox (sitectrl.box) for changes to site properties that require adding, removing, or altering a component on a site system. This is in addition to monitoring its own inbox.

▶ The Discovery Data Manager, Inventory Data Loader, Software Inventory Processor, and State System components maintain trusted inboxes under the inboxes\auth folder for signed files.

▶ The Management Point File Dispatcher transfers files from its inboxes (MP outbox folders) to the inboxes of other components. To accomplish this, it uses the inboxes of the following components as its outboxes: Client Configuration Manager, Discovery Data Manager, Distribution Manager, Inventory Processor, Software Metering Processor, State System, and Status Manager.

The core components that maintain a ConfigMgr site are the Executive Service, Site Component Manager, Site Control Manager, and Site Hierarchy Manager:

▶ The Executive Service is the host process in which most other components run. The Executive Service exists on every ConfigMgr site system other than the site database server.

▶ The Site Component Manager is a separate service that configures and manages other components.

▶ The Site Hierarchy Manager and Site Control Manager work together to maintain the site settings. Each ConfigMgr site maintains site control information in the ConfigMgr database for that site.

Site control information includes the parent site, sender addresses, client and server components, and various other site properties. Site control data is stored in the site database and replicated as global data to all sites in the hierarchy.

Here is an example where an administrator makes a change to a site property using the ConfigMgr console, showing how ConfigMgr components interact:

1. The console application reads the current site control file and calculates a delta based on the settings applied by the administrator. The console code then invokes the CommitSCF method of the SMS_SiteControlFile WMI object to apply the changes in the database.

2. The SMS Provider executes the method against the database. The CommitSCF method inserts the changes into the SiteControl table. Inserting data into the SiteControl table fires the SMSDBMON_SiteControl_SiteControl_AddUpd_HMAN_ins trigger. This creates a new entry in the TableChangeNotifications table.

3. The Database Monitor reads the TableChangeNotifications and processes the change notification.
4. The Database Monitor drops an empty site control file in the Hierarchy Manager inbox to notify Hierarchy Manager of the site changes.

5. Hierarchy Manager updates related tables in the site database.

Figure 3.34 illustrates these steps.

![Diagram illustrating changes made to a site property]

After the site control information in the database is updated, ConfigMgr uses SQL replication to replicate this data as global data.

Most of the remaining components work together, implementing specific feature sets. An important example of this is file-based replication between sites. Here is what will occur when a ConfigMgr component has file data to replicate to another site:

1. The component with data to replicate to another site copies the file(s) to one of the subfolders of the Outbound folder in the Replication Manager’s inbox. The subfolders are named high, normal, or low to indicate the priority of the replication job. The file names begin with the destination site code for routing purposes.

2. The Replication Manager compresses the file(s) to its process folder and moves them to its ready folder. Replication Manager then creates a job file under the Scheduler inbox.
3. The Scheduler processes the instruction file and creates instruction and package files in the tosend folder (inboxes\schedule.box\tosend). It then transfers the files to the appropriate sender.

4. The Sender copies the files to the SMS_SITE share on the destination site server. This share is the despooler\receive inbox.

5. At the destination site, the Despooler validates the signature from of the source site server, decompresses the files, and moves them to the Replication Manager inbox.

6. The Replication Manager moves the file to the appropriate inbox of the component for which the file is intended. The Replication Manager also initiates any replication to additional sites that may be required.

The “Viewing Detailed Process Activity” section looks into the inner workings of these processes.

Inside the ConfigMgr Database

The ConfigMgr site database is a SQL Server database that contains data about your ConfigMgr infrastructure and objects, the client systems you manage, and other discovered resources. The default name of the site database is CM_<site code> (where <site code> indicates the primary site the database is associated with). Although the exact number of objects in a ConfigMgr site database varies, there are generally several thousand objects. Management applications, including the ConfigMgr console, use WMI to access the database.

ConfigMgr Tables and Views

SQL Server stores data in tables. If you are new to SQL, you can think of a table as similar to a spreadsheet with rows and columns of data. A view is a window into the data. A view retrieves data from one or more tables and presents it to the user or calling application. Microsoft’s Configuration Manager developers provide an extensive set of database views that presents the underlying data tables in a consistent way. The views abstract away many of the details of the underlying table structure, which may change with future product releases. The reports in ConfigMgr use SQL views. Chapter 18 presents numerous examples of reports based on the SQL views. You can use the views to understand the internal structure of the database. The next sections present a subset of these views and provide information about how the views are organized and named.

Most of the Configuration Manager SQL views correspond to ConfigMgr WMI classes. In many cases, the views also reflect the underlying table structure, with minor formatting changes and more meaningful field names. Many views also combine related data from multiple tables.

Most ConfigMgr administration tasks do not require you to work directly with SQL statements. You can enter SQL statements directly into ConfigMgr reports and database maintenance tasks. Chapter 18 discusses reports, and Chapter 21, “Backup, Recovery, and
Maintenance,” discusses database maintenance tasks. To understand the internal structure and operation of the database, however, requires looking at it with SQL tools.

**Using SQL Server Management Studio**

The primary user interface for administering SQL Server 2008 is the SQL Server Management Studio. To access the Configuration Manager views, follow these steps:

1. **Launch the SQL Server Management Studio from Start -> All Programs -> Microsoft SQL Server 2008 -> SQL Server Management Studio.**

2. After connecting to the site database server SQL instance, expand the `<servername>\database\CM_<site code>\views` in the tree control in the left pane.

**CAUTION: DO NOT MODIFY THE SITE DATABASE DIRECTLY**

The site database is critical to the functioning of your site. This section presents tools you can use to view the site database. This information can be useful for understanding how Configuration Manager works and for using ConfigMgr data in reporting. Do not attempt to create, delete, or modify any database objects, or to modify data stored in the database, unless asked to do so by Microsoft support personnel. Remember to test all modifications before applying them to your production environment.

**Viewing Collections**

The “WMI on Configuration Manager Servers” section of this chapter looked in some detail at the `Collection` WMI object. This object provides access to the properties and methods of the ConfigMgr collections defined in the site database. The SQL view `v_Collection` provides access to much of the same data. Figure 3.35 shows the tree control expanded in the left pane to display the column definitions for `v_Collection`, whereas the view on the right displays some of the column values visible when opening the view. These columns correspond to `SMS_Collection` WMI class properties (refer to Figure 3.32). Notice that the `MemberClassName` column provides the name of the view for the collection membership. These views correspond to the WMI objects specified in the `MemberClassName` property of the `SMS_Collection` WMI class.

**FIGURE 3.35** The `v_Collection` SQL view displays the descriptive properties of the site’s ConfigMgr collections.
The \textit{v\_Collection} view is one of several views referencing ConfigMgr objects. Similar views include \textit{v\_Advertisement}, \textit{v\_Package}, and \textit{v\_Roles}. The naming conventions for views generally map to the corresponding WMI classes, according to the following rules:

- WMI class names begin with SMS\_, and SQL view names begin with v or v\_.
- View names more than 30 characters are truncated.
- The WMI property names are the same as the field names in the SQL views.

\textbf{Site Properties}

Basic ConfigMgr site properties are stored in the Sites table and exposed though several views and stored procedures. As an example, \textit{v\_site} displays the basic configuration of the current site and its child sites. The sysreslist table stores information about the site systems. An example of a stored procedure that retrieves data from the sites and sysreslist tables is GetMPLocationForIPSubnet, which displays management point information for an IP subnet. The SMSData table includes additional site details, exposed through \textit{v\_identification}.

The tables and views discussed so far relate to the ConfigMgr objects and infrastructure. The database also contains a wealth of data gathered by various discovery methods and client inventory. Chapter 9 discusses discovery and inventory. Discovery and inventory data is stored in resource tables and presented in resource views. The naming conventions for resource views are as follows:

- Views displaying current inventory data are named \textit{v\_GS\_<group name>}.  
- Views displaying inventory history data are named \textit{v\_HS\_<group name>}.  
- Views containing discovery data are named \textit{v\_<resource type name>\_<architecture name>\_<group name>\_} for data contained in WMI scalar properties and \textit{v\_<resource type name>\_<architecture name>\_<group name>\_} for data contained in WMI array properties.  
- Inventory data for custom architectures is presented in views named \textit{v\_<resource type number>\_<group name>} and \textit{v\_<resource type number>\_<group name>}. Custom architectures are created by adding IDMIF files to the inventory as described in Chapter 9.

\textbf{Other Views}

Several views are included that present metadata on other views and serve as keys to understanding the view schema. The \textit{v\_SchemaViews} view, displayed in Figure 3.36, lists the views in the view schema family, and shows the type of each view.

Here is the SQL statement that generates the \textit{V\_SchemaViews} view:

\begin{verbatim}
CREATE VIEW [dbo].[v_SchemaViews] As SELECT CASE
WHEN name like 'v[\_]RA[\_]\%' THEN 'Resource Array'
WHEN name like 'v[\_]R[\_]\%' THEN 'Resource'
WHEN name like 'v[\_]HS[\_]\%' THEN 'Inventory History'
\end{verbatim}
WHEN name like 'v\[_\]GS\[_\]%' THEN 'Inventory'
WHEN name like 'v\[_\]CM\[_\]%' THEN 'Collection'
WHEN name like '%Summ%' THEN 'Status Summarizer'
WHEN name like '%Stat%' THEN 'Status'
WHEN name like '%Permission%' THEN 'Security'
WHEN name like '%Secured%' THEN 'Security'
WHEN name like '%Map%' THEN 'Schema'
WHEN name = 'v_SchemaViews' THEN 'Schema'
ELSE 'Other'
END
As 'Type', name As 'ViewName' FROM sysobjects
WHERE type='V' AND name like 'v\[_\]'

If you examine the SQL statement, you can see that the selection criteria in the CASE statement use the naming conventions to determine the type of each view.

FIGURE 3.36  V_SchemaViews provides a list and categorization of ConfigMgr views.

The v_ResourceMap view presents data from the DiscoveryArchitectures table, which defines the views representing discovery data. Table 3.4 displays the data provided by the v_ResourceMap view.

ConfigMgr uses the fields in Table 3.4 in the following manner:

- The ResourceType field is the key used throughout the resource views to associate resources with the appropriate discovery architecture.
The DisplayName field is a descriptive name of the discovery architecture.

The ResourceClassName indicates the view that contains basic identifying information for each discovered instance of the architecture.

### TABLE 3.4 The v_ResourceMap View

<table>
<thead>
<tr>
<th>ResourceType</th>
<th>DisplayName</th>
<th>ResourceClassName</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Unknown System</td>
<td>v_R_UnknownSystem</td>
</tr>
<tr>
<td>3</td>
<td>User Group</td>
<td>v_R_UserGroup</td>
</tr>
<tr>
<td>4</td>
<td>User</td>
<td>v_R_User</td>
</tr>
<tr>
<td>5</td>
<td>System</td>
<td>v_R_System</td>
</tr>
<tr>
<td>6</td>
<td>IP Network</td>
<td>v_R_IPNetwork</td>
</tr>
</tbody>
</table>

As an example, the v_R_System represents discovery data from the System_DISC table. This view provides the unique Resource ID of each computer system discovered by ConfigMgr as well as basic system properties such as the NetBIOS name, operating system, and AD domain. Each resource view containing system information includes the Resource ID field, allowing you to link resources such as hard drives and network cards with the system to which they belong.

The v_ResourceAttributeMap view displayed in Figure 3.37 presents resource attribute types extracted from discovery property definition data in the DiscPropertyDefs table.

![FIGURE 3.37 v_ResourceAttributeMap lists the attributes used in resource views.](image)
The ConfigMgr development team appends many of the column names with “0” to avoid possible conflicts with SQL reserved words.

The v_GroupMap view lists the inventory groups and views associated with each inventory architecture. Table 3.5 displays some v_GroupMap entries. Each inventory architecture represents a WMI class specified for inventory collection in the client agent settings.

Each entry in Table 3.5 specifies the resource type, a unique GroupID, the inventory and inventory history views that present the group data, and the Management Information Format (MIF) class from which the inventory data for the group is derived.

The v_GroupAttributeMap lists the attributes associated with each inventory group, and the v_ReportViewSchema view provides a list all classes and properties.

This section examined several of the SQL views that Microsoft provides. You can learn a considerable amount about the internal structure of ConfigMgr by using SQL Server Management Studio to explore the database on your own. You may want to look at the views, the underlying tables, and some of the stored procedures ConfigMgr uses. The examples in this section show how you can analyze and understand these objects.

Viewing Detailed Process Activity

The “WMI in ConfigMgr,” “Components and Communications,” and “Inside the ConfigMgr Database” sections described the ConfigMgr technical architecture. This section presents some tools you can use to view the inner working of ConfigMgr in detail. The section includes a detailed example to illustrate the use of these tools.

System Center 2012 ConfigMgr provides two built-in mechanisms that allow you to view and analyze ConfigMgr operations in detail:

- ConfigMgr components generate status messages to report milestone activity and problem occurrences. System administrators can view status messages and use them in queries and reports. You can also configure the status message system to invoke automated actions in response to specified status messages.
- ConfigMgr components generate extensive logs that give additional detail about their activity.

Both the status message system and logging are highly configurable and provide valuable windows into the system.

Digging into ConfigMgr logs is one of the best ways to gain a deep understanding of ConfigMgr internals. Much of the material in this chapter is drawn from analyzing log files. Chapter 21 covers configuring the status message system. Appendix A discusses the various ConfigMgr logs in detail. This part of the chapter discusses the use of status messages and logs for looking at the inner working of ConfigMgr.
### TABLE 3.5 The v_GroupMap View (Partial Listing)

<table>
<thead>
<tr>
<th>ResourceType</th>
<th>GroupID</th>
<th>DisplayName</th>
<th>InvClassName</th>
<th>InvHistoryClassName</th>
<th>MIFClass</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1</td>
<td>System</td>
<td>v_GS_SYSTEM</td>
<td>v_HS_SYSTEM</td>
<td>SYSTEM</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>Workstation Status</td>
<td>v_GS_WORKSTATION_STATUS</td>
<td>v_HS_WORKSTATION_STATUS</td>
<td>MICROSOFT</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>CCM_RecentlyUsedApps</td>
<td>v_GS_CCM_RECENTLY_USED_APPS</td>
<td>v_HS_CCM_RECENTLY_USED_APPS</td>
<td>MICROSOFT</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>Add Remove Programs</td>
<td>v_GS_ADD_REMOVE_PROGRAMS</td>
<td>v_HS_ADD_REMOVE_PROGRAMS</td>
<td>MICROSOFT</td>
</tr>
<tr>
<td>5</td>
<td>14</td>
<td>Add Remove Programs (64)</td>
<td>v_GS_ADDREMOVE_PROGRAMS_64</td>
<td>v_HS_ADDREMOVE_PROGRAMS_64</td>
<td>MICROSOFT</td>
</tr>
<tr>
<td>5</td>
<td>21</td>
<td>CD-ROM</td>
<td>v_GS_CDROM</td>
<td>v_HS_CDROM</td>
<td>MICROSOFT</td>
</tr>
<tr>
<td>5</td>
<td>22</td>
<td>Computer System</td>
<td>v_GS_COMPUTER_SYSTEM</td>
<td>v_HS_COMPUTER_SYSTEM</td>
<td>MICROSOFT</td>
</tr>
<tr>
<td>5</td>
<td>23</td>
<td>Disk</td>
<td>v_GS_DISK</td>
<td>v_HS_DISK</td>
<td>MICROSOFT</td>
</tr>
<tr>
<td>5</td>
<td>24</td>
<td>Partition</td>
<td>v_GS_PARTITION</td>
<td>v_HS_PARTITION</td>
<td>MICROSOFT</td>
</tr>
<tr>
<td>5</td>
<td>25</td>
<td>Logical Disk</td>
<td>v_GS_LOGICAL_DISK</td>
<td>v_HS_LOGICAL_DISK</td>
<td>MICROSOFT</td>
</tr>
</tbody>
</table>
The ConfigMgr logs are text files, and you can view them in Windows Notepad or your favorite text editor. Most administrators prefer to use the ConfigMgr Trace Log Tool (CMTrace) rather than a text editor to display log files. The log viewer formats log entries, provides search and highlighting features, and provides error lookup. You can optionally turn on an auto-refresh feature to update the displayed log in near real time.

**NOTE: CONFIGURATION MANAGER TRACE LOG TOOL (CMTRACE)**

Microsoft’s Configuration Manager Trace Log Tool (CMTrace) for System Center Configuration Manager eases the ability to view log files. CMTrace.exe can be found in the tools directory on the root on the ConfigMgr 2012 installation media. Previous versions of this tool do not work with ConfigMgr 2012 logs.

Process Monitor is a tool you can use to capture detailed process activity on Windows systems. It provides extensive filtering options that allow you to drill down on activity related to specific folders, view only the operation of selected threads, and so forth. More information on Process Monitor and a link to download this useful tool are available at http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx.

The SQL Server Profiler allows you to capture detailed activity on your SQL Server. The profiler provides extensive filtering options that allow you to record the specific SQL activity in which you are interested. You can use this tool though the SQL Server Profiler user interface or use the ConfigMgr stored procedures spDiagStartTrace and spDiagStopTrace to capture activity ConfigMgr SQL activity. SQL Server Profiler ships with Microsoft SQL Server; the SQL Online Books describe its use in detail.

The “Components and Communications” section presented an example of how ConfigMgr components work together to process a site change. This section takes a closer look at WMI and SQL activity associated with the same site change as captured in logs and other tools. In this example, an administrator uses the ConfigMgr console to modify a site component. This results in the following sequence of events:

1. The console application invokes the SMS Provider WMI object for the modified site control item. The SMS Provider log file (smsprov.log) shows this activity.

2. The provider implements code that applies the update to the database. You can use either the SQL Server Profiler tool or the ConfigMgr SQL logging option to capture the SQL statements the provider uses.

3. The database contains special stored procedures, known as triggers, which automatically carry out additional processing when the update occurs. The triggers write records for auditing purposes and to provide notification to the Database Notification Monitor (SMSDBMON) component. You can use SQL Management Studio to locate and understand the triggers.

4. SMSDBMON processes the data and notified additional components of the change. The Database Notification Monitor log (smsdbmon.log) shows SMSDBMON polling the database for changes. The Process Monitor tool shows file system activity by the Database Notification Monitor thread as it writes to other components’ inboxes.
5. Additional threads carry out work to complete the site change. These threads record their activity in status messaged and logs.

Here is a detailed look at the activity just described.

Figure 3.38 shows a portion of the smsprov.log file as displayed in the log viewer.

![Image of log viewer displaying smsprov.log file]

The smsprov.log file shows calls to the SMS Provider from management applications. The bottom pane of the log viewer displays the details of the highlighted log entry. The entry in Figure 3.35 shows that the user ODYSSEY\bholt modified an instance of class SMS_SCI_SiteDefinition. The SMS_SCI_SiteDefinition, displayed in Figure 3.39, provides an interface to binary data stored in the SiteControl table.

Using the SQL Server Profiler lets you see SQL requests sent to the SQL Server database. (For information about the SQL Server Profiler, see [http://msdn.microsoft.com/en-us/library/ms187929.aspx](http://msdn.microsoft.com/en-us/library/ms187929.aspx).)

**TIP: USING SQL LOGGING TO CAPTURE SQL ACTIVITY**

An alternative to using the SQL Server Profiler to capture SQL activity is to enable SQL logging, as described in Appendix A. This adds details of SQL commands directly into the logs for components that access the database. Turning SQL logging on or off requires you to restart the Executive service.
The following SQL commands show the application SMS Provider inserting data into the `vSMS_SC_SiteDefinition_Properties` view:

```
IF NOT EXISTS (select 1 from vSMS_SC_SiteDefinition_Properties where ID = 0 and Name = N'Comments')
insert into vSMS_SC_SiteDefinition_Properties (ID, Name, Value1, Value2, Value3)
values (0, N'Comments', N'Central Administration Site (CAS)', N'', 0)
ELSE update vSMS_SC_SiteDefinition_Properties set ID = 0, Name = N'Comments',
    Value1 = N'Central Administration Site (CAS)', Value2 = N'', Value3 = 0
    where ID = 0 and Name = N'Comments'
```

You can use SQL Server Management Studio to view the underlying tables for a view. Figure 3.40 shows that `vSMS_SC_SiteDefinition_Properties` is based on the `SC_SiteDefinition_Property` table.

Figure 3.41 shows the `SC_SiteDefinition_Property` table in the Object Explorer tree on the left with the text of the SMSDBAudit trigger in the right text pane. A trigger is a special type of SQL stored procedure that runs automatically when changes are made to table data. The SMSDB Audit trigger (SMSDBAuditTrigger_SC_SiteDefinition_Property_INS_UPD_DEL) inserts a row into the SCCM_Audit table when the data in the `SC_SiteDefinition_Property` table changes.
FIGURE 3.40 The Site Definition Properties View depends on the SC_SiteDefinition_Property table.

FIGURE 3.41 The SC_SiteDefinition_Property Table displaying a trigger definition.
The following query displays entries in the SCCM_Audit table associated with changes made by the SMS Provider:

```sql
SELECT [ID], [TransactionID], [TableName], [By_Machine], [By_User]
    , [By_Component], [ChangeXML], [ChangeTime]
FROM [CM_CAS].[dbo].[SCCM_Audit]
WHERE By_Component = 'SMS Provider' and TableName = 'SC_SiteDefinition_PropertyList'
```

The ChangeXML column from the site description change is as follows:

```
<Changes><Change OP="U"><NewValue><row ID="68" SiteNumber="0" Name="Comments"
Value1="Central (CAS) site" Value2="" Value3="0" /></NewValue>
<OLDValue><row ID="68" SiteNumber="0" Name="Comments" Value1="CAS site"
Value2="" Value3="0" /></OLDValue></Change></Changes>
```

Another trigger, SMSDBMON_SC_SiteDefinition_Property_SQLServerSSBPORT_UPD_HMAN_upd, inserts data into the TableChangeNotifications table as follows:

```sql
BEGIN
    INSERT INTO TableChangeNotifications(Component,TableName,ActionType,Key1,Key2,
    Key3) SELECT all 
        N'SQLServerSSBPORT_UPD_HMAN',N'SC_SiteDefinition_Property',2,IsNULL(convert(nvarchar(256),SiteNumber),N''),N'',N'' FROM inserted WHERE Name = 'SSBPort' AND 
        UPDATE(Value3) AND (dbo.fnIsParentOrChildSite(SiteNumber) != 0 OR SiteNumber = 
        dbo.fnGetSiteNumber())
    IF @@ERROR != 0 ROLLBACK TRAN
END
```

The SMSDBMON prefix indicates that this trigger is owned by the ConfigMgr Database Notification Monitor component. Many of the database tables have triggers that write to the TableChangeNotifications table when changes occur. The Database Notification Monitor log (smsdbmon.log) shows the activity of the maintenance thread, which maintains these triggers. The same thread also maintains the various site maintenance tasks in the database.

The Database Notification Monitor polling thread regularly executes the spGetChangeNotifications stored procedure shown in this SQL Server Profiler trace:

```
[SMS_DATABASE_NOTIFICATION_MONITOR] exec spGetChangeNotifications
```

The spGetChangeNotifications stored procedure reads the TableChangeNotifications table in batches of up to 1000 transactions. The Database Notification Monitor then processes any new entries it finds. The smsdbmon file shows the following activity from the polling thread:

```
RCV: UPDATE on SiteControl for SiteControl_AddUpd_HMAN [CAS ] [9811]
RCV: UPDATE on SiteControl for SiteControl_AddUpd_SiteCtrl [CAS ] [9812]
```
Notice the Database Notification Monitor receives notifications that site control data has been updated and drops files in the Hierarchy Manager and Site Control Manager inboxes. These are zero byte files; however, Windows generates a directory change notification when the file is created. ConfigMgr components subscribe to change notifications for their inboxes. The SQL command in the final log entry deletes the change notification entries after processing the changes. This is why you cannot directly view the output of the associated trigger in the TableChangeNotifications table as was possible with the SCCM_Audit table.

To see even more detail of the process activity that carries out the site modification, use Process Monitor to capture the file system activity of the SMSExec process during the site change. Here is a partial listing for some Process Monitor event details during the site change, with comments added:

***SMSDBMON file drops files in HMAN and SITECTRL inboxes***
Event Class:      File System
Operation:        CreateFile
Result:  SUCCESS
Path:    F:\Program Files\Microsoft Configuration Manager\inboxes\hman.box\CAS.SCU

*** SMSEXEC thread 5248 detects a Directory Change Notification***
*** Thread ID 5248 matches a thread ID in the Hierarchy Manager log***
Name:    smsexec.exe
Event Class:      File System
Operation:        NotifyChangeDirectory
Result:  SUCCESS
Path:    F:\Program Files\Microsoft Configuration Manager\inboxes\hman.box
TID:     5248
Duration:         27.4709051
Filter:  FILE_NOTIFY_CHANGE_FILE_NAME, FILE_NOTIFY_CHANGE_DIR_NAME

Several threads detect the file system changes. The Hierarchy Manager does much of the processing and will serve as an example of ConfigMgr process activity. The Hierarchy Manager Log (Hman.log) now shows:

Processing site control file: Site CAS
The actual processing is performed by executing SQL statements against the database. With SQL Tracing enabled, the log then shows a large number of SQL SELECT statements retrieving data from tables and views such as SC_SiteDefinition, vSMS_SC_SiteDefinition_Properties and vSMS_SC_Component_Properties. After retrieving data about the site, Hierarchy Manager logs the following entry:

Update the Sites table: Site=CAS Parent=

This is followed by a number of SQL statements, including updates to the SysReslist table and calls to the spUpdateSites stored procedure, which updates the Sites table. Hierarchy Manager then updates the SiteControlNotification table to create a site control notification for the site. Finally, the thread raises the following status message:

Hierarchy Manager successfully processed "F:\Program Files\Microsoft Configuration Manager\inboxes\hman.box\CAS.SC", which represented the site control file for site "Odyssey Central Site" (CAS).

Process Monitor can display registry access as well as file access. You could use Process Monitor to see the details of Hierarchy Manager retrieving the registry values it uses to construct a connection string to the site database and accessing the SQL client libraries to initiate the database connection.

**SQL Replication Crash Course**

A major change in System Center 2012 ConfigMgr is the use of SQL Server replication for intersite communications. SQL Server replication largely replaces the inbox structure and file transfer methods of data exchange used in ConfigMgr 2007 and SMS. ConfigMgr sites are now able to process data and replicate it to other sites rather than requiring multiple sites to process the same data files. When you add a site to an existing hierarchy, ConfigMgr automatically configures SQL replication during site installation.

ConfigMgr uses two types of database replication:

- Snapshot replication is used for initial replication when a new site is created in a hierarchy.
- The ConfigMgr Database Replication Service uses the SQL Server Service Broker for ongoing data replication.

SQL Server also supports other types of replication that are not used by ConfigMgr and are not discussed in this chapter.

When you add a new site to the hierarchy, the initial snapshot replication uses the SQL Server bulk copy program (BCP) to export site data to a file. ConfigMgr then uses file-based replication to replicate the database extract to the parent site and loads it into the database through the BCP process.

The SQL Server Service Broker provides messaging services for SQL Server applications. Some advantages of the Service Broker include...
Asynchronous messaging: When an application submits a message to a Service Broker queue, the application can continue to process other work and leave the message delivery details to the Service Broker.

Transactional processing: Applications can send a set of related messages as a transaction. The transaction will not be committed until all messages are successfully processed, and can be rolled back if one of the messages fails.

Message sequencing: The Service Broker handles the details of providing messages to the receiver in the correct order.

Database engine integration: The Service Broker is part of the database engine, which improved performance and leverage the existing connection and security context.

Here are some of the key objects that Service Broker uses for message delivery:

- **Messages**: These are units of data. Each message has a specific message type. For example one of the message types defined by ConfigMgr is a notification that an Alert variable has changed.

- **Queues**: Queues receive messages and hold them for delivery.

- **Conversations**: These are asynchronous, reliable, long-running exchanges of messages. Each conversation has a priority so that messages in higher priority conversations will be processed before lower priority conversations.

- **Services**: Services are the endpoints for conversations. A service implements the set of tasks required to produce or consume messages.

ConfigMgr uses SQL Server change tracking to detect changes to the database tables that are in scope for replication. SQL Server change tracking is a new feature introduced with SQL Server 2008. Applications can enable database tables for change tracking. After a table is enabled for change tracking, the database engine maintains information about changes to the table. Applications can access the information to determine what rows in the table have changed and can then query the table to retrieve the modified data. Executing the following query against the ConfigMgr database displays a list of tables that are enabled for change tracking:

```sql
select name from sys.tables where object_id in (select object_id from sys.change_tracking_tables) order by name
```

These tables contain data that will be replicated to other sites if changes occur. The list will generally contain several hundred tables and will vary depending on the whether the site’s role in the hierarchy and the number of locally updated objects. Some ConfigMgr data is local to the site and not replicated. Tables containing local data are not enabled for change tracking. Chapter 5 discusses ConfigMgr replication scopes and planning considerations related to replication.
Configuration Manager Database Replication

Several ConfigMgr components work together to replicate data between sites. The code that carries out replication resides in several places:

- The Executive service
- Stored procedures defined in the site database
- Managed code in .NET assemblies

ConfigMgr creates several Service Broker objects for its own use. Figure 3.42 displays the ConfigMgr Service Broker Queues and Services nodes in the tree pane along with the corresponding sections of the default Service Broker report.

The SQL statements used to create these objects reveal how they work together. Here is the procedure to display the SQL language used to create an object:

1. Right-click on the object in the Object Explorer tree.
2. Select **Script [objecttype] as -> CREATE to “-> New Query Editor Window”** where objecttype may be “Service,” “Queue,” and so on.

The queue used by the data replication service (DRS) to replicate global data is the ConfigMgrDRSQueue queue. The ConfigMgr DRS is implemented as managed code and runs within the Common Language Runtime (CLR) component of the .NET Framework integrated into SQL Server. CLR integration allows procedural language code to run in close proximity to the database engine, which provides performance advantages and other optimizations. Figure 3.43 shows the ConfigMgr managed code assemblies, together with the functions and procedures that depend on the MessageHanderService assembly.
The code for the MessageHanderService, contained in `<ConfigMgrInstallPath>\bin\x64\messagehandlerervice.dll`, implements much of the DRS functionality. For more information on SQL Server CLR integration, see http://msdn.microsoft.com/en-us/library/ms131089.aspx.

![Managed code assemblies in the CAS site database and message handler service dependent objects.](image)

**NOTE: ENABLING CLR INTEGRATION**

CLR integration is disabled by default in SQL Server. ConfigMgr Setup will enable CLR integration. You should consider the impact on other databases if ConfigMgr will be sharing a SQL Server instance.

Here is the object definition for the ConfigMgrDRSQueue:

```
CREATE QUEUE [dbo].[ConfigMgrDRSQueue] WITH STATUS = ON ,
RETENTION = OFF ON [PRIMARY]
```

The ConfigMgrDRS_SiteCAS service uses the ConfigMgrDRSQueue and is defined as follows:

```
CREATE SERVICE [ConfigMgrDRS_SiteCAS] AUTHORIZATION [dbo] ON QUEUE
[dbo].[ConfigMgrDRSQueue] ([CriticalPriority],
[HighPriority],
[LowNormalPriority],
[LowPriority],
[NormalPriority])
```
CHAPTER 3   Looking Inside Configuration Manager

Related service broker objects define the various DRS message types, broker priorities, local routes and routes to other sites, and contracts. As an example, the route to site PR2 is defined as

CREATE ROUTE [ConfigMgrDRSRoute_SitePR2]  AUTHORIZATION [dbo]  WITH  SERVICE_NAME = N'ConfigMgrDRS_SitePR2' , ADDRESS = N'TCP://Ambassador.odyssey.com:4022'

A contract specifies the broker priorities for various message types. Figure 3.44 shows the CriticalPriority contract. All message types specified as critical priority will be delivered before messages of lower priorities in the same queue.

![The message broker critical priority contract.](image)

Table 3.6 shows the priority, service name, contract, message type, and message body for some typical messages from the ConfigMgrDRSQueue. For purposes of this discussion, the message body has been cast into a human readable form. The actual messages contain additional metadata including the conversation group ID and sequencing information.
### TABLE 3.6  Sample Message Data from ConfigMgrDRSQueue

<table>
<thead>
<tr>
<th>Priority</th>
<th>service_name</th>
<th>service_contract_name</th>
<th>message_type_name</th>
<th>casted_message_body</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>ConfigMgrDRS_SiteCAS</td>
<td>HighPriority</td>
<td>DRS_SyncStart</td>
<td>&lt;DRS_SyncStart SourceSite=&quot;PR2&quot; SyncId=&quot;21AC43A3-9A35-48D2-BE92-40FDE527335D&quot; ReplicationGroup=&quot;Alerts&quot; StartTime=&quot;2012-01-05T00:40:24.467&quot; BuildNumber=&quot;7678&quot;/&gt;</td>
</tr>
<tr>
<td>7</td>
<td>ConfigMgrDRS_SiteCAS</td>
<td>HighPriority</td>
<td>DRS_SyncData</td>
<td>&lt;DRS_SyncData BuildNumber=&quot;7678&quot; LastSyncVersionToSource=&quot;98540&quot; ThisVersion=&quot;230384&quot; SyncId=&quot;21AC43A3-9A35-48D2-BE92-40FDE527335D&quot; ReplicationGroupId=&quot;8&quot; MessageId=&quot;B214790C-717E-4BB7-83B6-2F851114C47C&quot;&gt;&lt;Operation Type=&quot;U&quot; TableName=&quot;AlertVariable_G1&quot; Context=&quot;&quot;&gt;&lt;row ID=&quot;23&quot; Value_Int=&quot;9&quot; LastChangeTime=&quot;2012-01-05T00:39:29.573&quot;/&gt;&lt;/Operation&gt;&lt;/DRS_SyncData&gt;</td>
</tr>
<tr>
<td>7</td>
<td>ConfigMgrDRS_SiteCAS</td>
<td>HighPriority</td>
<td>DRS_SyncEnd</td>
<td>&lt;DRS_SyncEnd SourceSite=&quot;PR2&quot; SyncId=&quot;21AC43A3-9A35-48D2-BE92-40FDE527335D&quot; ReplicationGroup=&quot;Alerts&quot; LastSyncVersionFromSource=&quot;230384&quot;/&gt;</td>
</tr>
<tr>
<td>Priority</td>
<td>service_name</td>
<td>service_contract_name</td>
<td>message_type_name</td>
<td>casted_message_body</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------</td>
<td>----------------------</td>
<td>------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>5</td>
<td>ConfigMgrDRS_SiteCAS</td>
<td>NormalPriority</td>
<td>DRS_SyncData</td>
<td>&lt;DRS_SyncData BuildNumber=&quot;7678&quot; LastSyncVersionToSource=&quot;98544&quot; ThisVersion=&quot;356796&quot; SyncId=&quot;DCBA3151-830F-4A86-93AE-2D197686487F&quot; ReplicationGroupId=&quot;3&quot; MessageId=&quot;9A6BC0AA-A996-4D67-A028-6B764492E2ED&quot;/&gt;</td>
</tr>
</tbody>
</table>
The ConfigMgr SMS_REPLICATION_CONFIGURATION_MONITOR (RCM) executive thread component identifies the data replication, connects to the database, and initiates DRS synchronization. Figure 3.45 shows a sample of RCM database activity. The SQL Server Profiler template used to capture these events, ReplicationActivity.tdf, is included as online material for this book, see Appendix D, “Available Online,” for information.

![FIGURE 3.45 SQL Server Profiler Trace Showing RCM Component Activity.](image)

Here are some SQL stored procedures that carry out much of the work for the RCM:

- **spDRSInitiateSynchronizations**: RCM drives the replication process by calling this procedure for each message priority. spDRSInitiateSynchronizations extracts changed data from the ReplicationData table, constructs the appropriate message type and calls the spGetSSBDialogHandle to retrieve a handle for a dialog on the message builder queue, ConfigMgrDRSMsgBuilder. The procedure then uses the dialog handle to insert the message into the ConfigMgrDRSMsgBuilder queue.

- **spGetSSBDialogHandle**: This procedure first attempts to retrieve a handle from the Service Broker dialog pool (dbo.SSB_DialogPool) that matches the contract and conversation required for the message. If there is not an existing handle the procedure verifies that a valid route exists, and then creates a new handle in the dialog pool and initializes a new dialog. ConfigMgrDRSMsgBuilder returns a dialog handle to the calling procedure.

- **spDRSMsgBuilderActivation**: This is the activation stored procedure for the ConfigMgrDRSMsgBuilder queue. This means that the procedure automatically fires when there are messages in the queue. The procedure performs various checks and then calls the procedure spDRSSendChangesForGroup. spDRSSendChangesForGroup updates replication metadata table and then calls additional procedures to obtain an handle on the site or global DRS message queue and insert the message into the queue.

You can view the full text of these procedures using the same method described in the beginning of this section to script the object broker object definition language to a query editor window.
TIP: VIEWING REPLICATION STATUS WITH SPDIAGDRS

The SQL stored procedure `spDiagDRS` provides detailed status of the replication queues, message activity and replicated data at your site. To execute this procedure, locate `dbo.spDiagDRS` under `Programmability -> Stored Procedures` in the site database, right-click and choose `Execute Stored Procedure`. You can optionally enter values for specific values for the table, column, and value you wish to examine. For example, you would enter `BoundaryGroup`, `Name`, and `Headquarters` to view the replication status or the boundary group named Headquarters. Leave these parameters blank to view general replication status.

File-Based Replication

ConfigMgr uses file-based replication for certain operations such as transferring package content to distribution points in child sites. Chapter 5, “Network Design,” describes the scenarios that use file replication and the relevant configuration options. The “Components and Communications” section presented an overview of how file-based replication works. This section uses the transfer of the file content to illustrate in more detail how file-based replication works. ConfigMgr components work together to prepare file content, schedule replication, and execute Windows file copy operations.

Again processing begins when the Database Notification Monitor detects a change in the site database. In this case, an administrator has initiated distribution of a package to a distribution point at a secondary site. The Database Notification Monitor log shows `DBMON` dropping a package notification file in the Distribution Manager inbox:

```
RCV: INSERT on PkgNotification for PkgNotify_Add [PR100003] 72057594037942821
SMS_DATABASE_NOTIFICATION_MONITOR 1/10/2012 12:57:45 PM 3652 (0x0E44)
SND: Dropped F:\Program Files\Microsoft Configuration Manager\inboxes\distmgr.box\PR100003.PKN 72057594037942820

SMS_DATABASE_NOTIFICATION_MONITOR 1/10/2012 12:57:45 PM 3652 (0x0E44)
```

Here are some status messages showing Distribution Manager processing the request to distribute a package to a child site:

```
Distribution Manager is beginning to process package "MOFComp" (package ID = PR100003).
Distribution Manager is preparing to send the compressed image of package "PR100003" to child site "SS1".
Distribution Manager instructed Scheduler and Sender to send package "PR100003" to child site "SS1".
```

The Distribution Manager log shows additional detail about the processing between the time that Distribution Manager began preparing to send the compressed image and the time it instructed the Scheduler and Sender to send the package.
Needs to send the compressed package for package PR100003 to site SS1 1/10/2012 12:57:57 PM 4892 (0x131C)

Sending a copy of package PR100003 to site SS1 1/10/2012 12:57:57 PM 4892 (0x131C)
The reporting site of site SS1 is this site. 1/10/2012 12:57:58 PM 4892 (0x131C)
Use drive F for storing the compressed package. 1/10/2012 12:57:58 PM 4892 (0x131C)
Incremented ref count on file F:\SMSPKG\PR100003.SS1.PCK, count = 1 1/10/2012 12:57:59 PM 4892 (0x131C)
Setting CMiniJob transfer root to F:\SMSPKG\PR100003.SS1.PCK 1/10/2012 12:57:59 PM 4892 (0x131C)
Incremented ref count on file F:\SMSPKG\PR100003.SS1.PCK, count = 2 1/10/2012 12:57:59 PM 4892 (0x131C)
Decremented ref count on file F:\SMSPKG\PR100003.SS1.PCK, count = 1 1/10/2012 12:57:59 PM 4892 (0x131C)
Created minijob to send compressed copy of package PR100003 to site SS1. Transfer root = F:\SMSPKG\PR100003.SS1.PCK. 1/10/2012 12:57:59 PM 4892 (0x131C)

This shows Distribution Manager creating the compressed package F:\SMSPKG\PR100003.SS1.PCK. Distribution Manager then notifies the Scheduler and Sender by dropping a JOB file in its inbox. The details of the notification process are not logged but can be seen through Process Monitor events such as the ones shown in Table 3.7.

TABLE 3.7 File Operations That Initiate Intersite Replication

<table>
<thead>
<tr>
<th>Operation</th>
<th>Details</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateFile</td>
<td>\ATHENA.ODYSSEY.COM\SMS_PR1\inboxes\schedule.box\0000005F.JOB</td>
<td>Distribution Manager</td>
</tr>
<tr>
<td>WriteFile</td>
<td>\ATHENA.ODYSSEY.COM\SMS_PR1\inboxes\schedule.box\0000005F.JOB</td>
<td>Distribution Manager</td>
</tr>
<tr>
<td>ReadFile</td>
<td>\ATHENA.ODYSSEY.COM\SMS_PR1\inboxes\schedule.box\0000005F.JOB</td>
<td>Scheduler</td>
</tr>
</tbody>
</table>

The component names shown in Table 3.7 are not displayed in the Process Monitor output but are determined by matching the thread IDs (TIDs) to the TIDs in the log files.

Here is an extract from the Scheduler log showing the Scheduler creating an instruction file for the Sender:

<Activating JOB 0000005F> [Software Distribution for MOFComp, Package ID = PR100003] 1/10/2012 12:58:12 PM 5844 (0x16D4)

  Destination site: SS1, Preferred Address: *, Priority: 2 1/10/2012 12:58:12 PM 5844 (0x16D4)
  Instruction type: MICROSOFT\SMS\MINIJOBINSTRUCTION\PACKAGE 1/10/2012 12:58:12 PM 5844 (0x16D4)
Creating instruction file:
\\ATHENA.ODYSSEY.COM\SMS_PR1\inboxes\schedule.box\tosend\0000005F.Iem 1/10/2012 12:58:12 PM 5844 (0x16D4)

Transfer root: F:\SMSPKG\PR100003.SS1.PCK 1/10/2012 12:58:12 PM 5844 (0x16D4)
Instruction (and package) file created. Mark job active. 1/10/2012 12:58:12 PM 5844 (0x16D4)

<JOB STATUS - ACTIVE> 1/10/2012 12:58:12 PM 5844 (0x16D4)
<Updating JOB 0000005F> [Software Distribution for MOFComp, Package ID = PR100003] 1/10/2012 12:58:12 PM 5844 (0x16D4)

Destination site: SS1, Preferred Address: *, Priority: 2 1/10/2012 12:58:12 PM 5844 (0x16D4)
Created new send request ID: 2002NPR1 1/10/2012 12:58:13 PM 5844 (0x16D4)

The following excerpts from the LAN Sender log show the major phases of the sending operation. First, the Sender connects to the Scheduler's outbox (\..\schedule.box\outboxes\LAN) to check for sender instructions. The Sender then finds the send request and establishes a connection to the destination site.

Connecting to F:\Program Files\Microsoft Configuration Manager\inboxes\schedule.box\outboxes\LAN.
COutbox::TakeNextToSend(pszSiteCode)
Retrieved the snapshot for priority 2, there are 1 files in the snapshot.
Found send request. ID: 2002NPR1, Dest Site: SS1
Created sending thread (Thread ID = 1AF4)
Trying the No. 1 address (out of 1)
Passed the xmit file test, use the existing connection

The next major phase of the sender operation is to locate the package and instruction files and verify that they are not already on the destination server:

Package file = F:\SMSPKG\PR100003.SS1.PCK
Instruction file = F:\Program Files\Microsoft Configuration Manager\inboxes\schedule.box\tosend\0000005F.Iem
Checking for remote file \CHARON.odyssey.com\SMS_SITE\2002NPR1.PCK

The final major phase of the sending process is to actually transmit the data, together with package instructions that will allow the Despooler component at the receiving site to unpack and correctly route the files:

Attempt to create/open the remote file \CHARON.odyssey.com\SMS_SITE\2002NPR1.PCK
Created/opened the remote file
Attempt to write 1024 bytes to \CHARON.odyssey.com\SMS_SITE\2002NPR1.PCK at position 0
Wrote 1024 bytes to \CHARON.odyssey.com\SMS_SITE\2002NPR1.PCK at position 0
Sending completed [F:\SMSPKG\PR100003.SS1.PCK]
Finished sending SWD package PR100003 version 1 to site SS1
TIP: USING NAL LOGGING TO CAPTURE NETWORK ACTIVITY

If you are interested in seeing even more detail of ConfigMgr network activity, you can enable Network Abstraction Layer logging. Appendix A describes NAL logging.

Other processes not detailed here due to space considerations include the receiving end of the site join, processing file signatures and hashes, and content status updates applied to the site database.

Summary

This chapter discussed the internal working of Configuration Manager. It looked at how ConfigMgr sites publish information in Active Directory and how ConfigMgr clients use directory information. The chapter then discussed how ConfigMgr clients and servers use WMI. It examined some of the internal storage of the ConfigMgr database, and how ConfigMgr processes and threads work together to implement key features. The chapter also examined how sites replicate data and content. Finally, the chapter presented examples of how you can use ConfigMgr status messages and logs along with some other tools to drill down into the inner workings of Configuration Manager.

The next chapter discusses how to leverage Configuration Manager features to design solutions and deliver value to your organization.
Symbols

7-Zip, 537, 571
64-bit site system requirements, 62
106-134 report server event errors, 946-958
802.1X authentication, 195
0x80004005 error code, 1061
[] (brackets), 851
% (percent sign), 851
/? property (CCMSetup), 435
“ ” (smart quotes), 610
_ (underscore), 851

A

About Configuration Manager command, 379
accepting risk, 1067-1123
access control entries (ACEs), 510
access control lists (ACLs), 99-100, 510
accessing SQL Server Management Studio, 134
access rules for mobile devices, 762-764
accountability, 1066-1123
accounts
  Active Directory Forest account, 1122
  Active Directory Group Discovery account, 1121
  Active Directory System Discovery account, 1121
  Active Directory User Discovery account, 1122
  AMT Provisioning and Discovery accounts, 1120
  AMT Remote Admin accounts, 1120
  Asset Intelligence Synchronization Point Proxy Server account, 1122
  Endpoint Protection SMTP Server Connection account, 1122
  Enrollment Point Connection account, 1118
  Exchange Server Connection account, 1122
  Exchange Server Connector Proxy Server account, 1122
  Health State Reference Publishing account, 1121
  Health State Reference Querying account, 1121
  machine accounts, assigning rights to, 1117
  Management Point database Connection Account, 1118
  MEBx accounts, 1120
  Multicast Connection account, 1118
  Remote Tools Permitted Viewer accounts, 1122
  Reporting Services Point account, 1118
  security accounts to support ConfigMgr infrastructure, 1117-1118
accounts for Active Directory discovery and publishing, 1121-1122
accounts for health state reference, 1121
accounts for OS deployment and software distribution, 1118-1119
accounts for Out of Band management, 1119-1120
accounts for software updates, 1121
database connection accounts, 1118
miscellaneous accounts, 1122
overview, 1116-1117
proxy server accounts, 1122
Software Update Point Connection account, 1121
Software Update Point Proxy Server account, 1121
Source Site account, 1122
Source Site Database account, 1118
Accounts subnode (console), 385
ACEs (access control entries), 510
ACLs (access control lists), 99-100, 510
actions
adding to reports, 902-903
Configuration Manager Service Manager console, 407-408
Active Directory, 81, 180
administrative access, securing, 1084-1085
ADUC (Active Directory Users and Computers) utility, 87-93
benefits of, 90-91
configuring sites to publish to, 89-90
discovery, 49-50
account security, 1121-1122
Active Directory Forest Discovery, 174, 297-298, 420-421
Active Directory Group Discovery, 174, 422-424
Active Directory System Discovery, 426-427
forests, publishing to, 420-421
integration into Systems Management Server (SMS) 2003, 39
planning
multi-forest and workgroup considerations, 182-183
schema extensions, 180-181
pre-installation requirements, 265
schema extensions, 180-181
created classes, 83-84
explained, 81
with ExtADSch.exe, 82-157
with LDIFDE (Lightweight Data Interchange Format Data Exchange) utility, 82-83
verifying, 85
viewing schema changes, 84-85
System Discovery, 173
System Management container
creating, 86-93
setting permissions on, 87-93
User Discovery, 174
Active Directory Forest account, 1122
Active Directory Forest subnode (console), 384
Active Directory Group Discovery account, 1121
Active Directory System Discovery account
Active Directory User Discovery account, 1122
Active Directory Users and Computers (ADUC) utility, 87-93
Active Management Technology (AMT), 1110-1115
Active Settings page (Add Site System Roles Wizard), 679
Active Source Hierarchy subnode (console), 385
Active state (alerts), 401
ActiveX filtering, 465
AD. See Active Directory
Adaptiva Software, 1235
Adcrl.log, 1189, 1203
Add Active Directory Location dialog, 423
Add Dependency dialog, 619
Add Driver to Boot Images page (Import New Driver Wizard), 974
Add Driver to Packages page (Import New Driver Wizard), 974
Add Groups dialog, 423
Add Hardware Inventory Class tool, 1217
Add Operating System Image Wizard, 976
Add Operating System Installer Wizard, 977
Add/Remove Programs class, 861
Address bar (console), 378
addresses, 49
Addresses subnode (console), 384
Address Resolution Protocol (ARP) cache, 485
Add Site System Roles Wizard, 301-304, 678-683, 793-796, 1026-1029
AddtoConfigurationMof.txt file, 1213-1214
AddtoSMSDefMof.mof file, importing, 1218
AddtoSmsDefMof.txt file, 1217
AForestDisc.log, 1192
admin console logs, enabling, 1182-1210
Administering System Center 2012 Configuration Manager (course), 1234
administration. See RBA (role-based administration)
Administration workspace, 383
administrative access, securing at Active Directory level, 1084-1085
auditing administrative actions, 1086-1089 at database level, 1085
Administrative Security folder, 1088
administrative security reports, 913-958, 1078-1079
Administrative Users subnode (console), 385
administrative users, managing, 1069-1070
AdminStudio, 1235
/ADMINUI switch (Prereqchk.exe), 269
ADRs (automatic deployment rules), 706-707
ADService.log, 1203
Adsgdis.log, 1192
ADSIEdit, 86-93
Adsysdis.log, 1192
ADUC (Active Directory Users and Computers) utility, 87-93
Adusrdis.log, 1192
Advanced Client (SMS 2003), 39-40
advanced queries, 851-852
date and time functions in, 853-854
time examples of, 854-857
querying for computers/disks with prompted value, 855-856
querying for devices not in specified collection, 856-857
querying for devices with hardware scan in last 15 days, 854-855
querying for devices without Microsoft Silverlight installed, 855
querying for newly discovered devices, 855
extended WQL limitations, 852-853
advanced reporting techniques, 903-904
Advanced settings (antimalware policy), 806
Afterbackup.bat, 1129
agent settings (NAP), 744

How can we make this index more useful? Email us at indexes@samspublishing.com
Agerlund, Kent, 1234
akbmgr.log, 1196
AI_Update_Service_Point, 1175
AIUpdateSvc.log, 1196
AIUSMSI.log, 1196
AIUSSetup.log, 1196
alerts
  compliance strategy, 527-528
  configuring, 402-404
  deleting, 403
  disabling, 402
  enabling, 402
for Endpoint Protection
  alerts for device collections, 812-813
  alert subscriptions, 813-814
  email notifications, 810-812
  overview, 809-810
explained, 53
locations, 403
managing, 402
overview, 401
postponing, 402
refreshing, 402
reports, 913
restart notifications, 721-722
for SQL replication, 1144
for software updates, 717-718
subscribing to, 404
viewing, 401
Alerts node (console), 386
Alerts page
  Automatic Deployment Rule Wizard, 803
  Deploy Software Updates Wizard, 701
  Deploy Software Wizard, 1012
All Audit Status Messages for a Specific User query, 870
All Software Update list, 692-696
All Software Updates subnode (console), 386
AMT (Active Management Technology), 1110-1115
Amtpmgr.log, 1203
AMT Provisioning and Discovery accounts, 1120
Amtproxymgr.log, 1204
AMT Remote Admin accounts, 1120
AMTSPSetup.log, 1203
AND operator, 850
Antimalware Activity Report, 821
antimalware policies, 788-792
  automatic removal of antimalware software, 829-830
  custom antimalware policies, 807
  default antimalware policy, 804
  importing, 808
  malware remediation status, 817
  merging, 809
  on-demand scanning, 819-820
Antimalware Policies subnode (console), 388
App Controller, 33
AppDeploy site, 1235
AppDiscovery.log, 1195
AppEnforce.log, 1195
ApplntentEval.log, 1195
Applicability page (Import New Driver Wizard), 974
Application Administrator, 1071
Application Author, 1071
Application Catalog, 46, 55, 64, 169, 465, 577-580, 662-665
application compatibility, 1051-1052
Application configuration items, 497
Application Deployment Evaluation Cycle, 602
Application Deployment Manager, 1071
Application Deployment Summarizer, 1173
application installation log files, 1207-1208
application management
   Application Catalog, 46, 55, 64, 169, 465, 577-580, 662-665
   application management logs, 1194-1195
dependencies, 56
deployment, 56
deployment types, 57
global conditions, 55
global expressions, 56
packages, 56
requirement rules, 55
Software Center, 57
Application Management node (console), 385
application model, 63
definition of, 59
deleting, 622
dependencies, adding, 617-618
deployment, 654-659
   end-user experience, 660-665
   explained, 567-569
global conditions, 569
Microsoft Application Virtualization, 568, 595-599
monitoring and troubleshooting, 665-666
Nokia SIS File, 568
requirements, 568-569
Script Installer, 568, 599-601
simulating, 667
Windows Installer, 568, 592-595
Windows Mobile Cabinet, 568
detection methods
   custom script detection methods, 607-610
   explained, 569, 602
   file-based detection methods, 604-606
   for Windows Installer applications, 602-603
   registry-based detection methods, 606-607
distributing. See software distribution
   explained, 566
exporting, 620-621
global conditions
   versus collections, 610
   custom global conditions, 612-616
device global conditions, 611-612
   explained, 610-611
   user global conditions, 612
How can we make this index more useful? Email us at indexes@samspublishing.com
importing, 620-621
Package Conversion Manager (PCM), 623-626
properties
  Application Catalog tab, 577-580
  Content Locations tab, 591
  Deployment Type - Content tab, 583-590
  Deployment Type - Dependencies tab, 590
  Deployment Type - Detection Method tab, 586
  Deployment Type - General tab, 582-590
  Deployment Type - Programs tab, 584-590
  Deployment Type - Requirements tab, 590
  Deployment Type - Return Codes tab, 590
  Deployment Types tab, 582-590
  Deployment Type - User Experience tab, 587-590
  Distribution Settings tab, 580-581
  General tab, 576-577
  References tab, 580
  Supersedence tab, 591
  retiring, 622
  revision history, 619-620
  superceding, 621-622
  user device affinity, 569-571
  Windows Installer-based applications, creating, 571-576
  wrappers, 601
Applications subnode (console), 385
Application Statistics Summarizer, 1173
application virtualization, 41
Application Virtualization deployment type.
  See Microsoft Application Virtualization deployment type
Apply Data Image task, 999
Apply Driver Package task, 1001
Apply Network Settings task, 1002
Apply Operating System Image task, 998-999
Apply Windows Settings task, 1003
AppProvider.log, 1195
Approval Requests subnode (console), 385
App-V deployment type. See Microsoft Application Virtualization deployment type
architecture design. See design
archive_reports.sms, 1159
ARP (Address Resolution Protocol) cache, 485
assessing environment, 163-165
asset data, timeliness of, 12
Asset Intelligence, 40
  Asset Intelligence node (console), 388
  Asset Intelligence Synchronization Point Proxy Server account, 1122
  logs, 1196
  reports, 913-919
  synchronization point, 47, 168
Asset Intelligence Synchronization Point Proxy Server account, 1122
Asset Manager, 1071
Assets and Compliance workspace, 380
  light management model (mobile devices), 764-765
  monitoring Endpoint Protection with, 819
  monitoring malware with, 819
  assigned site, identifying and contacting, 222
  assigning
    clients, 453-454
    rights to machine accounts, 1117
Assign option (SCUP), 736
associations
  computer associations, 1036-1038
definition of, 96
security scopes, associating with roles, 1077-1078
asynchronous messaging, 147
Athena MDM, 784, 1235
attacks, 1097
attack surface reduction, 1091
attribute reference criterion type, 847
attributes
  attribute classes, 840
  query attributes, 840-841
auditing
  administrative actions, 1086-1089
  audit messages, retention of, 1167-1169
  namespaces, 100-101
  remote control, 476
authentication, 802.1X, 195
authoring
  compliance authoring, 523-526
  CP Studio, 525
  Microsoft tools, 524
  organization, 523-524
  Security Compliance Manager (SCM), 525-526
  custom reports. See reports, custom reports
AutoAdminLogon class
  creating, 1214-1215
  enabling, 1219
  selecting, 1217
Auto Apply Drivers task, 1001
auto deployment rules for definition updates, 799-904
Automatically Remove Previously Installed Antimalware Software Before Endpoint Protection Is Installed setting, 828
automatic deployment rules (ADRs), 706-707
Automatic Deployment Rules subnode (console), 386
Automatic Deployment Rule Wizard, 800-804
automation
  automatic deployment rules (ADRs), 706-707
  client upgrades, 450-451
  image creation, 1040-1042
  IT automation challenges, 10
  lack of, 12
  overview, 33-34
  publications, 737
  removal of antimalware software, 829-830
  sidewide client push, 444-447
availability, 1066-1123
avoiding risk, 1067-1123
awebsctl.log, 1194
awebsvcMSI.log, 1195
B
Background Intelligent Transfer Service. See BITS (Background Intelligent Transfer Service)
backstage (console), 378-379
backup log files, 1191
backups. See also Backup Site Server maintenance task
  backup log files, 1191
  customizing, 1129
  migrating to new environment, 1139-1140
  new features, 66
How can we make this index more useful? Email us at indexes@samspublishing.com
backups

operating system backups, 1129
restoring, 1129-1136
SSRS (SQL Server Reporting Services), 882-884
troubleshooting, 1128
Backup Site Server maintenance task, 1125-1129, 1145-1148
bandwidth, 210
  bandwidth control in distribution points, 74
  bandwidth throttling, 227
baselines
  configuration baselines
    creating, 513
    definition of, 495
    deploying, 515-516
    evaluation conditions, 513
    exporting, 522
    filtering, 513
    locked configuration baselines, 521
    monitoring, 516-517
Beaumont, Steve, 1236
best practices
  custom reports, 912
  reporting, 884-885
  SSRS (SQL Server Reporting Services)
    optimization, 951
Bink, Steven, 1235
BitFlag column (RBAC_ObjectOperations), 1081
BitLocker
  disabling, 995
  enabling, 994
BitNumber column (RBAC_ObjectOperations), 1081
BITS (Background Intelligent Transfer Service)
  ConfigMgr client settings, 232-233
device settings, 461-462
explained, 59-60, 229-230
group policy, 231-233
multiple interfaces and file integrity checking, 233
new features, 64
versions, 230-231
/BitSPriority: property (CCMSetup), 436
blocked or unresponsive ports,
  troubleshooting, 249-250
blocking
  client, 450
  synchronization of mobile devices, 765
blogs, 452, 1235-1237
bootable media, 980
boot critical drivers, 1056
boot images, 1048-1049
  certificates for, 1106
  customizing, 983-984
  distribution points, 981
  drivers in, 981-982
  importing, 984
  overview, 977
  PXE booting, 977-979
  removable media, 979-981
Boot Images subnode (console), 386
boundaries
  boundary groups, 227-229
    configuration, 298-300
    planning, 170-172
  fast network and slow network boundaries,
    227-229
  migration planning, 337-338
  new features, 65-66
  planning, 170-172
  troubleshooting, 258
Boundsies subnode (console), 384
Boundary Group page (Create Secondary Site Wizard), 291
boundary groups, 227-229
configuration, 298-300
planning, 170-172
Boundary Groups page (Create Site System Server Wizard), 639
Boundary Groups subnode (console), 384
brackets ([ ]), 851
Brady, Niall, 1234, 1237
BranchCache, 61, 234-236, 647-648
Browse File System dialog, 604
Browser, 879
built-in reports
administrative security reports, 913
alert reports, 913
asset intelligence reports, 913-919
client push reports, 919
client status reports, 919-920
compliance and settings management reports, 920-921
device management reports, 921-923
driver management reports, 923
Endpoint Protection reports, 924
hardware reports, 924-926
migration reports, 927
NAP (network access protection) reports, 927
network reports, 928
operating system reports, 928
Out of Band management reports, 928
power management reports, 928-929
site - client information reports, 930-931
site - discovery and inventory information reports, 931
site - general reports, 932
site - server information reports, 932
software distribution reports, 933-936
software metering reports, 936-937
software reports, 932-933
software update reports, 937-940
state migration reports, 940
status message reports, 941-942
task sequence reports, 942-943
upgrade assessment - Windows 7 reports, 944
user reports, 944
virtual applications reports, 944-945
Wake on LAN reports, 945
built-in roles, 1071-1073
Buntinx, Kenny, 1232
business requirements
enabling with infrastructure optimization, 27
establishing, 162-163
bypassing maintenance windows, 709
C
CAB files, 522
CacheConfig class, 116
caching, report caching, 950
Canceled state (alerts), 401
capacity planning, 188-189
capture media, 980
Capture Media Wizard, 1043
Capture Network Settings task, 1002
Capture Operating System Image account, 1119
Capture Operating System Image task, 1000
Capture User State task, 996-997
Capture Windows Settings task, 1002
CAS (Central Administration Site), 45
    installing, 271-278
    planning, 168
/CAS switch (Prereqchk.exe), 268
CAs (certificate authorities), 184
CAS.log, 1184
catalogs
    Application Catalog, 46, 55, 64, 169, 465, 577-580, 662-665
    in SCUP (System Center Update Publisher), 733-734
    update catalog, 682
Catalog subnode (console), 388
Ccm32BitLauncher.log, 1184
CCMADMINS property (Client.msi), 439
CCMALLOWSILENTREBOOT property (Client.msi), 441
CCMALWAYSINF property (Client.msi), 439
Ccmonca.log, 1200
CCMCERTISSUERS property (Client.msi), 439
CCMCERTSEL property (Client.msi), 440
CCMCERTSTORE property (Client.msi), 440
CCMDEBUGLOGGING property (Client.msi), 440
CCMENABLELOGGING property (Client.msi), 440
CCMEVALHOUR property (Client.msi), 439
CCMEVALEXECLOG property (Client.msi), 439
CCMEXECLOG property (Client.msi), 439
CcmEval.log, 1184
CcmEvalTask.log, 1185
ccmeval.xml, 455
CcmExec.log, 1185
CCMFIRSTCERT property (Client.msi), 440
CCMHOSTNAME property (Client.msi), 440
CCMHTTPSPORT property (Client.msi), 440
CCMINSTALLDIR property (Client.msi), 439
CCM_InstalledComponent class, 116
Cmlsapi.log, 1193
Ccm.log, 253-254, 1189
CCMLOGLEVEL property (Client.msi), 441
CCMLOGMAXHISTORY property (Client.msi), 441
CCMLOGMAXSIZE property (Client.msi), 441
CCM namespace, 111
CcmPerf.log, 1185, 1199
CcmRepair.log, 1183
CcmRestart.log, 1185
CCMSDKProvider.log, 1185, 1195
CCMSetup.exe, 435-437, 1175
CCMSetup.log, 254, 1183, 1201
CCM_SoftwareDistributionClientConfig class, 119-120
CCR files, creating manually, 444
CD-ROM reports, 924
Central Administration Sites. See CAS
centrally managed client settings, 66
certificate authorities (CAs), 184
Certificate Authority console, 1099-1100
Certificate Enrollment Wizard, 1102
CertificateMaintenance.log, 1185
certificate revocation list (CRL), 185
certificates, 1099
    for AMT (Active Management Technology), 1110-1115
    for boot images, 1106
certificate services, 183-186
    managing, 732
    mobile device enrollment certificate template, 1108-1109
PKI web server certificates for IIS site systems, 1099-1104
public certificate authorities, 731
certificate services, 183-186
Certificates Export Wizard, 1108
Certificates subnode (console), 385
Certificate Templates console, 1099
CertMgr.log, 1189
change control and portability (task sequences), 1017-1019
Change.log, 1194
changing
ports, 215
site properties, 131-132
charts
Client Activity pie chart, 457
Client Check pie chart, 458
creating, 897-902
Chart Wizard, 897-902
chassis types, 847
Check Application Title with Inventory Information maintenance task, 1147-1148
checking CRL (certificate revocation list), 185
child configuration items, 512
child primary sites
configuring for data gathering, 345-347
installing, 286-287
SUP (software update point) placement, 677
chmgr.log, 1189
choosing site codes, 168
Ciagent.log., 529 1196, 1200, 1206
Cidm.log, 1189
CIDownloader.log, 1185
CIM (Component Information Model), 1233
CIMOM (Common Information Model Object Manager), 93
CIM_StatisticalInformation class, 111
CIM Studio, 103-104
CIMV2 namespace
connecting to, 103-104
Win32_LogicalFileSecuritySetting class., 111
Win32_LogicalShareSecuritySetting class
associations, 108-111
properties, 104-106
sample help entry, 106-107
Win32_Perf class, 111
CItaskManager.log, 529
CTaskMgr.log, 1185, 1196
classes
Add/Remove Programs, 861
AutoAdminLogon
creating, 1214-1215
enabling, 1219
selecting, 1217
CacheConfig, 116
CCM_InstalledComponent, 116
CCM_SoftwareDistributionClientConfig, 119-120
CIM_StatisticalInformation, 111
common classes, 96
Computer System, 861
core classes, 95
Disk Drives, 862
extended classes, 96
InventoryDataItem, 113
Logical Disk, 862
Memory, 862
Network Adapter Configuration, 862
Operating System, 862
Power Configuration, 862
Processor, 862
Recently Used-Applications, 862
Server Feature, 862
Services, 862
Shares, 862
SMS_Client, 116
SMS_Collection, 121-122
Software Files, 862
Software Products, 862
System, 96
System Enclosure, 862
System Resource, 861
User Group Resource, 861
User Resource, 861
Virtual Machine, 862
Win32_LogicalFileSecuritySetting, 111
Win32_LogicalShareAccess, 109
Win32_LogicalShareAuditing, 109
Win32_LogicalShareSecuritySetting
  class associations, 108-111
  methods, 106-107
  properties, 104-106
Win32_Perf, 111
Win32Reg_AddRemovePrograms, 115
Workstation Status, 862
Classifications page (Add Site System Roles Wizard), 681
Clean Up Migration Data function, 367-369
Clear Install Flag maintenance task, 1148
Clear Install Flag site maintenance task, 428
Clendenen, Anthony, 1236
Client Activity pie chart, 457
Client Activity subnode (console), 387
Client Approval, 449-450
ClientAuth.log, 1185
client certificates, deploying, 1104-1106
Client Check pie chart, 458
Client Configuration Manager, 253
Client Configuration Requests (CCRs)
  Processed Unsuccessfully query, 870
Client Health subnode (console), 387
ClientIDManagerStartup.log, 1185
ClientLocation.log, 1185
client logs
  application management client log files, 1195
  asset intelligence client log files, 1196
  client installation logs, 1183-1184
  client operations logs, 1184-1187
  compliance management client log files,
  1196-1197
  endpoint protection log files, 1197
  metering client log files, 1198
  mobile device management client logs, 1187
  power management log files, 1204-1205
  remote control log files, 1205
  software updates client computer log files,
  1206-1207
  Windows Update Agent logs, 1187-1188
Client Management Licenses, 166-167
Client Management Suite, 166
Client.msi.log, 437-441, 1183, 1201
client operations logs, 1184-1187
client policy device settings, 463
Client Policy settings, 175
client push, 172
  automatic sideway client push, 444-447
  enabling, 442-444
overview, 442
reports, 919
Client Push Installation Properties dialog, 444
clients
architecture, 174-177
assignment, 222, 453-454
BITS (Background Intelligent Transfer Service) settings, 232-233
blocking/unblocking, 450
centrally managed client settings, 66
client health status enhancements, 68
client logs
application management client log files, 1195
asset intelligence client log files, 1196
client installation logs, 1183-1184
client operations logs, 1184-1187
compliance management client log files, 1196-1197
endpoint protection log files, 1197
metering client log files, 1198
mobile device management client logs, 1187
power management log files, 1204-1205
remote control log files, 1205
software updates client computer log files, 1206-1207
Windows Update Agent logs, 1187-1188
client management, 297
Client Management Suite, 166
client operating systems, discovering, 245-246
client push, 172
  automatic sidewise client push, 444-447
  enabling, 442-444
overview, 442
reports, 919
Client Status Reporting (CSR), 454-458
client-to-management point connectivity, testing, 250
client-to-server communications
  client ports and protocols, 215-220
  client protocols, 222-224
  identifying and contacting client’s assigned site, 222
  initial communication, 221
  NAP (Network Access Protection), 224
security, 1098
custom client settings for Endpoint Protection, 788, 814-815
definition of, 419
discovery, 172-174, 245
  Active Directory Forest Discovery, 420-421
  Active Directory Group Discovery, 422-424
  Active Directory System Discovery, 426-427
  Delta discovery, 422
  Heartbeat Discovery, 427-428
  Network Discovery, 429-431
purpose of, 419
Endpoint Protection Client
  automatic removal of antimalware software, 829-830
  client/server communication, 829
  explained, 824-827
  removing, 830
  settings, 827-829

How can we make this index more useful? Email us at indexes@samspublishing.com
explained, 50-51
hardware dependencies, 432-433
installing, 172-174
  automatic upgrades, 450-451
  Client Approval, 449-450
  client push, 442-447
  with logon scripts, 441-442
  manual installation, 435-441
  software update point (SUP), 448
  troubleshooting installation, 252-254,
  451-453
Internet-based clients, supporting
  dedicated sites, 238-239
  explained, 237-238
  planning, 193-194
  sites spanning internet network and
  perimeter network, 240
  site-to-site communications across inner
  firewall, 239-240
  Web proxies and proxy enrollment
  points, 240-241
manually importing into ConfigMgr, 431
migration, 322, 370-371
offline clients, 252
ports, 215-220
protocols, 222-224
remote control. See remote control
reports
  client push reports, 919
  client status reports, 919-920
  site - client information reports, 930-931
Resource Explorer, 483-484
roaming clients, 692
settings
  Background Intelligent Transfer Service
  (BITS) device settings, 461-462
client policy device settings, 463
compliance settings device
  settings, 463
Computer Agent device settings,
  464-466
computer restart device settings, 466
Endpoint Protection device settings, 466
hardware inventory device settings,
  467-470
in-depth management model, 775-778
Network Access Protection (NAP) device
  settings, 470-471
overview, 176, 459-461
Power Management settings, 471
priority, 461
Remote Control device settings,
  471-476
software deployment device
  settings, 476
software inventory device settings,
  477-478
software metering device settings,
  479-480
Software Updates device settings, 481,
  687-689
state messaging device settings, 482
User and Device Affinity settings,
  482-483
software dependencies, 433
Software Update-Based Client
  Installation, 448
supported platforms, 433-435
upgrading, 450-451
WMI client operations, 116-120
WOL (Wake On LAN)
  configuring, 486-487
  explained, 484
  implementing, 487-488
prerequisites, 484-485
subnet-directed WOL, 485-486
unicast WOL, 485
Client Settings node (console), 384
Client Status node (console), 387
Client Status Reporting (CSR), 41, 454-458
collection migration jobs
    collection migration with associated objects, 352-357
    collection only migration, 349-352
    explained, 349
configuring alerts for, 812-813
configuring to appear in Collection view, 816
creating, 628-630, 866, 1223-1224
device collections, 1223-1224
direct rules, 630-631
exclude rule, 634
explained, 52, 535, 714-715
folders, 67
versus global conditions, 610
include/exclude rules, 67, 634
incremental updates, 634-635
limiting collection, 332-335
new features, 67
querying for devices not in specified collection, 856-857
query rules, 631-633
reports, 934
NAP (Network Access Protection), 224
security, 1098
cloud computing
    cloud-based configuration monitoring, 34
    proliferation of, 12-13
CLR integration, enabling, 149
CMHttpsReadiness.log, 1185
CmRcService.log, 1205
CMTrace, 1059, 1180
CMTrace (ConfigMgr Trace Log Tool), 140
CMTrace.exe, 272
Cochrane, Mark, 1212
coexistence considerations (migration), 327
collection migration jobs
    collection migration with associated objects, 352-357
    collection only migration, 349-352
    explained, 349
collections
    associating with distribution point groups, 641
collection limiting, 67, 332-333
common classes (WMI), 96
Common Information Model Object Manager (CIMOM), 93

communications
  client-to-server communications
    client ports and protocols, 215-220
    client protocols, 222-224
    identifying and contacting client’s assigned site, 222
    initial communication, 221
    NAP (Network Access Protection), 224
    security, 1098
  network issues affecting site communications, 258-259
    security, 1098
  server. See server communications

site-to-site communications
  across inner firewall, 239-240
  database replication, 225-226
  data priorities, 227
  file-based replication, 226-227

comparison operators, 508

compatibility (application), 1051-1052

Complete Installation page (Create Secondary Site Wizard), 291

Completion page
  Create Application Wizard, 573-575
  Create Configuration Item Wizard, 502
  Deploy Software Updates Wizard, 702

compliance, 59, 1067
  client, 747
  compliance authoring, 523-526
    CP Studio, 525
    Microsoft tools, 524
    organization, 523-524
    Security Compliance Manager (SCM), 525-526
  compliance management log files, 1196-1197
  compliance scanning, 716-717

configuration baselines
  creating, 513
  definition of, 495
  deploying, 515-516
  evaluation conditions, 513
  exporting, 522
  filtering, 513
  locked configuration baselines, 521
  monitoring, 516-517

configuration items
  child configuration items, 512
  compliance rules, 507-510
  creating with Create Configuration Item Wizard, 497-503
  definition of, 495
  evaluation criteria, 496
  exporting, 522
  filtering, 496-497
  locked configuration items, 521
  mobile device settings, 511-512
  types of, 497
    Windows settings, 503-507
      configuring, 493-495
      CPs (configuration packs), 521-522
      device settings, 463
      evaluation, 517-519
      groups, 698
      in-depth management model (mobile devices), 782
      log files, 529
      new features, 68, 493
      overview, 491-493
      reports, 526-527, 920-921, 937-938
rules, 507-510
strategy
alerts, 527-528
on-demand results, 527
overview, 525-526
reporting, 526-527
status message IDs, 530
troubleshooting, 529-531
versioning, 519-521
Compliance Rules page (Create Configuration Item Wizard), 501
Compliance Settings Manager, 1071
Compliance Settings node (console), 388
Compon.log, 1189
CompName.vbs, 1241
Component Information Model (CIM), 1233
components. See also specific components explained, 124-125
inboxes, 124
interaction between, 131-133
table of, 125-129
component servers, 46
Component Status subnode (console), 387
Component Status Summarizer, 1173
Compsumm.log, 1189
Computer Agent settings, 175, 464-466
Computer Association Properties dialog box, 1036-1037
computer associations, 1036-1038
color settings, 175, 466
Computer System class, 861
ComRegSetup.log, 1189
Concero, App Controller, 33
conditions, applying to tasks, 1008-1010
confidence, 1066-1123
/configuration property (CCMSetup), 437
ConfigMgr 2007, migrating to System Center 2012. See migration
ConfigMgr Component Logging dialog box, 1182
ConfigMgr database. See databases
ConfigMgrDRSQueue, 151-152
ConfigMgrPrereq.log, 1188
ConfigMgrSetup.log, 1189-1191
ConfigMgrSoftwareCatalog.log, 1195
ConfigMgr Trace Log Tool (CMTrace), 140
ConfigMgr Wiki, 1212
configuration. See also migration
alerts, 402-404
alerts for device collections, 812-813
alert subscriptions, 813-814
email notifications, 810-812
overview, 809-810
Backup Site Server maintenance task, 1126-1129
baselines, 59
creating, 513
definition of, 495
deploying, 515-516
evaluation conditions, 513
exporting, 522
filtering, 513
monitoring, 516-517
client settings
Background Intelligent Transfer Service (BITS) device settings, 461-462
client policy device settings, 463
compliance settings device settings, 463
Computer Agent device settings, 464-466
discovery settings, 756-757
Exchange ActiveSync (EAS) Connector settings, 757-762
general settings, 754-755
installation programs, 551-559
PKI web server certificates for IIS site systems, 1099-1104
pre-installation requirements. See pre-installation requirements publishing to Active Directory forest, 420-421
RBAC (role-based access control)
data sources, 881
reporting services point, 880-881
remote assistance, 472-474
remote control, 472-474
SCUP (System Center Update Publisher), 729-733
"shift and drift," 11
sites
Active Directory Forest Discovery, 297-298
active source sites, 343-344
boundary groups, 298-300
child sites, 345-347
client management, 297
configuring sites to publish to Active Directory, 89-90
reporting functionality, 297
SSRS (SQL Server Reporting Services), 876-881
SUPs (software update points), 683-684
troubleshooting network configuration issues, 247
WOL (Wake On LAN), 486-487
Configuration Baselines subnode
(console), 388

computer restart device settings, 466
Endpoint Protection device settings, 466
hardware inventory device settings, 467-470
Network Access Protection (NAP) device settings, 470-471
overview, 459-461
Power Management settings, 471
priority, 461
Remote Control device settings, 471-476
software deployment device settings, 476
software inventory device settings, 477-478
software metering device settings, 479-480
Software Updates device settings, 481
state messaging device settings, 482
User and Device Affinity settings, 482-483
compliance settings, 493-495
configuration items, 59
child configuration items, 512
compliance rules, 507-510
creating with Create Configuration Item Wizard, 497-503
definition of, 495
evaluation criteria, 496
exporting, 522
filtering, 496-497
locked configuration items, 521
mobile device settings, 511-512
types of, 497
Windows settings, 503-507
Configuration Manager hierarchy, 324-325
Exchange Server Connector, 754-762
account settings, 755-756
configuration packs (CPs), 521-522
Conflicting Records subnode (console), 387
connectivity problems, troubleshooting, 247-248
Connect to a New Site command, 378
Connect to Network Folder task, 993
consistency (process), 13
console
 Address bar, 378
 Administration workspace, 383
alerts
 configuring, 402-404
 deleting, 402
 disabling, 402
 enabling, 402
 locations, 403
 managing, 402
 overview, 401
 postponing, 402
 refreshing, 402
 subscribing to, 404
 viewing, 401
Assets and Compliance workspace, 380
backstage, 378-379
Configuration Manager Console Setup Wizard, 391-394
Configuration Manager Service Manager console
 actions, 407-408
 launching, 406
 overview, 404-405
Configuration Manager Setup wizard
 restoring backups, 1130-1136
 site maintenance, 1136-1139
Configuration.mof file, extending hardware inventory
 cautions, 1211
 example, 1213-1224
 process overview, 1212-1213
 with community tools, 1212
Configuration Pack Catalog, 522

How can we make this index more useful? Email us at indexes@samspublishing.com
converting legacy packages with Package Conversion Manager, 623-626
copying user state, 1038-1039
Copy Packages Wizard, 637
Core CAL Suite, 166
core classes (WMI), 95
Count of Mobile Devices by Operating System report, 782
CPs (configuration packs), 521-522
CP Studio, 525, 1228
Create Application Wizard, 571-576
Create Automatic Deployment Rule Wizard, 706-707
Create Boundary Group Wizard, 298-300
Create Child Configuration Item Wizard, 512
Create Configuration Baseline dialog, 514
Create Configuration Item Wizard, 497-503
  Completion page, 502
  Compliance Rules page, 501
  Detection Methods page, 499
  General page, 497-498
  Mobile Device Settings page, 502
  Platform Applicability page, 502
  Progress page, 502
  Settings page, 501
  Summary page, 502
  Supported Platforms page, 502
Create Deployment Type Wizard
  creating Application Virtualization deployment type, 595-599
  creating Script Installer deployment type, 599-601
  creating Windows Installer deployment type, 592-595
Create Device Collection Wizard, 628-630, 1223-1224
Create Direct Membership Rule Wizard, 630-631
Create Global Condition dialog, 614-616
Create Migration Job Wizard, 347-348
Create Object dialog box, 87
Create Query Wizard, 834, 841-844
Create Report Wizard, 890-892
Create Requirement dialog, 594, 616
Create Secondary Site Wizard, 289-294
Create Site System Server Wizard, 637-640
Create Software Metering Rule Wizard, 480
Create Software Update Wizard, 738-741
Create Status Message Query Wizard, 868-870
Create Subscription Wizard, 887-889
Create Task Sequence Wizard, 1041-1042, 1047-1050
CreateTSMedia.log, 1201
creation phase (OSD), 970
Criterion Properties dialog, 632-633, 843-844
criterion types (queries), 846-848
CRL (certificate revocation list), 185
Crumbaker, Ron, 1236
cryptography, 183, 1096-1097. See also PKI (public key infrastructure)
CSR (Client Status Reporting), 41, 454-458
CSTR() function, 903
Customer Experience Improvement Program, 379
customizing
  antimalware policies, 807
  backups, 1129
  boot images, 983-984
  client settings for Endpoint Protection, 788-792, 814-815
  commands, 1020
  console, 400-401

How can we make this index more useful? Email us at indexes@samspublishing.com
global conditions, 612-616
migration reports, 369
packages, 562
reports
advanced reporting techniques, 903-904
best practices, 912
building, 893-902
development tool selection, 893
interactive features, 902-903
parameters, 902
Server Uptime Report example, 904-911
subreports, 903
roles, 1073-1074
schedules, 461
script detection methods, 607-610
with PowerShell, 608-609
with VBScript, 609-610
task sequences, 1019-1020
updates, 737-741
tables. See tables
views, 133-134
collection views, 134-135
site property views, 135
v_GroupAttributeMap view, 138
v_GroupMap view, 138
v_ReportViewSchema view, 138
v_ResourceAttributeMap view, 137
v_ResourceMap view, 136-137
V_SchemaViews view, 135-136
Database Notification Monitor, 144
Database Replication node (console), 387
data flow, 206-208
data gathering, 322, 345-347
DataHdr.log, 1192
data priorities, 227
Data Protection Manager (DPM), 32
data sources, 881, 894
Data Source Settings dialog, 895
data Source tab (packages), 543-544
DataTransferService.log, 1185
data warehouse, 957-958
DateAdd(), 853
date and time operators, 848
DateDiff(), 853, 905
date/time functions, 853-854, 905
dcdiag, 84
dcmagent.log, 529
Dcmagent.log, 1196
DCMReporting.log, 529, 1197
DcmWmiProvider.log, 529, 1197
DCOM (Distributed Component Object Model), 409, 413-414
Ddm.log, 1192
 Deleting Aged Data

- **Delete Aged Endpoint Protection Health Status History Data maintenance task**, 1149
- **Delete Aged Enrolled Devices maintenance task**, 1150
- **Delete Aged Inventory History maintenance task**, 1150
- **Delete Aged Log Data maintenance task**, 1146, 1150, 1155
- **Delete Aged Replication Tracking Data maintenance task**, 1147, 1150, 1155
- **Delete Aged Software Metering Data maintenance task**, 1151
- **Delete Aged Software Metering Summary Data maintenance task**, 1151
- **Delete Aged Status Messages maintenance task**, 1151, 1168
- **Delete Aged Threat Data maintenance task**, 1151
- **Delete Aged User Device Affinity Data maintenance task**, 1151
- **Deleted Aged Status Messages maintenance task**, 1146
- **Delete Inactive Client Discovery Data maintenance task**, 1152
- **Delete Obsolete Alerts maintenance task**, 1146, 1152
- **Delete Obsolete Client Discovery Data maintenance task**, 1147, 1152, 1164
- **Delete Obsolete Forest Discovery Sites and Subnets maintenance task**, 1147, 1153
- **Delete option**
  - Queries node, 834
  - SCUP, 736
- **Delete Secondary Site Wizard**, 312-314
- **Delete site maintenance tasks**, 1164
- **Delete Unused Application Revisions maintenance task**, 1153
- **delta discovery**, 41, 422

**DDR files**
- obsolete records, 1162-1164
- retention, 1155-1162
- saving data in XML format, 1159
- debug logging, enabling, 1181-1210
- dedicated sites for Internet-based clients, 238-239
- **Default Actions setting (antimalware policy)**, 805
- default antimalware policy, 804
- **DEFAULTSITESERVERNAME switch (consolesetup.exe)**, 394
- defining priority, 461
- definition updates
  - auto deployment rules for, 799-804
  - delivery of, 830-831
  - synchronizing, 797-799
- **Definition Updates setting (antimalware policy)**, 806
- **Delay Before Retrying (minutes) setting (senders)**, 226
- **delegation, planning**, 1065-1067
- **Delete Aged Application Request Data maintenance task**, 1148
- **Delete Aged Client Operations maintenance task**, 1147-1148
- **Delete Aged Collected Files maintenance task**, 1149
- **Delete Aged Computer Association Data maintenance task**, 1149
- **Delete Aged Delete Detection Data maintenance task**, 1147-1149
- **Delete Aged Devices Managed by the Exchange Server Connector maintenance task**, 1149-1150
- **Delete Aged Device Wipe Record maintenance task**, 1149
- **Delete Aged Discovery Data maintenance task**, 1149

*How can we make this index more useful? Email us at indexes@samspublishing.com*
denial of service (DoS) attacks, 1097

dependencies
adding to applications, 617-618
client hardware dependencies, 432-433
client software dependencies, 433
Endpoint Protection, 787-788
explained, 56
feature dependencies (ConfigMgr 2012), 75-76
migrating by, 338-339
migration dependencies configuration, 339-342
ConfigMgr 2007 migration user account configuration, 339-341
System Center 2012 migration user account configuration, 341-342
deploy.cab, 999
Deploy Configuration Baselines dialog, 515-516
deployment. See also detection methods; software distribution
ADRs (automatic deployment rules), 706-707
Application Deployment Evaluation Cycle, 602
applications, 654-659
client certificates, 1104-1106
configuration baselines, 515-516
console, 388-389
with Configuration Manager Console Setup Wizard, 391-394
console placement, 389
prerequisites, 390-391
supported platforms, 389
unattended console installation, 394-395
content refresh data, 213-214
definition of, 536
deployment deadline, 464
deployment types (DTs), 57, 567-569
  global conditions, 569
Microsoft Application Virtualization, 568, 595-599
Nokia SIS File, 568
requirements, 568-569
Script Installer, 568, 599-601
Windows Installer, 568, 592-595
Windows Mobile Cabinet, 568
device settings, 476
distribution point client certificates, 1106-1108
Endpoint Protection to test collections, 789
end-user experience
  Application Catalog, 662-665
  Software Center, 660-662
explained, 56, 715
image deployment, 1047-1050
in-depth management model (mobile devices), 780-782
monitoring, 665-666
OSD (operating system deployment). See OSD (operating system deployment)
packages, 536, 654-659, 704-705
reports
  deployment management reports, 938-939
  deployment states reports, 939-940
  program deployment status reports, 935-936
simulating, 667
task sequences, 1010-1016
troubleshooting, 665-666
update deployments, 698-703, 723-724
Deployment Image Servicing and Management (DISM), 967
Microsoft Application Virtualization
creating, 595-599
explained, 568
Nokia SIS File, 568
requirements, 568-569
Script Installer
creating, 599-601
explained, 568
Windows Installer
creating, 592-595
explained, 568
Windows Mobile Cabinet, 568
Deployment Types tab (applications), 582-590
Deployment Type - User Experience tab (applications), 587-590
Deploy Software Updates Wizard, 698-703
Deploy Software Wizard, 654-659, 1011-1016
depth management (MDM), 65
design
Active Directory, 180
multi-forest and workgroup considerations, 182-183
schema extensions, 180-181
certificate services, 183-186
hierarchy planning
boundaries and boundary groups, 170-172
client architecture, 174-177
client discovery and installation methods, 172-174
Configuration Manager sites, 167-169
content management, 178-180
hierarchy structure, 169-170
overview, 167
user-centric management, 178
internet-based clients, planning for, 193-194
devices, mobile. See mobile device management
OOB (out of band) management planning, 195-197
overview, 80, 161
site planning
capacity planning, 188-189
server architecture, 189-190
site servers and site systems planning, 186-188
software updates, 190-193, 714-715
solution architecture
business requirements, 162-163
environment assessment, 163-165
overview, 161
testing
overview, 197-198
pilot deployment, 204
proof of concept, 198-204
Despool.log, 1189
Detail pane (console), 377
detection methods
custom script detection methods, 607-610
with PowerShell, 608-609
with VBScript, 609-610
explained, 569, 602
file-based detection methods, 604-606
registry-based detection methods, 606-607
for Windows Installer applications, 602-603
Detection Methods page (Create Configuration Item Wizard), 499
Detection Rule dialog, 604
device collections. See collections
Device Collections node (console), 388
devices, mobile. See mobile device management
Devices node (console), 387
diagnosing errors, 1061
diagnostic rule, 630-631
disabling alerts, 402
BitLocker, 995
discovery
client discovery, 172-174
Active Directory Forest Discovery, 297-298, 420-421
Active Directory Group Discovery, 422-424
Active Directory System Discovery, 426-427
Delta discovery, 422
Heartbeat Discovery, 427-428
Network Discovery, 429-431
purpose of, 419
DDR files, 1155-1162
discovery data, querying, 860-861
discovery logs, 1192
discovery methods, 49-50
heartbeat discovery, 1156
Network Discovery
client discovery, 245
Distribution Point Upgrades subnode (console) 1269

client operating systems, discovering, 245-246
explained, 241-243
network topology, discovering, 243-245
types of, 1156
Discovery Methods subnode (console), 384
Discretionary ACL (DACL), 100
Disk Drives class, 862
disk reports, 924-925
Disks category tasks, 993-995
DISM (Deployment Image Servicing and Management), 967
Dism.log, 1201
displaying. See viewing
Distmgr.log, 1189
Distribute Content Wizard, 1016
Distributed Component Object Model. See DCOM (Distributed Component Object)
distributed enterprises, challenges of implementing, 10
distributing software. See software distribution
Distribution Manager, 256
Distribution Point Configuration Status subnode (console), 387
distribution point groups (DPGs), 58
Distribution Point Groups node (console), 385
Distribution Point Group Status subnode (console), 387
Distribution Point page
Create Secondary Site Wizard, 291
Create Site System Server Wizard, 637
distribution points (DPs), 47, 635-637, 981
BranchCache, 647-648
certificate, deploying, 1106-1108
configuration status, 645
Content Library, 654
distribution point client certificates, 1106-1108
distribution point groups (DPGs), 58
associating collections with, 641
creating, 640
group status, 645
explained, 57-58, 535, 1020-1021
importing/exporting content, 652-653
installing, 637-640
migration planning, 330-331
monitoring status of, 642-645
content status, 643-645
distribution point configuration status, 645
distribution point group status, 645
multicasting, 1023-1025
new features, 74-75
placement, 180
preferred distribution points, 648
prestaged content, 648-652
creating, 650
importing, 650-652
PXE, 1021-1023
refreshing content on, 646
removing content from, 646-647
sending content to, 642
shared distribution points, 366-367
troubleshooting content distribution, 654
updating content on, 645-646
validating content on, 647
Distribution Points node (console), 385
Distribution Points page (Deploy Software Wizard), 658-659, 1012
Distribution Point Upgrades subnode (console), 385

How can we make this index more useful? Email us at indexes@samspublishing.com
Distribution Settings tab (applications), 545-547, 580-581
Distribution Status node (console), 387
DmCertEnroll.log, 1187
DMCertResp.htm, 1187
DmClientHealth.log, 1199
DmClientRegistration.log, 1199
DmClientSetup.log, 1187
DmClientXfer.log, 1187
DmCommonInstaller.log, 1187
DmInstaller.log, 1187
DmpDatastore.log, 1199
DmpDiscovery.log, 1199
DmpHardware.log, 1199
DmpIsapi.log, 1199
Dmpmsi.log, 1198
DmpMsi.log, 1199
Dmprp.log, 1198
DmpSetup.log, 1198-1199
DmpSoftware.log, 1199
DmpStatus.log, 1199
DmSvc.log, 1187
DNSSUFFIX property (Client.msi), 439
documentation
  of log files, 1180
  POC (proof of concept), 199
document maps, 903
DoS (denial of service) attacks, 1097
downloading
  updates, 726-727
  WMI Administrative Tools, 103
Download Location page
  Create Automatic Deployment Rule Wizard, 707
  Deploy Software Updates Wizard, 701
Download Settings page
  Automatic Deployment Rule Wizard, 803
  Deploy Software Updates Wizard, 701
Download Software Updates Wizard, 705
/downloadtimeout: property (CCMSetup), 437
/DP switch (Prereqchk.exe), 269
DPGs (distribution point groups), 58
DPM (Data Protection Manager), 32
DPs. See distribution points
DriverCatalog.log, 1201
driver management reports, 923
Driver Packages subnode (console), 386
drivers
  boot critical drivers, 1056
  in boot images, 981-982
  categories of, 971-972
  driver management, 923, 1030-1032
driver packages, 975-976
importing, 972-977
overview, 971
tasks, 1000-1001
Drivers category tasks, 1000-1001
Drivers subnode (console), 386
Drive Settings page
  Create Secondary Site Wizard, 291
  Create Site System Server Wizard, 639
DSI (Dynamic Systems Initiative)
  importance of, 18
  Microsoft product integration, 16-18
  overview, 16
  SML (Service Modeling Language), 18-19
DTs. See deployment types
DumpVariables.vbs, 1242
Duplicate option (SCUP), 736
dynamic collection, 42
dynam rules, 631-633
Dynamic Systems Initiative. See DSI (Dynamic Systems Initiative)

E

easdisc.log, 1198
EAS (Exchange ActiveSync Service)
    access rules for mobile devices, 762-764
    Connector settings, 757-762
eavesdropping attacks, 1097
Edit option (SCUP), 736
email
    EAS settings in Exchange Server
    Connector, 760
    notifications, configuring, 810-812
Enable BitLocker task, 994-995
ENABLESQM switch (consolesetup.exe), 394
enabling. See also configuration
    alerts, 402
    AutoAdminLogon class, 1219
    BitLocker, 994
    business with infrastructure optimization, 27
    client push, 442-447
    CLR integration, 149
    command-line support, 1058-1059
    logging, 1181-1183
    multicasting, 1023-1025
    PXE, 1021-1023
    Trace Logging, 101-102
Endpoint Protection, 34, 785-787, 1068
    alerts
        alert subscriptions, 813-814
        for device collections, 812-813
    email notifications, 810-812
    overview, 809-810
    antimalware policies
        custom antimalware policies, 807
        default antimalware policy, 804
        importing, 808
        merging, 809
    compared to Forefront Endpoint Protection (FEP) 2010, 786-787
    custom client agent settings, 815
    custom client device settings, 814-815
    definition updates, 830-831
    dependencies, 787-788
    deploying to test collections, 789
    device settings, 466
Endpoint Protection Manager, 1071
endpoint protection point, 169
log files, 1197
monitoring status in
    configuring collections to appear in
    Collection view, 816
    Operational State view, 818-819
    Security State view, 816
new features, 75-77
on-demand scanning, 819-820
planning
    antimalware policies, 788-792
    custom client settings, 788-792
    test collections, deploying to, 789

How can we make this index more useful? Email us at indexes@samspublishing.com
prerequisites, 787-788
reports, 924
SUP configuration
  auto deployment rules for definition updates, 799-804
  synchronizing definition updates, 797-799
Windows firewall policies, 823
EndpointProtectionAgent.log, 1185
Endpoint Protection Client
  automatic removal of antimalware software, 829-830
  client/server communication, 829
  explained, 824-827
  removing, 830
  settings, 827-829
Endpoint Protection node (console), 388
Endpoint Protection page (Add Site System Roles Wizard), 794
Endpoint Protection SMTP Server Connection account, 1122
end user experience
  Application Catalog, 662-665
  new features, 73
  Software Center, 660-662
  software updates
    notifications, 717-718
    Software Center, 718-720
    system restarts and restart notifications, 721-722
    update installation, 720-721
    wiping mobile devices, 767-768
  enforcement, lack of, 12
  enrolling mobile devices, 779-780
  enrollment log files, 1198
  Enrollment Point Connection account, 1118
  enrollment point role, 771-772
  Enrollmentservice.log, 1198
  Enrollmentweb.log, 1198
  EnrollsvMsi.log, 1198
  EnrollwebMsi.log, 1198
  Enterprise CAL Suite, 166
  environment
    assessing, 163-165
    POC environment, building, 199-200
  EPCtrlMgr.log, 1197
  EPMgr.log, 1197
  EPSetup.log, 1197
  errors
    Client Configuration Manager status messages, 253
diagnosing, 1061
Distribution Manager status messages, 256
report server event errors, 946-949
Site Component Manager status messages, 251-252
Erskine, Sam, 1237
Evaluate Collection Members maintenance task, 1153
Evaluate Provisioned AMT Computer Certificates maintenance task, 1153
evaluating
  compliance, 517-519
  configuration baselines, 513
evaluation criteria, 496
Evaluation Schedule page (Create Automatic Deployment Rule Wizard), 707
EventLogForwarder.log, 1197
Exchange ActiveSync (EAS)
  access rules for mobile devices, 762-764
  Connector settings, 757-762
Exchange Server Connection account, 1122
Exchange Server Connector
  configuring, 754-762
  account settings, 755-756
  discovery settings, 756-757
  Exchange ActiveSync (EAS) Connector settings, 757-762
  general settings, 754-755
  logs, 1198
  Proxy Server account, 1122
Exchange Server Connectors subnode (console), 384
exclude rule, 634
Exclusion settings (antimalware policy), 805
exclusive permissions, 510
Execmgr.log, 1185
execution context, 1016-1017
ExecutionLog, 951
ExecutionLog2, 951
ExecutionLog3, 951
execution log data, 951-952
Execution Manager (WMI), 118
existential type compliance rules, 509
Exit command (console), 379
Expire option (SCUP), 736
Export Application Wizard, 620-621
exporting
  applications, 620-621
  configuration baselines, 522
  configuration items, 522
  objects, 652-653
  query results
    between sites, 863-866
    to text file, 863
    task sequences, 1017
Export Objects Wizard, 863-866
Export option (SCUP), 736
Export Queries option, 834, 863
Export Task Sequence Wizard, 1017-1018
expressions, global, 56
ExpressionSolver.log, 1185
ExtADSch.exe, 82-157
ExtAdSch.log, 1189
ExtADSch.log file, 85
extended classes (WMI), 96
extended WQL limitations, 852-853
extending
  Active Directory schema, 81, 180-181
    created classes, 83-84
    with ExtADSch.exe, 82-157
    with LDIFDE (Lightweight Data Interchange Format Data Exchange) utility, 82-83
    verifying schema extensions, 85
    viewing schema changes, 84-85
  extensibility features in mobile device management, 783-784
  hardware inventory, 1211-1213
    cautions, 1211
    device collections, creating, 1223-1224
    example, 1213-1224
    process overview, 1212-1213
    with community tools, 1212
ExternalEventAgent.log, 1185

F
fallback sites, 66, 307-309
Fallback Status Points (FSPs), 47, 169, 185, 301-304, 332
FAQShop.com, 1226
fast network boundaries, 227-229
feature dependencies (ConfigMgr 2012), 75-76
feature packs, 40
file-based detection methods, 604-606
file-based replication, 154-157, 226-227
FileBfTS.log, 1185
files
AddtoConfigurationMof.txt file, 1213-1214
AddtoSmsDefMof.mof file, 1218
AddtoSmsDefMof.txt file, 1217
CAB files, 522
ccmeval.xml, 455
CCR files, 444
ciagent.log, 529
CITaskManager.log, 529
Configuration.mof file. See Configuration.mof file
dcmagent.log, 529
DCMReporting.log, 529
DcmWmiProvider.log, 529
deploy.cab, 999
file-based detection methods, 604-606
file-based replication, 154-157, 226-227
file data, replicating to another site, 132-133
IDMIF files, 469
inventoryagent.log file, 1220
integrity checking, 233
LDF file, 83
log files. See also specific log files
admin console logs, 1182-1210
application management logs, 1194-1195
asset intelligence logs, 1196
backup log files, 1191
client installation logs, 1183-1184
client operations logs, 1184-1187
compliance management log files, 1196-1197
compliance settings log files, 529
content management, 1191-1192
debug and verbose logging, 1181-1192
discovery logs, 1192
enabling, 1181-1183
endpoint protection log files, 1197
inventoryagent.log file, 1220
inventory logs, 1192
log file reader, 272
metering logs, 1197-1198
migration logs, 1194
mobile device management client logs, 1187
mobile device management log files, 1198-1199
MP log files, 1192-1194
NAL logging, 1182-1210
Network Access Protection (NAP) log files, 1199-1200
OSD log files, 1201-1203
Out of Band (OOB) Management log files, 1203-1204
power management log files, 1204-1205
related documentation, 1180
remote control log files, 1205
reporting log files, 1205
role-based administration, 1183-1210
searching with Splunk, 1209-1210
server setup logs, 1188-1189
site server common logs, 1189-1191
smsprov.log, 141
software and application installation log files, 1207-1208
software updates log files, 1205-1207
SQL logging, 1183
SSRS (SQL Server Reporting Services) logs, 945
Trace Logging, 101-102
troubleshooting client installation with,
viewing, 1180
Windows Application Event logs, 1179
Windows setup log files, 1061
Windows Update Agent logs, 1187-1188
WOL (Wake On LAN) log files, 1207
WSUS server log files, 1194
MIF files, 469
NOIDMIF files, 469
.PCK files, 636
smsprov.mof file, 123
text files, exporting query results to, 863
file system conditions, 614-615
FileSystemFile.log, 1185
filtering
ActiveX filtering, 465
configuration baselines, 513
configuration items, 496-497
status messages, 1169-1172
firewalls
site-to-site communications across,
Windows firewall policies, 823
Flexera AdminStudio, 1235
folders, 67
Administrative Security folder, 1088
Out Of Band Management folder, 1088
Status Messages - Audit folder, 1087
Wbem folder, 94
forced scans, 716
/forcereboot property (CCMSetup), 436
Forefront Endpoint Protection. See Endpoint Protection
Forest Discovery (AD), 174
forests (AD), publishing to, 420-421
Format and Partition Disks task, 994
FORMAT() function, 903
forums, 1237-1238
Fspisapi.log, 1199
Fspmgr.log, 1189
Fspmsi.log, 303, 1189
FSP property (Client.msi), 437-439
FSPs (Fallback Status Points), 47, 169, 185,
301-304, 332
FSPStateMessage.log, 1186
Full Administrator, 1071
full content publications, 737
full hierarchy, uninstalling, 314-316
full joins, 860
Functional Specification, 199
functions
DateAdd(), 853
DateDiff(), 853, 905
GetDate(), 854
VB functions, 903
G
GenAppList.vbs, 1242
General category tasks, 989-993
Connect to Network Folder task, 993
Install Application task, 990-991
Install Package task, 991
General category tasks

Install Software Updates task, 992
Join Domain or Workgroup task, 992
Restart Computer task, 993
Run Command Line task, 989-990
Set Task Sequence Variable task, 993
General configuration items, 497

General page
Add Site Roles Wizard, 302
Create Application Wizard, 571
Create Automatic Deployment Rule Wizard, 706
Create Boundary Group Wizard, 299
Create Configuration Item Wizard, 497-498
Create Device Collection Wizard, 629
Create Secondary Site Wizard, 290
Deploy Software Updates Wizard, 698-699
Deploy Software Wizard, 654, 1011
General Query Settings page (Create Query Wizard), 842

general resources, 1225-1229
general settings
   EAS settings in Exchange Server Connector, 758
   Exchange Server Connector, 754-755
General tab (applications), 543, 576-577
GetDate(), 854
GetProcs.vbs, 1242
GetSecurityDescriptor method, 108, 110
global conditions, 55, 569
   versus collections, 610
custom global conditions, 612-616
device global conditions, 611-612
explained, 610-611
user global conditions, 612

Global Conditions subnode (console), 385
global expressions, 56
Globally Unique Identifiers. See GUIDs
global roaming, 39
Group Discovery (AD), 174
grouping tasks, 1008-1010
group policy
   BITS (Background Intelligent Transfer Service), 231-233
   Group Policy installation, 173
   software update settings, 689-692
Group Policy installation, 173
groups
   Active Directory Group Discovery, 422-424
   boundary groups, 227-229
   configuration, 298-300
   planning, 170-172
   compliance groups, 698
distribution point groups
   associating collections with, 641
   creating, 640
DPGs (distribution point groups), 58
group policy
   BITS (Background Intelligent Transfer Service), 231-233
   Group Policy installation, 173
   software update settings, 689-692
group update deployments, 698
Schema Admins group, 83
software update groups, 696-698
GUIDs (Globally Unique Identifiers), 500
GUID data source, 881
SMBIOS GUIDs, 1014
H

HAL types, 1054-1057
hard-link migration, 1038
hardware dependencies, 432-433
hardware inventory
device settings, 467-470
extending
cautions, 1211
device collections, creating, 1223-1224
eexample, 1213-1224
process overview, 1212-1213
with community tools, 1212
initiating, 1220
new features, 69
with WMI, 112-116
hardware reports, 924-926
hardware requirements, 262, 1054-1057
Hardware Requirements subnode (console), 388
hash validation, 636
Head, Michael, 1234
health checks (client), 454-458
health policies, 745-746
Health State Reference Publishing account, 1121
Health State Reference Querying account, 1121
heartbeat discovery, 427-428, 771-772, 1156
Help command (console), 379
Hermes. See SMS (Systems Management Server) 1.0
hidden behavior, 397
Hierarchy Configuration node (console), 384

hierarchy planning
boundaries and boundary groups, 170-172
client architecture, 174-177
client discovery and installation methods, 172-174
Configuration Manager sites, 167-169
content management, 178-180
hierarchy model, 43, 63
hierarchy structure, 169-170
installing and configuring, 324-325
migration planning, 320-321
overview, 167
security, 1089-1090
site hierarchies, 43-44
uninstalling, 314-316
history of Configuration Manager, 37-42
System Center 2012 Configuration Manager, 42
System Center Configuration Manager 2007, 41-42
Systems Management Server 1.x, 38
Systems Management Server 2.0, 38
Systems Management Server 2003, 39
Hite, Don, 1235
Hman.log, 1183, 1189
HTTP, 214
HTTPS, 185, 214
Hudson, Matthew, 1235

IBCM, 241
identifying client’s assigned site, 222
IDMIF files, 469

How can we make this index more useful? Email us at indexes@samspublishing.com
IGD (Internet Gateway Device), 230

IGNOREAPPVVERSIONCHECK property (Client.msi), 439
IIF function, 903

Image Capture phase (task sequences), 987

images
boot images, 1048-1049
customizing, 983-984
distribution points, 981
importing, 984
overview, 977
PXE booting, 977-979
removable media, 979-981
deployment, 1047-1050
image creation
automatic image creation, 1040-1042
explained, 1039-1040
manual image creation, 1042-1044
image upkeep, 1044-1045
maintenance, 1052-1054
offline software updates, 1045-1047
operating system images, 976
Images category tasks, 998-1000

Import Computer Information Wizard, 431
Import Information page (Create Application Wizard), 573

importing
AddtoSMSDefMof.mof file, 1218
antimalware policies, 808
applications, 620-621
boot images, 984
clients into ConfigMgr, 431
configuration packs (CPs), 521-522
drivers, 972-977
objects, 652-653

prestaged content, 650-652
query results between sites, 863-866
Import New Driver Wizard, 972-977
Import Objects option, 834
Import Package from Definition Wizard, 571
Import Task Sequence Wizard, 1018-1019

Inactive Mobile Devices That Are Managed by the Exchange Server Connector report, 783

Inboxast.log, 1190
inboxes, 124
Inboxmgr.log, 1190
Inboxmon.log, 1190
include/exclude rules, 67
include rule, 634
Incorrect Service Principal Name registration, 254
incremental updates, 634-635

in-depth management model (mobile devices), 768-783
client settings, 775-778
compliance settings, 782
enrolling mobile devices, 779-780
heartbeat discovery, 771-772
light management model versus, 753
PKI (public key infrastructure), 771
reports, 782-783
site roles, 771-772
software deployment, 780-782

individual update deployments, 698
individual update status, 723
Infected Computers report, 822
infrastructure, optimizing, 25-29
Infrastructure Administrator, 1071
Infrastructure Optimization Model, 25-29
Infront Consulting Group, 1234
initial client to server communication, 221
site installations

initiating hardware inventory, 1220
inner joins, 858
Installable Rules page (Create Software Update Wizard), 740
Install Application task, 990-991
installation
clients
automatic upgrades, 450-451
blocking/unblocking clients, 450
Client Approval, 449-450
client push, 442-447
Endpoint Protection Client, 827-829
installation methods, 172-174
with logon scripts, 441-442
manual installation, 435-441
network issues affecting client installation, 252-254
software update point (SUP), 448
troubleshooting installation, 451-453
Configuration Manager hierarchy, 324-325
console
with Configuration Manager Console Setup Wizard, 391-394
unattended console installation, 394-395
distribution points, 637-640
planning, 263
pre-installation requirements
Active Directory requirements, 265
prerequisite checker, 265-269
prerequisite files downloader, 269-270
supported SQL Server requirements, 263-265
Windows components, 262-263
SCUP (System Center Update Publisher), 728-729
site installations

CAS (Central Administration Site), 271-278
hierarchy, 270-271
primary sites, 278-287
secondary sites, 288-294
stand-alone sites, 271
troubleshooting, 315-316
unified installer, 270
site system installations
fallback sites, 307-309
fallback status point, 301-304
Out of Band service point, 304-306
SMPs (state migration points), 1026-1029
SSRS (SQL Server Reporting Services), 873-876
SUP (software update point), 677-683
uninstallation process
full hierarchy, 314-316
primary sites, 309-312
secondary sites, 312-314
update installation, 720-721
WSUS (Windows Server Update Services), 265
installation programs, configuring, 551-559
Installation Source Files page (Create Secondary Site Wizard), 290-292
Install Client option (Queries node), 834
Install Configuration Manager Client Wizard, 446-447
Install Deployment Tools task, 999
Installed Rules page (Create Software Update Wizard), 740
Install Package task, 991
Install Software Updates task, 992
/INSTALLSQLEXPRESS switch (Prereqchk.exe), 269

How can we make this index more useful? Email us at indexes@samspublishing.com
INSTR() function, 903
integrity, 1066-1123
intermittently connected users, 241
Internet-based clients, supporting, 237-238
dedicated sites, 238-239
planning, 193-194
sites spanning internet network and perimeter network, 240
site-to-site communications across inner firewall, 239-240
Web proxies and proxy enrollment points, 240-241
Internet Gateway Device (IGD), 230
InternetProxy.log, 1186
intrásıte server communications
   basic network services, 214
   HTTP and HTTPS, 214
   overview, 208-214
   replication of deployment content refresh data, 213-214
   RPC (Remote Procedure Call), 209
   with SQL Server, 208-209
Inventoried Software subnode (console), 388
inventory
   hardware inventory
      device settings, 467-470
      extending, 1211-1224
      initiating, 1220
      new features, 69
      with WMI, 112-116
   software inventory device settings, 477-478
inventoryagent.log, 1186, 1220
InventoryDatatem class, 113
inventory data, querying, 861-863
inventory logs, 1192
Invproc.log, 1192
Ipconfig, 247
IP Network object type, 839
IPSec (IP Security), 186
ISNOTHING() function, 904
ISO 20000, 24-25
IsReadOnly column (RBAC_ObjectOperations), 1081
IsTypeWideOperation column (RBAC_ObjectOperations), 1081
IT automation challenge, 10
ITIL (IT Infrastructure Library), 19-21
IT, 161
IT service triangle, 14
ITSM (IT service management). See service management

J
Jarvernet, Kaido, 1235
jobs, migration
   collection migration jobs, 349-357
   explained, 322, 347
   object migration jobs, 357-362
   objects modified after migration jobs, 362-366
   Join Domain or Workgroup task, 992
/JOIN switch (Prereqchk.exe), 269
joins, 858-860
   full joins, 860
   inner joins, 858
   left joins, 860
   outer joins, 860
   right joins, 860
Jones, Garth, 1235
How can we make this index more useful? Email us at indexes@sams Publishing.com

K

KB925282, 453
Kelbey, John, 1233
dee pairs, 184
Kierkegaard, Søren, 509
Kissinger, Sherry, 1212, 1236
known computers, 1012-1014
Kozeniauskas, Andrius, 1236

L

lab environment, proving concepts in, 200-203
LangPackDir switch (consoleetup.exe), 394
language configuration, modifying, 1139
Language Selection page (Deploy Software Updates Wizard), 702
Languages page (Add Site System Roles Wizard), 682
latency, 210, 227
launching Service Manager console, 406
LDF file, 83
LDIFDE (Lightweight Data Interchange Format Data Exchange) utility, 82-83
Leary, Brian, 1234
LEFT() function, 903
left joins, 860
legacy clients
Legacy Client (SMS 2003), 39
supported mobile devices, 770
legacy migration reports, 369
legacy packages, converting, 623-626
libraries
content library, 58, 73, 179, 214, 654
ITIL (IT Infrastructure Library), 19-21
licensing
patches, 191
planning for, 165-167
reference URLs, 1229
Licensing Core CAL and Enterprise Suite Volume Licensing Brief, 166
light management (MDM), 65
light management model (mobile devices), 753-768
access rules, 762-764
Assets and Compliance workspace, 764-765
end users wiping devices, 767-768
Exchange Server Connector, configuring, 754-762
in-depth management model versus, 753
Resource Explorer, 765-767
troubleshooting, 764
Lightweight Data Interchange Format Data Exchange (LDIFDE) utility, 82-83
limiting collection, 332-335
list of values criterion type, 847
List pane, 377, 835-837
Live Links, 1242
LoadState.exe, 968
local administration of site systems, securing, 1094-1095
local state storage, 1033
Locate Driver page (Import New Driver Wizard), 973
location
of alerts, 403
of console, 389
of servers, 236-237
of sites, 236-237
LocationCache.log, 1186
LocationServices.log, 1186, 1200, 1206
locked configuration baselines/items, 521
log file reader, 272
log files. See also specific log files
  admin console logs, 1182-1210
  application management logs, 1194-1195
  asset intelligence logs, 1196
  backup log files, 1191
  client installation logs, 1183-1184
  client operations logs, 1184-1187
  compliance management log files, 1196-1197
  compliance settings log files, 529
  console log, troubleshooting, 411-412
  content management, 1191-1192
  debug and verbose logging, 1181-1210
  discovery logs, 1192
  enabling, 1181-1183
  endpoint protection log files, 1197
  inventoryagent.log file, 1220
  inventory logs, 1192
  log file reader, 272
  metering logs, 1197-1198
  migration logs, 1194
  mobile device management client logs, 1187
  mobile device management log files, 1198-1199
  MP log files, 1192-1194
  NAL logging, 1182-1210
  Network Access Protection (NAP) log files, 1199-1200
  OSD log files, 1201-1203
  Out of Band (OOB) Management log files, 1203-1204
  power management log files, 1204-1205
  related documentation, 1180
remote control log files, 1205
reporting log files, 1205
role-based administration, 1183-1210
searching with Splunk, 1209-1210
server setup logs, 1188-1189
site server common logs, 1189-1191
smsprov.log, 141
software and application installation log files, 1205-1207
software updates log files, 1205-1207
SQL logging, 1183
SSRS (SQL Server Reporting Services) logs, 945
Trace Logging, 101-102
troubleshooting client installation with, 253-254
troubleshooting client installation with, 1180
Windows Application Event logs, 1179
Windows setup log files, 1061
Windows Update Agent logs, 1187-1188
WOL (Wake On LAN) log files, 1207
WSUS server log files, 1194
Logical Disk class, 862
logical operators, 850
login script installation, 173, 441-442
/logon property (CCMSetup), 435
Lv, Minfang, 480

M
machine accounts, assigning rights to, 1117
maintenance
database maintenance, 1165-1166
DDR files
obsolete records, 1162-1164
retention, 1155-1162
image maintenance, 1052-1054
maintenance tasks
about, 1145
Backup Site Server, 1125-1129, 1145, 1148
Check Application Title with Inventory Information, 1147-1148
Clear Install Flag, 1148
Delete Aged Application Request Data, 1148
Delete Aged Client Operations, 1147-1148
Delete Aged Collected Files, 1149
Delete Aged Computer Association Data, 1149
Delete Aged Delete Detection Data, 1147-1149
Delete Aged Devices Managed by the Exchange Server Connector, 1149-1150
Delete Aged Device Wipe Record, 1149
Delete Aged Discovery Data, 1149
Delete Aged Endpoint Protection Health Status History Data, 1150
Delete Aged Enrolled Devices, 1150
Delete Aged Inventory History, 1150
Delete Aged Log Data, 1146, 1150, 1155
Delete Aged Replication Tracking Data, 1147, 1150, 1155
Delete Aged Software Metering Data, 1151
Delete Aged Software Metering Summary Data, 1151
Delete Aged Status Messages, 1151, 1168
Delete Aged Threat Data, 1151
Delete Aged User Device Affinity Data, 1151
Deleted Aged Status Messages, 1146
Delete Inactive Client Discovery Data, 1152
Delete Obsolete Alerts, 1146, 1152
Delete Obsolete Client Discovery Data, 1152, 1164
Delete Obsolete Forest Discovery Sites and Subnets, 1147, 1153
Delete site maintenance tasks, 1164
Delete Unused Application Revisions, 1153
Evaluate Collection Members, 1153
Evaluate Provisioned AMT Computer Certificates, 1153
monitoring effects of, 1155
Monitor Keys, 1146, 1153, 1165
Rebuild Indexes, 1146, 1153-1155, 1166
Summarize Installed Software Data, 1154
Summarize Software Metering File Usage Data, 1154
Summarize Software Metering Monthly Usage Data, 1154
Update Application Catalog Tables, 1154
Site Maintenance Wizard, 1136-1139
language configuration, modifying, 1139
site resets, 1138
SMS Provider configuration, modifying, 1138
SQL Server configuration, modifying, 1138
status messages, 1166-1167
user data, 1052
MaintenanceCoordinator.log, 1186
maintenance windows, 708-710
malware, antimalware policies, 788-792
automatic removal of antimalware software, 829-830

How can we make this index more useful? Email us at indexes@samspublishing.com
custom antimalware policies, 807
default antimalware policy, 804
importing, 808
malware remediation status, 817
merging, 809
on-demand scanning, 819-820
Managed Object Format files. See MOF files
management
administrative users, 1069-1070
alerts, 402
applications. See application management
certificates, 732
content
content library, 58
distribution point groups (DPGs), 58
distribution points, 57-58
drivers, 1030-1032
MDM (mobile device management), 65
operations management, 31
report security, 890
revision history, 619-620
risk, 1066-1067
service management. See
service management
software updates, 59
systems management. See
systems management
WMI, 98-103
management controller, provisioning, 196-197
Management Licenses (MLs), 166-167
management points (MPs), 47
database connection account, 1118
migration planning, 331
new features, 65
man in the middle (MITM) attacks, 1097
manual client installation, 173, 435-441
CCMSetup.exe properties, 435-437
Client.msi properties, 437-441
manual image creation, 1042-1044
manual update synchronization, 687
MAPS (Microsoft Active Protection Service),
795, 806
Master Project Plan (MPP), 199
Maximum Concurrent Sendings (All Sites)
setting (senders), 226
Maximum Concurrent Sendings (Per Site)
setting (senders), 226
maximum runtime, 709
McAl Lynn, Duncan, 1236
McsExec.log, 1203
McsiSAPI.log, 1203
McsMgr.log, 1203
McsMSI.log, 1203
McsPerf.log, 1203
McsPrv.log, 1203
McsSetup.log, 1203
MCSExec.log, 1203
MDM. See mobile device management
MDT (Microsoft Deployment Toolkit), 961
Mead, Wally, xxix, 1232
MEBx accounts, 1120
Membership Rules page (Create Device
Collection Wizard), 629
memory reports, 925
Memory class, 862
merging antimalware policies, 809
Meringer, Torsten, 1237
MessageHandlerService, 149
message sequencing, 147
messaging
asynchronous messaging, 147
message sequencing, 147
packages, 570-571
planning
  boundaries, 337-338
  central site and hierarchy concepts, 320-321
  coexistence considerations, 327
  migration objects constraints and rules, 323-324
overview, 320
premigration activities, 324-326
security considerations, 332-335
site mode, 321
site servers and site roles, 328-332
supported objects, 321-323
reports, 927
  custom migration reports, 369
  legacy reports, 369
  SSRS reports, 369
shared distribution points, 366-367
source hierarchy, 322
source sites, 322, 343-344
state migration points. See SMPs (state migration points)
troubleshooting, 371-372
Migration Jobs subnode (console), 385
migration logs, 1194
Migration node (console), 385
milestones, reporting with status messages, 1166-1167
minimum hardware requirements, 262
misdirection attacks, 1097
missing or incorrect Service Principal Name registration, 254
mitigating risk, 1067-1123
MITM (man in the middle) attacks, 1097
MLs (Management Licenses), 166-167
mobile device and AMT enrollment points, 47
mobile device enrollment certificate template, 1108-1109
mobile device enrollment proxy points, 47
mobile device management (MDM)
  blocking synchronization, 765
  challenges presented by, 751-752
  client logs, 1187
  enrolling, 47, 779-780
  extensibility features, 783-784
  in-depth management model, 768-783
    client settings, 775-778
    compliance settings, 782
    enrolling mobile devices, 779-780
    heartbeat discovery, 771-772
    light management model versus, 753
    PKI (public key infrastructure), 771
    reports, 782-783
    site roles, 771-772
    software deployment, 780-782
light management model, 753-768
  access rules, 762-764
  Assets and Compliance workspace, 764-765
  end users wiping devices, 767-768
  Exchange Server Connector, configuring, 754-762
  in-depth management model versus, 753
    Resource Explorer, 765-767
    troubleshooting, 764
log files, 1198-1199
mobile device enrollment certificate template, 1108-1109
overview, 65, 753
planning for, 752
settings for configuration items, 511-512
supported ConfigMgr legacy clients, 770
wiping data, 766-768
Mobile Device Settings page (Create Configuration Item Wizard), 502
modern reports, 925
modes, native, 41
Mofcomp.exe, 1215-1216
MOF (Managed Object Format) files, 97
  AddtoSMSDefMof.mof file, importing, 1218
  Configuration.mof. See Configuration.mof file
  opening, 1213
MOF (Microsoft Operations Framework), 21-24
MOF Snippets, 1212
monitoring
  client status, 68
  configuration baselines, 516-517
  deployments, 665-666
  maintenance task effects, 1155
  migration, 322
  with OpsMgr, 1174-1175
software updates
  individual update status, 723
  software update reports, 724
  update deployment status, 723-724
SQL replication, 1140-1143
status, 642-645
  content status, 643-645
  distribution point configuration status, 645
  distribution point group status, 645
  in Endpoint Protection, 816-819
  task sequence deployment, 1057-1058
Monitoring workspace, 381-383
Monitor Keys maintenance task, 1146, 1153, 1165
Moss, Scott, 1236
Move option (Queries node), 834
MP_ClientIDManager.log, 1201
MP_ClientREG.log, 1193
/MP: property (CCMSetup), 435
/MP switch (Prereqchk.exe), 269
Mpcontrol.log, 1193
MP_Ddr.log, 1193
MP_DriverManager.log, 1193
MP_DriverMGR.log, 1201
Mpfdm.log, 1194
MP_Framework.log, 1193
MP_GetAuth.log, 1193
MP_GetPolicy.log, 1193
MP_Hinv.log, 1193
MP_Location.log, 1193, 1201
MP log files, 1192-1194
MPMSI.log, 1194
MP_OOBMgr.log, 1193
MPP (Master Project Plan), 199
MP_Policy.log, 1193
MP_Relay.log, 1193
MP_Retry.log, 1193
MPSetup.log, 1194
MP_SinvCollFile.log, 1193
MP_Sinv.log, 1193
MPs (management points), 47
MP_Status.log, 1193
MSF (Microsoft Solutions Framework), 21
MSI logs, 1184-1210
msxml6_x64MSI.log, 1189
Mtrmgr.log, 1198
Multicast Connection account, 1118

How can we make this index more useful? Email us at indexes@samspublishing.com
1288  multicasting

multicasting, 1023-1025
Multicast page (Create Site System Server Wizard), 639
multi-forest design (AD), 182-183
multiple interfaces (BITS), 233
MVLSImport.log, 1196
myITforum, 1212, 1225
My Reports, 879

N
“nag” restart notifications, 721
NAL logging, 1182-1210
Named Pipes, 209
name resolution, troubleshooting, 248-249
namespaces, 97
  ACLs (Access Control Lists), 99-100
  auditing, 100-101
  CCM namespace, 111
  CIMV2 namespace
    connecting to, 103-104
    Win32_LogicalFileSecuritySetting class., 111
    Win32_LogicalShareSecuritySetting class, 104-111
    Win32_LogicalShareSecuritySetting Class, 104
    Win32_Perf class, 111
  SMS namespace, 111
NAP (Network Access Protection), 60, 224, 742, 1067
  agent settings, 744
  client compliance, 747
  device settings, 470-471
  log files, 1199-1200
  prerequisites, 742-744
  remediation, 748
  reports, 927
  system health, 744-746
  native mode, 41
  Navigation pane (console), 377
  netdiag, 84, 1238
  Netdisc.log, 1192
  Netperf, 1239
  Network Access Protection. See NAP (Network Access Protection)
  Network Adapter Configuration class, 862
  network adapter reports, 926
  network design
    BITS (Background Intelligent Transfer Service)
      advantages of, 230
      ConfigMgr client settings, 232-233
      explained, 229-230
      group policy, 231-233
      multiple interfaces and file integrity checking, 233
      versions, 230-231
    BranchCache, 234-236
    client-to-server communications
      client ports and protocols, 215-220
      client protocols, 222-224
      identifying and contacting client’s assigned site, 222
      initial communication, 221
    NAP (Network Access Protection), 224
data flow, 206-208
  fast network and slow network boundaries, 227-229
  intermittently connected users, 241
Internet-based clients, supporting dedicated sites, 238-239
explained, 237-238
sites spanning internet network and perimeter network, 240
site-to-site communications across inner firewall, 239-240
Web proxies and proxy enrollment points, 240-241
intrasite server communications
basic network services, 214
HTTP and HTTPS, 214
overview, 208
replication of deployment content refresh data, 213-214
RPC (Remote Procedure Call), 209
key decision criteria, 206
latency versus bandwidth, 210
Network Discovery
client discovery, 245
client operating systems, discovering, 245-246
explained, 241-243
network topology, discovering, 243-245
overview, 205-206
server and site placement, 236-237
site-to-site communications
database replication, 225-226
data priorities, 227
file-based replication, 226-227
troubleshooting
basic connectivity problems, 247-248
blocked or unresponsive ports, 249-250
missing or incorrect Service Principal Name registration, 254
name resolution issues, 248-249
network configuration issues, 247
network issues affecting client installation, 252-254
network issues affecting site communications, 258-259
network issues affecting site configuration, 251-252
network issues affecting software distribution, 254-258
overview, 246
timeout issues, 250
Network Discovery, 173-174, 429-431
client discovery, 245
client operating systems, discovering, 245-246
explained, 241-243
network topology, discovering, 243-245
Network Load Balancing Deployment guide, 1233
network protection. See NAP (Network Access Protection)
network reports, 928
network security
certificates for AMT (Active Management Technology), 1110-1115
client certificate deployment, 1104-1106
client-to-server communications security, 1098
distribution point client certificates, 1106-1108
mobile device enrollment certificate template, 1108-1109
PKI web server certificates for IIS site systems, 1099-1104
server-to-server communications security, 1098
site-to-site security, 1099
types of attacks, 1097

How can we make this index more useful? Email us at indexes@samspublishing.com
newly discovered devices, querying for, 855
New Package Wizard, 559-561
New Task Sequence Wizard, 984-986
Niehaus, Michael, 1234
/NOCRLCheck property (CCMSetup), 436
nodes (console), 384-388
NOIDMIF files, 469
Nokia SIS File deployment type, 568
Noncompliance Severity for Reports, 511
non-exclusive permissions, 510
/noexecute property (CCMSetup), 436
Notictrl.log, 1197
notifications. See alerts
NOT operator, 850
/NOUI switch (Prereqchk.exe), 268
Ntsvrdis.log, 1190
null value criterion type, 846
Number of Retries setting (senders), 226
numerical operators, 848

O

object migration jobs, 357-362
object properties, 509
objects
  exporting, 652-653
  importing, 652-653
  migration
    collection migration with associated
    objects, 352-357
    object migration jobs, 357-362
    objects modified after migration jobs,
    362-366
    object types, 839-840
    RBAC_Adms, 1080

network topology, discovering, 243-245
Never Triggered state (alerts), 401
New Computer deployment scenario, 963
new features
  64-bit site system requirements, 62
  Application Catalog web services point, 64
  Application Catalog website point, 64
  application model, 63
  backup, 66
  BITS, 64
  boundaries, 65-66
  centrally managed client settings, 66
  client health status enhancements, 68
  collections, 67
  compliance settings, 68, 493
  console, 64
  content distribution, 636-637
  content library, 73
  distribution points, 74-75
  Endpoint Protection, 75-77
  end user experience, 73
  fallback sites, 66
  hardware inventory, 69
  hierarchy model, 63
  management points, 65
  MDM (mobile device management), 65
  OSD (operating system deployment), 73-74,
  961-963
  packages, 63
  power management, 70-72
  recovery, 66
  Remote Control, 69
  role-based administration, 66
  software updates, 72, 670
  user-centric management, 62
operators

opening MOF files, 1213
Operating System class, 862
Operating System configuration items, 497
operating system deployment. See OSD
Operating System Deployment Manager, 1072
Operating System Images subnode (console), 386
Operating System Installers subnode (console), 386
operating systems
backups, 1129
client operating systems, discovering, 245-246
client support for, 433-435
ConfigMgr requirements, 262-263
crash, recovery from, 1130
deployment. See OSD (operating system deployment)
installers, 976-977
operating system images, 976
reports, 928
security, 1116
Operating Systems node (console), 386
Operational State view, 818-819
OperationName column (RBAC_Categories), 1080
operators
comparison operators, 508
logical operators, 850
precedence, 850
relational operators, 848-849

How can we make this index more useful? Email us at indexes@samspublishing.com
Oppalfens, Kim, 1236
OpsMgr, 1174-1175
optimizing
infrastructure, 25-29
SSRS (SQL Server Reporting Services)
best practices, 951
report caching, 950
report snapshots, 950
report timeout values, 950
subscriptions, 950
Optional configuration items, 514
Optional Information page (Create Software Update Wizard), 740
Options dialog (Report Builder), 898
Oracle VirtualBox, 1040
orchestration, 727-728
Orchestrator, 33-34
organization compliance authoring, 523-524
organizing query list pane, 835-837
OR operator, 850
OSD (operating system deployment)
account security, 1118-1119
advantages of, 960-961
boot images
customizing, 983-984
distribution points, 981
drivers in, 981-982
importing, 984
overview, 977
PXE booting, 977-979
removable media, 979-981
challenges
application compatibility, 1051-1052
hardware considerations, 1054-1057
image maintenance, 1052-1054
user data, maintaining, 1052
deployment scenarios, 963-964
distribution points
explained, 1020-1021
multicasting, 1023-1025
PXE, 1021-1023
drivers
boot critical drivers, 1056
categories of, 971-972
driver management, 1030-1032
driver packages, 975-976
importing, 972-977
in boot images, 981-982
overview, 971
Feature Pack, 40
image operations
image creation, 1039-1044
image deployment, 1047-1050
image upkeep, 1044-1045
offline software updates, 1045-1047
log files, 1201-1203
new features, 73-74, 961-963
operating system images, 976
operating system installers, 976-977
OSD Support Team blog, 1236
overview, 959-960
phases, 968-970
creation, 970
planning, 969
preparation, 969-970
productionization, 970
testing, 970
SMPs (state migration points)
explained, 1025-1026
installing, 1026-1029
selection, 1029
user state without, 1038-1039
tasks
  Apply Data Image task, 999
  Apply Driver Package task, 1001
  Apply Network Settings task, 1002
  Apply Operating System Image task, 998-999
  Apply Windows Settings task, 1003
  Auto Apply Drivers task, 1001
  Capture Network Settings task, 1002
  Capture Operating System Image task, 1000
  Capture User State task, 996-997
  Capture Windows Settings task, 1002
  Connect to Network Folder task, 993
  Convert Disk to Dynamic task, 994
  Disable BitLocker task, 995
  Enable BitLocker task, 994-995
  explained, 989
  Format and Partition Disks task, 994
  Install Application task, 990-991
  Install Deployment Tools task, 999
  Install Package task, 991
  Install Software Updates task, 992
  Join Domain or Workgroup task, 992
  placement, 1003-1005
  Prepare ConfigMgr Client for Capture task, 999-1000
  Prepare Windows for Capture task, 1000
  Release State Store task, 997-998
  Request State Store task, 995
  Restart Computer task, 993
  Restore User State task, 997
  Run Command Line task, 989-990
  Set Task Sequence Variable task, 993

setup Windows and ConfigMgr task, 999

task sequences
  change control and portability, 1017-1019
  custom commands, 1020
  customizing, 1019-1020
  deploying, 1010-1016
  execution context, 1016-1017
  explained, 984-986
  exporting, 1017
  monitoring task sequence deployment, 1057-1058
  phases, 986-987
  properties, 988
  targeting and execution, 1010-1016
  task conditions and grouping, 1008-1010
  task placement, 1003-1005
  variables, 1005-1008

tools
  Sysprep, 965-966
  USMT (User State Migration Tool), 968
  WAIK (Windows Automated Installation Kit), 966-968

troubleshooting
  command-line support, 1058-1059
  smsts.log file, 1060-1061
  USMT, 1061
  Windows setup log files, 1061
  user device affinity, 1049-1050
  user state
  computer associations, 1036-1038
  explained, 1032-1034
  USMT, 1034-1036
  without SMP, 1038-1039

OSDComputerName, 1008

How can we make this index more useful? Email us at indexes@samspublishing.com
OSDDomainName, 1008
OSDDomainOUName, 1007
OSDMigrateAdditionalCaptureOptions, 1008
OSD (Operating System Deployment) Feature Pack, 40
OSDStateStorePath, 1008, 1038
OSD Support Team blog, 1236
OSDTimeZone, 1008
Outboxmon.log, 1190
outer joins, 860
Out Of Band Management folder, 1088
out of band (OOB) management. See OOB (out of band) management
out of band service points, 47
overlapping boundaries, 172

P

Package Conversion Manager (PCM), 623-626
Package Conversion Wizard, 624-626
Package Definition Wizard, 537-543
Package Information page (Create Software Update Wizard), 738
Package object type, 839
packages, 63
    creating
custom packages, 562
    with New Package Wizard, 559-561
    from Package Definition Wizard, 537-543
types of packages, 536-537
deploying, 536, 654-659
    end-user experience, 660-665
    monitoring and troubleshooting deployments, 665-666
    simulating deployments, 667
deployment packages, 704-705
    distributing. See software distribution
driver packages, 975-976
explained, 56, 534
installation program, configuring, 551-559
migrating to System Center 2012, 570-571
Package Conversion Manager (PCM), 623-626
properties, 543-559
    Content Locations tab, 548
    Data Access tab, 544-545
    Data Source tab, 543-544
    Distribution Settings tab, 545-547
    General tab, 543
    installation program configuration, 551-559
    program properties, 548-551
    Reporting tab, 547-548
    Security tab, 548
repackaging software, 562-563
status reports, 935-936
testing, 563-564
troubleshooting, 563-564
USMT packages, creating, 1035-1036
Packages subnode (console), 385
parameters, adding to reports, 902
passwords
    EAS settings in Exchange Server Connector, configuring, 760
    for mobile devices, 752
PatchDownloader.log, 726, 1207
patches
    Patch Management, 190, 1067
testing, 190-191, 671
Patch Management, 190, 1067
Pause.vbs, 1242
PKI (public key infrastructure), 183-186
with Configuration Manager, 185-186
explained, 184-185
in-depth management model (mobile devices), 771
web server certificates for IIS site systems, 1099-1104
placement
of console, 389
of servers, 236-237
of sites, 236-237
of SSRS (SQL Server Reporting Services), 872-873
of SUPs (software update points), 677-683
of tasks, 1003-1005
planning
Active Directory, 180
multi-forest and workgroup considerations, 182-183
schema extensions, 180-181
certificate services, 183-186
delegation, 1065-1067
Endpoint Protection
antimalware policies, 788-792
custom client settings, 788-792
test collections, deploying to, 789
hierarchy planning
boundaries and boundary groups, 170-172
client architecture, 174-177
client discovery and installation methods, 172-174
Configuration Manager sites, 167-169
content management, 178-180
hierarchy structure, 169-170
overview, 167
user-centric management, 178

How can we make this index more useful? Email us at indexes@samspublishing.com
planning

installation, 263
licensing, 165-167
migration
boundaries, 337-338
central site and hierarchy concepts, 320-321
coeexistence considerations, 327
migration objects constraints and rules, 323-324
overview, 320
premigration activities, 324-326
security considerations, 332-335
site mode, 321
site servers and site roles, 328-332
supported objects, 321-323
mobile device management, 752
OOB (out of band) management planning, 195-197
OSD planning phase, 969
security, 1065-1067
site planning
capacity planning, 188-189
server architecture, 189-190
site servers and site systems planning, 186-188
software updates, 190-193, 670-672
planning phase (OSD), 969
Platform Applicability page (Create Configuration Item Wizard), 502
platforms. See operating systems
POC (proof of concept), 198-204
building POC environment, 199-200
documentation, 199
goals, 198
proving concepts in lab environment, 200-203
proving concepts in production environment, 203-204
requirements, 198
policies
antimalware policies, 790-792
automatic removal of antimalware software, 829-830
custom antimalware policies, 807
default antimalware policy, 804
importing, 808
malware remediation status, 817
merging, 809
on-demand scanning, 819-820
client policy device settings, 463
group policy
BITS (Background Intelligent Transfer Service), 231-233
software update settings, 689-692
health policies, 745-746
Windows firewall policies, 823
PolicyAgent.log, 1186
Policy Agent Provider, 118
PolicyAgentProvider.log, 1186
PolicyEvaluator, 1206
PolicyEvaluator.log, 1186
Policypv.log, 1190
PolicySdk.log, 1186
portability of task sequences, 1017-1019
portictl.log, 1195
portlwebMSI.log, 1195
PortQry, 249, 1239
PortQryUI, 249, 1239
ports
blocked or unresponsive ports, troubleshooting, 249-250
changing, 215
client ports, 215-220
NAP (Network Access Protection) requirements, 224
specifying alternate ports, 221
Postponed state (alerts), 401
postponing alerts, 402
Post-Windows phase (task sequences), 987
Power Configuration class, 862
power management
log files, 1204-1205
new features, 70-72
reports, 928-929
settings, 471
PowerShell
custom detection method script, 608-609
drilling down WMI with, 121-123
Scriptomatic, 121, 1238
precedence
of operators, 850
for task sequence variables, 1006
preferred distribution points, 648
pre-installation requirements
Active Directory requirements, 265
prerequisite checker, 265-269
splash screen prerequisite check, 266-267
stand-alone prerequisite checker, 268-269
prerequisite files downloader, 269-270
supported SQL Server requirements, 263-265
Windows components, 262-263
WSUS (Windows Server Update Services), 265
premigration activities, 324-326
ensuring source site(s) is at supported version, 325
installing and configuring ConfigMgr hierarchy, 324-325
preparing ConfigMgr 2007 site for migration, 325
preparing source sites and destination sites for migration, 325-326
preparation phase (OSD), 969-970
Prepare ConfigMgr Client for Capture task, 999-1000
Prepare Windows for Capture task, 1000
Prereqchk.exe, 268-269, 390
prerequisite checker, 265-269
splash screen prerequisite check, 266-267
stand-alone prerequisite checker, 268-269
prerequisite files downloader, 269-270
Prerequisites page (Create Software Update Wizard), 740
PrestageContent.log, 1191, 1195
Prestage Content Wizard, 637
prestaged content, 648-652
creating, 650
with distribution points, 74
importing, 650-652
prestaged media, 42, 981
prestart commands, 983
/PRI switch (Prereqchk.exe), 268
primary devices, 565, 569
primary sites, 45
installing
checklist of activities, 279
child primary sites, 286-287
stand-alone primary sites, 282-285
supported site roles, 278-281
planning, 168
uninstalling, 309-312
primary users, 567
priority, defining, 461

How can we make this index more useful? Email us at indexes@samspublishing.com
private keys, 184
processes
  process consistency, lack of, 13
  Process Monitor, 140, 1238
  viewing process activity, 138-146
Process Monitor, 140, 1238
Processor class, 862
processor reports, 926
production environment, proving concepts in, 203-204
productionization phase (OSD), 970
product releases
  System Center 2012 Configuration Manager, 42
  System Center Configuration Manager 2007, 41-42
  Systems Management Server 1.x, 38
  Systems Management Server 2.0, 38
  Systems Management Server 2003, 39
Products page (Add Site System Roles Wizard), 682
Program object type, 839
programs
  explained, 534-535
  installation programs, configuring, 551-559
  program deployment status reports, 935-936
  properties, 548-551
Progress page
  Create Configuration Item Wizard, 502
  Deploy Software Updates Wizard, 702
Prohibited configuration items, 514
prompted values
  querying with, 855-856
  prompted value criterion type, 846
proof of concept. See POC (proof of concept)
properties
  Active Directory
    forest properties, 421
    Group Discovery properties, 422
    User Discovery properties, 424-425
  application properties
    Application Catalog tab, 577-580
    Content Locations tab, 591
    Deployment Type - Content tab, 583-590
    Deployment Type - Dependencies tab, 590
    Deployment Type - Detection Method tab, 586
    Deployment Type - General tab, 587-590
    Deployment Type - Requirements tab, 590
    Deployment Type - Return Codes tab, 590
    Deployment Types tab, 582-590
    Deployment Type - User Experience tab, 587-590
    Distribution Settings tab, 580-581
    General tab, 576-577
    References tab, 580
    Supersedence tab, 591
CCMSetup.exe, 435-437
Client.msi, 437-441
definition of, 96
driver properties, 974
Heartbeat Discovery properties, 428
Network Discovery properties, 429
object properties, 509
package properties, 543-559
  Content Locations tab, 548
  Data Access tab, 544-545
queries

Data Source tab, 543-544
Distribution Settings tab, 545-547
General tab, 543
installation program configuration, 551-559
program properties, 548-551
Report tab, 547-548
Security tab, 548
program properties, 548-551
site properties
  Active Directory Forest Discovery, 297-298
  boundary groups, 298-300
  changing, 131-132
  client management, 297
  reporting functionality, 297
  viewing, 135
  task sequence properties, 988
  Win32_LogicalShareSecuritySetting class, 104-106
Properties option (Queries node), 834
protecting data. See DPM (Data Protection Manager)
protocols. See specific protocols
providers (WMI), 93
provisioning, 196-197, 1111
proxies, 240-241
proxy enrollment points, 240-241, 771-772
proxy server accounts, 1122
publications (SCUP), 735-737
public certificate authorities, 731
public forums, 1237
public key infrastructure. See PKI (public key infrastructure)
public keys, 184
Publisher, 879
publishing to Active Directory Forest, 420-421
Publish option (SCUP), 736
Pwrmgmt.log, 1204
PwrProvider.log, 1205
PXE, 1021-1023
  booting, 977-979
  PXE Settings page (Create Site System Server Wizard), 639
  PXE Settings page, 639
Q
/q switch (consolesetup.exe), 394
QMX (Quest Management Xtensions) for System Center, 784, 1235
qualifiers, 96
quality, TQM (Total Quality Management), 24
queries
  advanced queries, 851-852
  date and time functions in, 853-854
  examples of, 854-857
  extended WQL limitations, 852-853
  creating
    with Create Query Wizard, 841-844
    with third-party tools, 844
  criterion types, 846-848
  discovery data, querying, 860-861
  explained, 52-53
  inventory data, querying, 861-863
  joins, 858-860
    full joins, 860
    inner joins, 858
    left joins, 860
    outer joins, 860
    right joins, 860
  properties
  QM options (SCUP), 736
  QM update (SPUP), 737
How can we make this index more useful? Email us at indexes@samspublishing.com
queries

List pane, organizing, 835-837
operations, 858-860
operators
   logical operators, 850
   precedence, 850
   relational operators, 848-849
overview, 833
Queries node options, 834-835
relationships, 858-860
results
   creating collections based on, 866
   exporting to text file, 863
   importing/exporting between sites, 863-866
   viewing, 837-838
rules, 631-633
status message queries, 866-870
top 10 most executed reports query, 1241
values, 850-851
viewing, 837-838
wildcards, 851
WQL (WMI query language)
   attribute classes, 840
   attributes, 840-841
   converting to SQL, 857
   explained, 838-839
   limitations, 852-853
   object types, 839-840
Queries node (console), 386, 834-835
Query Rule Properties dialog, 632
Query Statement Properties dialog, 633, 842-843
Quest Management Xtensions (QMX) for System Center, 1235
queues
   ConfigMgrDRSQueue, 151-152
definition of, 147
quotation marks (*), 610

R

Rachui, Steve, 1230, 1233, 1237
Ramsey, Greg, 1235-1237
RBA (role-based administration), 66, 332, 630, 1183-1210
   administrative security reports, 1078-1079
   administrative users, managing, 1069-1070
   console
      “Show Me” behavior, 395-396
      three states of interaction, 397-398
      visibility of objects, 397
   cryptographic controls, 1096-1097
   explained, 1068-1069
   RBA data in site database, 1079-1084
   security roles, 1070-1074
      built-in roles, 1071-1073
      custom roles, 1073-1074
   security scopes, 1074-1078
RBAC (role-based access control), 877-881
   RBAC_Admins, 1080
   RBAC_Categories, 1080
   RBAC_CategoryMemberships, 1082
   RBAC_EdgedPermissions, 1082
   RBAC_InstancePermissions, 1082
   RBAC_ObjectOperations, 1080
   RBAC_RoleOperations, 1082
   RBAC_Roles, 1080
   RBAC_SecuredObjectTypes, 1080
Rcmctrl.log, 1190
Reactivate option (SCUP), 736
Read-only Analyst, 1072
Real-Time Protection setting (antimalware policy), 805
RebootCoordinator.log, 1206
reboots, 714
Rebuild Indexes maintenance task, 1146, 1153-1155, 1166
recent connections (console), viewing, 398
Recently Used-Applications class, 862
recovery
backups, 1129-1136, 1139-1140
new features, 66
reducing TCO (total cost of ownership), 17
References page (Create Boundary Group Wizard), 299-300
References tab (applications), 580
reference URLs
blogs, 1235-1237
genral resources, 1225-1229
Microsoft Configuration Manager resources, 1229-1233
public forums, 1237-1238
System Center Suite, 1237
third-party Configuration Manager resources, 1234-1235
utilities, 1238-1239
Refresh deployment scenario, 963
refreshing
alerts, 402
content on distribution points, 646
Refresh option (Queries node), 834
regional roaming, 39
registry-based detection methods, 606-607
RegKeytoMof tool, 1212
regsvr32, 84
regulatory compliance, 10, 491
relational operators, 848-849
relationships in queries, 858-860
releases. See product releases
Release State Store task, 997-998
Remediate Noncompliant Settings, 511
remediation, 68, 528, 748
remote assistance, 472-476
remote control
auditing, 476
capabilities, 474
configuring, 472-474
device settings, 471-476
log files, 1205
new features, 69
remote administration of client computers, 474-475
remote assistance, 475-476
Remote Desktop, 476
Remote Control Activity Initiated by a Specific User query, 870
RemoteControl.log, 1205
Remote Desktop, 476
remote machines, managing WMI on, 99
remote management technology (WS-MAN), 195
Remote Procedure Call (RPC), 209
Remote Tools Operator, 1072
Remote Tools Permitted Viewer accounts, 1122
removable media, 979-981
removing
content from distribution points, 646-647
Endpoint Protection Client, 830
repackaging software, 562-563

How can we make this index more useful? Email us at indexes@samspublishing.com
Replace deployment scenario, 964
replication. See SQL replication
  ConfigMgr database replication, 148-154
database replication, 225-226
deployment content refresh data, 213-214
file-based replication, 154-157, 226-227
  file data, 132-133
  SQL replication, 146-147
Replication Link Analyzer, 1143-1144
Replication Manager, 132
Replmgr.log, 1190
Report Builder, 879, 893, 897-902, 1239
  Server Uptime Report example, 904-911
  report caching, 950
reporting. See SSRS (SQL Server Reporting Services)
Reporting node (console), 386
reporting services point, 47, 169, 331, 880-881, 1118
Reporting tab (properties), 547-548
reports. See also SSRS (SQL Server Reporting Services)
  administrative security reports, 913-958, 1078-1079
  alert reports, 913
  Antimalware Activity Report, 821
  asset intelligence reports, 913-919
  audit message reports, 1087
  client push reports, 919
  client status reports, 41, 68, 919-920
  compliance and settings management reports, 920-921
  creating, 890-892
  custom reports
    advanced reporting techniques, 903-904
    best practices, 912
  building, 893-902
development tool selection, 893
  interactive features, 902-903
  parameters, 902
  Server Uptime Report example, 904-911
  subreports, 903
Dashboard Report, 822
default reports, 912-945
device management reports, 921-923
driver management reports, 923
Endpoint Protection reports, 924
hardware reports, 924-926
in-depth management model (mobile devices), 782-783
Infected Computers report, 822
migration reports, 369, 927
NAP (network access protection) reports, 927
network reports, 928
operating system reports, 928
out of band management reports, 928
overview, 30-31, 61, 1058
power management reports, 928-929
report caching, 950
reporting log files, 1205
report snapshots, 950
report timeout values, 950
running, 886
searching, 885-886
security, 890
site reports
  client information reports, 930-931
discovery and inventory information reports, 931
genral reports, 932
server information reports, 932
snapshots, 950
software distribution reports, 933-936
software metering reports, 936-937
software reports, 932-933
software update reports, 937-940
state migration reports, 940
status message reports, 941-942
status reporting, 54
subscriptions, 887-889
task sequence reports, 942-943
timeout values, 950
Top Users by Threats report, 821
upgrade assessment - Windows 7 reports, 944
user reports, 944
User Threat List report, 821
virtual applications reports, 944-945
Wake on LAN reports, 945
report server event errors, 946-949
Report Server Execution Log, 945
Report Server HTTP Log, 945
ReportServerService Trace Log, 945
Reports subnode (console), 386
report timeout values, 950
repository, troubleshooting, 103
Request State Store task, 995
Required configuration items, 514
Required Information page (Create Software Update Wizard), 739
requirement rules, 55
RESETKEYINFORMATION property (Client.msi), 440
resetting workspaces, 400
Resource Explorer, 483-484, 765-767
ResourceExplorer.log, 1182
resources
blogs, 1235-1237
general resources, 1225-1229
Microsoft Configuration Manager resources, 1229-1233
public forums, 1237-1238
System Center Suite, 1237
third-party Configuration Manager resources, 1234-1235
utilities, 1238-1239
Restart Computer task, 993
restart notifications, 721-722
restart settings, 466
RestoreExtraState, 1242
Restore User State task, 997
restoring
backups, 1129-1136, 1139-1140
new features, 66
results of queries
creating collections based on, 866
exporting to text file, 863
importing/exporting between sites, 863-866
viewing, 837-838
resynchronizing state message, 712
retention
of DDR files, 1155-1162
retention periods in Delete site maintenance tasks, 1164
of status messages, 1167-1169
retiring applications, 622
/retry: property (CCMSetup), 436
reviewing MSI logs, 1184
revision history, managing, 619-620
ribbon bar (console), 378
RIGHT() function, 903

How can we make this index more useful? Email us at indexes@samspublishing.com
right joins, 860
rights, assigning to machine accounts, 1117
risk acceptance, 1067
risk avoidance, 1067
risk mitigation, 1067
roaming
  clients, 692
  SMS (Systems Management Server) 2003, 39
role-based access control. See RBAC
  (role-based access control)
role-based administration. See RBA
  (role-based administration)
roles. See also RBA (role-based administration)
  associating security scopes with,
    1077-1078
distribution points. See distribution points
  Endpoint Protection role. See
  Endpoint Protection
  hierarchywide site system roles, 168-169
  in-depth management model (mobile devices), 771-772
RBAC (role-based access control), 877-880,
  1080-1082
security roles, 335, 1070-1074
  built-in roles, 1071-1073
  custom roles, 1073-1074
site roles, 328-332
site system roles, 46-48
SMPs (state migration points)
  explained, 1025-1026
  installing, 1026-1029
  selection, 1029
  user state without, 1038-1039
Role selection page (Add Site Roles Wizard), 303
RPC (Remote Procedure Call), 209
RS.exe, 1230
RSS Scripter, 1239
Ruleengine.log, 1190
rules
  ADRs (automatic deployment rules),
    706-707
  auto deployment rules for definition updates, 799-804
  compliance rules, 507-510
direct rules, 630-631
  exclude rule, 634
  include rule, 634
query rules, 631-633
requirement rules, 55
SCUP (System Center Update Publisher), 741
  status filter rules, 1169-1172
Run Command Line task, 989-990
Run option (Queries node), 834
sandboxed applications, 752
Sandys, Jason, 1237
Santiago, Carlos, 1236
Saved Searches option (Queries node), 834
saving DDR files in XML format, 1159
ScanAgent.log, 727, 1206
scan reports, 940
scans
  compliance scanning, 716-717
  on-demand scanning, 819-820
ScanAgent.log, 727, 1206
scan reports, 940
Scan Settings (antimalware policy), 805
ScanState.exe, 968
SCClient_<domain>@<username>_1.log, 1186
SCClient_<domain>@<username>_2.log, 1186
SCCM Audit table, 144
SCCM Expert's Start to Finish Guide to MOF Editing, 1212
scepinstall.exe, 830
Scheduled Scans setting (antimalware policy), 804
Schedule.log, 1190
Scheduler.log, 1186
Scheduler (WMI), 118
schedules
  custom schedules, 461
  simple schedules, 459
Scheduling page
  Deploy Software Updates Wizard, 700
  Deploy Software Wizard, 1011-1012
Scheduling tab (Deploy Software Wizard), 657
Schema Admins group, 83
schema extensions, 180-181
  created classes, 83-84
  explained, 81
  with ExtADSCh.exe, 82-157
  with LDIFDE (Lightweight Data Interchange Format Data Exchange) utility, 82-83
  verifying, 85
  viewing schema changes, 84-85
Schörling, Stefan, 1237
SCM (Security Compliance Manager), 525-526, 1228
SCNotify_<domain>@<username>_1.log, 1186
scope, security scopes, 333-335
  associating with roles, 1077-1078
  creating, 1076
  explained, 1074-1077
Script Installer deployment type, 568, 599-601
Scriptomatic, 121, 844, 1239
scripts
  custom detection method scripts
    with PowerShell, 608-609
    with VBScript, 609-610
  logon scripts, installing client with, 441-442
  OSD starter scripts, 1241-1242
SCSI reports, 926
SC_SiteDefinition_Property table, 142-143
SCUP (System Center Update Publisher), 1239
catalogs, 733-734
configuring, 729-733
custom updates, 737-741
explained, 728
installing, 728-729
publications, 735-737
rules, 741
update operations, 736-737
walkthrough, 742
/SDK switch (Prereqchk.exe), 269
SdmAgent.log, 1206
SDMAgent.log, 1200
SDM (System Definition Model), 17
/SEC switch (Prereqchk.exe), 269
/SECUPGRADE switch (Prereqchk.exe), 269
Search bar (console), 378
searching reports, 885-886
secondary sites, 46
installing, 288-294
planning, 168
supported site roles, 288-289
SUP (software update point) placement, 677
uninstalling, 312-314

How can we make this index more useful? Email us at indexes@samspublishing.com
secure HTTP (HTTPS)

security

accounts

accounts to support ConfigMgr infrastructure, 1117-1118
accounts for Active Directory discovery and publishing, 1121-1122
accounts for OS deployment and software distribution, 1118-1119
accounts for out of band management, 1119-1120
accounts for software updates, 1121
accounts for health state reference, 1121
database connection accounts, 1118
miscellaneous accounts, 1122
overview, 1116-1117
proxy server accounts, 1122
administrative access, securing

at Active Directory level, 1084-1085
auditing administrative actions, 1086-1089
at database level, 1085
administrative security reports, 1078-1079
antimalware policies, 790-792
automatic removal of antimalware software, 829-830
custom antimalware policies, 807
default antimalware policy, 804
importing, 808
malware remediation status, 817
merging, 809
on-demand scanning, 819-820
certificates. See certificates
command-line support, 1059
compliance rule permissions, 510
compliance settings, 1067

console

DCOM permissions, 409, 413-414
overview, 408
SMS Provider permissions, 409
WMI permissions, 409-411, 414-416
content security

operating system deployment, 1116
policy and software distribution, 1115-1116
cryptography, 1096-1097
EAS settings in Exchange Server Connector, configuring, 760
Endpoint Protection, 1068
in hierarchy, 1089-1090
lack of, 11-12
migration, 332-335

collection limiting, 332-333
security roles, 335
security scopes, 333-335
NAP (network access protection), 927, 1067
networks
certificates for AMT (Active Management Technology), 1110-1115
client certificate deployment, 1104-1106
client-to-server communications security, 1098
distribution point client certificates, 1106-1108
mobile device enrollment certificate template, 1108-1109
PKI web server certificates for IIS site systems, 1099-1104
server-to-server communications security, 1098
site-to-site security, 1099
types of attacks, 1097
Patch Management, 1067
PKI (public key infrastructure), 183-186
planning, 1065-1067
report security
  administrative security reports, 913-958
  managing, 890
risk management, 1066-1067
role-based administration. See RBA
  (role-based administration)
security scopes
  associating with roles, 1077-1078
  creating, 1076
  explained, 1074-1077
site systems
  additional site systems, 1095
  attack surface reduction and server hardening, 1091
  local administration, 1094-1095
  physical security and hardware selection, 1090-1091
  security software, 1092-1094
  site database, 1095
  system software security, 1091
Windows firewall policies, 823
Security Administrator, 1072
Security Compliance Manager (SCM), 525-526
Security Compliance Manager (SCM) solution accelerator, 1228
Security node (console), 385
security roles, 335, 1070-1074
  built-in roles, 1071-1073
  custom roles, 1073-1074
  Security Roles object type, 840
Security Roles subnode (console), 385
security scopes, 333-335
  associating with roles, 1077-1078
  creating, 1076
  explained, 1074-1077
  Security Scopes object type, 840
Security Scopes subnode (console), 385
Security State view, 816-818
Security tab (packages), 548
Select Attributes dialog, 632
SelectImage.vbs, 1242
Sender.log, 1190
senders, 48-49, 226
sending content to distribution points, 642
sequences. See task sequences
server architecture, developing, 189-190
server communications
  client-to-server communications
    client ports and protocols, 215-220
    client protocols, 222-224
    identifying and contacting client’s assigned site, 222
    initial communication, 221
    NAP (Network Access Protection), 224
    security, 1098
intrasite server communications
  basic network services, 214
  HTTP and HTTPS, 214
  overview, 208-214
  replication of deployment content refresh data, 213-214
  RPC (Remote Procedure Call), 209
  with SQL Server, 208-209
Server Component Configuration Changes query, 870
Server Components Experiencing Fatal Errors query, 870

How can we make this index more useful? Email us at indexes@samspublishing.com
### Server Feature class

**Server Feature class**, 862

**Server logs**
- application management site server log files, 1194-1195
- asset intelligence site server log files, 1196
- backup log files, 1191
- content management, 1191-1192
- discovery logs, 1192
- inventory logs, 1192
- metering site server log files, 1197
- migration logs, 1194
- MP log files, 1192-1194
- Network Access Protection site server log files, 1199-1200
- reporting log files, 1205
- server setup logs, 1188-1189
- site server common logs, 1189-1191
- software update site server log files, 1205-1206
- WOL (Wake On LAN) site server log files, 1207
- WSUS server log files, 1194

**Server Management Licenses (MLs)**, 166-167

**Servers**
- architecture, developing, 189-190
- component servers, 46
- hardening, 1091
- list of services, 1175-1176
- placement, 236-237

**Server communications**
- client-to-server communications, 215-224
- intrasite server communications, 208-214
- site database servers, 46
- site servers, 46
- virtual servers, 320
- WMI on, 120-123

**Servers and Site System Roles subnode (console)**, 384

- server setup logs, 1188-1189
- server-to-server communications security, 1098
- Service Design volume (ITIL), 20

**Service management**
- DSI (Dynamic Systems Initiative)
  - importance of, 18
- Microsoft product integration, 16-18
  - overview, 16
- SML (Service Modeling Language), 18-19
- Infrastructure Optimization Model, 25-29
- ISO 20000, 24-25
- ITIL (IT Infrastructure Library), 19-21
- MOF (Microsoft Operations Framework), 21-24
  - overview, 15-16, 31
- Six Sigma, 24
- TQM (Total Quality Management), 24

**Service Manager**, 31
- actions, 407-408
- launching, 406
- logging, enabling/disabling, 1182-1210
- overview, 404-405

**Service Modeling Language (SML)**, 17, 18-19

**Service packs (SMS)**, 40

**ServicePortalWebService.log**, 1195
**ServicePortalWebSite.log**, 1195
**Service Principal Names (SPNs)**, 254, 265

/service property (CCMSetup), 436

**Services class**, 862

**Service Strategy volume (ITIL)**, 20
service triangle, 14
ServiceWindowManager.log, 1206
SetComputerName, 1242
SetDriverCategory.vbs, 1242
SetSecurityDescriptor method, 110
Set Security Scopes option (Queries node), 834
Set Task Sequence Variable task, 993
Settings category tasks, 1001-1003
settings management reports, 920-921
Settings page (Create Configuration Item Wizard), 501
Setupact.log, 1201
Setupapi.log, 1201
Setuperr.log, 1201
Setupmgr.exe, 999
setUppolicyevaluator.log, 1186
Setup Windows and ConfigMgr task, 999
Shared Data Set Wizard, 953-956
shared distribution points, 366-367
Shares class, 862
Shield, Greg, 1227
showing. See viewing
Show Install Status page (Create Secondary Site Wizard), 294
“Show Me” behavior, 395-396
SHV (System Health Validator) points, 47, 169, 742-744, 1199
Silect Software CP Studio, 525, 1228
Silverlight, querying for, 855
Simple Object Access Protocol (SOAP), 92
simple schedules, 459
simple value criterion type, 846
simulating deployment, 667
single-instance store, 636
Sinvproc.log, 1192
site codes, choosing, 168
Sitecomp.log, 1190
Site Component Manager status messages, 251-252
Site Component Status node, 295
Site Configuration node (console), 384
Sitectrl.log, 1190
site database servers, 46
Site Hierarchy node (console), 386
site installations
CAS (Central Administration Site), 271-278
hierarchy, 270-271
installation validation
console, 294-296
log files, 296
primary sites
checklist of activities, 279
child primary sites, 286-287
stand-alone primary sites, 282-285
supported site roles, 278-281
secondary sites, 288-294
stand-alone sites, 271
troubleshooting, 315-316
unified installer, 270
uninstallation process
full hierarchy, 314-316
primary sites, 309-312
secondary sites, 312-314
Site Maintenance wizard, 1136-1139
language configuration, modifying, 1139
site resets, 1138
SMS Provider configuration, modifying, 1138
SQL Server configuration, modifying, 1138
site mode, 321
Site object type, 840

site roles
  in-depth management model (mobile devices), 771-772
migration planning, 328-332

sites
CAS (Central Administration Site), 45, 168, 271-278
child sites, configuring for data gathering, 345-347
client’s assigned site, identifying and contacting, 222
configuring
  Active Directory Forest Discovery, 297-298
  boundary groups, 298-300
  client management, 297
  to publish to Active Directory, 89-90
  reporting functionality, 297
connecting console to, 398-399
dedicated sites for Internet-based clients, 238-239
definition of, 44
fallback sites
  configuration, 307-309
  explained, 66
hierarchies, 43-44, 167-169
hierarchywide site system roles, 168-169
importing/exporting query results between, 863-866
installation. See site installations
maintenance tasks. See maintenance tasks
migration planning, 320-321
placement, 236-237
planning
  capacity planning, 188-189
server architecture, 189-190
site servers and site systems planning, 186-188
primary sites, 45, 168
child primary sites, 286-287
installing, 278-287
stand-alone primary sites, 282-285
supported site roles, 280-281
uninstalling, 309-312
properties
  changing, 131-132
  viewing, 135
reports
  site - client information reports, 930-931
  site - discovery and inventory information reports, 931
  site - general reports, 932
  site - server information reports, 932
resets, 1138
secondary sites, 46, 168
installing, 288-294
supported site roles, 288-289
uninstalling, 312-314
senders, 226
site codes, choosing, 168
site roles
  in-depth management model (mobile devices), 771-772
  migration planning, 328-332
site servers, 46
  common logs, 1189-1191
  migration planning, 328-332
sites spanning internet network and perimeter network, 240
site systems. See site systems
How can we make this index more useful? Email us at indexes@samspublishing.com
smsbkup.ctl, 1129
Smsbkup.log, 1191
SMS_BOOTSTRAP.log, 1189
SMSCACHEDIR property (Client.msi), 438
SMSCACHEFLAGS property (Client.msi), 438
SMSCACHESIZE property (Client.msi), 437
SMSCache, 116
SMSClientInstallProperties, 1008
SmscliUI.log, 1186, 1206
SmsClrHost.log, 1197
SMS_Collection class, 121-122
SMSCONFIGSOURCE property (Client.msi), 438
Smsdbmon.log, 1191, 1205
SMSDBMON prefix, 144
SMSDIRECTORYLOOKUP property (Client.msi), 438
SMS_DM.log, 1198
SMSdpmon.log., 1192
smsdprov.log, 1192
SMSENROLLSRVSetup.log, 1191
SMSENROLLWEBSetup.log, 1191
Smsexec.log, 1191
SMS_EXECUTIVE, 1175
SMSFSPSetup.log, 1191
SMSMIME property (Client.msi), 439
SMS namespace, 111
SMSPORTALWEBSetup.log, 1191
SMS Provider, 46
configuration, modifying, 1138
console permissions, 409
SMSProv.log, 141, 1183, 1191
smsprov.mof file, 123
SMSPUBLICROOTKEY property (Client.msi), 440
Smsexec.log, 1013, 1202
SMSROOTKEYPATH property (Client.msi), 440
SMS_SERVER_BOOTSTRAP_<servername>, 1175
SMSSha.log, 1200
SmsSHVADCacheClient.log, 1199
SmsSHVCacheStore.log, 1199
SmsSHV.log, 1199
SmsSHVQuarValidator.log, 1200
SmsSHVRegistrySettings.log, 1200
SMSSHVSetup.log, 1200
SMSSIGNCERT property (Client.msi), 440
SMS_SITE_BACKUP, 1175
SMS_SITECODE=<AUTO | ABC> property (Client.msi), 437
SMS_SITE_COMPONENT_MANAGER, 1175
SMS_SITE_SQL_BACKUP, 1175
SMS_SITE_VSS_WRITER, 1175
SMSSMPSetup.log, 1202
Smssqlbkup.log, 1191
SMS (Systems Management Server) 1.x, 38
SMS (Systems Management Server) 2.0, 38
SMS (Systems Management Server) 2003, 39-40
SMSTrace, 1180
SMSTSCAssignUsersMode, 1008
Smsts.log, 1060-1061, 1202
SMSTSRebootDelay, 1008
Smstsvc.log, 1191
Smswriter.log, 1191
SMTP, testing with Telnet, 811
sniffer-based attacks, 1097
SOAP (Simple Object Access Protocol), 92
SoftwareCatalogUpdateEndpoint.log, 1195
Software Center, 660-662
explained, 57
software updates, 718-720
SoftwareCenterSystemTasks.log, 1195
software dependencies, 433
software deployment. See deployment
software distribution. See also deployment
collections
  creating, 628-630
direct rules, 630-631
exclude rule, 634
include rule, 634
incremental updates, 634-635
user collections versus device
collections, 635
distribution points
BranchCache, 647-648
Content Library, 654
distribution point groups, 640, 641
importing/exporting content, 652-653
installing, 637-640
monitoring status of, 642-645
overview, 635-637
preferred distribution points, 648
prestaged content, 648-652
refreshing content on, 646
removing content from, 646-647
sending content to, 642
troubleshooting content distribution, 654
updating content on, 645-646
validating content on, 647
network issues affecting software
distribution, 254-258
overview, 627-628
query rules, 631-633
reports, 933-936
security, 1115-1116
site system security software, 1092-1094
SoftwareDistribution.log, 1194
Software Files class, 862
software installation log files, 1207-1208
software inventory device settings, 477-478
Software Library workspace, 380-381
software metering
  device settings, 479-480
  explained, 60
  reports, 936-937
Software Metering node (console), 388
Software Metering Rule object type, 840
software packages. See packages
Software Products class, 862
software provisioning, 10
software reports, 932-933
Software Update-Based Client Installation, 448
Software Update configuration items, 497
Software Update Groups subnode
  (console), 386
Software Update Manager, 1072
Software Update Point Connection
  account, 1121
Software Update Point page (Add Site System
  Roles Wizard), 678-679
Software Update Point Proxy Server
  account, 1121
software update points. See SUPs
  (software update points)
Software Update Point Synchronization Status
  node (console), 387
software updates. See also NAP (Network
  Address Protection)
  account security, 1121
  ADRs (automatic deployment rules),
    706-707
All Software Update list, 692-696
architecture, 191-192

How can we make this index more useful? Email us at indexes@sams publishing.com
software updates

client settings, 687-689
compliance scanning, 716-717
definition updates, 830-831
deployment packages, 704-705
design and workflow, 714-715
device settings, 481
downloading, 726-727
download, 736-737
end user experience
notifications, 717-718
Software Center, 718-720
system restarts and restart notifications, 721-722
update installation, 720-721
group policy settings, 689-692
how they work, 192-193
log files, 1205-1207
management, 59
maximum runtime, 709
monitoring
individual update status, 723
software update reports, 724
update deployment status, 723-724
new features, 72, 670
offline software updates, 1045-1047
orchestration, 727-728
overview, 669-670
planning, 190-193, 670-672
prerequisites, 674-676
process, 711-714
reboots, 714
reports, 937-940
SCUP (System Center Update Publisher)
catalogs, 733-734
configuring, 729-733
custom updates, 737-741
explained, 728
installing, 728-729
publications, 735-737
rules, 741
update operations, 736-737
walkthrough, 742
software update groups, 696-698
superseded updates, 711
SUPs (software update points), 47, 448
configuring, 683-684, 797-804
explained, 676-677
installing, 677-683
manual update synchronization, 687
migration planning, 328-329
placement, 677
software update point-based installation, 172
troubleshooting, 725-726
update synchronization, 684-687
task sequences, 727
tools
WSUS (Windows Software Update Services), 673-674
WUA (Windows Update Agent), 673
troubleshooting, 725-727
client update scanning and deployment, 727
SUPs, 725-726
update downloads, 726-727
WSUS, 725-726
update deployments, 698-703, 724
update templates, 703-704
Software Updates node (console), 386
Software Updates page
  Automatic Deployment Rule Wizard, 801
  Create Automatic Deployment Rule Wizard, 706
solution architecture, developing
  business requirements, 162-163
  environment assessment, 163-165
  overview, 161
solution scenarios, planning for
  internet-based clients, 193-194
  OOB (out of band) management planning, 195-197
  software update planning, 190-193
sound card reports, 926
source hierarchy, 322
/source: property (CCMSetup), 436
Source Site account, 1122
Source Site Database account, 1118
source sites, 322
  configuring active source site, 343-344
  preparing for migration, 325-326
spDiagDRS, 154, 259
spDRSInitiateSynchronizations, 153
spDRSMsgBuilderActivation, 153
Specify Required Application dialog, 618
Specify Source Hierarchy page, 343-344
spGetChangeNotifications stored procedure, 144
spGetSSBDiagDialogHandle, 153
splash screen prerequisite check, 266-267
Splunk, 1209-1210
SPNs (Service Principal Names), 254, 265
spoofing attacks, 1097
spUpdateSites stored procedure, 146
SpyNet, 795

SQL (Standard Query Language)
  converting WQL to, 857
  logging, 1183
  SQL Profiler template, 1241
  SQL replication
    alerts, 1144
    monitoring, 1140-1143
    Replication Link Analyzer, 1143-1144
SQL Server
  configuration, modifying, 1138
  intrasite server communications, 208-209
  Management Studio, 134-138
  Profiler, 140-141, 1227
  replication, 146-147
  reporting. See SSRS (SQL Server Reporting Services)
  supported SQL Server requirements, 263-265
SQL Server 2008 R2 Best Practice Analyzer, 1227
SQL Server 2008 R2 Report Server log files, 945
SQL Server Management Studio
  accessing, 134
  collections, viewing, 134-135
  other views, 135-138
  site properties, viewing, 135
  version selection, 872
SQL Server Settings page (Create Secondary Site Wizard), 291, 292
/SQL switch (Prereqchk.exe), 269
SrcUpdateMgr.log, 1186
Srsmgr.log, 945, 1205
srsrpMSI.log, 945, 1205
Srsrpsetup.log, 945, 1205
Srsvacct.log, 1191

How can we make this index more useful? Email us at indexes@samspublishing.com
SSL bridging, 240
SSRS (SQL Server Reporting Services)
backing up, 882-884
best practices, 884-885
Client Status Reporting (CSR), 454-458
compliance strategy, 526-527
configuring, 297, 876-881
installing, 873-876
interactive features, 902-903
optimizing
best practices, 951
report caching, 950
report snapshots, 950
report timeout values, 950
subscriptions, 950
overview, 871-872
reporting log files, 1205
reports, 369
administrative security reports, 913-958
alert reports, 913
asset intelligence reports, 913-919
client push reports, 919
client status reports, 919-920
compliance and settings management reports, 920-921
creating, 890-892
custom reports. See custom reports
device management reports, 921-923
driver management reports, 923
Endpoint Protection reports, 924
hardware reports, 924-926
migration reports, 927
NAP (network access protection) reports, 927
network reports, 928
operating system reports, 928
out of band management reports, 928
parameters, 902
power management reports, 928-929
reporting from reporting services database, 951-956
running, 886
searching, 885-886
security, 890
site - client information reports, 930-931
site - discovery and inventory information reports, 931
site - general reports, 932
site - server information reports, 932
software distribution reports, 933-936
software metering reports, 936-937
software update reports, 724, 937-940
software reports, 932-933
state migration reports, 940
status message reports, 941-942
subreports, 903
subscriptions, 887-889
task sequence reports, 942-943
upgrade assessment - Windows 7 reports, 944
user reports, 944
virtual applications reports, 944-945
Wake on LAN reports, 945
server placement options, 872-873
SQL Server version selection, 872
support for, 41
System Center data warehouse, 957-958
troubleshooting
report server event errors, 946-949
SSRS logs, 945
stand-alone media, 979
stand-alone prerequisite checker, 268-269
stand-alone sites, 271, 282-285
Start to Finish Guide to MOF Editing (SCCM Expert), 1212
startup phase (task sequences), 986
state
  SMPs (state migration points)
    explained, 1025-1026
    installing, 1026-1029
    selection, 1029
    user state without, 1038-1039
state messaging
  device settings, 482
  resynchronizing, 712
  StateMessage.log, 1206
state migration reports, 940
user state
  computer associations, 1036-1038
  explained, 1032-1034
  USMT, 1034-1036
  without SMP, 1038-1039
StateMessage.log, 1206
State Messaging settings (client), 175
State Migration Point page (Add Site System Roles Wizard), 1026-1027
state migration points. See SMPs (state migration points)
Statesys.log, 1191
Statmgr.log, 1191
status
  Client Status Reporting (CSR), 454-458
  distribution points, 642-645
  explained, 53-54
  monitoring in Endpoint Protection, 816-819
package status reports, 935-936
program deployment status reports, 935-936
reports, 54, 919-920
software updates, 723
status summarizers, 54, 1172-1174
update deployment status, 723-724
StatusAgent.log, 1186
Status Message Queries subnode (console), 387
status messages
  Client Configuration Manager, 253
  Distribution Manager, 256
  IDs, 530
  milestones, 1166-1167
  queries, 866-870
  reports, 941-942
  retention, 1167-1169
  Site Component Manager, 251-252
  state filter rules, 54, 1169-1172
  status summarizers, 1172-1174
  suppressing, 1171
  viewing, 867-868
Status Messages - Audit folder, 1087
stored procedures
  spDiagDRS, 154
  spDRSInitiateSynchronizations, 153
  spDRSmsgBuilderActivation, 153
  spGetChangeNotifications, 144
  spGetSSBDialogHandle, 153
  spUpdateSites, 146
string relational operators, 848
subnet-directed WOL (Wake On LAN), 485-486
subnodes (console), 384-388
subreports, 903

How can we make this index more useful? Email us at indexes@samspublishing.com
subscriptions

alert subscriptions, 404, 813-814
report subscriptions, 887-889
SSRS (SQL Server Reporting Services), 950
Subscriptions subnode (console), 386
subselected value criterion type, 847
Sullivan, Kevin, 1236
Summarize Installed Software Data maintenance task, 1154
summarizers, status summarizers, 1172-1174
Summarize Software Metering File Usage Data maintenance task, 1154
Summarize Software Metering Monthly Usage Data maintenance task, 1154
Summary page
Create Application Wizard, 574
Create Configuration Item Wizard, 502
Create Query Wizard, 844
Deploy Software Updates Wizard, 702
Supercedence Rules page (Add Site System Roles Wizard), 681
superceding applications, 621-622
superseeded updates, 711
Superseeded Updates page (Create Software Update Wizard), 740
Supersedence tab (applications), 591
Supported Platforms page (Create Configuration Item Wizard), 502
supported SQL Server requirements, 263-265
suppressing status messages, 1171
SUPSetup, 1206
SUPs (software update points), 47, 448
configuring, 683-684
auto deployment rules for definition updates, 799-804
synchronizing definition updates, 797-799
explained, 676-677
installing, 677-683
manual update synchronization, 687
migration planning, 328-329
placement, 677
software update point-based installation, 172
troubleshooting, 725-726
update synchronization, 684-687
Swmproc.log, 1197
SWMTRReportGen.log, 1198
synchronization
definition updates, 797-799
manual update synchronization, 687
of mobile devices, blocking, 765
update synchronization, 684-687
Synchronization Schedule page (Add Site System Roles Wizard), 680
Synchronization Source page (Add Site System Roles Wizard), 680
Sysinternals website, 1228
Sysprep, 965-966
System Administrator, 880
System Center 2012 Endpoint Protection Status node (console), 387
System Center Central, 1226
System Center Configuration Manager (SMC) 2007, 41
System Center data warehouse, 957-958
System Center Suite, 1237
System Center Update Publisher. See SCUP
System Center Virtual User Group, 1226
System class, 96
System Definition Model (SDM), 17
System Discovery (AD), 173
System Enclosure class, 862
System Health Validator Point Properties
dialog, 743-744
System Health Validator (SHV) points, 47, 169,
742-744, 1199
System Management container
creating, 86-93
setting permissions on, 87-93
System Preparation (Sysprep), 965-966
System Resource class, 840, 861
system restarts and restart notifications,
721-722
System Role Selection page
Add Site System Roles Wizard, 678,
793, 1026
Create Site System Server Wizard, 637
systems management
challenges, 9-10
configuration “shift and drift”, 11
hurdles in distributed enterprise, 10
IT automation challenge, 10
lack of automation and enforcement, 12
lack of process consistency, 13
lack of security and control, 11-12
proliferation of virtualization and cloud
computing, 12-13
timeliness of asset data, 12
definition of, 14-15
Systems Management Server (SMS), 9
Systems Management Server (SMS) 1.x, 38
Systems Management Server (SMS) 2.0, 38
Systems Management Server (SMS) 2003,
39-40
system software security, 1091
System Status node (console), 387
System User, 880

How can we make this index more useful? Email us at indexes@samspublishing.com
<table>
<thead>
<tr>
<th>Task Sequence Editor Domain Joining account, 1119</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task Sequence Editor Network Folder Connection account, 1119</td>
</tr>
<tr>
<td>TaskSequenceProvider.log, 1202</td>
</tr>
<tr>
<td>Task Sequence Run As account, 1119</td>
</tr>
</tbody>
</table>
task sequences, 727. See also tasks
change control and portability, 1017-1019
custom commands, 1020
customizing, 1019-1020
deploying, 1010-1016
execution context, 1016-1017
explained, 984-986
exporting, 1017
monitoring task sequence deployment, 1057-1058
phases, 986-987
properties, 988
reports, 942-943
targeting and execution, 1010-1016
task conditions and grouping, 1008-1010
task placement, 1003-1005
variables, 1005-1008
Task Sequences subnode (console), 386
TCO (total cost of ownership), reducing, 17
TechNet, 1061, 1228, 1234
telnet, 249, 811
templates
SQL Profiler template, 1241
update templates, 703-704
test collections, deploying Endpoint Protection to, 789
testing
client-to-management point connectivity, 250
design
overview, 197-198
proof of concept, 198-204
OSD testing phase, 970
packages, 563-564
patches, 190-191, 671
pilot deployment, 204
virtualization in test environment, 202
testing phase (OSD), 970
text files, exporting query results to, 863
thick images, 1053
thin images, 1053
third-party Configuration Manager resources, 1234-1235
Thompson, Steve, 1237
Thomsen, Paul, 1236
Threat Overrides setting (antimalware policy), 806
threats, 10, 1066-1123
throttling, bandwidth throttling, 227
thumbs.db, 636
time and date operators, 848
time/date functions, 853-854
timeliness of asset data, 12
timeout issues, troubleshooting, 250
tools. See specific tools
Top 5 Malware option, 818
top 10 most executed reports query, 1241
top-level sites, 677
top-level software update point, 168
topology, discovering, 243-245
Top Users by Threats report, 821
total cost of ownership (TCO), reducing, 17
TQM (Total Quality Management), 24
Trace32, 1061, 1180
Trace Logging, enabling, 101-102
transactional processing, 147
Transition volume (ITIL), 20
Trent, Rob, 1225
Trent, Roger, 1236

How can we make this index more useful? Email us at indexes@samspublishing.com
troubleshooting

backups, 1128
boundaries, 258
client installation, 451-453
compliance settings, 529-531
console
common problems, 417
connectivity issues, 416
console logging, 411-412
permissions, 412-416
content distribution, 654
DDR files, 1159
deployments, 665-666
error codes, diagnosing, 1061
light management model (mobile devices), 764
migration, 371-372
MSI logs, 1184
network design
basic connectivity problems, 247-248
blocked or unresponsive ports, 249-250
missing or incorrect Service Principal Name registration, 254
name resolution issues, 248-249
network configuration issues, 247
network issues affecting client installation, 252-254
network issues affecting site communications, 258-259
network issues affecting site configuration, 251-252
network issues affecting software distribution, 254-258
overview, 246
timeout issues, 250
OSD (operating system deployment)
command-line support, 1058-1059
smsts.log file, 1060-1061
USMT, 1061
Windows setup log files, 1061
packages, 563-564
repository, 103
with services, 1175-1176
site installations, 315-316
SMTP settings, 811
software updates, 725-727
client update scanning and deployment, 727
SUP, 725-726
update downloads, 726-727
WSUS, 725-726
SSRS (SQL Server Reporting Services)
report server event errors, 946-949
SSRS logs, 945
with status messages
milestones, 1166-1167
retention of messages, 1167-1169
status filter rules, 1169-1172
status summarizers, 1172-1174
suppressing messages, 1171
USMT, 1061

UDA (user device affinity), 1049-1050
unattended console installation, 394-395
unblocking client, 450
underscore (_), 851
unforced scans, 716
unicast WOL (Wake On LAN), 485
unified installer, 270
/uninstall property (CCMSetup), 436
/uninstall switch (consolesetup.exe), 394
uninstalling
Endpoints Protection Client, 830
full hierarchy, 314-316
primary sites, 309-312
secondary sites, 312-314
Unknown Computer object type, 840
unknown computers, 840, 1014-1015
unresponsive ports, troubleshooting, 249-250
Update Application Catalog Tables
maintenance task, 1154
update catalog, 682
update deployments, 698-703, 723-724
Update Operating System Image Wizard,
1046-1047
updates
content on distribution points, 645-646
definition updates, 830-831
how they work, 192-193
log files, 1205-1207
offline software updates, 1045-1047
planning, 190-193
SCUP (System Center Update Publisher)
update operations, 736-737
software updates. See software updates
update catalog, 682
update deployments, 698-703, 723-724
update templates, 703-704
UpdatesDeployment.log, 727, 1207
UpdatesHandler.log, 727, 1207
UpdatesStore.log, 727, 1207
update templates, 703-704
upgrades
automatic upgrades, 450-451
upgrade assessment - Windows 7
reports, 944
Upgrade deployment scenario, 963
upgrade installation, 173
upkeep of images, 1044-1045
UserAffinity.log, 1186
/UsePKICert property (CCMSetup), 436
User and Device Affinity settings, 175,
482-483
user-centric management, 62, 178
user collections, 635
User Collections node (console), 387
user data, maintaining, 1052
user device affinity, 569-571, 1049-1050
User Discovery (AD), 174
User Experience page
Automatic Deployment Rule Wizard, 801
Deploy Software Updates Wizard, 700
Deploy Software Wizard, 657-658, 1012
user global conditions, 612
User Group Resource class, 840, 861
User Resource class, 840, 861
users
administrative users, managing, 1069-1070
device affinity, 569-571, 1049-1050
global conditions, 612
intermittently connected users, 241
primary users, 567
reports, 944
user data, maintaining, 1052
user state
computer associations, 1036-1038
explained, 1032-1034
USMT (User State Migration Tool), 968, 1034-1036, 1061, 1202
without SMP, 1038-1039

Users node (console), 387
user state
computer associations, 1036-1038
explained, 1032-1034
USMT (User State Migration Tool), 968
creating USMT packages, 1035-1036
explained, 1034
loadstate.log, 1202
scanstate.log, 1202
troubleshooting, 1061
versions, 1034-1035
without SMP, 1038-1039

User State category tasks, 995-998

User State Migration node (console), 388
User State Migration Tool. See USMT
User Threat List report, 821

USMT (User State Migration Tool), 968
creating USMT packages, 1035-1036
explained, 1034
loadstate.log, 1202
scanstate.log, 1202
troubleshooting, 1061
versions, 1034-1035

utilities. See specific utilities

V

validation
content validation, 75, 647
hash validation, 636

site installations
console, 294-296
log files, 296
values, query, 850-851
value type compliance rules, 507-508
van Surksum, Kenneth, 1237
variables, task sequence variables, 1005-1008
VB functions, 903
VBScript, 609-610
v_Collection view, 135
verbose logging, enabling, 1181-1210
verifying
DCOM permissions, 413-414
schema extensions, 85
WMI permissions, 414-416
Verma, Shitasnhu, 1236

versioning compliance settings, 519-521
versions of Systems Center
System Center Configuration Manager
2007, 41-42
Systems Management Server 1.x, 38
Systems Management Server 2.0, 38
Systems Management Server 2003, 39
v_GroupAttributeMap view, 138
v_GroupMap view, 138, 139
v_GS_ views, 135
v_G views, 135
v_HS_ views, 135
v_H views, 135
video card reports, 926
viewing
alerts, 401
collections, 134-135
log files, 1180
process activity, 138-146
queries, 837-838
query results, 837-838
recent connections (console), 398
schema changes, 84-85
site properties, 135
status messages, 867-868
views
  Collection view, 134-135, 816
  explained, 133-134
  Operational State view, 818-819
  Security State view, 816-818
site property views, 135
v_GroupAttributeMap view, 138
v_GroupMap view, 138, 139
v_ReportViewSchema view, 138
v_ResourceAttributeMap view, 137
v_ResourceMap view, 136-137
V_SchemaViews view, 135-136
vSMS_SC_SiteDefinition_Properties view, 142
View XML option (SCUP), 736
virtual applications reports, 944-945
VirtualApp.log, 1187
VirtualBox, 1040
virtualization, 41
  proliferation of, 12-13
  in test environments, 202
Virtual Machine class, 862
Virtual Machine Manager (VMM), 32-33
virtual private networks (VPNs), 193-194
virtual servers, 320
Visual Studio, 893
VMM (Virtual Machine Manager), 32-33
VPNs (virtual private networks), 193-194
v_RA_ views, 135
v_ReportViewSchema view, 138
v_ResourceAttributeMap view, 137
v_ResourceMap view, 136-137
v_R_ views, 135
V_SchemaViews view, 135-136
vSMS_SC_SiteDefinition_Properties view, 142
vulnerability, 1066-1123

W
WAIK (Windows Automated Installation Kit), 966-968
Wake On LAN. See WOL (Wake On LAN)
Wayback Machine, 1242
Wbem folder, 94
WBEMTest.exe, 103, 1216
WBEM (Web-Based Enterprise Management), 91
WCM.log, 683, 725, 1206
Web-Based Enterprise Management (WBEM), 91
Web proxies, 240-241
websites
  blogs, 1235-1237
  general resources, 1225-1229
  Microsoft Configuration Manager resources, 1229-1233
  public forums, 1237-1238
  System Center Suite, 1237
  third-party Configuration Manager resources, 1234-1235
  utilities, 1238-1239
wildcards, 851
Wilson, Ed, 121, 1238
Win32_LogicalFileSecuritySetting class, 1325
Win32_LogicalFileSecuritySetting class, 1325
Win32_LogicalShareAccess class, 109
Win32_LogicalShareAuditing class, 109
Win32_LogicalShareSecuritySetting class
class associations, 108-111
properties, 104-106
sample help entry, 106-107
Win32_Perf class, 111
Win32Reg_AddRemovePrograms class, 115
Windows Application Event log, 1179
Windows Application Log, 945
Windows Automated Installation Kit (WAIK), 966-968
Windows components, 262-263
Windows deployment. See OSD (operating system deployment)
Windows firewall policies, 823
Windows Firewall Policies subnode (console), 388
Windows Installer
deployment type
creating, 592-595
explained, 568
log files, 1208
Windows Installer-based applications
creating, 571-576
detection methods, 602-603
Windows IT Pro, 1228
Windows Management Instrumentation. See
WMI (Windows Management Instrumentation)
Windows Mobile Cabinet deployment type, 568
Windows PowerShell
custom detection method script, 608-609
drilling down WMI with, 121-123
Scriptomatic, 121, 1238
Windows remote management technology (WS-MAN), 195
Windows Server Catalog, 189
Windows Server Update Services. See WSUS
Windows setup log files, 1061
Windows Setup phase (task sequences), 987
Windows System Image Manager (WSIM), 967
Windows Update Agent (WUA), 673, 1187-1188
Windows WMI Control, 98-103
Winmgmt.exe, 94
WinPE, 967, 986
wiping mobile devices data, 766-768
wizards
Add Operating System Image Wizard, 976
Add Operating System Installer Wizard, 977
Add Site System Roles Wizard, 301-304, 678-683, 793-796, 1026-1029
Automatic Deployment Rule Wizard, 800-804
Capture Media Wizard, 1043
Certificate Enrollment Wizard, 1102
Certificates Export Wizard, 1108
Chart Wizard, 897-902
Configuration Manager Console Setup Wizard, 391-394
Configuration Manager Setup
restoring backups, 1130-1136
site maintenance, 1136-1139
Copy Packages Wizard, 637
Create Application Wizard, 571-576
Create Automatic Deployment Rule Wizard, 706-707
Create Boundary Group Wizard, 298-300
Create Child Configuration Item Wizard, 512
Create Configuration Item Wizard, 497-503
Completion page, 502
Compliance Rules page, 501
Detection Methods page, 499
General page, 497-498
Mobile Device Settings page, 502
Platform Applicability page, 502
Progress page, 502
Settings page, 501
Summary page, 502
Supported Platforms page, 502
Create Deployment Type Wizard
creating Application Virtualization deployment type, 595-599
creating Script Installer deployment type, 599-601
creating Windows Installer deployment type, 592-595
Create Database Wizard, 628-630, 1223-1224
Create Direct Membership Rule Wizard, 630-631
Create Migration Job Wizard, 347-348.
See also migration jobs
Create Query Wizard, 841-844
Create Report Wizard, 890-892
Create Secondary Site Wizard, 289-294
Create Site System Server Wizard, 637-640
Create Software Metering Rule Wizard, 480
Create Software Update Wizard, 738-741
Create Status Message Query Wizard, 868-870
Create Subscription Wizard, 887-889
Create Task Sequence Wizard, 1041-1042, 1047-1050
Delete Secondary Site Wizard, 312-314
Deploy Software Updates Wizard, 698-703
Deploy Software Wizard, 654-659, 1011-1016
Distribute Content Wizard, 1016
Download Software Updates Wizard, 705
Export Application Wizard, 620-621
Export Objects Wizard, 863-866
Export Task Sequence Wizard, 1017-1018
Import Computer Information Wizard, 431
Import New Driver Wizard, 972-977
Import Package from Definition Wizard, 571
Import task Sequence Wizard, 1018-1019
Install Configuration Manager Client Wizard, 446-447
Migrating Job Wizard, 348
New Package Wizard, 559-561
New Task Sequence Wizard, 984-986
Package Conversion Wizard, 624-626
Package Definition Wizard, 537
Prestage Content Wizard, 637
Shared Data Set Wizard, 953-956
Site Maintenance, 1136-1139
Update Operating System Image Wizard, 1046-1047
WMI (Windows Management Instrumentation)
Administrative Tools, 103, 1238
client operations, 116-120
Code Creator, 844, 1239
Code Generator, 844, 1239
console permissions, 409-411, 414-416
drilling down with PowerShell, 121-123
Execution Manager, 118
explained, 91-93
hardware inventory, 112-116
infrastructure, 93-95
managing, 98-103
### WMI (Windows Management Instrumentation)

**namespaces**
- CIMV2 namespace, 103-104
- ConfigMgr client namespaces, 111-112
- SMS namespace, 111

**Object Browser, 103**
- object model, 95-97
- on ConfigMgr servers, 120-123

**Policy Agent Provider, 118**
- providers, 93
- repository, troubleshooting, 103
- Scheduler, 118

**Win32_LogicalFileSecuritySetting class.** 111

**Win32_LogicalShareSecuritySetting class class associations**, 108-111
- properties, 104-106
- sample help entry, 106-107

**Win32_Perf class, 111**

**Windows WMI Control**, 98-103

**WMI Administrative Tools, 103**

**WMI Diag (WMI Diagnosis Utility), 102-103, 1238**

**WQL (WMI Query Language), 92**
- attributes, 840-841
- converting to SQL, 857
- explained, 838-839
- limitations, 852-853
- object types, 839-840
- WQL Query conditions, 615

**WMI Diag (WMI Diagnosis Utility), 102-103, 1238**

**WMIPrvse.exe, 95**

**WolCmgr.log, 1207**

**Wolmgr.log, 1207**

### WOL (Wake On LAN)
- configuring, 486-487
- explained, 484
- implementing, 487-488
- log files, 1207
- prerequisites, 484-485
- reports, 945
- subnet-directed WOL, 485-486
- unicast WOL, 485
- workflow for software updates, 714-715
- workgroups, planning, 182-183
- workspaces, 379
- Administration workspace, 383
  - Assets and Compliance workspace, 380, 819
  - Monitoring workspace, 381-383
  - resetting, 400
  - Software Library workspace, 380-381
- Workstation Status class, 862

**WQL (WMI Query Language), 92**
- attribute classes, 840
- attributes, 840-841
- converting to SQL, 857
- explained, 838-839
- limitations, 852-853
- object types, 839-840
- WQL Query conditions, 615
- wrappers, 601

**WSIM (Windows System Image Manager), 967**

**WS-MAN, 195**

**WS-Management, 92**

**WSUSCtrl.log, 683, 725, 1206**
WSUS (Windows Server Update Services), 673-674
log files, 1194
pre-installation requirements, 265
troubleshooting, 725-726
Wsyncmgr.log, 725, 1206
WUAHandler.log, 727, 1207
WUA (Windows Update Agent), 673, 1187-1188
WunderBar, 377

X-Y-Z
XML format, saving DDR files in, 1159
XML Notepad 2007, 1228
XMLStore.log, 1187

Zander, Roger, 1236