Charles Joy
Mark Gosson
Kerrie Meyler

with Pete Zerger, David Allen,
and Marcus Oh

System Center Opalis Integration Server 6.3

UNLEASHED

SAMS

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Charles Joy
Mark Gosson
Kerrie Meyler

with Pete Zerger,
David Allen, and Marcus Oh

System Center Opalis Integration Server 6.3

UNLEASHED

SAMS | 800 East 96th Street, Indianapolis, Indiana 46240 USA

System Center Opalis Integration Server 6.3 Unleashed

Copyright © 2012 by Sams Publishing

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

ISBN-13: 978-0-6723-3561-7

ISBN-10: 0-672-33561-1

Library of Congress Cataloging-in-Publication data:

Joy, Charles, 1979-

System center Opalis integration server 6.3 unleashed / Charles Joy,
Mark Gosson, Kerrie Meyler ; with Pete Zerger, David Allen, and Marcus
Oh.

p. cm.

Includes bibliographical references.

ISBN 978-0-672-33561-7

1. Electronic data processing–Management. 2. Computer
networks–Management. 3. Microsoft Windows server. 4. Computer
systems. I. Gosson, Mark. II. Meyler, Kerrie. III. Title.

QA76.9.M3J69 2012

004.6–dc23

2011027815

First Printing July 2011 with corrections July 2013

Trademarks

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

Warning and Disclaimer

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

Bulk Sales

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

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

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

International Sales
+1-317-581-3793
international@pearsontechgroup.com

Editor-in-Chief
Greg Wiegand

Executive Editor
Neil Rowe

Development Editor
Mark Renfrow

Managing Editor
Sandra Schroder

Project Editor
Seth Kerney

Copy Editor
Jovana Shirley

Indexer
Cheryl Lenser

Proofreader
Apostrophe Editing Services

Technical Editor
Jeff Fanjoy

Publishing Coordinator
Cindy Teeters

Book Designer
Gary Adair

Compositor
Mark Shirar

Contents at a Glance

Introduction 1

Part I Opalis Integration Server Overview and Concepts

1 Introducing Opalis Integration Server 6.3 5

2 Inside Opalis Integration Server 6.3 29

3 Architectural Design 55

Part II Installation and Implementation

4 Installing Opalis Integration Server 6.3 79

5 Policy Basics 115

6 Foundation Objects 153

7 Implementation and Best Practices 201

Part III Integration Packs and the SDK

8 OIS Integration 237

9 Integration with System Center Operations Manager 299

10 Integration with System Center Service Manager 313

11 Integration with System Center Configuration Manager 331

12 Integration with System Center Virtual Machine Manager 347

13 Integration with System Center Data Protection Manager 367

14 Data Center Scenarios 381

15 The Quick Integration Kit 397

Appendixes

A Support and Troubleshooting 469

B Reference URLs 495

C Available Online 503

Index 505

Table of Contents

Introduction 1

Part I Opalis Integration Server Overview and Concepts

1 Introducing Opalis Integration Server 6.3 5

What Is Opalis? 5
Automation, Orchestration, and Integration 6
Workflow 7
OIS Connects the Data Center 7
Microsoft's Automation Platform 8
Microsoft Before OIS 8
Adding OIS to the Picture 8
Making the Difference: The Data Bus 9
Flexibility 9
OIS in the Real World 10
Results 11
Where OIS Fits Within the System Center Suite 11
Enhancing, Extending, and Enabling System Center 12
Transforming the Data Center 14
The History of Opalis Software 15
Rendezvous with Destiny 15
Do the Robot! 16
What Rhymes with OIS? 18
Microsoft Acquires Opalis 21
Product Challenges 21
OIS 6.3 and Beyond 22
SCO 2012 Differences 23
SCO 2012 Similarities 23
Unknowns 23
Understanding IT Process Automation 24
A Brief History of IT Process Automation 24
Old Processes and Unwanted Artifacts 27
Not a Job Scheduler 28
An ITPA Tool, Not a Connector 28
Summary 28

2 Inside Opalis Integration Server 6.3 29

Component Overview 29
Optional Components 31
Required Components 32

SQL Datastore 32
- Installation and Configuration Objects 33
- Policy Authoring Objects 34
- Policy Execution Objects 36
- Policy History and Log Objects 38

Action Servers 39
- The OpalisActionService 39
- Connectivity 40
- PolicyModule.exe 43
- Redundancy 44

OIS Client 45
- OIS Client Connection to the OIS Datastore 47
- From XML to SQL 47

Management Server 48
- Primary Services 48
- Watchdog 49
- Additional Components 50

Opalis Operator Console 52

Summary 54

3 Architectural Design 55

Basic Architecture 55

Policy Lifecycle and Mechanics 56
- Check In 56
- Dormant Policy 57
- Starting the Policy 57
- Action Servers and Policy Instantiation 58
- PolicyModule.exe 58

Policy Limits and Queuing 60
- Action Server Policy Throttle 60
- Maximum Number of Policies to Run 60
- Desktop Heap Limitations and Policies 61
- Policy Maximums Based on Operating System 63
- Policy Size and Complexity 64
- CPU and Memory Resources Also Affect Policy Limits 64

Policy Queuing 64

Policy Spillover 65
- Policies Assigned to Specific Action Servers 66

Policy Failover 66

Deployment Models 67
- Simple Deployment 67

Resilient Deployment 68
Cross-Network Deployment 69
Cross-Network Action Servers 70
Multisite Manual Policy Sync 72
Multisite Invoke via Web Services 73
Multisite Hybrid Solution 74
Multisite Isolated Deployment 75
Security Models 76
Single Domain Security 76
Federated Domains 76
Untrusted Security Model 77
Summary 78

Part II Installation and Implementation

4 Installing Opalis Integration Server 6.3 79

Dependencies Explained 79
OIS 6.2.2 Dependency 80
Java and JBoss Dependency 80
Installation Prerequisites 80
Server Requirements 80
User Account Requirements 81
Trust But Verify 83
Downloading the Installation Media 83
Running the Installer 84
Installing the Management Server 85
Database Creation and Population 87
Licensing 90
Patching for 6.3 93
Deployment Manager 94
Action Server Installation 94
OIS Client Installation 97
Integration Pack Installation 99
Registering the IPs 100
Deploying the IPs 102
Manual Installation 105
The Opalis Operator Console 106
Gathering Files 107
Installing Java 108
Setting Environment Variables 108
Extracting Files 108
Using the PowerShell Script to Install the Opalis Operator Console 110
Securing the Opalis Operator Console 111

Testing the Opalis Operator Console 111
Configuring the Operator Console as a Service 113
Common Installation Problems 113
Summary 114

5 Policy Basics 115

Navigating the OIS Client 115
Understanding the Connections Window 116
Policies 116
Computer Groups 117
Action Servers 117
Global Settings 118
Using the Workspace Window 120
Accessing the Objects Window 120
Reviewing the Events Window 121
Viewing Status in the Log Window 122
The Log History Window: Looking Back 123
Audit History Window 124
Configuring the Client Using the Options Menu 124
Show Link Labels 124
Show Tooltips 125
Show Legacy Objects (Requires Client Restart) 125
Automatic Check Out 125
Prompt for Comment on Check In 126
Allow Empty Comment on Check In 126
Creating Policies 126
Objects 126
Monitor Objects 126
Link Handles 126
Links 127
Dragging and Dropping Objects 127
Configuring Objects 127
Linking Objects 128
The Policy Testing Console 129
Running a Policy 130
Examining the Logs 130
Stepping Through a Policy 130
Setting Breakpoints 131
Differences Between the PTC and the OIS Client 131
Policy Check In and Check Out 132
Starting a Policy in the OIS Client 132
Checking Logging in the OIS Client 133

Branching (Link Filters) . . . 134
- The Default Filter . . . 134
- Adding Filters . . . 134
- Include Filters and Exclude Filters . . . 135
- Link Options . . . 136

The Published Data Bus . . . 136
- Adding Data to the Bus . . . 137
- Types of Published Data . . . 139
- Subscribing to PD on the Bus . . . 139

The Opalis Operator Console . . . 140
- Starting and Stopping Policies . . . 141
- Viewing Policy Execution . . . 141
- Searching for Policies . . . 142
- Action Server View . . . 142
- Permissions . . . 142
- Events . . . 144

Triggering Policies from Within a Policy . . . 145
- The Custom Start Object . . . 145
- The Trigger Policy Object . . . 146

Policies Properties . . . 147
- General Tab . . . 147
- Action Servers Tab . . . 147
- Logging Tab . . . 148
- Event Notifications Tab . . . 149
- Run Behavior Tab . . . 149
- Policy Data Tab . . . 149

Importing and Exporting Policies . . . 150
- Exporting a Group of Policies . . . 151
- Exporting a Single Policy . . . 151
- Importing Policies . . . 151

Summary . . . 152

6 Foundation Objects 153

Basic Object Anatomy . . . 153

Extensibility Objects . . . 157
- Run Program . . . 158
- Query Database . . . 161
- Run .Net Script . . . 163
- Invoke Web Services . . . 167
- Query WMI . . . 169
- Run SSH Command . . . 170
- SNMP Objects . . . 172

Other Important Object Categories 173
  Email and Notification 174
  Workflow Control 177
  Text and File Management 181
  Counters 184
Legacy Objects 187
  The Wait Object 189
  Read, Filter, and Process Email (POP3/SMTP or Exchange) 190
  Other Legacy Objects 191
Remaining Objects 191
Use Case Examples 195
Summary 199

7 Implementation and Best Practices 201

The Policy Engine 201
  Policy Engine Rules 202
  Multi-Value Data Handling 206
  Flattening Multi-Value Data 207
  The Junction Object 208
  Pipeline Mode, Legacy Mode, and the Multiplication Effect 209
Complex Link Logic 210
Looping 212
  Object-Level Looping 212
  Policy-Level Looping 213
Scheduling 214
  The Check Schedule Object 214
  Applying Schedules to a Policy 214
Data Manipulation and Parsing 216
  OIS Data Manipulation Functions 217
  Parsing with the Query Database Object 219
  Parsing with the Run .Net Script Object 219
Dynamic Everything 221
Using Error Handling to Harden Your Policies 222
Securing Policies 225
Naming Conventions 226
Versioning, Backup, and Promotion 227
  Versioning 228
  Backing Up Policies 229
  Promotion 230
External Data Persistence 231
  Challenge: Haltable/Restartable Policies 232
  Solution: Integration Pack for Standard OIS Logging 234
Summary 235

Part III Integration Packs and the SDK

8 OIS Integration 237

Integration Overview 237

The IP for BladeLogic Operations Manager 238

BladeLogic Operations Manager IP Typical Use Case 238

BladeLogic Operations Manager IP Object List 239

BladeLogic Operations Manager IP Installation Notes 239

BladeLogic Operations Manager IP Supported Versions 239

BladeLogic Operations Manager IP Configuration Settings 239

The IPs for BMC Tools 240

The IP for BMC Atrium CMDB 240

The IP for BMC Event Manager 243

The IP for BMC Patrol 245

The IP for BMC Remedy AR System 247

The IPs for CA Tools 250

The IP for CA AutoSys 250

The IP for CA eHealth 252

The IP for CA Spectrum 254

The IP for CA Unicenter NSM 256

The IP for CA Unicenter Service Desk 257

The IP for EMC Smarts InCharge 260

EMC Smarts InCharge IP Typical Use Case 260

EMC Smarts InCharge IP Object List 260

EMC Smarts InCharge IP Installation Notes 261

EMC Smarts InCharge IP Supported Versions 261

EMC Smarts InCharge IP Configuration Settings 261

The IPs for HP Tools 262

The IP for HP Asset Manager 262

The IP for HP iLO and OA 264

The IP for HP Network Node Manager 266

The IP for HP OpenView Operations (Unix - HPUX) 268

The IP for HP OpenView Operations (Unix - Solaris) 270

The IP for HP OpenView Operations (Windows) 273

The IP for HP OpenView Service Desk 275

The IP for HP Service Manager 278

The IPs for IBM Tools 280

The IP for IBM Tivoli Enterprise Console 280

The IP for IBM Tivoli Netcool Omnibus 282

The IP for IBM Tivoli Storage Manager 284

The IP for Microsoft Active Directory 286

Microsoft Active Directory 2 IP Typical Use Case 286

Microsoft Active Directory 2 IP Object List 287

Microsoft Active Directory IP 2 Installation Notes 288

Microsoft Active Directory 2 IP Supported Versions 288
Microsoft Active Directory 2 IP Configuration Settings 289
The IP for Unix 289
Unix IP Typical Use Case 289
Unix IP Object List 290
Unix IP Installation Notes 291
Unix IP Supported Versions 291
Unix IP Configuration Settings 292
The IP for Veritas NetBackup 293
Veritas NetBackup IP Typical Use Case 293
Veritas NetBackup IP Object List 293
Veritas NetBackup IP Installation Notes 293
Veritas NetBackup IP Supported Versions 294
Veritas NetBackup IP Configuration Settings 294
The IP for VMware vSphere 295
VMware vSphere IP Typical Use Case 295
VMware vSphere IP Object List 295
VMware vSphere IP Installation Notes 297
VMware vSphere IP Supported Versions 297
VMware vSphere IP Configuration Settings 297
Summary 298

9 Integration with System Center Operations Manager 299

Requirements 299
Opalis Integration Server 6.3 299
System Center Operations Manager 2007 299
Installing the SCOM IP 300
Configuring the SCOM IP 300
Connectivity Requirements 300
Granting Access to the Connection Account 301
Configuring the Connection Account 301
Objects at a Glance 302
Objects in Depth 303
Use Case Scenarios 305
Incident Remediation 305
Server Maintenance Mode 307
Branch Office Maintenance Mode 309
Summary 312

10 Integration with System Center Service Manager 313

Requirements 313
Opalis Integration Server 6.3 313

System Center Service Manager 2010 314
Locale Settings 314
Installing the SCSM IP 314
Configuring the SCSM IP 314
Objects at a Glance 315
Objects in Depth 316
Use Case Scenarios 317
Close Resolved Incidents 318
Manage Incidents 320
Automating Change 323
Summary 330

11 Integration with System Center Configuration Manager 331

Requirements 331
Opalis Integration Server 6.3 331
System Center Configuration Manager 2007 332
Installing the SCCM IP 332
Configuring the SCCM IP 332
Creating the Connection Account 332
Granting Access to the Connection Account 333
Connectivity Requirements 335
Objects at a Glance 335
Objects in Depth 335
Use Case Scenarios 338
Creating and Populating a Collection 338
Checking Compliance 341
Advertising Software 344
Summary 346

12 Integration with System Center Virtual Machine Manager 347

Requirements 347
Opalis Integration Server 6.3 347
System Center Virtual Machine Manager 2008 348
Security Credentials 348
Installing the VMM IP 348
Configuring the VMM IP 348
Connectivity Requirements 348
Granting Access to the Connection Account 349
Configuring the Connection Account 349
Objects at a Glance 351
Objects in Depth 352
Use Case Scenarios 355

Virtual Machine Provisioning ... 356
VM Checkpoint and Recovery ... 360
Capacity and Lifecycle Management ... 363
Summary ... 366

13 Integration with System Center Data Protection Manager 367

Requirements ... 367
Opalis Integration Server 6.3 ... 367
System Center Data Protection Manager 2010 ... 368
Windows Management Framework ... 368
Installing the DPM IP ... 368
Configuring the DPM IP ... 369
Objects at a Glance ... 370
Objects in Depth ... 370
Use Case Scenarios ... 372
Creating a Recovery Point ... 372
Protecting a Data Source ... 375
Recovering a SQL Database ... 375
Checking DPM Server Storage Capacity ... 378
Summary ... 379

14 Data Center Scenarios 381

Requirements in the Dynamic Data Center ... 382
Use Case Scenarios ... 383
Server Maintenance and Reboot ... 383
Virtual Machine Provisioning and Configuration ... 386
Bulk User Account Provisioning ... 391
Summary ... 395

15 The Quick Integration Kit 397

Overview of QIK ... 397
Options and More Options ... 398
Planning Your QIK Project ... 400
Installing QIK ... 401
Installation Prerequisites ... 401
Running the Installer ... 402
Actions Performed by the Installer ... 406
Your IDE and the QIK Resources ... 410
Installing the QIK Integration Packs ... 415
QIK CLI Wizard ... 415
QIK SDK ... 432

SDK Prerequisites . . . 433
SDK Features and Functionality . . . 433
QIK API . . . 434
QIK Programming Models . . . 435
QIK Project Process . . . 436
QIK Code Samples . . . 437
Creating Integration Packs . . . 445
The QIK Wizard . . . 445
Using the QIK Wizard . . . 445
Deploying QIK Objects . . . 456
Test Mode . . . 456
Ready for Production . . . 462
Summary . . . 467

Appendixes

A Support and Troubleshooting 469

Product Footprint . . . 469
File System . . . 469
Registry Structure . . . 473
Running Processes and Services . . . 475
Start Menu Programs . . . 475
Background Executables . . . 476
Datastore . . . 477
Basic Troubleshooting . . . 477
Common Questions . . . 482
OOC Questions . . . 485
Foundation Object Questions . . . 486
Versions . . . 488
Log History . . . 489
Data Items Logged . . . 490
Log Purging . . . 491
Logging Levels . . . 492
TraceLogger Options . . . 493
Checking Logs . . . 493

B Reference URLs 495

General Resources . . . 495
Microsoft's OIS Resources . . . 496

Additional Resources 498
Blogs 500
The System Center Family 501
Public Forums 501

C Available Online 503

PowerShell Resources for Maintenance Mode 503
Live Links 503

Index 505

About the Authors and Contributors

Charles Joy, senior technology evangelist at Microsoft, began working at small start-up firms and moved on to companies such as Raytheon, Unisys, and later Opalis Software. Charles was responsible for implementing the world's largest OIS deployments. Charles has been a frequent presenter on OIS at MMS, TechEd (U.S., AU, and NZ), and numerous internal Microsoft conferences. He is also a frequent contributor on TechNet with a blog at http://blogs.technet.com/b/charlesjoy/.

Mark Gosson, senior technology evangelist at Microsoft, has worked in IT for more than 18 years. He worked at Opalis Software, Inc., from 2004 until its acquisition by Microsoft. At Opalis, he managed Field and Pre-Sales Engineering and was responsible for implementations at Opalis's largest customers. Mark has been a frequent presenter on OIS at MMS, TechEd (U.S., AU, and NZ), and numerous internal Microsoft conferences.

Kerrie Meyler, System Center MVP, is an independent consultant and trainer with more than 15 years of Information Technology experience, including work as a senior technical specialist at Microsoft. She has presented at TechEd, MMS, and Microsoft product launches. Kerrie is the lead author of a number of books in the Unleashed series, including *Microsoft System Center Operations Manager 2007 Unleashed* (Sams, 2008), *System Center Operations Manager 2007 R2 Unleashed* (Sams, 2010), *System Center Configuration Manager 2007 Unleashed* (Sams, 2009), and *System Center Service Manager 2010 Unleashed* (Sams, 2011).

Pete Zerger, System Center MVP, focuses on System Center management and data center automation. He presents at Microsoft conferences such as MMS and TechEd and manages System Center Central (http://www.systemcentercentral.com). Pete was a contributing author to *System Center Operations Manager 2007 R2 Unleashed* and *System Center Configuration Manager 2007 Unleashed*. He also writes courseware for Microsoft Learning, including Course 50507A, "Designing and Automating Workflows with Microsoft System Center Opalis."

Marcus Oh, System Center MVP, has more than 15 years of IT industry experience and is a technical manager for a large telecommunications provider. He specializes in Configuration Manager and Operations Manager. Marcus has written numerous articles for technology websites and blogs on OIS and other System Center products at http://marcusoh.blogspot.com/. Marcus runs the Atlanta Systems Management User Group (http://www.atlsmug.org) and coauthored *Professional SMS 2003, MOM 2005, and WSUS* (Wrox, 2006).

David Allen, System Center MVP, has more than 10 years of experience in the IT industry and is a systems management specialist. He has worked with OIS since the Microsoft acquisition, designing workflows and overseeing various levels of implementation. David presents at MMS, TechEd, and TechDays. He blogs at http://wmug.co.uk/blogs/aquilaweb/default.aspx and is the founder of http://www.scdpmonline.org.

Dedication

To IT professionals worldwide who use the System Center suite

Acknowledgments

Writing a book is an all-encompassing and time-consuming project, and this book certainly meets that description. The authors and contributors would like to offer appreciation to those who helped with *System Center Opalis Integration Server 6.3 Unleashed*.

Special thanks to Kaj Wierda, founding member and longtime Opalis employee, for his insight into the early years of ITPA. Thanks also to Akos Technology Services for lab assistance, to Scott Weisler of Akos for environment support, and to Michelle Cohen of Microsoft. Jeff Fanjoy, also of Microsoft, was invaluable as our technical editor.

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.

As an associate publisher for Sams Publishing, I welcome your comments. 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 better.

Please note that I cannot help you with technical problems related to the topic of this book. We do have a User Services group, however, where I will forward specific technical questions related to the book.

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

Email: feedback@samspublishing.com

Mail: Neil Rowe
Executive Editor
Sams Publishing
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.

Introduction

In December 2009, Opalis Software, Inc., became a wholly owned subsidiary of Microsoft Corporation. Opalis Software was best known for its IT Process Automation (ITPA)/Runbook Automation (RBA) offering Opalis Integration Server (OIS).

ITPA is a powerful capability that can assist in streamlining Information Technology (IT) operations by removing much of the overhead associated with manual responses to IT problems. OIS enables you to capture and document processes that integrate across an entire IT organization. This is a core building block for the future of IT and is the foundation for the automation necessary to deliver cloud computing—self-adjusting tools of computing resources that can be tuned based on real-time events.

Microsoft acquired Opalis Software to augment its System Center line of management software. The Opalis purchase enables Microsoft to integrate Opalis's process automation into its vision of the data center of the future. Microsoft does not sell Opalis as a separately licensed product; those of you already licensed for System Center with SMSE/D have the licensing rights for Opalis—you simply have to learn how to integrate it into your environment. That is the purpose of this book.

As part of the acquisition, Opalis Software released OIS 6.2.2, a remediated version of 6.2.1. Microsoft followed up with the release of OIS 6.3 in November 2010, which includes Windows Server 2008 support and Integration Packs (IPs) for products in the System Center suite. Because Microsoft chose to bring out a version of Opalis Integration Server without rebranding the software and while Opalis Software was still a subsidiary, it relies heavily on its 6.2.2

roots, particularly during the installation process. Moving forward, OIS 6.3 will be the last version of OIS. In March 2011, Microsoft announced System Center Orchestrator 2012, which will be the next version of the software it obtained with the Opalis acquisition.

How This Book Is Organized

This book is divided into four sections:

Part I, “Opalis Integration Server Overview and Concepts,” includes an introduction to the product and discusses its history, architectural concepts, and design. These topics are discussed in Chapter 1, “Introducing Opalis Integration Server 6.3,” Chapter 2, “Inside Opalis Integration Server 6.3,” and Chapter 3, “Architectural Design.”

Part II, “Installation and Implementation,” steps through the product installation. Because Microsoft released version 6.3 of OIS while Opalis Software was still a subsidiary of Microsoft, there are some inherent differences installing OIS 6.3 compared with the rest of the System Center suite. These are covered in Chapter 4, “Installing Opalis Integration Server 6.3.” Chapter 5, “Policy Basics,” begins the discussion of the different objects you can use to create your own policies. This goes into further depth in Chapter 6, “Foundation Objects,” and Chapter 7, “Implementation and Best Practices.”

Part III, “Integration Packs and the SDK,” focuses on integrating OIS into the data center through IPs. IPs are software components that plug into the larger OIS framework and are designed around a series of atomic tasks targeted to a specific application. OIS 6.2.2 ships with 28 IPs on the installation media integrating third-party software with the OIS engine, and with the 6.3 update, Microsoft added six additional IPs for System Center integration. The OIS 6.2.2 IPs are discussed in Chapter 8, “OIS Integration.” The System Center IPs are discussed in the following chapters:

- Chapter 9, “Integration with System Center Operations Manager”
- Chapter 10, “Integration with System Center Service Manager”
- Chapter 11, “Integration with System Center Configuration Manager”
- Chapter 12, “Integration with System Center Virtual Machine Manager”
- Chapter 13, “Integration with System Center Data Protection Manager”

Chapter 14, “Data Center Scenarios,” takes the System Center IPs to the next level by presenting examples that integrate objects from these IPs together in workflows and incorporate PowerShell to achieve true end-to-end automation. Just in case you still don’t have all the objects you need to accomplish your own integrations, Chapter 15, “The Quick Integration Kit,” gives you the tools to create your own IPs using the Quick Integration Kit (QIK).

By this time, you should have all the tools at your disposal necessary to become an OIS expert. The last section of the book includes three appendixes. Appendix A, “Support and Troubleshooting,” includes resources to assist you with problem solving, Appendix B, “Reference URLs,” incorporates useful references you can use for further information, and Appendix C, “Available Online,” is a guide to supplementary resources offered with the book that you can download from http://www.informit.com/store/product.aspx?isbn=9780672335617.

This book provides in-depth reference and technical information about Opalis Integration Server 6.3, as well as information on orchestrating with System Center and third party products through IPs. The material will be of interest for those shops using the System Center suite, Opalis Integration Server, and anyone interested in ITPA. 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.

This page intentionally left blank

CHAPTER 3

Architectural Design

IN THIS CHAPTER

- Basic Architecture
- Policy Lifecycle and Mechanics
- Policy Limits and Queuing
- Policy Spillover
- Policy Failover
- Deployment Models
- Security Models

When determining the best approach to deploy Opalis Integration Server (OIS), there are several factors to consider as you design an OIS instance. Before designing your instance, you should answer a number of questions about your environment, including network, domain structure, and location of your automation targets.

This chapter expands on the basic OIS architecture from Chapter 2, "Inside Opalis Integration Server 6.3," and explains how the components interact with one another during policy execution. It also discusses the major deployment models and identifies where each model would be most beneficial. In addition to architecture, this chapter reviews how the various security models affect an OIS deployment. You can use OIS in a wide range of environments and security models, from small networks to managed service providers. Each presents different challenges and requires different solutions.

Basic Architecture

Chapter 2 discussed the OIS components and explained their purpose. This chapter examines those same components as they work together to create, check-in, and execute policies. Because the policy is the core element of all automation, orchestration, and integration, this chapter looks into the lifecycle of a policy and examines how the OIS components support the phases of that lifecycle. Figure 3.1 shows the main components of OIS.

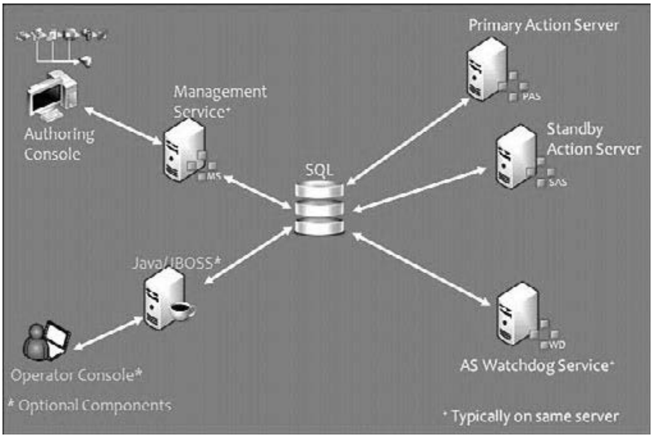


FIGURE 3.1 OIS architecture

Policy Lifecycle and Mechanics

The lifecycle of a policy begins with creating that policy in the OIS Client. For more information on how to create a policy, refer to Chapter 5, •Policy Basics.Ž As the policy is created, edited, or tested (within the Policy Testing Console), the policy data is stored locally by the OIS Client. The policy data remains in local storage until the policy is Checked In by the policy author.

NOTE: USE A RELEASE PROCESS WHEN DEALING WITH AUTOMATION

Many organizations find it easiest if their policy authors test their policies and check them into a production server after the author is satisfied with the results. This is a hazardous practice and not recommended for a production environment.

Because of the nature of automation, no single user should be trusted with design, testing, and promoting into production. The authors recommend, at a minimum, that someone other than the policy author perform testing and promoting a policy into production. Ideally, your organization already has a release process, with a testing or staging environment. In this case, include your OIS policies into these processes and environments.

Refer to Chapter 7, •Implementation and Best Practices,Ž for more information regarding this topic. Policies without safeguards can be dangerous things.

Check In

After the Check In button is pressed, the OIS Client contacts the Management Server so the policy can be written to the datastore. In this scenario, the Management Server acts as a proxy or broker so the OIS Client machines do not access the datastore directly„as doing so would mean every author would require write access to the various database tables.

The OIS Client transmits the policy in the form of object data and configuration data for those objects (based on the installed Foundation objects and the objects contained within any Integration Packs [IPs] deployed to the client). This policy data, which is loosely formatted eXtended Markup Language (XML) data, is taken by the Management Server and written into the datastore. The creation or update of a policy is a somewhat complex process and involves several tables. As an example, a new policy can easily create one or more new records in each of the following tables within the datastore:

- POLICIES
- OBJECTS
- (General object tables relating to each type of object used)
- LINKS
- FOLDERS
- SCHEDULES
- VARIABLES
- COUNTERS

CAUTION: TABLE INFORMATION IS FOR REFERENCE-ONLY

The information provided in this chapter regarding the OIS datastore and its tables is for reference-only. This information is intended to help you better understand policy mechanics and OIS in general. You should never directly manipulate data in the OIS datastore.

Dormant Policy

After the Management Server writes the policy to the datastore, nothing else happens as part of the transaction. The policy is now located within the datastore and visible to other OIS Clients should they look for it, but in terms of execution, the policy is now dormant. The policy has not yet been marked for execution and remains dormant until an OIS Client, Opalis Operator Console (OOC), Command Line executable, or Web Service invocation changes this state.

Starting the Policy

To start a policy that is checked in, someone typically uses the OIS Client and presses the Start button or presses the Start button within the OOC (or through one of the other programmatic start options). Regardless of how the request is initiated, the result is the datastore is updated such that the policy is now marked to start. This happens by updating the record for the policy within several policy related tables via the PublishPolicy stored procedure (the affected tables are POLICY_PUBLISH_QUEUE, POLICY_REQUEST_ACTION_SERVERS, POLICY REQUEST HISTORY, and POLICIES). The first two tables establish which Action Server the policy will run on (if more than one Action Server exists). The final update in the stored procedure alters the Published and Publishing Time columns in the Policies table. This updates the Published column from False to True and adds the current time to the Publishing Time column. (The term Published used by the datastore in this context is now archaic. In early versions of OIS 5.x, the Start button was labeled Publish, and because the database structure has not been fundamentally altered since then, the term Published remains.)

Action Servers and Policy Instantiation

Action Servers are designed to regularly update the datastore to report their heartbeat (every 15 seconds) and check if any new policies need to be executed (every 2 seconds). If there are no policies for the Action Server to run, it closes the connection and will retry in several seconds. However, if the Action Server finds a policy it can run, it gathers all the details about the policies from the related tables and then uses that information to instantiate an executable in memory. The name of the executable is always PolicyModule.exe (or PolicyModule.exe*32 on Windows 2008 systems as the PolicyModule.exe is a 32-bit application).

PolicyModule.exe

The Action Server instantiates one PolicyModule.exe for every submitted request to execute a policy. If a policy does not start with a Monitor object and a Start request is issued more than once, multiple instances of that policy can potentially run concurrently. This means if a given Action Server is running 17 policies, as viewed from the Operator Console, there will be 17 instances of PolicyModule.exe in memory at that time. Both active and idle (or monitoring) policies are in memory as PolicyModule.exe. As policies start, the Process ID (PID) of the policy is recorded to the datastore and is viewable from clients. In this way, a client can use the PID reported through logging to determine which instance of PolicyModule.exe belongs to a given policy.

There are two types of policies:

- Ad hoc
- Monitored

The mechanism is identical to check-in and start either type of policy, although the two behave differently when they execute. These policies are discussed in the following sections.

Policy Behavior (Ad hoc)

An *ad hoc policy* is any policy that does not begin with a monitor object. Ad hoc policies will load into memory as PolicyModule.exe and execute each object within the policy in turn until the policy runs out of objects along its given execution path. After the policy reaches its conclusion, the PolicyModule.exe exits and the policy terminates. An ad hoc policy does not reinstantiate until someone starts the policy again. However, if the policy is not permitted to finish normally (meaning it ends prematurely while there are still more objects along its given execution path)—perhaps caused by a server abend—the Action Server will not report the policy as completed to the datastore. As long as the policy is not reported as completed, the policy runs again (either by the same Action Server or by another if the first has failed or run out of capacity). This behavior is what most users expect when a policy fails.

A policy runs until it is complete; if interrupted before finishing, it will start again. Every policy starts with the first object, regardless of whether it failed previously. It is possible to design a policy to check to see if it previously ended prematurely, reload the relevant data, and start again; however, this is not the default policy behavior. For more information on building restartable policies, see Chapter 7.

Policy Behavior (Monitor)

A *monitored policy* is any policy that begins with a monitor object. (These policies can only contain one monitor object.) Monitored policies are sometimes referred to as *long running policies*. A monitored policy begins like an ad hoc policy, started by a user or external trigger; but because the first object in the policy is a monitor, the conditions of that monitor will dictate when the rest of the policy will trigger.

As an example, if the first object in a monitored policy is a File Monitor configured to wait for a file named datalog.xls to appear in C:\Drop, the policy loads and begins monitoring the C:\Drop folder for datalog.xls. Until that file appears, the remaining objects in the workflow will not run. This policy might stay in memory indefinitely waiting on the desired condition to occur.

After the desired condition occurs, two things take place:

- As soon as the monitor condition for the first object is satisfied, a new PolicyModule.exe instantiates to replace the monitoring activity.
- The policy executes just as an ad hoc job would, following all the objects along its given execution path.

By instantiating a new PolicyModule.exe as soon as the monitor condition is satisfied, the monitoring is constant and uninterrupted. If you are familiar with how a Transmission Control Protocol (TCP) port listener behaves, you can use this as an analogous behavior. As soon as the socket on port 3389 is filled by an incoming Remote Desktop Protocol (RDP) connection, a new socket on the same port is created. Monitored polices behave in a similar fashion.

After a monitored policy is running, it will not stop on its own. The user or an external trigger will have to stop the policy.

In both situations (monitored and ad hoc), the desired outcome of the policy is not the relevant measure. Regardless of whether the desired outcome is success or failure as long as the policy executes all of objects in its path, the Action Server reports the policy as successfully completed. In terms of policy management by the datastore and the Action Servers, this completion is the only one that matters.

Policy Limits and Queuing

The total number of concurrent policies an Action Server will run by default is 50 (ad hoc and monitored combined). This is known as the Action Server Policy Throttle (ASPT), which is set as part of the installation of OIS 6.2.2 and not modified with the 6.3 upgrade. When an Action Server reaches the maximum number of concurrent policies set by the ASPT, it will no longer run additional policies. If there are no other Action Servers available, the policy will queue and wait for resources to become available.

Consider an example using a single Action Server deployment. You have 49 policies running and your ASPT is set to the default of 50. You trigger two policies to start using the OOC. The first policy executes normally and becomes the 50th policy running on your Action Server. The second policy queues in the datastore and waits until one of the 50 running policies completes before it will run.

NOTE: MONITORED POLICIES COUNT AGAINST ASPT

As monitored policies never stop on their own, they take away policy slots from your Action Servers permanently (as long as you choose to run them). In a default configuration, if you have an Action Server with 40 monitored policies running, this only leaves room for 10 ad hoc policies, assuming all 40 monitored policies were idle and had not created new policies to replace them.

Action Server Policy Throttle

The throttle value of 50 is configurable by using aspt.exe found in %ProgramFiles(x86)%\Opalis Software\Opalis Integration Server\Management Service. The aspt executable allows you to change the value on all Action Servers or on a specific Action Server. The following is the usage for this executable:

```
aspt (ActionServerName or *) (MaxRunningPolicies 1-1000)
```

To set the policy throttle limit for all Action Servers to 300, enter the following:

```
aspt * 300
```

After you change the value for the ASPT, you must restart the Action Server service for any Action Server changed.

Maximum Number of Policies to Run

With the default ASPT of 50, a common question is how many policies can actually be run. There are a number of factors dictating how many policies can be run safely on a single Action Server. These factors include the following:

- Desktop Heap
- Operating System
- Policy size and complexity
- CPU and Memory resources

Refer to Chapter 7 for information on sizing.

Desktop Heap Limitations and Policies

The first resource typically fully consumed by an Action Server (especially those running Windows 2003) is not memory or CPU but the desktop heap. There are several heaps on a server, but when dealing with OIS, the heap being referred to is the desktop heap for the non-interactive desktops (desktop heap).

The default of 50 concurrent policies on a single Action Server is to help prevent exhaustion of the desktop heap. If a system runs out of desktop heap, it can experience unexpected runtime issues such as processes terminating and being unable to allocate proper resources to other processes.

NOTE: SPOTTING DESKTOP HEAP ISSUES

There is no single sign the desktop heap has been exhausted, although there are common symptoms that you might encounter. When checking the Action Server logs or the policy logs, you might see errors such as Out of Memory or Not Enough Storage. There might also be other messages that refer to problems allocating Named Pipes or Windows Sockets.

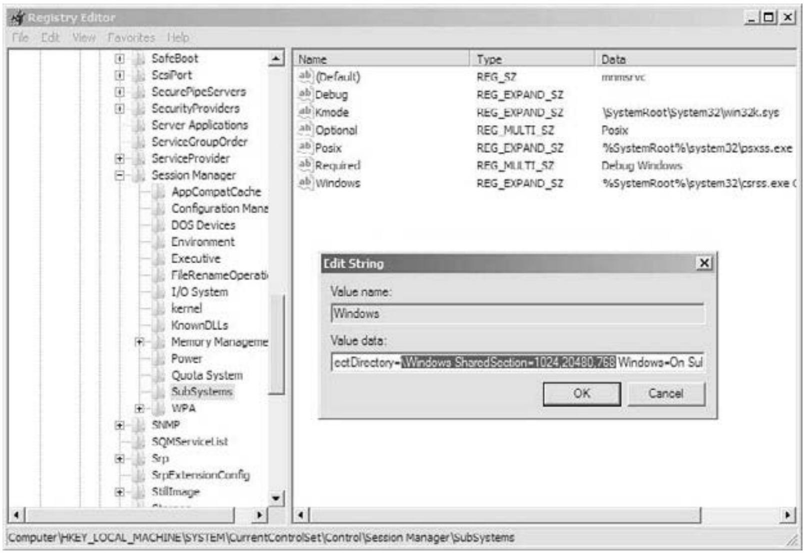
OIS policies all use desktop heap; although they might use different amounts. The amount consumed varies depending on which objects the policy uses and the total number of objects in the policy. The most reliable way to determine the actual consumption of desktop heap by policies is to monitor the resource as a policy runs. If your implementation reaches a steady state, this will give you the best possible estimation of your needs.

Information Technology (IT) organizations often want to have estimates before reaching a steady state„generally when designing the OIS architecture. As a guideline, you can estimate that each policy (policymodule.exe) will consume 10KB of desktop heap.

The desktop heap for the noninteractive desktops is the third parameter of the SharedSection= segment of the following registry value:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\
Session Manager\SubSystems\Windows
```

Figure 3.2 shows the registry location of the desktop heap, highlighting the Shared Windows Section. The value of the desktop heap for the noninteractive desktops is 768 in Windows Server 2008 (Figure 3.2) and 512 on Windows Server 2003.



Name	Type	Data
(Default)	REG_SZ	mmsrvc
Debug	REG_EXPAND_SZ	
Kmode	REG_EXPAND_SZ	\SystemRoot\System32\win32k.sys
Optional	REG_MULTI_SZ	Posix
Posix	REG_EXPAND_SZ	%SystemRoot%\system32\psxss.exe
Required	REG_MULTI_SZ	Debug Windows
Windows	REG_EXPAND_SZ	%SystemRoot%\system32\csrss.exe (

Value name: Windows

Value data: ectDirectory=\Windows SharedSection=1024,20480,768 Windows=On Sul

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems

FIGURE 3.2 The registry location of the desktop heap on Windows 2008

Estimating the Maximum Policy Count and Desktop Heap Size

Before setting the desktop heap, estimate the maximum number of policies you expect an Action Server to run.

The desktop heap for the noninteractive desktops can be estimated by

```
(Maximum # of concurrent policies) * 10 = (Desktop Heaps)
```

As an example, if you want to run 100 concurrent policies, 100 * 10 = 1000, rounding that number to the next highest memory size gives you 1024. The new value for the desktop heap in the registry segment would look like this:

```
SharedSection=1024,20480,1024
```

This example uses the estimate of 10K for a policy. After you have working examples of your policies, determine the actual value for your policies and revise the desktop heap size based on the actual value.

You will also want to consider that because the Service Control Manager creates a new desktop in the noninteractive window station for each service process running under a user account, increasing the desktop heap for non-interactive desktops reduces the number of user account services that can run on the system.

CAUTION: MAXIMUM TOTAL HEAP SIZE 48MB FOR WINDOWS 2003

On Windows 2003, the total desktop heap size must fit into the 48MB systemwide buffer. This means the total for all three heaps must be less that 48MB. On Windows 2008, the heap size is a dynamic kernel address range and not limited by the SessionViewSize.

Noninteractive sessions only have 20MB of the 48MB total available because Terminal Services are automatically enabled—which cuts the 48MB in half to 24MB. In addition, the System Interactive default allocation is 1024 (first value in the Shared attribute) and the Interactive Desktop is 3072 (second value in the Shared attribute), leaving only 20MB for all the noninteractive windows stations. SessionViewSize can be increased on a Windows Server 2003 computer; however, it has potentially significant impacts to other kernel memory resources and is not recommended.

Note that any command line interfaces (CLI) executed by the policies will consume desktop heap in the same Windows station as well. If you are a heavy user of Run Program objects or IPs that utilize CLI applications, consider increasing the 10KB value in your calculations to 15KB to ensure this is taken into account.

Increasing the Action Server's Desktop Heap

To increase the number of policies an Action Server can run, perform the following steps:

1. Increase the size of the desktop heap for noninteractive window stations on your Action Servers.
2. Modify the value of the ASPT on your Action Servers.
3. Reboot the Action Servers. Increasing the desktop heap is a Windows systemwide change and requires a reboot. Altering the ASPT requires you restart the Action Server Service.

You can find additional information about desktop heap in Knowledge Base (KB) article 184802, available at http://support.microsoft.com/kb/184802.

Policy Maximums Based on Operating System

OIS 6.3 Action Servers can run on Windows Server 2003 or 2008; the total number of concurrent policies supported by each operating system (OS) will differ. As the maximum total heap size for a Windows 2003 server is limited to 48MB, Action Servers on Windows 2003 are not able to run as many policies as those on Windows 2008 (assuming the heap size is maximized for each). The exact number of policies you can run should be determined by testing; however, you can use the following guidelines when estimating the maximum number of concurrent policies per Action Server:

- **Windows 2003—**250 concurrent policies
- **Windows 2008—**500 concurrent policies

These are only suggested maximums. Your Action Servers might not be able to run the maximums listed given other constraints. (As an example, if you have large policies, you might not be able to run 250 concurrent policies on a Windows 2003 Action Server.) You might be able to run more policies than these maximums, but if you attempt to do so, be sure you understand the performance aspects and implications involved. Normally, you would want to add more Action Servers rather than risk over committing those Action Servers you have.

NOTE: OIS 6.3 IS A 32-BIT APPLICATION

OIS 6.3 runs on Windows 2008; however, the applications, including policymodule.exe, are 32-bit applications. Because of this, the OIS resources will not be able to take full advantage of the 64-bit operating system.

Policy Size and Complexity

The total number of objects and type of objects in a policy will change the memory footprint and resource consumption considerably. There are no good sizing guidelines, as policies can vary incredibly in size. A four-object policy that creates help desk incidents based on a SQL query easily consumes more resources than a user provisioning policy with 20 objects. Imagine if the SQL query produces 5,000 rows, which in turn creates 5,000 incidents in the help desk. That four-object policy is far more resource intensive than passing one set of user data through the 20-object policy.

CPU and Memory Resources Also Affect Policy Limits

CPU and memory resources and other typical performance metrics are more likely to apply to Windows 2008 Action Servers rather than those running on Windows 2003. The reason for this is Windows 2003 servers are limited to about 250 concurrent policies, and modern server hardware can generally handle that load quite easily. As Windows 2008 can run about twice as many policies, it is possible that normal performance resources might become strained.

All the performance aspects—heap size, operating system, policy size, and performance metrics—should be methodically tested using real-world data. This is the best and most reliable method to understand what impact your policies will have on your Action Servers. The estimates provided in this chapter are only the starting point for your calculations.

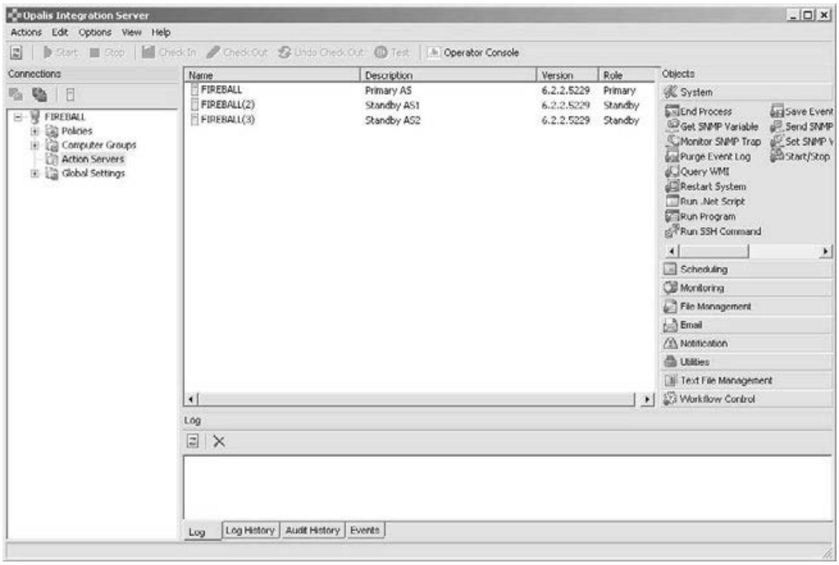
Policy Queuing

The ASPT sets the total number of concurrent policies an Action Server can run. When the ASPT is reached, if there is only one Action Server and it is running the maximum number of policies, any additional policies that are started will be queued. Policies that are queued remain in the queue until a running policy completes its execution, freeing up a policy slot. After there is a free policy slot, the first policy in the queue is instantiated on the Action Server. Policies are taken from the policy queue in a first in, first out (FIFO) model.

Unfortunately, there is no easy way to see how many policies are queued or which policies are queued. Queued policies are stored in the POLICY_PUBLISH_QUEUE table in the database; to determine how many policies were queued, you can view the contents of that table. The OOC policy view totals include queued policies, but there is no way to filter on queued policies as you can with those that are running.

Policy Spillover

When you have more than one Action Server, policies begin executing on the Primary Action Server (PAS), and continue to execute on the PAS until the ASPT for that server is reached. After the PAS reaches its ASPT (and only then), policies begin executing on the Standby Action Server (SAS). The SAS is used only when the PAS reaches its ASPT. As soon as there is at least one free policy slot on the PAS, new policies resume executing there. Figure 3.3 shows the list of Action Servers and their priority, which can be set in the OIS Client.



Name	Description	Version	Role
FIREBALL	Primary AS	6.2.2.5229	Primary
FIREBALL(2)	Standby AS1	6.2.2.5229	Standby
FIREBALL(3)	Standby AS2	6.2.2.5229	Standby

FIGURE 3.3 Action Server priority set by the OIS Client

As an example, if your ASPT is set to 50 for all Action Servers and the PAS is running 50 policies, the next policies that start will run on the SAS. However, if at any point one or more of the PAS's policies complete, the PAS would then be assigned policies again until it again reaches its ASPT.

There is no consideration given to the fact that the SAS might be idle when assigning policies. The PAS must reach its ASPT before policies "spillover" onto the SAS. Should you have more than one SAS, policies begin loading on the PAS, then spillover to the first SAS, and only then to the second SAS. Policies always attempt to load on the highest-ranking Action Server. (You can change the ranking order and role of Action Servers using the OIS Client.)

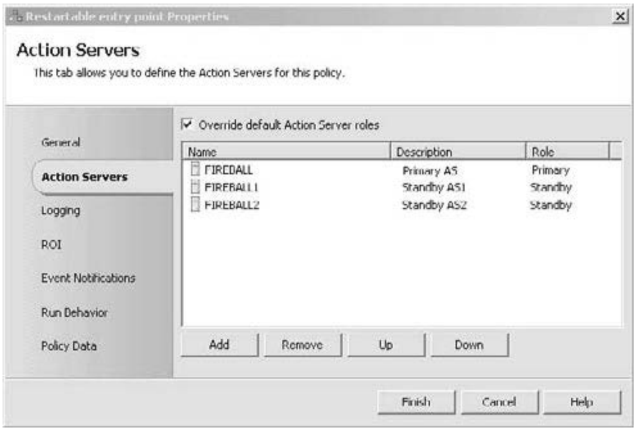
Regardless of how many Action Servers are available, policies will fill the PAS before spilling over to the SAS and will fill the first SAS before spilling over to the second SAS and so on. This is not a load balancing mechanism; it is much more helpful to think about the mechanism as spillover.

After all the Action Servers have reached their ASPT, any additional policies that are started will be queued. These queued policies will run as soon as a policy slot frees up on any of the Action Servers, but will always prefer the highest-ranking Action Server if more than one become free.

Policies Assigned to Specific Action Servers

The only time policy execution does not follow the standard spillover model is when a policy is set to Override Default Action Server Roles. This setting changes which Action Server acts as the PAS and SAS for the context of that specific policy. If a policy is configured to run only on one Action Server, the effect would be the same as running the policy in a single Action Server environment.

Exercise caution when using Override Default Action Server Roles. If a policy is set to run on a specific Action Server and that server has reached its ASPT, the policy must wait for a free policy slot regardless of how many other Action Servers have availability. If more than one Action Server is set using Override Default Action Server Roles, you can configure the rankings between the servers (and those will spill over according to the normal spill over rules), but the policy will run only on Action Servers in that list, even if others are free. Figure 3.4 shows a policy using the Override Default Action Server Roles feature.



Action Servers

This tab allows you to define the Action Servers for this policy.

☑ Override default Action Server roles

Name	Description	Role
FIREDALL	Primary AS	Primary
FIREBALL1	Standby AS1	Standby
FIREBALL2	Standby AS2	Standby

FIGURE 3.4 A Policy that is overriding the default Action Server settings

Policy Failover

When a policy is running and the Action Server where it is running fails, the policy restarts on another Action Server if one exists. When a policy fails over from one Action Server to another, it always restarts at the beginning of the policy, regardless of how many objects might have already completed in the policy that was lost when the Action Server failed.

NOTE: HAVING A POLICY PICK UP WHERE IT LEFT OFF

When a policy starts or is restarted, it always begins with the first object in policy. In some situations, this can be quite problematic, especially when executing the same objects again will cause issues in the infrastructure. In these cases, you can build your policy to check to see if it was running previously and include logic to determine what step it was on and then jump to the appropriate step. This will require a good deal of customization, but it is certainly possible.

Deployment Models

There are a number of ways to deploy OIS in your environment. However, most implementations of OIS will fit into a small set of deployment models. The following sections will list the most common models for deploying OIS, explain where each model is best suited, and present the relative advantages and disadvantages of each.

Simple Deployment

The simple deployment model is the simplest and most basic deployment model for OIS. This model has all the OIS components installed on one server and can use either an existing SQL server or it might also have SQL running on the OIS server. Figure 3.5 shows a diagram of a simple OIS deployment.

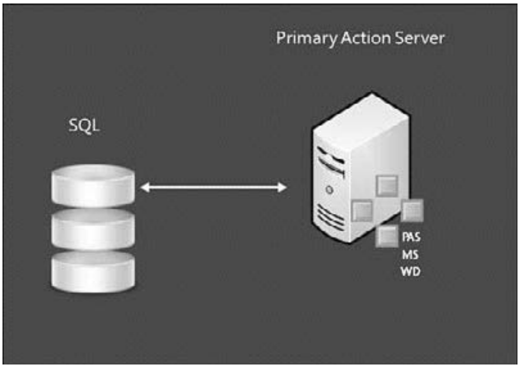


FIGURE 3.5 Simple deployment model

This model is best suited for a proof of concept, or a limited pilot, and you can use it in a testing environment. However, the simple deployment model is not recommended for a production environment, as it does not provide any fault tolerance for the OIS components. In this model, you normally install all the OIS components on a single server and use an existing SQL instance to host the OIS datastore. If the datastore is also installed on the OIS server, the entire system is at risk if there is a failure.

Here are advantages of this model:

- Simplest model to install and configure
- Can run every component on a single server or virtual machine (VM)
- Limits licensing required

Here are the disadvantages:

- Does not provide policy failover
- All automation stops when server is offline
- Becomes a single point of failure especially if SQL is installed on the same server

Resilient Deployment

The resilient deployment model is most commonly used. This model is suitable from small businesses to large enterprises. The resilience is provided by having two or more Action Servers and clustering SQL Server. In this model the OIS components, the datastore, and automation targets are all on a centralized high-speed network.

For the purposes of this book, a centralized high-speed network is one in which average communication takes place in less than 50ms, and there is little or no data loss. Figure 3.6 shows a diagram of a resilient deployment model.

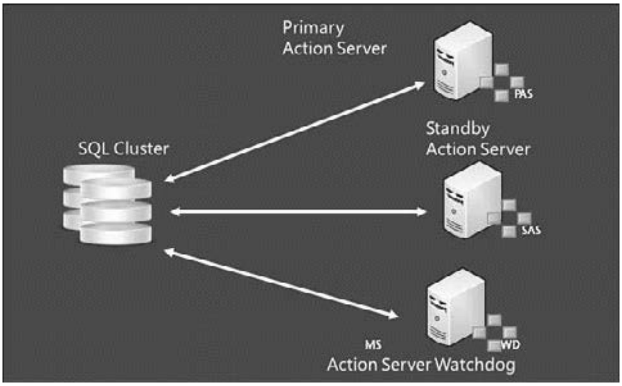


FIGURE 3.6 Resilient deployment model

NOTE: USE N+1 FOR ALL IMPLEMENTATION MODELS

This model, as with all those that follow, should use an *N*+1 formula to determine how many Action Servers are required (where *N* = the total number of Action Servers required to handle your maximum policy load). This provides an extra Action Server to take the policy load of any other Action Server that might fail.

This model is well suited for any implementation where the OIS components, datastore, and automation targets are all a centralized high-speed network.

Here are advantages of this model:

- Provides policy failover by having multiple Action Servers
- Provides resilient SQL through SQL clustering
- Provides a separate server to run the Action Server Watchdog service and provides alerting if an Action Server should fail
- Offers greater flexibility with additional Action Servers

Here are disadvantages:

- Additional resource demands because of extra Action Servers
- Additional resource demands from SQL clustering
- Additional management burden

Cross-Network Deployment

The cross-network deployment model is one in which Action Servers can reach across the network to perform automation on targets. This model is suitable for mid-size businesses or enterprises where remote sites have targets that require automation and are connected by a high-speed remote network, but these remote sites are ones in which it would be impractical or impossible to deploy an Action Server. Resilience is provided by having two or more Action Servers and by clustering SQL. In this model, the OIS components and the datastore are all on a centralized high-speed network and the automation targets are on high-speed remote networks.

For the purposes of this book, a high-speed remote network is one in which average communication takes places in less than 200ms, and there is little or no data loss. Figure 3.7 shows a diagram of a cross-network deployment model.

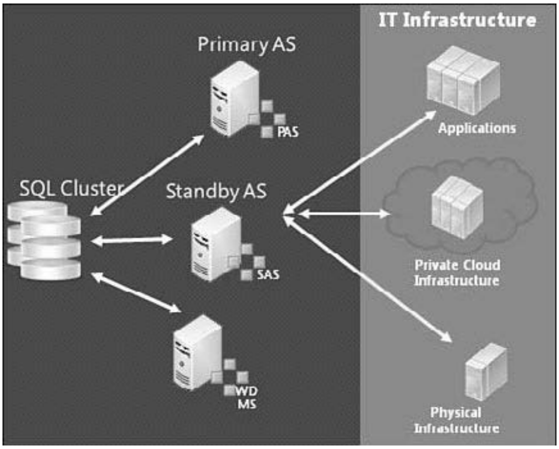


FIGURE 3.7 Cross-network deployment model

CAUTION: NOT ALL OBJECTS WILL PERFORM PROPERLY IN THIS MODEL

The cross-network model requires the remote automation target be within a 200ms latency bubble with the Action Server, but it is critical to note not every object within OIS will tolerate these connection latencies. If you want to implement this model, you will need to test the policies in your environment to confirm the objects do not timeout before they complete their primary functions.

This model is suited for any implementation where the OIS components and datastore are on a centralized high-speed network and where automation targets are on high-speed remote networks. Because not all objects will work over a remote network (see the "Caution" note in this section), this model might not be possible in every environment where it is desired.

Here are advantages of this model:

- Provides policy failover by having multiple Action Servers
- Allows Action Servers to reach into other networks to perform automation, especially when the Action Server cannot be placed in the remote network
- Provides resilient SQL through SQL clustering
- Provides a separate server to run the Action Server Watchdog service and provides alerting if an Action Server should fail
- Offers greater flexibility with additional Action Servers

Here are disadvantages:

- Additional resource demands because of extra Action Servers.
- Additional resource demands from SQL clustering.
- Not all policy objects can tolerate this model.
- Requires additional configuration of firewalls to allow traffic from any of the objects used to pass between sites.
- Additional management burden.

Cross-Network Action Servers

The cross-network action server model is one in which Action Servers are placed on a remote network to perform automation on targets there. This model is suitable for midsize businesses or enterprises where remote sites have targets that require automation and they are connected by a high-speed remote network; these remote sites are ones in which it is possible deploy an Action Server. Resilience is provided by having two or more Action Servers and by clustering SQL. In this model, the Management Server, Action Server Watchdog, and the datastore are all on a centralized high-speed network, and the Action Servers are on high-speed remote networks with the automation targets. Figure 3.8 shows a diagram of a cross-network action server model.

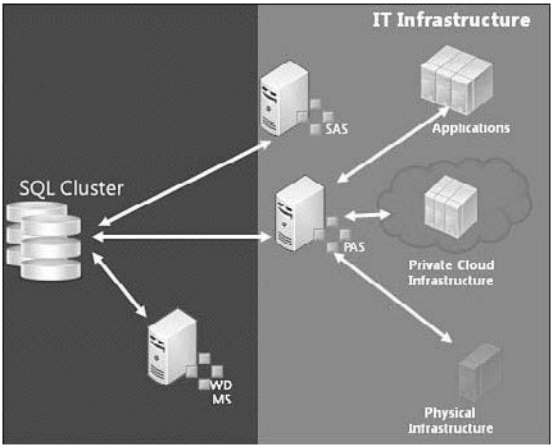


FIGURE 3.8 Deployment with Action Servers across networks

This model is suited for any implementation where the Management Server, Action Server Watchdog, and datastore are on a centralized high-speed network and where the Action Servers can be placed on the same high-speed remote network where the automation targets are located. This model requires that the remote network latency be less than 200ms. There must be little or no data loss; otherwise, this model will fail. Latency speeds in the 10-30ms range are recommended.

Here are advantages of this model:

- Provides policy failover by having multiple Action Servers
- Allows Action Servers to reside on remote networks to perform automation, assuming the network performance allows this
- Provides resilient SQL through SQL clustering
- Provides a separate server to run the Action Server Watchdog service and provides alerting if an Action Server should fail
- Can be used in some environments where the cross-network deployment model cannot

Here are disadvantages:

- Additional resource demands because of extra Action Servers
- Additional resource demands from SQL clustering
- Action Servers will tolerate only excellent network conditions in this model; without excellent conditions they will lose connectivity to the datastore
- Requires additional configuration of firewalls to allow SQL traffic between the sites
- Additional management burden

Multisite Manual Policy Sync

In some environments, the network performance will not be suitable to separate Action Servers from the datastore. If this is the case, it will be necessary to have one installation of the OIS components, including the datastore, at each location that requires automation. OIS installations are always standalone, and they will not communicate natively or share any data between installations (even when on the same network).

A multisite manual policy sync model is one where two or more installations of OIS are in use and there is a requirement or desire to use the policies on all installations. Because these installations will not be able to communicate with one another natively, policies that need to be shared must be exported manually and imported at the target OIS installation. This model provides a method to transfer policies but not policy data. Figure 3.9 shows a diagram of multisite manual policy synchronization.

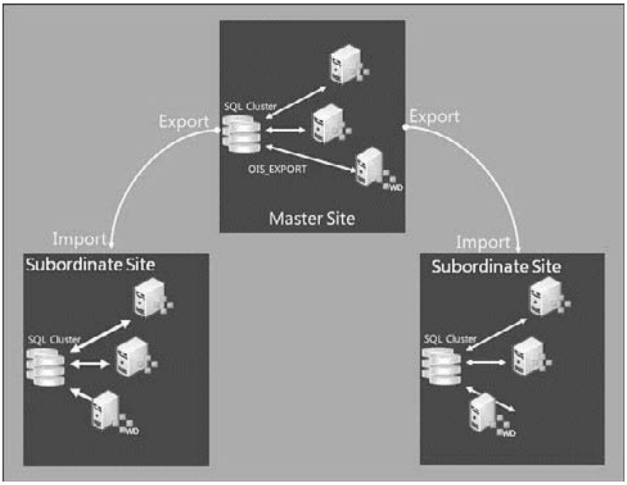


FIGURE 3.9 Manual policy sync model

NOTE: USE CARE WHEN IMPORTING POLICIES

There are a number of considerations when importing policies from other installations, just as when you promote a policy from testing to production. Refer to Chapter 7 for information.

This model is best suited for environments where network conditions require several installations of OIS and these installations need to transfer policies with one another. Using a manual process to transfer policies between is not a desirable solution given the effort involved, but if more than one installation is required, there is no other way to transfer the policies.

Here are advantages of this model:

- Provides a method for using the same policies on remote OIS installations
- Can provide uniform automation to several remote sites
- Has all the advantages of a resilient model
- Offers flexibility in what policies are loaded to which installation

Here are disadvantages:

- No policy or state data is shared between installations
- Requires manual effort to import or export policies
- Installations have potential to become out of sync with one another

Multisite Invoke via Web Services

In some environments, the network performance will not be suitable for Action Servers to be separate from the datastore. In this case, it will be necessary to have one installation of the OIS components, including the datastore, at each location that requires automation. OIS installations are always standalone and will not communicate natively.

A multisite invoke via Web Services model is one where the OIS installations communicate with one another over Web Services during custom policy execution. By installing the OOC, taking advantage of the Web Services, and building custom policies to use these components, you can have two standalone instances of OIS trade data or call actions on one another. Figure 3.10 shows a diagram of a multisite model using Web Services invocation.

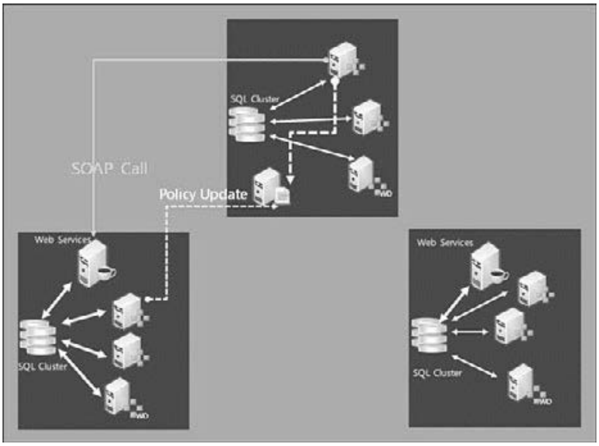


FIGURE 3.10 Multisite invoke via Web Services

This model is best suited for environments where data needs to be shared between OIS installations or where one OIS installation provides a critical service to others (such as trouble ticket creation).

Here are advantages of this model:

- Allows policies to interact with remote installations and networks
- Allows OIS data to be shared between remote installations
- Has all the advantages of a resilient model
- Allows any networked OIS instance to trigger a specific function on another OIS instance
- Offers flexibility in having differing policies at different locations
- Allows policy execution across untrusted environments by providing credentials at the connection point using the Invoke Web Services object

Here are disadvantages:

- Requires special development of all policies to accept or transfer data
- Requires the Operator Console be installed on target OIS systems
- At risk for failure if network connection is lost

Multisite Hybrid Solution

The multisite hybrid solution is a combination of both the multisite manual sync and the invoked Web Services model. It provides a method to use the same policies in separate installations while also allowing those installations to communicate with one another at runtime and share data. Figure 3.11 shows a diagram of a multi-site hybrid solution.

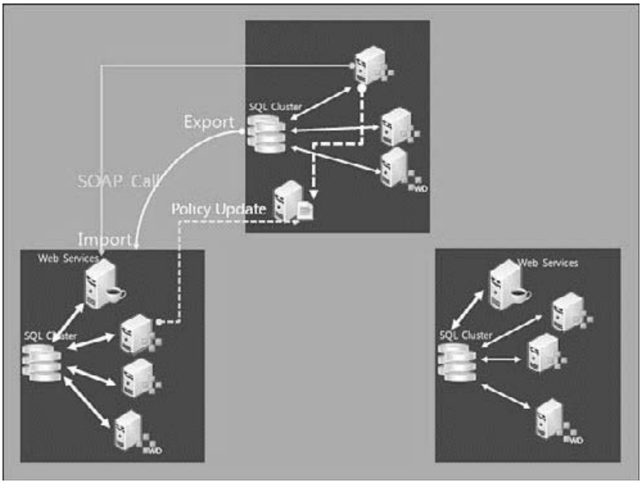


FIGURE 3.11 Multisite hybrid solution

This model is best suited for environments where data needs to be shared between OIS installations or where one OIS installation provides a critical service to others (such as trouble ticket creation) while also providing common policies to multiple installations.

Here are advantages of this model:

- Provides a method for using the same policies on remote OIS installations
- Can provide uniform automation to several remote sites
- Has all the advantages of a resilient model
- Allows policies to interact with remote installations and networks
- Allows OIS data to be shared between remote installations
- Offers flexibility in what policies are loaded to which installation

Here are disadvantages:

- Requires special development of all policies to accept or transfer data
- Requires the OOC be installed on target OIS systems
- Requires manual effort to import or export
- At risk for failure if network connection is lost
- Installations have potential to become out of sync with one another

Multisite Isolated Deployment

If your environment's network performance is not suitable to separate your Action Servers from the datastore or security limitations make this a necessity, but you still need automation on remote sites, you will use an isolated deployment. In this situation, you will need to use a multisite isolated deployment model. This model is simply several unrelated installations that share no information or policy imports. Figure 3.12 shows a diagram of an isolated multisite OIS deployment model.

This model is used only when there is no desire or no way to share data or policies between installations. This model is rarely used.

Here are advantages of this model:

- Each installation is highly available
- Provides resilient SQL through SQL clustering
- Has all the advantages of a resilient model
- Provides a separate server to run the Action Server Watchdog service and provides alerting if an Action Server should fail

Here are disadvantages:

- No data is shared between installations
- All policies are designed and implemented separately

- Additional maintenance burden
- No policies are shared between installations

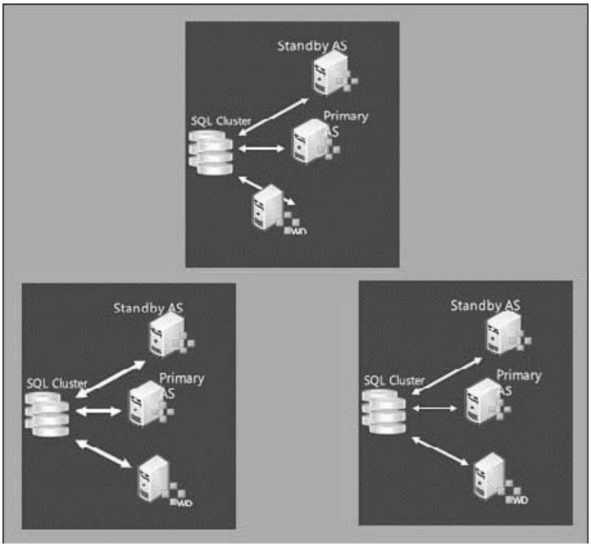


FIGURE 3.12 Isolated multisite OIS model

Security Models

There are a number of security models to use with your OIS implementation. The following sections list the most common security models for OIS implementations and explain the limitations of each model. The discussion does not list advantages or disadvantages, as the existing security infrastructure is not likely to change because of the addition of OIS.

Single Domain Security

The single domain security model is where all OIS components are used within a single Active Directory domain. This is the normal model used by most installations and the one for which OIS was primarily designed. There are no special considerations for using this model; the account used by Action Server service is the default privilege for all policies and should not present any challenges because all the resources are within the same domain. Figure 3.13 shows a diagram of a single domain security model.

Federated Domains

The federated domain security model is where all OIS components are used within a single Active Directory domain but the Action Servers act against automation targets in a second domain for which a trust relationship exists. This model is less common, although used by some organizations. The only considerations for using this model are that the account used by Action Server service has appropriate rights on the target systems by virtual of the trust relationship. Other than the trust itself, this model is essentially the same as the single domain Model. Figure 3.14 shows a diagram of a federated domain security model.

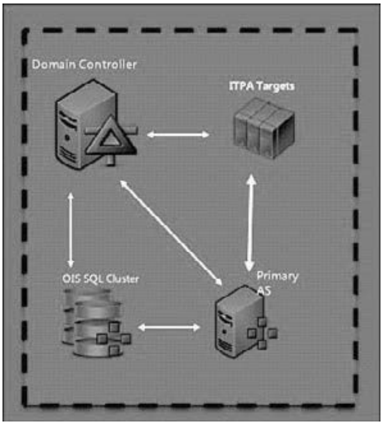


FIGURE 3.13 Single domain security

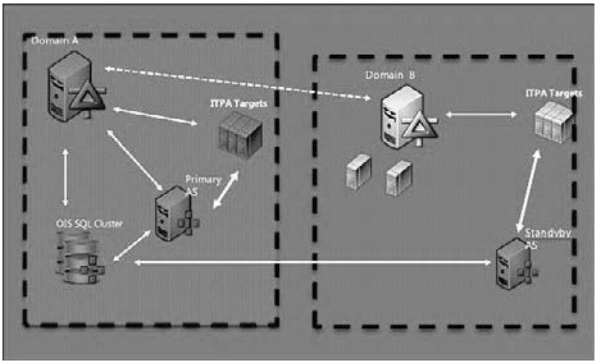


FIGURE 3.14 Federated domains

Untrusted Security Model

The untrusted security model is where two domains exist but there is no trust between them. Both domains require automation and require their own installations of OIS. Generally, this is an undesirable configuration for OIS as the two installations are needed because of a lack of trust. It might be possible to carry out some limited automation across untrusted domains using impersonation or by specifying credentials from the other domain, but this is a challenging configuration. Figure 3.15 shows a diagram of an untrusted security model.

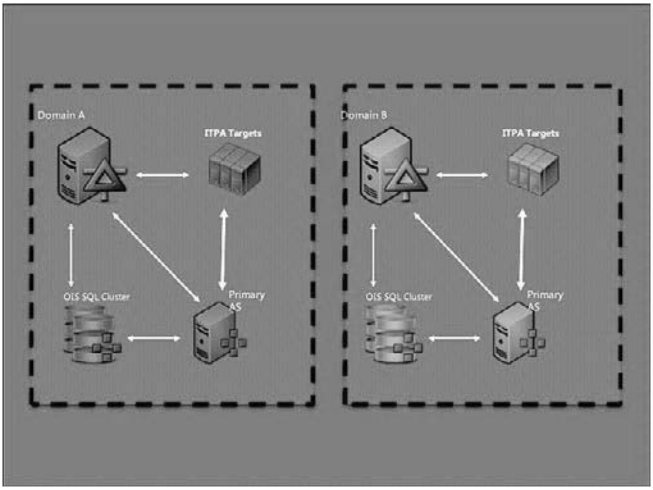


FIGURE 3.15 Untrusted security model

Summary

This chapter covered various aspects of OIS architecture. You learned about the lifecycle of a policy and what happens when a policy is started for both monitored policies and ad hoc policies. In addition, this chapter described how the various aspects of Action Server spillover and policy throttling behavior. It also provided a number of architectural models used for deploying OIS and the security models that might be used. In Chapter 4, •Installing Opalis Integration Server 6.3,Ž you will learn all the steps necessary to install OIS and the OOC.

Index

A

accessing OOC (Opalis Operator Console), 140

Action Server Policy Throttle (ASPT), 60

Action Server section (OIS Client Connections window), 117-118

Action Server view (OOC), 142

Action Server Watchdog Service, as required component, 32. *See also* OpalisActionServerWatchdog

Action Servers, 39-45

- clustering, 484-485
- connectivity, 40-43
- cross-network Action Servers deployment model, 70-71
- installation, 94-97
- number needed, 484
- OpalisActionService, 39-40
- policy failover, 66-67
- policy lifecycle
  - policy instantiation, 58
  - PolicyModule.exe, 58-59
- policy limits
  - desktop heap limitations, 61-63
  - operating system limitations, 63-64
- policy spillover, 65-66
- PolicyModule.exe, 43-44
- redundancy, 44-45
- as required components, 32
- service account, 82

Action Servers tab (policy properties), 147-148

ad hoc policies, 58-59, 214-215

Add Computer to Collection object, 335

Add/Edit Parameter dialog, CLI Wizard (QIK), 422-424

adding

link filters, 134-135

Published Data (PD) to Data Bus, 137-139

Advanced tab (object properties)

Invoke Web Services object, 168

Run .Net Script object, 165-166

Run Program object, 160-161

Run SSH Command object, 172

Send Email object, 174-176

Advertise Task Sequence object, 336

advertising software use case, SCCM IP, 344-345

Allow Empty Comment on Check In option (OIS Client), 126

Alternate Icon tab (object properties), 155-156

API for QIK SDK, 434

Append Line object, 182

Apply XSLT object, 194

architecture design. *See also* components of OIS (Opalis Integration Server)

deployment models, 67-76

cross-network Action Servers, 70-71

cross-network deployment, 69-70

multisite hybrid solution, 74-75

multisite invoke via Web Services, 73-74

multisite isolated deployment, 75-76

multisite manual policy sync, 72-73

resilient deployment, 68-69

simple deployment, 67-68

policy failover, 66-67

policy lifecycle, 56-59

check in, 56-57

dormant policy, 57

policy instantiation, 58

PolicyModule.exe, 58-59

starting policy, 57-58

policy limits, 60-64

ASPT (Action Server Policy Throttle), 60

CPU and memory resource limitations, 64

desktop heap limitations, 61-63

maximum running policies, 60-61

operating system limitations, 63-64

policy size and complexity, 64

policy queueing, 64-65

policy spillover, 65-66

security models, 76-77

federated domains, 76-77

single domain security, 76

untrusted security, 77

Arguments tab (Add/Edit Command dialog), CLI Wizard (QIK), 421-422

ASPT (Action Server Policy Throttle), 60

aspt.exe utility, 33

Assembly Details screen, CLI Wizard (QIK), 416

Assembly Information screen, CLI Wizard (QIK), 417-419

atlc.exe utility, 33

Audit History window (OIS Client), 124

Audit Trail, file system locations, 473

Authoring Console. *See* OIS Client

Automatic Check Out option (OIS Client), 125

automating change use case, SCSM IP, 323-330

automation

Microsoft automation platform, 8-11

Data Bus, 9

flexibility of, 9-10

ITPA (Information Technology Process Automation), 10-11

after OIS acquisition, 8-9

prior to OIS acquisition, 8

results of, 11

in OIS (Opalis Integration Server), 6

AVIcode, product description, 12

B

background executables, in product footprint (OIS), 476-477

backing up policies, 229-230

backup management, OIS (Opalis Integration Server) integration with, 14

Basic PD, 137

best practices

- backing up policies, 229-230
- complex link logic, 210-211
- data manipulation and parsing, 216-221
  - data manipulation functions, 217-218
  - Query Database object, 219
  - Run .Net Script object, 219-221
- error handling, 222-225
- external data persistence, 231-235
- hardcoded versus dynamic data, 221-222
- looping, 212-213
  - object-level looping, 212-213
  - policy-level looping, 213
- naming conventions, 226-227
- permissions, 225-226
- promotion, 230-231
- scheduling, 214-216
  - applying to policies, 214-216
  - Check Schedule object, 214
- versioning, 228-229

BladeLogic Operations Manager IP, 238-240

“Blank” variable, 119

blogs for information, 500

BMC Atrium CMDB IP, 240-243

BMC Event Manager IP, 243-244

BMC Patrol IP, 245-247

BMC Remedy AR System IP, 247-249

BPA (Business Process Automation), 24-25

BPM (Business Process Management), 24-25

branch office maintenance mode use case, SCOM IP, 309-312

branching policies, 134-136

- adding filters, 134-135
- default filter, 134
- include/exclude filters, 135

breakpoints, setting, 131

bulk processing in dynamic data center, 382

bulk user account provisioning use case, 391-394

Business Process Automation (BPA), 24-25

Business Process Management (BPM), 24-25

C

CA AutoSys IP, 250-252

CA eHealth IP, 252-254

CA Spectrum IP, 254-256

CA Unicenter NSM IP, 256-257

CA Unicenter Service Desk IP, 257-259

CAP (Connector Access Pack), 18

capacity and lifecycle management use case, VMM IP, 363-366

categories of OIS components, 30-31

change management

- in dynamic data center, 382
- OIS (Opalis Integration Server) integration with, 13

check in, in policy lifecycle, 56-57

Check Schedule object, 192, 214

checking compliance use case, SCCM IP, 341-344

checking DPM server storage capacity use case, DPM IP, 378-379

checking policies in/out, 132

CLI scripting support, in QIK (Quick Integration Kit), 399

CLI Wizard (QIK), 415-432

- Add/Edit Parameter dialog, 422-424
- Arguments tab (Add/Edit Command dialog), 421-422

Assembly Details screen, 416

Assembly Information screen, 417-419

Command Line syntax, 424-426

Commands screen, 419-421

Published Data tab (Add/Edit Command dialog), 426-430

client user interface for OIS (Opalis Integration Server), 6. *See also* OIS Client

close resolved incidents use case, SCSM IP, 318-320

clustering Action Servers, 484-485

CMDBs, 26

“code or script” objects, 154

Command Line syntax, CLI Wizard (QIK), 424-426

Command mode, Program mode versus, 160

Commands screen, CLI Wizard (QIK), 419-421

Common PD, 137-138

Compare Values object, 194

complex link logic, 210-211

components of OIS (Opalis Integration Server), 29-32, 55. *See also* architecture design

Action Servers, 39-45

categories of, 30-31

Management Server, 48-52

OIS Client, 45-48

Opalis Operator Console (OOC), 52-54

optional components, 31, 471-473

required components, 32, 470-471

SQL Datastore, 32-39

trace logging, 493

versions of, 488-489

Compress File object, 193

Computer Groups section (OIS Client Connections window), 117

configuration management, OIS (Opalis Integration Server) integration with, 13

Configuration Manager. *See also* SCCM IP

OIS (Opalis Integration Server) integration with, 13

product description, 12

as SCCM IP requirement, 332

configuration objects in SQL Datastore, 33-34

configuration settings

BladeLogic Operations Manager IP, 239-240

BMC Atrium CMDB IP, 242-243

BMC Event Manager IP, 244

BMC Patrol IP, 247

BMC Remedy AR System IP, 249

CA AutoSys IP, 251-252

CA eHealth IP, 253-254

CA Spectrum IP, 256

CA Unicenter NSM IP, 257

CA Unicenter Service Desk IP, 259

EMC Smarts InCharge IP, 261-262

HP Asset Manager IP, 263-264

HP iLO and OA IP, 265

HP Network Node Manager IP, 267-268

HP OpenView Operations HPUX IP, 269-270

HP OpenView Operations Solaris IP, 272

HP OpenView Operations Windows IP, 274-275

HP OpenView Service Desk IP, 277

HP Service Manager IP, 279-280

IBM Tivoli Enterprise Console IP, 281-282

IBM Tivoli Netcool Omnibus IP, 284

IBM Tivoli Storage Manager IP, 286

Microsoft Active Directory 2 IP, 289

Unix IP, 292-293

Veritas NetBackup IP, 294

VMware vSphere IP, 297

configuring

DPM IP, 369-370

objects, 127-128

QIK objects, 458-461

SCCM IP, 332-335

SCOM IP, 300-301

SCSM IP, 314-315

VMM IP, 348-350

Connect tab (object properties), Send Email object, 174-176

Connection account

- SCCM IP
  - creating, 332-333
  - granting access to, 333-334
- SCOM IP
  - configuring, 301
  - granting access to, 301
- VMM IP
  - configuring, 349-350
  - granting access to, 349

Connection tab (object properties), Query Database object, 161-163

Connections window (OIS Client), 116-120

- Action Server section, 117-118
- Computer Groups section, 117
- Global Settings section, 118-120
- Policies section, 116-117

connectivity

- of Action Servers, 40-43
- SCCM IP requirements, 335
- SCOM IP requirements, 300
- VMM IP requirements, 348

Connector Access Pack (CAP), 18

connectors, ITPA (Information Technology Process Automation) versus, 28

Copy File object, 182

counters, 118, 184-187

- Get Counter Value object, 185-186
- Modify Counter object, 185
- Monitor Counter object, 186-187
- as semaphores, 118

CPU limitations, policy limits, 64

Create Advertisement object, 336

Create Alert object, 303

Create Change with Template object, 316

Create Checkpoint object, 352

Create Collection object, 336

Create Disk from VHD object, 352

Create Folder object, 183

Create Incident with Template object, 316

Create Network Adapter object, 352

Create New Disk object, 352

Create Object object, 316

Create Recovery Point object, 371

Create Related Object object, 316

Create Relationship object, 316

Create VM from Template object, 353

Create VM from VHD object, 353

Create VM from VM object, 353

creating a recovery point use case, DPM IP, 372-375

creating and populating a collection use case, SCCM IP, 338-341

cross-network Action Servers deployment model, 70-71

cross-network deployment model, 69-70

Custom Start object, 145, 178

D

Data Bus, 9, 484

- Published Data (PD) on, 136-140
  - adding, 137-139
  - subscribing to, 139-140
  - types of, 139

Data Center Integration, 17

data centers

- dynamic data center
  - bulk user account provisioning use case, 391-394
  - requirements, 382-383
  - server maintenance and reboot use case, 383-386

virtual machine provisioning and configuration use case, 386-391

transformation with System Center Suite, 14-15

data manipulation and parsing, 216-221

data manipulation functions, 217-218

Query Database object, 219

Run .Net Script object, 219-221

data persistence, 231-235

Data Protection Manager. *See also* DPM IP

as DPM IP requirement, 368

OIS (Opalis Integration Server) integration with, 14

product description, 12

Database Configuration Utility, 33

database integration, troubleshooting, 483

datastore. *See* SQL Datastore

Declarative model (QIK SDK), 435, 437-442

Decompress File object, 193

default filter, 134

Delete Collection object, 336

Delete File object, 183

Delete Folder object, 183

Delete Line object, 182

Delete Relationship object, 316

dependencies, OIS 6.3 installation, 79-80

Dependencies screen (QIK Wizard), 450-451

Deploy Software Update object, 337

deploying IPs (Integration Packs), 102-104

Deployment Manager, 33

Action Server installation, 94-97

IP (integration pack) installation, 99-104

OIS 6.3 installation, 94

OIS Client installation, 97-99

deployment models, 67-76

for Action Servers, 42-43

cross-network Action Servers, 70-71

cross-network deployment, 69-70

multisite hybrid solution, 74-75

multisite invoke via Web Services, 73-74

multisite isolated deployment, 75-76

multisite manual policy sync, 72-73

resilient deployment, 68-69

simple deployment, 67-68

deployment styles in QIK (Quick Integration Kit), 399, 456-467

production mode deployment, 462-467

test mode deployment, 456-461

desktop heap limitations, 61-63

Details tab (object properties), 154-155

Custom Start object, 178

Get Counter Value object, 185-186

Invoke Web Services object, 167-168

Junction object, 179-180

Modify Counter object, 185

Monitor Counter object, 186-187

Publish Policy Data object, 180

Query Database object, 161-163

Query WMI object, 170

Run .Net Script object, 164-165

Run Program object, 159-160

Run SSH Command object, 171

Send Email object, 174-176

Send Event Log Message object, 176-177

Send Platform Event object, 176

Trigger Policy object, 178-179

development methods in QIK (Quick Integration Kit), 398

disaster recovery, OIS (Opalis Integration Server) integration with, 14

Disconnect Network Path object, 194

Do Not Exit tab (object-level looping), 213

documentation

folder location in QIK installation, 408-409

of processes, 26-27

dormant policy, 57

downloading

OIS 6.3 installation media, 83-84

OOC installation files, 107

DPM IP

configuring, 369-370

objects, 370-372

requirements, 367-368

use cases, 372-379

checking DPM server storage capacity, 378-379

creating a recovery point, 372-375

protecting a data source, 375

recovering a SQL database, 375-378

dragging and dropping objects, 127

dynamic data center

requirements, 382-383

use cases

bulk user account provisioning, 391-394

server maintenance and reboot, 383-386

virtual machine provisioning and configuration, 386-391

dynamic versus hardcoded data, 221-222

E

email and notification objects, 174-177

Send Email object, 174-176

Send Event Log Message object, 176-177

Send Platform Event object, 176

EMC Smarts InCharge IP, 260-262

End Process object, 192

environment variable setup, OOC installation, 108

%ENVVAR% variable, 119

error handling, 222-225, 382

Event Notifications tab (policy properties), 149

events in OOC (Opalis Operator Console), 144

Events window (OIS Client), 121-122

examples, folder location in QIK installation, 409-410

exclude filters, 135

executables, folder location in QIK installation, 406-407

Execution mode, Run Program object, 161

Exit tab (object-level looping), 212-213

exporting

policies, 151

policy groups, 151

policy XML exports, 229-230

extensibility objects, 157-173

Invoke Web Services object, 167-168

Query Database object, 161-163

Query WMI object, 169-170

Run .Net Script object, 163-166

Run Program object, 158-161

Run SSH Command object, 170-172

SNMP objects, 172-173

external data persistence, 231-235

extracting files, OOC installation, 108-109

F

federated domains security model, 76-77

File Information Data Storage, Foundation objects use case, 196-197

file management objects, 181-184, 193

file system for OIS files, 469-473

Filter Email object, 191

filters. *See* link filters

Find Text object, 194

"flattened objects do not produce multi-value data" policy engine rule, 205-206

flattening multi-value PD items, 207-208

flexibility of OIS (Opalis Integration Server), 9-10

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

folder locations, QIK (Quick Integration Kit) installation, 406-410

footprint (OIS). *See* product footprint (OIS)

Format Date/Time object, 194

Foundation objects, 153. *See also* objects

- anatomy of, 153-156
- counters, 184-187
  - Get Counter Value object, 185-186
  - Modify Counter object, 185
  - Monitor Counter object, 186-187
- email and notification objects, 174-177
  - Send Email object, 174-176
  - Send Event Log Message object, 176-177
  - Send Platform Event object, 176
- extensibility objects, 157-173
  - Invoke Web Services object, 167-168
  - Query Database object, 161-163
  - Query WMI object, 169-170
  - Run .Net Script object, 163-166
  - Run Program object, 158-161
  - Run SSH Command object, 170-172
  - SNMP objects, 172-173
- Legacy objects, 187-191
  - alternate usage, 188-189
  - Filter Email object, 191
  - Process Email object, 191
  - Read Email object, 190
  - Wait object, 189-190
- miscellaneous objects, 191-194
  - file management objects, 193
  - monitoring objects, 193
  - notification objects, 194
  - scheduling objects, 192
  - system objects, 192
  - text file management objects, 194
  - utilities, 194
- properties, 154
- text and file management objects, 181-184
- troubleshooting, 486-488
- use cases, 195-199
  - File Information Data Storage, 196-197
  - password reset and service account synchronization, 195
  - ticketing system synchronization, 195-196
  - Web Services TerraServer Querying, 197
  - Windows Event Scan with Query WMI, 198-199
- workflow control objects, 177-181
  - Custom Start object, 178
  - Junction object, 179-180
  - Publish Policy Data object, 180-181
  - Trigger Policy object, 178-179

functions, data manipulation, 217-218

G

General tab

- object properties, 155
- policy properties, 147

Generate Random Text object, 194

Get Activity object, 317

Get Advertisement Status object, 337

Get Alert object, 303

Get Checkpoint object, 353

Get Collection Member object, 337

Get Computer/IP Status object, 193

Get Counter Value object, 185-186

Get Data Source object, 371

Get Disk object, 353

Get Disk Space Status object, 193

Get DPM Server Capacity object, 371

Get File Status object, 183

Get Internet Application Status object, 193

Get Lines object, 182

Get Monitor object, 303-304

Get Network Adapter object, 353-354

Get Object object, 317

Get Process Status object, 193

Get Recovery Point object, 371

Get Relationship object, 317

Get Service Status object, 193

Get SNMP Variable object, 173

Get Software Update Compliance object, 337

Get VM object, 354

global configuration, QIK objects, 456-458

Global Settings section (OIS Client Connections window), 118-120

groups of policies, exporting, 151

H

haltable/restartable policies, 232-235

hardcoded versus dynamic data, 221-222

history

- of ITPA (Information Technology Process Automation), 24-27
- of Opalis Software, 15-22
  - challenges in transition to Microsoft, 21-22
  - introduction of OIS, 18-21
  - Microsoft acquisition of, 21
  - OpalisRendezVous, 15-16
  - OpalisRobot, 15, 16-18

HP Asset Manager IP, 262-264

HP iLO and OA IP, 264-265

HP Network Node Manager IP, 266-268

HP OpenView Operations HPUX IP, 268-270

HP OpenView Operations Solaris IP, 272

HP OpenView Operations Windows IP, 273-275

HP OpenView Service Desk IP, 275-277

HP Service Manager IP, 278-280

I

IBM Tivoli Enterprise Console IP, 280-282

IBM Tivoli Netcool Omnibus IP, 282-284

IBM Tivoli Storage Manager IP, 284-286

IDE, QIK (Quick Integration Kit) installation, 410-415

Imperative model (QIK SDK), 436, 442-445

impersonation, Action Servers and, 42

importing policies, 151-152

incident remediation use case, SCOM IP, 305-307

incident/change management, OIS (Opalis Integration Server) integration with, 13

include filters, 135

Information Technology Process Automation (ITPA), 10-11

- connectors versus, 28
- history of, 24-27
- process review, 27-28
- transition to, 19

Insert Line object, 182

installation

- BladeLogic Operations Manager IP, 239
- BMC Atrium CMDB IP, 242
- BMC Event Manager IP, 244
- BMC Patrol IP, 246
- BMC Remedy AR System IP, 248-249
- CA AutoSys IP, 250
- CA eHealth IP, 253
- CA Spectrum IP, 255
- CA Unicenter NSM IP, 257
- CA Unicenter Service Desk IP, 258
- EMC Smarts InCharge IP, 261
- HP Asset Manager IP, 263
- HP iLO and OA IP, 265
- HP Network Node Manager IP, 267
- HP OpenView Operations HPUX IP, 269

HP OpenView Operations Solaris IP, 271-272
HP OpenView Operations Windows IP, 274
HP OpenView Service Desk IP, 277
HP Service Manager IP, 279
IBM Tivoli Enterprise Console IP, 281
IBM Tivoli Netcool Omnibus IP, 283
IBM Tivoli Storage Manager IP, 285
Microsoft Active Directory 2 IP, 288
OIS 6.3
Action Server installation, 94-97
database creation and population, 87-90
dependencies, 79-80
Deployment Manager, 94
downloading installation media, 83-84
IP (integration pack) installation, 99-104
licensing, 90-92
Management Server installation, 85-87
manual installation, 105-106
OIS Client installation, 97-99
OOC installation, 106-113
patching, 93-94
requirements, 80-83
running installer, 84-85
troubleshooting, 113-114
QIK (Quick Integration Kit), 401-415
folder locations, 406-410
IDE, 410-415
IPs (Integration Packs), 415
requirements, 401-402
running installer, 402-405
SCOM IP, 300
Unix IP, 291
Veritas NetBackup IP, 293-294
VMware vSphere IP, 297

installation objects in SQL Datastore, 33-34

integer variables, counters as, 184

integration
in OIS (Opalis Integration Server), 6
options for, 397-398

Integration Packs (IPs). *See* IPs (Integration Packs)

Invoke .NET object,

Invoke Web Services object, 167-168

IPs (Integration Packs)
BladeLogic Operations Manager IP, 238-240
BMC Atrium CMDB IP, 240-243
BMC Event Manager IP, 243-244
BMC Patrol IP, 245-247
BMC Remedy AR System IP, 247-249
CA AutoSys IP, 250-252
CA eHealth IP, 252-254
CA Spectrum IP, 254-256
CA Unicenter NSM IP, 256-257
CA Unicenter Service Desk IP, 257-259
creating, with QIK (Quick Integration Kit), 445-455
described, 237-238
DPM IP
configuring, 369-370
objects, 370-372
requirements, 367-368
use cases, 372-379
EMC Smarts InCharge IP, 260-262
folder location in QIK installation, 407
HP Asset Manager IP, 262-264
HP iLO and OA IP, 264-265
HP Network Node Manager IP, 266-268
HP OpenView Operations HPUX IP, 268-270
HP OpenView Operations Solaris IP-272
HP OpenView Operations Windows IP, 273-275
HP OpenView Service Desk IP, 275-277
HP Service Manager IP, 278-280
IBM Tivoli Enterprise Console IP, 280-282

- IBM Tivoli Netcool Omnibus IP, 282-284
- IBM Tivoli Storage Manager IP, 284-286
- installation, 99-104
- licensing, 238
- Microsoft Active Directory 2 IP, 286-289
- QIK (Quick Integration Kit) installation, 415
- SCCM IP
  - configuring, 332-335
  - objects, 335-338
  - requirements, 331-332
  - use cases, 338-345
- SCOM IP
  - configuring, 300-301
  - installation, 300
  - objects, 302-305
  - requirements, 299-300
  - use cases, 305-312
- SCSM IP
  - configuring, 314-315
  - objects, 315-317
  - requirements, 313-314
  - use cases, 317-330
- Standard OIS Logging IP, 234-235
- troubleshooting, 482-483
- Unix IP, 289-293
- Veritas NetBackup IP, 293-294
- VMM IP
  - configuring, 348-350
  - objects, 351-355
  - requirements, 347-348
  - use cases, 355-366
- VMware vSphere IP, 295-297

ITIL (Information Technology Infrastructure Library), 26

ITPA (Information Technology Process Automation), 10-11
- connectors versus, 28
- history of, 24-27
- process review, 27-28
- transition to, 19

J

Java
- installation, 108
- OOC installation dependency, 80
- support in QIK (Quick Integration Kit), 399

JAVA_HOME environment variable, OOC installation, 108

Java/JBOSS Web Service, as optional component, 31

JBoss, OOC installation dependency, 80

job schedulers, OIS (Opalis Integration Server) versus, 28

Junction object, 179-180, 204-205, 208-209

"Junction object limits or truncates PD stream" policy engine rule, 204-205

L

legacy mode, pipeline mode versus, 209-210

Legacy objects, 187-191
- alternate usage, 188-189
- Filter Email object, 191
- Process Email object, 191
- Read Email object, 190
- Wait object, 189-190

License Manager, 33

licensing
- IPs (Integration Packs), 238
- OIS 6.3 installation, 90-92
- troubleshooting, 482

limits. *See* policy limits

link filters, 134-136
- adding, 134-135
- default filter, 134
- include/exclude filters, 135

link handles, 126-127

links
- complex link logic, 210-211
- creating, 128
- defined, 127
- "links filter execution data" policy engine rule, 204
- properties, 136

"links filter execution data" policy engine rule, 204

Live Links, 503-504

locale settings, as SCSM IP requirement, 314

log history, 489-492

Log History window (OIS Client), 123

log purging, 491-492

Log window (OIS Client), 122-123

logging levels, 492-494

Logging tab (policy properties), 148

logs, viewing
- in OIS Client, 133
- in PTC, 130

looping, 212-213
- object-level looping, 212-213
- policy-level looping, 213

M

maintenance mode, PowerShell scripts for, 503

Manage Checkpoint object, 354

manage incidents use case, SCSM IP, 320-322

Management Server, 48-52
- additional components, 50-52
- installation, 85-87
- OpalisActionServerWatchdog, 49-50
- policy lifecycle, check in, 56-57
- primary services, 48-49
- as required component, 32
- service account, 82

manual OIS 6.3 installation, 105-106

Map Network Path object, 194

Map Published Data object, 194

maximum running policies, 60-61

memory resource limitations, policy limits, 64

methods for policy execution process, 36

Microsoft
- acquisition of Opalis Software, 5, 21-22
- automation platform, 8-11
  - Data Bus, 9
  - flexibility of, 9-10
  - ITPA (Information Technology Process Automation), 10-11
  - after OIS acquisition, 8-9
  - prior to OIS acquisition, 8
  - results of, 11
- OIS resources for information, 496-498
- Opalis forums, 501

Microsoft Active Directory 2 IP, 286-289

Modify Counter object, 185

Monitor Alert object, 304

Monitor Computer/IP object, 193

Monitor Counter object, 186-187

Monitor Date/Time object, 192

Monitor Disk Space object, 193

Monitor Event Log object, 193

Monitor File object, 183

Monitor Folder object, 183, 193

Monitor Internet Application object, 193

Monitor .NET object, 458

Monitor Object object, 317

Monitor Process object, 193

Monitor Service object, 193

Monitor SNMP Trap object, 173

Monitor State object, 304

Monitor WMI object, 193

monitored policies, 59, 60, 216

monitoring objects, 126, 193

Move File object, 193

Move Folder object, 193

Move VM object, 354

multiplication effect (policy engine), 209-210

multisite hybrid solution deployment model, 74-75

multisite invoke via Web Services deployment model, 73-74

multisite isolated deployment model, 75-76

multisite manual policy sync deployment model, 72-73

multi-value PD items

- "flattened objects do not produce multi-value data" policy engine rule, 205-206
- flattening, 207-208
- handling, 206-207
- "run once for each multi-value PD item" policy engine rule, 203-204

N

naming conventions, 226-227

navigating OIS Client, 115-116

- Audit History window, 124
- Connections window, 116-120
- Events window, 121-122
- Log History window, 123
- Log window, 122-123
- Objects window, 120-121
- Options menu, 124-126
- Workspace window, 120

nesting data manipulation functions, 218

.NET attributes in QIK (Quick Integration Kit), 435

.NET support in QIK (Quick Integration Kit), 398

notification objects, 174-177, 194

- Send Email object, 174-176
- Send Event Log Message object, 176-177
- Send Platform Event object, 176

NOW() variable, 119

O

OBJECTINSTANCEDATA table (OIS datastore), 38

object-level looping, 212-213

objects. *See also* Foundation objects

- in BladeLogic Operations Manager IP, 239
- in BMC Atrium CMDB IP, 241
- in BMC Event Manager IP, 244
- in BMC Patrol IP, 246
- in BMC Remedy AR System IP, 248
- in CA AutoSys IP, 250-251
- in CA eHealth IP, 253
- in CA Spectrum IP, 254-255
- in CA Unicenter NSM IP, 257
- in CA Unicenter Service Desk IP, 258
- configuring, 127-128
- defined, 126
- in DPM IP, 370-372
- dragging and dropping, 127
- in EMC Smarts InCharge IP, 260-261
- in HP Asset Manager IP, 262-263
- in HP iLO and OA IP, 264
- in HP Network Node Manager IP, 266
- in HP OpenView Operations HPUX IP, 268-269
- in HP OpenView Operations Solaris IP, 270-271
- in HP OpenView Operations Windows IP, 273-274

in HP OpenView Service Desk IP, 275-277
in HP Service Manager IP, 278-279
in IBM Tivoli Enterprise Console IP, 280-281
in IBM Tivoli Netcool Omnibus IP, 283
in IBM Tivoli Storage Manager IP, 285
link handles, 126-127
links
creating, 128
defined, 127
properties, 136
in Microsoft Active Directory 2 IP, 287-288
monitor objects, 126
QIK object deployment, 456-467
production mode deployment, 462-467
test mode deployment, 456-461
QIK project process, 436
"run as often as object before you" policy engine rule, 202
"run once for each multi-value PD item" policy engine rule, 203-204
in SCCM IP, 335-338
in SCOM IP, 302-305
in SCSM IP, 315-317
in Unix IP, 290-291
in Veritas NetBackup IP, 293
in VMM IP, 351-355
in VMware vSphere IP, 295-296

Objects window
OIS Client, 120-121
QIK Wizard, 448-450

Object-Specific PD, 138-139

oedc.exe utility, 33

OIP files. *See* IPs (Integration Packs)

OIS (Opalis Integration Server)
advantages of, 7-8
automation, orchestration, integration in, 6
client user interface, 6
components, 29-32, 55
Action Servers, 39-45
categories of, 30-31
Management Server, 48-52
OIS Client, 45-48
Opalis Operator Console (OOC), 52-54
optional components, 31, 471-473
required components, 32, 470-471
SQL Datastore, 32-39
trace logging, 493
versions of, 488-489
history of Opalis Software, 15-22
challenges in transition to Microsoft, 21-22
introduction of OIS, 18-21
Microsoft acquisition of, 21
OpalisRendezVous, 15-16
OpalisRobot, 15, 16-18
job schedulers versus, 28
product description, 12
product footprint, 469-477
background executables, 476-477
in datastore, 477
file system, 469-473
Registry structure, 473-475
running processes/services, 475
Start Menu programs, 475-476
purpose of, 5-8
resources for information, 495-501
SCO (System Center Orchestrator) versus, 23-24
in System Center Suite, 11-12
troubleshooting
common questions, 482-488
policy troubleshooting, 477-482
workflows versus policies, 7

OIS 5.0, 18

OIS 6.0, 19-20

OIS 6.2.2, 20-21, 80

OIS 6.3, 22

as DPM IP requirement, 367

installation

Action Server installation, 94-97

database creation and population, 87-90

dependencies, 79-80

Deployment Manager, 94

downloading installation media, 83-84

IP (integration pack) installation, 99-104

licensing, 90-92

Management Server installation, 85-87

manual installation, 105-106

OIS Client installation, 97-99

OOC installation, 106-113

patching, 93-94

requirements, 80-83

running installer, 84-85

troubleshooting, 113-114

as SCCM IP requirement, 331

as SCOM IP requirement, 299

as SCSM IP requirement, 313

as VMM IP requirement, 347

OIS Client, 45-48

connection to OIS datastore, 47

installation, 97-99

navigating, 115-116

Audit History window, 124

Connections window, 116-120

Events window, 121-122

Log History window, 123

Log window, 122-123

Objects window, 120-121

Options menu, 124-126

Workspace window, 120

operating system support, 46

policies

checking in/out, 132

creating, 126-128

starting, 132-133

viewing logs, 133

as policy authoring utility, 34-36

policy creation process, 47-48

policy lifecycle

check in, 56-57

starting policy, 57-58

PTC (Policy Testing Console) versus, 131-132

as required component, 32

OIS datastore. *See* SQL Datastore

OIS Testing Console, troubleshooting, 482

online content available, 503-504

OOC (Opalis Operator Console), 52-54, 140

accessing, 140

Action Server view, 142

events, 144

file system locations, 472

installation, 106-113

configuring as service, 113

downloading files, 107

environment variable setup, 108

extracting files, 108-109

Java installation, 108

PowerShell script, 110-111

securing, 111

testing, 111-113

troubleshooting, 113-114

Java and JBoss dependency, 80

as optional component, 31

permissions, 142-144

policies

searching for, 142

starting/stopping, 141

viewing execution of, 141-142

troubleshooting, 485-486

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

Opalis forums, 501

Opalis Integration Pack File screen (QIK Wizard), 451-452

Opalis Integration Server. *See* OIS (Opalis Integration Server)

Opalis Operator Console (OOC). *See* OOC (Opalis Operator Console)

Opalis Software, history of, 15-22

- challenges in transition to Microsoft, 21-22
- introduction of OIS, 18-21
- Microsoft acquisition of, 5, 21
- OpalisRendezVous, 15-16
- OpalisRobot, 15, 16-18

OpalisActionServerWatchdog, 48, 49-50. *See also* Action Server Watchdog Service

OpalisActionService, 39-40. *See also* Action Servers

OpalisManagementService, 48, 49. *See also* Management Server

OpalisRemotingService, 48, 49

OpalisRendezVous, 15-16

OpalisRobot, 15, 16-18, 484

operating system limitations, policy limits, 63-64

operating system support for OIS Client, 46

Operations Manager. *See also* SCOM IP

- OIS (Opalis Integration Server) integration with, 14
- product description, 12
- as SCOM IP requirement, 299

optional components, 31, 471-473

Options menu (OIS Client), 124-126

orchestration in OIS (Opalis Integration Server), 6

Orchestrator. *See* SCO (System Center Orchestrator)

P

parsing data, 216-221

- data manipulation functions, 217-218
- Query Database object, 219
- Run .Net Script object, 219-221

PAS (Primary Action Server), policy spillover, 65-66

password reset and service account synchronization, Foundation objects use case, 195

patching

- OIS (Opalis Integration Server) integration with, 13
- OIS 6.3 installation, 93-94

Pause VM object, 355

PD. *See* Published Data (PD)

performance monitoring, OIS (Opalis Integration Server) integration with, 14

permissions

- for Action Servers, 41-42
- list of, 225-226
- for OOC (Opalis Operator Console), 142-144

persistence, 231-235

PGP Decrypt File object, 193

PGP Encrypt File object, 193

pic.exe utility, 34

pipeline mode, legacy mode versus, 209-210

planning QIK (Quick Integration Kit) projects, 400

policies

- applying schedules to, 214-216
- automatic import/export, 484
- best practices
  - backing up policies, 229-230
  - complex link logic, 210-211
  - data manipulation and parsing, 216-221
  - error handling, 222-225
  - external data persistence, 231-235

hardcoded versus dynamic data, 221-222

looping, 212-213

naming conventions, 226-227

permissions, 225-226

promotion, 230-231

scheduling, 214-216

versioning, 228-229

branching, 134-136

adding filters, 134-135

default filter, 134

include/exclude filters, 135

checking in/out, 132

creating, 126-128

configuring objects, 127-128

dragging and dropping objects, 127

link handles, 126-127

linking objects, 128

links, 127

monitor objects, 126

objects, 126

execution. *See* policy engine

exporting, 151

exporting groups of, 151

importing, 151-152

log history, 489-492

log purging, 491-492

properties, 147-150

Action Servers tab (policy properties), 147-148

Event Notifications tab (policy properties), 149

General tab (policy properties), 147

Logging tab (policy properties), 148

Policy Data tab (policy properties), 149-150

Run Behavior tab (policy properties), 149

running in PTC, 130

searching for, 142

starting, 132-133, 141

stepping through, 130-131

stopping, 141

testing, 129-132

triggering, 145-147

Custom Start object, 145

Trigger Policy object, 146-147

troubleshooting, 477-482

use cases. *See* use cases

viewing execution of, 141-142

viewing logs, 133

workflows versus, 7

Policies section (OIS Client Connections window), 116-117

POLICIES table (OIS datastore), 35

policy authoring objects in SQL Datastore, 34-36

policy complexity, 64

policy creation process in OIS Client, 47-48

Policy Data tab (policy properties), 149-150

policy engine, 201-202

Junction object, 208-209

multiplication effect, 209-210

multi-value PD items

flattening, 207-208

handling, 206-207

pipeline mode, legacy mode versus, 209-210

rules, 202-206

“flattened objects do not produce multi-value data”205-206

“Junction object limits or truncates PD stream”204-205

“links filter execution data”204

“run as often as object before you”202

“run once for each multi-value PD item”203-204

policy execution objects in SQL Datastore, 36-37

policy failover, 66-67

policy history and log objects in SQL Datastore, 38-39

policy instantiation, 58

policy lifecycle, 56-59

- check in, 56-57
- dormant policy, 57
- policy instantiation, 58
- PolicyModule.exe, 58-59
- release processes, importance of, 56, 83
- starting policy, 57-58

policy limits, 60-64

- ASPT (Action Server Policy Throttle), 60
- CPU and memory resource limitations, 64
- desktop heap limitations, 61-63
- maximum running policies, 60-61
- operating system limitations, 63-64
- policy size and complexity, 64

policy queueing, 64-65

policy size, 64

policy spillover, 65-66

Policy Testing Console (PTC), 129-132

- OIS Client versus, 131-132
- running policies, 130
- setting breakpoints, 131
- stepping through policies, 130-131
- viewing logs, 130

policy XML exports, 229-230

POLICY_PUBLISH_QUEUE table (OIS datastore), 36

policy-level looping, 213

PolicyModule.exe, 43-44, 58-59. *See also* policy engine

PowerShell script

- for maintenance mode, 503
- OOC installation, 110-111

prerequisites. *See* requirements

Primary Action Server (PAS), policy spillover, 65-66

Print File object, 193

Process Email object, 191

processes

- documentation of, 26-27
- reviewing, 27-28
- running processes/services, in product footprint (OIS), 475

Product Details screen (QIK Wizard), 446-448

product footprint (OIS), 469-477

- background executables, 476-477
- in datastore, 477
- file system, 469-473
- Registry structure, 473-475
- running processes/services, 475
- Start Menu programs, 475-476

production mode deployment, QIK objects, 462-467

Program mode, Command mode versus, 160

programming language support in QIK (Quick Integration Kit), 398-399

programming models for QIK SDK, 435-436

promoting policies, 230-231

Prompt for Comment on Check In option (OIS Client), 126

properties

- Foundation objects, 154
- of links, 136
- of policies, 147-150
  - Action Servers tab (policy properties), 147-148
  - Event Notifications tab (policy properties), 149
  - General tab (policy properties), 147
  - Logging tab (policy properties), 148
  - Policy Data tab (policy properties), 149-150
  - Run Behavior tab (policy properties), 149

Protect Data Source object, 371

protecting a data source use case, DPM IP, 375

PTC (Policy Testing Console), 129-132

- OIS Client versus, 131-132
- running policies, 130
- setting breakpoints, 131
- stepping through policies, 130-131
- viewing logs, 130

public forums, 501

Publish Policy Data object, 180-181

Published Data (PD)

- on Data Bus, 136-140
  - adding, 137-139
  - subscribing to, 139-140
  - types of, 139
- "Junction object limits or truncates PD stream" policy engine rule, 204-205
- multi-value PD items
  - "flattened objects do not produce multi-value data" policy engine rule, 205-206
  - flattening, 207-208
  - handling, 206-207
  - "run once for each multi-value PD item" policy engine rule, 203-204

Published Data tab

- Add/Edit Command dialog, CLI Wizard (QIK), 426-430
- object properties, Run.Net Script object, 164-165

Purge Event Log object, 192

Q

QIK (Quick Integration Kit)

- CLI Wizard, 415-432
  - Add/Edit Parameter dialog, 422-424
  - Arguments tab (Add/Edit Command dialog), 421-422
  - Assembly Details screen, 416
  - Assembly Information screen, 417-419
  - Command Line syntax, 424-426
  - Commands screen, 419-421
  - Published Data tab (Add/Edit Command dialog), 426-430
- deployment styles, 399
- development methods, 398
- file system locations, 471-472
- installation, 401-415
  - folder locations, 406-410
  - IDE, 410-415
  - IPs (Integration Packs), 415
  - requirements, 401-402
  - running installer, 402-405
- IPs (Integration Packs), creating, 445-455
- object deployment, 456-467
  - production mode deployment, 462-467
  - test mode deployment, 456-461
- planning projects, 400
- programming language support, 398-399
- SDK, 432-445
  - API, 434
  - code samples, 437-445
  - features and functionality, 433
  - programming models, 435-436
  - project process, 436
  - requirements, 433

QIK Wizard, 445-455

- Dependencies screen, 450-451
- Objects screen, 448-450
- Opalis Integration Pack File screen, 451-452
- Product Details screen, 446-448

Query Database object, 161-163, 219

Query WMI object, 169-170

Query XML object, 194

queuing policies, 64-65

Quick Integration Kit (QIK). ***See*** **QIK (Quick Integration Kit)**

R

RBA (Runbook Automation), 16-17, 25

Read Email object, 190

Read Line object, 182

Read Text Log object, 194

Recover SharePoint object, 372

Recover SQL object, 372

Recover VM object, 372

recovering a SQL database use case, DPM IP, 375-378

redundancy

- of Action Servers, 44-45
- SQL Datastore, 230

Refresh Client object, 337

Refresh Collection object, 338

registering IPs (Integration Packs), 100-101

Registry structure, 473-475

release processes, importance of, 56, 83

Remote Trigger, file system locations, 472-473

Remove VM object, 354

Rename File object, 193

Repair VM object, 354

required components, 32

- Action Servers, 39-45
  - connectivity, 40-43
  - OpalisActionService, 39-40
  - PolicyModule.exe, 43-44
  - redundancy, 44-45
- file system locations, 470-471
- Management Server, 48-52
  - additional components, 50-52
  - OpalisActionServerWatchdog, 49-50
  - primary services, 48-49
- OIS Client, 45-48
  - connection to OIS datastore, 47
  - operating system support, 46
  - policy creation process, 47-48
- Opalis Operator Console (OOC), 52-54
- SQL Datastore, 32-39
  - installation and configuration objects, 33-34
  - policy authoring objects, 34-36
  - policy execution objects, 36-37
  - policy history and log objects, 38-39

requirements. ***See also*** **required components**

- DPM IP, 367-368
- dynamic data center, 382-383
- OIS 6.3 installation, 80-83
  - server requirements, 80-81
  - trusted accounts, 83
  - user account requirements, 81-82
- QIK (Quick Integration Kit) installation, 401-402
- QIK SDK, 433
- SCCM IP, 331-332, 335
- SCOM IP, 299-300
- SCSM IP, 313-314
- VMM IP, 347-348

resilient deployment model, 68-69

resources for information, 495-501, 503-504

Restart System object, 192

restartable policies, 232-235

Resume VM object, 354

reviewing processes, 27-28

rules, policy engine, 202-206

- “flattened objects do not produce multi-value data”205-206
- “Junction object limits or truncates PD stream”204-205
- “links filter execution data”204
- “run as often as object before you”202
- “run once for each multi-value PD item” 203-204

"run as often as object before you" policy engine rule, 202

Run Behavior tab

object properties, 155

policy properties, 149

Run .Net Script object, 163-166, 219-221

"run once for each multi-value PD item" policy engine rule, 203-204

Run Program object, 42, 158-161

Run SSH Command object, 170-172

Runbook Automation (RBA), 16-17, 25

running

OIS 6.3 installer, 84-85

policies in PTC, 130

QIK (Quick Integration Kit) installer, 402-405

running processes/services, in product footprint (OIS), 475

S

sanitized policies

defined, 231

steps in, 231

SAS (Standby Action Server), policy spillover, 65-66

Save Event Log object, 192

SCCM IP

configuring, 332-335

objects, 335-338

requirements, 331-332

use cases, 338-345

advertising software, 344-345

checking compliance, 341-344

creating and populating a collection, 338-341

schedules, 120, 214-216

applying to policies, 214-216

Check Schedule object, 214

scheduling objects, 192

SCO (System Center Orchestrator), OIS (Opalis Integration Server) versus, 23-24

SCOM 2007, as SCOM IP requirement, 299

SCOM IP

configuring, 300-301

installation, 300

objects, 302-305

requirements, 299-300

use cases, 305-312

branch office maintenance mode, 309-312

incident remediation, 305-307

server maintenance mode, 307-309, 383-386

SCSM IP

configuring, 314-315

objects, 315-317

requirements, 313-314

use cases, 317-330

automating change, 323-330

close resolved incidents, 318-320

manage incidents, 320-322

SDK for QIK (Quick Integration Kit), 432-445

API, 434

code samples, 437-445

features and functionality, 433

folder location in QIK installation, 406

programming models, 435-436

project process, 436

requirements, 433

Search and Replace Text object, 182

searching for policies, 142

security

OOC installation, 111

release processes, importance of, 56, 83

security credentials, as VMM IP requirement, 348

Security Credentials tab (object properties), 155, 161

security models, 76-77

federated domains, 76-77

single domain security, 76

untrusted security, 77

Security tab (object properties), Invoke Web Services object, 168

semaphores, counters as, 118, 184

Send Email object, 174-176

Send Event Log Message object, 176-177

Send Page object, 194

Send Platform Event object, 176

Send SNMP Trap object, 173

Send Syslog Message object, 194

server maintenance mode use case, SCOM IP, 307-309, 383-386

server requirements, OIS 6.3 installation, 80-81

service accounts

Action Servers, 82

Management Server, 82

password reset and service account synchronization use case, 195

Service Manager. *See also* SCSM IP

OIS (Opalis Integration Server) integration with, 13

product description, 12

as SCSM IP requirement, 314

services

configuring OOC as, 113

running processes/services, in product footprint (OIS), 475

Set SNMP Variable object, 173

Show Legacy Objects option (OIS Client), 125

Show Link Labels option (OIS Client), 124

Show Tooltips option (OIS Client), 125

Shut Down VM object, 354

simple deployment model, 67-68

single domain security model, 76

SNMP objects, 172-173

software deployment, OIS (Opalis Integration Server) integration with, 13

solution areas

backup management, OIS integration with, 14

configuration management, OIS integration with, 13

incident/change management, OIS integration with, 13

performance monitoring, OIS integration with, 14

in System Center Suite, 11-12

virtualization, OIS integration with, 13

SQL Datastore, 32-39

database creation and population, 87-90

installation and configuration objects, 33-34

OIS Client connection to, 47

policy authoring objects, 34-36

policy execution objects, 36-37

policy history and log objects, 38-39

product footprint (OIS) in, 477

redundancy, 230

as required component, 32

Standard OIS Logging IP, 234-235

Standby Action Server (SAS), policy spillover, 65-66

Start Maintenance Mode object, 304

Start Menu programs, in product footprint (OIS), 475-476

Start VM object, 354

starting policies, 57-58, 132-133, 141

Start/Stop Service object, 192

state information, maintaining, 231-235

stepping through policies, 130-131

Stop Maintenance Mode object, 304

Stop VM object, 354

stopping policies, 141

stored procedures

for log purging, 38-39

for OIS datastore data modification, 35-36

for policy execution process, 36-37

subscribing to Published Data on Data Bus, 139-140

System Center Configuration Manager IP. *See* SCCM IP

System Center Data Protection Manager IP. *See* DPM IP

System Center Operations Manager IP. *See* SCOM IP

System Center Orchestrator. *See* SCO (System Center Orchestrator)

System Center Service Manager. *See* SCSM IP

System Center Suite

- data center transformation with, 14-15
- products in, 11-12
- resources for information, 501

System Center Virtual Machine Manager IP. *See* VMM IP

system objects, 192

T

tables

- for policy authoring process, 34-35
- for policy execution process, 36
- for policy logging process, 38

technical support. *See* resources for information; troubleshooting

test mode deployment, QIK objects, 456-461

- configuring, 458-461
- global configuration, 456-458

testing. *See also* release processes

- OOC installation, 111-113
- policies, 129-132
- troubleshooting, 482

text file management objects, 181-184, 194

ticketing system synchronization, Foundation objects use case, 195-196

trace logging, logging levels, 492-494

Trigger Policy object, 146-147, 178-179

triggering policies, 145-147

- Custom Start object, 145
- Trigger Policy object, 146-147

troubleshooting

- Foundation objects, 486-488
- OIS (Opalis Integration Server)
  - common questions, 482-488
  - policy troubleshooting, 477-482
- OIS 6.3 installation, 113-114
- OOC (Opalis Operator Console), 485-486
- resources for information, 495-501

trusted accounts, OIS 6.3 installation, 83

U

Unix IP, 289-293

"Unknown Object" error, troubleshooting, 483-484

untrusted security model, 77

Update Activity object, 317

Update Alert object, 304

Update Disk object, 355

Update Network Adapter object, 355

Update Object object, 317

Update VM object, 355

Upload Attachment object, 317

URLs for information, 495-501

use cases

- BladeLogic Operations Manager IP, 238
- BMC Atrium CMDB IP, 240
- BMC Event Manager IP, 243
- BMC Patrol IP, 245
- BMC Remedy AR System IP, 248
- CA AutoSys IP, 250
- CA eHealth IP, 252-253

CA Spectrum IP, 254

CA Unicenter NSM IP, 256

CA Unicenter Service Desk IP, 257-258

DPM IP, 372-379

checking DPM server storage capacity, 378-379

creating a recovery point, 372-375

protecting a data source, 375

recovering a SQL database, 375-378

EMC Smarts InCharge IP, 260

Foundation objects, 195-199

File Information Data Storage, 196-197

password reset and service account synchronization, 195

ticketing system synchronization, 195-196

Web Services TerraServer Querying, 197

Windows Event Scan with Query WMI, 198-199

HP Asset Manager IP, 262

HP iLO and OA IP, 264

HP Network Node Manager IP, 266

HP OpenView Operations HPUX IP, 268

HP OpenView Operations Solaris IP, 270

HP OpenView Operations Windows IP, 273

HP OpenView Service Desk IP, 275

HP Service Manager IP, 278

IBM Tivoli Enterprise Console IP, 280

IBM Tivoli Netcool Omnibus IP, 282-283

IBM Tivoli Storage Manager IP, 284

Microsoft Active Directory 2 IP, 286-287

SCCM IP, 338-345

advertising software, 344-345

checking compliance, 341-344

creating and populating a collection, 338-341

SCOM IP, 305-312

branch office maintenance mode, 309-312

incident remediation, 305-307

server maintenance mode, 307-309, 383-386

SCSM IP, 317-330

automating change, 323-330

close resolved incidents, 318-320

manage incidents, 320-322

Unix IP, 289-290

Veritas NetBackup IP, 293

VMM IP, 355-366

capacity and lifecycle management, 363-366

virtual machine provisioning, 356-359, 386-391

VM checkpoint and recovery, 360-363

VMware vSphere IP, 295

user account requirements, OIS 6.3 installation, 81-82

user interface for OIS (Opalis Integration Server), 6. *See also* OIS Client

utilities, 194

V

variables, 119, 221-222

Veritas NetBackup IP, 293-294

version compatibility, 483

versioning policies, 228-229

versions

BladeLogic Operations Manager IP, 239

BMC Atrium CMDB IP, 242

BMC Event Manager IP, 244

BMC Patrol IP, 246

BMC Remedy AR System IP, 249

CA AutoSys IP, 251

CA eHealth IP, 253

CA Spectrum IP, 255

- CA Unicenter NSM IP, 257
- CA Unicenter Service Desk IP, 259
- EMC Smarts InCharge IP, 261
- HP Asset Manager IP, 263
- HP iLO and OA IP, 265
- HP Network Node Manager IP, 267
- HP OpenView Operations HPUX IP, 269
- HP OpenView Operations Solaris IP, 272
- HP OpenView Operations Windows IP, 274
- HP OpenView Service Desk IP, 277
- HP Service Manager IP, 279
- IBM Tivoli Enterprise Console IP, 281
- IBM Tivoli Netcool Omnibus IP, 283
- IBM Tivoli Storage Manager IP, 285
- Microsoft Active Directory 2 IP, 288
- OIS components, 488-489
- Unix IP, 291
- Veritas NetBackup IP, 294
- VMware vSphere IP, 297

viewing

- policy execution, 141-142
- policy logs, 133
- PTC logs, 130

Virtual Machine Manager. *See also* VMM IP

- OIS (Opalis Integration Server) integration with, 13
- product description, 12
- as VMM IP requirement, 348

virtual machine provisioning use case, VMM IP, 356-359, 386-391

virtualization, OIS (Opalis Integration Server) integration with, 13

VM checkpoint and recovery use case, VMM IP, 360-363

VMM IP

- configuring, 348-350
- objects, 351-355
- requirements, 347-348
- use cases, 355-366
  - capacity and lifecycle management, 363-366
  - virtual machine provisioning, 356-359, 386-391
  - VM checkpoint and recovery, 360-363

VMware vSphere IP, 295-297

W

Wait object, 189-190

watchdog services. *See* OpalisActionServerWatchdog

Web Services, multisite invoke via Web Services deployment model, 73-74

Web Services TerraServer Querying, Foundation objects use case, 197

websites for information, 495-501

Windows Event Scan with Query WMI, Foundation objects use case, 198-199

Windows Management Framework, as DPM IP requirement, 368

Windows PowerShell 2.0, as DPM IP requirement, 368

WinRM 2.0, as DPM IP requirement, 368

workflow control objects, 177-181

- Custom Start object, 178
- Junction object, 179-180
- Publish Policy Data object, 180-181
- Trigger Policy object, 178-179

workflow engines, OIS 5.0 to OIS 6.0, 19-20

workflows

- in dynamic data center, 382-383
- policies versus, 7
- use cases. *See* use cases

Workspace window (OIS Client), 120

Write To Database object, 194

Write Web Page object, 194

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